

# VMware NSX: Install, Configure, Manage [V4.0]

Lecture Manual

Copyright © 2022 VMware, Inc. All rights reserved. This manual and its accompanying materials are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware vSphere® vMotion®, VMware vSphere® Client™, VMware vSphere® 2015, VMware vSphere®, VMware vShield Endpoint™, VMware vCenter Server®, VMware vCenter®, VMware View®, VMware Horizon® View™, VMware Verify™, VMware vSphere® Distributed Switch™, VMware Pivotal Labs® Platform Deployment™, VMware Pivotal Labs® Navigator™, VMware NSX-T™, VMware NSX® Network Detection and Response™, VMware NSX® Manager™, VMware NSX® Gateway Firewall™, VMware NSX® Firewall for Bare Metal, VMware NSX® Firewall with Advanced Threat Prevention, VMware NSX® Firewall, VMware NSX® Edge™, VMware NSX® Distributed IDS/IPS™, VMware NSX® Distributed Firewall™, VMware NSX® Data Center Enterprise Plus, VMware NSX® Data Center, VMware NSX® Advanced Load Balancer Controller™, VMware NSX® Advanced Load Balancer™, VMware NSX® Advanced Load Balancer™ – Basic Edition, VMware NSX®, VMware NSX® Professional, VMware NSX® for Remote Office Branch Office, VMware NSX® for Desktop, VMware NSX® Enterprise Plus, VMware Go™, VMware ESXi™, and VMware ACE™ are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

The training material is provided “as is,” and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or noninfringement, are disclaimed, even if VMware, Inc., has been advised of the possibility of such claims. This material is designed to be used for reference purposes in conjunction with a training course.

The training material is not a standalone training tool. Use of the training material for self-study without class attendance is not recommended. These materials and the computer programs to which it relates are the property of, and embody trade secrets and confidential information proprietary to, VMware, Inc., and may not be reproduced, copied, disclosed, transferred, adapted or modified without the express written approval of VMware, Inc.



# Contents

Module 1	Course Introduction.....	1
1-2	Course Introduction .....	1
1-3	Importance .....	1
1-4	Learner Objectives.....	1
1-5	Course Outline .....	2
1-6	Typographical Conventions.....	3
1-7	References.....	3
1-8	VMware Online Resources.....	4
1-9	VMware Learning Overview.....	5
1-10	VMware Certification Overview.....	6
1-11	VMware Credentials Overview .....	7
Module 2	VMware Virtual Cloud Network and VMware NSX .....	9
2-2	Importance .....	9
2-3	Lesson 1: VMware Virtual Cloud Network and VMware NSX.....	10
2-4	Learner Objectives.....	10
2-5	Virtual Cloud Network Framework.....	11
2-6	NSX Portfolio.....	13
2-7	Product Name Changes to VMware NSX 4.x .....	15
2-8	Use Cases for NSX .....	15
2-9	NSX Features (1).....	16
2-10	NSX Features (2).....	16
2-11	NSX 4.0.0.1 Deprecated Features.....	17
2-12	High-Level Architecture of NSX .....	18
2-13	Management and Control Planes.....	19
2-14	About the NSX Management Cluster .....	20
2-15	NSX Management Cluster with Virtual IP Address.....	22

2-16	NSX Management Cluster with Load Balancer .....	23
2-17	About the NSX Policy.....	24
2-18	About NSX Manager .....	25
2-19	NSX Policy and NSX Manager Workflow .....	26
2-20	About NSX Controller.....	27
2-21	Control Plane Components (1).....	28
2-22	Control Plane Components (2).....	29
2-23	Control Plane Change Propagation .....	30
2-24	Control Plane Sharding Function .....	31
2-25	Managing Controller Failure .....	32
2-26	About the Data Plane .....	33
2-27	Data Plane Functions .....	33
2-28	Data Plane Components.....	34
2-29	Data Plane Communication Channels .....	35
2-30	Review of Learner Objectives.....	36
2-31	Key Points.....	36
<b>Module 3 Preparing the NSX Infrastructure .....</b>		<b>37</b>
3-2	Importance .....	37
3-3	Module Lessons.....	37
3-4	Lesson 1: Deploying the NSX Management Cluster .....	38
3-5	Learner Objectives.....	38
3-6	Implementing NSX in vSphere .....	38
3-7	Considerations for Deploying NSX Manager .....	39
3-8	NSX Manager Node Sizing .....	39
3-9	Deploying NSX Manager from an OVF Template.....	40
3-10	Methods to Access NSX Manager .....	41
3-11	Accessing the NSX UI.....	42
3-12	Accessing the NSX CLI .....	43
3-13	Accessing NSX Manager with API.....	45
3-14	Registering vCenter Server with NSX Manager .....	46
3-15	Verifying vCenter Server Registration with NSX Manager.....	47
3-16	Deploying Additional NSX Manager Instances (1) .....	47
3-17	Deploying Additional NSX Manager Instances (2) .....	48
3-18	Management Cluster Status: GUI (1).....	48
3-19	Management Cluster Status: GUI (2).....	49
3-20	Configuring the Virtual IP Address.....	50

3-21	Management Cluster Status: CLI (1) .....	51
3-22	Management Cluster Status: CLI (2) .....	52
3-23	Replacing Self-Signed Certificates (1) .....	53
3-24	Replacing Self-Signed Certificates (2) .....	54
3-25	Lab 1: Reviewing the Lab Environment and Topologies .....	55
3-26	Lab 2: Reviewing the Configuration of the Predeployed NSX Manager Instance .....	55
3-27	Lab 3: (Simulation) Deploying a Three-Node NSX Management Cluster .....	56
3-28	Review of Learner Objectives .....	56
3-29	Lesson 2: Navigating the NSX UI .....	57
3-30	Learner Objectives .....	57
3-31	NSX Manager Policy and Manager Views .....	57
3-32	User Interface Preferences for Policy and Manager Modes .....	58
3-33	About the Networking Tab .....	59
3-34	About the Security Tab .....	59
3-35	About the Inventory Tab .....	60
3-36	About the Plan & Troubleshoot Tab .....	61
3-37	About the System Tab .....	62
3-38	Review of Learner Objectives .....	62
3-39	Lesson 3: Preparing the Data Plane .....	63
3-40	Learner Objectives .....	63
3-41	Data Plane Components and Functions .....	64
3-42	Overview of the Transport Node .....	64
3-43	Transport Node Components and Architecture .....	65
3-44	Physical Connectivity of a Transport Node .....	66
3-45	About IP Address Pools .....	67
3-46	About Transport Zones (1) .....	68
3-47	About Transport Zones (2) .....	69
3-48	Transport Node Switch Configuration .....	70
3-49	About VDS .....	71
3-50	About N-VDS .....	72
3-51	Creating Transport Zones .....	73
3-52	Reviewing the Transport Zone Configuration .....	74
3-53	VDS Operational Modes .....	75
3-54	Physical NICs, LAGs, and Uplinks .....	77
3-55	About Uplink Profiles .....	78
3-56	Default Uplink Profiles .....	79

3-57	About Teaming Policies .....	80
3-58	Teaming Policy Modes .....	81
3-59	About LLDP .....	82
3-60	About Transport Node Profiles .....	83
3-61	Benefits of Transport Node Profiles .....	84
3-62	Prerequisites for Transport Node Profile .....	85
3-63	Creating a Transport Node Profile.....	85
3-64	Attaching a Transport Node Profile to the vSphere Cluster .....	86
3-65	Reviewing the ESXi Transport Node Status (1) .....	87
3-66	Reviewing the ESXi Transport Node Status (2) .....	88
3-67	Verifying the ESXi Transport Node by CLI.....	89
3-68	Lab 4: Preparing the NSX Infrastructure .....	90
3-69	Review of Learner Objectives.....	90
3-70	Lesson 4: DPU-Based Acceleration for VMware NSX.....	91
3-71	Learner Objectives.....	91
3-72	Traditional Infrastructure Challenges.....	92
3-73	Next-Generation Infrastructure with DPUs.....	93
3-74	DPU-Based Acceleration Use Cases .....	94
3-75	SmartNICs Ecosystem.....	95
3-76	Architecture Changes with DPUs.....	96
3-77	SmartNIC Hardware Components .....	97
3-78	Network Offloading with SmartNICs.....	98
3-79	Supported NSX Features.....	99
3-80	NSX Traffic Flow with DPUs.....	100
3-81	Networking Configurations: SmartNIC Only .....	101
3-82	Networking Configurations: SmartNIC with Standard NICs .....	102
3-83	Installing NSX with DPUs (1) .....	103
3-84	Installing NSX with DPUs (2) .....	104
3-85	Installing NSX with DPUs (3) .....	105
3-86	Installing NSX with DPUs (4) .....	106
3-87	Installing NSX with DPUs (5) .....	107
3-88	Installing NSX with DPUs (6) .....	108
3-89	Review of Learner Objectives.....	109
3-90	Key Points (1) .....	109
3-91	Key Points (2) .....	109

Module 4	NSX Logical Switching .....	111
4-2	Importance .....	111
4-3	Module Lessons.....	111
4-4	Lesson 1: Overview of Logical Switching Architecture.....	112
4-5	Learner Objectives.....	112
4-6	Use Cases for Logical Switching.....	113
4-7	Prerequisites for Logical Switching.....	114
4-8	Logical Switching Terminology.....	115
4-9	About Segments (1).....	116
4-10	About Segments (2).....	117
4-11	About Tunneling.....	118
4-12	About Geneve .....	119
4-13	Geneve Header Format .....	120
4-14	Logical Switching: End-to-End Communication.....	122
4-15	Review of Learner Objectives.....	123
4-16	Lesson 2: Configuring Segments .....	124
4-17	Learner Objectives.....	124
4-18	Segment Configuration Tasks .....	124
4-19	Creating Segments .....	125
4-20	Creating Segments Workflow .....	126
4-21	Viewing Configured Segments.....	127
4-22	Attaching a VM to a Segment .....	128
4-23	Workflow: Attaching a VM to a Segment (1).....	129
4-24	Workflow: Attaching a VM to a Segment (2).....	130
4-25	Verifying the Segment Port Status.....	131
4-26	About Network Topology .....	132
4-27	Using Network Topology to Validate the Segment Configuration.....	133
4-28	Review of Learner Objectives.....	133
4-29	Lesson 3: Configuring Segment Profiles.....	134
4-30	Learner Objectives.....	134
4-31	About Segment Profiles (1) .....	134
4-32	About Segment Profiles (2) .....	135
4-33	Default Segment Profiles.....	136
4-34	Applying Segment Profiles to Segments .....	136
4-35	Applying Segment Profiles to Segment Ports .....	137
4-36	SpoofGuard Segment Profile.....	138

4-37	Creating a SpoofGuard Segment Profile .....	139
4-38	IP Discovery Segment Profile.....	140
4-39	Creating an IP Discovery Segment Profile .....	141
4-40	MAC Discovery Segment Profile .....	142
4-41	Segment Security Profile.....	144
4-42	QoS Segment Profile .....	145
4-43	Review of Learner Objectives.....	146
4-44	Lesson 4: Logical Switching Packet Forwarding.....	147
4-45	Learner Objectives.....	147
4-46	NSX Controller Tables.....	148
4-47	TEP Table Update (1).....	148
4-48	TEP Table Update (2).....	149
4-49	TEP Table Update (3).....	150
4-50	TEP Table Update (4).....	151
4-51	MAC Table Update (1) .....	152
4-52	MAC Table Update (2) .....	153
4-53	MAC Table Update (3) .....	154
4-54	MAC Table Update (4).....	155
4-55	About the ARP Table .....	156
4-56	ARP Table Update (1) .....	156
4-57	ARP Table Update (2).....	157
4-58	ARP Table Update (3).....	158
4-59	ARP Table Update (4).....	159
4-60	Unicast Packet Forwarding Across Hosts (1) .....	160
4-61	Unicast Packet Forwarding Across Hosts (2) .....	161
4-62	Unicast Packet Forwarding Across Hosts (3) .....	162
4-63	Unicast Packet Forwarding Across Hosts (4) .....	163
4-64	Overview of BUM Traffic.....	164
4-65	Managing BUM Traffic: Head Replication.....	166
4-66	Managing BUM Traffic: Hierarchical Two-Tier Replication .....	167
4-67	Lab 5: Configuring Segments.....	168
4-68	Review of Learner Objectives.....	168
4-69	Key Points.....	169
<b>Module 5 NSX Logical Routing .....</b>		<b>171</b>
5-2	Importance .....	171
5-3	Module Lessons.....	171

5-4	Lesson 1: Overview of Logical Routing .....	172
5-5	Learner Objectives.....	172
5-6	Use Cases for Logical Routing.....	172
5-7	Prerequisites for Logical Routing.....	173
5-8	Logical Routing in NSX .....	174
5-9	Tier-0 and Tier-1 Gateways .....	176
5-10	Single-Tier Topology .....	177
5-11	Multitier Topology .....	178
5-12	Edge Nodes and Edge Clusters .....	179
5-13	Tier-0 Gateway Uplink Connections .....	180
5-14	Gateway Components: Distributed Router and Service Router (1) .....	181
5-15	Gateway Components: Distributed Router and Service Router (2) .....	182
5-16	Realization of Distributed Routers and Service Routers.....	183
5-17	Gateway Components in a Single-Tier Topology .....	184
5-18	Gateway Components in a Multitier Topology (1).....	185
5-19	Gateway Components in a Multitier Topology (2).....	186
5-20	Gateway Interfaces .....	187
5-21	Review of Learner Objectives.....	188
5-22	Lesson 2: NSX Edge and Edge Clusters.....	189
5-23	Learner Objectives.....	189
5-24	About the NSX Edge Node.....	190
5-25	About the NSX Edge Cluster .....	191
5-26	NSX Edge Node Form Factors .....	192
5-27	NSX Edge VM Sizing Options .....	193
5-28	Prerequisites for Deploying the NSX Edge Node VM.....	194
5-29	Deployment Considerations for NSX Edge Node VM Interfaces .....	195
5-30	Deploying the NSX Edge Node VM with Multiple N-VDS .....	196
5-31	Deploying the NSX Edge Node VM with a Single N-VDS.....	197
5-32	NSX Edge Node VM Network Offloading with SmartNICs .....	198
5-33	Requirements for the NSX Edge Bare-Metal Node.....	199
5-34	Prerequisites for Deploying the NSX Edge Bare-Metal Node.....	200
5-35	Deployment Methods for NSX Edge Nodes.....	200
5-36	Deploying NSX Edge Nodes from the NSX UI (1).....	201
5-37	Deploying NSX Edge Nodes from the NSX UI (2).....	202
5-38	Deploying NSX Edge Nodes from vCenter.....	203
5-39	Using PXE to Deploy NSX Edge Nodes from an ISO File .....	204

5-40	Installing NSX Edge on Bare Metal.....	205
5-41	Joining NSX Edge Bare Metal with the Management Plane.....	206
5-42	Verifying the Edge Transport Node Status.....	207
5-43	Changing the NSX Edge VM Resource Reservations .....	208
5-44	Changing Node Settings .....	209
5-45	Enabling UPT Mode on NSX Edge Node VMs .....	210
5-46	Postdeployment Verification Checklist .....	211
5-47	Creating an NSX Edge Cluster .....	212
5-48	Lab 6: Deploying and Configuring NSX Edge Nodes.....	213
5-49	Review of Learner Objectives.....	213
5-50	Lesson 3: Configuring Tier-0 and Tier-1 Gateways .....	214
5-51	Learner Objectives.....	214
5-52	Gateway Configuration Tasks .....	215
5-53	Creating the Tier-1 Gateway .....	216
5-54	Connecting Segments to the Tier-1 Gateway .....	217
5-55	Using Network Topology to Validate the Tier-1 Gateway Configuration .....	218
5-56	Testing East-West Connectivity.....	219
5-57	Creating the Uplink Segments.....	220
5-58	Creating the Tier-0 Gateway (1).....	221
5-59	Creating the Tier-0 Gateway (2).....	222
5-60	Configuring Routing .....	222
5-61	Connecting the Tier-1 and Tier-0 Gateways.....	223
5-62	Enabling Route Advertisement in the Tier-1 Gateway .....	224
5-63	Configuring Route Redistribution on the Tier-0 Gateway .....	225
5-64	Using Network Topology to Validate the Tier-0 Gateway Configuration.....	226
5-65	Testing North-South Connectivity .....	227
5-66	Lab 7: Configuring the Tier-1 Gateway .....	228
5-67	Review of Learner Objectives.....	228
5-68	Lesson 4: Configuring Static and Dynamic Routing.....	229
5-69	Learner Objectives.....	229
5-70	Static and Dynamic Routing.....	230
5-71	Tier-0 Gateway Routing Configurations (1).....	231
5-72	Tier-0 Gateway Routing Configurations (2).....	232
5-73	Configuring Static Routes on a Tier-0 Gateway (1).....	233
5-74	Configuring Static Routes on a Tier-0 Gateway (2).....	234
5-75	Configuring Dynamic Routing with BGP on Tier-0 Gateways (1).....	235



5-76	Configuring Dynamic Routing with BGP on Tier-0 Gateways (2) .....	236
5-77	Verifying the BGP Configuration of the Tier-0 Gateways.....	237
5-78	BGP Route Aggregation.....	238
5-79	Configuring Route Aggregation with BGP .....	239
5-80	Configuring Dynamic Routing with OSPF on Tier-0 Gateways (1) .....	240
5-81	Configuring Dynamic Routing with OSPF on Tier-0 Gateways (2) .....	241
5-82	Configuring Dynamic Routing with OSPF on Tier-0 Gateways (3) .....	242
5-83	Verifying OSPF Configuration of the Tier-0 Gateways.....	243
5-84	OSPF Route Summarization.....	244
5-85	Configuring Route Summarization with OSPF .....	245
5-86	Lab 8: Creating and Configuring a Tier-0 Gateway with OSPF .....	245
5-87	Lab 9: Configuring the Tier-0 Gateway with BGP .....	246
5-88	Review of Learner Objectives.....	246
5-89	Lesson 5: ECMP and High Availability.....	247
5-90	Learner Objectives.....	247
5-91	About Equal-Cost Multipath Routing.....	248
5-92	Enabling ECMP in BGP.....	249
5-93	Enabling ECMP in OSPF.....	249
5-94	About High Availability .....	250
5-95	Active-Active HA Mode .....	251
5-96	Active-Active Topology with BGP.....	252
5-97	Active-Active Topology with OSPF.....	253
5-98	Active-Standby HA Mode.....	254
5-99	Active-Standby Topology with BGP .....	255
5-100	Active-Standby Topology with OSPF .....	256
5-101	Failover Detection Mechanisms .....	257
5-102	About BFD .....	258
5-103	Failover Scenario with BFD .....	259
5-104	Failover Scenario with Dynamic Routing .....	260
5-105	Failover Modes .....	261
5-106	Review of Learner Objectives.....	261
5-107	Lesson 6: Logical Routing Packet Walk.....	262
5-108	Learner Objectives.....	262
5-109	Single-Tier Routing: Egress to Physical Network (1) .....	262
5-110	Single-Tier Routing: Egress to Physical Network (2) .....	263
5-111	Single-Tier Routing: Egress to Physical Network (3) .....	264

5-112	Single-Tier Routing: Egress to Physical Network (4) .....	265
5-113	Single-Tier Routing: Egress to Physical Network (5) .....	266
5-114	Single-Tier Routing: Egress to Physical Network (6) .....	267
5-115	Single-Tier Routing: Ingress from Physical Network (7) .....	268
5-116	Single-Tier Routing: Ingress from Physical Network (8) .....	269
5-117	Single-Tier Routing: Ingress from Physical Network (9) .....	270
5-118	Single-Tier Routing: Ingress from Physical Network (10) .....	271
5-119	Single-Tier Routing: Ingress from Physical Network (11) .....	272
5-120	Multitier Routing: Egress to Physical Network (1) .....	273
5-121	Multitier Routing: Egress to Physical Network (2) .....	274
5-122	Multitier Routing: Egress to Physical Network (3) .....	275
5-123	Multitier Routing: Egress to Physical Network (4) .....	276
5-124	Multitier Routing: Egress to Physical Network (5) .....	277
5-125	Multitier Routing: Egress to Physical Network (6) .....	278
5-126	Multitier Routing: Egress to Physical Network (7) .....	279
5-127	Multitier Routing: Egress to Physical Network (8) .....	280
5-128	Multitier Routing: Egress to Physical Network (9) .....	281
5-129	Multitier Routing: Ingress from Physical Network (10) .....	282
5-130	Multitier Routing: Ingress from Physical Network (11) .....	283
5-131	Multitier Routing: Ingress from Physical Network (12) .....	284
5-132	Multitier Routing: Ingress from Physical Network (13) .....	285
5-133	Multitier Routing: Ingress from Physical Network (14) .....	286
5-134	Multitier Routing: Ingress from Physical Network (15) .....	287
5-135	Multitier Routing: Ingress from Physical Network (16) .....	288
5-136	Review of Learner Objectives .....	288
5-137	Lesson 7: VRF Lite .....	289
5-138	Learner Objectives .....	289
5-139	About VRF Lite .....	290
5-140	VRF Lite Requirements and Limitations .....	291
5-141	Use Cases for VRF Lite .....	292
5-142	VRF Lite Topologies .....	293
5-143	VRF Lite Gateway Interfaces .....	294
5-144	VRF Lite: Control and Data Planes .....	295
5-145	Configuring VRF Lite .....	296
5-146	Deploying the Default Tier-0 Gateway .....	297
5-147	Adding Uplink Interfaces to the Default Tier-0 Gateway .....	298

5-148	Configuring BGP for the Default Tier-0 Gateway .....	299
5-149	Adding the Uplink Trunk Segment for the VRF Gateway .....	300
5-150	Deploying the VRF Gateway .....	301
5-151	Adding Uplink Interfaces to the VRF Gateway .....	302
5-152	Configuring the BGP for the VRF Gateway .....	303
5-153	Connecting a Tier-1 Gateway to the VRF Gateway .....	304
5-154	VRF Lite Validation .....	305
5-155	Lab 10: Configuring VRF Lite .....	306
5-156	Review of Learner Objectives .....	306
5-157	Key Points (1) .....	307
5-158	Key Points (2) .....	307
<b>Module 6 NSX Logical Bridging .....</b>		<b>309</b>
6-2	Importance .....	309
6-3	Lesson 1: NSX Logical Bridging .....	310
6-4	Learner Objectives .....	310
6-5	Overview of Logical Bridging .....	310
6-6	Logical Bridging Use Cases .....	311
6-7	Routing and Bridging for Physical-to-Virtual Communication .....	312
6-8	Example of Virtual-to-Physical Routing .....	314
6-9	Example of Virtual-to-Physical Bridging .....	315
6-10	Logical Bridging Components .....	316
6-11	Using Multiple Bridge Profiles .....	317
6-12	Creating an Edge Bridge Profile .....	318
6-13	Creating a Layer 2 Bridge-Backed Segment .....	319
6-14	Monitoring the Bridged Traffic Statistics .....	320
6-15	Review of Learner Objectives .....	321
6-16	Key Points .....	321
<b>Module 7 NSX Firewalls .....</b>		<b>323</b>
7-2	Importance .....	323
7-3	Module Lessons .....	323
7-4	Lesson 1: NSX Segmentation .....	324
7-5	Learner Objectives .....	324
7-6	Traditional Security Challenges .....	324
7-7	About Zero-Trust Security .....	325
7-8	About NSX Segmentation .....	326

7-9	Use Cases for NSX Segmentation .....	327
7-10	NSX Segmentation Benefits.....	328
7-11	Enforcing Zero-Trust with NSX Segmentation .....	329
7-12	Step 1: Creating Virtual Security Zones.....	330
7-13	Step 2: Identifying the Application Boundaries .....	331
7-14	Step 3: Implementing Micro-Segmentation.....	333
7-15	Step 4: Securing Through Context.....	334
7-16	Review of Learner Objectives.....	335
7-17	Lesson 2: NSX Distributed Firewall.....	336
7-18	Learner Objectives.....	336
7-19	NSX Firewalls.....	337
7-20	Features of the Distributed Firewall.....	338
7-21	Distributed Firewall: Key Concepts.....	339
7-22	Overview of a Security Policy .....	340
7-23	Distributed Firewall Policy Categories.....	341
7-24	About Distributed Firewall Policies.....	342
7-25	Distributed Firewall Rule Processing within a Policy .....	343
7-26	Applied To Field for the Policy.....	344
7-27	Configuring Distributed Firewall Policy Settings .....	345
7-28	Configuring Time-Based Firewall Policies.....	346
7-29	Creating Distributed Firewall Rules.....	347
7-30	Configuring Distributed Firewall Rule Parameters.....	348
7-31	Specifying Sources and Destinations for a Rule .....	349
7-32	Creating Groups.....	349
7-33	Adding Members and Member Criteria for a Group.....	350
7-34	Creating Groups Based on Tags.....	351
7-35	Specifying Services for a Rule.....	352
7-36	Adding a Context Profile to a Rule.....	353
7-37	Configuring Context Profile Attributes .....	354
7-38	Custom FQDN Filtering.....	355
7-39	Setting the Scope of Rule Enforcement.....	356
7-40	Specifying the Action for a Rule .....	357
7-41	Distributed Firewall Rule Settings.....	358
7-42	Blocking Malicious IPs in the Distributed Firewall.....	359
7-43	Enable or Disable Malicious IP Feeds .....	360
7-44	Default Malicious IP Group .....	361

7-45	Creating a Custom Malicious IP Group .....	362
7-46	Default Malicious IP Block Rules.....	363
7-47	Configuring Rules to Block Malicious IPs.....	363
7-48	Saving and Viewing the Distributed Firewall Configuration.....	364
7-49	Rolling Back to a Saved Distributed Firewall Configuration .....	365
7-50	Distributed Firewall Configuration Export and Import .....	366
7-51	Distributed Firewall Architecture .....	367
7-52	Distributed Firewall Architecture: ESXi .....	368
7-53	Distributed Firewall Rule Processing: ESXi.....	370
7-54	Lab 11: Configuring the NSX Distributed Firewall.....	371
7-55	Review of Learner Objectives.....	371
7-56	Lesson 3: Use Case for Security in Distributed Firewall on VDS.....	372
7-57	Learner Objectives.....	372
7-58	About Distributed Firewall on VDS.....	373
7-59	Supported Features .....	374
7-60	Distributed Firewall on VDS Requirements.....	375
7-61	Installation Workflow.....	376
7-62	Preparing the Cluster for Security .....	376
7-63	Validating the Security Cluster Preparation from the NSX UI .....	377
7-64	Transport Node Preparation.....	378
7-65	Autoconfigured Transport Node Profile.....	378
7-66	VLAN Transport Zones.....	379
7-67	Discovered Segments (1).....	380
7-68	Discovered Segments (2).....	381
7-69	Configuring Segment Profiles .....	382
7-70	Using VDS Attributes to Define NSX Groups.....	383
7-71	Review of Learner Objectives.....	383
7-72	Lesson 4: NSX Gateway Firewall.....	384
7-73	Learner Objectives.....	384
7-74	About the Gateway Firewall .....	385
7-75	Predefined Gateway Firewall Categories .....	387
7-76	Gateway Firewall Policy.....	388
7-77	Configuring Gateway Firewall Policy Settings.....	389
7-78	Configuring Gateway Firewall Rules.....	390
7-79	Configuring Gateway Firewall Rules Settings .....	391
7-80	Gateway Firewall Architecture.....	392

7-81	Gateway Firewall Rule Processing.....	393
7-82	Lab 12: Configuring the NSX Gateway Firewall.....	394
7-83	Review of Learner Objectives.....	394
7-84	Key Points.....	395
<b>Module 8 NSX Advanced Threat Prevention.....</b>		<b>397</b>
8-2	Importance .....	397
8-3	Module Lessons.....	397
8-4	Lesson 1: NSX Intrusion Detection and Prevention .....	398
8-5	Learner Objectives.....	398
8-6	About NSX Distributed IDS/IPS .....	399
8-7	Use Cases for NSX Distributed IDS/IPS.....	400
8-8	About Behavior-Based IDS/IPS.....	401
8-9	Requirements for NSX Distributed IDS/IPS .....	402
8-10	About IDS/IPS Signatures.....	403
8-11	About IDS/IPS Profiles.....	404
8-12	About IDS/IPS Policies and Rules .....	405
8-13	IDS/IPS Signature Curation .....	406
8-14	NSX Distributed IDS/IPS Architecture .....	407
8-15	Configuring NSX Distributed IDS/IPS .....	408
8-16	Configuring IDS/IPS Signatures .....	409
8-17	Global Intrusion Signature Management .....	410
8-18	Configuring Custom IDS/IPS Profiles.....	412
8-19	Configuring IDS/IPS Rules.....	413
8-20	Monitoring IDS/IPS Events (1) .....	414
8-21	Monitoring IDS/IPS Events (2) .....	415
8-22	About North-South IDS/IPS.....	416
8-23	Use Cases for North-South IDS/IPS .....	416
8-24	Requirements for Configuring North-South IDS/IPS .....	416
8-25	North-South IDS/IPS Architecture .....	417
8-26	Configuring North-South IDS/IPS.....	418
8-27	Configuring North-South IDS/IPS Rules .....	418
8-28	Monitoring North-South IDS/IPS Events.....	419
8-29	Lab 13: Configuring Distributed Intrusion Detection and Prevention .....	420
8-30	Review of Learner Objectives.....	420
8-31	Lesson 2: NSX Application Platform.....	421
8-32	Learner Objectives.....	421

8-33	About NSX Application Platform .....	421
8-34	Prerequisites for NSX Application Platform Deployment .....	422
8-35	Setting Up a Private Harbor Registry .....	423
8-36	NSX Application Platform Form Factors.....	424
8-37	NSX Application Platform Deployment (1).....	425
8-38	NSX Application Platform Deployment (2).....	426
8-39	NSX Application Platform Predeployment Checks .....	427
8-40	NSX Application Platform Deployment Validation.....	428
8-41	NSX Application Platform Services .....	429
8-42	Objects Created During the NSX Application Platform Deployment.....	431
8-43	Basic kubectl Commands.....	432
8-44	Namespaces Available After NSX Application Platform Deployment.....	433
8-45	Pods Available After NSX Application Platform Deployment .....	434
8-46	Lab 14: (Simulation) Deploying NSX Application Platform.....	435
8-47	Review of Learner Objectives.....	435
8-48	Lesson 3: NSX Malware Prevention.....	436
8-49	Learner Objectives.....	436
8-50	About Malware Prevention.....	437
8-51	About East-West Malware Prevention.....	439
8-52	Use Cases for East-West Malware Prevention.....	440
8-53	Requirements for East-West Malware Prevention .....	441
8-54	East-West Malware Prevention Architecture.....	442
8-55	NSX Application Platform Components .....	443
8-56	ESXi Host Components.....	445
8-57	East-West Malware Prevention Packet Flow for Known Files.....	447
8-58	East-West Malware Prevention Packet Flow for Unknown Files .....	448
8-59	Activating Malware Prevention on NSX Application Platform .....	449
8-60	Setting the Cloud Region.....	450
8-61	Validating the Malware Prevention Installation .....	451
8-62	Service Registration.....	452
8-63	Service Registration Validation from the NSX UI .....	452
8-64	Service Deployments.....	453
8-65	Service Deployment Validation from the NSX UI.....	454
8-66	Service Deployment Validation from vCenter Server .....	455
8-67	Creating East-West Malware Prevention Profiles .....	456
8-68	Creating Rules for East-West Malware Prevention.....	457

8-69	About North-South Malware Prevention .....	458
8-70	Use Cases for North-South Malware Prevention .....	459
8-71	Requirements for North-South Malware Prevention .....	460
8-72	North-South Malware Prevention Architecture .....	461
8-73	NSX Edge Components.....	462
8-74	North-South Malware Prevention Packet Flow for Known Files .....	463
8-75	North-South Malware Prevention Packet Flow for Unknown Files.....	464
8-76	Enabling Malware Prevention on Tier-1 Gateways.....	466
8-77	Creating North-South Malware Prevention Profiles.....	466
8-78	Creating Rules for North-South Malware Prevention .....	467
8-79	Malware Prevention Dashboard (1).....	468
8-80	Malware Prevention Dashboard (2).....	469
8-81	About the Allowlist .....	470
8-82	Lab 15: (Simulation) Configuring Malware Prevention for East-West Traffic.....	471
8-83	Review of Learner Objectives.....	471
8-84	Lesson 4: NSX Intelligence.....	472
8-85	Learner Objectives.....	472
8-86	About NSX Intelligence .....	473
8-87	Use Cases for NSX Intelligence.....	474
8-88	NSX Intelligence Requirements .....	474
8-89	NSX Intelligence Activation .....	475
8-90	Validating the NSX Intelligence Deployment.....	476
8-91	Granular Data Collection .....	477
8-92	NSX Intelligence Visualization (1).....	478
8-93	NSX Intelligence Visualization (2).....	479
8-94	NSX Intelligence Recommendations (1) .....	480
8-95	NSX Intelligence Recommendations (2) .....	481
8-96	NSX Intelligence Recommendations (3) .....	483
8-97	NSX Intelligence Recommendations (4) .....	484
8-98	NSX Suspicious Traffic Detection .....	485
8-99	Configuring Detector Definitions .....	487
8-100	Visualizing Detected Threats (1).....	488
8-101	Visualizing Detected Threats (2).....	489
8-102	Review of Learner Objectives.....	489
8-103	Lesson 5: NSX Network Detection and Response.....	490
8-104	Learner Objectives.....	490



8-105	About NSX Network Detection and Response .....	491
8-106	NSX Network Detection and Response Use Cases.....	492
8-107	NSX Network Detection and Response High-Level Architecture.....	493
8-108	NSX Network Detection and Response in NSX Deployments.....	494
8-109	NSX Network Detection and Response Architecture (1).....	495
8-110	NSX Network Detection and Response Architecture (2).....	496
8-111	NSX Network Detection and Response Requirements.....	498
8-112	NSX Network Detection and Response Activation (1).....	499
8-113	NSX Network Detection and Response Activation (2) .....	501
8-114	Validating the NSX Network Detection and Response and NSX Cloud Connector Deployments.....	502
8-115	Visualizing and Mitigating Attacks .....	503
8-116	Accessing the NSX Network Detection and Response UI .....	504
8-117	Campaign Overview: Active Threats and Attack Stages.....	505
8-118	Campaign Blueprint.....	505
8-119	Campaign Timeline .....	506
8-120	Reviewing Events.....	506
8-121	Lab 16: (Simulation) Using NSX Network Detection and Response to Detect Threats 507	
8-122	Review of Learner Objectives.....	507
8-123	Key Points (1).....	508
8-124	Key Points (2) .....	508
<b>Module 9 NSX Services .....</b>		<b>509</b>
9-2	Importance .....	509
9-3	Module Lessons.....	509
9-4	Lesson 1: Configuring NAT .....	510
9-5	Learner Objectives.....	510
9-6	About NAT .....	511
9-7	About SNAT.....	512
9-8	About DNAT .....	513
9-9	About Reflexive NAT .....	514
9-10	Configuring SNAT and DNAT .....	515
9-11	Configuring Reflexive NAT .....	517
9-12	Stateful Active-Active Services.....	519
9-13	Stateful Active-Active Interface Group.....	521
9-14	Stateful Active-Active SNAT .....	522

9-15	Stateful Active-Active Configuration.....	523
9-16	Configuring Interface Groups.....	524
9-17	Configuring Stateful SNAT and DNAT.....	525
9-18	About NAT64.....	526
9-19	Configuring NAT64 Rules.....	527
9-20	Lab 17: Configuring Network Address Translation.....	528
9-21	Review of Learner Objectives.....	528
9-22	Lesson 2: Configuring DHCP and DNS Services.....	529
9-23	Learner Objectives.....	529
9-24	About DHCP.....	530
9-25	About DHCP Relay.....	531
9-26	DHCP in NSX.....	531
9-27	DHCP Local Server.....	532
9-28	DHCP Relay.....	533
9-29	Gateway DHCP.....	534
9-30	DHCP Workflow.....	534
9-31	Creating a DHCP Profile.....	535
9-32	Assigning the DHCP Profile to a Segment.....	536
9-33	Assigning the DHCP Profile to a Gateway.....	537
9-34	Configuring DHCP Services.....	538
9-35	About DNS Services.....	539
9-36	About DNS Forwarder.....	540
9-37	DNS Workflow.....	540
9-38	Creating DNS Zones.....	541
9-39	Creating DNS Forwarder Services.....	542
9-40	Establishing Forwarder Connectivity.....	543
9-41	Configuring DHCP to Allocate DNS.....	544
9-42	Review of Learner Objectives.....	544
9-43	Lesson 3: Configuring NSX Advanced Load Balancer.....	545
9-44	Learner Objectives.....	545
9-45	About NSX Advanced Load Balancer.....	545
9-46	Benefits of NSX Advanced Load Balancer.....	546
9-47	NSX Advanced Load Balancer Feature Edition Comparison (1).....	547
9-48	NSX Advanced Load Balancer Feature Edition Comparison (2).....	548
9-49	NSX Advanced Load Balancer Architecture.....	549
9-50	NSX Advanced Load Balancer Deployment Workflow.....	550

9-51	NSX Advanced Load Balancer Consumption Workflow.....	551
9-52	Requirements for NSX Advanced Load Balancer.....	552
9-53	Deploying the NSX Advanced Load Balancer Controller Cluster.....	553
9-54	Service Engines Deployment and Connectivity.....	554
9-55	Creating a Cloud Connector (1).....	555
9-56	Creating a Cloud Connector (2).....	556
9-57	Creating a Service Engine Group.....	557
9-58	NSX Advanced Load Balancer Components.....	559
9-59	NSX Advanced Load Balancer Topologies.....	560
9-60	VIP Placement and Route Redistribution.....	561
9-61	North-South Traffic.....	562
9-62	East-West Traffic (1).....	563
9-63	East-West Traffic (2).....	564
9-64	Accessing the NSX Advanced Load Balancer UI.....	565
9-65	Creating a Virtual IP Address.....	566
9-66	Creating a Server Pool.....	567
9-67	Configuring Load-Balancing Algorithms.....	570
9-68	Configuring Health Monitor Profiles.....	571
9-69	Configuring Persistence Profiles.....	572
9-70	Configuring Server Pool Security Settings.....	573
9-71	Creating a Virtual Service.....	574
9-72	Validating Virtual Services and Server Pools.....	576
9-73	Lab 18: Configuring NSX Advanced Load Balancer.....	577
9-74	Review of Learner Objectives.....	577
9-75	Lesson 4: IPSec VPN.....	578
9-76	Learner Objectives.....	578
9-77	Use Cases for IPSec VPN.....	578
9-78	IPSec VPN Protocols and Algorithms.....	579
9-79	IPSec VPN Methods.....	580
9-80	IPSec VPN Modes.....	581
9-81	IPSec VPN Types.....	582
9-82	NSX IPSec VPN Deployment.....	583
9-83	IPSec VPN: High Availability.....	584
9-84	IPSec VPN Workflow.....	585
9-85	Configuring an IPSec VPN Service.....	586
9-86	Configuring DPD Profiles.....	587

9-87	Configuring IKE Profiles.....	588
9-88	Configuring IPsec Profiles.....	589
9-89	Adding a Local Endpoint.....	590
9-90	Configuring IPsec VPN Sessions.....	591
9-91	Configuring Policy-Based IPsec VPN Sessions (1) .....	592
9-92	Configuring Policy-Based IPsec VPN Sessions (2) .....	593
9-93	Configuring Route-Based IPsec VPN Sessions .....	594
9-94	Traceflow and Live Traffic Analysis Support for VPN .....	595
9-95	Review of Learner Objectives.....	596
9-96	Lesson 5: L2 VPN.....	597
9-97	Learner Objectives.....	597
9-98	About Layer 2 VPN.....	598
9-99	L2 VPN Architecture.....	599
9-100	L2 VPN Edge Packet Flow.....	600
9-101	L2 VPN Considerations .....	601
9-102	Recommended L2 VPN Clients.....	602
9-103	About Autonomous Edge .....	603
9-104	Sample L2 VPN Network Topology .....	604
9-105	L2 VPN Server Workflow .....	604
9-106	Configuring an IPsec VPN Service .....	605
9-107	Adding a Local Endpoint.....	606
9-108	Adding an L2 VPN Server Service .....	607
9-109	Adding an L2 VPN Server Session.....	608
9-110	Attaching Segments to the L2 VPN (1).....	609
9-111	Attaching Segments to the L2 VPN (2).....	610
9-112	L2 VPN Client Workflow .....	610
9-113	Configuring an L2 VPN Client Service .....	611
9-114	Adding an L2 VPN Client Session (1) .....	612
9-115	Adding an L2 VPN Client Session (2) .....	613
9-116	Attaching Segments to the L2 VPN Client.....	614
9-117	Lab 19: Deploying Virtual Private Networks.....	615
9-118	Review of Learner Objectives.....	615
9-119	Key Points (1) .....	616
9-120	Key Points (2) .....	616
<b>Module 10 NSX User and Role Management .....</b>		<b>617</b>
10-2	Importance .....	617

10-3	Module Lessons.....	617
10-4	Lesson 1: Integrating NSX with VMware Identity Manager.....	618
10-5	Learner Objectives.....	618
10-6	About VMware Identity Manager.....	619
10-7	Benefits of Integrating VMware Identity Manager with NSX.....	620
10-8	Prerequisites for VMware Identity Manager Integration.....	621
10-9	Configuring VMware Identity Manager.....	622
10-10	Overview of the VMware Identity Manager and NSX Integration.....	623
10-11	Creating an OAuth Client.....	623
10-12	Obtaining the SHA-256 Certificate Thumbprint.....	624
10-13	Configuring the VMware Identity Manager Details in NSX.....	625
10-14	Verifying the VMware Identity Manager Integration.....	626
10-15	Default UI Login.....	627
10-16	UI Login with VMware Identity Manager.....	628
10-17	Local Login with VMware Identity Manager.....	629
10-18	Review of Learner Objectives.....	629
10-19	Lesson 2: Integrating NSX with LDAP.....	630
10-20	Learner Objectives.....	630
10-21	About LDAP.....	630
10-22	Benefits of Integrating LDAP with NSX.....	631
10-23	Authentication with LDAP.....	631
10-24	Adding an Identity Source.....	632
10-25	Configuring the LDAP Server.....	633
10-26	UI Login with LDAP.....	634
10-27	Review of Learner Objectives.....	634
10-28	Lesson 3: Managing Users and Configuring RBAC.....	635
10-29	Learner Objectives.....	635
10-30	NSX Users.....	635
10-31	Activating Guest Users.....	636
10-32	Using Role-Based Access Control.....	637
10-33	Built-In Roles (1).....	638
10-34	Built-In Roles (2).....	638
10-35	Custom Role-Based Access Control.....	639
10-36	Creating Custom Roles (1).....	640
10-37	Creating Custom Roles (2).....	641
10-38	Multitenancy Hierarchy Model in NSX 4.0.1.....	642

10-39	Object-Based RBAC in a Multitenancy Environment .....	643
10-40	Role Assignment .....	644
10-41	Lab 20: Managing Users and Roles.....	645
10-42	Review of Learner Objectives.....	645
10-43	Key Points.....	645
<b>Module 11 NSX Federation.....</b>		<b>647</b>
11-2	Importance .....	647
11-3	Module Lessons.....	647
11-4	Lesson 1: Federation Architecture .....	648
11-5	Learner Objectives.....	648
11-6	About NSX Federation.....	649
11-7	NSX Federation Components: Global Manager .....	650
11-8	NSX Federation Components: Local Manager .....	650
11-9	NSX Federation Components: Global Manager and Local Manager Clusters .....	651
11-10	Federation Configuration Types.....	652
11-11	Ownership of Logical Configuration (1) .....	652
11-12	Ownership of Logical Configuration (2) .....	653
11-13	Infrastructure Ownership .....	654
11-14	Global Configuration .....	655
11-15	Local Configuration.....	656
11-16	Federation Configuration Example .....	657
11-17	Federation Configuration Example Workflow (1) .....	658
11-18	Federation Configuration Example Workflow (2) .....	659
11-19	Review of Learner Objectives.....	659
11-20	Lesson 2: Installing and Onboarding Federation .....	660
11-21	Learner Objectives.....	660
11-22	NSX Federation: Prerequisites .....	660
11-23	Onboarding Process.....	661
11-24	Active Global Manager Configuration.....	662
11-25	Adding Standby Global Manager (1).....	663
11-26	Adding Standby Global Manager (2).....	664
11-27	Adding a Location .....	665
11-28	Validating the Local Manager .....	666
11-29	Location Onboarding.....	667
11-30	Onboarding Preparation.....	669
11-31	Verifying Onboarding .....	670

11-32	Review of Learner Objectives.....	670
11-33	Lesson 3: Federation Networking.....	671
11-34	Learner Objectives.....	671
11-35	Stretched Networking (1).....	671
11-36	Stretched Networking (2).....	672
11-37	Tier-0 and Tier-1 Gateways: Logical Topologies (1).....	673
11-38	Tier-0 and Tier-1 Gateways: Logical Topologies (2).....	674
11-39	Tier-0 and Tier-1 Gateways: Logical Topologies (3).....	675
11-40	Single-Location Tier-0 Gateway Deployments.....	676
11-41	Single-Location Tier-1 Gateway Deployments.....	677
11-42	Multilocation Tier-0 and Tier-1 Gateway Deployments (1).....	678
11-43	Multilocation Tier-0 and Tier-1 Gateway Deployments (2).....	679
11-44	Multilocation T0-Stretched Gateway Modes (1).....	680
11-45	Multilocation T0-Stretched Gateway Modes (2).....	681
11-46	Multilocation T1-Stretched Gateway Modes (1).....	682
11-47	Multilocation T1-Stretched Gateway Modes (2).....	683
11-48	About RTEP.....	684
11-49	Stretched Layer-2 Network.....	685
11-50	Stretched L2: VNI Mapping.....	686
11-51	About Federation L2 Bridging.....	687
11-52	Components of Federation L2 Bridging.....	688
11-53	Federation L2 Bridge Communication.....	689
11-54	Federation Traceflow.....	690
11-55	Review of Learner Objectives.....	690
11-56	Lesson 4: Federation Security.....	691
11-57	Learner Objectives.....	691
11-58	Stretched Security in NSX Federation.....	692
11-59	Use Cases for Security.....	693
11-60	Security Configuration Workflow.....	694
11-61	About Regions.....	695
11-62	About Groups.....	696
11-63	GM Groups and Span Example (1).....	697
11-64	GM Groups and Span Example (2).....	698
11-65	Group Membership Criteria.....	699
11-66	Group Membership Based on the VM Tag (1).....	700
11-67	Group Membership Based on the VM Tag (2).....	701

11-68	About GM-Based Policy .....	702
11-69	About GM-Based Rules.....	703
11-70	Overlap of GM and LM Sections.....	704
11-71	GM DFW Management Enhancement.....	705
11-72	Global DFW Exclusion List Enhancement .....	706
11-73	Time-Based DFW Rules Enhancement .....	707
11-74	Review of Learner Objectives.....	708
11-75	Key Points.....	708



# Module 1

## Course Introduction

### 1-2 Course Introduction

### 1-3 Importance

NSX is the network virtualization and security platform that enables the virtual cloud network. The virtual cloud network is a software-defined approach to networking that extends across data centers, clouds, and application frameworks. An application might run on virtual machines, containers, or bare metal. NSX brings networking and security closer to the location where the application runs. The application framework that you create can support virtual machines running on ESXi hosts, containers, bare-metal servers, and public clouds.

In an NSX environment, you can select the technologies that best suit your applications. You can also perform your daily operational and management tasks with various tools supported by NSX.

### 1-4 Learner Objectives

- Describe the architecture and main components of NSX
- Explain the features and benefits of NSX
- Deploy the NSX Management cluster and NSX Edge nodes
- Prepare ESXi hosts to participate in NSX networking
- Create and configure segments for layer 2 forwarding
- Create and configure Tier-0 and Tier-1 gateways for logical routing
- Use distributed and gateway firewall policies to filter east-west and north-south traffic in NSX
- Configure Advanced Threat Prevention features
- Configure network services on NSX Edge nodes
- Use VMware Identity Manager and LDAP to manage users and access
- Explain the use cases, importance, and architecture of Federation

# 1-5 Course Outline

1. Course Introduction
2. VMware Virtual Cloud Network and VMware NSX
3. Preparing the NSX Infrastructure
4. NSX Logical Switching
5. NSX Logical Routing
6. NSX Logical Bridging
7. NSX Firewalls
8. NSX Advanced Threat Prevention
9. NSX Services
10. NSX User and Role Management
11. NSX Federation

## 1-6 Typographical Conventions

The following typographical conventions are used in this course.

Conventions	Usage and Examples
Monospace	Identifies command names, command options, parameters, code fragments, error messages, filenames, folder names, directory names, and path names: <ul style="list-style-type: none"><li>• Run the <code>esxtop</code> command.</li><li>• ... found in the <code>var/log/messages</code> file.</li></ul>
<b>Monospace Bold</b>	Identifies user inputs: <ul style="list-style-type: none"><li>• Enter <b><code>ipconfig /release</code></b>.</li></ul>
<b>Boldface</b>	Identifies user interface controls: <ul style="list-style-type: none"><li>• Click the <b>Configuration</b> tab.</li></ul>
<i>Italic</i>	Identifies book titles: <ul style="list-style-type: none"><li>• <i>vSphere Virtual Machine Administration</i></li></ul>
< >	Indicates placeholder variables: <ul style="list-style-type: none"><li>• &lt;ESXi_host_name&gt;</li><li>• ... the Settings/&lt;Your_Name&gt;.txt file</li></ul>

## 1-7 References

Title	Location
<i>NSX Administration Guide</i>	<a href="https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-FBFD577B-745C-4658-B713-A3016D18CB9A.html">https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-FBFD577B-745C-4658-B713-A3016D18CB9A.html</a>
<i>NSX Installation Guide</i>	<a href="https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-3E0C4CEC-D593-4395-84C4-150CD6285963.html">https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-3E0C4CEC-D593-4395-84C4-150CD6285963.html</a>
<i>NSX Upgrade Guide</i>	<a href="https://docs.vmware.com/en/VMware-NSX/4.0/upgrade/GUID-E04242D7-EF09-4601-8906-3FA77FBB06BD.html">https://docs.vmware.com/en/VMware-NSX/4.0/upgrade/GUID-E04242D7-EF09-4601-8906-3FA77FBB06BD.html</a>

## 1-8 VMware Online Resources

Documentation for NSX: <https://docs.vmware.com/en/VMware-NSX/index.html>

Documentation for VMware Validated Solutions: <https://core.vmware.com/vmware-validated-solutions>.

VMware Communities: <http://communities.vmware.com>

- Start a discussion.
- Access the knowledge base.
- Access documentation, technical papers, and compatibility guides.
- Access communities.
- Access user groups.

VMware Support: <http://www.vmware.com/support>

VMware Hands-on Labs: <http://labs.hol.vmware.com>

VMware Learning: <http://www.vmware.com/learning>

- Access course catalog.
- Access worldwide course schedule.

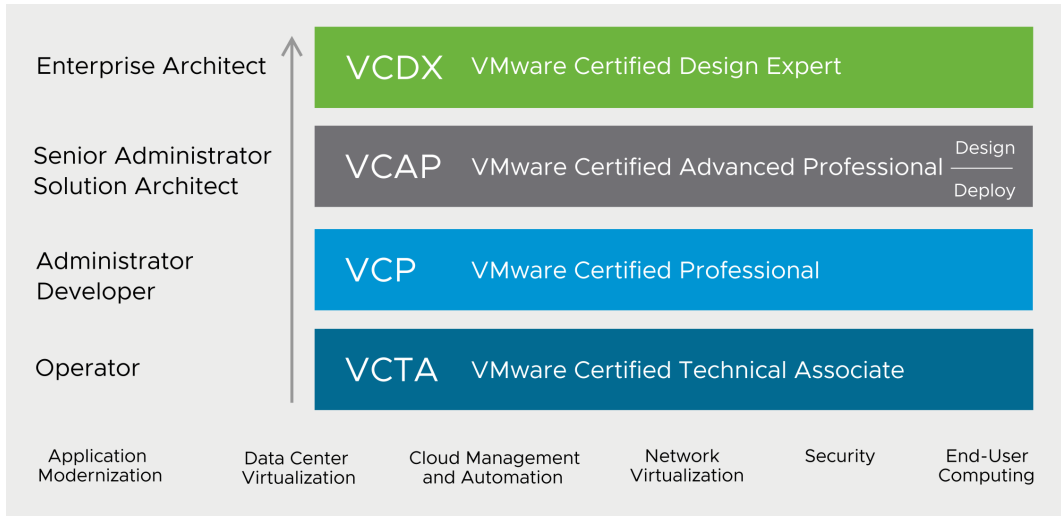
# 1-9 VMware Learning Overview

You can access the following Education Services:

- VMware Learning Paths:
  - Help you find the course that you need based on the product, your role, and your level of experience
  - Can be accessed at <https://vmware.com/learning>
- VMware Customer Connect Learning, which is the official source of digital training, includes the following options:
  - On Demand Courses: Self-paced learning that combines lecture modules with hands-on practice labs
  - VMware Lab Connect: Self-paced, technical lab environment where you can practice skills learned during instructor-led training
  - Certification Exam Prep: Comprehensive video-based reviews of exam topics and objectives to help you take your certification exam
- For more information, see <https://vmware.com/learning/connect-learning>.

## 1-10 VMware Certification Overview

VMware certifications validate your expertise and recognize your technical knowledge and skills with VMware technology.



VMware certification sets the standards for IT professionals who work with VMware technology. Certifications are grouped into technology tracks. Each track offers one or more levels of certification (up to four levels).

For the complete list of certifications and details about how to attain these certifications, see <https://vmware.com/certification>.

## 1-11 VMware Credentials Overview

VMware badges are digital emblems of skills and achievements. Career certifications align to job roles and validate expertise across a solution domain. Certifications can cover multiple products in the same certification.



Specialist certifications and skills badges align to products and verticals and show expanded expertise.



Digital badges have the following features:

- Easy to share in social media (LinkedIn, Twitter, Facebook, blogs, and so on)
- Validate and verify achievement
- Contain metadata with skill tags and accomplishments
- Based on Mozilla's Open Badges standard

For the complete list of digital badges, see <http://www.pearsonvue.com/vmware/badging>.





## Module 2

# VMware Virtual Cloud Network and VMware NSX

## 2-2 Importance

As a network administrator, you must understand the VMware Virtual Cloud Network framework and the solutions that it offers for addressing challenges in your data center. You must also understand the VMware NSX architecture and components so that you can properly design, deploy, and manage a data center that meets your business requirements.

## 2-3 Lesson 1: VMware Virtual Cloud Network and VMware NSX

### 2-4 Learner Objectives

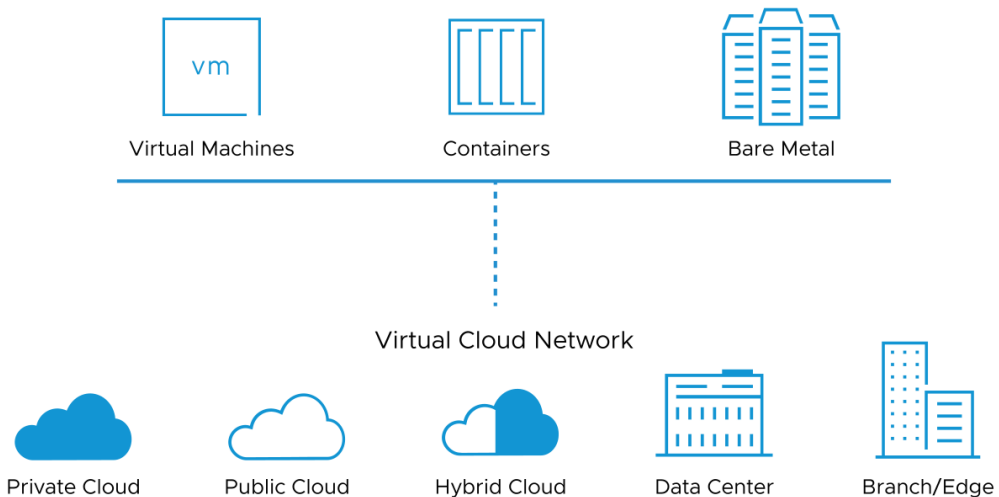
- Describe the purpose of VMware Virtual Cloud Network and its framework
- Identify the benefits and recognize the use cases for NSX
- Describe how VMware NSX fits into the NSX product portfolio
- Recognize features and the main elements in the NSX architecture
- Enumerate the deprecated features in NSX 4.0.x
- Describe the NSX policy and centralized policy management
- Describe the NSX management cluster and the management plane
- Identify the functions of control plane components, data plane components, and communication channels

## 2-5 Virtual Cloud Network Framework

Virtual Cloud Network is the VMware framework for connecting and protecting different types of workloads running across various environments.

The Virtual Cloud Network framework is built on the NSX technology.

Virtual Cloud Network is a software layer. This layer provides connectivity between data center, cloud, and edge infrastructure with data visibility and security.



Virtual Cloud Network connects and protects applications and data, regardless of their physical locations. Virtual Cloud Network also connects and protects workloads running across any environment. Workloads might be running on premises in a customer data center, in a branch, or in a public cloud such as Amazon AWS or Microsoft Azure.

Virtual Cloud Network enables organizations to embrace cloud networking as the software-defined architecture for connecting components in a distributed world.

Virtual Cloud Network is a ubiquitous software layer that provides maximum visibility into, and context for, the interaction among various users, applications, and data. NSX supports various types of endpoints.

The VMware software-based approach delivers a networking and security platform that enables customers to connect, secure, and operate an end-to-end architecture to deliver services to applications.

The VMware software-based approach provides the following benefits:

- Enables you to design and build the next-generation policy-driven data center.

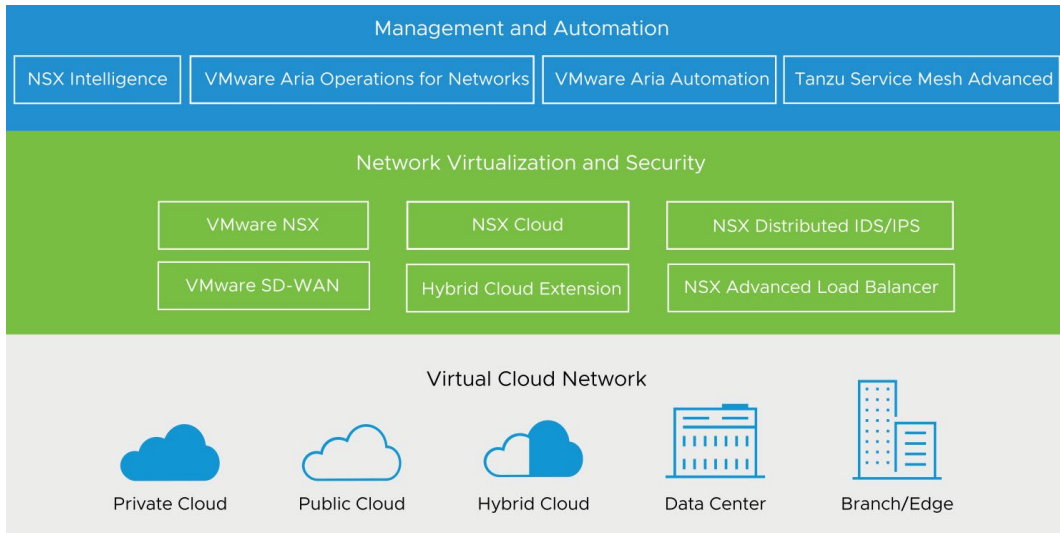
This data center connects, secures, and automates traditional hypervisors and new microservices-based (container) applications across a range of deployment targets such as the data center, cloud, and so on.

- Embeds security in the platform by compartmentalizing the network through micro-segmentation, encrypting in-flight data, and automatically detecting and responding to security threats.
- Delivers a WAN solution that provides full visibility, metrics, control, and automation of all endpoints.

## 2-6 NSX Portfolio

NSX provides consistent networking and security across the entire IT environment.

Virtual Cloud Network is based on a robust portfolio of products built on the foundations of the concept of any infrastructure, any cloud, any application, any platform, and any device. Virtual Cloud Network includes several key solutions that provide security, integration, extensibility, automation, and elasticity.



VMware Virtual Cloud Network enables you to run your applications everywhere.

NSX supports cloud-native applications, bare-metal workloads, ESXi hypervisors, public clouds, and multiple clouds.

You can bring key capabilities from one central control point to wherever your applications run.

Network virtualization and security includes the following solutions:

- NSX is the industry's only complete layer 2 to layer 7 software-defined networking stack, including networking, load balancing, security, and analytics. With NSX, you can provision networking and security services across ESXi hypervisors and bare-metal servers.
- NSX Cloud extends the networking and security capabilities of NSX to the public cloud. You can provide your workloads running natively on Amazon AWS or Microsoft Azure with consistent networking and security policies, helping you improve scalability, control, and visibility.
- NSX Distributed IDS/IPS is an advanced threat detection engine built to detect lateral threat movement on east-west network traffic across multicloud environments.

- NSX Advanced Load Balancer enables you to deliver multicloud application services such as load balancing, application, security, autoscaling, container networking, and web application firewall.
- VMware SD-WAN virtualizes WAN connections to deliver high-performance, reliable branch access to cloud services, private data centers, and SaaS-based enterprise applications.
- VMware HCX makes it easy to migrate thousands of virtual machines within and across data centers or clouds, without requiring a reboot.

The NSX portfolio supports management and automation tools:

- NSX Intelligence is a distributed analytics solution that provides visibility and dynamic security policy enforcement for NSX environments. NSX Intelligence enables network and application security teams to deliver a granular security posture, simplify compliance analysis, and enable proactive security. It also supports network traffic analysis to help identify advanced threats in the environment.
- VMware Aria Operations for Networks (former name: VMware vRealize Network Insight) provides visibility across virtual and physical networks. It helps with operations management for NSX and NSX Cloud.
- VMware Aria Automation (former name: vRealize Automation) is the VMware infrastructure automation platform for the modern software-defined data center. When used with NSX, it automates an application's network connectivity, security, performance, and availability.
- Tanzu Service Mesh Advanced, built on VMware NSX, is the VMware enterprise-class service mesh solution that provides consistent control and security for microservices, end users, and data across the most demanding multicluster and multicloud environments.

## 2-7 Product Name Changes to VMware NSX 4.x

NSX-T Data Center is now called NSX.



The new name better reflects the multifaceted value that NSX brings to customers. The update is apparent in the product graphical user interface as well as documentation. The change neither affects the functionality of the product nor changes the API to affect compatibility with previous releases.

## 2-8 Use Cases for NSX

NSX can be used in several ways.



Security



Multicloud  
Networking



Automation



Cloud-Native  
Applications

You can use NSX for the following purposes:

- Security: Delivers application-centric security at the workload level to prevent the lateral spread of threats
- Multicloud networking: Brings consistency in networking and security across varied sites and streamlines multicloud operations
- Automation: Enables faster deployment through automation by reducing manual, error-prone tasks
- Cloud-native applications: Enables native networking and security for containerized workloads across application frameworks

## 2-9 NSX Features (1)

Platform	Networking	Security and Services
<ul style="list-style-type: none"><li>• Policy-driven configuration</li><li>• Bare-metal server support</li><li>• Support for VMs and containers</li><li>• Support for Amazon AWS and Microsoft Azure instances</li><li>• HTML 5 UI for management plane</li><li>• Data Plane Development Kit (DPDK)-based NSX Edge nodes: VM or bare-metal form factor</li><li>• Multisite/Federation</li><li>• V2T migration</li><li>• DPU-Based Acceleration</li></ul>	<ul style="list-style-type: none"><li>• Overlay or VLAN-backed logical switching</li><li>• Layer 2 bridging and QoS</li><li>• Distributed routing</li><li>• Static routing and equal-cost multipath (ECMP) routing</li><li>• BGP and OSPF support</li><li>• Duplicate IP detection</li><li>• Bidirectional Forwarding (BFD) for fast convergence</li><li>• VRF Lite and EVPN</li><li>• Rate limiting</li><li>• Layer 3 multicast</li></ul>	<ul style="list-style-type: none"><li>• Gateway firewall</li><li>• Distributed firewall</li><li>• IDPS</li><li>• Malware Prevention</li><li>• URL Filtering and FQDN Analysis</li><li>• TLS Inspection</li><li>• NSX Intelligence</li><li>• NSX Network Detection and Response</li><li>• NAT and NAT64</li><li>• DNS and DHCP</li><li>• Load Balancing</li><li>• L2 VPN and IPsec VPN</li></ul>

## 2-10 NSX Features (2)

Automation	Operations	Troubleshooting
<ul style="list-style-type: none"><li>• REST/JSON API support</li><li>• Upstream OpenStack support and partner ecosystem</li><li>• Tag-based security grouping</li><li>• Inventory support</li><li>• Management Plane to Policy Promotion Tool</li></ul>	<ul style="list-style-type: none"><li>• Getting Started wizards</li><li>• Dashboards</li><li>• Role-based access control</li><li>• Object-based access control</li><li>• Upgrade coordinator</li><li>• Backup and restore</li><li>• vRealize Log Insight</li></ul>	<ul style="list-style-type: none"><li>• IP Flow Information Export (IPFIX)</li><li>• Port mirroring</li><li>• Traceflow</li><li>• Network Topology views</li><li>• Selective technical support logs</li><li>• Monitoring Dashboard and statistics</li><li>• Alarms</li></ul>



## 2-11 NSX 4.0.0.1 Deprecated Features

The following NSX features are deprecated in NSX 4.0.0.1:

- N-VDS host switch
- KVM hypervisor
- NSX Advanced Load Balancer Policy API and UI

Since NSX 4.0.0.1, N-VDS host switch will not be supported for ESXi hosts. In a brownfield environment, you must migrate the ESXi hosts to VDS before upgrading to NSX 4.0.0.1.

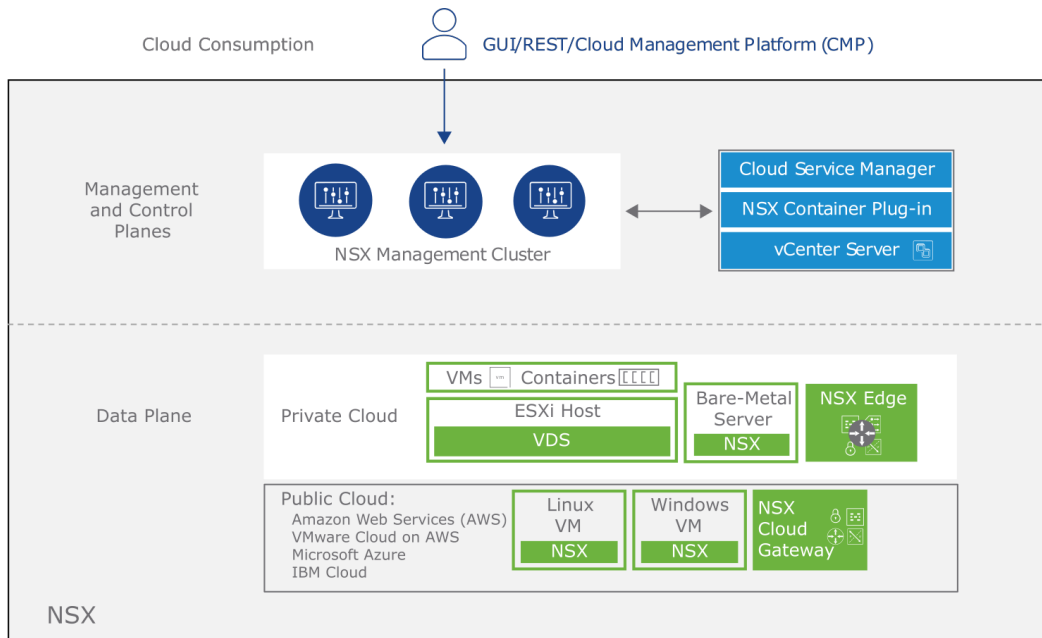
N-VDS will remain the supported virtual switch on NSX Edge nodes, native public cloud NSX agents, and bare-metal workloads.

NSX 4.0.0.1 no longer supports KVM-based hypervisors. In a brownfield environment, you must remove the KVM transport nodes from NSX before upgrade.

NSX Advanced Load Balancer UI and Policy API are deprecated from NSX 4.0.0.1. All configuration tasks for load balancers integrated with NSX environments should be performed directly through the NSX Advanced Load Balancer UI and API. For all orchestration integrations use cases, use the NSX Advanced Load Balancer API or UI.

## 2-12 High-Level Architecture of NSX

The three main elements of NSX architecture are the management, control, and data planes. This architectural separation enables scalability without affecting workloads.



Each plane has its own components:

- **Management plane:** The management plane is designed with advanced clustering technology, which allows the platform to process large-scale concurrent API requests. NSX Manager provides the REST API and a web-based UI interface entry point for all user configurations.
- **Control plane:** The control plane manages computing and distributing the runtime virtual networking and security state of the NSX environment. The control plane includes a central control plane (CCP) and a local control plane (LCP). This separation significantly simplifies the work of the CCP and enables the platform to extend and scale for various endpoints. The management plane and control plane are converged. Each manager node in NSX is an appliance with converged functions, including management, control, and policy.

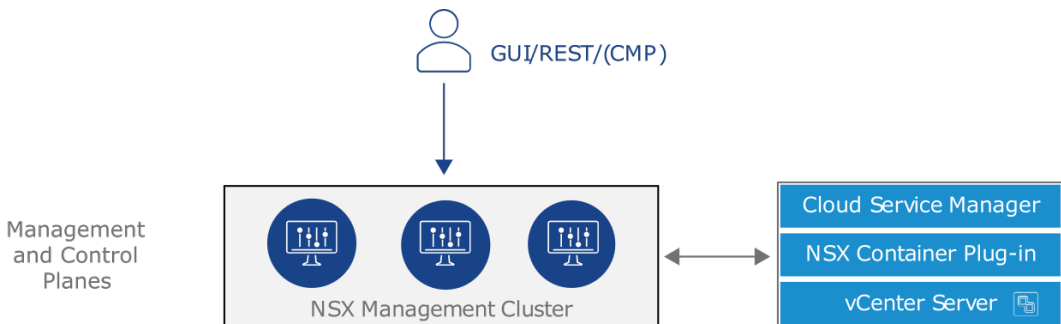
- Data plane: The data plane includes a group of ESXi hosts and NSX Edge nodes. The group of servers and edge nodes prepared for NSX are called transport nodes. Transport nodes manage the distributed forwarding of network traffic. The ESXi hosts managed by vCenter Server use vSphere Distributed Switch (VDS) for the traffic forwarding.
- Consumption plane: Although the consumption plane is not part of NSX, it provides integration into any CMP through the REST API and integration with VMware cloud management planes, such as vRealize Automation:
  - The consumption of NSX can be driven directly through the NSX UI.
  - Typically, end users tie network virtualization to their cloud management plane for deploying applications.
  - Integration is also available through OpenStack (Red Hat, VMware Integrated OpenStack, and so on), Kubernetes, and Tanzu Application Service.

The management plane performs all operations. These operations include create, read, update, and delete (CRUD).

## 2-13 Management and Control Planes

In NSX, the management plane and control plane are part of a single NSX management cluster:

- The management plane provides the REST API and web-based UI interface for all user configurations.
- The control plane manages computing and distributing the network runtime state.



## 2-14 About the NSX Management Cluster

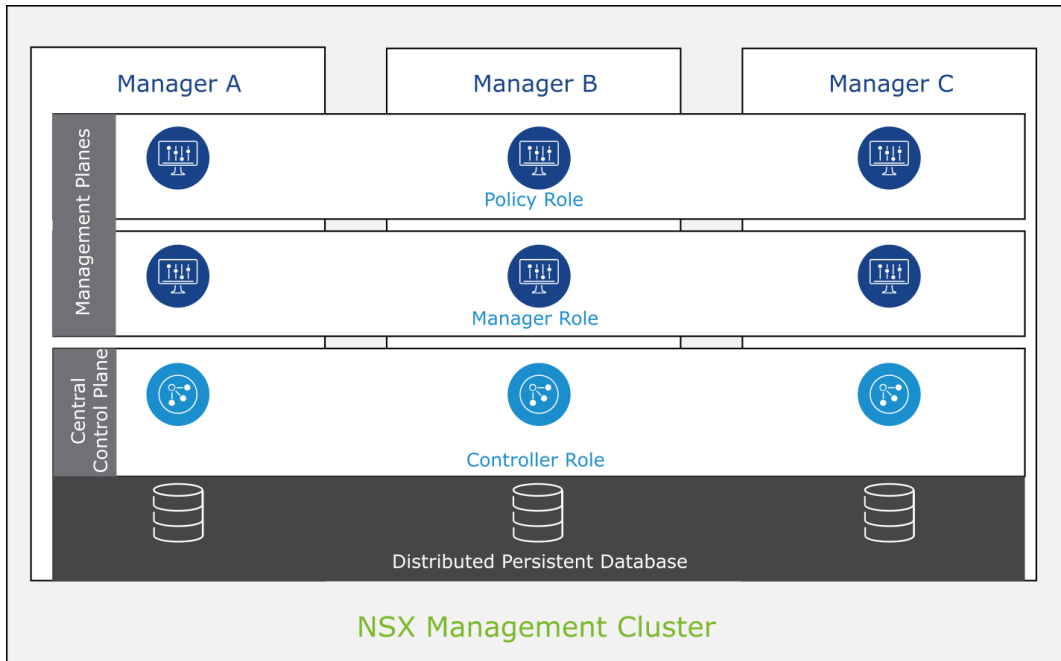
The NSX management cluster is formed by a group of three NSX Manager nodes for high availability and scalability.

The NSX Manager appliance has the built-in policy, manager, and controller roles:

- The management plane includes the policy and manager roles.
- The central control plane (CCP) includes the controller role.

The desired state is replicated in the distributed persistent database, providing the same configuration view to all nodes in the cluster.

The NSX Manager appliance is available in different sizes for different deployment scenarios.



NSX Manager is a standalone appliance. It includes the manager, controller, and policy roles. As a result of this integrated approach, users do not need to install the manager, controller, and policy roles as separate VMs.

The diagram shows that the manager and controller instances run on all three nodes and provide resiliency. Three manager nodes can handle requests from users through the API or UI, resulting in shared workloads and efficiency.

Although the three services are merged on each node in the cluster, separate resources (CPU, memory, and so on) are allocated for each of the services.

The distributed persistent database runs across all three nodes, providing the same configuration view to each node. A manager or controller running on one node has the same view of the configuration topology as managers or controllers running on the other two nodes.

NSX Manager is available in different sizes for different deployment scenarios:

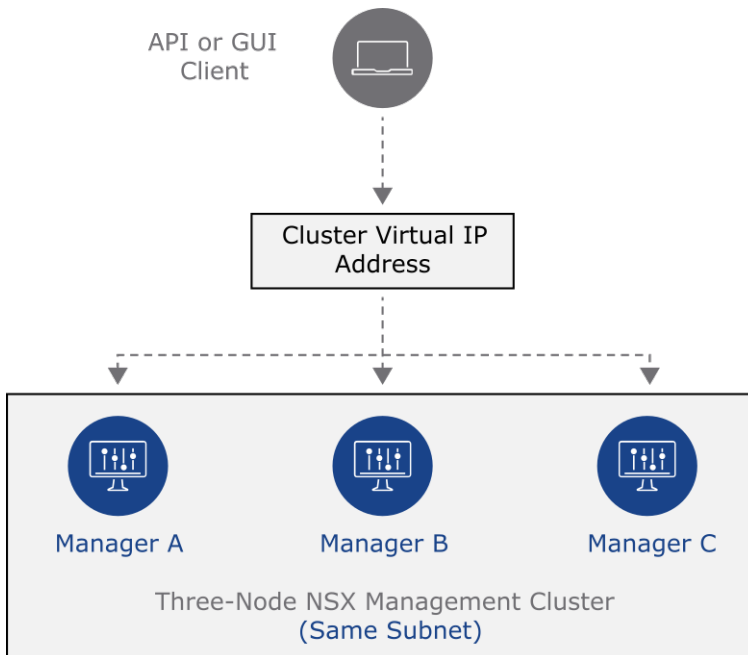
- A small appliance for lab or proof-of-concept deployments
- A medium appliance for deployments up to 64 hosts
- A large appliance for customers who deploy to a large-scale environment

For information, see VMware Configuration Maximums at <https://configmax.vmware.com>.

## 2-15 NSX Management Cluster with Virtual IP Address

The NSX management cluster is highly available. It is configured in the following way:

- All managers must be on the same subnet.
- One manager node is elected as the leader.
- The cluster's virtual IP address is attached to the leader manager.
- Traffic is not load balanced across the managers while using VIP.
- The cluster virtual IP address is used for traffic destined for NSX Manager nodes.
- Traffic destined for any transport node uses the management IP of the node.
- A single virtual IP address is used for API and GUI client access.



The API and GUI are available on all three manager nodes in the cluster. When a user request is sent to the virtual IP address, the active manager (the leader that has the virtual IP address attached) responds to the request. If the leader fails, the two remaining managers elect a new leader. The new leader responds to the requests sent to that virtual IP address.

Load-balancing requests and traffic are not balanced across managers while using VIP.

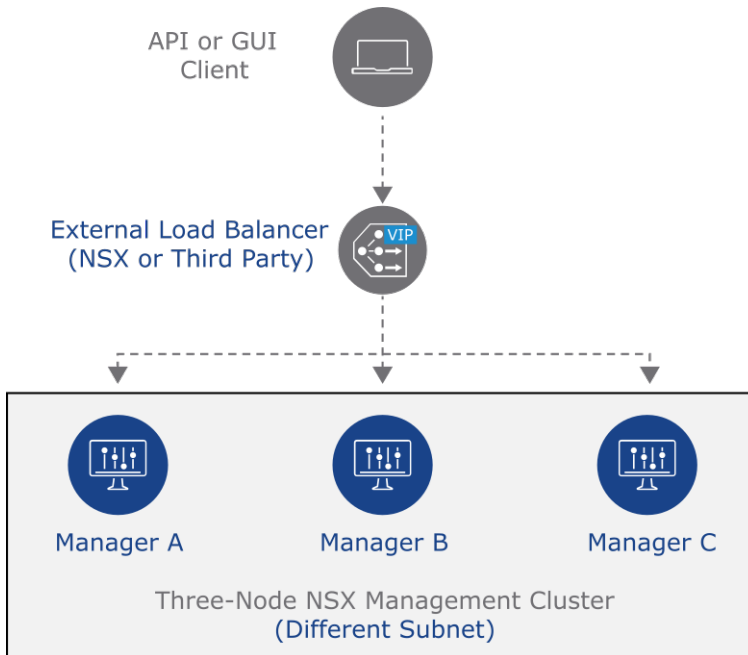
If the leader node that owns VIP fails, a new leader is elected. The new leader sends a GARP request to take the ownership of the VIP. The new leader node then receives all new API and UI requests from users.

The diagram shows an administrator's perspective, where a single IP address (the virtual IP address) is always used to access the NSX management cluster.

## 2-16 NSX Management Cluster with Load Balancer

A load balancer provides high availability to the NSX management cluster:

- All nodes are active.
- GUI and API are available on all managers.
- Traffic to the virtual IP address is load balanced to multiple manager nodes.
- The manager nodes can be in different subnets.

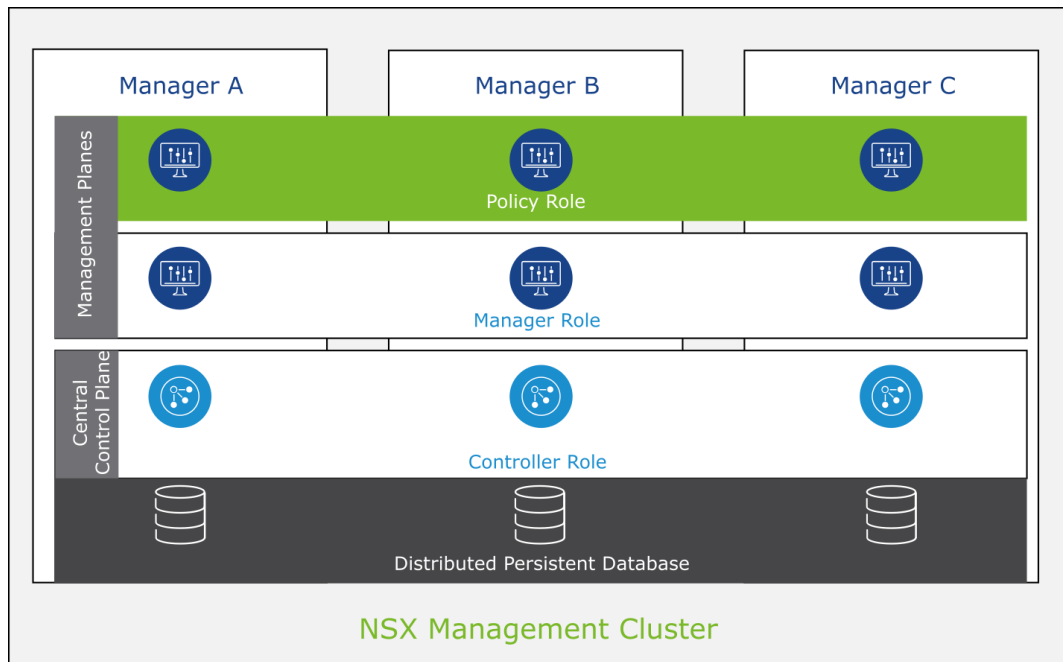


The diagram shows how a traditional load balancer can balance the traffic across multiple manager nodes.

## 2-17 About the NSX Policy

The policy role performs several functions:

- Provides a centralized location for configuring networking and security across the environment
- Enables users to enter the intended configuration in the NSX UI
- Enables users to specify the final desired state of the system without being concerned about the current state or underlying implementation

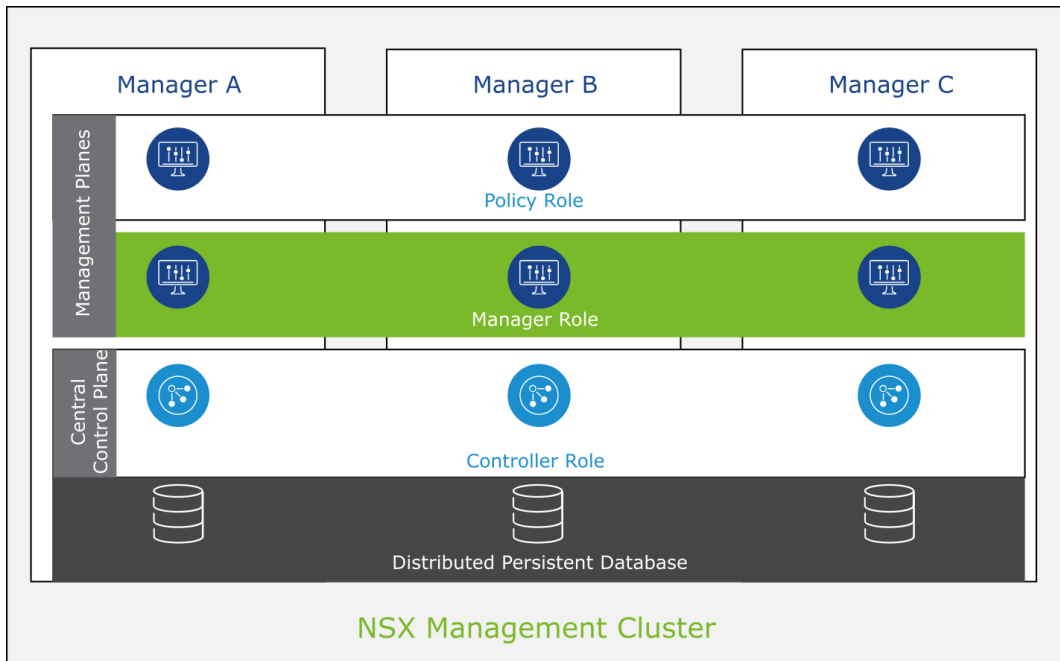




## 2-18 About NSX Manager

NSX Manager performs several functions:

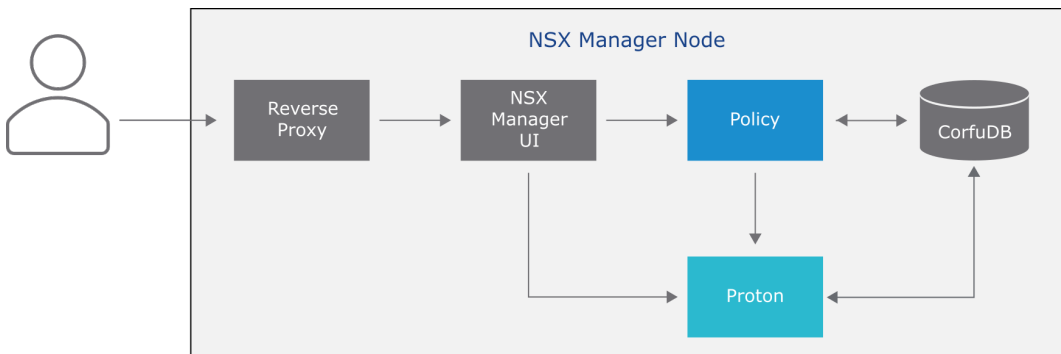
- Installs and prepares the data plane components
- Receives and validates the configuration from NSX policy
- Publishes the configuration to the CCP
- Retrieves the statistical data from the data plane components



## 2-19 NSX Policy and NSX Manager Workflow

The components of an NSX Manager node interact with each other:

- Reverse proxy is the entry point to NSX Manager.
- The policy role manages all networking and security policies and enforces them in the manager role.
- Proton is the core component of the NSX Manager node. Proton manages various functionalities such as logical switching, logical routing, distributed firewall.
- Both NSX policy and Proton persist data in CorfuDB.



Reverse proxy has authentication and authorization capabilities.

NSX Policy Manager and Proton are internal web applications that communicate with each other through HTTP.

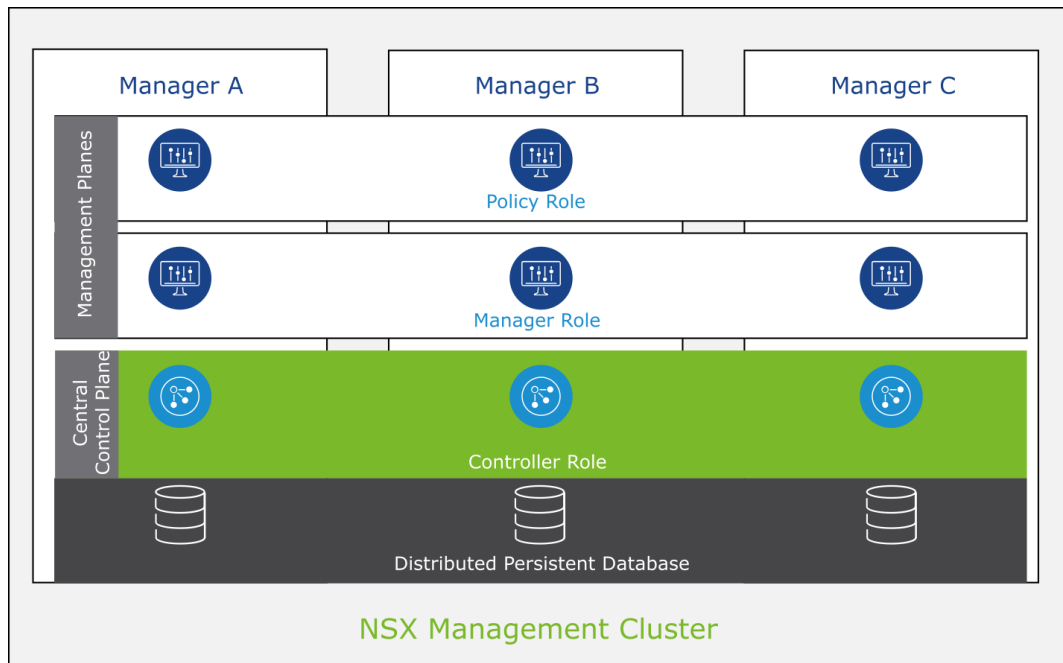
CorfuDB is a distributed persistent in-memory object store. Persistence is achieved by writing each transaction in a shared transaction log file. Queries are served from memory and provide better performance and scalability.

## 2-20 About NSX Controller

NSX Controller maintains the realized state of the system and configures the data plane.

The main functions of NSX Controller include:

- Providing control plane functionality, such as logical switching, routing, and distributed firewall
- Computing all ephemeral runtime states based on the configuration from the management plane
- Disseminating topology information reported by the data plane elements
- Pushing stateless configurations to forwarding engines

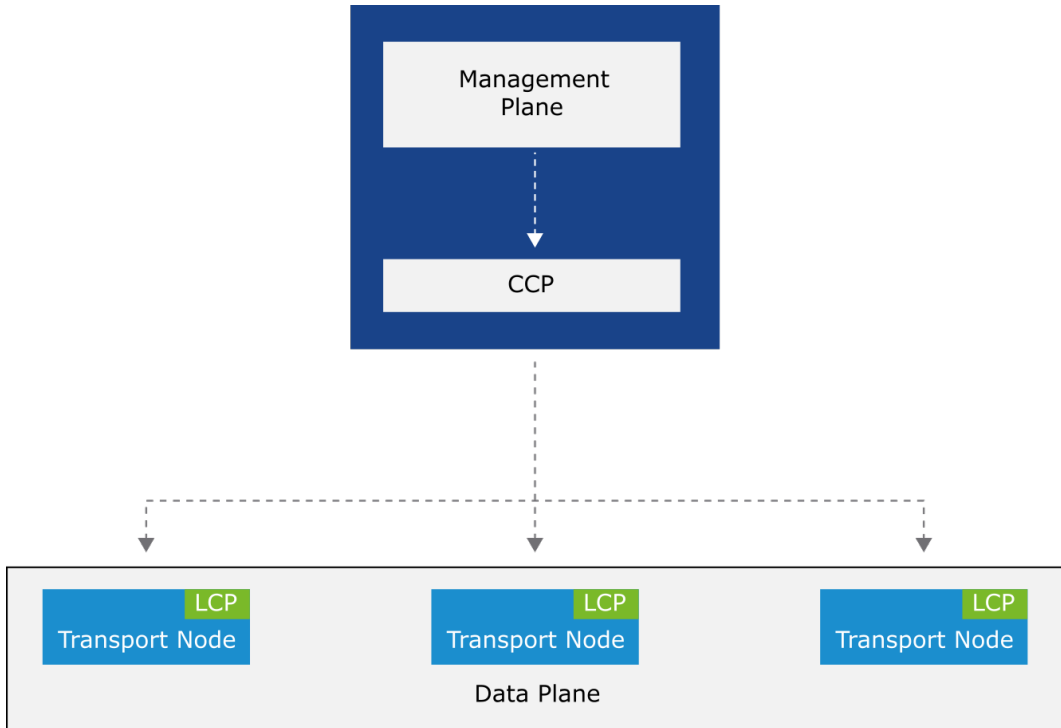


## 2-21 Control Plane Components (1)

In NSX, the control plane is divided into the CCP and local control plane (LCP).

The CCP exists as part of the NSX Manager nodes and is offered by the NSX Controller role.

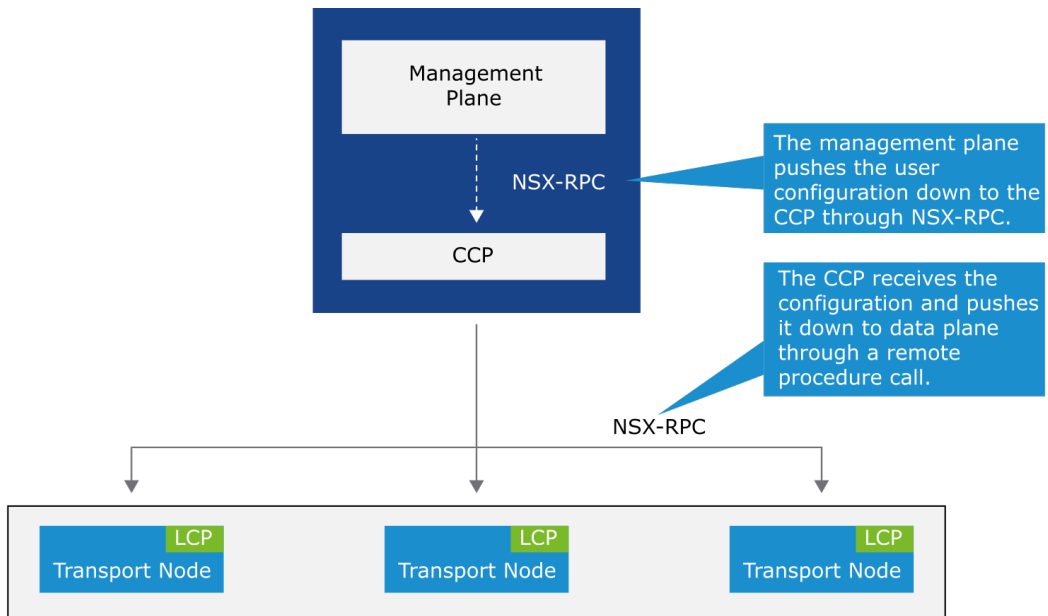
The LCP exists on host transport nodes or on NSX Edge transport nodes.



## 2-22 Control Plane Components (2)

The CCP and LCP perform different functions:

- The CCP:
  - Computes the ephemeral runtime state based on the configuration from the management plane
  - Disseminates information reported by the data plane elements by using the LCP
- The LCP:
  - Monitors the local link status
  - Computes local ephemeral runtime states based on updates from the data plane and the CCP
  - Pushes stateless configurations to forwarding engines



The CCP computes and disseminates the ephemeral runtime state based on the configuration from the management plane and topology information reported by the data plane elements.

The LCP runs on the compute endpoints. It computes the local ephemeral runtime state for the endpoint based on updates from the CCP and local data plane information. The LCP pushes stateless configurations to forwarding engines in the data plane and reports the information back to the CCP. This process simplifies the work of the CCP significantly and enables the platform to scale to thousands of different types of endpoints (hypervisor, container host, bare metal, or public cloud).

The NSX-RPC messaging protocol is a messaging solution for all communications between the management plane, CCP, and data plane.

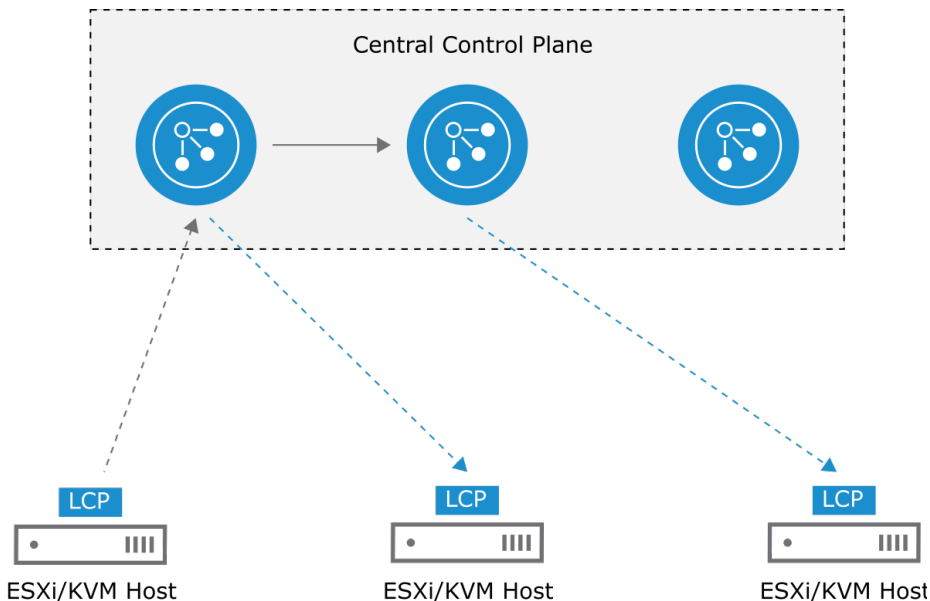
Remote procedure call (RPC) is a protocol that one program can use to request a service from another program on another computer without understanding the network details.

## 2-23 Control Plane Change Propagation

The CCP receives the configuration information from NSX Manager and propagates the information to the LCP of the transport nodes.

The LCP on each transport node interacts with the CCP.

If a change occurs, the LCP on the transport node notifies its assigned CCP, which further propagates these changes to the transport nodes.



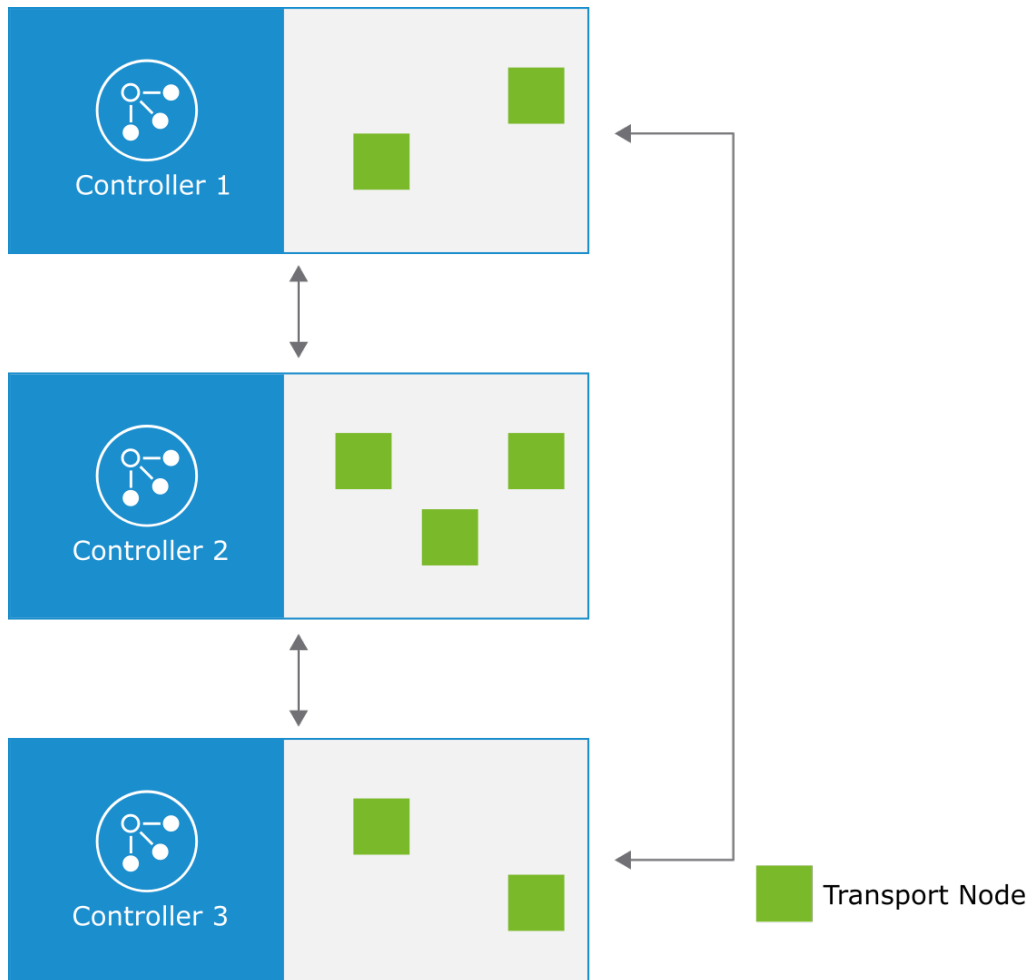
The LCP on the transport node reports local runtime changes to its designated CCP node. The designated CCP node receives the changes and propagates the changes to other controllers in the cluster. All controllers propagate the changes to the transport nodes that they manage.

## 2-24 Control Plane Sharding Function

The NSX management cluster includes a three-node CCP.

The control plane uses a sharding mechanism to distribute workloads:

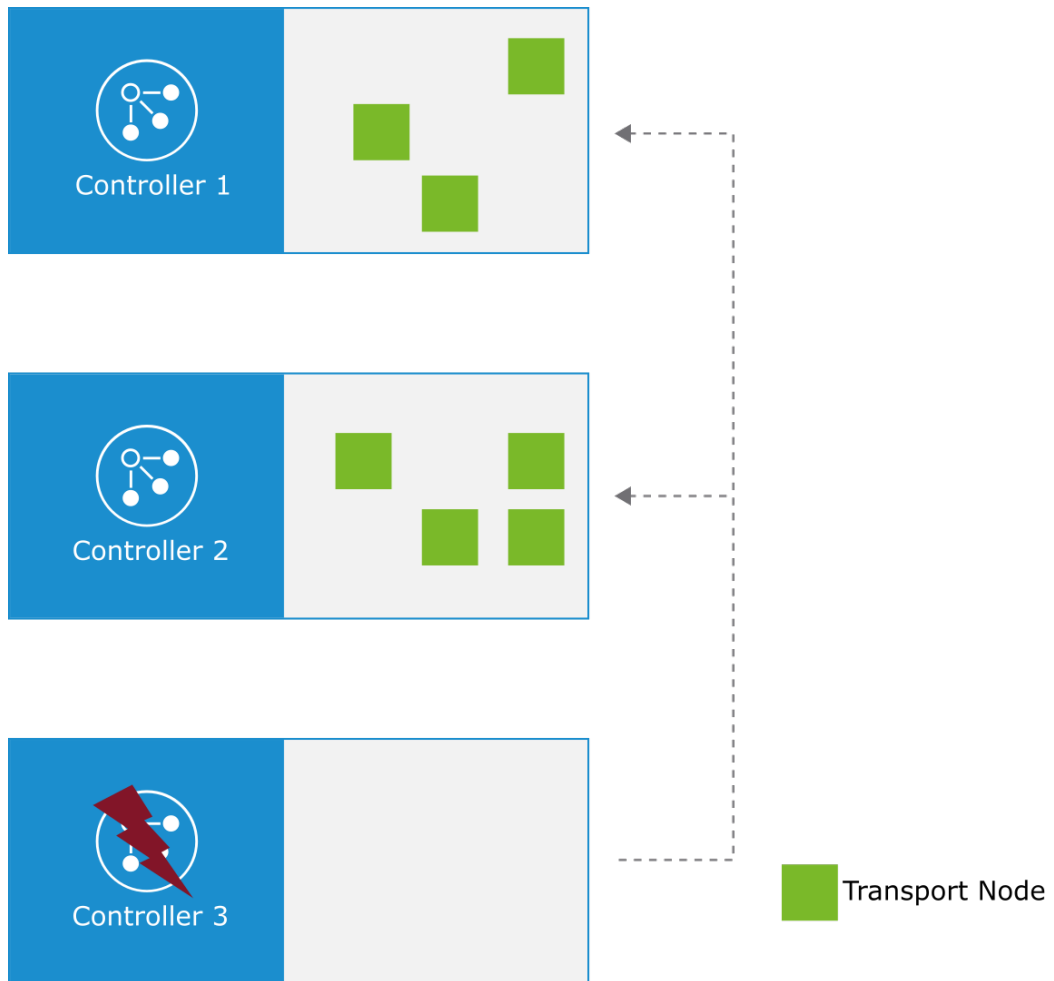
- Each transport node is assigned to a controller for L2 and L3 configuration and distributed firewall rule distribution.
- Each controller receives configuration updates from the management and data planes but maintains only the relevant information on the nodes that it is assigned to.



## 2-25 Managing Controller Failure

When a controller fails, its load is redistributed:

- The sharding table is recalculated to redistribute the load among the remaining controller nodes.
- This recalculation provides high availability and dual-active prevention.
- The traffic in the data plane continues to flow without being affected.



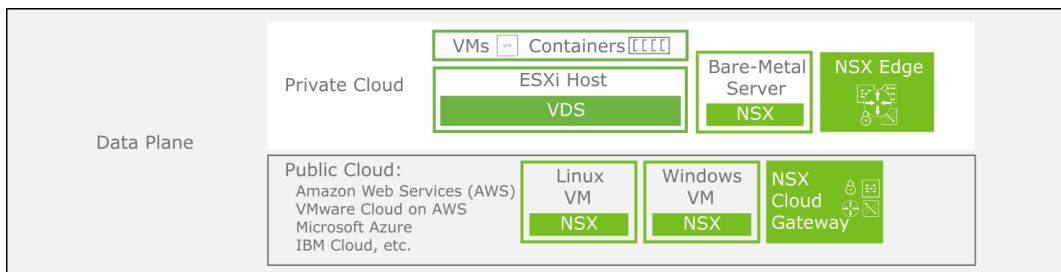
In the diagram, controller 3 is assigned to two transport nodes. When controller 3 fails, the nodes are moved to controllers 1 and 2.



## 2-26 About the Data Plane

The data plane has several components and functions:

- Includes multiple endpoints (ESXi hosts, bare-metal servers, and NSX Edge nodes)
- Contains various workloads, such as VMs, containers, and applications running on bare-metal servers
- Forwards data plane traffic
- Uses a scale-out distributed forwarding model
- Implements logical switching, distributed and centralized routing, and firewall filtering



## 2-27 Data Plane Functions

The data plane forwards packets based on configurations populated by the control plane and reports topology information to the control plane.

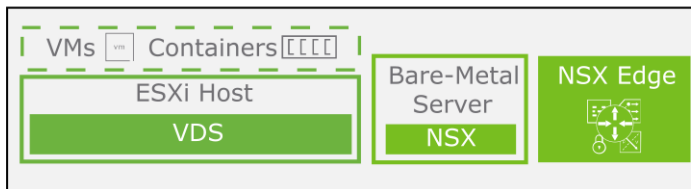
The data plane has the following responsibilities:

- Maintains the status of and manages failover between multiple links or tunnels
- Performs stateless forwarding based on tables and rules populated by the control plane
- Maintains packet-level statistics

## 2-28 Data Plane Components

Types of data plane components, called transport nodes, include:

- Hypervisor transport nodes:
  - Act as forwarding plane for the VM and container traffic
  - Support ESXi hypervisors
- Bare-metal transport nodes:
  - Include Linux-based and Windows workloads running on bare-metal servers
  - Include containers running on bare-metal servers without a hypervisor
- NSX Edge cluster:
  - Contains edge transport nodes (VM or bare-metal form factors)
  - Provides stateful and gateway services

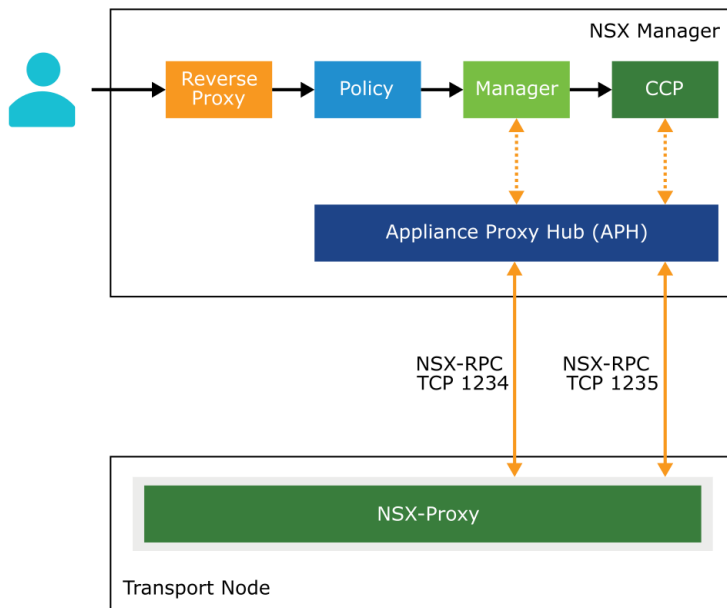


## 2-29 Data Plane Communication Channels

Appliance Proxy Hub (APH) acts as a communication channel between NSX Manager and the transport node.

APH offers the following functions:

- Runs as a service on NSX Manager
- Provides secure connectivity based on NSX-RPC
- Uses port 1234 for communication between the management plane and transport node
- Uses port 1235 for communication between the CCP and transport node



The NSX Manager management plane communicates with the transport nodes by using APH Server over NSX-RPC/TCP through port 1234.

CCP communicates with the transport nodes by using APH Server over NSX-RPC/TCP through port 1235.

The NSX-Proxy on the transport node receives the NSX-RPC messages from NSX Manager and CCP.

The nsx-appl-proxy APH service runs on NSX Manager.

## 2-30 Review of Learner Objectives

- Describe the purpose of VMware Virtual Cloud Network and its framework
- Identify the benefits and recognize the use cases for NSX
- Describe how VMware NSX fits into the NSX product portfolio
- Recognize features and the main elements in the NSX architecture
- Enumerate the deprecated features in NSX 4.0.x
- Describe the NSX policy and centralized policy management
- Describe the NSX management cluster and the management plane
- Identify the functions of control plane components, data plane components, and communication channels

## 2-31 Key Points

- VMware Virtual Cloud Network is a ubiquitous software layer that connects and protects any workload across any environment.
- The NSX family is a portfolio of various offerings, including NSX, vRealize Network Insight, NSX Cloud, NSX Intelligence, NSX Distributed IDS/IPS, NSX Advanced Load Balancer, Tanzu Service Mesh Advanced, VMware SD-WAN, and VMware HCX.
- In an NSX management cluster, each node performs the management, control, and policy roles.
- NSX policy provides consistency in networking and security configuration across the NSX environment.
- The data plane in NSX forwards packets based on tables populated by the control plane and reports topology information to the control plane.

Questions?

## Module 3

# Preparing the NSX Infrastructure

### 3-2 Importance

As the network administrator, you must plan and deploy a network infrastructure that meets the business requirements and growth of users and applications. You must thoroughly understand the function and configuration of the NSX management cluster and transport nodes to ensure a fully prepared environment for NSX.

### 3-3 Module Lessons

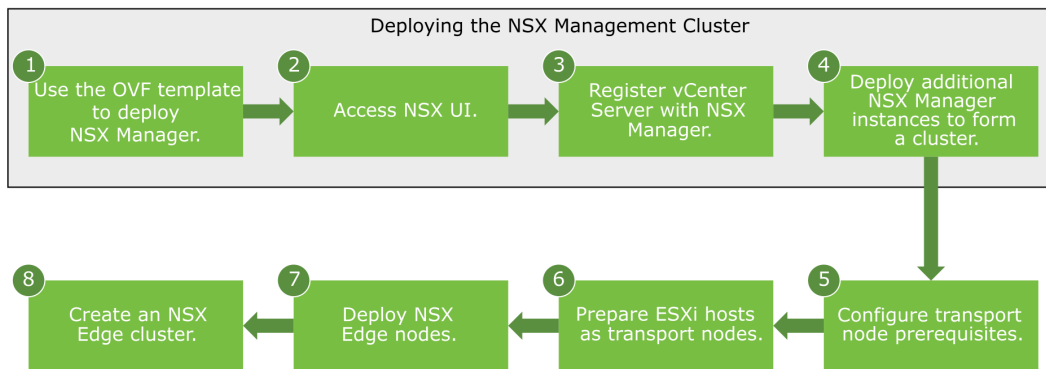
1. Deploying the NSX Management Cluster
2. Navigating the NSX UI
3. Preparing the Data Plane
4. DPU-Based Acceleration for VMware NSX

## 3-4 Lesson 1: Deploying the NSX Management Cluster

### 3-5 Learner Objectives

- Explain the deployment workflows for the NSX infrastructure
- Deploy NSX Manager on ESXi hosts
- Verify the deployment status of NSX Manager nodes and the NSX management cluster
- Explain the procedure to import and replace certificates

### 3-6 Implementing NSX in vSphere



The vSphere environment infrastructure preparation workflow is as follows:

1. Deploy an NSX Manager node from an OVF template.
2. Access the NSX UI.
3. Register vCenter Server with NSX Manager.
4. Deploy additional NSX Manager nodes to form an NSX management cluster.
5. Preconfigure transport nodes, including transport zones, IP pools, and uplink profiles.
6. Prepare ESXi hosts as transport nodes.
7. Deploy the NSX Edge node (VM or bare metal):
  - Transport node preparation
  - NSX Edge cluster formation
8. Create an NSX Edge cluster.

# 3-7      Considerations for Deploying NSX Manager

You should consider the following factors before deploying NSX Manager instances:

- NSX Manager can be deployed on ESXi hosts managed by vCenter Server or on standalone ESXi hosts.
- Automated deployment of additional NSX Manager instances by using the UI or API is supported only on ESXi hosts managed by vCenter Server.
- Implementing NSX Manager in KVM is no longer supported.

NSX Manager combines the roles of the policy, manager, and controller in a single node (virtual appliance).

For supported ESXi hypervisor versions, see VMware Product Interoperability Matrix at [https://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](https://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

# 3-8      NSX Manager Node Sizing

NSX Manager supports the small, medium, and large form factors.

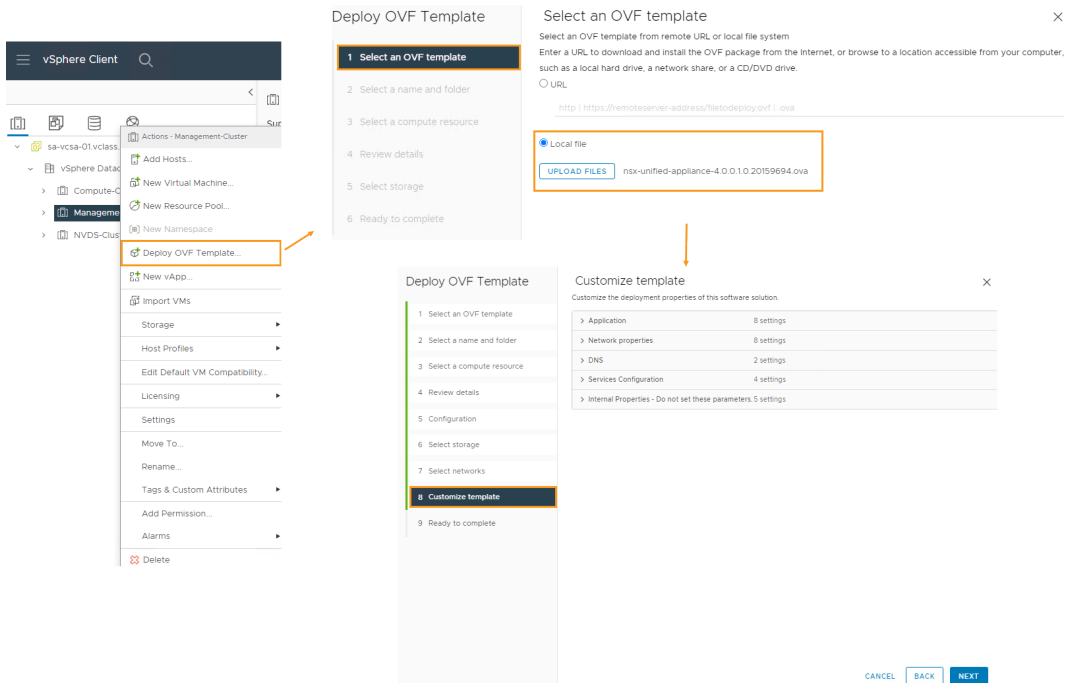
Form Factor	Number of CPUs	Memory (GB)	Hard Disk (GB)
Small	4	16	300
Medium	6	24	300
Large	12	48	300

NSX Manager is available in different sizes for different deployment scenarios:

- A small appliance for lab or proof-of-concept deployments
- A medium appliance for deployments with up to 64 hosts
- A large appliance for customers who deploy large-scale environments

## 3-9 Deploying NSX Manager from an OVF Template

In vSphere, use the OVF Template to deploy the first NSX Manager instance.



You can select an OVF template from a remote URL or your local file system.

You can select the size of NSX Manager to be Small, Medium, or Large.

In NSX 4.0.0.1, you can deploy NSX Manager using an IPv6 address.

You customize the OVF template with the NSX Manager configuration. The Customize Template step has several sections:

- **Application:** Configure the passwords for the GRUB root user, system root user, admin user, and audit user.
- **Network Properties:** Configure the host name, IPv4, and IPv6 network configurations.
- **DNS:** Configure your DNS server information.
- **Services Configuration:** Configure NTP server and SSH settings.



By default, any password must meet the following requirements:

- Minimum of 12 characters in length
- At least one uppercase character
- At least one lowercase character
- At least one numeric character
- At least one special character
- At least five unique characters

## 3-10 Methods to Access NSX Manager

After you install and configure NSX Manager, you can access and manage it in the following ways:

- Log in to the NSX UI through a supported browser.
- Log in to NSX Manager through the CLI.
- Access NSX Manager with API.

For information about NSX Manager browser support, see *NSX Installation Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-AECA2EE0-90FC-48C4-8EDB-66517ACFE415.html>.

## 3-11 Accessing the NSX UI

You enter the FQDN or IP address of the newly deployed NSX Manager instance.

Log in with the admin user name and password.

VMware NSX | Login

Not secure <https://sa-nsxmgr-01.vclass.local/login.jsp>

Infrastructure vSphere VMware NSX 3-Tier App NAT Web Server Har

Welcome to  
VMware NSX™

admin

.....

LOG IN

[Forgot Password?](#)

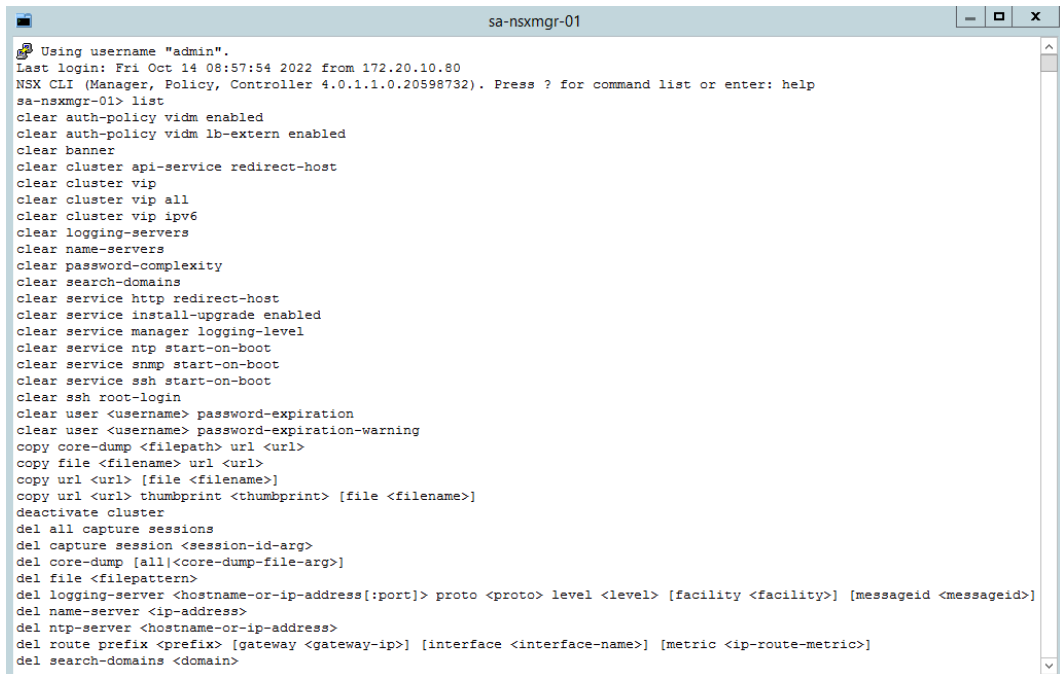
## 3-12 Accessing the NSX CLI

You can access the NSX CLI in the following ways:

- Open an SSH session and enter the admin user credentials that were configured during the NSX Manager installation.
- You can also use the NSX Manager virtual machine console to access the NSX CLI.

The NSX CLI is also available on all types of transport nodes and provides a consistent view of the NSX configuration across the environment.

Use the `list` command to retrieve all available commands to query and configure the environment.



```
sa-nxmgr-01
Using username "admin".
Last login: Fri Oct 14 08:57:54 2022 from 172.20.10.80
NSX CLI (Manager, Policy, Controller 4.0.1.1.0.20598732). Press ? for command list or enter: help
sa-nxmgr-01> list
clear auth-policy vidm enabled
clear auth-policy vidm lb-extern enabled
clear banner
clear cluster api-service redirect-host
clear cluster vip
clear cluster vip all
clear cluster vip ipv6
clear logging-servers
clear name-servers
clear password-complexity
clear search-domains
clear service http redirect-host
clear service install-upgrade enabled
clear service manager logging-level
clear service ntp start-on-boot
clear service snmp start-on-boot
clear service ssh start-on-boot
clear ssh root-login
clear user <username> password-expiration
clear user <username> password-expiration-warning
copy core-dump <filepath> url <url>
copy file <filename> url <url>
copy url <url> [file <filename>]
copy url <url> thumbprint <thumbprint> [file <filename>]
deactivate cluster
del all capture sessions
del capture session <session-id-arg>
del core-dump [all|<core-dump-file-arg>]
del file <filepath>
del logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>]
del name-server <ip-address>
del ntp-server <hostname-or-ip-address>
del route prefix <prefix> [gateway <gateway-ip>] [interface <interface-name>] [metric <ip-route-metric>]
del search-domains <domain>
```

You can access the CLI mode of NSX Manager either through the NSX Manager virtual machine console or by connecting remotely over SSH by using PuTTY.

You can access the NSX CLI mode through SSH only if the SSH mode is enabled in the NSX Manager appliance.

By default, the following levels of access are available when connecting through the CLI mode:

- **Root:** This role can view, deploy, and configure any component in NSX by using the Linux-based commands.

Root is an admin-level role. You must access this role only with technical support assistance.

- **Admin:** This role can view, deploy, and configure any component in NSX by using the CLI commands.
- **Audit:** This role can view settings, events, and reports. This role is read-only.

To access the admin mode, log in as the admin user through SSH or through the NSX Manager console by using the admin credentials.

To access the audit mode:

1. Start a PuTTY session or open the NSX Manager virtual machine console.
2. Log in by using the audit user name and password.

Use the `list` command to retrieve all available commands to query and configure the environment.

For example, you can use the `get` command to query information, for example, the `get services` command.

## 3-13 Accessing NSX Manager with API

REST APIs are used when you cannot use the GUI or when you want to automate by using scripting or other tools.

NSX Manager provides the following functions with API:

- NSX Manager accepts API requests on TCP port 443 over HTTPS application protocol to programmatically create, retrieve, modify, or delete NSX objects.
- You can use the following commands:
  - HTTPS GET commands to read and retrieve objects
  - HTTPS PUT, PATCH, or POST to create or update objects
  - HTTPS DELETE to delete objects
- To use the NSX API, you must configure a client and verify that the required ports are open between your client and NSX Manager.

For information about the various API calls and functionality, see *NSX API Guide* at <https://developer.vmware.com/apis/1487/nsx>.

## 3-14 Registering vCenter Server with NSX Manager

You register vCenter Server to NSX.

The screenshot shows the NSX Manager interface. The top navigation bar has tabs: Home, Networking, Security, Inventory, Plan & Troubleshoot, and System (highlighted with a blue box). The left sidebar has a 'Compute Managers' section highlighted with a blue box. The main content area shows the 'Compute Managers' table with a '+ ADD COMPUTE MANAGER' button highlighted with a green box. A green arrow points from this button to the 'New Compute Manager' dialog box. The dialog box contains the following fields:

- Name: sa-vcsa-01.vclass.local
- Description: vCenter Server as a compute manager
- Type: vCenter
- FQDN or IP Address: sa-vcsa-01.vclass.local  
E.g. FQDN subdomain.example.com OR IPv4 10.10.10.10 OR IPv6 fc7e:1206:db42::1
- HTTPS Port of Reverse Proxy: 443
- Username: administrator@vsphere.local
- Password: (masked with dots)
- SHA-256 Thumbprint: (empty field)
- Create Service Account: ☒ Yes  
Supported for vCenter Server 7.0 or later
- Enable Trust: ☒ Yes  
Supported for vCenter Server 7.0 or later
- Access Level: ☒ Full Access to NSX (required for vSphere for Kubernetes and vSphere Lifecycle Manager)  
☐ Limited Access to NSX (required for vSphere Lifecycle Manager)

At the bottom of the dialog box are 'CANCEL' and 'ADD' buttons.

You add the configuration details to register the vCenter Server system to NSX.

You turn on the **Create a Service Account** toggle for features, such as vSphere Lifecycle Manager, which must authenticate with NSX APIs. During registration, the compute manager creates a service account.

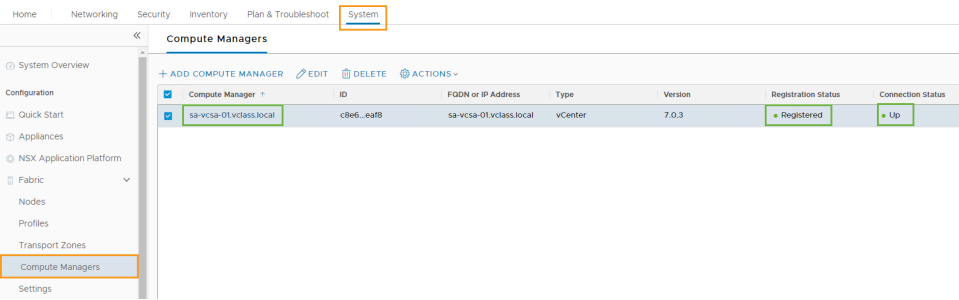
The Enable Trust feature for vCenter Server 7.0 or later enables vCenter Server to execute tasks on NSX Manager.

The following access level options are available:

- **Full Access to NSX:** This access level ensures that vSphere with Tanzu and vSphere Lifecycle Manager can communicate with NSX. This access level is selected by default.
- **Limited Access to NSX:** This access level ensures that vSphere Lifecycle Manager can communicate with NSX.

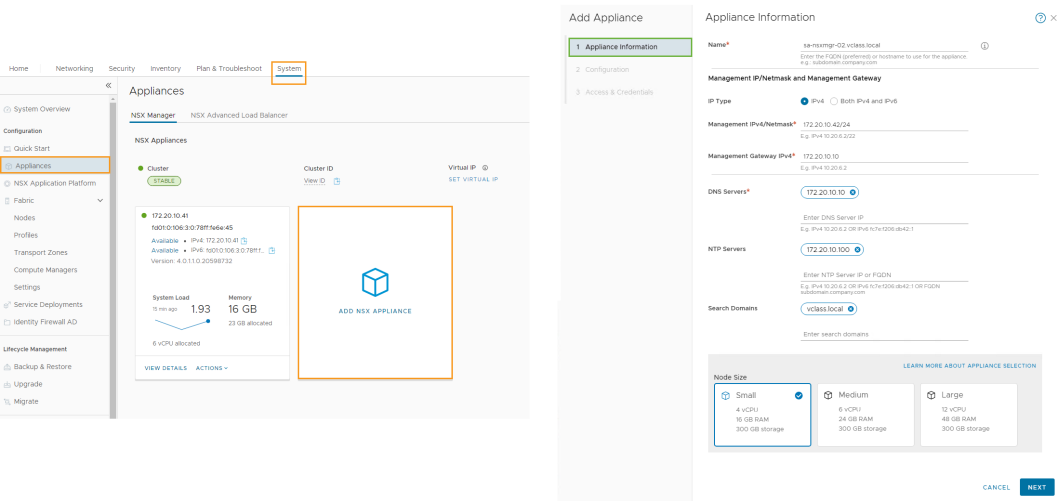
# 3-15 Verifying vCenter Server Registration with NSX Manager

You verify that vCenter Server is successfully registered and the connection status appears as Up.



# 3-16 Deploying Additional NSX Manager Instances (1)

You can deploy the second and third NSX Manager nodes from the NSX UI.



The screenshot shows the process for automatically deploying additional NSX Manager instances from the NSX UI.

To automatically deploy additional NSX Manager instances from the NSX UI, you must register a vCenter Server to NSX.

## 3-17 Deploying Additional NSX Manager Instances (2)

The image shows two side-by-side screenshots of the NSX Manager 'Add Appliance' wizard. The left screenshot is the 'Configuration' step, and the right screenshot is the 'Access & Credentials' step.

**Configuration Step:**

- 1 Appliance Information
- 2 Configuration
- 3 Access & Credentials

Configuration fields:

- Compute Manager\*: sa-vcsa-01-vc1class local
- Compute Cluster\*: Management-Cluster (domain-c179750)
- Resource Pool: Select resource pool
- Host: Select host
- Datastore\*: SA-Shared-01-NSX (datastore-176762)
- Virtual Disk Format: Thin Provision (By default, Thin Provision format is supported)
- Network\*: Pg-SA-Management

**Access & Credentials Step:**

- 1 Appliance Information
- 2 Configuration
- 3 Access & Credentials

Access & Credentials fields:

- Enable SSH: ☐ no
- Enable Root Access: ☐ no
- System Root Credentials
  - System Username: root
  - Root Password\*: [password field]
  - Confirm Root Password\*: [password field]
- Admin CLI Credentials
  - CLI Username\*: admin
  - CLI Password\*: ☒ Same as root password
- Audit CLI Credentials
  - Audit CLI Username\*: audit
  - Audit CLI Password\*: ☒ Same as root password

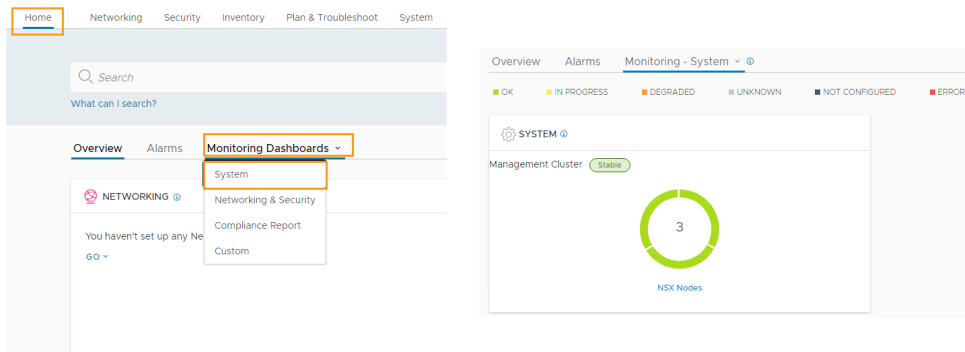
Buttons: CANCEL, BACK, NEXT, INSTALL APPLIANCE

For information about manually joining the NSX Manager nodes to form a cluster, see *NSX Installation Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-9F3C8273-FA5F-41C8-85CA-436F8D34977D.html>.

## 3-18 Management Cluster Status: GUI (1)

The NSX management cluster is formed automatically.

You can view the status of the nodes in the cluster from the NSX UI.



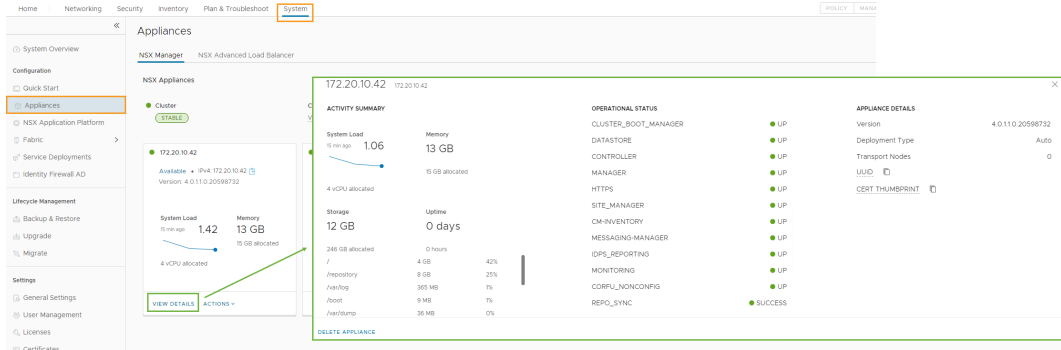
You can check the status of nodes by selecting **Home > Monitoring Dashboard > System** in the NSX UI.

Different colors indicate different messages. Red indicates degraded performance, for example, memory usage of NSX Manager is consistently higher than 90 percent for the past 5 minutes.



## 3-19 Management Cluster Status: GUI (2)

On the Overview page in the NSX UI, you can view the status of the management cluster and its nodes.



The following parameters describe the NSX Manager details:

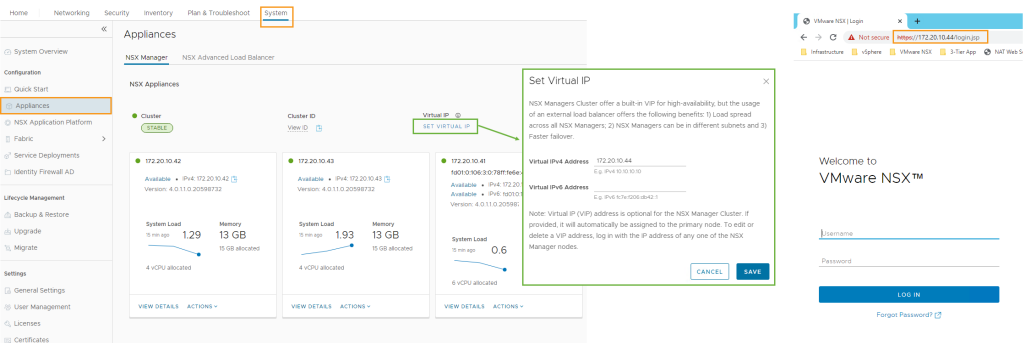
- **Version:** Describes the current running version of NSX Manager.
- **System Load:** Includes CPU, memory, and storage usage details.

The following functions are performed by the most relevant operational components:

- **Cluster\_Boot\_Manager:** Cluster Boot Manager is responsible for orchestrating the clustering services on the NSX Manager nodes.
- **Datastore:** Storage containers for files.
- **Controller:** Controller is an advanced distributed state management system that provides control plane functions for NSX logical switching and routing functions.
- **Manager:** Manager provides a GUI and REST APIs for creating, configuring, and monitoring NSX components such as logical switches, logical routers, firewall, and so on.
- **HTTPS:** The main HTTPS endpoint where API is involved. The component distributes incoming calls among components of NSX Manager.

# 3-20 Configuring the Virtual IP Address

You can manually configure a virtual IP address for the NSX management cluster. You access the GUI by using the configured virtual IP.



You can configure a virtual IP address for the management cluster to provide the availability among the management nodes:

- The virtual IP address is not set by default.
- When assigning Virtual IP, all the NSX Manager VMs in the cluster must be configured in the same subnet.
- The leader node of the NSX management cluster assumes ownership of the VIP to service any API and UI request. Any API and UI request coming in from clients is directed to the leader node. If the leader node that owns VIP becomes unavailable, NSX elects a new leader. The new leader owns the VIP.
- You might need to wait a few minutes for the newly configured address to take effect.

To add the virtual IP address, click **SET VIRTUAL IP**.

## 3-21 Management Cluster Status: CLI (1)

Run `get cluster status` to query the NSX management cluster status.

```
sa-nsxmgr-01> get cluster status
Tue Sep 27 2022 UTC 09:04:20.354
Cluster Id: f7cf47e8-f444-4bb2-8463-b515e3f3c0e1
Overall Status: STABLE

Group Type: DATASTORE
Group Status: STABLE

Members:
  UUID                                FQDN                                IP                                STATUS
  439e1d42-e02f-d0d6-3da5-28eb038e05cf  sa-nsxmgr-01                        172.20.10.41                     UP
  216ca0d1-1613-44c2-84be-ea43ee507529  sa-nsxmgr-02.vclass.local          172.20.10.42                     UP
  b624f459-6c1a-4dea-b2cb-a63c6071df16  sa-nsxmgr-03.vclass.local          172.20.10.43                     UP

Group Type: CLUSTER_BOOT_MANAGER
Group Status: STABLE

Members:
  UUID                                FQDN                                IP                                STATUS
  439e1d42-e02f-d0d6-3da5-28eb038e05cf  sa-nsxmgr-01                        172.20.10.41                     UP
  216ca0d1-1613-44c2-84be-ea43ee507529  sa-nsxmgr-02.vclass.local          172.20.10.42                     UP
  b624f459-6c1a-4dea-b2cb-a63c6071df16  sa-nsxmgr-03.vclass.local          172.20.10.43                     UP

Group Type: CONTROLLER
Group Status: STABLE

Members:
  UUID                                FQDN                                IP                                STATUS
  13781a02-06d9-4823-a39d-5c3f0614b708  sa-nsxmgr-01                        172.20.10.41                     UP
  f1ecd69b-caff-432d-8059-6def4389bbf7  sa-nsxmgr-02.vclass.local          172.20.10.42                     UP
```

You connect to an appliance in the cluster and enter the **get cluster status** command. The number and status of the nodes in the cluster appear.

The example output lists the Cluster Boot Manager, controller, and manager groups. It also shows each group's status with its members and member status.

## 3-22 Management Cluster Status: CLI (2)

Run `get services` to query the NSX Manager services status.

```
sa-nsxmgr-01> get services
Tue Sep 27 2022 UTC 09:05:51.746
Service name:          applianceproxy
Service state:         running

Service name:          async_replicator
Service state:         running
Logging level:         info

Service name:          auth
Service state:         running
Logging level:         info

Service name:          cluster_manager
Service state:         running

Service name:          cm-inventory
Service state:         running

Service name:          controller
Service state:         running
Listen address:
```

Run `get interfaces` to get information about the NSX Manager network interfaces.

```
sa-nsxmgr-01> get interfaces
Tue Sep 27 2022 UTC 09:09:10.359
Interface: eth0
  IPv4 Address:
    Address: 172.20.10.41/24
    MAC address: 00:50:56:06:ad:a8
    MTU: 1500
    Default gateway: fd01:0:106:3:0:78ff:fe6e:5
    Broadcast address: 172.20.10.255
  IPv6 Addresses:
    - Address: fd01:0:106:3:0:78ff:fe6e:45/64
    - Address: fe80::250:56ff:fe06:ada8/64
  Link status: up
  Admin status: up
  RX packets: 3393029
  RX bytes: 760449004
  RX errors: 0
  RX dropped: 599
  TX packets: 2346584
  TX bytes: 22819189293
  TX errors: 0
  TX dropped: 0
```

The following common misconfigurations might exist when troubleshooting an NSX Manager node:

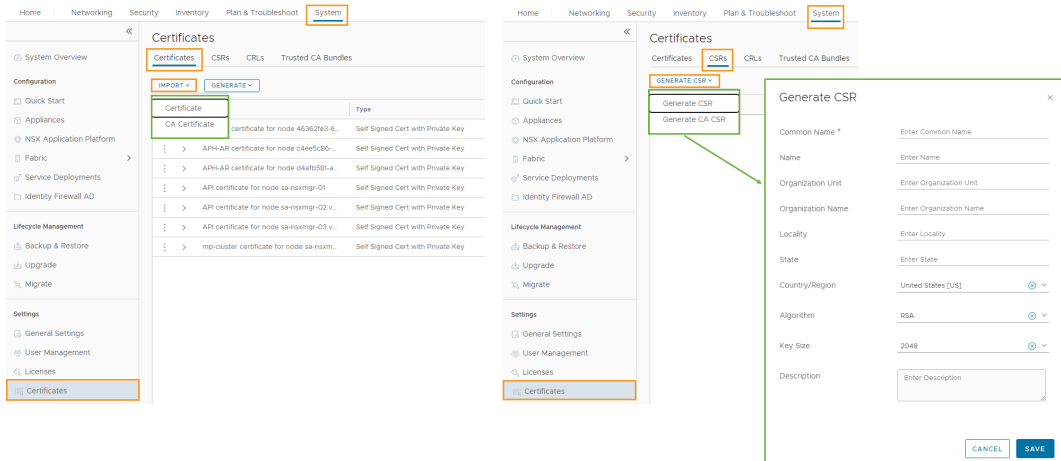
- ESXi host with insufficient resources (CPUs, memory, or hard disk)
- Incorrect network details, such as the gateway address, network mask, DNS, and so on

## 3-23 Replacing Self-Signed Certificates (1)

After you install NSX, the manager nodes and cluster have self-signed certificates.

Perform the following tasks if your security requirements do not include the use of self-signed certificates:

- Replace the self-signed certificates with CA-signed certificates.
- Use a different certificate for each node.



NSX Manager requires a signed certificate to authenticate the identity of the NSX Manager web service and encrypt information sent to the NSX Manager web server. As a security recommendation, you use CA-signed certificates instead of self-signed certificates.

To replace the self-signed certificates with CA-signed certificates:

1. Generate a certificate signing request (CSR).
2. You send the CSR file to a certificate authority (CA) to apply for a digital identity certificate.
3. Import the certificate in NSX Manager.
4. Replace the self-signed certificates with CA-signed certificates

To generate a CSR:

1. Log in with admin privileges to an NSX Manager instance.
2. Select **System** > **Settings** > **Certificates**.
3. Click the **CSRs** tab.

4. Select **GENERATE CSR > GENERATE CSR** and enter the CSR details.
5. Click **SAVE**.

To import a CA-signed certificate:

1. Log in with admin privileges to an NSX Manager instance.
2. Select **System > Settings > Certificates**.
3. Select **Import > Certificate** and enter the certificate details.
4. Click **SAVE**.

## 3-24 Replacing Self-Signed Certificates (2)

You can replace the certificate for a manager node or the manager cluster virtual IP (VIP) by making an API call:

- To replace the certificate of a manager node, use the POST API call:

```
https://<nsx-  
mgr>/api/v1/node/services/http?action=apply_certificate&cert  
ificate_id=<certificate_id>
```

- To replace the certificate of the manager cluster VIP, use the POST API call:

```
https://<nsx-mgr>/api/v1/cluster/api-  
certificate?action=set_cluster_certificate&certificate_id=<c  
ertificate_id>
```

After importing the CA-signed certificate in NSX Manager, replace the certificate:

1. In your browser, log in with admin privileges to an NSX Manager instance at <https://<nsx-manager-ip-address>>.
2. Select **System > Settings > Certificates**.
3. Expand the certificate to show its details and copy the certificate ID.

Ensure that the **Service Certificate** option was set to No when this certificate was imported.

4. To replace the certificate of a manager node, use the POST `/api/v1/node/services/http?action=apply_certificate` API call.

For example, POST `https://<nsx-mgr>/api/v1/node/services/http?action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f`

5. To replace the certificate of the manager cluster VIP, use the POST `/api/v1/cluster/api-certificate?action=set_cluster_certificate` API call.

For example, POST `https://<nsx-mgr>/api/v1/cluster/api-certificate?action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac`

This step is not necessary if you did not configure VIP. For more information, see NSX REST API at <https://developer.vmware.com/apis/1487/nsx>.

## 3-25 Lab 1: Reviewing the Lab Environment and Topologies

Review the lab environment and network topologies:

1. Use the Lab Environment
2. Review the Networking Topologies

## 3-26 Lab 2: Reviewing the Configuration of the Predeployed NSX Manager Instance

Verify the NSX Manager appliance settings:

1. Access the Lab Environment
2. Prepare for the Lab
3. Verify the Licensing for vCenter Server and ESXi Hosts
4. Verify the NSX Manager Configuration and Licensing
5. Use the NSX CLI to Review the NSX Management Cluster Information
6. Register vCenter Server as a Compute Manager

## 3-27 Lab 3: (Simulation) Deploying a Three-Node NSX Management Cluster

Deploy a three-node NSX Management cluster from the NSX UI:

1. Prepare for the Lab
2. Deploy the Second NSX Manager Instance
3. Deploy the Third NSX Manager Instance
4. Configure the Virtual IP Address
5. Review the NSX Management Cluster Information from the NSX CLI

## 3-28 Review of Learner Objectives

- Explain the deployment workflows for the NSX infrastructure
- Deploy NSX Manager on ESXi hosts
- Verify the deployment status of NSX Manager nodes and the NSX management cluster
- Explain the procedure to import and replace certificates



## 3-29 Lesson 2: Navigating the NSX UI

### 3-30 Learner Objectives

- Distinguish between the Policy and the Manager UI
- Navigate the Policy and the Manager UI main configuration window

### 3-31 NSX Manager Policy and Manager Views



The NSX Manager interface provides the following modes for configuring resources:

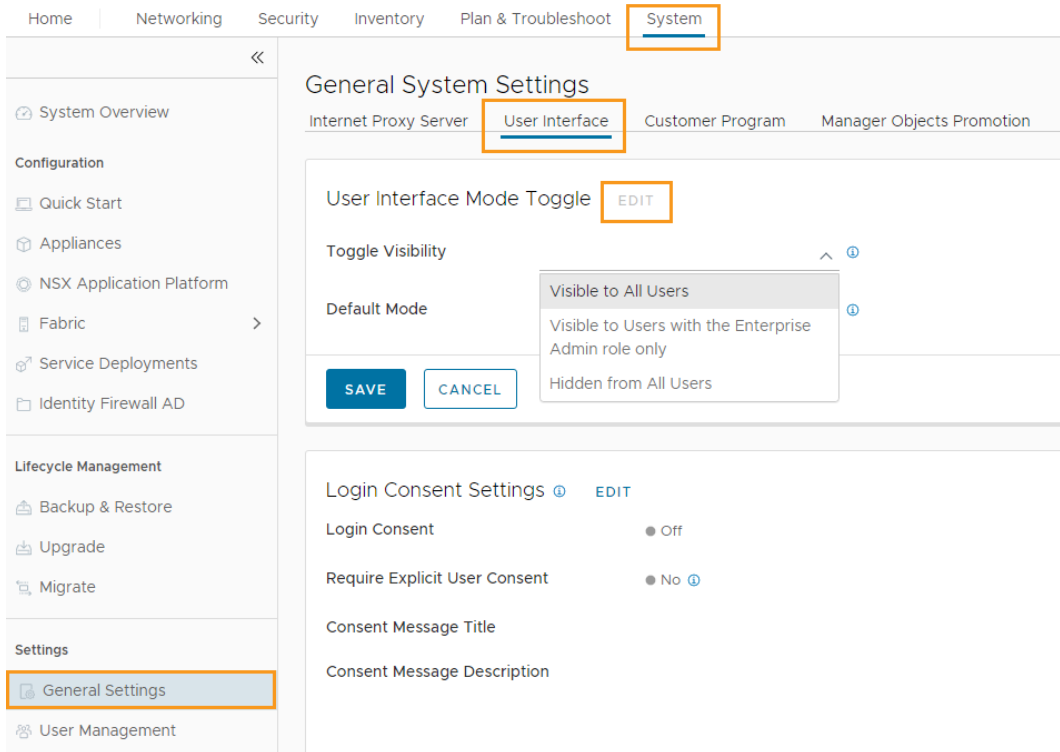
- Policy mode:
  - Recommended mode for configuring NSX
  - Default mode for new installations
  - Supported by Federation Global Manager
  - Does not support some features
- Manager mode

Use the Manager mode UI in the following instances:

- When NSX is integrated with cloud management platforms, for example, VMware Aria Automation (former name: vRealize Automation), VMware Integrated OpenStack, and so on.
- To work with objects that are not available in the Policy mode.

## 3-32 User Interface Preferences for Policy and Manager Modes

By default, new installations display the UI in Policy mode, and the **UI Mode** toggle is hidden. You can change the visibility of the UI mode toggle under **System > Settings > General Settings > User Interface**.



Environments that contain objects created through the Manager mode, such as from NSX upgrades or cloud management platforms, display the **UI Mode** toggle by default in the top-right corner of the UI.

# 3-33 About the Networking Tab

On the **Networking** tab, you can configure functions such as switching, routing, and layer 3 services. Layer 3 services include NAT, VPN, load balancing, and so on. A Policy view and a Manager view are available.

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

Policy

Manager

Segments

NSX Distributed Port Groups Profiles

ADD SEGMENT

EXPAND ALL

Filter by Name, Path and more

	Name	Connected Gateway	Transport Zone	Subnets	Ports / Interfaces	Status	Alarms
	App-Segment	T1-GW-01	Prod-Overlay-TZ   Overlay	172.16.20.1/24	0	Success	0
	DB-Segment	T1-GW-01	Prod-Overlay-TZ   Overlay	172.16.30.1/24	0	Success	0
	Web-Segment	T1-GW-01	Prod-Overlay-TZ   Overlay	172.16.10.1/24	0	Success	0

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

Policy

Manager

Switches

Ports

Switching Profiles

Edge Bridge Profiles

ADD

EDIT

DELETE

ACTIONS

search

Logical Switch	ID	Admin Status	Logical Ports	Traffic Type	Config State	Transport Zone
App-Segment	da66..aa87	Up	1	Overlay : 71680	Success	Prod-Overlay-TZ
DB-Segment	49cd...7313	Up	1	Overlay : 69632	Success	Prod-Overlay-TZ
Web-Segment	c96d...6c1f	Up	1	Overlay : 68608	Success	Prod-Overlay-TZ

A segment in the Policy view is called a logical switch in the Manager view.

The Tier-0 or Tier-1 gateways in the Policy view are called Tier-0 or Tier-1 logical routers in the Manager view.

# 3-34 About the Security Tab

On the **Security** tab, you can create firewall policies and endpoint security policies.

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

Policy

Manager

Distributed Firewall

All Rules Category Specific Rules

ACTIONS

REVERT

PUBLISH

ETHERNET (1)

EMERGENCY (0)

INFRASTRUCTURE (2)

ENVIRONMENT (0)

APPLICATION (7)

ADD POLICY

ADD RULE

CLONE

UNDO

DELETE

...

Filter by Name, Path and more

	Name	ID	Applied To	Sources	Destinations	Services	Context Profiles	Applied To	Action
	3-TIER POLICY	(3)	DFW						Success
	Allow Web Traffic	2025		Web-Servers	App-Servers	TCP (Source An...	None	DFW	Allow
	Allow DB Traffic	2026		App-Servers	DB-Servers	MySQL	None	DFW	Allow

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

Policy

Manager

Firewall

General Ethernet Exclusion List Settings About

ADD RULE

ADD SECTION

CLONE

DELETE

UP

DOWN

MORE

Filter

	#	Name	Source	Destination	Service	Context Profile	Applied To	Action	Popularity Index
		3-TIER POLICY					Applied To: All	Rules	
		Allow Web Traffic ID: 2025	Web-Servers	App-Servers	TCP: Src:Any, Dest:8443	Any	Distributed Firewall	Allow	
		Allow DB Traffic ID: 2026	App-Servers	DB-Servers	MySQL	Any	Distributed Firewall	Allow	

# 3-35 About the Inventory Tab

On the **Inventory** tab, you can review information about services, groups, VMs, containers, physical servers, and context profiles.

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

POLICY

MANAGER

Inventory Overview

Services

Groups

Profiles

Virtual Machines

Containers

Physical Servers

Tags

Services

ADD SERVICE

EXPAND ALL

Filter by Name, Path and more

	Name	Service Entries	Status
>	Active Directory Server	TCP (Source: Any   Destination: 464)	Success
>	Active Directory Server UDP	UDP (Source: Any   Destination: 464)	Success
>	AD Server	TCP (Source: Any   Destination: 1024)	Success
>	CIM-HTTP	TCP (Source: Any   Destination: 5988)	Success
>	CIM-HTTPS	TCP (Source: Any   Destination: 5989)	Success

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

POLICY

MANAGER

Inventory Overview

Inventory

Groups

Services

Context Profiles

Virtual Machines

Services

+ ADD

EDIT

DELETE

ACTIONS

search

	NSService	ID	Type	Protocol	Destination Ports	Source Ports	Members	Defined By
	Active Directory Server	5c15...aa36	NSService	TCP	464			System
	Active Directory Server UDP	d0f1...8361	NSService	UDP	464			System
	AD Server	ed5d...db9	NSService	TCP	1024			System
	CIM-HTTP	886e...2681	NSService	TCP	5988			System
	CIM-HTTPS	c194...d795	NSService	TCP	5989			System

## 3-36 About the Plan & Troubleshoot Tab

On the **Plan & Troubleshoot** tab, you can select **IPFIX**, **Port Mirroring**, **Traceflow**, and **Consolidated Capacity** for monitoring and troubleshooting.

The image displays two screenshots of the 'Plan & Troubleshoot' tab in a network management interface, specifically the 'Traceflow' section.

**Top Screenshot:**

- Navigation:** Home, Networking, Security, Inventory, **Plan & Troubleshoot** (highlighted), System. On the right, there are tabs for **POLICY** and **MANAGER**, with a help icon.
- Left Sidebar:** Discover & Plan (Discover & Take Action, Recommendations), Troubleshooting tools (IPFIX, Port Mirroring, **Traffic Analysis** (highlighted), Consolidated Capacity).
- Traceflow Section:**
  - Packet Information:** Includes fields for IP Type (IPv4), Traffic Type (Unicast), Protocol Type (ICMP), ICMP ID (0), and Sequence (0). A 'RESET' link is present.
  - Source:** Includes fields for Type (Virtual Machine) and VM Name (Select VM). A 'RESET' link is present.
  - Destination:** Includes fields for Type (Virtual Machine) and VM Name (Select VM). A 'RESET' link is present.

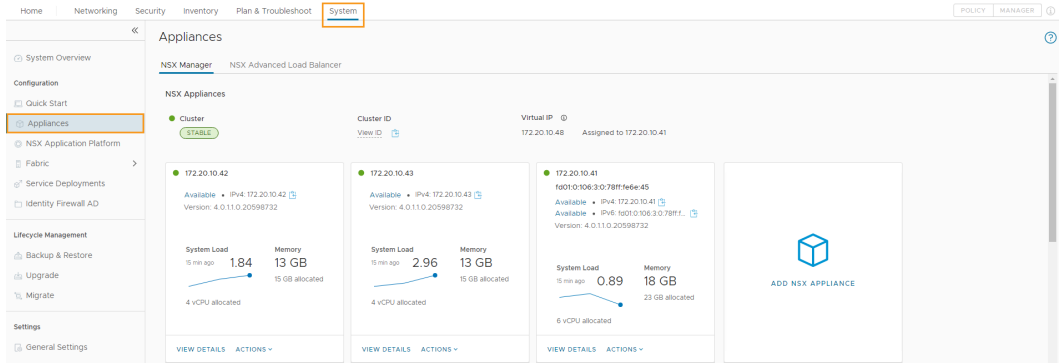
**Bottom Screenshot:**

- Navigation:** Home, Networking, Security, Inventory, **Plan & Troubleshoot** (highlighted), System. On the right, there are tabs for **POLICY** and **MANAGER**, with a help icon.
- Left Sidebar:** Port Connection, **Traceflow** (highlighted), Port Mirroring, IPFIX, Consolidated Capacity.
- Traceflow Section:**
  - IP Address:** Includes a field for IP Address (IPv4) and a note: 'Reset the entire source and destination selections below if IP address type is changed.'
  - Traffic Type:** Includes a field for Traffic Type (Unicast).
  - Source:** Includes fields for Type (Virtual Machine) and VM Name\* (Select VM).
  - Destination:** Includes fields for Type (Virtual Machine) and VM Name\* (Select VM).

The Manager view does not have the Discover & Plan functionality, which is only found in the policy view.

## 3-37 About the System Tab

On the **System** tab, you can deploy the transport node and management cluster, add licenses, register compute managers, and so on.



The Overview page shows the number and details of the management nodes and the cluster.

The **System** tab does not have separate Policy and Manager views.

## 3-38 Review of Learner Objectives

- Distinguish between the Policy and the Manager UI
- Navigate the Policy and the Manager UI main configuration window

## 3-39 Lesson 3: Preparing the Data Plane

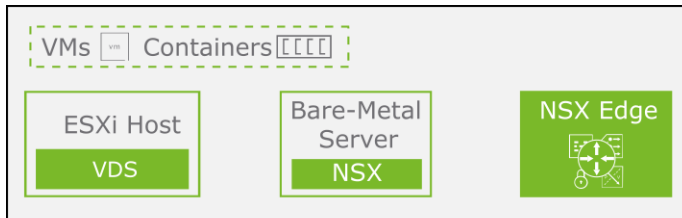
### 3-40 Learner Objectives

- Describe the functions of transport zones, transport nodes, N-VDS, and VDS.
- Explain the relationships between transport nodes, transport zones, N-VDS, and VDS.
- Create IP pools for the node address assignment
- Describe and configure uplink profiles
- Prepare ESXi hosts to participate in NSX networking
- Verify the status of ESXi transport nodes and VIB installation

## 3-41 Data Plane Components and Functions

The NSX data plane contains several types of endpoints with different functions:

- Performs stateless forwarding and encapsulation or decapsulation of packets based on tables populated by the control plane.
- Uses a scale-out distributed forwarding model and carries data over designated transport networks in the physical network.
- Performs logical switching, distributed and centralized routing, and firewall filtering.



Various Types of Endpoints Supported in the Data Plane

## 3-42 Overview of the Transport Node

NSX requires transport nodes to perform networking (overlay or VLAN) and security functions.

A transport node is responsible for forwarding the data plane traffic that originates from VMs, containers, or applications running on bare-metal servers.

NSX supports the following types of transport nodes:

- ESXi Hypervisor
- Bare-metal server (RHEL, CentOS, Ubuntu, SLES, Oracle Linux, Windows)
- NSX Edge



## 3-43 Transport Node Components and Architecture

Each transport node contains:

- Virtual distributed switch: A vSphere Distributed Switch (VDS) or virtual distributed switch managed by NSX (N-VDS). It is the core data plane component on the transport nodes.

VDS is the only virtual switch supported on ESXi hosts.

N-VDS is the virtual switch supported on NSX Edge nodes and bare-metal workloads.

