CCIE Security v6

Authored By:

Khawar Butt

Hepta CCIE # 12353
(R/S, Security, SP, Voice, Storage,Data Center,Wireless)

CCDE # 20110020

Comprehensive coverage of the CCIE Security v6 Exam

Table of Contents

Initial E-Mail Server and Client Setup in the Network
Initializing the ESA Appliance from CLI
Initializing the ESA Appliance from GUI Using the System Setup Wizard
Configuring E-mail Communication using ESA as SMTP Relay Agent
Module 2 – Configuring Incoming Filters Using ESA
Configuring Incoming Filter – Blocking E-Mails with Strings
Configuring Incoming Filter – Blocking E-Mails based on File Size
Module 3 – Configuring Outgoing Filters Using ESA
Configuring Outgoing Filters – Block E-Mails with Smart Filters
Configuring Outgoing Filters – Block E-mails based on File Types
Configuring Web Security Appliance (WSA)
Module 1 – Initial Configuration of the Web Filtering Appliance [WSA]
Basic Network Setup for Web Access
Initializing the WSA Appliance from CLI
Initializing the WSA Appliance from GUI Using the System Setup Wizard
Configuring the Router – WSA Relationship for WCCP
Module 2 – Configuring Web Filtering Using WSA
Creating Identities Used for Web Filtering
Category Based Blocking on the WSA
Configuring Custom URL Policies
Blocking / Permiting Specific Identities
Software Defined Access (SDA)
Module 1 – Configuring the Non-SDA Components
Configuring DNAC & ISE Integration
Configuring Border Switch Initial Configuration
Configure the Fusion Router to communicate to SDA Fabric via the Border
Module 2 – Configuring the DNAC Design Components
DNAC Design - Network Hierarchy – Site & Building
DNAC Design – Server Configuration – AAA, NTP etc
DNAC Design - Device Credentials
DNAC Design - IP Address Pools