- NSX-Proxy: It is an agent running on all transport nodes that receives configuration and control plane data from CCP.

### ESXi Transport Node

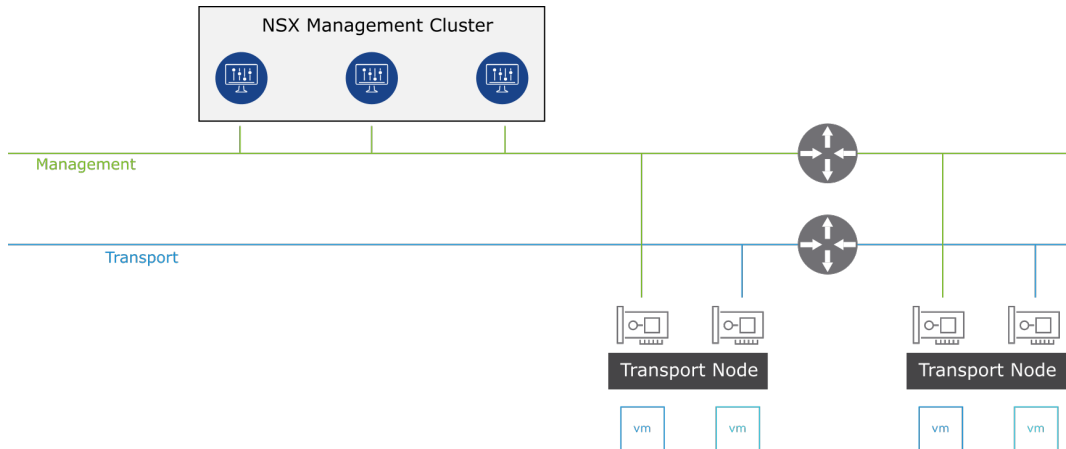


Since NSX 4.0.0.1, the N-VDS host switch is not supported for ESXi hosts. In a brownfield environment, you must migrate the ESXi hosts to VDS before upgrading to NSX 4.0.0.1.

## 3-44 Physical Connectivity of a Transport Node

For the physical connectivity of a transport node, you can select one of these options:

- Use dedicated physical NICs for management and transport (overlay or VLAN) traffic.
- Share the physical NIC for both management and transport traffic.

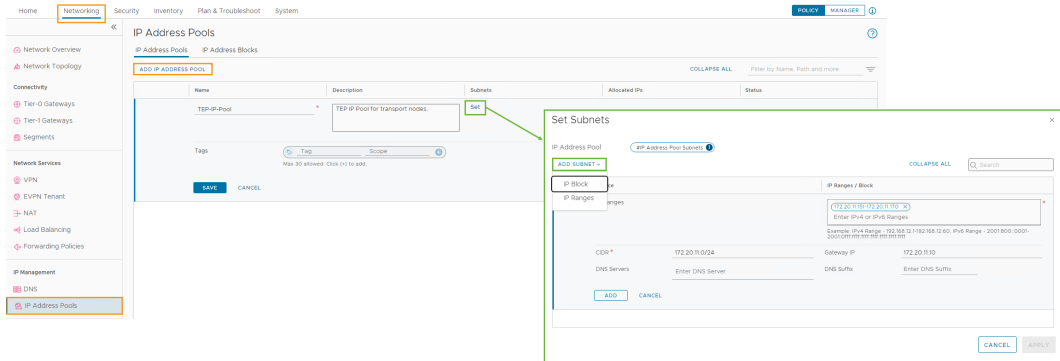


## 3-45 About IP Address Pools

Each transport node has a tunnel endpoint (TEP). The tunnel endpoint (TEP) enables transport nodes to participate in the NSX overlay.

Each TEP requires an IP address. You can create one or more IP address pools to assign addresses to TEPs.

One or more TEPs can be assigned to each transport node.



An IP pool is a container created for assigning IP addresses to tunnel endpoints (TEPs).

You can manually configure IP address pools.

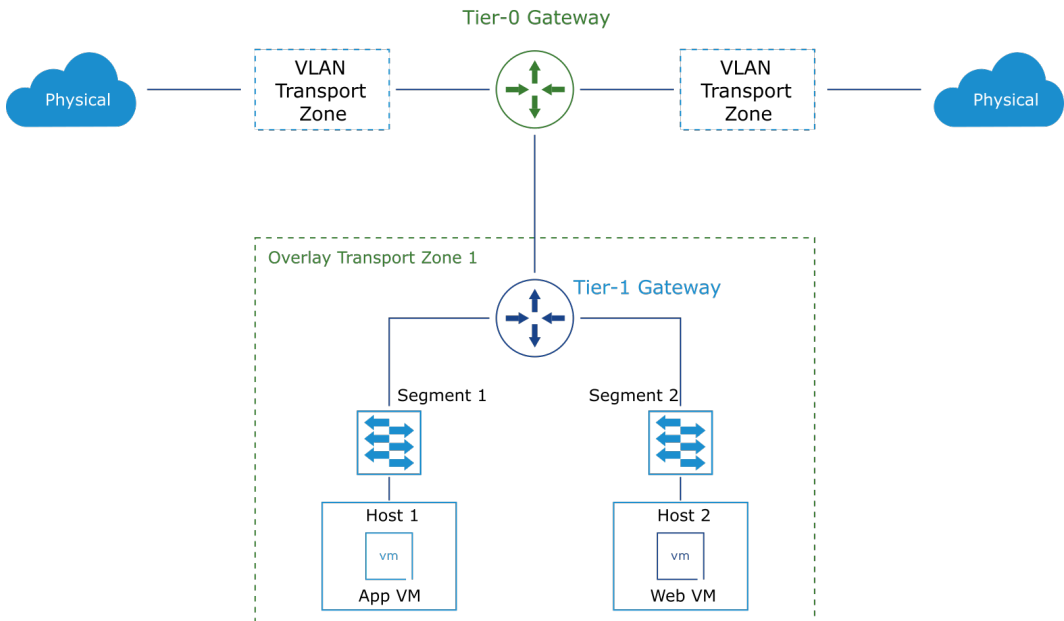
Each transport node has a TEP. Each TEP has an IP address. These IP addresses can be in the same subnet or in different subnets, depending on the IP pools or DHCP configured for the transport nodes.

## 3-46 About Transport Zones (1)

A transport zone defines the span of a logical network over the physical infrastructure.

Transport nodes can participate in the following transport zones:

- Overlay:
  - Used as the internal tunnel between NSX hosts and NSX Edge transport nodes
  - Carries Geneve-encapsulated traffic
- VLAN:
  - Used at NSX Edge uplinks to establish northbound connectivity
  - Can carry the 802.1Q tagged traffic



A transport zone defines a collection of transport nodes that can communicate with each other across a physical infrastructure over one or more interfaces (TEPs).

A transport zone can accommodate either overlay or VLAN traffic.

The VLAN transport zones are used to connect the NSX Edge uplinks and the upstream physical routers to establish north-south connectivity.

Transport nodes are ESXi hosts, NSX Edge nodes, and bare-metal nodes that participate in an NSX overlay.

## 3-47 About Transport Zones (2)

Transport zones determine which hosts can participate in a particular network and have the following characteristics:

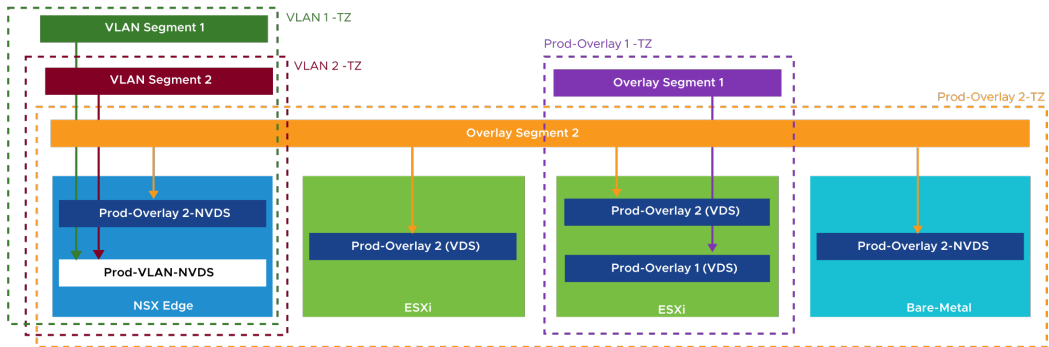
- A single transport zone can have all types of transport nodes (ESXi, bare-metal servers, and NSX Edge).
- A transport zone does not represent a security boundary.
- A transport node can belong to multiple transport zones: one overlay transport zone and multiple VLAN transport zones.
- A segment can belong to only one transport zone.

## 3-48 Transport Node Switch Configuration

A transport node uses N-VDS or VDS to connect to the transport zone.

A transport node switch can be configured in the following ways:

- ESXi transport nodes can use only VDS switches.
- N-VDS is the virtual switch supported on NSX Edge nodes, native public cloud NSX agents, and bare-metal workloads.
- Each N-VDS or VDS switch can be associated with multiple transport zones.
- Each N-VDS or VDS switch requires its own physical NICs.



Since NSX 4.0.0.1, an N-VDS host switch is not supported for ESXi hosts.

An edge transport node only has one N-VDS attached to an overlay transport zone.

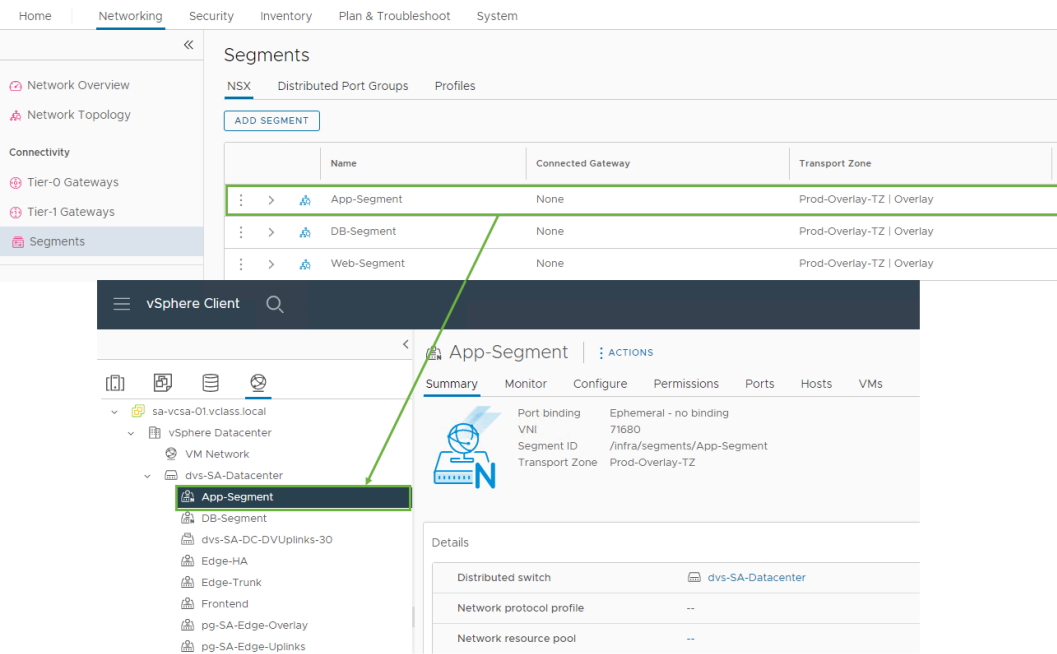
If multiple VLAN segments are backed by the same VLAN ID, only one of those segments is realized.

To validate the versions of vSphere compatible with NSX 4.0.0.1, see VMware Product Interoperability Matrix at <https://interopmatrix.vmware.com/Interoperability>.

# 3-49 About VDS

The ESXi hosts managed by vCenter Server are configured to use only VDS during the transport node preparation.

The segments from NSX Manager are realized as distributed port groups in vCenter Server.



Configuring NSX on a standalone ESXi host is no longer supported because VDS is the only supported virtual switch and an N-VDS host switch is not supported for ESXi hosts since NSX 4.0.0.1.

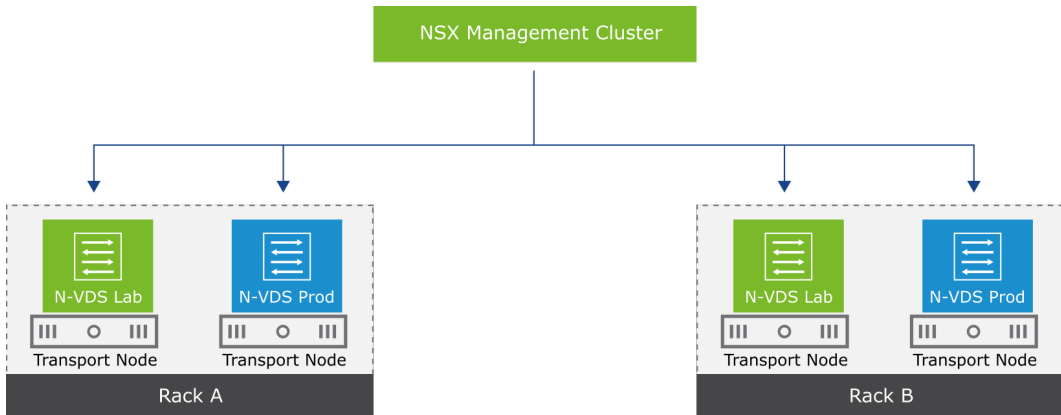
The VDS MTU size must be set to 1,600 bytes or greater from the vSphere Client to utilize it with NSX.

VDS can attach to only a single overlay transport zone and multiple VLAN transport zones.

## 3-50 About N-VDS

N-VDS is a software logical switch that provides the forwarding service on a transport node. NSX Manager creates and centrally manages each N-VDS instance.

N-VDS instances are created and distributed across NSX Edge and bare-metal transport nodes with a consistent configuration.



N-VDS performs the switching functionality on a transport node:

- N-VDS typically owns several NICs of the bare-metal transport node.
- N-VDS instances are created on a host or NSX Edge transport nodes.
- N-VDS instances configured on different transport nodes are independent.
- N-VDS has a name assigned for grouping and management.

For example, the diagram shows two N-VDS instances that are configured on the edge node and bare-metal transport nodes: one N-VDS named Lab and another N-VDS named Prod (production).

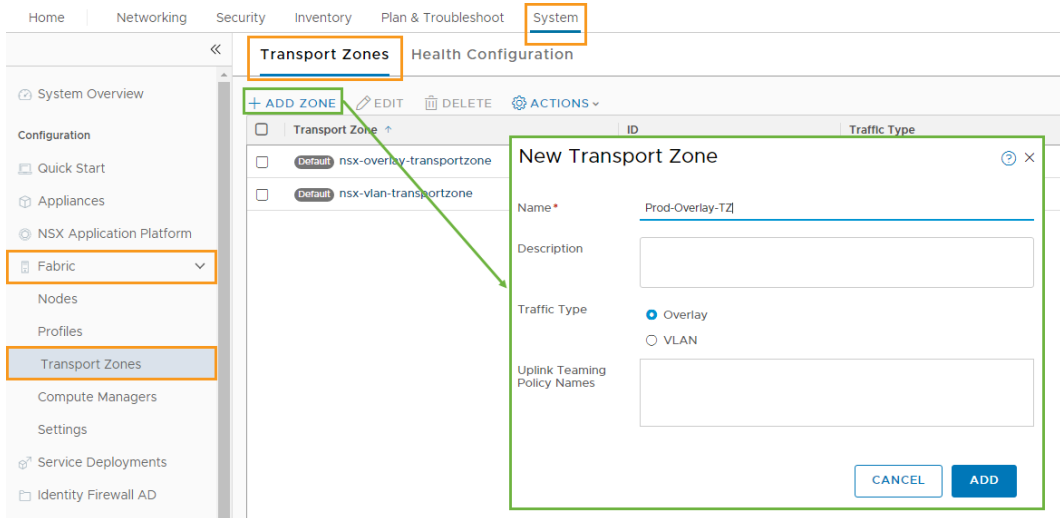


## 3-51 Creating Transport Zones

Transport zones have the following characteristics:

- Dictate which transport nodes and which workloads can participate in a network.
- When using ESXi transport nodes, transport zones can span one or more vSphere clusters.

When creating a transport zone, you must specify the traffic type.



Transport zones dictate which transport nodes and which workloads can participate in a network:

- The overlay transport zone is used by ESXi transport nodes, NSX Edge nodes, and bare-metal transport nodes for the overlay traffic.
- The VLAN transport zone is used by NSX Edge and host transport nodes for their VLAN uplinks.

An NSX environment can contain one or more transport zones, depending on your requirements.

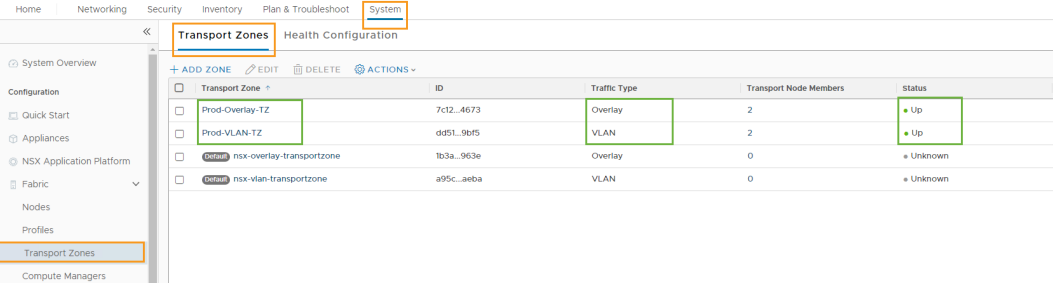
By default, NSX Manager has the following preconfigured transport zones:

- nsx-overlay-transportzone for the overlay traffic type
- nsx-vlan-transportzone for the VLAN traffic type

NSX does not allow VMs in different transport zones in the layer 2 network to connect. The span of a segment is limited to a transport zone. So virtual machines in different transport zones cannot be on the same layer 2 network.

# 3-52    Reviewing the Transport Zone Configuration

You can verify the configuration and status of your transport zones from the NSX UI.



In the example, two transport zones are created. PROD-Overlay-TZ is an overlay transport zone used by ESXi transport nodes and NSX Edge nodes. PROD-VLAN-TZ is the VLAN transport zone used by NSX Edge and ESXi transport nodes for its VLAN uplinks.

## 3-53 VDS Operational Modes

VDS switches can be configured in one of three modes based on performance requirements:

- Standard datapath: Configured for regular workloads, where normal workload traffic throughput is expected.
- Enhanced datapath: Configured for telecom workloads, where high traffic throughput is expected on the workloads.
- Enhanced Network Stack (ENS) Interrupt: An interrupt-driven version of Enhanced datapath.

### Add Transport Node Profile



Uplink Profile \*

nsx-default-uplink-hostswitch-profile

OR Create New Uplink Profile

IP Assignment (TEP) \*

Use IP Pool

IP Pool \*

TEP-IP-Pool

Teaming Policy Uplink Mapping

Uplinks	VDS Uplinks
uplink-1	Uplink 5
uplink-2	Uplink 6

Advanced Configuration

Mode \*

Standard

Standard

Enhanced Datapath – Standard

Enhanced Datapath – Performance

CANCEL

ADD

The Enhanced Data Path virtual switch is optimized for Network Function Virtualization (NFV), where the workloads typically perform networking functions with very demanding requirements in terms of latency and packet rate. To benefit from this mode, workloads must be compiled with DPDK and will use VMXNET3 for their vNIC. This mode is only available to ESX hypervisor (6.7 and later, recommended 6.7 U2 and later) and unavailable on NSX Edge nodes and Public Cloud Gateway.

ENS Interrupt and Enhanced datapath requires compatible NICs and CPU cores dedicated to packet processing to support Telco-type environments with high packet count and small packet size (64 bytes).

For information about identifying suitable hardware components, see VMware Compatibility Guide at <https://www.vmware.com/resources/compatibility/search.php>.

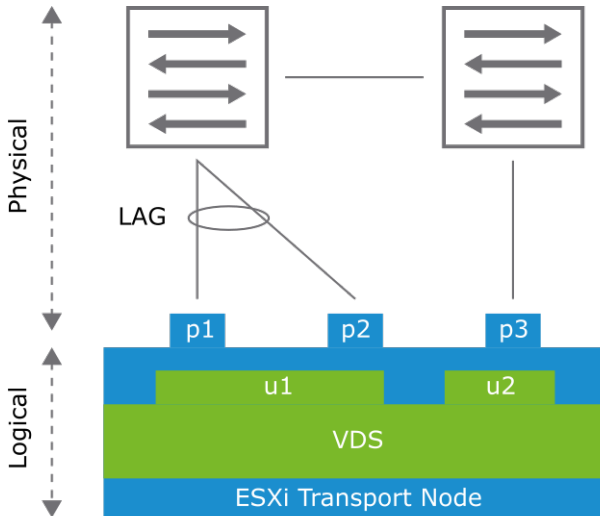
Telecom service providers use SDN to deploy network function virtualization (NFV), which virtualizes a physical server or other dedicated hardware.

## 3-54 Physical NICs, LAGs, and Uplinks

A host can have several physical ports called physical NICs. Several physical NICs can be bundled to form an aggregated link called LAG.

Uplinks are logical interfaces on VDS.

With a VDS implementation, the ESXi host uplinks must be configured to carry the overlay and VLAN traffic.



- Physical NICs on the host: p1, p2, and p3
- Uplinks on the VDS: u1, u2

**Mappings:**

- u2 maps to p3.
- u1 maps to the LAG that includes p1 and p2.

Link Aggregation Groups (LAGs) use Link Aggregation Control Protocol (LACP) for the transport network.

Map the uplinks on NSX to uplinks on VDS and not to physical NICs directly.

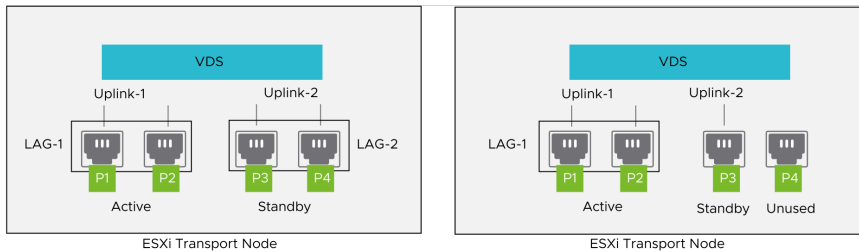
In the example, logical uplink 1 is mapped to a physical LAG (including physical port p1 and p2). Logical uplink 2 is mapped to physical port p3.

## 3-55 About Uplink Profiles

The uplink profile is a template that defines how VDS connects to the physical network.

The uplink profile specifies the following details:

- Format of the uplinks of VDS
- Default teaming policy applied to those uplinks
- Active and standby uplinks
- Transport VLAN used for overlay traffic
- MTU of the uplinks



An uplink profile is a container of properties or capabilities that you want your network adapters to have. It allows you to consistently configure identical capabilities for network adapters across multiple hosts or nodes.

When an administrator modifies a parameter in the uplink profile, it is automatically updated in all the transport nodes following the uplink profile.

If NSX Edge is installed on bare metal, you can use the default uplink profile. The default uplink profile requires one active uplink and one passive standby uplink.

# 3-56 Default Uplink Profiles

Uplink profiles enable you to configure consistent capabilities for network adapters across multiple transport nodes.

You can find the default uplink profiles by navigating to **System > Fabric > Profiles > Uplink Profiles** in the NSX UI.

HomeNetworkingSecurityInventoryPlan & TroubleshootSystem

Uplink ProfilesEdge Cluster ProfilesConfigurationTransport Node ProfilesNode Profiles

System Overview

Configuration

Quick Start

Appliances

NSX Application Platform

Fabric

Nodes

Profiles

Transport Zones

Compute Managers

Settings

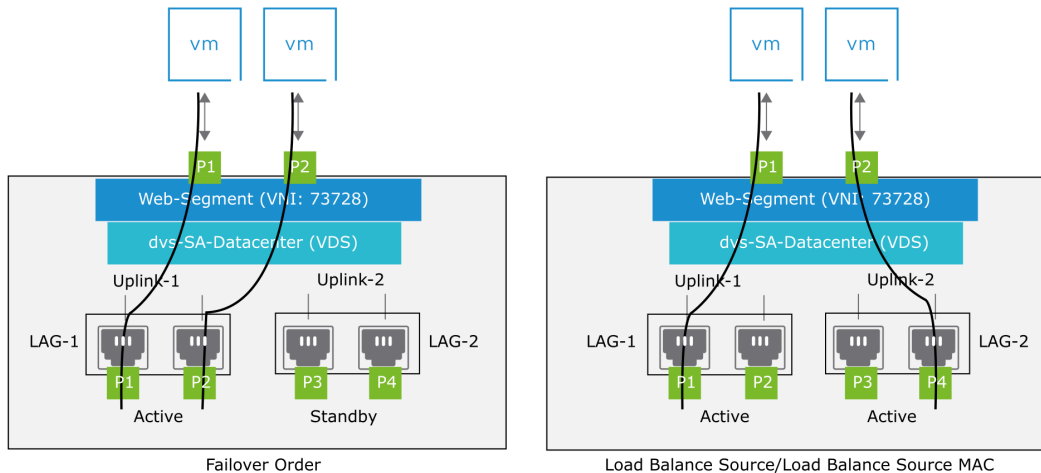
+ ADD PROFILEEDITDELETEACTIONS

Uplink Profile	ID	Teaming Policy	Active Uplinks	Standby Uplinks	Transport VLAN	MTU
<input type="checkbox"/> nix-default-loadbalance-u...	fb38...2e0d	Load Balance Source	uplink-1uplink-2uplink-3uplin...		0	1700 (Global MTU)
<input type="checkbox"/> nix-default-uplink-hostswit...	0a26...dc9f	Falover Order	uplink-1	uplink-2	0	1700 (Global MTU)
<input type="checkbox"/> nix-edge-tag-uplink-profile	x352...5f3f	Falover Order	lag		0	1700 (Global MTU)
<input type="checkbox"/> nix-edge-multiple-vrtps-u...	ce82...1107	Load Balance Source	uplink-1uplink-2		0	1700 (Global MTU)
<input type="checkbox"/> nix-edge-single-rtc-uplink...	c732...e3dc	Falover Order	uplink-1		0	1700 (Global MTU)

79

## 3-57 About Teaming Policies

As part of the uplink profile configuration, the teaming policy defines the uplink redundancy and failover model. Only one teaming policy can be applied to an entire VDS.



The teaming policy only defines how the NSX virtual switch balances traffic across its uplinks. The uplinks can in turn be individual pNICs or LAGs. A LAG uplink has its own hashing options. However, those hashing options only define how traffic is distributed across the physical members of the LAG uplink, whereas the teaming policy defines how traffic is distributed between NSX virtual switch uplinks.



# 3-58 Teaming Policy Modes

You can select a teaming policy for the new uplink profile:

- **Failover Order:** Uses one active port and a list of standby ports
- **Load Balanced Source:** Uses a list of active ports as input
- **Load Balanced Source Mac:** Determines the uplink based on the source VM's MAC address

New Uplink Profile ? ×

Name \* Labs-Uplink-Profile

Description

LAGs

+ ADD 

🗑️

 DELETE

<input type="checkbox"/> Name *	LACP Mode	LACP Load Balancing *	Uplinks *	LACP Time Out
No LAGs found				

Teamings

+ ADD 

📄

 CLONE 

🗑️

 DELETE

<input checked="" type="checkbox"/> Name *	Teaming Policy *	Active Uplinks *	Standby Uplinks
<input checked="" type="checkbox"/> [Default Teaming]	Failover Order <div>⌵</div>	uplink-1	
	Failover Order		
	Load Balance Source		
	Load Balance Source MAC Address		

Active uplinks and Standby uplinks are used to associate with the Physical NICs while adding Transport Nodes. ~~deleted nodes, these nodes will be used~~

Transport VLAN 

0

⌵

MTU 

1700

⌵

🔊

 Note: For N-VDS, if left empty, the default value will be 1700. MTU is not applicable for VDS.

CANCEL

ADD

The image shows that you can specify a type of teaming policy for the uplink profile.

You can select from the following teaming policy modes:

- **Failover Order:** An active uplink is specified with an optional list of standby uplinks. If the active uplink fails, the next uplink in the standby list replaces the active uplink. No actual load balancing is performed with this option.
- **Load Balanced Source:** A list of active uplinks is specified, and each interface on the transport node is pinned to one active uplink based on the source port ID. This configuration allows use of several active uplinks at the same time.
- **Load Balanced Source Mac:** This option determines the uplink based on the source VM's MAC address.

The number of VTEPs on transport nodes is determined by the NIC teaming policy:

- The failover order NIC teaming policy creates a single VTEP on transport nodes.
- The load balance source and source MAC create multiple VTEPs on transport nodes.

## 3-59 About LLDP

The Link Layer Discovery Protocol (LLDP) is used to advertise a device’s identity, the device’s abilities, and other devices connected in the same network.

LLDP provides the following benefits:

- Simplifies the use of network management tools in a multivendor environment
- Provides accurate discovery of physical network topologies, which simplifies troubleshooting in enterprise networks

LLDP is configured as a vCenter Server distributed switch advanced property in the vSphere Client.

Distributed Switch - Edit Settings | dvs-SA-Datacenter X

General

Advanced

Uplinks

MTU (Bytes)

9000

Multicast filtering mode

IGMP/MLD snooping

Discovery protocol

Type

Cisco Discovery Protocol

Operation

(disabled)  
Cisco Discovery Protocol  
Link Layer Discovery Protocol

Administrator contact

Name

Other details

CANCEL

OK

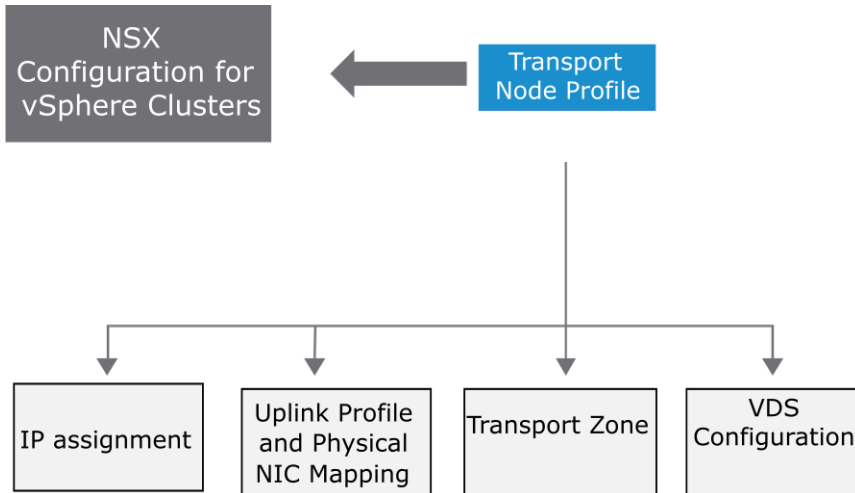
## 3-60 About Transport Node Profiles

A transport node profile captures the configuration required to create a transport node.

The transport node profile can be applied to an existing vSphere cluster to create transport nodes for the member hosts.

A transport node profile defines:

- Transport zones
- VDS switch configuration
- Uplink profile
- IP assignment
- Mapping of physical NICs



Transport node creation begins when a transport node profile is applied to a vSphere cluster.

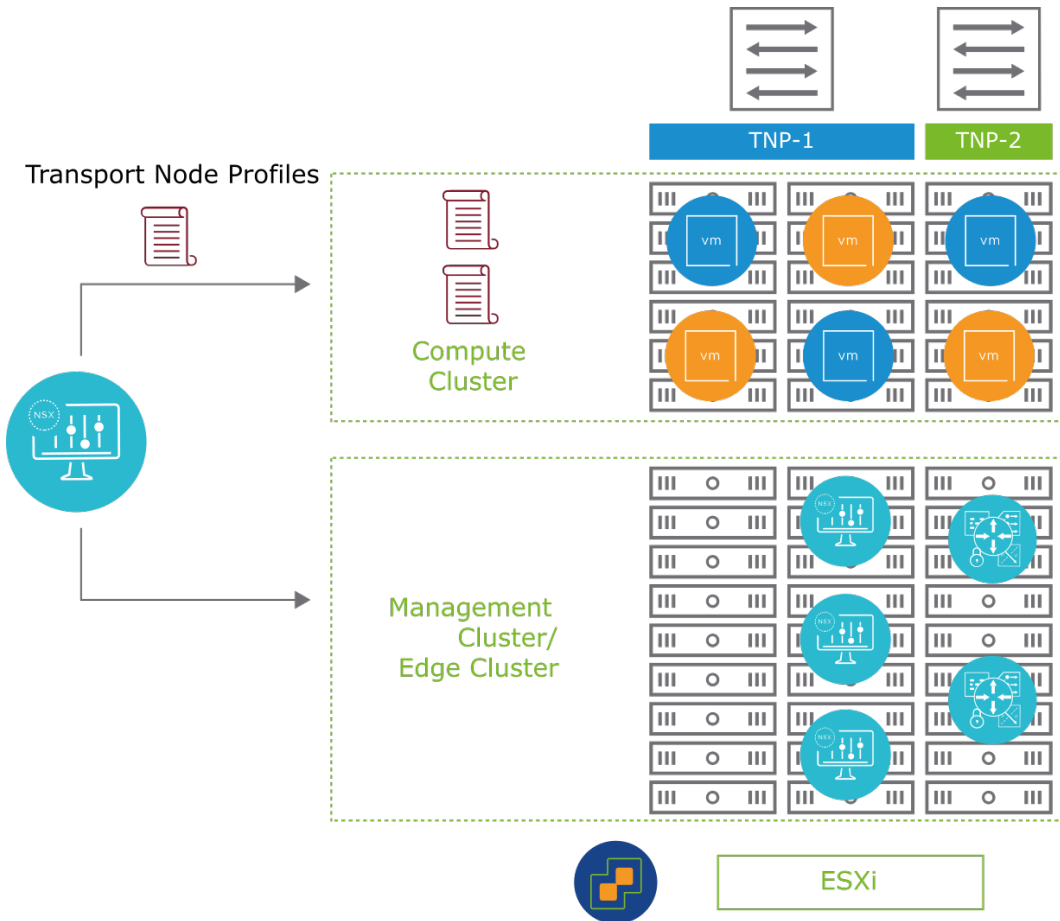
NSX Manager prepares the hosts in the cluster and installs the NSX components on them.

Transport nodes are created based on the configuration specified in the transport node profile.

## 3-61 Benefits of Transport Node Profiles

Transport node profiles make deployments easier for customers by using vSphere clusters:

- Speed deployments
- Enable the faster deployment of NSX infrastructure components
- Drive consistency and avoid manual errors
- Can be reused multiple times



## 3-62 Prerequisites for Transport Node Profile

Before you configure transport node profiles, several requirements must be met:

- The ESXi hosts planned to configure NSX are part of a vCenter Server instance.
- The ESXi hosts are added in the vSphere cluster.
- The vCenter Server instance is added to NSX Manager as a compute manager.
- The transport zone is configured.
- An IP address pool is configured, or the DHCP server is available in the network.

## 3-63 Creating a Transport Node Profile

You create a transport node profile with the VDS setting and define the transport zone.

Add Transport Node Profile

Name \*

ESXi-TN-Profile

Description

+ ADD SWITCH

New Node Switch

Name \*

sa-vcsa-01.vclass.local

dvs-SA-Datacenter

Transport Zone \*

Prod-Overlay-TZ

OR Create New Transport Zone

Uplink Profile \*

nsx-default-uplink-hostswitch-profile

OR Create New Uplink Profile

CANCEL

ADD

Add Transport Node Profile

IP Assignment (TEP) \*

Use IP Pool

IP Pool \*

TEP-IP-Pool

Teaming Policy Uplink Mapping

Uplinks	VDS Uplinks
Uplink-1	Uplink 5
Uplink-2	Uplink 6

Advanced Configuration

Mode \*

Standard

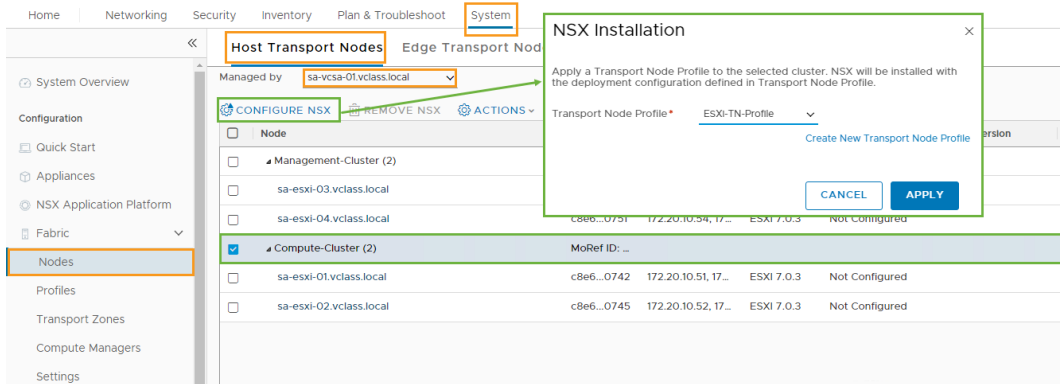
CANCEL

ADD

When modifying a transport node profile, the clusters using that profile are immediately updated. Also, when an ESXi host is added to a cluster, the host is updated with the transport node profile attached to the cluster.

## 3-64 Attaching a Transport Node Profile to the vSphere Cluster

You apply a transport node profile to a vSphere cluster.



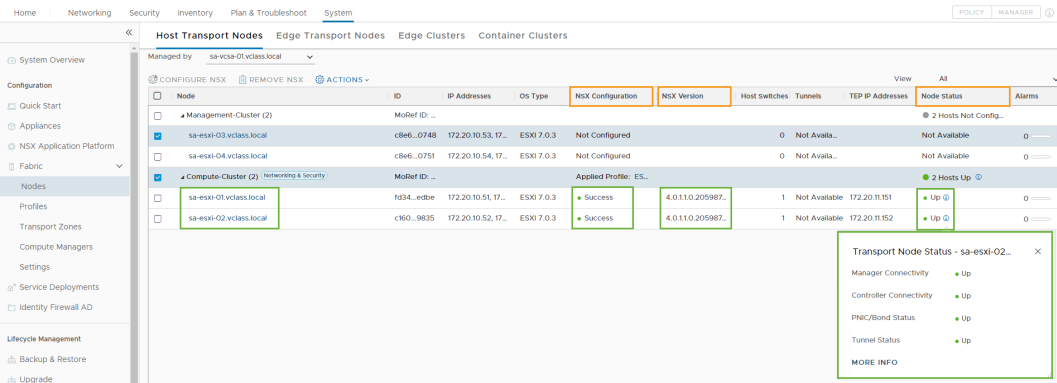
To configure NSX on ESXi hosts managed by vCenter Server in a vSphere cluster:

1. Select the vSphere cluster and click **CONFIGURE NSX**.
2. From the **Transport Node Profile** drop-down menu, select the transport node profile to attach to the vSphere cluster and click **APPLY**.

Attaching a transport node profile is required only when configuring ESXi hosts managed by vCenter Server at the cluster level.

# 3-65    Reviewing the ESXi Transport Node Status (1)

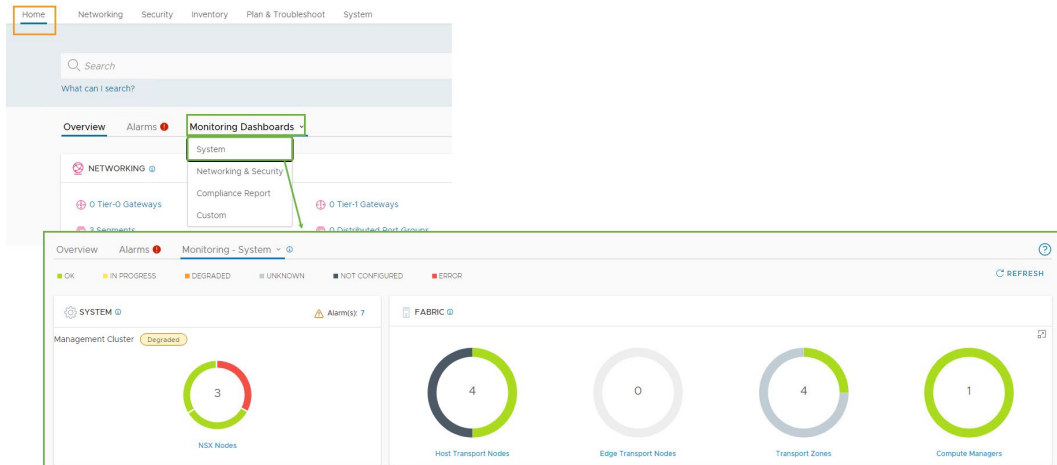
After the ESXi host is prepared, you verify that the Configuration Status appears as Success, the NSX version appears, and the Node Status appears as Up.



The screenshot shows that the ESXi hosts prepared for NSX, sa-esxi-01.vclass.local, and sa-esxi-02.vclass.local are automatically listed as transport nodes in the NSX UI.

## 3-66 Reviewing the ESXi Transport Node Status (2)

You can view the status of the host transport nodes from the NSX Manager dashboard.



You can check the status of host transport nodes in the System view of the dashboard. Point to the circle and messages appear. These messages provide details about the nodes. For example, in the screenshot, out of four nodes, two nodes are configured as transport nodes and two nodes are not configured for NSX.

The following colors define:

- Green: Indicates a healthy environment where all components are working without issues
- Red: Indicates a critical issue
- Orange: Indicates degraded performance
- Gray: Indicates not configured



## 3-67 Verifying the ESXi Transport Node by CLI

The NSX kernel modules are packaged in VIB files and downloaded to hosts. The kernel modules provide services such as distributed routing, distributed firewall, and so on.

```
[root@sa-esxi-01:~] esxcli software vib list | grep nsx
nsx-adf 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-cfgagent 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-context-mux 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-cpp-libs 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-esx-datapath 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-exporter 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-host 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-ids 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-monitoring 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-mpa 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-nestdb 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-netopa 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-opsagent 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-platform-client 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-proto2-libs 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-proxy 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-python-gevent 1.3.5.py35-19972216 VMware VMwareCertified
nsx-python-greenlet 0.4.14.py35-19345965 VMware VMwareCertified
nsx-python-logging 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-python-protobuf 2.6.1-19195979 VMware VMwareCertified
nsx-python-utils 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-sfhc 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-shared-libs 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsx-vdpi 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
nsxcli 4.0.1.1.0-7.0.20598730 VMware VMwareCertified
```

After an ESXi host is prepared for NSX, VIBs are installed for the host to participate in networking and security operations.

The functions of the VIBs are defined as follows:

- nsx-esx-datapath: Provides NSX data plane packet-processing functionality.
- nsx-exporter: Provides host agents that report runtime state to the aggregation service.
- nsx-host: Provides metadata for the VIB bundle that is installed on the host.
- nsx-mpa: Provides communication between NSX Manager and hypervisor hosts.
- nsx-python-protobuf: Provides Python bindings for protocol buffers.
- nsx-sfhc: Service fabric host component (SFHC) provides a host agent for managing the life cycle of the hypervisor as a fabric host.
- nsxcli: Provides the NSX CLI on hypervisor hosts.

## 3-68 Lab 4: Preparing the NSX Infrastructure

Deploy transport zones, create IP pools, and prepare hosts for use by NSX:

1. Prepare for the Lab
2. Create Transport Zones
3. Create IP Pools
4. Prepare the ESXi Hosts

## 3-69 Review of Learner Objectives

- Describe the functions of transport zones, transport nodes, N-VDS, and VDS.
- Explain the relationships between transport nodes, transport zones, N-VDS, and VDS.
- Create IP pools for the node address assignment
- Describe and configure uplink profiles
- Prepare ESXi hosts to participate in NSX networking
- Verify the status of ESXi transport nodes and VIB installation

## 3-70 Lesson 4: DPU-Based Acceleration for VMware NSX

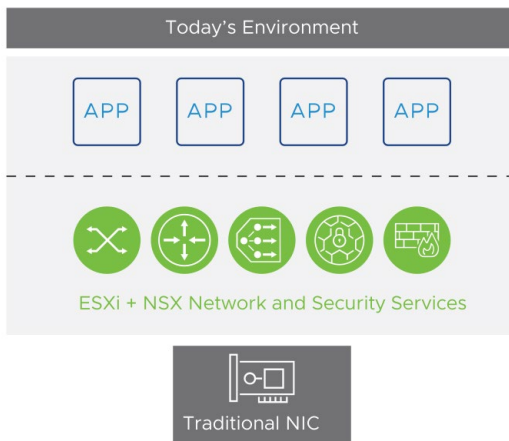
### 3-71 Learner Objectives

- Define a DPU
- Describe the use cases and benefits of DPU-based acceleration
- Explain the architectural components of a DPU
- Describe the hardware and networking configurations supported with DPUs
- Define the NSX features supported by DPUs
- Install NSX using DPUs

## 3-72 Traditional Infrastructure Challenges

Some of the challenges in today's environments include:

- Meeting new application requirements
- Shared hypervisor computing resources between applications and infrastructure (network, storage, and hypervisor management tasks)
- Effect of network and security service performance on applications
- Inadequate isolation between provider and tenant in multitenant environments based on bare-metal clouds



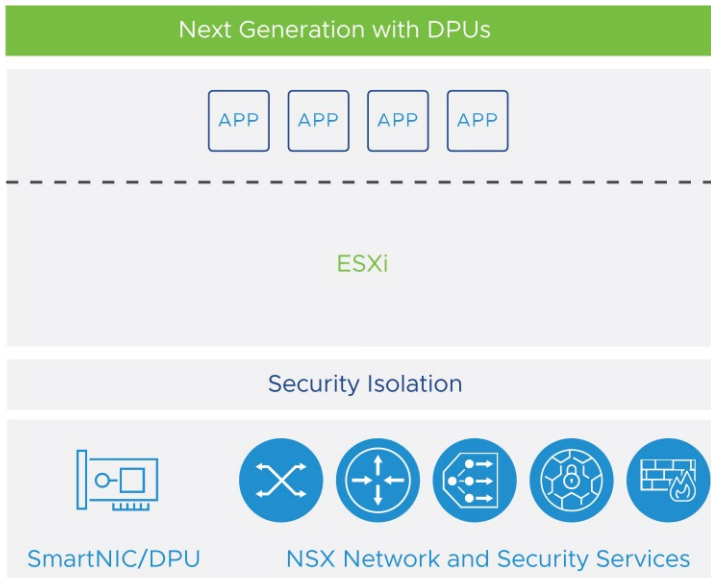
The following challenges are faced in the traditional infrastructure:

- Modern applications require speed of delivery, application availability, security of applications, and better performance
- Hypervisor computing resources are not dedicated for modern applications and create CPU and I/O bottlenecks.
- Need for computing resources increases exponentially as you move to higher speeds such as 25, 100, and 200 Gbps.
- Network and security services, such as line rate speeds or encryption, have a cost on performance because the hypervisor resources are shared with other applications and infrastructure services.
- Bare-metal clouds interest customers with demands for high-performance workloads, direct hardware access, and custom multitenant environments. They do not provide the isolation between the provider network and tenant network in SDDC environments.

## 3-73 Next-Generation Infrastructure with DPUs

DPUs offer the following advantages:

- Dedicated computing resources and hardware acceleration
- Full datapath offloading to achieve high throughput and low latency
- Security services enabled in the DPU without performance impact
- Enhanced observability and operations capabilities for monitoring, troubleshooting, logging, and compliance
- Isolation between tenant and provider both on ESXi and bare-metal platforms (available in future releases)



DPUs are also called SmartNICs.

Next-generation infrastructure runs NSX services directly in the SmartNIC. This architecture is known as DPU-based acceleration for NSX.

## 3-74 DPU-Based Acceleration Use Cases

DPU-based acceleration has the following use cases:

- Applications with high network bandwidth demand and low latency
- Security services offloading for a better performance
- Enhanced observability requirements



These are the benefits of DPU-based acceleration:

- Networking offloads for high-bandwidth applications such as video streaming applications
- Security offloads for a better performance for applications with high security or encryption demands
- Enhanced observability such as duplication and encapsulation tasks for remote L3SPAN, packet captures, and IPFIX collection that are offloaded to the DPU or SmartNIC

## 3-75 SmartNICs Ecosystem

These SmartNIC or DPU vendors are currently supported.

Nvidia

AMD/Pensando

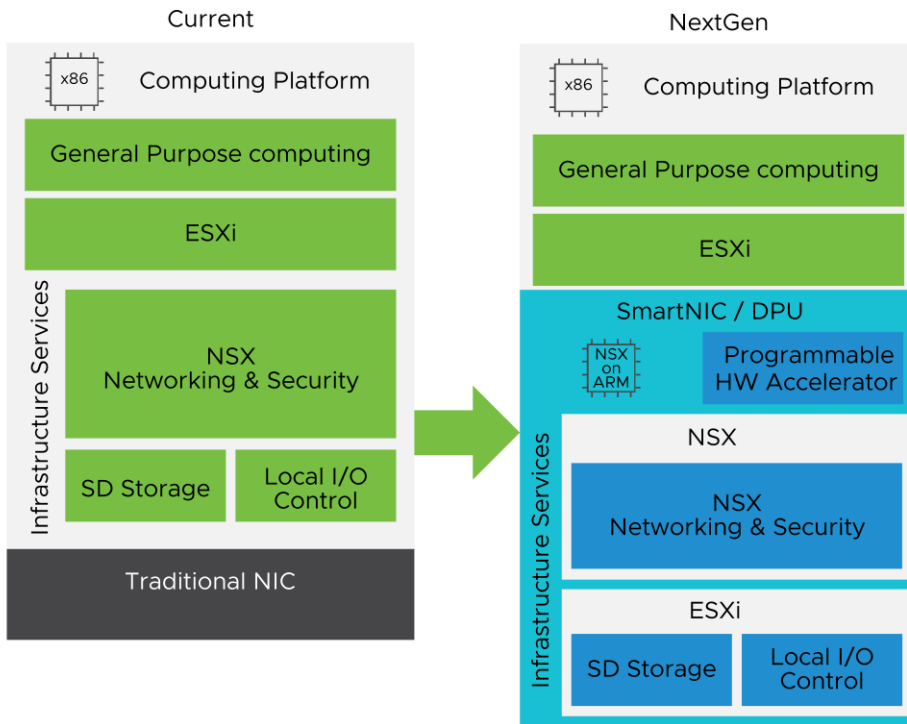
SmartNIC vendors that currently integrate with NSX are Nvidia and Pensando (AMD).

As a part of the new generation infrastructure with SmartNICs, leading system OEMs such as Dell Technologies, HPE, and Lenovo use SmartNICs in their integrated platforms.

## 3-76 Architecture Changes with DPUs

DPU-based architecture includes the following changes:

- NSX and Infrastructure services, such as storage and I/O control, are offloaded to the DPU's processor.
- ESXi and NSX instances run directly in the DPUs.



The new architecture runs the infrastructure services on the SmartNIC or DPU providing the necessary separation between application workloads that run on the x86 computing platform and the infrastructure services.

SmartNIC hardware is independent from the x86 server and has a programmable pipeline with dedicated CPUs. This architecture allows network and storage virtualization to run directly on the NIC. It saves the x86 CPU cycles and improves the performance through offload.

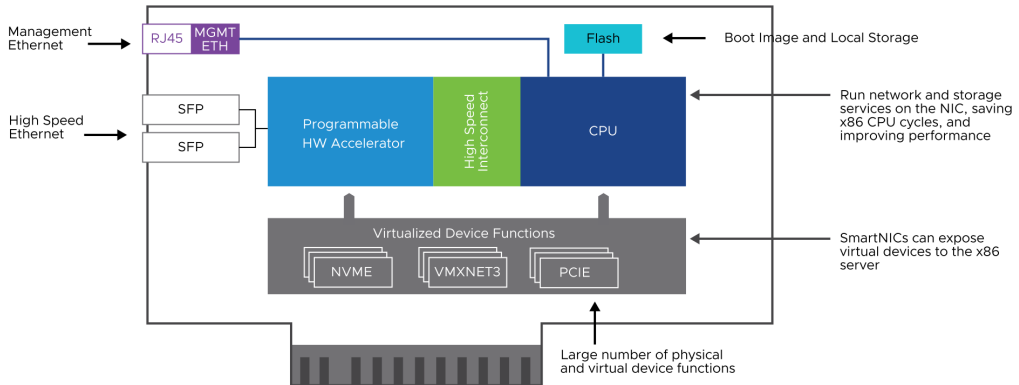
These instances are required to run the ESXi and NSX functionalities on the new architecture with DPUs:

- Lightweight ESXi that runs on the ARM processors in the DPU
- NSX components (transport node components) that run on the DPU



## 3-77 SmartNIC Hardware Components

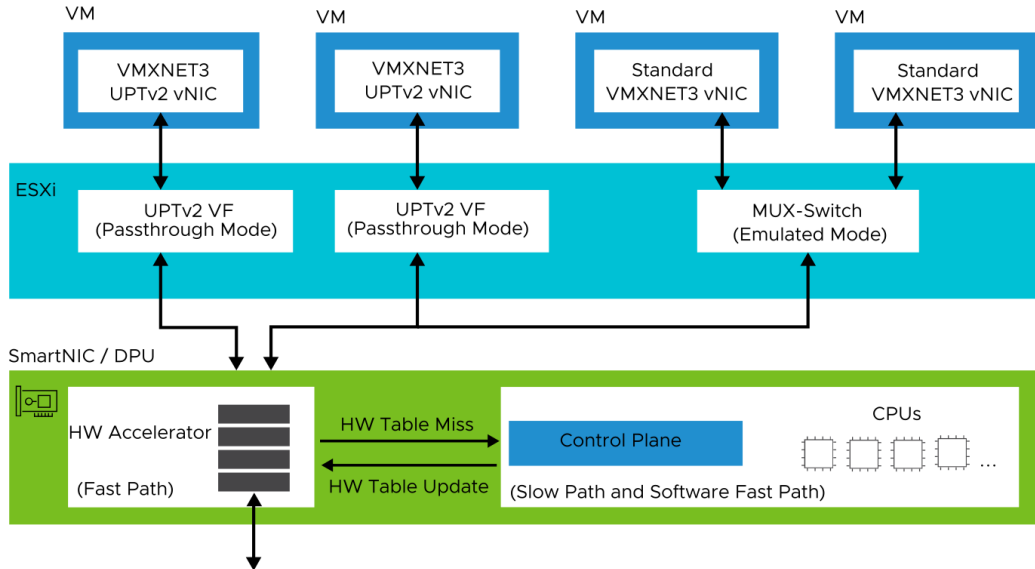
A SmartNIC or DPU has main components.



SmartNIC or DPU components:

- Flash memory to store the boot image and local storage.
- Ethernet port for management purposes.
- Two SFP ports for high-speed Ethernet (more than two ports are not supported).
- Programmable hardware accelerator packet processing pipeline for datapath offloading.
- Embedded processors with their own memory to save server x86 CPU cycles and improve network performance.
- High-speed interconnect to provide very low latency and high bandwidth communication between the programmable hardware accelerator and the SmartNIC's embedded CPUs.
- Virtualized device functions to show virtual device functions to the x86 server. Several physical and virtual devices are included (NVME, VMXNET3, and PCIE).

## 3-78 Network Offloading with SmartNICs



Network offloading on SmartNICs is achieved with the following components:

- SmartNIC contains a control plane with dedicated CPUs for slow path and software fast path forwarding.
- SmartNIC hardware accelerator is a dedicated hardware for fast path forwarding, providing line-rate speeds. This high speed can be achieved in one of the following ways:
  - NSX packet processing, currently implemented in software, can use the packet processing hardware pipelines designed in SmartNICs.
  - NSX software packet processing can be moved from the server to the SmartNIC. This method reduces the server CPU consumption and the associated cache and memory resources, which are currently shared with the VM and container workloads.
  - VMs can use passthrough VFs and use the NSX functionalities. The hardware packet processing pipeline and embedded processors can implement the NSX datapath functionalities for that traffic.

SmartNIC architecture provides the benefits of both passthrough and current NSX Enhanced Data Path with the new VMXNET3 UPTv2 drivers.

A dedicated UPTv2 VF (Virtual Functions) module implements the new UPT architecture in the ESXi.

UPTv2 Virtual Functions present the virtualized instances of the physical network adapter.

SmartNICs traffic for emulated devices, such as standard VMXNET3 VNICs, passes through a shared MUX switch implemented in the ESXi to forward the traffic.

SmartNIC support for VMXNET3 UPTv2 has the following advantages:

- VNICs can work in passthrough mode while preserving the functionalities of emulated VNICs such as vSphere vMotion.
- VMs can use networking hardware from multiple vendors without using vendor-specific guest drivers.

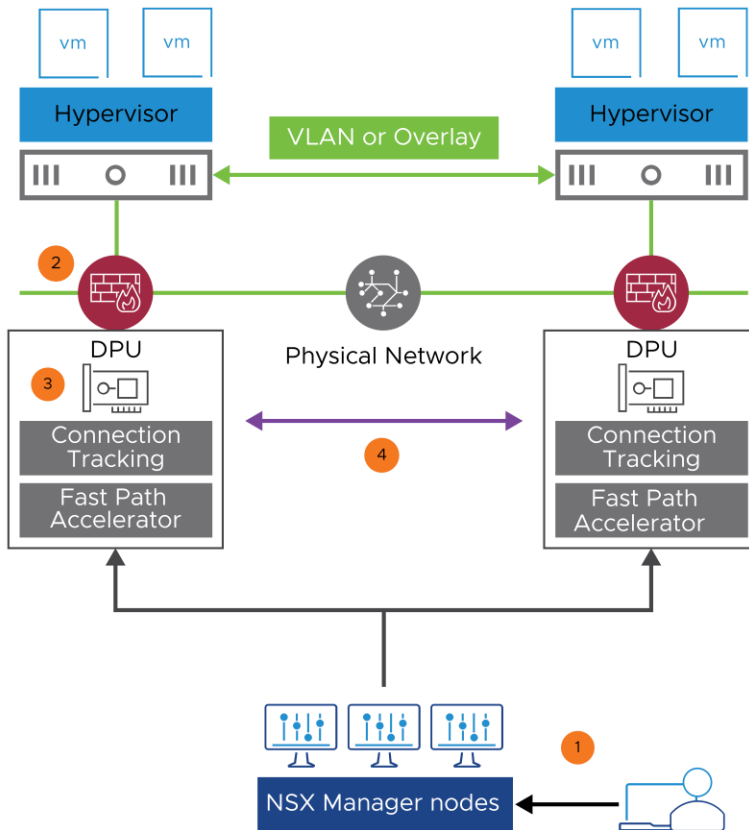
## 3-79 Supported NSX Features

NSX 4.0.1 supports the following features with DPUs:

- L2 and L3 overlay networking
- L2 VLAN networking
- Observability features such as packet capture, IPFIX, TraceFlow, and port mirroring
- East-west security features such as DFW, IDS, and IPS (Tech Preview)

Technology preview (Tech Preview) software is an unreleased, concept version of a VMware software, in object form only, excluding any open-source software provided with such software. The media and documentation are provided by VMware to the licensee for which the licensee is granted a use license pursuant to an agreement.

## 3-80 NSX Traffic Flow with DPUs



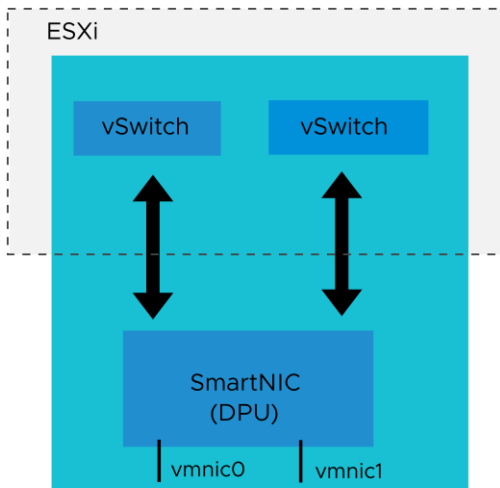
Traffic flow has the following process:

1. User enables network offloading to the DPUs.
2. When the first packet arrives, it is considered as a flow miss and processed at software level.
3. The new packet is forwarded for software slow path processing:
  - If a packet is not allowed by a rule, the packet is dropped and a flow's entry is not created.
  - If the packet is allowed, a flow entry is created.
4. When the software processing successfully inserts a flow entry, it programs the flows (fastpath flows) in the DPU hardware for faster processing.

## 3-81 Networking Configurations: SmartNIC Only

You can configure an ESXi with a SmartNIC with the following considerations:

- Only one SmartNIC is supported per host in NSX 4.0.1.
- SmartNIC uplinks can only be attached to vSphere Distributed Switch (VDS) compatible with network offloads.
- A SmartNIC has two uplinks so that it can be associated with a maximum of two virtual switches.



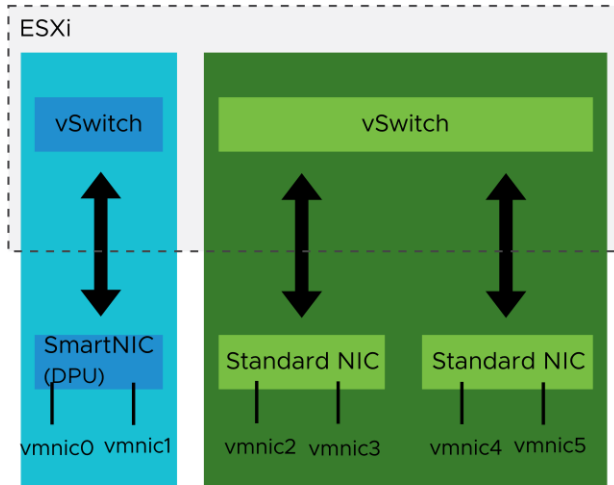
SmartNIC (DPU) Only

Current uplink profiles, such as active-active, active-standby, and LAG, are supported with SmartNICs.

## 3-82 Networking Configurations: SmartNIC with Standard NICs

You can configure ESXi with a SmartNIC and standard NICs with the following considerations:

- Uplinks from SmartNICs and standard NICs must not be part of the same VDS.
- Uplink profiles on SmartNICs must use the uplinks from the same SmartNIC.



SmartNIC (DPU) with Standard NICs

## 3-83 Installing NSX with DPUs (1)

Create a vSphere 8.0 VDS version with the network offloads compatibility enabled.

The screenshot shows the 'New Distributed Switch' wizard in vSphere, specifically the 'Configure settings' step. On the left, a sidebar lists four steps: '1 Name and location', '2 Select version', '3 Configure settings' (which is highlighted with a dark blue bar), and '4 Ready to complete'. The main area is titled 'Configure settings' and includes a close button (X) in the top right. Below the title, a subtitle reads: 'Specify network offloads compatibility, number of uplink ports, resource allocation and default port group.' The settings are as follows: 'Network Offloads compatibility' is a dropdown menu currently showing 'None', with a list of options 'None', 'Pensando', and 'NVIDIA BlueField' (the last two are highlighted in blue); 'Number of uplinks' is a text input field with the value '4'; 'Network I/O Control' is a dropdown menu set to 'Enabled'; 'Default port group' has a checked checkbox labeled 'Create a default port group'; and 'Port group name' is a text input field with the value 'DPortGroup'. At the bottom right, there are three buttons: 'CANCEL' (light blue), 'BACK' (light blue with a border), and 'NEXT' (dark blue).

Select **Configure settings** > **Network Offloads compatibility** and select a supported SmartNIC from the drop-down menu. NVIDIA BlueField and Pensando are the available options.

A vSphere 8.0 distributed switch with network offloads compatibility enabled is required to connect hosts with DPUs.

Installation is only supported in greenfield deployments.

## 3-84 Installing NSX with DPUs (2)

Add a host with a DPU installed to the VDS.

nsx-offload-dswitch - Add and Manage Hosts

1 Select task

2 Select hosts

3 Manage physical adapters

4 Manage VMkernel adapters

5 Migrate VM networking

6 Ready to complete

Select hosts

Select hosts to add to this distributed switch.

① Hosts compatibility on this switch is set to NVIDIA BlueField.

All hostsSelected (1)

SELECT ALLCLEAR SELECTIONCOMPATIBLEINCOMPATIBLE

<input checked="" type="checkbox"/>	Host	Host state	Cluster	Compatibility
<input checked="" type="checkbox"/>	w2-hs-dmz-f0609.isvlab.vmware.com	Connected	N/A	Compatible

☒ 11 hosts1 hosts

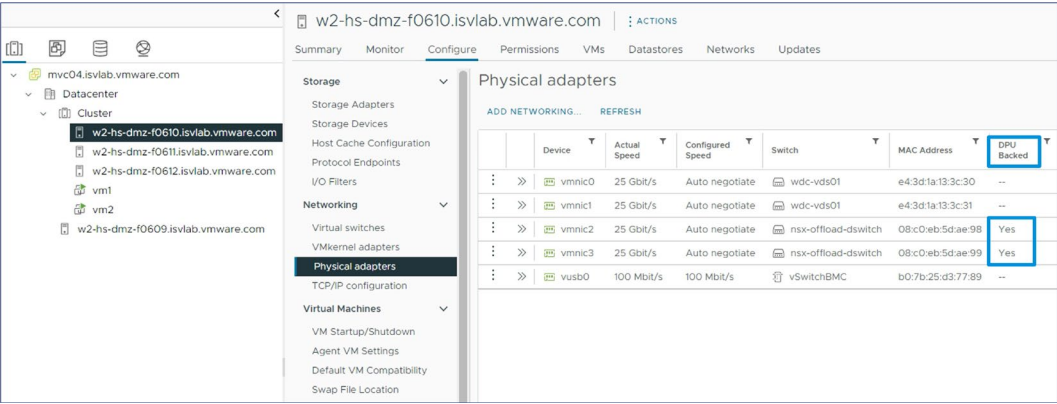
CANCELBACKNEXT

You can filter the hosts that are compatible by turning on the **Compatible** toggle.



# 3-85 Installing NSX with DPUs (3)

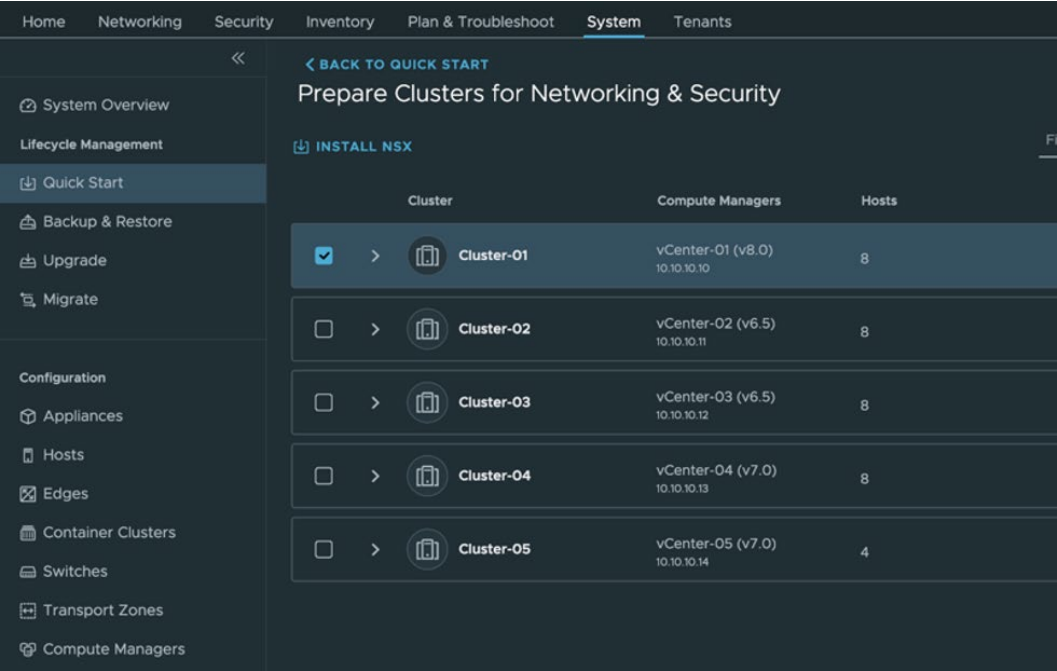
Select **Physical adapters** by navigating to the host menu **Configure > Networking** to validate that the DPU adapters (SmartNIC) are detected.



In the screenshot, `vmnic2` and `vmnic3` are DPU-backed adapters (SmartNIC).

# 3-86 Installing NSX with DPUs (4)

Select the cluster and click **Install NSX** to install NSX in a cluster with the DPU adapters.



Select the cluster that is connected to the virtual distributed switch configured with network offloads compatibility.

## 3-87 Installing NSX with DPUs (5)

Verify that the DPU uplinks exist in the cluster by reviewing the NSX installation details.

### Installation Details

NSX will be installed for the selected cluster with the following configuration.

Cluster01

8 Hosts  
ESXi 8.0

IP Assignment: DHCP

Customize Host Switch

System recommendations are prepopulated, you can modify anytime after installation.

VDS Switch: Select VDS switch

Transport Zone: TZ-01, TZ-VLAN

Uplink Profile: nsx-default-uplink-hostswitch-profile

#### Switch Teaming Policy Mapping

Uplinks	VDS Uplinks
Uplink-1 (active)	uplink1 (DPU)
Uplink-2 (standby)	uplink2 (DPU)

CANCEL INSTALL

Verify that the VDS uplinks are detected as DPUs.

# 3-88 Installing NSX with DPUs (6)

Select **Host Transport Nodes** from the **Configuration** menu and verify that the host transport nodes are DPU supported.

The screenshot shows the NSX Configuration console. On the left is a navigation menu with 'Nodes' selected. The main panel is titled 'Host Transport Nodes' and shows a list of nodes. The node 'w2-hs-dmz-f0610.isvlab.vmware.com' is selected. The 'Physical Adapters' tab is active, displaying a table of network interfaces. The 'DPU Backed' column indicates that vmnic2 and vmnic3 are DPU backed (Yes), while other interfaces are not (No).

Interface Id	Admin Status	Link Status	MTU	Interface Details	DPU Backed
vmk0	Up	Up	1500	1	No
vmk1	Up	Up	1500	1	No
vmk2	Up	Up	9000	1	No
vmk3	Up	Up	9000	1	No
vmnic0	Up	Up	9000	1	No
vmnic1	Up	Up	9000	1	No
vmnic2	Up	Up	1600	1	Yes
vmnic3	Up	Up	1600	1	Yes
vusb0	Up	Up	1500	1	No

In the screenshot, vmnic2 and vmnic3 are DPU supported.

## 3-89 Review of Learner Objectives

- Define a DPU
- Describe the use cases and benefits of DPU-based acceleration
- Explain the architectural components of a DPU
- Describe the hardware and networking configurations supported with DPUs
- Define the NSX features supported by DPUs
- Install NSX using DPUs

## 3-90 Key Points (1)

- The management plane, control plane, and policy functions are deployed in NSX Manager.
- You can deploy the NSX Manager nodes on ESXi hosts.
- The NSX UI has two sections called Policy and Manager.
- The ESXi hosts that are managed by vCenter Server can only use VDS during the transport node preparation.
- A transport zone defines a collection of hosts that can communicate with each other across a physical network infrastructure. Overlay and VLAN are the available types of transport zone.

## 3-91 Key Points (2)

- Uplink profiles enable you to configure consistent identical capabilities for network adapters across multiple hosts or nodes.
- A teaming policy applies to each VDS uplink and defines how VDS uses its uplinks for redundancy and load balancing.
- VIBs install kernel modules that run in the hypervisor kernel and provide services such as distributed routing, distributed firewall, and other capabilities.
- DPUs accelerate the network performance in the SDDC and allow customers to free computing resources from the hypervisors.
- The NSX instance runs directly in the DPU.

Questions?



## Module 4

# NSX Logical Switching

## 4-2 Importance

To build and run layer 2 switching in NSX, you must understand the overall architecture and components that interact during logical switching. You must deploy, configure, and manage layer 2 features that are provided by NSX, such as segments, segment profiles, and Generic Network Virtualization Encapsulation (Geneve).

## 4-3 Module Lessons

1. Overview of Logical Switching Architecture
2. Configuring Segments
3. Configuring Segment Profiles
4. Logical Switching Packet Forwarding

## 4-4 Lesson 1: Overview of Logical Switching Architecture

### 4-5 Learner Objectives

- Describe the functions of NSX segments
- Recognize different types of segments
- Explain tunneling and the Geneve encapsulation protocol
- Describe the interaction between components in logical switching



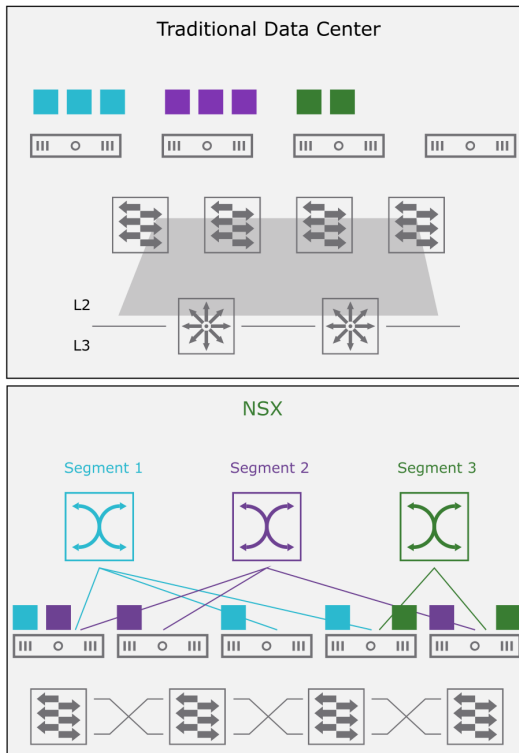
## 4-6 Use Cases for Logical Switching

Traditional data center switching challenges:

- Multitenant or application segmentation
- VM mobility requirement of layer 2 everywhere
- Large layer 2 physical network sprawl because of STP issues
- Hardware memory table (MAC and FIB) limits

NSX logical switching benefits:

- Scalable multitenancy across the data center
- Ability to use the existing physical topology
- Enabling layer 2 over layer 3 infrastructure by using overlay networks
- Segments that span across physical hosts and network switches



## 4-7 Prerequisites for Logical Switching

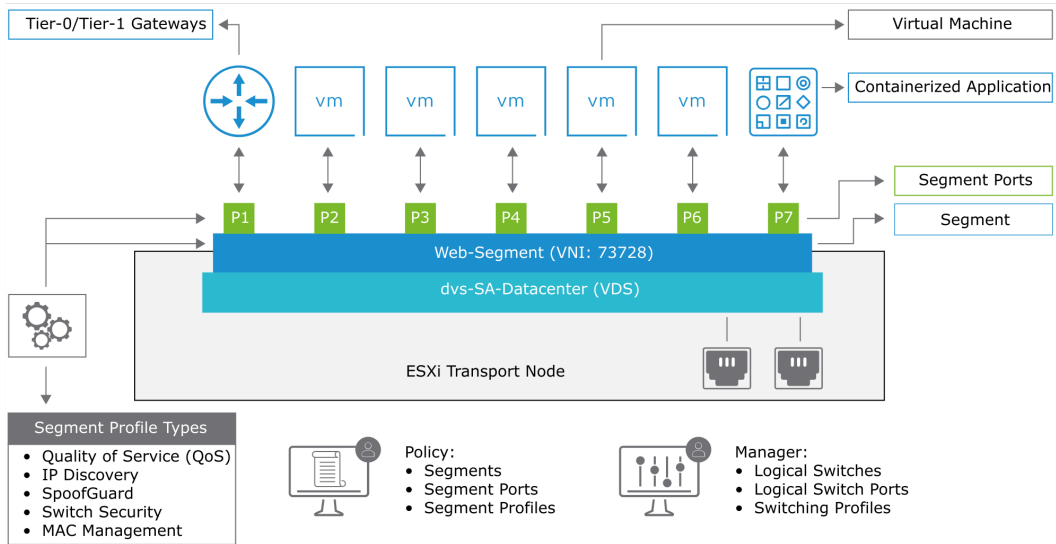
Before configuring logical switching, ensure that the following conditions are met:

- The NSX management cluster must be formed, stable, and ready to use.
- The transport nodes preparation must be complete.

Transport nodes are ESXi hosts, bare-metal servers, and NSX Edge instances that participate in NSX.

## 4-8 Logical Switching Terminology

Logical switching involves several concepts.



A segment, also called a logical switch, reproduces switching functionality in an NSX virtual environment. Segments are similar to VLANs. Segments segregate networks and provide network connections to which you can attach VMs. The VMs can then communicate with each other over tunnels between ESXi hosts if the VMs are connected to the same segment. Each segment has a virtual network identifier (VNI), similar to a VLAN ID. However, unlike VLANs, VNIs scale beyond the limits of VLAN IDs.

A segment contains multiple segment ports. Entities such as routers, VMs, or containers are connected to a segment through the segment ports.

Segment profiles include layer 2 networking configuration details for logical switches and logical ports. NSX Manager supports several types of switching profiles and maintains one or more system-defined default switching profiles for each profile type.

Segment profiles contain different configurations of the logical ports. These profiles can be applied at a port level or at a segment level. Profiles applied on a segment are applicable on all ports of the segment unless they are explicitly overwritten at the port level. Multiple segment profiles are supported, including IP Discovery, MAC Discovery, SpoofGuard, Segment Security, and Quality of Service (QoS).

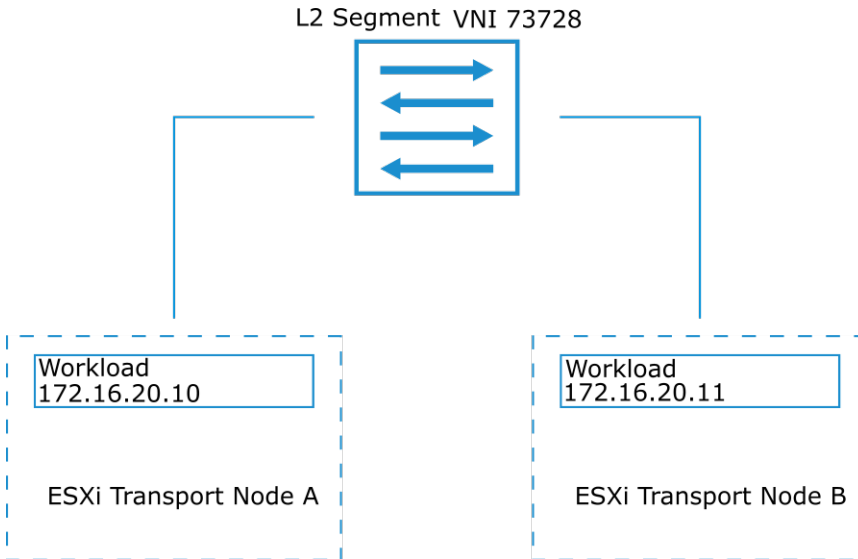
The virtual distributed switch (VDS for ESXi transport nodes and N-VDS on bare-metal servers) is configured on each transport node, which provides layer 2 functionality within the transport zone.

## 4-9 About Segments (1)

A segment is a representation of a layer 2 broadcast domain across transport nodes.

VMs attached to the same segment can communicate with each other, even across transport nodes.

Each segment is assigned a virtual network identifier (VNI), which is similar to a VLAN ID.



One or more VMs can be attached to a segment. The VMs connected to a segment can communicate with each other through tunnels between hosts.

Segments are similar to VLANs. Segments separate networks from each other. Each segment has a virtual network identifier (VNI), similar to a VLAN ID.

## 4-10 About Segments (2)

The type of segment created on a host depends on the transport zone to which it is attached.

A transport zone defines the span of a segment.

A segment is created either in an overlay or VLAN-based transport zone.

Each overlay segment is created as NSX distributed port groups in vCenter Server.

Segment configuration changes are allowed only from the NSX UI and API.

Workloads, such as VMs and containers, are connected to the segment ports.

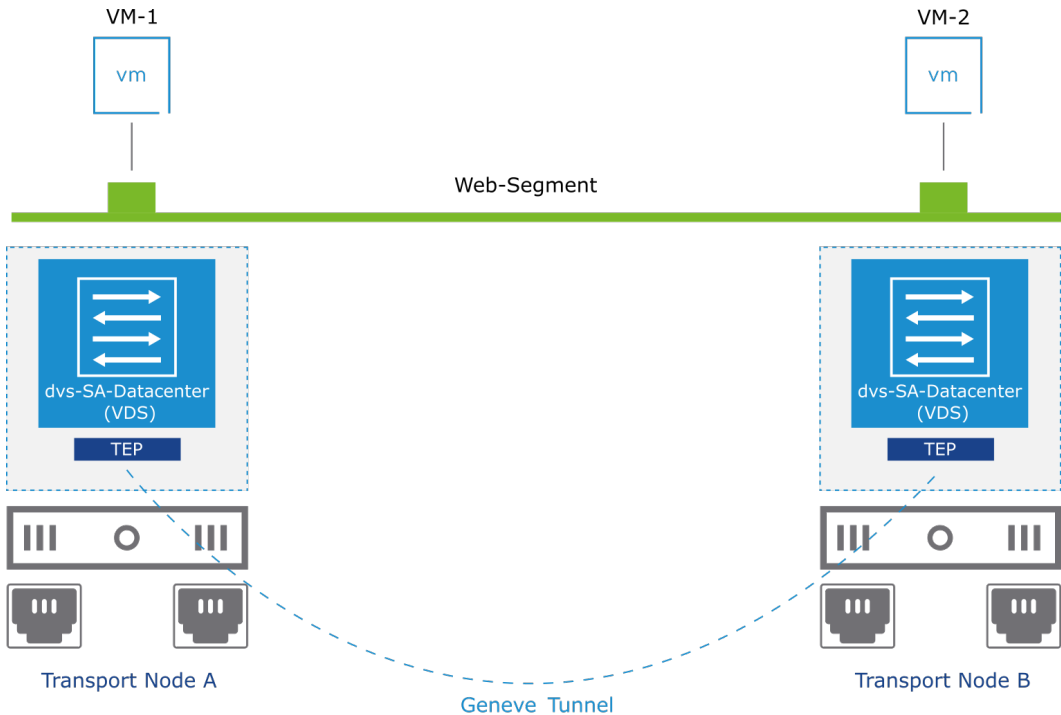
## 4-11 About Tunneling

Tunneling encapsulates the virtual network traffic data and carries it over the physical network.

NSX uses Geneve to encapsulate the data traffic.

Tunnels are set up between tunnel endpoints (TEPs).

VM frames are encapsulated with Geneve tunnel headers and sent across the tunnel.



The NSX overlay network implementation is based on tunneling. It provides isolation between the underlay network (physical network) and the overlay network (virtual network). This isolation is achieved by encapsulating the overlay frame with a Geneve header.

The underlying transport network can be another layer 2 network, or it can cross layer 3 boundaries.

The transport node endpoints in an NSX overlay network are called the tunnel endpoints (TEPs):

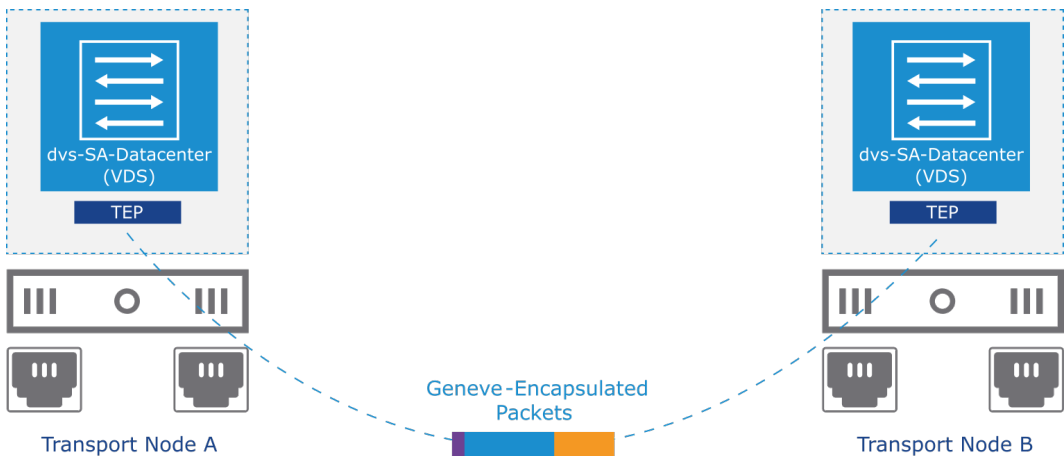
- TEPs are the source and destination IP addresses used in the external IP header to identify the transport nodes.
- TEPs typically carry two types of traffic: VM traffic and control (health check) traffic.

## 4-12 About Geneve

Geneve is an IETF overlay tunneling mechanism providing L2 over L3 encapsulation of data plane packets.

The Geneve-encapsulated packets are communicated in the following ways:

1. The source TEP encapsulates the VM's frame in the Geneve header.
2. The encapsulated UDP packet is transmitted to the destination TEP over port 6081.
3. The destination TEP decapsulates the Geneve header and delivers the source frame to the destination VM.



NSX uses a tunneling encapsulation mechanism called Geneve.

The Geneve protocol is comparable to other tunneling protocols (such as VXLAN, NVGRE, and STT) and is more flexible.

The Geneve protocol encapsulates only data plane packets.

The Geneve-encapsulated packets are communicated over standard back planes, switches, and routers:

- Packets are sent from one tunnel endpoint to one or more tunnel endpoints using unicast addressing.
- The Geneve protocol does not modify the end-user application and the VMs in which the application runs.
- The tunnel endpoint encapsulates the end-user Ethernet frame in the Geneve header.
- The completed Geneve packet is transmitted to the destination endpoint in a standard User Datagram Protocol (UDP) packet. Both IPv4 and IPv6 are supported.

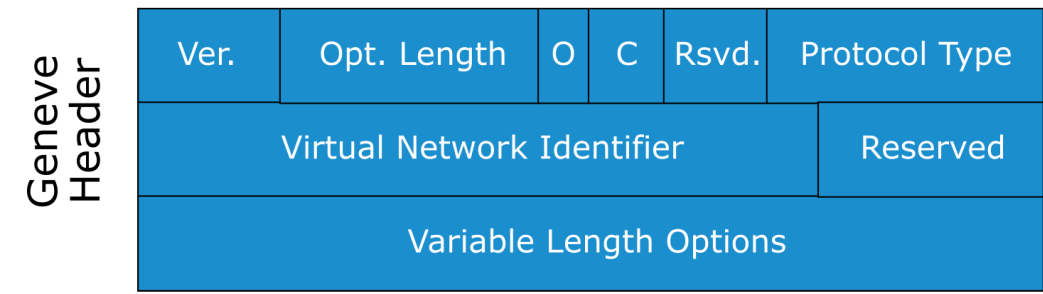
- The receiving tunnel endpoint strips the Geneve header, interprets any included options, and directs the end-user frame to its destination in the virtual network.
- The Geneve specification offers recommendations on ways to achieve efficient operation by avoiding fragmentation and taking advantage of equal-cost multipath (ECMP) routing and NIC hardware offload facilities.

# 4-13 Geneve Header Format

The Geneve protocol offers a new approach to encapsulation and offers control plane independence between tunnel endpoints.

The Geneve header has the following features:

- Runs on UDP
- Adds an 8-byte UDP header
- Uses the port number 6081
- Uses a 24-bit VNI to identify the segment
- Is supported by tcpdump and Wireshark tools



To support the needs of network virtualization, the tunneling protocol draws on the evolving capabilities of each type of device in both the underlay and overlay networks.

This process imposes a few requirements on the data plane tunneling protocol:

- The data plane is generic and extensible enough to support current and future control planes.
- Tunnel components are efficiently implemented in both hardware and software without restricting capabilities to the lowest common denominator.
- High performance over existing IP addresses is required.



The Geneve packet format includes a compact tunnel header encapsulated in UDP over either IPv4 or IPv6. A small, fixed tunnel header provides control information, as well as a base level of functionality and interoperability with a focus on simplicity. This header is followed by a set of variable options for future development. The payload consists of a protocol data unit of the indicated type, such as an Ethernet frame.

The following fields are in a Geneve header:

- Version (2 bits): The current version number is 0.
- Options Length (6 bits): This variable results in a minimum total Geneve header size of 8 bytes and a maximum of 260 bytes.
- O (1 bit): Operations, Administration, and Maintenance (OAM) packet. This packet contains a control message instead of a data payload.
- C (1 bit): This field indicates that critical options are present.
- Rsvd. (6 bits): The Reserved field must be zero on transmission and ignored on receipt.
- Protocol Type (16 bits): The field indicates the type of protocol data unit appearing after the Geneve header.
- Reserved (8 bits): The Reserved field must be zero on transmission and ignored on receipt.
- Virtual Network Identifier: A unique VNI identifies each logical network. The VNI uniquely identifies the segment that the inner Ethernet frame belongs to. It is a 24-bit number that is added to the Geneve frame, allowing a theoretical limit of 16 million separate networks. The NSX VNI range is 5,000 through 16,777,216.

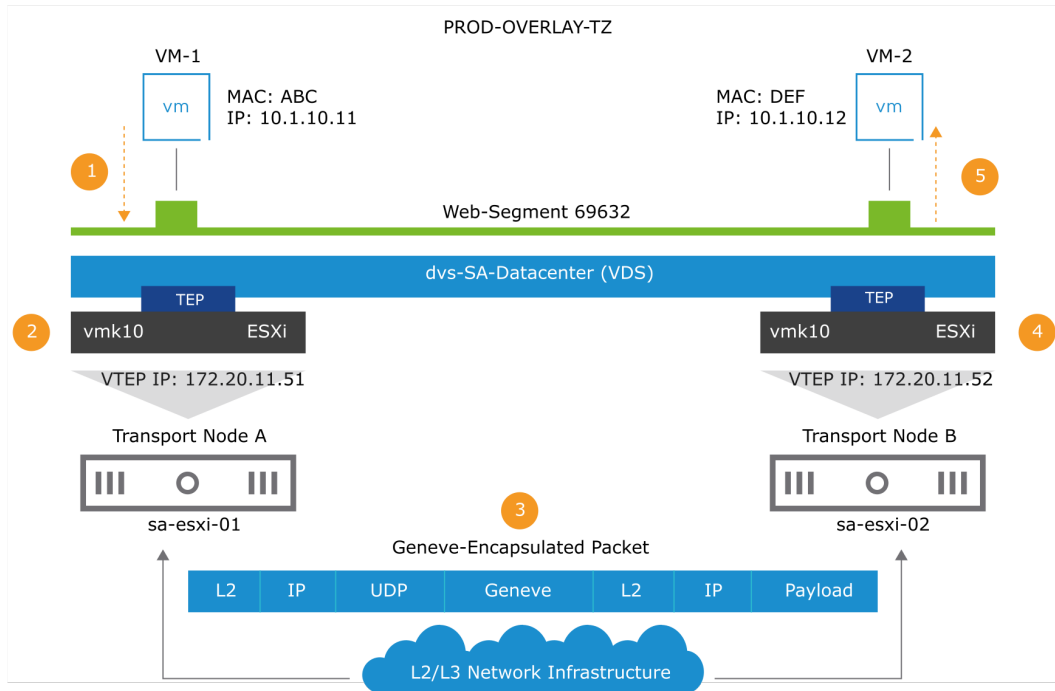
The base Geneve header is followed by zero or more options in type-length-value format. Each option includes a 4-byte option header and a variable amount of option data interpreted according to the type. Geneve provides NSX-T Data Center with the complete flexibility of inserting metadata in the type, length, and value fields that can be used for new features. One of the examples of this metadata is the VNI. You must use an MTU of 1600 to account for the encapsulation header.

The Geneve protocol offers the following benefits:

- Supports proprietary type, length, and value fields
- Can add new metadata to the encapsulation without revising the Geneve standard
- Allows VMware to develop software-based features without hardware dependencies
- Provides the same kind of NIC offloads as VXLAN (check compatibility list)
- Is open so that third-party tools, such as Wireshark, can decode it

## 4-14 Logical Switching: End-to-End Communication

Two VMs connected to the same segment communicate end to end.



The example diagram shows the following details:

- The ESXi host sa-esxi-01 is configured as a transport node using vSphere Distributed Switch (dvs-SA-Datacenter) as a host switch with TEP IP: 172.20.11.51. The VMkernel interface VMK10 is created on the ESXi host.
- The ESXi host sa-esxi-02 is configured as a transport node using vSphere Distributed Switch (dvs-SA-Datacenter) as a host switch with TEP IP: 172.20.11.52. The VMkernel interface VMK10 is created on the ESXi host.
- The sa-esxi-01 and sa-esxi-02 host transport nodes are configured in the transport zone named PROD-OVERLAY-TZ.
- Transport node A (sa-esxi-01) is running VM-1 with IP address 10.1.10.11 and MAC address ABC.

- Transport node B (sa-esxi-02) is running VM-2 with IP address 10.1.10.12 and MAC address DEF.
- VM-1 and VM-2 are connected to the segment ports on Web-Segment 69632. This web segment is an overlay-based segment configured in the transport zone named PROD-OVERLAY-TZ.
- When VM-1 communicates with VM-2, the source hypervisor encapsulates the packet with the Geneve header and sends it to the destination transport node, which decapsulates the packet and forwards it to the destination VM.

During VM-1 to VM-2 communication:

1. VM-1 sends the traffic to Web-Segment.
2. The source hypervisor encapsulates the packet with the Geneve header.
3. The source transport node forwards the packet to the physical network.
4. The destination transport node receives the packet and performs the decapsulation.
5. The destination TEP forwards the L2 frame to the destination VM.

## 4-15 Review of Learner Objectives

- Describe the functions of NSX segments
- Recognize different types of segments
- Explain tunneling and the Geneve encapsulation protocol
- Describe the interaction between components in logical switching

## 4-16 Lesson 2: Configuring Segments

### 4-17 Learner Objectives

- Use the NSX UI to create segments
- Attach VMs to segments
- Describe the workflow for segments creation
- Review the switching configuration using the Network Topology

### 4-18 Segment Configuration Tasks

To create segments and attach VMs to segments:

1. Create a segment.
2. Attach a VM to a segment.
3. Verify the segment port status.
4. Verify the layer 2 VM-to-VM connectivity.

## 4-19 Creating Segments

You use the NSX UI to create segments.

**Home** | **Networking** | Security | Inventory | Plan & Troubleshoot | System | **POLICY** | MANAGER

---

<< **Segments**

NEX Distributed Port Groups Profiles

**ADD SEGMENT** EXPAND ALL Filter by Name, Path and more

Name	Connected Gateway	Transport Zone	Subnets	Ports / Interfaces	Status	Alarms
Web-Segment	None	Prod-Overlay-TZ	172.16.10.1/24 CDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CDR e.g. fc7e:f206:db42::1/48 <a href="#">SET DHCP CONFIG</a>	Set		

Admin State ☒

> L2 VPN

> Additional Settings

Description  Tags  Scope

Max 30 allowed. Click (+) to add.

**NOTE** - Before further configurations can be done, fill out mandatory fields (\*) above and click **Save**.

SEGMENT PROFILES

**SAVE** CANCEL

A segment connects to gateways and VMs. A segment performs the functions of a logical switch.

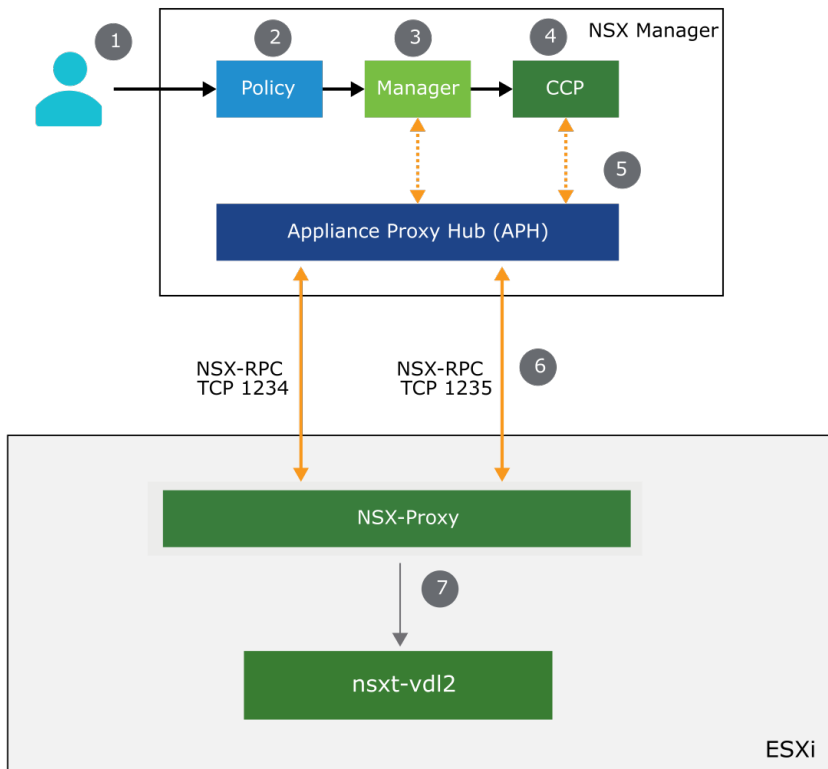
To create segments:

1. From your browser, log in to NSX Manager and select **Networking > Segments > NSX > ADD SEGMENT**.
2. In the **Segment Name** text box, enter the segment name.
3. From the **Connected Gateway** drop-down menu, select one option.
  - **None**
  - **Tier-0 Gateway**
  - **Tier-1 Gateway**
4. From the **Transport Zone** drop-down menu, select the transport zone.
5. Enter the segment subnet in the **Subnets** text box.
6. Click **Save** to save the segment configuration.

## 4-20 Creating Segments Workflow

To create segments:

1. A user creates a segment through the NSX UI.
2. The policy role pushes the configuration to the manager role.
3. NSX Manager realizes the segment information as logical switches in the Corfu database.
4. The manager role forwards the segment information to the CCP.
5. The CCP sends the information to the APH.
6. The APH service sends the switching configuration to the local control plane (nsx-proxy) over port 1235.
7. The nsx-proxy agent forwards the switching configuration to the nsxt-vdl2 kernel module, which creates and configures the segments in the datapath.



# 4-21 Viewing Configured Segments

You can connect to vCenter Server with the vSphere Client to view the configured segments.

Segments

NSX Distributed Port Groups Profiles

ADD SEGMENTEXPAND ALLFilter by Name, Path and more

	Name	Connected Gateway	Transport Zone	Subnets	Ports / Interfaces	Status	Alarms
>	App-Segment	T1-GW-01	Prod-Overlay-TZ   Overlay	172.16.20.1/24	0	Success	0
>	DB-Segment	T1-GW-01	Prod-Overlay-TZ   Overlay	172.16.30.1/24	0	Success	0
>	Web-Segment	T1-GW-01	Prod-Overlay-TZ   Overlay	172.16.10.1/24	0	Success	0

vSphere Client

dvs-SA-Datacenter

SummaryMonitorConfigurePermissionsPortsHostsVMsNetworks

Manufacturer: VMware, Inc. Version: 7.0.3

Switch Details

Notes

Tags

Features

Network I/O ControlSupported

NetFlowSupported

Link Layer Discovery ProtocolSupported

Link Aggregation Control ProtocolEnhanced support

Link Aggregation TimeoutSupported

Port mirroringSupported

IGMP/MLD snoopingSupported

Segments are represented as NSX distributed port groups in vCenter Server.

# 4-22 Attaching a VM to a Segment

You can attach a VM to a segment.

Edit Settings

sa-web-01

×

Virtual Hardware

VM Options

ADD NEW DEVICE

> CPU	1	▼	ⓘ
> Memory	2	▼	GB ▼
> Hard disk 1	16	▼	GB ▼
> SCSI controller 0	VMware Paravirtual		
> Network adapter 1 *	Web-Segment	▼	<input checked="" type="checkbox"/> Connected
> CD/DVD drive 1	Client Device	▼	<input type="checkbox"/> Connected
> Video card	Specify custom settings ▼		
VMCI device			
> Other	Additional Hardware		

CANCEL

OK

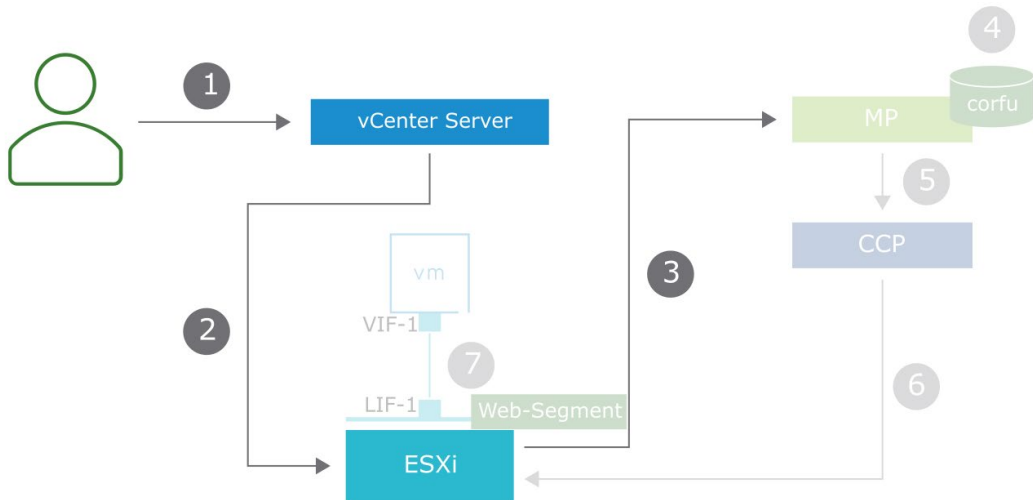
You attach the VM to the desired segment by editing its settings in the vSphere Client.



## 4-23 Workflow: Attaching a VM to a Segment (1)

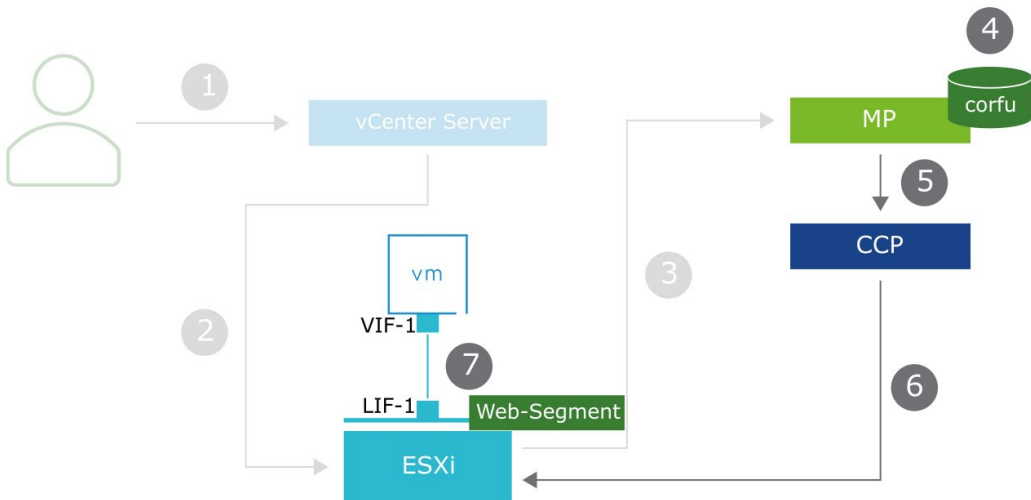
To attach a VM managed by vCenter Server to a segment:

1. You attach a VM to a segment (Web-Segment in this example) from vCenter Server.
2. vCenter Server sends the request to the ESXi host.
3. The ESXi host sends the request to the management plane.



## 4-24 Workflow: Attaching a VM to a Segment (2)

4. NSX Manager configures logical interface 1 (LIF 1) on the segment with a virtual interface (VIF 1) attachment.
5. NSX Manager advertises the attachment configuration to the CCP.
6. The CCP sends the request to the ESXi host on which the VM resides.
7. LIF 1 is created on Web-Segment with VIF 1 attached.



# 4-25 Verifying the Segment Port Status

You verify that the status of the segment and the status of the port (to which the VM is connected) appear as Success. VMs attached to the same segment should be able to ping each other.

Segments

NSX

Distributed Port Groups

Profiles

ADD SEGMENT

EXPAND ALL

Filter by Name, Path and more

	Name	Connected Gateway	Transport Zone	Subnets	Ports / Interfaces	Status	Alarms
	Web-Segment	T1-GW-01 Gateway Connectivity <span>● On</span>	Prod-Overlay-TZ   Overlay	172.16.10.1/24	<span>2</span>	<span>● Success</span>	0

Admin State ● Up

> L2 VPN

> Additional Settings

Description Not Set

> SEGMENT PROFILES

> EVPN

Set Segment Ports / View Gateway Interfaces

Segment Web-Segment Ports / Interfaces

Segment Ports (2) Gateway interfaces (0)

ADD SEGMENT PORT

EXPAND ALL

Filter by Name, Path and more

	Segment Port Name	Connected To	Admin State	Status
>	sa-web-01 vmx@ab9f8291-5fda-416a-9257-57833498b17d	ID: ab9f8291-5fda-416a-9257-57833498b17d Type: <a href="#">View More</a>	<span>● Up</span>	<span>● Success</span>
>	sa-web-02 vmx@fa0c615c-dfcf-445a-984e-c3d9823dd011	ID: fa0c615c-dfcf-445a-984e-c3d9823dd011 Type: <a href="#">View More</a>	<span>● Up</span>	<span>● Success</span>

REFRESH

1 - 2 of 2

CLOSE

VIEW STATISTICS

RELATED GROUPS

NEW DAD STATUS

After you successfully set up the segment and attach VMs to it, you can test the connectivity between VMs on the same segment. In the example, you can test the connectivity in the following way:

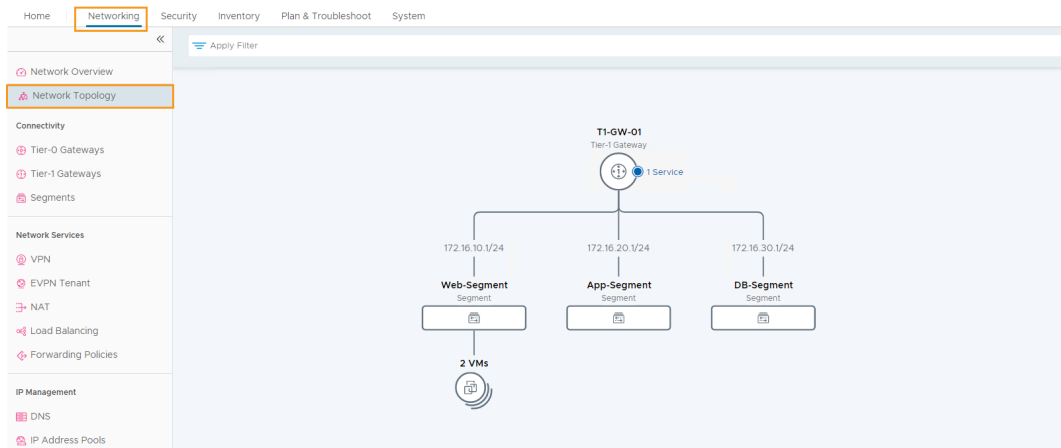
- Using SSH or the VM console, log in to the sa-web-01 (172.16.10.11) VM, which is attached to Web-Segment.
- Ping the sa-web-02 (172.16.10.12) VM, which resides on another ESXi host. This VM is also attached to Web-Segment.

## 4-26 About Network Topology

The Network Topology feature enables users to understand how the different NSX networking components are configured and interconnected.

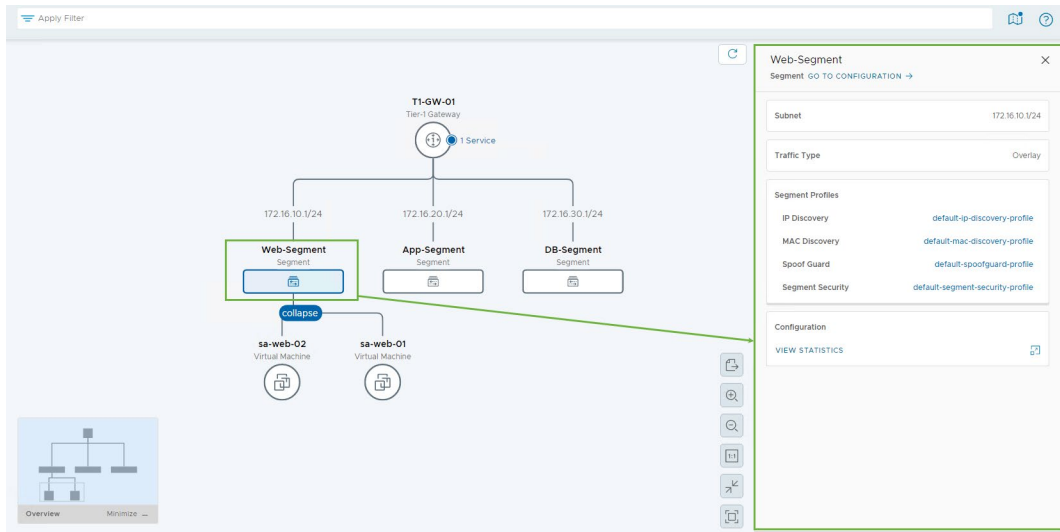
This feature displays:

- Tier-0 and Tier-1 gateways with their attached segments and workloads
- Details for each VM, segment, and Tier-1 and Tier-0 gateways
- IP addresses configured in the network
- Underlying fabric infrastructure details of the network topology



## 4-27 Using Network Topology to Validate the Segment Configuration

The Network Topology tool shows the segment configuration and the VMs that are attached to segments.



If you click the individual segment, a panel opens with details about the segment, such as the subnet, traffic type, and the attached segment profiles as shown in the screenshot.

## 4-28 Review of Learner Objectives

- Use the NSX UI to create segments
- Attach VMs to segments
- Describe the workflow for segments creation
- Review the switching configuration using the Network Topology

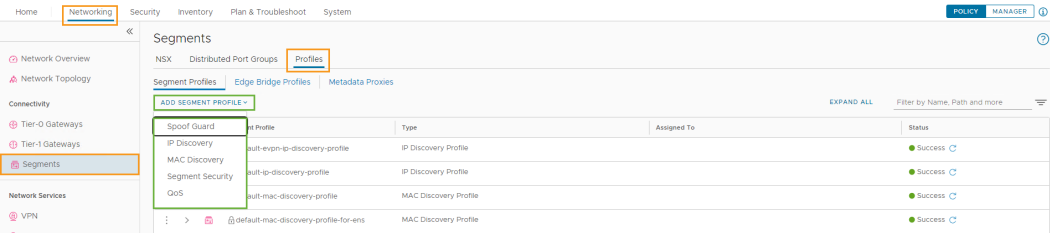
# 4-29 Lesson 3: Configuring Segment Profiles

## 4-30 Learner Objectives

- Describe the purpose of segment profiles
- Identify the functions of the segment profiles in NSX
- Create segment profiles and attach them to segments and ports

## 4-31 About Segment Profiles (1)

Segment profiles provide layer 2 networking configuration details for segments and ports. You can create various types of segment profiles from the NSX UI.



## 4-32 About Segment Profiles (2)

Each type of segment profile has a different function:

Segment Profile	Function
SpoofGuard	Helps prevent NIC spoofing by authenticating the IP and MAC address of the virtual NIC
IP Discovery	Learns the VM MAC and IP addresses
MAC Discovery	Supports MAC learning and MAC address change
Segment Security	Provides stateless layer 2 and layer 3 security
Quality of Service (QoS)	Provides high-quality and dedicated network performance for preferred traffic

NSX supports several types of segment profiles and maintains one or more system-defined default segment profiles:

- SpoofGuard prevents traffic with incorrect source IP and MAC addresses from being transmitted.
- The IP Discovery profile uses DHCP snooping, Address Resolution Protocol (ARP) snooping, or VMware Tools to learn the VM MAC and IP addresses.
- The MAC Discovery profile supports two functionalities: MAC learning and MAC address change.
- Segment Security provides stateless layer 2 and layer 3 security by checking the ingress traffic to the segment and matching the IP address, MAC address, and protocols to a set of allowed addresses and protocols. Unauthorized packets are dropped.
- QoS provides high-quality and dedicated network performance for preferred traffic.

# 4-33 Default Segment Profiles

The system default segment profiles are not editable.

Segments

NSX Distributed Port Groups Profiles

Segment Profiles Edge Bridge Profiles Metadata Proxies

ADD SEGMENT PROFILE

EXPAND ALL Filter by Name, Path and more

	Segment Profile	Type	Assigned To	Status
>	default-evpn-ip-discovery-profile	IP Discovery Profile		Success
>	default-ip-discovery-profile	IP Discovery Profile		Success
>	default-mac-discovery-profile	MAC Discovery Profile		Success
>	default-mac-discovery-profile-for-ens	MAC Discovery Profile		Success
>	default-non-vif-segment-security-profile	Segment Security Profile		Success
>	default-non-vif-segment-security-profile-f	Segment Security Profile		Success
>	default-qos-profile	QoS Profile		Success
>	default-segment-security-profile	Segment Security Profile		Success
>	default-segment-security-profile-for-ens	Segment Security Profile		Success
>	default-spoofguard-profile	Spoof Guard Profile		Success
>	default-vlan-ip-discovery-profile	IP Discovery Profile		Success

You cannot edit or delete the default segment profiles, but you can create custom segment profiles.

# 4-34 Applying Segment Profiles to Segments

You can apply default or user-created profiles to a segment.

Segments

NSX Distributed Port Groups Profiles

ADD SEGMENT

EXPAND ALL Filter by Name, Path and more

Name	Connected Gateway	Transport Zone	Subnets	Ports / Interfaces	Status	Alarms
Web-Segment	T1-GW-01   Tier-1 Gateway Connectivity	Prod-Overlay-TZ	172.16.10.1/24 CIDR e.g. 10.22.12.1/23 Gateway CIDR IPv6 CIDR e.g. fc7e:1206:db42:1/48 SET DHCP CONFIG			
Admin State						
> L2 VPN						
> Additional Settings						
Description	Description		Tags	Tag Scope		
Max 30 allowed. Click (+) to add						
<div>SEGMENT PROFILES</div> <div><div>IP Discovery</div><div>default-ip-discovery-profile</div><div>Spoof Guard</div><div>default-spoofguard-profile</div></div> <div><div>MAC Discovery</div><div>default-mac-discovery-profile</div><div>Segment Security</div><div>default-segment-security-profile</div></div> <div><div>QoS</div><div>None</div></div>						
> EVPN						

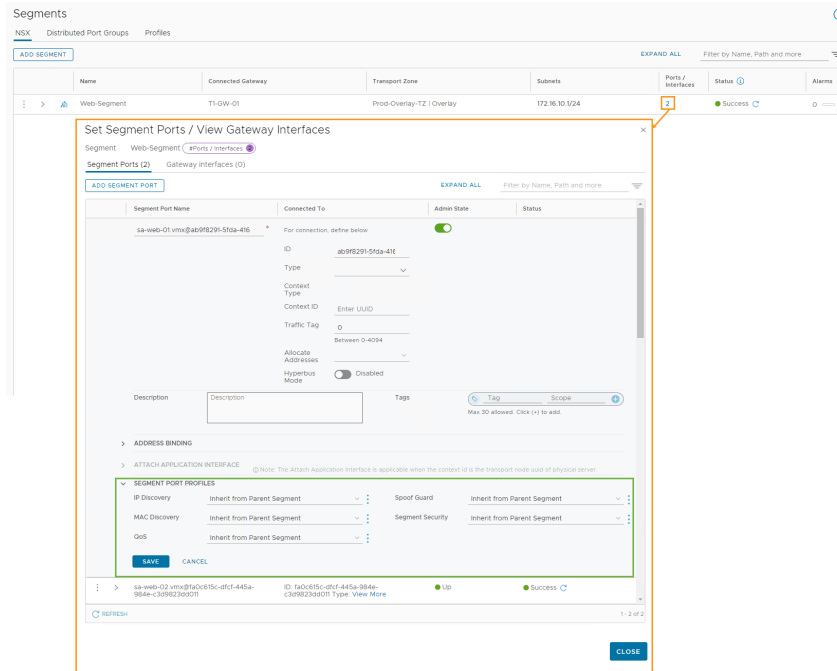
Edit the segment to modify the segment profiles.

CLOSE EDITING



## 4-35 Applying Segment Profiles to Segment Ports

You can apply default or custom profiles to segment ports. A segment or segment port can be associated with only one segment profile of each type.



For example, two QoS segment profiles cannot be associated with a segment or segment port.

When the segment profile is associated or disassociated from a segment, the segment profile for the child segment ports is applied based on the following criteria:

- If the parent segment has a profile associated with it, the child segment port inherits the segment profile from the parent.
- If the parent segment does not have a segment profile associated with it, a default segment profile is assigned to the segment, and the segment port inherits that default segment profile.
- If you explicitly associate a custom profile with a segment port, this custom profile overrides the existing segment profile.

You can associate a custom segment profile with a segment and retain the default segment profile for one of the child segment ports. You must make a copy of the default segment profile and associate it with the specific segment port.

# 4-36 SpoofGuard Segment Profile

The purpose of the SpoofGuard profile is to prevent traffic with incorrect source IP and MAC addresses from being transmitted. SpoofGuard provides the following functions:

- Prevents a rogue VM from assuming the IP address of an existing VM
- Ensures that the IP addresses of VMs are not altered without intervention
- Ensures that distributed firewall rules are not inadvertently or deliberately bypassed

The SpoofGuard profile includes several features.

SpoofGuard Feature	SpoofGuard Function
MAC SpoofGuard	Authenticates the MAC address of a packet.
IP SpoofGuard	Authenticates the MAC and IP addresses of a packet.
Dynamic ARP Inspection	ARP and GARP SpoofGuard and ND SpoofGuard validation are checked against the MAC source, IP source, and IP-MAC source mapping in the ARP, GARP, and ND payload.

SpoofGuard provides protection against spoofing with MAC+IP+VLAN bindings. If a VM's IP address does not match the IP address on the corresponding logical port and switch address binding in SpoofGuard, the VM's vNIC is prevented from accessing the network entirely. SpoofGuard can be configured at the port or switch level.

SpoofGuard might be used in your environment for the following reasons:

- Preventing a rogue VM from assuming the IP address of an existing VM.
- Ensuring that the IP addresses of VMs cannot be altered without intervention. You might not want VMs to alter their IP addresses without proper change control review. You can use SpoofGuard to ensure that the VM owner cannot alter the IP address and continue working unimpeded.
- Ensuring that the distributed firewall rules are not inadvertently (or deliberately) bypassed. For distributed firewall rules created using IP sets as sources or destinations, a VM could have its IP address forged in the packet header, thereby bypassing the rules in question.

## 4-37 Creating a SpoofGuard Segment Profile

SpoofGuard ensures that address bindings are enforced in the datapath.

If the IP address of a VM changes, traffic from the VM might be blocked by SpoofGuard until the corresponding configured port-segment address bindings are updated with the new IP address.

The screenshot shows the NSX configuration interface for creating a SpoofGuard Segment Profile. The 'Segments' section is active, with tabs for 'NSX', 'Distributed Port Groups', and 'Profiles'. Under 'Profiles', there are sub-tabs for 'Segment Profiles', 'Edge Bridge Profiles', and 'Metadata Proxies'. A dropdown menu 'ADD SEGMENT PROFILE' is open, showing options: 'Spoof Guard' (highlighted), 'IP Discovery', 'MAC Discovery', 'Segment Security', and 'GoS'. The main configuration area for the 'custom-spoofguard-profile' is visible. It includes a 'Port Bindings' section with a 'Disabled' toggle. Below this is a 'Description' field and a 'Tags' section with a 'Tag' and 'Scope' dropdown. At the bottom, there are 'SAVE' and 'CANCEL' buttons.

A SpoofGuard profile applied to a segment or a port blocks traffic determined to be spoofed. When SpoofGuard is configured, if the IP address of a VM changes, traffic from the VM might be blocked until the corresponding configured port or segment address bindings are updated with the new IP address.

You can enable SpoofGuard for the port groups containing the guests. When enabled for each network adapter, SpoofGuard inspects packets for the prescribed MAC and its corresponding IP address.

A SpoofGuard profile can be applied to a segment or a port:

- At the port level, the allowed MAC, VLAN, or IP allowlist is provided through the Address Bindings property of the port. When the VM sends traffic, it is dropped if its MAC, VLAN, or IP address does not match the MAC, VLAN, or IP properties of the port. The port-level SpoofGuard deals with traffic authentication, that is, the traffic consistent with VIF configuration.
- At the segment level, the allowed MAC, VLAN, or IP allowlist is provided through the Address Bindings property of the segment. This property is typically an allowed IP range or subnet for the segment, and the segment-level SpoofGuard deals with traffic authorization.

Traffic must be permitted by the port and the segment levels by SpoofGuard before it is allowed into a segment. Enabling or disabling port-level and segment-level SpoofGuard can be controlled using the SpoofGuard segment profile.

## 4-38 IP Discovery Segment Profile

The IP Discovery segment profile uses the following mechanisms to learn the MAC and IP addresses of VMs:

- DHCP/DHCPv6 snooping
- ARP snooping
- VMware Tools
- ND snooping
- Duplicate address detection

Learned addresses are shared with the CCP to achieve ARP/ND suppression.

In NSX, the IP Discovery profile works in the following ways:

- DHCP/DHCPv6 Snooping inspects the packets exchanged between the VM DHCP/DHCPv6 client and the DHCP/DHCPv6 server to learn the VM's IP and MAC addresses.
- ARP Snooping inspects a VM's outgoing ARPs and GARPs to learn the IP and MAC addresses of the VM.
- The VMware Tools software runs on a VM hosted on ESXi and can provide the VM's configuration information.
- ND Snooping is the IPv6 equivalent of ARP snooping. It inspects neighbor solicitation (NS) and neighbor advertisement (NA) messages to learn the IP and MAC addresses.
- Duplicate address detection checks whether a newly discovered IP address is already present on the realized binding list for a different port.

The VMware Tools IP Discovery method can also provide the VM's configuration information and is available for only VMs hosted by ESXi.

The IP Discovery profile might be used in the following scenario: The distributed firewall depends on the IP-to-port mapping to create firewall rules. Without IP Discovery, the distributed firewall must find the IP of a logical port through SpoofGuard and manual address bindings, which is a cumbersome and error-prone process.

## 4-39 Creating an IP Discovery Segment Profile

You can create an IP Discovery segment profile on the **Segment Profiles** tab in the NSX UI.

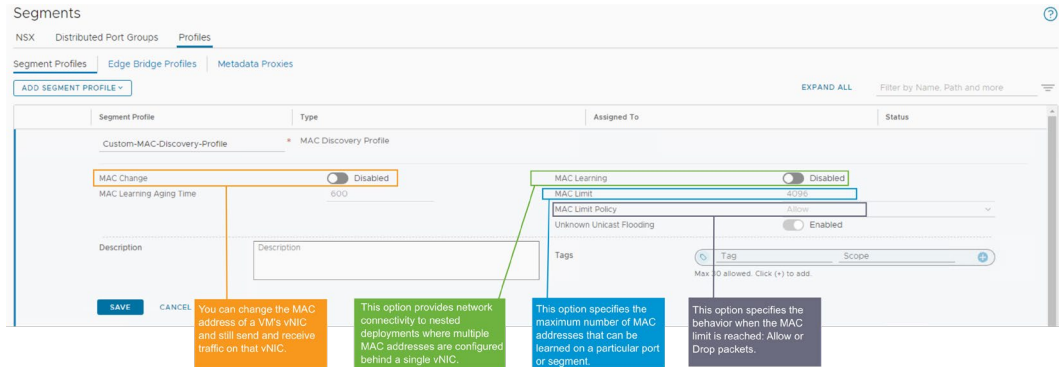
The screenshot displays the NSX UI's 'Segments' section, specifically the 'Profiles' tab. A sidebar on the left contains a menu with 'Spoof Guard', 'IP Discovery' (highlighted with an orange box), 'MAC Discovery', 'Segment Security', and 'GoS'. The main area shows a table with one entry: 'custom-IP-Discovery-Profile' of type 'IP Discovery Profile'. Below the table, the configuration for this profile is shown. It includes several settings: 'Duplicate IP Detection' (Disabled), 'ARP Snooping' (Enabled), 'ARP Binding Limit' (1), 'ND Snooping' (Disabled), 'ND Snooping Limit' (3), and 'ARP ND Binding Limit Timeout (minutes)' (10). On the right side, there are four more settings: 'DHCP Snooping' (Enabled), 'DHCP Snooping - IPv6' (Disabled), 'VMware Tools' (Enabled), 'VMware Tools - IPv6' (Disabled), and 'Trust on First Use' (Enabled). At the bottom, there is a 'Description' field and a 'Tags' section with a 'Tag' and 'Scope' dropdown. A 'SAVE' button is at the bottom left.

In the screenshot, a custom IP Discovery profile named Custom- IP-Discovery-Profile is created. After the profile is created, it can be applied to various segments.

By default, the discovery methods, ARP snooping and ND snooping, operate in a mode called trust on first use (TOFU). In the TOFU mode, when an address is discovered and added to the realized bindings list, that binding remains in the realized list forever. TOFU applies to the first  $n$  unique <IP, MAC, VLAN> bindings discovered using ARP/ND snooping, where  $n$  is the binding limit that you can configure. You can disable TOFU for ARP/ND snooping. The methods then operate in trust on every use (TOEU) mode. In the TOEU mode, when an address is discovered, it is added to the realized bindings list, and when it is deleted or expires, it is removed from the realized bindings list. DHCP snooping and VMware Tools always operate in the TOEU mode.

## 4-40 MAC Discovery Segment Profile

The MAC Discovery profile supports MAC learning, MAC address change, unknown unicast flooding, MAC limit, and MAC limit policy functions.



The MAC Discovery profile supports source MAC address learning:

- Source MAC address-based learning is a common feature in the physical world for learning the MAC address of a machine. The MAC Learning feature provides network connectivity to deployments where multiple MAC addresses are configured behind one vNIC. For example, in a nested hypervisor deployment, an ESXi VM runs on an ESXi host and multiple VMs run in the ESXi VM.
- Without MAC Learning, when the ESXi VM's vNIC connects to a segment port, its MAC address is static. VMs running inside the ESXi VM do not have network connectivity because their packets have different source MAC addresses. With MAC Learning, the source MAC address of every packet coming from the vNIC is inspected, the MAC address is learned, and the packet is allowed to go through. If a MAC address that is learned is not used for 10 minutes, it is removed. This aging property is not configurable.
- MAC Learning also supports Unknown Unicast Flooding. When a unicast packet is received by a port that has an unknown destination MAC address, the packet is flooded out on all segment ports that have MAC Learning and Unknown Unicast Flooding enabled. This property is enabled by default, but only if MAC Learning is enabled.

The MAC Discovery profile also supports a VM's ability to change its MAC address:

- A VM connected to a port with MAC Change enabled can run an administrative command to change the MAC address of its vNIC and still send and receive traffic on that vNIC.
- This feature (disabled by default) is used when a VM needs the ability to change its MAC address and not lose network connectivity.

The number of MAC addresses that can be learned is configurable. The maximum value is 4,096, which is the default. You can also set the policy for when the limit is reached. The options are:

- Drop: Packets from an unknown source MAC address are dropped. Packets inbound to this MAC address are treated as unknown unicast. The port receives the packets only if it has unknown unicast flooding enabled.
- Allow: Packets from an unknown source MAC address are forwarded although the address is not learned. Packets inbound to this MAC address are treated as unknown unicast. The port receives the packets only if it has unknown unicast flooding enabled.

If you enable both MAC Learning and MAC Change, you should also enable SpoofGuard to improve security.

For information about creating a MAC Discovery profile and associating the profile with a segment or a port, see *NSX Administration Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-C24D09FC-E213-4920-BD12-60063AC3B08E.html>.

## 4-41 Segment Security Profile

The Segment Security profile provides stateless layer 2 and layer 3 security. It protects segment integrity by filtering malicious attacks from VMs in the network.

The screenshot shows the NSX Segment Security Profile configuration page. The interface includes tabs for Segment Profiles, Edge Bridge Profiles, and Metadata Proxies. The Segment Profiles tab is active, showing a table with columns for Segment Profile, Type, Assigned To, and Status. Below the table, the configuration for the 'Custom-Segment-Security-Profile' is displayed. This configuration includes sections for BPDUs, DHCP, and Rate Limits. The BPDUs section has a 'BPDUs Filter' toggle set to 'Disabled' and a 'BPDUs Filter Allow List' table. The DHCP section has 'Server Block' and 'Client Block' toggles set to 'Disabled', and a 'Non-IP Traffic Block' toggle set to 'Enabled'. The Rate Limits section has 'Receive Broadcast' and 'Receive Multicast' rate limits set to '0'. The interface also includes a 'Tags' section and a 'Scope' dropdown. Several callouts are present: an orange box at the bottom left states 'Blocks all traffic to the BPDUs destination MAC address.'; a green box at the bottom center states 'Specifies the destination MAC address from the BPDUs destination MAC address list to allow traffic to the permitted destination.'; a blue box at the bottom center states 'Sets the rate limits to protect against ingress or egress broadcast or multicast traffic.'; an orange box at the bottom right states 'Allows only IPv4, IPv6, ARP, GARP, and BPDUs traffic.'; and a purple box at the bottom right states 'Blocks IPv6 router advertisements.'.

The Segment Security profile provides stateless layer 2 and layer 3 security by checking the ingress traffic to the segment and dropping unauthorized packets sent from VMs. The profile matches the IP address, MAC address, and protocols to a set of allowed addresses and protocols.

You can configure the Bridge Protocol Data Unit (BPDU) filter, DHCP snooping, DHCP server block, and rate limiting options:

- **BPDU Filter:** When the BPDU filter is enabled, all BPDU traffic is blocked for each port on the segment.
- **BPDU Filter Allow List:** You click the destination MAC address from the BPDU destination MAC addresses list to allow traffic to the permitted destination.
- To enable DHCP filtering, you turn on the **Server Block** and **Client Block** toggles. DHCP Server Block blocks traffic from a DHCP server to a DHCP client. It does not block traffic from a DHCP server to a DHCP relay agent.
- DHCP filtering can also be configured for IPv6 traffic by using the **Server Block-IPv6** and **Client Block-IPv6** options.
- Turning on the **Non-IP Traffic Block** toggle allows only IPv4, IPv6, ARP, GARP, and BPDU traffic. The rest of the non-IP traffic is blocked. The permitted IPv4, IPv6, ARP, GARP, and BPDU traffic is based on other policies set in address binding and SpoofGuard configurations. By default, this option is disabled to allow non-IP traffic to be handled as regular traffic.



- Turn on the **RA Guard** toggle to filter out ingress IPv6 router advertisements. The ICMPv6-type 134 packets are filtered out. This option is enabled by default.
- You can configure rate limits for the ingress or egress broadcast and multicast traffic. Rate limits are configured to protect the segment or the VM from threats such as broadcast storms. To avoid any connectivity problems, the minimum rate limit value must be greater than or equal to 10 PPS.

## 4-42 QoS Segment Profile

The QoS profile provides high-quality network performance for preferred traffic that requires high bandwidth.

This profile supports the following methods:

- Class of Service (CoS)
- Differentiated Services Code Point (DSCP)

The screenshot shows the 'Segments' configuration page in NSX, specifically the 'Profiles' tab. A 'Custom-QoS-Profile' is selected, and the 'QoS Profile' configuration is visible. The interface includes fields for DSCP Mode (set to 'Trusted'), Priority (0), and Class of Service (0). There are checkboxes for Traffic Direction (Ingress, Ingress Broadcast, Egress) and bandwidth settings (Mbps avg/peak, Kbps avg/peak). A 'Tags' section allows adding up to 30 tags. Callouts provide detailed explanations for several settings:

- DSCP with Trusted mode:** Specifies whether the DSCP value is copied from the inner header to outer IP header.
- COS Value:** 0 through 7, with 7 being the highest. DSCP Priority Value: 0 through 63, with 0 being the highest.
- Bandwidth:** Sets the peak bandwidth rate to prevent congestion.
- Burst Size:** Sets the average ingress and egress transmit rate.

QoS provides high-quality and dedicated network performance for preferred traffic that requires high bandwidth. The QoS mechanism achieves this performance by providing sufficient bandwidth, controlling latency and jitter, and reducing data loss for preferred packets even with network congestion. This level of network service is provided by using the existing network resources efficiently.

The QoS profile supports the following methods:

- Class of Service (CoS): Marks the packet's layer 2 header to specify its priority
- Differentiated Services Code Point (DSCP): Inserts a code value into the packet's layer 3 header for prioritization

The layer 2 CoS allows you to specify priority for data packets when traffic is buffered in the segment because of congestion. The layer 3 DSCP detects packets based on their DSCP values. CoS is always applied to the data packet regardless of the trusted mode.

NSX trusts the DSCP setting applied by a VM or modifies and sets the DSCP value at the segment level. In each case, the DSCP value is propagated to the outer IP header of encapsulated frames. In this way, the external physical network can prioritize the traffic based on the DSCP setting on the external header. When DSCP is in the trusted mode, the DSCP value is copied from the inner header. When in the untrusted mode, the DSCP value is not preserved for the inner header. DSCP settings work only on tunneled traffic. These settings do not apply to traffic inside the same hypervisor.

You can use the QoS segment profile to configure the average ingress and egress bandwidth values to set the transmit limit rate. To prevent congestion on the northbound network links, you can use the peak bandwidth rate to specify the upper limit that traffic on a segment is allowed to burst. The settings in a QoS segment profile do not guarantee the bandwidth but help limit the use of network bandwidth. The actual bandwidth you observe is determined by the link speed of the port or the values in the segment profile, whichever is lower.

For information about the QoS segment profile, see *NSX Administration Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-62BB7145-EDD7-4611-A50D-17F4A0EAE57C.html>.

## 4-43 Review of Learner Objectives

- Describe the purpose of segment profiles
- Identify the functions of the segment profiles in NSX
- Create segment profiles and attach them to segments and ports

## 4-44 Lesson 4: Logical Switching Packet Forwarding

### 4-45 Learner Objectives

- Describe the functions of each table used in packet forwarding
- Describe how BUM traffic is managed in switching
- Explain how ARP suppression is achieved

## 4-46 NSX Controller Tables

NSX Controller maintains a set of tables that are used for identifying the data plane component associations and for traffic forwarding.

To achieve network virtualization, a network controller must configure the hypervisor virtual segment with network flow tables that form the logical broadcast domains.

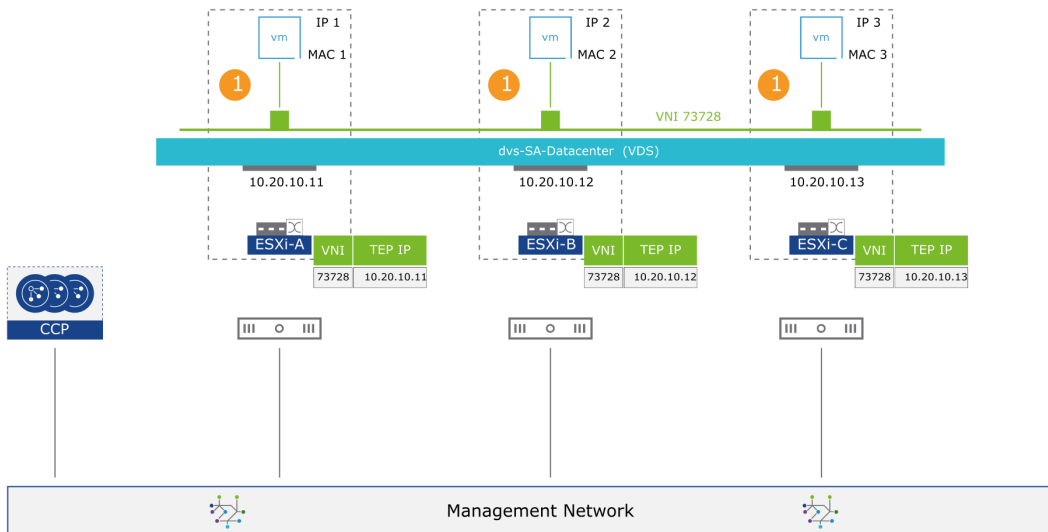
Several network flow tables are available:

- TEP Table: Maintains VNI-to-TEP IP bindings
- ARP Table: Maintains the VM MAC-to-VM IP mapping
- MAC Table: Maintains the VM MAC address-to-TEP IP mapping

## 4-47 TEP Table Update (1)

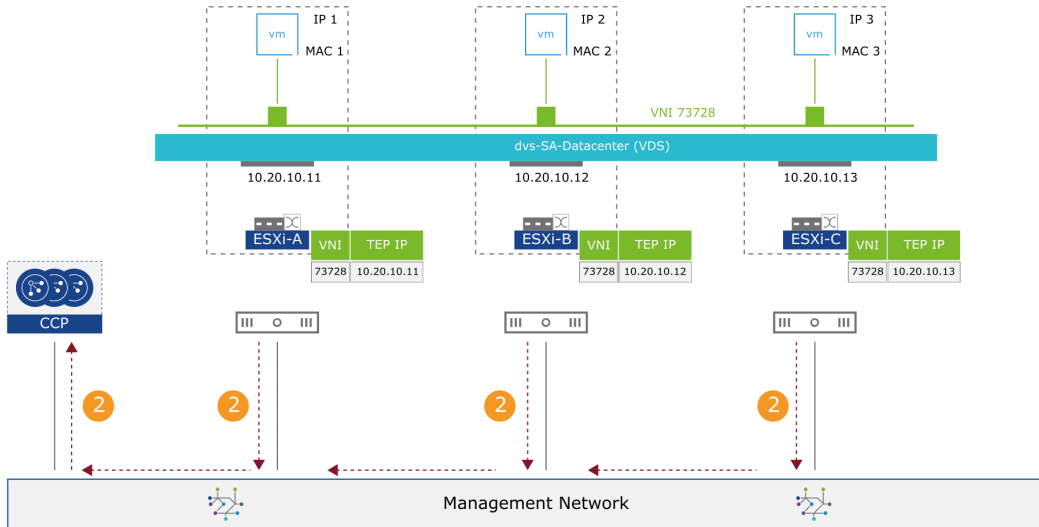
When a powered-on VM is connected to a segment:

1. The VNI-to-TEP mapping is registered on the transport nodes in its local TEP table.



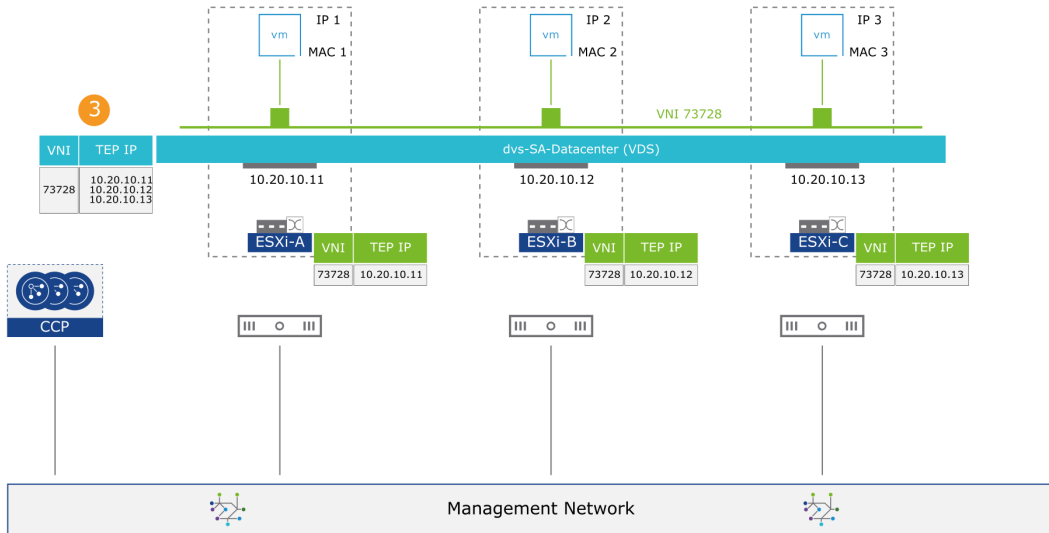
## 4-48 TEP Table Update (2)

- Each transport node updates the CCP about the learned VNI-to-TEP IP mapping.



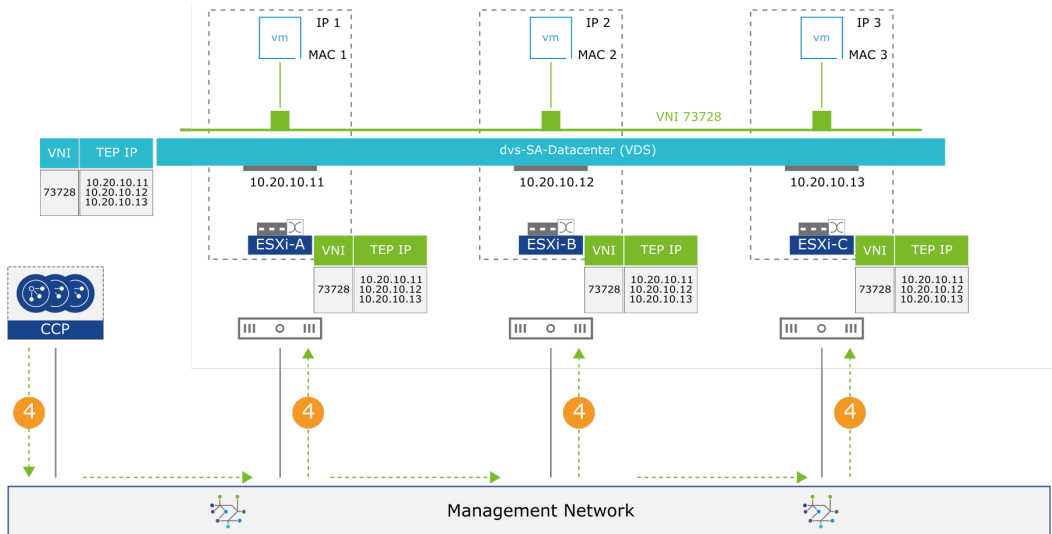
## 4-49 TEP Table Update (3)

- The CCP maintains the consolidated entries of VNI-to-TEP IP mappings.



## 4-50 TEP Table Update (4)

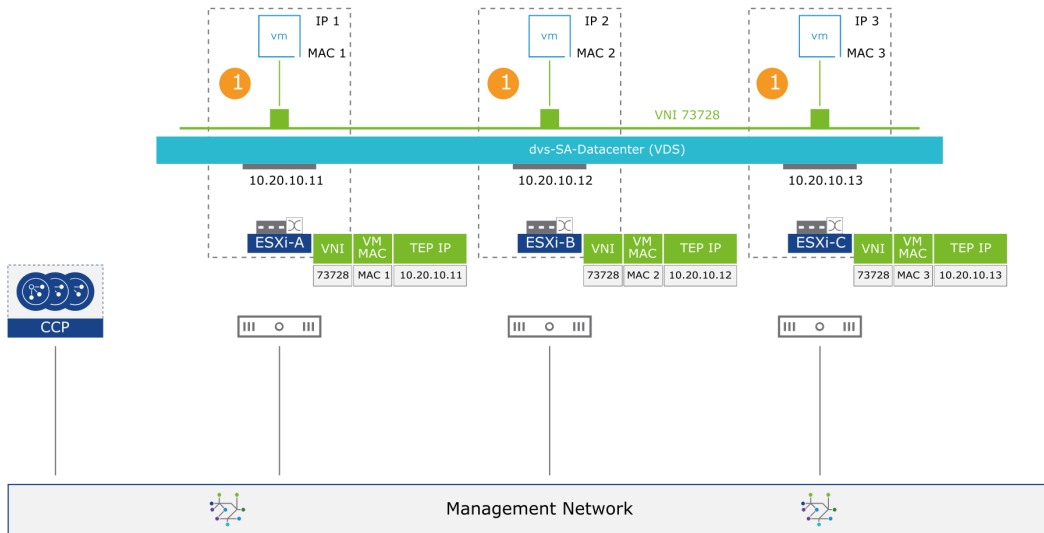
4. The CCP sends the updated TEP table to all the transport nodes where the VNI is realized.



## 4-51 MAC Table Update (1)

When a powered-on VM is connected to a segment:

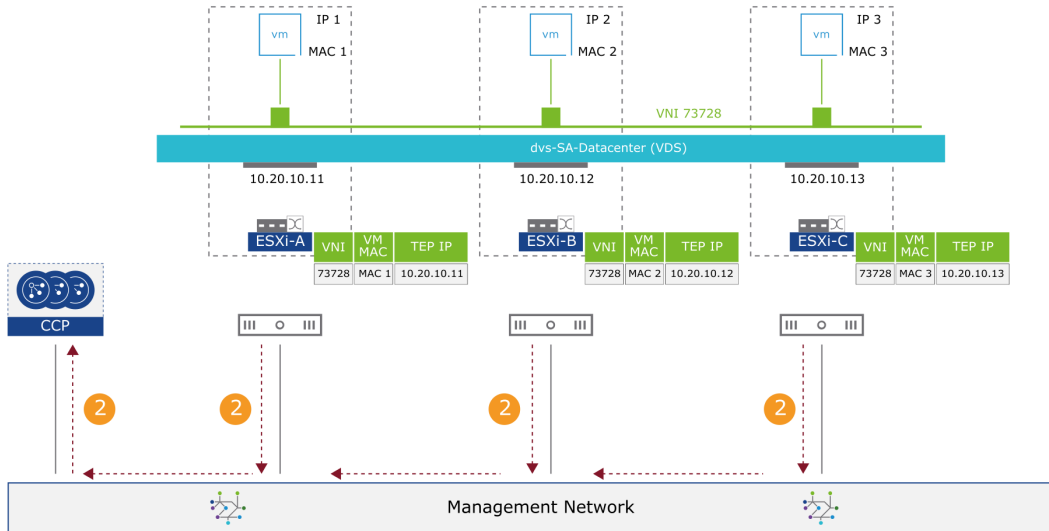
1. The VM MAC-to-TEP IP mapping is registered on the transport nodes in its local MAC table.





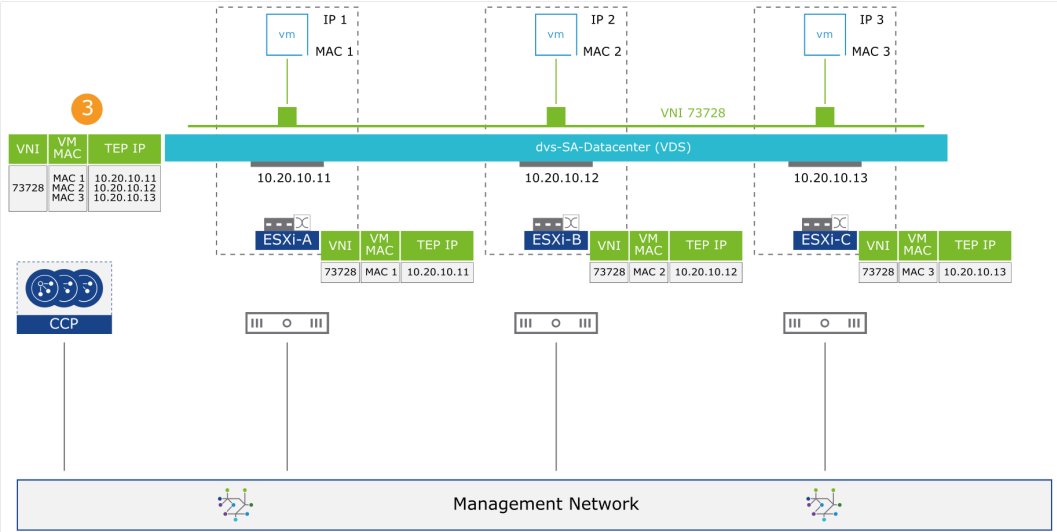
## 4-52 MAC Table Update (2)

- Each transport node updates the CCP about the learned VM MAC-to-TEP IP mapping.



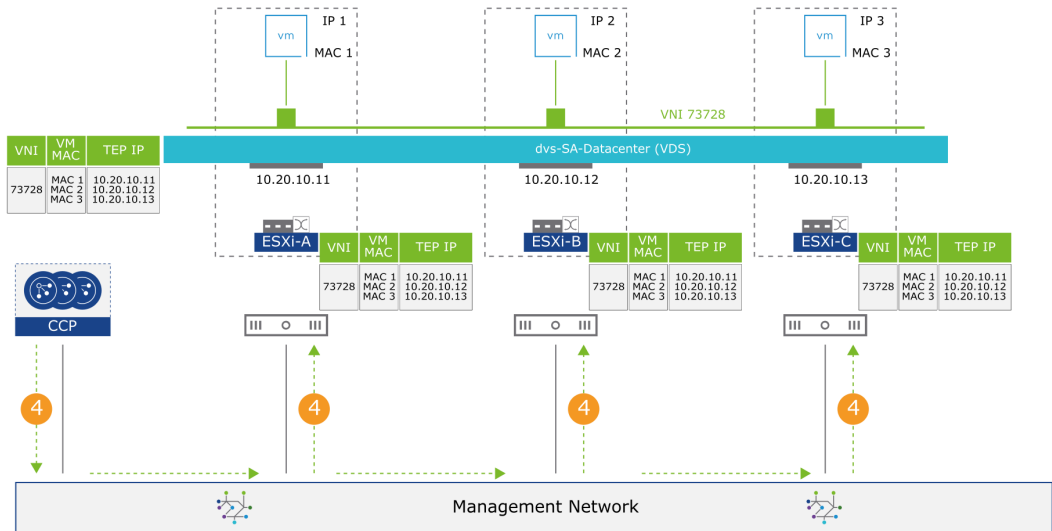
# 4-53 MAC Table Update (3)

3. The CCP maintains the consolidated entries of VM MAC-to-TEP IP mappings.



## 4-54 MAC Table Update (4)

4. The CCP sends the updated MAC table to all the transport nodes where the VNI is realized.



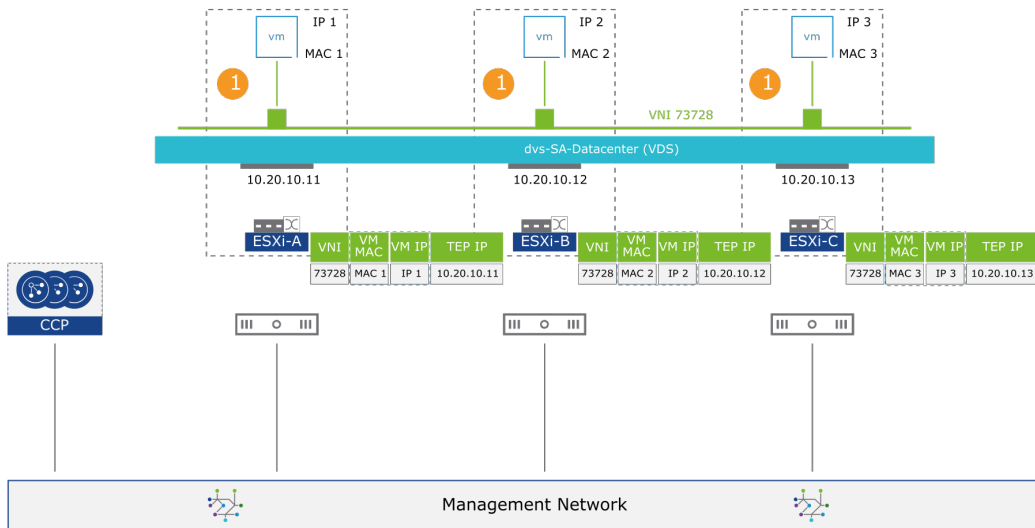
## 4-55 About the ARP Table

The ARP suppression technique reduces the amount of ARP flooding in segments:

- NSX uses the ARP table maintained in the CCP to provide ARP suppression.
- Transport nodes learn the MAC-to-IP association by snooping the ARP and DHCP traffic.
- The mapping is recorded each time a VM initiates a communication (sends or receives traffic).
- The learned information is pushed from each transport node to the control plane.

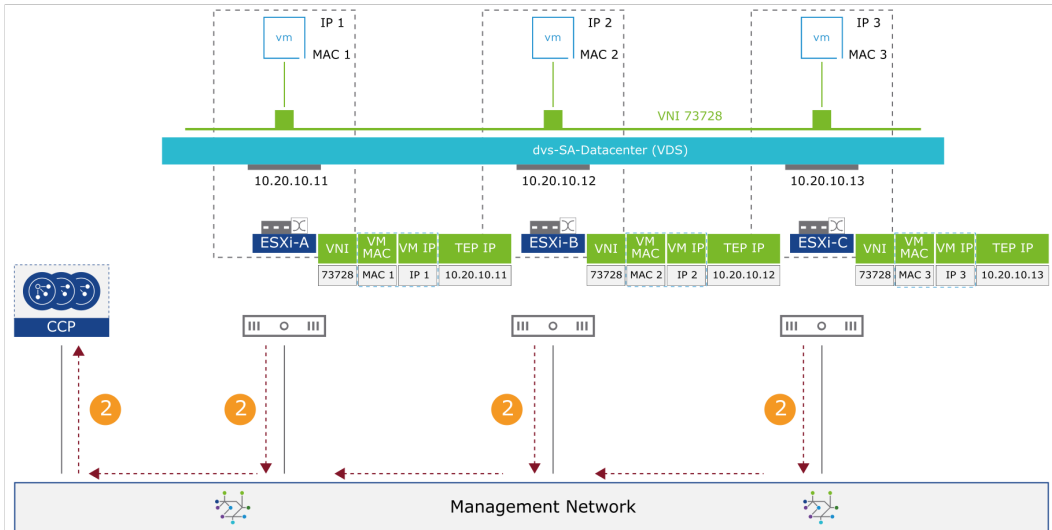
## 4-56 ARP Table Update (1)

1. Each transport node records the local VM IP-to-MAC mapping in its local table.



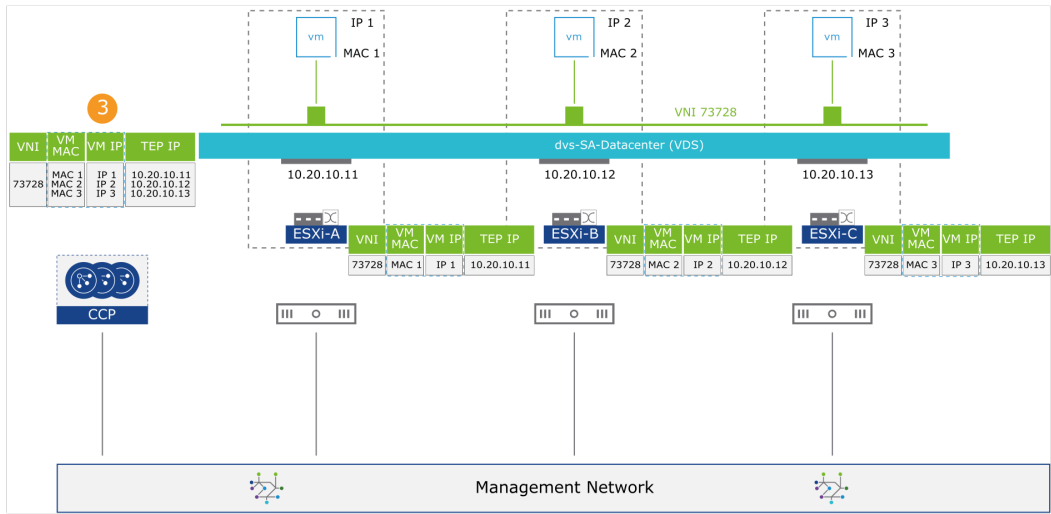
## 4-57 ARP Table Update (2)

- Each transport node sends known VM IP-to-MAC mappings to the CCP.



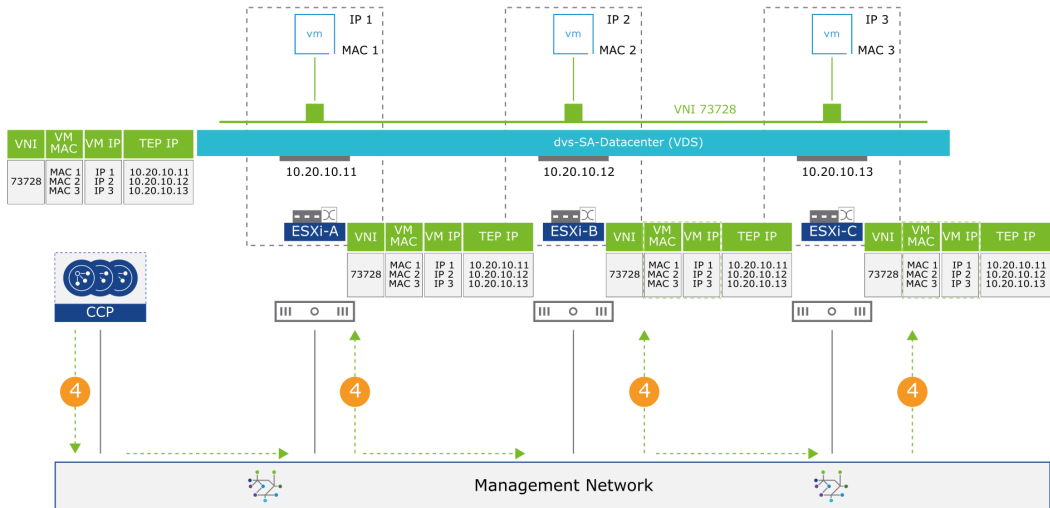
## 4-58 ARP Table Update (3)

- The CCP updates its ARP table based on the VM IP-to-MAC mappings received from transport nodes.