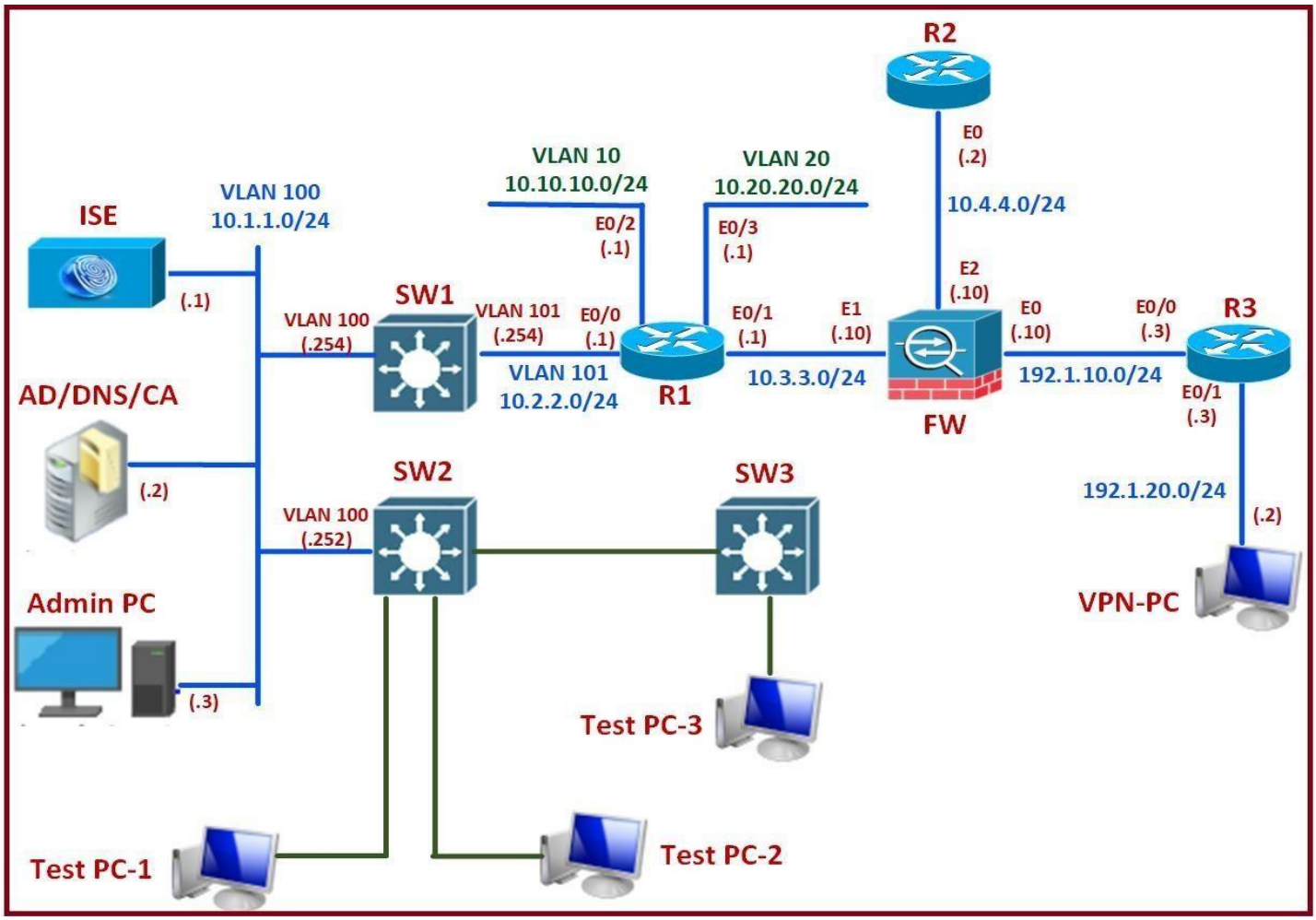
Module 3 – Using LAN Automation to discover the devices
DNAC Discovery – Discover the Seed Device (Border)
DNAC Provisioning - Assign Seed Device to Building
DNAC Provisioning – Enable LAN Automation to Discover the Fabric
Provision the devices to HQ Site
Module 4 – Creating & Configuring the Fabric & L3Handoff
Reserve the IP Pools for HQ Site for Overlay & Underlay
Create VNs for the Fabric
Create the Transit Network (L3HANDOFF)
Configure Host Onboarding
Provision the Control/Border Device
Provision the Edge Devices
Configure the Fusion Router to match the border configuration
Module 5 – Configuring ISE for SDA
Configure User & Groups on ISE
Configure Authorization Profiles for the DNAC VNs
Configure Authorization Policies for the DNAC VNs
Configure the DHCP Server to provide IP Configuration to Clients
Verifying Macro Segmentation
Module 6 – Configuring Micro-Segmentation
Create the SGTs
Re-configure ISE Authorization Policies to use SGTs
Using a default contract to block all communications between SGTs
Creating a Custom SG ACL Contracts to Control Traffic
Applying and verifying a Custom SG ACL- Contract