## 4-59 ARP Table Update (4)

4. The CCP sends the updated ARP table to all the transport nodes.



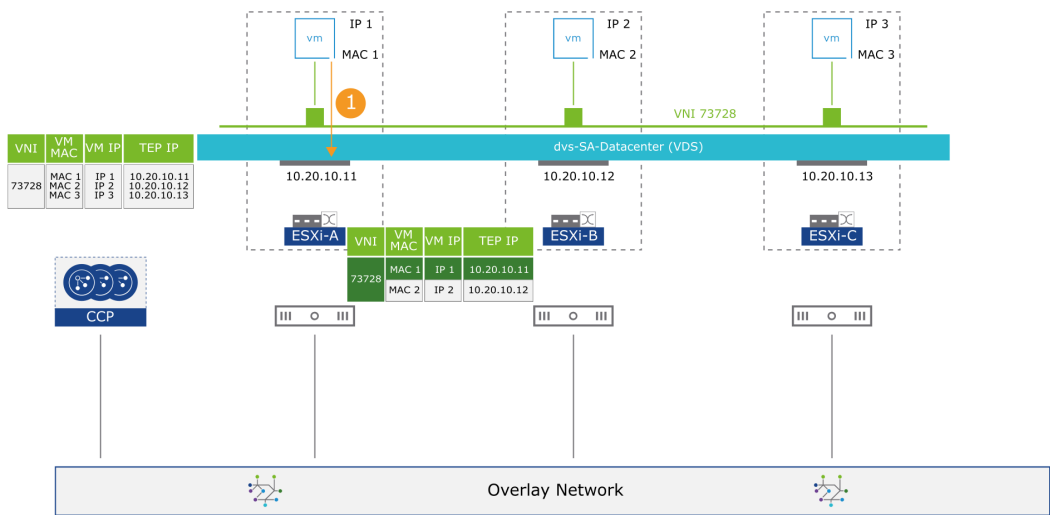
The ARP table values in both the CCP and the transport nodes are flushed after 10 minutes.

# 4-60 Unicast Packet Forwarding Across Hosts

## (1)

VM1 assumes that the ARP is resolved:

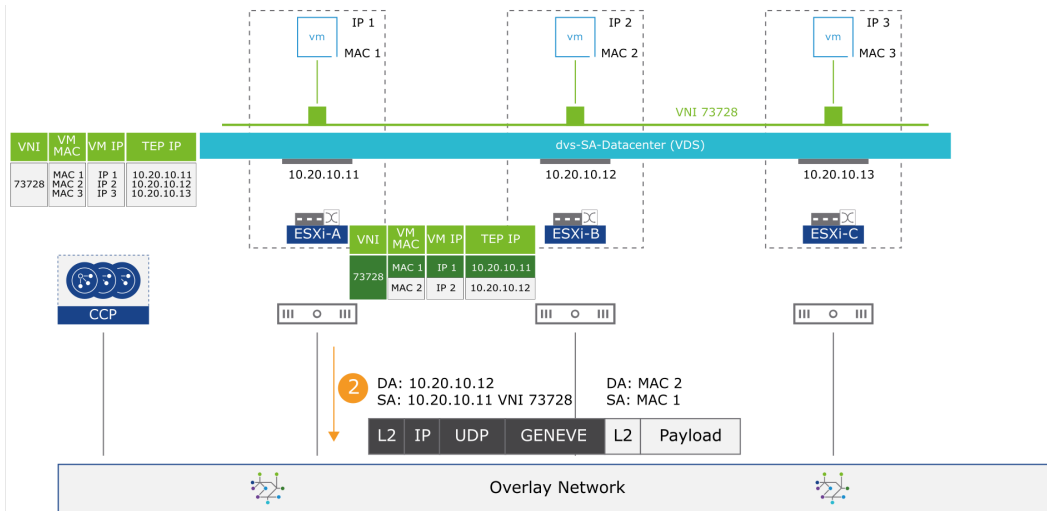
1. VM1 starts sending traffic to VM2.





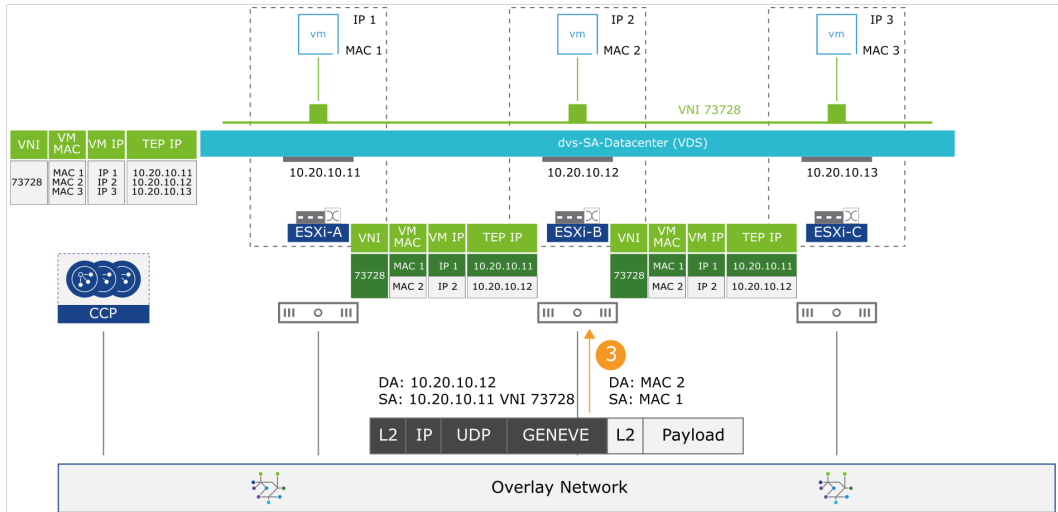
## 4-61 Unicast Packet Forwarding Across Hosts (2)

- The original packet is encapsulated in the Geneve header by the ESXi-A source transport node.



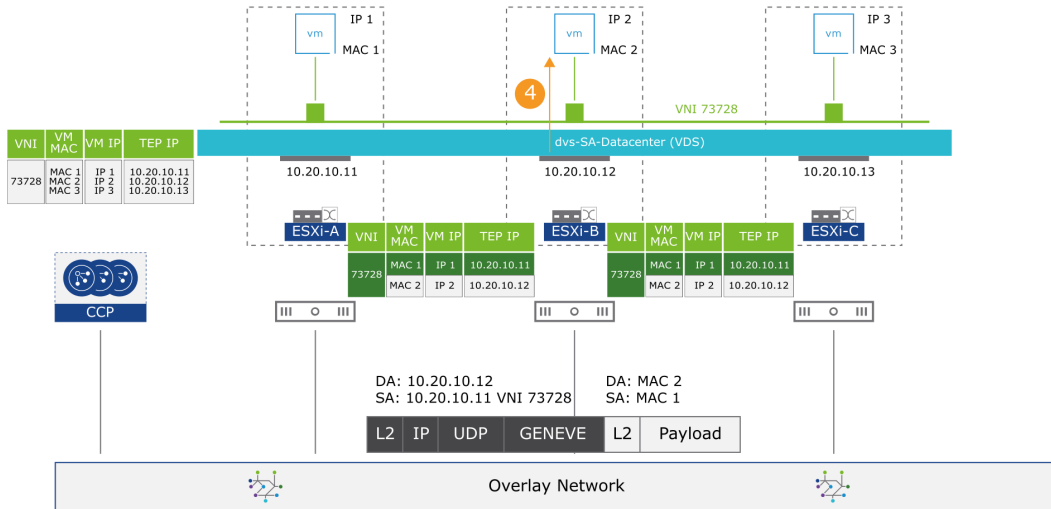
## 4-62 Unicast Packet Forwarding Across Hosts (3)

3. The packet is sent to the ESXi-B destination transport node.



## 4-63 Unicast Packet Forwarding Across Hosts (4)

- The destination transport node decapsulates the Geneve header and delivers the original source VM frame to VM2



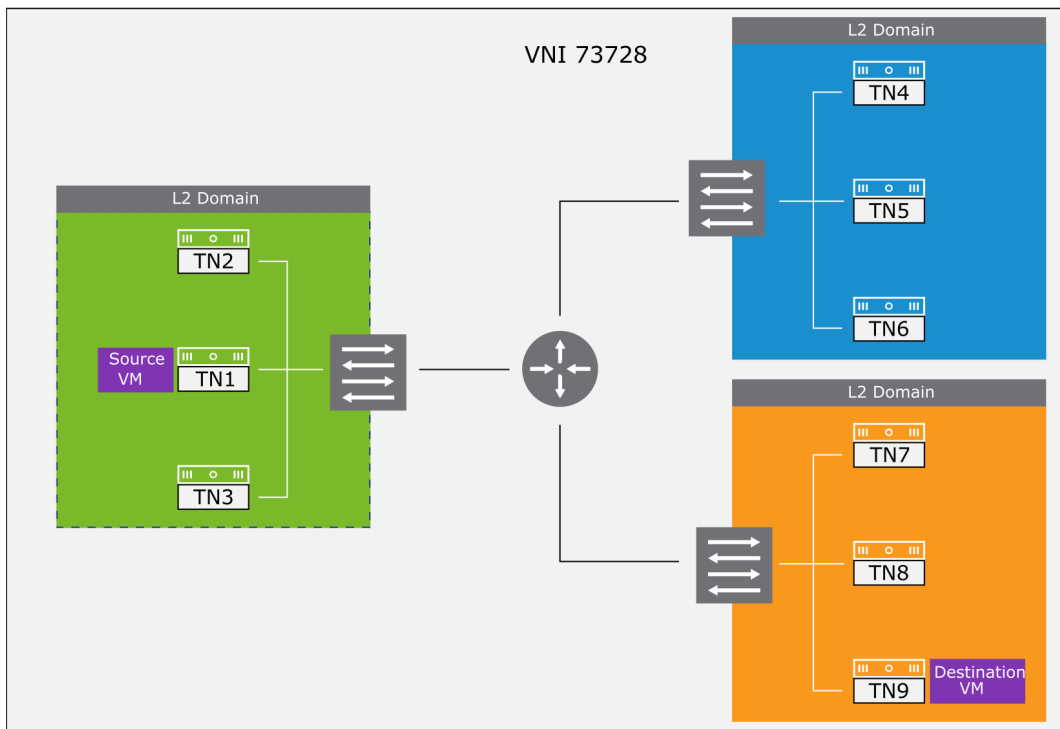
## 4-64 Overview of BUM Traffic

A VM's broadcast, unknown unicast, and multicast (BUM) traffic must be flooded to all other VMs that belong to the same segment.

The BUM traffic originated by a VM on a transport node must be replicated to remote transport nodes (running the VMs connected to the same segment).

The following BUM traffic replication modes are supported:

- Hierarchical Two-Tier Replication
- Head Replication



All broadcast, unicast, and multicast (BUM) traffic is treated the same: flooded to all participating ESXi hosts in the segment. The replication is performed in software.

Each host transport node has a tunnel endpoint. Each TEP has an IP address. These IP addresses can be in the same subnet or in different subnets, depending on your configuration of IP pools or DHCP for your transport nodes.

When two VMs on different hosts communicate directly and ARP is resolved, unicast-encapsulated traffic is exchanged between the two TEP IP addresses without any need for flooding. However, as with any layer 2 network, sometimes traffic that is originated by a VM, such as an ARP request, needs to be flooded. For the layer 2 BUM traffic, the packet must be sent to all the other VMs belonging to the same segment.

In the diagram, Source VM residing on transport node 1 (TN1) must send traffic to Destination VM residing on TN9. The destination's VM MAC address is unknown to TN1 or the control plane. Therefore, the Source VM sends an ARP request (broadcast frame) seeking the destination VM's MAC address. TN1 floods this ARP request frame to all other transport nodes within VNI 73728. The destination VM on TN9 receives the ARP request and responds with an ARP reply. ARP tables on hosts are updated to reduce future flooding.

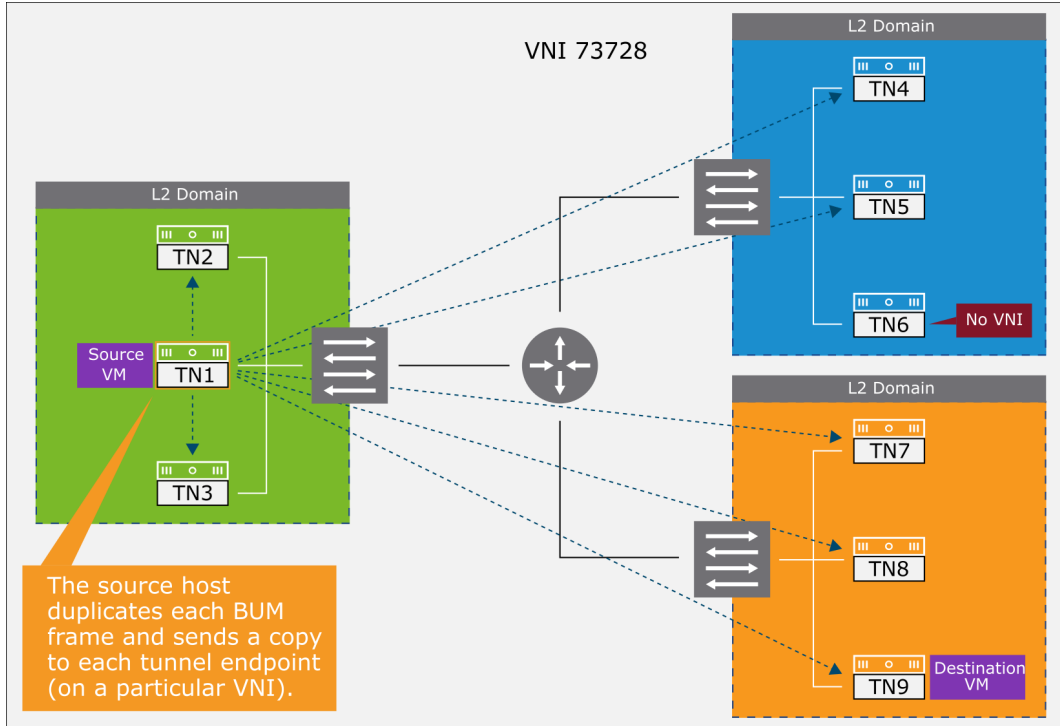
To enable flooding, the NSX segment supports the following types of replication modes:

- Head Replication mode: This mode is also called Source Mode or Headend Replication. The source host duplicates each BUM frame and sends a copy to each TEP (on a particular VNI) that it knows.
- Hierarchical Two-Tier Replication: This mode is also called the MTEP mode. It involves a host in another L2 domain that performs replication of BUM traffic to other hosts within the same VNI.

The TEP only replicates traffic in which the replication option TLV is set in the Geneve header.

## 4-65 Managing BUM Traffic: Head Replication

The Head replication mode performs source-based replication. The BUM packet is replicated by the source transport node to all other transport nodes participating in that VNI.



In this example, a BUM packet arrives on TN1:

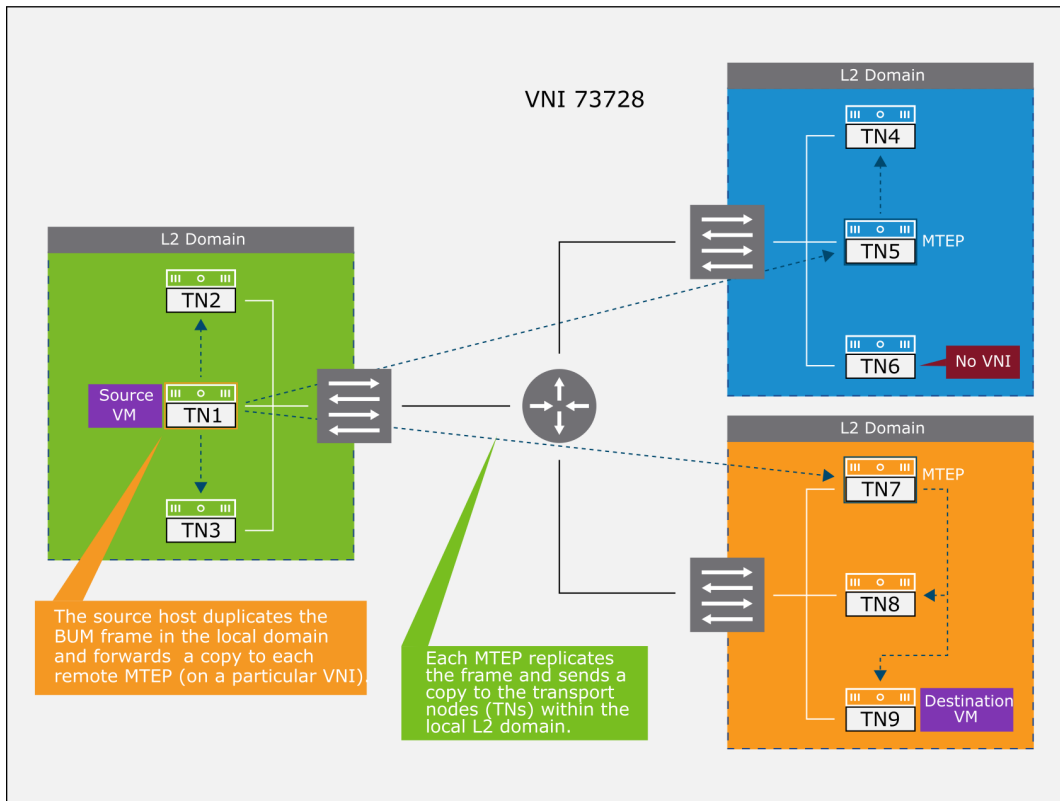
- TN1 replicates to TN2 and TN3 because they are in the same L2 domain.  
TN1 replicates because the control plane does not have the desired information.
- Meanwhile, TN1 also needs to replicate the packet to the remote transport nodes (TN4 and TN5 in one L2 domain and TN7, TN8, TN9 in another L2 domain).
- Because TN6 does not participate in VNI 73728, the packet is not replicated to TN6.

## 4-66 Managing BUM Traffic: Hierarchical Two-Tier Replication

The source transport node replicates the BUM packet locally within its L2 domain.

The source transport node elects a proxy TEP (MTEP) from each remote L2 domain and sends the BUM packet to each proxy TEP.

The proxy TEP replicates the BUM packet to the transport nodes within its L2 domain.



Hierarchical two-tier mode is also known as the MTEP replication mode.

In the diagram, a BUM packet arrives on TN1:

- An MTEP is elected for each L2 domain (segment). TN1 elects an MTEP for each remote L2 domain.
- TN1 replicates the BUM traffic locally to TN2 and TN3.

- TN1 sends a copy of the BUM packet to each remote MTEP with the replication option TLV embedded in the Geneve header.

The role of MTEP is to replicate the received BUM packet locally and forward it to other TNs within the same L2 domain.

- MTEP TN7 forwards the BUM packet to TN8 and TN9.
- MTEP TN5 forwards the packet to TN4.
- Because TN6 does not participate in VNI 73728, the packet is not sent to TN6.

## 4-67 Lab 5: Configuring Segments

Create segments for VMs residing on the ESXi hosts:

1. Prepare for the Lab
2. Create Segments
3. Attach VMs to Segments
4. Use Network Topology to Validate the Logical Switching Configuration
5. Test Layer 2 Connectivity and Verify the Configuration of Segments

## 4-68 Review of Learner Objectives

- Describe the functions of each table used in packet forwarding
- Describe how BUM traffic is managed in switching
- Explain how ARP suppression is achieved



## 4-69 Key Points

- A segment is a representation of the L2 broadcast domain across transport nodes.
- A VNI is assigned to each segment.
- Types of segments are overlay segments and VLAN segments.
- Geneve is an IETF overlay tunneling mechanism that provides L2 over L3 encapsulation of data plane packets.
- Segment profiles provide L2 networking configuration details for segments and ports.
- Five types of segment profiles are available: SpoofGuard, IP Discovery, MAC Discovery, Segment Security, and QoS.
- You can apply default or custom segment profiles to segments or ports.
- Network flow tables used in packet forwarding include TEP, ARP, and MAC table.
- BUM traffic replication supports head mode and hierarchical two-tier mode.

Questions?



# Module 5

## NSX Logical Routing

### 5-2 Importance

In NSX, logical routing provides an optimized and scalable way to manage east-west and north-south traffic. You must understand the NSX logical routing architecture, routing components, and routing features to build an efficient and secure layer 3 network infrastructure.

### 5-3 Module Lessons

1. Overview of Logical Routing
2. NSX Edge and Edge Clusters
3. Configuring Tier-0 and Tier-1 Gateways
4. Configuring Static and Dynamic Routing
5. ECMP and High Availability
6. Logical Routing Packet Walk
7. VRF Lite

## 5-4 Lesson 1: Overview of Logical Routing

### 5-5 Learner Objectives

- Explain the function and features of logical routing
- Describe the architecture of NSX two-tier routing
- Differentiate between north-south and east-west routing
- Describe the gateway components
- Recognize the various types of gateway interfaces

### 5-6 Use Cases for Logical Routing

In NSX, logical routing is used in many ways:

- Support for single or multitenant deployment models
- Separation of tenants and networks
- Solution for cloud environments with containerized workloads
- Optimized routing path and simplified routing in virtual networks
- Distributed routing and centralized services in data centers
- Ability to extend logical networks to physical environments

The NSX logical routing has many use cases:

- The logical routing functionality focuses on multitenant environments. Gateways can support multiple instances where a separation of tenants and networks is required.
- Logical routing is optimized for cloud environments. It suits containerized workloads and multicloud data centers.
- The distributed routing architecture provides optimal routing paths. Routing is done closest to the source. For example, traffic from two VMs on different subnets residing on the same host can be routed in the kernel. The traffic does not need to leave the host to be routed. This method helps avoid hairpinning.
- NSX Edge transport nodes that host gateways provide network services that cannot be distributed to hosts.
- Gateways exist where east-west routing, north-south routing, and centralized services (such as NAT or VPN) are required.

- A dynamic routing protocol is not needed between the two-tiered gateways, simplifying data center routing.
- Logical routing makes it easy to extend logical networks to physical environments.

## 5-7 Prerequisites for Logical Routing

For logical routing to work, certain requirements must be met:

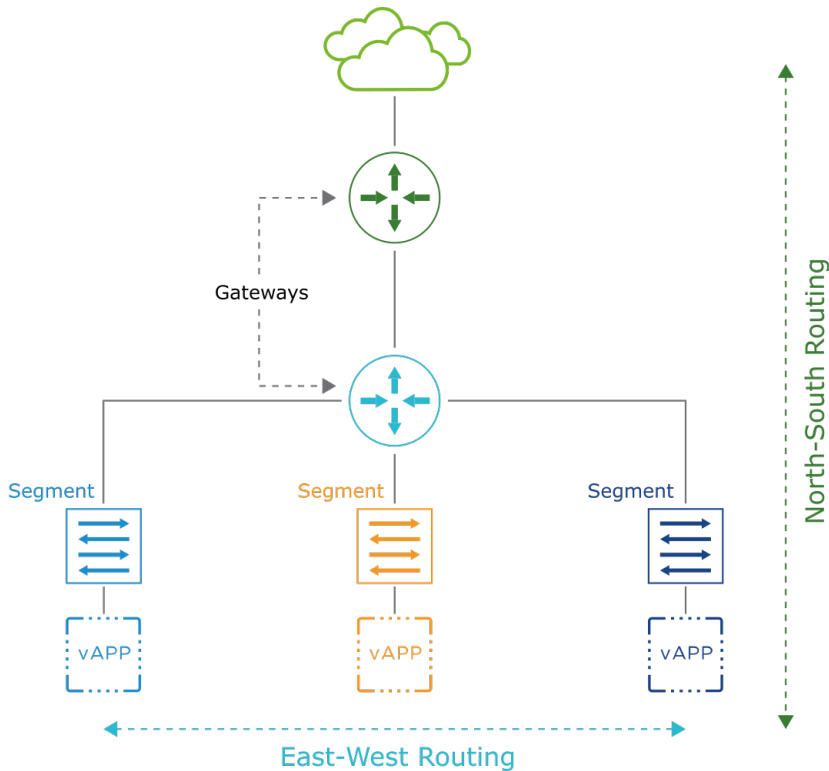
- The NSX management cluster must be formed and available.
- Transport zones and N-VDS/VDS should be created.
- Hypervisors must be prepared as NSX transport nodes and added to the management plane.
- Transport nodes must be attached to the appropriate transport zones.
- An N-VDS/VDS instance must be created on each transport node.
- The NSX Edge nodes must be deployed and preconfigured according to the requirements.

N-VDS virtual switch is not supported on ESXi transport nodes from NSX 4.0.0.1. N-VDS is still supported on NSX Edge transport nodes.

## 5-8 Logical Routing in NSX

The NSX gateways provide the following features:

- North-south and east-west routing
- Static and dynamic routing
- Multitenancy
- High availability
- IPv6 and multicast
- Centralized services such as gateway firewall, Network Address Translation (NAT), or VPN



Logical Routing in NSX

An NSX gateway reproduces routing functionality in a virtual environment:

- Logical routing is distributed and decoupled from the underlying hardware. Basic forwarding decisions are made locally on the prepared transport nodes.
- The services running on the NSX Edge nodes provide layer 3 functionalities, such as Network Address Translation (NAT).
- When multiple gateway instances are installed, multitenancy and network separation are supported on a single gateway. Logical routing is enhanced for most cloud use cases that involve multiple service providers and tenants.

The NSX gateways provide north-south and east-west connectivity:

- North-south routing enables tenants to access public networks. Traffic leaves or enters a tenant administrative domain. Connections to and from the entities outside the tenant's premises are considered north-south traffic.
- East-west traffic flows between various networks in the same tenant. Traffic is sent between logical networks (segments) under the same administrative domain.

# 5-9 Tier-0 and Tier-1 Gateways

NSX provides Tier-0 and Tier-1 gateways. Each gateway has distinct characteristics.

Tier-0 Gateway	Tier-1 Gateway
Owned and configured by the provider or infrastructure administrator	Owned and configured by tenants
Supports static or dynamic routing	Does not use dynamic routing protocols
Supports equal-cost multipath (ECMP) routing to upstream physical gateways	Does not support ECMP routing
Forwards the traffic between logical and physical networks (north-south)	Enables routing between segments (east-west) and must be connected to a Tier-0 gateway to provide external connectivity
Requires an NSX Edge cluster	Only requires an NSX Edge cluster if centralized services are configured

Gateways are distributed across the kernel of each host. A gateway can be deployed as either a Tier-0 or a Tier-1 gateway:

- Tier-0 gateways provide north-south connectivity.
- Tier-1 gateways provide east-west connectivity.

The Tier-1 gateway must connect to the Tier-0 gateway to access external networks. The Tier-0 gateway is directly connected to upstream physical gateways.

The Tier-1 gateway does not require an NSX Edge node if no services are used. It has connections (preprogrammed by the management plane) toward its upstream Tier-0 gateway

Both Tier-0 and Tier-1 gateways support stateful services, such as NAT. Stateful services are centralized on NSX Edge nodes.

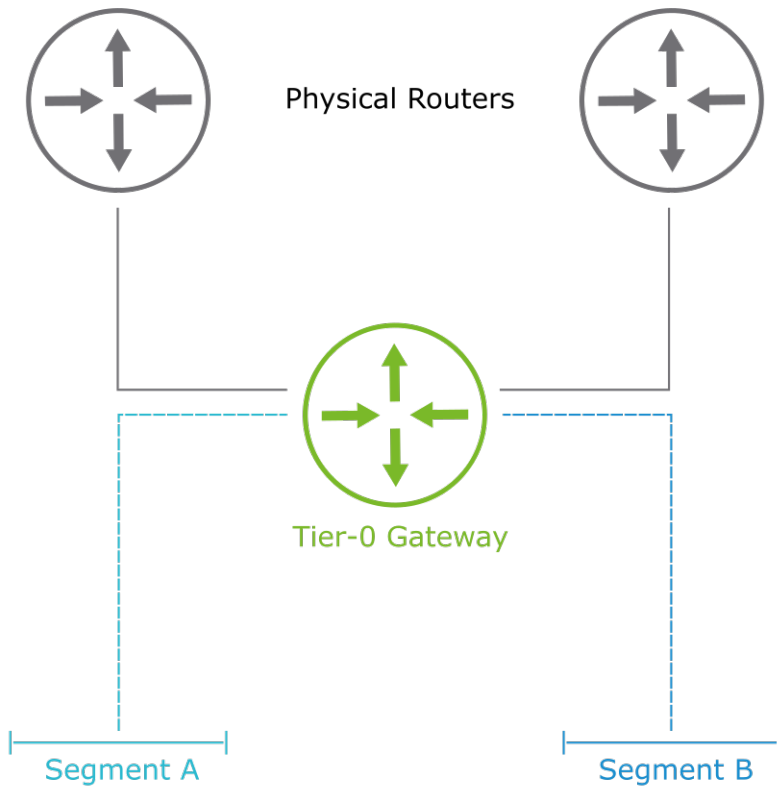
Dynamic routing processes are centralized services while packet forwarding is stateless.



## 5-10 Single-Tier Topology

In a single-tier topology:

- Only Tier-0 gateways are included.
- Segments are connected directly to the Tier-0 gateway.

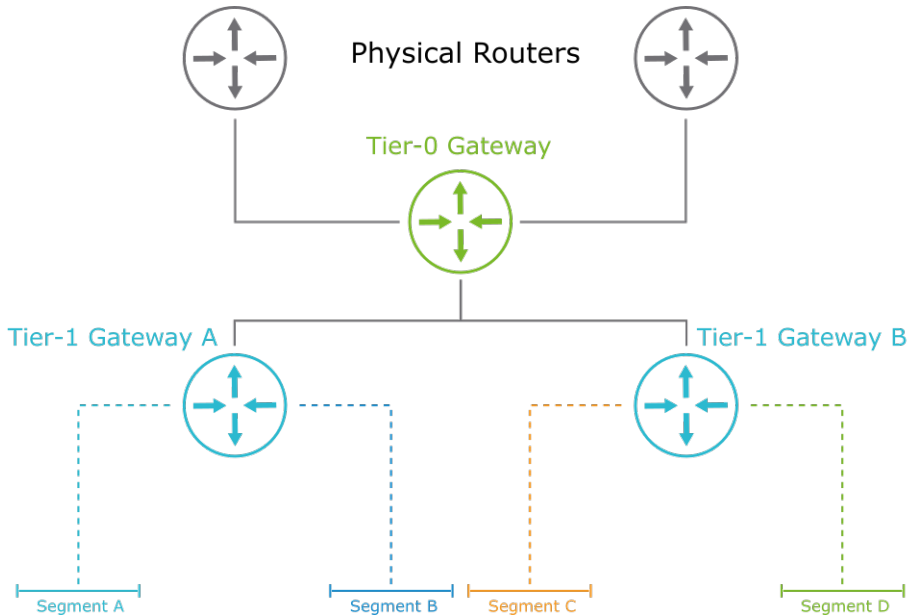


In a single-tier deployment, only Tier-0 gateways are used. Tier-1 gateways are not used. The segments are directly connected to the Tier-0 layer. The service provider provides upstream connectivity. The tenant performs southbound connectivity.

## 5-11 Multitier Topology

In a multitier topology:

- Tier-0 and Tier-1 gateways are included.
- Tier-1 gateways are connected to the Tier-0 gateways.
- Segments are connected to the Tier-1 gateways.



In the diagram, segments A, B, C, and D are connected to the Tier-1 gateways.

The two-tier routing topology is not mandatory. If the provider and the tenant do not need to be separated, a single-tier topology can be used.

In most use cases, the provider owns and configures the Tier-0 gateway. The tenants own and configure the Tier-1 gateway. Cloud management platforms typically provision Tier-1 gateways.

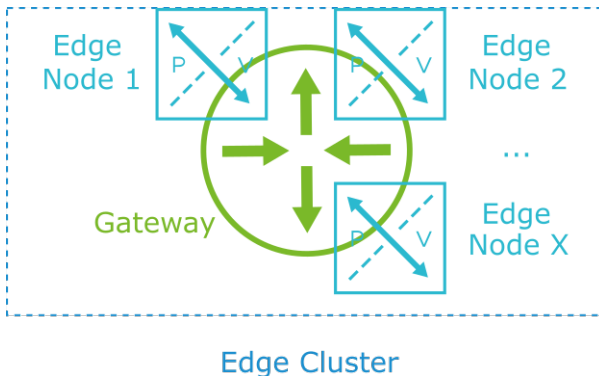
## 5-12 Edge Nodes and Edge Clusters

NSX Edge nodes have the following functions:

- Provide connectivity to external networks.
- Required to host the Tier-0 gateways.
- Run gateways with centralized and stateful services such as NAT or VPN.

An NSX Edge cluster is a group of edge nodes:

- NSX Edge clusters provide redundancy and scalability.
- NSX Edge nodes must join an edge cluster.



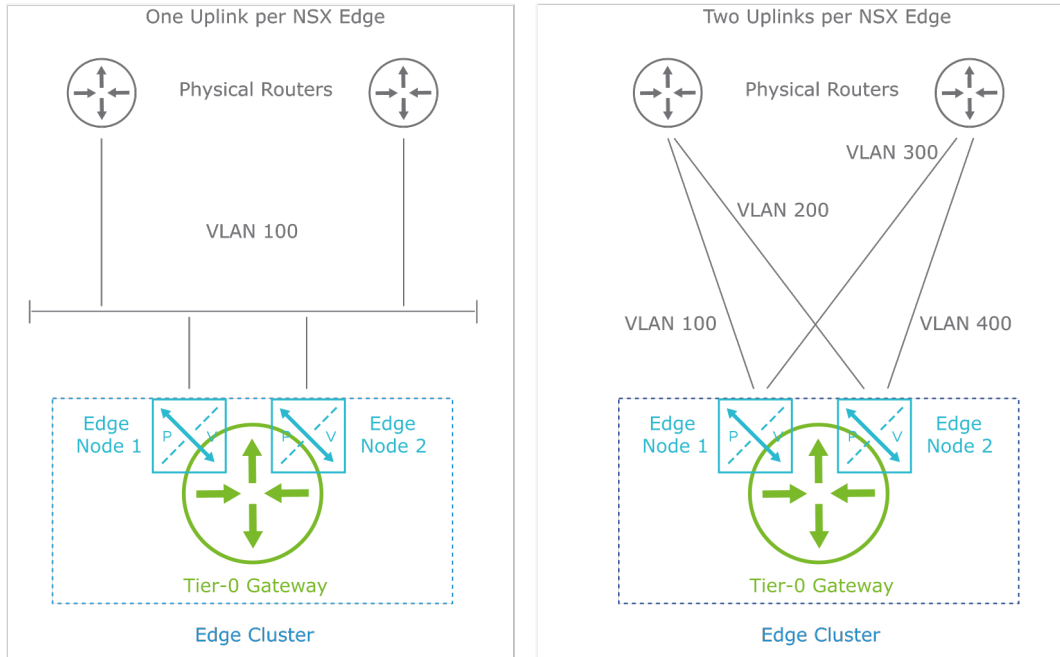
NSX Edge nodes provide computational resources to deliver dynamic routing and services for NSX gateways.

An NSX Edge node can only host one Tier-0 gateway.

An NSX Edge cluster can have up to 10 edge nodes.

## 5-13 Tier-0 Gateway Uplink Connections

Each Tier-0 gateway can have one or more uplinks to physical networks per NSX Edge node.



The diagram shows two different configurations for the uplinks of the NSX Edge nodes:

- On the left, the Tier-0 gateway has one uplink per NSX Edge node mapped to one VLAN to connect to external networks.
- On the right, the Tier-0 gateway has two uplinks per NSX Edge node mapped to different VLANs.

In both scenarios, the NSX Edge cluster contains two NSX Edge nodes.

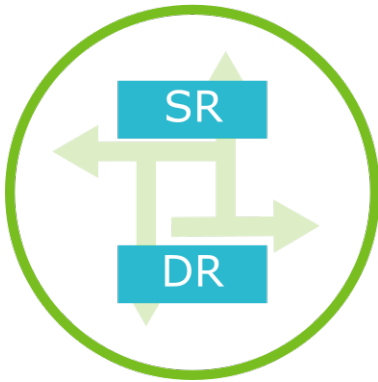
The Tier-0 deployment can be active-active or active-standby. When using a dynamic routing protocol, ECMP can be enabled for multiple northbound uplinks.

## 5-14 Gateway Components: Distributed Router and Service Router (1)

A distributed router (DR) has the following features:

- Provides basic packet-forwarding functionalities
- Spans all transport nodes (host and edge transport nodes)
- Runs as a kernel module in the ESXi hypervisor
- Provides distributed routing functionality
- Provides first-hop routing for workloads

### Gateway



A service router (SR) has the following features:

- Provides north-south routing
- Provides centralized services, such as NAT and VPN
- Required for uplinks to external networks
- Deployed in edge transport nodes

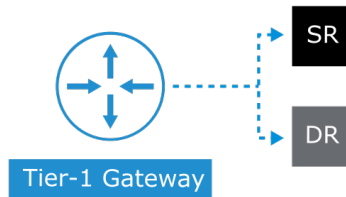
## 5-15 Gateway Components: Distributed Router and Service Router (2)



SRs implement centralized services and are required for uplinks.

DRs implement distributed forwarding.

Gateway



A gateway can be either a Tier-0 or a Tier-1 gateway, depending on the design requirements:

- A Tier-0 gateway provides north-south connectivity:
  - In a single-tier topology, the Tier-0 gateway also provides east-west connectivity.
- A Tier-1 gateway provides east-west connectivity.

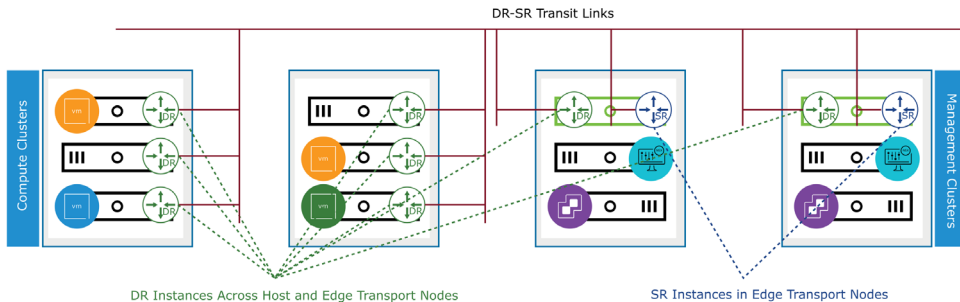
A Tier-1 and a Tier-0 gateway can have DR and SR components:

- The DR component is distributed among all hypervisors and provides basic packet forwarding:
  - A DR is always created when creating a gateway.
- The SR component is only located in the NSX Edge nodes and provides services:
  - An SR is automatically created on the edge node when you configure the gateway with an edge cluster.

## 5-16 Realization of Distributed Routers and Service Routers

Distributed routers and service routers are realized in the following manner:

- Distributed router instances can be realized on host and edge transport nodes.
- Service router instances are realized only on edge transport nodes.
- Distributed routers and service routers are automatically interconnected.

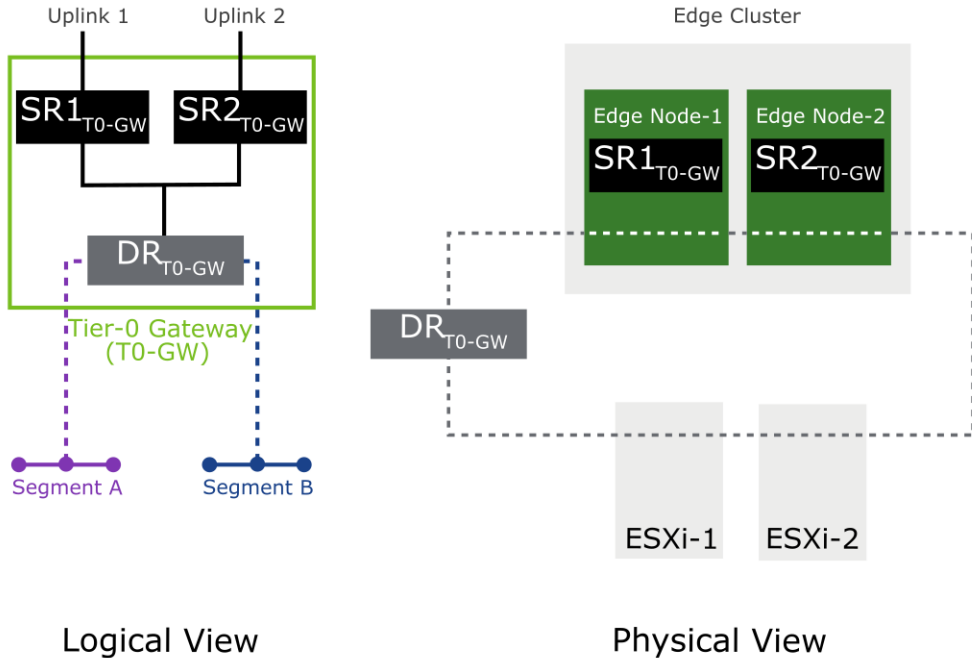


The diagram shows that SR and DR instances can be distributed across the Compute and Management clusters.

SR instances are only realized on the edge transport nodes that are running in the Management cluster while DR instances span across both clusters as they run in host transport nodes and in edge transport nodes. The service and distributed routers are interconnected through the TransitLink ports that are automatically created at the time of deployment.

## 5-17 Gateway Components in a Single-Tier Topology

The diagram shows a logical and physical view of a single-tier configuration.



The diagram represents a single-tier topology where the Tier-0 gateway (T0-GW) has two uplinks configured to physical networks and each uplink is connected to a different SR to provide redundancy.

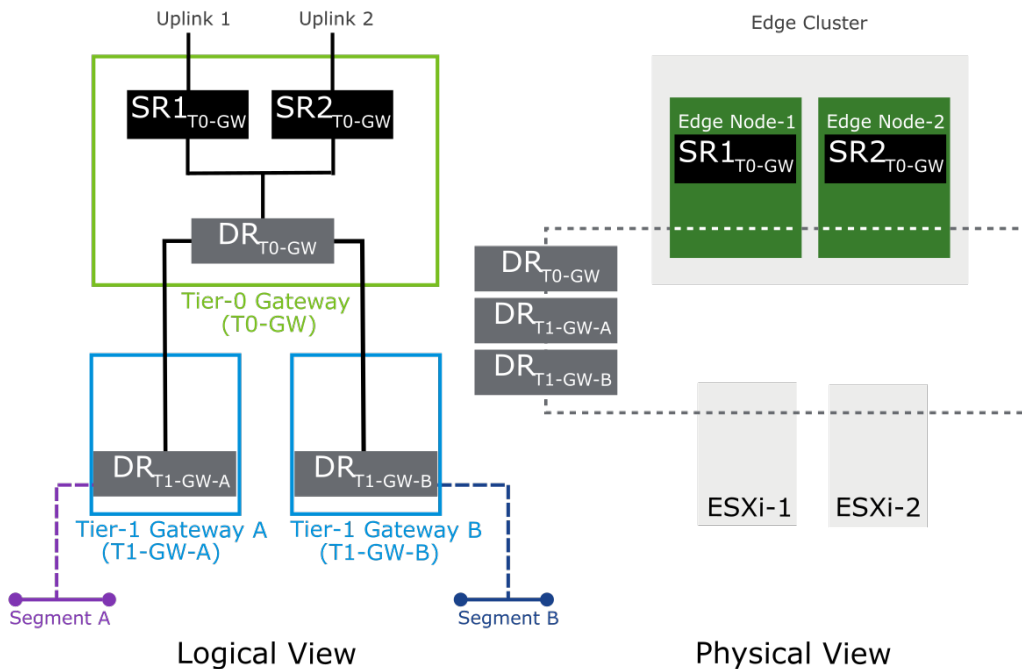
In the physical view, the DR component of the Tier-0 gateway is distributed across all transport nodes (ESXi-1, ESXi-2, Edge Node-1, and Edge Node-2), whereas the SR components are located only on the NSX Edge nodes.

In active-active mode, up to eight SRs can be used to connect the uplinks.



## 5-18 Gateway Components in a Multitier Topology (1)

The diagram shows a logical and physical view of a multitier configuration in which the Tier-1 gateways are not configured with an NSX Edge cluster.



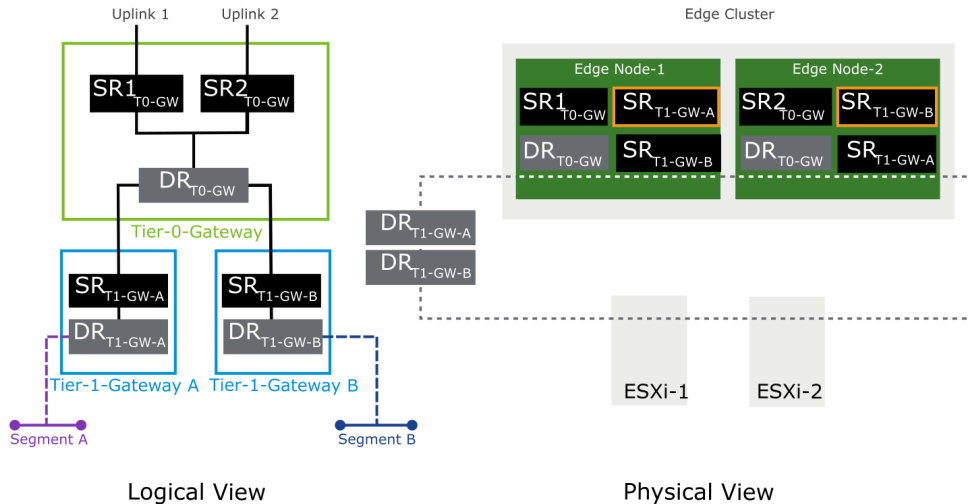
The diagram represents a multitier topology in which the Tier-0 gateway (T0-GW) has two uplinks configured to physical networks. The two Tier-1 gateways have no configured services and therefore were not configured with an NSX Edge cluster. The Tier-1 gateways have no SR components.

In the physical view, the DR component of the Tier-0 gateway is visible. The DR component of Tier-1 Gateway A and the DR component of Tier-1 Gateway B are distributed across all transport nodes (ESXi-1, ESXi-2, Edge Node-1, and Edge Node-2).

The Tier-0 gateway is configured as active-active. SR1 is in Edge Node-1, and SR2 is in Edge Node-2.

## 5-19 Gateway Components in a Multitier Topology (2)

The diagram shows the logical and physical views of a multitier configuration with services configured on both Tier-1 gateways.



The diagram represents a multitier topology in which the Tier-0 gateway (T0-GW) has two uplinks configured to physical networks.

Some services are configured on the two Tier-1 gateways. Each gateway has an SR component.

The DR component of Tier-1 Gateway A and the DR component of Tier-1 Gateway B are distributed across all transport nodes (ESXi-1, ESXi-2, Edge Node-1, and Edge Node-2).

The DR component of the Tier-0 gateway is distributed across the NSX Edge transport nodes (Edge Node-1 and Edge Node-2). It is not distributed across the host transport nodes (ESXi-1 and ESXi-2) when the Tier-1 gateway SR components are deployed.

The Tier-0 gateway has each uplink connected to a different SR. SR1 is in Edge Node-1, and SR2 is in Edge Node-2.

Tier-1 gateways are automatically configured in Active Standby mode so that the SRs are deployed on the two NSX Edge nodes. You can select the preferred active node in each gateway:

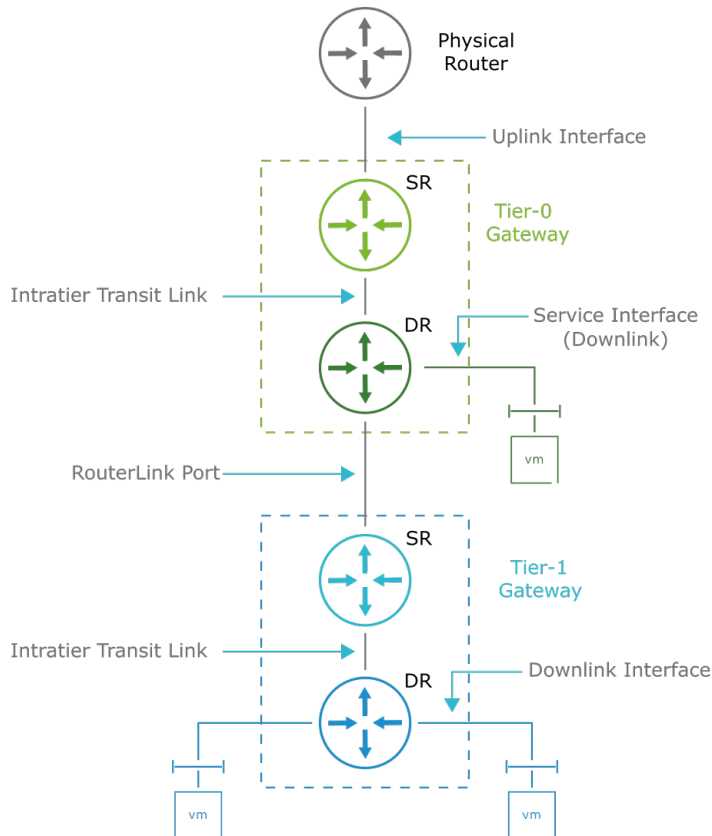
- Edge Node-1 is the active node for Tier-1 Gateway A
- Edge Node-2 is the active node for Tier-1 Gateway B

A dedicated NSX Edge cluster can be used to deploy Tier-1 gateways with services to achieve better performance in larger environments.

## 5-20 Gateway Interfaces

The following types of interfaces are used by gateways:

- Uplink interfaces connect the Tier-0 gateways to upstream physical devices.
- Downlink interfaces connect segments (logical switches) to gateways.
- RouterLink ports connect the Tier-0 and Tier-1 gateways.
- An intratier TransitLink is an internal link between the distributed and service routers on a gateway.
- The service interface is a special interface for VLAN-based services and partner service redirection.



In a logical router deployment in NSX, different types of connections require different types of interfaces:

- The uplink interface provides connections to the external physical infrastructure. VLAN and overlay interface types are supported depending on the use case. The uplink interface is where the external BGP peerings and OSPF adjacencies can be established. External service connections, such as IPSec VPN, can also be used through the uplink interface.
- The downlink interface connects workload networks (where endpoint VMs are running) to the routing infrastructure. A downlink interface is configured to connect to a logical switch (corresponding to the segment defined at the policy). This interface provides the default gateway for the VMs in that subnet.
- RouterLink is a type of interface that connects Tier-0 and Tier-1 gateways. The interface is created automatically when Tier-0 and Tier-1 gateways are connected through an internal logical switch also created automatically. It uses a subnet assigned from the 100.64.0.0/16 IPv4 address space by default.
- The intratier TransitLink connection is also created when a service router is created. It is an internal logical switch between the distributed and service routers on a gateway. By default, the intratier TransitLink has an IP address in the 169.254.0.0/24 subnet range.
- The service interface is a special-purpose port to enable services for VLAN-based networks. North-south service insertion is another use case that requires a service interface to connect a partner appliance and redirect north-south traffic for partner services. Service interfaces are supported on both active-standby Tier-0 logical routers and Tier-1 routers. Firewall, NAT, and VPNs are supported on this interface. The service interface is also a downlink.

## 5-21 Review of Learner Objectives

- Explain the function and features of logical routing
- Describe the architecture of NSX two-tier routing
- Differentiate between north-south and east-west routing
- Describe the gateway components
- Recognize the various types of gateway interfaces

## 5-22 Lesson 2: NSX Edge and Edge Clusters

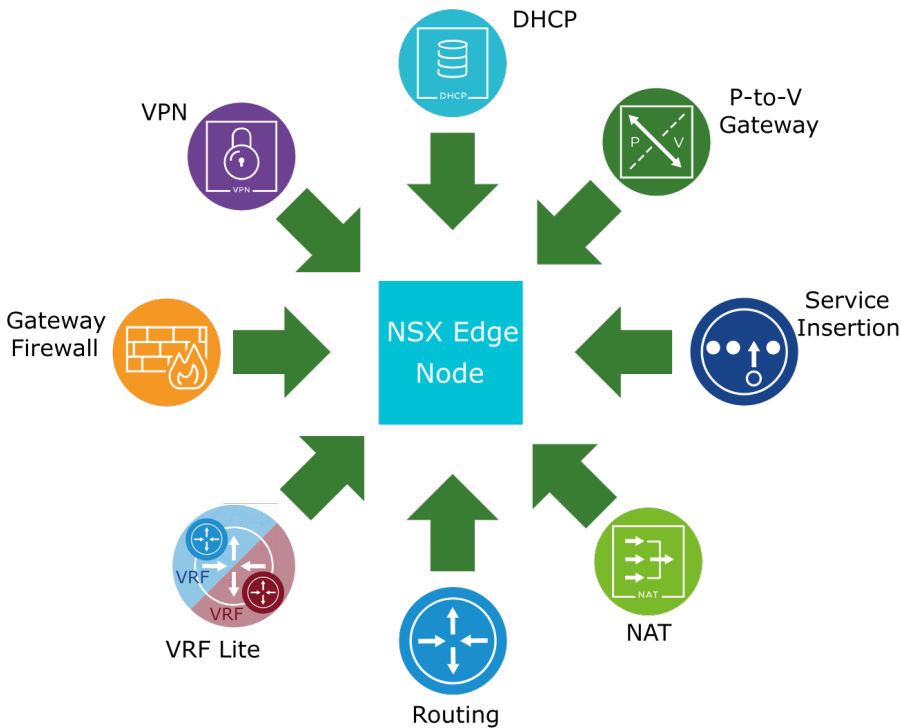
### 5-23 Learner Objectives

- Explain the main functions and features of the NSX Edge node
- Describe the functions of the NSX Edge cluster
- Identify the NSX Edge node form factors and sizing options
- Describe the different NSX Edge node deployment methods

## 5-24 About the NSX Edge Node

The NSX Edge node has several functions:

- Provides connectivity to external networks
- Hosts the Service Router components of Tier-0 and Tier-1 gateways
- Runs the dynamic routing processes and services such as DHCP, NAT, or VPN
- Establishes Geneve tunnels for the overlay networks
- Enables Service Insertion with third-party vendors



NSX Edge is a component of NSX transport zones.

NSX Edge nodes support Data Plane Development Kit (DPDK) for faster packet forwarding in high-performance environments.

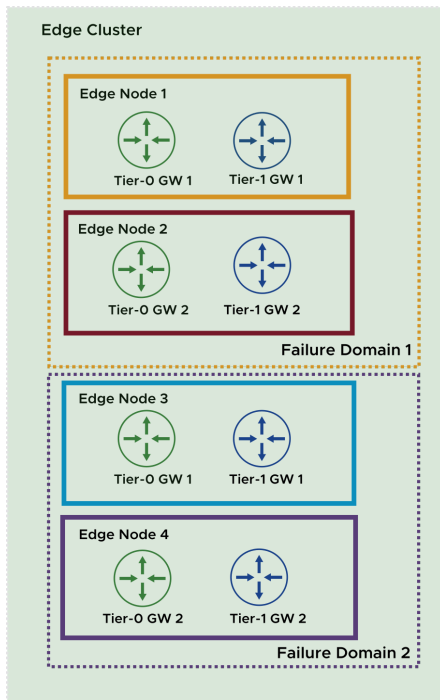
NSX Edge nodes use:

- Container-based architecture for most services
- Separate routing tables for management and overlay traffic

## 5-25 About the NSX Edge Cluster

An NSX Edge cluster is formed by a group of edge nodes and has the following characteristics:

- Provides extra resources to scale out.
- Provides high availability.
- Supports up to 10 edge nodes, and a maximum of 160 clusters can be configured.
- Failure domains can be defined within an edge cluster.



Edge nodes must join an edge cluster to be used as a transport node

An edge cluster can be formed with edge nodes of different form factor types.

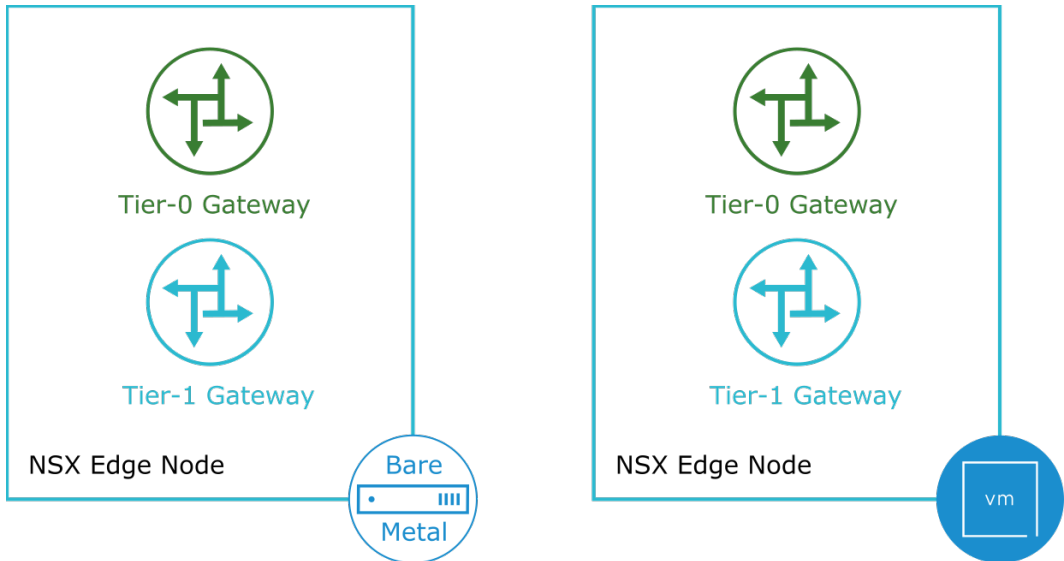
Failure domains can be configured with NSX APIs and are used to automatically place the Tier-1 gateway active and standby instances. Failure domains guarantee service availability, for example, if a rack failure occurs. Active and standby Tier-1 gateway services always run in different failure domains.

The NSX edge cluster scaling and maximums are available at <https://configmax.vmware.com>.

## 5-26 NSX Edge Node Form Factors

The NSX Edge node supports the following form factors:

- VM on an ESXi host
- Bare-metal node





# 5-27 NSX Edge VM Sizing Options

For NSX Edge nodes deployed as VMs on hypervisors, several deployment sizes are available.

Size	Memory	vCPU	Disk Space	VM Hardware Version
Small	4 GB	2	200 GB	ESXi 6.0 or later (VM version 11 or later)
Medium	8 GB	4	200 GB	ESXi 6.0 or later (VM version 11 or later)
Large	32 GB	8	200 GB	ESXi 6.0 or later (VM version 11 or later)
Extra Large	64 GB	16	200 GB	ESXi 6.0 or later (VM version 11 or later)

An NSX Edge node that is deployed as a VM runs on ESXi host hypervisors.

For an NSX Edge node VM deployment, the following sizes are available:

- The small appliance is for proof-of-concept deployments.
- The medium size is suitable when only L2 through L4 features, such as NAT, routing, and L4 firewall, are required and the total throughput requirement is less than 2 Gbps.
- The large size is suitable when only L2 through L4 features, such as NAT, routing, and L4 firewall, are required and the total throughput is 2 through 10 Gbps.
- The extra large size is suitable when the total throughput required is multiple Gbps for VPN and north-south Malware Detection.

For additional information, see *NSX 4.0 Installation Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-3E0C4CEC-D593-4395-84C4-150CD6285963.html>.

## 5-28 Prerequisites for Deploying the NSX Edge Node VM

For deploying an NSX Edge node in the VM form factor, the following prerequisites must be satisfied:

- The supported deployment media are OVA, OVF, ISO, and preboot execution environment (PXE).
- You can only deploy the NSX Edge node VM on an ESXi hypervisor.
- If using PXE, the password for root and admin users must be encrypted with SHA-512.
- The host name must not contain invalid characters.
- You cannot remove or replace VMware Tools on the NSX Edge node VM.
- The required ports and protocols must be open.
- All the edge nodes in an edge cluster should use the same NTP service.

For DPDK support, the underlaying platform must meet the following requirements:

- CPU must have AESNI capability.
- CPU must have 1 GB Huge Page support.

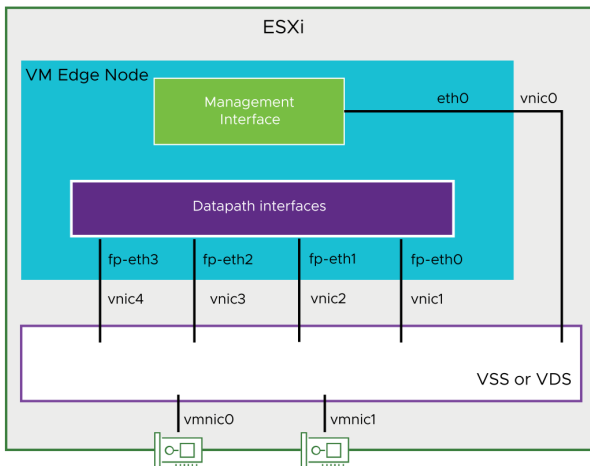
For more information, see *NSX 4.0 Installation Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-3E0C4CEC-D593-4395-84C4-150CD6285963.html>.

For information about the required ports and protocols, see VMware Ports and Protocols at <https://ports.esp.vmware.com/home/NSX>.

## 5-29 Deployment Considerations for NSX Edge Node VM Interfaces

An edge node deployment requires various interface types and assignments:

- In the vSphere virtual switch, you must allocate at least two ports for the NSX Edge node.
- The first interface must be defined for management access (eth0) by using one NSX Edge VM vNIC.
- The other four interfaces are datapath interfaces (fp-ethX) and are dedicated for overlay tunneling and uplink connections by using the remaining vNICs.



Edge node VM deployment requires specific interface assignments:

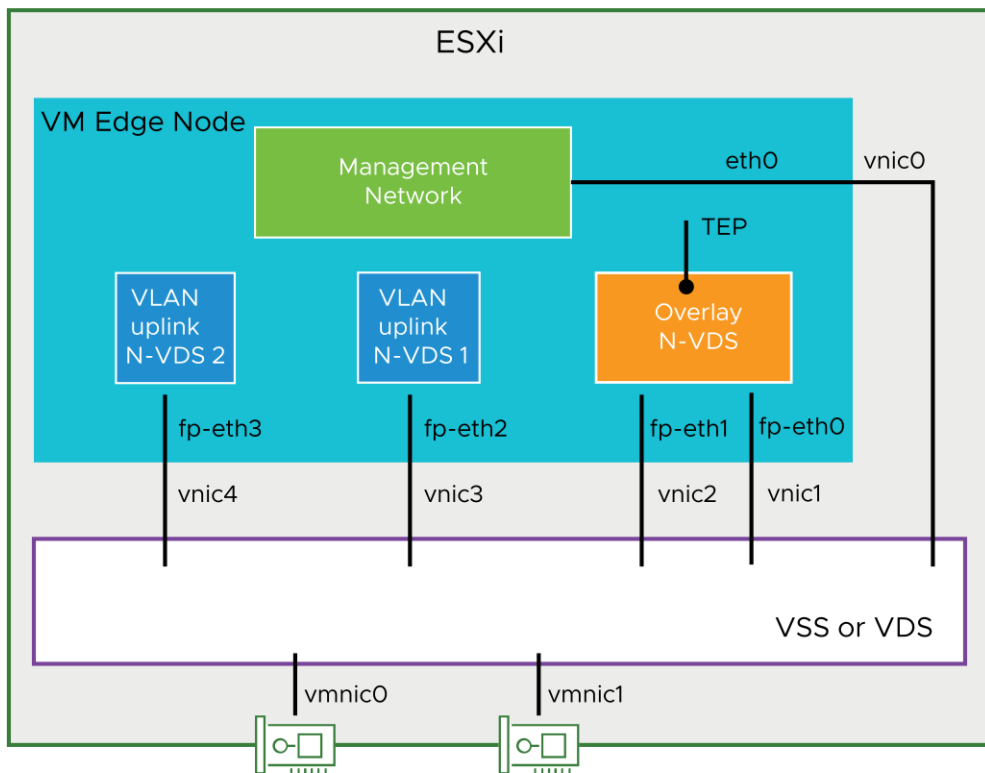
- The first interface of the deployment must be assigned to a management interface.
- Other interfaces must be assigned to the datapath process that creates the overlay or VLAN-based N-VDS.

From NSX-T Data Center 3.2.1, you can use up to four datapath interfaces (fp-ethx) for greenfield deployments. For brownfield deployments upgraded to NSX-T Data Center 3.2.1, you can redeploy the NSX Edge nodes if you need four interfaces for datapath as stated in the VMware NSX-T Data Center 3.2.1 Release Notes at <https://docs.vmware.com/en/VMware-NSX/3.2.1/rn/vmware-nsxt-data-center-321-release-notes/index.html>.

## 5-30 Deploying the NSX Edge Node VM with Multiple N-VDS

An edge node VM with multiple N-VDS has the following characteristics:

- Five vNICs are available on the VM.
- The first internal interface is dedicated for management (eth0).
- The remaining interfaces are allocated for the datapath module (fp-ethX).
- Connectivity to VSS and VDS is supported in the hypervisors.
- Multiple N-VDS exist on the edge for overlay and VLAN uplink traffic.



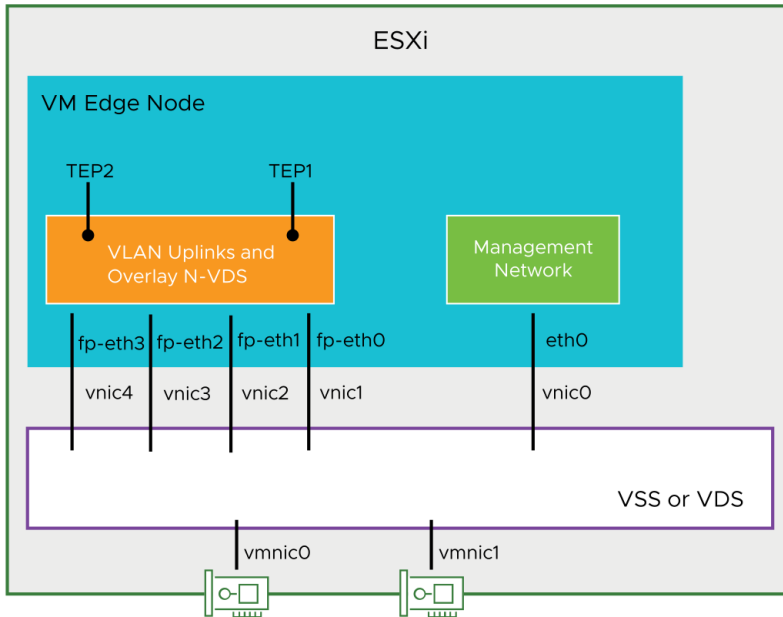
The fp-ethx interfaces can be assigned to overlay or external VLAN traffic.

Each N-VDS in the edge node can have its own teaming policy.

## 5-31 Deploying the NSX Edge Node VM with a Single N-VDS

An edge node VM with single N-VDS has the following characteristics:

- Single N-VDS in the VM edge node.
- It carries both overlay and VLAN uplink traffic.
- Two TEPs are configured to provide load balancing for the overlay traffic.



Use the predefined uplink profile, `nsx-edge-multiple-vsteps-uplink-profile`, to configure the edge node VM with two TEPs. TEPs are mapped to each of the uplinks configured in the uplink profile for the overlay traffic.

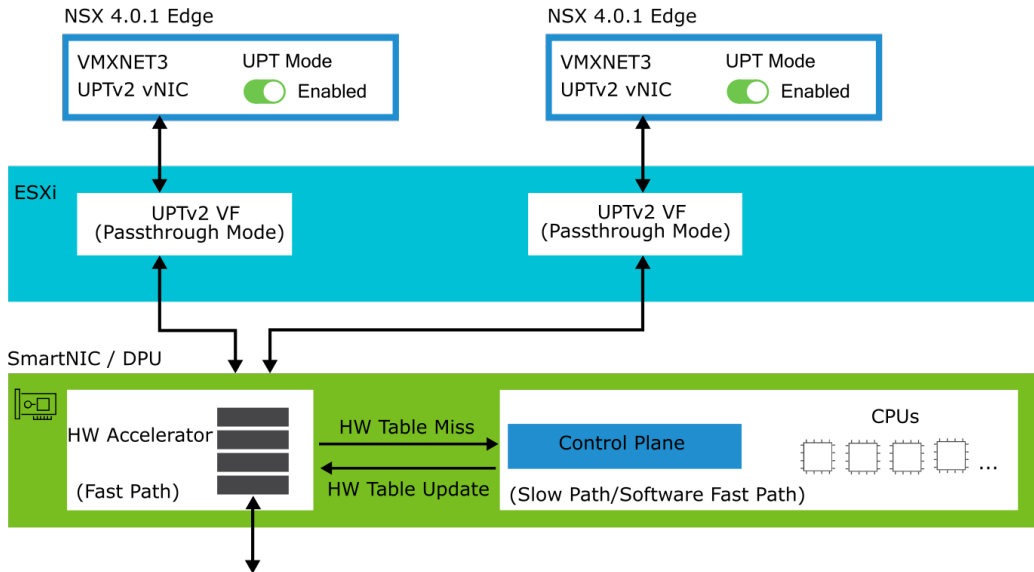
The ESXi TEP and the edge node TEP IP addresses are in the same subnet.

A named teaming policy can be used for each VLAN uplink traffic for better load balancing of the traffic across the uplinks and override the default teaming policy.

This architecture aligns with the existing support for a single N-VDS in bare-metal edge nodes.

## 5-32 NSX Edge Node VM Network Offloading with SmartNICs

Like any other VM, you can achieve network offloading of NSX Edge traffic using the new SmartNIC framework. To use this feature, enable Uniform Passthrough (UPT) mode in NSX Edge.



NSX 4.0.1 Edge, using VMXNET3 UPTv2 vNICs, can work in passthrough mode while preserving the functionalities of emulated vNICs such as vSphere vMotion.

# 5-33 Requirements for the NSX Edge Bare-Metal Node

The NSX Edge node can be installed on bare-metal hardware.

Form Factor	Memory	CPU Cores	Disk	DPDK CPU Requirements
Bare metal (minimum requirements)	32 GB	8	200 GB	AES-NI 1 GB Huge Page support
Bare metal (recommended requirements)	256 GB	24	200 GB	AES-NI 1 GB Huge Page support

The NSX Edge bare metal supports only specific CPU types and has some NIC requirements.

For a list of requirements, see *NSX 4.0 Installation Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-3E0C4CEC-D593-4395-84C4-150CD6285963.html>.

If the hardware is not listed, the storage, video adapter, or motherboard components might not work on the NSX Edge node.

## 5-34 Prerequisites for Deploying the NSX Edge Bare-Metal Node

For deploying an NSX Edge node in the bare-metal form factor, the following prerequisites must be satisfied:

- The only supported deployment media is ISO either with or without the preboot execution environment (PXE).
- The bare-metal form factor has specific hardware requirements.
- If using PXE, the password for root and admin users must be encrypted with SHA-512.
- The host name must not contain invalid characters.
- The required ports and protocols must be open.
- All the edge nodes in an edge cluster should use the same NTP service.

For more information, see *NSX 4.0 Installation Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-3E0C4CEC-D593-4395-84C4-150CD6285963.html>.

For information about the required ports and protocols, see VMware Ports and Protocols at <https://ports.esp.vmware.com/home/NSX>.

## 5-35 Deployment Methods for NSX Edge Nodes

The following ways are available to deploy an edge node in the VM form factor:

- Use the NSX UI.
- Deploy an OVF template in vCenter.
- Use the OVF tool command-line utility.
- Use an ISO file and a PXE server to automate the network configuration.

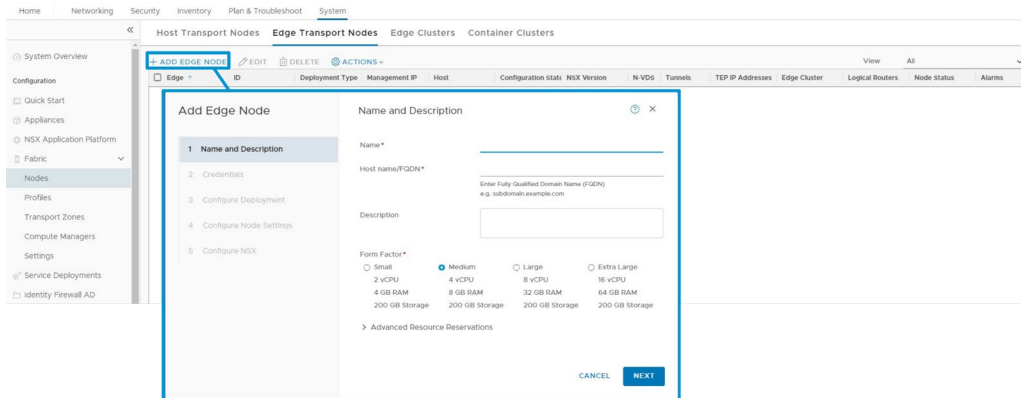
For the bare-metal form factor, an ISO file is used for the installation:

- You can use a PXE server to automate the network configurations.



## 5-36 Deploying NSX Edge Nodes from the NSX UI (1)

You can deploy edge transport nodes directly from the NSX UI by navigating to **System > Fabric > Nodes > Edge Transport Nodes**.



In the NSX UI, select **System > Fabric > Nodes** and click the **Edge Transport Nodes** tab to add an edge VM.

On the Name and Description page of the Add Edge VM wizard, configure the following settings:

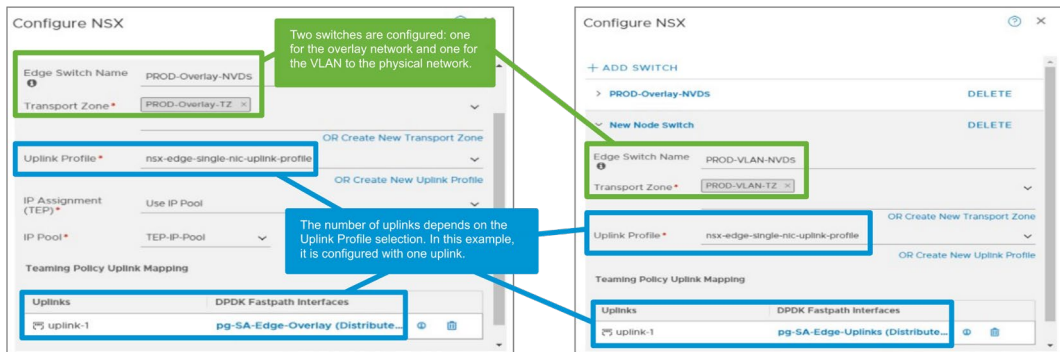
- Name
- Host name/FQDN
- Form factor

You can also select the resource reservation (CPU, memory, and shares) during the NSX Edge deployment.

## 5-37 Deploying NSX Edge Nodes from the NSX UI (2)

The datapath interfaces are defined when adding the edge transport node:

- The number of TEP interfaces is based on the Uplink Profile selection.
- An NSX Edge node can belong to one overlay network and multiple VLAN transport zones.
- An NSX Edge node must belong to at least one VLAN transport zone to provide uplink access.
- The uplink profile determines the number of uplinks.



All nonmanagement links on the edge node are used for the uplinks and tunnels.

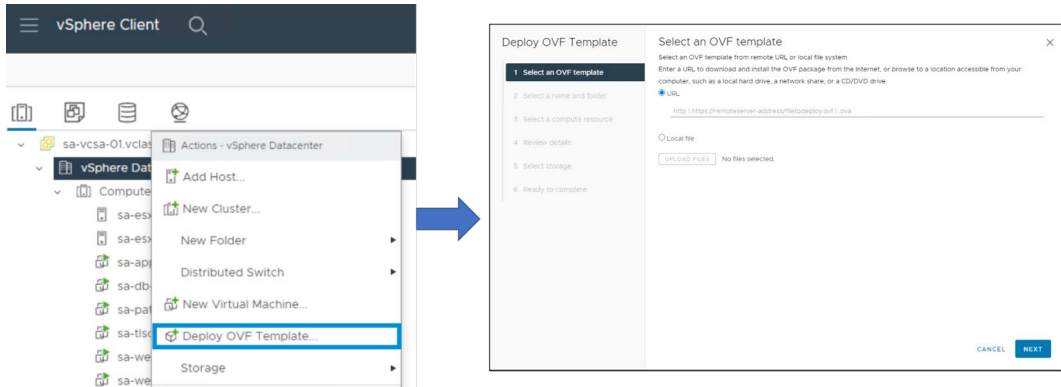
In the example, one uplink is used for the tunnel endpoint (overlay network), and another uplink is used for the external physical network (VLAN).

During the N-VDS creation, the uplinks can be individually assigned per N-VDS. The uplink profiles (single-nic-uplink-profile in the diagram) determine the number of uplink interfaces.

You can modify the datapath interfaces later by editing the edge transport nodes.

## 5-38 Deploying NSX Edge Nodes from vCenter

You can deploy NSX Edge nodes in the vSphere Client from an OVF template.



The NSX Edge nodes can be installed or deployed using various methods. If you prefer an interactive edge installation, you can use a UI-based VM management tool, such as the vSphere Client connected to vCenter.

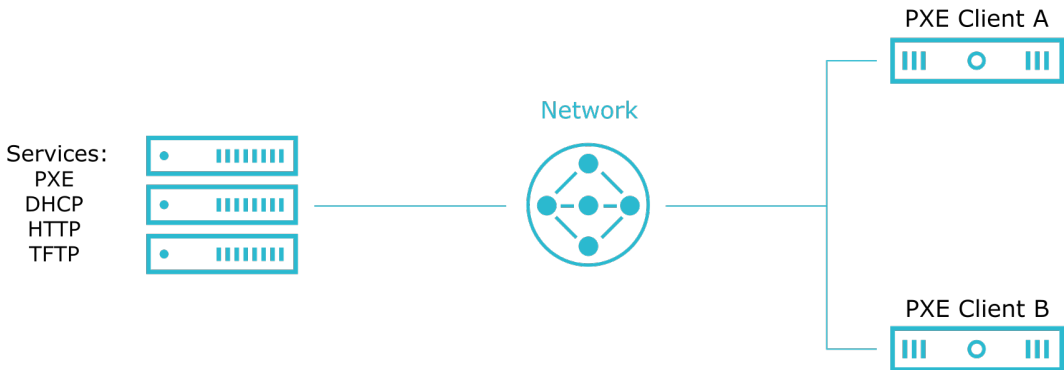
The image shows the option to deploy through vCenter or the vSphere Client. A wizard guides you through the steps so that you can provide the required details.

This process does not register the NSX Edge node with the management plane. Additional command-line operations are required.

## 5-39 Using PXE to Deploy NSX Edge Nodes from an ISO File

By using PXE, the networking settings, such as IP address, gateway, network mask, NTP, and DNS, are automatically configured.

The PXE boot process includes several components, including DHCP, HTTP, and TFTP servers.



This operation automates the installation process. You can preconfigure the deployment with all the required network settings for the appliance.

The password for root and admin users must be encrypted with SHA-512.

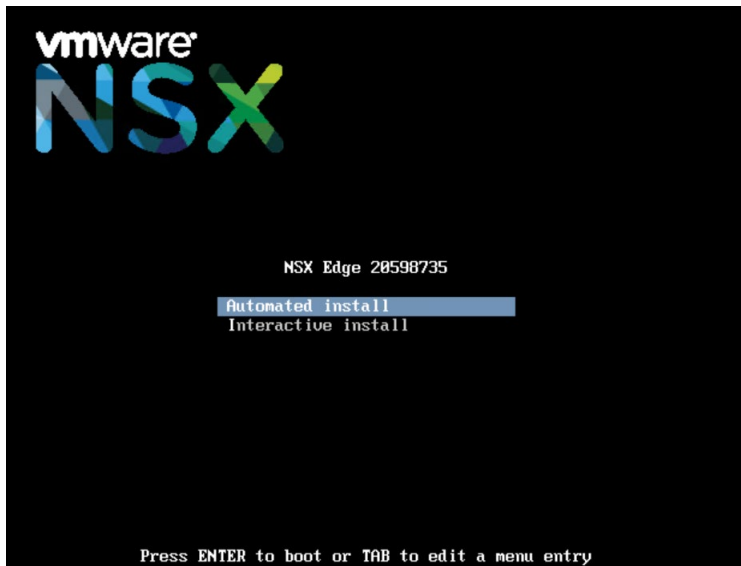
The preboot execution environment (PXE) boot can also be used to install NSX Edge nodes on a bare-metal platform.

The PXE method supports only the NSX Edge node deployment. It does not support NSX Manager deployments.

## 5-40 Installing NSX Edge on Bare Metal

To install NSX Edge on bare metal using an ISO file:

1. Verify that the system BIOS mode is set to Legacy BIOS.
2. Create a bootable disk with the NSX Edge ISO file on it.
3. Boot the physical machine from the disk.
4. Select **Automated install**.



Manual installation is also available when you install NSX Edge nodes on a bare-metal server.

After the listed requirements are verified, the installation process should start automatically from the installation media.

After the bootup and power-on processes are complete, the system requests an IP address (manual or DHCP).

By default, the following credentials are used:

- Root login password: vmware
- Password: default

Further setup procedures include enabling the interfaces and joining the edge node to the management plane.

You can use PXE to automate the network configuration installation.

## 5-41 Joining NSX Edge Bare Metal with the Management Plane

Installing the NSX Edge node by any method other than the NSX UI does not automatically join NSX Edge to the management plane.

To join an NSX Edge node with the management plane:

1. Open an SSH session to the NSX Manager appliance and retrieve the SSL thumbprint by entering `get certificate api thumbprint` at the command prompt.
2. Open an SSH session to the edge node and run the `join management-plane` command.

```
sa-nsxmgr-01> get certificate api thumbprint
78ca1577cdba966fe0a5809069459261f3e309d1a505b6283c9ce0ab53f4e435

sa-nsxedge-02> join management-plane 172.20.10.41 username admin password VMware!VMware!
thumbprint 78ca1577cdba966fe0a5809069459261f3e309d1a505b6283c9ce0ab53f4e435

Node successfully registered and Edge restarted

sa-nsxedge-02> get managers
- 172.20.10.41 Connected
```

The NSX Edge node successfully joined the management plane.

The manual installation of NSX Edge nodes does not include an automated procedure to ensure that the management plane sees edge nodes as available resources.

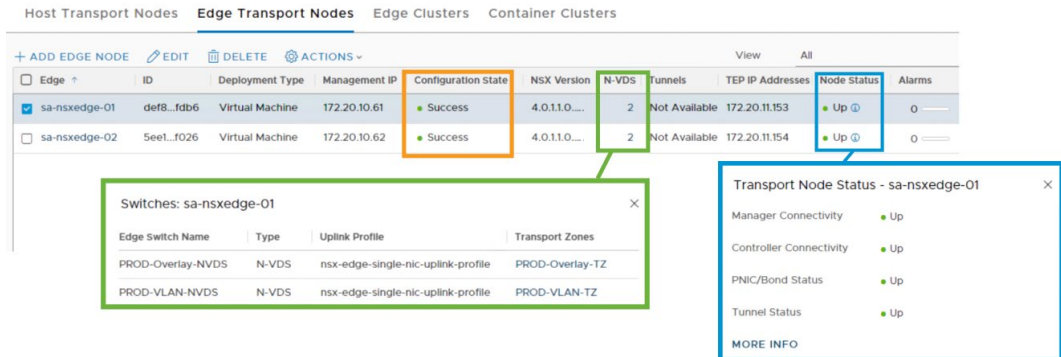
You must join NSX Edge with the management plane so that they can communicate with each other.

Joining NSX Edge nodes to the management plane ensures that the edge nodes are available from the management plane as managed nodes.

First, you must verify that you have administration privileges to access NSX Edge nodes and the NSX UI. Then you can use the CLI to join the NSX Edge nodes to the management plane.

## 5-42 Verifying the Edge Transport Node Status

In the NSX UI, navigate to **System > Fabric > Nodes > Edge Transport Nodes** to verify the nodes status and configuration state.



Host Transport Nodes <b>Edge Transport Nodes</b> Edge Clusters   Container Clusters										
+ ADD EDGE NODE   EDIT   DELETE   ACTIONS										
Edge	ID	Deployment Type	Management IP	Configuration State	NSX Version	N-VDS	Tunnels	TEP IP Addresses	Node Status	Alarms
<input checked="" type="checkbox"/>	sa-nsxedge-01	def8...fdb6	Virtual Machine	172.20.10.61	Success	4.0.1.1.0...	2	Not Available	172.20.11.153	Up
<input type="checkbox"/>	sa-nsxedge-02	5ee1...f026	Virtual Machine	172.20.10.62	Success	4.0.1.1.0...	2	Not Available	172.20.11.154	Up

Switches: sa-nsxedge-01

Edge Switch Name	Type	Uplink Profile	Transport Zones
PROD-Overlay-NVDS	N-VDS	nsx-edge-single-nic-uplink-profile	PROD-Overlay-TZ
PROD-VLAN-NVDS	N-VDS	nsx-edge-single-nic-uplink-profile	PROD-VLAN-TZ

Transport Node Status - sa-nsxedge-01

- Manager Connectivity: Up
- Controller Connectivity: Up
- PNIC/Bond Status: Up
- Tunnel Status: Up

MORE INFO

In the NSX UI, select **System > Fabric > Nodes** and click the **Edge Transport Nodes** tab to view the status of the edge nodes known by NSX Manager or the management plane.

The **Edge Transport Nodes** tab lists the following categories:

- Configuration state
- Node status
- N-VDS
- NSX version

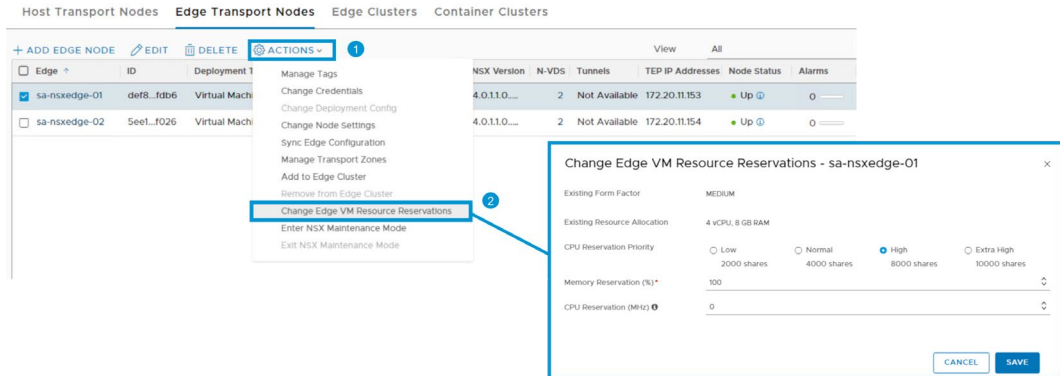
Clicking the information icon next to the node status provides additional information about the reasons for a given status.

Clicking the number of N-VDS gives information about the attached transport zones.

If you want to verify the datapath interfaces, click **Edit** on the given edge transport node.

## 5-43 Changing the NSX Edge VM Resource Reservations

You can change the VM resource reservation for the NSX Edge VMs deployed by using NSX Manager. Navigate to **Actions > Change Edge VM Resource Reservations**.



To change the NSX Edge VM resource reservations:

1. Click **Change Edge VM Resource Reservations** to access the reservations for the selected NSX Edge node.
2. Select the reservations to be changed:
  - **CPU Reservation Priority**
  - **Memory Reservation (%)**
  - **CPU Reservation (MHz)**



## 5-44 Changing Node Settings

Select **Change Node Settings** from the **Actions** menu to modify the NSX Edge node settings.

The screenshot displays the NSX Manager interface. At the top, there are tabs for 'Host Transport Nodes', 'Edge Transport Nodes', 'Edge Clusters', and 'Container Clusters'. The 'Edge Transport Nodes' tab is active. Below the tabs, there is a table of nodes. The first node, 'sa-nsxedge-01', is selected. A blue box labeled '1' highlights the 'ACTIONS' menu, and a blue box labeled '2' highlights the 'Change Node Settings' option in the dropdown menu. The 'Change Node Settings' dialog is open, showing the following fields:

- Host name/FQDN: sa-nsxedge-01.vclass.local
- Search Domain Names: vclass.local
- DNS Servers: 172.20.10.10
- NTP Servers: 172.20.10.100
- Enable UPT mode for datapath interface: No

The dialog has 'CANCEL' and 'SAVE' buttons at the bottom right.

To change the NSX Edge node settings:

1. Click **Change Node Settings** to access the settings for the selected NSX Edge node.
2. Select the settings to be changed:
  - **Host name/FQDN**
  - **Search Domain Names**
  - **Allow SSH Login**
  - **DNS Servers**
  - **NTP Servers**
  - **UPT Mode**

## 5-45 Enabling UPT Mode on NSX Edge Node VMs

You enable the Uniform Passthrough (UPT) mode on an NSX Edge VM during Edge node setting configuration.

The screenshot shows the 'Add Edge Node' configuration interface. On the left, a sidebar lists five steps: 1 Name and Description, 2 Credentials, 3 Configure Deployment, 4 Configure Node Settings (highlighted), and 5 Configure NSX. The main area is titled 'Configure Node Settings' and contains the following fields:

- Management IP Assignment:** Radio buttons for DHCP and Static (selected). Below are fields for Management IP (172.20.10.65/24) and Default Gateway (172.20.10.10).
- Management Interface:** A dropdown menu showing 'pg-SA-Management (Distributed VI...'.
- Search Domain Names:** A text field containing 'vclass.local'.
- DNS Servers:** A text field containing '172.20.10.10'.
- NTP Servers:** A text field containing '172.20.10.100'.
- Enable UPT mode for datapath interface:** A toggle switch that is turned on (green), with the label 'Yes'.

At the bottom right, there are three buttons: 'CANCEL', 'PREVIOUS', and 'NEXT'. A blue callout box with the text 'Enable Uniform Passthrough Mode' points to the UPT toggle switch.

You enable the Uniform Passthrough (UPT) mode on an NSX Edge node to improve overall system performance and reduce latency.

Changing the NSX Edge UPT mode on a production NSX Edge node affects services.

The NSX Edge UPT mode setting will only be applicable when:

- At least one of the host's datapath interfaces is SmartNIC-enabled.
- The vSphere supported hardware is version 20 or later.

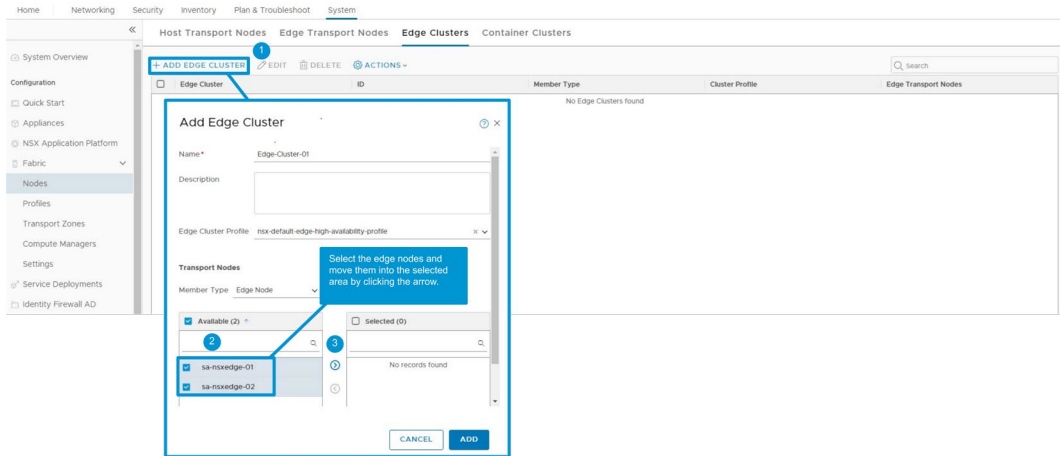
## 5-46 Postdeployment Verification Checklist

After deployment, you can verify the connectivity of the NSX Edge nodes in several ways:

- ✓ If you enabled SSH, verify that you can use SSH to access the newly deployed edge nodes.
- ✓ Verify that you can ping your NSX Edge node.
- ✓ Verify that the NSX Edge nodes can ping their corresponding default gateway.
- ✓ Verify that the NSX Edge nodes can ping the hypervisor hosts that are in the same network as the NSX Edge nodes.
- ✓ Verify that the NSX Edge nodes can reach their configured DNS server and NTP server.

## 5-47 Creating an NSX Edge Cluster

You can deploy an NSX Edge cluster from the NSX UI by navigating to **System > Fabric > Nodes > Edge Clusters**.



You might want to create an NSX Edge cluster for the following reasons:

- Having a multinode cluster of NSX Edge nodes ensures that at least one NSX Edge node is always available.
- An NSX Edge cluster is required to configure Tier-0 gateways uplinks and enable stateful services such as NAT, load balancer, and so on.

To configure an NSX Edge cluster:

1. Click **+ADD EDGE CLUSTER** to start the process for creating an NSX Edge cluster.
2. Select a predefined NSX Edge cluster profile or select **nsx-default-edge-high-availability-profile**, which is the default profile.
3. Include NSX Edge node members in the NSX Edge cluster.

An NSX Edge transport node can be added to only one NSX Edge cluster.

After creating the NSX Edge cluster, you can later edit it to add NSX Edge nodes.

## 5-48 Lab 6: Deploying and Configuring NSX Edge Nodes

Deploy NSX Edge nodes and configure them as transport nodes:

1. Prepare for the Lab
2. Deploy Two NSX Edge Nodes
3. Configure an Edge Cluster

## 5-49 Review of Learner Objectives

- Explain the main functions and features of the NSX Edge node
- Describe the functions of the NSX Edge cluster
- Identify the NSX Edge node form factors and sizing options
- Describe the different NSX Edge node deployment methods

## 5-50 Lesson 3: Configuring Tier-0 and Tier-1 Gateways

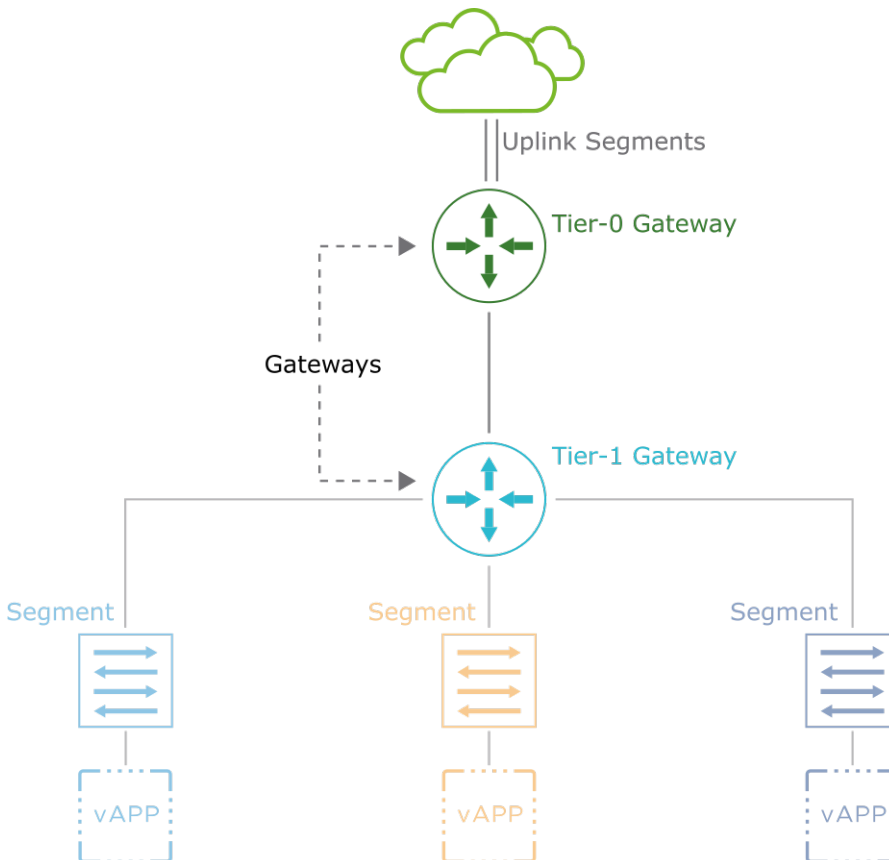
### 5-51 Learner Objectives

- Describe how to configure a Tier-1 gateway
- Explain how to configure a Tier-0 gateway
- Test end-to-end connectivity provided by Tier-0 and Tier-1 gateways

## 5-52 Gateway Configuration Tasks

To achieve full network connectivity, you must configure the following components:

1. Create the Tier-1 gateway and its segments.
2. Connect the segments to the Tier-1 gateway.
3. Create uplink segments.
4. Create the Tier-0 gateway and define the uplink connections.
5. Configure static or dynamic routing on the Tier-0 gateway.
6. Configure the connectivity between the Tier-0 and Tier-1 gateways.
7. Enable route advertisement and redistribution.



Depending on the environment, the order of the configuration tasks can vary. Sometimes you might want to create the Tier-0 gateway before the Tier-1 gateway.

Before configuring the Tier-1 and Tier-0 gateways, verify the following settings:

- Your NSX management cluster is stable.
- At least one NSX Edge node is installed.
- An NSX Edge cluster is configured.

The gateways are not automatically connected to each other during the creation process. The management plane cannot determine which Tier-1 instance should connect to which Tier-0 instance. You must manually connect the gateways after their creation.

After you manually connect these instances, the management plane programs the routes in these instances to establish connectivity between tiers.

## 5-53 Creating the Tier-1 Gateway

Create a Tier-1 gateway by navigating to **Networking > Connectivity > Tier-1 Gateways**.

The screenshot shows the NSX web interface for creating a Tier-1 Gateway. The left sidebar contains navigation links: Network Overview, Network Topology, Connectivity, Tier-0 Gateways, Tier-1 Gateways (selected), Segments, Network Services, VPN, EVPN Tenant, NAT, Load Balancing, and Forwarding Policies. The main panel is titled 'Tier-1 Gateways' and includes a table with columns: Name, HA Mode, Linked Tier-0 Gateway, #Linked Segments, and Status. An 'ADD TIER-1 GATEWAY' button is highlighted with a blue box. A callout box points to the 'HA Mode' dropdown, which is set to 'Active Standby', with the text: 'Select Distributed Only if you are not planning to configure any stateful services. Otherwise select Active Standby or Active Active modes.' Another callout box points to the 'Edge Cluster' dropdown, which is set to 'Select Edge Cluster', with the text: 'You only have to select an Edge Cluster for Active Standby and Active Active modes.' The form includes fields for 'Enter Name', 'Edges Pool Allocation Size', 'Description', and 'Route Advertisement'. A 'SAVE' button is at the bottom.

Select the **Distributed Only** HA mode if you are not planning to use any stateful services on the Tier-1 gateway.

In the Distributed Only HA mode, no edge cluster is required for the Tier-1 gateway. No SR is created for the Tier-1 gateway (only the DR component is created). This method saves resources and protects from unintended hairpinning of traffic over the edge nodes.



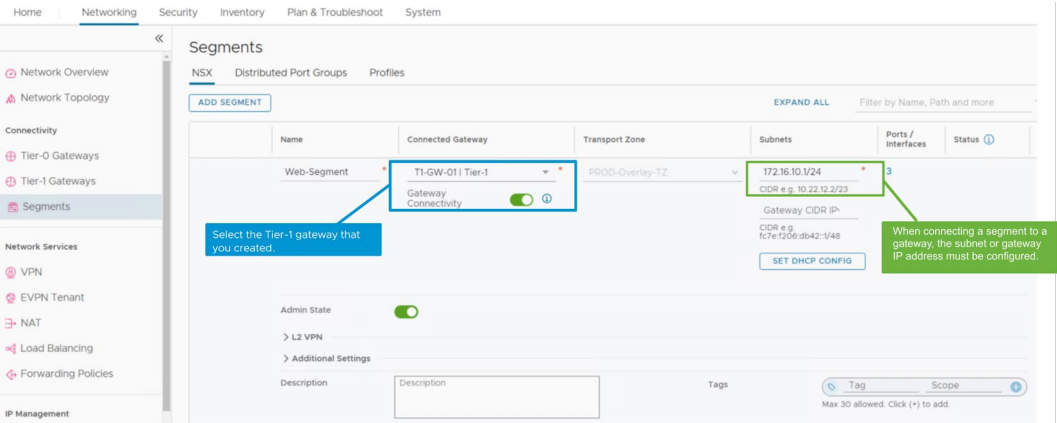
In the Active Standby HA mode, traffic is processed by the active Tier-1 gateway member. The standby member only takes over the traffic if the active member fails.

In the Active Active HA mode, if the Tier-1 gateway is connected to a Tier-0 gateway with stateful services, the Tier-1 gateway also supports stateful services.

For Active Standby and Active Active HA modes, an edge cluster is required to provide the resources for stateful services.

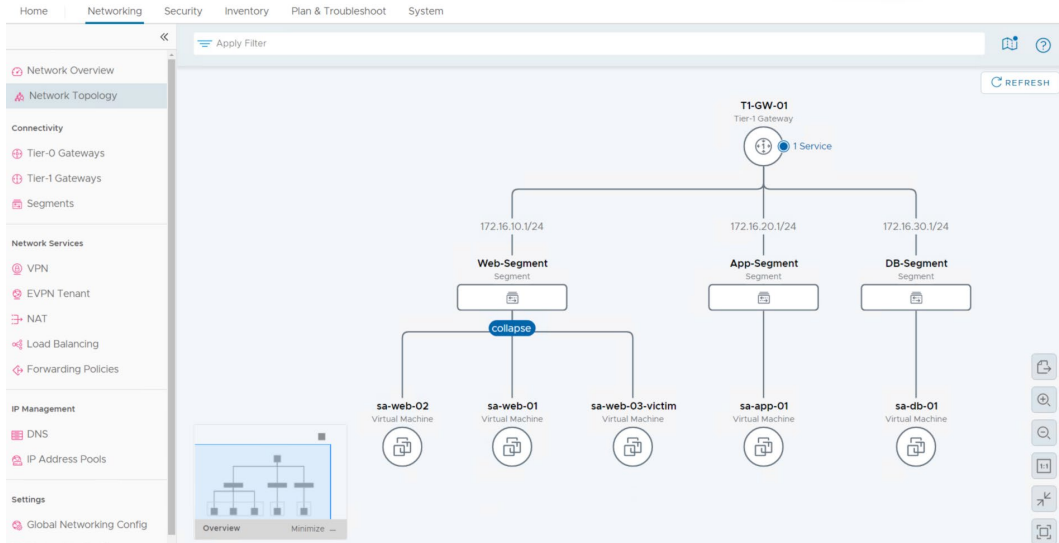
# 5-54 Connecting Segments to the Tier-1 Gateway

Connect segments to the Tier-1 gateway by navigating to **Networking > Connectivity > Segments > NSX**.



## 5-55 Using Network Topology to Validate the Tier-1 Gateway Configuration

The topology diagram shows the segments connected to T1-GW-01 and its subnets.



Pointing to an entity highlights the path to the root, for example, VM or segment or Tier-1 gateway.

If the magnification level is less than 1, then the entity names are not displayed in the topology diagram.

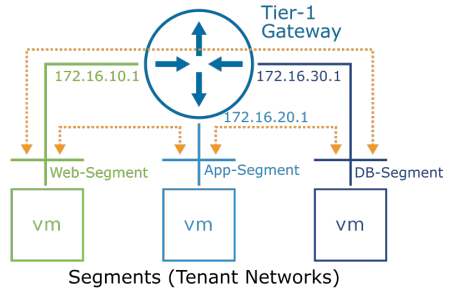
Clicking an entity opens the side panel with more details per entity type. An entity might be a VM, a segment, or gateways,

## 5-56 Testing East-West Connectivity

VMs on various subnets (segments) attached to the Tier-1 gateway can reach each other.

A ping from a VM(172.16.10.11) on a segment (Web-Segment) to another VM (172.16.20.11) on another segment (App-Segment) should work as a result of distributed routing.

```
root@sa-web-01 [ ~ ]# ping 172.16.20.11
PING 172.16.20.11 (172.16.20.11) 56(84) bytes of data.
64 bytes from 172.16.20.11: icmp_seq=1 ttl=63 time=3.76 ms
64 bytes from 172.16.20.11: icmp_seq=2 ttl=63 time=1.58 ms
64 bytes from 172.16.20.11: icmp_seq=3 ttl=63 time=1.65 ms
64 bytes from 172.16.20.11: icmp_seq=4 ttl=63 time=1.71 ms
64 bytes from 172.16.20.11: icmp_seq=5 ttl=63 time=1.74 ms
^C
--- 172.16.20.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.575/2.088/3.762/0.838 ms
root@sa-web-01 [ ~ ]#
```



The Tier-1 gateway is created and the interfaces for various logical networks are configured. You can verify the east-west connectivity in the tenant environment.

# 5-57 Creating the Uplink Segments

Create the uplink segments that are associated with the Tier-0 gateway uplinks.

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

Segments

NSX Distributed Port Groups Profiles

ADD SEGMENT

COLLAPSE ALL

Active Filter

	Name	Connected Gateway	Transport Zone	Subnets
⋮	Uplink-1	None	PROD-VLAN-TZ   VLAN	Not Set
	Uplink Teaming Policy	Not Set	VLAN	0
	Admin State	Up		
	> L2 VPN			
	> Additional Settings			
	Description	Not Set	Tags	0
>	SEGMENT PROFILES			
⋮	Uplink-2	None	PROD-VLAN-TZ   VLAN	Not Set
	Uplink Teaming Policy	Not Set	VLAN	0
	Admin State	Up		
	> L2 VPN			
	> Additional Settings			
	Description	Not Set	Tags	0

Upstream Physical Router

Uplink-1

Uplink-2

Tier-0 Gateway

Tier-1 Gateway

Each Tier-0 gateway can have multiple uplink connections, depending on the requirements and the actual configuration.

In the example, two different segments are configured to connect the Tier-0 gateway uplink interfaces.

## 5-58 Creating the Tier-0 Gateway (1)

Create a Tier-0 gateway by navigating to **Networking > Connectivity > Tier-0 Gateways**.

The screenshot shows the 'Tier-0 Gateways' configuration page. The left sidebar contains a navigation menu with 'Tier-0 Gateways' selected. The main area displays a table of existing gateways, with a new entry 'T0-GW-01' being added. A modal window is open for configuring 'T0-GW-01'. The modal includes fields for 'Name', 'HA Mode' (set to 'Active Active'), 'Stateful' (a toggle switch), 'Edge Cluster' (a dropdown menu), and 'DHCP Config'. Below these are sections for 'Additional Settings', 'Route Distinguisher for VRF Gateways', 'Description', and 'Tags'. A 'NOTE' section states: 'Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save.' The bottom of the modal has sections for 'INTERFACES', 'ROUTING', 'BGP', 'OSPF', 'ROUTE RE-DISTRIBUTION', and 'MULTICAST', along with 'SAVE' and 'CANCEL' buttons. A success message at the bottom left states: 'Tier-0 Gateway T0-GW-01 is successfully created. Do you want to continue configuring this Tier-0 Gateway?' with 'YES' and 'NO' buttons. Annotations with arrows point to the 'ADD GATEWAY' button, the 'Tier-0' dropdown, the 'Stateful' toggle, the 'Edge Cluster' dropdown, and the 'SAVE' button.

Turn on Stateful in Active Active HA Mode if you need to enable stateful services.

Because Tier-0 is configured with uplinks, a cluster has to be specified.

You must save the configurations before you can configure the interfaces.

Tier-0 Gateway T0-GW-01 is successfully created. Do you want to continue configuring this Tier-0 Gateway?

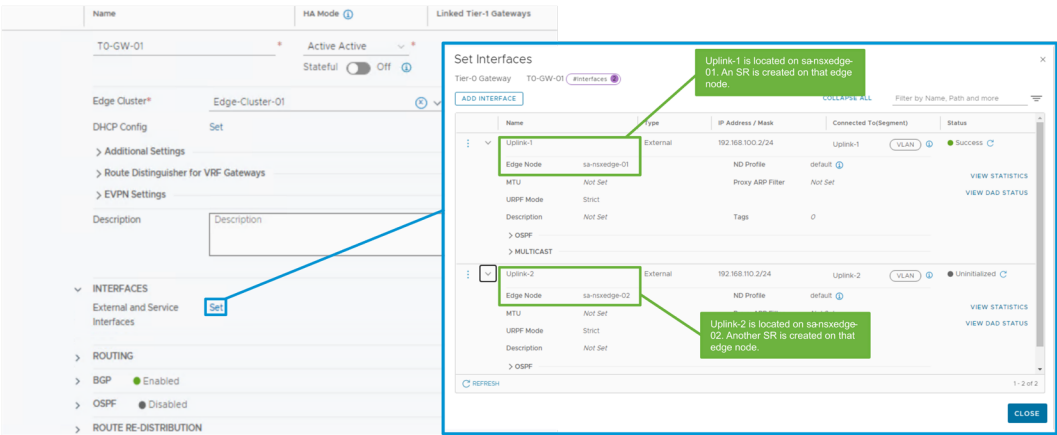
YES | NO

SAVE CANCEL

Enable stateful services for Active Active HA mode if you need the Tier-0 gateway to support services that need connection state tracking. Turn off stateful services if you want to run only stateless services.

# 5-59 Creating the Tier-0 Gateway (2)

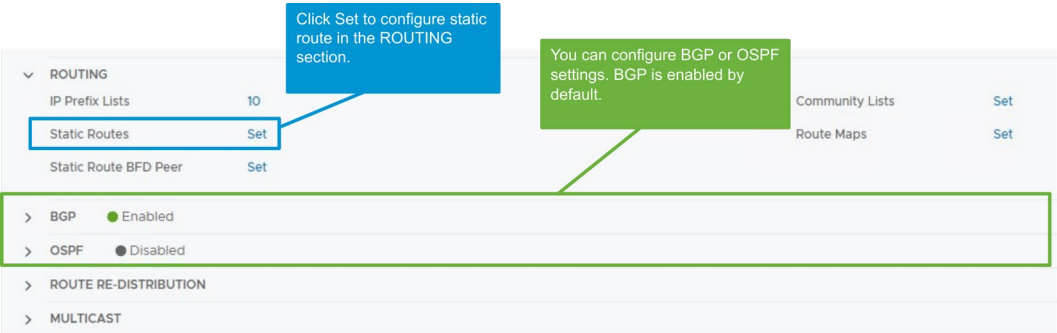
Configure the Tier-0 gateway interfaces to associate with the previously created uplink segments.



After Tier-0 is created, you can set up the interfaces.

# 5-60 Configuring Routing

Configure static or dynamic routing to the remote networks by editing the Tier-0 gateway.

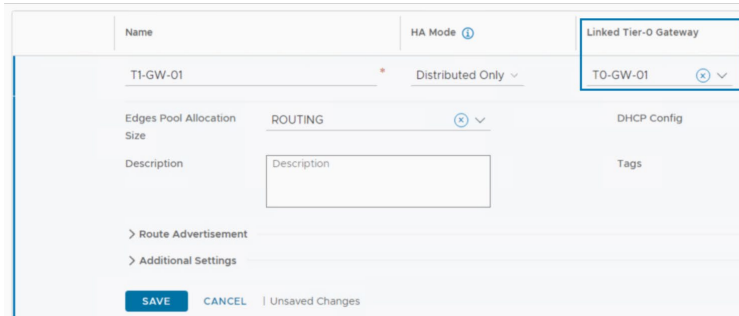


You can configure a static or dynamic route to remote networks. BGP is the dynamic routing protocol enabled by default.

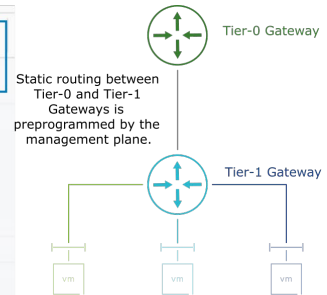
BGP and OSPF routing protocols can be active at the same time but for simplicity, you must disable BGP before enabling the OSPF dynamic routing protocol.

## 5-61 Connecting the Tier-1 and Tier-0 Gateways

Connect the Tier-1 gateway to the Tier-0 gateway by navigating to **Networking > Connectivity > Tier-1 Gateways** and editing the Tier-1 gateway.



The screenshot shows the configuration page for a Tier-1 Gateway named 'T1-GW-01'. The 'Linked Tier-0 Gateway' dropdown menu is highlighted with a blue box and shows 'T0-GW-01' as the selected option. Other visible settings include 'HA Mode' set to 'Distributed Only', 'Edges Pool Allocation Size' set to 'ROUTING', and a 'Description' text area. At the bottom, there are 'SAVE', 'CANCEL', and 'Unsaved Changes' buttons.

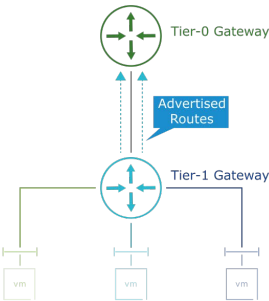


Edit the Tier-1 gateway to connect it to the desired Tier-0 gateway to provide north-south routing and access to external networks.

# 5-62 Enabling Route Advertisement in the Tier-1 Gateway

Enable route advertisement on the Tier-1 gateway for tenant networks to be propagated to the Tier-0 gateway.

Name	HA Mode ⓘ	Linked Tier-0 Gateway	#Linked Segments
T1-GW-01	Distributed Only ▾	TO-GW-01 ⓘ ▾	
Edges Pool Allocation Size	ROUTING ⓘ ▾	DHCP Config	Set
Description	<div>Description</div>	Tags	<div>Tag</div> <div>Max 30 allowed. Click</div>
▼ Route Advertisement			
All Static Routes	<input type="checkbox"/>	All NAT IP's	<input type="checkbox"/>
All DNS Forwarder Routes	<input type="checkbox"/>	All LB VIP Routes	<input type="checkbox"/>
All Connected Segments & Service Ports	<input checked="" type="checkbox"/>	All LB SNAT IP Routes	<input type="checkbox"/>
All IPsec Local Endpoints	<input checked="" type="checkbox"/>	Set Route Advertisement Rules	Set
> Additional Settings			
<div>SAVE</div> <div>CANCEL</div>   Unsaved Changes			

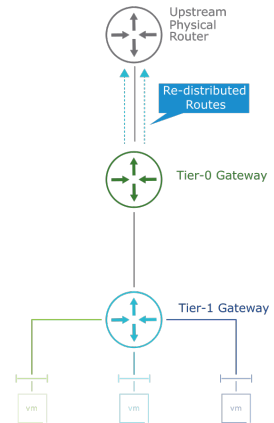
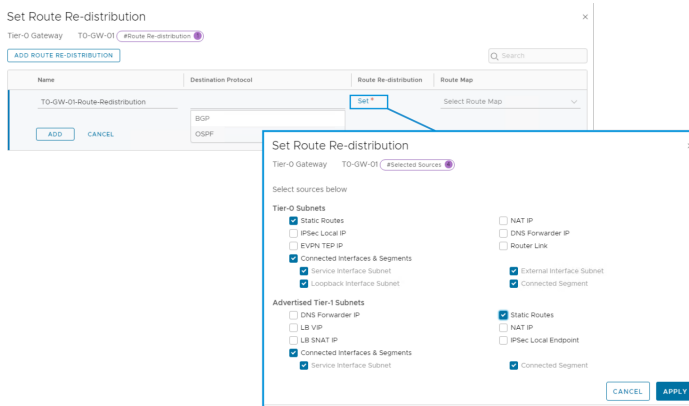


Using route advertisement ensures that the networks defined for tenant segments are available for the connected Tier-0 gateway, which can advertise them with the preferred dynamic routing protocol.



## 5-63 Configuring Route Redistribution on the Tier-0 Gateway

Configure route redistribution on the Tier-0 gateway to redistribute learned routes to the upstream routers.



Navigate to **Networking > Connectivity > Tier-0 Gateway** and edit the Tier-0 gateway to configure route redistribution.

BGP and OSPF are the supported destination protocols.

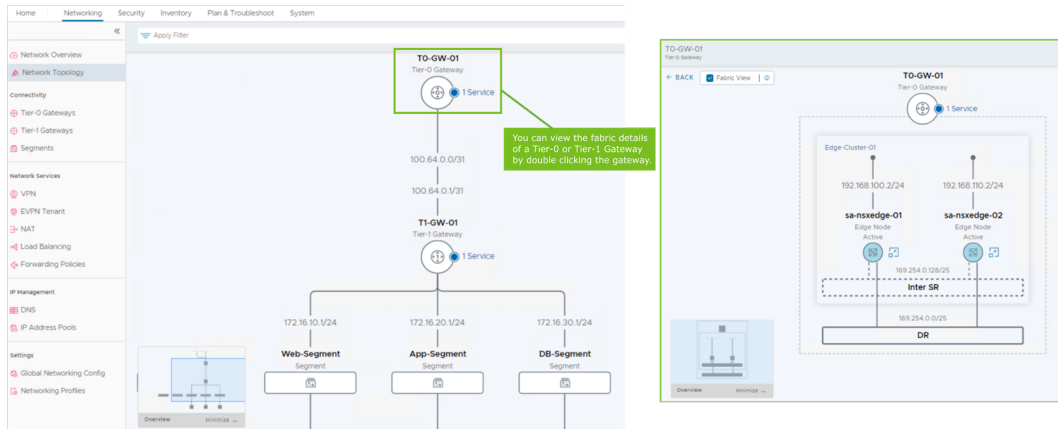
If only static routes are used in your environment, you do not have to configure route redistribution in Tier-0 gateways.

Redistribution into OSPF happens with the following considerations:

- Routes are redistributed as OSPF E2 route type (N2 in NSSA areas).
- Redistribution of OSPF E1 routes (N1 in NSSA areas) is not supported.
- The OSPF cost of the redistributed routes is always 20.

## 5-64 Using Network Topology to Validate the Tier-0 Gateway Configuration

Network Topology shows the Tier-0 gateway connected to the Tier-1 gateway and their network subnets.



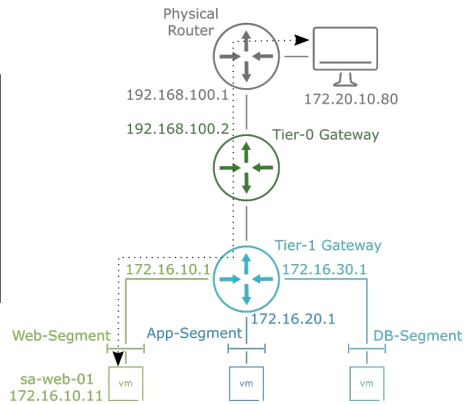
The topology diagram shows the IP addresses, such as uplink IPs, router link IPs, and interface IPs, between the NSX objects based on the magnification level.

If the magnification level is less than 1, then the entity names do not appear in the topology diagram.

## 5-65 Testing North-South Connectivity

VMs on the tenant networks can communicate with external workloads.

```
root@sa-web-01 [ ~ ]# ping 172.20.10.80
PING 172.20.10.80 (172.20.10.80) 56(84) bytes of data:
64 bytes from 172.20.10.80: icmp_seq=1 ttl=125 time=9.14 ms
64 bytes from 172.20.10.80: icmp_seq=2 ttl=125 time=2.87 ms
64 bytes from 172.20.10.80: icmp_seq=3 ttl=125 time=2.95 ms
64 bytes from 172.20.10.80: icmp_seq=4 ttl=125 time=2.90 ms
64 bytes from 172.20.10.80: icmp_seq=5 ttl=125 time=2.79 ms
^C
--- 172.20.10.80 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.787/4.130/9.142/2.506 ms
root@sa-web-01 [ ~ ]#
```



In the diagram and the command output, the sa-web-01 (172.16.10.11) VM can ping the Tier-0 gateway (192.168.100.2) and the upstream physical router (192.168.100.1), assuming that routing is configured on the physical router.

sa-web-01 can also ping a remote VM 172.20.10.80.

Complete north-south connectivity is now established.

## 5-66 Lab 7: Configuring the Tier-1 Gateway

Create and configure a Tier-1 gateway for east-west L3 connectivity:

1. Prepare for the Lab
2. Create a Tier-1 Gateway
3. Connect Segments to the Tier-1 Gateway
4. Use Network Topology to Validate the Tier-1 Gateway Configuration
5. Test East-West L3 Connectivity

## 5-67 Review of Learner Objectives

- Describe how to configure a Tier-1 gateway
- Explain how to configure a Tier-0 gateway
- Test end-to-end connectivity provided by Tier-0 and Tier-1 gateways

## 5-68 Lesson 4: Configuring Static and Dynamic Routing

### 5-69 Learner Objectives

- Distinguish between static and dynamic routing
- Configure static routes on the Tier-0 gateway
- Configure BGP on the Tier-0 gateway
- Configure OSPF on the Tier-0 gateway

## 5-70 Static and Dynamic Routing

Static routing:

- Static route configuration is a manual procedure performed by administrators.
- The configuration process enables fine-tuning of route selection.
- Route changes cannot be made dynamically.
- Limited scalability is because of administrative overhead.
- Failover planning is possible:
  - Network administrators must design and account for all network failure scenarios.
  - Route redundancy must be configured manually.

Dynamic routing:

- Dynamic route configuration enables gateways to exchange information about the network.
- Routing protocols are used to dynamically obtain routes to access the networks.
- Routers inform neighbor gateways when a network change occurs.

Dynamic routing protocol categories:

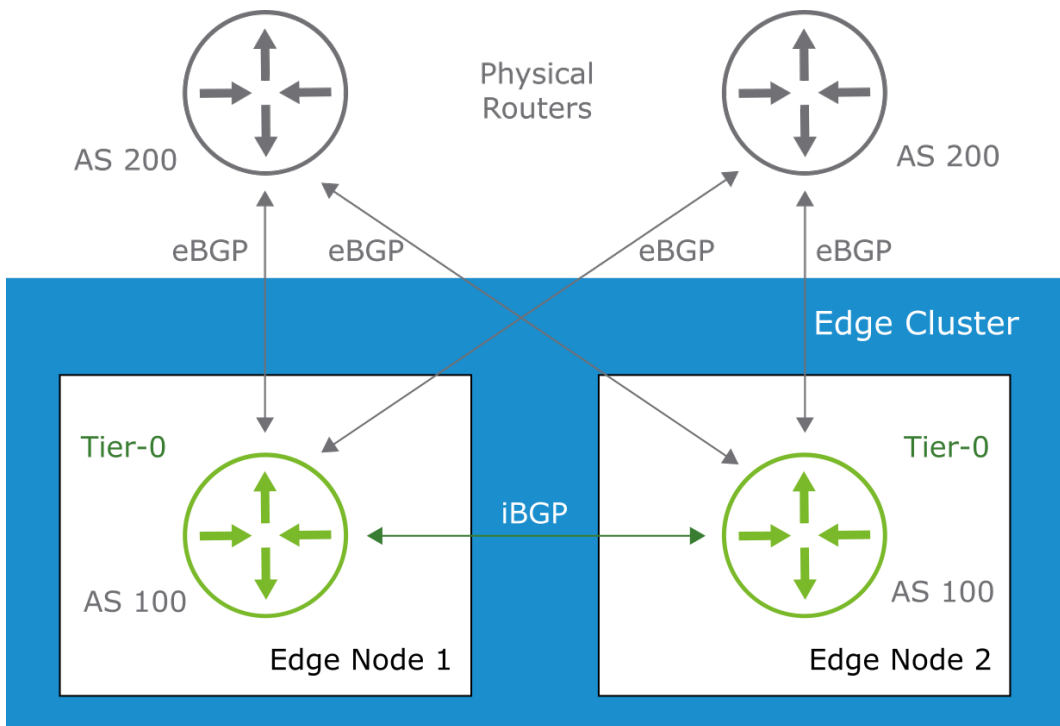
- Interior Gateway Protocols (IGPs): These protocols are used for routing in a single routing domain under the administration of a single organization. Some IGP routing protocols are RIP, EIGRP, OSPF, and IS-IS.
- Exterior Gateway Protocols (EGPs): These protocols are used to establish network connectivity between autonomous systems (AS) run by different organizations. BGP protocol is an example of an EGP.

NSX implements Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF).

## 5-71 Tier-0 Gateway Routing Configurations (1)

The Tier-0 gateway supports the following routing configurations:

- Static routing toward upstream physical gateways
- Dynamic routing using Border Gateway Protocol (BGP):
  - External BGP (eBGP) sessions with peers in a different autonomous system (AS)
  - Internal BGP (iBGP) sessions with peers in the same AS



In the diagram, external BGP (eBGP) is used to establish neighbor relationships between Tier-0 and upstream physical gateways with different AS network prefixes that are exchanged between the Border Gateway Protocol (BGP) peers.

The BGP dynamic neighbor enables peering to a group of remote neighbors.

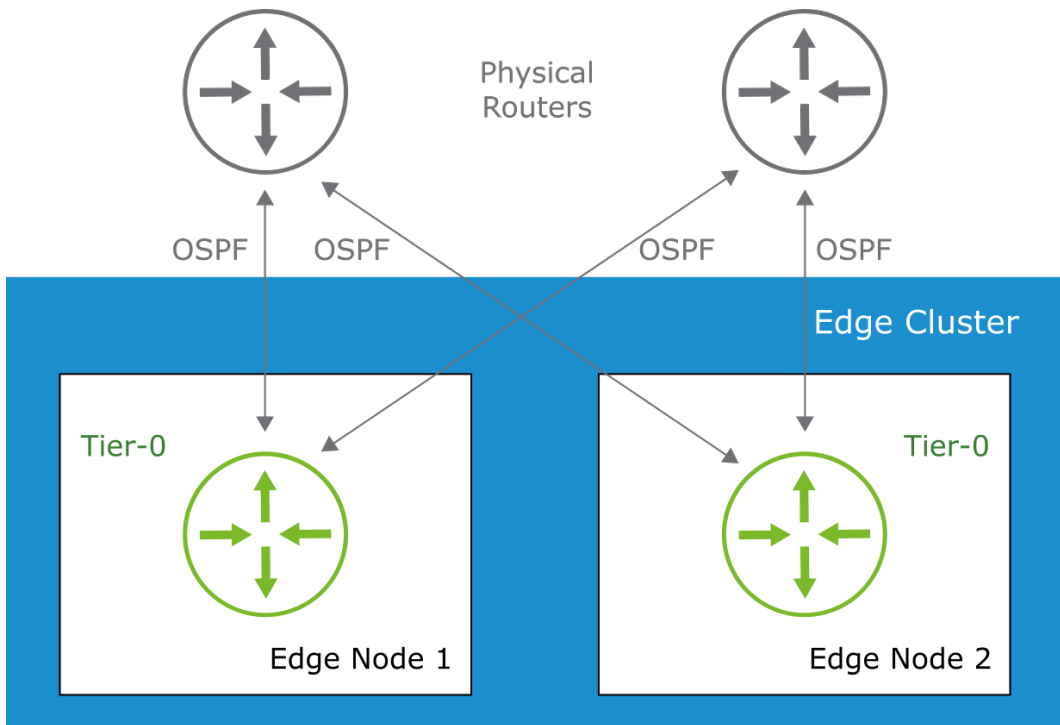
BGP supports 4-byte autonomous system number (ASN).

The Tier-0 gateway BGP topology should be configured with redundancy and symmetry between the Tier-0 gateways and the external peers.

## 5-72 Tier-0 Gateway Routing Configurations (2)

Tier-0 gateways also support dynamic routing configurations using Open Shortest Path First (OSPF):

- OSPF over point-to-point networks
- OSPF over broadcast networks



Open Shortest Path First (OSPF) is available since NSX-T Data Center 3.1.1.

In the diagram, OSPF establishes adjacencies between Tier-0 and upstream physical gateways.

OSPF adjacencies have the following characteristics:

- OSPF is a link state routing protocol, and OSPF establishes and maintains neighbor relationships for exchanging routing updates with other routers.
- Two OSPF routers are neighbors if they are members of the same subnet and share the same area ID, subnet mask, timers, and authentication.
- Setting a password is optional. Authentication methods can be MD5 hashing or clear text.



These adjacencies can be established over broadcast networks or point-to-point networks.

Broadcast and point-to-point networks are defined as follows:

- Broadcast networks support multiple routers connected to the same network. A single broadcast packet can reach all the attached routers. The Ethernet protocol is an example of a broadcast network.
- Point-to-point networks are networks that only join a single pair of routers. They are typically seen on WAN links.

## 5-73 Configuring Static Routes on a Tier-0 Gateway (1)

You can configure static routes in the ROUTING section of the Tier-0 gateway.

The screenshot shows the 'Tier-0 Gateways' configuration page in a network management interface. The left sidebar contains a navigation menu with sections: Connectivity (Network Overview, Network Topology, Tier-0 Gateways, Tier-1 Gateways, Segments), Network Services (VPN, EVPN Tenant, NAT, Load Balancing, Forwarding Policies), and IP Management (DNS, IP Address Pools). The main panel is titled 'Tier-0 Gateways' and shows a configuration for 'TO-GW-01'. It includes fields for Name, HA Mode (Active/Active), Stateful (On/Off), Edge Cluster (Edge-Cluster-01), DHCP Config (Set), and a Description field. Under the 'INTERFACES' section, the 'ROUTING' tab is selected, showing 'IP Prefix Lists' (TO), 'Static Routes' (Set), and 'Static Route BFD Peer' (Set). Callouts point to these settings: 'Click Set to Configure Static Routes.' points to 'Static Routes', and 'Click Set to Configure Peers That Support BFD Protocol.' points to 'Static Route BFD Peer'. To the right of the screenshot is a network diagram. It shows a 'Physical Router' at the top, connected to a 'Tier-0' gateway below it, which is then connected to a 'Tier-1' gateway at the bottom. The Physical Router has two uplinks: 'Uplink 1' (192.168.100.1) and 'Uplink 2' (192.168.110.1). The Tier-0 gateway has two interfaces: '192.168.100.2' and '192.168.110.2'. A cloud icon labeled '200.1.1.0/24' is connected to the Physical Router.

## 5-74 Configuring Static Routes on a Tier-0 Gateway (2)

You can add one or multiple static routes and configure the next hops.

Set Static Routes

Tier-0 Gateway TO-GW-01 #Static Routes 0

ADD STATIC ROUTE

Filter by Name, Path and more

Name	Network	Next Hops	Status
to-200-net	200.1.1.0/24 <small>e.g. IPv4 10.10.0.0/23 or IPv6 2001:db8:1234::/48</small>	<div>Set</div>	

SAVE

CANCEL

Set Next Hops

Tier-0 Gateway TO-GW-01 | Static Route to-200-net #Next Hops 0

SET NEXT HOPS

Q Search

IP Address	Admin Distance	Scope
192.168.100.1 <small>Leave it blank to set as 'NULL' or enter IPv4/IPv6 Address</small>	1 <small>Between (1 - 255)</small>	<div>Uplink-1 X</div> <div>Uplink-2</div> <div>Tier-0 Interface</div>

ADD

CANCEL

Select the Uplink to Access the Next Hop.

Physical Router

200.1.1.0/24

192.168.100.1 192.168.110.1

Uplink 1 192.168.100.2 Uplink 2 192.168.110.2

Tier-0

Tier-1

## 5-75 Configuring Dynamic Routing with BGP on Tier-0 Gateways (1)

To configure dynamic routing, you can configure BGP in the BGP section of the Tier-0 gateway.

The screenshot displays the 'Tier-0 Gateways' configuration interface. A blue box highlights the 'ROUTING' section, specifically the 'BGP' configuration area. Within this area, a green box highlights the 'BGP' toggle (set to 'On') and the 'Local AS\*' field (set to '100'). A green callout bubble points to the 'BGP' toggle with the text 'Turn on the BGP toggle and enter the Local AS.' Another green callout bubble points to the 'BGP Neighbors' link with the text 'You can configure the BGP neighbors by clicking Set.' The 'BGP Neighbors' link is also highlighted with a green box. Other visible settings include 'Inter SR iBGP' (On), 'ECMP' (On), 'Multipath Relax' (On), 'Graceful Restart' (Helper Only), 'Graceful Restart Stale Timer' (600), and 'Route Aggregation' (Set). The interface includes a 'SAVE' button and a 'CANCEL' button, along with a note 'Unsaved Changes'.

BGP is enabled by default on Tier-0 gateways. You must set the local AS and configure the BGP neighbors.

You can also configure the following advanced BGP settings:

- Inter-SR routing so Service Routers (SRs) components exchange routing information through iBGP in the same Tier-0 gateway.
- Multipath Relax to enable ECMP across different neighboring ASNs if all other BGP attributes are equal.
- Route advertisement filtering using:
  - IP prefix lists to define the networks with subnet masks that are permitted or denied based on a match condition.
  - Community lists to specify the BGP communities allowed. A community is a BGP attribute that can be used to tag a specific set of routes that share common properties.
  - Route maps include a sequence of IP prefix lists or community lists with an associated action to filter or modify the routes advertised. When a match occurs, the gateway performs the action and stops scanning the rest of the route map.

## 5-76 Configuring Dynamic Routing with BGP on Tier-0 Gateways (2)

You can configure BGP neighbors by adding their AS number, IP addresses, and source addresses.

Set BGP Neighbors

Tier-0 Gateway BGP-TO-GW-... (#Neighbors 0)

ADD BGP NEIGHBOR

Enter the IP Address of the Neighbor.

Enter the Remote AS Number.

COLLAPSE ALL Filter by Name, Path and more

IP Address	BFD	Remote AS number	Route Filter	Allowas-in	Status
192.168.100.1	Disabled	200 E.g. 65000	Set	Disabled	
Source Addresses		Graceful Restart		Helper Only	
192.168.100.2					
Max Hop Limit		Description			
1 Range 1 to 255					
> TIMERS & PASSWORD					
SAVE CANCEL					

Select the Source Address Used to Establish the BGP Session with the Neighbor

You can also configure the following advanced BGP settings:

- Bidirectional Forwarding Detection (BFD) is an end-to-end protocol that can detect forwarding path failures.
- Enable Allowas-in to prevent BGP process from dropping the routes received that contain the same AS as the one defined in the Tier-0 gateway. Do not enable unless required because the default BGP configuration designed to avoid loops might break.
- Graceful Restart can eliminate or reduce the disruption of traffic associated with routes learned from a BGP neighbor when a control plane failover occurs. The default mode is Helper Only.

# 5-77 Verifying the BGP Configuration of the Tier-0 Gateways

You verify the BGP Connectivity Status for each neighbor.

Set BGP Neighbors

Tier-0 GatewayBGP-T0-GW-...#Neighbors

ADD BGP NEIGHBOREXPAND ALLFilter by Name, Path and more

	IP Address	BFD	Remote AS number	Route Filter	Allows-in	Status
>	192.168.110.1	Disabled	200	1	Disabled	Success
>	192.168.100.1	Disabled	200	1	Disabled	Success

Select the Edge Node.

Verify the Connection Status and the Source Address Used.

Review the Prefixes Exchanged in the BGP Session.

BGP Connectivity Status | 192.168.100.1

Edge Node sa-nxedge-02

Connection Status	Established
Source Address	192.168.100.2
Local Port	41645
Remote Port	179
Messages Received	17
Messages Sent	16
Time since established	678 seconds
Total In Prefix Count	7
Total Out Prefix Count	5
Connection Drop Count	0
Established Connection Count	1

addPath IPv4 Unicast Rx, IPv4

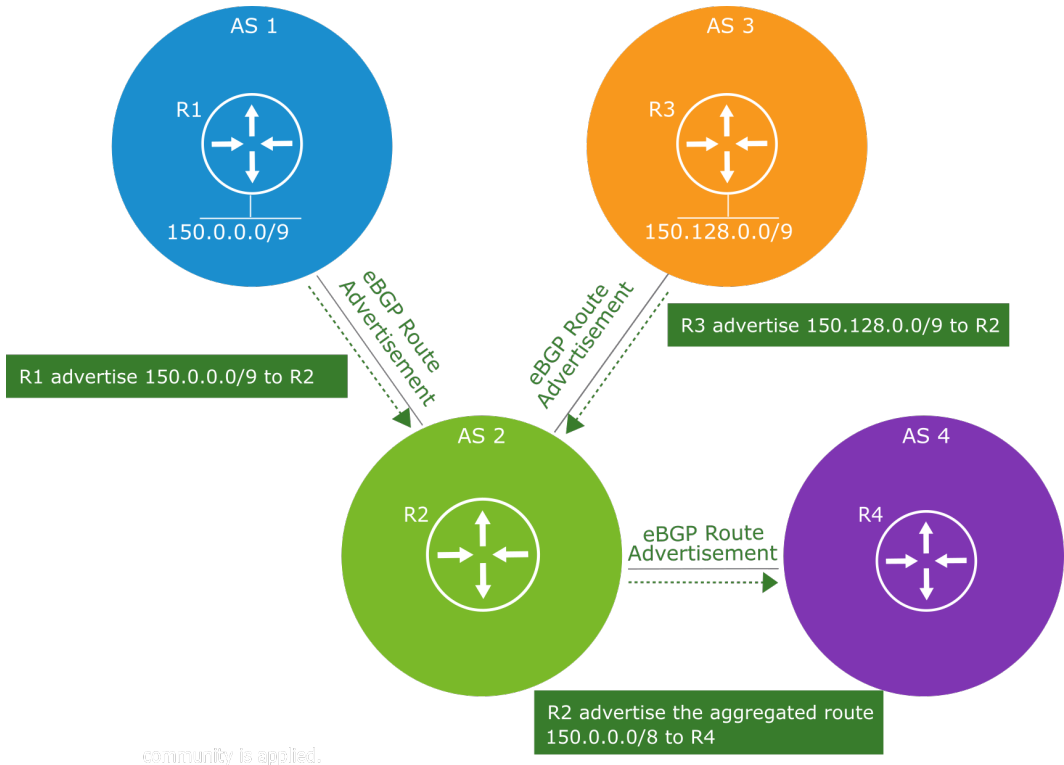
CLOSE

You can also use the `get bgp neighbor summary nsxcli` command to verify that the BGP neighbor state is established.

## 5-78 BGP Route Aggregation

Route aggregation is a BGP feature that allows the aggregation of specific routes into one route:

- Reduces the size of the routing tables
- Reduces the number of advertised routes
- Accelerates the best path calculation



The aggregated routes can be received from different AS.

## 5-79 Configuring Route Aggregation with BGP

Route aggregation can be configured in the BGP section of the Tier-0 gateway.

The screenshot displays the 'Tier-0 Gateways' configuration page. On the left, the 'ROUTING' section is expanded, showing 'BGP' is enabled. The 'Route Aggregation' option is highlighted with a blue box and a 'Set' button. A blue arrow points from this 'Set' button to the 'Set Route Aggregation' dialog box on the right.

The 'Set Route Aggregation' dialog box contains the following fields and options:

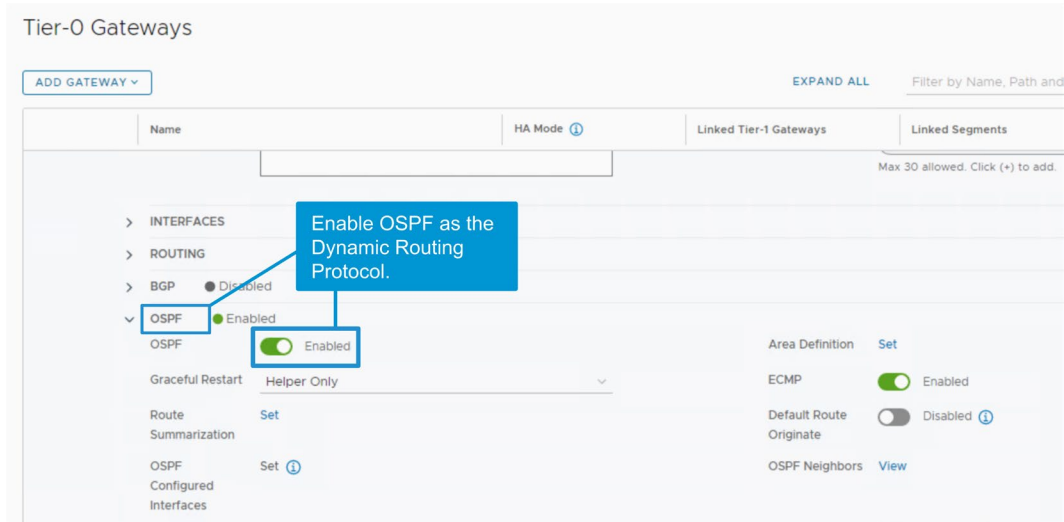
- Tier-0 Gateway:** BGP-T0-GW-...
- #Route Aggregation:** 1
- ADD PREFIX:** A button to add a new prefix.
- Prefix:** A text field containing '150.0.0.0/8' and a hint 'CIDR e.g. 10.22.0.0/22'.
- Summary - Only:** A dropdown menu set to 'Yes'.
- Buttons:** 'ADD' and 'CANCEL' buttons are located below the Prefix field.
- Footer:** 'CANCEL' and 'APPLY' buttons.

Two green callout boxes provide instructions:

- One points to the Prefix field with the text: 'Add the Prefix you want to Advertise.'
- Another points to the Summary - Only dropdown with the text: 'Set Summary-Only to Yes to Advertise only the Summarized Prefix.'

## 5-80 Configuring Dynamic Routing with OSPF on Tier-0 Gateways (1)

OSPF is not enabled by default in the Tier-0 gateway configuration. It must be enabled before setting any parameter.



The OSPF protocol is not enabled by default when creating a Tier-0 gateway.

Turn on the **OSPF** toggle to enable OSPF.

OSPF Router-ID cannot be manually configured in the UI. It is automatically populated.

Enable OSPF Graceful Restart to keep sending traffic if a control plane failover occurs in a ToR router.



## 5-81 Configuring Dynamic Routing with OSPF on Tier-0 Gateways (2)

You configure the area for the Tier-0 gateway.

Set Area Definition

Tier-0 Gateway OSPF-T0-G... #Area Definitions

ADD AREA DEFINITION

Only one Area Definition can be configured.

Search

Area ID	Type	Authentication	Key ID	Password	Status
0	Normal	MD5	1	*****	

Description

Area Type can be Normal or NSSA.

Authentication can be none, MD5, or using a plain text password.

Tag Scope

Max 30 allowed. Click (+) to add.

SAVE CANCEL

An OSPF network is divided into areas that are the logical groupings of hosts and networks:

- OSPF routers in an area have the same detailed topology for only their own area.
- An area border router (ABR) is the OSPF boundary between two areas.
- In a single-area OSPF, any area can be used. Area 0 is not required.
- The Tier-0 gateways do not have ABR functionality currently.
- All inter-area traffic traverses area 0, preventing routing loops.

NSX supports the following OSPF area types:

- Standard Area: Nonbackbone area that must be connected to a backbone area using an Area Border Router (ABR).
- Backbone Area: Must be designed while considering redundancy and cannot be partitioned. This area has knowledge of the entire topology. Inter-area traffic must flow through this area.
- Not-so-Stubby Area (NSSA): Blocks external routes from other areas (inter-area) but can import external routes type-2 from other AS.

Stub Areas, Totally Stubby Areas, and Virtual links to connect areas to the Backbone Area through nonbackbone areas are not supported in NSX.

Follow these criteria when configuring the areas in Tier-0 gateways:

- Area Definition supports only one area per Tier-0 gateway.
- Area ID must be either a single number (0) or use dotted format (0.0.0.0).
- Area type can be Normal (Standard or Backbone) or NSSA.
- Authentication is optional and can be configured using MD5 (hashing) or Password (plain text).

## 5-82 Configuring Dynamic Routing with OSPF on Tier-0 Gateways (3)

Configure the Tier-0 gateway interfaces that will form OSPF adjacencies.

Set OSPF Configured Interfaces

Tier-0 Gateway OSPF-TO-G... #OSPF Configured Interfaces

CONFIGURE INTERFACE COLLAPSE ALL Search

Interface	Area ID	Network Type	OSPF	Status
OSPF-Uplink-2	0	Broadcast	Enabled	Success
BFD Enabled				
OSPF Hello Interval (Seconds) 10				
BFD Profile default				
OSPF Dead Interval (Seconds) 40				
OSPF-Uplink-1		Broadcast	Enabled	Success
BFD Enabled				
OSPF Hello Interval (Seconds) 10				
BFD Profile default				
OSPF Dead Interval (Seconds) 40				

Select the area ID. If it is an interface connected to the Backbone area, the ID must be 0.

Select Broadcast or P2P (Point-to-Point) Network Type.

You must follow these criteria when configuring OSPF in the interfaces:

- You can configure a maximum of two uplink interfaces in OSPF per edge node.
- The two interfaces on the NSX Edge node must be in the same area.
- You can configure BFD on the OSPF-enabled interfaces.
- The BFD Hello interval supports a minimum value of 500 milliseconds for an interface configured in an edge VM and 50 milliseconds for an interface configured on bare-metal edges. Dead interval minimum values are 1,500 milliseconds for edge VM and 150 milliseconds for bare-metal edges.

## 5-83 Verifying OSPF Configuration of the Tier-0 Gateways

You verify the OSPF Neighbors State.

OSPF Neighbors

Tier-0 Gateway OSPF-TO-G... #Neighbors

Last Updated On: Oct 10, 2022, 7:53:28 AM

EXPAND ALL Search by Neighbor IP and Edge Node

	Neighbor IP Address	Interface	Source	Edge Node	Priority	State
✓	192.168.210.1	uplink-361.192.168.200.2	192.168.200.1	sa-nxsedge-01	1	Full
	Uptime	1.622s Seconds		Dead Time	38.336s Seconds	
	Retransmit Request Counter	1		Request Counter	0	
	Database Summary Counter	0				
>	192.168.210.2		192.168.210.1	sa-nxsedge-01		Full

Check the Uptime and Dead Time Timers.

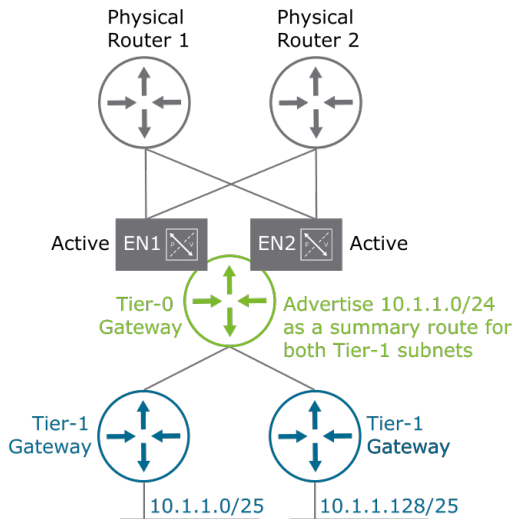
Verify the Neighbor State is Full.

You can also use the `get ospf neighbor nsxcli` command to verify that the OSPF adjacencies are established.

## 5-84 OSPF Route Summarization

You must use route summarization in large-scale environments for the following reasons:

- Reduce the Link State Advertisement (LSA) flooding
- Preserve CPU and memory resources
- Ease troubleshooting



Link State Advertisements (LSAs) are the messaging system used in OSPF routing protocol:

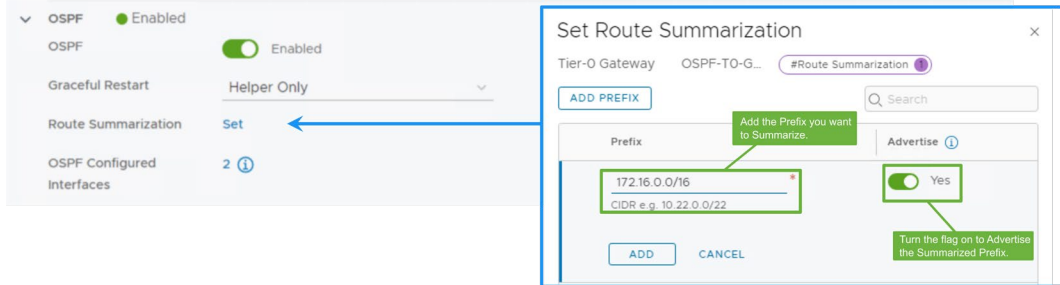
- LSAs are exchanged between routers.
- LSAs contain information regarding OSPF links and their status.
- Different types of LSA exist depending on the type of information exchanged.
- LSAs are stored in a local Link State Database (LSDB) in each OSPF router.

The diagram displays:

- Network 10.1.1.0/24 can be advertised as a summary route for both /25 Tier-1 gateway segments.
- The LSA for the summary route is advertised as a type 5 LSA. These LSA types are used to inform about redistributed routes from other routing protocols including static routes. The summarized route is advertised as an OSPF external route of type-2 (N E2).

## 5-85 Configuring Route Summarization with OSPF

Set Route Summarization in the OSPF section to define the summarized networks.



## 5-86 Lab 8: Creating and Configuring a Tier-0 Gateway with OSPF

Create a Tier-0 gateway and use OSPF to configure the north-south end-to-end connectivity:

1. Prepare for the Lab
2. Create an Uplink Segment
3. Create a Tier-0 Gateway
4. Connect the Tier-0 and Tier-1 Gateways
5. Use Network Topology to Validate the Tier-0 Gateway Configuration
6. Test the End-to-End Connectivity

## 5-87 Lab 9: Configuring the Tier-0 Gateway with BGP

Create a Tier-0 gateway and use BGP to configure the north-south end-to-end connectivity:

1. Prepare for the Lab
2. Create an Uplink Segment
3. Create a Tier-0 Gateway
4. Connect the Tier-0 and Tier-1 Gateways
5. Use Network Topology to Validate the Tier-0 Gateway Configuration
6. Test the End-to-End Connectivity

## 5-88 Review of Learner Objectives

- Distinguish between static and dynamic routing
- Configure static routes on the Tier-0 gateway
- Configure BGP on the Tier-0 gateway
- Configure OSPF on the Tier-0 gateway

## 5-89 Lesson 5: ECMP and High Availability

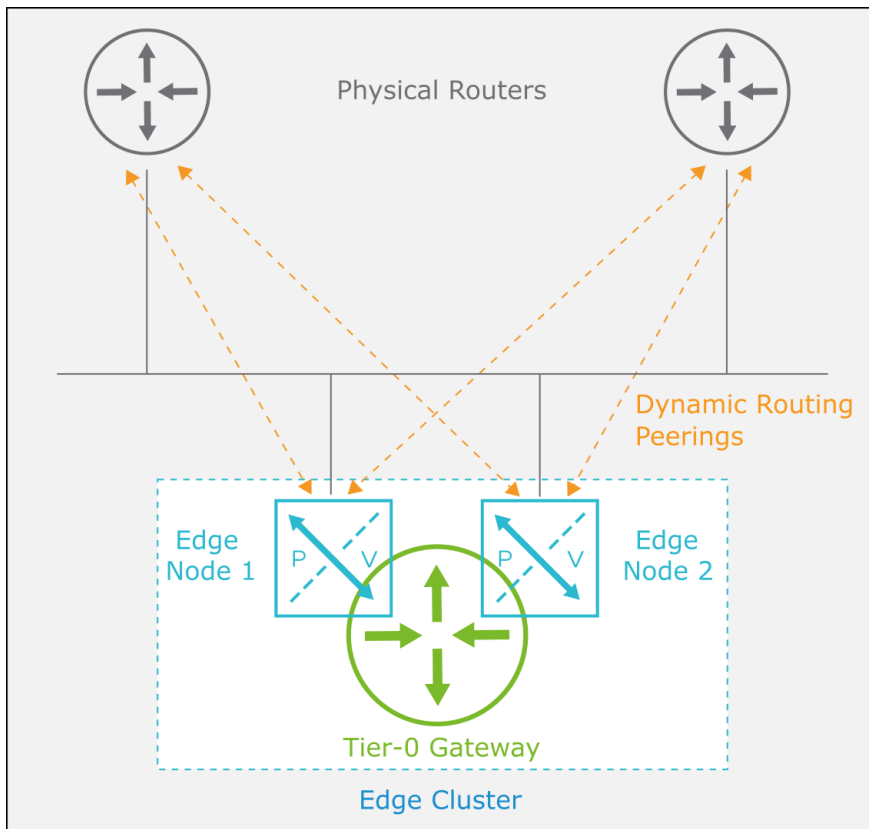
### 5-90 Learner Objectives

- Explain the purpose of ECMP routing
- Use the NSX UI to configure ECMP routing
- Identify the active-active and active-standby modes for high availability
- Recognize failure conditions and explain the failover process

## 5-91 About Equal-Cost Multipath Routing

Equal-cost multipath (ECMP) routing has several features and functions:

- ECMP routing increases the north-south communication bandwidth by combining multiple uplinks.
- ECMP routing performs traffic load balancing.
- ECMP routing provides fault tolerance for failed paths.
- A maximum of eight ECMP paths are supported.
- ECMP hashing is based on a 5-tuple algorithm.
- ECMP routing is available for Tier-0 gateway uplinks.

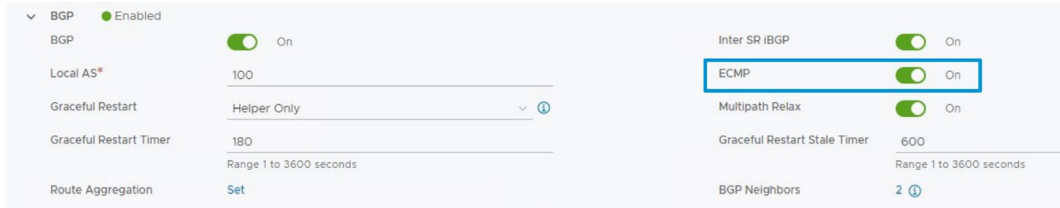


ECMP hashing is based on a 5-tuple algorithm that uses source IP address, destination IP address, source port, destination port, and IP protocol. This method allows a better distribution of the traffic across all the available paths.



## 5-92 Enabling ECMP in BGP

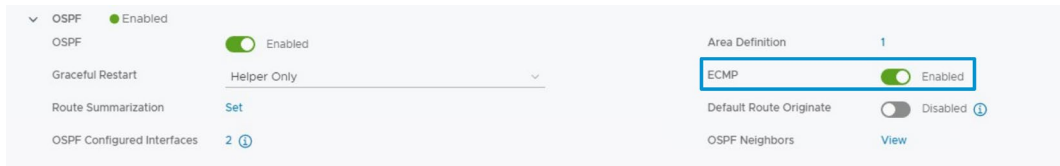
ECMP is enabled by default on Tier-0 gateways when Border Gateway Protocol (BGP) is enabled. ECMP can be disabled in the BGP section on the Tier-0 Gateway configuration page.



The screenshot shows the BGP configuration page. On the left, under the 'BGP' section, the 'BGP' toggle is 'On', 'Local AS\*' is '100', 'Graceful Restart' is 'Helper Only', 'Graceful Restart Timer' is '180', and 'Route Aggregation' is 'Set'. On the right, under the 'Inter SR iBGP' section, the 'ECMP' toggle is 'On' and is highlighted with a blue box. Other settings include 'Multipath Relax' (On), 'Graceful Restart Stale Timer' (600), and 'BGP Neighbors' (2).

## 5-93 Enabling ECMP in OSPF

ECMP is enabled by default on Tier-0 gateways when Open Shortest Path Protocol (OSPF) is enabled. ECMP can be disabled in the OSPF section on the Tier-0 Gateway configuration page.



The screenshot shows the OSPF configuration page. On the left, under the 'OSPF' section, the 'OSPF' toggle is 'Enabled', 'Graceful Restart' is 'Helper Only', 'Route Summarization' is 'Set', and 'OSPF Configured Interfaces' is '2'. On the right, under the 'Area Definition' section, the 'ECMP' toggle is 'Enabled' and is highlighted with a blue box. Other settings include 'Default Route Originate' (Disabled) and 'OSPF Neighbors' (View).

When configuring ECMP in OSPF, a maximum of two uplink interfaces can be enabled per edge node.

## 5-94 About High Availability

You can configure high availability on the gateways for redundancy.

High availability can be configured in the following modes:

- Active-active:
  - All the edge nodes are active and run the gateway services simultaneously.
  - The workload is distributed between all nodes to prevent overloading one single node.
- Active-standby:
  - One edge node is active, and one edge node remains on standby.
  - The standby node takes over when the active node becomes unavailable.

Grouping edge nodes offers the benefits of high availability for edge node services. The service router runs on an edge node and has two modes of operation: active-active or active-standby.

The active-active mode is offered on NSX Edge and has the following characteristics:

- Logical routing is active on more than one NSX Edge node at a time.
- Active-active mode is stateless by default. In stateless mode, no tracking tables are kept with the state of connections and services.
- From NSX 4.0.1, when creating a Tier-0 or a Tier-1 the high availability mode can be configured to stateful active-active if you are planning to host stateful services like NAT.