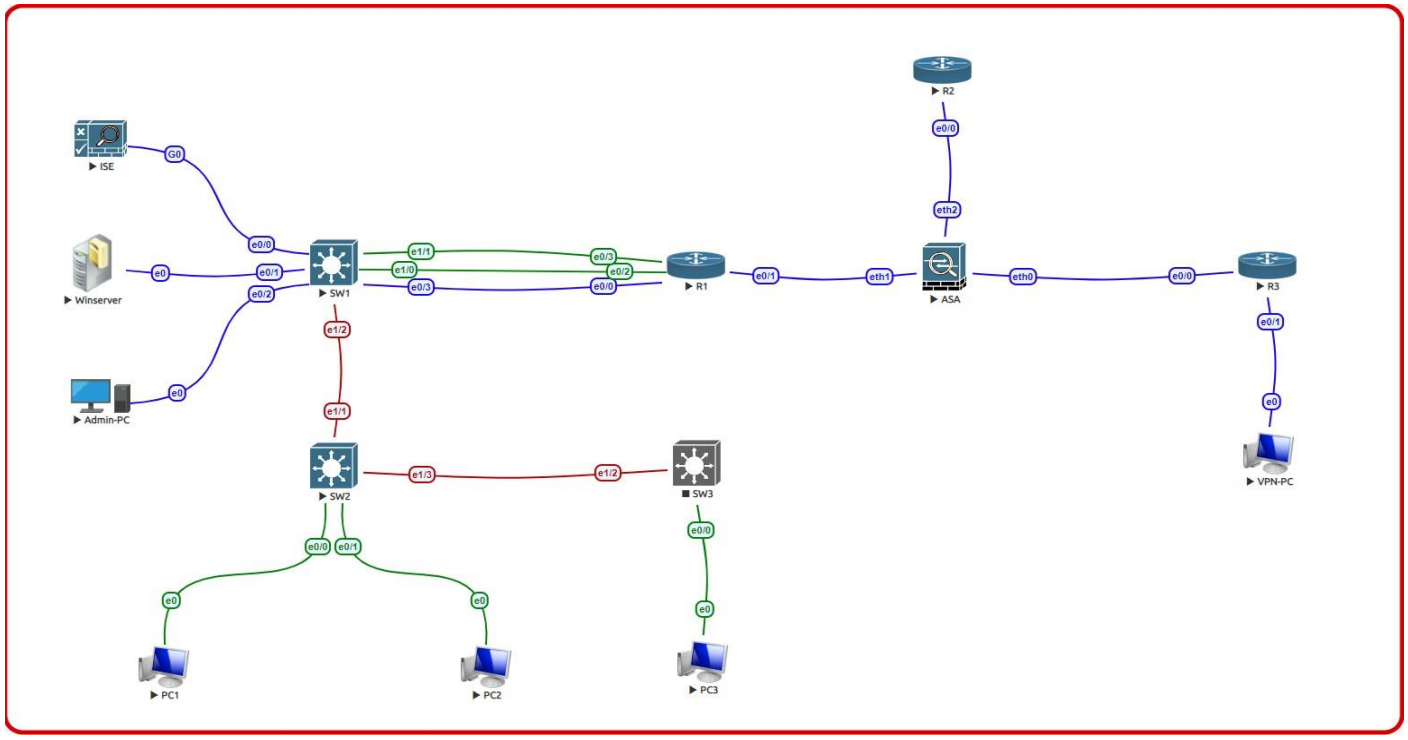
CCIE Security v6 – Identity Service Engine (ISE)

Module 1 – Initiailizing ISE

Module 1 – Initializing ISE

Lab 1 – Configuring the Base Network





Lab Scenario:

- Configuring the Base Network with VLANs, IP Addressing & Routing

Initial Setup:

- Not required.

Lab Tasks:

Task 1

Configure SW1 E 1/2 Interface as a Trunk towards SW2 E 1/1 Interface. Use Dot1q as the trunking encapsulation.

SW1
Interface E 1/2 switchport trunk encap dot1q switchport mode trunk
SW2
Interface E 1/1 switchport trunk encap dot1q switchport mode trunk

Task 2

Configure VLANs on SW1 & SW2 that will be used in the network. Create the following VLANS:

- VLAN 10
- VLAN 20
- VLAN 100
- VLAN 201

SW1
VLAN 10,20,100,101
SW2
VLAN 10,20,100,101

Task 3

Configure VLAN 100 based on the following:

- Assign ports on SW1 connecting to ISE, AD/DNS/CA Server & Admin PC to VLAN 100.
- Also configure SVI's for VLAN 100 on SW1 and SW2 based on the Logical Diagram above.
- Configure the Admin PC with the following configuration:
  - IP Address: 10.1.1.3/24
  - Default Gateway: 10.1.1.254
  - DNS: 10.1.1.2

SW1

```
Interface range e 0/0-2
 switchport mode access
 switchport access vlan 100
!
IP routing
!
Interface VLAN 100
 Ip address 10.1.1.254 255.255.255.0
 No shut
```

SW2

```
IP routing
!
Interface VLAN 100
 Ip address 10.1.1.252 255.255.255.0
 No shut
```

Admin PC

Ethernet Interface 1:

IP Address: 10.1.1.3
Subnet Mask: 255.255.255.0
Default Gateway: 10.1.1.254
DNS-Server: 10.1.1.2

Task 4

Configure VLAN 101 based on the following:

- Assign the Port on SW1 connecting to R1 E 0/0 to VLAN 101.
- Configure IP Addresses on SW1 (SVI 101) and R1 (E0/0) based on the logical diagram.

SW1
Interface E 0/3 switchport mode access switchport access vlan 101 ! Interface VLAN 101 Ip address 10.2.2.254 255.255.255.0 No shut
R1
Interface E 0/0 Ip address 10.2.2.1 255.255.255.0 No shut

Task 5

Configure VLAN 10 based on the following:

- Assign the Port on SW1 connecting to R1 E 0/2 to VLAN 10.
- Configure IP Addresses on R1 (E0/2) based on the logical diagram.

SW1
Interface E 1/0 switchport mode access switchport access vlan 10
R1
Interface E 0/2 Ip address 10.10.10.1 255.255.255.0 No shut

Task 6

Configure VLAN 20 based on the following:

- Assign the Port on SW1 connecting to R1 E 0/3 to VLAN 20.
- Configure IP Addresses on R1 (E0/3) based on the logical diagram.

SW1
Interface E 1/1 switchport mode access switchport access vlan 20
R1
Interface E 0/3 Ip address 10.20.20.1 255.255.255.0 No shut

Task 7

Configure IP Addresses on R1 (E 0/1) and ASA (E1) based on the logical diagram

R1
Interface E 0/1 Ip address 10.3.3.1 255.255.255.0 No shut
FW
Interface E1 Nameif Inside Ip address 10.3.3.10 255.255.255.0 No shut

Task 8

Configure IP Addresses on R2 (E 0/0) and ASA (E2) based on the logical diagram.

R2
Interface E 0/0 Ip address 10.4.4.2 255.255.255.0 No shut
FW
Interface E2 Nameif DMZ Security-level 50 Ip address 10.4.4.10 255.255.255.0 No shut

Task 9

Configure IP Addresses on R3 (E 0/0) and ASA (E0) based on the logical diagram.

R3
Interface E 0/0 Ip address 192.1.10.3 255.255.255.0 No shut
FW
Interface E0 Nameif Outside Ip address 192.1.10.10 255.255.255.0 No shut

Task 10

Configure IP Addresses on R3 (E 0/0) and VPN-PC 1st Ethernet Interface based on the logical diagram.

R3
Interface E 0/1 Ip address 192.1.20.3 255.255.255.0 No shut
VPN-PC
Ethernet Interface 1: IP Address: 192.1.20.2 Subnet Mask: 255.255.255.0 Default Gateway: 192.1.20.3

Task 11

Configure Routing for the L3 Network based on the following:

- Configure EIGRP on SW1, SW2, R1, R2 & ASA-FW.
- Enable all the Interfaces on SW1, SW2 & R1 in EIGRP 111.
- Only enable the Inside network in EIGRP 111 on the ASA Firewall.
- Inject a default route towards the Internal network on ASA using the Summary Command.
- Configure a Default Route on the ASA Firewall towards R3.

SW1
Router eigrp 111 Network 10.1.1.0 0.0.0.255 Network 10.2.2.0 0.0.0.255
SW2
Router eigrp 111 Network 10.1.1.0 0.0.0.255
R1
Router eigrp 111 Network 10.10.10.0 0.0.0.255 Network 10.20.20.0 0.0.0.255 Network 10.2.2.0 0.0.0.255 Network 10.3.3.0 0.0.0.255
R2

```
Router eigrp 111
 Network 10.0.0.0
```

ASA

```
Router eigrp 111
 Network 10.3.3.0 255.255.255.0
!
Interface E1
 Summary-address eigrp 111 0.0.0.0 0.0.0.0
!
Interface E2
 Summary-address eigrp 111 0.0.0.0 0.0.0.0
!
Route outside 0 0 192.1.10.3
```

Task 12

Configure R1 as a DHCP Relay agent for the 10.10.10.0/24 & 10.20.20.0/24 networks. Configure SW1 as a DHCP Server for VLANs 10,20 & 100.