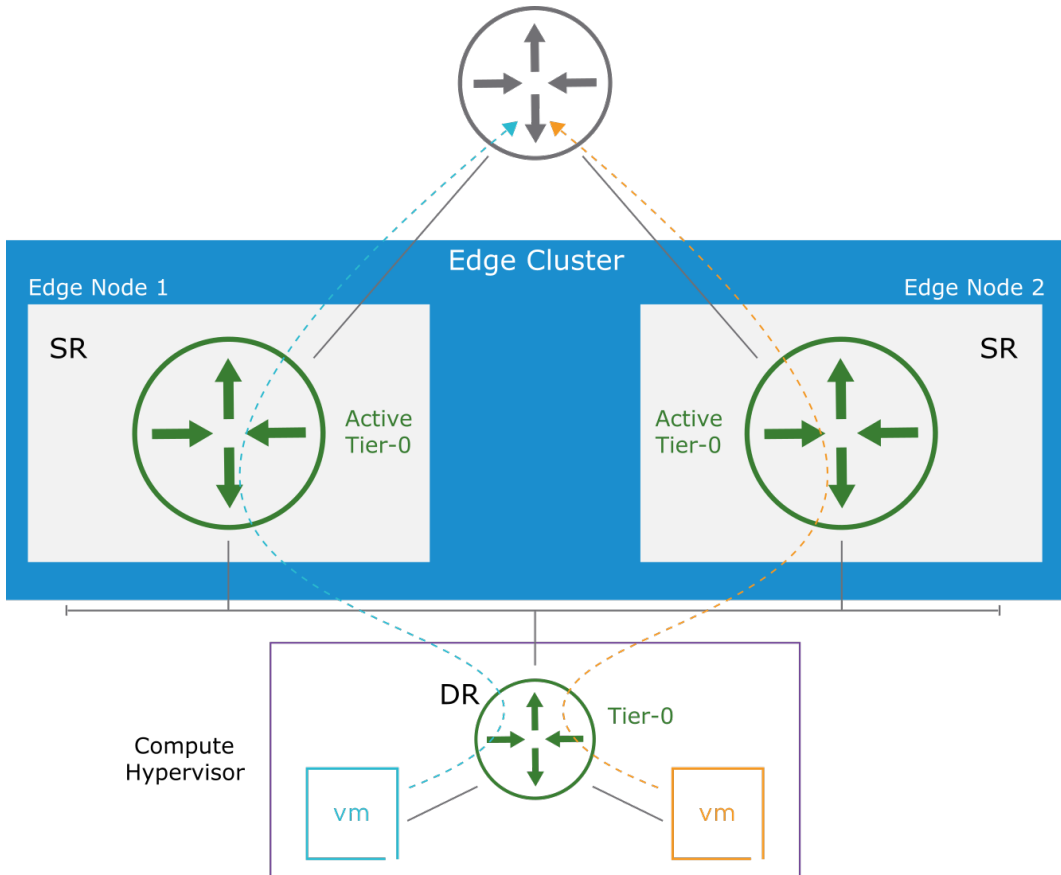
The active-standby mode is also offered on NSX Edge and has the following characteristics:

- Logical routing is active on only one NSX Edge node at a time.
- The standby node takes over if the active member has a failure.
- Active-standby mode can be configured on both Tier-0 and Tier-1 gateways.

## 5-95 Active-Active HA Mode

The active-active mode is the default high availability mode for Tier-0 gateways and provides:

- ECMP to load balance traffic across the different edge nodes.
- Logical routing services are active on more than one edge node at a time.
- NSX version 4.0.1 adds support for stateful services such as NAT in active-active HA mode.



Active-active is a high availability mode where a gateway is hosted on more than one edge node at a time:

- In the active-active mode, traffic is load-balanced across all members.
- For northbound traffic, the DR component sends traffic across the different active SR components.

- When one node fails, traffic is not disrupted but bandwidth is constrained.
- A gateway can span up to eight edge nodes to provide load balancing and redundancy.

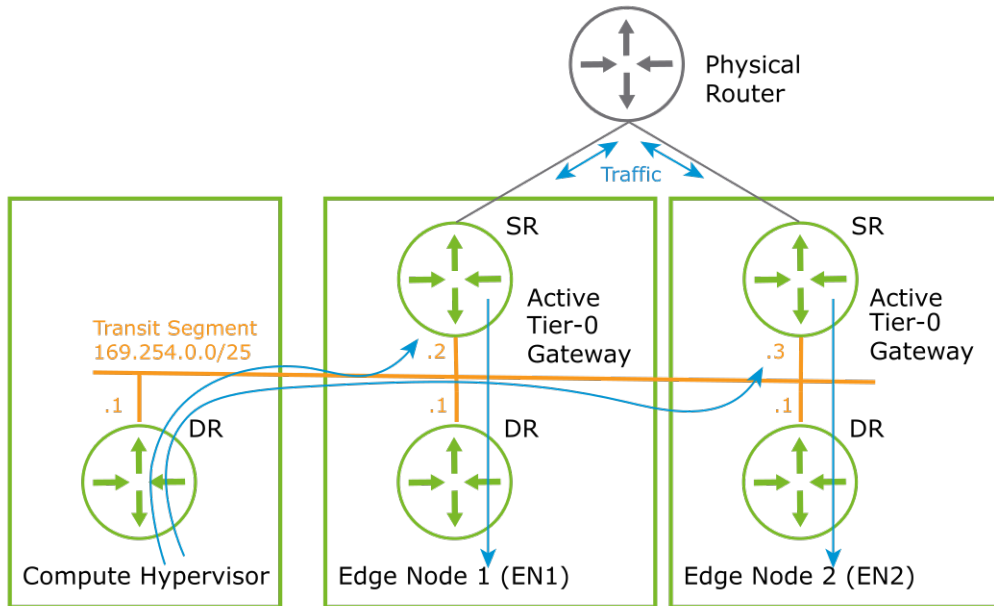
Active-active mode is stateless by default. So, services such as NAT and stateful firewall cannot be configured. Only routing and stateless services, such as reflexive NAT, are enabled.

NSX version 4.0.1 supports stateful services such as NAT in stateful active-active mode by pinning specific flows to an individual NSX Edge node.

## 5-96 Active-Active Topology with BGP

Active-active HA mode topologies with BGP have the following characteristics:

- BGP peering with physical routers is established in all SRs.
- The DRs load balance traffic across all SRs.



In the active-active mode, all the SRs process the northbound and southbound traffic.

Traffic flow considerations:

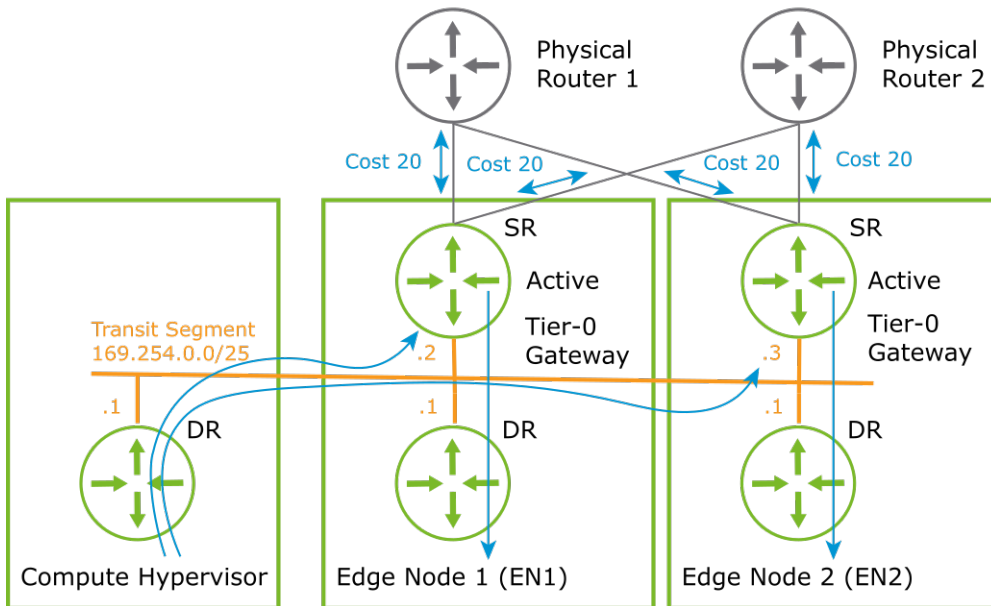
- In the diagram, DR sends traffic to both active SRs with IPs 169.254.0.2 and 169.254.0.3 in the Transit Segment.
- Routing decision is not influenced on BGP peers.

## 5-97 Active-Active Topology with OSPF

Active-active HA mode topologies with OSPF have the following characteristics:

- OSPF adjacencies with physical routers are established in all SRs using the same cost.
- The DRs load balance traffic across all SRs.

### Physical Topology



For the Tier-0 gateway in an active-active configuration with OSPF:

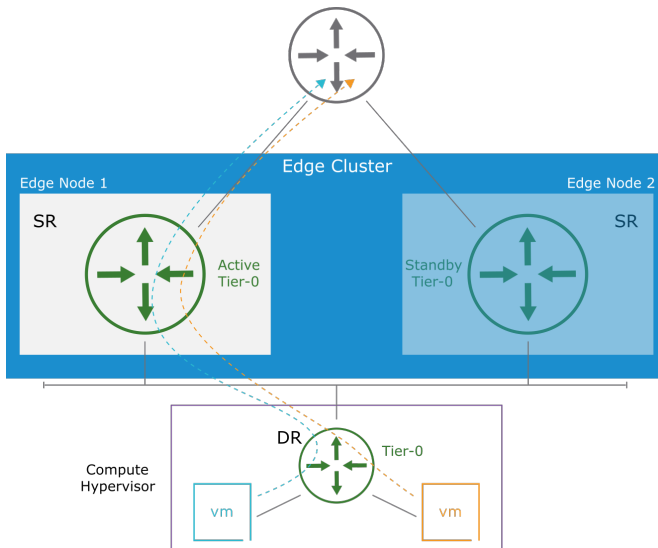
- ECMP can be leveraged with the physical routers but a maximum of two uplink interfaces can be enabled for OSPF per edge node.
- An OSPF cost of 20 is announced by all Tier-0 gateways, influencing the routing decision on physical routers with equal cost paths.

## 5-98 Active-Standby HA Mode

Active-standby is a high availability mode where a gateway is operational on only a single edge node at a time.

The following centralized stateful services are provided in the active-standby mode:

- Stateful Gateway Firewall
- VPN



Active-standby is a high availability mode where a gateway is operational on only a single edge node at a time.

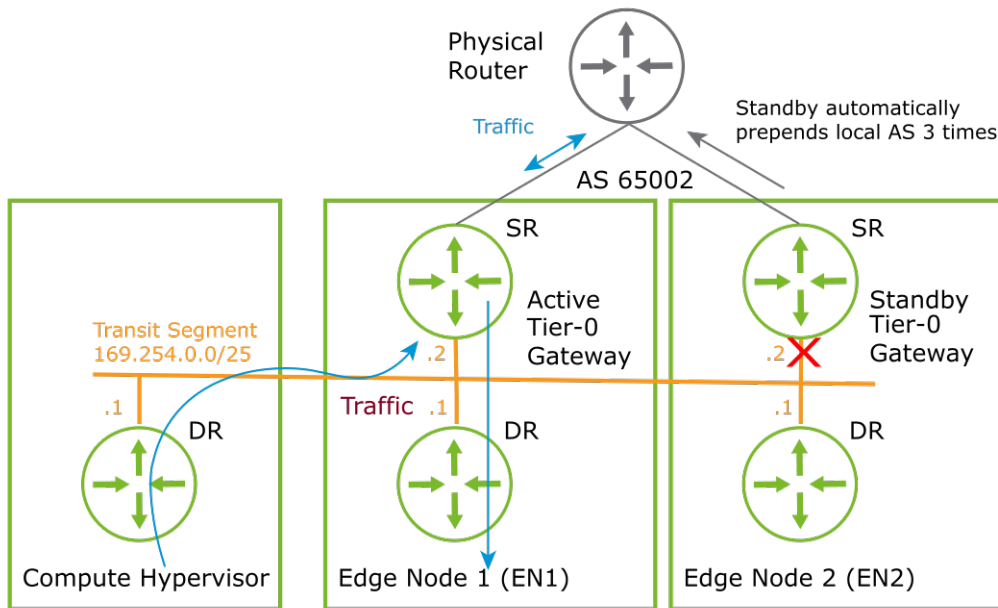
In the active-standby mode, an elected active member processes all traffic. If the active member fails, a new member is elected to be active:

- Tier-0:
  - The active-standby SRs have different northbound IP addresses and have dynamic routing sessions established on both links.
  - Gateway state is synchronized but does not actively forward traffic. Both SRs maintain dynamic routing peering with the physical gateway.
- Tier-1:
  - The active-standby SRs have the same northbound IP addresses.

## 5-99 Active-Standby Topology with BGP

Active-standby HA mode topologies with BGP have the following characteristics:

- BGP peering is still established on both SRs.
- The standby SR performs AS path prepending and does not forward traffic to the physical routers.
- The DR sends traffic to the active SR only.



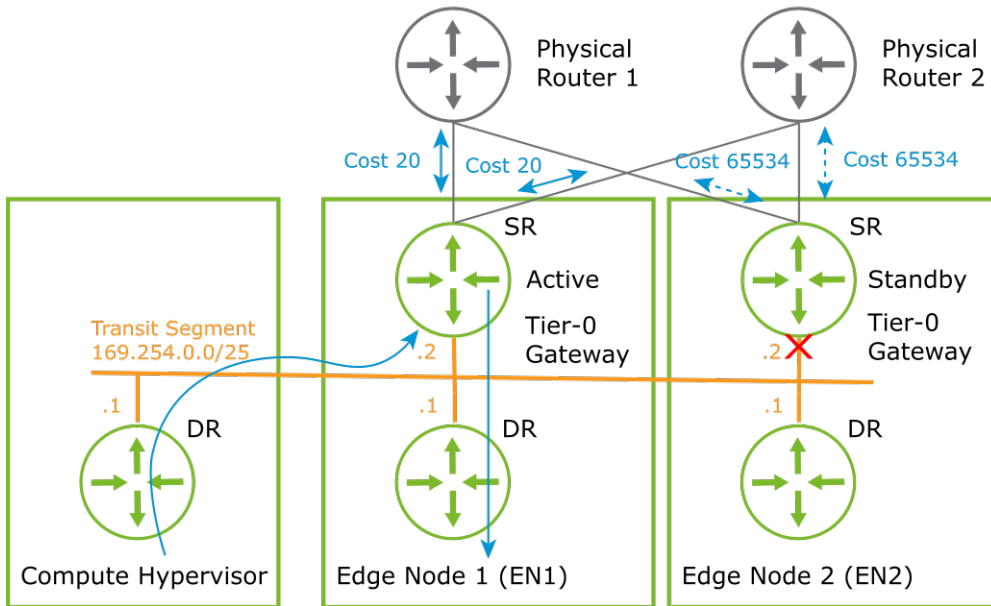
Traffic flow considerations in the active-standby mode with BGP:

- In the diagram, 169.254.0.2/25 is used on both active and standby SRs.
- The standby SR transit segment interface is down for datapath traffic.
- AS path prepending influences BGP peer path selection so the standby SR is less preferred to receive any traffic.
- BGP peering over the standby path ensures optimal BGP route convergence time during failover.

## 5-100 Active-Standby Topology with OSPF

The standby Tier-0 uses a high OSPF cost to influence route selection on physical routers.

### Physical Topology



The Tier-0 gateway is configured with two uplinks in an active-standby configuration:

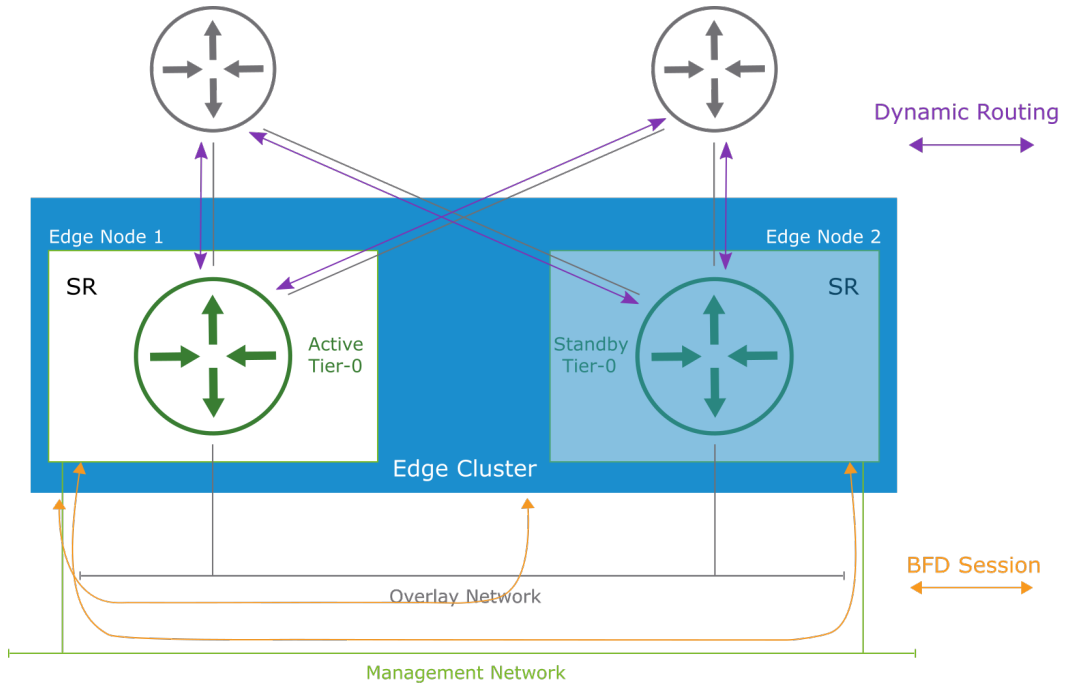
- From an OSPF standpoint, the standby Tier-0 is active.
- The standby Tier-0 uses the OSPF cost to influence the routing decisions on the physical routers.
- The OSPF cost sent by the standby Tier-0 is always 65534, a hard-coded value that cannot be adjusted.
- The route with the lowest value for cost is chosen as the best southbound route.
- The standby SR transit segment interface is down for datapath traffic.
- The DR sends traffic to the active SR only, using the active SR as the northbound route.



## 5-101 Failover Detection Mechanisms

The failover process uses the following mechanisms to check the connectivity between tiers:

- Bidirectional Forwarding Detection (BFD): On the management and overlay network
- Dynamic Routing Protocol (BGP or OSPF): On the uplinks

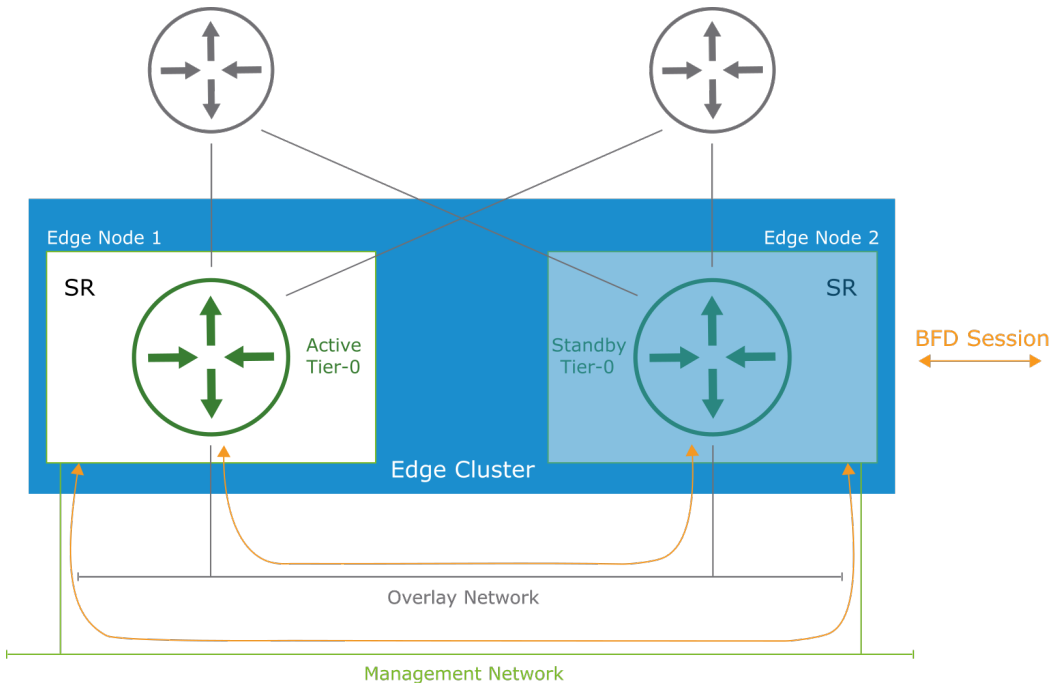


## 5-102 About BFD

High availability uses BFD to detect forwarding path failures.

BFD provides a low-overhead detection of faults even on physical media that do not support failure detection of any kind, such as Ethernet.

BFD keepalives are sent on both management and tunnel interfaces.

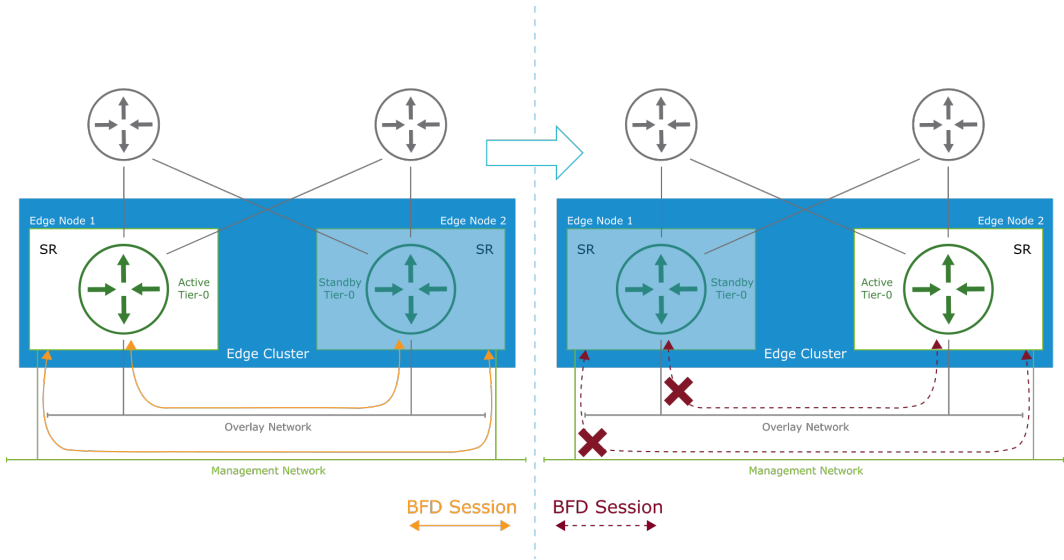


BFD is a network protocol used to detect faults between two forwarding engines connected by a link. Failures are detected per logical router. The conditions used to declare an edge node as down are the same in active-active and active-standby high availability modes.

To ensure uninterrupted routing of network traffic, the NSX Edge nodes exchange keepalive messages, which are BFD sessions running between the nodes. The edge nodes in an edge cluster exchange BFD keepalive on the management and tunnel interfaces. When the standby Tier-0 gateway fails to receive keepalives on both management and tunnel interfaces, it announces itself as active.

## 5-103 Failover Scenario with BFD

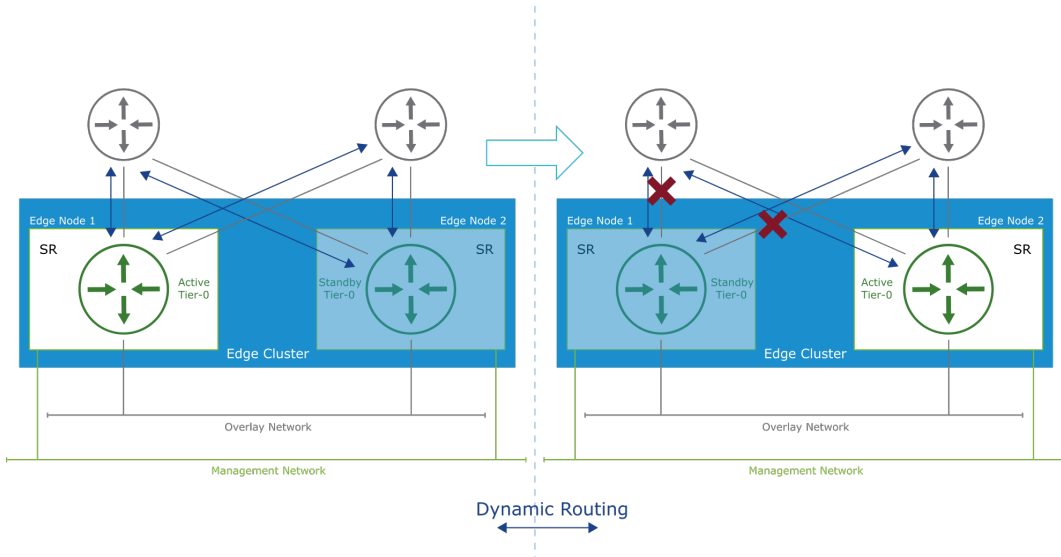
If a standby gateway fails to receive BFD keepalives on both management and tunnel interfaces, the gateway becomes active.



The BFD protocol provides fast detection of failure for forwarding paths or forwarding engines, improving convergence. Edge VMs support BFD with a minimum BFD timer of 500 milliseconds with three retries, providing 1.5 seconds failure detection time. Bare-metal edges support BFD with a minimum BFD timer of 50 milliseconds with three retries, which implies a 150 milliseconds failure-detection time.

## 5-104 Failover Scenario with Dynamic Routing

Dynamic routing peering sessions are established on the uplinks with physical routers. If an active gateway loses all its routing neighbors and a standby gateway is available, the active gateway steps down and becomes the standby gateway and the standby gateway is promoted to the new active gateway.



If an active gateway loses all its dynamic routing peerings and a standby gateway is configured, failover occurs. An active SR on an edge node is declared down when all the dynamic routing sessions on the peer SR are down.

This scenario is only applicable on Tier-0 with dynamic routing.

BGP or OSPF is configured on the uplink between each NSX Edge node and the exterior physical gateways.

Status is monitored during the dynamic routing keepalive exchanges.

The default BGP timers are a keepalive interval of 60 seconds and the minimum time between advertisements is 30 seconds. The default OSPF timers are a Hello interval of 10 seconds and a Dead interval of 40 seconds.

If all overlay tunnels to the compute hypervisors are down, the active edge node does not receive tunnel traffic from compute hypervisors. Then the standby edge node takes over.

## 5-105 Failover Modes

You can select different failover modes in active-standby HA mode:

- **Preemptive:** If the preferred node fails and recovers, it takes over its peer and becomes the active node. The peer changes its state to standby.
- **Non Preemptive:** If the preferred node fails and recovers, it checks whether its peer is active. If the peer is active, the preferred node stays in standby mode.

The screenshot shows the 'Tier-0 Gateways' configuration page in the NSX UI. The 'HA Mode' dropdown is set to 'Active Standby'. The 'Fail Over' dropdown is set to 'Non Preemptive'. A blue callout box points to the 'Fail Over' dropdown with the text: 'For Active Standby HA Mode, you can select Preemptive or Non Preemptive failover types.'

Preemptive and non-preemptive modes are used in a failback scenario after a failover occurs.

During the failover, the standby node becomes active.

The failback happens when the node that failed becomes available again:

- If non-preemptive mode is configured, nothing happens.
- If preemptive is configured, the original active (preferred) node takes over again.

## 5-106 Review of Learner Objectives

- Explain the purpose of ECMP routing
- Use the NSX UI to configure ECMP routing
- Identify the active-active and active-standby modes for high availability
- Recognize failure conditions and explain the failover process

# 5-107 Lesson 6: Logical Routing Packet Walk

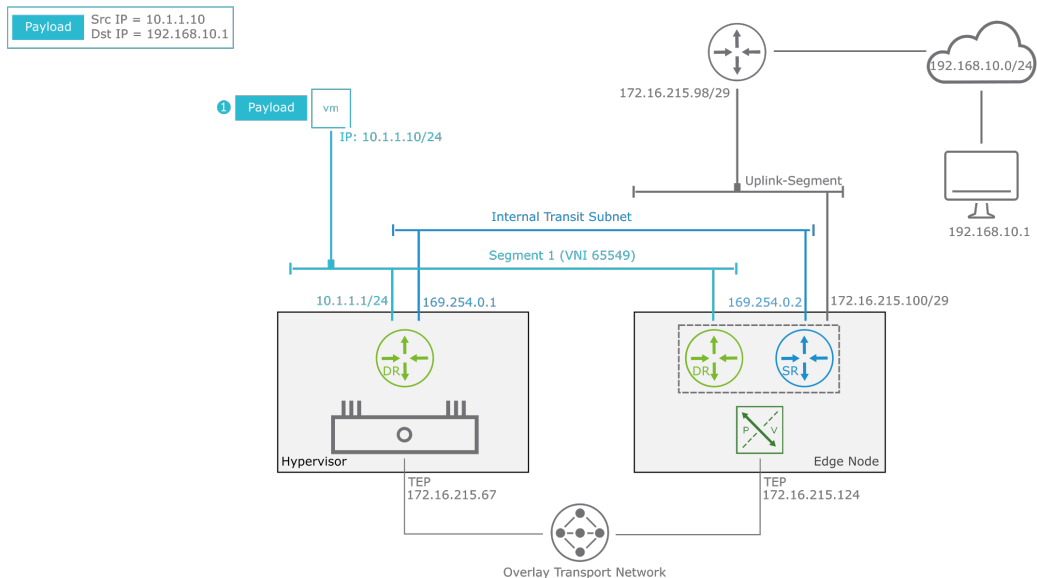
## 5-108 Learner Objectives

- Describe the datapath of single-tier routing
- Explain the datapath of multitier routing

## 5-109 Single-Tier Routing: Egress to Physical Network (1)

A packet is sent from the source VM 10.1.1.10 to the destination VM 192.168.10.1:

1. The packet is forwarded to its default 10.1.1.1 gateway.



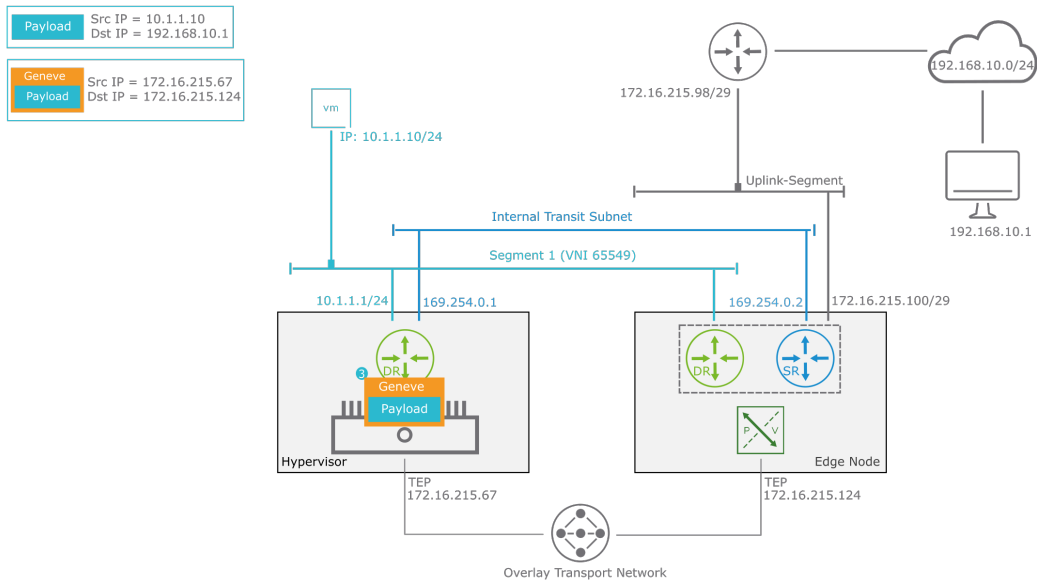
The default gateway 10.10.10.1/24 is on the Tier-0 DR (TO DR) component of the hypervisor where the VM resides.

The internal transit subnet 169.254.0.0/24 in the diagram, which connects the Tier-0 DR (TO DR) in the hypervisor with the Tier-0 SR (TO SR) in the NSX Edge node, is the default subnet, but it can be configured with a different range.



## 5-111 Single-Tier Routing: Egress to Physical Network (3)

- To send the packet from the hypervisor to the edge node, the packet is encapsulated with a Geneve header.

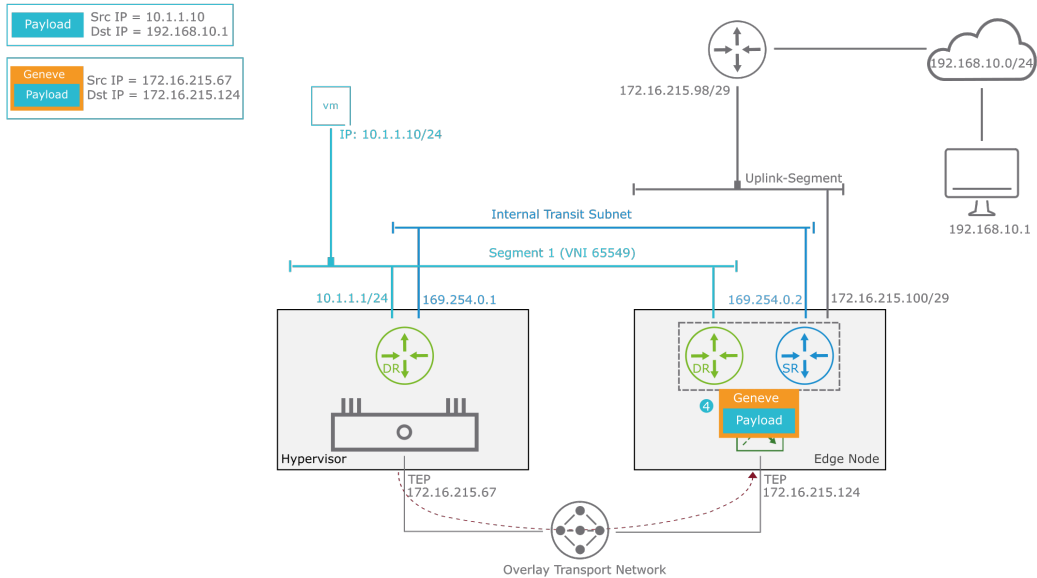


The source host (TEP 172.16.215.67) encapsulates the packet with a Geneve header to send it to the remote host (TEP 172.16.215.124). The original packet is intact.



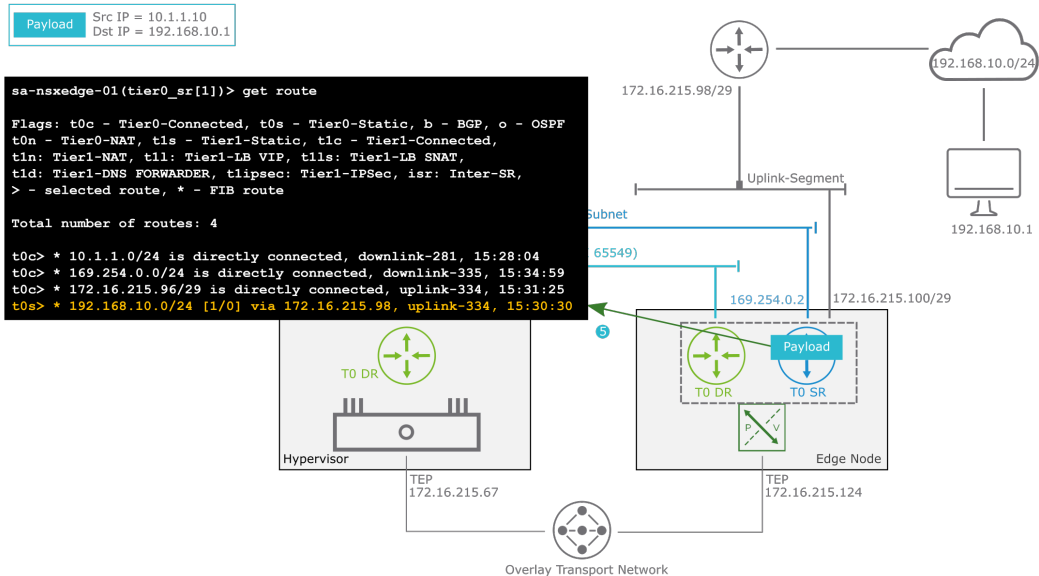
## 5-112 Single-Tier Routing: Egress to Physical Network (4)

4. The encapsulated packet is sent to the edge node across the overlay tunnel.



## 5-113 Single-Tier Routing: Egress to Physical Network (5)

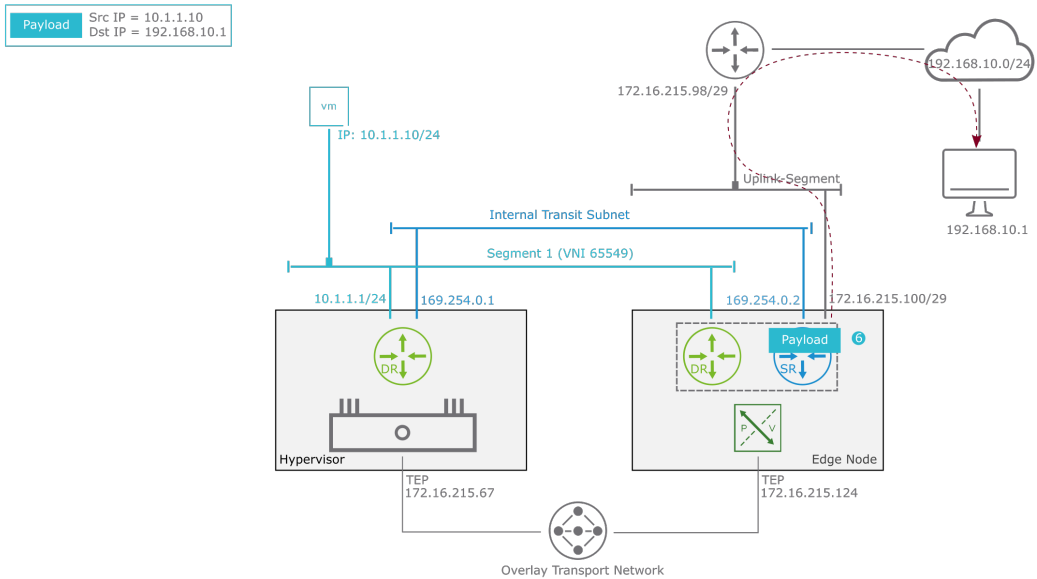
- The edge node decapsulates the packet and sends it to its SR component. The gateway (TO SR) routing table shows a route for the 192.168.10.0/24 network over the uplink segment.



To reach the destination 192.168.10.0/24 network, the next-hop 172.16.215.98 is used.

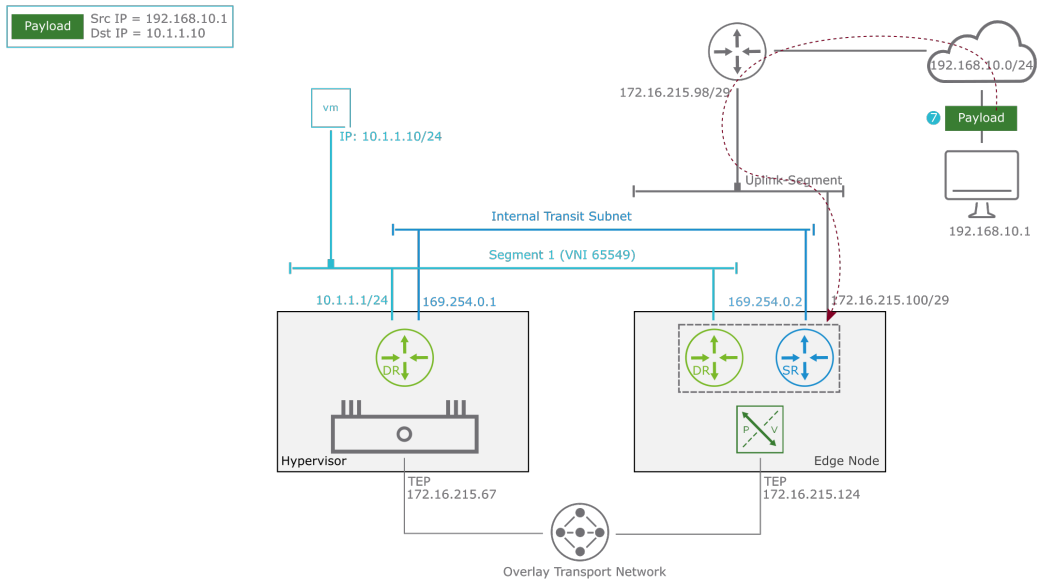
## 5-114 Single-Tier Routing: Egress to Physical Network (6)

- The edge node sends the packet to its upstream physical gateway, which routes the packet to its destination 192.168.10.1.



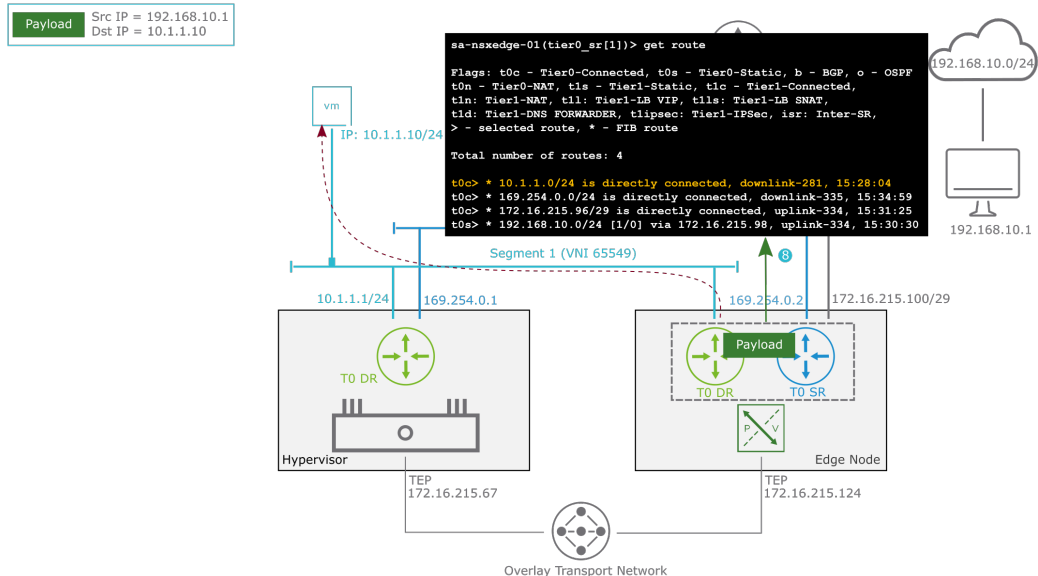
## 5-115 Single-Tier Routing: Ingress from Physical Network (7)

- For the return packet, the source VM 192.168.10.1 sends the packet to its default gateway, which routes the packet to the edge node.



## 5-116 Single-Tier Routing: Ingress from Physical Network (8)

- The SR and the DR components on an edge node share their routing table. A route is directly connected to the 10.1.1.0/24 network over Segment 1. The packet is sent to the remote host by using the TO DR interface.



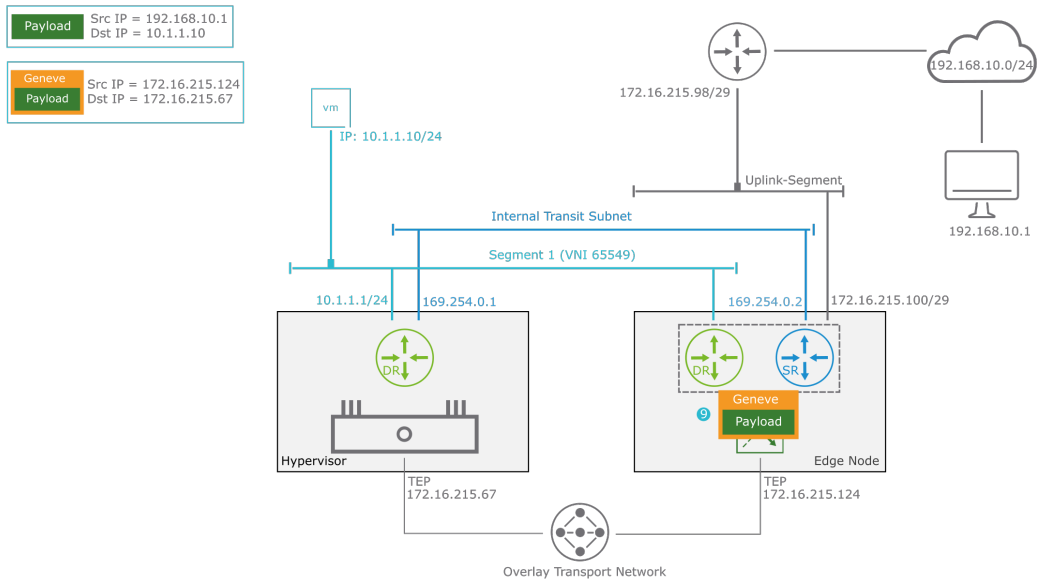
In the edge node, the SR and DR components share their routing table. This method removes the extra step of using the Internal Transit Subnet to route from SR to DR.

The Internal Transit Subnet is used when routing from a DR component from a hypervisor to an SR component in an edge node.

Because the routing table is shared, when the TO SR component in the edge receives the packet, it sends the packet to the remote host (Hypervisor with TEP 172.16.215.67) through the TO DR interface.

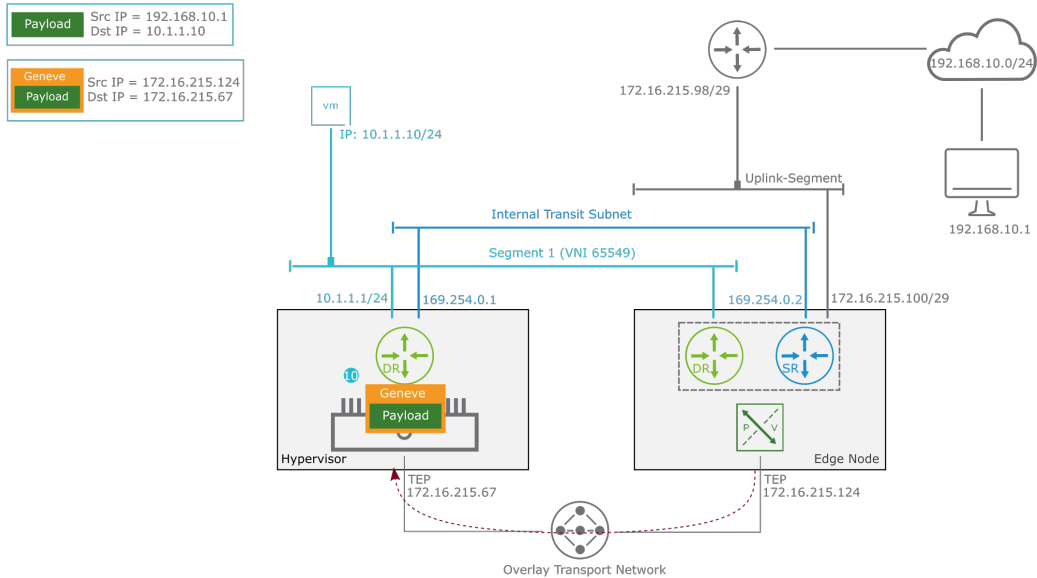
## 5-117 Single-Tier Routing: Ingress from Physical Network (9)

9. To send the packet from the edge node to the hypervisor, the packet is encapsulated with a Geneve header.



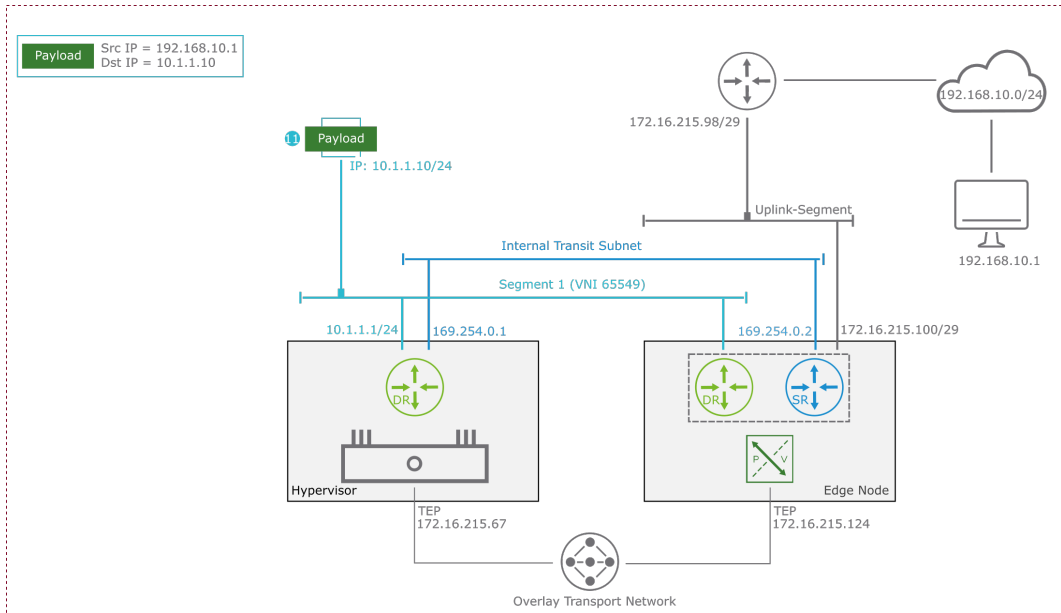
## 5-118 Single-Tier Routing: Ingress from Physical Network (10)

10. The encapsulated packet is sent across the overlay tunnel.



## 5-119 Single-Tier Routing: Ingress from Physical Network (11)

11. The receiving host decapsulates the packet and routes it to its destination (VM 10.1.1.10).

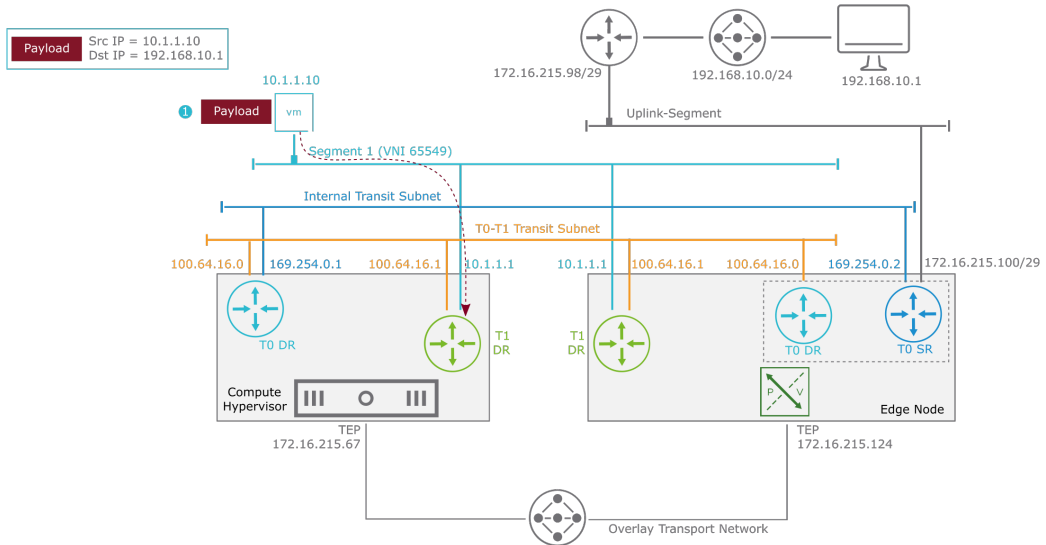




## 5-120 Multitier Routing: Egress to Physical Network (1)

A packet needs to be sent from the source VM 10.1.1.10 to the destination VM 192.168.10.1:

1. The packet is forwarded to its default 10.1.1.1 gateway.



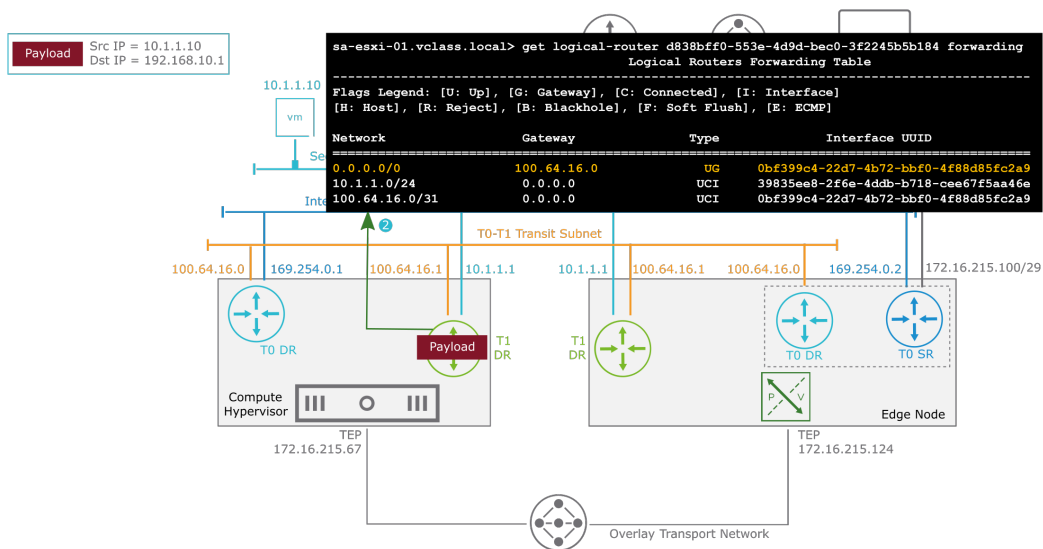
In the example, the Tier-1 gateway is a distributed router only and has no services configured, and therefore has no SR components.

The default gateway 10.10.10.1/24 is on the Tier-1 DR component of the hypervisor where the VM resides.

The Tier-0 Tier-1 (T0-T1) transit subnet 100.64.16.0/31 in the diagram, which connects the Tier-1 DRs (T1 DR) with the Tier-0 DRs (T0 DR) in the hypervisor and the NSX Edge node, is the default subnet, but it can be configured with a different range.

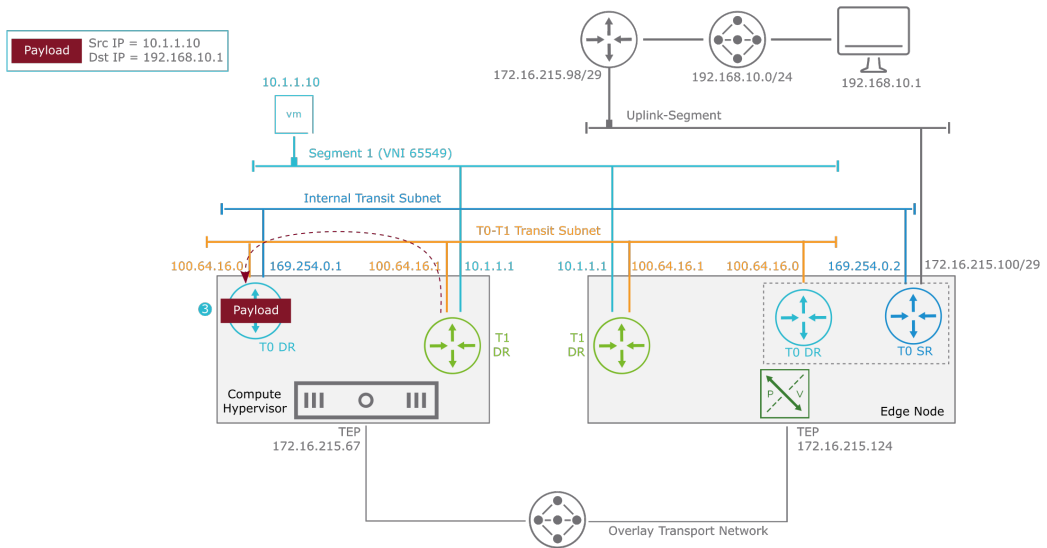
# 5-121 Multitier Routing: Egress to Physical Network (2)

- 2. The gateway (T1 DR) checks its forwarding table to make a routing decision. Because no specific route exists for the 192.168.10.0/24 network, the packet is sent to the default 100.64.16.0 gateway, which is the DR instance of Tier-0 on the same hypervisor.



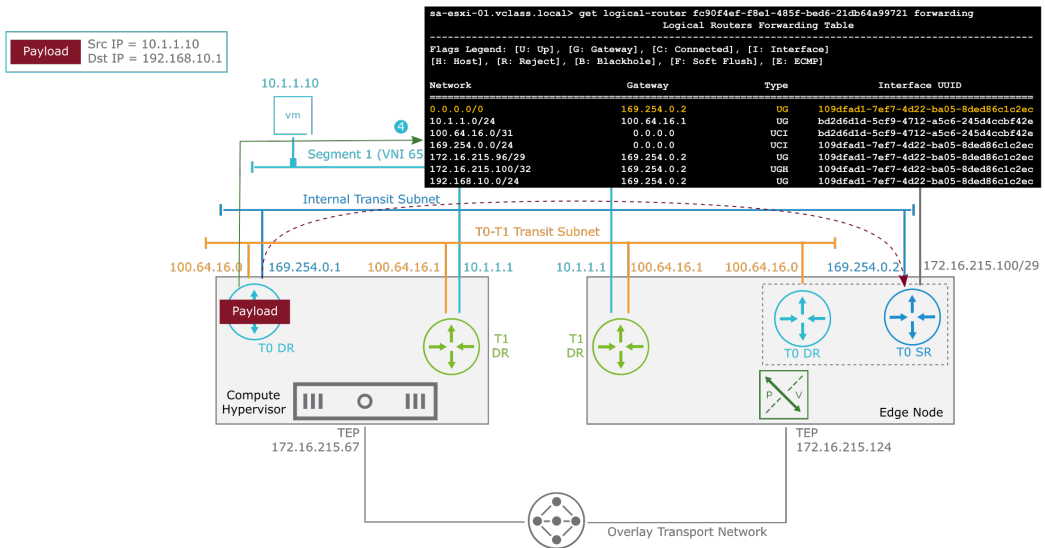
## 5-122 Multitier Routing: Egress to Physical Network (3)

- The packet is sent to the T0 DR instance on the same hypervisor through T0-T1 Transit Subnet.



## 5-123 Multitier Routing: Egress to Physical Network (4)

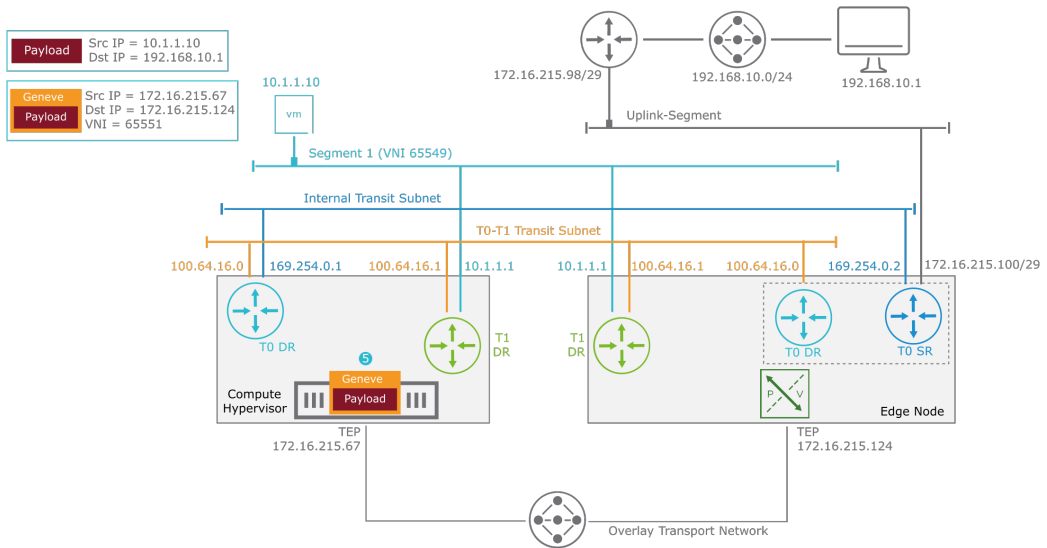
4. The gateway (T0 DR) checks its forwarding table to make a routing decision. The packet is sent to the default 169.254.0.2 gateway, which is the T0 SR component on the edge node.



The packet is sent to the default 169.254.0.2 gateway over the Transit segment. 169.254.0.2 is an interface of the Tier-0 SR component that attaches to the Internal Transit network.

## 5-124 Multitier Routing: Egress to Physical Network (5)

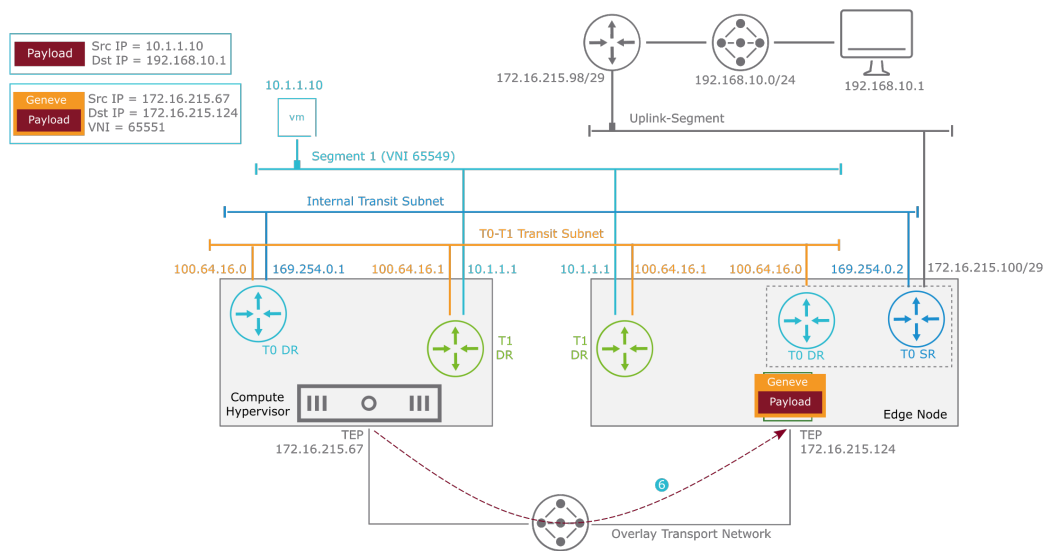
- To send the packet from the hypervisor to the edge node, the packet is encapsulated with a Geneve header.



The source host (TEP 172.16.215.67) encapsulates the packet with a Geneve header to send it to the edge node (TEP 172.16.215.124). The original packet is intact.

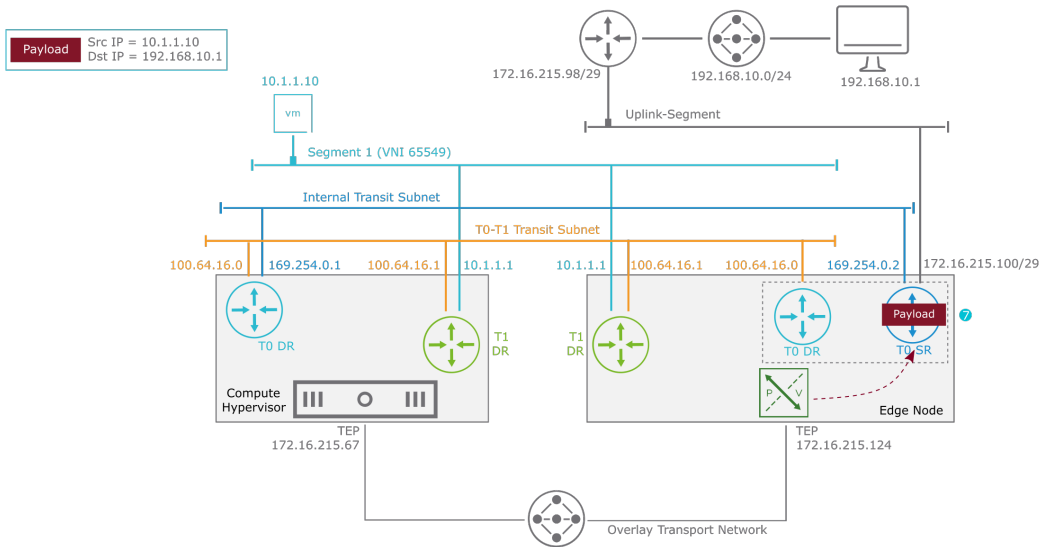
# 5-125 Multitier Routing: Egress to Physical Network (6)

6. The encapsulated packet is sent to the edge node across the overlay tunnel.



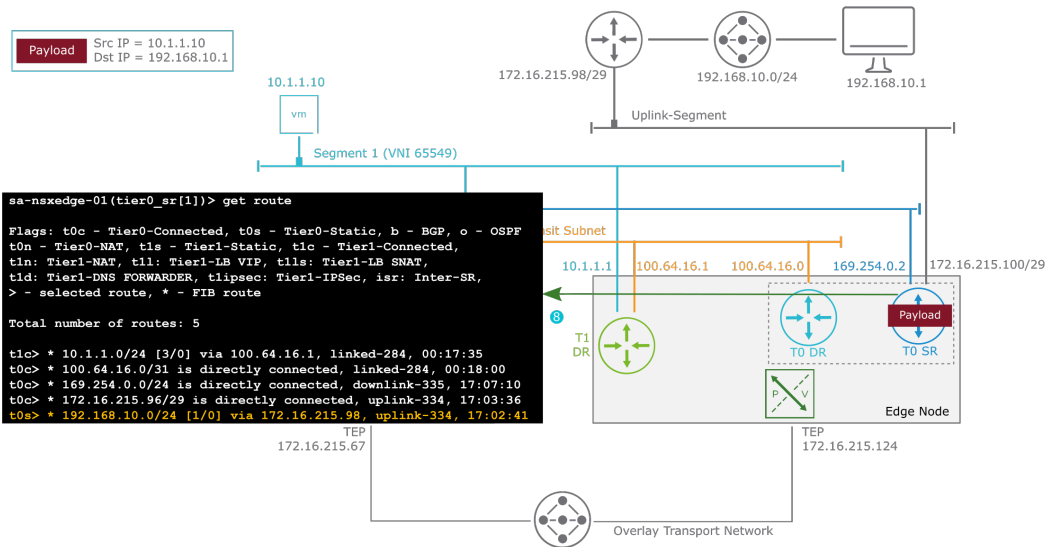
## 5-126 Multitier Routing: Egress to Physical Network (7)

7. The edge node decapsulates the packet and sends it to its T0 SR instance.



## 5-127 Multitier Routing: Egress to Physical Network (8)

8. The gateway (T0 SR) routing table shows a route for the 192.168.10.0/24 network over the uplink segment.

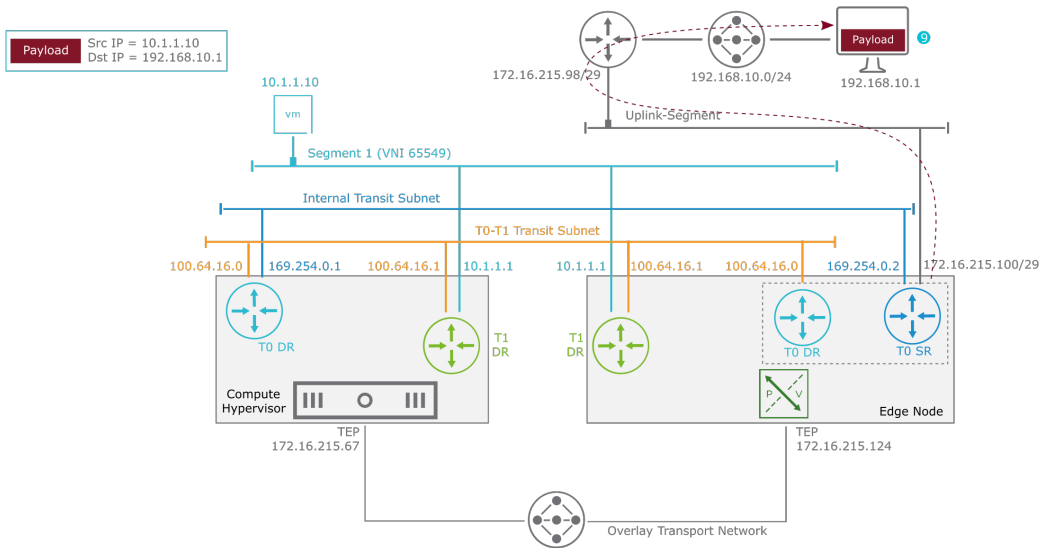


To reach the destination network 192.168.10.0/24, the next-hop 172.16.215.98, is used.



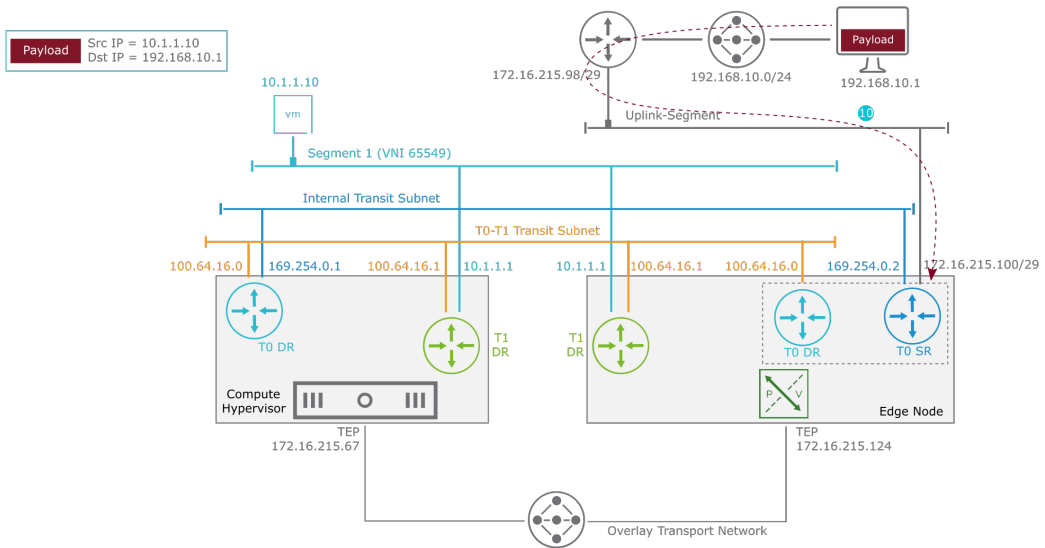
## 5-128 Multitier Routing: Egress to Physical Network (9)

9. The edge node sends the packet to its upstream physical gateway, which routes the packet to its destination, 192.168.10.1.



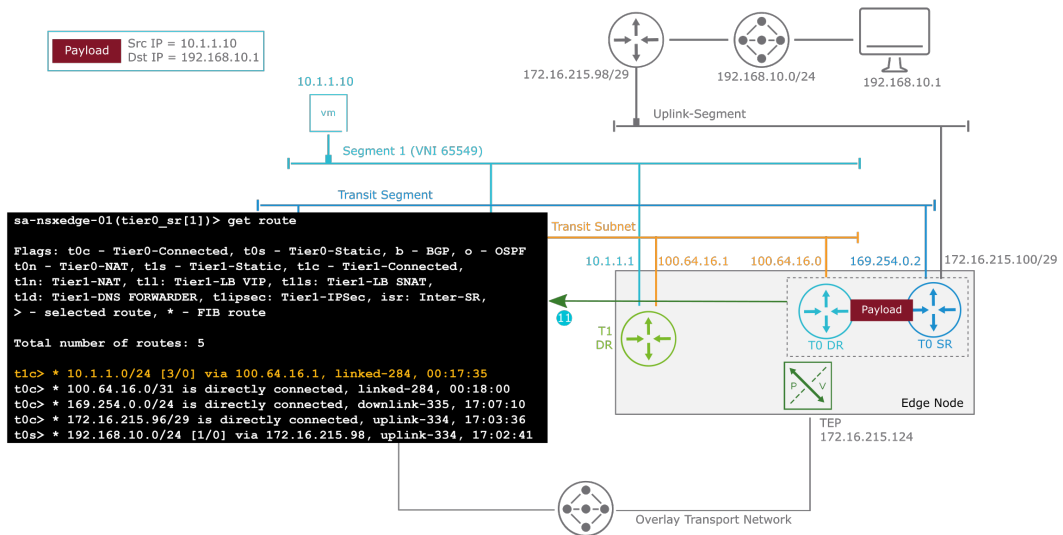
## 5-129 Multitier Routing: Ingress from Physical Network (10)

10. For the return packet, the source VM 192.168.10.1 sends the packet to its default gateway, which routes the packet to the edge node.



## 5-130 Multitier Routing: Ingress from Physical Network (11)

11. The SR and the DR components of the Tier-0 gateway share their routing table because they are both on the edge node. The routing decision is made to send the packet to the Tier-1 DR instance in the same edge node.



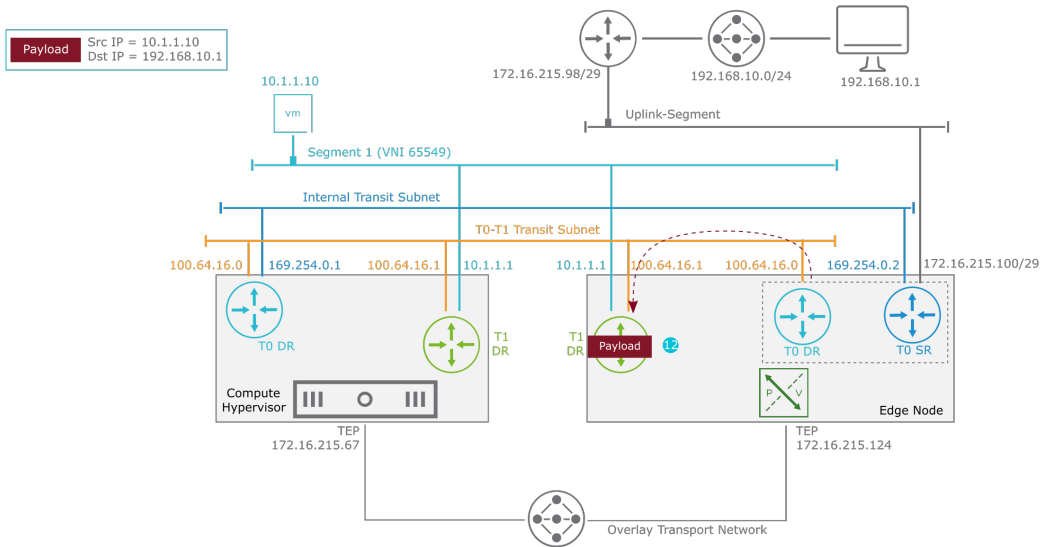
In the edge node, the SR, and DR components share their routing table. This method removes the extra step of using the Internal Transit Subnet to route from SR to DR.

The Internal Transit Subnet is used when routing from a DR component in a hypervisor to a SR component in an edge node.

As the routing table is shared, when the Tier-0 SR component receives the packet, the packet is sent to the Tier-1 DR component of the edge node through the DR interface.

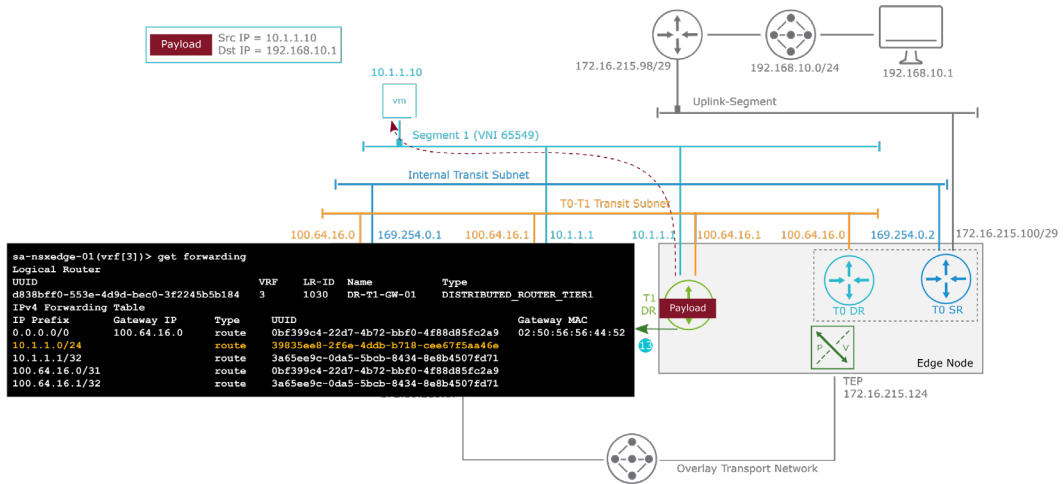
## 5-131 Multitier Routing: Ingress from Physical Network (12)

12. The packet is sent to the T1 DR instance on the edge node through T0-T1 Transit Subnet.



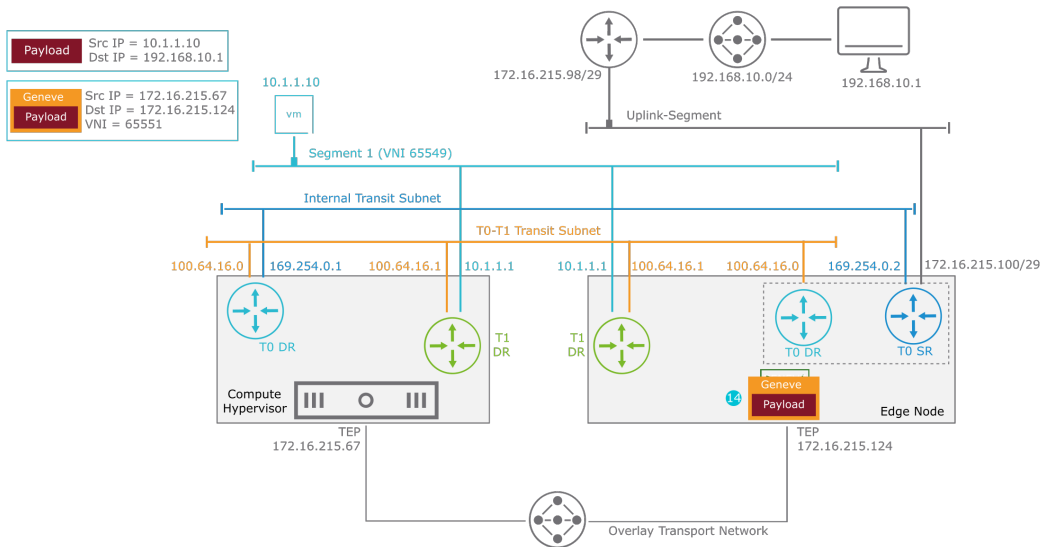
## 5-132 Multitier Routing: Ingress from Physical Network (13)

13. The gateway (T1 DR) checks its forwarding table to make a routing decision. A route is directly connected to the 10.1.1.0/24 network over Segment 1. The packet is sent to the remote host.



## 5-133 Multitier Routing: Ingress from Physical Network (14)

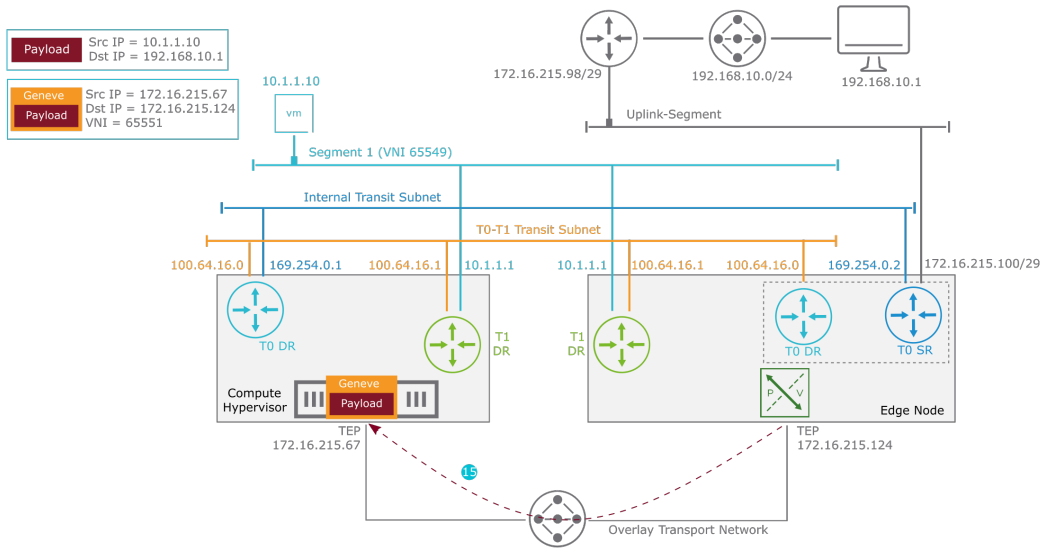
14. To send the packet from the edge node to the hypervisor, the packet is encapsulated with a Geneve header.



The source host (TEP 172.16.215.124) encapsulates the packet with a Geneve header to send it to the remote host (TEP 172.16.215.67). The original packet is intact.

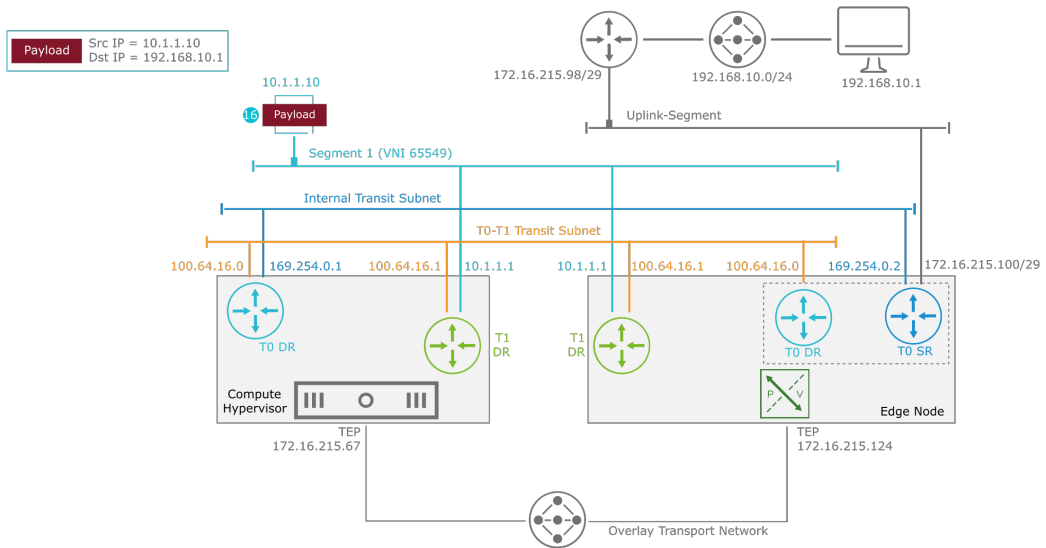
## 5-134 Multitier Routing: Ingress from Physical Network (15)

15. The encapsulated packet is sent to the edge node across the overlay tunnel.



## 5-135 Multitier Routing: Ingress from Physical Network (16)

16. The receiving host decapsulates the packet and routes it to its destination (VM 10.1.1.10).



## 5-136 Review of Learner Objectives

- Describe the datapath of single-tier routing
- Explain the datapath of multitier routing



## 5-137 Lesson 7: VRF Lite

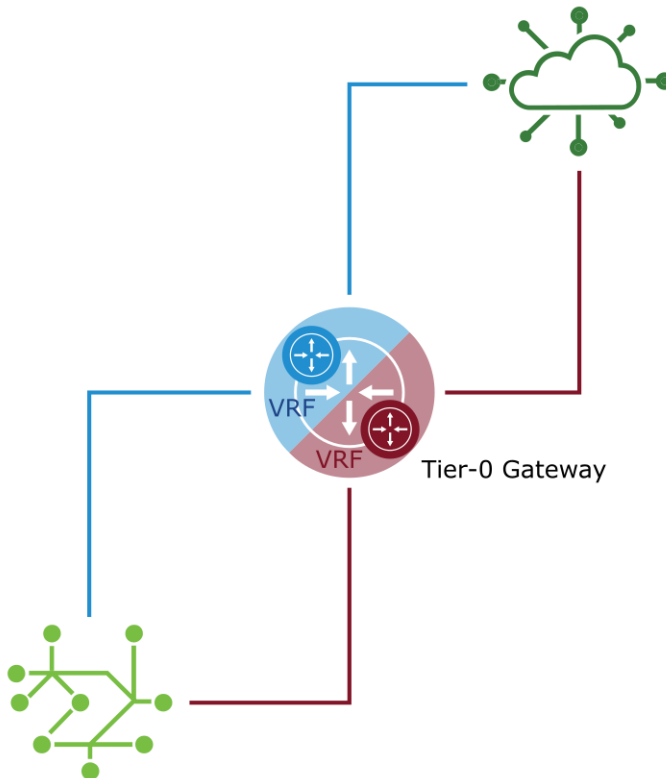
### 5-138 Learner Objectives

- Describe VRF Lite
- Explain the benefits of VRF Lite
- Configure and validate VRF Lite deployments

## 5-139 About VRF Lite

VRF Lite has the following characteristics:

- Multiple routing instances can be configured without deploying additional Tier-0 gateways and NSX Edge nodes.
- Logical routing isolation is provided in NSX and to external peers that are compatible with the VRF Lite technology.
- MPLS/MP-BGP protocols are not used.



Virtual Routing and Forwarding (VRF) allows the coexistence of multiple routing instances in one routing device. Independent routing and forwarding tables are maintained for each instance.

Separation between tenants and applications does not require additional Tier-0 gateways and NSX Edge nodes with VRF Lite.

VRF Lite provides logical routing isolation in NSX and spans it to external peer devices that support this technology.

VRF Lite differs from other VRF implementations because it does not rely on MPLS and MP-BGP protocols running in the physical network.

- Multiprotocol Label Switching (MPLS): This layer 2 protocol is used to forward traffic based on labels. MPLS does not use network addresses like IP protocol. These labels identify the paths between the endpoints in VRFs.
- Multiprotocol Border Gateway Protocol (MP-BGP): This BGP protocol extension is used to propagate the VRF routing information across MPLS network devices.

## 5-140 VRF Lite Requirements and Limitations

A VRF Lite deployment has the following requirements:

- A deployed Tier-0 gateway
- External connectivity with a layer 3 peer
- Peer device that supports 802.1Q protocol (VLAN tagging)

The following services cannot be configured in a VRF gateway:

- VPN
- OSPF routing

A Tier-0 gateway must be used to deploy VRF gateways. It is the default Tier-0 gateway and is the parent gateway of the VRF gateways.

The Tier-0 gateway, used as the default Tier-0 gateway, can be an existing Tier-0 gateway with connected Tier-1 gateways.

You can have more than one Tier-0 gateway with VRF gateways.

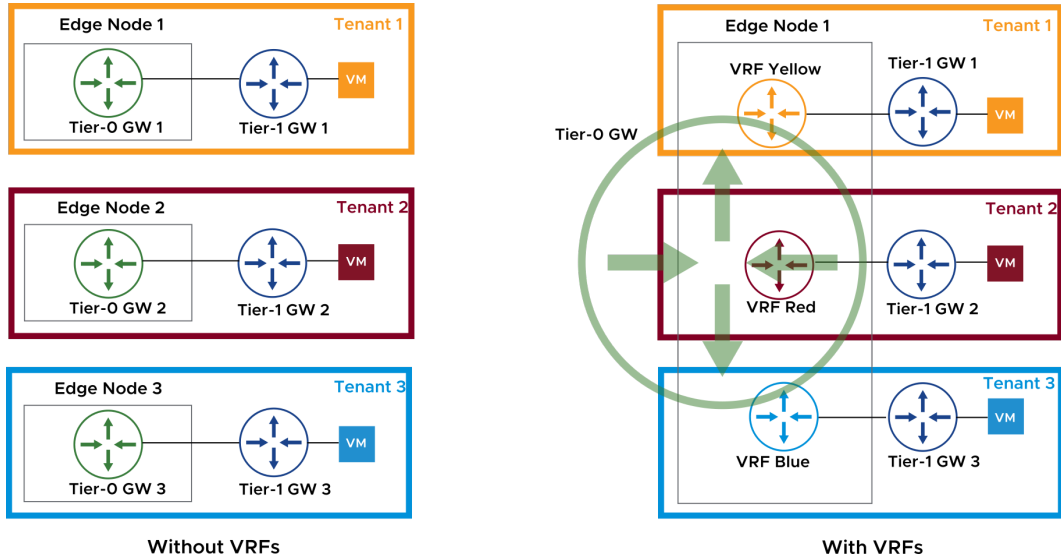
VLAN tagging is used to separate the VRFs in the uplink segment that connects with the external devices.

These limitations apply only to the VRF gateway. You can connect a Tier-1 gateway configured with a VPN to a VRF gateway and that is fully supported.

## 5-141 Use Cases for VRF Lite

VRF Lite can be used to enable the following features:

- Allow the same network address to coexist in different routing domains.
- Provide feature compatibility with existing network installations.
- Run multiple routing instances in the same gateway to optimize existing resources.



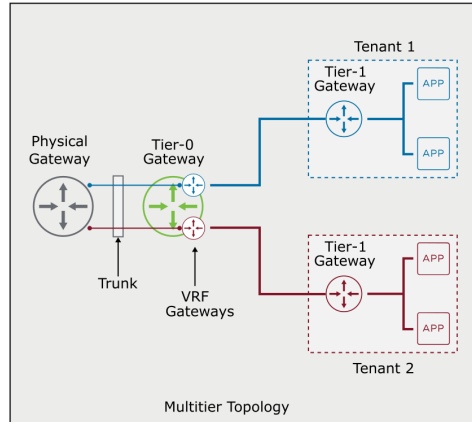
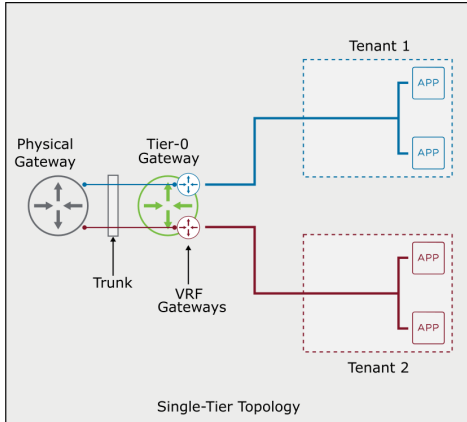
The only solution for customers that require separate network routing instances for each tenant is to deploy multiple Tier-0 gateways. However, these deployments can create scalability issues because only a single Tier-0 gateway can be deployed per NSX Edge node, specifically, for deployments based on bare-metal edges.

VRF Lite helps network administrators to deal with the overlapping of network ranges in the same routing domain between business units or after a merger.

It also allows existing VRF Lite deployments in the physical network infrastructure to be extended to NSX.

## 5-142 VRF Lite Topologies

VRF Lite can be deployed in single-tier and multitier topologies.



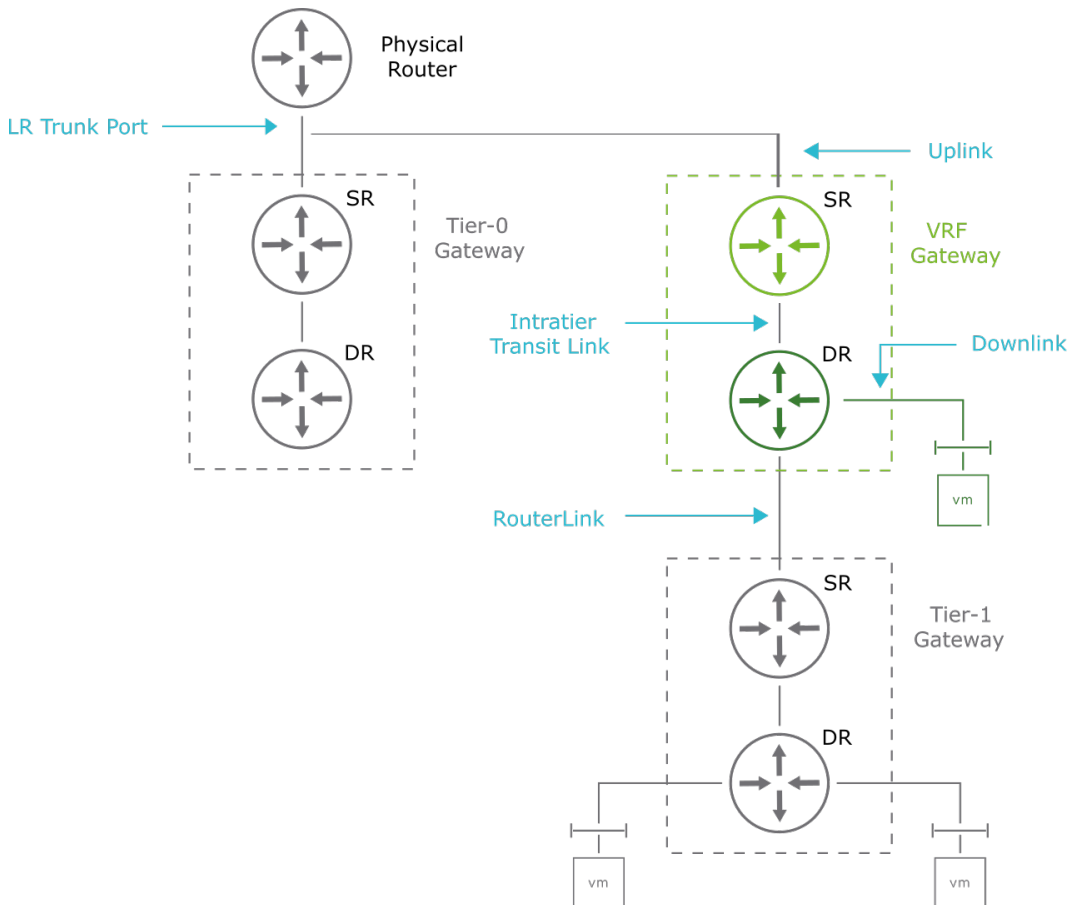
The following topology requirements must be considered:

- VRF gateways can only be deployed as Tier-0 gateways.
- A trunk is used to interconnect the different VRFs with the physical gateway.
- The physical gateway and the underlying infrastructure like vSphere Distributed Port Groups have to support trunking.
- Tenants can be connected to Tier-0 segments and Tier-1 segments.

## 5-143 VRF Lite Gateway Interfaces

The following types of interfaces are used with VRF gateways:

- The Logical Router (LR) trunk port connects the parent Tier-0 gateway to upstream physical devices.
- The VRF Uplink interface is internally connected to the LR trunk port of the parent Tier-0 gateway.
- The Intratier Transit Link is the internal link between the service router (SR) and distributed router (DR) of a VRF gateway.
- The Downlink interfaces connect VRF gateways to segments with attached workloads.
- The RouterLink ports connect VRF gateways with Tier-1 gateways.



The LR trunk port is a network interface while the VRF uplink port can be seen as a subinterface with a specific VLAN ID.

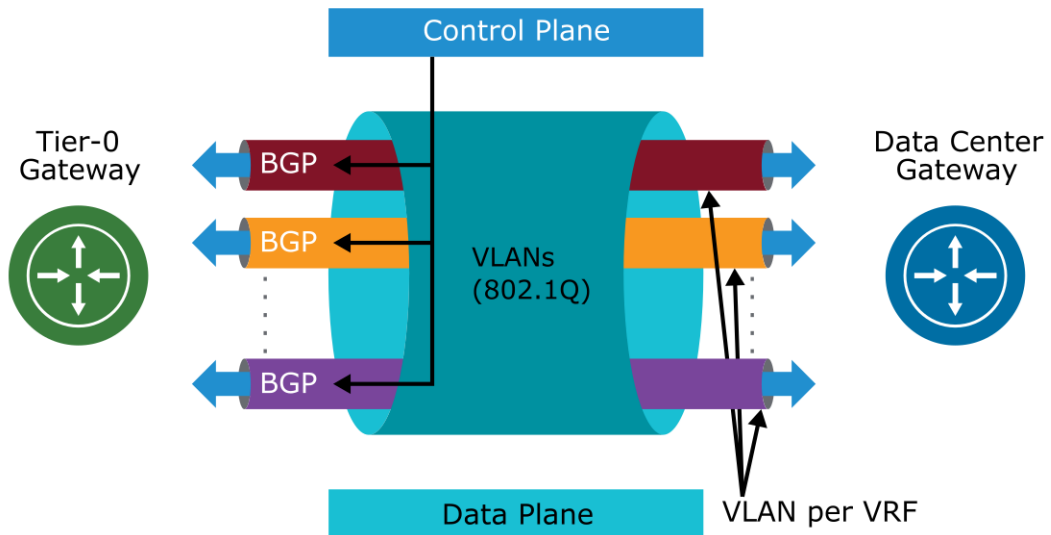
The LR trunk port is internally created in the parent Tier-0 gateway and is the only port connected to the uplink trunk segment.

The other interfaces are the same type as the interfaces used in the standard Tier-0 and Tier-1 gateways.

## 5-144 VRF Lite: Control and Data Planes

VLAN tagging (802.1Q) in the uplink trunk segment provides isolation for each VRF:

- VLAN is the channel for the data plane.
- BGP protocol instance in each VRF provides the control plane functionality.



A dedicated BGP instance runs in every VRF. You do not need to use the extensions in the MP-BGP protocol to exchange the VRF routing information.

BGP is the control plane because it dynamically propagates and updates routing information to all VRF peers.

Each VLAN is mapped to a VRF and only transports traffic for that VRF.

## 5-145 Configuring VRF Lite

Follow these steps to configure VRF Lite.



The deployment of a Tier-0 gateway is optional if an existing Tier-0 gateway is used instead as the default Tier-0 for the VRF gateway.

VRF gateways inherit the following configuration options from the default Tier-0 gateway:

- HA mode
- Edge cluster
- BGP AS number
- Graceful restart settings
- BGP multipath relax

You do not need to connect a Tier-1 gateway to the VRF gateways. Tenants can be directly connected to VRF gateways.



## 5-146 Deploying the Default Tier-0 Gateway

To deploy and configure the default Tier-0 gateway as a standard Tier-0 gateway:

1. Navigate to **Networking > Connectivity > Tier-0 Gateways** in the NSX UI.
2. Select **ADD GATEWAY > Tier-0**.

The screenshot displays the NSX UI for configuring a Tier-0 Gateway. The left sidebar contains a navigation menu with categories: Network Overview, Network Topology, Connectivity (selected), Network Services, and IP Management. Under Connectivity, 'Tier-0 Gateways' is selected. The main panel shows the 'Tier-0 Gateways' configuration page. At the top, there is an 'ADD GATEWAY' dropdown menu with 'Tier-0' selected. Below this, the configuration form includes the following fields and options:

- Name:** BGP-T0-GW-01
- HA Mode:** Active Active (with a dropdown arrow and a help icon)
- Edge Cluster:** Edge-Cluster-01 (with a dropdown arrow and a help icon)
- DHCP Config:** Set (with a help icon)
- Additional Settings:** A section with expandable options for 'Route Distinguisher for VRF Gateways'.
- Description:** A text input field with the placeholder 'Description'.
- Tags:** A section for adding tags.

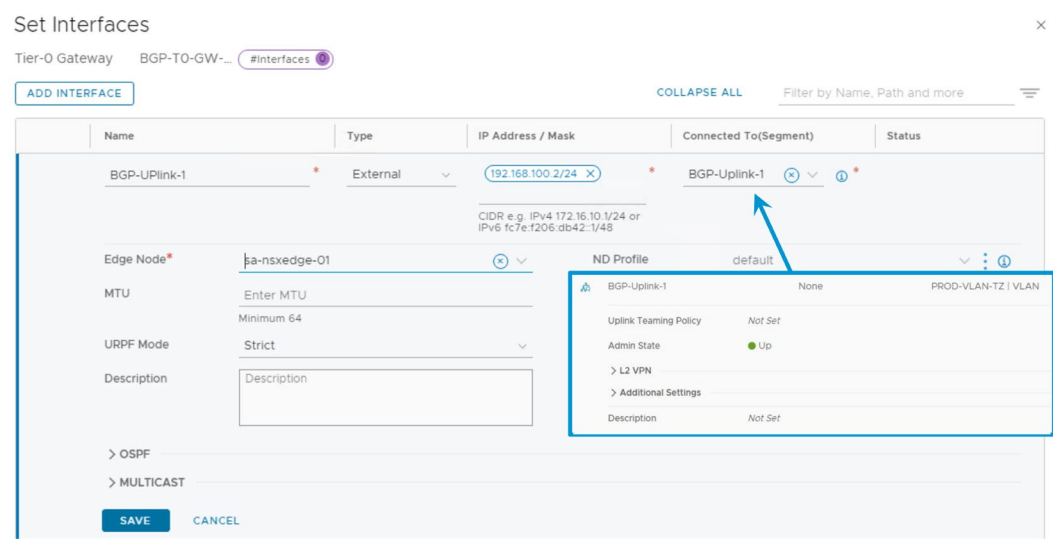
A note at the bottom of the form states: "NOTE - Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save." Below the note are expandable sections for 'INTERFACES', 'ROUTING', 'BGP', and 'OSPF'.

You configure the following parameters to deploy the default Tier-0 gateway:

- HA mode
- Edge cluster
- Uplink interfaces

# 5-147 Adding Uplink Interfaces to the Default Tier-0 Gateway

Connect the default Tier-0 uplink interfaces to the uplink segments in the Set Interfaces window.



A VLAN ID is not configured in the uplink interface.

Uplink interfaces are required to deploy the default Tier-0 gateway in the NSX Edge nodes.

## 5-148 Configuring BGP for the Default Tier-0 Gateway

Configure BGP parameters to use dynamic routing with external routers in the BGP configuration section.



VRF gateways inherit the global BGP configuration:

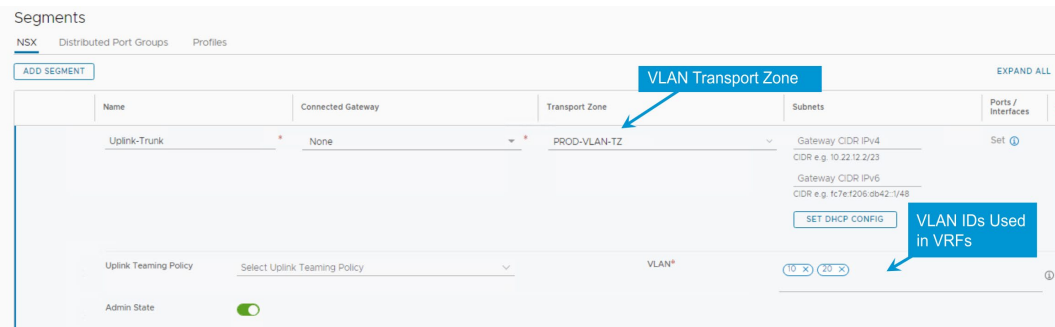
- Local AS
- Graceful restart
- Graceful restart timer
- Graceful restart stale timer
- Multipath relax

These parameters can only be changed in the default Tier-0 gateway.

# 5-149 Adding the Uplink Trunk Segment for the VRF Gateway

To configure the trunk segment for connecting the VRF gateway uplinks:

- 1. Navigate to **Networking > Connectivity > Segments > NSX** in the NSX UI.
- 2. Select **ADD SEGMENT**.



A segment is configured as a trunk when more than one VLAN is configured. A range of VLANs can also be specified (VLAN X-Y).

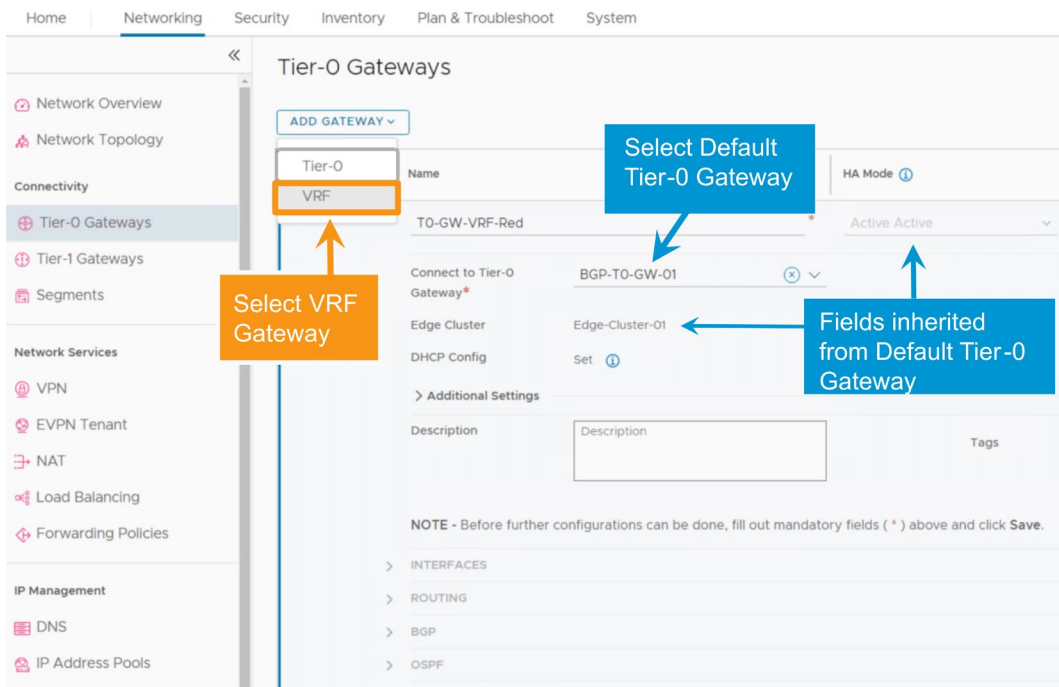
Uplink trunk segments specify which VLANs are allowed but do not add 802.1Q VLAN tagging. Tags are added in the uplink interface of VRF gateways.

You can configure a dedicated uplink trunk segment for each VRF uplink if the trunk is configured as a single VLAN range (X-X). As a best practice, you should connect the VRF uplinks to the same uplink trunk segment. This method reduces the number of resources required (segments, logical switch ports, and logical router ports).

## 5-150 Deploying the VRF Gateway

To deploy and configure the VRF gateway:

1. Navigate to **Networking > Connectivity > Tier-0 Gateways** in the NSX UI.
2. Select **ADD GATEWAY > VRF**.



Edge cluster and HA mode configuration values are automatically inherited from the default Tier-0 gateway.

You do not need to configure VRF settings for VRF Lite. These settings are used for Ethernet VPN (EVPN).

# 5-151 Adding Uplink Interfaces to the VRF Gateway

In the Set Interfaces window, connect the VRF gateway uplink interfaces to the uplink trunk segment.

Set Interfaces

VRF Gateway T0-GW-VRF-... #Interfaces 0

ADD INTERFACE

COLLAPSE ALL Filter by Name, Path and more

Name	Type	IP Address / Mask	Connected To(Segment)	Status
T0-GW-VRF-Red-Uplink *	External	192.168.10.2/24 * <small>CIDR e.g. IPv4 172.16.10.1/24 or IPv6 fc7e:1206:db42::1/48</small>	Uplink-Trunk	
Edge Node*	sa-nxedge-01	ND Profile	default	
MTU	Enter MTU Minimum 64	Proxy ARP Filter	Select Proxy	
URPF Mode	Strict	Access VLAN ID*	10	
Description	Description	Tags	VLAN IDs( 10, 20 )	
			Tag Scope	
			Max 30 allowed. Click (+) to add.	

Uplink-Trunk

Uplink Teaming Policy

Admin State

None

Not Set

PROD-VLAN-TZ | VLAN

VLAN

10

20

View Less

Not Set

Up

Access VLAN ID in Segment Range

VRF uplink interface configuration options:

- 802.1Q VLAN tagging is added at the uplink level.
- VRF gateway uplinks must be connected to a trunk segment.
- Access VLAN ID is required and must belong to the range specified for the trunk segment.

## 5-152 Configuring the BGP for the VRF Gateway

Set up the BGP parameters related to the VRF.

The screenshot shows the BGP configuration page for a VRF gateway. The BGP status is 'Enabled'. The Local AS is set to 100. The Graceful Restart is set to 'Helper Only' with a timer of 180 seconds. The Graceful Restart Stale Timer is set to 600 seconds. The Multipath Relax is set to 'On'. The BGP Neighbors section is set to 'Set'. An orange box labeled 'Not Supported in VRF Gateways' points to the 'Inter SR iBGP' toggle, which is currently 'Off'. A blue box labeled 'Parameters Inherited from Default Tier-0' points to the 'Local AS', 'Graceful Restart', 'Graceful Restart Timer', 'Graceful Restart Stale Timer', and 'Multipath Relax' settings. Below the configuration page, a table shows the BGP neighbors configuration.

IP Address	BFD	Remote AS number	Route Filter	Allows-in	Status
192.168.10.1	Disabled	10	1	Disabled	Success
Source Addresses		192.168.10.2		Graceful Restart	Helper Only
Max Hop Limit		1		Description	Not Set

The following parameters are inherited from the default Tier-0 gateway and cannot be modified at the VRF level:

- Local AS
- Graceful restart
- Graceful restart timer
- Graceful restart stale timer
- Multipath relax

Inter-SR iBGP is not supported in VRF gateways.

BGP can be enabled or disabled per VRF gateway.

Route aggregation and BGP neighbors are local configurations per VRF.

## 5-153 Connecting a Tier-1 Gateway to the VRF Gateway

To connect the Tier-1 gateway to the VRF gateway:

1. Navigate to **Networking > Connectivity > Tier-1 Gateways** in the NSX UI.
2. Select a Tier-1 Gateway and click **Edit** from the Actions menu next to >.
3. From the **Linked Tier-O Gateway** drop-down menu, select the VRF gateway.

The screenshot shows the 'Tier-1 Gateways' configuration page in the NSX UI. The main table lists the gateway 'T1-GW-VRF-Red' with 'Distributed Only' HA Mode and 'TO-GW-VRF-Red' as the 'Linked Tier-O Gateway'. The configuration details for 'T1-GW-VRF-Red' are visible, including 'Edges Pool Allocation Size' set to 'ROUTING' and a 'Description' field. A blue callout box with an arrow points to the 'TO-GW-VRF-Red' dropdown menu, with the text 'Select VRF Gateway'.

All Tier-O gateways and VRF gateways are listed in the **Linked Tier-O Gateway** drop-down menu.



# 5-154 VRF Lite Validation

Navigate to **Networking > Connectivity > Tier-O Gateways** to obtain the list of VRF gateways with its status and associated errors.

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

Network Overview

Network Topology

Connectivity

Tier-O Gateways

Tier-I Gateways

Segments

Network Services

VPN

EVPN Tenant

Tier-O Gateways

ADD GATEWAY

EXPAND ALL

Filter by Name, Path and more

	Name	HA Mode	Linked Tier-1 Gateways	Linked Segments	Status	Alarms
>	BGP-TO-GW-01	Active Active	1	0	Success	0
>	T0-GW-VRF-Blue	Active Active	1	0	Success	0
>	T0-GW-VRF-Red	Active Active	1	0	Success	0

Status - T0-GW-VRF-Red

Status: Success

Status on Transport Nodes

Errors

All | Failed/Down

Search

Transport Node	Status	Message
sa-nxedge-02	Success	

VRF gateways are marked with the VRF tag in the name field.

## 5-155 Lab 10: Configuring VRF Lite

Configure and verify the VRF Lite functionality to isolate routing domains:

1. Prepare for the Lab
2. Create the Uplink Trunk Segment
3. Deploy and Configure the VRF Gateways
4. Deploy and Connect the Tier-1 Gateways to the VRF Gateways
5. Create and Connect Segments to the Tier-1 Gateways
6. Attach VMs to Segments on Each VRF
7. Test the VRF End-to-End Connectivity
8. Review the Routing Tables in Each VRF
9. Verify the Routing Isolation Between VRFs

## 5-156 Review of Learner Objectives

- Describe VRF Lite
- Explain the benefits of VRF Lite
- Configure and validate VRF Lite deployments

## 5-157 Key Points (1)

- The NSX routing function meets the needs of service providers and tenants.
- An administrator manually performs static route configuration.
- Dynamic route configuration enables gateways to exchange information about the network.
- NSX logical routing commonly implements a two-tiered topology.
- Tier-1 gateways have downlink ports to connect to NSX segments and transit ports to connect to Tier-0 gateways.
- A gateway has two components: a distributed router and a service router.
- You can deploy an NSX Edge node through the NSX UI, the OVF tool, and an ISO file in a PXE environment.
- Joining NSX Edge nodes with the management plane ensures that NSX Manager and the NSX Edge nodes can communicate with one another.

## 5-158 Key Points (2)

- A multinode NSX Edge cluster helps ensure that at least one NSX Edge node is always available.
- NSX implements Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) dynamic routing protocols.
- External BGP (eBGP) is used to interchange autonomous system IP addresses with another autonomous system.
- OSPF is a link state routing protocol that maintains adjacencies with neighbor routers over Broadcast and Point-to-Point networks.
- ECMP routing increases the north-south communication bandwidth by adding an uplink to the Tier-0 gateway and configuring it for each NSX Edge node in an NSX Edge cluster.
- Multiple NSX Edge nodes can be pooled in a cluster for scale-out and redundancy.
- High availability supports two modes: active-active and active-standby.
- Stateful active-active high availability mode supports stateful services like NAT.
- VRF Lite enables you to configure multiple routing instances without deploying additional Tier-0 gateways and NSX Edge nodes.

Questions?



## Module 6

# NSX Logical Bridging

## 6-2 Importance

Logical bridging enables layer 2 communication between devices on NSX overlay-backed virtual networks and VLAN-backed physical networks. Logical bridging is also useful when you must split a subnet across physical and virtual workloads during a physical-to-virtual migration.

## 6-3 Lesson 1: NSX Logical Bridging

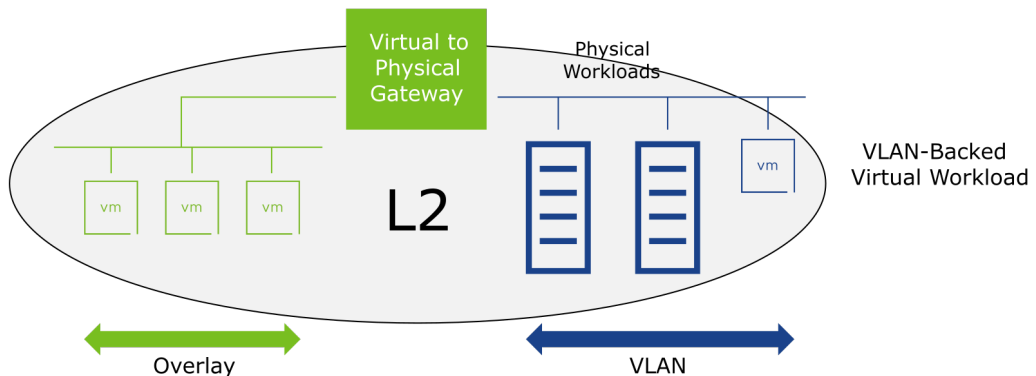
### 6-4 Learner Objectives

- Describe the purpose and function of logical bridging
- Distinguish between routing and bridging
- Create bridge profiles
- Create a bridge-backed segment and bridge traffic between virtual and physical environments

### 6-5 Overview of Logical Bridging

The bridging function provides layer 2 connectivity between the overlay segments and VLAN-backed physical networks:

- The layer 2 bridge feature is provided by the NSX Edge node.
- Traffic is bridged in and out of the NSX domain.
- The NSX Edge firewall provides granular control over the bridged traffic.



The bridge feature is available in bare-metal NSX Edge nodes and in NSX Edge VMs.

## 6-6 Logical Bridging Use Cases

Layer 2 bridging is used in the following common use cases:

- Performing a physical-to-virtual migration
- Connecting non-virtualized compute platforms

Layer 2 bridging is useful when you must split a subnet across physical and virtual workloads during a physical-to-virtual migration.

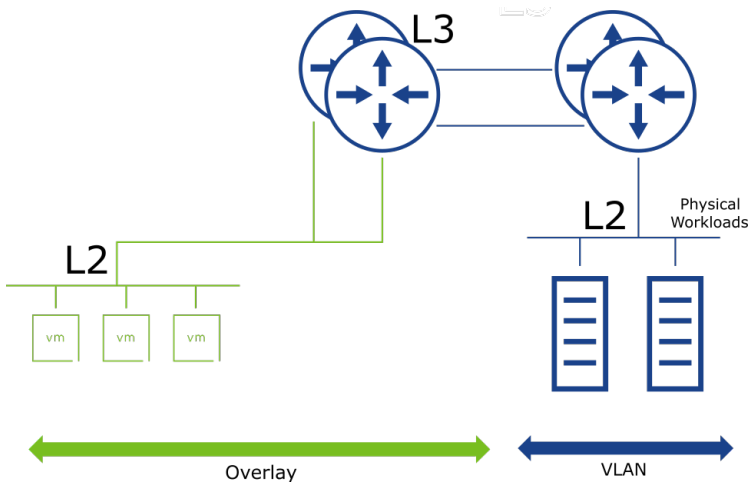
Layer 2 bridging also connects non-virtualized compute platforms.

## 6-7 Routing and Bridging for Physical-to-Virtual Communication

You can achieve physical-to-virtual communication through routing or bridging.

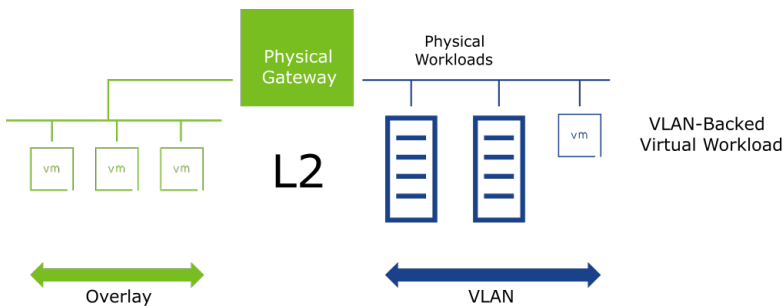
Routing:

- Standard layer 3 routing process between physical and virtual workloads
- Equal-cost multipath (ECMP) for scale-out and failure isolation



Bridging:

- The layer 2 flat broadcast domain is used for both physical and virtual workloads, resulting in limited domain size and lack of scalability.
- A single active bridge is needed for an overlay-to-VLAN pair.



Route when you can. Bridge when you have to.



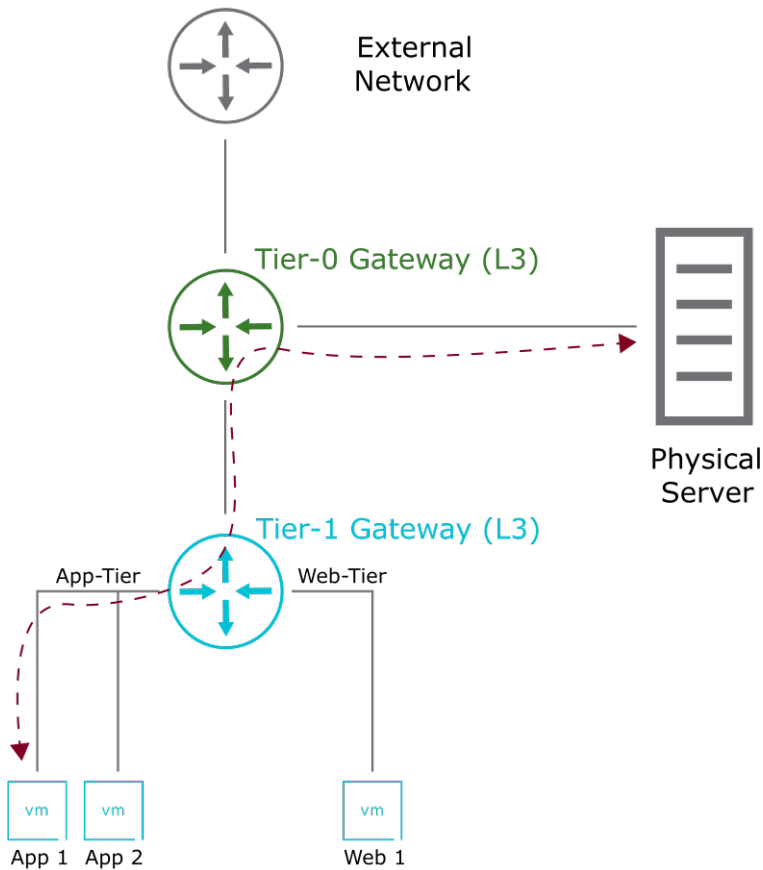
When connecting your physical workloads on traditional physical networks to a virtualized environment, you can use routers running standard routing protocols to route traffic between workloads in the two environments.

If you do not want to use routing and you must place your physical and virtual devices on a single layer 2 subnet, then you can enable bridging.

## 6-8 Example of Virtual-to-Physical Routing

Routing occurs between VMs in the NSX virtual environment and a server in the physical environment:

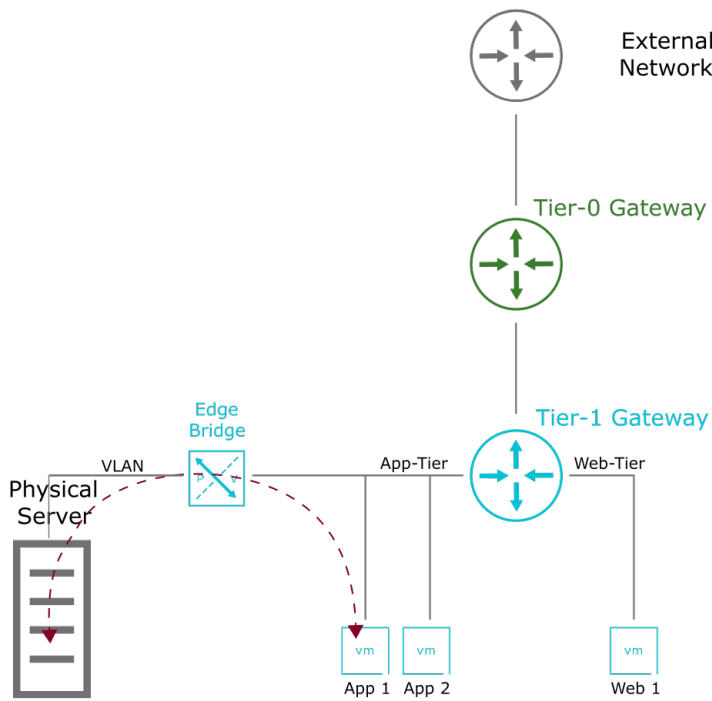
- The web tier and application tier belong to the NSX overlay.
- The physical server resides on a different subnet.
- The Tier-0 gateway provides north-south routing between the physical server and the application-tier servers.



## 6-9 Example of Virtual-to-Physical Bridging

Bridging occurs between a VM in the NSX virtual environment and a server in the physical environment on the same subnet:

- The application tier is in the NSX overlay.
- The physical server resides in the physical environment.
- The physical server is on the same subnet as the application tier servers.
- The communication between the physical server and the application tier occurs through the NSX Edge node.



The communication between the App1 VM and the physical server is realized by the gateway that performs bridging.

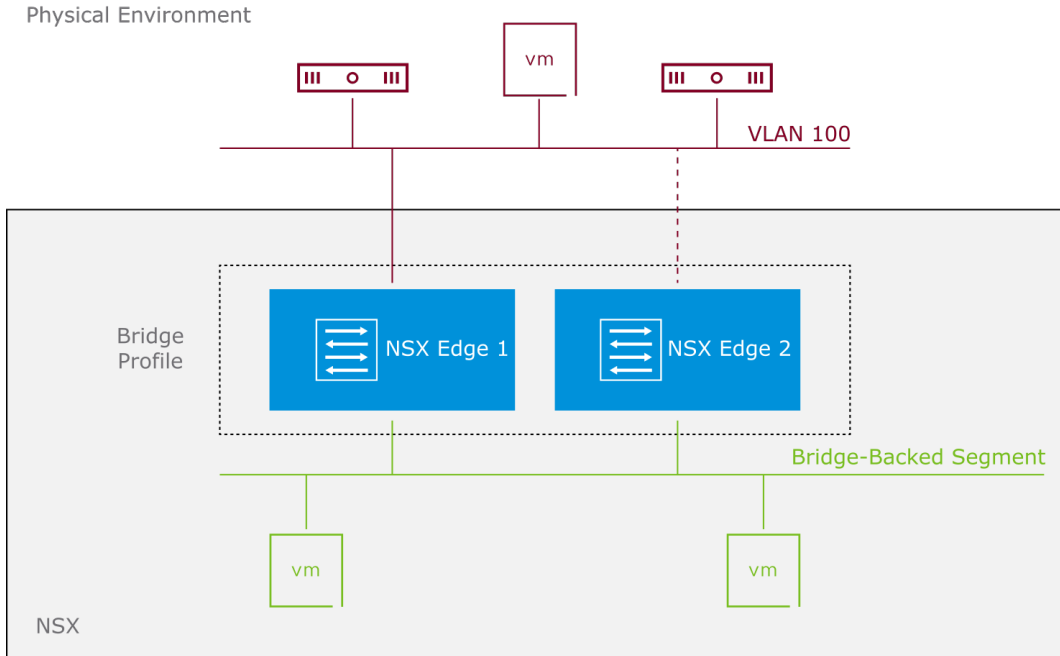
The diagram demonstrates how the physical server and the App1 server (virtual) can exist on the same subnet.

In the diagram, the traffic between the physical server and the application tier does not pass through the Tier-1 and Tier-0 gateways.

## 6-10 Logical Bridging Components

Layer 2 bridging consists of the following NSX components:

- A bridge profile is used to specify which edge nodes are involved in bridging.
- A bridge-backed segment is part of an overlay transport zone with an attached bridge profile.



You configure a bridge-backed segment to provide layer 2 connectivity between VMs in an NSX overlay and devices that are outside NSX.

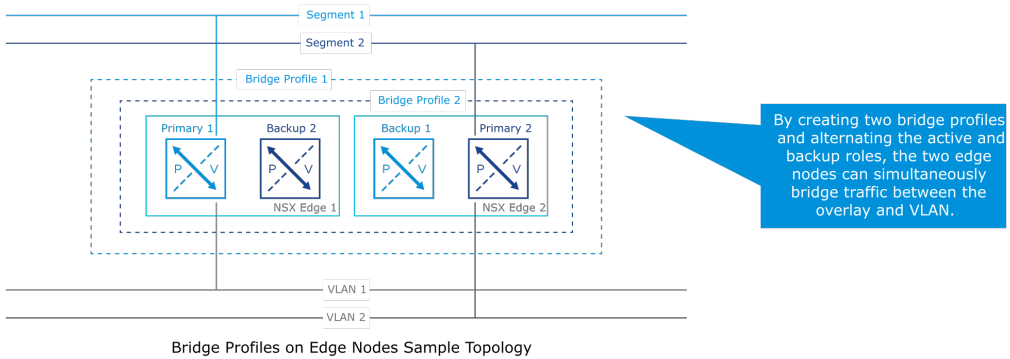
An NSX segment that is attached to a bridge profile provides the following information:

- VLAN to which traffic is bridged
- Physical port to be used (identified by the VLAN transport zone)

For more information about the additional edge configurations, see the section about configuring edge-based bridging in *NSX Administration Guide* at <https://docs.vmware.com/en/VMware-NSX/index.htmlhttps://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-FBFD577B-745C-4658-B713-A3016D18CB9A.html>.

## 6-11 Using Multiple Bridge Profiles

You can configure multiple bridge profiles on an NSX Edge node.



Bridge profile 1 maps VLAN 1 with Segment 1.

Bridge profile 2 maps VLAN 2 with Segment 2.

Edge 1 is the primary edge for bridge profile 1 and the backup edge for bridge profile 2.

Edge 2 is the primary edge for bridge profile 2 and the backup edge for bridge profile 1.

## 6-12 Creating an Edge Bridge Profile

To create an edge bridge profile, select **Networking > Connectivity > Segments > Profiles > Edge Bridge Profiles** in the NSX UI.

The screenshot shows the 'Add Edge Bridge Profile' configuration form in the NSX UI. The form is titled 'Segments' and has tabs for 'NSX', 'Distributed Port Groups', and 'Profiles'. The 'Profiles' tab is selected, and the 'Edge Bridge Profiles' sub-tab is active. The form includes a table with columns for Name, Edge Cluster, Primary Node, Backup Node, and Status. The 'Name' field is 'Edge-Bridge-Profile'. The 'Edge Cluster' field is 'Edge-Cluster-01'. The 'Primary Node' field is 'sa-nxvedge-01'. The 'Backup Node' field is 'sa-nxvedge-02'. The 'Fail Over' field is 'Preemptive'. The 'HA Mode' field is 'Active Standby'. The 'Description' field is empty. The 'Tags' field is empty. The 'Status' field is 'Active'. There are 'SAVE' and 'CANCEL' buttons at the bottom. Annotations highlight the 'Edge Cluster' field with the text 'Specify the edge cluster that is used for bridging.' and the 'Primary Node' and 'Backup Node' fields with the text 'Specify the node that has the primary role and the node that has the backup role in the edge cluster.'

When you configure an edge bridge profile, you select one of the following failover modes:

- **Preemptive:** The bridge on the primary edge node always becomes the active bridge when it becomes available again after a failure.
- **Non Preemptive:** The bridge on the primary edge node remains at standby if it becomes available after a failure when the bridge on the other edge node is already active.

After creating an edge bridge profile, additional configurations are required.

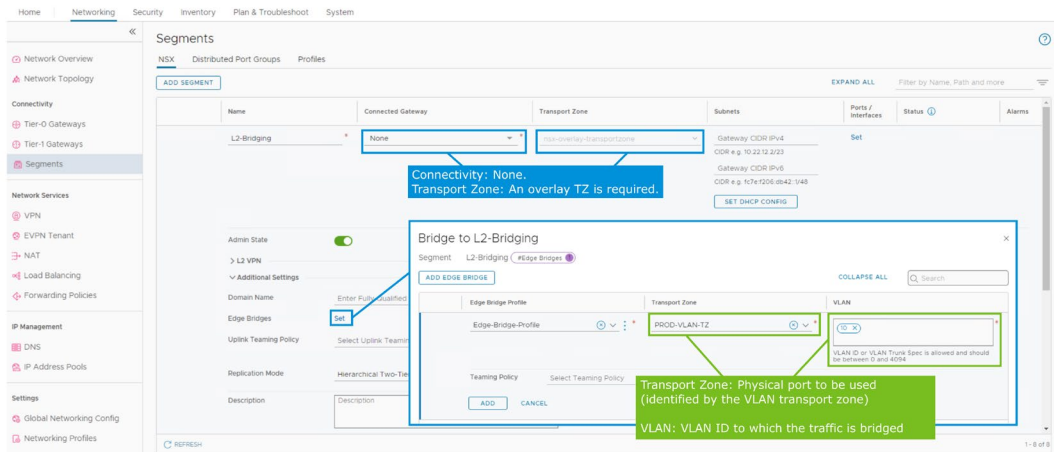
The following configuration options are available:

- Option 1: Configure the Promiscuous mode
- Option 2: Configure MAC address learning
- Option 3: Configure a sink port

## 6-13 Creating a Layer 2 Bridge-Backed Segment

The bridge-backed segment provides layer 2 connectivity to overlay VMs outside NSX:

- To create a segment, select **Networking > Connectivity > Segments > NSX**.
- After the segment creation, set up an edge bridge to attach the edge bridge profile.



Before configuring a bridge-backed logical segment, you must verify the following components:

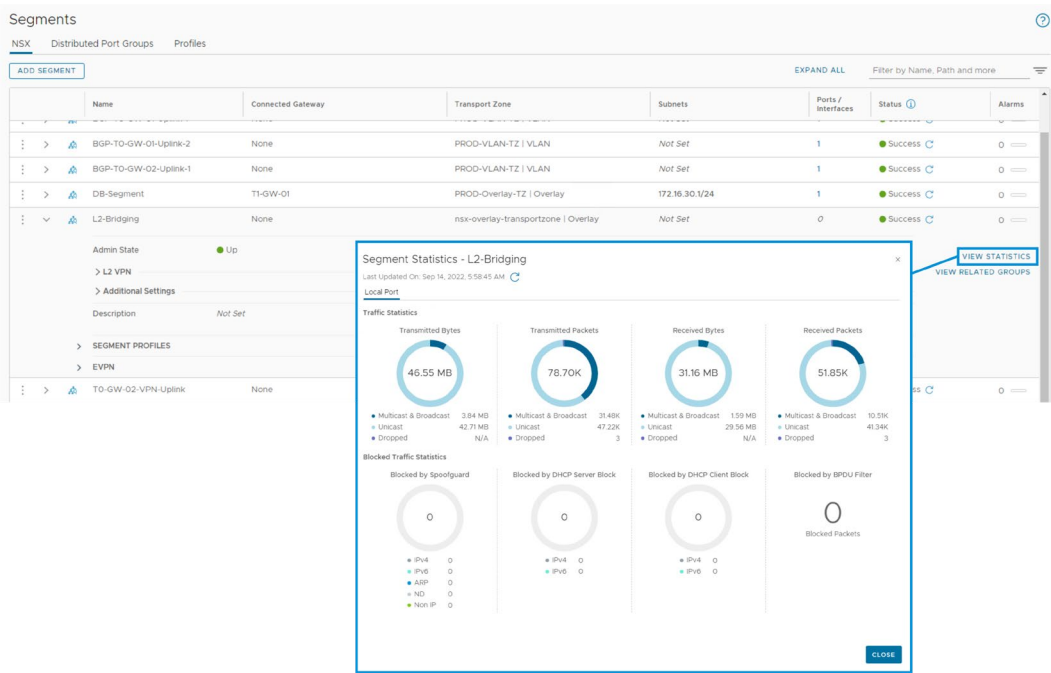
- A bridge profile must be configured.
- At least one ESXi host must exist to serve as a regular transport node. This node hosts VMs that require connectivity with devices outside an NSX deployment.
- A VM or another physical device must exist outside the NSX deployment. This physical device must be attached to a VLAN port matching the VLAN ID of the bridge-backed logical segment.

A regular transport node and a physical device are not mandatory for creating a bridge-backed logical segment. However, if the transport node and physical device are not available, you cannot use the bridge.

The option to add an edge bridge profile is not visible immediately after you create a segment. You must save the configuration and edit it again.

# 6-14 Monitoring the Bridged Traffic Statistics

To monitor the bridged traffic statistics, you expand the bridge-backed segment and then click **VIEW STATISTICS**.





## 6-15 Review of Learner Objectives

- Describe the purpose and function of logical bridging
- Distinguish between routing and bridging
- Create bridge profiles
- Create a bridge-backed segment and bridge traffic between virtual and physical environments

## 6-16 Key Points

- The NSX Edge layer 2 bridge is responsible for bridging traffic between the NSX overlay and VLAN-backed VMs or physical devices outside the NSX deployment.
- With a bridge profile, an NSX Edge cluster can provide layer 2 bridging to a segment.
- The traffic bridged in and out of the NSX domain is subject to the NSX Edge layer 2 bridge firewall.

Questions?



# Module 7

## NSX Firewalls

### 7-2 Importance

NSX includes a distributed firewall and gateway firewall to protect both east-west and north-south traffic. You must understand the architecture and configuration of the NSX firewalls to ensure that your workloads are protected.

### 7-3 Module Lessons

1. NSX Segmentation
2. NSX Distributed Firewall
3. Use Case for Security in Distributed Firewall on VDS
4. NSX Gateway Firewall

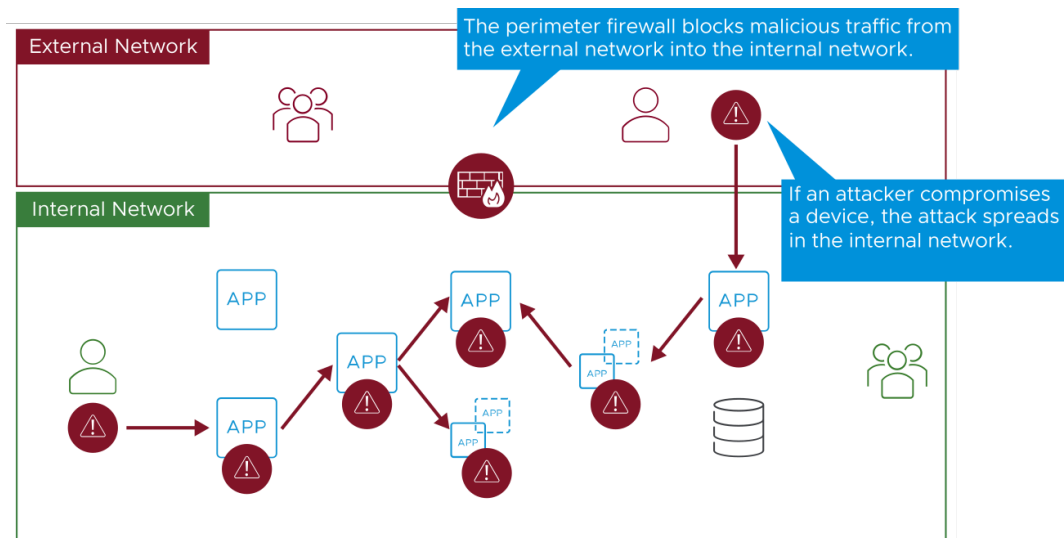
## 7-4 Lesson 1: NSX Segmentation

## 7-5 Learner Objectives

- Define NSX segmentation
- Recognize use cases for NSX segmentation
- Identify steps to enforce Zero-Trust with NSX segmentation

## 7-6 Traditional Security Challenges

The traditional security model assumes that all users and components in an organization's network can be trusted.



The foundation of IT security has remained almost the same for the last 30 years.

Traditional IT security is built on static information:

- If the device joined the domain.
- Whether the user has the correct password.
- Trusted users are within the firewall. Threats and attacks originate outside.

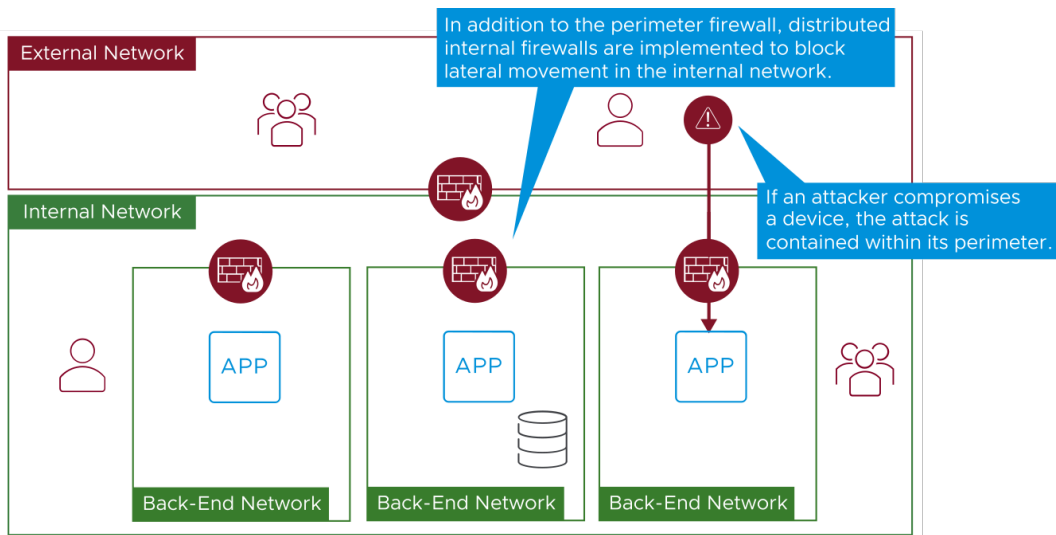
Virtual Private Network (VPN) and Multifactor Authentication (MFA) were introduced later to ensure external protection. But these types of authentication are not enough.

This approach assumes that a user's identity is not compromised and that all users act responsibly and can be trusted.

This traditional perimeter-centric security approach has proven inadequate for protecting modern IT environments.

## 7-7 About Zero-Trust Security

Zero-Trust is a security model that does not automatically trust entities in the security perimeter.



Zero-Trust is a security model that does not automatically trust entities in the security perimeter.

This model emerged to mitigate the increase of network attacks and insider threats that exploit the breaches of a traditional perimeter-centric approach to security.

The rapidly changing work styles and increased use of SaaS applications resulted in Zero-Trust security becoming one of the most important forms of alternative security.

Zero-Trust moves the architecture from a single large DMZ to multiple smaller boundaries around each application and data. If an attacker succeeds in penetrating one of these boundaries, the attacker can only move in that perimeter and be easily contained.

## 7-8 About NSX Segmentation

Segmentation is the process of dividing data center infrastructure into small zones, allowing fine-grain control and inspection of traffic flows.

NSX includes a distributed, scale-out internal firewall that simplifies and automates both macro-segmentation and micro-segmentation:

- Macro-segmentation isolates and secures specific environments.
- Micro-segmentation isolates and secures specific applications in an environment.



Macro-segmentation is also called network segmentation. Macro-segmentation isolates and secures specific environments (virtual zones), such as development and production, from each other. Attackers cannot move laterally between these environments.

Micro-segmentation enables security teams to define and enforce granular controls to the workload level of an application.

## 7-9 Use Cases for NSX Segmentation

NSX segmentation has the following use cases:

- Enforce a Zero-Trust architecture
- Rapidly deploy network segments
- Isolate and secure applications



With NSX, security teams can deploy network segments easily, enable application isolation, and enforce a Zero-Trust architecture with a single solution.

Use cases:

- NSX segmentation enforces a Zero-Trust architecture by creating granular policies between applications, services, and workloads.
- Network segments, virtual security zones, and partner domains are quickly created and configured as they are entirely defined in software. NSX also removes the need to architect the network again and to deploy discrete appliances.
- Critical applications and shared services are protected from being compromised by two mechanisms: discovery of application boundaries using NSX Intelligence and setting up segmentation policies at the application level. NSX also ensures that policies stay up to date as applications evolve or move.

## 7-10 NSX Segmentation Benefits

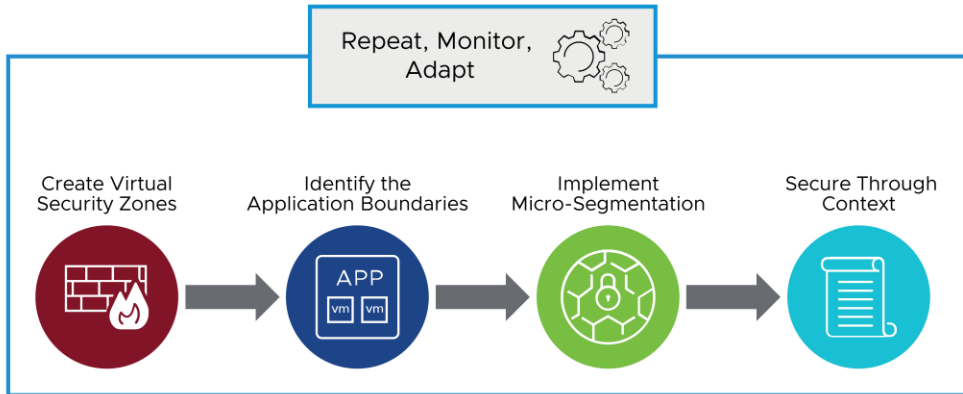
NSX Segmentation offers key business and functional benefits:

- Limits lateral movement within the data center
- Minimizes risks and the effect of security breaches
- Simplifies network traffic flows
- Uses the existing underlay network infrastructure
- Lowers capital expenditure and operating expenses
- Automates IT service delivery
- Securely enables business agility



## 7-11 Enforcing Zero-Trust with NSX Segmentation

NSX segmentation helps build a Zero-Trust approach to security by defining a security perimeter around each application.



NSX improves the security of today's modern workloads by preventing lateral movement using network segmentation. It is distributed, application-aware, and simple to operate.

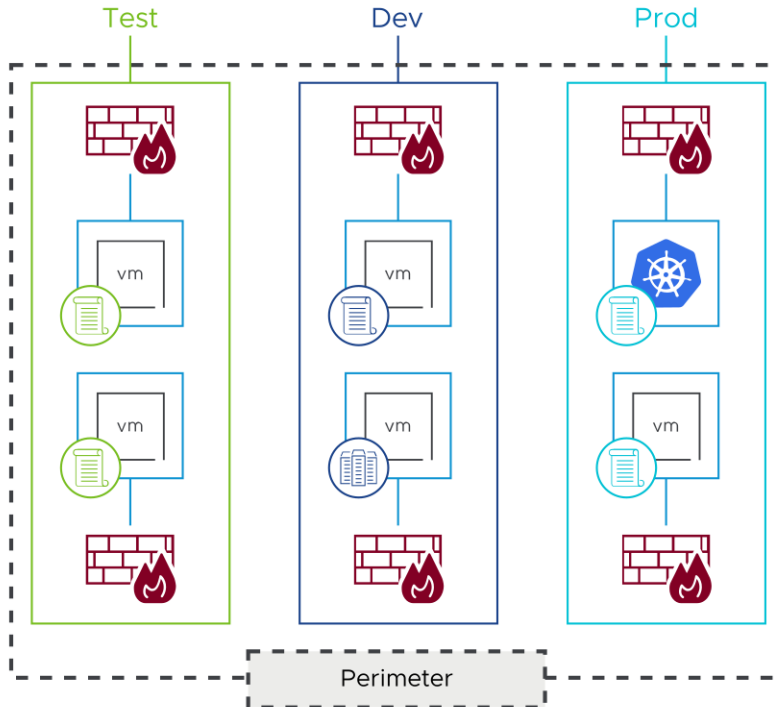
Follow this process to secure a data center environment with NSX segmentation:

1. Apply macro-segmentation to define virtual security zones.
2. In those security zones, identify the assets (understand the application behavior and network flows).
3. Implement micro-segmentation to secure every application.
4. Implement contextual security policies.

You must always monitor the environment for changes or unexpected behavior and adapt the security policies.

## 7-12 Step 1: Creating Virtual Security Zones

Protect segments of the network by creating virtual security zones.



Using macro-segmentation to isolate environments improves the security of the data center. It prevents lateral movement between virtual zones.

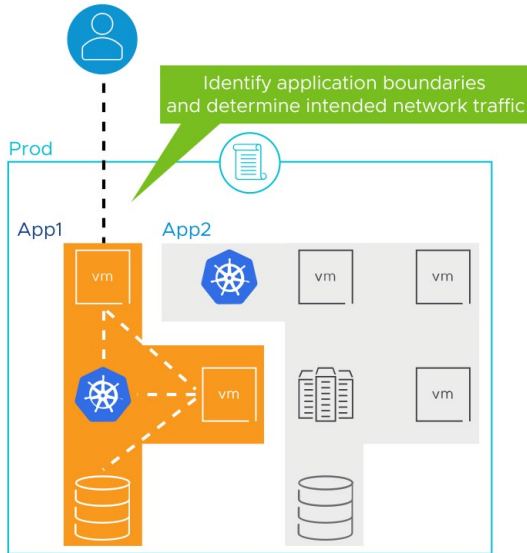
Depending on their business structure and use cases, a security team typically chooses to segment environments that should not be able to directly communicate with each other. Examples include different business units (such as HR, Finance, and so on), partner environment, and production environments.

Macro-segmentation provides a more flexible solution compared to a traditional appliance-based firewall. It enables organizations to easily expand the number of zones needed and adapts easily to changing network and security requirements as the business evolves.

Macro-segmentation is the first step to the Zero-Trust journey. It starts defining security zones in the data center environment that will be further secured.

## 7-13 Step 2: Identifying the Application Boundaries

Identify the virtual machines and containers used by an application and the network traffic that is necessary for the application to function.



When the network is macro-segmented into virtual security zones, you can move to micro-segmentation and secure applications in a virtual zone.

Before implementing micro-segmentation, assets must be identified:

- Define the application boundaries by identifying the VMs and containers that an application is using. Also, define the data, assets, applications, and services that need protection, such as:
  - Data: Credit Card Information, Protected Health Information (PHI), Personally Identifiable Information (PII), Intellectual Property
  - Assets: Point-of-sales terminals, manufacturing assets, IoT devices
  - Applications: Custom or off-the-shelf software
  - Services: DNS, DHCP, Active Directory, LDAP, and so on

- Identify how the traffic moves across the organization in relation to the previously defined boundaries.

You must look for the following types of traffic:

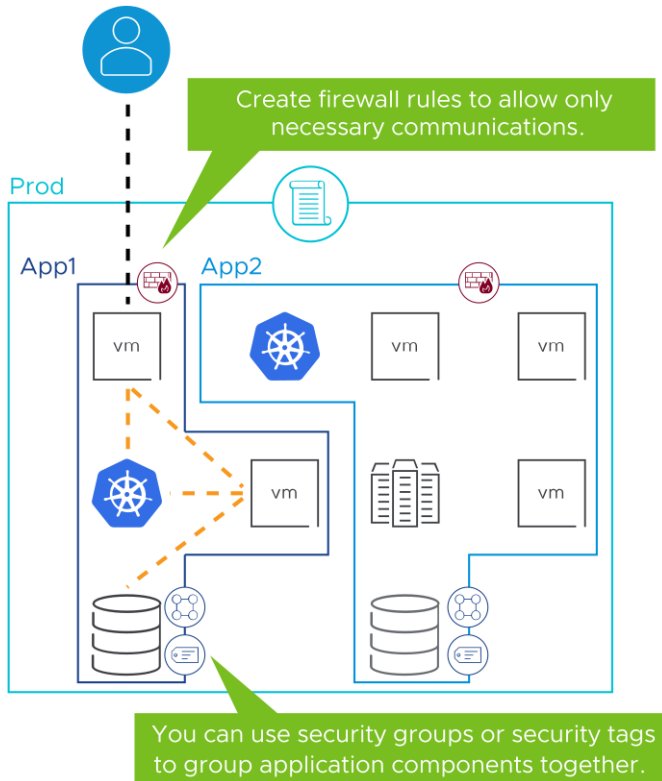
- External application traffic: Which user is connecting to the app, which shared services the application is using, and so on
- Internal application traffic: Communication between the different application components

A good understanding of the application footprint and the network traffic is the only way to determine and enforce policies that secure access to the data.

This identification process is tedious and time-consuming when performed manually. NSX Intelligence or VMware Aria Operations for Networks can be used to automate the discovery of the application boundaries.

## 7-14 Step 3: Implementing Micro-Segmentation

Use micro-segmentation to allow necessary network traffic.



After the application's composition and necessary network traffic are identified, firewall rules must be configured to allow the necessary network traffic.

NSX Distributed Firewall enables users to configure firewall rules from a single point, which are then pushed to all hosts that participate in the NSX network. The creation of rules can be automated with NSX Intelligence. NSX Intelligence can recommend distributed firewall rules based on the discovered traffic flows in the environment.

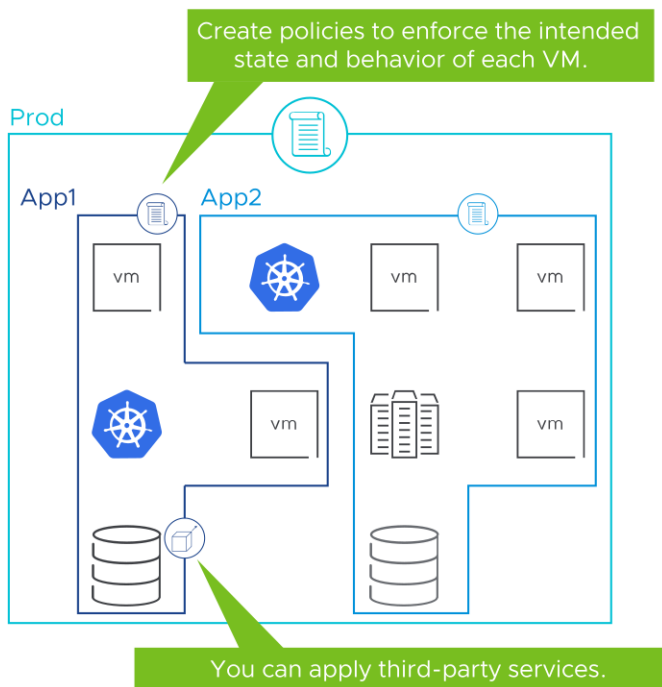
Micro-segmenting the network immediately reduces the attack surface of an application. It restricts the application to only communicate with the resources that it absolutely needs.

In this process, security tags and security groups can be used:

- Security tags enable labeling NSX objects.
- Security groups include different objects that are added both statically and dynamically and can be used as the source and destination of a firewall rule. Security groups can use security tags or other criteria (such as IP sets, MAC sets, segment ports, AD user groups, and so on) to group virtual machines together.

## 7-15 Step 4: Securing Through Context

Set up security policies to establish the behavior of virtual machines and containers.



This step secures the traffic and the context of the application by setting up policies based on the behavior of virtual machines and containers.

Security groups and tags can be used.

In the example, a security administrator wants to create a firewall policy to restrict network access to VMs with an earlier version of Windows:

1. Tag VMs with the OS version used.
2. Create a security group that gathers all VMs that do not match the OS version threshold.
3. Create a security policy to restrict access to the members of that security group.

When a VM is created and does not meet the OS version criteria, it is automatically put in that security group and blocked by the firewall rule. This approach removes the need for checking each VMs individually.

Third-party services can be integrated to create more granular control. For more information about a list of NSX partners, see NSX Data Center Technology Partners at <https://www.vmware.com/products/nsx/technology-partners.html>.

## 7-16 Review of Learner Objectives

- Define NSX segmentation
- Recognize use cases for NSX segmentation
- Identify steps to enforce Zero-Trust with NSX segmentation

## 7-17 Lesson 2: NSX Distributed Firewall

### 7-18 Learner Objectives

- Identify types of firewalls in NSX
- Describe features of distributed firewalls
- Create firewall policies
- Configure firewall rules
- Configure firewall rule attributes: groups, services, and profiles
- Configure the distributed firewall to block malicious IPs
- Save, roll back, export, and import the distributed firewall configuration
- Describe the distributed firewall architecture



## 7-19 NSX Firewalls

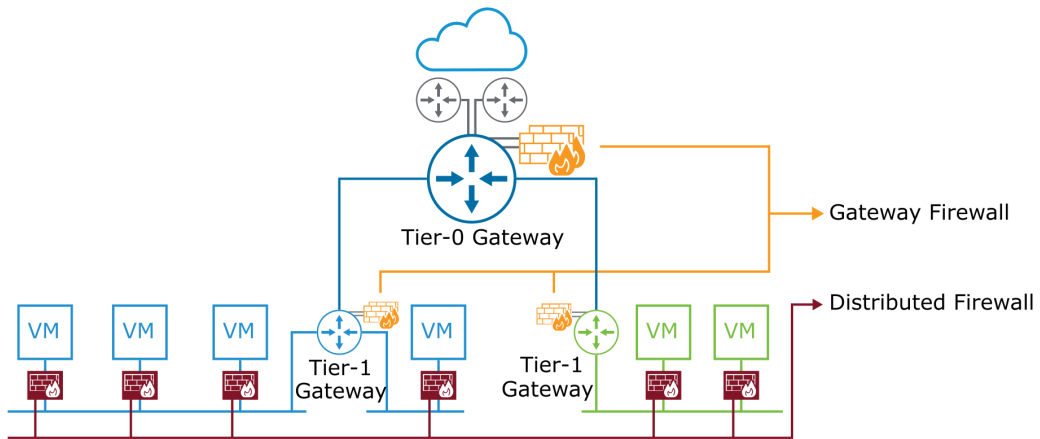
NSX includes the distributed firewall (east-west) and the gateway firewall (north-south).

The distributed firewall is a hypervisor, kernel-embedded stateful firewall:

- It resides in the kernel of the hypervisor and outside the guest OS of the VM.
- It controls the I/O path to and from the vNIC.

The gateway firewall is used for north-south traffic between the NSX gateways and the physical network:

- It applies to Tier-0 and Tier-1 gateway uplinks and service interfaces.
- It is a centralized stateful service enforced on the NSX Edge node.



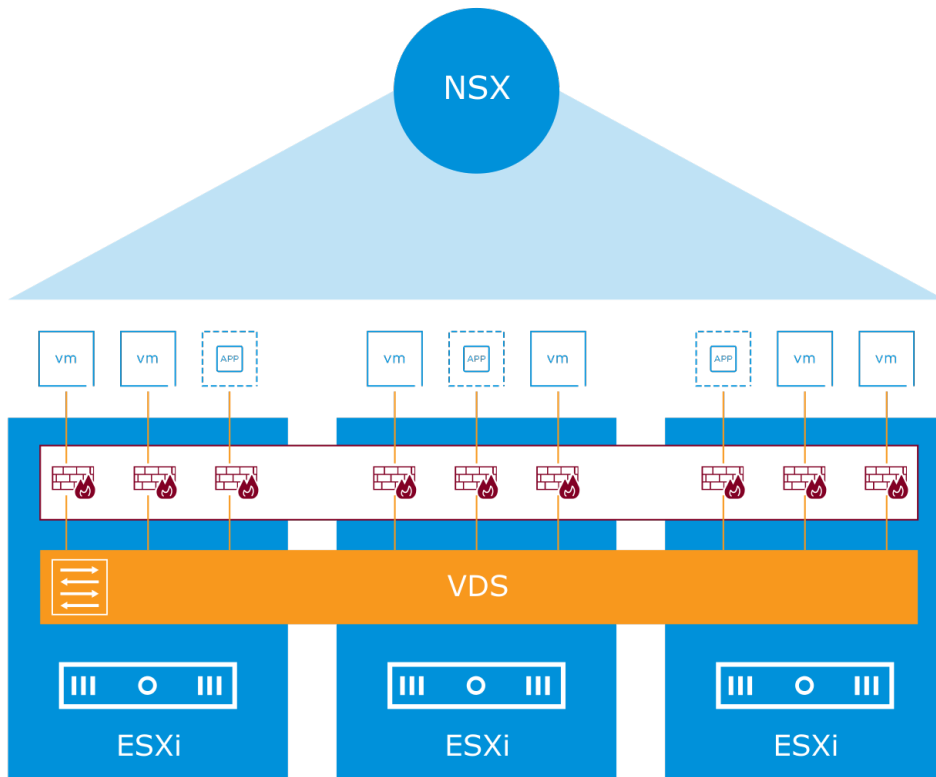
The gateway firewall can be used as perimeter, intertenant, or interzone firewall.