Configuration parameters for VLAN 10 are:

- Range: 10.10.10.101 – 10.10.10.200
- Default Gateway: 10.10.10.1
- DNS-Server: 10.1.1.2

Configuration parameters for VLAN 20 are:

- Range: 10.20.20.101 – 10.20.20.200
- Default Gateway: 10.20.20.1
- DNS-Server: 10.1.1.2

Configuration parameters for VLAN 100 are:

- Range: 10.1.1.101 – 10.1.1.200
- Default Gateway: 10.1.1.254
- DNS-Server: 10.1.1.2

SW1

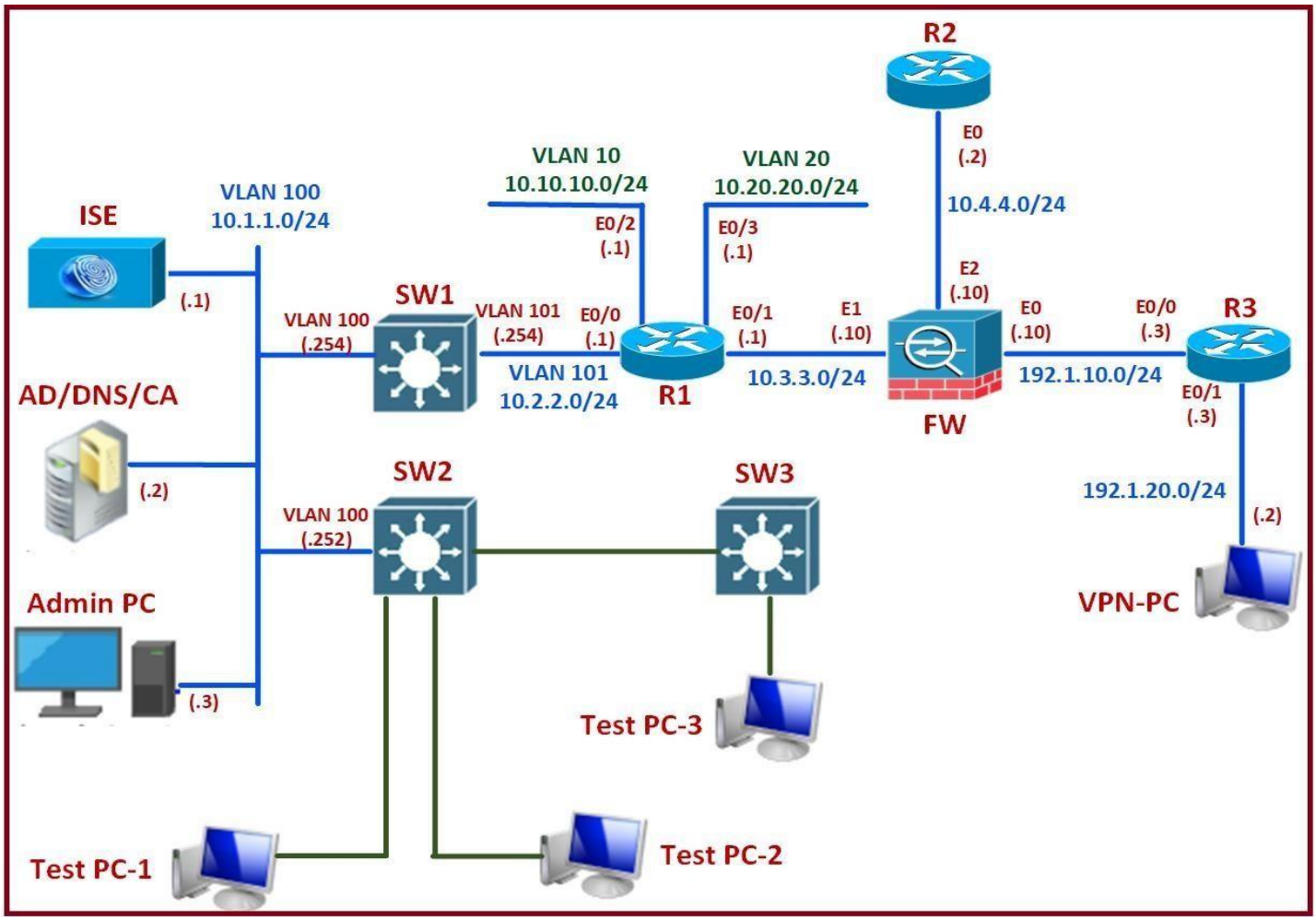
```
Ip dhcp excluded-address 10.10.10.1 10.10.10.100
Ip dhcp excluded-address 10.10.10.201 10.10.10.254
!
```

```
Ip dhcp excluded-address 10.20.20.1 10.20.20.100
Ip dhcp excluded-address 10.20.20.201 10.20.20.254
!
Ip dhcp excluded-address 10.1.1.1 10.1.1.100
Ip dhcp excluded-address 10.1.1.201 10.1.1.254
!
Ip dhcp pool VLAN10
 Network 10.10.10.0 /24
 Default-router 10.10.10.1
 Dns-server 10.1.1.2
!
Ip dhcp pool VLAN20
 Network 10.20.20.0 /24
 Default-router 10.20.20.1
 Dns-server 10.1.1.2
!
Ip dhcp pool VLAN100
 Network 10.1.1.0 /24
 Default-router 10.1.1.254
 Dns-server 10.1.1.2
```