## 7-20 Features of the Distributed Firewall

The distributed firewall provides visibility and control for virtualized workloads and networks.

The distributed firewall has the following main features:

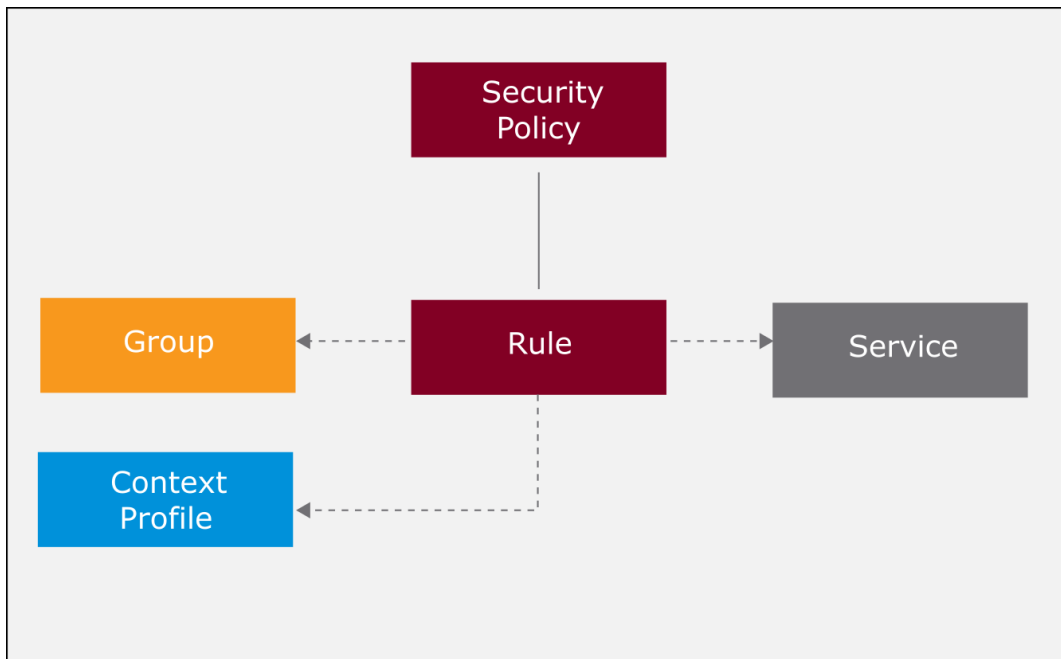
- Centralized configuration through the NSX UI or API
- Layer 2 stateless firewall rules
- Layer 3 stateless and stateful firewall rules
- Context-aware (layer 7) firewall rules
- Identity Firewall for Windows workloads
- FQDN Filtering
- Blocking Malicious IPs
- Time-based policies



## 7-21 Distributed Firewall: Key Concepts

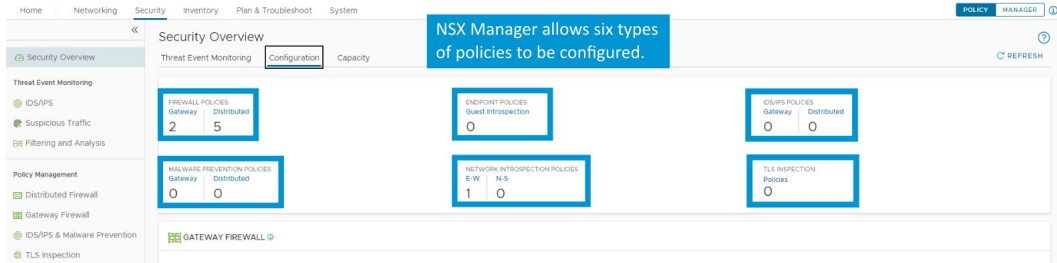
Several key concepts apply to distributed firewalls:

- Security policy: A collection of firewall rules and service configurations.
- Firewall rule: A set of instructions that determine whether a packet should be allowed or blocked.
- Group: A construct with multiple objects statically or dynamically pooled together.
- Service: Defines a port and protocol combination and is used to specify the type of traffic to be blocked or allowed in firewall rules.
- Context profile: Inspects the layer 7 content of the packets to allow or deny them.



## 7-22 Overview of a Security Policy

A security policy is a collection of firewall rules. You can configure different types of security policies from the NSX UI.



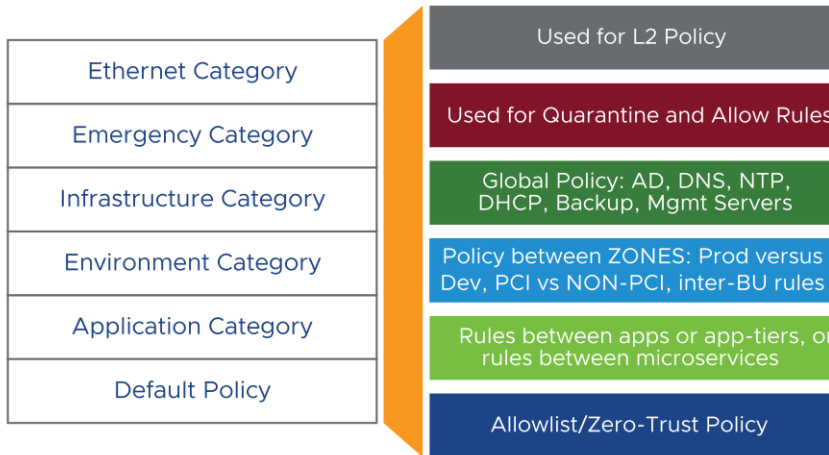
The NSX UI enables you to configure several types of policies:

- Firewall policies: Used for configuring firewall rules to control north-south and east-west traffic.
- Endpoint policies: Used for configuring Guest Introspection services and rules.
- IDS/IPS policies: You can use these policies to define Intrusion Detection and Prevention rules for east-west and north-south traffic.
- Malware Prevention policies: You can use these policies to define anti-malware rules for east-west and north-south traffic.
- Network Introspection policies: Used for configuring north-south and east-west traffic redirection rules.
- TLS Inspection: Used for configuring TLS Inspection rules for the north-south traffic.

## 7-23 Distributed Firewall Policy Categories

A Distributed Firewall policy is a collection of firewall rules applied to east-west traffic.

The NSX UI enables you to group distributed firewall policies into different categories.



The categories for distributed firewall rules include:

- Ethernet: All layer 2 policies. Layer 2 firewall rules are always evaluated before layer 3 rules.
- Emergency: Temporary firewall policies needed in emergency situations, such as blocking an attacker from attacking a web server.
- Infrastructure: Nonapplication policies specific to infrastructure components, such as AD, DNS, NTP, and so on.
- Environment: High-level policy groupings, for example, the production group cannot communicate with the testing group, or the testing group cannot communicate with the development group.
- Application: Specific and granular application policy rules, such as rules between applications or application tiers, or rules between microservices.
  - Application tiers: In a multitier application, the functionality of the application is separated into isolated functional areas, called application tiers.
  - Microservices: It is an architectural style that structures an application as a collection of services that are independently deployable.

Each of these categories has its own policies and rules. Firewall rules are enforced left to right and top to bottom across these categories.

You can reorder policies and rules in a specific category. However, you cannot move policies or rules across different categories.

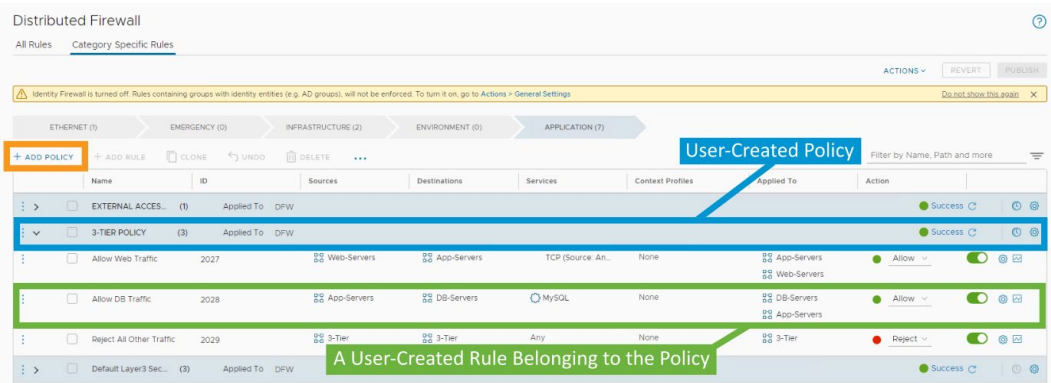
You can configure policies and rules under relevant categories.

## 7-24 About Distributed Firewall Policies

A firewall policy includes one or more firewall rules, which contain specific instructions for managing various types of traffic.

A policy can contain stateful or stateless rules for enforcement.

Policies are enforced in a top-to-bottom order.



In a firewall policy, each firewall rule contains instructions that determine the following factors:

- Source and destination for the packet
- Whether a packet should be allowed or blocked
- Protocols that the packet can use
- Ports that the packet can use

Policies are used for multitennancy, such as creating specific rules for sales and engineering departments in separate policies.

A policy can be defined as enforcing stateful or stateless rules. Stateless rules are treated as traditional stateless access-control lists (ACLs).

## 7-25 Distributed Firewall Rule Processing within a Policy

Firewall rules are processed in a top-to-bottom order:

- You can move rules up and down within a policy.
- The first match triggers rule enforcement.
- Packets that do not match any other rule are matched by the default rule.

Distributed Firewall

All Rules Category Specific Rules

ACTIONS REVERT PUBLISH

Warning: Identity Firewall is turned off. Rules containing groups with identity entities (e.g. AD groups), will not be enforced. To turn it on, go to Actions > General Settings. Do not show this path X

ETHERNET (1) EMERGENCY (0) INFRASTRUCTURE (2) ENVIRONMENT (0) APPLICATION (7)

+ ADD POLICY + ADD RULE CLONE UNDO DELETE ... Filter by Name, Path and more

Name	ID	Applied To	Sources	Destinations	Services	Context Profiles	Applied To	Action
EXTERNAL ACCESS...	(1)	Applied To DFW						Success
3-TIER POLICY	(3)	Applied To DFW						Success
Allow Web Traffic	2027		Web-Servers	App-Servers	TCP (Source An...	None	App-Servers Web-Servers	Allow
Allow DB Traffic	2028		App-Servers	DB-Servers	MySQL	None	DB-Servers App-Servers	Allow
Reject All Other Traffic	2029		3-Tier					Allow
Default Layer3 Sec...	(3)	Applied To DFW						Success
Default Rule NDP	3		Any					Allow
Default Rule DHCP	4		Any		DHCP-Server DHCP-Client	None	DFW	Allow
Default Layer3 Rule	2		Any	Any	Any	None	DFW	Allow

Firewall rules are enforced in the following ways:

- Like firewall policies, firewall rules are processed in the top-to-bottom order.
- Each packet is checked against the top rule in the rule table before moving down the subsequent rules in the table.
- The first rule in the table that matches the traffic parameters is enforced. Subsequent rules cannot be enforced because the search is terminated for that packet.

Because of this behavior, you must place the most granular policies at the top of the rule table.

Packets not matching other rules are enforced by the default rule. The default rule is originally set to the Allow action. This rule ensures that VM-to-VM communication is not broken during staging or migration phases. To implement a Zero-Trust model where only the specified traffic is allowed, the action for the default rule should be changed to block, and firewall policies defined to specify all traffic to be allowed.

## 7-26 Applied To Field for the Policy

When creating a Distributed Firewall policy, you can define the scope of the policy. It can be the full DFW or a specific security group.

The screenshot shows the 'Distributed Firewall' configuration page. At the top, there's a warning banner: 'Identity Firewall is turned off. Rules containing groups with identity entities (e.g. AD groups), will not be enforced. To turn it on, go to Actions > General Settings'. Below this, a breadcrumb trail shows categories: ETHERNET (1), EMERGENCY (0), INFRASTRUCTURE (2), ENVIRONMENT (0), and APPLICATION (7). The main table lists firewall rules. The 'Applied To' column is highlighted with an orange box. The first rule, 'EXTERNAL ACCES...', has 'Applied To' set to 'DFW'. The second rule, '3-TIER POLICY', also has 'Applied To' set to 'DFW'. Other rules like 'Allow Web Traffic' and 'Allow DB Traffic' have 'Applied To' set to 'App-Servers'. The 'Action' column shows 'Success' for most rules, and 'Reject' for 'Reject All Other Traffic'.

Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action
EXTERNAL ACCES... (1)						DFW	Success
3-TIER POLICY (3)						DFW	Success
Allow Web Traffic	2027	Web-Servers	App-Servers	TCP (Source An...	None	App-Servers Web-Servers	Allow
Allow DB Traffic	2028	App-Servers	DB-Servers	MySQL	None	DB-Servers App-Servers	Allow
Reject All Other Traffic	2029	3-Tier	3-Tier	Any	None	3-Tier	Reject
Default Layer3 Sec... (3)						DFW	Success

The Applied To field configured at the policy level overrides the Applied To field configured at the rules within it. You must configure the Applied To field either at the policy level or at the rule level, but not at both levels. For more granularity, consider configuring the Applied To field at the rule level.



## 7-27 Configuring Distributed Firewall Policy Settings

When creating a Distributed Firewall policy, you specify settings such as TCP Strict, Stateful, and Locked.

The screenshot shows the 'Distributed Firewall' configuration interface. A 'Settings' dialog box is open, titled 'Policy > 3-TIER POLICY'. It contains three settings: 'TCP Strict' (set to 'Yes'), 'Stateful' (set to 'Yes'), and 'Locked' (set to 'No'). Each setting has a help icon (i). Three callout boxes provide detailed explanations:

- TCP Strict:** If it is enabled on a section and a packet matches a rule in it, the packet is dropped if the packet does not belong to an existing session and the SYN flag of the packet is not set in the kernel.
- Stateful:** The distributed firewall performs stateful packet inspection and tracks the state of network connections. Packets matching a known active connection are allowed. Packets that do not match are inspected against the firewall rules.
- Locked:** This setting allows you to lock a policy while making configuration changes so that other users cannot make simultaneous modifications.

The background shows a list of firewall rules with columns for Name, ID, Applied To, and Sources. Rules include 'EXTERNAL ACCESS...', 'Default Layer3 Sec...', and '3-Tier'. The bottom right shows a 'Success' message and 'CANCEL'/'APPLY' buttons.

## 7-28 Configuring Time-Based Firewall Policies

You can configure security policies that are only valid for a specific period. You can specify the following parameters in the Time Window:

- Name
- Time zone (UTC or local to transport node)
- Frequency (weekly or one time)
- Recurring days
- Start and end date
- Start and end time

The screenshot displays the 'Distributed Firewall' configuration page. A 'Time Window' dialog box is open, allowing users to configure time-based rules. The dialog includes fields for Name, Time Zone (set to UTC), Frequency (set to WEEKLY), and Time Window (set to Every MON, TUE, WED, THU, FRI, SAT). It also features 'Starting On' and 'Ending On' date pickers, and 'From' and 'Till' time pickers. A note at the bottom states: 'Note: Please take into account the time difference between the configured and the local time zone on Transport Node.' The background shows a list of firewall rules, including 'EXTERNAL ACCESS...', '3-TIER POLICY', 'Allow Web Traffic', 'Allow DB Traffic', 'Reject All Other Traffic', and 'Default Layer3 Sec...'. A blue arrow points from the 'Time Window' dialog to the 'Success' status of a rule in the background.

The From and Till parameters must be configured in 30-minute increments. For example, from 09:00 to 09:30 is a valid configuration. However, if a user configures an interval from 09:15 to 09:45, a configuration error appears in the UI.

Before configuring a time-based rule, you must configure NTP servers for the transport nodes.

## 7-29 Creating Distributed Firewall Rules

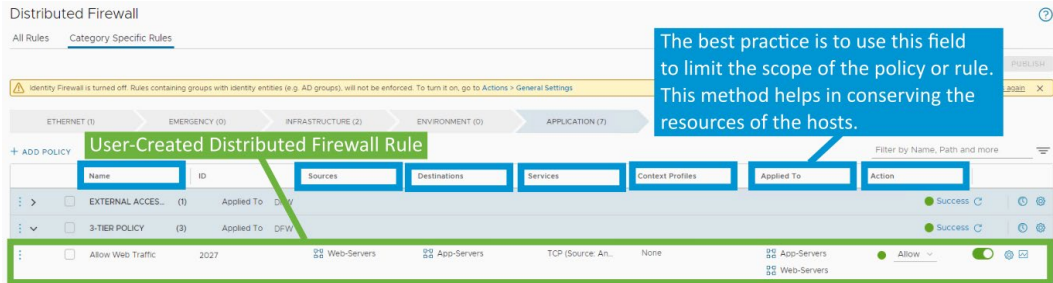
Rules are a set of criteria used to evaluate traffic flows. They contain instructions that determine whether a packet should be allowed, dropped, or rejected.

The screenshot displays the 'Distributed Firewall' configuration page. At the top, there are tabs for 'All Rules' and 'Category Specific Rules'. A yellow warning banner states: 'Identity Firewall is turned off. Rules containing groups with identity entities (e.g. AD groups), will not be enforced. To turn it on, go to Actions > General Settings'. Below this, a breadcrumb trail shows categories: ETHERNET (1), EMERGENCY (0), INFRASTRUCTURE (2), ENVIRONMENT (0), and APPLICATION (7). A toolbar includes '+ ADD POLICY', '+ ADD RULE', 'CLONE', 'UNDO', 'DELETE', and a filter icon. The main table lists firewall rules with columns for Name, ID, Applied To, Sources, Destinations, Services, Context Profiles, Applied To, and Action. A context menu is open over the 'Add Rule' button, showing options: 'Enable Logging For All Rules', 'Disable Logging For All Rules', 'Enable All Rules', 'Disable All Rules', 'Delete Policy', 'Add Rule' (highlighted with a green box), 'Add Policy Above', 'Add Policy Below', and 'Copy Path to Clipboard'. A green callout box points to the 'Add Rule' option with the text: 'Add rules to the Distributed Firewall policy.'

Name	ID	Applied To	Sources	Destinations	Services	Context Profiles	Applied To	Action
EXTERNAL ACCESS...	(1)	Applied To: DFW						Success
Enable Logging For All Rules		Applied To: DFW						Success
2027		Applied To: DFW	Web-Servers	App-Servers	TCP (Source An..	None	App-Servers	Allow
2028		Applied To: DFW	App-Servers	DB-Servers	MySQL	None	DB-Servers	Allow
2029		Applied To: DFW	3-Tier	3-Tier	Any	None	3-Tier	Reject

## 7-30 Configuring Distributed Firewall Rule Parameters

A distributed firewall rule includes parameters such as source, destination, service, and context profile. This rule defines the scope where the rules should be applied to and the action that should be taken on a rule match. It also provides an option of logging when the traffic matches a rule.



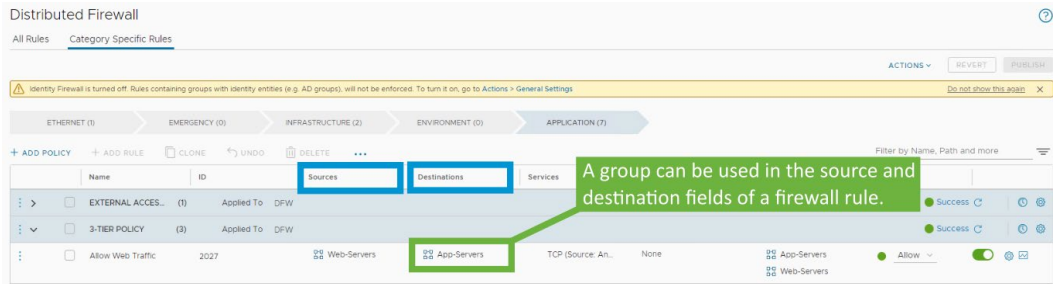
Several parameters can be defined when configuring a distributed firewall rule:

- **Name:** You can specify a name for the rule.
- **Sources:** You can use previously defined groups.
- **Destinations:** You can use previously defined groups.
- **Services:** You can specify a port and protocol combination.
- **Context Profiles:** You use context profiles to define context-aware or layer 7 rules.
- **Applied To:** Defines the scope of the rule. It can be the full DFW or a specific security group.
- **Action:** You can select from the following firewall rule actions:
  - **Allow**
  - **Drop**
  - **Reject**
- **ID:** NSX Manager automatically assigns an ID to a rule when it is created. The ID can be used for troubleshooting. A user cannot modify the ID.

The order of firewall rules determines how the traffic is managed. You can drag the rules in the UI to change the order.

## 7-31 Specifying Sources and Destinations for a Rule

When specifying sources and destinations for a firewall rule, you can use an IP or MAC address or an object (such as a group). If you do not specify these parameters, they match **Any**.

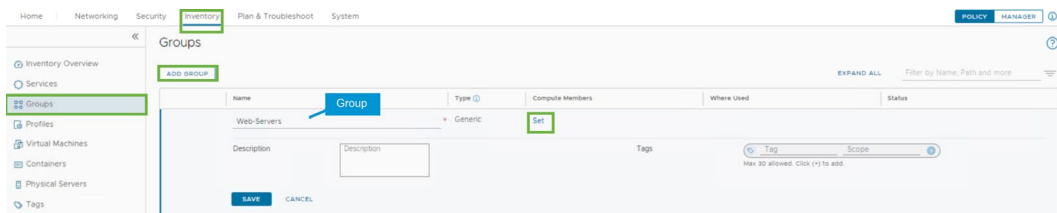


Both IPv4 and IPv6 addresses are supported for sources and destinations options of the firewall rule. Multicast addresses are also supported.

## 7-32 Creating Groups

A group defines a collection of assets on which security policies and rules can be applied.

A group can contain VMs, VIFs, segments, segment ports, IP and MAC addresses, AD user groups, and physical servers.



Before creating a group that includes AD users, you must add an AD domain to NSX Manager. You add this domain through the NSX UI by navigating to **System > Configuration > Identity Firewall AD > ADD ACTIVE DIRECTORY**.

The main use case for creating a group that includes AD users is to configure identity-based firewall rules.

# 7-33 Adding Members and Member Criteria for a Group

Groups can be defined by using dynamic or static membership criteria:

- Dynamic group inclusion for VMs can be based on tags, machine names, OS names, or computer names.
- Static group inclusion criteria apply to VMs, VIFs, segments, segment ports, IP sets, MAC sets, AD user groups, physical servers, and nested groups.

Set Members | Web-Servers

Dynamic Group Inclusion

To add compute members to a Group, you can statically or dynamically add members to a group.

Group Type (0)

Dynamic

IP Addresses Only

Membership Criteria (1)

Members (0)

IP Addresses (0)

MAC Addresses (0)

AD Groups (0)

ADD CRITERION

LEARN MORE ABOUT MEMBERSHIP CRITERIA

Criterion 1

Virtual Machine

Tag

Equals

web

Scope

Equals

Is set

Set Members | Web-Servers

Static Group Inclusion

To add compute members to a Group, you can statically or dynamically add members to a group.

Group Type (0)

Static

IP Addresses Only

Membership Criteria (1)

Members (0)

IP Addresses (0)

MAC Addresses (0)

AD Groups (0)

Category

Virtual Machines (0)

IP Sets (0)

MAC Sets (0)

Segment Ports (0)

Distributed Port Groups (0)

Distributed Ports (0)

VIFs (0)

Virtual Machines (0)

Physical Servers (0)

	Source	Tags	Operating System	Power State	Virtual Interface
<input type="checkbox"/>	sa-ess1-02 vclass.local	1	VMware Photon OS (64-bit)	Running	<a href="#">VIEW DETAILS</a>
<input type="checkbox"/>	sa-ess1-02 vclass.local	1	VMware Photon OS (64-bit)	Running	<a href="#">VIEW DETAILS</a>
<input type="checkbox"/>	sa-patchvm-01	0	Ubuntu Linux (64-bit)	Running	<a href="#">VIEW DETAILS</a>
<input type="checkbox"/>	sa-fiscient-01	0	Ubuntu Linux (64-bit)	Running	<a href="#">VIEW DETAILS</a>

350

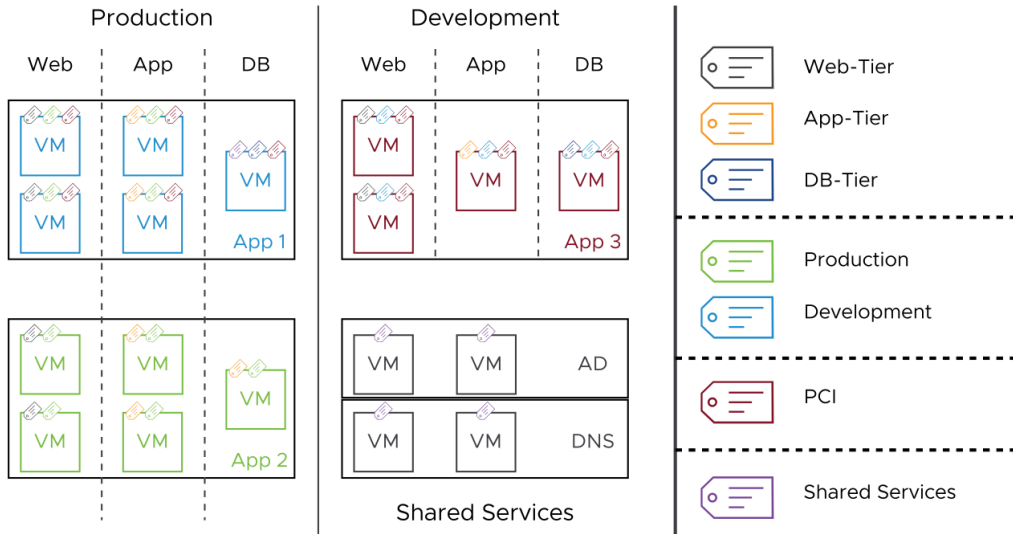
Technet24

## 7-34 Creating Groups Based on Tags

Tags are typically used to automate security policy enforcement for new applications being provisioned.

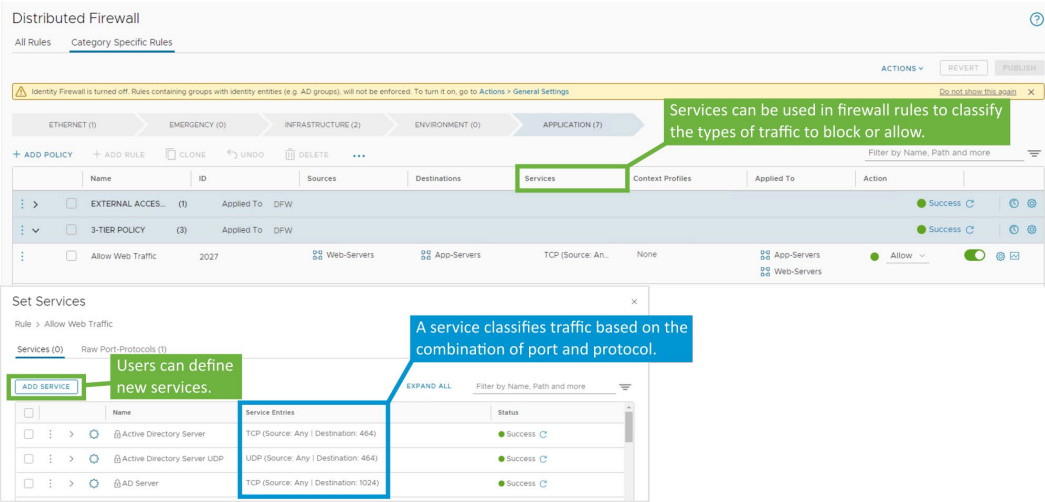
Security administrators can assign one or multiple tags to workloads based on a given criteria.

These tags can then be used to create dynamic security groups for use in firewall rules.



# 7-35 Specifying Services for a Rule

When configuring distributed firewall rules, you specify one or more services. Services contain the port and protocol definition for network traffic.



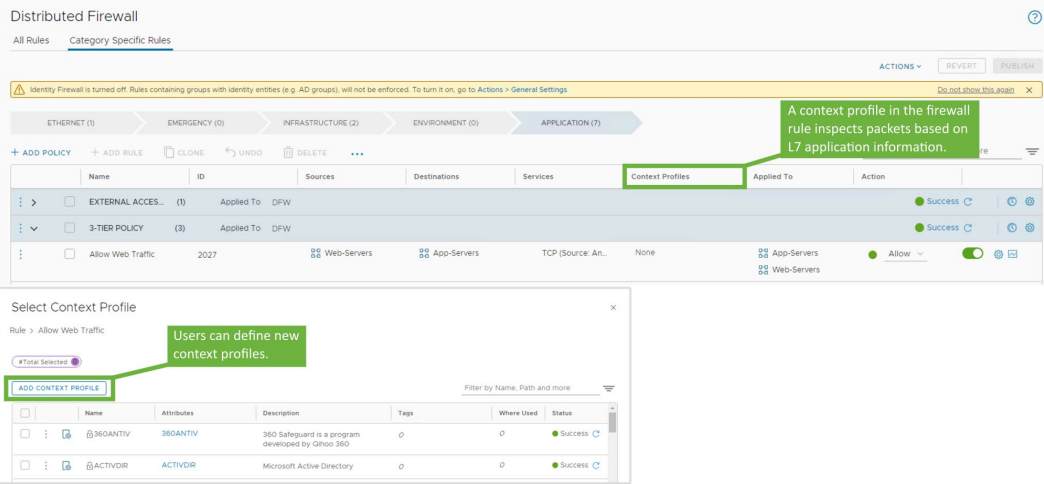
NSX includes an extensive list of predefined services. You cannot modify or delete these services. However, you can create additional services to meet your communication requirements.

You can create a service while configuring a distributed firewall rule. Alternatively, you can create additional services by navigating to **Inventory > Services > ADD SERVICE**.



# 7-36 Adding a Context Profile to a Rule

You can apply a context profile to a distributed firewall rule to enable a layer 7 firewall.

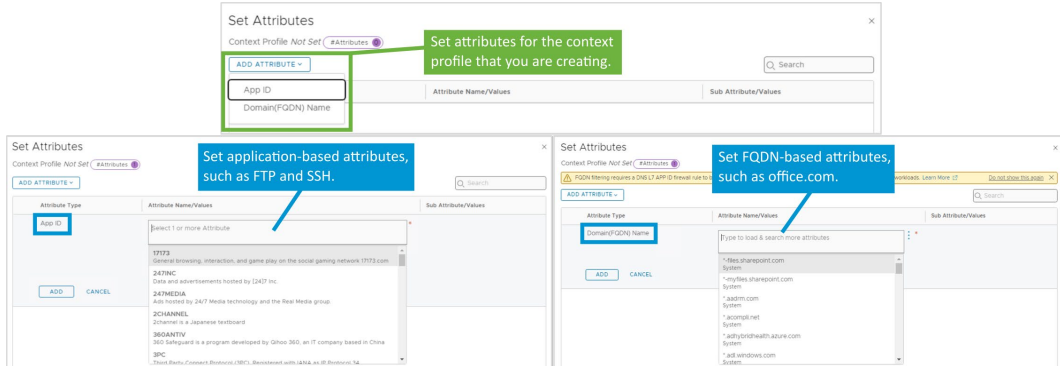


NSX Manager includes a list of predefined context profiles. You can also configure custom context profiles for your firewall rules. Layer 7 firewall rules can be defined only in a stateful firewall policy.

Alternatively, you can create context profiles by navigating to **Inventory > Profiles > Profiles > Context Profiles > ADD CONTEXT PROFILE**.

## 7-37 Configuring Context Profile Attributes

When creating a context profile for a distributed firewall rule, you configure two attributes: domain name and application ID.



A context profile defines context-aware attributes, including application ID, domain name, and subattributes such as application version or cipher set.

Context profiles for distributed firewall rules include the following main attributes:

- **DOMAIN\_NAME:** You can choose from a static list of fully qualified domain names (FQDNs) or add your own FQDN.
- **APP\_ID:** You can choose from a list of preconfigured applications. You cannot add applications. Examples include FTP, SSH, and SSL. Certain applications allow users to specify subattributes. For example, when choosing SSL Application, you can specify the TLS\_VERSION and the TLS\_CIPHER\_SUITE. For CIFS, you can specify the SMB\_VERSION.

## 7-38 Custom FQDN Filtering

You can add your own fully qualified domain name (FQDN) for custom filtering.

**Set Attributes**

Context Profile *Not Set* #Attributes 1

**ADD ATTRIBUTE** Search

Attribute Type	Attribute Name/Values	Sub Attribute/Values
Domain(FQDN) Name	Type to load & search more attributes	

**ADD** **CANCEL** **Add FQDN**

**Add FQDN**

Enter your own Custom Domain Name

FQDN	Created By	Where Used
Enter FQDN	User	

**CANCEL** **SAVE**

Alternatively, you can create context profiles by navigating to **Inventory > Profiles > Attribute Types > FQDNs > ACTIONS > Add FQDN**.

# 7-39 Setting the Scope of Rule Enforcement

The Applied To attribute optimizes the resource utilization on the ESXi hosts. It also helps in defining targeted policies at specific zones or tenants without affecting the policy defined on other zones or tenants.

Distributed Firewall

All RulesCategory Specific Rules

Identity Firewall is turned off. Rules containing groups with identity entries (e.g. AD groups), will not be enforced. To turn it on, go to Actions > General Settings.

ETHERNET (1)EMERGENCY (0)INFRASTRUCTURE (2)ENVIRONMENT (0)APPLICATION (8)

+ ADD POLICY+ ADD RULECLONEUNDODELETE...

Name	ID	Applied To	Sources	Destinations	Services	Context Profiles	Applied To	Action
EXTERNAL ACCESS PO...	(1)	Applied To	DFW					Success
3-TIER POLICY	(4)	Applied To	DFW					Success
Allow Web Traffic	2027		Web-Servers	App-Servers	TCP(Source Any I D...	None	App-ServersWeb-Servers	Allow
Allow DB Traffic	2028		App-Servers	DB-Servers	MySQL	None	DB-ServersApp-Servers	Allow
Allow SSH	2030		3-Tier				DFW	Allow
Reject All Other Traffic	2029		3-Tier				3-Tier	Reject
Default Layer3 Section	(3)	Applied To	DFW					Success

Filter by Name, Path and more

The Applied To attribute defines the scope of enforcement per rule.

You can apply rules to the distributed firewall or groups.

The appropriate use of the Applied To field is paramount to optimize resource utilization on the transport nodes and to avoid scalability issues. You must configure the Applied To field in a distributed firewall rule to match the security groups used as the source and destination.

Zones can be compared to departments in an organization, whereas tenants can be compared to different organizations managed by a service provider. In the NSX UI, you can create groups to represent zones or tenants.

356

Technet24

## 7-40 Specifying the Action for a Rule

You configure the following actions in a distributed firewall rule:

- Allow: Allows all traffic with the specified source, destination, and protocol.
- Drop: Drops packets with the specified source, destination, and protocol. Dropping a packet is a silent action with no notification to the source and destination systems.
- Reject: Rejects packets with the specified source, destination, and protocol. Rejecting a packet is a more graceful way to deny a packet, because it sends a destination unreachable message to the sender.

Distributed Firewall

All Rules Category Specific Rules

ACTIONS ▾ REVERT PUBLISH

⚠ Identity Firewall is turned off. Rules containing groups with identity entities (e.g. AD groups), will not be enforced. To turn it on, go to Actions > General Settings Do not show this again X

ETHERNET (1) EMERGENCY (0) INFRASTRUCTURE (2) ENVIRONMENT (0) APPLICATION (7)

+ ADD POLICY + ADD RULE CLONE UNDO DELETE ... Filter by Name, Path and more

	Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action
>	EXTERNAL A...	(1)	Applied To	DFW				Success
▼	3-TIER POLICY	(3)	Applied To	DFW				Success
	Allow Web Tra...	2027	Web-Se...	App-Ser...	TCP (So...	None	App-Ser... Web-Se...	Allow <input checked="" type="checkbox"/> Drop <input type="checkbox"/> Reject <input type="checkbox"/>
	Allow DB Traffic	2028	App-Ser...	DB-Serv...	MySQL	None	DB-Serv... App-Ser...	<input checked="" type="checkbox"/> Drop <input type="checkbox"/> Reject <input type="checkbox"/>
	Reject All Othe...	2029	3-Tier	3-Tier	Any	None	3-Tier	Reject <input checked="" type="checkbox"/> Drop <input type="checkbox"/> Allow <input type="checkbox"/>
>	Default Layer...	(3)	Applied To	DFW				Success

## 7-41 Distributed Firewall Rule Settings

You configure distributed firewall rules settings, such as logging, direction, and IP protocol.

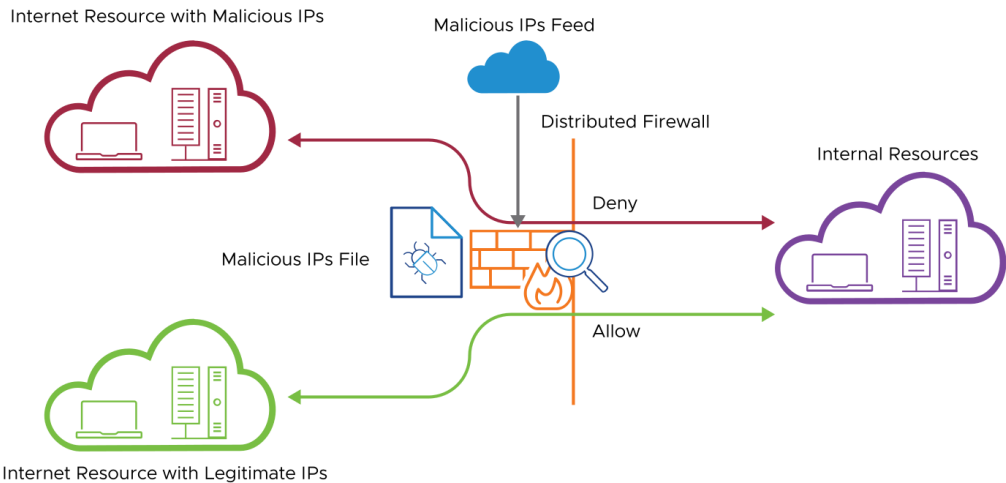
The screenshot shows the 'Distributed Firewall' management console. A table lists firewall rules, including 'Allow Web Traffic' (ID 2027) and 'Allow DB Traffic' (ID 2028). A 'Settings' dialog box is open for the 'Allow Web Traffic' rule. The dialog has tabs for 'Rule' and 'Settings'. The 'Settings' tab is active, showing options for 'Logging' (a toggle switch set to 'Disable'), 'Direction' (a dropdown menu set to 'In-Out'), 'IP Protocol' (radio buttons for 'IPv4', 'IPv6', and 'IPv4-IPv6', with 'IPv4-IPv6' selected), 'Log Label' (a text input field), and 'Comments' (a text area). A blue callout box points to the 'Logging' toggle with the text: 'Logging can be turned off or on. Logs are stored in the /var/log/dfwpktlogs.log file on ESXi hosts.' A green callout box points to the 'Direction' dropdown with the text: 'Matches the direction of a packet as it traverses the network.' A grey callout box points to the 'IP Protocol' radio buttons with the text: 'Matches the direction of a packet as it traverses the network.'

You can configure several settings for distributed firewall rules:

- **Logging:** You can turn logging off or on. Logs are stored in the `/var/log/dfwpktlogs.log` file on ESXi hosts.
- **Direction:** This setting matches the direction of traffic from the point of view of the destination object.
  - Considering VM as an object, **In** means that only traffic to the VM is checked, **Out** means that only traffic from the VM is checked, and **In-Out**, means that traffic in both directions is checked.
- **IP Protocol:** IPv4, IPv6, and IPv4-IPv6 protocols are supported.
- **Log Label:** Log labels can be used to identify a rule when analyzing the log files.

## 7-42 Blocking Malicious IPs in the Distributed Firewall

The Block Malicious IPs feature in NSX Distributed Firewall uses the Malicious IPs File or Malicious IPs Feed to filter the traffic in NSX.



The Block Malicious IPs feature in NSX Distributed Firewall was introduced in NSX 4.0.0.1.

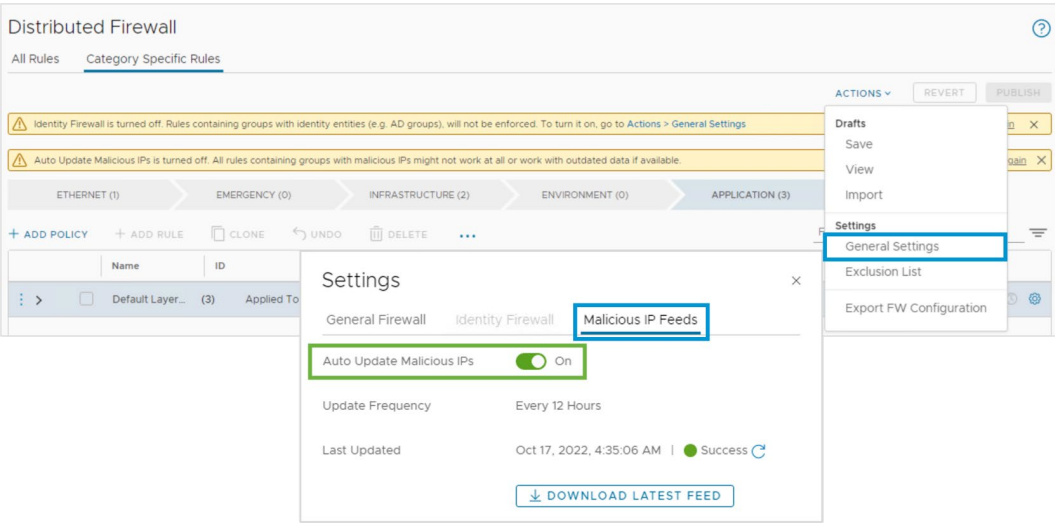
Traffic between any Internet resource with a malicious IP address and the internal resources is blocked by the distributed firewall by referring to the Malicious IPs Feed or Malicious IPs File.

The distributed firewall allows only traffic between an Internet resource with a legitimate IP address and the internal resources. A legitimate IP address does not have an entry in the Malicious IPs Feed or Malicious IPs File.

# 7-43 Enable or Disable Malicious IP Feeds

You can enable or disable the download of Malicious IP Feeds from NTICS in the NSX UI.

In the navigation pane on the left, select **Security > Policy Management > Distributed Firewall > Category Specific Rules**. Then, from the **ACTIONS** drop-down menu, select **General Settings**.



In the Settings dialog box, click the **Malicious IP Feeds** tab and turn on the **Auto Update Malicious IPs** toggle.

You can download the latest feed in the Settings dialog box. The automatic download frequency is 12 hours.



# 7-44 Default Malicious IP Group

A group called DefaultMaliciousIpGroup is created by default. It contains all the Malicious IPs obtained from the Malicious IPs Feed as its members.

Groups

ADD GROUP

EXPAND ALL

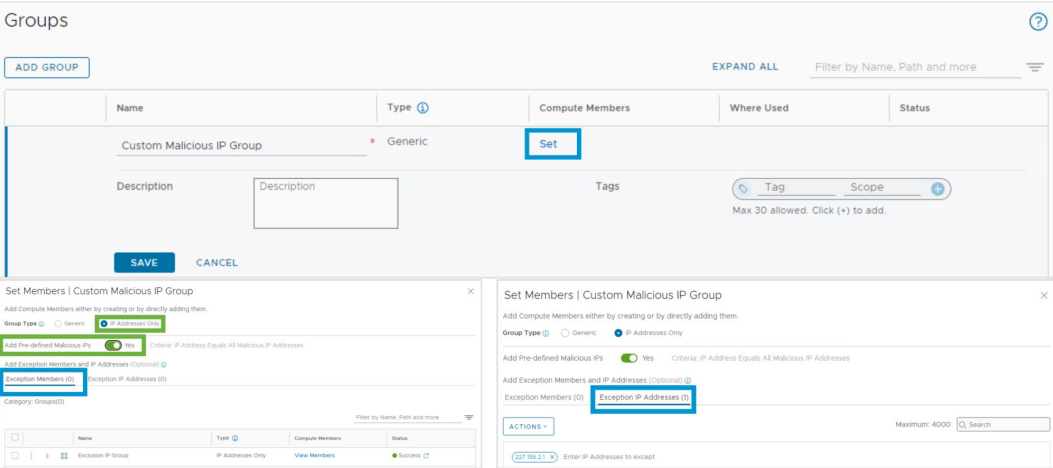
Filter by Name, Path and more

	Name	Type ⓘ	Compute Members	Where Used	Status
⋮ > ⚙	🔗 DefaultMaliciousIpGroup	IP Addresses Only	<a href="#">View Members</a>	<a href="#">Where Used</a>	● Success <a href="#">↗</a>
	Description	Default Malicious IP group	Tags	0	<a href="#">VIEW RELATED GROUPS</a>
⋮ > ⚙	🔗 Edge_NSGroup	Generic	<a href="#">View Members</a>	<a href="#">Where Used</a>	● Success <a href="#">↗</a>
⋮ > ⚙	🔗 Guest_VMs	Generic	<a href="#">View Members</a>	<a href="#">Where Used</a>	● Success <a href="#">↗</a>
⋮ > ⚙	🔗 NSX-APPLICATION-PLATFORM-HOST-CO...	Generic	<a href="#">View Members</a>	<a href="#">Where Used</a>	● Success <a href="#">↗</a>
⋮ > ⚙	🔗 Serviceinsertion_NSGroup	Generic	<a href="#">View Members</a>	<a href="#">Where Used</a>	● Success <a href="#">↗</a>
⋮ > ⚙	🔗 SystemVM_NSGroup	Generic	<a href="#">View Members</a>	<a href="#">Where Used</a>	● Success <a href="#">↗</a>

You cannot delete DefaultMaliciousIPGroup, but you can edit this group.

# 7-45 Creating a Custom Malicious IP Group

You can create a custom Malicious IP group by either adding exception members or exception IP addresses to the default Malicious IP group.



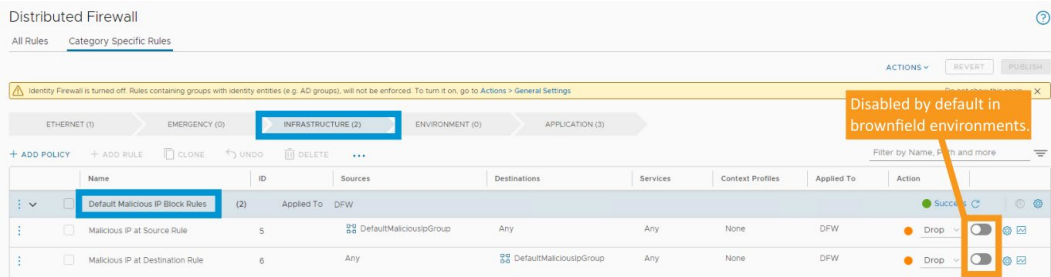
Next to Group Type, you must select **IP Addresses Only**.

Next to Add Pre-defined Malicious IPs, turn on the **Yes** toggle to include all the Malicious IPs from the Malicious IPs Feed.

The **Exception Members** and **Exception IP Addresses** tabs contain the IP addresses that you want to exclude from the pre-defined malicious IP address list during the distributed firewall rule processing.

## 7-46 Default Malicious IP Block Rules

A default policy with the name Default Malicious IP Block Rules is created in the infrastructure category of the distributed firewall rules.



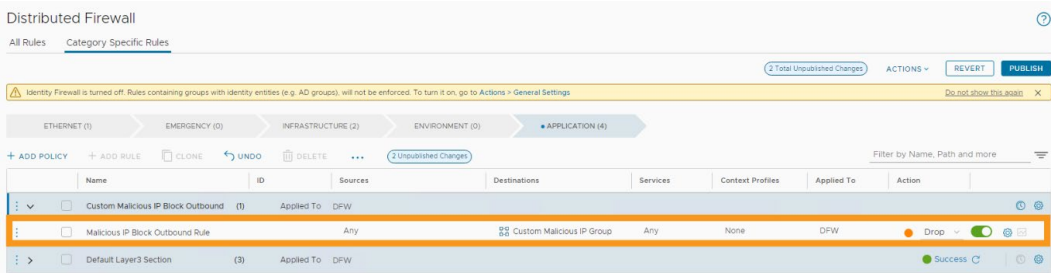
The first rule is to drop any traffic initiated by a malicious IP address from an external network to the internal network.

The second rule is to drop any traffic from the internal network to a malicious IP address in an external network.

Both the rules are enabled by default in a greenfield environment and disabled in a brownfield environment.

## 7-47 Configuring Rules to Block Malicious IPs

You can create a custom malicious IP address block rule and attach your custom Malicious IP group to it.



The configured rule drops any traffic from any internal source going to any destination IP address that is included in the group named Custom Malicious IP Group.

## 7-48 Saving and Viewing the Distributed Firewall Configuration

You can save and view distributed firewall configurations. Every time you publish a distributed firewall rule, a draft of the configuration is saved automatically.

The screenshot displays the 'Distributed Firewall' configuration page. At the top, there's a navigation bar with 'All Rules' and 'Category Specific Rules'. Below this, a yellow warning banner states: 'Identity Firewall is turned off. Rules containing groups with identity entities (e.g. AD groups), will not be enforced. To turn it on, go to Actions > General Settings'. The main area shows a sequence of configuration steps: ETHERNET (1), EMERGENCY (0), INFRASTRUCTURE (2), ENVIRONMENT (0), and APPLICATION (7). Below these steps is a table of rules:

	Name	ID	Applied To	Sources	Destinations	Services	Context Profiles	Applied To
>	EXTERNAL ACCES...	(1)	Applied To	DFW				
>	3-TIER POLICY	(3)	Applied To	DFW				
>	Default Layer3 Sec...	(3)	Applied To	DFW				

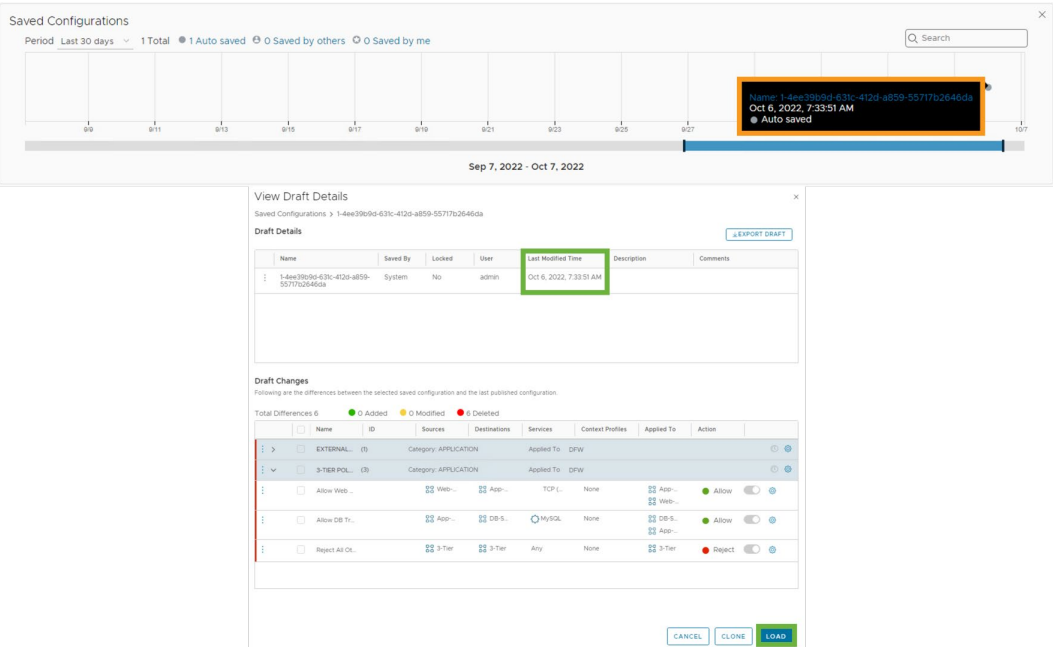
On the right side, there's an 'ACTIONS' menu with options: Drafts, Save, View, Import, and Settings. The 'Settings' menu is expanded, showing 'General Settings', 'Exclusion List', and 'Export FW Configuration'. Below the table, there's a 'Saved Configurations' section with a timeline from Sep 7, 2022, to Oct 7, 2022. The timeline shows three categories: '1 Auto saved', '0 Saved by others', and '0 Saved by me'. A blue bar highlights the 'Viewing the Saved Configuration' period.

From this view, you can see a timeline with all saved distributed firewall configurations. The following types of saved items are available:

- Auto saved: Drafts automatically saved by the system immediately after distributed firewall changes are published. This feature is enabled by default but can be disabled if required. Rolling back to the previous configuration requires reverting to the previously published autosave.
  - You can disable the Auto saved feature in the NSX UI by navigating to **Security > Policy Management > Distributed Firewall > ACTIONS > General Settings** and turn off the **Auto Save Drafts** toggle.
- Saved by others: Distributed firewall configurations saved by other users different from the user currently logged in to the system.
- Saved by me: Distributed firewall configurations saved by the user currently logged in to the system.

# 7-49 Rolling Back to a Saved Distributed Firewall Configuration

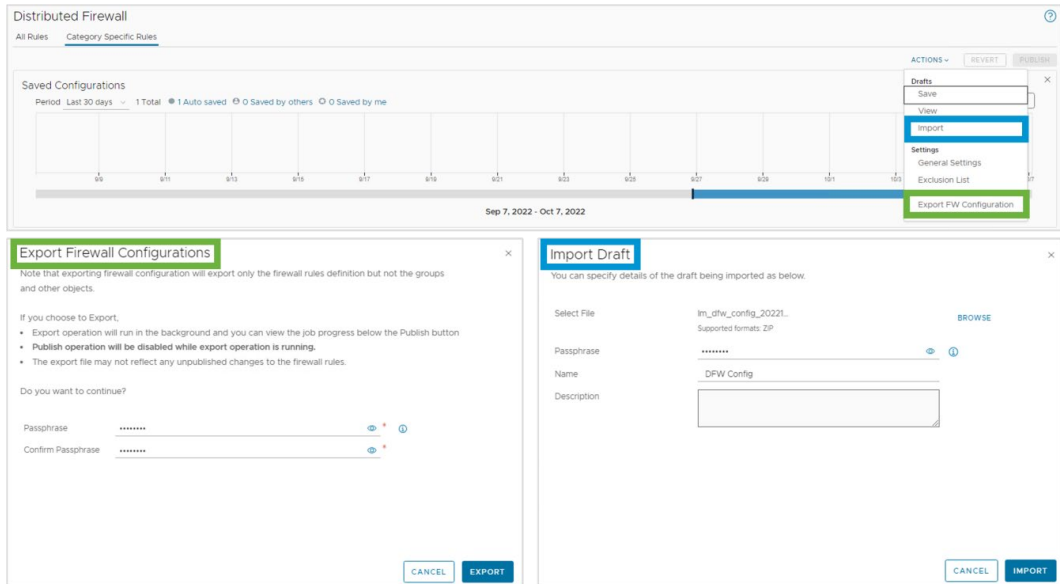
You can roll back to a previously saved distributed firewall configuration.



When you click the name of the saved configuration in the histogram, a new wizard displays details about the distributed firewall configuration on the top, including name, description, and creation date. The bottom part of the screen displays the differences between the saved configuration and the last published configuration.

## 7-50 Distributed Firewall Configuration Export and Import

You can also export and import the distributed firewall configuration.



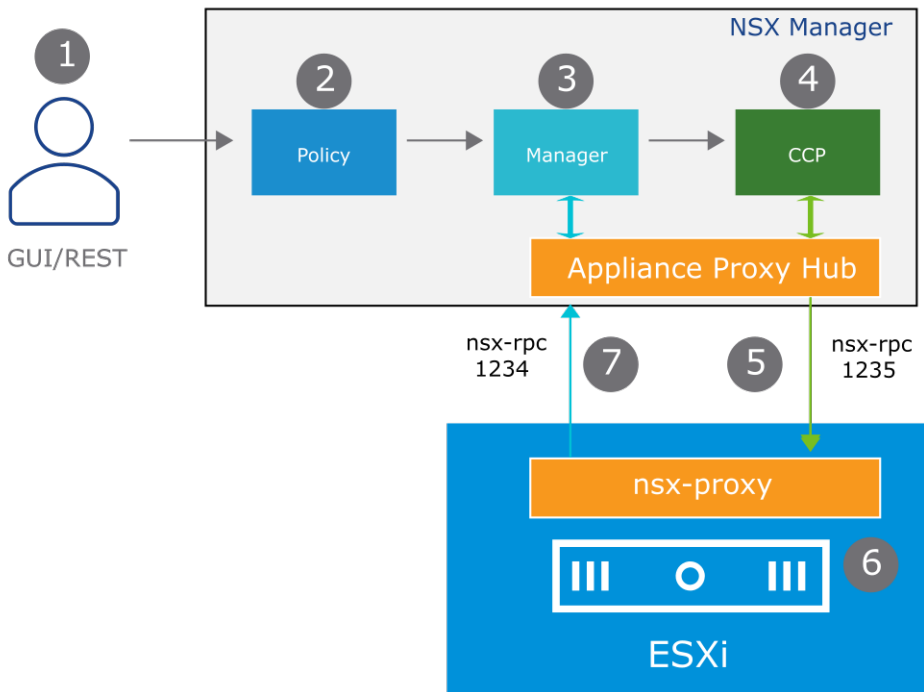
While exporting a firewall configuration, you must provide a passphrase. This passphrase is needed when importing this configuration into the firewall. After the export is complete, you can download the firewall configuration.

While importing a firewall configuration with the passphrase, you must also provide a name for this configuration. All the imports are saved as drafts in the firewall.

## 7-51 Distributed Firewall Architecture

The high-level distributed firewall workflow includes the following steps:

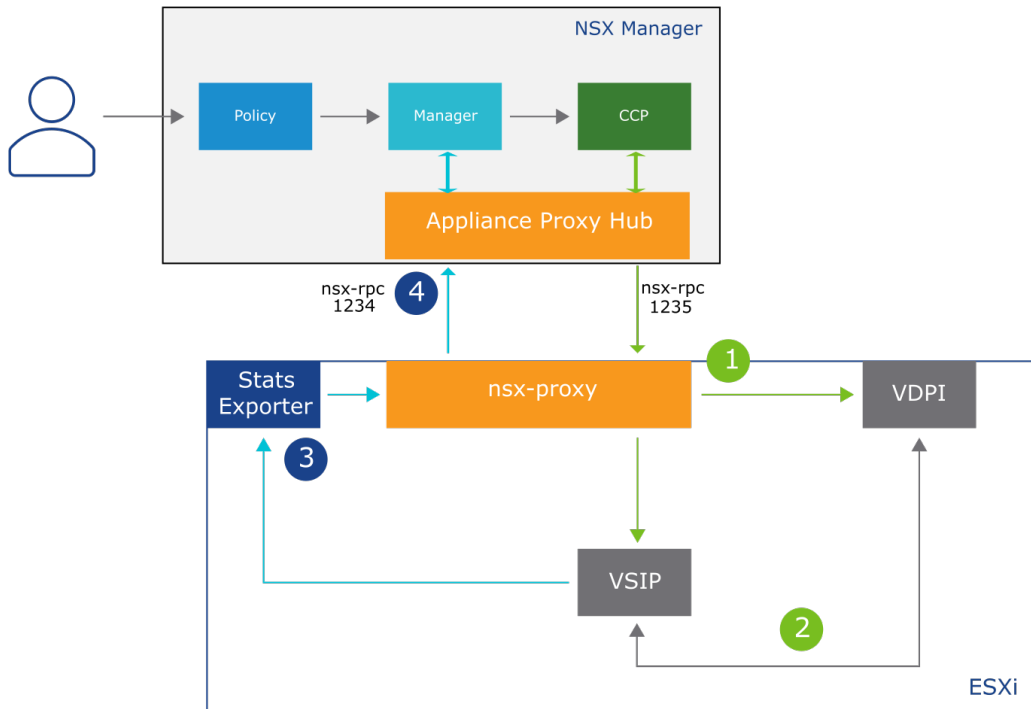
1. Users configure distributed firewall policies through the NSX UI or API.
2. The policy role processes these policies.
3. Distributed firewall policies are then pushed to the manager role and persisted.
4. The manager role forwards the distributed firewall rule configuration to the central control plane (CCP).
5. The CCP forwards the configuration to the LCP (nsx-proxy) through the Appliance Proxy Hub (APH).
6. The host transport nodes (ESXi) store the distributed firewall configuration and configure the datapath accordingly.
7. The transport nodes send rule statistics and status to NSX Manager.



## 7-52 Distributed Firewall Architecture: ESXi

On an ESXi host, the distributed firewall includes several components:

1. nsx-proxy receives the configuration changes from the CCP and configures datapath modules.
2. Datapath modules include the following components:
  - VSIP: Receives firewall rules and downloads them on each VM's vNIC
  - VDPI: Performs L7 packet inspection
3. Stats Exporter collects flow records from the distributed firewall data plane kernel modules and generates rules statistics.
4. nsx-proxy passes rules statistics and real-time data to the management plane.





The following datapath modules are responsible for distributed firewall rule processing:

- VMware Internetworking Service Insertion Platform (VSIP): This module is the main part of the distributed firewall kernel module that receives the firewall rules and downloads them on each VM's vNIC.
- VMware Deep Packet Inspection (VDPI): This deep packet inspection module daemon in the user space is responsible for L7 packet inspection. VDPI can identify application IDs and extract context for a traffic flow.

L7 rules, like the remaining DFW rules, are programmed into VSIP. VSIP forwards L7 packets to VDPI, which inspects and extracts the L7 information from the packets and returns them to VSIP.

Stats Exporter collects flow records from the VSIP kernel module and generates rule statistics.

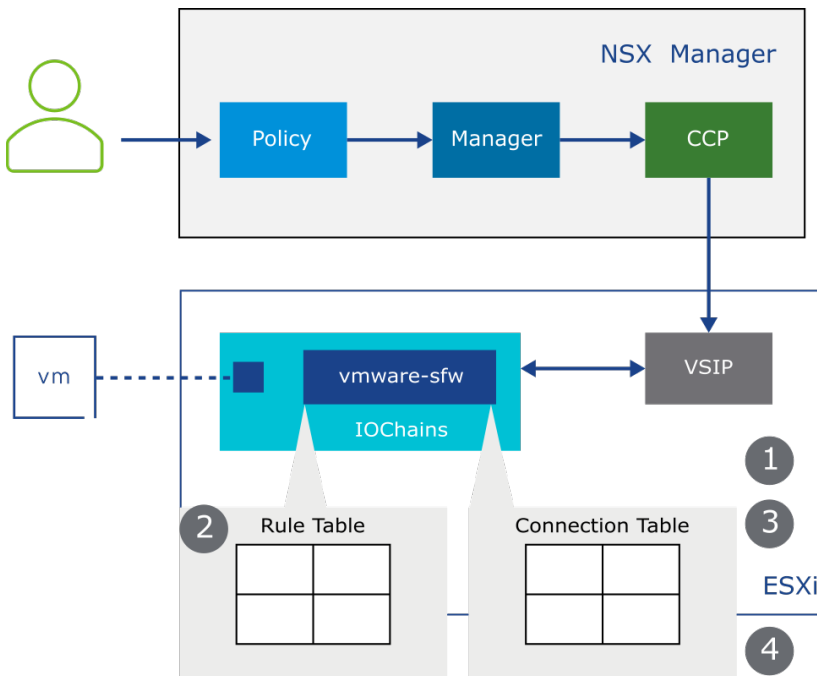
## 7-53 Distributed Firewall Rule Processing: ESXi

vmware-sfw is a software construct where distributed firewall rules are stored and enforced.

vmware-sfw maintains a rule table and a connection table.

When a distributed firewall rule is configured, its information is stored in the rule table. After the initial rule configuration, the traffic is managed as follows:

1. A lookup is performed in the connection table to check whether a connection exists.
2. If the connection is not present, the packet is matched against the rule table.
3. If the packet is allowed and the traffic type is stateful, a connection entry is created in the connection table.
4. All subsequent packets for the same connection are serviced directly from the connection table. Stateless packets are always matched against the rule table.



The vSphere ESXi network IOChain is a framework that enables you to insert functions into the network datapath.

The IOChain framework is used by NSX to host vmware-sfw, which is a software construct where distributed firewall rules are stored and enforced.

vmware-sfw maintains the following types of tables:

- Rule Table: Locally stores all applicable firewall rules
- Connection Table: Caches flow entries for stateful rules with an action

## 7-54 Lab 11: Configuring the NSX Distributed Firewall

Create NSX distributed firewall rules to allow or deny the application traffic:

1. Prepare for the Lab
2. Test the IP Connectivity
3. Create Security Tags
4. Create Security Groups based on Tags
5. Create Distributed Firewall Rules
6. Test the IP Connectivity After the Firewall Rule Creation
7. Prepare for the Next Lab

## 7-55 Review of Learner Objectives

- Identify types of firewalls in NSX
- Describe features of distributed firewalls
- Create firewall policies
- Configure firewall rules
- Configure firewall rule attributes: groups, services, and profiles
- Configure the distributed firewall to block malicious IPs
- Save, roll back, export, and import the distributed firewall configuration
- Describe the distributed firewall architecture

## 7-56 Lesson 3: Use Case for Security in Distributed Firewall on VDS

### 7-57 Learner Objectives

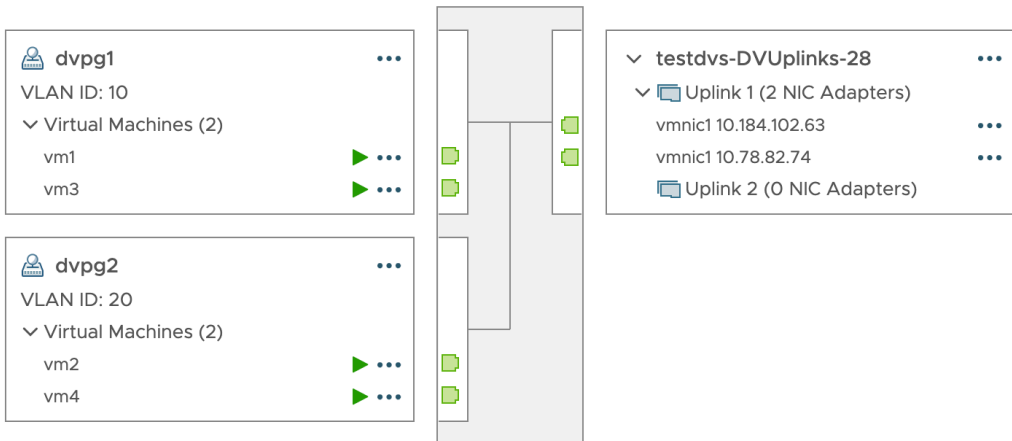
- List the distributed firewall on VDS requirements
- Configure the distributed firewall on VDS
- Validate the distributed firewall on VDS configurations

## 7-58 About Distributed Firewall on VDS

Distributed firewall on VDS enables NSX security features on existing vSphere distributed port groups (DVPG) without changing the vSphere platform.

Distributed firewall on VDS provides the following benefits:

- Removes the need for migrating workloads when configuring NSX security
- Implements the same security policies and rules for network objects irrespective of whether they are created or owned by NSX Manager or vSphere
- Enables the security administrator to deploy the distributed firewall and other security features without involving the networking administrators



Distributed firewall on VDS enables NSX Security features on workloads attached to a distributed port group (DVPG) managed by vCenter Server. Earlier versions of NSX required VMs to be attached to segments managed by NSX (VLAN or overlay) to take advantage of distributed security functions. This functionality has now been expanded to cover DVPG managed by vCenter Server.

Distributed firewall on VDS is also available in vSphere 6.7.

Distributed firewall on VDS is implemented on the NSX Management Plane based on information reported by the vCenter Server inventory.

## 7-59 Supported Features

Several features are supported when you prepare your vCenter Server cluster for NSX Security.



NSX Distributed Firewall



IPFix



Traceflow



IDS / IPS



NSX Intelligence



Malware Prevention

For all supported features, see *NSX Administration Guide* at <https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-E9FBE567-D136-41AF-B8D6-AE95416F4229.html#GUID-E9FBE567-D136-41AF-B8D6-AE95416F4229>.

# 7-60 Distributed Firewall on VDS Requirements

Installing the NSX distributed firewall on an existing VDS has the following requirements:

- The NSX version must be 3.2 or later.
- ESXi hosts are not prepared for NSX.
- All hosts in the cluster must have identical VDS configurations.
- The vCenter Server system must be registered as a Compute Manager in NSX Manager.

Supported VDS and vSphere versions:

VDS Version	vSphere Version
6.6.0	vSphere 6.7 and later
7.0.0	vSphere 7.0 Update 1 and later
7.0.2	vSphere 7.0 Update 2 and later
7.0.3	vSphere 7.0 Update 3 and later
8.0.0	vSphere 8.0.0 and later

This feature is only configurable with the NSX API or by using the Quick Start installation in the NSX UI or through the vCenter NSX plug-in.

VDS can span multiple vSphere clusters. The NSX security mode is enabled only on some clusters.

## 7-61 Installation Workflow

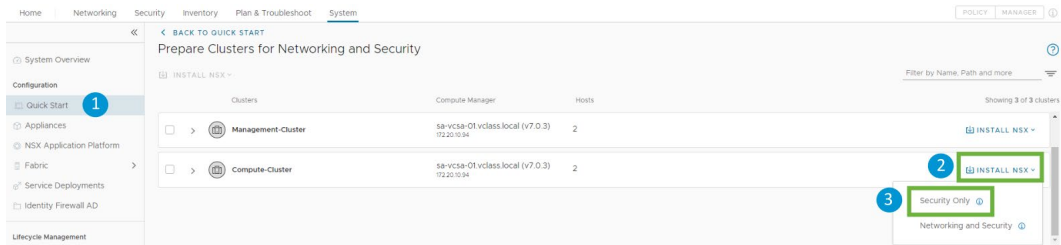
You follow these steps to install the NSX distributed firewall on a VDS with existing dvportgroups.



## 7-62 Preparing the Cluster for Security

To prepare clusters for NSX Security:

1. Navigate to **System > Configuration > Quick Start > Prepare Clusters for Networking and Security > GET STARTED**.
2. Select the clusters that you want to install.
3. Click **INSTALL NSX > Security Only**.



All hosts in the cluster must have identical VDS configuration to perform an NSX Quick Install.

You can also configure the host for security only with a REST API call.



## 7-63 Validating the Security Cluster Preparation from the NSX UI

You can validate the Security Cluster Preparation by navigating to **System > Configuration > Fabric > Nodes > Host Transport Nodes**.

The screenshot shows the NSX UI interface for Host Transport Nodes. The table displays the following data:

Node	ID	IP Addresses	OS Type	NSX Configuration	NSX Version	Host Switch	Tunnels	TEP IP Address	Node Status	Alarms
● 1 Host Not Configured										
● 2 Hosts Not Configured										
Applied Profile: 7a40c024-405d-4e1...										
sa-esxi-01.vclass.local	965e...b5d2	172.20.10.51, 172...	ESXi 7.0.3	Success	4.0.1.0.0.20364576	1	Not Available		Up	0
sa-esxi-02.vclass.local	74ac...6e3f	172.20.10.52, 17...	ESXi 7.0.3	Success	4.0.1.0.0.20364576	1	Not Available		Up	0

Annotations in the image:

- A green box highlights the 'Security' tag in the 'Node' column.
- An orange box highlights the 'Success' status in the 'NSX Configuration' column.
- A blue box highlights the 'VDS' type in the 'Host Switch' column.

You check the following parameters:

- The node status is UP.
- The NSX Configuration status is Success.
- The NSX version is correct.
- One host switch per VDS was created and the Type is VDS.

Because the cluster is not prepared for NSX networking features, it is not expected to have tunnels configured on the host.

# 7-64 Transport Node Preparation

All the ESXi hosts of the selected clusters are automatically configured as transport nodes in the back end.

During the transport nodes preparation, the following objects are created:

- Autoconfigured transport node profiles
- VLAN transport zones
- Discovered segments

When the ESXi hosts are prepared for NSX security, vCenter Server performs a full inventory sync with NSX Manager to share its objects.

# 7-65 Autoconfigured Transport Node Profile

A separate transport node profile is created for each cluster.

The screenshot shows the NSX Manager interface with the 'Transport Node Profiles' tab selected. The table lists two profiles: 'NSX Created' and 'ESXi-TH-Profile'. The 'NSX Created' profile is highlighted with a green box. A green callout points to this profile with the text: 'A transport node profile is automatically created by NSX for each prepared cluster.' A blue callout points to the 'Host Switch Name' column with the text: 'One host switch is automatically created by NSX for each VDS.'

Name	ID	Description	Transport Zones	Applied Clusters	Host Switch Type	Host Switch Name	Physical NICs	IP Assignment Type
NSX Created	7a40c024-405d-4a0e-1f02-0a0b	nsx.vlan-tz.security.7a...	Compute-Cluster		NSX Created	dvs-SA-Datacenter		DHCP
ESXi-TH-Profile	1b55-b67c	PROD-Overlay-TZ			NSX Created	dvs-SA-Datacenter		IP Pool

You can check the autocreated transport node profile by navigating to **System > Fabric > Profile > Transport Node Profile**.

A separate transport node profile is created for each cluster even if multiple clusters have identical VDS configuration.

The created transport node profiles are neither configurable nor editable.

# 7-66 VLAN Transport Zones

A VLAN transport zone is created for every VDS.

HomeNetworkingSecurityInventoryPlan & TroubleshootSystem

POLICYMANAGER ⓘ

Transport ZonesHealth Configuration

⏪

+ ADD ZONEEDITDELETEACTIONS -

Transport Zone	ID	Traffic Type	Transport Node Members	Status	Where Used
<input type="checkbox"/> PROD-Overlay-TZ	51fd...f576	Overlay	2	Up	Where Used
<input type="checkbox"/> PROD-VLAN-TZ	65d5...3560	VLAN	2	Up	Where Used
<input type="checkbox"/> <b>nsx-ovs</b> nsx-ovs-transportzone	1b3a...963e	Overlay	0	Unknown	Where Used
<input type="checkbox"/> <b>nsx-vlan</b> nsx-vlan-transportzone	a95c...aeba	VLAN	0	Unknown	Where Used
<input type="checkbox"/> <b>nsx-vlan-tz</b> security.7a40c024-405b-4e1e-b84f-dceffSec02060.rdv-SA-Datacenter	e468...c420	VLAN	2	Up	Where Used

You can check the autocreated transport zone by navigating to **System > Fabric > Transport Zones > Transport Zones**.

The created transport node profiles are neither configurable nor editable.

# 7-67 Discovered Segments (1)

Discovered segments are automatically created by the vCenter Server inventory module. For each vSphere DVPG, a distributed port group is created in NSX with its own NSX ID.

sa-vcsa-01.vclass.local

vSphere Datacenter

none

VM Network

dvs-SA-Datacenter

dvs-SA-DC-DVUplinks-30

Edge-HA

Edge-Trunk

Frontend

pg-SA-Edge-Overlay

pg-SA-Edge-Uplinks

pg-SA-Management

pg-SA-Production

pg-vMotion

Remote\_Network

web-dvpg

Workload-10

Workload-20

Segments

NSX Distributed Port Groups Profiles

	Distributed Port Group	Transport Zone	Ports
>	dvs-SA-Datacenter Edge-HA	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	0
>	dvs-SA-Datacenter Edge-Trunk	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	0
>	dvs-SA-Datacenter Frontend	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	0
>	dvs-SA-Datacenter pg-SA-Edge-Overlay	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	3
>	dvs-SA-Datacenter pg-SA-Edge-Uplinks	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	0
>	dvs-SA-Datacenter pg-SA-Management	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	1
>	dvs-SA-Datacenter pg-SA-Production	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	4
>	dvs-SA-Datacenter pg-vMotion	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	0
>	dvs-SA-Datacenter Remote_Network	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	0
>	dvs-SA-Datacenter web-dvpg	nsx vlan-tz security 7a40c024-405d-4e1e-b841-dcef5ecd2080 dvs-SA-Datacenter	3

A single instance of a port has two IDs: a vSphere ID and an NSX ID. The NSX Control plane uses the NSX ID.

Discovered segments can be consumed by the NSX security features such as the distributed firewall.

380

Technet24

# 7-68 Discovered Segments (2)

You can access the discovered segments by navigating to **Networking > Connectivity > Segments > Distributed Port Groups**.

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

POLICY

MANAGER

Segments

NSX

Distributed Port Groups

Profiles

EXPAND ALL

Filter by Name, Path and more

	Distributed Port Group	Transport Zone	Ports	Distributed Switch	Security Configuration
>	divs-SA-Datcenter-pg-SA-Edge-Uplinks	nsx.vlan-tz.security.7a40c024-405d-4efc-b841-dcef5ec02080.divs-SA-Datcenter	0	divs-SA-Datcenter	Configured
>	divs-SA-Datcenter-pg-SA-Management	nsx.vlan-tz.security.7a40c024-405d-4efc-b841-dcef5ec02080.divs-SA-Datcenter	1	divs-SA-Datcenter	Configured
>	divs-SA-Datcenter-pg-SA-Production	nsx.vlan-tz.security.7a40c024-405d-4efc-b841-dcef5ec02080.divs-SA-Datcenter	4	divs-SA-Datcenter	Configured
>	divs-SA-Datcenter-pg-vMotion	nsx.vlan-tz.security.7a40c024-405d-4efc-b841-dcef5ec02080.divs-SA-Datcenter	0	divs-SA-Datcenter	Configured
>	divs-SA-Datcenter-Remote_Network	nsx.vlan-tz.security.7a40c024-405d-4efc-b841-dcef5ec02080.divs-SA-Datcenter	0	divs-SA-Datcenter	Configured
>	divs-SA-Datcenter-web-dvpg	nsx.vlan-tz.security.7a40c024-405d-4efc-b841-dcef5ec02080.divs-SA-Datcenter	0	divs-SA-Datcenter	Configured

Port Group Id

dvportgroup-231756

Description

NSX system generated Segment for security

SEGMENT PROFILES

IP Discovery

IP Discovery

default-ip-discovery-profile

Segment Security

default-segment-security-profile

VLAN

15

Tags

0

VIEW RELATED GROUPS

Set Ports

Distributed Port Group

divs-SA-Data...

Ports

EXPAND ALL

Filter by Name, Path and more

	Port Name	VIF UUID	Admin State	Status
>	sa-web-01.vmx@118385090	118385090	Up	Success
>	sa-web-02.vmx@114129594	114129594	Up	Success
>	sa-web-03.vmx@1165486933	1165486933	Up	Success

Discovered segments do not appear in the NSX UI as segments, but they appear as distributed port groups.

VLAN tags are read and added from vCenter Server.

The vCenter Server inventory is monitored. Any change that occurs (DVPG added, host added, and so on) is reflected in NSX.

# 7-69    Configuring Segment Profiles

You can configure IP discovery, segment security, and Spoofguard from the NSX UI.

Segments

NSX Distributed Port Groups Profiles

EXPAND ALL Filter by Name, Path and more

	Distributed Port Group	Transport Zone	Ports	Distributed Switch	Security Configuration
>	dvs-SA-Datacenter pg-SA-Production	nsx-vlan-tz security a1855f13-34c8-4094-8c46-9d57a0ea2102 dvs-SA-Datacenter	6	dvs-SA-Datacenter	Configured
>	dvs-SA-Datacenter pg-vMotion	nsx-vlan-tz security a1855f13-34c8-4094-8c46-9d57a0ea2102 dvs-SA-Datacenter	0	dvs-SA-Datacenter	Configured
>	dvs-SA-Datacenter Remote_Network	nsx-vlan-tz security a1855f13-34c8-4094-8c46-9d57a0ea2102 dvs-SA-Datacenter	0	dvs-SA-Datacenter	Configured
>	dvs-SA-Datacenter web-dvpg	nsx-vlan-tz security a1855f13-34c8-4094-8c46-9d57a0ea2102 dvs-SA-Datacenter	3	dvs-SA-Datacenter	

Port Group Id

dvportgroup-201756

VLAN

15

Description

NSX system generated Segment for security

Tags

Tag Scope

Max 30 allowed. Click (+) to add.

SEGMENT PROFILES

IP Discovery default-ip-discovery-profile

Segment Security default-segment-security-profile

Spoof Guard default-spoofguard-profile

Annotations

vCenter Server must be used for editing some DVPG and dvport configurations, for example the VLAN ID.

Configurations that are specific to NSX, such as IP discovery, segment security, and Spoofguard, can be set from the NSX UI.

Create Segment Profile

Segment Profile Custom\_IP\_Discovery\_Profile Type IP Discovery Profile

Enable IP Detection Enabled

ARP Snooping Enabled

ARP Binding Limit 1

ND Snooping Disabled

ND Snooping Limit 3

ARP ND Binding Limit 10

Trust on First Use Enabled

CHOP Snooping Enabled

DHCP Snooping Disabled

IPsec Disabled

VMware Tools Enabled

VMware Tools - Plug Disabled

Description

Tags

Tag Scope

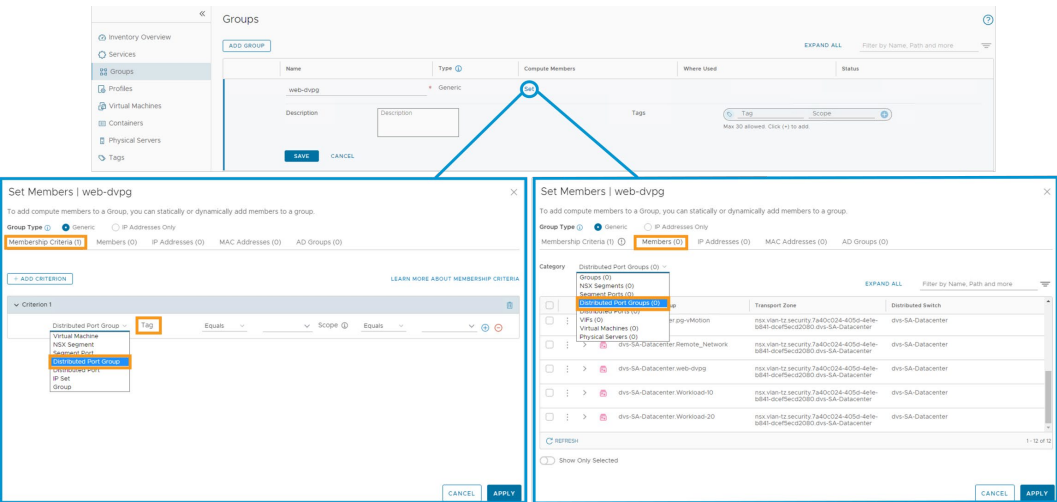
Max 30 allowed. Click (+) to add.

CANCEL

SAVE

# 7-70 Using VDS Attributes to Define NSX Groups

You can use Distributed Port, Distributed Port Groups, and their corresponding tags to define NSX Group membership.



You can select distributed port group and distributed port as members and membership criteria. You can use these groups when configuring distributed firewall rules.

# 7-71 Review of Learner Objectives

- List the Distributed Firewall on VDS requirements
- Identify the steps to configure Distributed Firewall on VDS
- Validate the configuration

## 7-72 Lesson 4: NSX Gateway Firewall

### 7-73 Learner Objectives

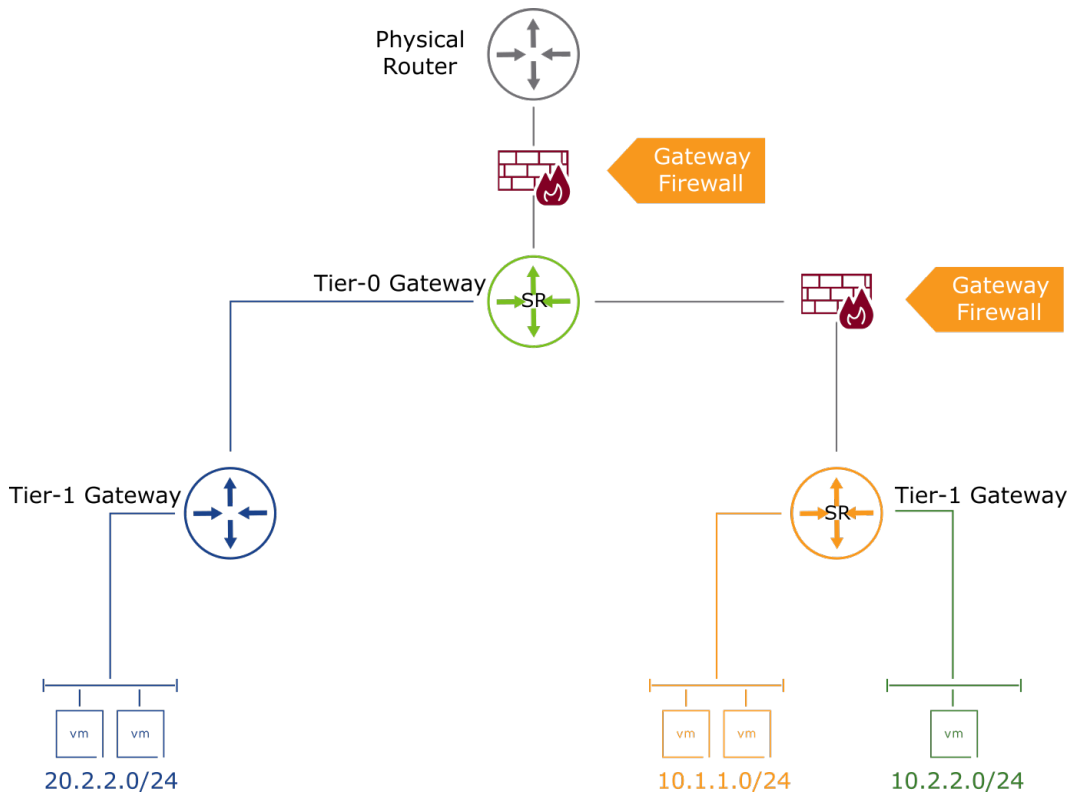
- Describe the functions of the gateway firewall
- Explain the purpose of a gateway policy
- Create gateway firewall policies and rules
- Describe the gateway firewall architecture



## 7-74 About the Gateway Firewall

The gateway firewall has the following characteristics:

- Stateful and stateless firewall for north-south traffic
- Independent of the distributed firewall
- Implemented on both Tier-0 and Tier-1 gateways and requiring the SR component of the router
- Enforced on the northbound-facing interface of the gateway



The NSX gateway firewall provides essential perimeter firewall protection that can be used in addition to a physical perimeter firewall. The gateway firewall supports stateless and stateful firewall rules.

The gateway firewall works independent of the distributed firewall. A user can consume the gateway firewall using either the UI or REST API framework provided by NSX Manager. The gateway firewall configuration is similar to the distributed firewall policy. This configuration is defined as a set of individual rules in a policy. Like the distributed firewall, the gateway firewall rules can use tagging and groups to build policies.

The gateway firewall is a centralized firewall implemented on the northbound-facing interface of the gateway (Tier-0 uplinks and Tier-1 RouterLinks). The firewall is implemented on a Tier-0 or Tier-1 service router (SR) component that is hosted on the NSX Edge node.

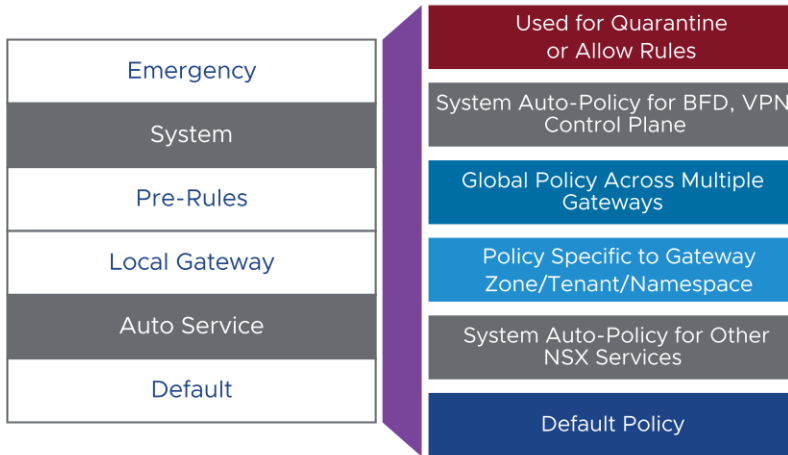
The service router component of a Tier-0 or Tier-1 gateway provides north-south routing functionality and centralized services, such as NAT, and so on.

From NSX 4.0.1, the Tier-0 gateway firewall supports stateful firewall filtering with both active-active and active-standby high availability modes.

The gateway firewall service is part of the NSX Edge node for both bare-metal and VM form factors. The gateway firewall is useful in developing PCI zones, multitenant environments, or DevOps-style connectivity without forcing the intertenant or interzone traffic onto the physical network. The gateway firewall datapath uses the Data Plane Development Kit (DPDK) framework supported on NSX Edge to provide better throughput.

## 7-75 Predefined Gateway Firewall Categories

The gateway firewall includes predefined categories on the **All Shared Rules** tab, where rules across all gateways are visible.



The gateway firewall includes several predefined categories for rules.

- Emergency: Used for quarantine and can also be used for Allow rules.
- System: Automatically generated by NSX and specific to internal control plane traffic, such as BFD rules, VPN rules, and so on.
- Pre Rules: Globally applied across all NSX gateways.
- Local Gateway: Rules specific to a particular NSX gateway.
- Auto Service: Autoplumbed rules applied to the data plane.
- Default: Rules that define the default gateway firewall behavior.

Categories are evaluated from left to right. Each category can have its own rules, which are evaluated top to bottom.

# 7-76 Gateway Firewall Policy

A Gateway Firewall policy includes one or more individual firewall rules and is applied to north-south traffic.

Gateway policies can be applied to Tier-0 and Tier-1 gateways and their interfaces.

Gateway Firewall

All Shared RulesGateway Specific RulesSettings

GatewayBGP-TO-GW-01 | Tier-0

Select the Tier-0 or Tier-1 gateway that the Gateway firewall policy applies to.

2 Total Unpublished ChangesACTIONSREVERTPUBLISH

Identity Firewall Service is turned off for Selected Gateway. To turn it on, go to the Settings Tab →Do not show this again

+ ADD POLICY+ ADD RULECLONEUNDODELETE...2 Unpublished ChangesFilter by Name, Path and more

	Name	ID	Sources	Destinations	Services	Applied To	Action
>	BLOCK EXTERNAL SSH TRAFFIC	(f)					Category: LOCAL GATEWAY
▼	Policy_Default_Infra-tier0-BGP-TO-GW-01	(f)					Category: DEFAULT
:	default_rule					AnyBGP-TO-GW-01	AllowSuccess

A default gateway policy exists to allow all traffic.

## 7-77 Configuring Gateway Firewall Policy Settings

To create a Gateway Firewall policy, you assign a policy name and configure the settings. You can also set a Time Window so that the policy is only applicable during the specified period.

The screenshot shows the 'Gateway Firewall' configuration page. The 'Settings' tab is active, showing a table with one policy: 'BLOCK EXTERNAL SSH TRAFFIC'. A 'Settings' dialog box is open for this policy, showing the following settings:

- TCP Strict:** Enabled (Yes)
- Stateful:** Enabled (Yes)
- Locked:** Disabled (No)

Annotations with colored boxes and arrows point to these settings:

- Blue box:** Drops packets that are not preceded by a complete three-way TCP handshake. Works only with a default ANY-ANY block rule configured.
- Green box:** Performs stateful packet inspection and tracks the state of network connection.
- Grey box:** Performs stateful packet inspection and tracks the state of network connection.

A yellow banner at the top states: 'Identity Firewall Service is turned off for Selected Gateway. To turn it on, go to the Settings Tab ->'. A tooltip points to the 'Settings' tab, stating: 'You can specify a Time Window for the gateway firewall rules.'

To create a Gateway Firewall policy, you assign a policy name.

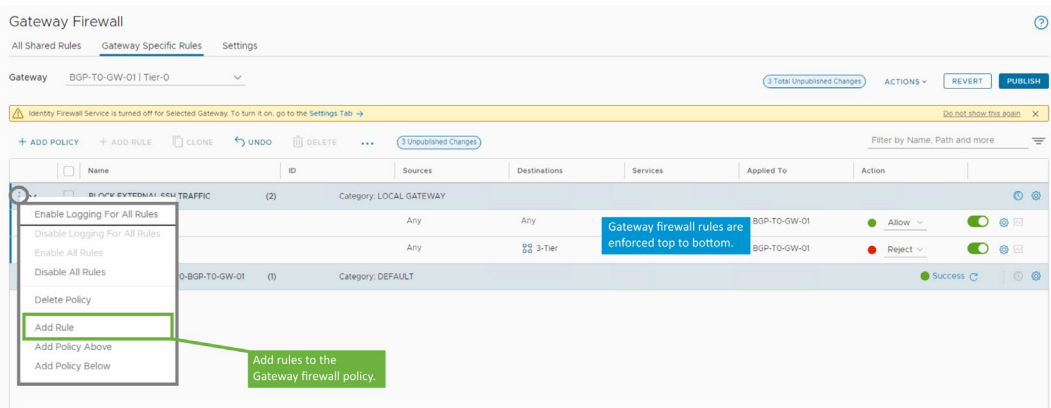
You can configure the following settings when creating a Gateway Firewall policy:

- **TCP Strict:** In certain circumstances, the firewall might not see the TCP three-way handshake for a particular flow (that is, due to asymmetric traffic). By default, the firewall does not enforce the need to see a three-way handshake and will pick up sessions that are already established. TCP Strict can be enabled per section to turn off midsession pickup. When enabling the TCP Strict mode for a particular firewall policy and using a default ANY-ANY Block rule, packets that do not complete the three-way handshake connection requirements and that match a TCP-based rule in this policy section are dropped.
- **Stateful:** When this option is enabled, the gateway firewall performs stateful packet inspection and tracks the state of network connections. Packets matching a known active connection are allowed by the firewall, and packets that do not match are inspected against the gateway firewall rules.
- **Locked:** This setting allows you to lock a policy while making configuration changes so that others cannot make modifications at the same time.

You can also set a Time Window so that the policy is only applicable during the specified period. For this feature, the NSX Edge nodes need to have an NTP server configured.

# 7-78    Configuring Gateway Firewall Rules

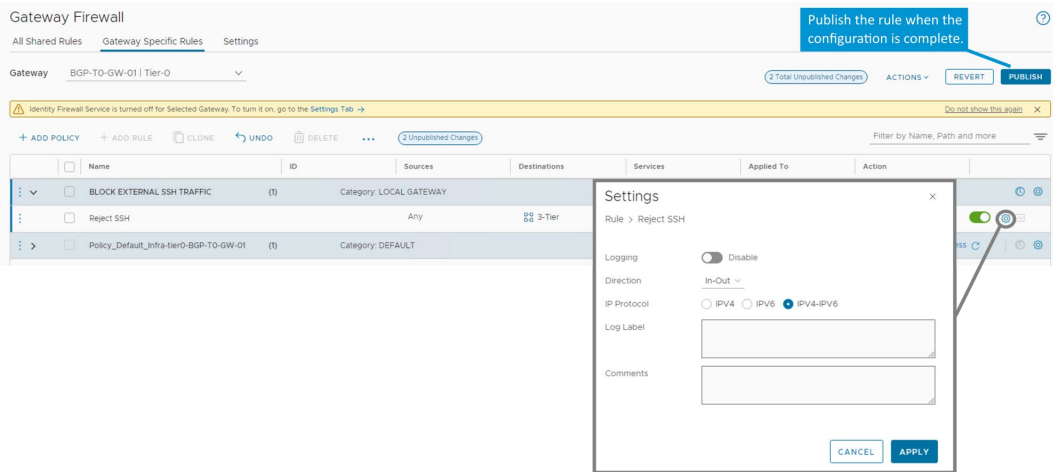
You create one or more rules in the policy to allow, drop, or reject traffic.



Context Profiles are only available on Tier-1 gateways.

## 7-79 Configuring Gateway Firewall Rules Settings

You can specify the logging, direction, and IP protocol for the gateway firewall rule. A firewall rule must be published for it to take effect.



The rules are logged in the Syslog file of the edge node.

You can access these logs from the CLI:

```
get log-file syslog
```

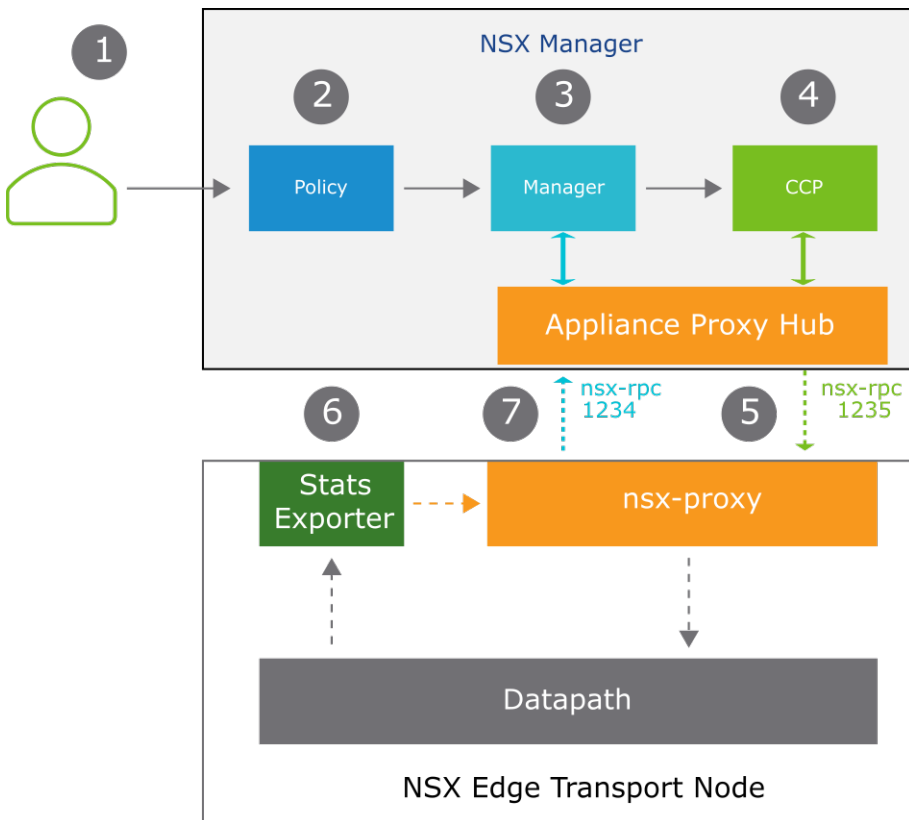
In the rule settings, you can also choose the direction and the IP protocol:

- In: The rule only checks traffic to the gateway interface.
- Out: The rule only checks traffic from the gateway interface.
- In-Out: The rule checks traffic from both directions.

## 7-80 Gateway Firewall Architecture

The gateway firewall workflow is as follows:

1. Users configure gateway policies from the NSX UI.
2. The policy role processes gateway policies.
3. Gateway policies are sent to the manager role, which validates and forwards them to the CCP.
4. The CCP distributes the firewall configuration through APH to the relevant edge nodes.
5. nsx-proxy receives the firewall configuration from the CCP and configures the edge data path.
6. The Stats Exporter collects flow records from the datapath and generates rule statistics.
7. nsx-proxy reports the firewall rules statistics and status to the management plane.





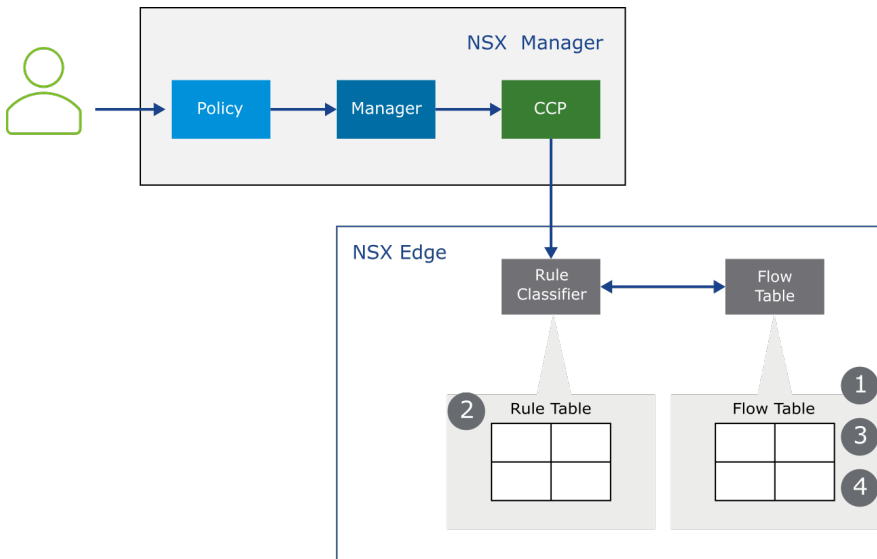
## 7-81 Gateway Firewall Rule Processing

On an NSX Edge node:

- Gateway Firewall rules are programmed into rule classifier.
- The flow table tracks established connections for stateful firewall rules.

When a Gateway Firewall rule is configured, its information is stored in a rule table in the Rule Classifier module. After the initial rule configuration, the traffic is managed as follows:

1. A lookup is performed in the flow table to check whether a connection exists.
2. If the connection is not present, the packet is matched against the rule table in Rule Classifier.
3. If the type of traffic is stateful, an entry is created in the flow table.
4. All subsequent packets for the same connection are serviced directly from the flow table. Stateless packets are always matched against the rule table.



The Rule Classifier maintains stateful and stateless rules for the following features:

- Gateway Firewall
- NAT
- IPSec
- Service Insertion

The flow table is responsible for tracking established connections for stateful firewall rules, and NAT edge services. When a new connection is made, the first packet is matched against the flow table to determine if a session exists.

A rule classifier and flow table are created for each gateway. If two gateways are present in the NSX Edge node, two rule classifier instances and flow tables are created: one for each gateway.

## 7-82 Lab 12: Configuring the NSX Gateway Firewall

Configure and test the NSX gateway firewall rules to control north-south traffic:

1. Prepare for the Lab
2. Test SSH Connectivity
3. Configure a Gateway Firewall Rule to Block External SSH Requests
4. Test the Effect of the Configured Gateway Firewall Rule
5. Prepare for the Next Lab

## 7-83 Review of Learner Objectives

- Describe the functions of the gateway firewall
- Explain the purpose of a gateway policy
- Create gateway firewall policies and rules
- Describe the gateway firewall architecture

## 7-84 Key Points

- Zero-Trust is a security model that does not automatically trust entities in the security perimeter.
- Macro-segmentation is the process of dividing data center infrastructure into smaller zones.
- Micro-segmentation helps to build a Zero-Trust approach to security by defining a security perimeter around each application.
- The distributed firewall is a hypervisor kernel-embedded stateful firewall.
- The distributed firewall resides outside the VM guest OS and controls the I/O path to and from the vNIC.
- The gateway firewall, also called the perimeter firewall, protects traffic from physical environments.

Questions?



## Module 8

# NSX Advanced Threat Prevention

## 8-2 Importance

NSX IDS/IPS, NSX Malware Prevention, NSX Intelligence, and NSX Network Detection and Response provide visibility and protection against advanced threats in your network. As a security administrator, you must learn to properly configure these features to successfully prevent malicious attacks against your environment.

## 8-3 Module Lessons

1. NSX Intrusion Detection and Prevention
2. NSX Application Platform
3. NSX Malware Prevention
4. NSX Intelligence
5. NSX Network Detection and Response

## 8-4 Lesson 1: NSX Intrusion Detection and Prevention

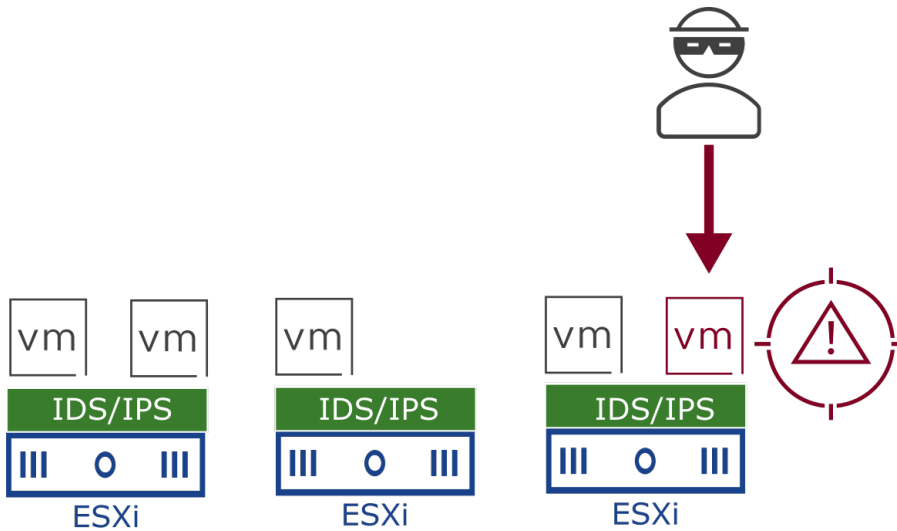
### 8-5 Learner Objectives

- Explain IDS/IPS and its use cases
- Define the IDS/IPS terminologies
- Describe the IDS/IPS architecture
- Configure IDS/IPS
- Interpret IDS/IPS events

## 8-6 About NSX Distributed IDS/IPS

NSX Distributed IDS/IPS uses real-time deep packet inspection to identify and prevent attempts at exploiting vulnerabilities in your applications:

- Protects virtual workloads from malicious traffic
  - Prevents lateral threat movement in the east-west traffic
- Uses signatures to identify malicious traffic patterns
- Is implemented as a distributed solution across multiple ESXi hosts



Using real-time deep packet inspection, NSX Distributed IDS/IPS performs the following tasks:

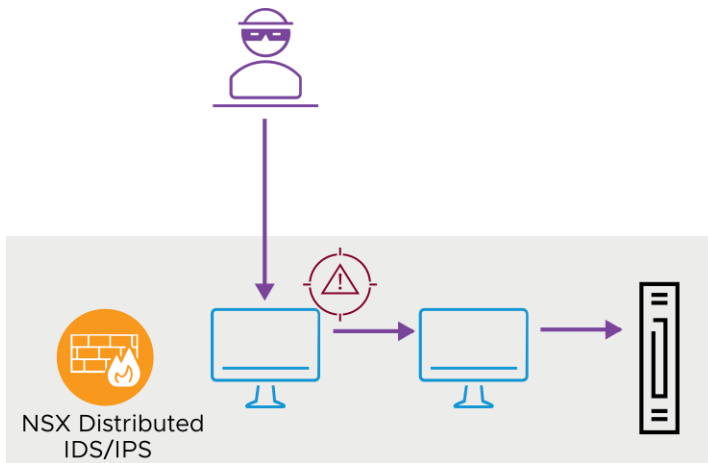
- Protects east-west traffic and prevents lateral threat movement: The objective of many malicious attacks is not solely to penetrate the network. After the attackers are in, they often pivot through multiple systems and explore the network to find their main target and gain access to it. NSX Distributed IDS/IPS recognizes and prevents lateral movement across the network when perimeter security is compromised.
- Uses signatures to identify malicious traffic patterns: NSX Distributed IDS/IPS uses an external cloud-based signature store to remain up to date with known malicious activity, including zero-day vulnerabilities. It helps protect against both L4 and L7 attacks.
- Is implemented as a distributed solution across multiple ESXi hosts: Similar to the distributed firewall architecture, NSX Distributed IDS/IPS is implemented as a kernel module in the ESXi hosts. This distributed architecture significantly reduces hairpinning by processing traffic that is closer to the source.

## 8-7 Use Cases for NSX Distributed IDS/IPS

NSX Distributed IDS/IPS protects against malicious activity, including the following activities:

- Exploits of known application-level vulnerabilities
- Application denial of service
- Lateral movement
- Client-side and server-side exploits

With NSX Distributed IDS/IPS, security administrators can augment or replace discrete appliances.



Application denial of service and client and server exploits have the following characteristics:

- Application denial of service: A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests.
- Client-side and server-side exploits: Client-side attacks exploit the trust between users and the website or server that they visit. Common client-side and server-side exploits are as follows:
  - Spoofing: Tricking the user into believing a website or server is legitimate.
  - Cross-site scripting (XSS): Executes code in the user's web browser with the aim of controlling a user's session or stealing login credentials.

With NSX Distributed IDS/IPS, security administrators can replace or augment discrete appliances. By using native IDS/IPS capabilities in NSX, you can replace traditional IDS/IPS appliances, including standalone, firewall-based, or virtual host-based solutions. You might also decide to keep the traditional IDS/IPS appliances, while using NSX Distributed IDS/IPS for additional east-west traffic protection.



## 8-8 About Behavior-Based IDS/IPS

Behavior-based IDS/IPS helps to detect unusual traffic, malicious attacks, and security breaches in the network when compared to a baseline of normal traffic.

Behavior-based IDS/IPS does not require a separate installation because it is part of the NSX Distributed IDS/IPS implementation.

Behavior-based IDS/IPS helps in the following scenarios:

- Identifying periodic callback behavior
- Identifying a client with a high failure rate in SSH authentication with a server
- Tunneling of network data over anonymous proxies such as TOR

Intrusion detection focuses on the use of knowledge-based signatures. These signatures incorporate specific knowledge about an attack.

Behavior-based IDS/IPS attempts to identify anomalous behavior by pinpointing potentially interesting events that are different or unusual compared to a baseline of normal traffic.

Behavior-based IDS/IPS also helps to detect and prevent possible zero-day attacks.

A few examples of such alerts:

- Identifying periodic callback behavior in a given flow: A variety of remote access Trojan (RAT) toolkits expose this type of behavior when checking in with a command-and-control server. RATs are a type of malware threat where an attacker takes control of your computer.
- Identifying a client with a high failure rate in SSH authentication with a server (can indicate a credential enumeration attack).
- Tunneling of network data over anonymous proxies such as TOR (not necessarily malicious, but unusual in an enterprise environment). TORs aim to conceal users' identities and their online activity from surveillance and traffic analysis by separating identification and routing.

## 8-9 Requirements for NSX Distributed IDS/IPS

Before using NSX Distributed IDS/IPS, administrators must consider the following factors:

- The NSX Distributed IDS/IPS components are installed as part of the host preparation.
- NSX Distributed IDS/IPS can be enabled at the vSphere cluster level and for standalone ESXi hosts.
- You can configure NSX Manager to download intrusion detection signatures from the Internet or manually download and upload the signatures to NSX Manager.
- The NSX environment must be configured with a valid license for NSX Distributed IDS/IPS.

For additional information about the type of licenses that are valid for NSX Distributed IDS/IPS, see the VMware NSX Datasheet at

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf>.

# 8-10 About IDS/IPS Signatures

An IDS/IPS signature contains metadata that is used to identify an attacker's attempt to exploit a known operating system or application vulnerability.

NSX Manager downloads IDS/IPS signatures daily from a cloud-based signature repository.

Signatures are classified into the following severity categories:

- Critical
- High
- Medium
- Low
- Suspicious

```
alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET EXPLOIT Adobe Coldfusion BlazeDS Java Object
Deserialization Remote Code Execution"; flow:established,to_server; content:"/amf"; http_uri;
content:"sun.rmi.server.UnicastRef"; http_client_body; content:"|f9 6a 76 7b 7c de 68 4f 76 d8 aa 3d 00 00 01 5b b0
4c 1d 81 80 01 00|"; fast_pattern; reference:url,exploit-db.com/exploits/43993/; reference:cve,2017-3066;
classtype:attempted-user; sid:2025836; rev:2; metadata:attack_target Server, affected_product adobe_coldfusion,
affected_version 11.0, cvssv2 10.0, cvssv3 9.8, created_at 2018_07_13, deployment Datacenter, former_category
EXPLOIT, performance_impact Low, signature_severity Major, updated_at 2020_08_25;)
```

<input type="checkbox"/>	Signature ID	IDS Severity	Details	Product Affected	Attack Target	Attack Type	CVSS	CVE(S)	Action ⓘ	State
<input type="checkbox"/>	2025836	HIGH	ET EXPLOIT Adobe Coldfusion BlazeDS Java Object Deserialization Remote Code Execution	adobe_coldfusion	Server	attempted-user	9.8	2017-3066	Alert ▾	<input checked="" type="checkbox"/>

An IDS/IPS signature contains metadata that is used to identify an attacker's attempt to exploit a known operating system or application vulnerability. Such metadata provides context about the attempt, such as the affected product, attack target, and so on.

IDS/IPS signatures are matched against traffic headers by using regular expressions.

NSX Manager downloads IDS/IPS signatures daily.

IDS/IPS signatures are classified into severity categories based on their Common Vulnerability Scoring System (CVSS) score.

# 8-11 About IDS/IPS Profiles

An IDS/IPS profile defines the IDS signatures that are included or excluded from detection.

	Name	Description	Tags	Status
<div><div></div><div></div></div>	DefaultIDSProfile		0	<div><div></div>Success</div>
<div><div>IDS Signatures</div><div>Included: 3105 Total: 6614</div><div><div></div>Critical (3105)</div><div><div></div>Additional Options</div><div>Filter intrusion signatures to include in this profile by attack type, CVSS and more.</div><div><div>Attack Types</div><div>0</div><div>CVSS</div><div>0</div><div>Attack Targets</div><div>0</div><div>Products Affected</div><div>0</div></div><div>Manage (optional) - change actions and/or exclude signatures specific to this profile. 0</div><div>Note: the available list of intrusion signatures to customize is based upon the selected attributes above.</div></div>				

The default IDS profile is configured to include all signatures that are labeled as critical.

## 8-12 About IDS/IPS Policies and Rules

An IDS/IPS policy is a collection of IDS/IPS rules. An IDS/IPS rule contains a set of instructions that determine which traffic is analyzed, including values for the following parameters:

- Sources and Destinations
- Services
- Security Profiles (IDS/IPS profile)
- Applied to
- Mode



	Name	ID	Sources	Destinations	Services	Security Profiles	Applied To	Mode	
	IDS/IPS Policy	(1)							Success
	IDS/IPS Rule	3048	Any	Any	Any	IDS/IPS Profile	DMZ	<b>Detect Only</b>	Success

IDS rules can be applied to the distributed firewall or to specific groups.

NSX includes the following modes for an IDS/IPS rule:

- Detect Only: Detects signatures and does not take any action on the traffic. It records and logs the intrusion.
- Detect & Prevent: Detects signatures and performs the action specified by the security administrator. Available actions are alert, drop, and reject.

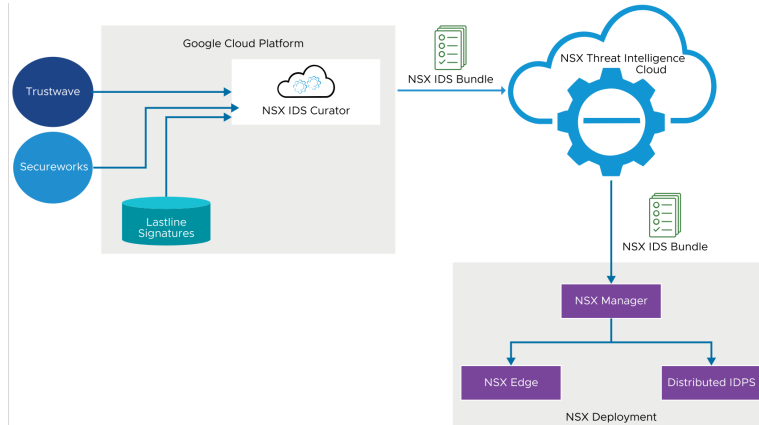
Different rules can be configured with different modes.

You typically start with the Detect Only mode. After tuning for false positives, you change to Detect & Prevent.

## 8-13 IDS/IPS Signature Curation

The NSX IDS curator engine combines the IDS signatures from Trustwave, Secureworks, and Lastline into a single signature set, which it pushes, as an NSX IDS bundle, to NSX Threat Intelligence Cloud.

NSX Threat Intelligence Cloud forwards the NSX IDS bundle to NSX Manager for consumption in the NSX environment.



The NSX IDS curator engine combines the IDS signatures from Trustwave, Secureworks, and Lastline into a single signature set and pushes it as an NSX IDS bundle to NSX Threat Intelligence Cloud. NSX Threat Intelligence Cloud forwards the NSX IDS bundle to NSX Manager for consumption in the NSX environment.

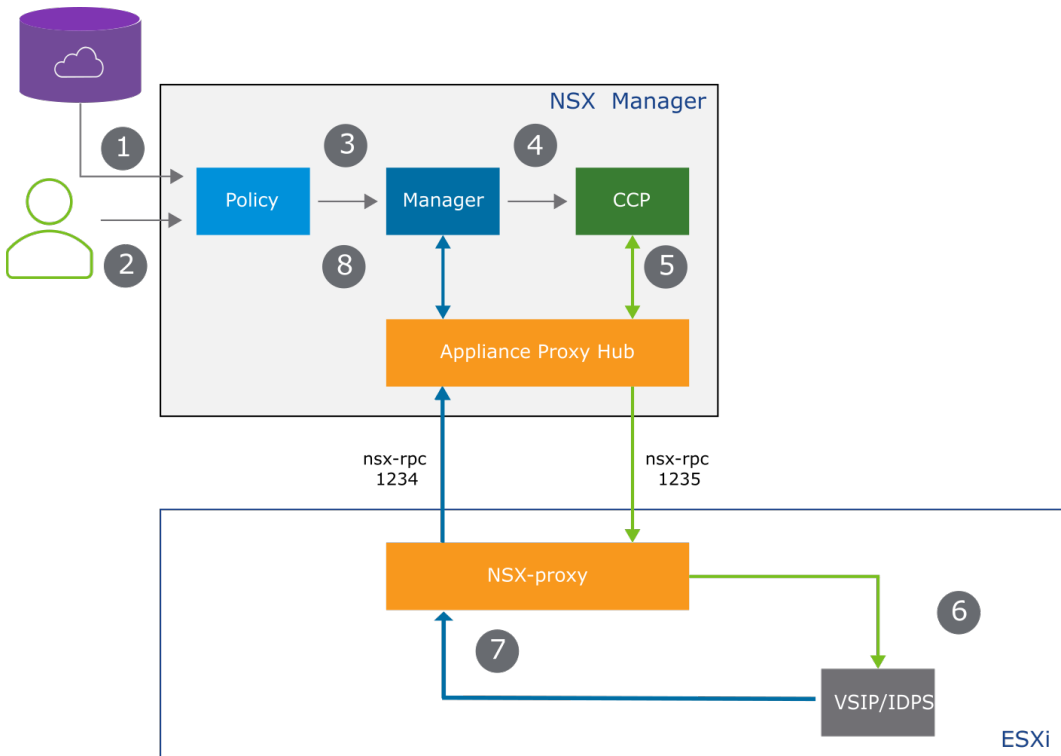
The NSX IDS curator engine performs the following tasks in the back end:

- Identifies low-quality signatures:
  - Avoids false positives.
  - Identifies noisy signatures.
- Identifies redundant signatures:
  - If two signatures match the same traffic, only one signature is kept.
- Adds signature metadata for the NSX UI fields:
  - MITRE ATT&CK tactics and techniques.
  - Impact, severity, and confidence levels.
- Ensures consistent values for existing signature metadata:
  - CVSS scores, signature\_severity, attack\_target, and classtype.

## 8-14 NSX Distributed IDS/IPS Architecture

NSX Distributed IDS/IPS operates as follows:

1. NSX Manager downloads curated IDS/IPS signatures from NSX Threat Intelligence Cloud.
2. Users configure IDS/IPS profiles and rules.
3. Policy stores the IDS/IPS configuration and passes it to NSX Manager.
4. NSX Manager passes the information to the central control plane (CCP).
5. CCP pushes the IDS/IPS configuration to hosts through the appliance proxy hub.
6. The ESXi hosts store the signature information locally and configure the datapath.
7. The ESXi hosts collect traffic data and send events to NSX Manager.
8. NSX Manager parses and displays these events in the UI.



VSIP

IDS signatures are written into the IDS module in the datapath, and IDS rules are stored in the VSIP module.

VSIP evaluates traffic against IDS rules. If a match is found, the packet is sent to IDS.

The IDS module evaluates the packets against IDS signatures.

Distributed firewall rules are always evaluated before distributed IDS/IPS rules. If a distributed firewall rule rejects a traffic flow, this traffic is never evaluated by IDS/IPS.

# 8-15    Configuring NSX Distributed IDS/IPS

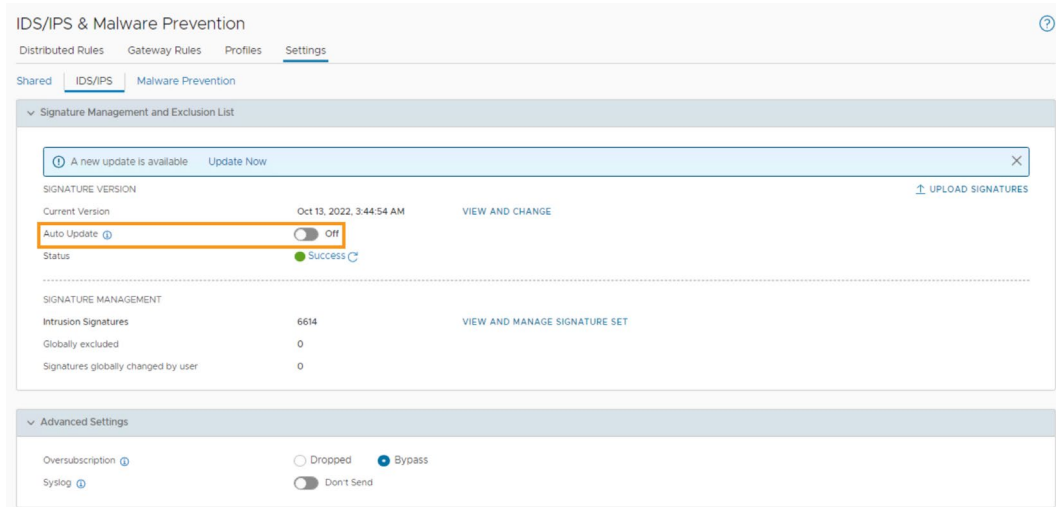
To enable distributed intrusion detection and prevention for standalone hosts or clusters, you select **Security > IDS/IPS & Malware Prevention > Settings > Shared**.





## 8-16 Configuring IDS/IPS Signatures

On the **IDS/IPS** tab, you can configure and manage signatures under Settings.



If the **Auto Update** toggle is On, signatures are automatically applied to the ESXi hosts after they are downloaded from the cloud. If the toggle button is Off, the signatures are stopped at the listed version.

# 8-17 Global Intrusion Signature Management

With Global Intrusion Signature Management, you can override the default action for a given signature and globally disable signatures that are not relevant to your environment.

Global Intrusion Signature Management

Globally customize recommended actions or exclude specific signatures to tailor fit your environment.

ACTION

EXCLUDE GLOBALLY

RESET

Take actions on multiple selected signatures.

Globally disable signature.

Details, Product

	Signature ID	IDS Severity	Details	Product Affected	Attack Target	Attack Type	CVSS	CVE(S)	Action	State
<input type="checkbox"/>	>	1060759	Critical	NSX - Detect Fareit	NONE	Client_Endpoint	trojan-activity		Reject	<input type="checkbox"/>
<input type="checkbox"/>	>	106083801	Critical	NSX - Detect Lethic	NONE	Client_Endpoint	trojan-activity		Reject	<input type="checkbox"/>
<input type="checkbox"/>	>	1060862	Critical	NSX - Detect Slingup	NONE	Client_Endpoint	trojan-activity		Alert	<input type="checkbox"/>
<input checked="" type="checkbox"/>	>	1060921	Critical	NSX - Detect Zeus activity	NONE	Client_Endpoint	trojan-activity		Alert	<input type="checkbox"/>
<input type="checkbox"/>	>	1060928	Critical	NSX - (Command and Control) Detect Napolar C&C communication	NONE	Client_Endpoint	trojan-activity		Alert	<input type="checkbox"/>
<input type="checkbox"/>	>	1061110	Critical	NSX - Detect DNSUnlocker	NONE	Client_Endpoint	trojan-activity		Alert	<input type="checkbox"/>
<input type="checkbox"/>	>	1061111	Critical	NSX - Detect Teslacrypt	NONE	Client_Endpoint	trojan-activity		Alert	<input type="checkbox"/>
<input type="checkbox"/>	>	1061143	Critical	NSX - Detect Teslacrypt	NONE	Client_Endpoint	trojan-activity		Alert	<input type="checkbox"/>
<input type="checkbox"/>	>	1061148	Critical	NSX - Detect Dridex Download	NONE	Client_Endpoint	trojan-activity		Alert	<input type="checkbox"/>
<input type="checkbox"/>	>	1061156	Critical	NSX - Detect Locky	NONE	Client_Endpoint	trojan-activity		Reject	<input type="checkbox"/>

Recommended Action

Alert

Alternative Actions

Drop

Reject

Globally override the action recommended by VMware.

1 REFRESH

< 1 / 133 >

1 - 50 of 6614

Show only User modified signatures

CANCEL

SAVE

If a signature is disabled globally, it is removed from custom profiles. You cannot include the disabled signature in newly created custom profiles.

All signatures are preconfigured with a default action that is recommended by VMware. You can override this action globally or per profile.

The following actions are available:

- Alert: This action is typically used in new deployments or for new signatures.
- Drop and Reject actions are commonly used in the following circumstances:
  - High-fidelity signatures with no false positives
  - High-impact exploits
  - After a signature is deployed in alert-only mode

Dropping a packet is a silent action with no notification to the source and destination systems. Rejecting a packet is a more graceful way to deny a packet because it sends a destination unreachable message to the sender. The drawback with rejecting a packet is that it can notify a potential attacker of the defense invoked.

## 8-18 Configuring Custom IDS/IPS Profiles

Using custom IDS/IPS profiles, you specify the IDS signatures that you want to include or exclude for detection based on their severity, attack type, attack target, CVSS, and affected products.

IDS/IPS & Malware Prevention

Distributed Rules Gateway Rules Profiles Settings

IDS/IPS Malware Prevention

ADD PROFILE EXPAND ALL Filter by Name, Path and more

Name	Description	Tags	Status
IDS/IPS Profile	IDS/IPS Profile for critical, high and suspicious signatures.	Tag Scope	

IDS Signatures Included: 6591 Total: 6614

Intrusion Severities

☒ Critical (3105) ☒ High (3119) ☐ Medium (22) ☐ Low (1) ☒ Suspicious (367)

Additional Options

Filter intrusion signatures to include in this profile by attack type, CVSS and more.

Attack Types Select CVSS Select

Attack Targets Select Products Affected Select

Manage (optional) - change actions and/or exclude signatures specific to this profile. Manage signatures for this profile >>

Note: the available list of intrusion signatures to customize is based upon the selected attributes above.

SAVE CANCEL

DefaultIDSPProfile 0 Success

Creating granular workload-specific profiles reduces noise and false positives in your environment.

You create custom IDS profiles by selecting **Security > IDS/IPS & Malware Prevention > Profiles**.

You configure the IDS signatures that you want to include or exclude for detection based on their severity and more granular criteria:

- **Attack Types:** Categorizes signatures by attack techniques such as Trojan activity or attempted denial of service (DoS). The types align with the MITRE ATT&CK framework.
- **Attack Targets:** Broad category of possible attack targets such as IoT, mobile client, or networking equipment.
- **CVSS:** Include or exclude signatures based on their CVSS score range (none, low, medium, high, and critical).
- **Products Affected:** Signatures specific to vulnerable applications or operating systems.

Globally disabled signatures are not available for inclusion in profiles.

You can also click the **Manage signatures for this profile** link to disable individual profile signatures that might not be relevant to your workloads, or to override the global action configured for a given signature.

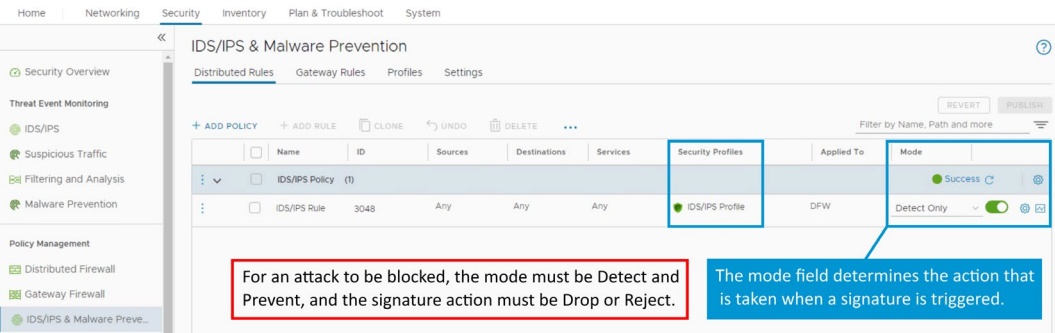
Suspicious IDS signatures are used to detect traffic anomalies in the network.

In a similar way, you create an IDS/IPS profile to specify the IDS signatures that you want to include or exclude for the detection of your north-south traffic.

## 8-19    Configuring IDS/IPS Rules

You specify how traffic is managed in your environment by configuring one or more rules with an IDS profile and the mode of operation.

As with distributed firewall rules, IDS/IPS rules are evaluated from top to bottom.



To create IDS policies and rules, you select **Security > Policy Management > IDS/IPS & Malware Prevention > Distributed Rules**.

The Sources, Destinations, Services, and Applied To values work in the same way as those in a distributed firewall rule.

IDS Profile specifies the group of signatures that the traffic is matched against.

Mode determines the action that is taken when a signature is triggered.

The following modes are available for an IDS/IPS rule:

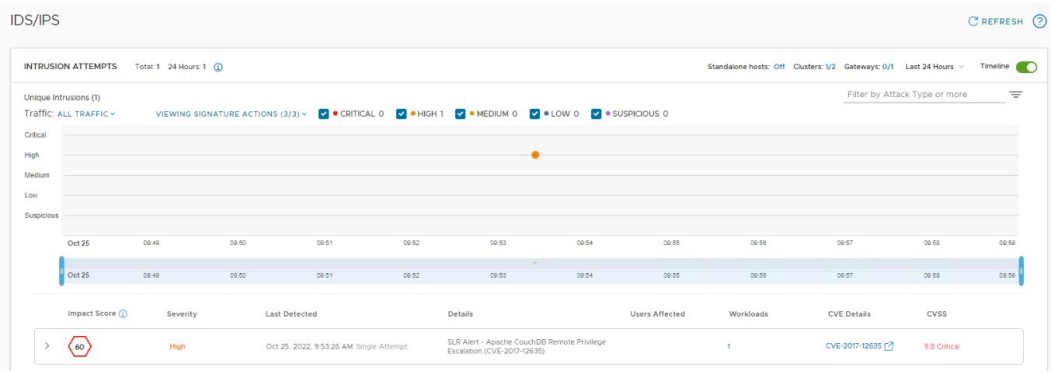
- Detect Only: Regardless of the global or per-signature action, only alerts are generated, and no preventive action is taken. This mode is equivalent to an intrusion detection system.
- Detect & Prevent: The action that is specified for the given signature either globally or at the profile level is taken (alert, drop, reject). The action that is specified at the profile level overrides the action configured globally. This mode is equivalent to an inline intrusion prevention system.

When configuring IDS/IPS rules, do not use the drop action in a rule that is configured with a security profile that includes suspicious-level signatures. With this configuration, you guarantee that any abnormal traffic is inspected.

Like distributed firewall rules, IDS/IPS rules are evaluated from top to bottom. You must place the most hit rules at the top to avoid the unnecessary evaluation of subsequent rules.

# 8-20 Monitoring IDS/IPS Events (1)

To monitor IDS/IPS events, you select **Security > Threat Event Monitoring > IDS/IPS**.



The **Events** tab shows all intrusion attempts that are detected by the system:

- Critical severity signature events appear in red.
- High severity signature events appear in orange.
- Medium severity signature events appear in yellow.
- Low severity signature events appear in gray.
- Suspicious signature events appear in purple.

Administrators can filter events based on their severity. Free-form text is also available for further filtering of events.

IDS events are graphically represented by using a histogram. Security administrators can specify the period that they are interested in by adjusting the vertical lines in the diagram.

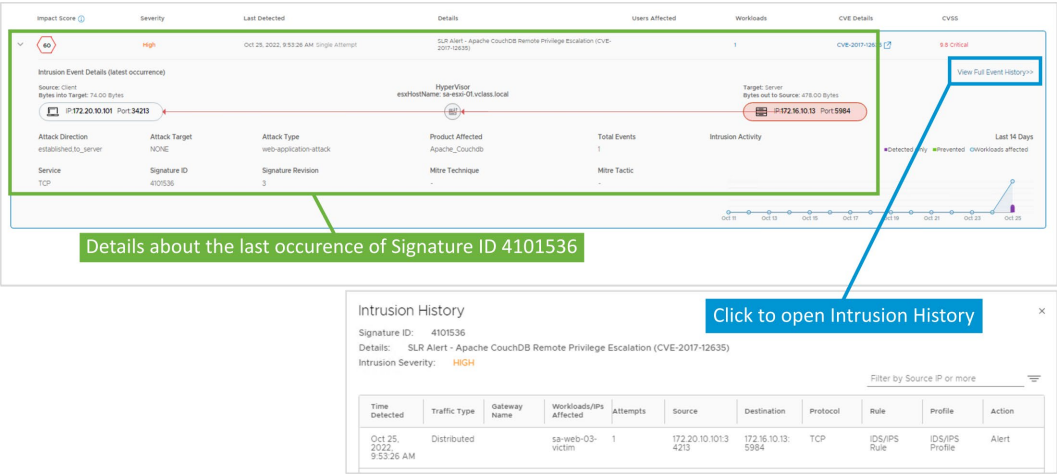
Each IDS/IPS event type is represented by a dot in the histogram. The size of the dot is proportional to the number of occurrences of an event.

Additional information about each type of event appears in a tabular format.

NSX Manager keeps the last 14 days of data or up to 1.5 million records.

# 8-21 Monitoring IDS/IPS Events (2)

Each event can be expanded to retrieve details about the intrusion attempt, including the attacker, victim, protocol, attack type, and so on.



Each event can be expanded to retrieve the following details:

- Signature ID
- Severity
- Details or description of the event
- Product affected
- Users affected
- VMs affected

Additional information appears for the last occurrence of the event:

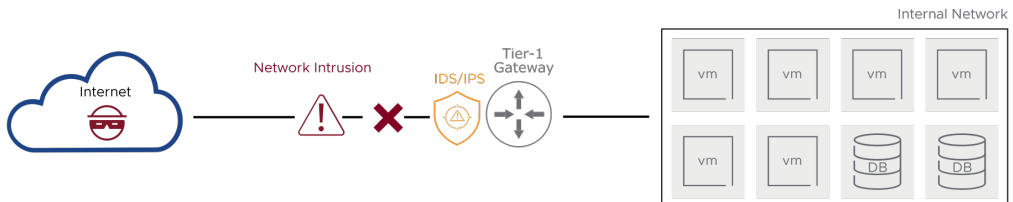
- Attacker and target IP addresses
- Bytes exchanged
- Attack and traffic flow direction

The Intrusion Activity diagram shows the occurrences for a particular signature event .

## 8-22 About North-South IDS/IPS

North-South IDS/IPS uses real-time deep packet inspection to identify and prevent attempts at exploiting vulnerabilities in your applications:

- Protects north-south traffic and prevents malicious traffic from entering your internal network
- Uses signatures to identify malicious traffic patterns
- Is enabled on a Tier-1 gateway



## 8-23 Use Cases for North-South IDS/IPS

You can configure North-South IDS/IPS for the following use cases:

- Detecting and preventing intrusions for north-south traffic based on signatures
- Detecting and preventing intrusion attempts across different zones in the data center
- Detecting and reporting suspicious anomalies in the network

## 8-24 Requirements for Configuring North-South IDS/IPS

Before using North-South IDS/IPS, security administrators must consider the following factors:

- NSX Manager has Internet connectivity to download the signatures from the cloud-based store. Proxy settings can be configured if necessary.
- North-South IDS/IPS is supported on a Tier-1 gateway that is backed by an NSX Edge cluster.
- The NSX environment is configured with a valid license for North-South IDS/IPS.

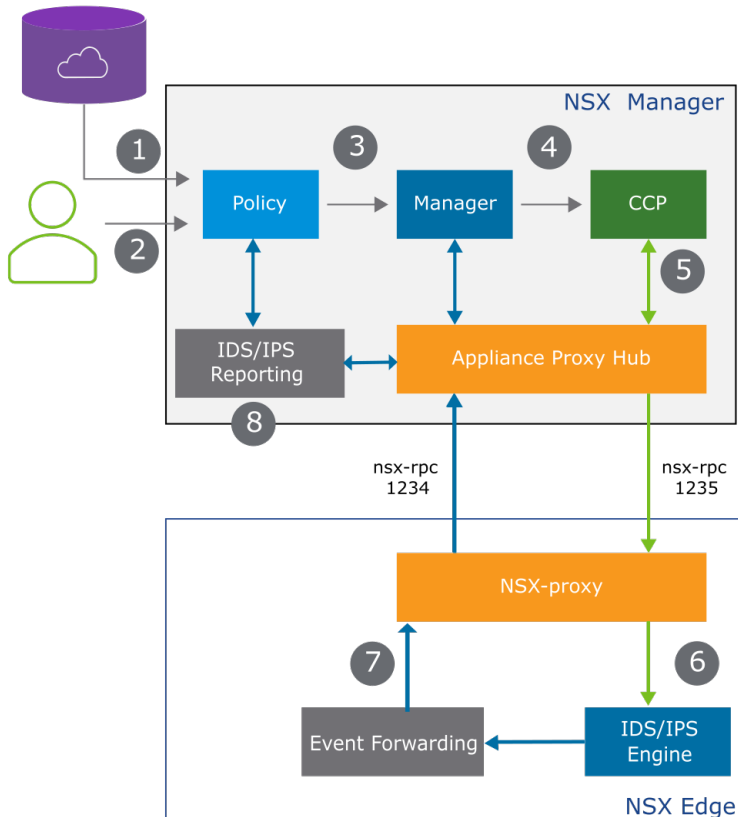
Additional gateway security capabilities are available with NSX security add-on licenses.



## 8-25 North-South IDS/IPS Architecture

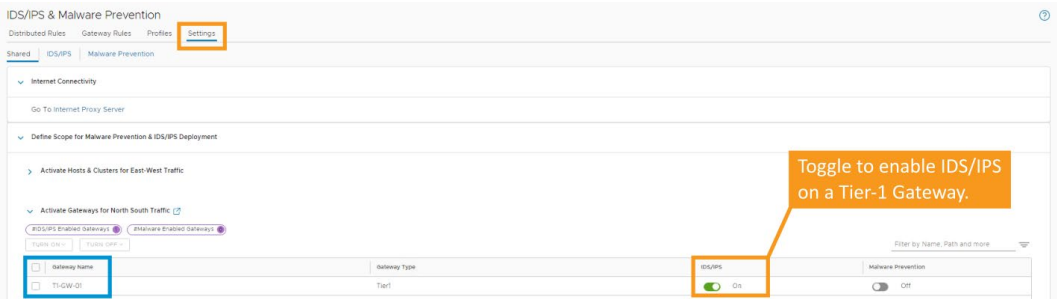
North-South IDS/IPS works as follows:

1. NSX Manager downloads IDS/IPS signatures from a cloud-based store.
2. NSX Policy stores the IDS/IPS configuration information in the database.
3. NSX Policy passes the information to NSX Manager.
4. NSX Manager passes the information to the CCP.
5. CCP pushes the IDS/IPS configuration through APH to NSX Edge using the NSX-proxy.
6. NSX Edge stores the signature information locally and configures the datapath.
7. The Event Forwarding module collects traffic data and sends events to NSX Manager.
8. IDS/IPS reporting on NSX Manager parses and shows these events in the NSX UI.



# 8-26 Configuring North-South IDS/IPS

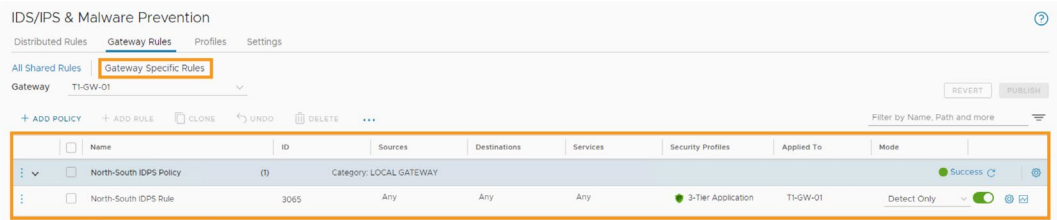
To enable north-south intrusion detection and prevention for Tier-1 gateways, you select **Security > IDS/IPS & Malware Prevention > Settings**.



# 8-27 Configuring North-South IDS/IPS Rules

You specify how traffic is managed in your environment by configuring one or more rules with an IDS profile and the mode of operation.

As with gateway firewall rules, gateway specific IDS/IPS rules are evaluated from top to bottom.



You create IDS policies and rules for a specific Tier-1 gateway by navigating to **Security > Policy Management > IDS/IPS & Malware Prevention > Gateway Rules** and selecting the relevant Tier-1 gateway

You create IDS policies and rules, which are shared between multiple gateways, by navigating to **Security > Policy Management > IDS/IPS & Malware Prevention > All Shared Specific Rules**.

The Sources, Destinations, Services, and Applied To fields operate in the same way as those in a gateway firewall rule.

Security Profiles specify the group of signatures that the traffic is matched against.

The Mode field in a North-South IDS/IPS rule determines the action that is taken when a signature is triggered.

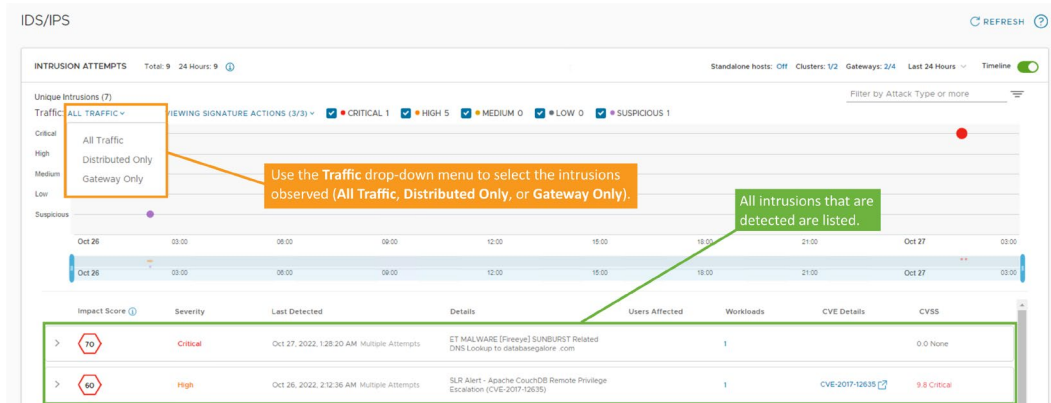
The following modes are available for a North-South IDS/IPS rule:

- Detect Only: Regardless of the global or per-signature action, only alerts are generated, and no preventive action is taken. This mode is equivalent to an intrusion detection system.
- Detect & Prevent: The action specified for the given signature either globally or at the profile level is taken (alert, drop, reject). The action specified at the profile level overrides the action configured globally. This mode is equivalent to an inline intrusion prevention system.

As with gateway firewall rules, the North-South IDS/IPS rules are evaluated from top to bottom. You must place the most hit rules at the top to avoid the unnecessary evaluation of subsequent rules.

## 8-28 Monitoring North-South IDS/IPS Events

You monitor North-South IDS/IPS events by navigating to **Security > Threat Event Monitoring > IDS/IPS**.



The same dashboard is used to monitor the north-south IDS/IPS events as in distributed IDS/IPS.

## 8-29 Lab 13: Configuring Distributed Intrusion Detection and Prevention

Configure Distributed Intrusion Detection and analyze malicious traffic:

1. Prepare for the Lab
2. Enable Distributed Intrusion Detection and Prevention
3. Download the Intrusion Detection and Prevention Signatures
4. Create an Intrusion Detection and Prevention Profile
5. Configure Intrusion Detection Rules
6. Generate Malicious Traffic
7. Create a Segment and Attach a VM
8. Generate Suspicious Traffic
9. Analyze Intrusion Detection Events
10. Modify the IDS/IPS Settings to Prevent Malicious Traffic
11. Generate and Analyze Intrusion Prevention Events

## 8-30 Review of Learner Objectives

- Explain IDS/IPS and its use cases
- Define the IDS/IPS terminologies
- Describe the IDS/IPS architecture
- Configure IDS/IPS
- Interpret IDS/IPS events

## 8-31 Lesson 2: NSX Application Platform

### 8-32 Learner Objectives

- Describe NSX Application Platform and its use cases
- Deploy NSX Application Platform
- Explain the NSX Application Platform architecture and services

### 8-33 About NSX Application Platform

NSX Application Platform is a container-based solution that is deployed on an existing Kubernetes cluster.

You must deploy NSX Application Platform before using the following NSX security features:

- NSX Malware Prevention
- NSX Intelligence
- NSX Network Detection and Response
- NSX Metrics

Before deploying NSX Application Platform, you must understand the concepts presented in the course *Kubernetes Fundamentals* at

<https://learning.customerconnect.vmware.com/oltpublish/site/program.do?dispatch=showCourseSession&id=663f8ec8-4078-11eb-8643-0cc47adeb5f8>.

## 8-34 Prerequisites for NSX Application Platform Deployment

To deploy NSX Application Platform, your environment must comply with the following prerequisites:

- Valid, non-expired NSX license
- Tanzu Kubernetes cluster (TKC) v1.20 through v1.22 or upstream Kubernetes v1.20 through v1.24.
- Network connectivity between your microservices environment and the NSX Management cluster
- Working DNS instance
- Time synchronized between NSX, vSphere, and your Kubernetes environments
- (Optional) Private Harbor registry with a chart repository service configured

This final item is only required if your Kubernetes environment does not have access to the Internet or if you have specific security restrictions.

For more information about the NSX Application Platform deployment prerequisites, including the supported Tanzu Kubernetes cluster and upstream Kubernetes versions, see *Deploying and Managing the VMware NSX Application Platform* at <https://docs.vmware.com/en/VMware-NSX/4.0/nsx-application-platform/GUID-D54C1B87-8EF3-45B3-AB27-EFE90A154DD3.html>

The use of a private Harbor instance is required if your Kubernetes environment does not have access to the Internet or you have specific security restrictions.

However, if your Kubernetes environment has external connectivity, you can use registry and repository hosted by VMware to simplify the NSX Application Platform deployment process. This deployment process uses an outbound connection only and does not retain customer data.

# 8-35 Setting Up a Private Harbor Registry

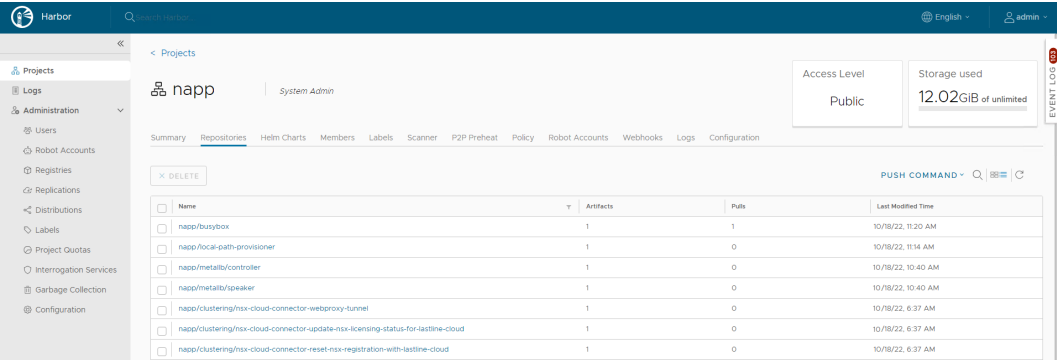
If your Kubernetes environment does not have access to the Internet, you must set up a private Harbor registry with a chart repository service before you deploy NSX Application Platform.

You then use this registry to upload the Helm charts and Docker images required to deploy NSX Application Platform.

The Helm charts specify the configuration settings to be used for the deployment.

The Docker images include the container images to be used for the deployment.

For production environments, the private Harbor instance must be configured using external certificate authority (CA)-signed certificates.



VMware Harbor Registry is an enterprise-class registry server that stores and distributes container images.

See the chapter about uploading the NSX Application Platform Docker images and Helm charts in *Deploying and Managing the VMware NSX Application Platform* at <https://docs.vmware.com/en/VMware-NSX/4.0/nsx-application-platform/GUID-FAC9DBE3-A8EE-4891-A723-942D0AB679F6.html#GUID-FAC9DBE3-A8EE-4891-A723-942D0AB679F6>

## 8-36 NSX Application Platform Form Factors

Based on the required features, NSX Application Platform can be deployed in different form factors:

- Standard
- Advanced
- Evaluation

The screenshot shows a web interface for selecting a form factor for a Kubernetes cluster configuration. At the top, it says "Form Factor\*" with a help icon. Below this, a message states: "The following form factors are applicable for your Kubernetes cluster configuration. Choose the form factor that supports the features that you need. [Learn more](#)".

There are two main sections: "Production Use" and "Non-production Use Only".

**Production Use**

- Standard** (1 Control & 3 Worker Kubernetes Nodes) - This option is selected with a blue checkmark.
  - Per Node:** 4 vCPU, 16 GB RAM, 200 GB Storage
  - Supported Features:** NSX Network Detection and Response, NSX Malware Prevention, Metrics
- Advanced** (1 Control & 3 Worker Kubernetes Nodes) - This option is not selected.
  - Per Node:** 16 vCPU, 64 GB RAM, 1 TB Storage
  - Supported Features:** NSX Network Detection and Response, NSX Malware Prevention, Metrics, NSX Intelligence

**Non-production Use Only**

- Evaluation** (1 Control & 1 Worker Kubernetes Nodes) - This option is not selected.
  - Per Node:** 16 vCPU, 64 GB RAM, 1 TB Storage
  - Available Features:** NSX Network Detection and Response, NSX Malware Prevention, Metrics, NSX Intelligence

The NSX Application Platform form factors have the following features:

- Standard:
  - Supports NSX Network Detection and Response, NSX Malware Prevention, and Metrics
  - Requires one controller and three worker nodes in the Kubernetes cluster
- Advanced:
  - Supports NSX Network Detection and Response, NSX Malware Prevention, NSX Intelligence, and Metrics
  - Requires one controller and three worker nodes in the Kubernetes cluster
- Evaluation:
  - Supports all available features
  - Requires one controller and one worker node in the Kubernetes cluster

This form factor is not supported in production environments. It is intended only for evaluation or proof-of-concept.



## 8-37 NSX Application Platform Deployment (1)

You deploy NSX Application Platform from the NSX UI by selecting **System > Configuration > NSX Application Platform**.

The Helm Repository and Docker Registry URLs must point to the registry and repository hosted by VMware or to your private Harbor instance.

[< BACK TO NSX APPLICATION PLATFORM](#)

Deploy NSX Application Platform

[Prepare to Deploy](#) > [Configuration](#) > [Precheck Platform](#) > [Review & Deploy](#)

Helm Repository\* ⓘ

[https://projects.registry.vmware.co...](https://projects.registry.vmware.com/)

CLEAR

Docker Registry\* ⓘ

[projects.registry.vmware.com/nsx\\_a...](https://projects.registry.vmware.com/nsx_a...)

CLEAR

NOTE: If your Kubernetes cluster does not have access to the Internet, download the Helm chart and Docker image files locally and use the URLs to those local copies. [Learn more](#) ⓘ

Platform Target Version ⓘ

[4.0.1-0.0-2060](#) ▾

Chart Name ⓘ

[NSX Application Platform](#)

# 8-38 NSX Application Platform Deployment (2)

During deployment, you must specify the configuration file for the underlying Kubernetes infrastructure. You also select the form factor based on your feature requirements.

[BACK TO NSX APPLICATION PLATFORM](#)

Deploy NSX Application Platform

Prepare to Deploy

Configuration

Precheck Platform

Configuration file for the Kubernetes cluster where the NSX Application Platform is to be deployed.

Kubernetes Configuration

Upload File\*

config

SELECT

UPLOAD

Uploaded

View Details

Cluster Type

Standard

Storage Class\*

local-path

Interface Service Name\*

k8s.vclass.local

Messaging Service Name\*

mk8s.vclass.local

Form Factor

The following form factors are applicable for your Kubernetes cluster configuration. Choose the form factor that supports the features that you need. [Learn more](#)

Production Use

Standard

(1 Control & 3 Worker Kubernetes Nodes)

Per Node

4 vCPU

16 GB RAM

200 GB Storage

Supported Features

NSX Network Detection and Response

NSX Malware Prevention Metrics

Advanced

(1 Control & 3 Worker Kubernetes Nodes)

Per Node

16 vCPU

64 GB RAM

1 TB Storage

Supported Features

NSX Network Detection and Response

NSX Malware Prevention Metrics

NSX Intelligence

Non-production Use Only

Evaluation

(1 Control & 1 Worker Kubernetes Nodes)

Per Node

16 vCPU

64 GB RAM

1 TB Storage

Available Features

NSX Network Detection and Response

NSX Malware Prevention Metrics

NSX Intelligence

Select the form factor based on the security features you are planning to use in your environment.

The configuration file for the Kubernetes cluster must be stored locally in the machine where NSX Application Platform deployment is being initiated. This file typically has a YAML format that must be provided by your Kubernetes administrator.

The exact steps required to obtain the Kubernetes cluster configuration file depend on the platform on which your Kubernetes cluster is running.

426

Technet24

In vSphere with Tanzu environments, you must work with your infrastructure administrator to create a kubeconfig file with a long-lived token to be used in the NSX Application Platform deployment. See the chapter about generating a TKC configuration file with a non-expiring token in *Deploying and Managing the VMware NSX Application Platform* at <https://docs.vmware.com/en/VMware-NSX/4.0/nsx-application-platform/GUID-52A52C0B-9575-43B6-ADE2-E8640E22C29F.html>

You can then use a file transfer utility to copy the YAML configuration file to your local system.

Apart from specifying the configuration file for the Kubernetes cluster and the desired form factor for the NSX Application Platform, you must also configure the following parameters during NSX Application Platform deployment:

- **Interface Service Name (FQDN):** The Interface Service Name is used as the HTTPS endpoint to connect to NSX Application Platform.

You must configure the FQDN with a static IP address in the DNS server before the NSX Application Platform deployment. The TKC or upstream Kubernetes cluster infrastructure must be able to assign this static IP address.

- **Messaging Service Name:** The Messaging Service Name value is an FQDN for the HTTPS endpoint that is used to receive the streamlined data from the NSX data sources.

# 8-39 NSX Application Platform Predeployment Checks

Before proceeding with the deployment of NSX Application Platform, the wizard checks the connection, resources, and correct configuration of the specified Kubernetes cluster.

< BACK TO NSX APPLICATION PLATFORM

Deploy NSX Application Platform

Prepare to Deploy > Configuration > Precheck Platform > Review & Deploy

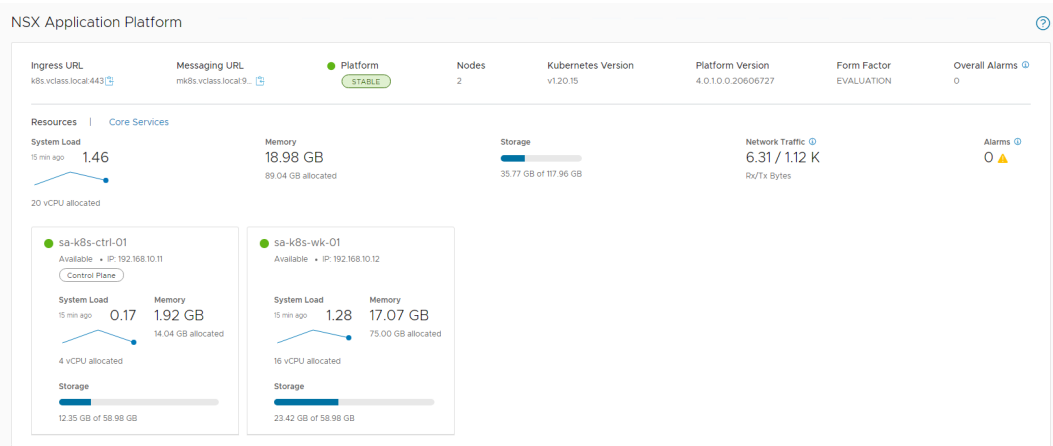
RUN PRECHECKS

STOP PRECHECKS

Name	Description	Status	Details
Version Compatibility Precheck	Check NSX Application Platform version compatibility	Completed	
Kubernetes Cluster Connection Precheck	Check connectivity between NSX manager and kubernetes cluster	Completed	
Kubernetes Tools Sync Precheck	Check whether kubernetes tools are compatible and sync with all managers	Completed	
Existing Namespaces Precheck	Check existing namespaces in kubernetes cluster	Completed	
Service Name/FQDN Validation Precheck	Check service name/fqdn	Completed	
Kubernetes Cluster DNS Domain Precheck	Check Kubernetes cluster dns domain	Completed	
Time Synchronization Precheck	Kubernetes cluster and NSX time sync	Completed	Warning
Kubernetes Cluster Available Resources Precheck	Check Kubernetes cluster node resources	Completed	

# 8-40 NSX Application Platform Deployment Validation

After the deployment, you can validate the status of NSX Application Platform nodes from the NSX UI.



The example illustrates the nodes available after the deployment of NSX Application Platform with an Evaluation form factor.

This type of deployment includes:

- One controller node: Used as the control plane
- One worker node: Used to perform data processing and analytics tasks

You can review the resource utilization at the overall cluster level, and you can also view the specific resource utilization for each node.

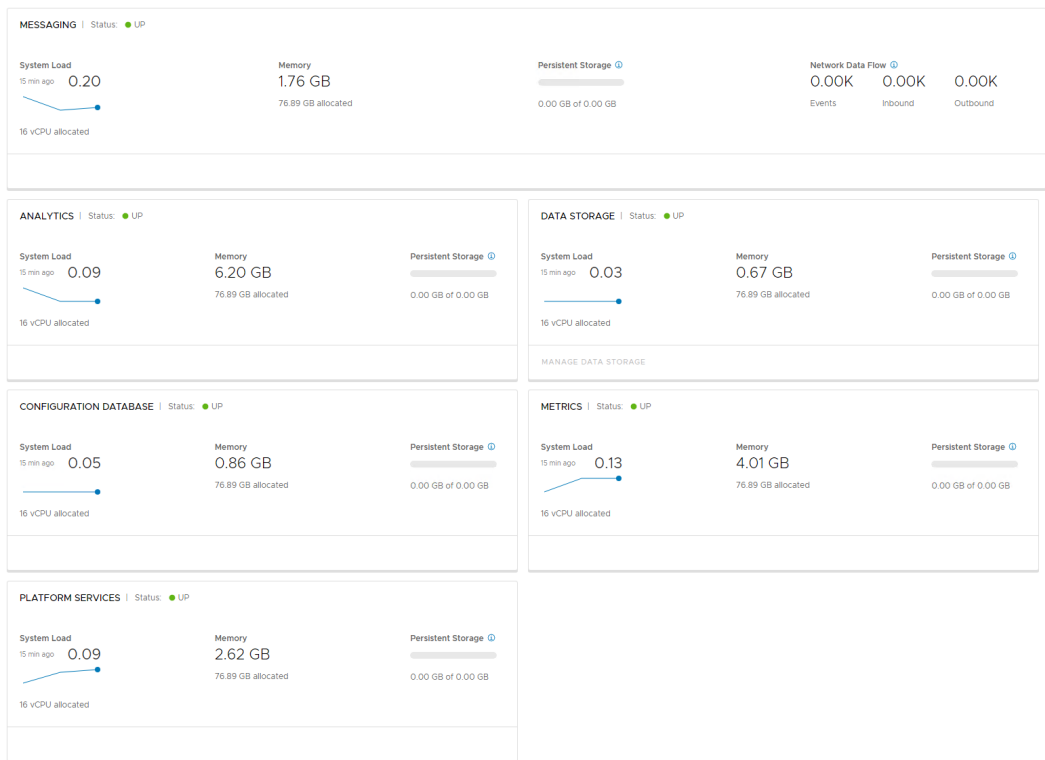
# 8-41 NSX Application Platform Services

The following core services are deployed as part of NSX Application Platform in both the Standard and Advanced form factors:

- Messaging
- Configuration Database
- Platform Services
- Metrics

The following core services are deployed as part of the Advanced form factor only:

- Analytics
- Data Storage



The following core services are deployed as part of NSX Application Platform in both the Standard and Advanced form factors:

- **Messaging:** Includes a distributed messaging system that is responsible for collecting network flows and events from the NSX transport nodes and system configuration from NSX Manager.
- **Configuration Database:** Database system used to store events and recommendations
- **Platform Services:** Includes all services related to certificate and cluster management
- **Metrics:** Collects key performance indicators from the NSX environment.

The following core services are deployed as part of the Advanced form factor only:

- **Analytics:**
  - Processes and correlates the network flows
  - Generates recommendations and events
- **Data Storage:** Includes a distributed database used to persistently store correlated flows

During the deployment of NSX Application Platform with a Standard form factor, only the messaging, configuration database, metrics, and platform services are enabled. Installing additional security features on top of NSX Application Platform with a Standard form factor enables additional services. For example, the installation of Malware Prevention and NSX Network Detection and Response automatically enables the analytics service.

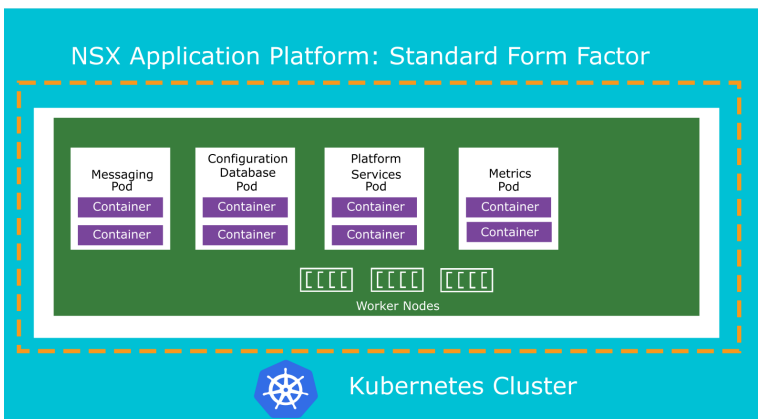
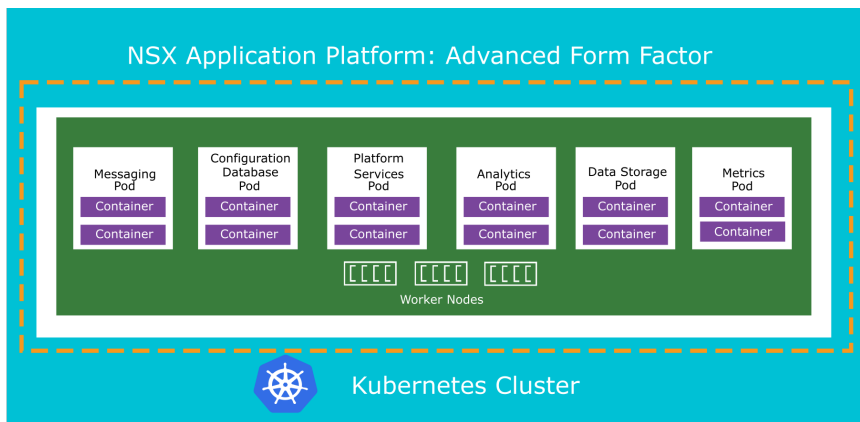
## 8-42 Objects Created During the NSX Application Platform Deployment

During the deployment of NSX Application Platform, several pods are automatically created in the Kubernetes cluster. The number of created pods depends on the form factor.

Pods run in the worker nodes and can run one or more container processes that provide functionality for multiple NSX security features.

One or more pods are deployed per core service of NSX Application Platform.

These pods run in a Kubernetes namespace called nsxi-platform.



## 8-43 Basic kubectl Commands

Because NSX Application Platform is a container-based solution, you must be familiar with the key kubectl commands to perform basic troubleshooting:

- List all the namespaces available in the Kubernetes cluster:

```
kubectl get namespaces
```

- List all pods available for a particular namespace:

```
kubectl get pods -n <namespace>
```

- Display the detailed state of all containers within a pod:

```
kubectl describe pod <pod-name> -n <namespace>
```

- Retrieve the logs for a pod in a given namespace:

```
kubectl logs <pod-name> -n <namespace>
```

- Retrieve the logs for a container running in a pod:

```
kubectl logs <pod-name> -c <container-name> -n <namespace>
```

- Get relevant events for a given namespace:

```
kubectl get events -n <namespace>
```

The `kubectl logs <pod-name> -n <namespace>` command works only if one container is running in a given pod. If multiple containers are running in a pod, you run the `kubectl logs <pod-name> -c <container-name> -n <namespace>` command instead.

You can add the `-f` flag to follow the log file. The `--timestamps` flag can be used to retrieve the date and time of the log events. The `-p` (previous) flag can be used to see the logs from a previously running container.



## 8-44 Namespaces Available After NSX Application Platform Deployment

The cert-manager, nsxi-platform, and projectcontour namespaces are automatically created as part of the NSX Application Platform deployment.

```
kadmin@SA-K8s-CTRL-01:~$ kubectl get namespaces
```

NAME	STATUS	AGE
<b>cert-manager</b>	<b>Active</b>	<b>3dlh</b>
default	Active	234d
kube-node-lease	Active	234d
kube-public	Active	234d
kube-system	Active	234d
local-path-storage	Active	123d
metallb-system	Active	234d
<b>nsxi-platform</b>	<b>Active</b>	<b>3dlh</b>
<b>projectcontour</b>	<b>Active</b>	<b>3dlh</b>

# 8-45 Pods Available After NSX Application Platform Deployment

The example shows an extract of the pods created during NSX Application Platform deployment.

```
kadmin@SA-K8s-CTRL-01:~$ kubectl get pods -n nsxi-platform
NAME                                READY   STATUS    RESTARTS   AGE
authserver-cd77bbd4b-47767          1/1     Running   0           3d
cluster-api-745655f4db-lxx42       2/2     Running   4           3d1h
common-agent-59ff698dbd-r6t17      1/1     Running   2           3d1h
common-agent-create-kafka-topic-hlpk9 0/1     Completed 0           3d1h
configure-druid-gqqzr               0/1     Completed 1           3d1h
create-kubeapi-networkpolicy-job-gbn6v 0/1     Completed 0           3d1h
druid-broker-7546b89dc4-vdjm6       1/1     Running   1           3d1h
druid-config-historical-0            1/1     Running   0           3d1h
druid-coordinator-d75498dcd-m7hdw    1/1     Running   1           3d1h
druid-historical-0                   1/1     Running   0           3d1h
druid-middle-manager-0               1/1     Running   0           3d1h
druid-overlord-899c4469c-z447b      1/1     Running   2           3d1h
fluentd-0                            1/1     Running   0           3d1h
kafka-0                              1/1     Running   0           3d
<Cropped output>
```

The example shows an extract of the pods created during NSX Application Platform deployment with an Evaluation form factor in the nsxi-platform namespace. The output is cropped. In a healthy environment, the status of all pods should be either Running or Completed. In a Standard form factor deployment, fewer pods are visible because the analytics and data storage pods are not deployed.

The example shows the following functions of the main pods:

- Druid is a time-series distributed database used to store correlated traffic flows.
- Fluentd provides a unified platform to collect logs from different sources.
- Kafka is a distributed messaging system that receives system configuration data from NSX Manager and traffic flows from the transport nodes.

## 8-46 Lab 14: (Simulation) Deploying NSX Application Platform

Deploy and validate NSX Application Platform:

1. Deploy NSX Application Platform
2. Validate the NSX Application Platform Deployment from the NSX UI
3. Validate the NSX Application Platform Deployment from the Kubernetes Cluster

## 8-47 Review of Learner Objectives

- Describe NSX Application Platform and its use cases
- Deploy NSX Application Platform
- Explain the NSX Application Platform architecture and services

## 8-48 Lesson 3: NSX Malware Prevention

### 8-49 Learner Objectives

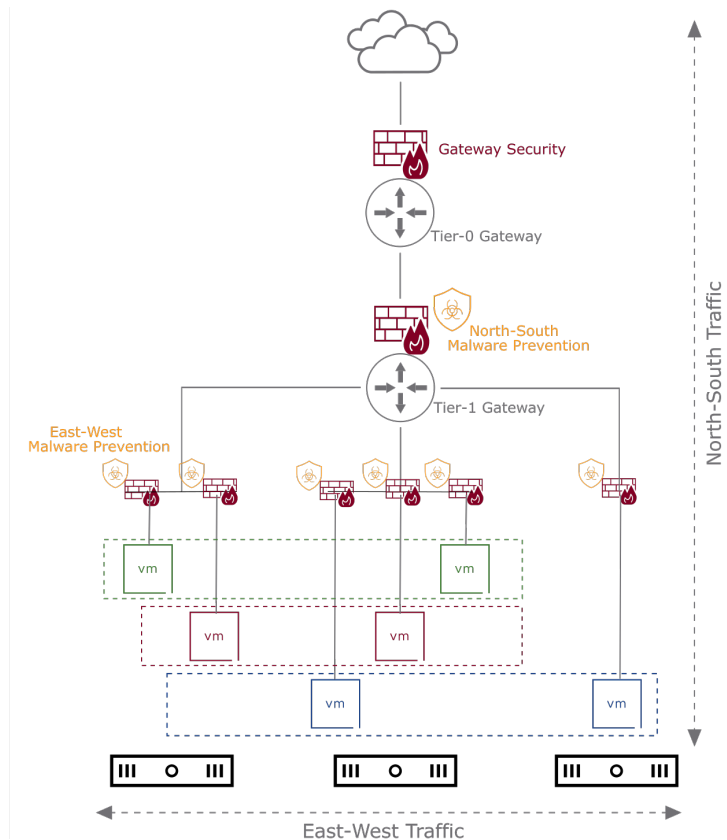
- Identify use cases for malware prevention
- Identify the components in the malware prevention architecture
- Describe the malware prevention packet flows for known and unknown files
- Configure malware prevention and validate the configurations

## 8-50 About Malware Prevention

Malware prevention detects and prevents malicious file transfers by combining signature-based detection of known malware with static and dynamic analyses of malware samples.

NSX Malware Prevention can be configured in the following locations:

- East-west malware prevention detects and prevents malicious files directly on the guest VMs.
- North-south malware prevention detects malicious files on the gateway firewall.



Malware prevention protects your environment against viruses, worms, trojan horses, spyware, and ransomware.

Malware prevention uses the following techniques to detect and prevent malicious file transfers:

- Signature-based detection uses databases of known malware patterns. It scans the file and memory of a system for any data that match the pattern of known malicious software.
- Static file analysis extracts the unique characteristics of a file, such as its structure, and uses machine learning algorithms to classify and identify malware indicators.
- Dynamic file analysis performs memory analysis and observes how the file interacts with the system, identifying indicators of malicious activity.

Static document analysis occurs when a file is examined without executing it, whereas dynamic analysis examines the actions of the file and can occur only when the file is executing. Both static and dynamic analysis are behavior-based malware detection mechanisms.

Malware prevention can be configured in the following locations:

- East-west malware prevention is configured directly on the guest VMs to protect malware from spreading laterally in the data center.
- North-south malware prevention is configured on the edge node to prevent malware from entering the perimeter.

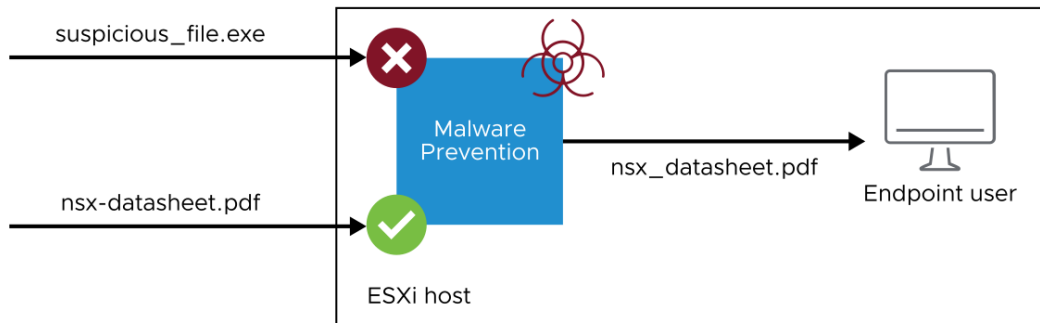
## 8-51 About East-West Malware Prevention

East-west malware prevention detects known malicious files on guest VMs and prevents them from being downloaded.

Guest Introspection agents are installed on the guest VMs and perform the following functions:

- Generate alerts if malicious known file hashes are detected
- Extract unknown files and send for local and cloud-based analysis

Alerts are generated based on the return verdict.



East-west malware prevention protects the data center from the spread of internal malware and from malware that makes it past the network perimeter. To perform these tasks, it monitors files downloaded on the guest VMs for malicious content.

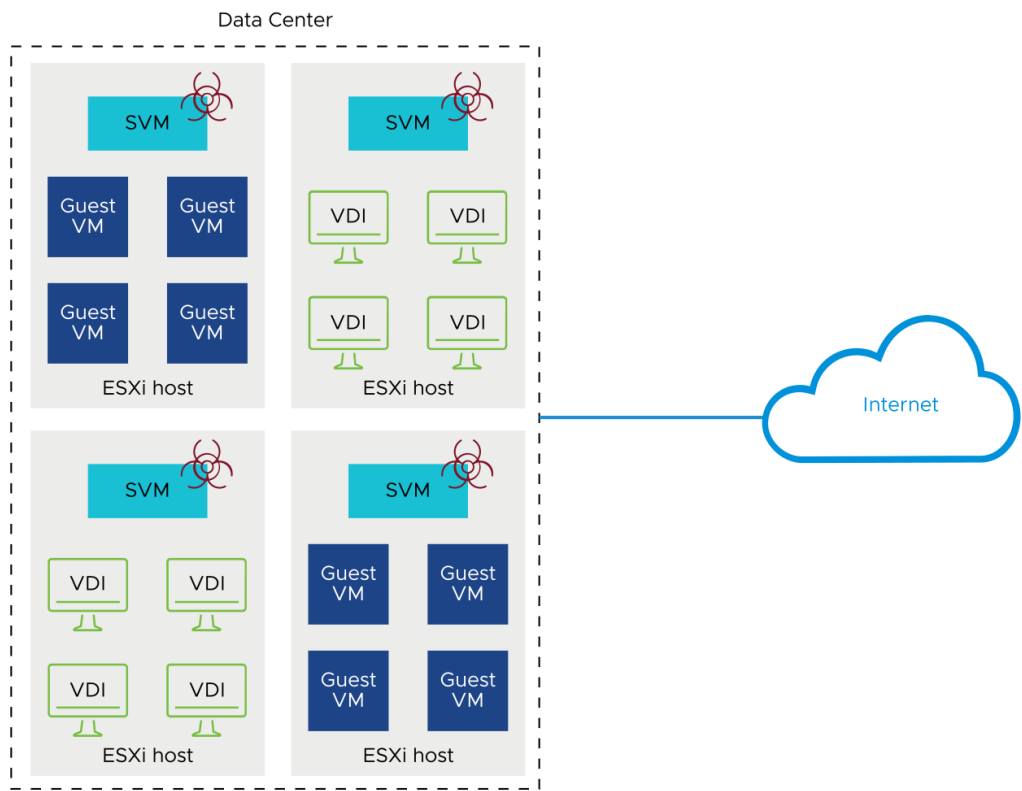
To detect and prevent malware from spreading in the environment, malware prevention combines signature-based detection of known malware with static and dynamic analyses of malware samples.

Local analysis, which is a combination of static analysis and machine learning-based analysis of files, is performed on the ESXi host.

Dynamic analysis is performed in a cloud-based environment and is optional.

# 8-52 Use Cases for East-West Malware Prevention

East-west malware prevention provides malware detection and prevention capabilities for data center and virtual desktop infrastructure (VDI) end users.



East-west malware prevention uses distributed firewall capabilities to protect end users from downloading malicious content.

East-west malware prevention protects guest VMs and virtual desktop infrastructures (VDIs) from lateral malware spreads. Each ESXi host includes a service virtual machine (SVM), which inspects all files that are downloaded at the guest level.



## 8-53 Requirements for East-West Malware Prevention

East-west malware prevention has the following requirements:

- The NSX environment must be configured with a valid license for malware prevention.
- At a minimum, NSX Application Platform must be deployed with the Standard form factor in the environment.
- The thin agent must be installed on every guest VM.
- NSX Manager must have Internet access.

Proxy settings can be configured if necessary.

For more information about the types of valid licenses for malware prevention, see "VMware NSX" at

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf>.

Cloud-based analysis is optional.

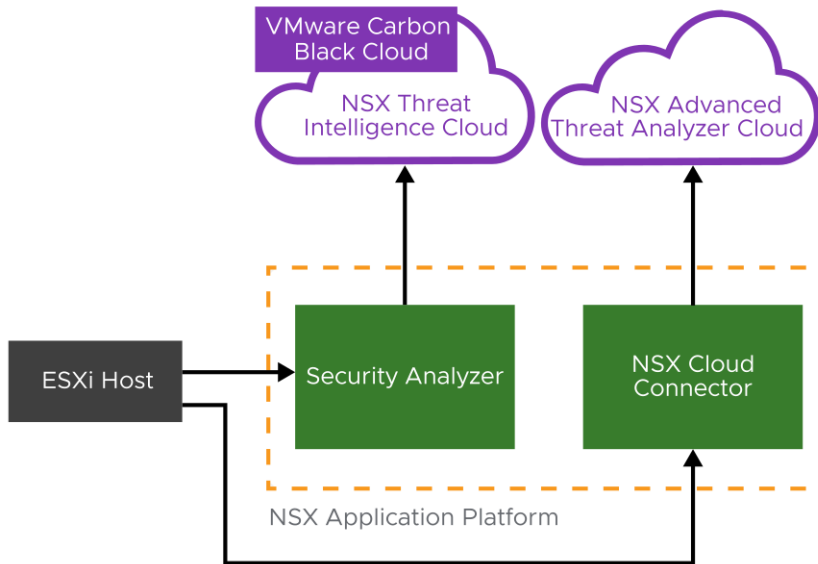
In Windows operating systems, the thin agent is installed as part of VMware Tools.

In Linux operating systems, the thin agent is a separate package that can be downloaded from the VMware web page. For more information about installing the Guest Introspection thin agent on Linux virtual machines, see *NSX Administration Guide* at

<https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-4871C429-CFE6-41C9-86C9-7FCFE9C95EC8.html>.

## 8-54 East-West Malware Prevention Architecture

East-west malware prevention includes ESXi hosts, NSX Application Platform, NSX Threat Intelligence Cloud, and NSX Advanced Threat Analyzer Cloud.



NSX Malware Prevention uses the following clouds:

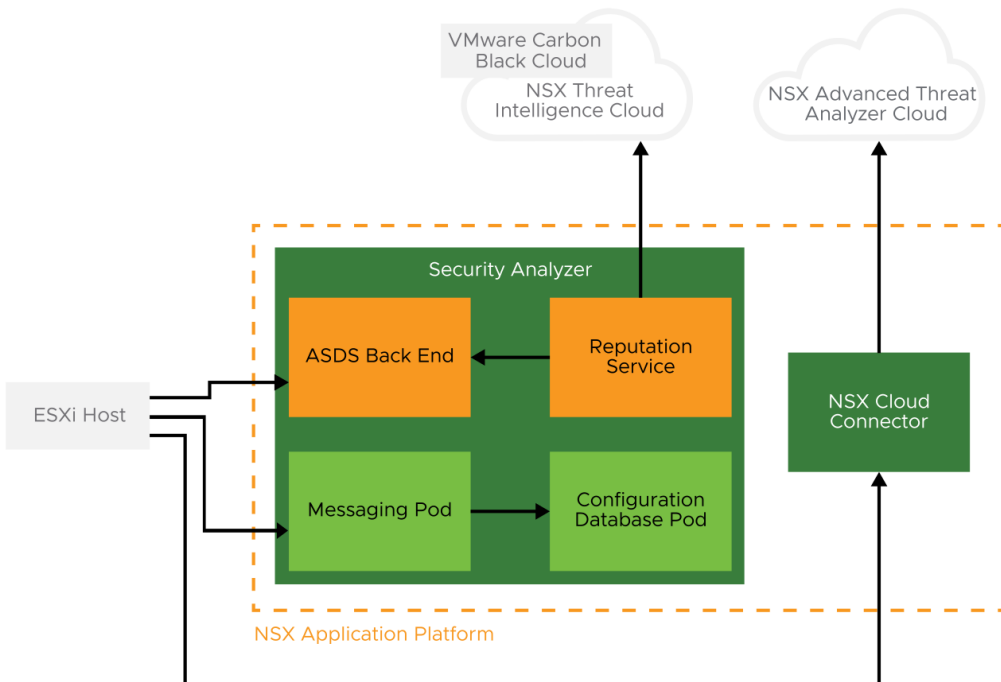
- NSX Threat Intelligence Cloud: Obtains file reputations from VMware Carbon Black Cloud and caches them for use in the NSX environment
- NSX Advanced Threat Analyzer Cloud: Performs machine learning-based detection and dynamic analysis of the files

## 8-55 NSX Application Platform Components

The NSX Malware Prevention feature requires an NSX Application Platform deployment.

In NSX Application Platform, the main components that are deployed for malware prevention are as follows:

- Security Analyzer:
  - Advanced Signature Distribution Service (ASDS) back end
  - Reputation service
  - Messaging pod
  - Configuration database pod
- NSX Cloud Connector



The Standard form factor is enough to use NSX Malware Prevention, but the Advanced form factor is mandatory to install NSX Intelligence.

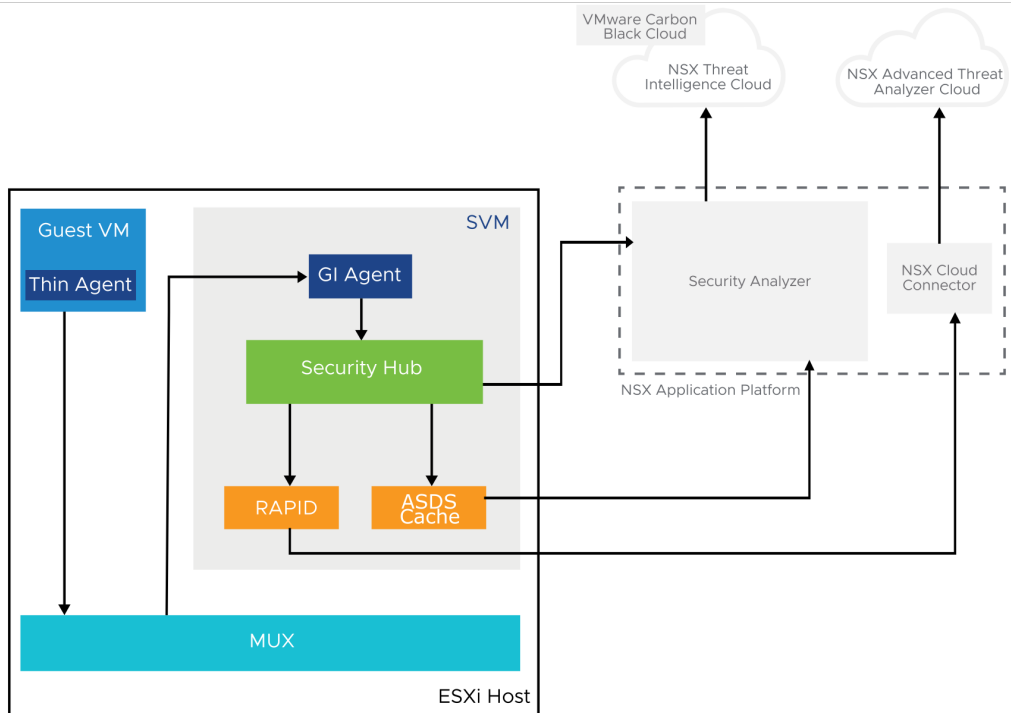
In NSX Application Platform, the main components that are deployed for malware prevention are as follows:

- Security Analyzer collects all information that is received from the messaging pod and fetches reputations and signatures from VMware Carbon Black Cloud through the reputation service. Security Analyzer maintains two databases:
  - The Configuration database pod contains all received file events.
  - The NSX Advanced Signature Distribution Service (ASDS) back end gathers the verdict and reputations for all known files.
- NSX Cloud Connector sends files for dynamic analysis to NSX Advanced Threat Analyzer Cloud. NSX Cloud Connector acts as a gateway between on-premises services and NSX Advanced Threat Analyzer Cloud. Its purpose is to centralize communication and provide an authenticated channel between clients and the cloud.

## 8-56 ESXi Host Components

The main ESXi host components for east-west malware prevention are as follows:

- Guest VM
- Context Multiplexer (MUX)
- Service VM:
  - Guest Introspection agent
  - Security hub
  - Rapid API for Detection (RAPID)
  - ASDS cache



The main ESXi host components for east-west malware prevention are as follows:

- Guest VM: Runs a Network Introspection agent, called the thin agent, which offloads files for scanning to the service virtual machine (SVM)

In Windows operating systems, the thin agent is installed as part of VMware Tools and includes the following components:

- NSX Network Introspection (vnetWFP.sys)
- NSX File Introspection (vsepfilt.sys)
- VMCI (vsock.sys)

Beginning with NSX 4.0.1, east-west malware prevention is also supported for Linux VMs. The Guest Introspection thin agent for Linux is available as part of the operating system specific packages (OSPs). The packages are hosted on the VMware packages portal.

- Context Multiplexer (MUX): Relays messages between the guest VMs and the SVM, maintains the SVM configuration, and processes the east-west malware prevention policies  
The MUX is installed as a VIB during transport node preparation.
- SVM: VM appliance that is deployed on every ESXi host part of a malware prevention-enabled cluster

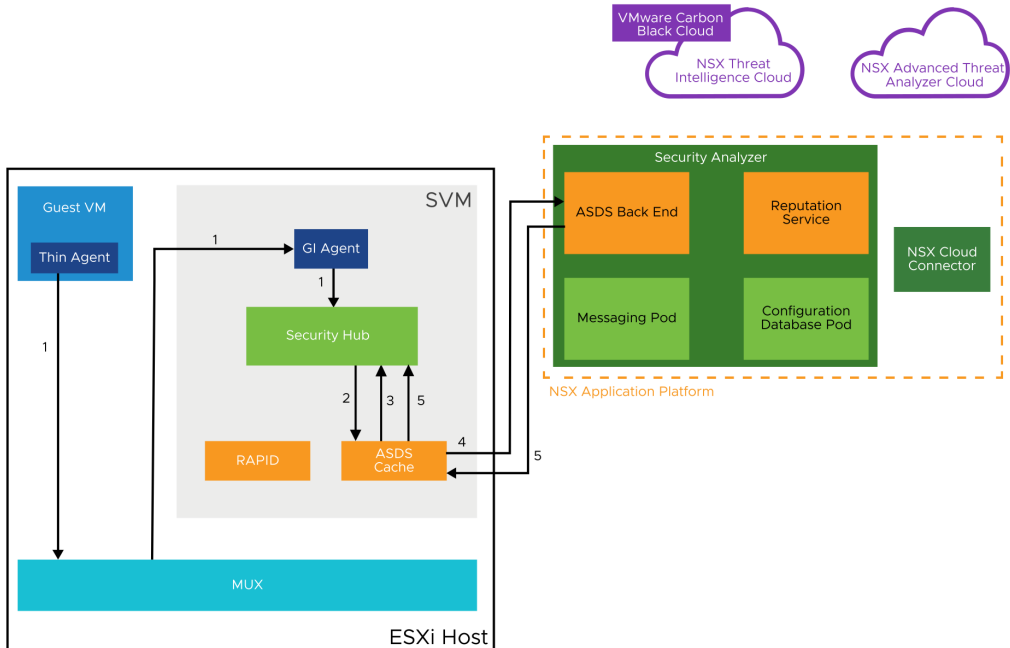
The SVM monitors files that are offloaded from the guest VMs, performs local analysis, and connects to NSX Application Platform for file reputation and cloud-based analysis. The SVM contains the following modules:

- Guest Introspection agent: Relays event and data received from the guest VM to the security hub
- Security hub: Collects file events, obtains verdicts for known files, and sends files for local and cloud-based analysis
- Rapid API for Detection (RAPID): Provides local analysis of the files through a combination of static analysis and machine learning-based analysis
- Advanced Signature Distribution Service (ASDS) cache: Maintains a database of known files verdicts and reputations

The ASDS back end is present in the Security Analyzer and each SVM maintains an ASDS local cache.

## 8-57 East-West Malware Prevention Packet Flow for Known Files

A packet flow occurs when a transfer of a known file is detected on the guest VM.

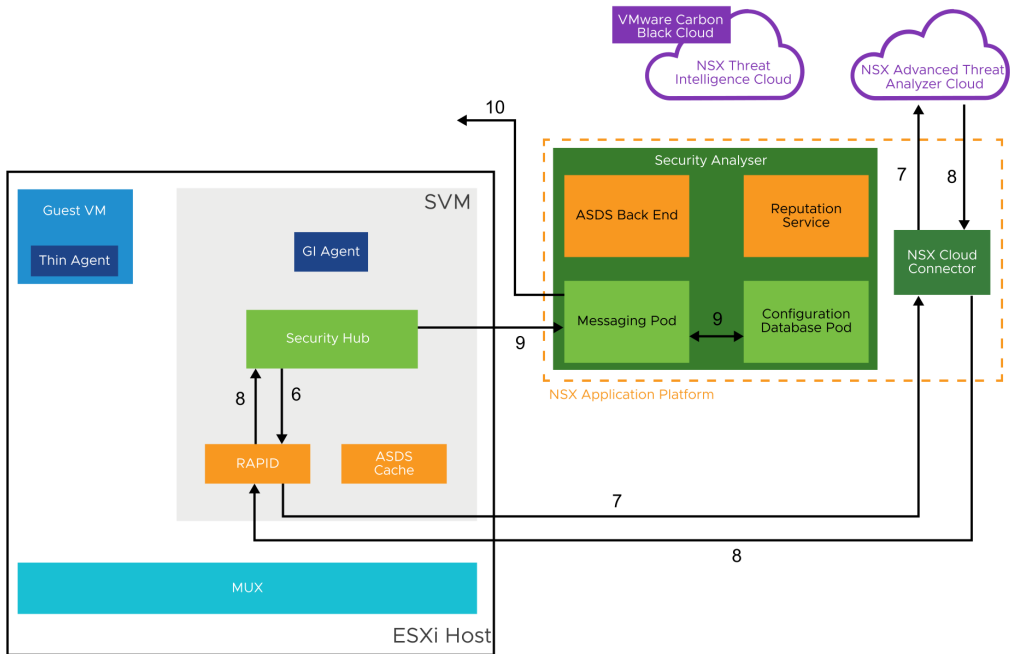


The following packet flow occurs when a file transfer is detected on the guest VM:

1. The thin agent extracts the file, computes the hash, and provides information to the security hub through the MUX and the Guest Introspection agent.
2. The security hub checks whether the file is known in the local ASDS cache by sending the hash.
3. The local cache sends the verdict back.
4. If the file is not in the local cache, ASDS queries the ASDS back end internally for the file reputation.
5. The ASDS back end sends the verdict back to the security hub, and the appropriate action is taken.

## 8-58 East-West Malware Prevention Packet Flow for Unknown Files

If the security hub cannot retrieve the file reputation from the ASDS back end, the file is considered unknown and is sent for local and cloud-based analysis.



If the security hub cannot retrieve the file reputation from the ASDS back end, the file is considered unknown and is sent for local and cloud-based analysis:

6. The security hub sends the file to the RAPID module to perform local analysis.
7. Based on the malware prevention policy and local analysis results, RAPID sends the file to the NSX Advanced Threat Analyzer Cloud for analysis through the NSX Cloud Connector.

This step occurs only if the policy is set up for cloud-based analysis. If cloud-based analysis is not set up, only the local analysis verdict is sent to the security hub.



- NSX Advanced Threat Analyzer Cloud sends the combined verdicts of the local and cloud-based analysis to the security hub, and the appropriate action is taken.

If the verdict of a file is malicious, and if the file's type is portable executable, the security hub sends the file's hash to the reputation service to cross-check its reputation. This step is performed to reduce false positives. The file reputation service queries VMware Carbon Black Cloud to retrieve the file reputation.

- The security hub collects verdicts and statistics and sends an event to the security analyzer.
- The security analyzer reports the verdict and statistics to NSX Manager.

The security analyzer polls the security hub for the local and cloud-based analysis verdicts and updates the ASDS back end accordingly. This data is used for future downloads of the same file.

## 8-59 Activating Malware Prevention on NSX Application Platform

To enable NSX Malware Prevention in the NSX UI, you select **System > Configuration > NSX Application Platform** and click the NSX Malware Prevention tile.


The screenshot displays the NSX Application Platform configuration page. The left sidebar contains navigation options: System Overview, Configuration (Quick Start, Appliances, NSX Application Platform, Fabric, Service Deployments, Identity Firewall AD), Lifecycle Management (Backup & Restore, Upgrade, Migrate), and Settings (General Settings, User Management, Licenses, Certificates, Support Bundle). The main content area shows system metrics for two hosts, a list of features to be activated, and three tiles for NSX Intelligence, NSX Network Detection and Response, and NSX Malware Prevention. The NSX Malware Prevention tile is highlighted with a green box and a callout.

Click NSX Malware Prevention to activate this feature on the NSX Application Platform.

# 8-60 Setting the Cloud Region


You select the cloud region, run prechecks, and then click **ACTIVATE**.

The NSX Malware Prevention installation deploys both NSX Cloud Connector and the components required for malware prevention.

 NSX Malware Prevention


NSX Malware Prevention uses VMware NSX Advanced Threat Prevention cloud services to fetch periodic detection updates and upload data for deeper analysis.

Select Cloud Region ⓘ



☒

United States 1



☐

European Union 1

NOTE: The same Cloud Region selection is used in both the Malware Protection and the Network Detection and Response features.

Additional Features (Any one)

NSX Intelligence

NSX Network Detection and Response

Suspicious Network Activity

IDS/IPS

It is mandatory to run the prechecks to ensure all prerequisites are met.

RUN PRECHECKS

Name	Description	Status
NSX Advanced Threat Analyzer Cloud Eligibility	Validate license is eligible for cloud integration	Not Started
NSX Advanced Threat Analyzer Cloud Reachability	Validate selected cloud region can be reached and meets user selection criteria	Not Started

CANCEL

ACTIVATE

You specify the NSX Advanced Threat Analyzer Cloud instance that you want your environment to connect to.

The FQDN for the United States cloud is nsx.west.us.lastline.com, and the FQDN for the European cloud is nsx.nl.emea.lastline.com. NSX Malware Prevention uses HTTPS port 443 to access NSX Advanced Threat Analyzer Cloud.

450

Technet24

Before proceeding with the installation of NSX Malware Prevention, the installation wizard verifies that the license is valid and that NSX Advanced Threat Analyzer Cloud is accessible.

NSX Cloud Connector is a shared component between NSX Network Detection and Response and NSX Malware Prevention. The NSX Cloud Connector deployment is skipped if NSX Network Detection and Response is already configured in the environment.

In environments in which both these features are installed, changing the cloud region requires reinstalling both NSX Network Detection and Response and NSX Malware Prevention. Modifying the cloud region after the installation is not supported.

## 8-61 Validating the Malware Prevention Installation

You can validate the successful installation of NSX Malware Prevention from the NSX UI.

**NSX MALWARE PREVENTION**

Status: ● UP

Region: United States 1

Feature Version: 4.0.1.0.0.20606727

GO TO NSX MALWARE PREVENTION

ACTIONS ▾

# 8-62 Service Registration

Before you can use malware prevention on the transport nodes, you must register the malware prevention service and deploy SVMs on each host.

You register the malware prevention service with NSX Manager with the following API call:

POST `https://sa-nsxmgr-01.vclass.local/napp/api/v1/malware-prevention/svm-spec`

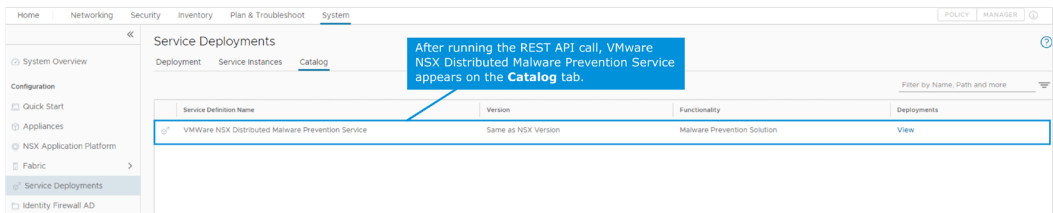
Body:

```
{
  "ovf_url": "<OVF_PATH>",
  "deployment_spec_name": "MPS-SVM"
}
```

You must use a REST API call to register malware prevention.

# 8-63 Service Registration Validation from the NSX UI

You validate the malware prevention service registration in the NSX UI by selecting **System > Configuration > Service Deployments > Catalog**.



## 8-64 Service Deployments

To deploy the SVMs on each host, you select **System > Configuration > Service Deployments > Deployment**.

Service Deployments

Deployment Service Instances Catalog

Partner Service \* VMware NSX Distributed Malware Prevention Service VIEW SERVICE DETAILS

DEPLOY SERVICE

COLLAPSE ALL Search

Service Deployment Name	Compute Manager	Cluster	Data Store	Networks	Status	Alarms
E-W MPS *	sa-vcasa-01vclass local	Compute-Cluster	SA-Shared-01-NSX	SA		

Deployment Specification: MPS-SVM - Medium Deployment Template: MPS\_Attributes\_For\_OVF\_1

NOTE - Fetching Datastore and

SAVE CANCEL

Configure Attributes \*

Add the RSA public key of the SVM.

Networks

Please select all nics to be used for deployment

Nic Information	Network	Network Type	IP Pool
eth0 - Control Nic	System Configured	System Configured	System Configured
<input checked="" type="checkbox"/> eth0 - Management Nic	Remote_Network	Static IP Pool	SVM IP Pool

MANAGE IP POOLS

CANCEL SAVE

You can configure the SVM management network with Static IP Pool or DHCP.

The deployment of the SVMs is cluster-based:

- All hosts inside the cluster are deployed with an instance of the service.
- If a new host is added to the cluster, it is automatically deployed with a service instance.

After clicking **SAVE**, the deployment of the SVMs on each ESXi host starts. You can monitor the deployment by looking at the tasks in vCenter Server.

# 8-65 Service Deployment Validation from the NSX UI

You can validate the service instance deployment from the NSX UI by selecting **System > Configuration > Service Deployments > Service Instances**.

Service Deployments ?

Deployment Service Instances Catalog

Partner Service VMware NSX Distributed M VIEW SERVICE DETAILS

One SVM instance is deployed on each ESXi host in the cluster.

EXPAND ALL Search

	Service Instances Name	Service Deployment Name	Deployed To	Deployment Mode	Deployment Status	Health Status	Alarms
>	@ <sup>1</sup> ServiceInstance_EW_ServiceDeployment /96ad1be-4277-4ed3-804c-e70dd3f26c14_1	E-W MPS	Host : sa-esxi-01.vclass.local	Standalone	● Up ⓘ	● Up ⓘ	0
>	@ <sup>1</sup> ServiceInstance_EW_ServiceDeployment /96ad1be-4277-4ed3-804c-e70dd3f26c14_2	E-W MPS	Host : sa-esxi-02.vclass.local	Standalone	● Up ⓘ	● Up ⓘ	0

In a healthy environment, both the Deployment Status and the Health Status appear as Up.

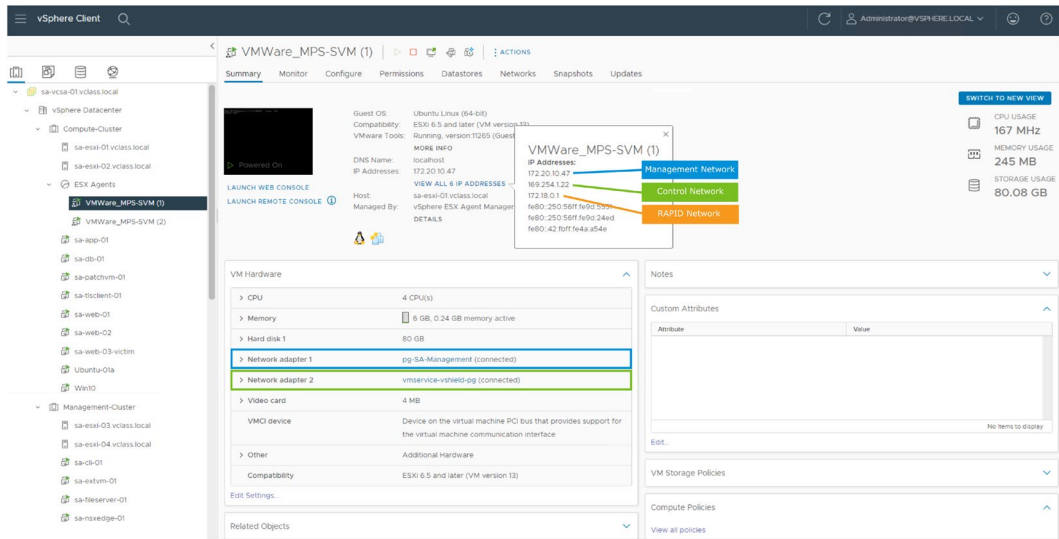
You can check alarms for the NSX Malware Prevention feature by selecting **Home > Alarms > Alarms**.

The following alarms are available for NSX Malware Prevention:

- Analyst API Services Unreachable
- Database Unreachable
- File Extraction Service Unreachable
- NTICS Reputation Service Unreachable
- Service Status Down

## 8-66 Service Deployment Validation from vCenter Server

You can validate the service instance deployment from vCenter Server.



The SVM is deployed in vCenter Server and runs with the following IP addresses:

- The Management network is defined by the administrator during the configuration.
- The Control network is defined by the system and gets the IP 169.254.1.22.
- 172.18.0.1 is an internal IP address used to connect the RAPID container. Therefore, it is not connected to an external network like the other two IP addresses.

## 8-67 Creating East-West Malware Prevention Profiles

The NSX Malware Prevention profile defines the types of files to be analyzed.

The screenshot shows the NSX Manager interface for creating a Malware Prevention profile. The left sidebar shows the navigation menu with 'Security > Policy Management > IDS/IPS & Malware Prevention > Profiles > Malware Prevention' selected. The main panel shows the 'ADD PROFILE' form for a new profile named 'EW MP Profile'. The 'Submission Criteria' section is expanded, showing a grid of file categories with checkboxes. A green box highlights the 'File Category' section with the text 'Select the type of files to be analyzed.' An orange box highlights the 'Cloud File Analysis' section with the text 'If you select this check box, unknown files are sent for dynamic analysis to the NSX Advanced Threat Analyzer Cloud.' The 'Cloud File Analysis' checkbox is checked. The 'SAVE' button is visible at the bottom left of the form.

Name	Description	Tags	Status
EW MP Profile			

Submission Criteria

File Category

- ☒ Document
- ☒ Executable
- ☒ Media
- ☒ Archive
- ☒ Data
- ☒ Script
- ☒ Other File Type

Cloud File Analysis

- ☒ Send the files to VMware NSX Advanced Threat Prevention cloud service

SAVE CANCEL

You create a profile for malware prevention by selecting **Security > Policy Management > IDS/IPS & Malware Prevention > Profiles > Malware Prevention**.

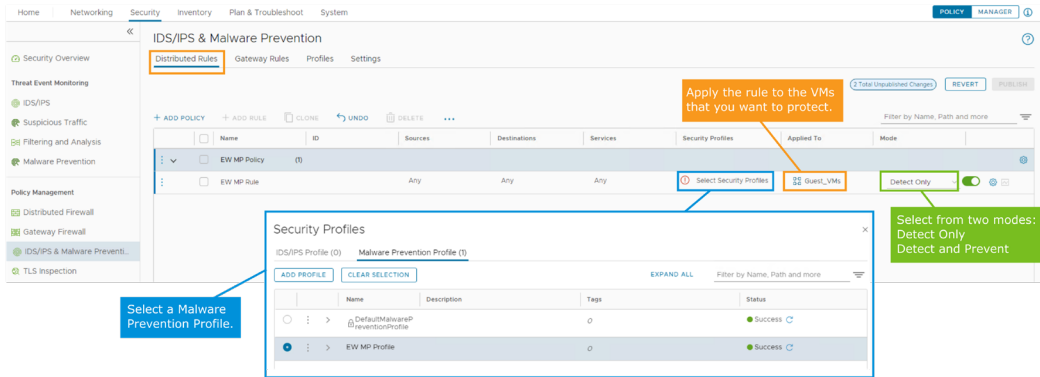
In earlier versions of NSX-T Data Center, only executable files were supported for east-west malware prevention.

Since NSX 4.0.1, all file types are available when configuring east-west malware prevention. The file types are specified in the Malware Prevention Profile.



## 8-68 Creating Rules for East-West Malware Prevention

To create a rule, you select **Security > Policy Management > IDS/IPS & Malware Prevention > Distributed FW Rules**.



A malware prevention policy is a collection of malware prevention rules.

A malware prevention rule contains a set of instructions that determine which file is analyzed, including the source and destination, the services, the malware prevention profile, where to apply the rule, and the detection mode.

Malware prevention rules must be applied to the group of VMs that you want to protect. The rules do not work if they are applied to the distributed firewall.

NSX 4.0.1 includes the following modes for a malware prevention rule:

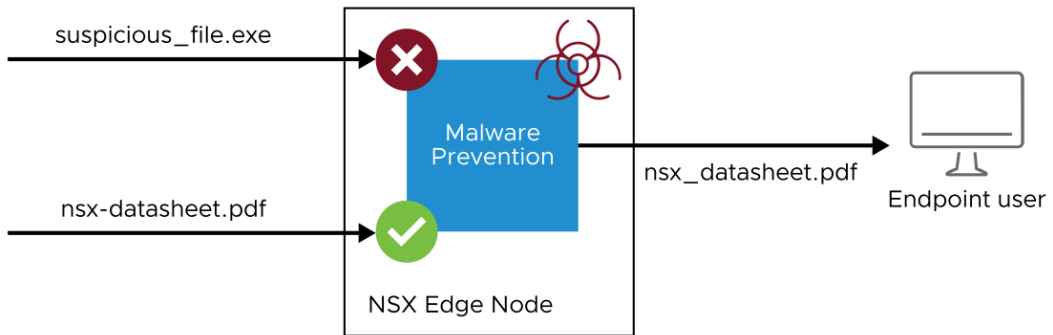
- Detect Only: Detects malware and does not act
- Detect and Prevent: Detects and blocks malware

Only one malware prevention profile can be attached to a rule. However, a rule can have both a malware prevention profile and an IDS/IPS profile.

## 8-69 About North-South Malware Prevention

North-south malware prevention detects known malicious files when they enter the perimeter on the NSX gateway firewall.

If the file is unknown, NSX Edge extracts the file and sends it for local and cloud-based analysis. The verdict is computed, and alerts are generated.



In NSX 4.0.1, only north-south malware detection of the malicious files is supported.

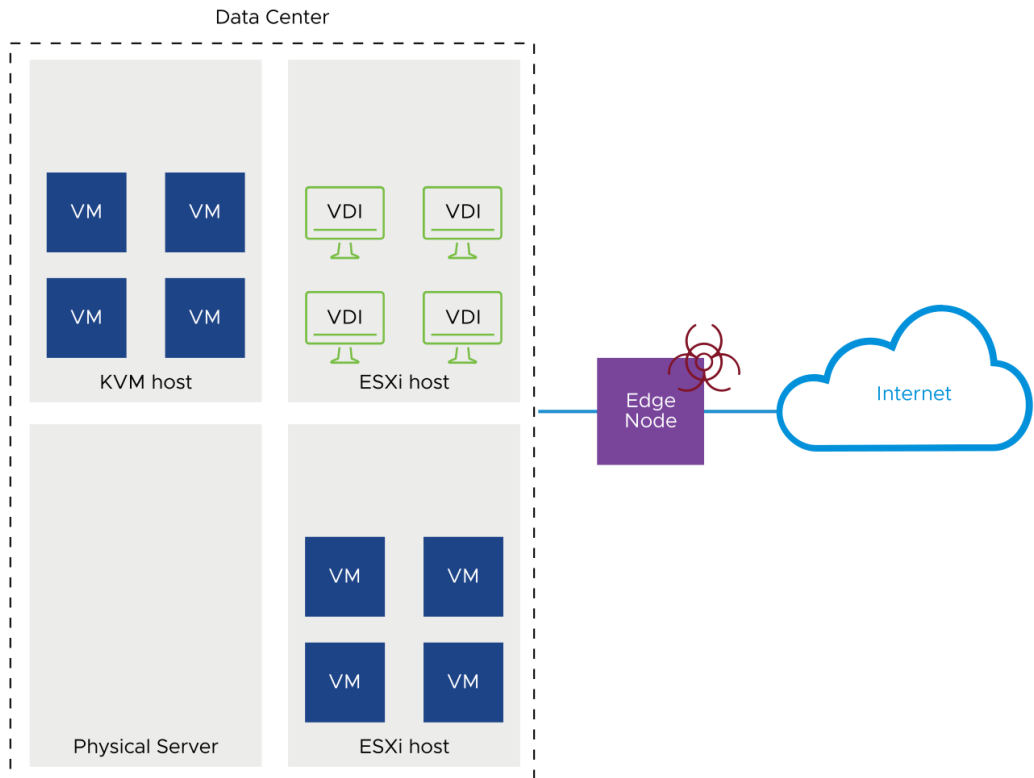
The detection system compares the file hashes (SHA1/MD5/SHA256) to file hashes of known malware.

Local analysis, which is a combination of static analysis and machine learning-based analysis of the files, is performed in the NSX Edge node.

Dynamic analysis is performed in a cloud-based environment and is optional.

## 8-70 Use Cases for North-South Malware Prevention

North-south malware prevention provides malware detection capabilities at the perimeter of the data center.



North-south malware prevention monitors and generates alerts when users want to download malicious files from an external network or from public clouds.

## 8-71 Requirements for North-South Malware Prevention

North-south malware prevention has the following requirements:

- The NSX environment must be configured with a valid license for malware prevention.
- At a minimum, NSX Application Platform with the Standard form factor must be deployed in the environment.
- North-South malware prevention is only supported on Tier-1 gateways.
- The form factor of the NSX Edge nodes must be extra large.
- NSX Manager must have Internet access.

Proxy settings can be configured if necessary.

For more information about the types of valid licenses for malware prevention, see "VMware NSX" at

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf>.

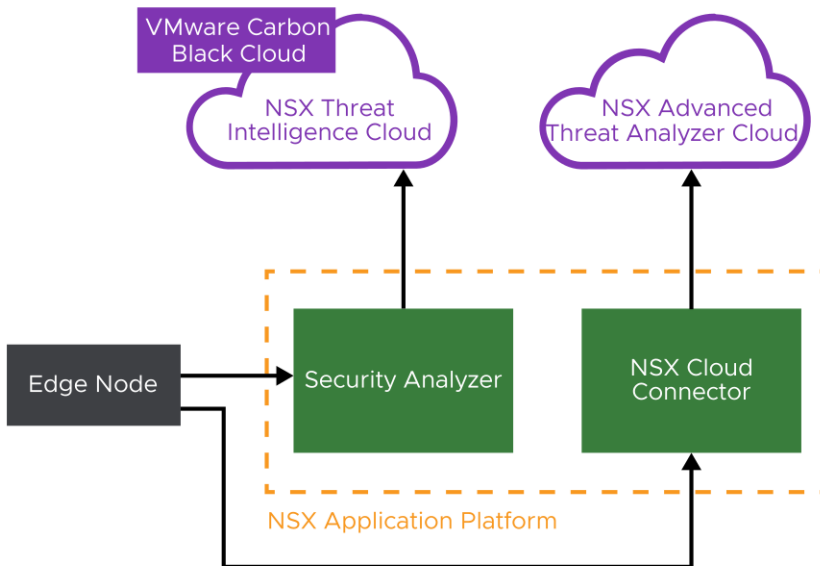
The sizing requirement for extra large NSX Edge nodes are 16 vCPUs, 64 GB of RAM, and 200 GB of storage.

Beginning with NSX 4.0.1, NSX Malware Prevention can be also configured on a bare-metal edge node.

Cloud-based analysis is optional.

## 8-72 North-South Malware Prevention Architecture

North-south malware prevention architecture includes the NSX Edge node, NSX Application Platform, NSX Threat Intelligence Cloud, and NSX Advanced Threat Analyzer Cloud.

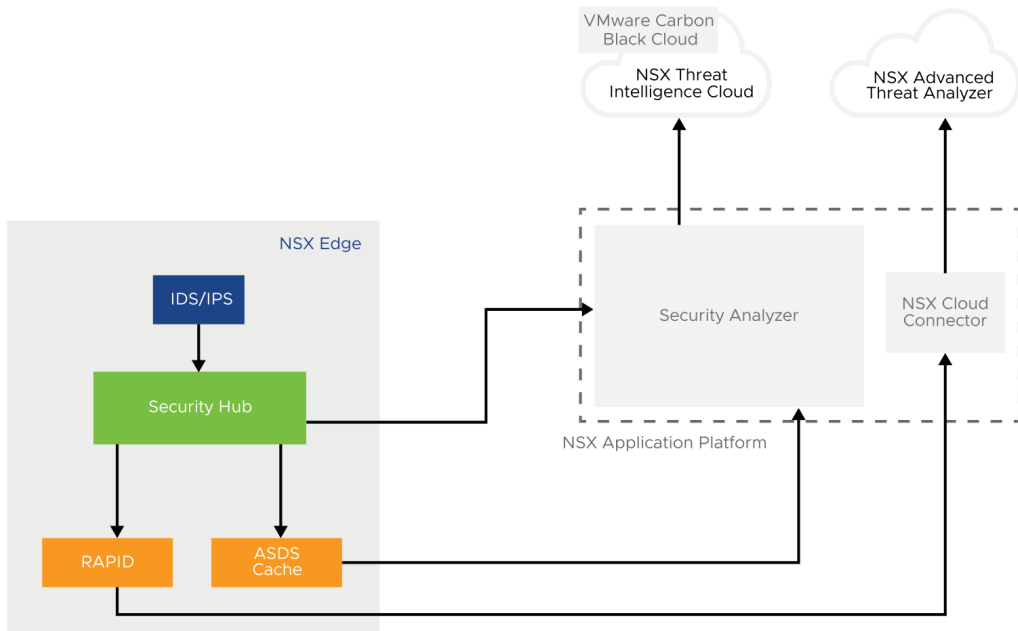


The north-south malware prevention architecture shares the same components as east-west malware prevention, with the difference that the NSX Edge node is used in place of the ESXi hosts.

## 8-73 NSX Edge Components

The main components on the edge node for north-south malware prevention are as follows:

- IDS/IPS engine
- Security hub
- RAPID
- ASDS Cache

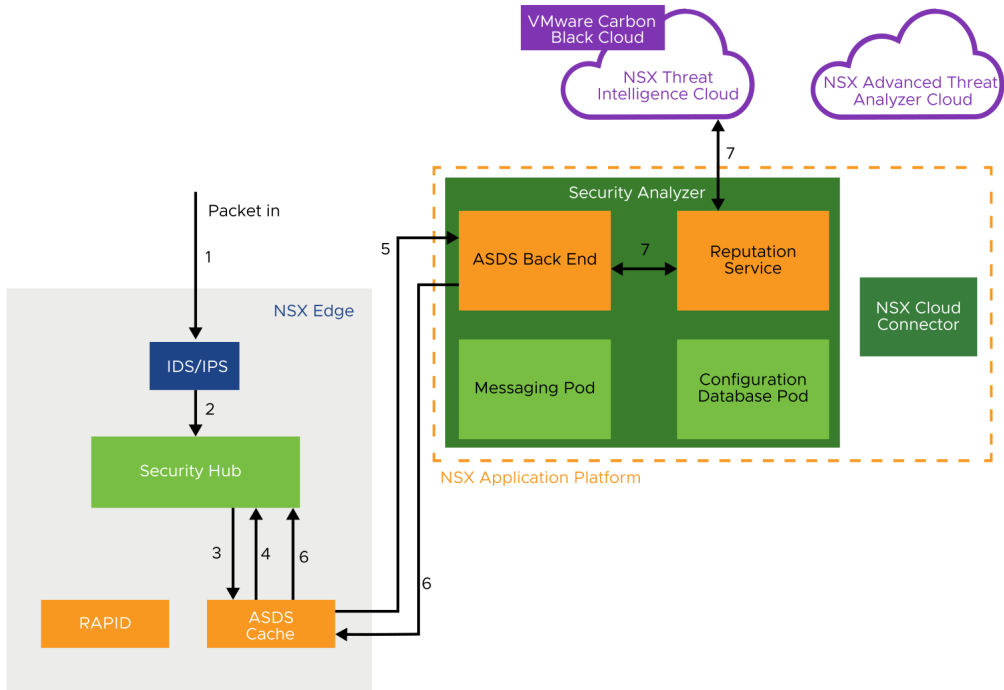


The main components on the edge node for north-south malware prevention perform the following functions:

- IDS/IPS engine: Extracts files and relays events and data to the security hub  
North-south malware prevention uses the file extraction features of the IDS/IPS engine that runs on NSX Edge for north-south traffic.
- Security hub: Collects file events, obtains verdicts for known files, sends files for local and cloud-based analysis, and sends information to the security analyzer
- RAPID: Provides local analysis of the file
- ASDS Cache: Caches reputation and verdicts of known files

## 8-74 North-South Malware Prevention Packet Flow for Known Files

The packet flow for north-south malware prevention is similar to east-west malware prevention.

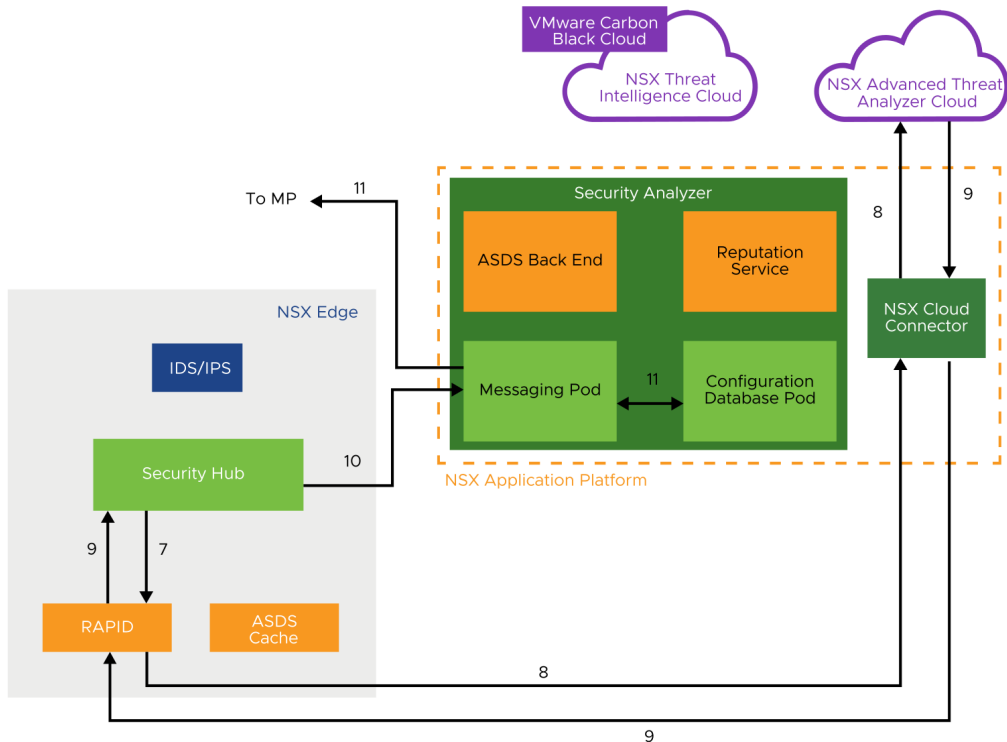


The packet flow process includes the following steps:

1. A file transfer of a known file is detected on the NSX Edge node.
2. The IDS/IPS engine running on the NSX Edge node extracts the file, computes the hash, and provides information to the security hub.
3. The security hub uses the hash to verify whether the file is known to the local ASDS cache.
4. The local ASDS cache sends the verdict back.
5. If the file is not in the local cache, ASDS queries the ASDS back end internally for the file reputation.
6. The ASDS back end sends the verdict back to the security hub, and appropriate action is taken.

## 8-75 North-South Malware Prevention Packet Flow for Unknown Files

If the security hub cannot retrieve the file reputation from the ASDS back end, the file is sent for local and cloud-based analysis.



If the security hub cannot retrieve the file reputation from the ASDS back end, the file is sent for local and cloud-based analysis:

7. The security hub sends the file to the RAPID module to perform local analysis.
8. Based on the NSX Policy and local analysis results, RAPID sends the file to NSX Advanced Threat Analyzer Cloud for analysis through NSX Cloud Connector.

This step takes place only if the policy is set up for cloud-based analysis. If cloud-based analysis is not set up, only the local analysis verdict is used and sent back to the security hub.



9. NSX Advanced Threat Analyzer Cloud sends the combined verdicts of the local and cloud-based analysis to the security hub, and the appropriate action is taken.

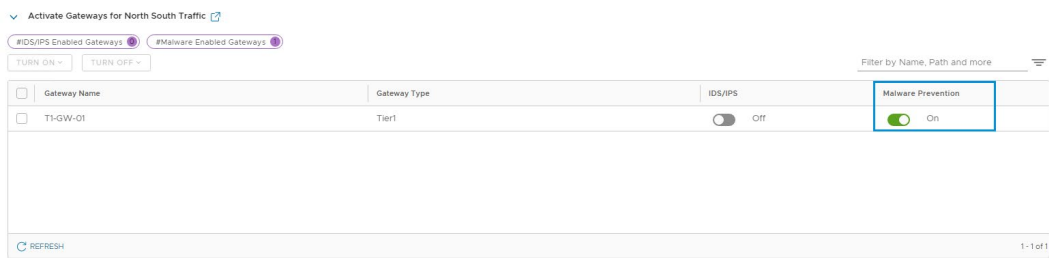
If the verdict of a file is malicious and the file's type is Portable Executable, the security hub sends the file's hash to the reputation service to cross-check its reputation. This step is performed to reduce the number of false positives. The file reputation service queries VMware Carbon Black Cloud to retrieve the file reputation.

10. The security hub collects verdict information and statistics and sends an event to the security analyzer.
11. The security analyzer reports the verdict and statistics to NSX Manager.

The security analyzer polls the security hub for the local and cloud-based analysis verdicts and updates the ASDS back end accordingly. These data are used for future download of the same file.

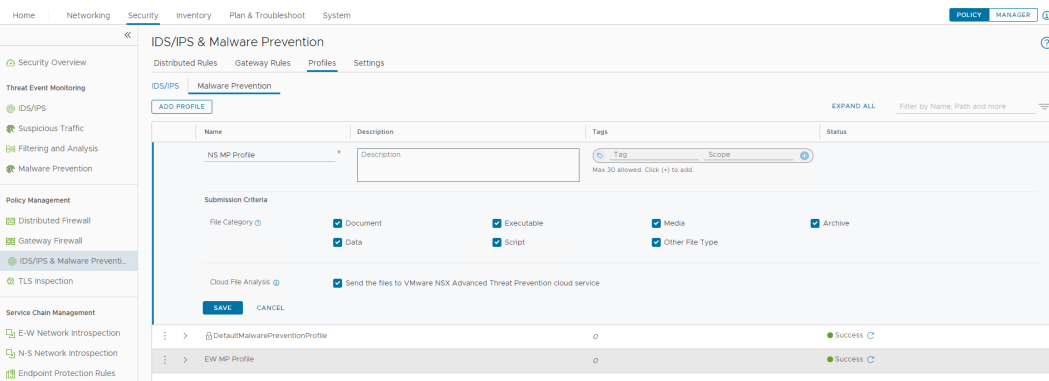
# 8-76 Enabling Malware Prevention on Tier-1 Gateways

To enable malware prevention on the selected Tier-1 gateways, you select **Security > Policy Management > IDS/IPS & Malware Prevention > Settings > Shared** and turn on the **Malware Prevention** toggle.



# 8-77 Creating North-South Malware Prevention Profiles

You create a malware prevention profile by selecting **Security > Policy Management > IDS/IPS & Malware Prevention > Profiles > Malware Prevention**.



## 8-78 Creating Rules for North-South Malware Prevention

Gateway firewall rules specify the parameters on which north-south malware prevention is applied. The rules are enforced on the selected Tier-1 gateway.

The screenshot displays the Palo Alto Networks configuration interface for 'IDS/IPS & Malware Prevention'. The left sidebar shows the navigation menu with 'Policy Management' expanded. The main area shows the 'Gateway Rules' tab under 'Distributed Rules'. A rule named 'NS MP Policy' is selected, and the 'Security Profiles' dialog is open. The dialog shows a list of profiles, including 'DefaultMalwareP', 'EW MP Profile', and 'NS MP Profile'. A callout box points to the 'NS MP Profile' with the text 'Select a Malware Prevention Profile.' Another callout box points to the 'Detect Only' toggle, which is turned on, with the text 'North-south malware prevention only supports malware detection.'

Home Networking Security Inventory Plan & Troubleshoot System POLICY MANAGER

IDS/IPS & Malware Prevention

Distributed Rules Gateway Rules Profiles Settings

All Shared Rules Gateway Specific Rules

Gateway T1-GW-01

1 Total Unpublished Changes REVERT PUBLISH

+ ADD POLICY + ADD RULE CLONE UNDO DELETE ... Unpublished Changes

Filter by Name, Path and more

Name	ID	Sources	Destinations	Services	Security Profiles	Applied To	Mode
NS MP Policy (1)		Any	Any	Any	Select Security Profiles	T1-GW-01	Detect Only

Security Profiles

IDS/IPS Profile (0) Malware Prevention Profile (1)

ADD PROFILE CLEAR SELECTION EXPAND ALL Filter by Name, Path and more

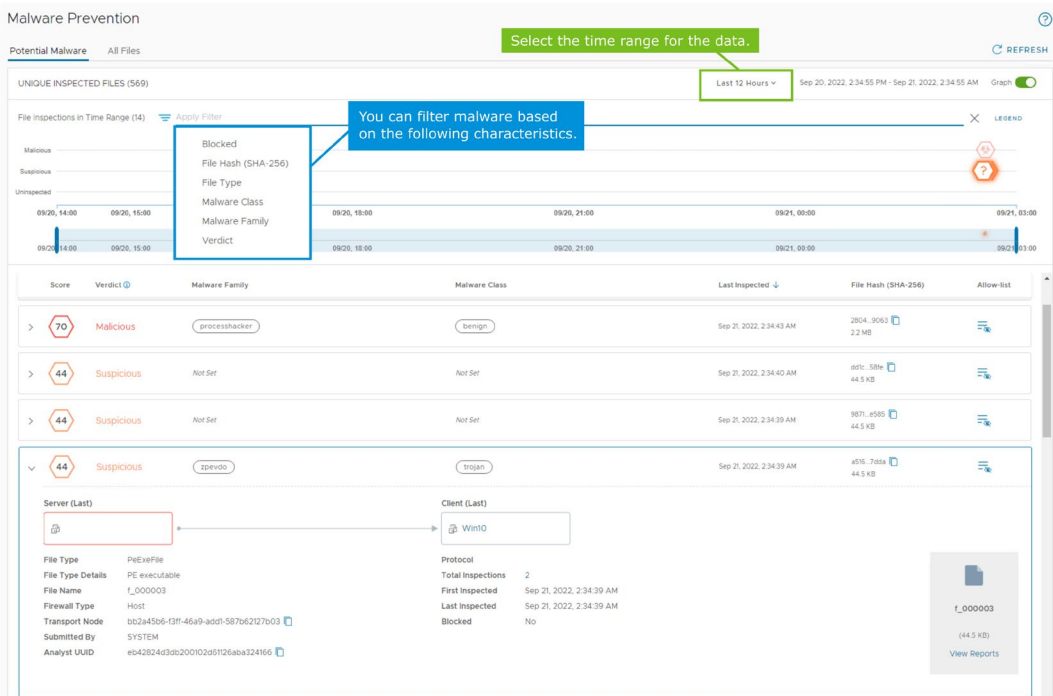
Name	Description	Tags	Status
DefaultMalwareP	Default Malware Prevention Profile	0	Success
EW MP Profile	Endpoint Protection Malware Prevention Profile	0	Success
NS MP Profile	North-South Malware Prevention Profile	0	Success

Only one malware prevention profile can be attached to a rule. But a rule can have both a malware prevention profile and an IDS/IPS profile.

You create a rule by selecting **Security > Policy Management > IDS/IPS & Malware Prevention > Gateway FW Rules**.

# 8-79 Malware Prevention Dashboard (1)

On the **Potential Malware** tab, you can find the list of all detected files that are potentially harmful to the system for both east-west and north-south traffic.



You can access the UI dashboard by selecting **Security > Threat Event Monitoring > Malware Prevention**.

On the **Potential Malware** tab, only files with a potentially harmful verdict appear. Files with a benign verdict are not shown on this tab.

The NSX UI shows the number of files detected, the time of the detection, the verdict (malicious, suspicious, or uninspected), and the malware family and class.

Files are categorized based on their score range:

- 70 through 100 (red): Malicious
- 30 through 69 (orange): Suspicious
- 1 through 30 (green): Benign

Benign files appear on the **All Files** tab, not the **Potential Malware Files** tab.

- -1 (gray): Uninspected

Uninspected files are not analyzed because they appear in the allow list. Files in the allow list are not blocked even if they are classified as suspicious or malicious.

The following filters can be used to search through the inspected files:

- Blocked: Specifies whether the file has been blocked or not by a malware prevention rule
- File Hash: Searches using the hash value, which is a unique value corresponding to the content of the file.
- File Type: Filters based on the type of the file, for example, .doc, .pdf, .exe, and so on
- Malware Class: Defines the type of threat, for example, virus, trojan horse, worm, adware, ransomware, spyware, and so on
- Malware Family: Identifies a specific group of malware files that typically originate from the same source code or are developed by the same authors, for example, valyria, darkside, and so on
- Verdict: Filters based on the decision taken about the files

## 8-80 Malware Prevention Dashboard (2)

On the **All Files** tab, you can find the list of all inspected files.

**Malware Prevention**

Potential Malware **All Files**

UNIQUE INSPECTED FILES (137)

File Type: PdfDocFile

Score	Verdict	Malware Family	Malware Class	Last Inspected	File Hash (SHA-256)	Allow-list
0	Benign	Not Set	Not Set	Aug 19, 2022, 2:50:59 AM	6395...n5f9 212 MB	

Server (Last) → Client (Last)

File Type: PdfDocFile

File Type Details: PDF document

File Name: vmware-rsx-network-virtualization-design-guide.pdf

File Hash: f3cf203-a7c1-4931-b889-2a5804e0f1ba

Firewall Type: Host

Transport Node: SYSTEM

Submitted By: Analyst UMD

Protocol: Total Inspections: 2

First Inspected: Aug 19, 2022, 2:50:57 AM

Last Inspected: Aug 19, 2022, 2:50:59 AM

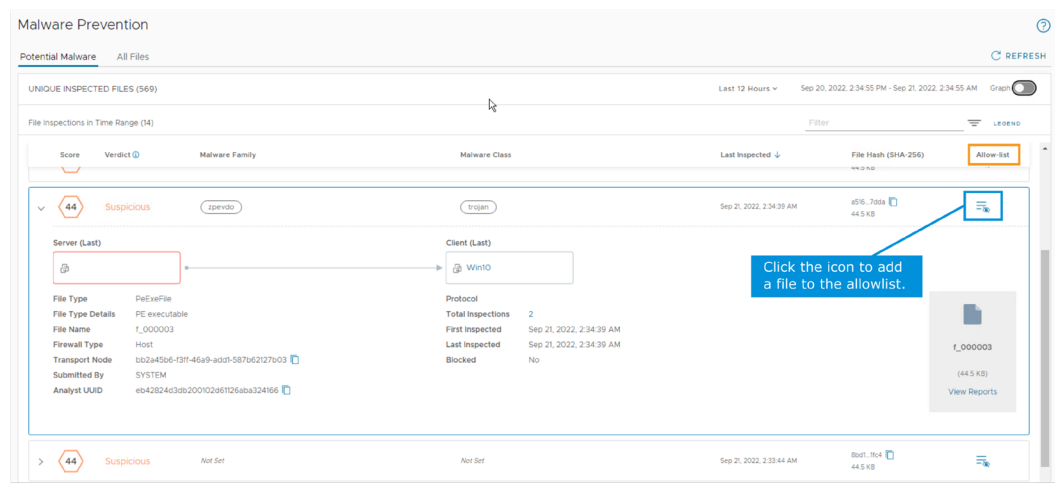
Blocked: No

If you expand the arrow, you get information such as:

- The file type
- The type of firewall
- On which transport node the file has been detected
- The number of inspections
- If the file has been blocked or not

# 8-81 About the Allowlist

Files in the allowlist are not blocked even if they are classified as suspicious or malicious.



You can add files to the allowlist after they are detected by the system. You select **Security > Threat Event Monitoring > Malware Prevention**.

You can list all files that are present in the allowlist by selecting **Security > Policy Management > IDS/IPS & Malware Prevention > Settings > Malware Prevention**.

Files in the allow list appear as uninspected files (grey color) in the Malware Prevention dashboard.

## 8-82 Lab 15: (Simulation) Configuring Malware Prevention for East-West Traffic

Configure malware prevention for east-west traffic:

1. Install Malware Prevention
2. Validate the Malware Prevention Deployment from the CLI
3. Register the Malware Prevention Service
4. Deploy the Service Instances
5. Validate the Service Instances Deployments
6. Create a Malware Prevention Profile
7. Configure the East-West Malware Prevention Rules
8. Download Files from the Guest VM
9. Review the Malware Prevention Dashboard

## 8-83 Review of Learner Objectives

- Identify use cases for malware prevention
- Identify the components in the malware prevention architecture
- Describe the malware prevention packet flows for known and unknown files
- Configure malware prevention and validate the configurations

## 8-84 Lesson 4: NSX Intelligence

### 8-85 Learner Objectives

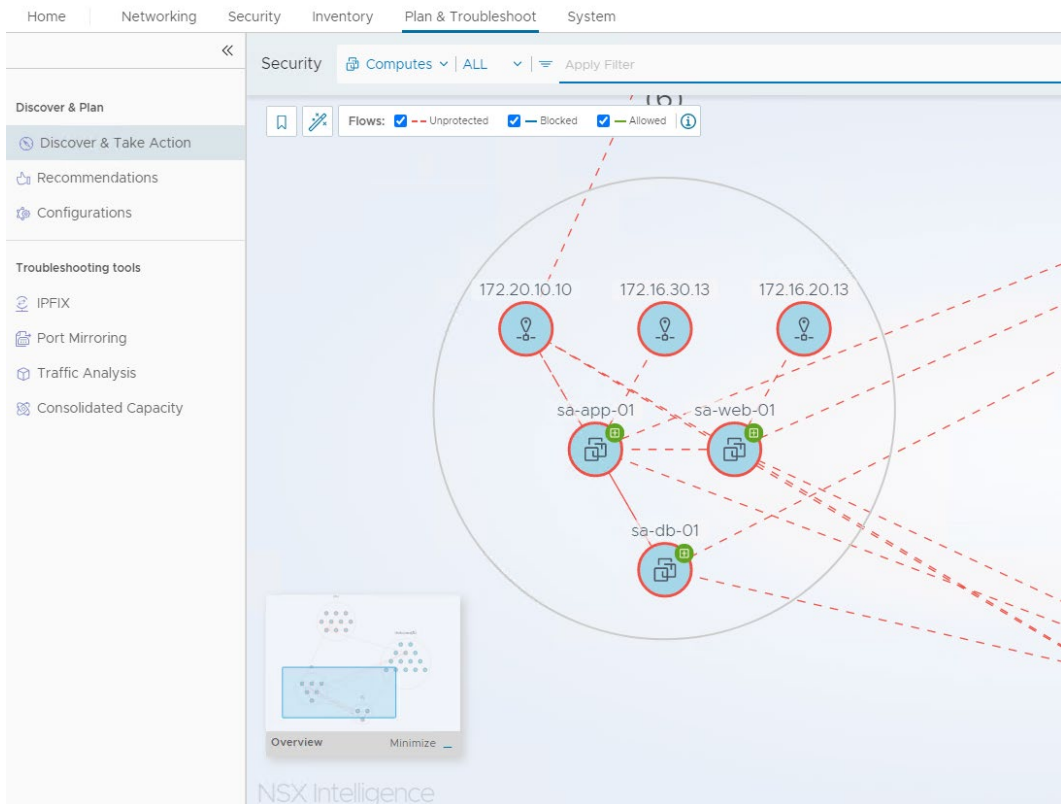
- Describe NSX Intelligence and its use cases
- Explain NSX Intelligence system requirements
- Activate NSX Intelligence
- Explain NSX Intelligence visualization, recommendation, and network traffic analysis capabilities



## 8-86 About NSX Intelligence

NSX Intelligence is a distributed analytics solution that provides visibility and dynamic security policy enforcement for NSX environments. Features of NSX Intelligence include:

- Visualization of the data center objects and traffic flows
- Recommendations for micro-segmentation planning
- Suspicious Traffic Detection to identify abnormal traffic patterns



## 8-87 Use Cases for NSX Intelligence

NSX Intelligence enables several capabilities for security administrators.



Visibility



Policy  
Recommendations



Suspicious Traffic  
Detection

NSX Intelligence enables the following capabilities for security administrators:

- Visibility: Provide insight about the micro-segmentation traffic flows
- Policy recommendations: Generate security recommendations and dynamically enforce security policies
- Suspicious Traffic Detection: Use AI techniques to detect malicious network behaviors

## 8-88 NSX Intelligence Requirements

The requirements for using NSX Intelligence are as follows:

- NSX Application Platform with an Advanced form factor must be deployed in the environment.
- You must have a valid NSX license to avail the NSX Intelligence features.
- You must have an Enterprise Administrator role to start and stop data collection.

Before deploying NSX Intelligence, ensure that you have the correct NSX license for the NSX Intelligence features that you are planning to use in your environment. For more information about the product offerings for NSX 4.0.x security, see VMware knowledge base article [89137] at <https://kb.vmware.com/s/article/89137>.

The Enterprise Administrator role starts and stops data collection. Other user roles, such as Security Administrators, can visualize the NSX Intelligence data and create and apply recommendations. However, an Enterprise Administrator role is mandatory to start and stop data collection.

# 8-89 NSX Intelligence Activation

Before you can start using the visualization, recommendation, and suspicious traffic detection capabilities of NSX Intelligence, you must activate the NSX Intelligence feature from the NSX UI or API.

The activation process runs some prechecks to ensure that the feature can successfully run in the environment.

Features

You can activate these features based on the selected form factor and the valid NSX Data Center license that is in effect. [Learn more](#)

METRICS

Status: UP

Feature Version: 4.0.10.0.20606727

Data Collection

NSX Application Platform

NSX

NSX INTELLIGENCE

NSX NETWORK DETECTION AND RESPONSE

NSX MALWARE PREVENTION

NSX Intelligence

NSX Intelligence is a native distributed analytics engine that leverages workload and network context available within NSX to provide deep traffic flow visibility, firewall policy recommendations, and suspicious traffic detection.

It is mandatory to run the prechecks to ensure all prerequisites are met.

RUN PRECHECKS

Name	Description	Status	Reason
Advanced Features License Check	Validate optional advanced license requirements	Not Started	
NSX License Validation	Validate minimum license requirement is met	Not Started	

CANCEL

ACTIVATE

You can activate NSX Intelligence from the NSX UI by selecting **System > Configuration > NSX Application Platform**. The NSX Intelligence tile can be found under the features section of NSX Application Platform.

NSX Intelligence is unavailable if NSX Application Platform is not deployed with an Advanced form factor in the environment or if the required licenses are not available.

For more information about upgrading from an earlier version of NSX Intelligence to NSX Intelligence 4.0.1 or later, see *Activating and Upgrading VMware NSX Intelligence* at <https://docs.vmware.com/en/VMware-NSX-Intelligence/4.0/install-upgrade/GUID-9F91CFBC-DE26-451C-90E0-5AC07117BFFD.html>

475

## 8-90 Validating the NSX Intelligence Deployment

You can use common kubectl commands to better understand the state of the NSX Intelligence deployment:

- Validate the successful deployment of the NSX Intelligence pods:

```
kubectl get pods -n nsxi-platform
```

- Display the detailed state of all containers within a pod:

```
kubectl describe pod <pod-name> -n nsxi-platform
```

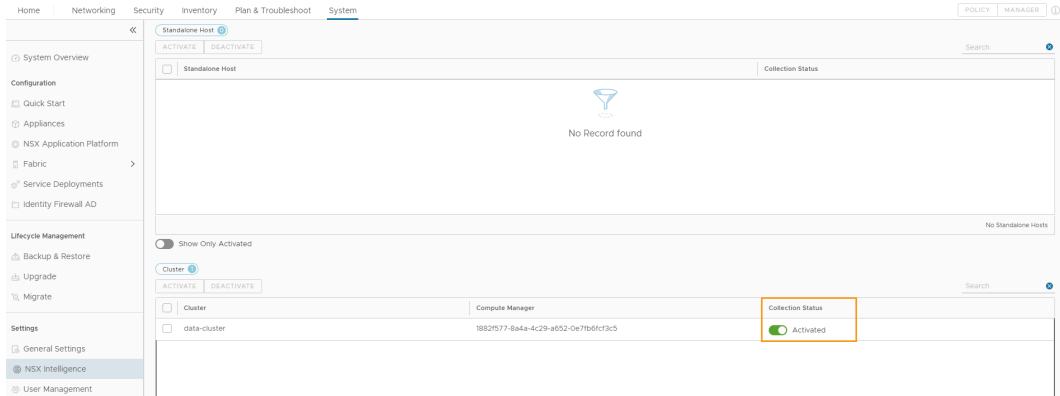
- Review the logs for a given pod:

```
kubectl logs <pod-name> -n nsxi-platform
```

The activation of NSX Intelligence on NSX Application Platform deploys additional pods on the Kubernetes cluster. You can use common kubectl commands to better understand the state of the NSX Intelligence deployment and to review the logs for a particular pod, if required.

## 8-91 Granular Data Collection

NSX Intelligence provides the ability to select the standalone hosts or clusters for which you want to enable data collection.

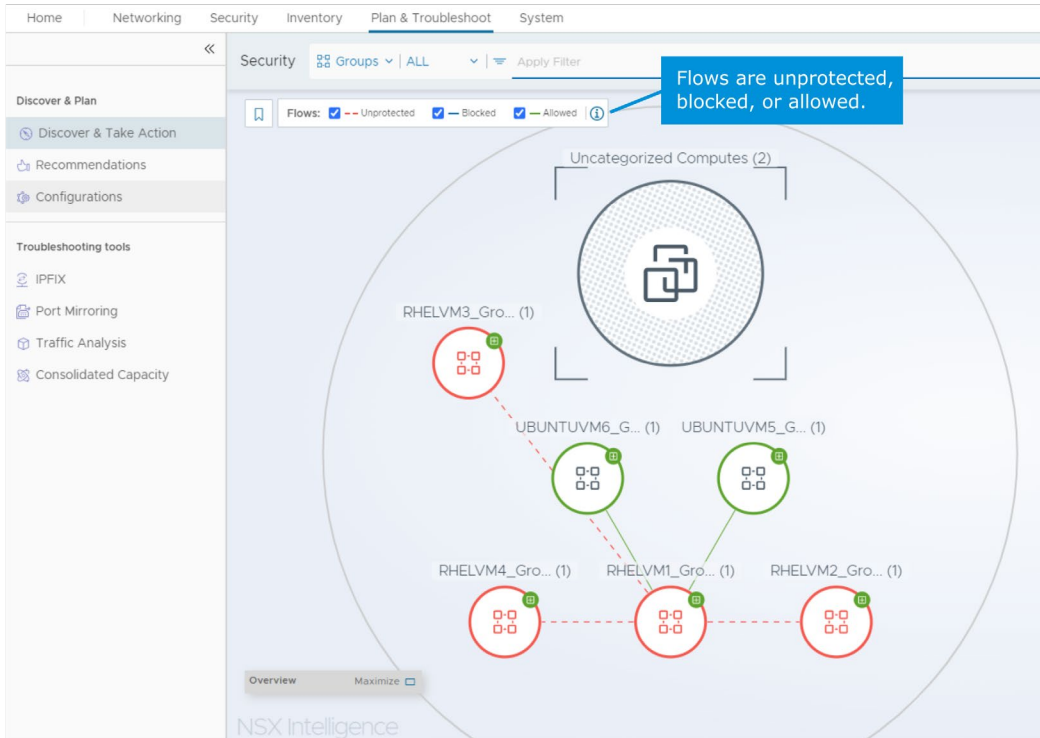


On new deployments of NSX Intelligence, data collection is enabled by default on all hosts and clusters. As an NSX Administrator, you can choose to collect data for particular standalone hosts or clusters. This method helps reduce the amount of data to capture and process, which improves the amount of resources available in the environment.

You can adjust the NSX Intelligence data collection settings from the NSX UI by selecting **System > Settings > NSX Intelligence**.

## 8-92 NSX Intelligence Visualization (1)

You can visualize flows for VMs and security groups by selecting **Plan & Troubleshoot** > **Discover & Plan** > **Discover & Take Action**.



Users can filter data flows based on security groups, VMs, physical servers, and IP addresses.

NSX Intelligence offers a time range for the visualization of traffic flows called Now, which you can use to visualize the most recent flows in your environment.

Traffic flows display public IP addresses used as sources and destinations.

In addition, NSX Intelligence offers enhanced filtering capabilities to more granularly define flows that are displayed in the canvas.

Data flows are divided into the following categories:

- Unprotected: The traffic flow matches the default firewall rule to allow, drop, or reject any traffic from any source and any destination. More granular security policies are needed to secure the environment.
- Blocked: The traffic flow matches a more granular rule than the default rule that drops or rejects traffic.
- Allowed: The traffic flow matches a more granular rule than the default rule that allows traffic.

## 8-93 NSX Intelligence Visualization (2)

You can examine the details of traffic flows by clicking the corresponding line in the canvas.

Flow Details between Groups | ⌚ Last 24 Hours

Showing flow details for RHELM1\_Group → UBUNTUVM6\_Group

Completed Flows | Active Flows

#Flow(s) 1

COLLAPSE ALL | Filter

Source		Destination		Services	Latest Flow
Compute	Group	Compute	Group		
▼ rhelvm1	RHELM1_Group	ubuntuvm6	UBUNTUVM6_Group	SSH	● Allowed
FQDN		Source User		End Time	Oct 22, 2022, 7:01:09 AM
Application ID		Process		Source Rx/Tx	73/49 Packets
Destination Rx/Tx ① 50/73 Packets		Source IP 172.16.100.1		Destination IP ①	172.16.100.6

The screenshot shows details about an allowed SSH flow between the rhelvm1 and ubuntuvm6 VMs.

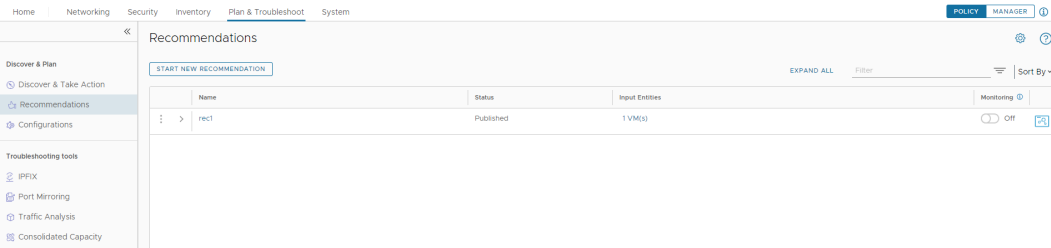
Each flow includes the following information:

- Source: Name of the source VM, the source IP address, the user, and the process run
- Destination: Name of the destination VM and the destination IP address
- Services: Service or services identified in the flow
- App ID: Application ID, if applicable
- FQDN: Fully qualified domain name, if applicable
- Latest Flow: Unprotected, allowed, or blocked
- End Time: Time when the flow ended

# 8-94 NSX Intelligence Recommendations (1)

You can start security recommendations by selecting **Plan & Troubleshoot > Discover & Plan > Recommendations**.

You can initiate multiple recommendations at one time. However, they are processed sequentially.



Many application owners do not have access to the NSX UI. So, you must be able to export the recommendation in a readable format.

In previous versions of NSX, only the JavaScript Object Notation (JSON) format was supported for the export.

You can now export the recommendation in the comma-separated values (CSV) format.

The CSV format stores values in a text file using a comma to separate every value. This format is typically used to store tabular data.



## 8-95 NSX Intelligence Recommendations (2)

Recommendations analyze traffic data for a given security group or set of VMs for a specified period. Recommendations suggest security groups, services, and distributed firewall rules.

You configure the following parameters to start a recommendation:

- Selected Entities in Scope
- Time Range
- Connectivity Strategy
- Recommendation Output
- Group Reuse Threshold
- Recommendation Service Type
- Exclusion

### Start New Recommendation

For a selected set of entities (Groups, VMs, Physical Servers), NSX Intelligence will recommend DFW rules for East-West traffic, which can be validated and published. The recommended rules include new policies, groups, and services for applications.

Recommendations discovery can take up to 5-30 minutes to complete. The discovery status can be tracked from the "Recommendations" tab

Recommendation Name REC2

Note: This will be used as a suffix when naming new recommended groups and rules

Description

Recommendation 2

Selected Entities in Scope

6 Group(s)

A new section will be created for the recommendation.

Time Range

Last 24 Hours

Advanced Options

Connectivity Strategy

Create Rules For

All Traffic

Default Rule

None

Recommendation Output

Compute-based IP-based

Group Reuse Threshold

10% 80% 100%  
Aggressive Reuse Minimal Reuse

Recommendation Service Type

L4 Services L7 Context Profiles

Exclusion

Exclude Flows

Multicast flows Broadcast flows

Exclude Infrastructure Workloads

Deactivated

CANCEL

START DISCOVERY

You configure the following parameters to start a recommendation:

- **Selected Entities in Scope:** VMs, physical servers, and security groups can be used as inputs for the recommendation. Security groups can include virtual machines, segment ports, segments, and VIFs.

NSX Intelligence allows the selection of multiple groups as the scope for a new recommendation. These groups must contain no more than 250 effective compute entities in total.

To enhance the fidelity of the recommendations in brownfield deployments, NSX Intelligence also considers the existing distributed firewall policies that are applied to the groups selected as the scope for a new recommendation.

- **Time Range:** This parameter is the period for which data is analyzed. It ranges from the last 1 month to the last 1 hour.
- **Connectivity Strategy:**
  - **Create Rules For:**
    - **All Traffic:** This default option considers all outbound, inbound, and intra-application traffic flow types.
    - **Incoming and Outgoing Traffic:** This option considers all traffic flow types that originate both inside and outside the application boundary.
    - **Incoming Traffic:** This option only considers traffic flow that originates outside the application boundary.
  - **Default Rule:**
    - **None:** This default option does not create any default rule for the security policy.
    - **Allowlist:** This option creates a default drop rule.
    - **Denylist:** This option creates a default allow rule.
- **Recommendation Output:**
  - **Compute-based:** This default option recommends security groups, including VMs.
  - **IP-based:** This option recommends security groups, including a static list of IPs.
- **Group Reuse Threshold:** Users can customize the group reuse threshold to determine whether existing groups should preferably be reused or new ones created instead. A low threshold of around 10 percent represents an aggressive group reuse, whereas a high threshold of 100 percent indicates minimal group reuse. The default group reuse threshold is set to 80 percent.

Beginning with NSX 4.0.1, NSX Intelligence can reuse some of the ipset groups already present in the NSX inventory when making recommendations to avoid having too many groups.

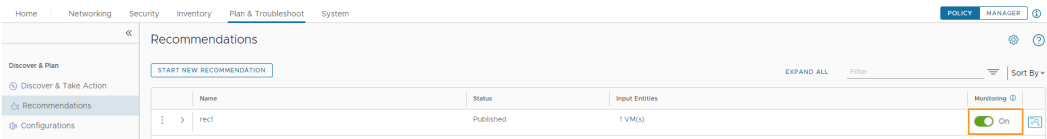
- Recommendation Service Type:
  - L4 Services: This default option generates L4 services and rules as an output for the recommendation.
  - L7 Context Profiles: L7 rules, including context-profile information, are recommended for flows with L7 application ID information. If application information is not available, L4 recommendations are generated.
- Exclusion:
  - Exclude Flows: This setting specifies the traffic flow types to exclude during the recommendation analysis. Default values are Broadcast flows and Multicast flows. These flow types are not relevant for application category rules. Excluding broadcast flows, multicast flows, or both flow types can help optimize the DFW rule recommendation analysis.
  - Exclude Infrastructure Workload: New to NSX 4.0.1, this feature classifies the VMs in the environment. An algorithm determines which VMs are part of the network infrastructure. The administrator can then decide to exclude those infrastructure VMs from the workload recommendation, which reduces noise from the infrastructure during the recommendation and the visualization of the workloads.

# 8-96 NSX Intelligence Recommendations (3)

The Monitoring column indicates whether VM changes are detected after the initial recommendation.

If VMs change their group membership after the initial analysis session, a rerun flag is set and users are prompted to rerun the recommendation to analyze changes.

You can turn the **Monitoring** toggle on or off.



Home	Networking	Security	Inventory	Plan & Troubleshoot	System	POLICY	MANAGER	?
Recommendations								
START NEW RECOMMENDATION								
EXPAND ALL Filter Sort By								
	Name	Status	Input Entities	Monitoring				
:	>	rec1	Published	1 VM(s) On				

# 8-97 NSX Intelligence Recommendations (4)

The recommended distributed firewall rules, security groups, and services can be published in NSX Manager.

Recommendations

1 Review Recommendations

2 Sequence & Publish

REC 2

Showing recommended Policy Rules for the selected input entities (0 Groups, 5 VMs, 0 Physical Servers) as well as the other entities they communicate with. The recommended rules cover **All Traffic** flows. [LEARN MORE](#)

Filter

NSX Intelligence

Recommended Policies

Rules (3)

Groups (4)

Services (0)

Flows Used For Recommendations

Category: Application

Name	Sources	Destinations	Services	Profiles	Applied To	Action	
Policy-1 (REC 22082... (3)	Applied To 1 Groups					Default Rule	None
<a href="#">New</a> Rule-1 (REC 2...	Group-1 (REC 2...	Group-2 (REC ...	DNS-UDP	None	Group-1 (REC 2...	Allow	
<a href="#">New</a> Rule-2 (REC 2...	Group-1 (REC 2...	Any	NTP	None	Group-1 (REC 2...	Allow	
<a href="#">New</a> Rule-3 (REC 2...	Group-3 (REC ...	Group-4 (REC ...	NBNS-Broadc... NBDG-Broadc...	None	Group-1 (REC 2...	Allow	

CANCEL

CONTINUE LATER

PROCEED

After the recommendation session is completed, recommendations about the distributed firewall rules, security groups, and services that should be created to secure the environment are provided. You can publish these recommendations in NSX Manager and the distributed firewall rules, security groups, and services are automatically configured for you. You can customize the recommendations before final publication. This customization can include changing the names of the recommended rules and security groups.

Beginning with NSX 4.0.1, you can review and change the group name by directly clicking the group on the **Rules** tab.

## 8-98 NSX Suspicious Traffic Detection

The NSX Suspicious Traffic Detection feature analyses the data collected by NSX Intelligence and flags suspicious activities using the supported detectors:

- Data Upload/Download
- Destination IP Profiler
- DNS Tunneling
- Domain Generation Algorithm (DGA)
- Horizontal Port Scan
- LLMNR/NBT-NS Poisoning and Relay
- Netflow Beacons
- Network Traffic Drop
- Port Profiler
- Server Port Profiler
- Remote Services
- Uncommonly Used Port
- Unusual Network Traffic Pattern
- Vertical Port Scan

NSX Intelligence supports the detection of the following threats:

- Data Upload/Download: Detects and alerts if an unusually large amount of data is uploaded or downloaded from a VM
- Destination IP Profiler: Detects and alerts if a VM connects to an IP address that is not part of its typical communication pattern
- DNS Tunneling: Detects and alerts about an unusual volume of differing DNS requests towards the same root DNS name

This action might suggest an attempt to exfiltrate data over DNS.

- Domain Generator Algorithm (DGA): Detects and alerts about suspicious DNS traffic from a VM, indicating potential activity from DGA malware

DGAs are used by cybercriminals to prevent their servers from being blocked or taken down. The algorithm produces new domains on demand that a malware sample can use as its Command & Control server.

- Horizontal Port Scan: Detects and alerts if an intruder tries to attack a single port or service across multiple VMs

Horizontal Port Scan is also known as sweeping.

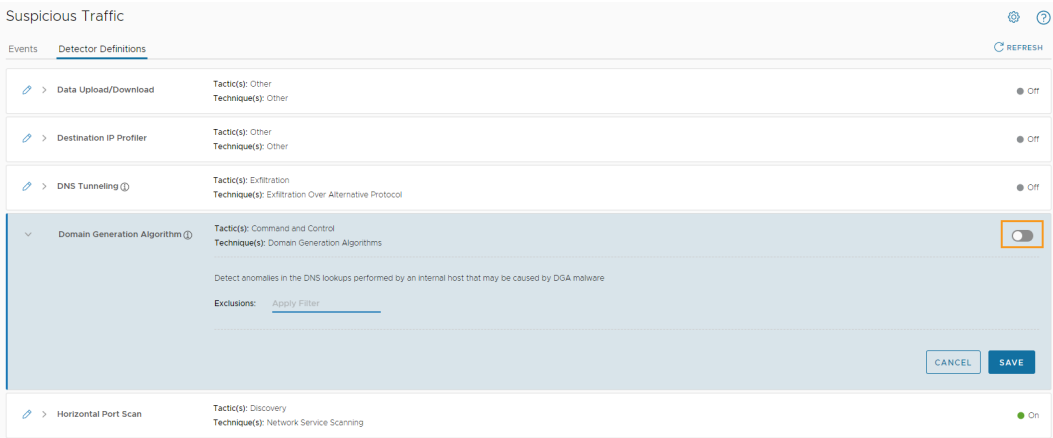
- LLMNR/NBT-NS Poisoning Relay: Detects and alerts if a VM sends an unusual number of responses to LLMNR/NBT-NS requests
- Netflow Beacons: Detects and alerts if a VM indicates beaconing behavior, such as contacting one or more hosts at regular intervals and transferring a similar number of bytes
- Network Traffic Drop: Detects and alerts if an unusually high amount of traffic is dropped by a distributed firewall rule
- Port Profiler: Detects and alerts about suspicious ports accessed from a source VM
- Server Port Profiler: Detects and alerts about suspicious ports accessed on a target machine
- Remote Services: Detects and alerts if suspicious behavior is observed for remote connections such as telnet, SSH, VNC, and remote RDP/RDS sessions.
- Uncommonly Used Port: Detects and alerts if a nonstandard port is used for a given a protocol

For example, SSH traffic runs on a port other than the standard port 22.

- Unusual Network Traffic Pattern: Detects and alerts about deviations from predicted network traffic patterns for a given VM
- Vertical Port Scan: Detects and alerts if an intruder tries to attack multiple open ports or services of a target VM

# 8-99    Configuring Detector Definitions

You can enable the detectors you are interested in on the **Detector Definitions** tab in the NSX UI. All detectors are disabled by default.



Suspicious Traffic Detection is only supported for hosts and clusters that have data collection enabled.

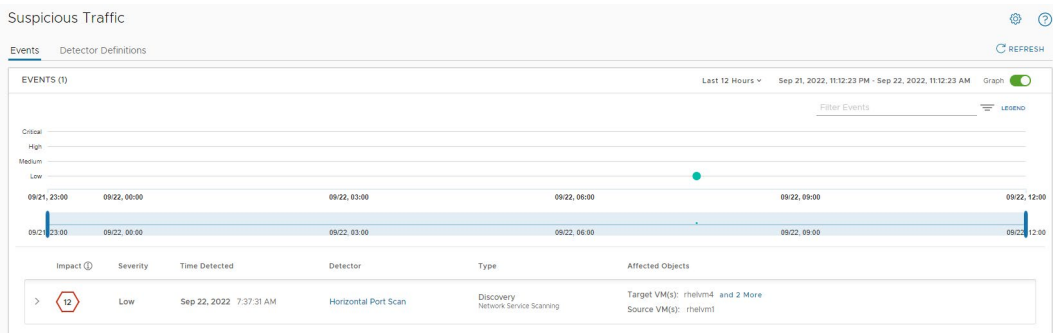
When data collection is enabled, you can enable the detectors you are interested in by selecting **Security > Threat Event Monitoring > Suspicious Traffic > Detector Definitions**.

Click the pencil icon next to the name of the detector to enter edit mode and turn on the toggle.

All detectors are disabled by default. You must explicitly turn on each detector that you want to use in your NSX environment.

# 8-100 Visualizing Detected Threats (1)

Detected Threats are displayed on the **Events** tab. Threats are classified according to the MITRE ATT&CK Framework.



You visualize the threat detection events by selecting **Security > Threat Event Monitoring > Suspicious Traffic > Events**.

The **Events** tab displays all threat detection events identified in the system, classified according to the MITRE ATT&CK framework:

- Persistence events appear in dark orange.
- Credential Access events appear in light blue.
- Discovery events appear in green.
- Command and Control events appear in light purple.
- Lateral Movement events appear in light orange.
- Collection events appear in dark gray.
- Exfiltration events appear in red.

The event classification is also specified in the Type section of the event description.

Events that cannot be clearly mapped to an existing MITRE ATT&CK framework tactic or technique are categorized under the Other category.

Threat detection events are graphically represented by a histogram. Security administrators can specify the period that they are interested in by adjusting the blue vertical lines.

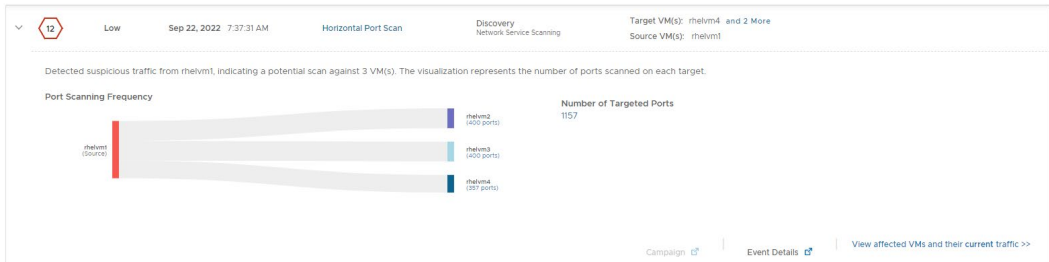
Each threat event type is represented by a dot in the histogram. The size of the dot is proportional to the number of occurrences of an event.

Additional information about each type of event appears in a tabular format.



## 8-101 Visualizing Detected Threats (2)

Each detected threat can be expanded to retrieve additional details, including its impact score, severity, detector type, affected objects, detected anomalies, and so on.



The impact score for a given event is calculated by combining its severity and the confidence of the detector technique.

The detector type is also displayed in the event details, along with a brief description.

The affected objects, such as target or source VMs, are also displayed here.

Finally, depending on the detector type, the deviation between the normal pattern of behavior and the anomaly is also included.

## 8-102 Review of Learner Objectives

- Describe NSX Intelligence and its use cases
- Explain NSX Intelligence system requirements
- Activate NSX Intelligence
- Explain NSX Intelligence visualization, recommendation, and network traffic analysis capabilities

# 8-103 Lesson 5: NSX Network Detection and Response

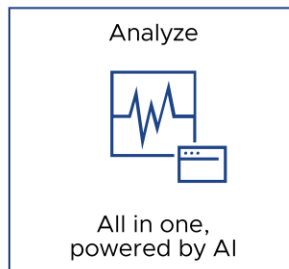
## 8-104 Learner Objectives

- Describe NSX Network Detection and Response and its use cases
- Explain the architecture of NSX Network Detection and Response
- Activate NSX Network Detection and Response
- Describe the visualization capabilities of NSX Network Detection and Response

## 8-105 About NSX Network Detection and Response

NSX Network Detection and Response is an advanced threat prevention platform that provides complete network visibility, detection, and prevention of sophisticated threats:

- Collects network traffic across on-premises networks, cloud, and hybrid cloud infrastructures
- Uses artificial intelligence techniques to analyze network traffic and gain insights into advanced threats
- Helps security teams to visualize the entire attack and trigger the appropriate response



## 8-106 NSX Network Detection and Response Use Cases

Security teams use NSX Network Detection and Response to perform several functions.



Detect All  
Threat  
Movements



Visualize  
the Entire  
Attack



Prevent  
Intrusions  
Faster



Reduce  
False  
Positives

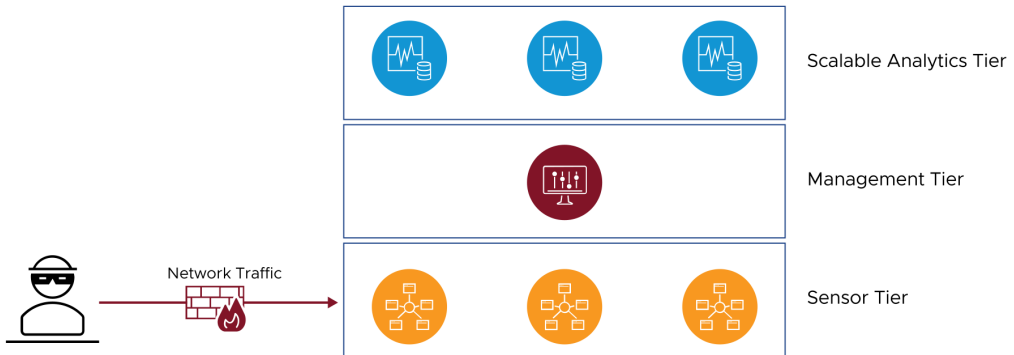
Security teams can use NSX Network Detection and Response for the following purposes:

- Detect all threat movements: NSX Network Detection and Response can detect threats entering the network perimeter (north-south) as well as attacks that move laterally in the network perimeter (east-west).
- Visualize the entire attack: With NSX Network Detection and Response, you can visualize a complete campaign blueprint and a detailed threat timeline across the network so that you can quickly understand the scope of an attack and prioritize resources. Additionally, NSX Network Detection and Response maps to the MITRE ATT&CK tactics and techniques for greater understanding of the key events in a campaign.
- Prevent intrusions faster: NSX Network Detection and Response uses real-time, scalable AI and machine learning to detect and stop threats at wire speed.
- Reduce false positives: NSX Network Detection and Response delivers the industry's highest-fidelity insights into advanced threats and reduces false positives by up to 90 percent. NSX Network Detection and Response learns in real time to update detection fidelity.

## 8-107 NSX Network Detection and Response High-Level Architecture

The high-level architecture of NSX Network Detection and Response contains the following tiers:

- Scalable Analytics tier
- Management tier
- Sensor tier



The high-level architecture of NSX Network Detection and Response contains distinct tiers with the following functions:

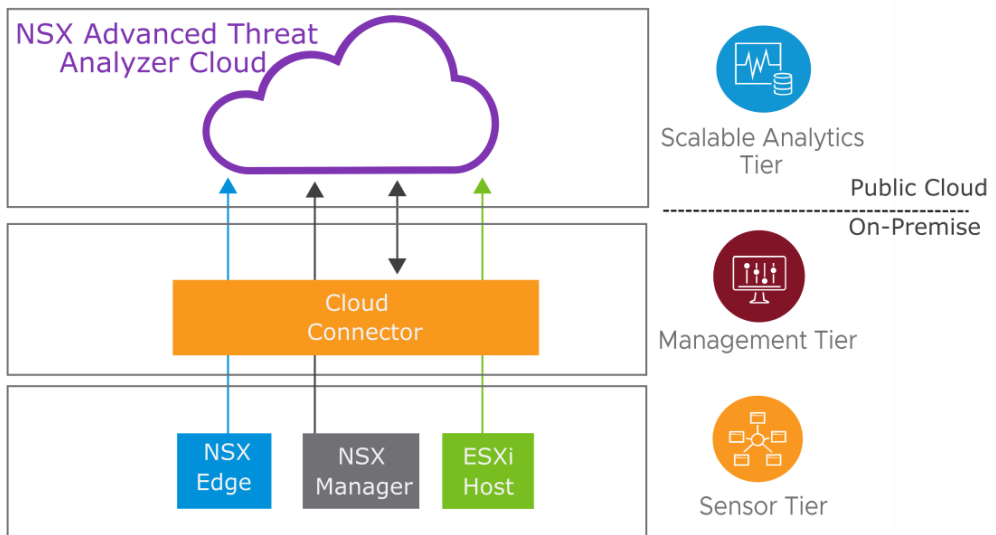
- The Scalable Analytics tier is like the brain of NSX Network Detection and Response. It is a distributed analytics platform containing multiple nodes that perform deep content inspection, network traffic analysis, network and asset profiling, and anomaly detection.
- The Management tier provides the REST API and a web-based UI for all user configurations. It also displays alerts and intrusion events.
- The Sensor tier includes one or more sensors, and it is responsible for collecting network traffic across the environment.

## 8-108 NSX Network Detection and Response in NSX Deployments

The capabilities of NSX Network Detection and Response are closely integrated with on-premises NSX deployments:

- NSX Network Detection and Response collects security events and system configuration data from the NSX Edge nodes, NSX Manager, and ESXi hosts (Sensor tier).
- The collected data is analyzed and correlated using a cloud-based distributed analytics platform called NSX Advanced Threat Analyzer Cloud (Scalable Analytics tier).
- NSX Cloud Connector displays alerts and intrusion events through a web-based UI (Management tier).

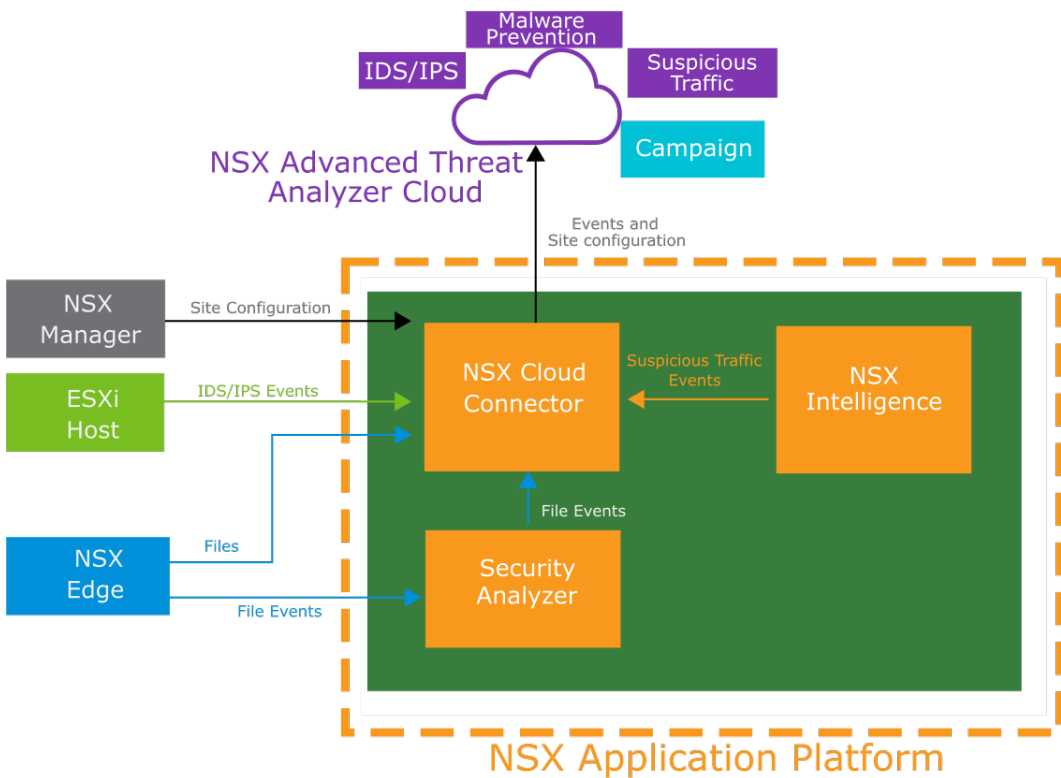
NSX Network Detection and Response is also used for dynamic file analysis or sandboxing when malware prevention is enabled in the NSX environment.



## 8-109 NSX Network Detection and Response Architecture (1)

NSX Network Detection and Response collects the following data from the NSX platform:

- IDS/IPS events from the ESXi hosts
- Suspicious traffic events from NSX Intelligence
- Files and malware prevention events from the NSX Edge nodes and Security Analyzer
- Site configuration data from NSX Manager

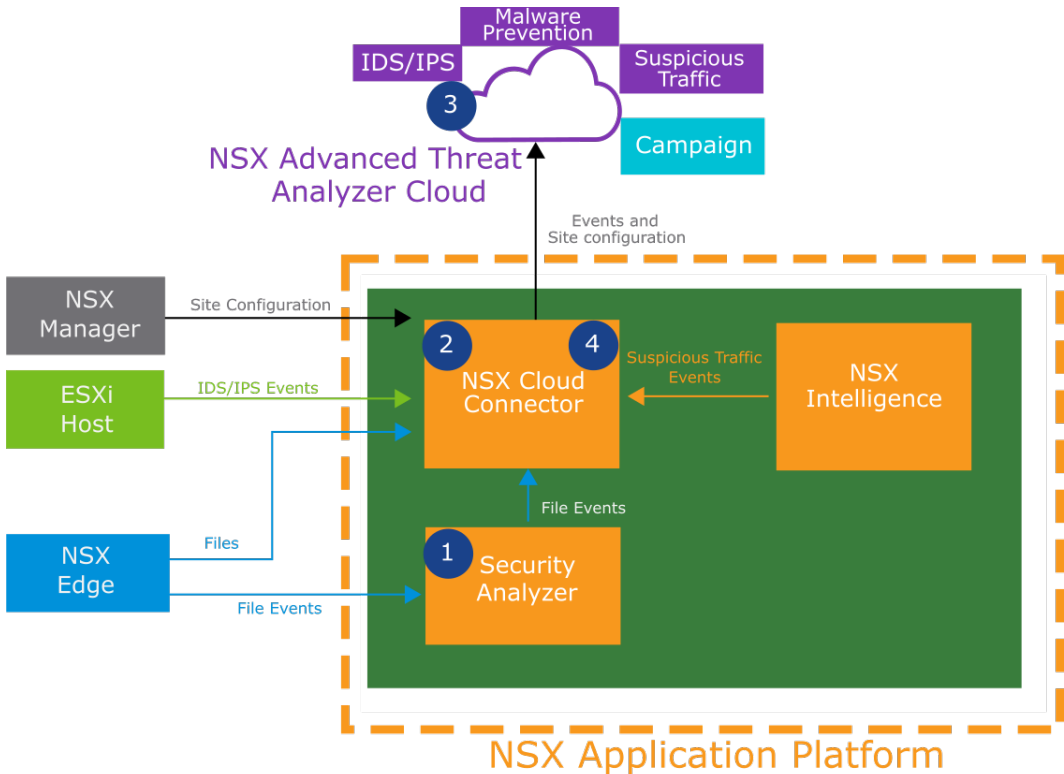


North-south IDS/IPS events and east-west malware prevention events are not yet collected.

## 8-110 NSX Network Detection and Response Architecture (2)

Data collected from the NSX environment is aggregated and analyzed as follows:

1. Security Analyzer receives malware prevention events from the NSX Edge nodes and forwards them to NSX Cloud Connector.
2. NSX Cloud Connector gathers IDS/IPS events, malware prevention events and files, and suspicious traffic events from NSX and forwards them to NSX Advanced Threat Analyzer Cloud.
3. NSX Advanced Threat Analyzer Cloud analyzes and correlates the IDS/IPS, malware prevention, and suspicious traffic events and provides insights about ongoing campaigns.
4. Campaign information appears in the NSX Network Detection and Response UI.





Data collected from the NSX environment is aggregated and analyzed as follows:

1. Security Analyzer receives file events from the malware prevention modules in the NSX Edge nodes and persists them locally. These events are then forwarded to NSX Cloud Connector.
2. NSX Cloud Connector serves as a gateway between the on-premises deployment of NSX and the NSX Advanced Threat Analyzer Cloud distributed analytics platform. Its purpose is to centralize communication with NSX Advanced Threat Analyzer Cloud services and provide an authenticated channel between clients and the cloud. It gathers IDS/IPS events from the ESXi hosts, malware prevention events and files from the NSX Edge node, and suspicious traffic events from NSX Intelligence. The Cloud Connector then forwards all the information to the NSX Advanced Threat Analyzer Cloud for further analysis.
3. NSX Advanced Threat Analyzer Cloud analyzes and correlates the IDS/IPS, malware prevention, and suspicious traffic events and provides insights about ongoing campaigns. A campaign is a set of related events that use specific techniques and can be mapped to the MITRE ATT&CK Framework stages to define an attack story.
4. Campaign information is displayed in the NSX Network Detection and Response UI, which resides in NSX Cloud Connector. The NSX Network Detection and Response UI is separate from the NSX UI, but it can be cross-launched from NSX Manager.

## 8-111 NSX Network Detection and Response Requirements

Before sending events and data to NSX Advanced Threat Analyzer Cloud for campaign correlation, you must activate the NSX Network Detection and Response feature from the NSX UI.

The requirements for activating NSX Network Detection and Response are as follows:

- As a minimum, NSX Application Platform must be deployed with a Standard form factor in the environment. The Advanced and Evaluation form factors are also supported.
- NSX Detection and Response requires an NSX Advanced Threat Prevention license.
- NSX Advanced Threat Analyzer Cloud must be reachable from NSX Application Platform.

By installing NSX Network Detection and Response, customers accept sending the following data to the public cloud:

- Files for sandboxing or event correlation
- IDS/IPS and malware prevention events for correlation
- Suspicious traffic events for correlation, if NSX Intelligence is available in the environment


NSX Advanced Threat Analyzer Cloud must be reachable from NSX Application Platform. Deployments without Internet connectivity are not supported.

# 8-112 NSX Network Detection and Response Activation (1)

You activate NSX Network Detection and Response by selecting **System > Configuration > NSX Application Platform > Features**.

The NSX Network Detection and Response activation deploys both NSX Cloud Connector and the components required by NSX Network Detection and Response.


As part of the activation, you specify the NSX Advanced Threat Analyzer Cloud instance that you want your environment to connect to.


 NSX Network Detection and Response

NSX Network Detection and Response sends alert data to VMware NSX Advanced Threat Prevention cloud services to perform correlation and visualization.

Cloud Region

Select Cloud Region ⓘ

☒  United States 1

☐  European Union 1

ⓘ To maximize the NSX Network Detection and Response feature, activate at least one of the following additional features. Any activated feature will use the same cloud region selected above.

Additional Features (Any one)

NSX Intelligence

NSX Malware Prevention

Suspicious Network Activity

IDS/IPS

Cloud Connectivity and Licensing Checks Before NDR Activation

It is mandatory to run the prechecks to ensure all prerequisites are met.

RUN PRECHECKS

Name	Description	Status
NSX Advanced Threat Analyzer Cloud Eligibility	Validate license is eligible for cloud integration	✔ Completed
NSX Advanced Threat Analyzer Cloud Reachability	Validate selected cloud region can be reached and meets user selection criteria	✔ Completed

CANCEL

ACTIVATE

NSX Cloud Connector is a shared component between NSX Network Detection and Response and NSX Malware Prevention. The NSX Cloud Connector deployment is skipped if the NSX Malware Prevention feature is already configured in the environment.

In environments in which both these features are activated, changing the cloud region requires reinstalling both NSX Network Detection and Response and NSX Malware Prevention. Modifying the cloud region after installation is not supported.

To fully use the capabilities of NSX Network Detection and Response, you enable the following NSX features in the environment:

- NSX Intelligence
- NSX Malware Prevention
- Suspicious Network Activity: Refers to the Suspicious Traffic Detection capabilities provided by NSX Intelligence
- NSX Distributed IDS/IPS

Before proceeding with the activation of NSX Network Detection and Response, the activation wizard verifies that the applied NSX Advanced Threat Prevention license is valid and that NSX Advanced Threat Analyzer Cloud is accessible.

The FQDN for the United States cloud is `nsx.west.us.lastline.com` and the FQDN for the European cloud is `nsx.nl.emea.lastline.com`. NDR uses HTTPS port 443 to access NSX Advanced Threat Analyzer Cloud.

Additional cloud regions might become available over time.

## 8-113 NSX Network Detection and Response Activation (2)

You can validate the successful activation of NSX Network Detection and Response from the NSX UI.

**NSX NETWORK DETECTION  
AND RESPONSE**

Status: ● UP

Region: United States 1

Feature Version: 4.0.1.0.0.20606727

GO TO NSX NETWORK DETECTION AND ...

ACTIONS ▾

# 8-114 Validating the NSX Network Detection and Response and NSX Cloud Connector Deployments

To verify that the NSX Cloud Connector and NSX Network Detection and Response components are running, you run the following command in your Kubernetes cluster:

```
kubectl get pods -n nsxi-platform | egrep "(cloud-connector|nsx-ndr) "
```

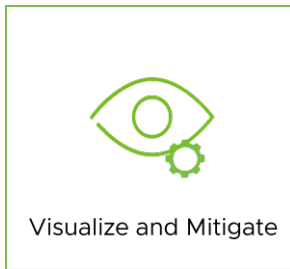
```
kadmin@SA-K8s-CTRL-01:~$ kubectl get pods -n nsxi-platform | egrep "(cloud-connector|nsx-ndr) "
cloud-connector-check-license-status-596bff9666-4rqgf      2/2      Running      0      14h
cloud-connector-file-server-5bb8957bf4-t9smv             1/1      Running      0      14h
cloud-connector-proxy-759cc5b69f-kncvb                   2/2      Running      0      14h
cloud-connector-register-wgpmx                           0/2      Completed    0      14h
cloud-connector-update-license-status-6b8fc876c8-qh4kj    2/2      Running      0      14h
nsx-ndr-enable-ids-b26vk                                  0/1      Completed    0      14h
nsx-ndr-feature-switch-watcher-notifier-ndr-79886f475f-96tqc 1/1      Running      0      14h
nsx-ndr-setup-kafka-hq4jq                                 0/1      Completed    0      14h
nsx-ndr-upload-config-db847644b-vm7mw                    2/2      Running      0      14h
nsx-ndr-worker-file-event-processor-8cc6b7f58-nhbqx       2/2      Running      0      14h
nsx-ndr-worker-file-event-uploader-77b4f9c95b-nmrpc       2/2      Running      0      14h
nsx-ndr-worker-ids-event-processor-df54bb4f9-bnvtk        2/2      Running      0      14h
nsx-ndr-worker-monitored-host-uploader-6f6f6c9f75-j62vn   2/2      Running      0      14h
nsx-ndr-worker-ndr-event-processor-5dffb58878-x5dfh       2/2      Running      0      14h
nsx-ndr-worker-ndr-event-uploader-684f7976d-2mj8x        2/2      Running      0      14h
```

In a healthy environment, all NSX Cloud Connector and NSX Network Detection and Response pods must show a status of Running or Completed. The example output in the screenshot corresponds to an environment with a Evaluation form factor in which NSX Intelligence is not installed. In an Advanced form factor deployment with NSX Intelligence installed, additional pods are available, such as nsx-ndr-worker-nta-event-processor that is responsible for processing Suspicious Traffic events from NSX Intelligence.

## 8-115 Visualizing and Mitigating Attacks

NSX Network Detection and Response creates attack visualizations that give security teams the required context to quickly understand the scope of an attack and prioritize their response, including:

- Extent and duration of every event
- Active threats and affected hosts
- Communication between local and external systems
- Data sets accessed and harvested

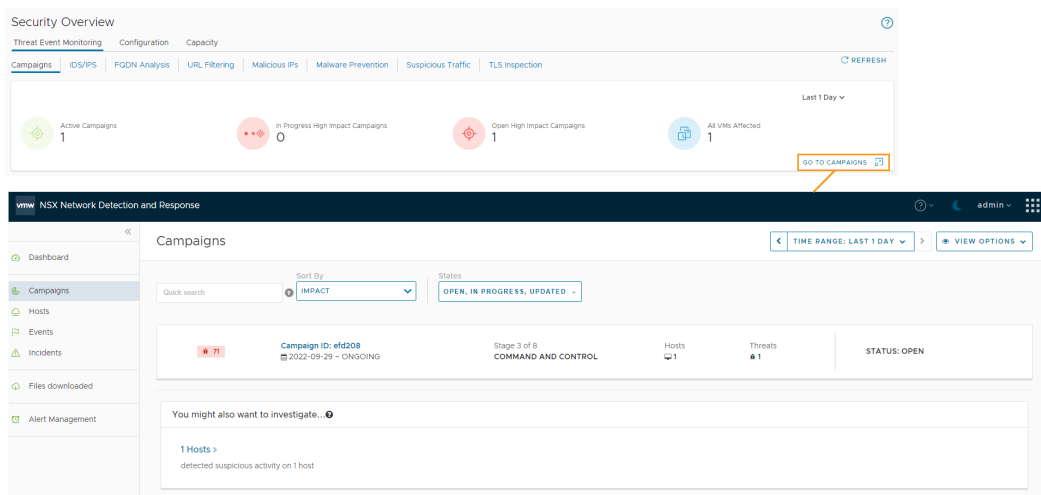


# 8-116 Accessing the NSX Network Detection and Response UI

The NSX Network Detection and Response UI is installed as a plug-in in the NSX UI during the NSX Cloud Connector deployment.

You can access the NSX Network Detection and Response UI by clicking the **GO TO CAMPAIGNS** link in the Security Overview page.

Alternatively, you can access the NSX Network Detection and Response UI from the NSX Network Detection and Response tile in NSX Application Platform.

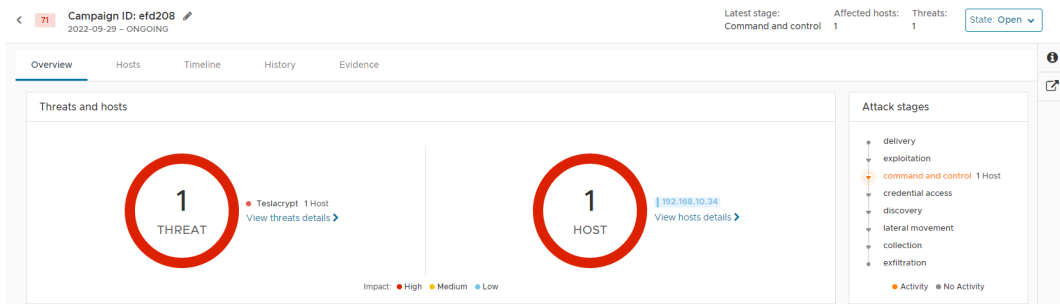




## 8-117 Campaign Overview: Active Threats and Attack Stages

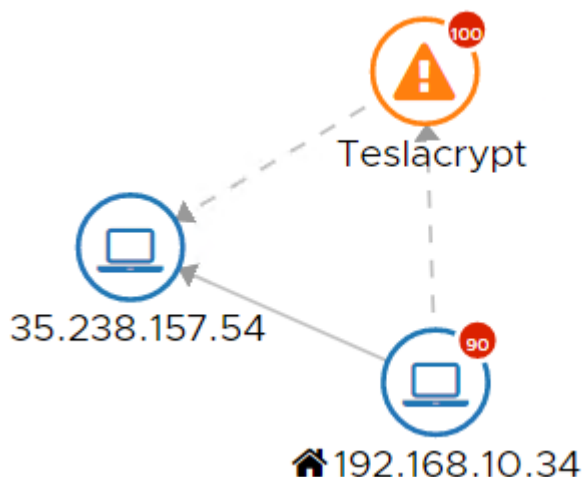
NSX Network Detection and Response provides a summary of malicious activity in the network by showing the affected hosts and the stages of the active threats.

In alignment with the MITRE ATT&CK framework, NSX Network Detection and Response classifies malicious activity by attack stage.



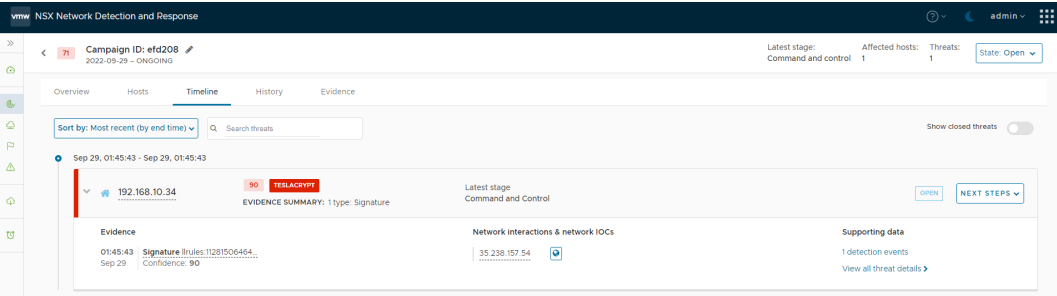
## 8-118 Campaign Blueprint

NSX Network Detection and Response includes a dynamic blueprint that shows how an attack enters and moves laterally across the network, including compromised hosts and external communications.



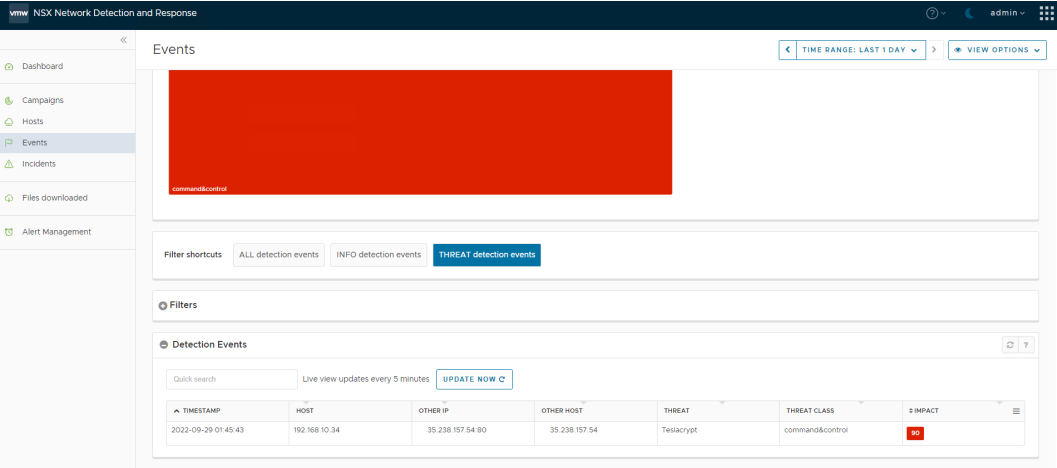
# 8-119 Campaign Timeline

NSX Network Detection and Response also provides a detailed chronology of each stage of an attack to assist with remediation.



# 8-120 Reviewing Events

You can review all events discovered in the environment by selecting **Events** in the NSX Network Detection and Response UI.



Depending on the severity of the event and other events occurring in the environment at the time, an event might be correlated into a campaign. Regardless of whether the event is part of the campaigning, it appears on the Events page in the NSX Network Detection and Response UI.

## 8-121 Lab 16: (Simulation) Using NSX Network Detection and Response to Detect Threats

Install and use NSX Network Detection and Response to detect and visualize advanced threats:

1. Install NSX Network Detection and Response
2. Validate the NSX Network Detection and Response Deployment from the CLI
3. Enable NSX Distributed IDS/IPS for a vSphere Cluster
4. Create an NSX Distributed IDS/IPS Profile
5. Configure NSX Distributed IDS/IPS Rules
6. Generate Malicious Traffic
7. Analyze Threat Detection Events and Campaigns

## 8-122 Review of Learner Objectives

- Describe NSX Network Detection and Response and its use cases
- Explain the architecture of NSX Network Detection and Response
- Activate NSX Network Detection and Response
- Describe the visualization capabilities of NSX Network Detection and Response

## 8-123 Key Points (1)

- NSX IDS/IPS uses real-time deep packet inspection to identify and prevent attempts at exploiting vulnerabilities in your applications.
- NSX Distributed IDS/IPS protects against malicious activity, including the exploits of known application-level vulnerabilities, application denial of service, lateral movement, and client-side and server-side exploits.
- You enable IDS/IPS at the Tier-1 gateway to protect the perimeter of your NSX environment.
- Behavior-based IDS/IPS helps to detect unusual traffic, malicious attacks, and security breaches in the network when compared to a baseline of normal traffic.
- NSX Application Platform is a container-based solution that is deployed on an existing Kubernetes cluster.
- NSX Application Platform must be deployed before using the NSX security features, such as NSX Malware Prevention, NSX Intelligence, NSX Network Detection and Response, and Metrics.
- NSX Malware Prevention detects and prevents malicious file transfers by combining signature-based detection of known malware with static and dynamic analyses of malware samples.

## 8-124 Key Points (2)

- East-west malware prevention protects the data center from the spread of internal malware and from malware that passes the network perimeter. It uses the Guest Introspection agents, installed on every guest VM, to extract files.
- North-south malware prevention detects known malicious files when they enter the perimeter on the NSX Edge gateway firewall. It uses the IDS/IPS engine of the NSX Edge node to extract files.
- NSX Intelligence is a native distributed analytics solution that provides visibility and dynamic security policy enforcement for NSX environments.
- The NSX Suspicious Traffic Detection feature analyses the data collected by NSX Intelligence and flags suspicious activities using detectors.
- NSX Network Detection and Response is an advanced threat prevention platform that provides complete network visibility, detection, and prevention of sophisticated threats.
- NSX Network Detection and Response capabilities are integrated with on-premises NSX deployments.

Questions?

## Module 9

# NSX Services

## 9-2 Importance

NSX provides several services that can help you address operational challenges in the virtual network architecture.

## 9-3 Module Lessons

1. Configuring NAT
2. Configuring DHCP and DNS Services
3. Configuring NSX Advanced Load Balancer
4. IPSec VPN
5. L2 VPN

## 9-4 Lesson 1: Configuring NAT

### 9-5 Learner Objectives

- Explain the role of network address translation (NAT)
- Distinguish between source and destination NAT
- Describe how reflexive NAT works
- Describe stateful active-active SNAT and DNAT operation
- Explain how NAT64 facilitates communication between IPv6 and IPv4 networks

# 9-6     About NAT

Network address translation (NAT) is a service that maps one IP address space to another. You can configure NAT on Tier-0 and Tier-1 gateways. NSX supports various NAT rule configurations, depending on the gateway type and the NSX Edge HA mode.

Supported NAT Rules	Gateway Type	NSX Edge HA Mode
SNAT / DNAT / NAT64	Tier-0 and Tier-1	Active-Standby
Reflexive NAT	Tier-0 only	Stateless Active-Active
Stateful Active-Active SNAT / DNAT	Tier-0 and Tier-1	Stateful Active-Active

Network address translation (NAT) was designed originally to conserve the public Internet address space. During the 1990s, Internet providers quickly depleted the available IPv4 address supply. NAT became the primary method for IPv4 address conservation. NAT performs one-to-one mapping (one public IP address is mapped to one private IP address) or one-to-many mapping (one public IP address is mapped to multiple private IP addresses).

You can create different NAT rules:

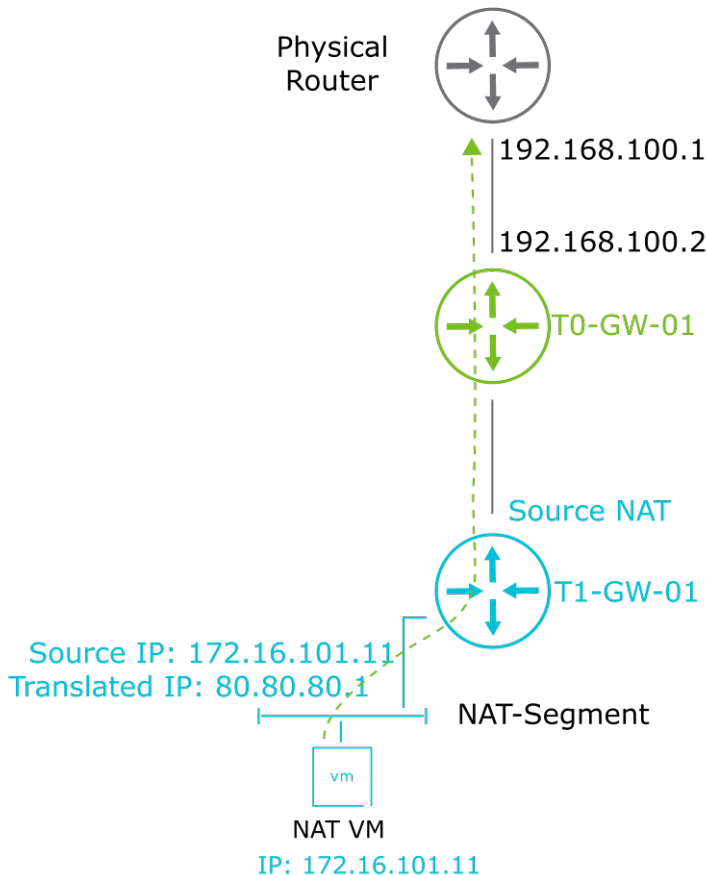
- Source NAT (SNAT) translates the source IP of the outbound packets to a known public IP address so that the application can communicate with the outside world without using its private IP address. SNAT also tracks the reply.
- Destination NAT (DNAT) enables access to internal private IP addresses from the outside world by translating the destination IP address when inbound communication is initiated. DNAT also manages the reply. For both SNAT and DNAT, users can apply NAT rules based on the 5-tuple match criteria.
- NAT64 is a mechanism for translating IPv6 packets into IPv4 packets.
- Reflexive NAT rules are stateless access control lists (ACLs) that must be defined in both directions. These rules do not track the connection. Reflexive NAT rules are applied when stateful NAT cannot be used.
- Introduced in NSX 4.0.1, stateful active-active SNAT/DNAT is achieved by using an external server IP hash to ensure symmetric northbound and southbound traffic through an edge by punting traffic between edge nodes.

## 9-7 About SNAT

The SNAT rule changes the source address in the IP header of a packet. The rule can also change the source port in the TCP or UDP headers.

In the diagram, as packets are received from the NAT VM, the T1-GW-01 Tier-1 gateway changes the source IP address of the packets from 172.16.101.11 to 80.80.80.1.

You can selectively bypass an existing SNAT rule for specific traffic by creating a No SNAT rule.



SNAT changes the source address in the IP header of a packet. It can also change the source port in the TCP/UDP headers.

The typical usage is to change a private (rfc1918) address into a public address for packets leaving your network. You can create a rule to either enable or disable the source NAT.

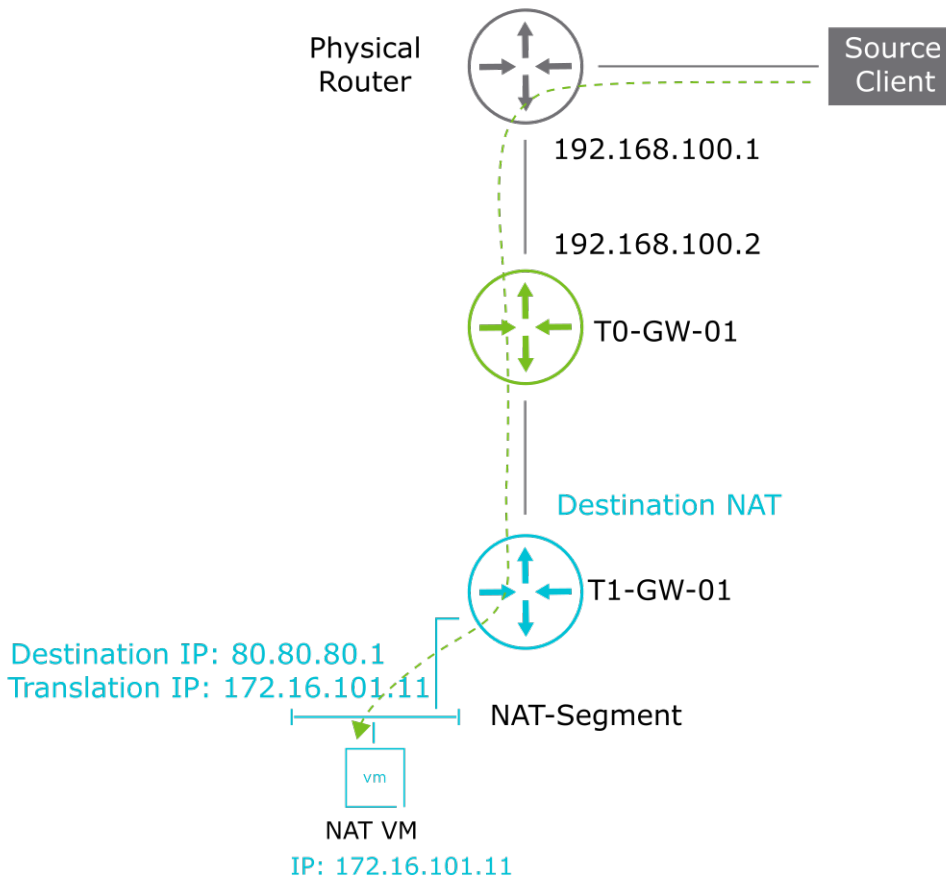


## 9-8 About DNAT

The DNAT rule changes the destination address in the IP header of a packet. It can also change the destination port in the TCP or UDP headers.

This rule is typically used to redirect incoming packets with a destination public IP address to a private IP address in the network.

You can selectively bypass an existing DNAT rule for specific traffic by creating a No DNAT rule.

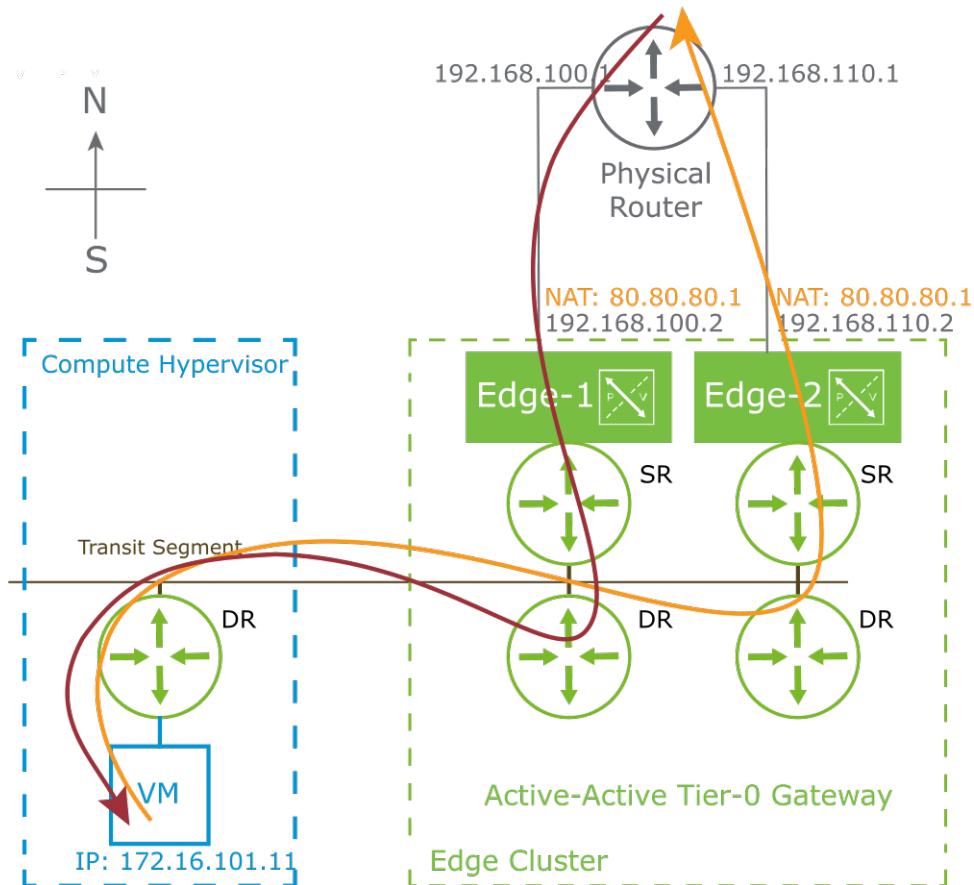


## 9-9 About Reflexive NAT

You can use the reflexive NAT rule when a Tier-0 gateway runs in stateless active-active mode and when stateful NAT might lead to issues because of asymmetric paths.

Reflexive NAT rules are stateless access control lists (ACLs) that must be defined in both directions. These rules do not track connections and are sometimes called stateless NAT.

In the diagram, because the same NAT is applied to the NSX Edge Edge-1 and the NSX Edge Edge-2, asymmetric flows are supported.



When Tier-0 is running in a stateless active-active mode, you cannot configure stateful NAT where asymmetrical paths might cause issues. For active-active routers, you can use reflexive NAT, which is also called stateless NAT.

For reflexive NAT, you can configure a single source address to be translated or a range of addresses. If you configure a range of source addresses, you must also configure a range of translated addresses. The size of the two ranges must be the same. The address translation is deterministic. The first address in the source address range is translated to the first address in the translated address range. The second address in the source range is translated to the second address in the translated range, and so on.

In the diagram, the source VM (172.16.101.11) on the internal network sends a packet to an external client (x.x.x.x) on the Internet. The packet is routed to the Tier-0 gateway hosted on NSX Edge Edge-2, which creates a reflexive NAT entry with source IP 172.16.101.11 and translated IP 80.80.80.1. When the return traffic arrives on NSX Edge Edge-1 (with the destination 80.80.80.1), the same reflexive NAT entry is used to translate 80.80.80.1 to 172.16.101.11. Because the same NAT is applied to NSX Edge Edge-1 and NSX Edge Edge-2, asymmetric flows are supported.

## 9-10 Configuring SNAT and DNAT

SNAT and DNAT are configured on the Tier-1 or Tier-0 gateway in the following use cases:

- You typically use SNAT to change a private address into a public address for packets leaving your network.
- You typically use DNAT to redirect incoming packets with a destination public address or port to a private IP address or port in your network.

NAT

Gateway

T1-GW-02-NAT | Tier-1

#Total NAT Rules

View

NAT

ADD NAT RULE

COLLAPSE ALL

Filter by Name, Path and more

Name	Action	Match		Translated IP   Port	Apply To	Enabled	Status
		Source IP	Destination IP   Port				
DNAT-Rule	DNAT	Any	80.80.80.1   Port: Not Set	172.16.101.11   Port: Not Set   Service: Not Set	0	Yes	Success
Logging	No			Priority	0	DNAT Rule	
Firewall	Match Internal Address			Apply to Policy Based VPN	Bypass		
Description	Not Set			Tags	0		
SNAT-Rule	SNAT	172.16.101.11	Any   Port: Not Set	80.80.80.1   Port: Not Set   Service: Not Set	0	Yes	Success
Logging	No			Priority	0	SNAT Rule	
Firewall	Match Internal Address						
Description	Not Set			Tags	0		

To configure SNAT and DNAT, you provide values for the following options:

- **Name:** Provide a name for the NAT rule.
- **Action:** Specify the action of the NAT rule if a match occurs.
- **Source IP:** Specify a source IP address or an IP address range in CIDR format. If you leave this text box blank, the NAT rule applies to all sources outside the local subnet.

- **Destination IP:** Specify a destination IP address or an IP address range in CIDR format.
- **Destination Port:** Specify a destination port.
- **Translated IP:** The new IP address as the result of NAT.
- **Service:** Select a single service entry on which the NAT rule is applied.
- **Applied To:** Select objects that this NAT rule applies to. The available objects are gateways, interfaces, labels, service instance endpoints, and virtual endpoints.
- **Enabled:** To enable or disable the NAT rule.
- (Optional) **Logging:** Used in analysis and troubleshooting. The default is no logging.
- **Priority:** A lower value means a higher priority. The default is 0.
- **Firewall** includes the following options:
  - **Match External Address:** To match the firewall rule with the external address of the NAT rule
  - **Match Internal Address:** To match the firewall rule with the internal address of the NAT rule
  - **Bypass:** To skip the firewall stage
- (Optional) **Tags:** Specify to group NSX objects.

## 9-11 Configuring Reflexive NAT

When a Tier-0 gateway runs in stateless active-active mode, you can use reflexive NAT:

- The address translation is sequential, for example, the first address in the source range is translated to the first address in the translated range, and so on.
- The two ranges (source range and translated range) must be of equal size.

The screenshot shows the NAT configuration page for a gateway named 'BGP-TO-GW-011 Tier-0'. A table lists NAT rules, with 'Web01-ReflexiveNAT' highlighted. Below the table, configuration options for the selected rule are shown.

Name	Action	Source IP	Match	Destination IP   Port	Translated IP   Port	Apply To	Enabled	Status
Web01-ReflexiveNAT	Reflexive	172.16.10.11	Enter Destination IP IPv4 Address or CIDR or IP address list	80.80.80.1	Set	Yes		

Logging: ☐ No

Priority: 0

Note: A lower value means a higher priority. The default is 0.

Firewall: Match Internal Address

Description:

Tags:  Tag  Scope

Max 30 allowed. Click (+) to add.

Buttons: SAVE, CANCEL

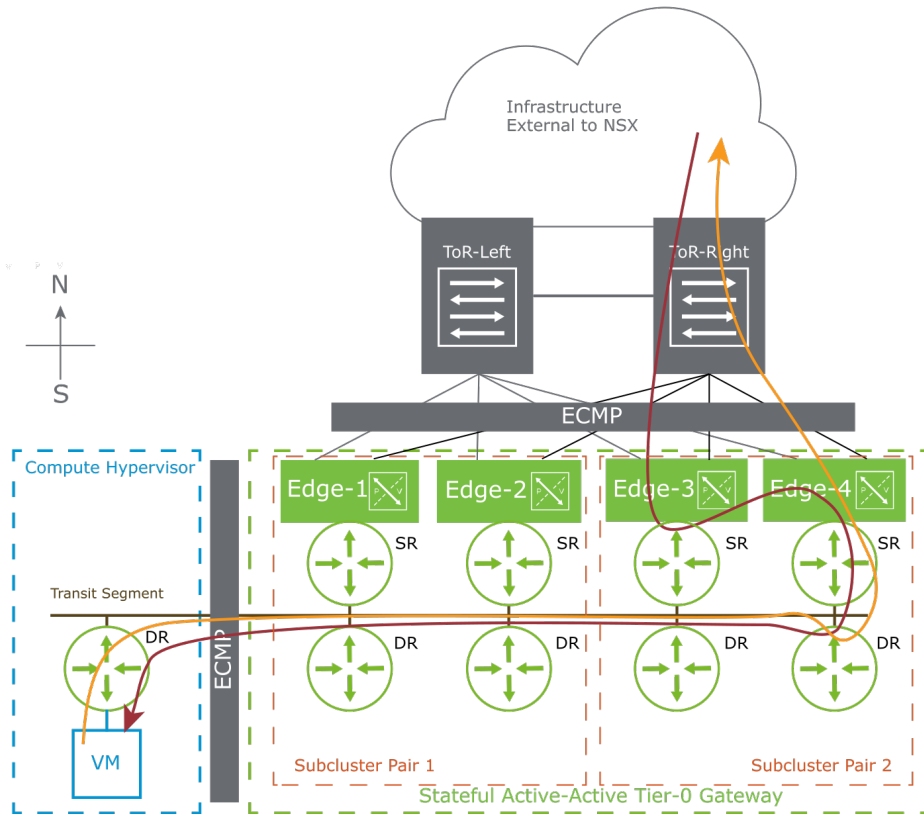
To configure reflexive NAT, you provide values for the following options:

- **Name:** Provide a name for the NAT rule.
- **Action:** Specify the action, Reflexive, if a match occurs.
- **Source IP:** Specify a source IP address or an IP address range in CIDR format. If you leave this text box blank, the NAT rule applies to all sources outside the local subnet.
- **Destination IP:** Specify a destination IP address or an IP address range in CIDR format.
- **Destination Port:** Specify a destination port.
- **Translated IP:** The new IP address as the result of NAT.
- **Service:** Select a single service entry on which the NAT rule is applied.
- **Applied To:** Select objects that this NAT rule applies to. The available objects are gateways, interfaces, labels, service instance endpoints, and virtual endpoints.
- **Enabled:** To enable or disable the NAT rule.
- (Optional) **Logging:** Used in analysis and troubleshooting. The default is no logging.
- **Priority:** A lower value means a higher priority. The default is 0.

- **Firewall** includes the following options:
  - **Match External Address:** To match the firewall rule with the external address of the NAT rule
  - **Match Internal Address:** To match the firewall rule with the internal address of the NAT rule
  - **Bypass:** To skip the firewall stage
- (Optional) **Tags:** Specify to group NSX objects.

## 9-12 Stateful Active-Active Services

NSX version 4.0.1 introduces a new architecture that supports stateful active-active services. This architecture includes SNAT and DNAT. This architecture supports stateful active-active services by pinning specific flows to an individual edge.



Northbound and southbound traffic path selections are enforced by a common ECMP mechanism, which is a hash of the external server IP.

In the diagram, by enforcing a common ECMP hash based on the external server IP, with the ability to punt traffic between edges, the stateful session is maintained with bidirectional traffic through Edge-4.

Northbound path selection:

- The compute hypervisor has 4-way ECMP to the edge SRs.
- The compute hypervisor performs a 5-tuple hash, based on protocol number, source address, destination address, source port, and destination port.
- In this example, Edge-4 is selected as the northbound path.

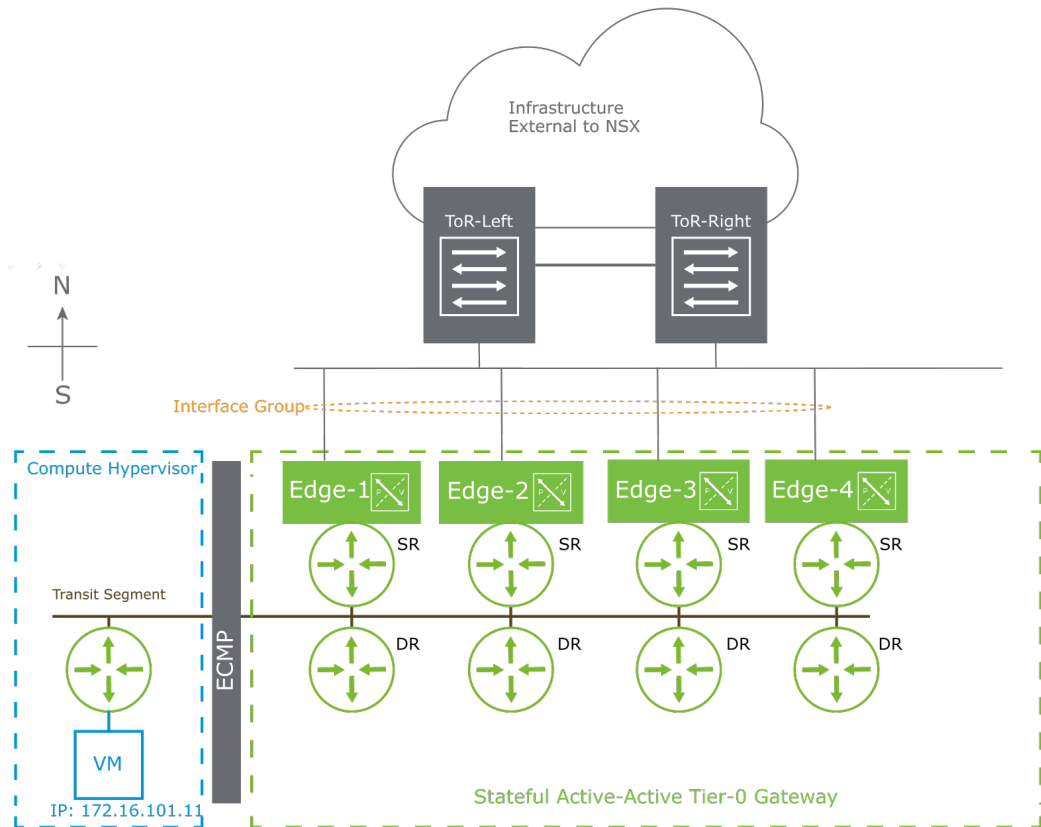
Southbound path selection:

- Both Tor-Left and Tor-Right have 4-way ECMP to the Edge SRs.
- In this example, Tor-Right has performed a hardware vendor hash, selecting Edge-3.
- An IP hash is performed, based on the external server source IP, and traffic is punted from Edge-3 to Edge-4.



## 9-13 Stateful Active-Active Interface Group

Stateful active-active introduces the requirement for an Interface Group to which stateful services, such as NAT, are applied.

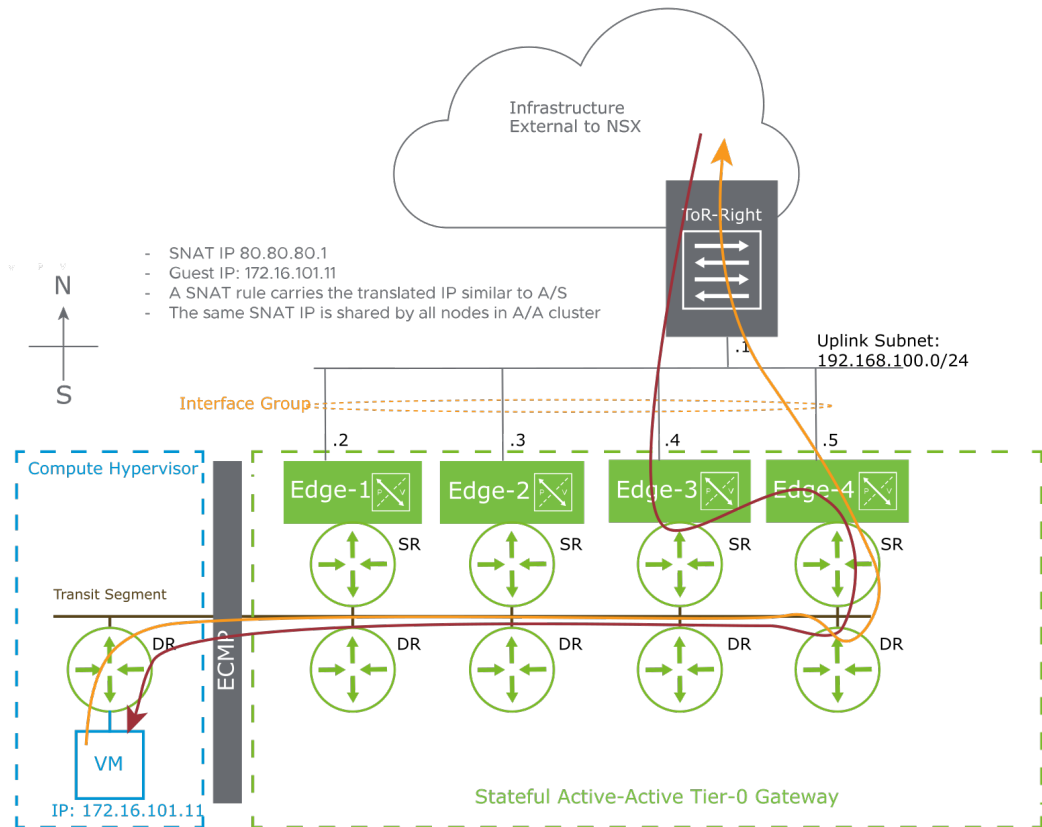


The stateful active-active interface group has the following requirements:

- The Interface Group has exactly one interface from every edge node in the edge cluster.
- A separate Interface Group is required for each uplink interface on an edge.
- For Edges with two uplinks, two Interface Groups are required
- In the scenario, each edge has one uplink interface, and one interface group is required.

## 9-14 Stateful Active-Active SNAT

Stateful active-active SNAT is similar to the active-standby SNAT, where an SNAT rule carries the translated IP address and all nodes share the same SNAT IP in the A/A cluster.



Symmetric traffic path selection is achieved by enforcing a common ECMP hash based on the external server target IP.

The SNAT rule changes the source address in the IP header of a packet. In the example, the SNAT session is pinned to Edge-4 to consistently translate SNAT 172.16.101.11 traffic to 80.80.80.1.

## 9-15 Stateful Active-Active Configuration

On a new NSX gateway, enable Stateful Active-Active using the Stateful toggle, when the HA mode is set to Active-Active.

The screenshot displays the NSX Tier-0 Gateway configuration interface. At the top, the title is "Tier-0 Gateways". Below it, there's a table with columns: Name, HA Mode, Linked Tier-1 Gateways, Linked Segments, Status, and Alarms. The first row shows a gateway named "TO-GW-01" with HA Mode set to "Active Active". A blue callout box points to the "Stateful" toggle switch, which is currently turned "On", with the text "Stateful toggle is enabled".

Below the table, the configuration details for "TO-GW-01" are shown. The "Edge Cluster" is set to "Edge-Cluster-01". There are sections for "DHCP Config", "Additional Settings", and "Route Distinguisher for VRF Gateways". A "Description" field is present. A "NOTE" states: "Before further configurations can be done, fill out mandatory fields (\*) above and click Save." Below this, there are expandable sections for "INTERFACES", "ROUTING", "BGP", "OSPF", "ROUTE RE-DISTRIBUTION", and "MULTICAST". A "SAVE" button is at the bottom left.

A blue callout box points to a warning message: "Warning message that HA mode for this Tier-0 Gateway cannot be modified after Stateful has been enabled". To the right, a "Confirm" dialog box is open, asking: "Once you turn on stateful services and save the configuration, you cannot modify the HA mode for this Tier-0 Gateway. Do you want to continue?". It has "NO" and "YES" buttons.

The feature does not support converting from a stateless to a stateful Active-Active gateway configuration. A new gateway must be deployed.

After you enable the gateway stateful services and save the configuration, you cannot modify the HA mode for the gateway.

# 9-16    Configuring Interface Groups

From the gateway configuration, interfaces and interface groups, create an external interface group to include all gateway uplink interfaces.

Set Interface Groups

Tier-0 Gateway

T0-GW-01

#Interface Groups

You can only create an Interface Group for External and Service interface types. Ensure that all External/Service interfaces are part of an Interface Group, and each interface is only part of one group.

ADD INTERFACE GROUP

Interface Group Name

COLLAPSE ALL

Filter by Name, Path and more

Name	Type	Interfaces	Status
T0-GW-01-External-Interface-Group-01	External	T0-GW-01-Uplink-01 T0-GW-01-Uplink-02	

IP Address Pools

Select IP Address Pools

Description

Description

Tags

Tag Scope

Max 30 allowed. Click (+) to add.

SAVE

CANCEL

All Tier-0 uplink interfaces are added to Interface Group

REFRESH

No Interface Groups

CLOSE

In the example, the Tier-0 Gateway has two uplink interfaces. You must add both the interfaces to the interface group.

## 9-17 Configuring Stateful SNAT and DNAT

Stateful active-active SNAT and DNAT configuration are similar to the active-standby SNAT and DNAT configuration, except that the NAT rule is applied to the interface group.

The screenshot displays the NAT configuration page for Gateway 'TY-QW-02-NAT-Tier1'. It shows two NAT rules: a DNAT rule and a SNAT rule. Both rules have 'Apply To' set to '1'. Two orange callout boxes point to these 'Apply To' fields with the text 'Apply To is set to the Interface Group'.

The DNAT rule configuration is as follows:

Name	Action	Match	Translated IP / Port	Apply To	Enabled	Status
DNAT Rule	DNAT	Any	172.16.101.1 (Port: Not Set)	1	Yes	Success

The SNAT rule configuration is as follows:

Name	Action	Match	Translated IP / Port	Apply To	Enabled	Status
SNAT Rule	SNAT	172.16.101.1	Any (Port: Not Set)	1	Yes	Success

The 'Applied To' modal for the DNAT rule shows the following configuration:

Name	Type	Object Details
RGW-User-1	To interface	View Details
RGW-User-2	To interface	View Details
<b>TY-QW-02-External-Interface-Group-01</b>	<b>To interface Group</b>	<b>Interface Group</b>

The modal also includes a 'Show Only Selected' checkbox and 'CANCEL' and 'APPLY' buttons.

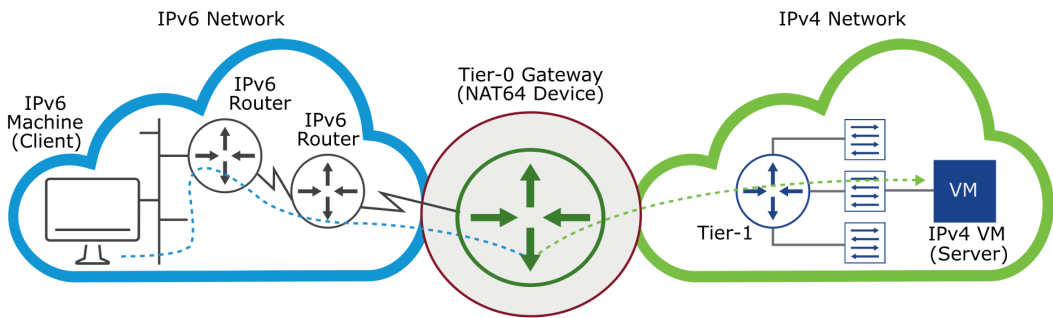
Stateful active-active SNAT and DNAT configuration are similar to the active-standby SNAT and DNAT configuration, except for the following parameter:

- **Applied To:** Select the interface group to which this NAT rule applies.

## 9-18 About NAT64

NAT64 is a mechanism for translating IPv6 packets into IPv4 packets:

- NAT64 allows IPv6-only clients to communicate with IPv4 servers.
- Changes are not needed in the IPv6 or IPv4 nodes.
- NAT64 is supported on Tier-0 and Tier-1 gateways.
- NAT64 is stateful and requires the Tier-0 gateway to be deployed in active-standby mode.
- NAT64 requires the Tier-1 gateway to be configured with an active-standby edge cluster.



The NAT64 mechanism enables IPV6 to IPV4 connectivity. NAT64 is based on the RFC 6146 and RFC 6145 standards.

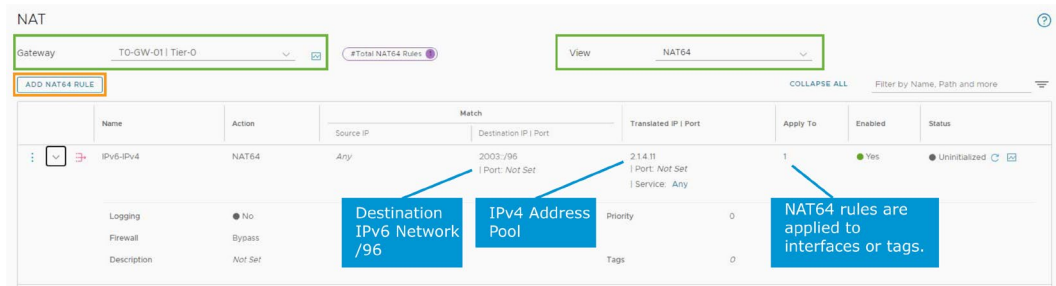
NAT64 allows an IPv6-only client to initiate communications to an IPv4-only server. IPv6 must initiate the traffic.

NAT64 translates IPv6 packets to IPv4 packets and forwards them to the IPv4 network. This functionality is designed so that changes are not required to either IPv6 or IPv4 nodes.

## 9-19 Configuring NAT64 Rules

To configure NAT64 rules:

1. Navigate to **Networking > Network Services > NAT**.
2. Select **NAT64** from the **View** drop-down menu.
3. Specify the Tier-0 or Tier-1 gateway where you want to create the rule and click **ADD NAT64 RULE**.



In the example, NAT64 rules are created on TO-GW-01.

You configure the following parameters in a NAT64 rule:

- **Name:** Name for the NAT64 rule.
- **Action:** The only supported action is NAT64, which translates between IPv6 and IPv4 addresses.
- (Optional) **Source:** IPv6 or IPv6 address range in CIDR format.
- **Destination:** IPv6 or IPv6 address range in CIDR format. The prefix must be /96 because the destination IPv4 IP is embedded as the last 4 bytes in the IPv6 address.
- **Translated:** This address is the IPv4 address or address pool for the source IPv6 address. The IPv4 address(es) must have a route enabled at the Tier-1 gateway if this is configured on the Tier-0 gateway or the return path is unknown.
- **Applied To:** NAT64 rules can only be applied to uplink interfaces or tags.
- **Enabled:** To enable or disable the NAT64 rule.
- (Optional) **Logging:** Used in analysis and troubleshooting. The default is no logging.
- **Priority:** A lower value means a higher priority. The default is 0.

- **Firewall** includes the following options:
  - **Match External Address:** To match the firewall rule with the external address of the NAT rule
  - **Match Internal Address:** To match the firewall rule with the internal address of the NAT rule
  - **Bypass:** To skip the firewall stage
- (Optional) **Tags:** Specify to group NSX objects.

## 9-20 Lab 17: Configuring Network Address Translation

Configure source and destination network address translation rules on the Tier-1 gateway:

1. Prepare for the Lab
2. Create a Tier-1 Gateway for Network Address Translation
3. Create a Segment
4. Attach a VM to NAT-Segment
5. Configure NAT
6. Configure NAT Route Redistribution
7. Verify the IP Connectivity

## 9-21 Review of Learner Objectives

- Explain the role of network address translation (NAT)
- Distinguish between source and destination NAT
- Describe how reflexive NAT works
- Describe stateful active-active SNAT and DNAT operation
- Explain how NAT64 facilitates communication between IPv6 and IPv4 networks



## 9-22 Lesson 2: Configuring DHCP and DNS Services

### 9-23 Learner Objectives

- Explain how DHCP and DHCP Relay are used for IP address allocation
- Configure DHCP services in NSX
- Describe how to use a DNS forwarder service
- Configure DNS forwarder services in NSX

## 9-24 About DHCP

DHCP allows clients to automatically obtain network configuration settings, such as IP addresses, subnet masks, default gateways, and DNS configuration, from a DHCP server.

### DHCP Discover: "Locate all available DHCP servers"



**DHCP Offer: "DHCP Server IP is 172.16.0.1,  
Proposed IP address 172.16.0.100/24."**

The DHCP protocol eliminates the need for individually configuring network devices manually.

The operation can be summarized as follows:

- The DHCP client broadcasts a DHCP Discover message to locate all available DHCP servers on the subnet.
- A DHCP server broadcasts a DHCP Offer message, informing the client that it is available, proposing a client IP address, subnet mask, default gateway IP address, DNS IP address, IP lease time, and a DHCP server IP address.
- The DHCP client broadcasts a DHCP Request message to the server, requesting the proposed IP network configuration data.
- The DHCP server broadcasts an acknowledgment.
- The DHCP client configures its network interface with the proposed IP network configuration.

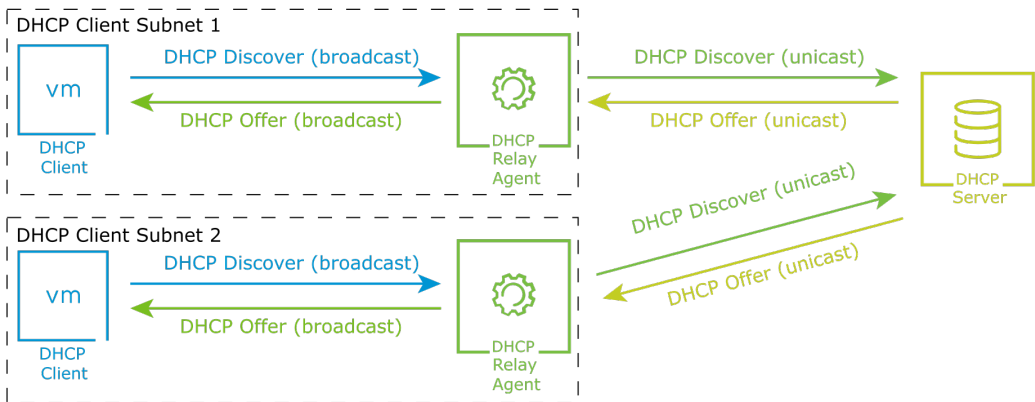
The IP allocation process is based on broadcast traffic.

A DHCP server must be available to host a range of addresses for each client subnet.

# 9-25 About DHCP Relay

A DHCP relay agent offers a more centralized approach to providing DHCP services across multiple subnets.

A DHCP relay agent forwards requests and replies between a DHCP server and a DHCP client, offering the flexibility of placing the DHCP server on a remote network.



From the DHCP client perspective, the IP allocation process remains broadcast based.

The DHCP relay agent converts the local DHCP broadcast message into a unicast message and sends the unicast message to the DHCP server.

A DHCP relay agent is required for each DHCP client subnet.

By using DHCP relay agents, a DHCP server can service multiple DHCP client subnets.

# 9-26 DHCP in NSX

NSX supports three types of DHCP services.

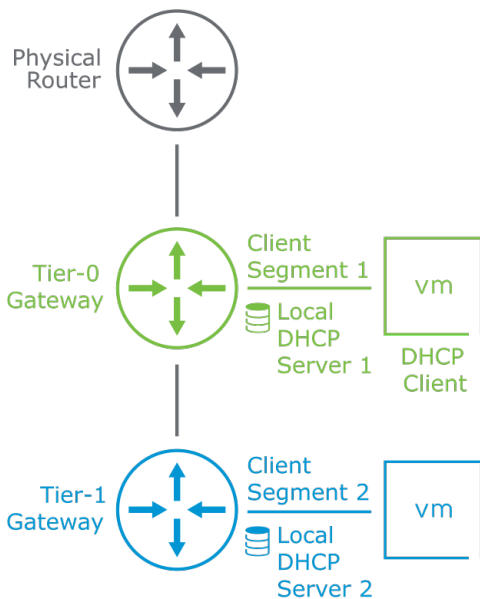
DHCP Service Type	Description
DHCP Local Server	A DHCP server that is centrally managed by NSX. This server is local to a single segment.
DHCP Relay	A DHCP relay agent is local to a single segment that relays client requests to an external DHCP server.
Gateway DHCP	A DHCP server that is centrally managed by NSX. This server is available to all segments that are connected to the gateway.

## 9-27 DHCP Local Server

DHCP Local Server is a DHCP service managed by NSX that is local to the segment and not available to the other segments in the network.

- It provides a dynamic IP assignment service only to the VMs that are attached to the segment.
- It runs as a service (service router) in the edge nodes of an NSX Edge cluster.
- The IP address of a local DHCP server must be in the subnet that is configured on the segment.
- It supports Tier-0 and Tier-1 gateways and segments not connected to a gateway.
- It can service VLAN-backed or overlay-backed segments.

DHCP Local Server Topology



In this configuration, the DHCP requests are managed in the NSX environment without relying on an external DHCP server.

DHCP Local Server runs as a service (service router) in the edge nodes of an NSX Edge cluster.

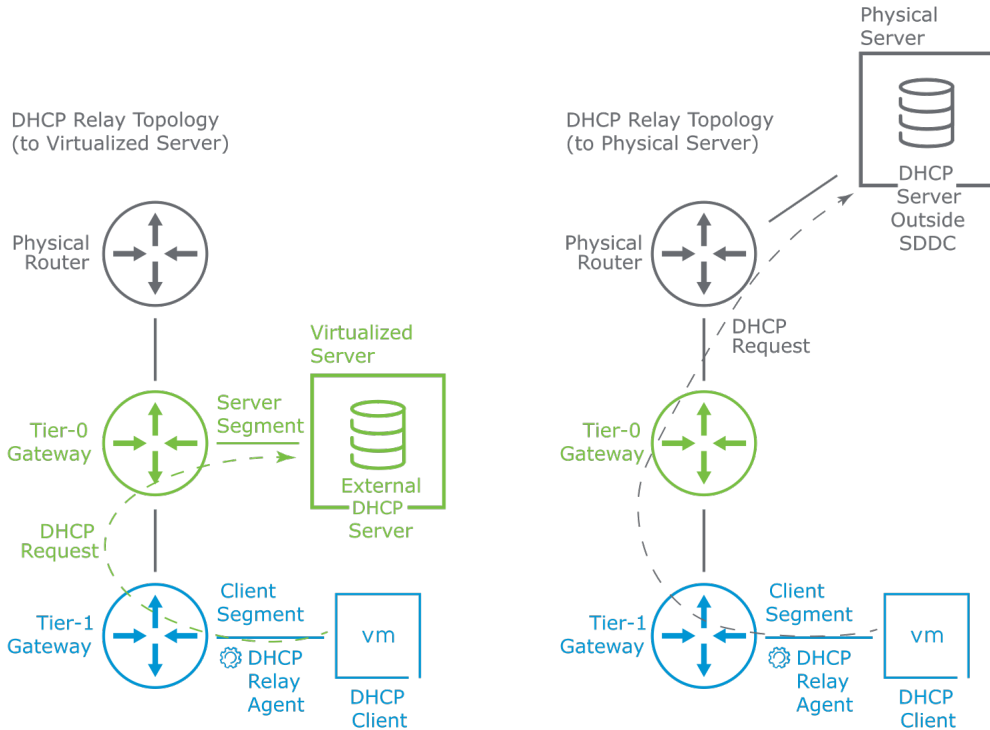
For standalone segments, DHCP Local Server is selected by default.

## 9-28 DHCP Relay

A DHCP relay agent is local to a single segment and relays client requests to an external DHCP server.

The DHCP servers can be located inside or outside the SDDC.

The DHCP client segment must be connected to either a Tier-0 or Tier-1 gateway.

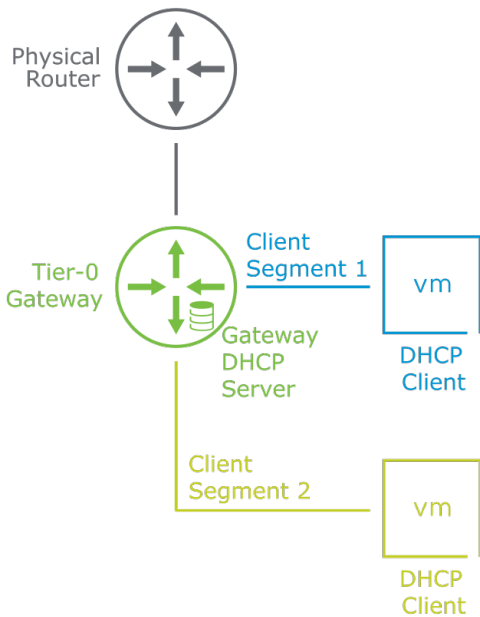


# 9-29 Gateway DHCP

Gateway DHCP is a DHCP server that is centrally managed by NSX. This server is available to all segments that are connected to the gateway.

By default, segments that are connected to a Tier-0 or Tier-1 gateway use Gateway DHCP.

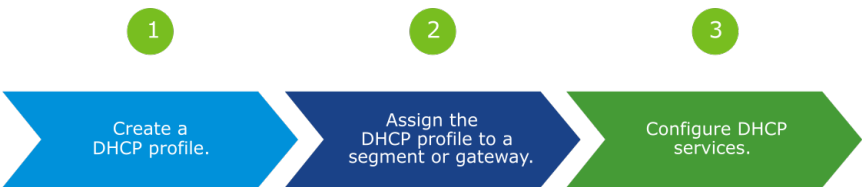
Gateway DHCP Server Topology



The IP address of a Gateway DHCP server can be different from the subnets that are configured in the segments.

Individual segments connected to a gateway configured for Gateway DHCP can be selectively configured to use different DHCP types, Local DHCP Server, or DHCP Relay.

# 9-30 DHCP Workflow



## 9-31 Creating a DHCP Profile

To create a DHCP Profile, click **Networking > Networking Profiles > DHCP > ADD DHCP PROFILE** and select either **DHCP Relay** or **DHCP Server** as the required profile type.

The image displays two screenshots of the 'Networking Profiles' configuration interface, specifically the 'ADD DHCP PROFILE' section under the 'DHCP' tab.

**Option 1: Create a DHCP profile of type DHCP Relay.**

The top screenshot shows the configuration for a DHCP Relay profile. The 'Name' field is 'DHCP-Relay-Profile', the 'Profile Type' is 'DHCP Relay', and the 'Server IP Address' field is '172.20.10.10'. The 'Where Used' field is '0'. The 'Description' field is empty. The 'Tags' field is empty. The 'SAVE' button is highlighted.

**Option 2: Create a DHCP profile of type DHCP Server.**

The bottom screenshot shows the configuration for a DHCP Server profile. The 'Name' field is 'DHCP-Local-Server-Profile', the 'Profile Type' is 'DHCP Server', and the 'Server IP Address' field is 'Enter CIDR'. The 'Where Used' field is '0'. The 'Edge Cluster' field is 'Edge-Cluster-01'. The 'Auto Allocate Edges' field is 'Yes'. The 'Standby Relocation' field is 'No'. The 'Description' field is empty. The 'Tags' field is empty. The 'SAVE' button is highlighted.

To create a DHCP Profile, you provide values for the following options:

- **Name:** You use this name to identify the DHCP profile.
- **Profile Type:** Select either **DHCP Relay** or **DHCP Server**.
- **Server IP Address** is based on DHCP type
- (Optional) **Tags:** Add tags to label static bindings so that you can quickly search or filter bindings, troubleshoot and trace binding-related issues, or do other tasks.

For DHCP Server profiles, you provide values for these additional options:

- **Edge Cluster:** Select an NSX Edge cluster from the drop-down menu.
- **Auto Allocate Edges:** Yes (default) The first edge node becomes the active edge for DHCP services, and the second edge node becomes the standby edge for DHCP services.
- **Standby Relocation:** No (default) If the edge node where the active or standby DHCP server is running fails, a new standby DHCP server is created on another edge node to maintain high availability.

## 9-32 Assigning the DHCP Profile to a Segment

To assign the DHCP profile to a segment, click **Networking > Segments > Edit an existing segment > SET DHCP CONFIG** and select a configured profile.

The screenshot shows the NSX Segments configuration interface. The main table lists segments with columns for Name, Connected Gateway, Transport Zone, Subnets, Ports / Interfaces, Status, and Alarms. A segment named 'App-Segment' is highlighted. Below the table, a 'SET DHCP CONFIG' button is visible. A modal dialog box titled 'Set DHCP Config' is open, showing the configuration for the selected segment. The dialog includes fields for 'DHCP Type' (set to 'DHCP Relay') and 'DHCP Profile' (set to 'DHCP-Relay-Profile'). A note at the bottom states: 'IPv4 Server & IPv6 server settings are not required here for DHCP Relay'.

Name	Connected Gateway	Transport Zone	Subnets	Ports / Interfaces	Status	Alarms
App-Segment	T1-GW-01   Tier-1	PROD-Overlay-TZ	172.16.20.1/24 CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. fc7e:f206:db42::1/48	1		

SET DHCP CONFIG

Set DHCP Config

Segment: App-Segment

DHCP Type: DHCP Relay

DHCP Profile: DHCP-Relay-Profile

IPv4 Server & IPv6 server settings are not required here for DHCP Relay

To assign the DHCP profile to a segment, you provide values for the following options:

- **DHCP Type:** Select either **DHCP Relay** or **DHCP Server**.
- **DHCP Profile:** Select the configured DHCP profile.



## 9-33 Assigning the DHCP Profile to a Gateway

To assign the DHCP Profile to a gateway, click **Networking > Tier-0 or Tier-1 Gateway**, edit the gateway, set the DHCP Config, and select a configured profile.

The screenshot shows the 'Tier-1 Gateways' configuration page. A table lists gateway configurations. The first entry, 'T1-GW-01', is selected. To its right, the 'DHCP Config' tab is highlighted with an orange box, and a 'Set' button is visible. An orange-bordered dialog box titled 'Set DHCP Configuration' is open over the 'Set' button. The dialog contains the following fields:

- Choose either DHCP Server or No Dynamic IP Allocation.
- Type: A dropdown menu with 'DHCP Server' selected.
- DHCP Server Profile: A dropdown menu with 'DHCP-Local-Server-Profile' selected.
- Lease Time: 86400 seconds.
- Server Address: 100.96.0.1/30.
- Buttons: 'CANCEL' and 'SAVE'.

Name	HA Mode	Linked Tier-0 Gateway	#Linked Segments	Status	Alarms
T1-GW-01	Active Standby	T0-GW-01			

Edge Cluster\*: Edge-Cluster-01

Auto Allocate Edges: ☒ Yes

Edges Pool Allocation Size: ROUTING

Description:

Fail Over: Non Preemptive

Standby Relocation: ☐ No

DHCP Config: Set

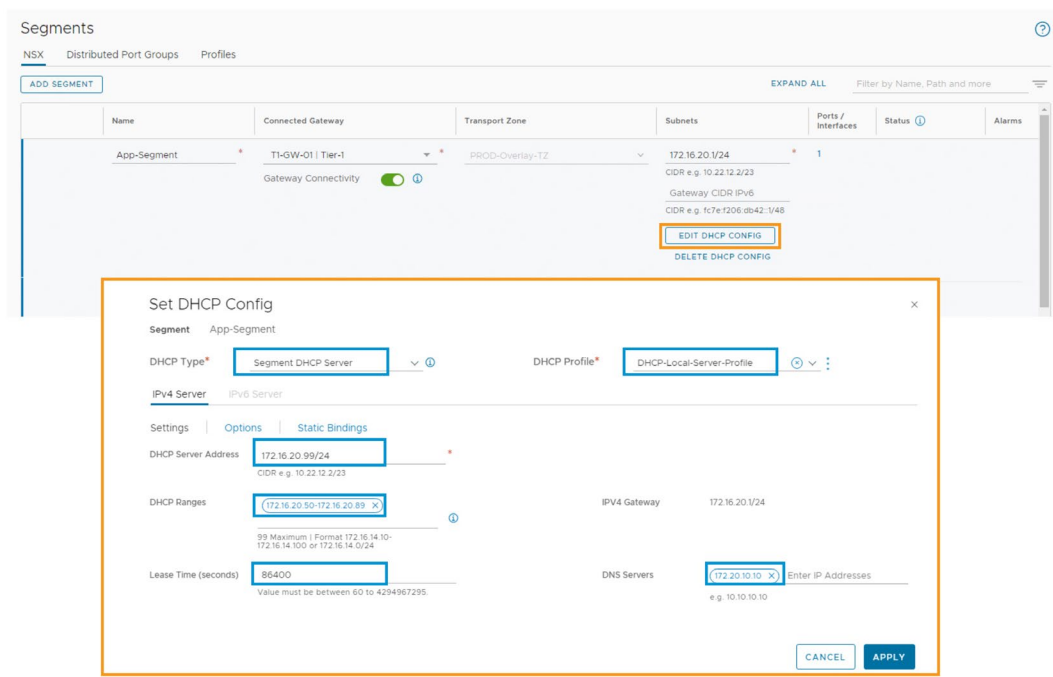
Tags:

To assign the DHCP profile to a gateway, you provide values for the following options:

- **Type:** Select either **DHCP Relay** or **DHCP Server**.
- **DHCP Profile:** Select the configured DHCP profile.

# 9-34 Configuring DHCP Services

To configure DHCP services, click **Networking > Segments > Edit an existing segment > EDIT DHCP CONFIG.**



To configure DHCP services, you provide values for the following options:

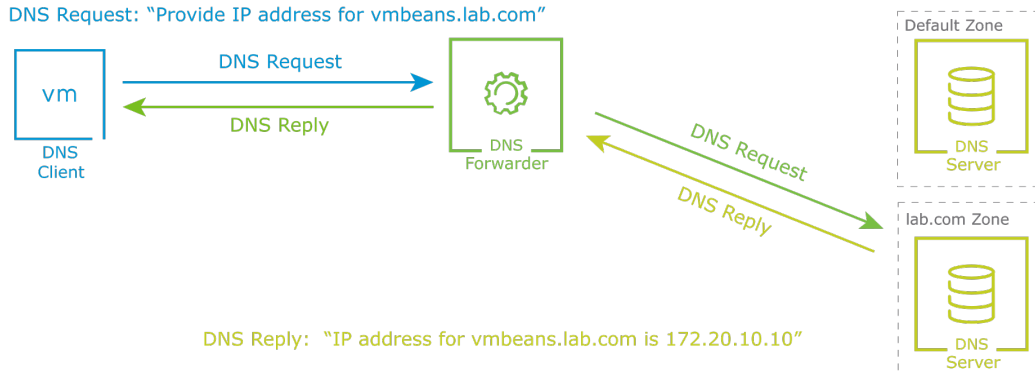
- **DHCP Type:** Select the existing **DHCP Relay** or **DHCP Server** by name.
- **DHCP Profile:** Select the configured DHCP profile.
- **DHCP Server Address:** If you are configuring a DHCP local server, server IP address is required.
- **DHCP Ranges:** Optionally enter the DHCP IP pool range.
- **Lease Time:** Optionally enter the amount of time in seconds for which the IP address is bound to the DHCP client.
- **DNS Servers:** Optionally enter the IP address of the domain name server (DNS) to use for name resolution. A maximum of two DNS servers are permitted.

## 9-35 About DNS Services

A DNS server translates domain names to IP addresses.

A DNS zone is a distinct portion of the domain name space in DNS.

Depending on the DNS zone, a DNS forwarder can forward DNS queries to specific DNS servers.



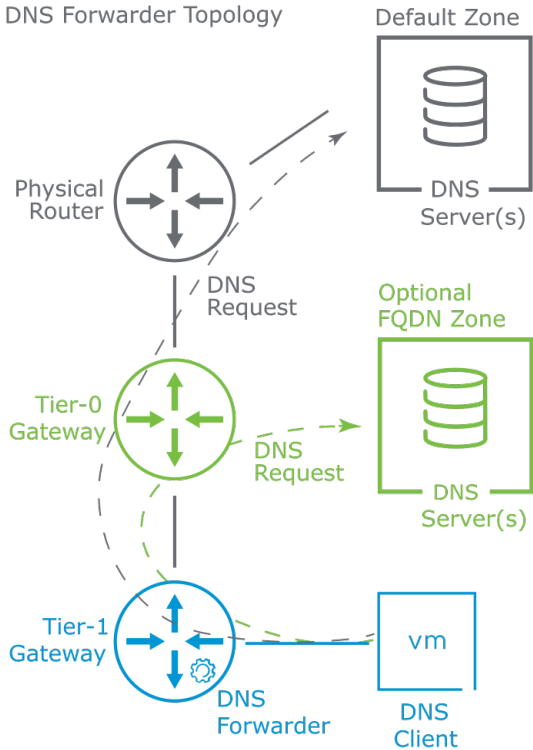
The resource to resolve, `vmbeans.lab.com`, is in the `lab.com` DNS namespace. The DNS forwarder can be configured to forward DNS queries to the `lab.com` DNS zone servers.

## 9-36 About DNS Forwarder

In NSX, the DNS client requests can be forwarded to the external DNS server by configuring a DNS forwarder in Tier-0 or Tier-1 gateways. The DNS forwarder provides the following functions:

- Forwards DNS requests from clients to upstream DNS servers
- Can optionally forward DNS requests to FQDN zones
- Caches the responses received from the upstream servers, reducing system load and improving performance

DNS Forwarder Topology



## 9-37 DNS Workflow



## 9-38 Creating DNS Zones

A default DNS zone is required. Optionally, you can configure one or more FQDN DNS zones. To create DNS zones, click **Networking > DNS > DNS Zones > ADD DNS ZONE**.

The image displays two screenshots of the 'ADD DNS ZONE' configuration interface. The top screenshot is for a 'Default Zone' and the bottom is for an 'FQDN Zone'.

**Default Zone Configuration:**

- Name:** Default-Zone
- Domain:** Any
- DNS Servers:** 172.20.10.10
- Source IP:** Enter Source IP
- Description:** (Empty text box)
- Tags:** (Empty tag input)
- Buttons:** SAVE, CANCEL

**FQDN Zone Configuration:**

- Name:** Lab-Zone
- Domain:** lab.com
- DNS Servers:** 172.20.10.20
- Source IP:** Enter Source IP
- Description:** (Empty text box)
- Tags:** (Empty tag input)
- Buttons:** SAVE, CANCEL

To create DNS zones, you provide values for the following options:

- **Name:** You use this name to identify the DNS zone.
- **Domain:** Select **Any** for the default zone. Select an FQDN for the domain for an FQDN zone.
- **DNS Servers:** Enter the IP address of up to three remote DNS servers for this DNS zone.
- (Optional) **Source IP:** You must specify a source IP if the DNS forwarder service listener IP is an internal address that is not reachable from the external upstream DNS server.
- (Optional) **Tags:** Specify to group NSX objects.

When you configure a DNS zone, you can specify a source IP for a DNS forwarder to use when forwarding DNS queries to an upstream DNS server. If you do not specify a source IP, the DNS query packet source IP will be the DNS forwarder's listener IP.

## 9-39 Creating DNS Forwarder Services

To create a DNS forwarding services, click **Networking** > **DNS** > **DNS Services** > **ADD DNS SERVICE**.

The screenshot shows the 'ADD DNS SERVICE' form in the NSX Manager interface. The form is titled 'DNS Services' and has tabs for 'DNS Services' and 'DNS Zones'. The 'ADD DNS SERVICE' button is highlighted with an orange box. The form contains several fields: 'Name' (DNS-Service), 'Tier-0/Tier-1 Gateway' (T1-GW-01), 'DNS Service IP' (172.16.0.10), 'Default DNS Zone' (Default-Zone), 'FQDN Zones' (a dropdown menu showing 'Lab-Zone-30'), 'Log Level' (Info), 'Description' (a text area), 'Admin Status' (Enabled), 'Cache Size' (1024), and 'Tags' (a dropdown menu showing 'Tag'). The 'SAVE' button is highlighted with a blue box.

To create DNS forwarder services, you provide values for the following options:

- **Name:** You use this name to identify the DNS forwarder service.
- **Tier-0/Tier-1 Gateway:** Specify the gateway for the service.
- **DNS Service IP:** Clients send DNS queries to this IP address, which is also known as the DNS forwarder's listener IP.
- **Default DNS Zone:** Select the default DNS zone.
- (Optional) **FQDN Zones:** Select up to five FQDN zones.
- **Admin Status:** Enable or disable the DNS forwarder service.
- (Optional) **Log Level:** Used in analysis and troubleshooting. The default log level is info.
- **Cache Size:** Specify the DNS forwarder cache size.
- (Optional) **Tags:** Specify to group NSX objects.

When you configure a DNS zone, you can specify a source IP for a DNS forwarder to use when forwarding DNS queries to an upstream DNS server. If you do not specify a source IP, the DNS query packet source IP will be the DNS forwarder's listener IP.

## 9-40 Establishing Forwarder Connectivity

The external upstream DNS servers require IP connectivity to the DNS forwarder, which can be achieved using route advertisement or SNAT.

The screenshot displays two panels from the AWS Management Console. The left panel, titled 'Option 1: Forwarder Route Advertisement', shows the 'Route Advertisement' section for a Transit Gateway (TG-DW-01). It includes settings for 'Edge Cluster', 'Auto Allocate Edges', 'Edges Pool Allocation Size', 'Description', 'Routing', 'DHCP Config', 'Tags', 'Fail Over', 'Non Preemptive', 'Standby Relocation', and 'Set'. The 'Route Advertisement' section is expanded, showing 'All Static Routes', 'All DNS Forwarder Routes', 'All Connected Segments & Service Keys', and 'All IPsec Local Endpoints'. The right panel, titled 'Option 2: Forwarder SNAT', shows the 'NAT' section for the same Transit Gateway. It includes a table with columns for 'Name', 'Action', 'Source IP', 'Match', 'Translated IP / Port', 'Apply To', 'Enabled', and 'Status'. A rule named 'DNS-Forwarder-SNAT' is shown with the action 'SNAT', source IP '10.0.0.0/24', and translated IP '100.66.100.2'. The 'Match' section includes 'Destination IP / Port' and 'Destination Port'.

**Option 1: Forwarder Route Advertisement**

Edge Cluster: Edge-Cluster-01  
Auto Allocate Edges: Yes  
Edges Pool Allocation Size: ROUTING  
Description:   
Routing:   
DHCP Config:   
Tags:   
Fail Over: Non Preemptive  
Standby Relocation: No  
Set: Tag Scope  
Max 30 allowed. Click (+) to add.

**Option 2: Forwarder SNAT**

Gateway: TG-DW-01 | Tier-1

**ADD NAT RULE**

Name	Action	Source IP	Match	Translated IP / Port	Apply To	Enabled	Status
DNS-Forwarder-SNAT	SNAT	10.0.0.0/24	Destination IP / Port Enter Destination IP IPV4 Address or CIDR or IP address or Enter Destination Port Destination Port	100.66.100.2 IPV4 Address or CIDR DNS-TCP: 53 Service / Port	Set	Yes	

If the DNS listener IP is not routed, forwarder connectivity can be established by:

- Using gateway route advertisement to announce the listener IP.
- Using gateway SNAT to translate the listener IP to a public IP.

## 9-41 Configuring DHCP to Allocate DNS

To optionally configure DHCP services to allocate DNS Servers, click **Networking** > **Segments** > **Edit an existing segment** > **EDIT DHCP CONFIG**, and configure DNS Servers.

The screenshot displays the NSX Segments configuration page. The 'App-Segment' is selected, showing its configuration: Name (App-Segment), Connected Gateway (T1-GW-01 | Tier-1), Transport Zone (PROD-Overlay-TZ), Subnets (172.16.20.1/24), and Ports / Interfaces (1). The 'EDIT DHCP CONFIG' button is highlighted. The 'Set DHCP Config' dialog box is open, showing the 'IPv4 Server' tab. The configuration includes: DHCP Type (Segment DHCP Server), DHCP Profile (DHCP-Local-Server-Profile), DHCP Server Address (172.16.20.99/24), DHCP Ranges (172.16.20.50-172.16.20.89), Lease Time (86400 seconds), and DNS Servers (172.20.10.10). The 'APPLY' button is visible at the bottom right of the dialog.

Name	Connected Gateway	Transport Zone	Subnets	Ports / Interfaces	Status	Alarms
App-Segment	T1-GW-01   Tier-1 Gateway Connectivity: <span style="color: green;">ON</span>	PROD-Overlay-TZ	172.16.20.1/24 CIDR e.g. 10.22.12.2/23 Gateway CIDR IPv6 CIDR e.g. fc7e:1206:db42::1/48	1		

### Set DHCP Config

Segment: App-Segment

DHCP Type\*: Segment DHCP Server | DHCP Profile\*: DHCP-Local-Server-Profile

**IPv4 Server** | IPv6 Server

Settings | Options | Static Bindings

DHCP Server Address: 172.16.20.99/24  
CIDR e.g. 10.22.12.2/23

DHCP Ranges: 172.16.20.50-172.16.20.89 | IPv4 Gateway: 172.16.20.1/24

Lease Time (seconds): 86400  
Value must be between 60 to 4294967295

DNS Servers: 172.20.10.10 | Enter IP Addresses  
e.g. 10.10.10.10

CANCEL APPLY

## 9-42 Review of Learner Objectives

- Explain how DHCP and DHCP Relay are used for IP address allocation
- Configure DHCP services in NSX
- Describe how to use a DNS forwarder service
- Configure DNS forwarder services in NSX



## 9-43 Lesson 3: Configuring NSX Advanced Load Balancer

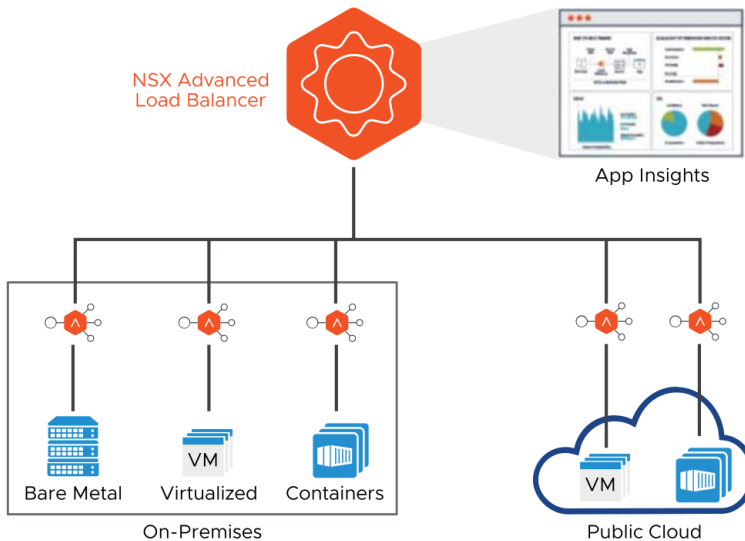
### 9-44 Learner Objectives

- Describe NSX Advanced Load Balancer and its use cases
- Explain the NSX Advanced Load Balancer architecture
- Deploy NSX Advanced Load Balancer
- Explain the NSX Advanced Load Balancer components and how they manage traffic
- Configure virtual IP addresses, server pools, and virtual services

### 9-45 About NSX Advanced Load Balancer

VMware will use NSX Advanced Load Balancer as part of its load-balancing strategy.

NSX Advanced Load Balancer provides multicloud load balancing, web application firewall, application analytics, and container ingress services across data centers and clouds.



## 9-46 Benefits of NSX Advanced Load Balancer

NSX Advanced Load Balancer offers several advantages.

End-to-End  
Automation



Higher  
Performance



Easy to  
Troubleshoot



On-Demand  
Scalability



NSX Advanced Load Balancer offers the following advantages:

- End-to-end automation: NSX Advanced Load Balancer fully automates the life cycle management and placement of load-balancing components.
- Higher performance: NSX Advanced Load Balancer provides optimal traffic flows with no traffic hairpinning. Additionally, it supports ECMP-based active-active scale-out mode.
- Easy to troubleshoot: NSX Advanced Load Balancer offers native built-in log analysis and rich analytics tools that provide end-to-end visibility of the environment. This improved visibility reduces the troubleshooting time from days to minutes.
- On-demand scalability: The NSX Advanced Load Balancer platform automatically scales horizontally based on the traffic needs and rebalances the load across all components to ensure high performance.

## 9-47 NSX Advanced Load Balancer Feature Edition Comparison (1)

The table provides a feature comparison between the Basic and Enterprise licenses of NSX Advanced Load Balancer.

Pillars	Feature	Basic	Enterprise
Licensing	License/Entitlement	As a part of NSX-DC ADV/ENT License Seamless upgrade to NSX-ALB Enterprise	NSX-ALB Enterprise License
Local Traffic Management	L4 LB	TCP and UDP Fast Path and Proxy No L4 SSL/TLS	TCP, UDP, DNS, SIP, RADIUS DSR, TLS support, PROXY protocol support
	L7 LB	Limited to basic L7 features; no HTTP/2	HTTP/2, content rewrite, compression, caching
	L3/4 Policies	Policies limited to connection drops No DataScript support	Full-featured, including DataScripts and live IP Reputation
	L7 Policies	Basic match and actions	Match on: IPReputation DB, string groups and much more Actions to: Rate-limit, ICAP and much more
Global Traffic Management	Global Server Load Balancing	✗	Enterprise grade GSLB
Application Security	SSL/TLS	Limited feature set	Dynamic CRLs, OCSP stapling, TLSv1.3, HSM, and cert management
	Application Rate Limiting	✗	Rate limiter can be applied for L4,L7, DNS, and WAF
	DDoS Protection	✗	L3, L4 and L7 DDos protection
	Intelligent WAF	✗	CRS, learning/PSM, IP Reputation, application signatures, bot detection

NSX Data Center Advanced and NSX Data Center Enterprise Plus editions include the NSX Advanced Load Balancer Basic entitlement. The Basic entitlement provides load-balancing features that are equivalent to the native NSX load balancer.

The NSX Advanced Load Balancer Enterprise edition requires an additional license and provides all features available in NSX Advanced Load Balancer, including GSLB, WAF, multicloud support, and so on.

For more information about the licenses and features available for NSX Advanced Load Balancer, see "NSX Advanced Load Balancer Editions" at <https://avinetworks.com/docs/22.1/nsx-license-editions/>

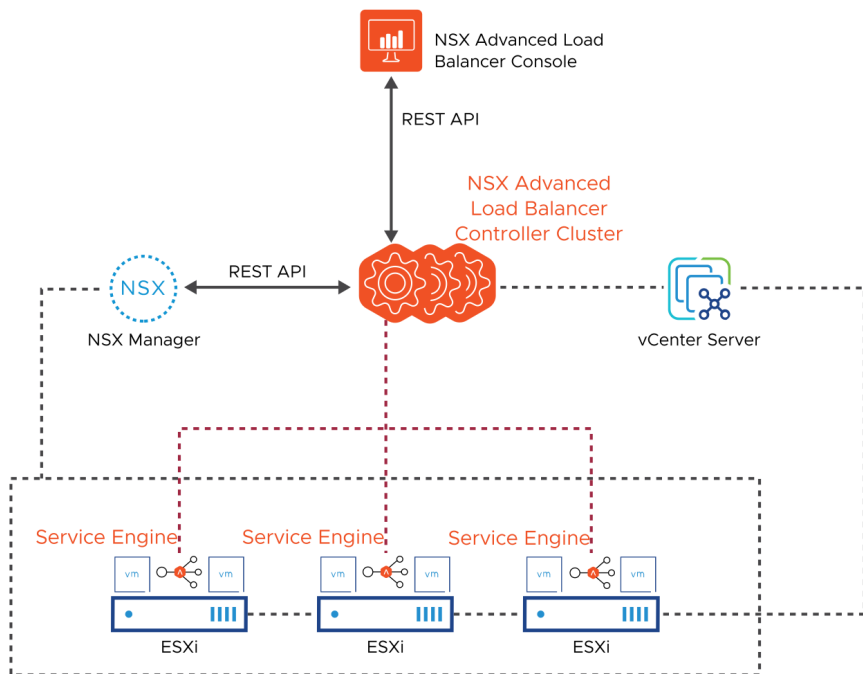
# 9-48 NSX Advanced Load Balancer Feature Edition Comparison (2)

Pillars	Feature	Basic	Enterprise
Container Ingress	Service Type LB	Yes	Yes
	Container Ingress	Limited Ingress	Full Ingress DNS and GSLB integration Multi K8s cluster & multi-AZ support
Software Defined Platform	Administration	Basic LB administration	Fully multi-tenant & granular RBAC Rich alerts and events Various 3rd part integrations Integrations with various IDPs
	Scale and HA	Active/Standby only	Active/Active deployments BGP and cloud-native ECMP support Autoscale of load balancers
	Flexible upgrades	✗	Flexible LCM across tenants/clouds/se-groups
	Ecosystem automation	No Access Cloud	Native integrations with all major public & private clouds and container orchestration platforms
	Pulse	✗	Case Management Live Security Threat Updates
Advanced Analytics	Application Visibility / Analytics	✗	Advanced application telemetry Log insights

## 9-49 NSX Advanced Load Balancer Architecture

The NSX Advanced Load Balancer architecture consists of two main components:

- NSX Advanced Load Balancer Controller:
  - Central repository for the configuration and policies related to load-balancing services.
  - Provides a user interface to perform configuration and management tasks.
  - Responsible for deploying Service Engines.
  - Typically deployed as a three-node cluster for high availability.
- Service engine (SE):
  - Performs application load-balancing operations.
  - Collects real-time analytics from application traffic flows.



The NSX Advanced Load Balancer architecture is built on software-defined principles. It separates the data and control plane to deliver scalable application load balancing. The platform provides a dynamic, centrally managed pool of load-balancing resources for virtual machines and containers.

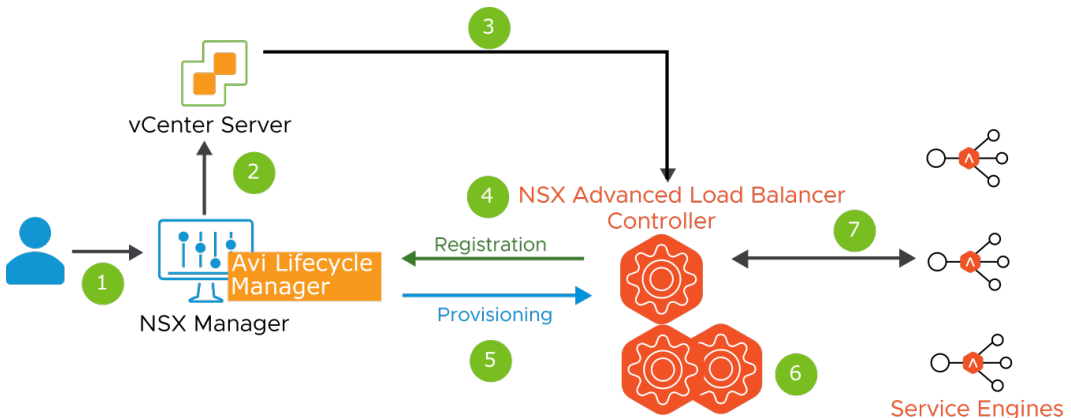
Since NSX 4.0.0.1, the configuration of NSX Advanced Load Balancer using the NSX UI and NSX API is deprecated. This feature should not be used because it will be removed completely in future releases. The installation of the NSX Advanced Load Balancer Controller cluster and the cross-launch of the NSX Advanced Load Balancer UI from NSX will continue to be supported. However, all configuration tasks for load balancers integrated with NSX environments should be performed directly through the NSX Advanced Load Balancer UI or API.

NSX Advanced Load Balancer Controller continues to interact with vCenter Server and NSX Manager through APIs for autodiscovery of SDDC objects such as ESXi hosts, segments, Tier-1 Gateways, and so on.

## 9-50 NSX Advanced Load Balancer Deployment Workflow

To deploy NSX Advanced Load Balancer:

1. The user uploads the NSX Advanced Load Balancer Controller .ova file to NSX Manager.
2. NSX Manager invokes the NSX Advanced Load Balancer Controller node deployment in vCenter Server.
3. vCenter Server deploys NSX Advanced Load Balancer Controller.
4. On startup, NSX Advanced Load Balancer Controller registers with NSX Manager by using the Avi Lifecycle Manager (Avi LCM).
5. After registration, Avi LCM performs the basic configuration of NSX Advanced Load Balancer Controller.
6. In a cluster deployment, the NSX Advanced Load Balancer Controller instances 2 and 3 are deployed, and the cluster is created.
7. Service engine VMs are created or deleted based on the load-balancer configuration.



The NSX Advanced Load Balancer Controller OVA must be version 20.1.6 or later. Previous versions of the image are not accepted. Only one OVA file can be uploaded at a time. The disk space required for the OVA bundle is about 4 GB.

Before registration of NSX Advanced Load Balancer Controller with the Avi Lifecycle Manager, trust is established between the two entities using certificates.

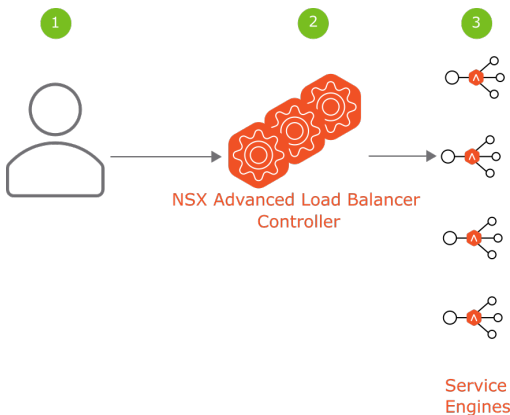
During the provisioning phase, the Avi Lifecycle Manager configures the following parameters on the controller:

- Admin user password
- DNS and NTP servers
- Controller cluster information, including the cluster VIP if specified during the deployment

## 9-51 NSX Advanced Load Balancer Consumption Workflow

Since NSX 4.0.0.1, all services related to NSX Advanced Load Balancer are configured directly using the NSX Advanced Load Balancer UI or API:

1. The user configures NSX Advanced Load Balancer through the NSX Advanced Load Balancer UI or API.
2. NSX Advanced Load Balancer Controller receives the load balancing configuration and disseminates it to the service engines.
3. The Service Engines perform load balancing operations and manage all client and server-facing network interactions.



## 9-52 Requirements for NSX Advanced Load Balancer

Before using NSX Advanced Load Balancer in your NSX environment, you must complete the following tasks:

1. Deploy the NSX Advanced Load Balancer Controller cluster for the NSX UI.
2. Create a cloud connector from the NSX Advanced Load Balancer UI.
3. (Optional) Create a service engine group from the NSX Advanced Load Balancer UI.

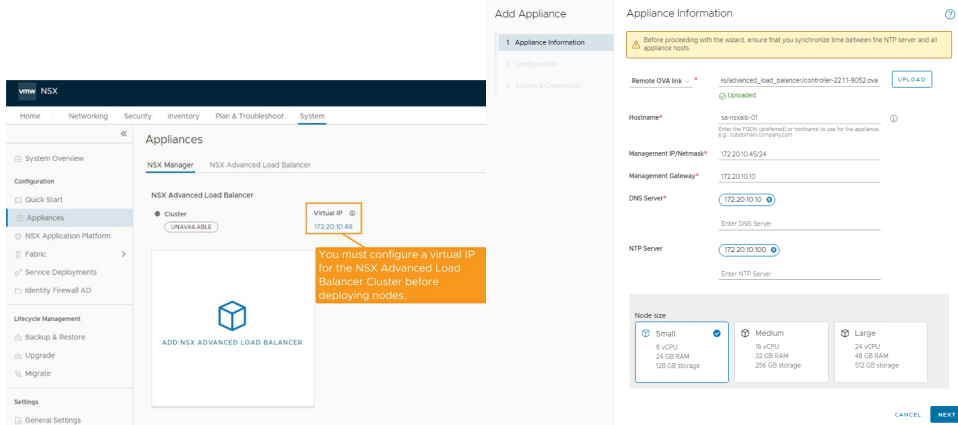


A cloud connector is used to integrate the NSX Advanced Load Balancer platform with the NSX environment. The cloud connector defines the connectivity information for the service engines, including the NSX segments and the Tier-1 gateway they are connected to.



## 9-53 Deploying the NSX Advanced Load Balancer Controller Cluster

You can deploy the NSX Advanced Load Balancer Controller cluster from the NSX UI by navigating to **System > Configuration > Appliances > NSX Advanced Load Balancer**.



Before deploying the NSX Advanced Load Balancer Controller cluster:

- vCenter Server must be registered with NSX as a Compute Manager.
- A virtual IP address must be configured for the NSX Advanced Load Balancer Controller cluster.

Each NSX Advanced Load Balancer Controller cluster requires only one management IP address. This IP address is used to configure the controller. The management IP address is also used by the controller to communicate with the service engines.

In a cluster deployment, the management IP addresses for all controllers must belong to the same subnet.

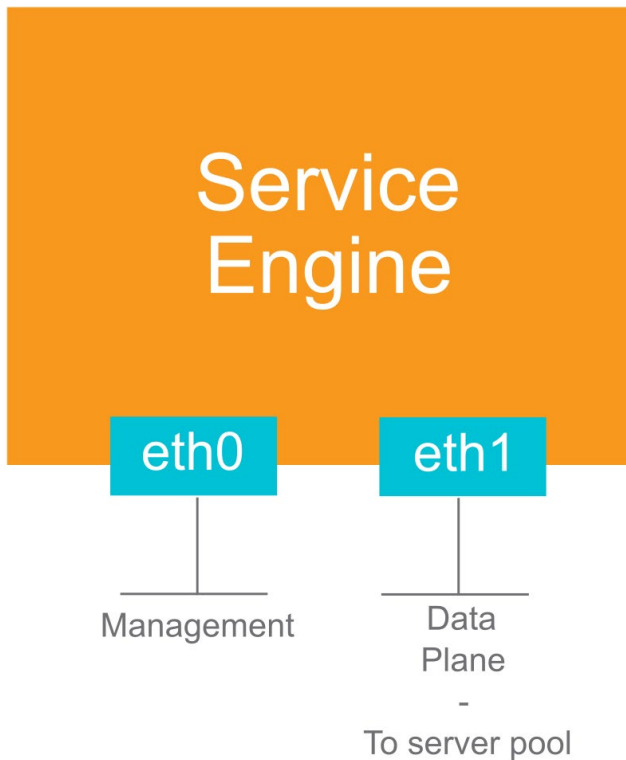
An NSX Advanced Load Balancer Controller cluster includes one or three nodes. All nodes must be deployed individually. To ensure that the cluster quorum is maintained, the deployment of the second node is queued until the third node is deployed.

## 9-54 Service Engines Deployment and Connectivity

The NSX Advanced Load Balancer Controller cluster creates or deletes service engine VMs based on the load-balancer configuration.

Each service engine requires two IP addresses:

- Management IP address: Used for communication with the NSX Advanced Load Balancer Controller cluster.
- Data plane IP address: Used for communication with the server pool network.



## 9-55 Creating a Cloud Connector (1)

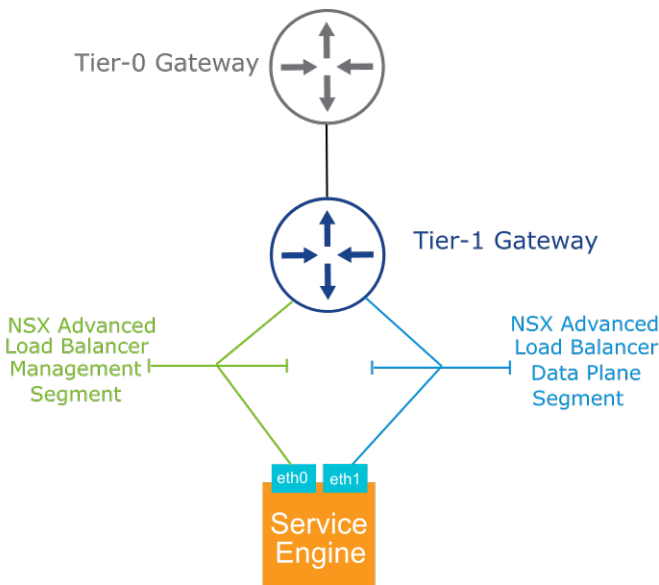
Before NSX Advanced Load Balancer Controller can create service engine VMs, you must create a cloud connector for the NSX environment.

The cloud connector defines the connectivity information for both the management and the data plane networks of the service engines, including:

- NSX transport zone
- NSX segment
- Tier-1 gateway used as the default gateway

In a typical deployment, separate NSX segments are used for the management and data plane interface of the service engines.

All required NSX constructs must be manually preconfigured in NSX Manager before creating the cloud connector.



Placing the service engines on NSX segments directly connected to a Tier-0 gateway is not supported.

Both NSX overlay and NSX VLAN-backed segments can be used to configure the management and data plane network for the service engines.

All required NSX constructs, including transport zones, Tier-1 gateway, and segments, must be manually preconfigured in NSX Manager before creating the cloud connector.

# 9-56 Creating a Cloud Connector (2)

You create a Cloud Connector from the NSX Advanced Load Balancer UI by navigating to **Infrastructure > Clouds**.

NEW CLOUD

nsxcloud

GeneralNSX-TIPAM/DNS

General

Name\*

nsxcloud

Type\*

NSX-T Cloud

Changing the Cloud type is only supported from the Clouds page by clicking 'Convert Cloud Type'.

☐ DHCP

Object Name Prefix\*

nsxcloud

Select this option if DHCP is available to manage the SE IP addresses.

Prefix for naming all NSX Advanced Load Balancer objects in NSX.

NSX-T

Credentials

NSX-T Manager Address

172.20.10.41

NSX-T Manager Credentials

nsxuser

CHANGE CREDENTIALS

Management Network

Transport Zone\*

PROD-Overlay-TZ (Overlay)

Tier1 Logical Router\*

TH-GW-01

Overlay Segment

ALB-MANAGEMENT

SE Management Transport Zone, Tier-1 Gateway, and Segment.

Data Networks

Transport Zone\*

PROD-Overlay-TZ (Overlay)

Data Network Segment(s)

ADD

☐ Logical Router

Overlay Segment

☐ TH-GW-01

ALB-DATAPLANE

SE Data Plane Transport Zone, Tier-1 Gateway, and Segment.

The cloud connector wizard first connects to NSX Manager to fetch the network constructs available and presents them as options to configure the SE management and data plane networks.

Only one management network is supported for all SE groups created for the NSX environment.

## 9-57 Creating a Service Engine Group

A service engine group is a method of grouping service engines to provide data plane isolation and redundancy:

- Multiple SE groups might exist in the NSX environment.
- SE groups are used to manage load-balancing traffic for a given load balancer service.
- If a service engine fails, another service engine within the same SE group takes over.

Creating a service engine group is optional. A default service engine group is automatically created for the NSX cloud. However, you can modify the existing service engine group or create another service engine group.

**New Service Engine Group:**

Basic Settings | **Advanced**

Service Engine Group Name\*  
NSX SE Group

Metric Update Frequency ⓘ  
☐ Real-Time Metrics 30 min

• High Availability & Placement Settings •

High Availability Mode ⓘ  
Legacy HA: ☐ Active/Standby  
Elastic HA: ☐ Active/Active ☒ N + M (buffer)

VS Placement across Service Engines ⓘ  
☒ Compact ☐ Distributed

Virtual Services per Service Engine ⓘ  
10 Maximum

☐ Service Engine Self-Election ⓘ

• Service Engine Capacity and Limit Settings •

Max Number of Service Engines ⓘ  
10 Maximum

Memory per Service Engine ⓘ  
2 GB

vCPU per Service Engine ⓘ  
1

Disk per Service Engine ⓘ  
15 GB

☒ Memory Reserve ☐ CPU Reserve

To create a service engine group from the NSX Advanced Load Balancer UI, navigate to **Infrastructure > Cloud Resources > Service Engine Group**.

The high availability mode of the SE group controls the behavior of the SE group if an SE failure occurs. It also controls how the load is distributed across SEs.

The following high availability modes are available:

- Legacy high availability active-standby mode: This mode is primarily intended to mimic a legacy appliance for easy migration to NSX Advanced Load Balancer. It deploys two services engines: one in active and the other in standby mode.
- Elastic high availability N+M mode: This default mode deploys N active SEs for load-balancing purposes, but also deploys M additional SEs within the service group as a buffer to absorb any SE failures.
- Elastic high availability active-active mode: This high availability mode load balances services across a minimum of two SEs that are both in active mode.

Active-standby is the only availability mode supported with the Basic Edition licensing. To avail of N+M and active-active high availability modes, you must purchase an NSX Advanced Load Balancer Enterprise license.

The VS Placement across SEs option determines whether the creation of load-balancing services also creates new SEs or uses those already available.

The following options exist:

- Compact: Attempts to place load balancer services on already existing service engines. This option is default for elastic high availability N+M and legacy high availability active-standby mode.
- Distributed: Maximizes load-balancing performance by deploying new service engines and avoiding placements on existing SEs. This option is the default for elastic high availability active-active mode.

For more information about the SE group configuration options, see "Service Engine Group" at <https://avinetworks.com/docs/22.1/service-engine-group/>.

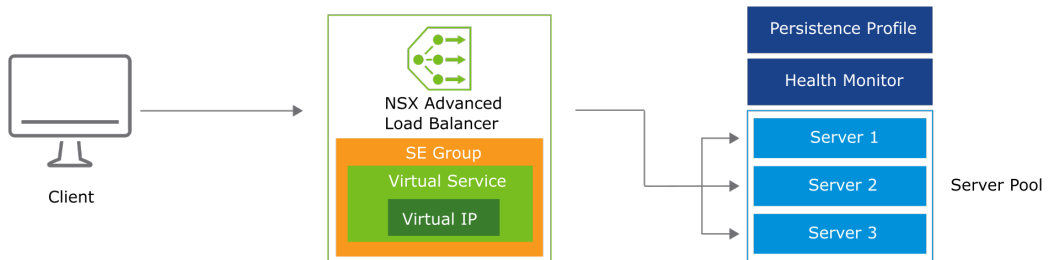
## 9-58 NSX Advanced Load Balancer Components

NSX Advanced Load Balancer includes several components:

- A virtual service is a software construct containing a virtual IP address, a port, and a protocol.

The virtual service is associated with a single SE group and attached to a Tier-1 gateway.

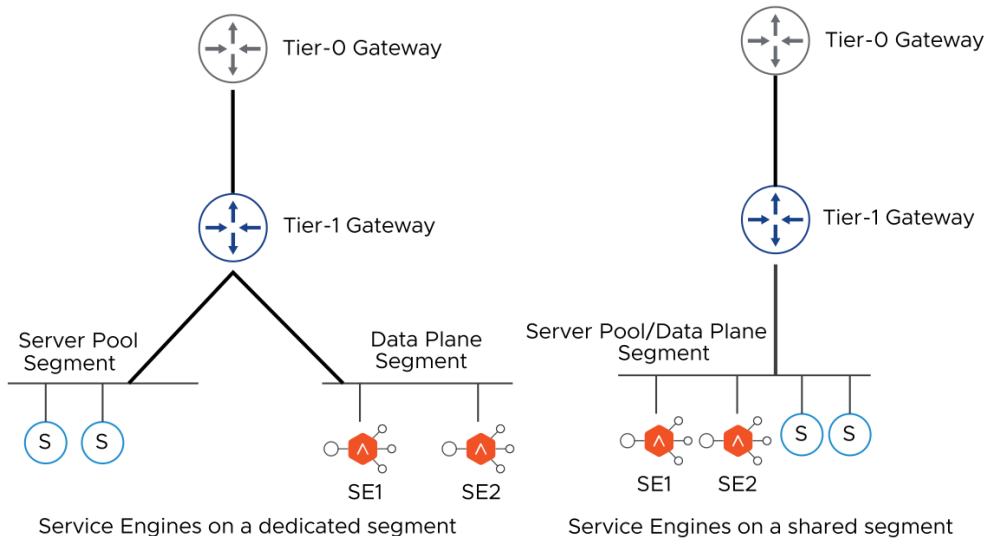
- A server pool is associated with a virtual service and includes the group of servers responsible for load balancing the client requests.
- A health monitor is attached to a server pool and verifies the status of the servers within it.
- A persistence profile is attached to a server pool and reconnects clients to the same pool member.



A virtual service is a software construct containing a virtual IP address, a port, and a protocol. External clients use this combination to access the servers behind the load balancer.

## 9-59 NSX Advanced Load Balancer Topologies

NSX Advanced Load Balancer supports different topologies for the SE and server pool deployment.



NSX Advanced Load Balancer supports two different topologies for the SE and server pool deployment:

- Service engines on a dedicated segment: This option allows you to manage the IP address assignments for the SE data plane interfaces and the server pool separately. The NSX segment used for the SE data plane must be created in NSX before creating an NSX Cloud Connector in NSX Advanced Load Balancer Controller.
- Service engines on a shared segment: With this option, the SE data plane interfaces share the same address space as the server pool servers and reside in the same NSX segment.



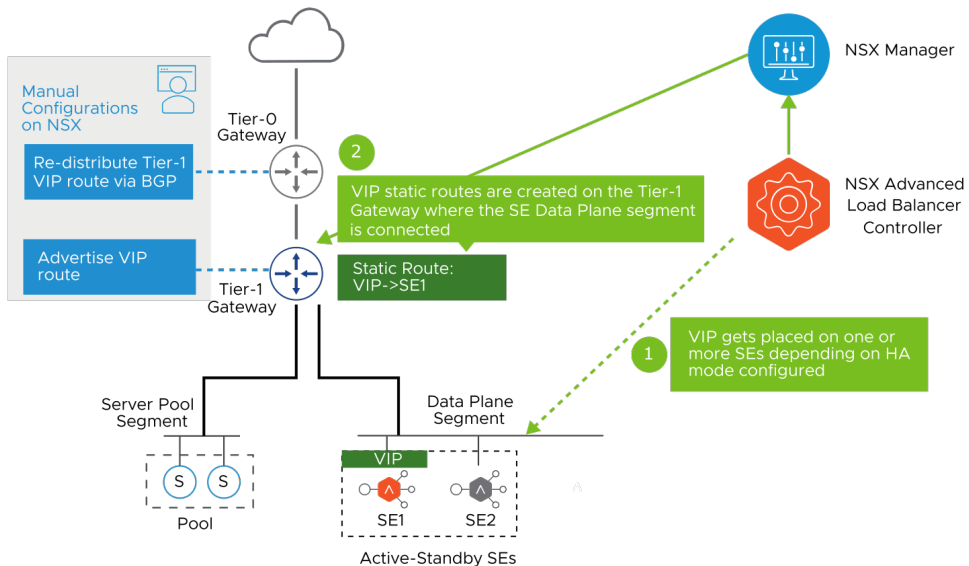
## 9-60 VIP Placement and Route Redistribution

Before deploying a virtual service, the Tier-1 and Tier-0 gateways must be configured to distribute the LB VIP.

During the virtual service configuration, the following actions are automatically performed:

1. The VIP is placed on one or more service engines depending on the high availability mode configured.
2. VIP static routes are created on the Tier-1 gateway where the SE data plane network is connected.

The VIP static routes include as many next hops as available service engines.



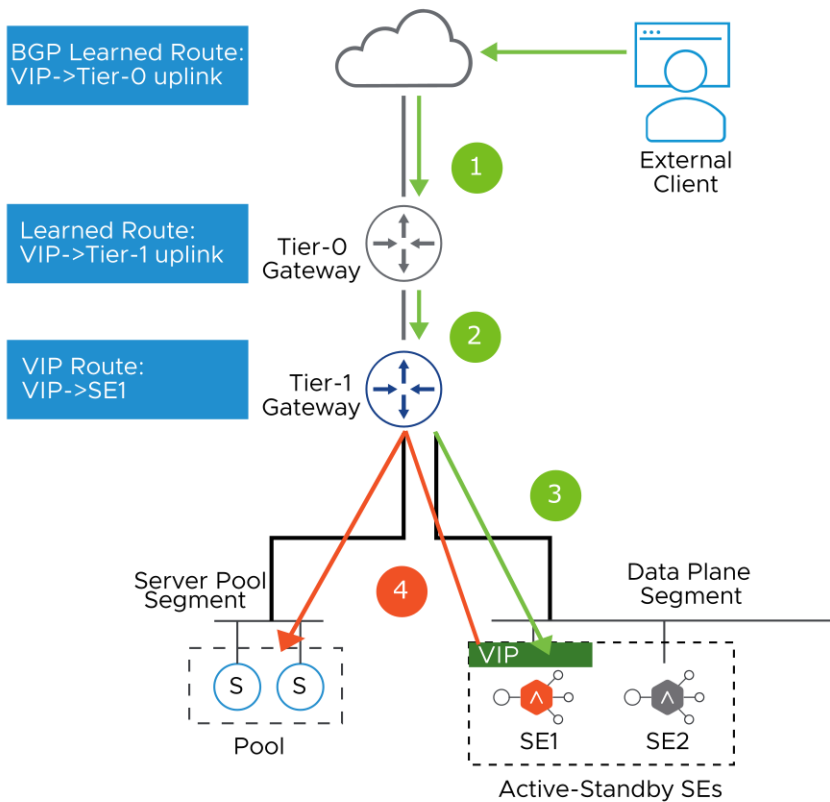
The NSX administrator is expected to configure the Tier-1 gateway to advertise the virtual service VIP with the Tier-0 gateway. For north-south reachability of the VIP, the administrator should also configure the Tier-0 gateway to redistribute the VIP to the external router through BGP.

After a virtual service is placed on an SE group, NSX Advanced Load Balancer Controller creates VIP static routes on the Tier-1 gateway where the SE data plane network is connected. The VIP static routes include as many next hops as available service engines. These static routes do not need to be advertised or redistributed, because they are only locally relevant to the Tier-1 gateway and the back-end service engines for ECMP purposes.

## 9-61 North-South Traffic

An external client request to the VIP is managed as follows:

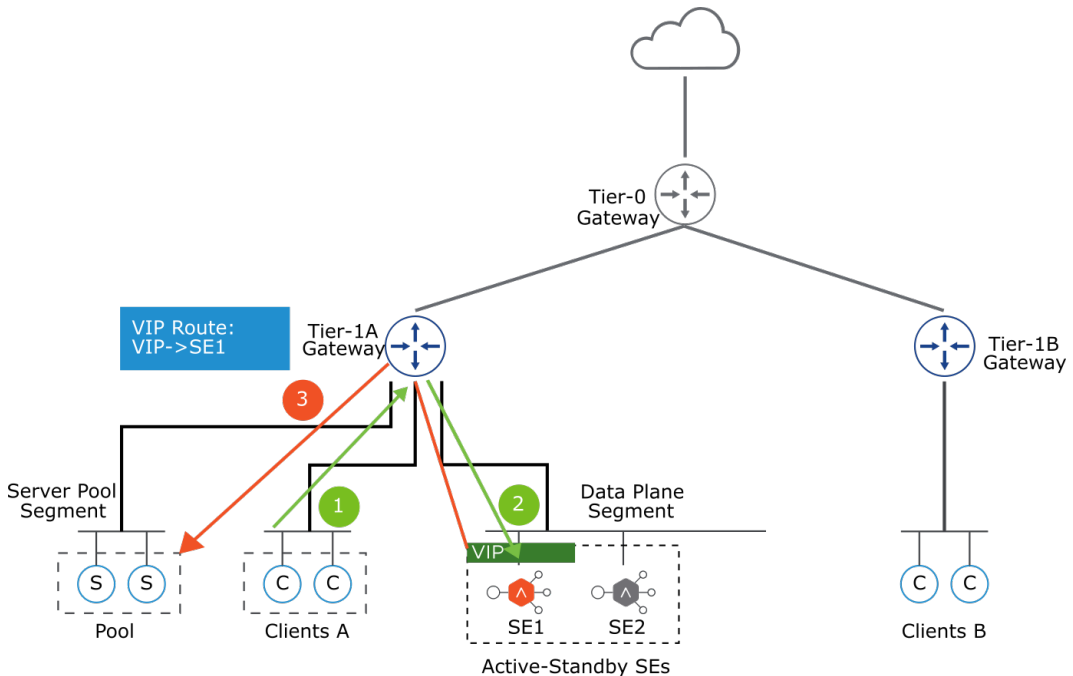
1. The external client traffic enters through the uplink of the Tier-0 gateway.
2. The Tier-0 gateway forwards the traffic to the appropriate Tier-1 gateway.
3. Using the static VIP routes, the Tier-1 gateway routes the request to the VIP on the service engines.
4. The service engines forward the traffic to the back-end server pool through the Tier-1 gateway.



## 9-62 East-West Traffic (1)

An internal client request to a VIP connected to the same Tier-1 gateway is managed as follows:

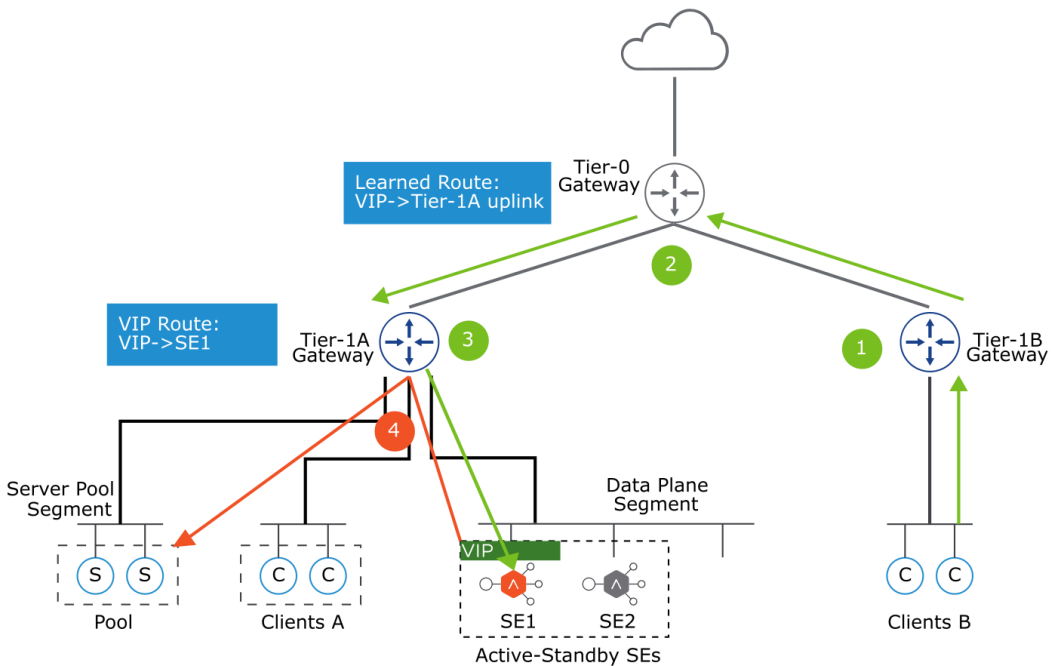
1. The request is sent to the Tier-1A gateway where the client network is connected.
2. Using the static VIP routes, the Tier-1A gateway routes the request to the VIP on the service engines.
3. The service engines forward the traffic to the back-end server pool through the Tier-1A gateway.



## 9-63 East-West Traffic (2)

An internal client request to a VIP connected to a different Tier-1 gateway is managed as follows:

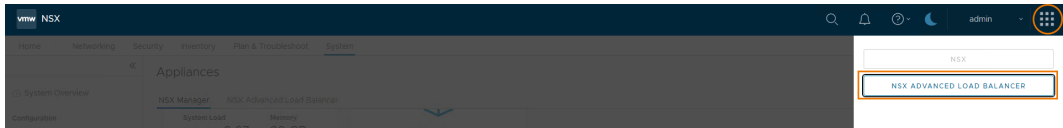
1. The request is sent to the Tier-1B gateway where the client network is connected.
2. The traffic is routed to the Tier-0 gateway, which forwards it to the Tier-1A gateway.
3. Using the static VIP routes, the Tier-1A gateway routes the request to the VIP on the service engines.
4. The service engines forward the traffic to the back-end server pool through the Tier-1A gateway.



## 9-64 Accessing the NSX Advanced Load Balancer UI

Since NSX 4.0.0.1, the configuration of all NSX Advanced Load Balancer components must be performed directly through the NSX Advanced Load Balancer UI or API, even if the solution is integrated with an NSX environment.

You can cross-launch to the NSX Advanced Load Balancer UI from NSX or log in directly to the deployed NSX ALB Controller.



# 9-65 Creating a Virtual IP Address

You create a virtual IP address that you can associate with a virtual service.

During the creation of the virtual IP, you specify the Tier-1 gateway to which the service engine data plane network is connected.

CREATE VS VIP

VIP-Web

GeneralRBAC

General

Name\*VIP-Web

Cloud  
nsxcloud

VRF Context  
T1-GW-01

Tier1 Logical Router  
T1-GW-01

VIPs (1)

ADD

<input type="checkbox"/>	Enabled	VIP ID	IP Address	IPv6 Address	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	192.168.100.7	-	<div><div></div><div></div></div>

Items per page10

You create a Virtual IP address by navigating to **Applications > VS VIPs** in the NSX Advanced Load Balancer UI.

During the creation of the virtual IP, you specify the cloud connector and the Tier-1 gateway to which the service engine data plane network is connected.

The Virtual IP address can be static or autoallocated from a preconfigured pool. It is possible to configure IPv4, IPv6 addresses, or both.

## 9-66 Creating a Server Pool

When configuring a server pool, you specify the pool members, load-balancing algorithm, health monitors, persistence profiles, and other parameters.

**CREATE POOL**

Web-Pool

General

Servers

Health Monitor

Profiles/Policies

SSL

Fail Action

RBAC

**General**

☒ **Enable Pool**

**Name\***  
Web-Pool

**Description**  
Description

**Cloud**  
nsxcloud

**VRF Context**  
T1-GW-01

**Default Server Port**  
80

**Load Balance Algorithm**  
Round Robin

☐ **Enable Request Queuing**

☐ **Enable Real Time Metrics**

☐ **Enable Routing Pool**

**Tier1 Logical Router\***  
T1-GW-01

Allows the configuration of advanced settings for the server pool.

Load-balancing algorithm.

CREATE POOL

Web-Pool

General

Servers

Health Monitor

Profiles/Policies

SSL

Fail Action

RBAC

Servers

Select Servers By

☒ IP Address, Range or DNS Name
 ☐ IP Group
 ☐ Security Group

Enter IP Address

Accepts single, range, and DNS name

ADD

The server pool can be defined by static membership criteria, IP Groups and NSX-native Security Groups.

Servers (2)

Servers currently configured in the pool.

<input type="checkbox"/>	Enabled	Server Name	IP Address	Port	Ratio	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	sa-web-01	172.16.10.11	80	1	<a href="#">✎</a> <a href="#">✕</a> <a href="#">▼</a>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	sa-web-02	172.16.10.12	80	1	<a href="#">✎</a> <a href="#">✕</a> <a href="#">▼</a>

Items per page 10 ▼

Server Deactivation Type

☒ Disallow New Connections
 ☐ Allow New Connections

Graceful Deactivate Timeout ⓘ

1

Minutes

☐ Enable HTTP2 ⓘ

☐ Lookup Server by Name ⓘ

☐ Rewrite Host Header to Server Name ⓘ

You create a Server Pool by navigating to **Applications > Pools** in the NSX Advanced Load Balancer UI.

You specify the following parameters during the creation of a server pool:

- Name: A unique name for the server pool.
- Cloud: The cloud connector details for the NSX environment.
- VRF Context: Virtual Routing Framework (VRF) is a method to isolate traffic in a system. VRF is also called a route domain in the load balancer community. A global VRF context is created by default. Network administrators might create custom VRF contexts to isolate traffic between different tenants or subsets.
- Default Server Port: New connections to servers will use this destination service port. The default port is 80.
- Load-balancing algorithm: The selected load-balancing algorithm controls how the incoming connections are distributed among the servers in the pool.
- Tier-1 gateway (logical router): Specify the Tier-1 gateway that you want to attach the server pool to. This value matches the Tier-1 gateway specified for the virtual service and VIP.



- Servers or pool members can be configured according to the following criteria:
  - IP Address, range, or DNS name: Manually enter the IP address, DNS name, and port for each member.
  - IP Group: Select an existing IP pool profile or create a profile.
  - Security Group: Select a native NSX grouping.
- You can verify server health by applying one or more health monitors in the Health Monitor section. Active monitors generate traffic from each service engine and mark a server up or down based on the response. The passive monitor listens only to client-to-server communication.
- In the Profiles and Policies section, you can configure a persistence profile to ensure that subsequent connections from the same client connect to the same server. Persistent connections are critical for most servers that maintain the client session information locally, such as HTTP applications that need to keep users' information for some time. This section also allows you to configure autoscaling policies for the load balancer.
- In the SSL section, you can enable SSL encryption between the service engines and the back-end servers.

For more information about the server pool configuration options, see the Avi Networks website at <https://avinetworks.com/docs/22.1/architectural-overview/applications/pools/>.

# 9-67    Configuring Load-Balancing Algorithms

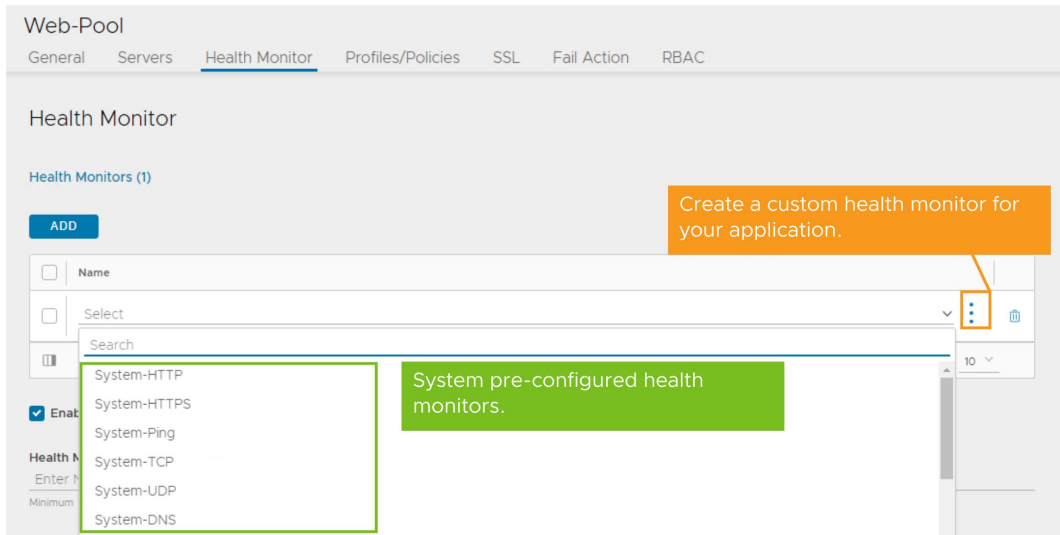
Load-balancing algorithms control how the incoming connections are distributed among the servers in the pool. The table includes a summary of the commonly used algorithms.

Load-Balancing Algorithms	Methods
Least Connections (Default)	New connections are sent to the server that currently has the least number of outstanding concurrent connections.
Round Robin	New connections are sent to the next eligible server in the pool in sequential order.
Fastest Response	New connections are sent to the server that is currently providing the fastest response to new connections or requests.
Consistent Hash	New connections are distributed across the servers using a hash key.
Least Load	New connections are sent to the server with the lightest load, regardless of the number of connections that server has.
Fewest Servers	Instead of trying to distribute all connections or requests across all servers, NSX Advanced Load Balancer determines the fewest number of servers required to satisfy the current client load.

For a full list of supported load balancing algorithms, see "Load Balancing Algorithms" at <https://avinetworks.com/docs/22.1/load-balancing-algorithms/>

## 9-68 Configuring Health Monitor Profiles

Health monitors validate the status of the servers in a pool to make forwarding decisions. You can configure health monitor profiles for HTTP, HTTPS, TCP, and UDP applications amongst others.



In the server pool creation wizard, you use the **Health Monitor** tab to configure active and passive health monitors for the pool members.

Some active health monitors that are preconfigured in the system are as follows:

- **System-HTTP:** Sends a request to a web server and validates either the HTTP response code or the HTML response data.
- **System-HTTPS:** Used to validate the health of HTTPS encrypted web servers. It relies on the same mechanism as the HTTP monitor.
- **System-Ping:** Validates the status of the server by sending a ping command and receiving a reply.
- **System-TCP:** Validates that the server can successfully establish a TCP connection.
- **System-UDP:** Sends a UDP datagram to the server and matches the server's response against the expected response data.
- **System-DNS:** Queries name servers for an A record and matches the resolved response against an expected IP address.

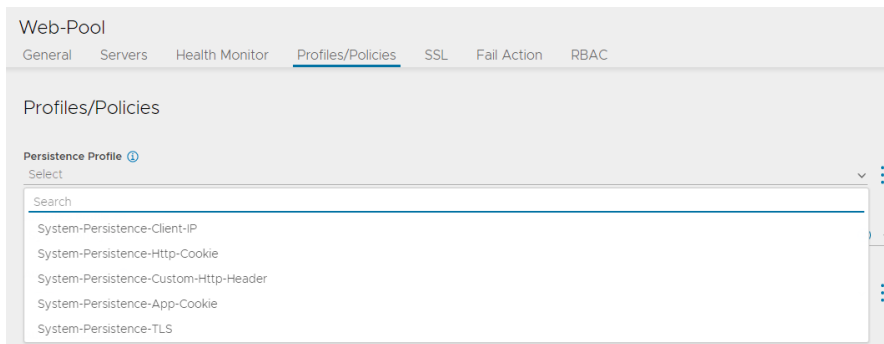
You can also create custom health monitor profiles for your applications.

## 9-69 Configuring Persistence Profiles

Persistence profiles ensure the stability of stateful applications by directing all related connections to the same back-end server.

NSX Advanced Load Balancer supports the following types of persistence profiles:

- Client IP
- HTTP Cookie
- Custom HTTP Header
- App Cookie
- TLS



In the server pool creation wizard, you use the **Profiles/Policies** tab to configure persistence profiles.

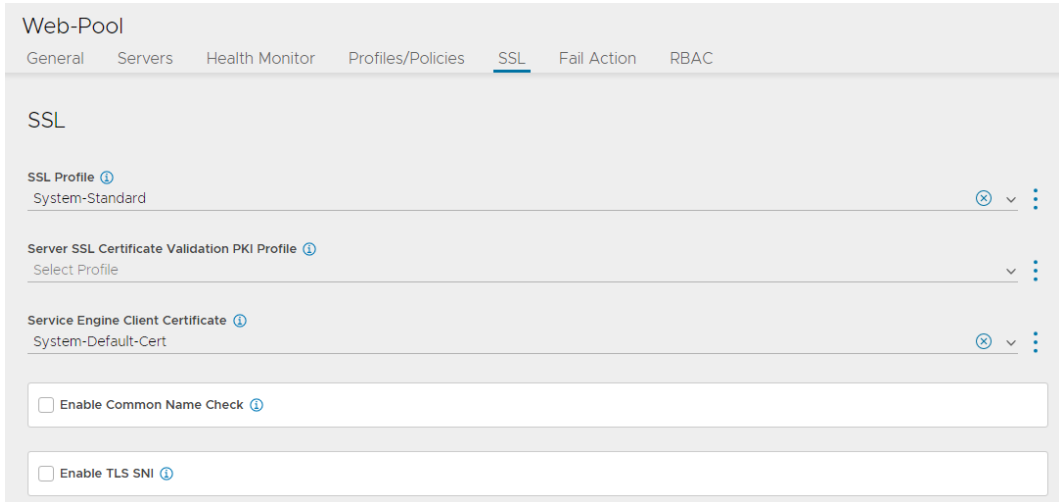
NSX Advanced Load Balancer supports the following types of persistence profiles:

- **Client IP:** NSX Advanced Load Balancer maintains a table with the client's source IP address. The client's source IP address is kept in the table for a given period of time. While the IP address remains in the table, any new connection by the user will be sent to the same server.
- **HTTP Cookie:** The NSX Advanced Load Balancer service engines insert an HTTP cookie into a server's first response to a client. In this mode, no configuration changes are required on the back-end servers.
- **Custom HTTP Header:** This method allows to specify an HTTP header for persistence.
- **App Cookie:** Rather than NSX Advanced Load Balancer inserting its own cookie into HTTP responses for persistence, this mode relies on an existing cookie that is inserted by the back-end server.
- **TLS:** Applicable to virtual services that are terminating SSL or TLS. This method embeds user persistence information within TLS session information.

## 9-70 Configuring Server Pool Security Settings

You can encrypt the traffic between the service engines and the back-end servers by enabling SSL in the server pool.

The chosen SSL profile defines which ciphers and SSL versions are used to encrypt the traffic.



The screenshot shows the 'Web-Pool' configuration interface with the 'SSL' tab selected. The page has a top navigation bar with tabs: General, Servers, Health Monitor, Profiles/Policies, SSL (active), Fail Action, and RBAC. Below the tabs, the 'SSL' section contains three main configuration items, each with a dropdown menu and a settings icon (three dots):

- SSL Profile**: Set to 'System-Standard'.
- Server SSL Certificate Validation PKI Profile**: Set to 'Select Profile'.
- Service Engine Client Certificate**: Set to 'System-Default-Cert'.

Below these items are two checkboxes, each with an information icon (i):

- ☐ **Enable Common Name Check**
- ☐ **Enable TLS SNI**

In the server pool creation wizard, you use the **SSL** tab to configure security settings for the server pool.

You can encrypt the traffic between the service engines and the back-end servers by specifying the following parameters:

- **SSL Profile**: The SSL profile defines which ciphers and SSL versions are supported to encrypt the traffic.
- **Server SSL Certificate Validation PKI Profile**: This option validates the certificate presented by the server against the selected PKI profile. When not enabled, the service engine automatically accepts the certificate presented by the server when sending health checks.
- **Service Engine Client Certificate**: When establishing an SSL connection with a server, either for normal client-to-server communications or when executing a health monitor, the service engine presents this certificate to the server.

Additionally, you can also enable Common Name Check and TLS SNI from the **SSL** tab.

## 9-71 Creating a Virtual Service

When creating a virtual service, you specify its virtual IP, port and protocol combination, and the server pool responsible for managing the back-end traffic.

The screenshot displays the 'New Virtual Service: VS-Web' configuration interface. It features a progress bar at the top with four steps: Step 1: Settings, Step 2: Policies, Step 3: Analytics, and Step 4: Advanced. The main configuration area is divided into several sections:

- Settings:** Includes a 'Name' field with the value 'VS-Web', an 'Enabled' toggle, and a 'VIP Address' dropdown menu showing 'VIP-Web'.
- Service Port and Protocol:** Includes a 'Services' field with the value '80', and checkboxes for 'HTTP2' and 'SSL'.
- TCP/UDP and Application Profiles:** Includes a 'TCP/UDP Profile' dropdown menu showing 'System-TCP-Proxy', an 'Application Profile' dropdown menu showing 'System-HTTP', and a 'WAF Policy' dropdown menu showing 'Select WAF Policy'.
- Bot Detection Policy:** Includes a 'Bot Detection Policy' dropdown menu showing 'Select Bot Detection Policy'.
- ICAP Profile:** Includes an 'ICAP Profile' dropdown menu showing 'Select ICAP Profile'.
- Error Page Profile:** Includes an 'Error Page Profile' dropdown menu showing 'Select Error Page Profile'.
- Pool/Pool Group:** Includes a 'Pool' radio button, a 'Pool Group' radio button, and a 'Pool' dropdown menu showing 'Web-Pool'.

You create a server pool by navigating to **Applications > Virtual Services** in the NSX Advanced Load Balancer UI. The NSX Advanced Load Balancer UI offers two methods for creating a virtual service: basic setup and advanced setup. The advanced setup allows users more granular control over the settings of the virtual service, including the reuse of preconfigured or existing server pools. The same information included in the advanced setup is available whenever a Virtual Service is edited, regardless of how it was created (Basic or Advanced). In both the basic and advanced setups, you must specify the cloud connector before configuring the virtual service.

In an advanced setup, you specify the following main parameters during the creation of a virtual service instance:

- **Name:** Provide a unique name for the new virtual service.
- **VS VIP:** Select an existing virtual service IP address from the drop-down menu or create an address.
- **TCP/UDP Profile:** Use the TCP/UDP profile to set the virtual service to listen for UDP Fast Path, TCP Fast Path, or TCP Proxy. If the application profile is set to an HTTP profile, the TCP/UDP profile must be set to proxy the TCP connections.

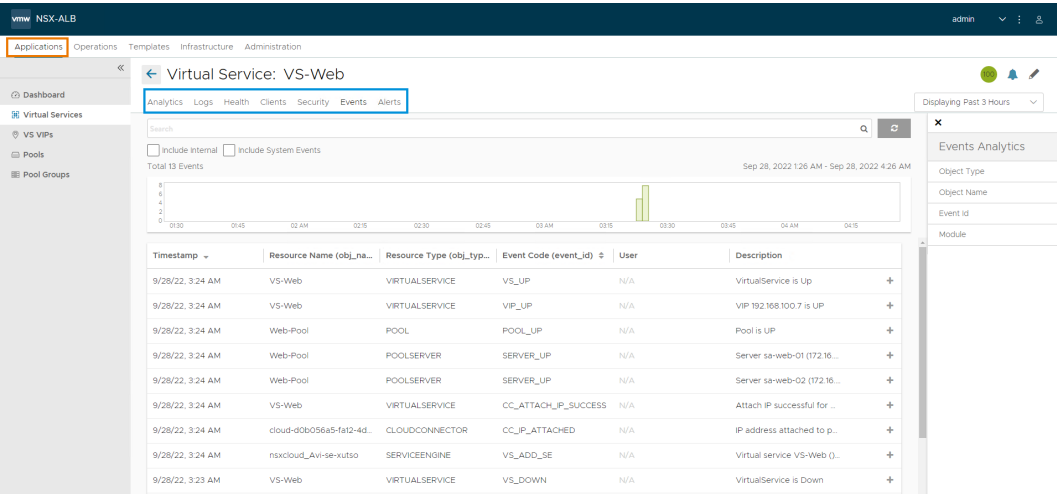
- **Application Profile:** Determines the behavior of the virtual services, based on application type. Some commonly used profiles are as follows:
  - **System-DNS:** Default for processing DNS traffic and uses UDP port 53.
  - **System-FTP:** Used for load balancing FTP workloads for both active and passive FTP modes.
  - **System-HTTP:** Default for processing nonsecure layer 7 HTTP traffic and uses port 80.
  - **System-L4-Application:** The virtual service listens for layer 4 requests on the port that you specify in the Service Port field. Select this option to use the virtual service for non-HTTP applications, such as mail or a database.
  - **System-Secure-HTTP:** Default for processing secure layer 7 HTTPS traffic. Uses port 443.
  - **System-Secure-HTTP-VDI:** Default for processing virtual desktop HTTP traffic.
  - **System-SSL-Application:** The virtual service listens for secure layer 4 requests. Selecting this option autopopulates port 443 in the Service Port field.
  - **System-Syslog:** Default for processing Syslog traffic.
- **Services:** Specify a port number or range for the virtual service.
- **Pool/Pool Group:** Select the pool to use for this virtual service using the **Pool** drop-down menu. A pool may only be associated with one virtual service. However, the same servers can belong to multiple pools using unique port combinations.

For more information about the Virtual Service configuration options, see [Create a Virtual Service](https://avinetworks.com/docs/22.1/architectural-overview/applications/virtual-services/create-virtual-service/) at <https://avinetworks.com/docs/22.1/architectural-overview/applications/virtual-services/create-virtual-service/>.

# 9-72 Validating Virtual Services and Server Pools

On the **Applications** tab in the NSX Advanced Load Balancer UI, you can review the following details for each virtual service and server pool instance:

- Analytics
- Logs
- Health
- Clients/servers
- Security (virtual service)
- Events
- Alerts



On the **Applications** tab in the NSX Advanced Load Balancer UI, you can review the following details for each virtual service and server pool instance:

- Analytics: Provides insights into performance through the real-time analysis of key performance indicators.
- Logs: Logs are indexed on NSX Advanced Load Balancer Controller. Logs can be viewed and filtered locally in the NSX Advanced Load Balancer UI.
- Health: The health score denotes both the responsiveness of the virtual service or pool, and any vulnerabilities.



- Clients/servers: The **Clients** tab is available for virtual services and displays information about clients accessing that service. The **Servers** tab is available for server pools and displays information about the status, health, and throughput of each member.
- Security: This tab is only available for virtual services. It provides detailed security information, including SSL and DDoS information.
- Events: Events are used to provide a history of relevant changes that have occurred in a virtual service or service pool.
- Alerts: Alerts are intended to inform administrators of significant events within a virtual service or service pool.

## 9-73 Lab 18: Configuring NSX Advanced Load Balancer

Configure NSX Advanced load-balancing services:

1. Prepare for the Lab
2. Create Segments for NSX Advanced Load Balancer
3. Deploy NSX Advanced Load Balancer Controller
4. Access the NSX Advanced Load Balancer UI
5. Create a Cloud Connector for NSX
6. Configure Service Engine Networks and Routing
7. Test the Connectivity to Web Servers
8. Create a Virtual Service
9. Configure Route Advertisement and Route Redistribution for the Virtual IP

## 9-74 Review of Learner Objectives

- Describe NSX Advanced Load Balancer and its use cases
- Explain the NSX Advanced Load Balancer architecture
- Deploy NSX Advanced Load Balancer
- Explain the NSX Advanced Load Balancer components and how they manage traffic
- Configure virtual IP addresses, server pools, and virtual services

## 9-75 Lesson 4: IPSec VPN

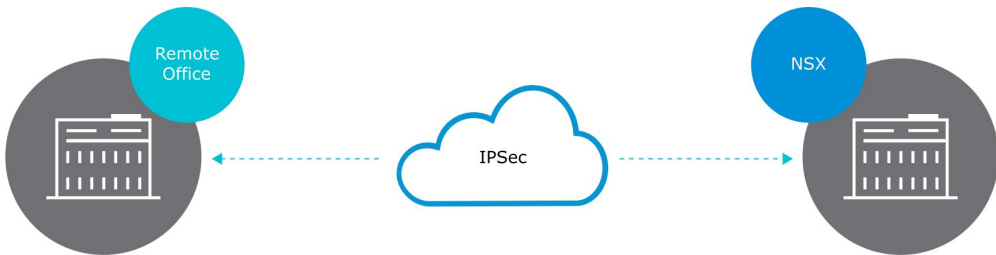
### 9-76 Learner Objectives

- Explain how IPSec-based technologies are used to establish VPNs
- Compare policy-based and route-based IPSec VPN
- Describe IPSec VPN requirements in NSX
- Create and configure IPSec VPN tunnels
- Identify Traceflow and Live Traffic Analysis enhancements for VPN tunnels

### 9-77 Use Cases for IPSec VPN

IPSec VPN has several use cases:

- Enables businesses to interconnect remote IP networks securely
- Extends IP networks to remote offices
- Uses a routing-based connection between different, nonoverlapping IP subnets
- Provides a secure communication channel for other nonsecure protocols, such as Generic Routing Encapsulation (GRE)



IPSec VPN secures the traffic that flows between two networks. These networks are connected over a public network through IPSec gateways called endpoints.

NSX Edge supports site-to-site IPSec VPN between an NSX Edge instance and remote IPSec-capable gateways.

NSX Edge can be one or both endpoints, supporting site-to-site IPSec VPN with another NSX Edge or another vendor's IPSec gateway.

# 9-78 IPsec VPN Protocols and Algorithms

IPsec VPN includes several protocols and algorithms:

IPsec Service	IPsec Algorithms and Protocols
Key management	Internet Key Exchange (IKE)
Authentication	Preshared key Certificates
Encryption	Advanced Encryption Standard (AES)
Data integrity	Secure Hash Algorithm (SHA)

IPsec is not a single protocol. It is a suite of protocols designed to provide confidentiality, authentication, and integrity for a VPN.

To accomplish these goals, IPsec uses Internet Key Exchange (IKE) to:

- Manage the connection to a peer.
- Define security associations used to secure and validate data exchanges.
- Define security protocols used to carry IP traffic over the VPN.
- IKE runs over UDP port 500. If NAT is detected in the gateway, the port is set to UDP 4500.
- IKEv1 (RFC 2409) and IKEv2 (RFC 5996) are supported.

Security Associations (SA): An SA is a basic component of IPsec and contains information about the security parameters negotiated between peers.

The following types of SAs are available:

- IKE (or ISAKMP) SA
- IPsec SA

The IKE SA is used for the control plane of the VPN and contains a combination of mandatory and optional values:

- Encryption Algorithm: Mandatory
- Hash Algorithm: Mandatory
- Authentication Method: Mandatory
- Diffie-Hellman Group: Mandatory
- Lifetime: Optional

## 9-79 IPSec VPN Methods

IPSec VPN tunnel packets can use different types of headers:

- The authentication header (AH) provides data integrity and authentication without encryption.
- The encapsulating security payload header (ESP) provides encryption, data integrity, and authentication.

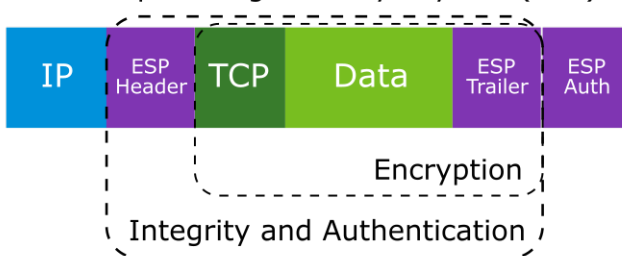
IP Data Packet



Authentication Header (AH)



Encapsulating Security Payload (ESP)



The authentication header does not provide encryption, whereas the encapsulating security payload header enables the encryption of the protected payload.

## 9-80 IPsec VPN Modes

IPsec VPN supports the following modes:

- Transport mode:
  - Preserves the original IP header
  - Typically used for remote-access VPN
- Tunnel mode:
  - Encapsulates the entire IP datagram with a new header
  - Used for site-to-site VPN between IPsec-enabled gateways
  - Mode used by NSX

IP Data Packet



Authentication Header (AH)



Transport Mode



Tunnel Mode

Encapsulating Security Payload (ESP)



Transport Mode

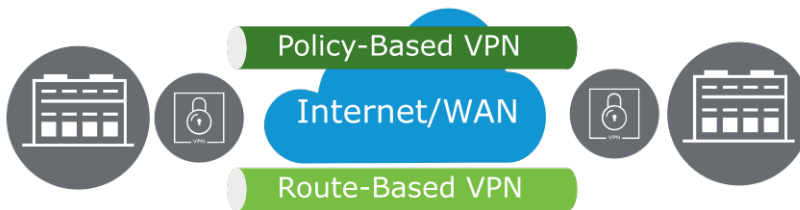


Tunnel Mode

## 9-81 IPSec VPN Types

The following IPSec VPN types are available.

- Policy-based VPN:
  - A VPN policy is used to determine which traffic is protected by IPSec and passes through the VPN tunnel.
  - This static configuration requires modification of the VPN policy when network topology changes occur.
- Route-based VPN:
  - The remote IPSec VPN gateway is a BGP peer and protected local and remote networks are learned based on routes exchanged by using BGP.
  - Routes are learned over a specific interface called a Virtual Tunnel Interface (VTI).



Additional route-based VPN properties:

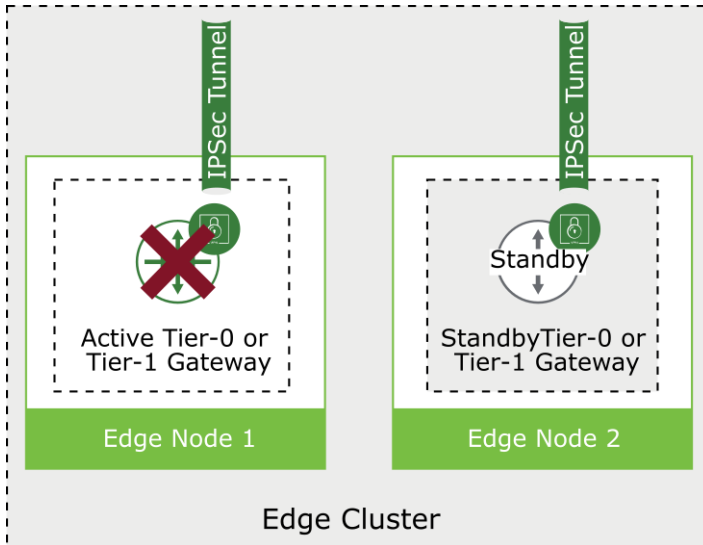
- All packets routed through the VTI are protected by using IPSec.
- OSPF dynamic routing is not supported for routing through IPSec VPN tunnels.
- Tunnel redundancy is supported:
  - By using BGP only.
  - Do not use static routing or OSPF to achieve VPN tunnel redundancy.
  - The primary tunnel is active, whereas the secondary tunnel is standby.
  - If the peer is unreachable on the primary tunnel, the secondary tunnel becomes active.

## 9-82 NSX IPSec VPN Deployment

When you deploy IPSec VPN, you should consider several factors:

- IPSec VPN services are available on both Tier-1 and Tier-0 gateways.
- Protected networks must be segments created through the NSX UI or policy APIs.
- Segments can be connected to either Tier-0 or Tier-1 gateways to use VPN services.
- Tenants with overlapping networks require NAT on Tier-0 gateways.
- VPN-based dynamic routing for VTI is supported on Tier-0 gateways only.
- NSX supports site-to-site IPSec VPNs in tunnel mode.
- IPSec tunnels use the DPDK-accelerated performance.

## 9-83 IPsec VPN: High Availability



IPsec VPN high availability has the following characteristics:

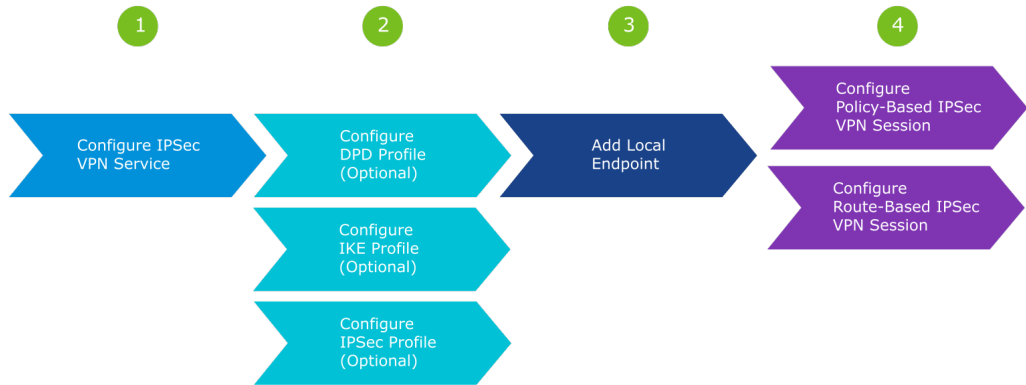
- VPN supports active-standby high availability on the Tier-1 and Tier-0 gateways.
- VPN services use gateway-level failover.
- VPN configuration and VPN state are synchronized.
- Tunnels are re-established without renegotiation on failover.

Additional IPsec VPN high availability properties:

- This feature is supported for both policy-based and route-based IPsec VPN services.
- You can use high availability virtual IP addresses for external connections.



## 9-84 IPSec VPN Workflow



All Step 2 profile configurations are optional.

In Step 4, you add an IPSec VPN session that is either policy-based or route-based.

## 9-85 Configuring an IPSec VPN Service

To configure an IPSec VPN service, you select **Networking > VPN > VPN Services > ADD SERVICE > IPSec**. Then you specify the values for the options.

The screenshot shows the 'VPN' configuration page with tabs for 'VPN Services', 'IPSec Sessions', 'L2 VPN Sessions', 'Local Endpoints', and 'Profiles'. The 'ADD SERVICE' button is highlighted with a red box. Below it, a table lists the configured service: 'IPSec-VPN-01' of type 'IPSec' associated with 'T1-GW-01'. The configuration details for this service are shown below the table:

Name	Service Type	Tier-0/Tier-1 Gateway	Sessions	Status	Alarms
IPSec-VPN-01	IPSec	T1-GW-01	Set	Info	

Configuration details for the selected service:

- Admin Status:** Enabled (toggle switch)
- Session Sync:** Enabled (toggle switch)
- Description:**
- IKE Log Level:** Info (dropdown menu)
- Tags:**  Tag  Scope  (Max 30 allowed. Click (+) to add.)

Global Bypass Rules:

NOTE - Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save.

You configure the following settings for an IPSec service:

- **Name:** You enter a name for the IPSec service.
- **Tier-0/Tier1 Gateway:** From the **Tier-0/Tier-1 Gateway** drop-down menu, select a Tier-0/Tier-1 gateway to associate with this IPSec VPN service.
- **Admin Status:** This option enables or disables the IPSec VPN service. By default, the value is set to **Enabled** to enable the service on the Tier-0 gateway.
- **IKE Log Level:** This option enables VPN service logging. The IKE logging level determines the amount of information that you want collected for the IPSec VPN traffic. The default is set to the Info level.
- **Session Sync:** This option enables or disables the stateful synchronization of VPN sessions. By default, this parameter is set to Enabled.
- **Tags:** You enter a value for tags if you want to include this service in a tag group.

## 9-86 Configuring DPD Profiles

Dead peer detection (DPD) is a method for detecting whether an IPsec connection is alive. To configure a DPD profile, you select **DPD PROFILES** on the **PROFILES** tab.

The screenshot shows the NSX VPN configuration interface. At the top, there are tabs for VPN Services, IPsec Sessions, L2 VPN Sessions, Local Endpoints, and Profiles. The Profiles tab is selected. Below the tabs, there is a 'Select Profile type:' dropdown menu with 'DPD PROFILES' selected. To the left of the main configuration area, there is a sidebar with 'ADD DPD PROFILE' and 'EXPAND ALL' buttons. The main configuration area contains a table with columns: Name, DPD Probe Mode, DPD Probe Interval (seconds), Retry Count, Sessions, and Status. The 'Name' column has a text input field with 'DPD-Profile' entered. The 'DPD Probe Mode' column has a dropdown menu with 'Periodic' and 'On Demand' options. The 'DPD Probe Interval (seconds)' column has a text input field with '60' entered. The 'Retry Count' column has a text input field with '10' entered. Below the table, there is a section for 'Admin Status' with a toggle switch set to 'Enabled'. There is also a 'Description' text input field and a 'Tags' section with a 'Tag' and 'Scope' dropdown menu. At the bottom, there are 'SAVE' and 'CANCEL' buttons.

This step is optional after you configure an IPsec service.

A DPD profile specifies the number of seconds to wait between probes to detect whether an IPsec peer is alive.

NSX provides a system-generated DPD profile, nsx-default-l3vpn-dpd-profile, which is assigned by default when you configure an IPsec VPN service.

To configure a DPD profile, you select values for the following options:

- **Name:** You use the name to identify the service.
- **DPD Probe Mode:**
  - **Periodic:** For a periodic DPD probe mode, a DPD probe is sent every time the specified DPD probe interval time is reached.
  - **On Demand:** For an on-demand DPD probe mode, a DPD probe is sent if no IPsec packet is received from the peer site after an idle period. The value in the **DPD Probe Interval** text box determines the idle period used.
- **DPD Probe Interval (sec):** You provide a value in seconds to define at which times a DPD detection packet should be sent.
- **Retry Count:** The number of allowed retries.
- **Admin Status:** This setting enables or disables the profile.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.

## 9-87 Configuring IKE Profiles

The Internet Key Exchange (IKE) profile defines the algorithms that are used to authenticate, encrypt, and establish a shared secret. To configure an IKE profile, you select **IKE PROFILES**.

VPN

VPN Services | IPsec Sessions | L2 VPN Sessions | Local Endpoints | **Profiles**

Select Profile type: **IKE PROFILES**

**ADD IKE PROFILE** EXPAND ALL Filter by Name, Path and more

Name	IKE Version	Encryption Algorithm	Digest Algorithm	Diffie-Hellman	Sessions	Status
nsx-ikev1-profile	IKE V1	AES 128	SHA2 256	Group 14		
SA Lifetime (seconds): 86400						
Description		Tags		Tag Scope		
Max 30 allowed. Click (+) to add.						
<b>SAVE</b> <b>CANCEL</b>						
> > > CNSA	IKE V2	AES 256	SHA2 384	Group 15	View More	0 Success
> > > FIPS	IKE FLEX	AES 128	SHA2 256	Group 20		0 Success

This step is optional after you configure an IPsec service.

You specify the following settings to configure an IKE profile:

- **Name:** You use the name to identify the service.
- **IKE Version:** The options are IKE V1, IKE V2, or IKE FLEX. The selection depends on your business requirements.
- **Encryption Algorithm:** The encryption algorithm used during the Internet Key Exchange (IKE) negotiation.
- **Digest Algorithm:** The secure hashing algorithm used during the IKE negotiation.
- **Diffie-Hellman:** The cryptography schemes that the peer site and the NSX Edge instance use to establish a shared secret over an insecure communications channel.
- **SA Lifetime (sec):** The lifetime (in seconds) of the security associations (individual communicating peer identifiers) after which a renewal is required.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.

## 9-88 Configuring IPsec Profiles

The IPsec profile defines the security parameters used for negotiations to establish and maintain a secure tunnel between two peers. To configure the IPsec profile, you select **IPSEC PROFILES**.

The screenshot shows the 'VPN' management interface with the 'Profiles' tab selected. The 'Select Profile type:' dropdown is set to 'IPSEC PROFILES'. An 'ADD IPSEC PROFILE' button is visible. Below, a table lists the profile configuration for 'nsx-tunnel-profile'. The 'Encryption Algorithm' is 'AES GCM 128', the 'Digest Algorithm' is 'SHA256', and the 'PFS' toggle is enabled. The 'PFS Group' is 'Group 14'. The 'SA Lifetime (seconds)' is 3600. The 'Description' field is empty. The 'Tags' section shows a 'Tag' and 'Scope' dropdown. 'SAVE' and 'CANCEL' buttons are at the bottom.

Name	Encryption Algorithm	Digest Algorithm	PFS	PFS Group	Sessions	Status
nsx-tunnel-profile	AES GCM 128	Select Algorithms	<input checked="" type="checkbox"/>	Group 14		

SA Lifetime (seconds): 3600

Description:

Tags:  Tag  Scope

Max 30 allowed. Click (+) to add

This step is optional after you configure an IPsec service.

You provide values for the following settings to configure the IPsec profile:

- **Name:** You use the name to identify the service.
- **Encryption Algorithm:** The encryption algorithm used during the Internet Protocol Security (IPsec) negotiation.
- **Digest Algorithm:** The secure hashing algorithm used during the IPsec negotiation.
- **PFS Group:** This setting specifies the Perfect Forward Secrecy (PFS) group, which adds protection to the keys used for building secure channels. You can enable or disable this option.
- **SA Lifetime (sec):** The setting specifies the lifetime (in seconds) of the security associations (individual communicating peer identifiers) after which a renewal is required.
- **DF Bit:** This setting defines whether the encrypted traffic should copy the Don't Fragment (DF) bit from the inner payload to the encrypted traffic.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.

## 9-89 Adding a Local Endpoint

To add the local endpoint, you select **Local Endpoints**. This step is required in preparation for configuring an IPsec VPN session.

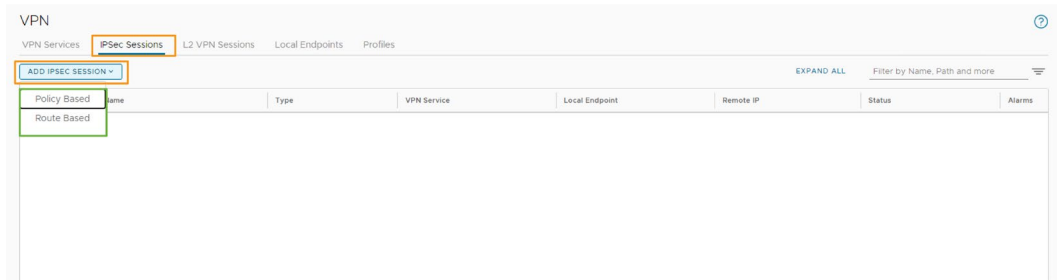
The screenshot shows the 'Local Endpoints' configuration page. At the top, there are tabs for 'VPN Services', 'IPSec Sessions', 'L2 VPN Sessions', 'Local Endpoints' (which is selected), and 'Profiles'. Below the tabs, there is a button 'ADD LOCAL ENDPOINT'. A table lists the endpoints with columns: Name, VPN Service, IP Address, Site Certificate, Sessions, and Status. The first row is highlighted with a green border and contains the values: 'vpn-01-endpoint', 'IPSec-VPN-01', '11.4.100', 'Select Certificate', and empty cells for Sessions and Status. Below the table, there are sections for 'Trusted CA / Self Signed Certificates', 'Local ID', 'Description', 'Certificate Revocation List', and 'Tags'. The 'Local ID' field is labeled 'Enter Local ID' and the 'Description' field is labeled 'Description'. There are 'SAVE' and 'CANCEL' buttons at the bottom left.

You provide values for the following settings to add the local endpoint:

- **Name:** You use the name to identify the local endpoint.
- **VPN Service:** This setting is the predefined service to use with this session.
- **IP Address:** The IP address of the local endpoint.
  - For an IPsec VPN service running on a Tier-0 gateway, the local endpoint IP address must be different from the Tier-0 gateway's uplink interface IP address.
  - For an IPsec VPN service running on a Tier-1 gateway, the route advertisement for IPsec local endpoints must be enabled in the Tier-1 gateway configuration.
- **Site Certificate:** Local site certificate, used for certificate-based authentication mode for the IPsec VPN session.
- **Trusted CA / Self Signed Certificates:** Remote site certificate, used for certificate-based authentication mode for the IPsec VPN session.
- **Certificate Revocation List:** A list of digital certificates that were revoked before their scheduled expiration date and should no longer be trusted.
- **Local ID:** Used for identifying the local NSX Edge instance. This local ID is the peer ID configured on the remote site. The local ID can be any string but is typically the public IP address of the VPN or a fully qualified domain name (FQDN) for the local VPN service.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.

## 9-90 Configuring IPsec VPN Sessions

You add an IPsec session to define the VPN type: either policy-based or route-based. You can find this configuration option by selecting **Networking > VPN > IPsec Sessions > ADD IPSEC SESSION**.



## 9-91 Configuring Policy-Based IPsec VPN Sessions (1)

When you select the policy-based option, IPsec tunnels are used to connect multiple local subnets that are behind the NSX Edge instance, with peer subnets on the remote VPN site.

The screenshot shows the NSX VPN configuration page for a "Policy-Based-Session". The interface includes a top navigation bar with tabs for "VPN Services", "IPSec Sessions" (selected), "L2 VPN Sessions", "Local Endpoints", and "Profiles". Below the navigation bar, there is a table listing VPN sessions. The "Policy-Based-Session" is highlighted, showing its details in a form below. The form includes fields for Name, Type, VPN Service, Local Endpoint, Remote IP, Status, Compliance Suite, Authentication Mode, Pre-shared Key, Remote ID, Description, Admin Status, Local Networks, Remote Networks, and Tags. The "Policy-Based-Session" is configured with the following settings:

Name	Type	VPN Service	Local Endpoint	Remote IP	Status
Policy-Based-Session	Policy Based	IPsec-VPN-01	vpn-01-endpoint	11.5.100	Enabled

Additional settings for the "Policy-Based-Session":

- Compliance Suite: None
- Authentication Mode: PSK
- Pre-shared Key: [Redacted]
- Remote ID: 11.5.100
- Description: [Empty field]
- Admin Status: Enabled
- Local Networks: 192.168.100.0/24
- Remote Networks: 2.2.5.0/24
- Tags: [Empty field]

To configure the policy-based IPsec session, you specify the following settings:

- **Name:** You use the name to identify the service when you need to use it.
- **Type:** This setting is already defined by the previous selection.
- **VPN Service:** This setting is the predefined service to use with this session.
- **Local Endpoint:** This setting is the earlier configured local endpoint for use with this configuration session.
- **Remote IP:** The setting specifies the IP address of the remote IPsec-capable gateway for building the secure connection.
- **Authentication Mode:** This setting defines whether to use the preshared key (PSK) or certificate-based connection authentication.
- **Local Networks** and **Remote Networks:** These settings define the interesting traffic that should be encrypted through this VPN session.
- **Pre-shared Key:** This setting specifies the string to define the key if the authentication mode is PSK.
- **Remote ID:** This setting defines the identifier of the remote peer for verifying the authenticity of the peering.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.



## 9-92 Configuring Policy-Based IPsec VPN Sessions (2)

In the **Advanced Properties** section, you select the predefined IKE, IPsec, and DPD profiles from the drop-down menus. You also define which side initiates the connection.

The screenshot displays the 'VPN' configuration page with the 'IPsec Sessions' tab selected. A table lists existing sessions, with 'Policy-Based-Session' highlighted. Below the table, the configuration details for this session are shown. The 'Advanced Properties' section is expanded, revealing dropdown menus for IKE, IPsec, and DPD profiles, all set to 'nsx-default-13vpn-ike-profile', 'nsx-default-13vpn-tunnel-profile', and 'nsx-default-13vpn-dpd-profile' respectively. The 'Connection Initiation Mode' is set to 'Initiator'.

VPN

VPN Services | **IPsec Sessions** | L2 VPN Sessions | Local Endpoints | Profiles

**ADD IPSEC SESSION** EXPAND ALL Filter by Name, Path and more

Name	Type	VPN Service	Local Endpoint	Remote IP	Status	Alarms
Policy-Based-Session	Policy Based	IPsec-VPN-01	vpn-01-endpoint	11.5.100 e.g. 10.10.10.10		

Compliance Suite: None

Authentication Mode: PSK

Pre-shared Key\*: .....

Remote ID: 11.5.100

Description: Description

Admin Status: ☒ Enabled

Local Networks: 192.168.100.0/24

Remote Networks: 2.2.5.0/24

Tags: Tag Scope

Max 30 allowed. Click (+) to add.

**Advanced Properties**

IKE Profiles: nsx-default-13vpn-ike-profile

IPsec Profiles: nsx-default-13vpn-tunnel-profile

DPD Profiles: nsx-default-13vpn-dpd-profile

Connection Initiation Mode: Initiator

TCP MSS Clamping: On Demand

Respond Only

**SAVE** CANCEL

## 9-93 Configuring Route-Based IPSec VPN Sessions

When you select the route-based option, tunneling is provided on traffic that is based on routes that were learned dynamically over a virtual tunnel interface (VTI).

The screenshot shows the 'VPN' configuration page with the 'IPSec Sessions' tab selected. A table lists the configured sessions, with 'Route-Based Session' highlighted. Below the table, the configuration details for this session are shown:

- Name:** Route-Based Session
- Type:** Route Based
- VPN Service:** IPSec-VPN-01
- Local Endpoint:** vpn-01-endpoint
- Remote IP:** 172.16.20.1
- Compliance Suite:** None
- Authentication Mode:** PSK
- Pre-shared Key:** (masked)
- Admin Status:** Enabled
- Tunnel Interface:** 192.168.5.1/24 (CIDR e.g. 10.22.11.2/23)
- Remote ID:** 172.16.20.1
- Tags:** (empty)

Buttons for 'SAVE' and 'CANCEL' are at the bottom left.

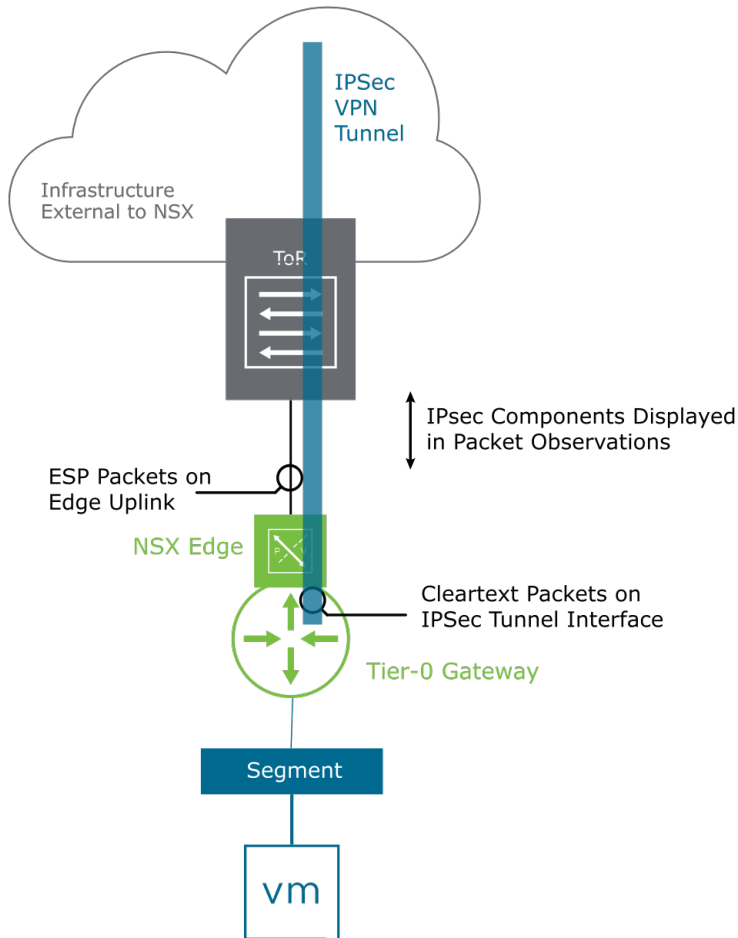
To configure a route-based IPSec session, you define the following settings:

- **Name:** You use the name to identify the service for later use.
- **Type:** This setting is already defined by the previous selection.
- **VPN Service:** This setting is the predefined service to use with this session.
- **Local Endpoint:** This setting defines an earlier configured local endpoint to use with this session configuration.
- **Remote IP:** This setting defines the IP address of the remote IPSec-capable gateway for building the secure connection.
- **Compliance suite:** You can specify a security compliance suite such as CNSA, FIPS, Foundation, PRIME, or Suite-B to configure the security profiles used for an IPSec VPN session.
- **Authentication Mode:** This setting defines whether to use a preshared key (PSK) or certificate-based connection authentication.
- **Admin Status:** This setting enables and disables the service.
- **Tunnel Interface:** This setting defines the IP address of the local virtual tunnel interface (VTI) that is created to use with this session.
- **Pre-shared Key:** This setting provides the string for defining the key if the authentication mode is PSK.
- **Remote ID:** This setting specifies the identifier of the remote peer for verifying the authenticity of the peering.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.

## 9-94 Traceflow and Live Traffic Analysis Support for VPN

NSX 4.0.0.1 introduces the following enhancements to observe live packets in a VPN tunnel:

- IPsec components are displayed in packet observations in Traceflow and Live Traffic Analysis.
- You can observe the ESP packets on a Tier-0 uplink interface in Live Traffic Analysis.
- You can observe the cleartext packets on an IPsec Tunnel interface.



## 9-95 Review of Learner Objectives

- Explain how IPSec-based technologies are used to establish VPNs
- Compare policy-based and route-based IPSec VPN
- Describe IPSec VPN requirements in NSX
- Create and configure IPsec VPN tunnels
- Identify Traceflow and Live Traffic Analysis enhancements for VPN tunnels

## 9-96 Lesson 5: L2 VPN

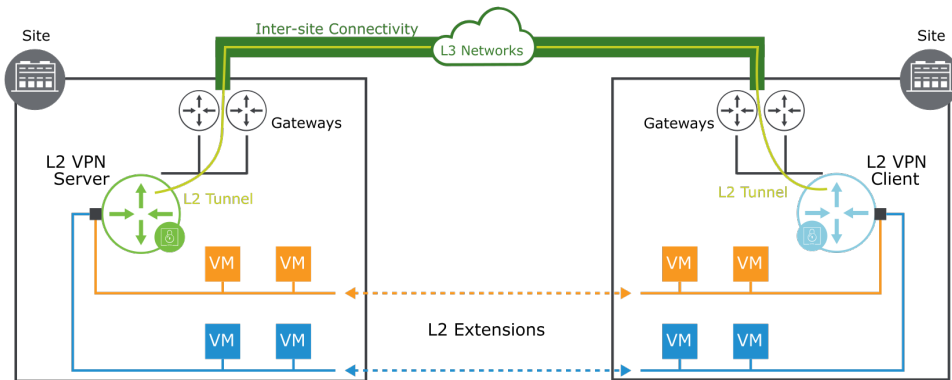
### 9-97 Learner Objectives

- Describe L2 VPN technologies in NSX
- Identify various supported L2 VPN endpoints
- Create and configure L2 VPN secure connections

## 9-98 About Layer 2 VPN

Layer 2 VPN connectivity enables you to extend L2 networks across data centers securely.

- Extends L2 networks (overlay-backed segments and VLAN-backed segments) across sites on the same broadcast domain
- Enables VM mobility, such as vSphere vMotion migration and disaster recovery without IP address changes
- Enables hybrid cloud solutions



L2 tunnels are established between L2 VPN endpoints that are interconnected over L3 networks.

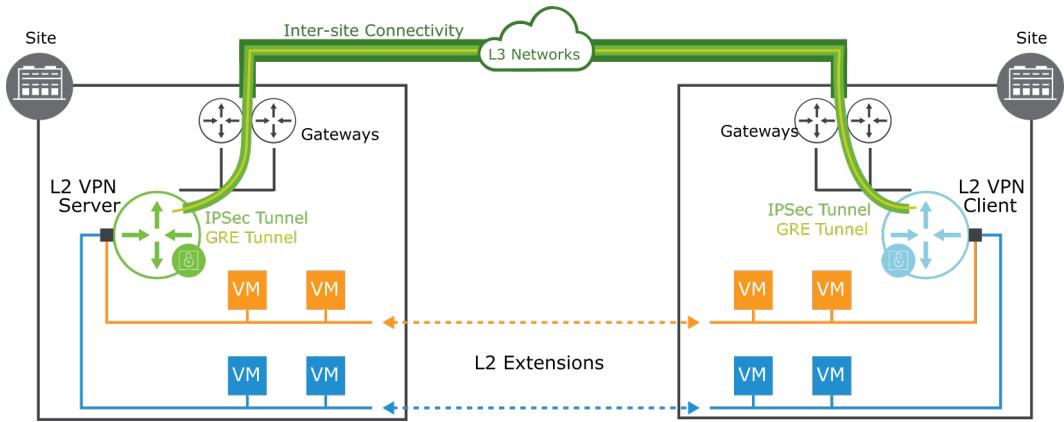
The NSX L2 VPN architecture includes:

- L2 VPN server: The client is connected to this destination.
- L2 VPN client: This source initiates communication with the destination L2 VPN server.

## 9-99 L2 VPN Architecture

NSX L2 VPNs are established using the following layers of encapsulation:

- An outer Internet Protocol Security (IPSec) tunnel to provide secure encrypted communication
- An inner Generic Routing Encapsulation (GRE) tunnel to support multicast traffic

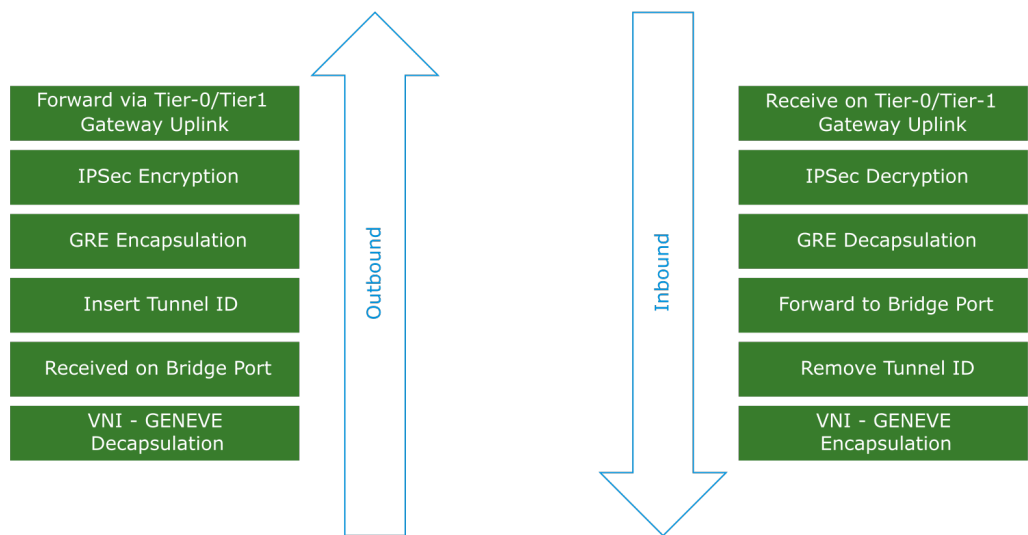


Combined, GRE tunnels over IPSec provide the secure extension of multicast traffic between sites, required to stretch an L2 broadcast domain. On their own:

- IPsec tunnels are unable to support multicast traffic
- GRE tunnels are not secure

# 9-100 L2 VPN Edge Packet Flow

The inbound and outbound L2 VPN Edge packet flows illustrate the sequence of operations that includes GRE and IPsec tunneling.



For outbound L2 VPN traffic (traffic from the internal network behind the edge node) that is destined for any remote L2 network, the first step is to decapsulate the Geneve frames. The destination address of the internal frame designates whether traffic goes through the local bridge port toward remote sites or is locally managed. Further steps are inserting the ID for the proper VLAN and sending the traffic to the local VTI interface to encapsulate into GRE, which gets protected by IPsec and is forwarded to any given destination.

In the inbound direction, when receiving L2 VPN traffic that is identified by the IPsec engine, the traffic requires IPsec decryption first and GRE decapsulation. After being sent to the bridge interface, traffic is sent to local networks. The required Geneve encapsulation parameters are based on the actual tunnel IDs for the traffic.



## 9-101 L2 VPN Considerations

When deploying L2 VPN, you must consider several important points:

- L2 VPN services are supported on both Tier-0 and Tier-1 gateways.
- Segments can be connected to either Tier-1 or Tier-0 gateways to use L2 VPN services.
- Only one L2 VPN service (either client or server) can be configured for either Tier-0 or Tier-1 gateway.
- An L2 VPN session can extend up to 512 L2 segments.

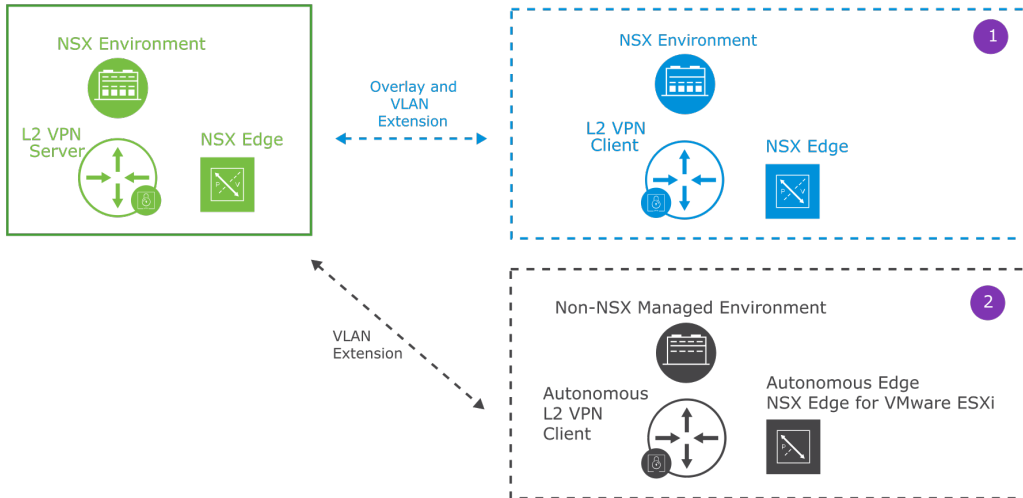


In NSX, layer 2 VPN has the following additional characteristics:

- The hub-and-spoke topology is supported.
- Tunnel redundancy is not supported. L2 VPN relies on edge high availability.
- L2 VPN interoperability is available only in NSX and does not support third-party interoperability.
- The supported number of L2 VPN server and client sessions depends on the size and type of the edge node. To review recommended L2 VPN configuration limits, see the VMware Configuration Maximums tool at <https://configmax.vmware.com/home>.

## 9-102 Recommended L2 VPN Clients

The following L2 VPN clients are supported:



The following L2 VPN clients are recommended:

1. NSX Managed NSX Edge in a separate NSX Managed environment.
  - Overlay and VLAN segments can be extended.
2. Autonomous Edge:
  - Enables L2 VPN access from a non-a NSX environment to NSX environments.
  - Deployed by using an OVF file on a host that is not managed by NSX.
  - Only VLAN segments can be extended.

Additional L2 VPN Client details including the supported software versions are available in the NSX Administration Guide at <https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-86C8D6BB-F185-46DC-828C-1E1876B854E8.html>.

## 9-103 About Autonomous Edge

Autonomous edge has the following characteristics:

- Is deployed by using an OVF file on a host that is not managed by NSX
- Extends VLAN-backed segments
- Acts as an NSX Edge gateway, which can be deployed on on-premises data centers and public clouds (for example, Amazon AWS and Microsoft Azure)
- Runs independently without the management plane/central control plane installed in the NSX domain
- Is powered with the high-performing Data Plane Development Kit (DPDK)

vm NSX Autonomous Edge

SUMMARY

PORT

L2VPN

BACKUP/RESTORE

UPGRADE

REFRESH

Appliance

Management Address

172.20.10.70/19

API Server Role

PRIMARY

Total Memory / Used

8160.204 MB / 87.08%

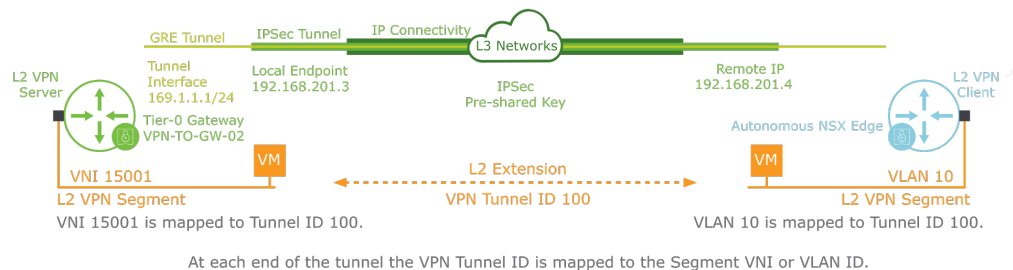
CPU Cores / Load

4 / 1.20%

# 9-104 Sample L2 VPN Network Topology

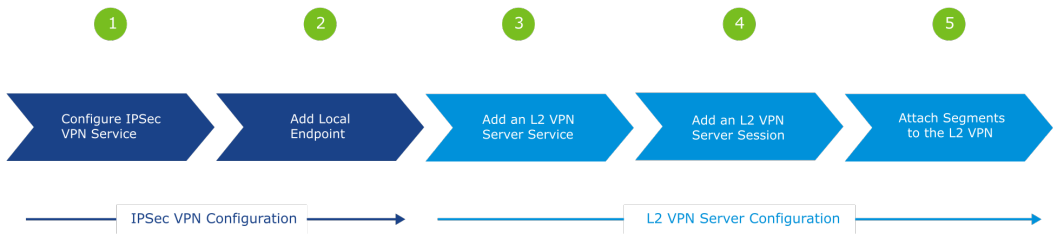
This sample L2 VPN network topology and IP addressing assignments serve as a guide to illustrate parameters used in the L2 VPN configuration steps.

Sample L2 VPN Network Topology Diagram



# 9-105 L2 VPN Server Workflow

The L2 VPN Server uses the IPsec features of the gateway. To configure an L2 VPN server, you must first configure a supporting IPsec VPN and then an L2 VPN.



## 9-106 Configuring an IPsec VPN Service

To configure the IPsec VPN service to be used for L2 VPN, you select **Networking > VPN > VPN Services > ADD SERVICE > IPsec**, to associate the service with a Tier-0 or Tier-1 gateway.

The screenshot shows the 'VPN' configuration page with the 'VPN Services' tab selected. The 'ADD SERVICE' button is highlighted. Below it, a table lists the configured services. The first service is 'IPsec-for-L2VPN-Service' with 'IPsec' as the Service Type and 'VPN-T0-GW-02' as the Tier-0/Tier-1 Gateway. The configuration details for this service are shown below the table: Admin Status is 'Enabled', Session Sync is 'Enabled', and there is a description field. The IKE Log Level is set to 'Info'. There are also tags and a global bypass rules section. A note at the bottom states: 'NOTE - Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save.' The 'SAVE' button is highlighted.

Name	Service Type	Tier-0/Tier-1 Gateway	Sessions	Status	Alarms
IPsec-for-L2VPN-Service	IPsec	VPN-T0-GW-02	Set		

Admin Status: ☒ Enabled

Session Sync: ☒ Enabled

Description:

IKE Log Level: Info

Tags:  Tag  Scope

Max 30 allowed. Click (+) to add.

> Global Bypass Rules

NOTE - Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save.

**SAVE** CANCEL

To configure the IPsec for L2 VPN service, you provide values for the following options:

- **Name:** You use this name to identify the IPsec for L2 VPN service.
- **Service Type:** IPsec has been selected.
- **Tier-0/Tier-1 Gateway:** Specify the gateway for the service.
- **Admin Status:** To enable or disable the IPsec for L2 VPN session.
- **Session Sync:** To enable or disable the stateful synchronization of the IPsec for L2 VPN session.
- **IKE Log Level:** The Internet Key Exchange log level. The default is Info level.
- **Tags:** Enter a value for Tags if you want to include this service in a tag group.
- **Global Bypass Rules:** Enter the list of local and remote subnets between which IPsec protection is bypassed.

## 9-107 Adding a Local Endpoint

To add the IPsec endpoint to be used for L2 VPN, you select **Networking > VPN > Local Endpoints**. You click **ADD LOCAL ENDPOINT** to define the local side of the IPsec connection.

The screenshot shows the 'Local Endpoints' configuration page. At the top, there are tabs for 'VPN Services', 'IPsec Sessions', 'L2 VPN Sessions', 'Local Endpoints' (which is selected), and 'Profiles'. Below the tabs is a table with columns: Name, VPN Service, IP Address, Site Certificate, Sessions, and Status. A new endpoint is being added with the following values: Name: 'IPsec-for-L2VPN-Local-Endpoint', VPN Service: 'IPsec-for-L2VPN-Ser...', IP Address: '192.168.201.3', and Local ID: '192.168.201.3'. The 'ADD LOCAL ENDPOINT' button is highlighted. Below the table, there are sections for 'Trusted CA / Self Signed Certificates', 'Certificate Revocation List', and 'Tags'. The 'Local ID' field is set to '192.168.201.3'. The 'Tags' section has a 'Tag' field and a 'Scope' dropdown.

To add the local endpoints, you provide values for the following options:

- **Name:** You use this name to identify the local endpoints.
- **VPN Service:** This setting specifies which IPsec VPN service to use with the endpoint.
- **IP Address:** This setting is the IPsec tunnel local endpoint IP address.
- **Site Certificate:** You use this setting with certificate-based authentication to specify which certificate to use with this endpoint.
- **Trusted CA / Self Signed Certificate:** A public key certificate.
- **Local ID:** This setting specifies the IPsec ID of the local side. The local ID is usually the same as the local IP address.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.

## 9-108 Adding an L2 VPN Server Service

To add the L2 VPN Server service, you select **Networking > VPN > VPN Services**. To begin, you click **ADD SERVICE** and select **L2 VPN Server** to define an L2 VPN Server service.

The screenshot shows the 'VPN Services' configuration page. The 'VPN Services' tab is selected, and the 'ADD SERVICE' button is highlighted. The configuration form is as follows:

Name	Service Type	Tier-0/Tier-1 Gateway	Sessions	Status	Alarms
L2VPN-Server-Service *	L2 VPN Server	VPN-TO-GW-02	Set		

Below the table, the 'Hub & Spoke' toggle is set to 'Disabled'. There is a 'Description' text box and a 'Tags' section with a 'Tag' and 'Scope' dropdown. A note at the bottom states: 'NOTE - Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save.' At the bottom of the form are 'SAVE' and 'CANCEL' buttons.

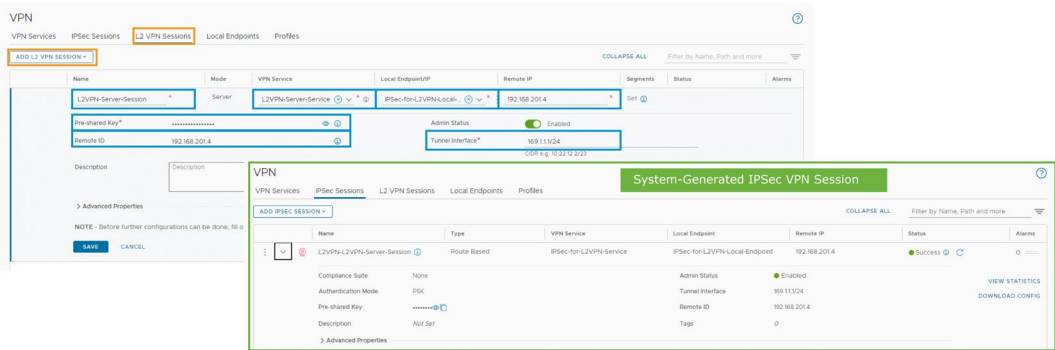
To add the L2 VPN server service, you provide values for the following options:

- **Name:** You use this name to identify the L2 VPN server service.
- **Service Type:** L2 VPN Server has been selected.
- **Tier-0/Tier-1 Gateway:** Specify the gateway for the service.
- **Sessions:** To apply an L2 VPN server session to this L2 VPN server service.
- **Hub & Spoke:** By default, the value is set to Disabled, which means the traffic received from the L2 VPN clients is only replicated to the segments connected to the L2 VPN server. If this property is set to Enabled, the traffic from any L2 VPN client is replicated to all other L2 VPN clients.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.

# 9-109 Adding an L2 VPN Server Session

To add the L2 VPN Server session, you select **Networking > VPN > L2 VPN Sessions**. You click **ADD L2 VPN SESSION** to complete the L2 VPN Server configuration.

A system-generated IPsec VPN session supports the L2 VPN session.



To add the L2 VPN session, you provide values for the following options:

- **Name:** You use this name to identify the L2 VPN session.
- **Mode:** Server has been selected.
- **VPN Service:** This setting specifies which L2 VPN server service to use with this L2 VPN session.
- **Local Endpoint/IP:** This setting specifies which local endpoint to use with this L2 VPN session.
- **Remote IP:** The IP address of the client-side IPsec tunnel endpoint.
- **Segments:** Used to connect logical segments to this L2 VPN server service.
- **Pre-shared Key:** A shared secret common to both L2 VPN client and the L2 VPN server configurations.
- **Admin Status:** To enable or disable the L2 VPN server session.
- **Remote ID:** This setting specifies the IPsec ID of the remote side. The remote ID is usually the same as the remote IP address.
- **Tunnel Interface:** The IP address of the server-side GRE tunnel endpoint.
- **Tags:** For cloud-based installations, almost every entity can hold a tag.



# 9-110 Attaching Segments to the L2 VPN (1)

You identify the segments that should be extended through the L2 VPN tunnels. You can click the vertical ellipsis icon to edit an existing segment or create a segment.

You can optionally configure a local egress gateway IP so that all VMs on the segment use it as their default gateway.

Segments

NSX Distributed Port Groups Profiles

ADD SEGMENT EXPAND ALL Filter by Name, Path and more

Name	Connected Gateway	Transport Zone	Subnets	Ports / Interfaces	Status	Alarms
L2VPN-Segment *	None *	PROD-Overlay-TZ	<div>Gateway CIDR IPv4 CIDR e.g. 10.22.12.2/23</div> <div>Gateway CIDR IPv6 CIDR e.g. fc7e:f206:db42::1/48</div> <div>SET DHCP CONFIG</div>			

Admin State ☒

L2 VPN

Segment needs to have either Subnets or VPN defined, or both.

L2 VPN

VPN Tunnel ID \*

Additional Settings

Description

Local Egress Gateway IP

Enter IP Address

Tags

Tag Scope

NOTE - Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save

SEGMENT PROFILES

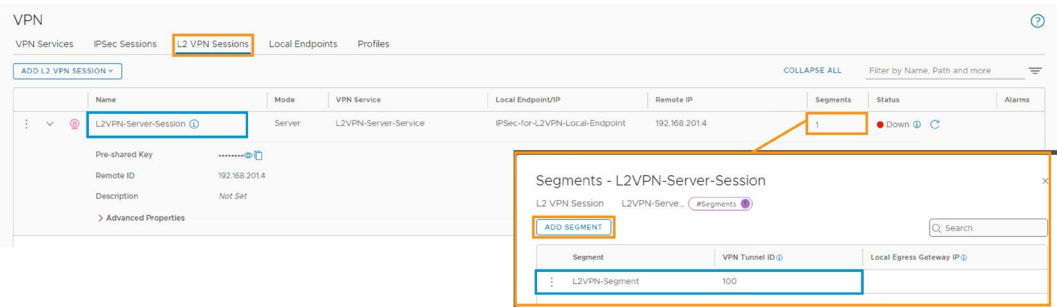
SAVE CANCEL

When you attach the L2 VPN segments, the following key settings are available:

- L2 VPN:** This setting defines the previously configured L2 VPN session. The segment that is defined is used through that session.
- VPN Tunnel ID:** This number is used to identify the communicating local and remote L2 networks. The same ID on both sides means that they are on the same L2 broadcast domain.
- Local Egress Gateway IP:** The IP address of the local gateway that the VMs on the segment use as their default gateway. The same IP address can be configured in the remote site on the extended segment.

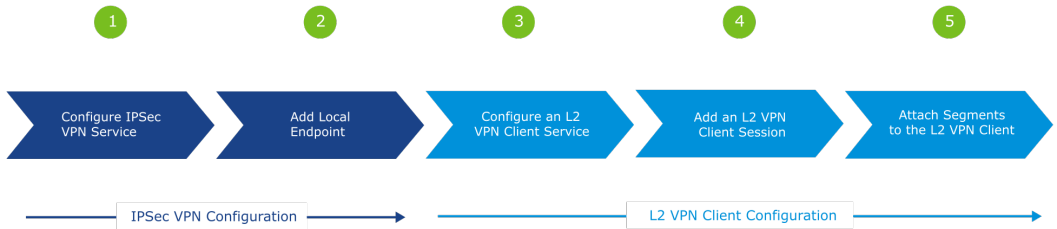
# 9-111 Attaching Segments to the L2 VPN (2)

You can also attach segments on the L2 VPN Session page. After selecting the edit mode and clicking **SEGMENTS**, you can add segments and define the tunnel ID for each segment.



# 9-112 L2 VPN Client Workflow

Perform the following steps to deploy an L2 VPN Client.



For steps 1 and 2, follow the L2 VPN server configuration steps, switching local and remote endpoint IPs.

## 9-113 Configuring an L2 VPN Client Service

To configure an L2 VPN Client service, you select **Networking > VPN > VPN Services**. To begin, you click **ADD SERVICE** and select **L2 VPN Client** to define an L2 VPN Client service.

The screenshot shows the 'VPN Services' configuration page in the NSX interface. The 'VPN Services' tab is selected, and the 'ADD SERVICE' button is highlighted. Below the tabs, there is a table with columns: Name, Service Type, Tier-0/Tier-1 Gateway, Sessions, Status, and Alarms. The 'Name' field is filled with 'L2-VPN-Client-Service', the 'Service Type' is 'L2 VPN Client', and the 'Tier-0/Tier-1 Gateway' is 'VPN-T0-GW-01'. The 'Sessions' column has a 'Set' link. Below the table, there is a 'Description' field and a 'Tags' section with a 'Tag' and 'Scope' dropdown. A note at the bottom states: 'NOTE - Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save.' There are 'SAVE' and 'CANCEL' buttons at the bottom.

Name	Service Type	Tier-0/Tier-1 Gateway	Sessions	Status	Alarms
L2-VPN-Client-Service *	L2 VPN Client	VPN-T0-GW-01	Set		

NOTE - Before further configurations can be done, fill out mandatory fields ( \* ) above and click Save.

SAVE CANCEL

To configure the L2 VPN Client service, you provide values for the following options:

- **Name:** You use this name to identify the L2 VPN client service.
- **Service Type:** L2 VPN client has been selected.
- **Tier-0/Tier-1 Gateway:** Specify the gateway for the service.
- **Tags:** For grouping NSX objects.

## 9-114 Adding an L2 VPN Client Session (1)

Before creating an L2 VPN Client session, you must obtain or download the peer code from the L2 VPN server.

**VPN**

VPN Services    IPSec Sessions    **L2 VPN Sessions**    Local Endpoints    Profiles

+ ADD L2 VPN SESSION ▼

COLLAPSE ALL    Filter by Name, Path and more

Name	Mode	VPN Service	Local Endpoint/IP	Remote IP	Segments	Status	Alarms
L2VPN-Server-Session ⓘ	Server	L2VPN-Server-Service	IPSec-for-L2VPN-Local-Endpoint	192.168.201.4	1	Down ⓘ ⌂	1 🚩
Pre-shared Key		Admin Status		Enabled			
Remote ID		Tunnel Interface		169.111/24			
Description		Tags		0			
<a href="#">VIEW STATISTICS</a>							
<a href="#">DOWNLOAD CONFIG</a>							
<a href="#">Advanced Properties</a>							

```

{
  "transport_tunnel_path": "/infra/tier-0s/VPN-T0-GW-02/ipsec-vpn-services/IPSec-for-L2VPN-Server/sessions/L2VPN-L2VPN-Server-Session_",
  "peer_config": {
    "id": "H5tsc2l0ZUshbmU0IjMwMTQzOTI1MTkxODV2c2v2vb1tImlhY1RheEJwIjoIMTY5LSJlNC42Hk4YiIiwzMHV0VGRwSXA0IiwkaXNjaXUybnV0eGxhcCI6ImV0Y3F5cHRBbmRpdWkiLCQ0I0IjZXMtZW50YSByNTY1LCAuc2s0IjMtTXdhcmx1V2NDZFY2FhIiwidmVubV5scyIGw3SiibG93IEt5MzJCIEt5MS4xNjauMjAxLjQ1LCA3ZnVySWQ0I0I0OT10MTYALjIwMS42IiwibG93YXNkdW1jCCTGI6JE20SA4tJEUMiByNCJ9XK0..."
  }
}

```

The peer code is a Base64-encoded configuration string that is available from the L2 VPN server through the **DOWNLOAD CONFIG** option or through a REST API call.

## 9-115 Adding an L2 VPN Client Session (2)

You configure the local and remote IP addresses and the peer code, which was retrieved in a previous step. You can also click the **Admin Status** toggle to enable or disable the session.

The screenshot shows the 'L2 VPN Sessions' configuration page. At the top, there are tabs for 'VPN Services', 'IPSec Sessions', 'L2 VPN Sessions' (which is selected), 'Local Endpoints', and 'Profiles'. Below the tabs is a button 'ADD L2 VPN SESSION' and a link 'EXPAND ALL'. A table lists the sessions with columns: Name, Mode, VPN Service, Local Endpoint/IP, Remote IP, Segments, Status, and Alarms. One session is listed: 'L2VPN-Client-Session' with Mode 'Client', VPN Service 'L2-VPN-Client-Service', Local Endpoint/IP '192.168.201.4', and Remote IP '192.168.201.3'. Below the table, the 'Peer Configuration' section shows a text area with a peer code: 'c30i0JhZXM122N1L3NoY80yNTYtLCJwC2p0UjWTXdhcmUxiVZNq2FyZTEhliwidHVubmVscyl6W3si69jYWxjZC6gE5M4NjguMjAxLjQlLCJwZWVvYy5WQl0ixOTluMTY4LjwM54z2wibG9jYWxWdGJCC6gE2OS4xLjUuM8yNCj9XX0w'. The 'Admin Status' toggle is set to 'Enabled'. At the bottom, there are buttons for 'SAVE', 'CANCEL', and 'Unsaved Changes'.

Name	Mode	VPN Service	Local Endpoint/IP	Remote IP	Segments	Status	Alarms
L2VPN-Client-Session	Client	L2-VPN-Client-Service	192.168.201.4	192.168.201.3	Set	Enabled	

Peer Configuration: c30i0JhZXM122N1L3NoY80yNTYtLCJwC2p0UjWTXdhcmUxiVZNq2FyZTEhliwidHVubmVscyl6W3si69jYWxjZC6gE5M4NjguMjAxLjQlLCJwZWVvYy5WQl0ixOTluMTY4LjwM54z2wibG9jYWxWdGJCC6gE2OS4xLjUuM8yNCj9XX0w

Admin Status: Enabled

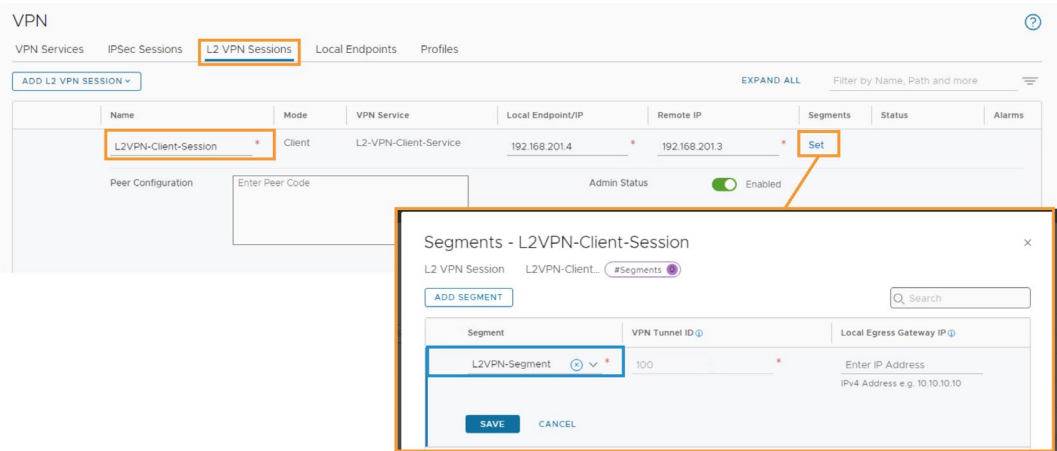
SAVE CANCEL | Unsaved Changes

To configure the L2 VPN client session, you provide values for the following options:

- **Name:** You use this name to identify the L2 VPN client session.
- **Mode:** Client has been selected.
- **VPN Service:** This setting specifies which L2 VPN client service to use with this L2 VPN session.
- **Local Endpoint/IP:** This setting specifies which L2 VPN client local endpoint to use with this L2 VPN session.
- **Remote IP:** The IP address of the server-side IPsec tunnel endpoint.
- **Peer Configuration:** The peer code downloaded from the L2 VPN server.
- **Admin Status:** To enable or disable the L2 VPN client session.

# 9-116 Attaching Segments to the L2 VPN Client

On the Set Segments page, you define the network and the tunnel ID. The same configuration is also available by selecting the **SEGMENTS** option.



## 9-117 Lab 19: Deploying Virtual Private Networks

Configure the VPN tunnel and verify the operation:

1. Prepare for the Lab
2. Deploy a New NSX Edge Node to Support the VPN Deployment
3. Configure a New Edge Cluster
4. Deploy and Configure a New Tier-0 Gateway and Segments for VPN Support
5. Create an IPSec VPN Service
6. Create an L2 VPN Server and Session
7. Configure a Predeployed Autonomous Edge as an L2 VPN Client
8. Verify the Operation of the VPN Setup

## 9-118 Review of Learner Objectives

- Describe L2 VPN technologies in NSX
- Identify various supported L2 VPN endpoints
- Create and configure L2 VPN secure connections

## 9-119 Key Points (1)

- NAT can be configured on Tier-0 and Tier-1 gateways.
- Typically, source translation is used to change a private address to a public address for packets leaving your network.
- Typically, destination translation is used to redirect incoming packets with a destination of a public address to a private IP address in your network.
- Reflexive NAT can be used when a Tier-0 gateway runs in stateless active-active mode with asymmetric traffic paths.
- Tier-0 and Tier-1 gateways in stateful active-active mode support stateful services including SNAT and DNAT.
- The NAT64 mechanism translates IPv6 packets to IPv4 packets.
- DHCP is a standard networking protocol for dynamically distributing network configuration parameters, such as IP addresses for interfaces.
- A DNS is a computer application that implements a service for resolving a computer name to an IP address.

## 9-120 Key Points (2)

- Since NSX 4.0.0.1 the configuration of NSX Advanced Load Balancer using the NSX UI and NSX API is deprecated. Network administrators should configure load-balancers integrated with NSX environments directly through the NSX Advanced Load Balancer UI or API.
- NSX Advanced Load Balancer includes multiple components such as virtual IP address, virtual service, and a server pool with associated health and monitor profiles.
- IPSec VPN services are available on Tier-0 gateways to interconnect different IP networks.
- Using the GRE over IPSec, L2 VPN tunnels can be used to extend layer 2 networks.

Questions?



# Module 10

## NSX User and Role Management

### 10-2 Importance

You must manage users and roles to enforce the least user privilege and provide clear separation of duties. By integrating NSX with VMware Identity Manager or LDAP, you can configure role-based access control (RBAC) for external users.

### 10-3 Module Lessons

1. Integrating NSX with VMware Identity Manager
2. Integrating NSX with LDAP
3. Managing Users and Configuring RBAC

## 10-4 Lesson 1: Integrating NSX with VMware Identity Manager

### 10-5 Learner Objectives

- Describe the purpose of VMware Identity Manager
- Identify the benefits of integrating NSX with VMware Identity Manager
- Configure the integration between NSX and VMware Identity Manager
- Verify the integration between NSX and VMware Identity Manager

## 10-6 About VMware Identity Manager

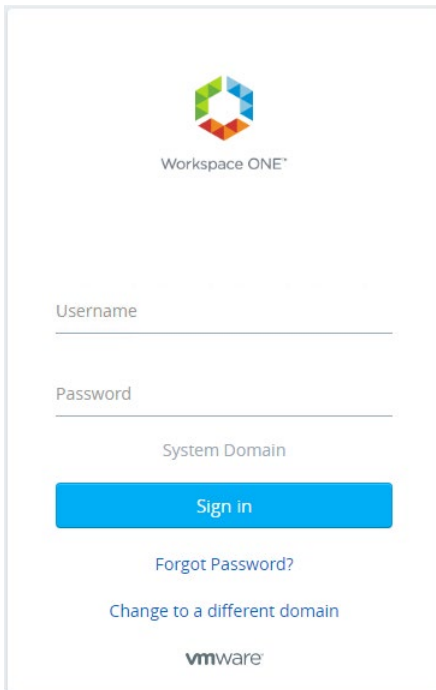
VMware Identity Manager is an identity as a service (IDaaS) solution.

VMware Identity Manager provides the following services for software as a service (SaaS), web, cloud, and native mobile applications:

- Application provisioning
- Conditional access controls
- Single sign-on (SSO)

VMware products can use VMware Identity Manager as an enterprise SSO solution.

VMware Identity Manager is based on the OAuth 2.0 authorization framework.



Workspace ONE\*

Username

Password

System Domain

Sign in

[Forgot Password?](#)

[Change to a different domain](#)

vmware

To verify the version compatibility between NSX and VMware Identity Manager, use the VMware Product Interoperability Matrix at <https://interopmatrix.vmware.com/Interoperability>.

VMware Identity Manager is now offered as Workspace ONE Access.

## 10-7 Benefits of Integrating VMware Identity Manager with NSX

The integration of VMware Identity Manager with NSX provides the following benefits related to user authentication:

- Support for extensive authentication, authorization, and accounting (AAA) systems, including:
  - RADIUS
  - Smart cards and common access cards
  - RSA SecureID
  - LDAP and OpenLDAP based on Active Directory (AD)
- Enterprise SSO:
  - Common authentication platform across multiple VMware solutions
  - Seamless SSO experience

NSX has its own native LDAP and Active Directory integration, but VMware Identity Manager also offers this capability.

## 10-8 Prerequisites for VMware Identity Manager Integration

The following prerequisites must be met before integrating VMware Identity Manager with NSX:

1. Deploy the VMware Identity Manager appliance from an OVF template.
2. Configure time synchronization for the VMware Identity Manager virtual machine.
3. Perform an initial configuration of the VMware Identity Manager appliance.

The screenshot shows the VMware Identity Manager Setup Wizard interface. At the top is a blue header with the VMware logo on the left and 'Welcome Admin | ? Help | Log out' on the right. On the left side, there is a vertical navigation pane with four steps: 'Get Started' (checked), 'Set Passwords' (checked), 'Select Database' (active, highlighted with a blue circle), and 'Setup Review'. The main content area is titled 'Select Database'. It contains the following fields and options: 'Database Type' with radio buttons for 'Internal Database' (selected) and 'External Database'; a 'JDBC URL' text input field with a link below it that says 'Consult documentation for supported JDBC URLs'; 'Database Username' and 'Database Password' text input fields; and a 'Test Connection' button. At the bottom right of the main area are two buttons: 'Go Back' and 'Continue'.

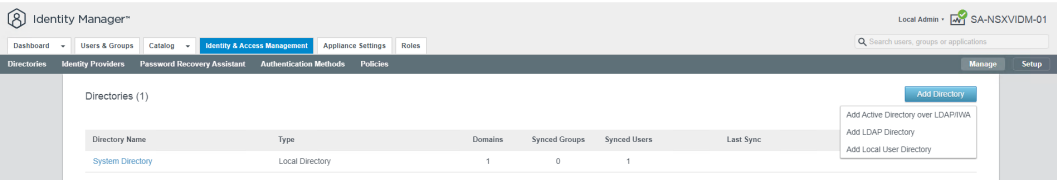
The following steps must be completed before integrating VMware Identity Manager with NSX:

1. From the vSphere Client, deploy the VMware Identity Manager appliance from an OVF template.
2. Synchronize the VMware Identity Manager virtual machine time with the ESXi host where it is running.
  - a.. Right-click the VM and select **Edit Settings > VM Options**.
  - b.. Scroll down to the Time section and select the **Synchronize guest time with host** check box.
3. After deploying the VMware Identity Manager appliance, use the Setup wizard available at [https://<VMware\\_Identity\\_Manager\\_FQDN>](https://<VMware_Identity_Manager_FQDN>).
  - a.. Set passwords for the admin, root, and remote SSH user.
  - b.. Select a database.

# 10-9    Configuring VMware Identity Manager

After the initial setup, connect to the VMware Identity Manager administration console. In the console, you configure the following settings:

- Identity sources
- Authentication methods
- Access policies



You can access the VMware Identity Manager Administration console at [https://<VMware\\_Identity\\_Manager\\_FQDN>:443/SAAS/admin](https://<VMware_Identity_Manager_FQDN>:443/SAAS/admin).

The following identity sources are supported in VMware Identity Manager:

- Active Directory (AD) over LDAP or AD with integrated Windows authentication
- LDAP
- Local directory

To configure authentications methods, select **Identity & Access Management > Authentication Methods**.

To define access policies, select **Identity & Access Management > Policies**.

Administrators can configure rules that specify the network ranges and types of devices that users can use to sign in.

## 10-10 Overview of the VMware Identity Manager and NSX Integration

After both NSX and VMware Identity Manager appliances are deployed and configured, you can integrate these components:

1. Create an OAuth client for NSX in VMware Identity Manager.
2. Obtain the SHA-256 certificate thumbprint for the VMware Identity Manager appliance.
3. Configure the VMware Identity Manager details in NSX.

## 10-11 Creating an OAuth Client

Before enabling the integration of VMware Identity Manager and NSX, you must register NSX as a trusted OAuth client in VMware Identity Manager:

1. From the VMware Identity Manager administration console, click the **Catalog** tab.
2. Select **Settings > Remote App Access**.
3. On the Clients page, click **Create Client**.

The screenshot displays the VMware Identity Manager administration console. The top navigation bar includes 'Dashboard', 'Users & Groups', 'Catalog', 'Identity & Access Management', 'Appliance Settings', and 'Roles'. The 'Catalog' tab is selected. On the left, the 'Global Catalog Settings' sidebar shows 'Remote App Access' as the active section. The main content area is titled 'Remote App Access' and contains a 'Clients' tab. A 'Create Client' dialog box is open, showing the following fields:

- Access Type**: Service Client Token
- Client ID**: sa-nsxmgr-01-OAuthClient
- Scope**: admin
- Shared Secret**: khkzCtCteBwVJSA5ggv7n0FOnkysFYqvMvqAT4NfuzUwV
- Issue Refresh Token**: ☒ Refresh Token
- Token Type**: Bearer
- Access Token Time-To-Live (TTL)**: 3 hours
- Refresh Token Time-To-Live (TTL)**: 90 days (1 day is 24 hours)
- Idle Token Time-To-Live (TTL)**: 4 days (1 day is 24 hours)

The dialog box also includes a 'Generate Shared Secret' button and a 'Create Client' button. The background shows a list of existing clients with columns for Client ID, Name, and Actions.

VMware Identity Manager uses the OAuth 2.0 authorization framework to enable NSX and its users to access specific data and services.

Before enabling the integration between VMware Identity Manager and NSX, you must register NSX as a trusted OAuth client in VMware Identity Manager.

When configuring NSX details, you select **Service Client Token** from the **Access Type** drop-down menu. This selection indicates that the application, NSX in this example, accesses the APIs for itself. The application does not access the APIs for a particular user.

You must specify a client ID to uniquely identify NSX. You need this value to enable the VMware Identity Manager integration.

You must also click **Generate Shared Secret**. You need this value to enable the VMware Identity Manager integration.

Leave the default settings for all other options.

On the Create Client page, you can optionally set the token time-to-live values by specifying the access, refresh, and idle timers.

## 10-12 Obtaining the SHA-256 Certificate Thumbprint

Before you configure the integration between NSX and VMware Identity Manager, you must obtain the SHA-256 certificate thumbprint of the VMware Identity Manager appliance:

1. Use SSH to log in to the VMware Identity Manager appliance.
2. Run the `sudo -s` command to gain root access.
3. Navigate to the VMware Identity Manager configuration directory.

```
cd /usr/local/horizon/conf
```

4. Retrieve the SHA-256 certificate thumbprint of VMware Identity Manager.

```
openssl x509 -in sa-nsxvidm-01.vclass.local_cert.pem -noout  
-sha256 -fingerprint
```

You need the SHA-256 certificate thumbprint value when you enable the VMware Identity Manager integration.

Use SSH to log in to the VMware Identity Manager appliance with user `sshuser`.



## 10-13 Configuring the VMware Identity Manager Details in NSX

To enable the VMware Identity Manager integration from the NSX UI:

1. Select **System > Settings > User Management > Authentication Providers**.
2. Click the **VMware Identity Manager** tab.
3. Click **EDIT**.
4. Provide the configuration information and click **SAVE**.

### Edit VMware Identity Manager Configuration ×

External Load Balancer Integration	<input type="checkbox"/> Disabled
VMware Identity Manager Integration	<input checked="" type="checkbox"/> Enabled
VMware Identity Manager Appliance	<div>sa-nsxvidm-01.vclass.local *</div> <div>Enter Fully Qualified Domain Name (FQDN) e.g. identity.domain.com</div>
OAuth Client ID	<div>sa-nsxmgr-01-OAuthClient *</div>
OAuth Client Secret	<div>..... *</div>
SSL Thumbprint	<div>SHA256 Fingerprint=34:07:CE:47:A9:E *</div>
NSX Appliance	<div>sa-nsxmgr-01.vclass.local *</div> <div>Fully Qualified Domain Name (FQDN) is recommended e.g. policy.domain.com</div>

CANCEL

SAVE

In the **OAuth Client ID** and **OAuth Client Secret** text boxes, you enter the client ID and shared secret that you generated when you created the OAuth client for NSX in VMware Identity Manager.

In the **SSL Thumbprint** text box, you enter the SHA-256 certificate thumbprint value that you generated from the VMware Identity Manager appliance command line.

The value entered in the **NSX Appliance** text box must be used to access NSX Manager after the integration. If you enter the fully qualified domain name (FQDN) of NSX Manager and try to access the appliance through its IP address, the authentication fails.

If a virtual IP (VIP) is set up in the NSX Management cluster, you cannot use the external load balancer integration even if you enable it. You can either have VIP or the external load balancer while configuring VMware Identity Manager, but not both. Disable VIP if you want to use the external load balancer.

# 10-14 Verifying the VMware Identity Manager Integration

You can validate the successful communication between NSX and VMware Identity Manager from the NSX UI.

User Management

User Role Assignment

Local Users

Roles

Authentication Providers

LDAP

VMware Identity Manager

OpenID Connect

VMware Identity Manager

External Load Balancer Integration	<div>Disabled</div>
VMware Identity Manager Connection	<div>Up</div>
VMware Identity Manager Integration	<div>Enabled</div>
VMware Identity Manager Appliance	sa-nsxvidm-01.vclass.local
OAuth Client ID	sa-nsxmgr-01-OAuthClient
NSX Appliance	sa-nsxmgr-01.vclass.local

Navigate to **System > Settings > User Management > Authentication Providers > VMware Identity Manager** to validate the VMware Identity Manager integration. If the integration is successful, the VMware Identity Manager integration appears as Enabled. The VMware Identity Manager appliance, the OAuth Client ID, and the NSX Appliance fields are populated.

## 10-15 Default UI Login

The default login page appears when integration with VMware Identity Manager is not enabled.

Welcome to  
VMware NSX™

Username

Password

LOG IN


[Forgot Password?](#) 



The default login page also appears if integration with VMware Identity Manager is configured, but VMware Identity Manager is down or not reachable at the time of the login.

## 10-16 UI Login with VMware Identity Manager

After the integration with VMware Identity Manager is enabled, you are redirected to the VMware Identity Manager login page for authentication.



Workspace ONE™

Username

---

Password

---

System Domain

[Sign in](#)

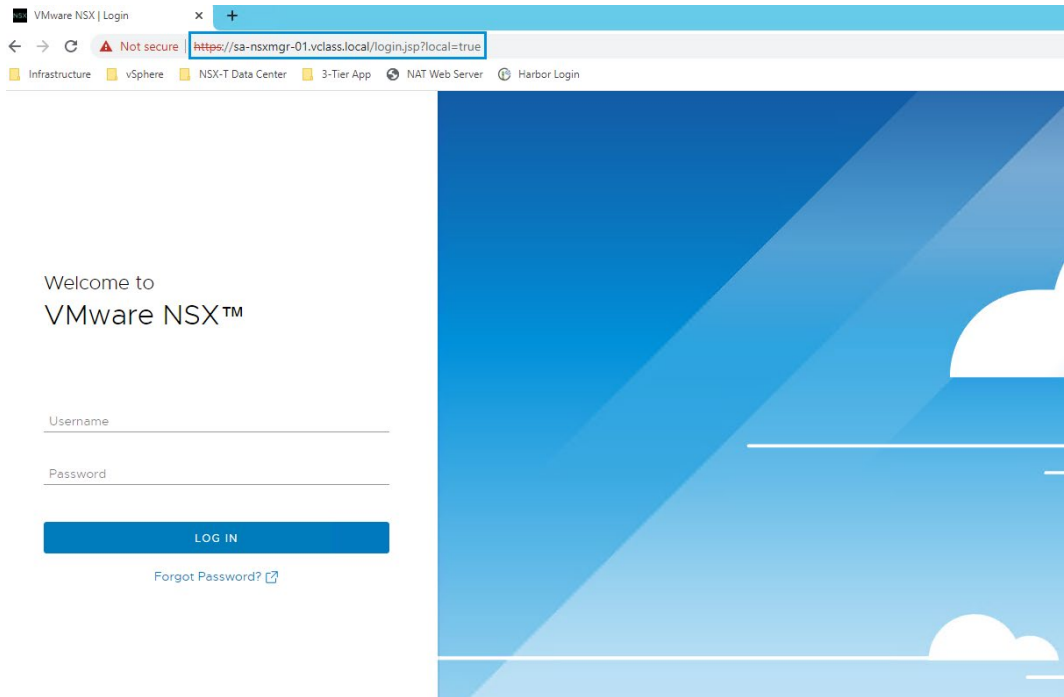
[Forgot Password?](#)

[Change to a different domain](#)

vmware™

## 10-17 Local Login with VMware Identity Manager

For troubleshooting or administration, you might need to bypass VMware Identity Manager when the integration is enabled. Go to [https://<NSX\\_Manager\\_FQDN>/login.jsp?local=true](https://<NSX_Manager_FQDN>/login.jsp?local=true).



## 10-18 Review of Learner Objectives

- Describe the purpose of VMware Identity Manager
- Identify the benefits of integrating NSX with VMware Identity Manager
- Configure the integration between NSX and VMware Identity Manager
- Verify the integration between NSX and VMware Identity Manager

## 10-19 Lesson 2: Integrating NSX with LDAP

### 10-20 Learner Objectives

- Identify the benefits of integrating NSX with LDAP
- Describe the LDAP authentication architecture
- Configure the integration between NSX and LDAP

### 10-21 About LDAP

The Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing and managing distributed directory services.

Distributed directory services store information about users and groups, the network infrastructure, and network services.

NSX supports the following directory services or identity sources:

- Active Directory over LDAP
- OpenLDAP



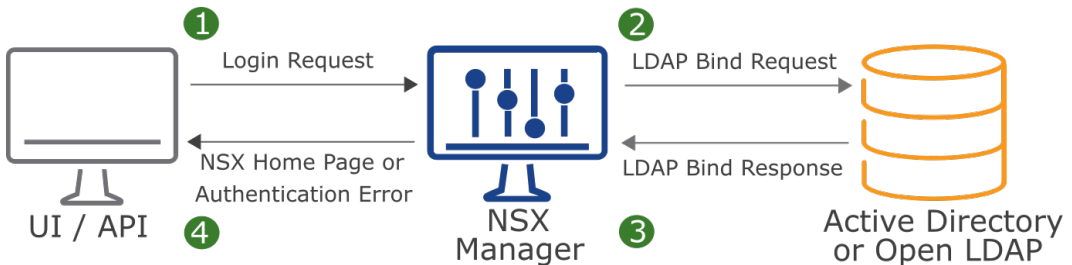
## 10-22 Benefits of Integrating LDAP with NSX

Integrating LDAP with NSX offers the following benefits:

- Reuses the existing directory service infrastructure
- Does not require the deployment of the VMware Identity Manager appliance
- Is simple to configure and manage

## 10-23 Authentication with LDAP

LDAP authentication operates as follows.



After integrating LDAP with NSX, the authentication process is as follows:

1. The user initiates a login request from the UI or the API.
2. NSX Manager receives the login request and creates an LDAP bind request to the appropriate identity source, for example, Active Directory.
3. The identity source returns an LDAP bind response to NSX Manager.
4. The bind response might succeed or fail during authentication. If the status is success, NSX Manager provides the appropriate access privilege based on the assigned RBAC role for the user or group. If the status is failure, NSX Manager displays an authentication error.

# 10-24 Adding an Identity Source

You can add up to three identity sources.

User Management

User Role Assignment

Local Users

Roles

Authentication Providers

LDAP

VMware Identity Manager

OpenID Connect

ADD IDENTITY SOURCE

Maximum: 3

COLLAPSE ALL

Filter by Name, Path and more

Name	Domain Name (FQDN)	Type	LDAP Servers	Connection Status
vclass	vclass.local Example: example.com	Active Directory over LDAP	Set	
Base DN *	CN=Users,DC=vclass,DC=local	Alternative Domain Names	Enter Alternative Domain Names	
Description	Example: CN=Users,DC=Corp,DC=local		Example: example.com	
<div>SAVE</div> <div>CANCEL</div>				

You can add a new identity source by navigating to **System > Settings > User Management > Authentication Providers > LDAP**

You specify the following settings as part of the identity source configuration:

- **Name:** The name of the identity source.
- **Domain Name:** The domain that you want to add as an identity source.
- **Type**

The following types of identity sources are available:

- **Active Directory over LDAP**
- **Open LDAP**

- **LDAP Servers:** The connection settings to your LDAP servers.
- **Base DN:** The point from where a server searches for users.



## 10-25 Configuring the LDAP Server

As part of adding an identity source, you specify the connection settings to the LDAP server.

The screenshot shows the 'User Management' console with the 'Authentication Providers' tab selected. A table lists existing providers, including 'vclass' with type 'Active Directory over LDAP'. A 'Set' button is visible next to it. A modal dialog titled 'Set LDAP Server' is open, showing the configuration form for a new LDAP server. The form includes fields for Hostname/IP, LDAP Protocol, Port, Enabled status, Certificate, Bind Identity, and Password. The 'ADD LDAP SERVER' button is highlighted in the dialog.

Three LDAP servers are allowed per LDAP domain. The servers are tried in order with each request.

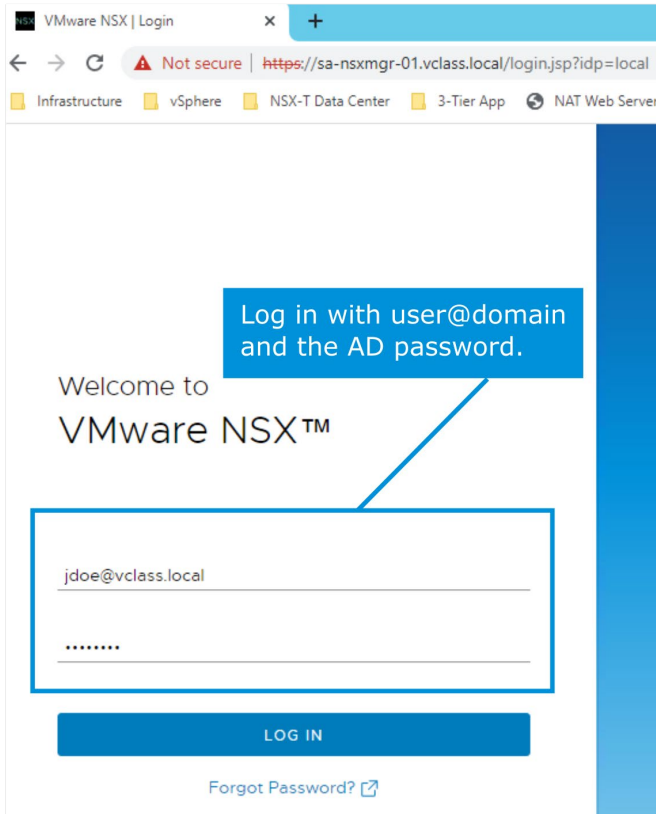
You specify the following settings when configuring the connection to the LDAP server:

- **Hostname/IP:** The fully qualified domain name or the IP address of the LDAP server. In LDAPS configurations, the FQDN must match the host name in the LDAP server certificate.
- **LDAP Protocol:** LDAP (unsecured) or LDAPS (secured).
- **Port:** The default LDAP port 389 and LDAPS port 636 are used for the directory sync. Do not change the default values.
- **Use StartTLS:** This toggle is available only for the LDAP protocol. If enabled, SSL/TLS is used to establish a secure connection.
- **Certificate:** The LDAP server provides a certificate as part of the ADD/Check status workflow. Accept the certificate.
- **Bind Identity:** Domain account with read permission for all objects in the domain tree.
- **Password:** Password for the bind identity account.

To verify that you can connect to the LDAP server, click **Check Status** (under Connection Status).

## 10-26 UI Login with LDAP

You log in as an Active Directory or OpenLDAP user by specifying the domain name on the NSX login page.



If a domain is not provided, local authentication is performed.

## 10-27 Review of Learner Objectives

- Identify the benefits of integrating NSX with LDAP
- Describe the LDAP authentication architecture
- Configure the integration between NSX and LDAP

# 10-28 Lesson 3: Managing Users and Configuring RBAC








## 10-29 Learner Objectives

- Identify the different types of users in NSX
- Recognize permissions and roles available in NSX
- Create and configure custom roles
- Explain object-based RBAC in a multitenancy environment
- Assign roles to users

## 10-30 NSX Users

The following types of users can access the NSX environment:

- Local users
- Principal identity users
- External users:
  - Active Directory and OpenLDAP users
  - Users managed by VMware Identity Manager

User Management			
<div>User Role Assignment   Local Users   Roles   Authentication Providers</div>			
<div>ADD PRINCIPAL IDENTITY   ADD ROLE FOR OPENID CONNECT USER</div>			
	User/User Group Name	Roles	Type
⋮	 admin	Enterprise Admin	Local User
⋮	 audit	Auditor	Local User
⋮	 guestuser1	Auditor	Local User
⋮	 guestuser2	Auditor	Local User
⋮	 napp_platform_egress	Nsx Application Platform Role	Principal Identity User
⋮	 napp_platform_ingress	Network Admin	Principal Identity User
⋮	 napp_platform_kafka	Network Admin	Principal Identity User

Local users have been preconfigured by the system:

- admin has the Enterprise Administrator role and cannot be modified.
- audit has the Auditor role. It can be renamed but it cannot be configured with other roles.
- guestuser1 and guestuser2 can be renamed and configured with RBAC roles.

Principal identity users are unique users. These users own the object that they create and ensure that the object can only be modified or deleted by the owning principal identity. Principal identity users are authenticated by client certificate. The authentication is local to NSX Manager. Principal identities are usually used by third-party management platforms, such as VMware Integrated OpenStack, Tanzu Kubernetes Grid Integrated Edition, VMware Aria Automation, and so on, but they are also used by NSX Application Platform.

The napp\_platform\_egress, napp\_platform\_ingress, and napp\_platform\_kafka principal identity users are added when NSX Application Platform is installed. Each of these users is configured with a specific role, which cannot be modified.

OpenID Connect is a simple security layer built on top of the OAuth2 authentication protocol. NSX supports the OAuth2 workflow that involves redirecting a user to an external identity provider (IDP). OpenID Connect users are authenticated by the IDP and the information about the authenticated sessions are sent to NSX. IDP partners are not supported.

## 10-31 Activating Guest Users

The two local users, guestuser1 and guestuser2, are inactive by default and can be activated by using the NSX UI or the API.

You can activate the two guest users by navigating to **System > Settings > User Management > Local Users**.

User Management

User Role Assignment Local Users Roles Authentication Providers

EXPAND ALL

	User Name	User ID	Status
>	admin	10000	Active
>	audit	10002	Active
>	guestuser1	10003	Not Active
>	guestuser2	10004	Not Active

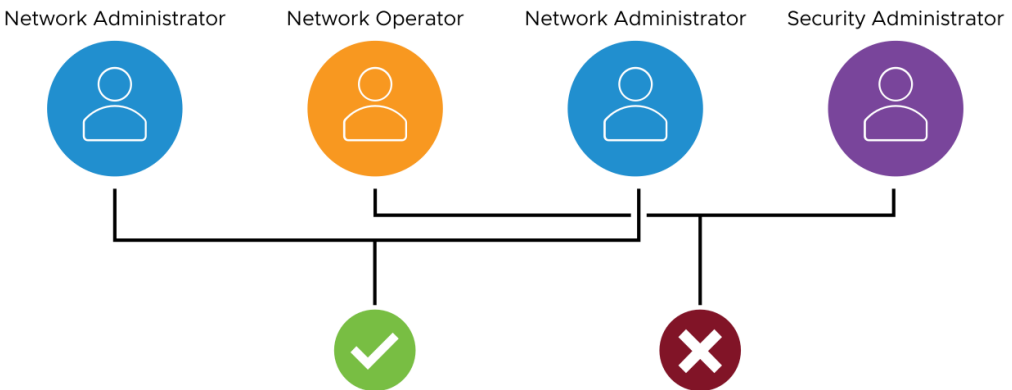
The two local users, guestuser1 and guestuser2, can only be activated by the admin user. Unlike the admin and audit users, guestuser1 and guestuser2 can be configured with RBAC roles.

## 10-32 Using Role-Based Access Control

RBAC enables you to restrict system access to users based on their role in the company.

Users are assigned roles, and each role has specific permissions:

- Local users, admin, and audit are preconfigured with specific roles that cannot be modified.
- Guest users, principal identity users, and external users can be configured with any of the built-in roles or custom roles.



Role-based access control (RBAC) is a method to enforce the least privilege and separation of duties principles.

# 10-33 Built-In Roles (1)

NSX provides built-in roles.

Role	Description
Auditor	Read permissions on all features
Enterprise Admin	Full access permissions on all features
GI Partner Admin	Role used for third-party endpoint protection service insertion
LB Admin	Read permissions on all networking services and full access permissions on load-balancing features
LB Operator	Read permissions on all networking services and load-balancing features
Netx Partner Admin	Role used for third-party Network Introspection service insertion
Network Admin	Full access permissions on all networking services

# 10-34 Built-In Roles (2)

Role	Description
Network Operator	Read permissions on all networking services and execute permissions on monitoring and troubleshooting tools
Org Admin	Performs CRUD operations in the allocated Org object in a multitenancy environment
Project Admin	Performs CRUD operations in the allocated Project object in a multitenancy environment
Security Admin	Full access permissions on all security configurations
Security Operator	Read permission on all security configurations and execute permissions on monitoring and troubleshooting tools
Support Bundle Collector	Permission only to generate a support bundle
VPN Admin	Read permissions on all networking services and full access permissions on VPN features

## 10-35 Custom Role-Based Access Control

The custom role-based access control (Custom RBAC) feature enables you to create custom roles in addition to the existing built-in roles.

Custom RBAC has the following common use cases:

- Provide flexibility to create custom roles and grant custom permissions to NSX users.
- Extend the current RBAC capabilities beyond the built-in roles with preconfigured permissions.
- Help companies to meet regulatory guidelines and compliance requirements for RBAC.



When default roles cannot enforce least user privileges and clear separation of duties, Custom RBAC helps enforce these options by providing more granularity. Custom RBAC provides flexibility and customization opportunities for specific deployment considerations and use cases.

# 10-36 Creating Custom Roles (1)

You can either clone an existing role or create a role in the NSX UI.

Home

Networking

Security

Inventory

Plan & Troubleshoot

System

<<

User Management

User Role Assignment

Local Users

Roles

Authentication Providers

ADD ROLE

	Role Name	Created By
⋮ >	Auditor	System
⋮ >	Enterprise Admin	System
⋮ >	GI Partner Admin	System
⋮ >	LB Admin	System
⋮ >	LB Operator	System
⋮ >	Netx Partner Admin	System
⋮ >	Network Admin	System
⋮ >	Clone Network Operator	System
⋮ >	Org Admin	System
⋮ >	Project Admin	System
⋮ >	Security Admin	System
⋮ >	Security Operator	System
⋮ >	Support Bundle Collector	System
⋮ >	VPN Admin	System

System Overview

Configuration

Quick Start

Appliances

NSX Application Platform

Fabric

Service Deployments

Identity Firewall AD

Lifecycle Management

Backup & Restore

Upgrade

Migrate

Settings

General Settings

User Management

Licenses

Certificates

Only an Enterprise administrator can create a custom role. However, Enterprise administrators can delegate the custom role creation to another custom role.



## 10-37 Creating Custom Roles (2)

You can set permissions for the new role.

The screenshot shows the 'User Management' interface with the 'Roles' tab selected. A role named 'natvpruser' is being configured. The 'Permissions' section shows 'Networking' and 'Security' with 'Read-only' buttons. A green callout box points to the 'Read-only' button for 'Networking' with the text: 'Click any of the permissions to access the Set Permissions menu.'

The 'Set Permissions' dialog is open, showing the role 'natvpruser' and a 'RESET ALL PERMISSIONS' button. The 'Networking' tab is selected, and a table lists various categories and their permissions. A blue callout box points to the 'VPN' and 'NAT' rows with the text: 'In this example, the users get full access to the VPN and NAT services and read-only access to the other networking features.'

Category	Description	Permission
▼ Networking		-- Mixed --
> Connectivity	Gateways, Segments, Bridges, Multicast	Read-only
▼ Network Services	VPN, NAT, Load Balancer, NSX Cloud Forwarding	-- Mixed --
VPN	VPN services, sessions, local endpoints, and profiles	Full Access
NAT	NAT Rules	Full Access
Load Balancing	Load balancers, virtual servers, server pools, profiles, and monitors	Read-only
Forwarding Policy	Forwarding policies for NSX Cloud	Read-only
Statistics	Routing tables, Forwarding tables and related statistics ⓘ	Read-only
> IP Management	DNS, IP Addresses	Read-only

Note: All features supported in NSX may not be available for role customization. See documentation for default role permissions for NSX and NSX Intelligence

CANCEL APPLY

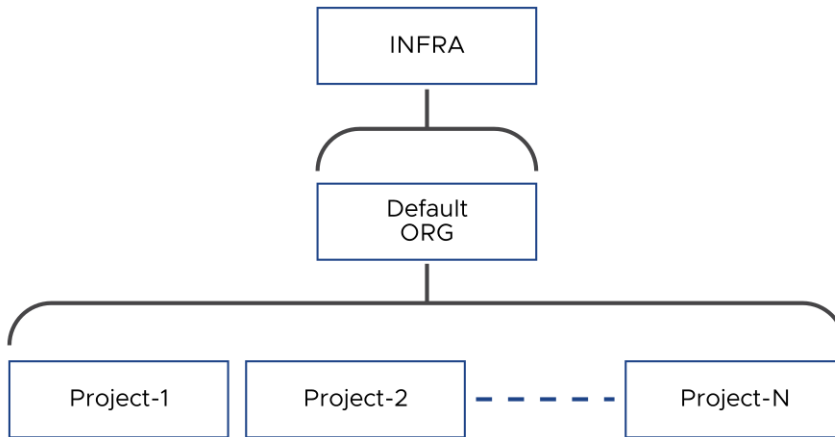
The following NSX features are not supported with the Custom RBAC role:

- Upgrade
- Migrate
- Fabric
- TraceFlow
- NSX Intelligence
- Inventory of physical servers and containers

# 10-38 Multitenancy Hierarchy Model in NSX 4.0.1

NSX 4.0.1 has expanded its data model to support multitenancy by introducing the following new constructs:

- ORG: Represents the provider space
- Project: Represents the tenant space



ORG and Project are referred to as objects that contain the NSX resources.

Default ORG is a multitenancy organization container created by default by the NSX system. The ORG can represent:

- Provider spaces in a service provider scenario
- Companies that might have different departments or business units

Project is a container that provides isolation for specific networking and security constructs in an organization.

The Project can represent:

- Tenant spaces in a service provider scenario
- Different departments or business units in a company

An ORG can have more than one Project. Each Project has its own separate and isolated space.

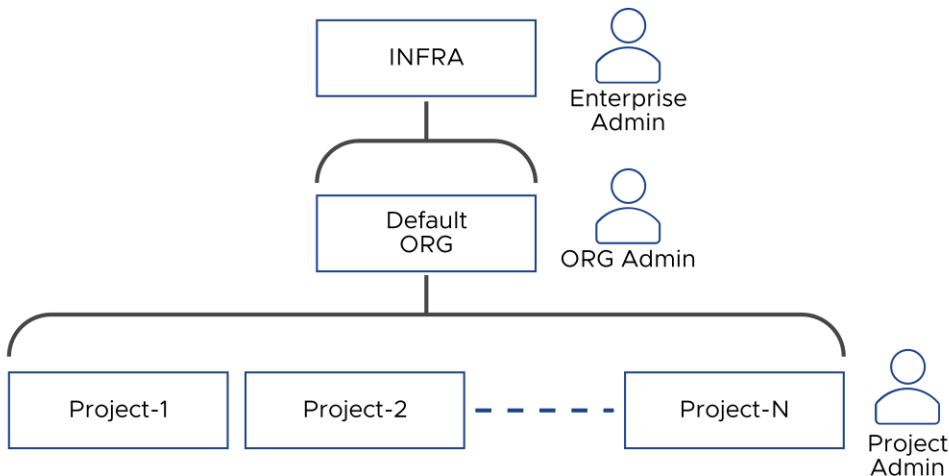
Projects are created by an Enterprise Admin or an ORG Admin.

## 10-39 Object-Based RBAC in a Multitenancy Environment

In NSX 4.0.1, the following new user roles are available for RBAC:

- ORG Admin:
  - Creates Projects
  - Provides role binding between Project Admin and Project object
  - Performs CRUD operations in the allocated ORG object
- Project Admin:
  - Performs CRUD operations in the allocated Project object

Object-based RBAC is only configurable through NSX API in NSX 4.0.1



Role binding is used to bind a user role to an object. The user can perform CRUD operations in an object based on its role binding.

Role binding is hierarchical in nature. Users at any level can see all the role bindings for themselves and the users below them.

Users at any level can provide role bindings for the users below them. For example, an Enterprise Admin can provide role bindings between an ORG Admin user and an ORG and between a Project Admin user and a Project.

An Enterprise Admin can perform CRUD operations across the entire NSX infrastructure.

Object-based RBAC is only configurable through NSX API in NSX 4.0.1. NSX UI support is expected in future releases.

# 10-40 Role Assignment

You can add, change, and delete role assignments for users or user groups:

1. Select **System > Settings > User Management > User Role Assignment**.
2. Click **ADD ROLE FOR PROVIDERS** and select a user type.
  - **LDAP**
  - **VMware Identity Manager**
3. Select the search domain.
4. Search for the users or user groups that you want to assign the roles to.
5. Select a role or roles and click **SAVE**.

User Management

User Role Assignment

Local Users

Roles

Authentication Providers

ADD PRINCIPAL IDENTITY

ADD ROLE FOR PROVIDERS

User/User Group Name	Roles	Type
VCLASS * jdoe@vclass.local *	Security Operator X	LDAP User
<div>SAVE CANCEL</div>		
<div><div></div><div>admin</div></div>		Local User
<div><div></div><div>audit</div></div>		Local User
<div><div></div><div>guestuser1</div></div>		Local User
<div><div></div><div>guestuser2</div></div>		Local User

When selecting a role for a user, you can choose from built-in or custom roles that were created previously.

Auditor

Enterprise Admin

GI Partner Admin

LB Admin

LB Operator

Network Admin

Network Operator

Netx Partner Admin

## 10-41 Lab 20: Managing Users and Roles

Integrate NSX Manager with Active Directory over LDAP:

1. Prepare for the Lab
2. Add an Active Directory Domain as an Identity Source
3. Assign NSX Roles to Domain Users and Test Permissions
4. Modify an Existing Role and Test the Role Permissions

## 10-42 Review of Learner Objectives

- Identify the different types of users in NSX
- Recognize permissions and roles available in NSX
- Create and configure custom roles
- Explain object-based RBAC in a multitenancy environment
- Assign roles to users

## 10-43 Key Points

- VMware Identity Manager provides application provisioning, conditional access controls, and SSO for SaaS, web, cloud, and native mobile applications.
- You can integrate NSX with VMware Identity Manager and configure RBAC for users that VMware Identity Manager manages.
- You can add Active Directory over LDAP or OpenLDAP identity sources to NSX and configure RBAC for these users.
- Role-based access control (RBAC) enables you to restrict system access to users based on their role in the company.
- The Custom RBAC feature in NSX enables administrators to create custom roles in addition to the existing built-in roles.

Questions?



# Module 11

## NSX Federation

### 11-2 Importance

In NSX, Federation enables network administrators to define global configuration settings and policies that span multiple sites. You must understand the Federation architecture and configuration, logical switching, logical routing, and security to successfully configure NSX Federation in your environment.

### 11-3 Module Lessons

1. Federation Architecture
2. Installing and Onboarding Federation
3. Federation Networking
4. Federation Security

## 11-4 Lesson 1: Federation Architecture

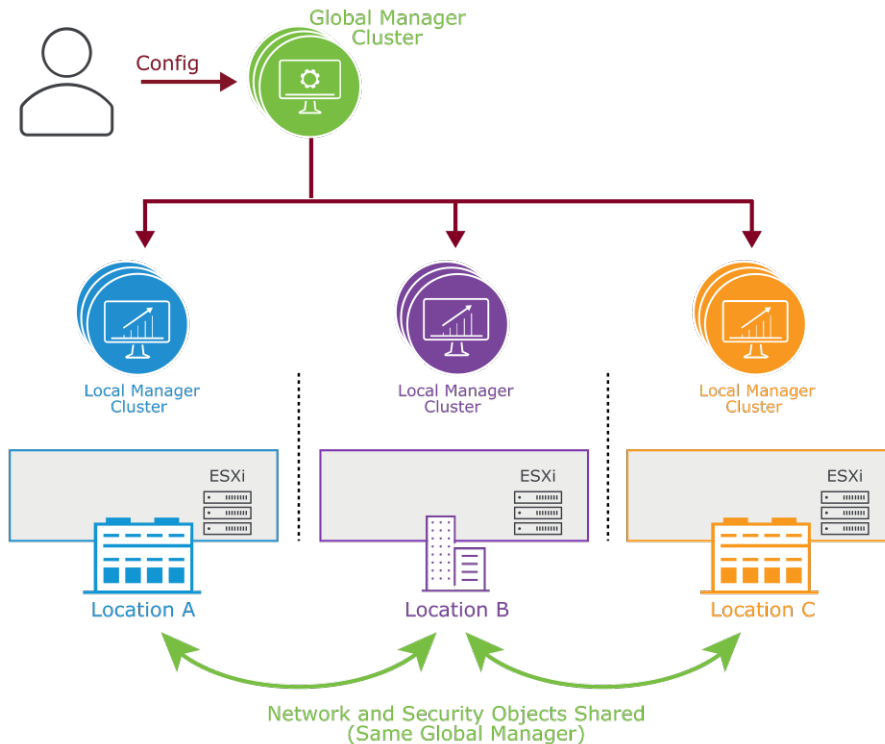
### 11-5 Learner Objectives

- Describe Federation and its use cases
- Describe the requirements and limitations of Federation
- Describe the Federation configuration workflow



## 11-6 About NSX Federation

NSX Federation offers globally managed network and security services across multiple locations, improving scale and design flexibility. NSX supports up to eight federated locations.



NSX Federation supports multilocation deployments and offers:

- A single interface for managing networking and security
- Improved network agility and business continuity
- Consistent policy configuration and enforcement
- Simplified disaster recovery and avoidance

Having multiple federated sites brings the following benefits:

- High availability of applications
- Better application response time
- Cost-effective hosting solution based on the application criticality
- Configuration during mergers or acquisitions

## 11-7 NSX Federation Components: Global Manager

The NSX Federation architecture has two main components: Global Manager and Local Manager.

A Global Manager appliance provides the GUI and the REST APIs for configuring objects across geographical sites. Global Manager has the following characteristics:

- Global configurations are replicated to the standby Global Manager appliance.
- Global configurations are sent to the relevant Local Manager appliances.
- Configurations that require protection against site failures must be configured in Global Manager.
- During site onboarding, you can move the existing Local Manager configuration to Global Manager.

Global Manager  
Cluster



## 11-8 NSX Federation Components: Local Manager

Local Manager provides management for a single site. UI and API access are available through the Local Manager virtual IP address.

Local Manager performs the following functions:

- Realizes global configurations that are sent by Global Manager
- Continues to accept user configurations pertaining to the local site
- Owns the infrastructure preparation and configuration, for example, transport node preparation, edge configurations, transport zones, IP address pools, and so on

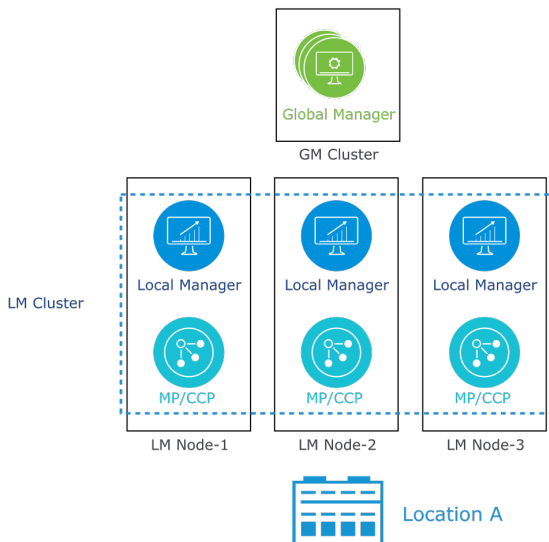
Local Manager  
Cluster



## 11-9 NSX Federation Components: Global Manager and Local Manager Clusters

Global Manager and Local Manager have the following characteristics:

- Global Manager and Local Manager appliances are deployed in a VM form factor.
- The Global Manager node does not include a control plane.
- Global Manager appliances are deployed as three-node clusters that can be in a single location or spread across three locations.
- Local Manager appliances are deployed as three-node clusters in each location for high availability and scalability.
- Local Manager appliances can selectively override some global object configuration parameters.



Global Manager nodes are deployed with an Open Virtualization Format (OVF) template and form a cluster with three nodes.

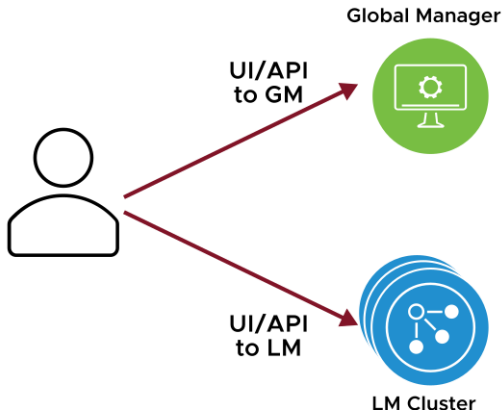
The Global Manager node includes a management plane. It does not include a control plane.

Local Manager can selectively override some global object configuration. For example, Local Manager can configure site-specific Border Gateway Protocol (BGP) timer configurations on a global Tier-0 gateway.

## 11-10 Federation Configuration Types

NSX Federation supports the following types of configurations:

- Global configuration:
  - The GM node receives the configuration.
- Local configuration:
  - The LM cluster receives the configuration on a given location.



## 11-11 Ownership of Logical Configuration (1)

Network objects that are created by GM are owned by GM:

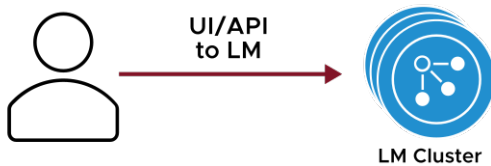
- Tier-0 and Tier-1 gateways, segments, segment profiles, and so on, can be configured from GM.
- GM is the single source of truth for these objects. These objects can only be modified or deleted by GM.
- The GM-created objects are visible to LM but are read-only.



## 11-12 Ownership of Logical Configuration (2)

Network objects that are created by LM are owned by LM:

- Tier-0 and Tier-1 gateways, segments, segment profiles, and so on, can be configured from LM.
- LM is the single source of truth for these objects. These objects can only be modified or deleted by LM.
- The LM-created objects are not visible to GM.
- During the onboarding process, you can move the object to GM. Then, LM loses ownership of these objects.



The following configurations can be imported from the Local Manager into Global Manager:

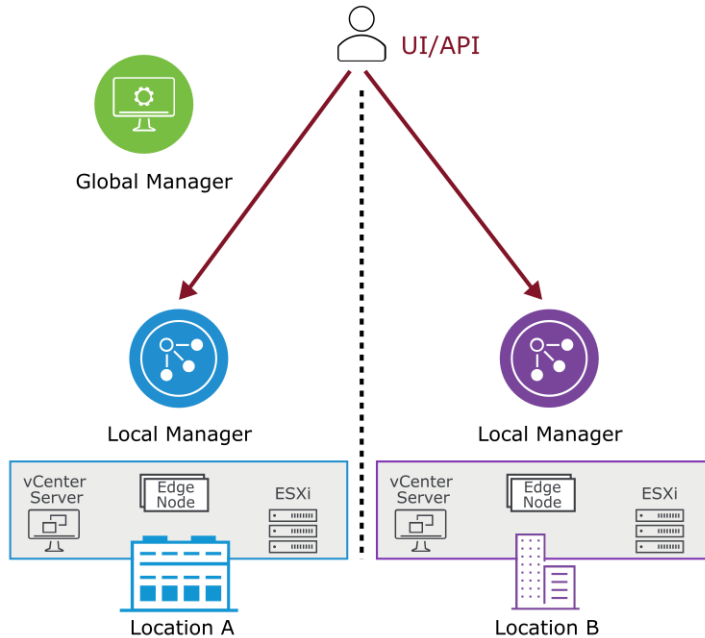
- T0 gateway
- T1 gateway
- Firewall security policies
- Services
- Security profiles
- Context profiles
- Services
- Groups
- NAT
- DHCP
- DNS
- Gateway profiles
- Time-based firewall (supports import/onboard)

For more information about the local manager configurations supported for importing into global manager, see *NSX-T Data Center Installation Guide* at: <https://docs.vmware.com/en/VMware-NSX/4.0/installation/GUID-388CE659-3FE3-4EF4-ABA3-AE3FCAA191E9.html>

## 11-13 Infrastructure Ownership

LM always manages infrastructure objects:

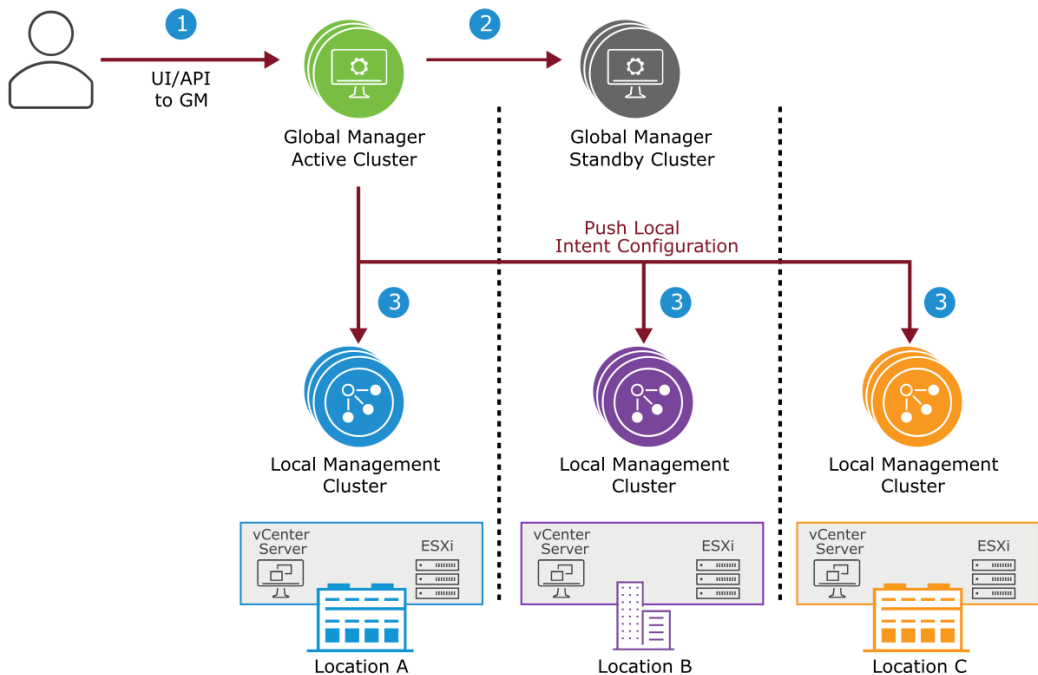
- These objects include transport nodes, edge nodes, transport zones, and so on.
- LM completely owns infrastructure preparation.
- Objects can only be created, modified, or deleted by LM.



## 11-14 Global Configuration

The global configuration workflow is as follows:

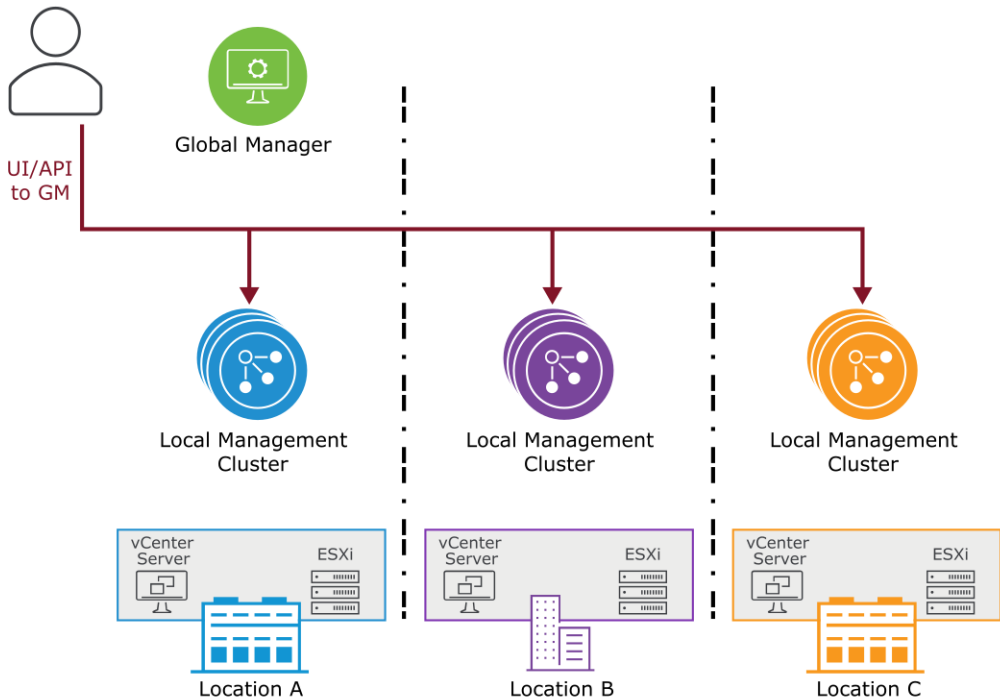
1. The user sends the configuration to the active GM.
2. The active GM stores locally and replicates the configuration to the standby GM.
3. The active GM sends it to the relevant LMs.



## 11-15 Local Configuration

The local configuration workflow is as follows:

- A user can also send the configuration to LM at each location, as required.
- Each LM stores the configuration locally.
- No configuration is sent to GM.

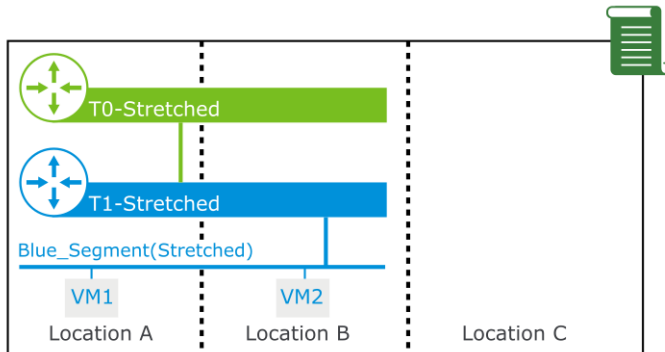




## 11-16 Federation Configuration Example

In the configuration example, networks are created and realized only in two locations (Location A and Location B).

T0, T1, and their associated segment are stretched to Location A and Location B.



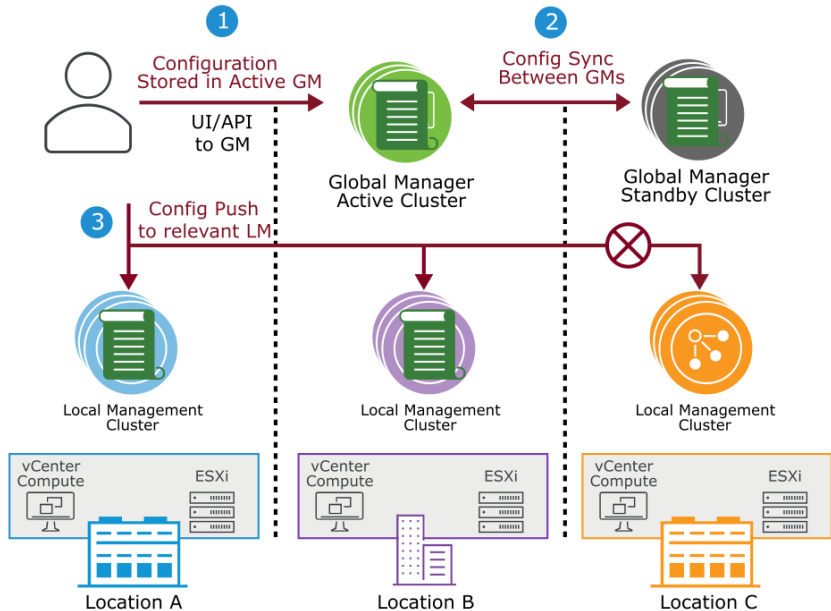
Blue\_Segment associated with T1 is also stretched to Location A and Location B.

Two VMs (VM1 and VM2) are connected to Blue\_Segment.

This configuration is realized in GM and LMs across locations.

## 11-17 Federation Configuration Example Workflow (1)

As the T0, T1, and their associated segment are only stretched to Locations A and B, the configuration is not sent to LM at Location C.

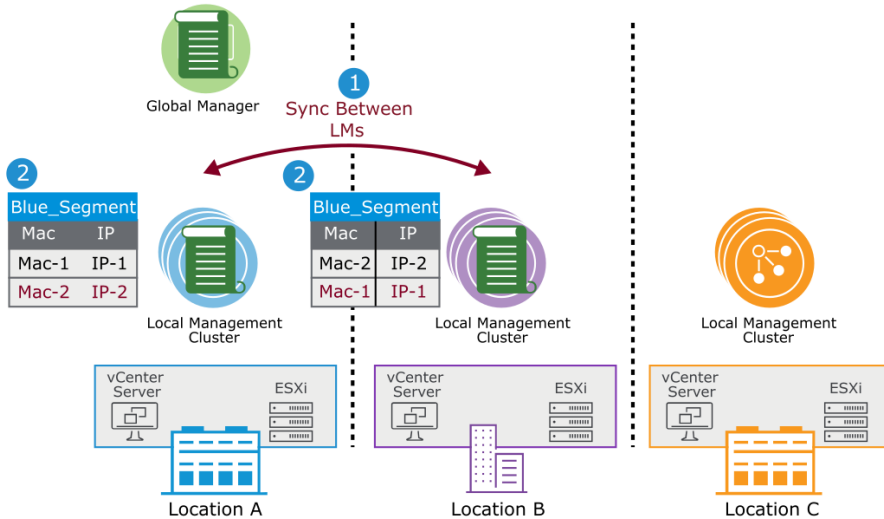


In the example, the user wants to apply a configuration that is stretched to Location A and Location B only:

1. The user sends the configuration by using REST over HTTPS to the active GM node in Location A, which stores the configuration locally.
2. The active GM replicates the configuration to the standby GM.
3. GM pushes the configuration to LM clusters of Location A and Location B, because the configuration is intended only for them. The configuration is not sent to LM at Location C.

## 11-18 Federation Configuration Example Workflow (2)

LMs of each location initiate a sync operation to exchange the Control Plane configuration of a given topology.



In the example, the control plane of LM in each location learns the IP and MAC information of the VMs associated with Blue\_Segment:

1. LMs at each location initiate a sync operation to exchange the IP and MAC information of VMs associated with Blue\_Segment.
2. Each LM stores the realization information of a given topology discovered through the sync operation. As a result, the Control Plane of LM in each location has the IP and MAC information of all the VMs associated with Blue\_Segment across Location A and Location B.

LM does not update control plane information to GM, because GM has no control plane. However, the GM UI enables you to see the inventory of all locations by querying the relevant LMs.

## 11-19 Review of Learner Objectives

- Describe Federation and its use cases
- Describe the requirements and limitations of Federation
- Describe the Federation configuration workflow

# 11-20 Lesson 2: Installing and Onboarding Federation

## 11-21 Learner Objectives

- Describe the prerequisites for Federation
- Configure GM as active and standby in the primary and secondary location
- Describe location onboarding

## 11-22 NSX Federation: Prerequisites

NSX Federation requires several prerequisites.

Location-to-Location Latency, Stretched Networking Use Case	Up to 150 ms
Location-to-Location Latency, Stretched Security Use Case	Up to 500 ms
WAN Bandwidth	No congestion for the management plane or the data plane
WAN MTU	1,700 bytes
Data Plane	For different Internet Service Providers (ISPs), a public address must be advertised from both locations
Compatibility	All appliances in an NSX Federation environment must have the same version installed.

Location-to-location traffic must satisfy the following characteristics:

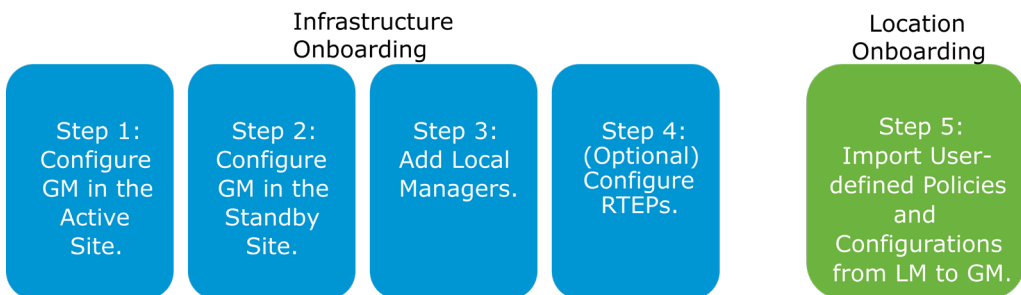
- A maximum 150 ms Latency (RTT) between locations in the stretched networking use case, where networking objects, such as Tier-0 gateways, Tier-1 gateways, or segments span multiple sites.
- A maximum 500 ms Latency (RTT) between locations in the stretched security use case, supported since NSX-T Data Center 3.2.1. If present, networking objects do not span multiple sites.

- Allow IP and firewall connectivity across sites:
  - Allow Management traffic between GM and LM.
  - Allow Data plane traffic between edge nodes (RTEP).
  - Do not configure NAT for Management and RTEP networks.
- WAN bandwidth requirement:
  - No congestion for the Management plane (GM to LM traffic).
  - No congestion for the data plane.
- WAN MTU requirement:
  - MTU of 1,700 bytes or more to avoid the edge node RTEP traffic fragmentation.
- Version requirement:
  - All appliances in an NSX Federation environment must have the same version installed.
- Global Manager supports only Policy Mode. NSX Federation does not support Manager Mode.

## 11-23 Onboarding Process

The onboarding process involves infrastructure onboarding and location onboarding.

The onboarding process includes several steps.



The infrastructure onboarding process is repeated for each location until all locations are on board.

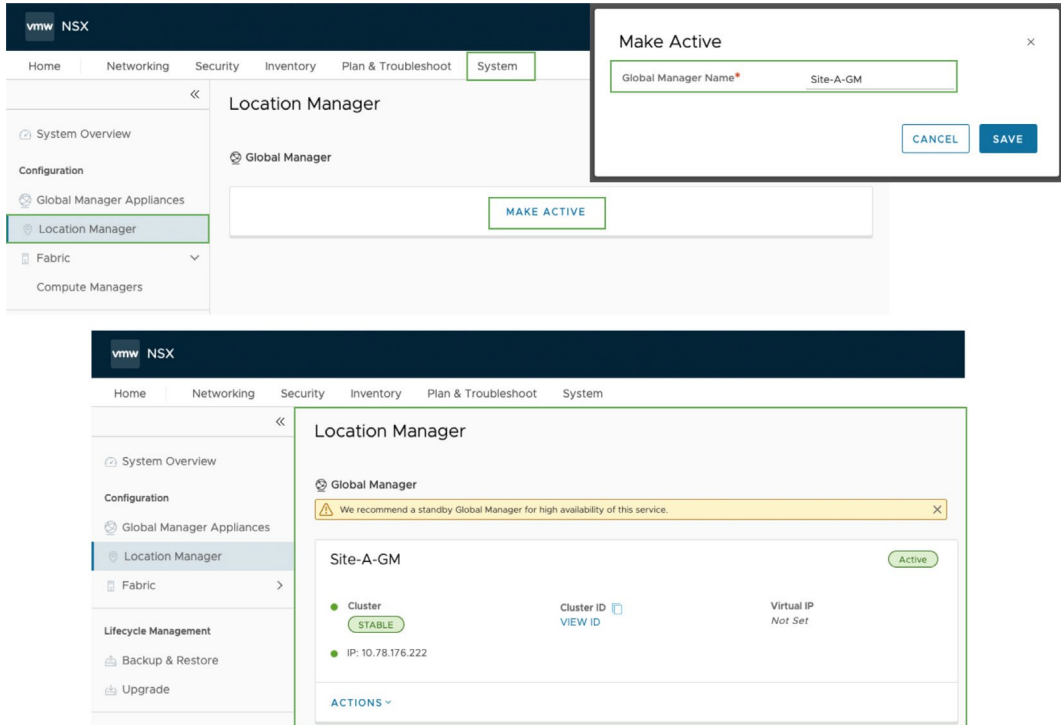
RTEP configuration is required for stretched networking functionality.

Location onboarding promotes existing objects on a local manager into the global manager configuration.

The onboarding process does not affect running workloads.

## 11-24 Active Global Manager Configuration

From the Site-A-GM UI, select **MAKE ACTIVE** to designate the GM as active.



The **Location Manager** tab is the central management point for configuring GMs (active and standby).

You can add different locations from this tab to GM. The managers in these locations are Local Manager (LM).

You can configure the standby GM from the active GM site to provide flexibility for configuring the Federation component from a single console.

## 11-25 Adding Standby Global Manager (1)

You must add a standby GM. If the active GM fails, the standby GM can be activated from its UI.

The screenshot displays the VMware NSX Global Manager web interface. The top navigation bar includes the VMware NSX logo, a dropdown menu for 'Site-A-GM Global Manager', and user information 'admin'. The main navigation tabs are Home, Networking, Security, Inventory, Plan & Troubleshoot, and System. The left sidebar contains sections for System Overview, Configuration (with Location Manager highlighted), Lifecycle Management, and Settings. The main content area is titled 'Location Manager' and features a yellow warning banner: 'We recommend a standby Global Manager for high availability of this service.' Below this, the 'Site-A-GM' status is shown as 'Active' with a 'Cluster' status of 'STABLE'. A table lists the 'Cluster ID' as 'VIEW ID' and the 'Virtual IP' as 'Not Set'. A button labeled 'ADD STANDBY GLOBAL MANAGER' is prominently displayed. The 'Locations' section below has a map icon and a button to 'ADD ON-PREM LOCATION'.

You can configure the standby GM from the active GM site to provide flexibility for configuring the Federation component from a single console.

## 11-26 Adding Standby Global Manager (2)

You provide the Location B GM information. The certificate thumbprint of the GM is required.

Add Standby Global Manager

Add a Global Manager in standby mode. Standby Global Manager syncs with active Global Manager and receives all global configurations.

Global Manager Name\*

Site-B-GM

FQDN/IP\*

10.78.185.84

Username\*

admin

Password\*

Admin!23Admin

SHA-256 Thumbprint\*

f7c71d32ab32d4e8371416d305cc1a5a5d4df7792b7b0cb236ab50da2f8f1bad

COMPATIBILITY

Version

4.0.1

CHECK VERSION COMPATIBILITY

CANCEL

SAVE

```
Site-B-GM> get certificate api thumbprint
```

```
f7c71d32ab32d4e8371416d305cc1a5a5d4df7792b7b0cb236ab50da2f8f1bad
```


The compatibility check is mandatory because it checks version compatibility between the two GMs.

From the CLI, run `get certificate api thumbprint` to fill the details of the SHA-256 thumbprint in the UI.



## 11-27 Adding a Location

You add the location from **ADD ON-PREM LOCATION**, and provide the details about NSX Manager at Location A.




Add New Location

**ADD ON-PREM LOCATION**

Add New Location

⌵


 After this location is added, security policies, groups, and profiles from Site-A-GM appear ahead of existing or new local configurations because GM configurations have a higher priority than local configurations.

Name your new location so you can identify it in your Global Manager.

Location Name\*


FQDN/IP\*

Username\*

Password\*  

SHA-256 Thumbprint\* 


d20338688332eff3108d7be02c83813d6cf21af3daf0a3731d98372c269a8c1b



COMPATIBILITY

CHECK VERSION COMPATIBILITY

Version

4.0.1 

CANCEL

SAVE

```
Site-A-LM> get certificate api thumbprint
```

```
d20338688332eff3108d7be02c83813d6cf21af3daf0a3731d98372c269a8c1b
```

The SHA-256 certificate thumbprint is required.

You can obtain the certificate thumbprint by using the following command on NSX Manager:

```
get certificate api thumbprint
```

## 11-28 Validating the Local Manager

The **Location Manager** tab on LM provides information about the Sync status of LM to GM.

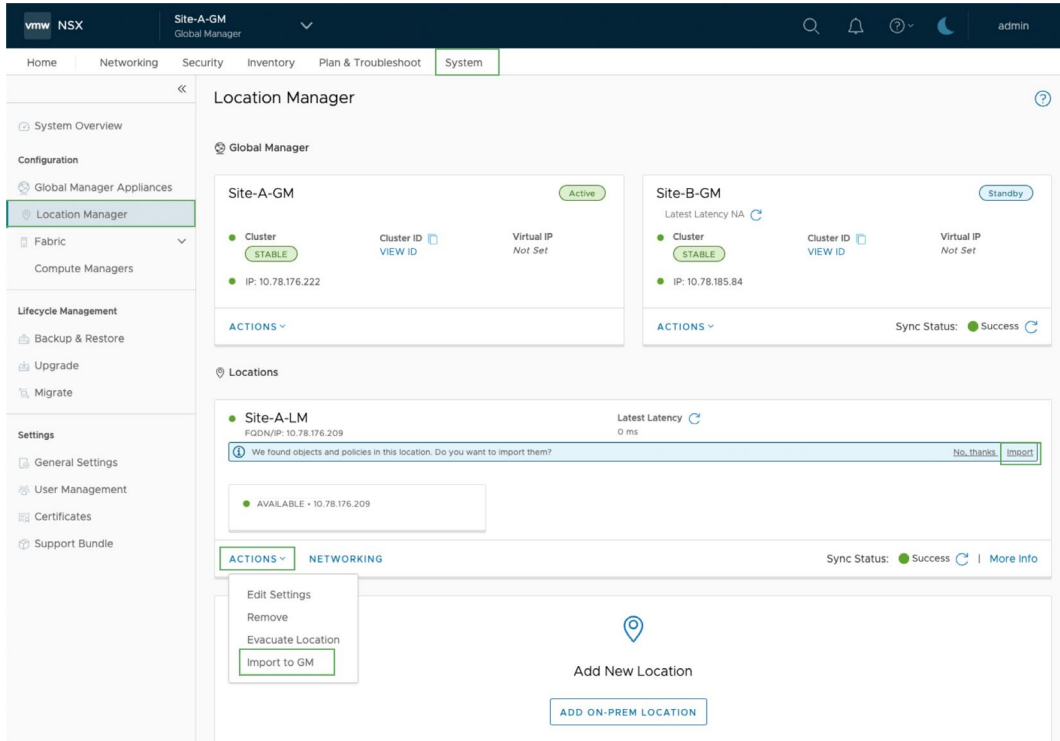
The screenshot displays the VMware NSX Location Manager interface. The top navigation bar includes the NSX logo, a dropdown menu for 'Site-A-LM On-Prem', and search, notification, and user icons. The left sidebar contains navigation links for Home, Networking, System Overview, Configuration (Quick Start, Appliances, Location Manager), NSX Application Platform, Fabric, Service Deployments, Identity Firewall AD, Lifecycle Management (Backup & Restore, Upgrade), and Settings (General Settings). The main content area is titled 'Location Manager' and shows a 'Full Sync Successful' status for Site-A-LM. A diagram illustrates the sync process between Site-A-LM and Site-B-GM. Below the diagram, the 'Global Manager' section lists Site-A-GM (Active) and Site-B-GM (Standby) with their respective cluster member IP addresses and sync status.

Site	Status	Cluster Members
Site-A-LM	Full Sync Successful	10.78.176.209
Site-A-GM	Active	10.78.176.222
Site-B-GM	Standby	10.78.185.84

The **Location Manager** tab also provides details about the active and standby GM. The details are read-only.

# 11-29 Location Onboarding

You can optionally onboard a location by promoting LM objects to the GM.



LM objects can be imported either during onboarding or after onboarding. The screenshot shows an option to import after your location is onboarded.

If the default transport zone is not found for the Local Manager at site Site-A-LM, then wait for default transport zone discovery or reload the enforcement point and retry.

A mandatory check verifies that the LM is backed up and is a prerequisite to onboarding a location.

The import takes time. During this time, no downtime occurs.

You can use this time to prepare the Networking and Security workloads and configuration.

Import of configurations into the Global Manager is blocked if you have any of the following configurations in your Local Manager. You must remove unsupported configurations to proceed with importing. After your supported Local Manager configurations are successfully imported into Global Manager, you can add the configurations for any of the unsupported features back into your Local Manager.

The following Local Manager configurations are not supported for importing into Global Manager:

- DHCP dynamic binding
- Distributed IDS
- Distributed security for vCenter VDS Port Groups
- Endpoint protection
- Forwarding policies
- Guest introspection
- Identity firewall
- IDS/IPS
- L2 Bridge
- Load balancer
- Malware prevention
- Metadata proxy
- Multicast
- Network detection and response
- Network introspection
- Routing protocols (OSPF)
- Routing VPN and EVPN
- Service insertion
- TO VRF
- TLS inspection
- URL filtering

# 11-30 Onboarding Preparation

Prepare for location onboarding by specifying a site-specific prefix or suffix.

Global Manager

Site-A-GM

Cluster

Cluster ID

Virtual IP

10.78.176.222

Active

VIEW ID

Not Set

Locations

Site-A-LM

FGDN/IP: 10.78.176.209

Imported to GM

Latest Latency

0 ms

10.78.176.209

Site-B-LM

FGDN/IP: 10.78.176.20

Latest Latency

1 ms

10.78.176.20

Prepend onboarded objects with "Site-B-LM-"

Preparing for Import

10 objects in Site-B-LM can be renamed and are listed below.

Entity Type	Count	Conflict
Network	8	0
Tier-0 Gateways	1	0
Tier-1 Gateways	1	0

10 Site B objects to onboard

You can prefix/suffix here. All 10 objects in Site-B-LM will carry forward this name change.

Prefix

Site-B-LM-

For example: Site-B-LM-siteb-t0gw-01  
Above listed objects will be updated with this prefix value, while import.

NO, CANCEL

NEXT

Virtual IP

Not Set

Sync Status: Success

No, thanks

Import

Success

More Info

When LM objects are imported to GM, you must mark them to differentiate these objects. To distinguish better, you add either a prefix or a suffix. You can define the prefix or suffix. In this example, Site B onboarded objects are prepended with the text Site-B-LM- for location tracking.

## 11-31 Verifying Onboarding

After LM Onboarding, verify that onboarded network and security objects are now global.

The top screenshot shows the 'Tier-0 Gateways' page in the NSX Manager. A callout box labeled 'Onboarded global group object at Site B' points to the entry 'Site-B-LM-siteb-t0gw-01' which has a 'GM' tag. The table below shows the details of this gateway.

Name	HA Mode	Linked Tier-1 Gateways	Linked Segments	Status	Alarms
Site-B-LM-siteb-t0gw-01 (GM)	Active Active	1	0	Success	0

The bottom screenshot shows the 'Groups' page. The table below lists the groups, including 'Global-IP-address-Group' which has a 'GM' tag.

Name	Type	Compute Members	Where Used	Status
Edge_NSGroup	Generic	<a href="#">View Members</a>	<a href="#">Where Used</a>	Success
Global-IP-address-Group (GM)	IP Addresses Only	<a href="#">View Members</a>	<a href="#">Where Used</a>	Success

In this example, onboarded objects, Site-B-LM-siteb-t0gw-01 and Global-IP-address-Group, are now global.

## 11-32 Review of Learner Objectives

- Describe the prerequisites for Federation
- Configure GM as active and standby in the primary and secondary location
- Describe location onboarding

## 11-33 Lesson 3: Federation Networking

### 11-34 Learner Objectives

- Describe the stretched networking concepts in Federation
- Explain the supported Tier-0 and Tier-1 stretched topologies
- Explain Layer 2 concepts related to NSX Federation
- Identify network types that can be interconnected using L2 Bridging in federated environments

### 11-35 Stretched Networking (1)

NSX Federation supports the stretching of the following networking constructs across locations:

- Tier-0 gateways (T0)
- Tier-1 gateways (T1)
- Segments

The following services are supported on stretched T1 gateways:

- NAT
- Gateway firewall
- IPv6
- DHCP
- DNS



The Global Manager UI enables the user to create stretched networks, for example, segments, gateways and security policies, and rules.

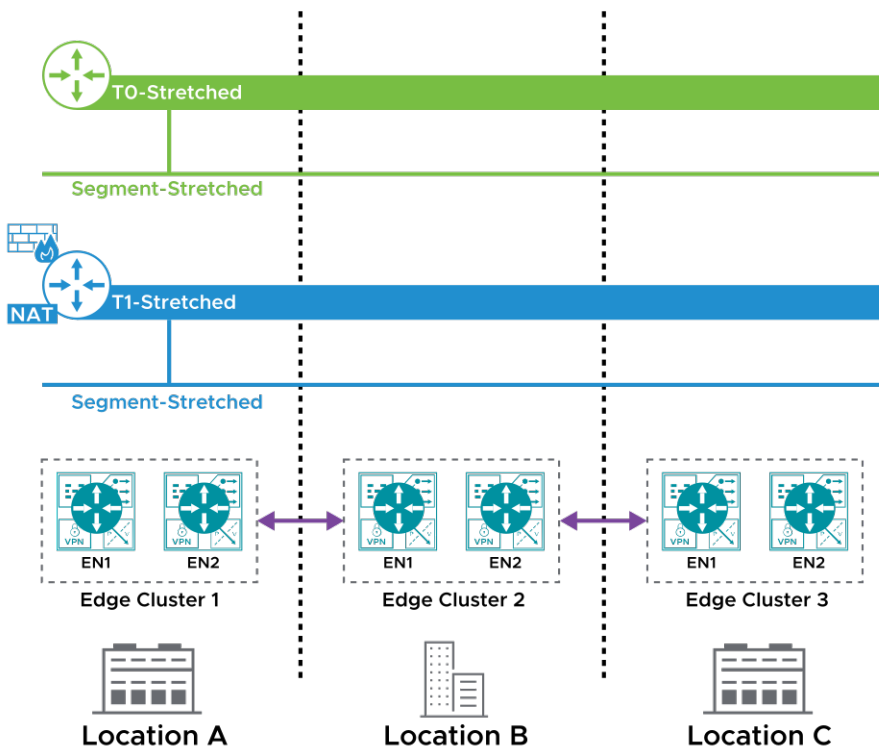
## 11-36 Stretched Networking (2)

GM can stretch the Tier-0 and Tier-1 gateways across locations:

- All segments that are connected to the downlink port of the stretched T1 gateway are automatically stretched across locations.

The edge nodes are used to forward cross-location traffic:

- This method eliminates the need for tunnels between hypervisors across locations.
- The edge nodes use RTEPs to provide cross-location communication.



Remote Tunnel Endpoints (RTEPs) are created from the LM UI.

On the edge nodes, RTEPs are configured to forward the traffic across sites.

NSX does not encrypt the traffic, but the user can encrypt this cross-location traffic with a third-party tool.

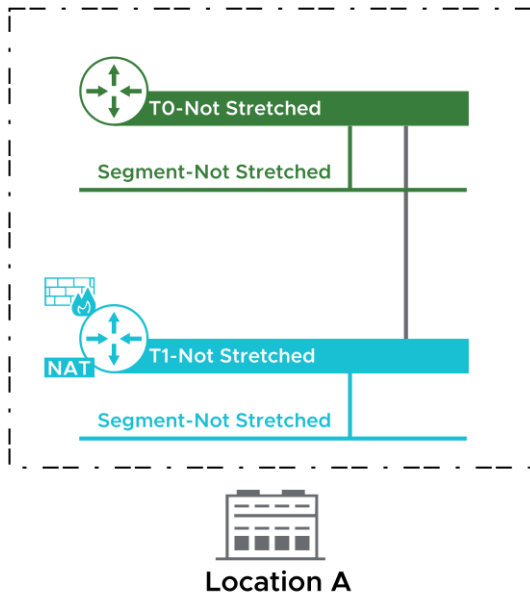


## 11-37 Tier-0 and Tier-1 Gateways: Logical Topologies (1)

GM supports stretch networks for cross-location communication and nonstretched networks for a local location.

A GM-supported configuration has the following features:

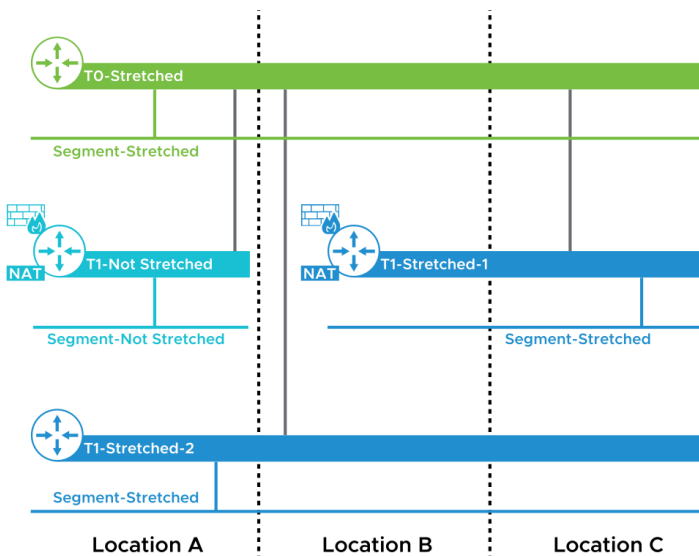
- Tier-0 and Tier-1 gateways can still be local to Location Manager.
- Tier-0 and Tier-1 gateways can stretch across locations.
- Segments connected to the stretched Tier-0/Tier-1 gateways are automatically stretched across locations.
- Segments connected to nonstretched Tier-0/Tier-1 gateways are local to the location.



## 11-38 Tier-0 and Tier-1 Gateways: Logical Topologies (2)

GM-supported configuration:

- Tier-0 and Tier-1 gateways can be stretched to all or some of the locations.
- Segments associated with stretched for the Tier-0/Tier-1 gateway are also stretched to the same span:
  - The span of a segment is equal to the span of the Tier-0/Tier-1 gateway.
- If the scope of the Tier-1 gateway is equal to or is a subset of the Tier-0 gateway, a stretched Tier-0 gateway can connect to a nonstretched Tier-1 gateway.
- For a Tier-1 gateway without services, the span of Tier-1 is equal to the span of the Tier-0 gateway.



The example includes the stretched network objects, including the stretched segments and stretched Tier-0 and Tier-1 gateways.

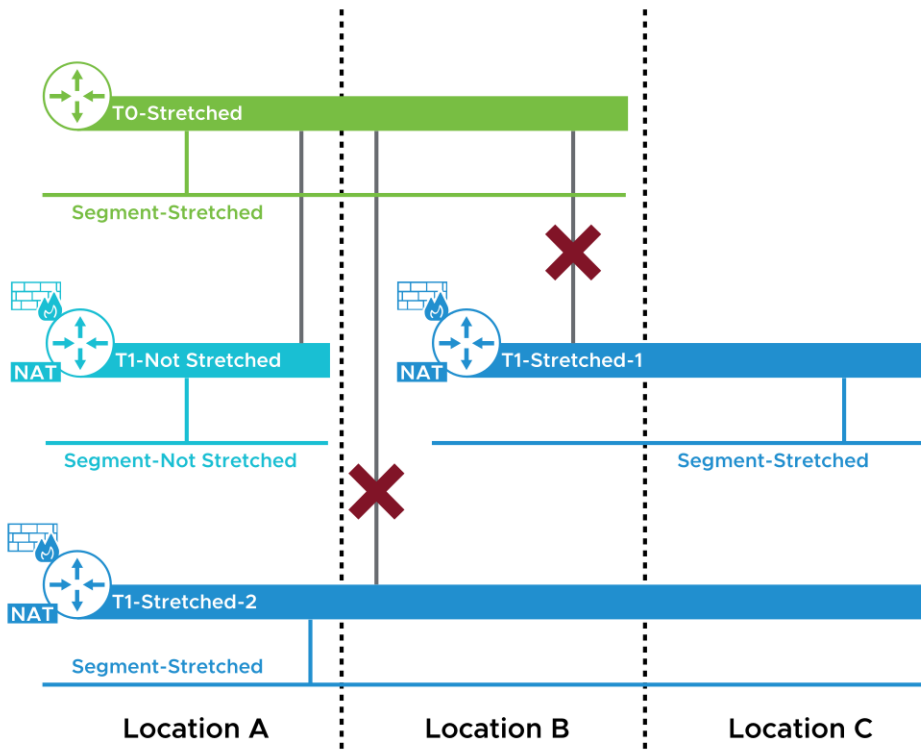
Spans have the following properties:

- The span of the segment is equal to the span of the Tier-0 and Tier-1 gateways.
- The span of the Tier-0 gateway is equal to the span of the Tier-1-no services gateway, or conversely.
- The span of the Tier-0 gateway is equal to or a subset of the span of the Tier-1 gateway.

## 11-39 Tier-0 and Tier-1 Gateways: Logical Topologies (3)

In the example, the span of the T0-Stretched and both T1-Stretched gateways are not the same. These connections are not possible.

However, the span of T1-Not Stretched is a subset of the T0-Stretched span. The connection is possible.



The example shows how a stretched and nonstretched network can co-exist.

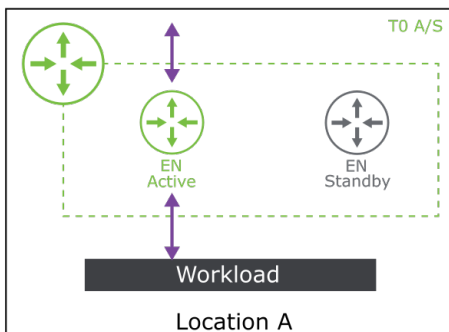
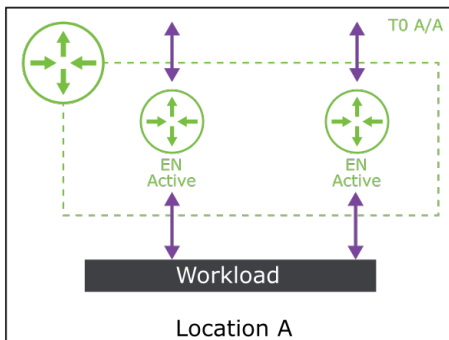
A nonstretched Tier-1 gateway is local to Location A only and Tier-0 gateway is stretched across Location A and Location B. The connection is possible because the nonstretched Tier-1 gateway is a subset of the Tier-0 Stretched gateway.

A connection is not possible between T1-Stretched-1 and T1-Stretched-2 to T0-Stretched because T0-Stretched is not stretched to Location C.

## 11-40 Single-Location Tier-0 Gateway Deployments

GM supports the following configuration for Tier-0 gateways for each location:

- Tier-0 is deployed in A/A mode in a location:
  - All Tier-0 gateways are active on all the NSX Edge nodes in the edge cluster.
  - The traffic ingresses or egresses from all the edge nodes with the active Tier-0 gateway.
- Tier-0 is deployed in A/S mode in a location:
  - One Tier-0 gateway is active on one NSX Edge node and one standby gateway exists in the edge cluster.
  - The traffic ingresses or egresses from the edge nodes with the active Tier-0 gateway.

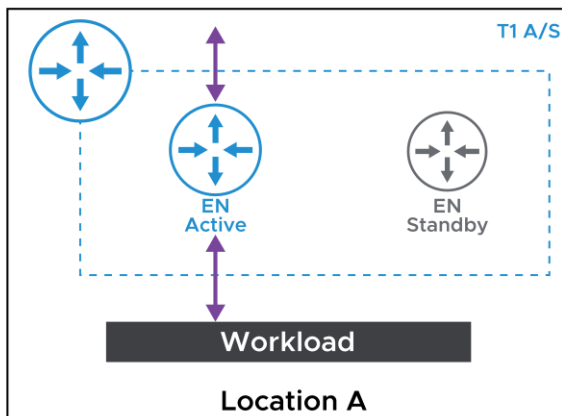


## 11-41 Single-Location Tier-1 Gateway Deployments

GM supports the configuration for the Tier-1 gateway for each location.

Tier-1 is deployed in A/S mode in a location:

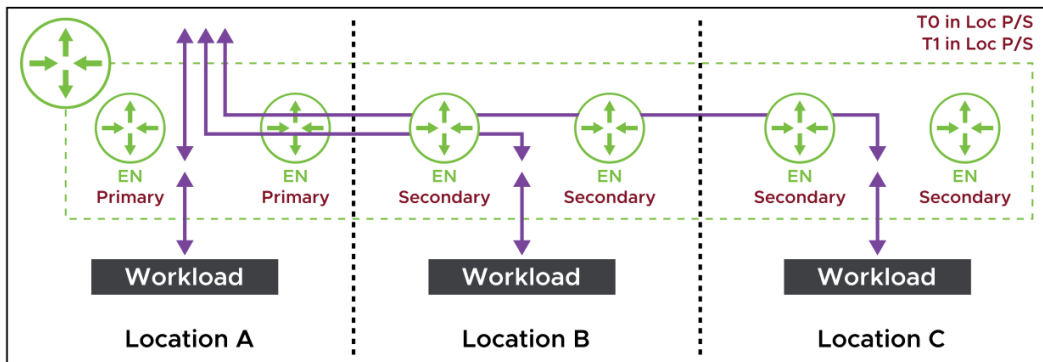
- The Tier-1 gateway is active on one NSX Edge node and is standby on another node.
- The traffic ingresses or egresses from the edge node deployed with the active Tier-0 gateway.



## 11-42 Multilocation Tier-0 and Tier-1 Gateway Deployments (1)

A location is configured as either primary or secondary:

- Only one location can be configured as primary, and all other locations are secondary.
- T0/T1 can be deployed in primary and secondary (P/S) locations:
  - Traffic to T0 from T1 and segments is contained in the location.
  - One location is active to send northbound egress traffic for a destination.



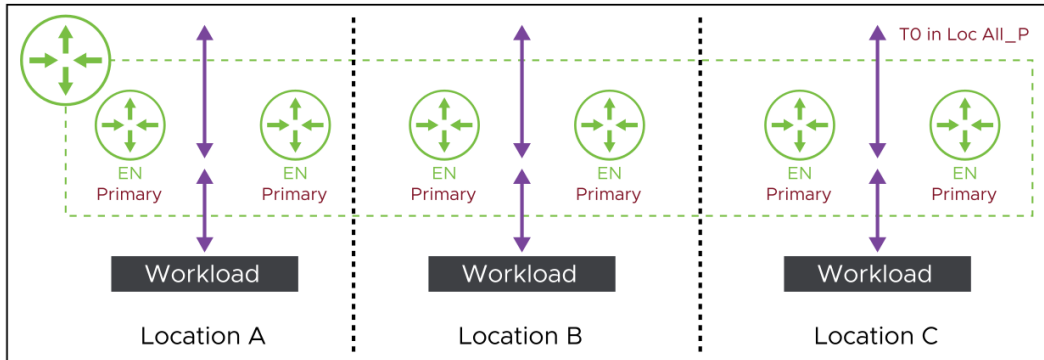
Location A is primary, and all northbound egress traffic is routed by using the primary Tier-0 gateways edge node.

The Tier-1 gateways at Location B and Location C send the traffic through RTEPs to the Location A edge uplink.

## 11-43 Multilocation Tier-0 and Tier-1 Gateway Deployments (2)

T0 can be deployed in all primary locations (All\_P):

- Traffic to Tier-0 gateway from Tier-1 gateway and segments is contained in the location.
- All locations have an active Tier-0 gateway to send northbound egress traffic.

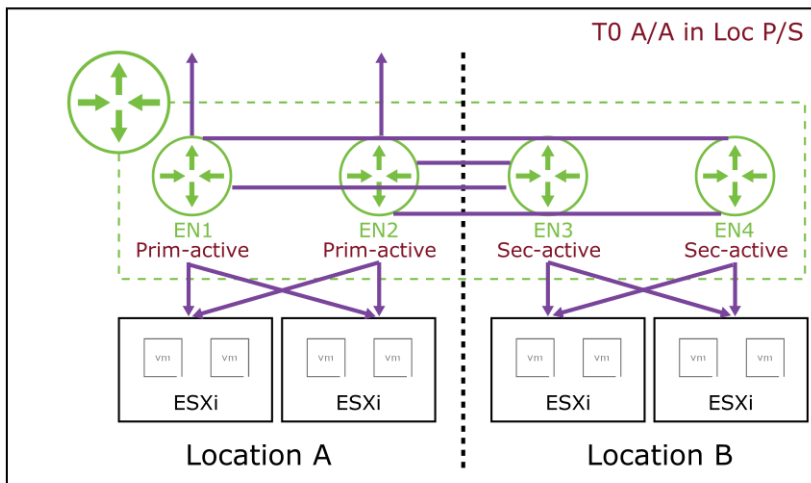


For all primary locations, the northbound egress traffic is routed locally.

## 11-44 Multilocation T0-Stretched Gateway Modes (1)

Tier-0 is deployed in A/A mode in P/S locations:

- For the Tier-0 gateway configured in the active-active HA mode, the Tier-0 gateway will be active on all the NSX Edge nodes in the edge cluster.
- For the Tier-0 gateways configured in the primary-secondary mode, the north-south traffic from all locations is forwarded to the Tier-0 gateways configured in a primary location.
- The Tier-0 gateway in the active-active high availability mode does not support stateful NAT. However, stateless NAT can be used.



In the diagram:

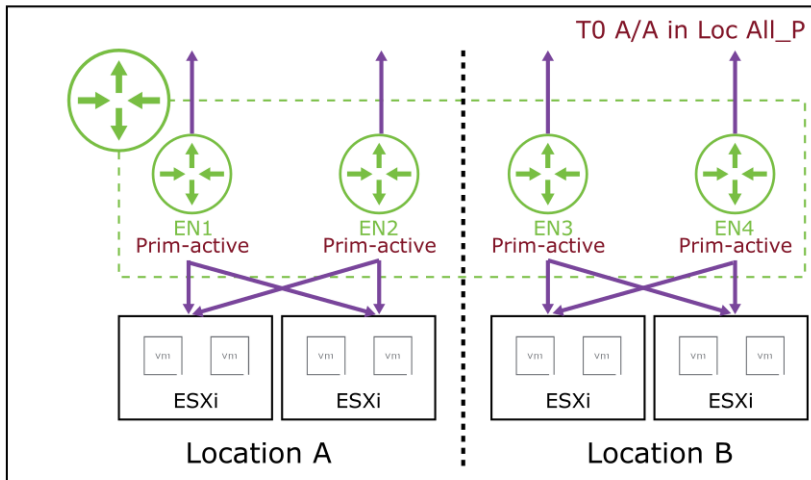
- Location A is primary, and Location B is secondary.
- Tier-0 gateways are deployed in active-active mode for both locations.
- RTEP IPs are configured on EN1, EN2, EN3, and EN4.
- EN3 and EN4 at Location B egress northbound traffic to either EN1 or EN2, or both, on Location A.



## 11-45 Multilocation T0-Stretched Gateway Modes (2)

Tier-0 is deployed in A/A mode in all primary locations:

- For the Tier-0 gateway configured in active-active HA mode, the Tier-0 gateway will be active on all the NSX Edge nodes in the edge cluster.
- For the Tier-0 gateway configured in a primary setup, northbound and southbound are sent and received through their respective Tier-0 gateways in their location.
- This configuration is also called A/A Local\_Egress.
- Tier-0 does not support services in this deployment mode:
  - Stateless NAT can be used.



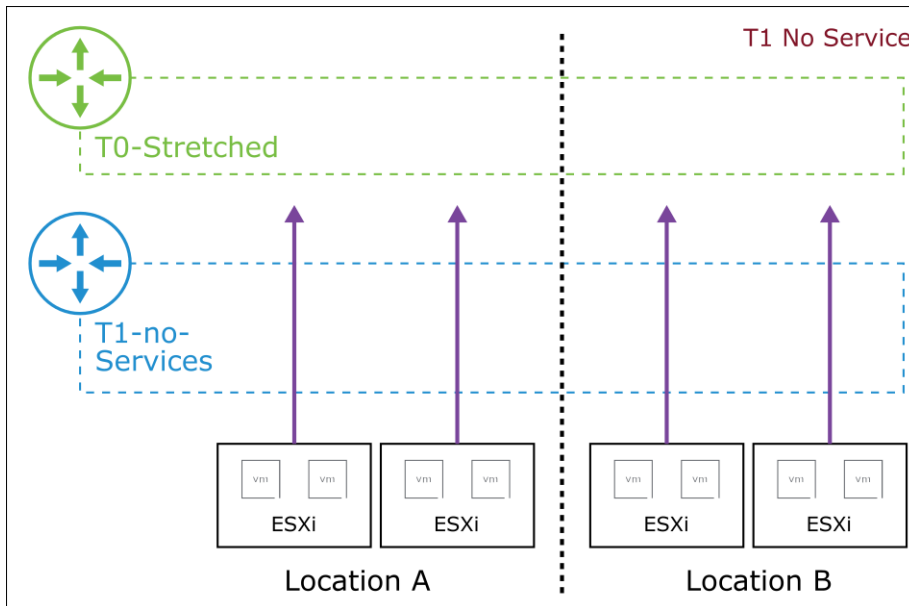
In the diagram:

- Both locations are primary.
- Tier-0 gateways are deployed in active-active mode for both locations.
- In this use case for local egress, all Tier-0 sites route the northbound traffic locally.

## 11-46 Multilocation T1-Stretched Gateway Modes (1)

Tier-1 is deployed without services:

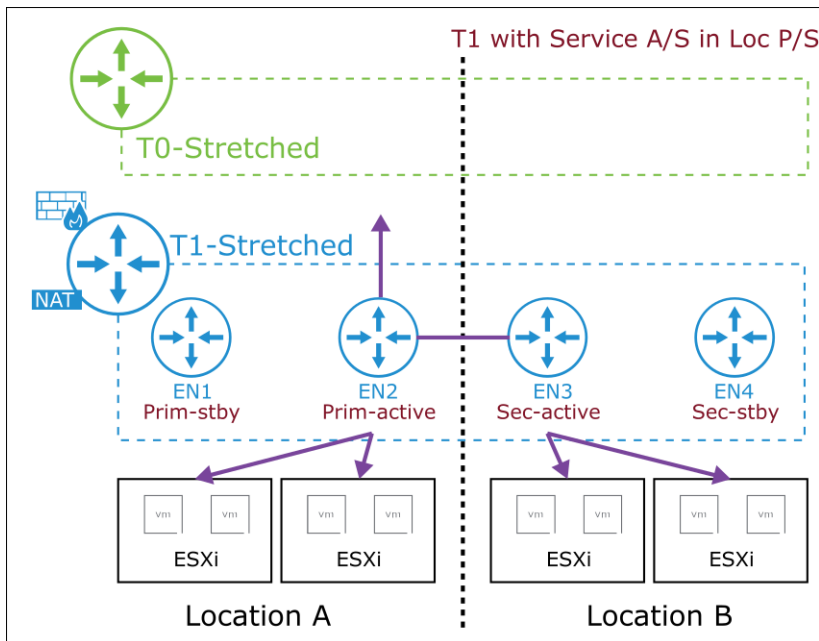
- Tier-1 is deployed without services in all locations.
- Only Distributed Router (DR) is realized because services are not configured and Service Router (SR) does not exist.
- Tier-1 routes the northbound traffic directly to T0-Stretched on the hypervisor.
- For workloads connected to T1-Stretched across locations, the communication happens through edge nodes (RTEP) configured for L2 Stretch.
- The T1-no-Services gateway does not require edge nodes for routing, but edge is required for L2 stretching.



## 11-47 Multilocation T1-Stretched Gateway Modes (2)

Tier-1 is deployed in A/S mode in P/S locations:

- The edge nodes in each location must support Tier-1.
- Services are enabled on Tier-1 in this deployment mode.
- Active edge nodes in both primary and secondary locations can receive southbound traffic for their respective locations.
- Only the primary location's active edge node can send the northbound traffic of both locations to stretched Tier-0.



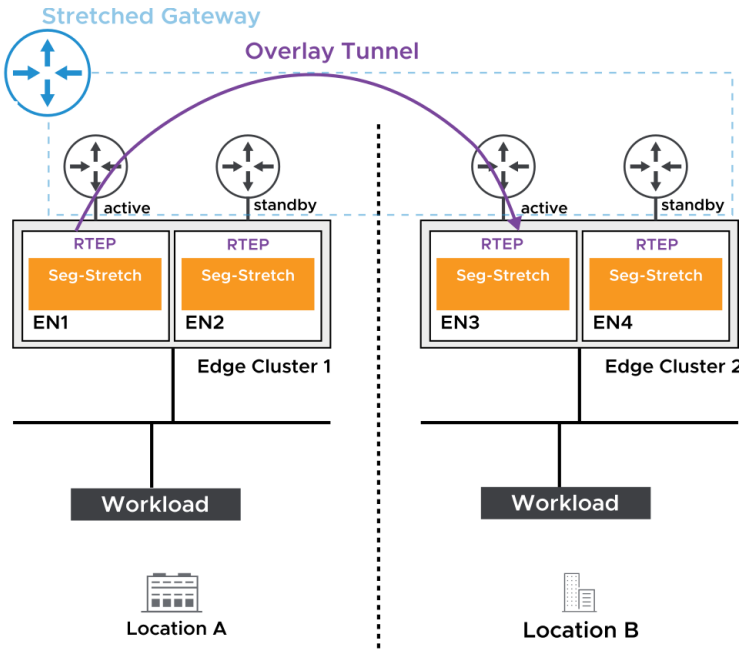
The concept is similar to active-standby Tier-0, where the active node on the primary site routes the traffic.

RTEP configured on Tier-0 routes the traffic across locations.

## 11-48 About RTEP

RTEP is an edge node IP that is used for edge node communication across sites:

- RTEPs use Geneve encapsulation to communicate.
- Only one RTEP IP can be configured per edge node.
- The RTEP configuration is done from the LM.



To configure RTEP:

1. Click **Site-A-GM** from UI Selector.
2. Click the **System** tab to display the configuration for Location Manager.
3. Click **Location Manager** to display details about the location where you want to create the RTEP.
4. On Site-A-LM, click **Networking**.

You can select the LM edge node cluster where you need to configure RTEP.

5. Click **CONFIGURE**.

You can navigate to Local Manager for the selected site.

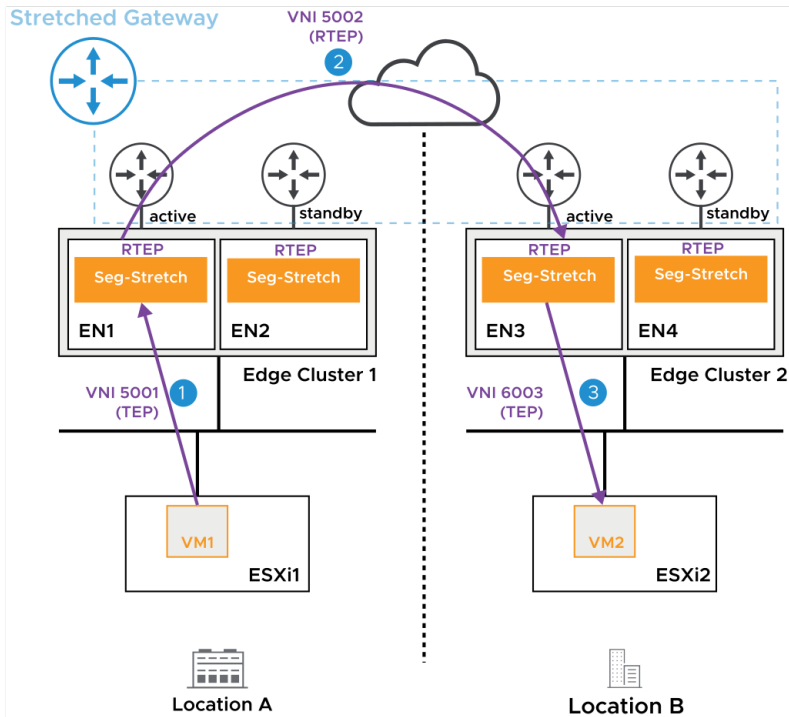
## 11-49 Stretched Layer-2 Network

The cross-location layer-2 communication is provided by the edge nodes of an edge cluster in each location.

This method avoids the management of many tunnels and BFD sessions between all hosts across locations.

The L2 stretched communication workflow includes:

1. The source ESXi host sends frames to the edge node (TEP-TEP communication).
2. The source edge node forwards a frame to the destination edge node (RTEP-RTEP communication).
3. The destination edge node forwards a frame to the destination ESXi host (TEP-TEP communication).

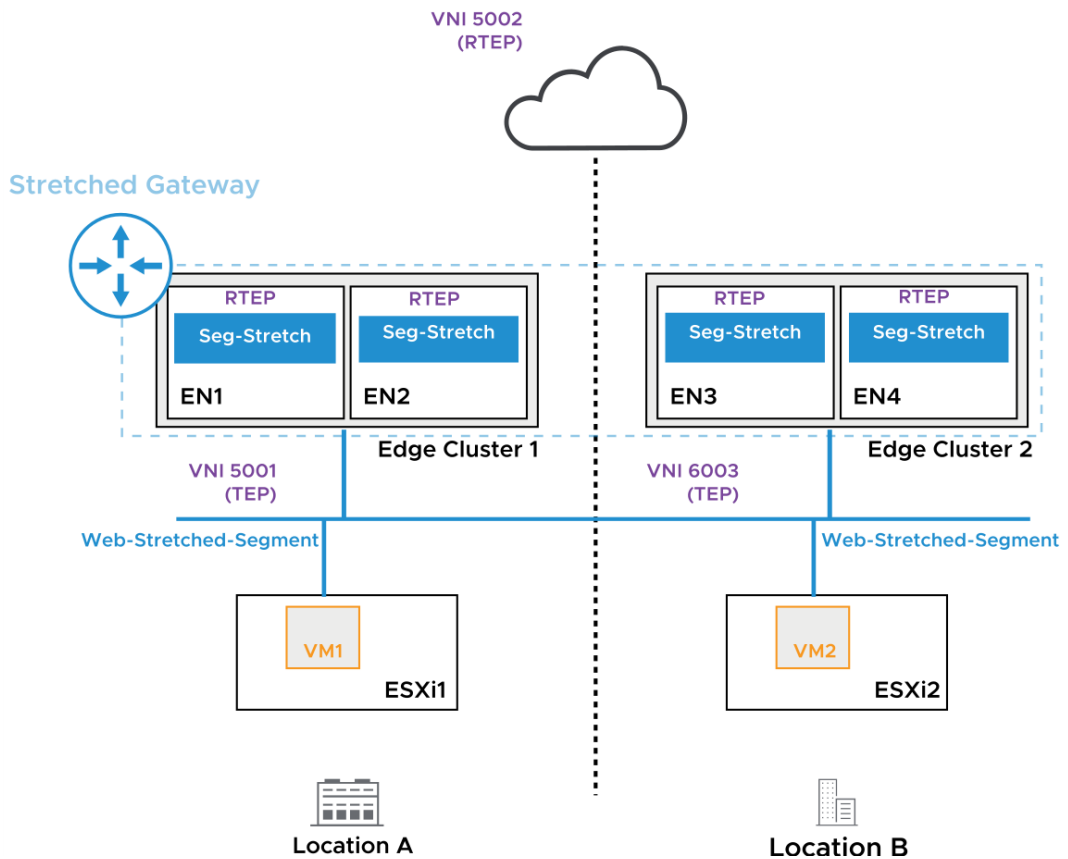


The MAC address of a remote VM is learned through RTEP on the edge nodes. The edge node passes this information to its local transport node.

## 11-50 Stretched L2: VNI Mapping

When a stretched segment is created from GM:

- GM requests each LM to create a local segment:
  - The VNI selection is local to LM and can be different VNIs in different locations.
- GM selects the VNI for RTEP.
- LM does the TEP-VNI:RTEP-VNI mapping:
  - This mapping is only available in edge nodes.



Example: If you create a stretched segment from GM and it is stretched to two locations, then the VNI id can be 5001 on one location. On another location, the stretched segment VNI id can be 6003.

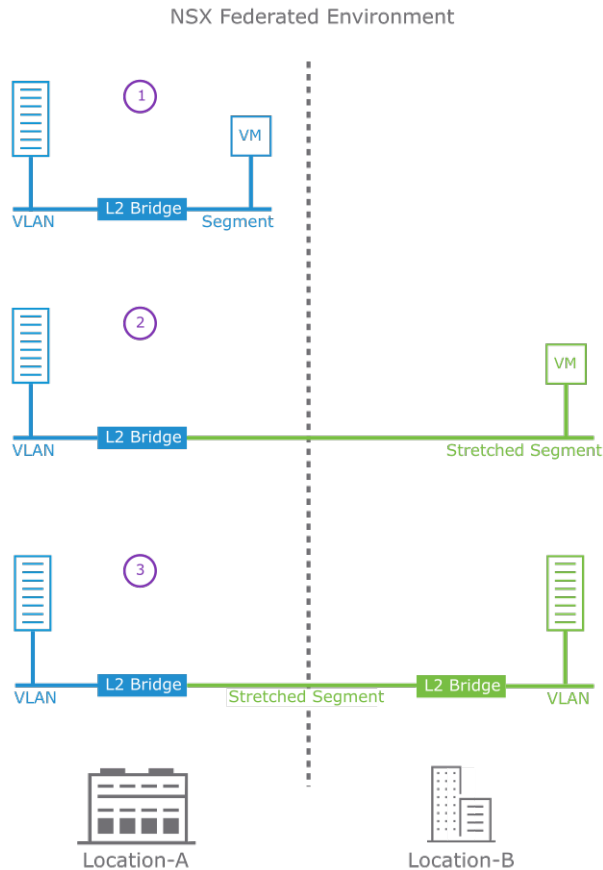
VNI can be different, but UUID of the stretched segment will be same across all locations.

## 11-51 About Federation L2 Bridging

NSX-T Data Center 3.2.2 supports L2 Bridging across locations.

L2 Bridging can be used to interconnect:

1. A VLAN-backed network to an overlay segment at the same location
2. A VLAN-backed network to a stretched overlay segment across locations
3. A VLAN-backed network to a VLAN-backed network, over a stretched overlay segment, across locations

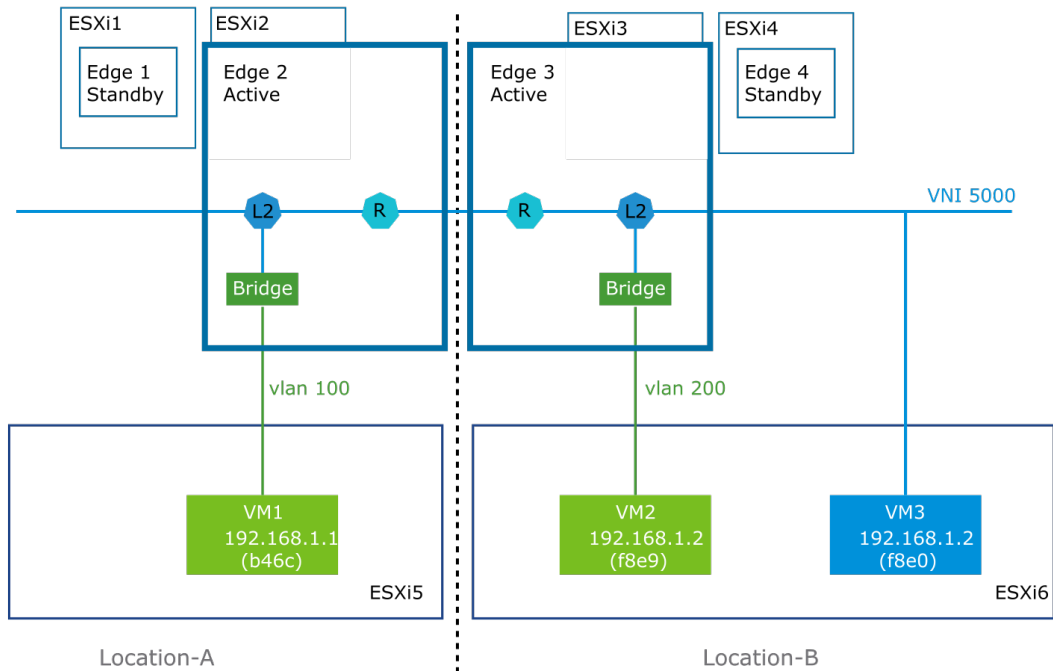


A stretched Tier-0 or stretched Tier-1 gateway is used to interconnect stretched overlay segments across locations.

## 11-52 Components of Federation L2 Bridging

Federation L2 Bridge components include:

- RTEP (R): An edge node interface used for edge node communication across sites
- Bridge: A connecting point between an overlay segment and a VLAN-backed network
- L2forwarder (L2): An edge node that is responsible for forwarding bridged traffic
- Edge Bridge Profile: Contains the L2 Bridge configuration details, including location, Edge cluster, primary node, and secondary node.

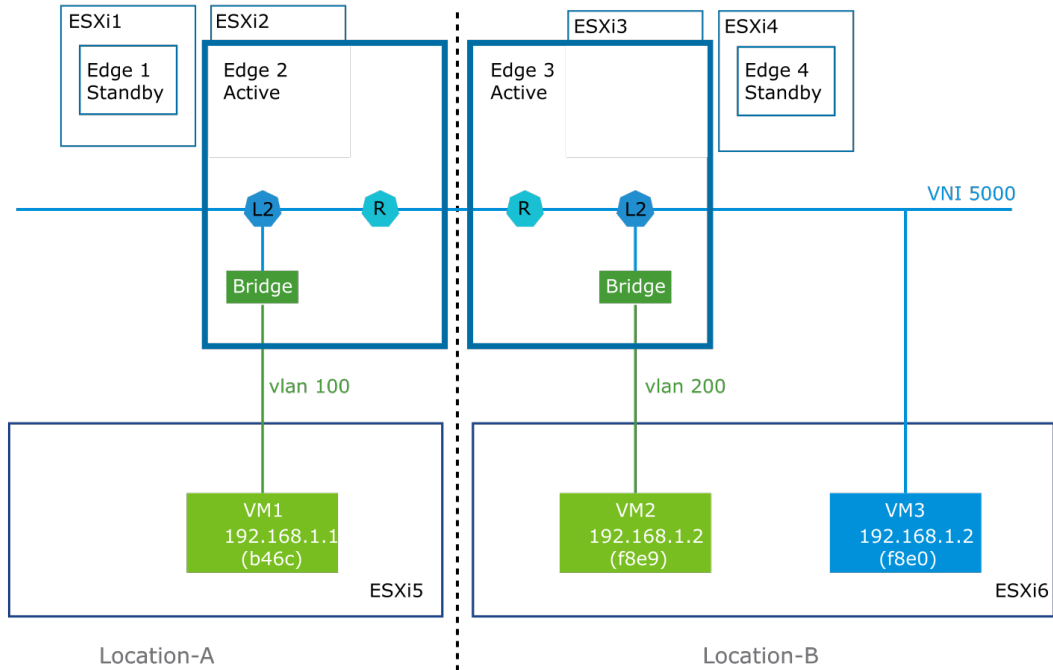




## 11-53 Federation L2 Bridge Communication

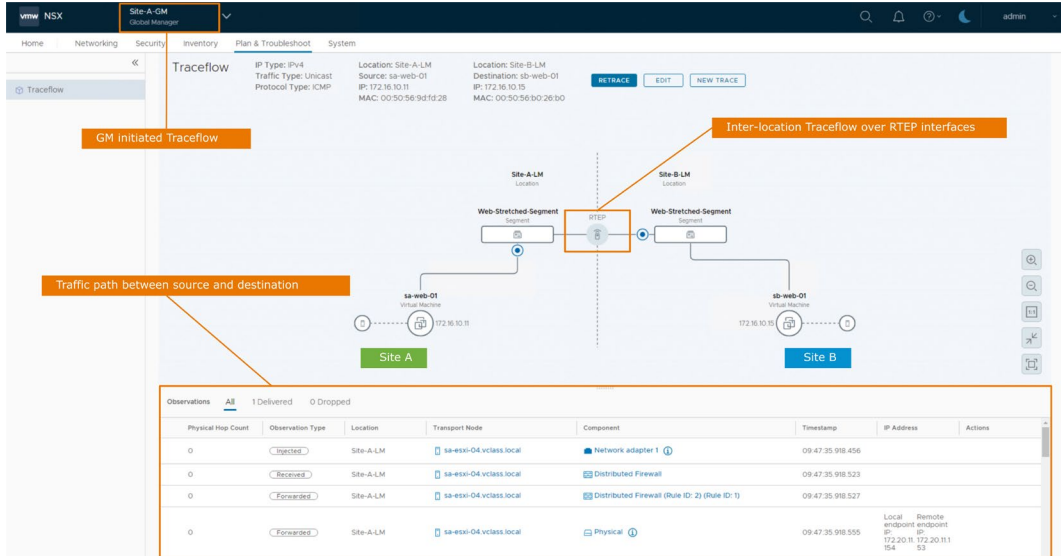
Federation L2 Bridge Communication is as follows:

- When VM1's MAC address is learned by the Bridge, Edge 2 will forward that MAC address to Edge 3 through the RTEP (R).
- The communication across locations, occurs between RTEP (R) interfaces on the Active Edge Node 1 and Active Edge Node 3.



## 11-54 Federation Traceflow

Traceflow analysis is supported across multiple locations, is initiated from the GM, and can assist with network troubleshooting in federated deployments.



Traceflow identifies the path that a packet takes to reach its destination or, conversely, where a packet is dropped along the way. Each entity reports the packet handling on input and output, to determine whether issues occur when receiving a packet or when forwarding the packet.

In this inter-location Traceflow example:

- Traceflow is from source location Site A, VM sa-web-01 to destination Site B, VM sb-web-01
- Traffic between sites is Geneve encapsulated between RTEP interfaces

## 11-55 Review of Learner Objectives

- Describe the stretched networking concepts in Federation
- Explain the supported Tier-0 and Tier-1 stretched topologies
- Explain Layer 2 concepts related to NSX Federation
- Identify network types that can be interconnected using L2 Bridging in federated environments

## 11-56 Lesson 4: Federation Security

### 11-57 Learner Objectives

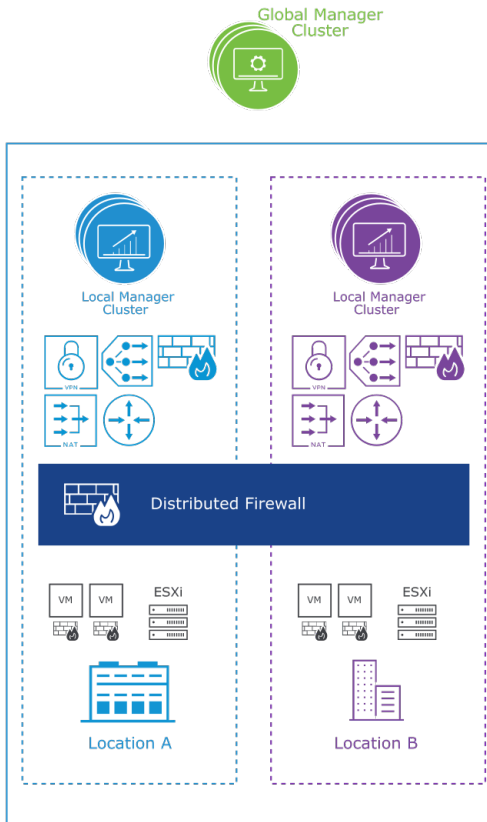
- Explain the Federation security use cases
- Explain the security configuration workflows
- Describe the Federation security components

## 11-58 Stretched Security in NSX Federation

The guiding security principles for NSX also apply to NSX Federation, except that the boundaries are extended to support multiple locations.

NSX Federation supports stretching of the following security constructs across multiple locations to centralize and simplify security policies:

- Distributed firewall
- Gateway firewall
- FQDN filtering
- L7 App ID context support



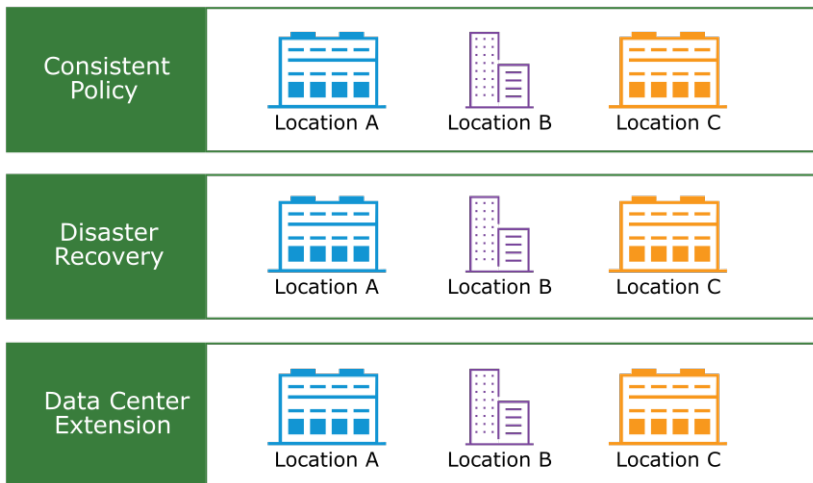
The following security features are not supported:

- Identity Firewall
- NSX Distributed IDS/IPS
- Network Introspection
- Endpoint protection
- Malware prevention
- Network detection and response

## 11-59 Use Cases for Security

Federation security has the following use cases:

- Provide consistent policy across deployments managed using NSX Federation
- Effective disaster recovery ensuring continuity of established security framework
- Extension of network and security framework to another location for increased capacity

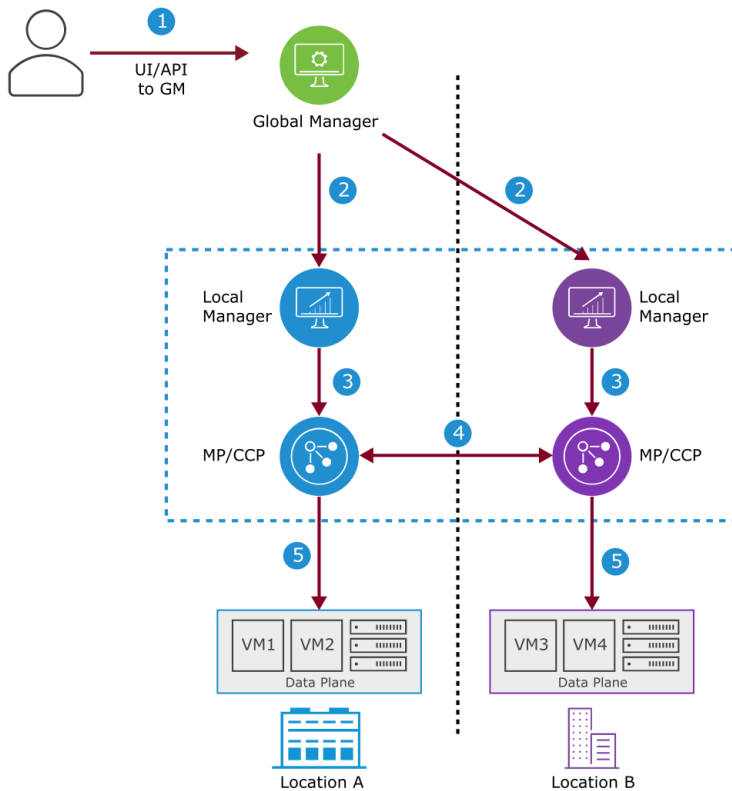


Federation provides central security for data centers managed on premises, such as data center extension with a centralized pane.

## 11-60 Security Configuration Workflow

The security configuration workflow includes the following steps:

1. The user sends the configuration to Global Manager (GM).
2. GM sends the configuration to Local Manager (LM) for each location.
3. LM forwards the configuration to MP/CCP.
4. The central control planes (CCPs) at each location synchronize the configuration across locations.
5. Each CCP sends the consolidated configuration to the data plane.



## 11-61 About Regions

A Region is a collection of locations, which is used to create focused groups for security and networking policies.

Regions can be global, regional, or local.

Some regions are created automatically after the onboarding process in GM.

You can create more regions.

The screenshot displays the 'Regions' page in the VMware NSX Global Manager interface. The page features a table with the following columns: Name, Locations, Groups, and Security Policies. The table lists four regions: Global, Region A+B, Site-A-LM, and Site-B-LM. Annotations highlight specific regions: 'Global Region (System-Based)' points to the 'Global' row, 'Regional Region (Manually Created)' points to the 'Region A+B' row, and 'Local Regions (System-Based)' points to the 'Site-A-LM' and 'Site-B-LM' rows. A search bar is located on the right side of the table.

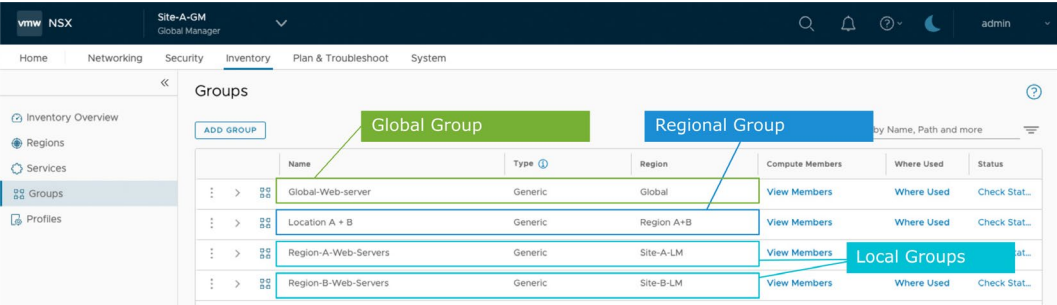
Name	Locations	Groups	Security Policies
Global	Site-A-LM Site-B-LM	0	0
Region A+B	Site-A-LM Site-B-LM	0	0
Site-A-LM	Site-A-LM	0	0
Site-B-LM	Site-B-LM	0	0

Global, Site-A-LM, and Site-B-LM are created by the system while registering and onboarding to GM of LM. Up to eight locations can appear on this page based on the number of supported locations in NSX Federation.

Region A+B is created manually. In the use case, regional groups were added based on the regions. Locations A and B were manually added.

# 11-62 About Groups

The NSX objects can be grouped to use in firewall rules that apply to Global, Regional, or Local regions.



Groups are defined based on the region. They can be Global, Regional, or Local.

The Global groups span across all sites in Federation and have the following characteristics:

- Created from the Global Manager NSX UI.
- Global groups are owned by NSX and are created with discovered objects. They can also be imported from a file (IP or MAC list).
- Users can only create, update, and delete Global Groups from the GM.
- Both GM and LM can read Global groups.
- Global groups cannot be used as nested members in LM-based policies.

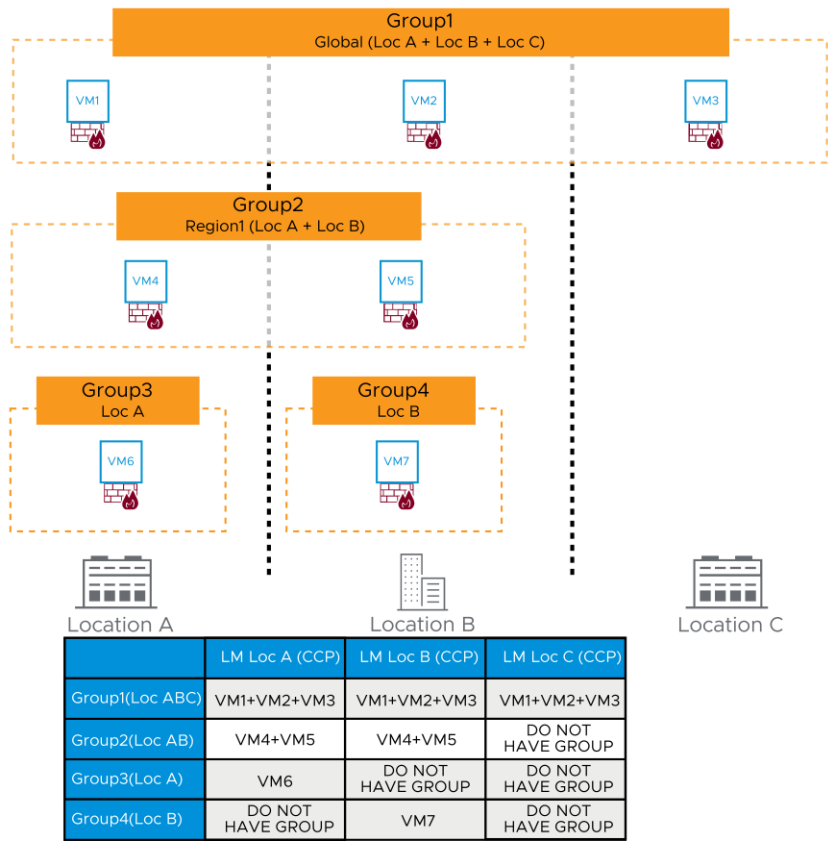
The Regional groups span across two or more locations, for example, Location A+B.

The Local groups are specific to the site, for example, Region-A-Web-Servers, Region-B-Web-Servers, and Region-A-App-Servers.



# 11-63 GM Groups and Span Example (1)

In this example, GM groups were created with various location spans.



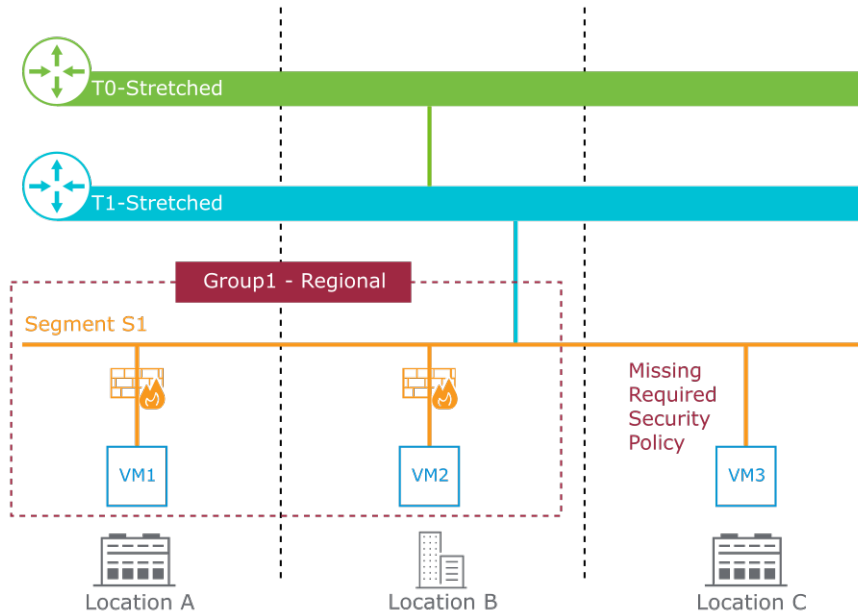
In the example, groups are as follows:

- Group1: Global, stretched to all sites, Locations A, B, and C
- Group2: Regional, stretched to Locations A and B
- Group3: Local to Location A
- Group4: Local to Location B

The GM sends groups to each LM within the group's span.

## 11-64 GM Groups and Span Example (2)

The span of a group must align with the span of the objects to be included in that group.



In the example, Group1 was created using Segment S1 as its membership:

- The span of Group1 is Location A and Location B.
- Segment S1 spans Location A, B, and C.
- The span of the group does not align with the span of the required objects, resulting in a security exposure.
- The required security policy is not applied to VM3.

## 11-65 Group Membership Criteria

You dynamically assign members to a group based on one or more criteria

Set Members | Global-Web-Servers Region: Global ×

Add Compute Members either by creating or by directly adding them.

Select Group Type ⓘ

☒ Generic ☐ IP Addresses Only

Membership Criteria (1) Members (0) IP Addresses (0) MAC Addresses (0)

+ ADD CRITERION Maximum: 5 Criteria

▼ Criterion 1 🗑️

Virtual Machine	Computer Name	Contains	web
<div><div>Virtual Machine</div><div>NSX Segment</div><div>Segment Port</div><div>Distributed Port Group</div><div>Distributed Port</div><div>Group</div></div>	<div><div>Name</div><div>Tag</div><div>OS Name</div><div>Computer Name</div></div>	<div><div>Equals</div><div>Contains</div><div>Starts With</div><div>Ends With</div><div>Not Equals</div></div>	<div><div>+</div><div>-</div></div>

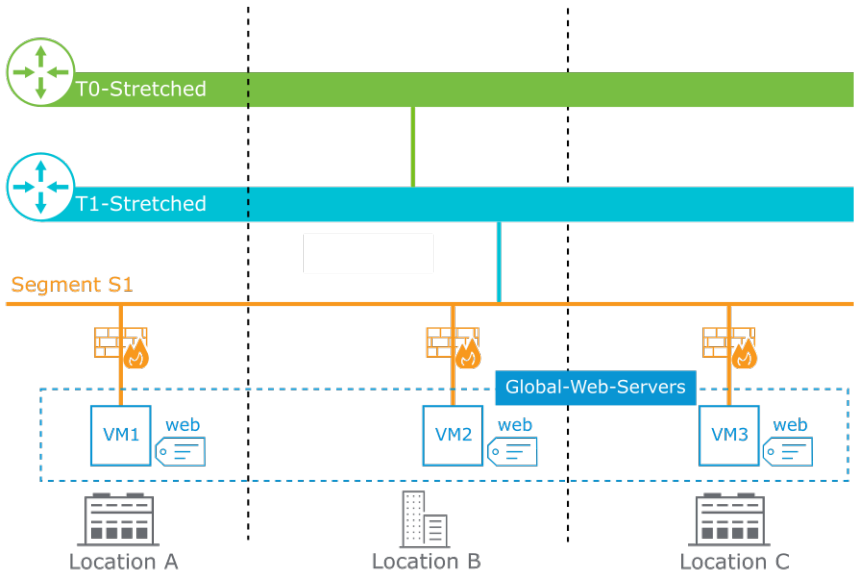
A criterion can have one or more conditions:

- NSX uses the logical AND operator after each condition within a criterion.
- Multiple criteria can be combined where OR is the default logical operator between conditions, and where an option exists to use the logical AND operator.

In this example, VMs with a computer name that starts with web are dynamically added to the Global-Web-Servers global group.

# 11-66 Group Membership Based on the VM Tag (1)

Group membership criteria can include VM-based tags.

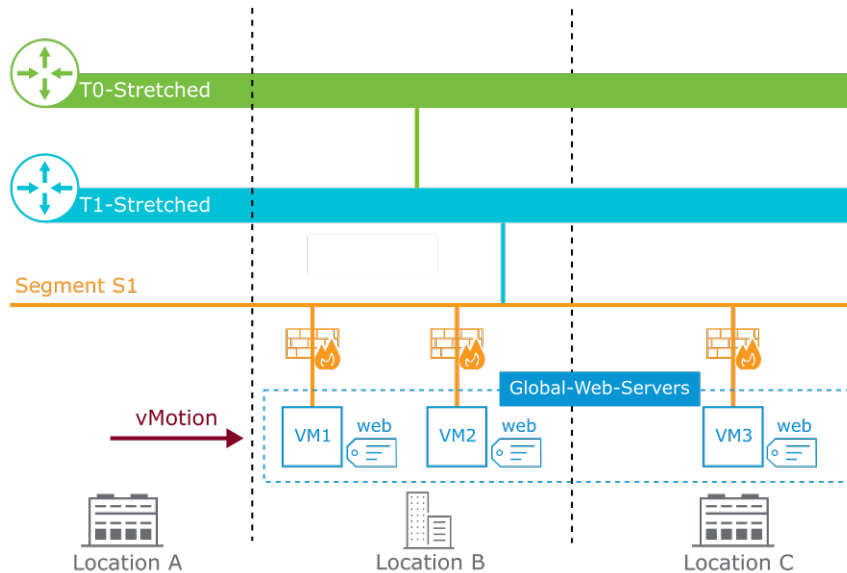


In the example, the membership criteria for the group, Global-Web-Servers, is based on the VM tag web.

## 11-67 Group Membership Based on the VM Tag

### (2)

Tags are applied to VMs even after migration with vSphere vMotion to Location B, which allows them to maintain group membership.



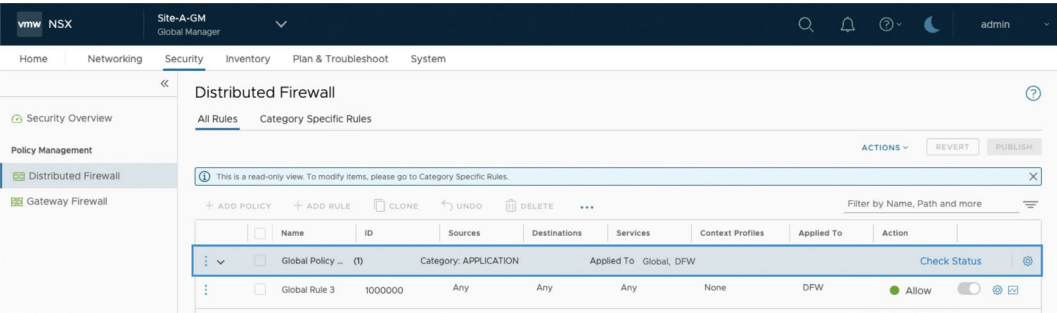
In the example, the Global-Web-Servers group members are maintained when VM1 is migrated using vSphere vMotion to Location B.

# 11-68 About GM-Based Policy

A GM-based policy is a collection of one or more firewall rules.

You can configure the following settings for a policy:

- **Applied To** in the policy is set to **DFW**:
  - All logical switch ports (VMs and containers) of the span receive the rules in that section.
- **Applied To** in the policy is set to **Group**:
  - All group members (VMs and containers) receive the rules in that section.



GM can create FW in all categories except Ethernet and Emergency.

You can create a section and apply it to a location, groups, and so on.

When **Applied To** in the policy is set to **Group**, this setting overrides the **Applied To** for the DFW rule.

# 11-69 About GM-Based Rules

GM-based rules enforce traffic based on objects and tags.

You can configure the following settings for a rule:

- **Applied To** in the rule is set to **DFW**:
  - All logical switch ports (VMs and containers) of the span receive the rules within that section.
- **Applied To** in the rule is set to **Group**:
  - All group members (VMs and containers) receive the rules within that section.

vmw NSX

Site-A-GM  
Global Manager

Search

Notifications

Help

Dark Mode

admin

HomeNetworkingSecurityInventoryPlan & TroubleshootSystem

<<

Security Overview

Distributed Firewall

Gateway Firewall

Distributed Firewall

All RulesCategory Specific Rules

INFRASTRUCTURE (0)

ENVIRONMENT (0)

APPLICATION (3)

+ ADD POLICY

+ ADD RULE

CLONE

UNDO

DELETE

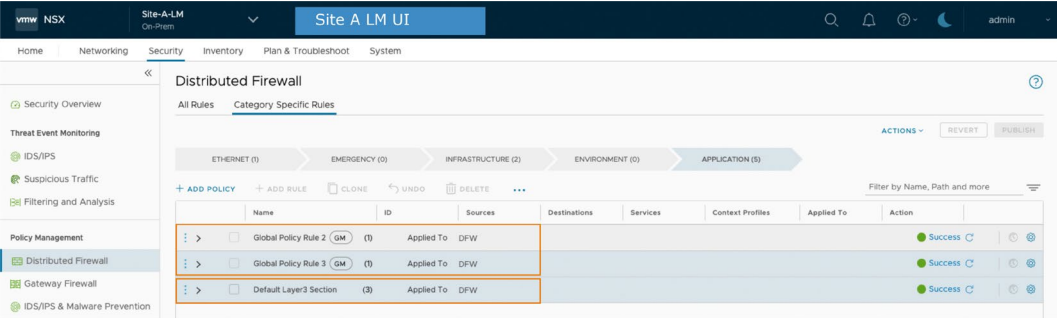
...

Filter by Name, Path and more

	Name	ID	Sources	Destinations	Services	Context Profiles	Applied To	Action	
⌵	Global Policy Rule 2	(1)	Applied To	Global, DFW					Check Status
⋮	Global Rule 2	1000001	Any	Any	Any	None	DFW	Allow	⌵
⌵	Global Policy Rule 3	(1)	Applied To	Global, DFW					Check Status
⋮	Global Rule 3	1000000	Any	Any	Any	None	app_vm_group	Allow	⌵

# 11-70 Overlap of GM and LM Sections

GM and LM can create gateway firewall and distributed firewall sections in the same category. For GM and LM sections created in the same category, GM sections are always at the top.



Except the Ethernet and Emergency categories where only LM can create sections:

- GM and LM sections are individually created under the Tier-0 or Tier-1 gateway firewall and under the distributed firewall.
- GM rules are always above LM.



# 11-71 GM DFW Management Enhancement

From NSX 4.0.1, DFW can be centrally enabled and disabled on all registered LMs from the GM.

The screenshot displays the NSX Distributed Firewall (DFW) management interface. The top navigation bar includes tabs for Home, Networking, Security, Inventory, Plan & Troubleshoot, and System. The left sidebar shows the Policy Management section with options for Distributed Firewall and Gateway Firewall. The main content area is titled "Distributed Firewall" and includes a "Global Manager UI" button. A "Settings" dialog box is open, showing the "General" tab for "Distributed Firewall". The dialog includes a section for "Activate Distributed Services Status for Locations" with a "TURN ON" button. Below this, a table lists locations and their DFW status:

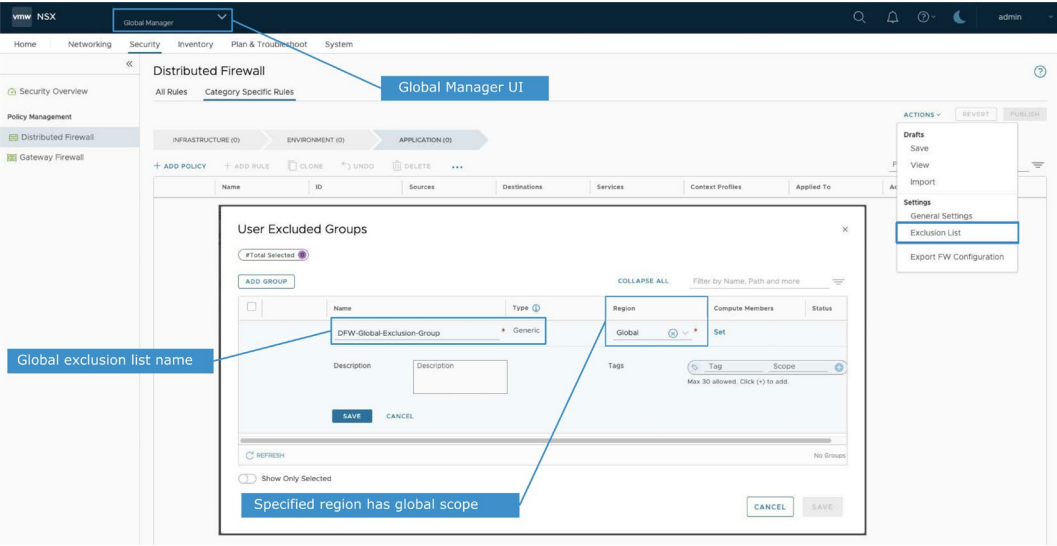
Location Name	Distributed Services Status
Site-A-LM	On
Site-B-LM	On

The "TURN ON" button is highlighted with a blue box and labeled "Centrally enable or disable DFW". The "Settings" dialog also includes a "REVERT" button and a "PUBLISH" button. The bottom right corner of the dialog shows "1 - 2 of 2" and "CANCEL" and "SAVE" buttons.

You cannot override the global DFW configuration setting from a LM.

# 11-72 Global DFW Exclusion List Enhancement

From NSX 4.0.1, you can globally exclude a set of virtual machines from distributed firewall protection centrally from the GM.



A DFW exclusion list excludes a set of virtual machines from distributed firewall protection.

Two exclusion lists exist on the LM. One list is from the GM and the other list is its own locally defined exclusion list. All excluded members of these two lists are sent to the Management Plane as a unified exclusion list, to be applied to the LM.

## 11-73 Time-Based DFW Rules Enhancement

From NSX 4.0.1, you can globally define time-based DFW rules, centrally from the GM, which are pushed to all registered LMs.

The screenshot displays the NSX Global Manager UI for Distributed Firewall configuration. The main interface shows the 'Distributed Firewall' section with tabs for 'All Rules' and 'Category Specific Rules'. A modal window titled 'Time Window' is open, providing a form to define a time window for a policy. The modal includes a table with columns: Name, Time Zone, Time Window, Where Used, and Status. The 'Global-Time-Wind' is set to 'UTC'. The 'Frequency' is 'WEEKLY'. The 'Time Window' is 'Every'. The 'Starting On' date is '5/26/2022' and the 'Ending On' date is '5/26/2022'. The 'Time Window' is set to 'From 10:00' to 'Till 10:30'. The modal also includes a 'Description' field and buttons for 'SAVE', 'CANCEL', and 'APPLY'. A 'REFRESH' button is also present. The modal is titled 'Time Window' and has a close button in the top right corner. A note at the bottom of the modal states: 'Note: Please take into account the time difference between the configured and the local time zone on Transport Node.'

Global Manager UI

Add time window

Time window properties

With time windows, security administrators can restrict traffic from a source or to a destination, for a specific time period.

## 11-74 Review of Learner Objectives

- Explain the Federation security use cases
- Explain the security configuration workflows
- Describe the Federation security components

## 11-75 Key Points

- Federation provides consistent policy and operational simplicity with multisite functionality for data centers.
- GM performs onboarding for multiple sites.
- GM creates stretched networks by using Tier-0 and Tier-1 routers.
- The edge node delivers cross-location communication to avoid connecting hypervisors across sites.
- The guiding security principles for NSX also apply to NSX Federation, except that the boundaries are extended to support multiple locations.

Questions?