R1

```
Interface E0/2
 Ip helper-address 10.2.2.254
!
Interface E0/3
 Ip helper-address 10.2.2.254
!
no ip forward-protocol udp 137
no ip forward-protocol udp 138
no ip forward-protocol udp 37
no ip forward-protocol udp 49
no ip forward-protocol udp 53
no ip forward-protocol udp 69
```

Lab 2 – Configuring Passwords in ISE



Lab Scenario:

- Configuring Passwords in ISE

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the ISE CLI Administrator password based on the following:

- The Default password on Eve-NG for ISE is Test123.
- It will prompt you to change the password.
- Change it to Cisco@123

ISE

```
ISE2-3 login: admin
Password:
You are required to change your password immediately (password aged)
Changing password for admin.
(current) UNIX password: Test123
Enter new UNIX password: Cisco@123
Retype new UNIX password: Cisco@123
```

Task 2

Change the ISE CLI admin password to **Kbits@123.**

ISE

```
ISE2-3/admin# password
Enter old password: Cisco@123
Enter new password: Kbits@123
Confirm new password:  Kbits@123
```

Task 3

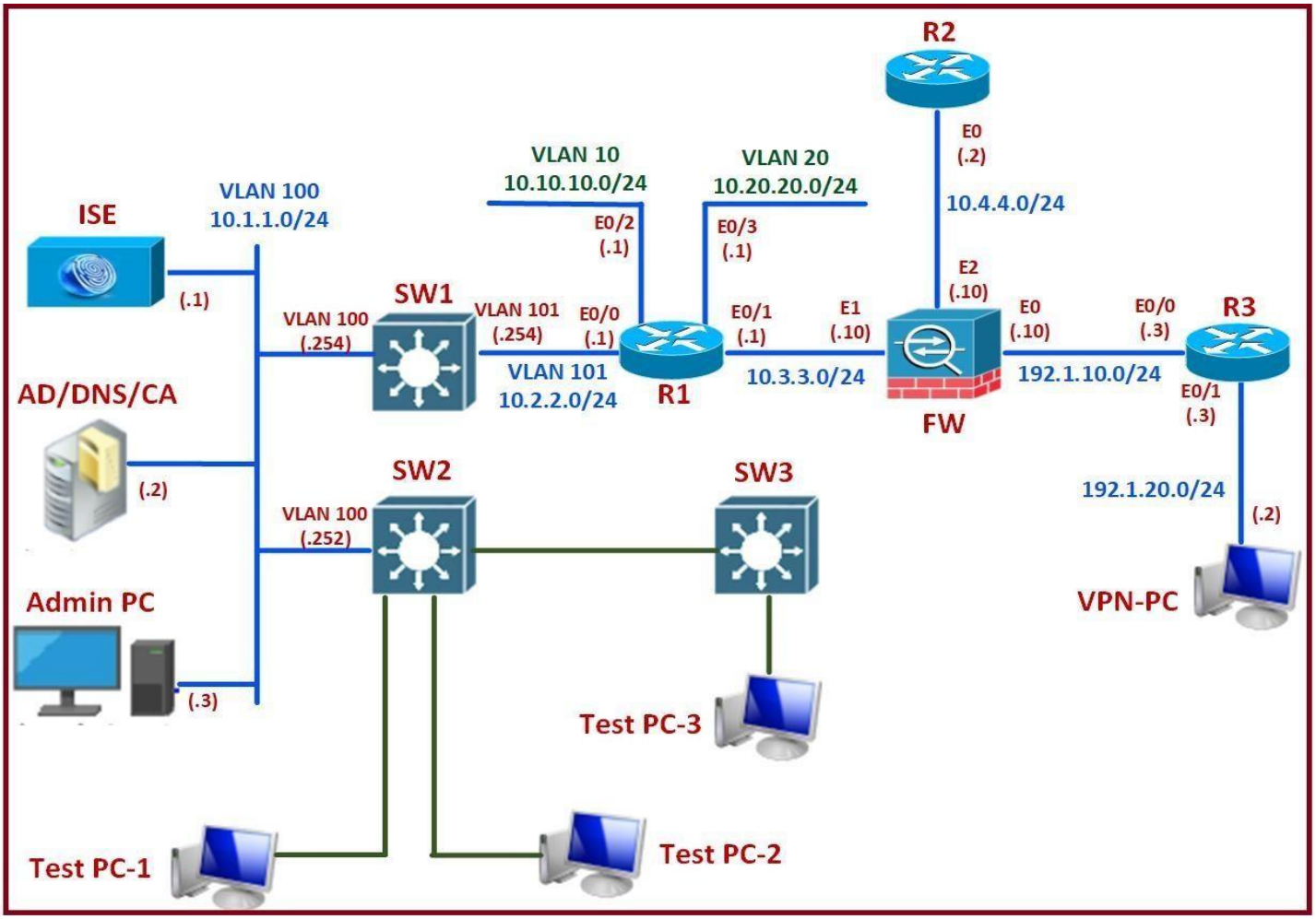
Reset the ISE GUI Admin password to **Kbits@123**.

ISE

```
ISE2-3/admin# application reset-passwd ise admin
Enter new password: Kbits@123
Confirm new password: Kbits@123

Password reset successfully.
```

Lab 3 – Configuring Network Configuration of ISE



Lab Scenario:

- Configure the Network Settings for ISE

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure/Verify ISE Network Parameters based on the following:

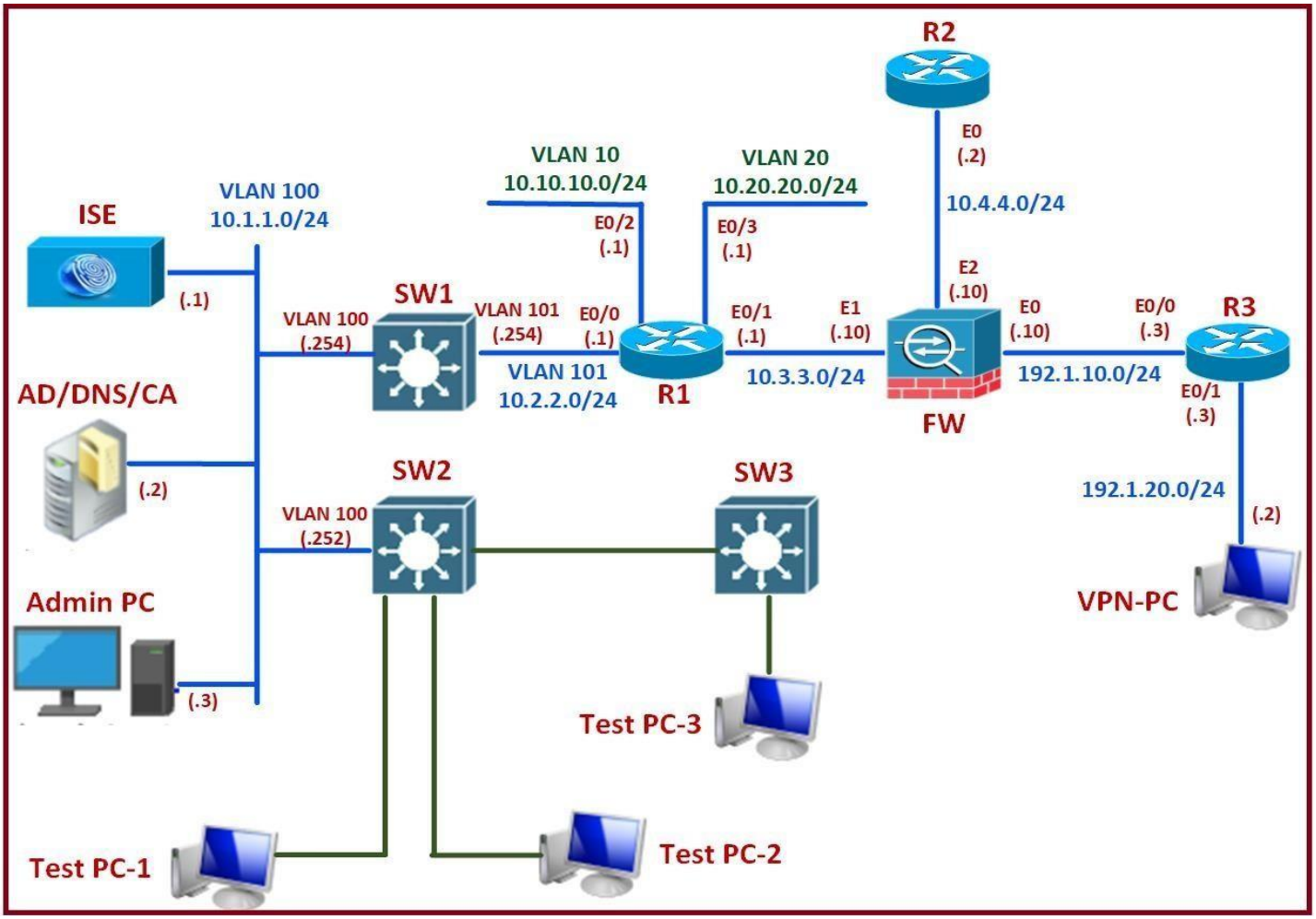
- IP Address: 10.1.1.1/24
- Default-Gateway: 10.1.1.254
- DNS Server (Name Server): 10.1.1.2
- Domain Name: kbits.live
- Hostname: ISE

ISE

```
Config t
!
hostname ISE1
!
ip domain-name Kbits.live
!
interface GigabitEthernet 0
 ip address 10.1.1.1 255.255.255.0
!
Ip default-gateway 10.1.1.254
!
no ip name-server 10.1.1.254
ip name-server 10.1.1.2
```

Note: It will prompt you to restart the ISE Application. Type “yes” to process. It will take a bit to come back.

Lab 4 – Initializing ISE - GUI



Lab Scenario:

- Configure RADIUS Log Settings in ISE.
- Enable Services.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure RADIUS settings based on the following:

- Configure ISE RADIUS setting to allow repeated Failures & suppress failied atempts. This is done to see the logs as we are testing configurations.
- Configure ISE RADIUS to display all Successful authentications in the log even if they are repeated. This is done to see the logs as we are testing configurations.

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Administration -> System -> Settings -> Protocols -> RADIUS"**

3. Uncheck "Reject RADIUS requests from clients with repeated failures".

4. Uncheck "Suppress repeated failed clients".

5. Uncheck "Suppress repeated successful authentications"

6. Click **Save.**

Task 2

Configure RADIUS settings based on the following:

- Configure ISE to run the Device Administration and pxGrid services.
- We will be using TACACS+ for Device Administration in a later section.
- We will be using pxGrid services for the ISE to FMC integration.

ISE

1. Browse to "**Administration -> System -> Deployment -> ISE1"**

2. Check to enable the following Services:

   - pxGrid
   - Device Admin Service.

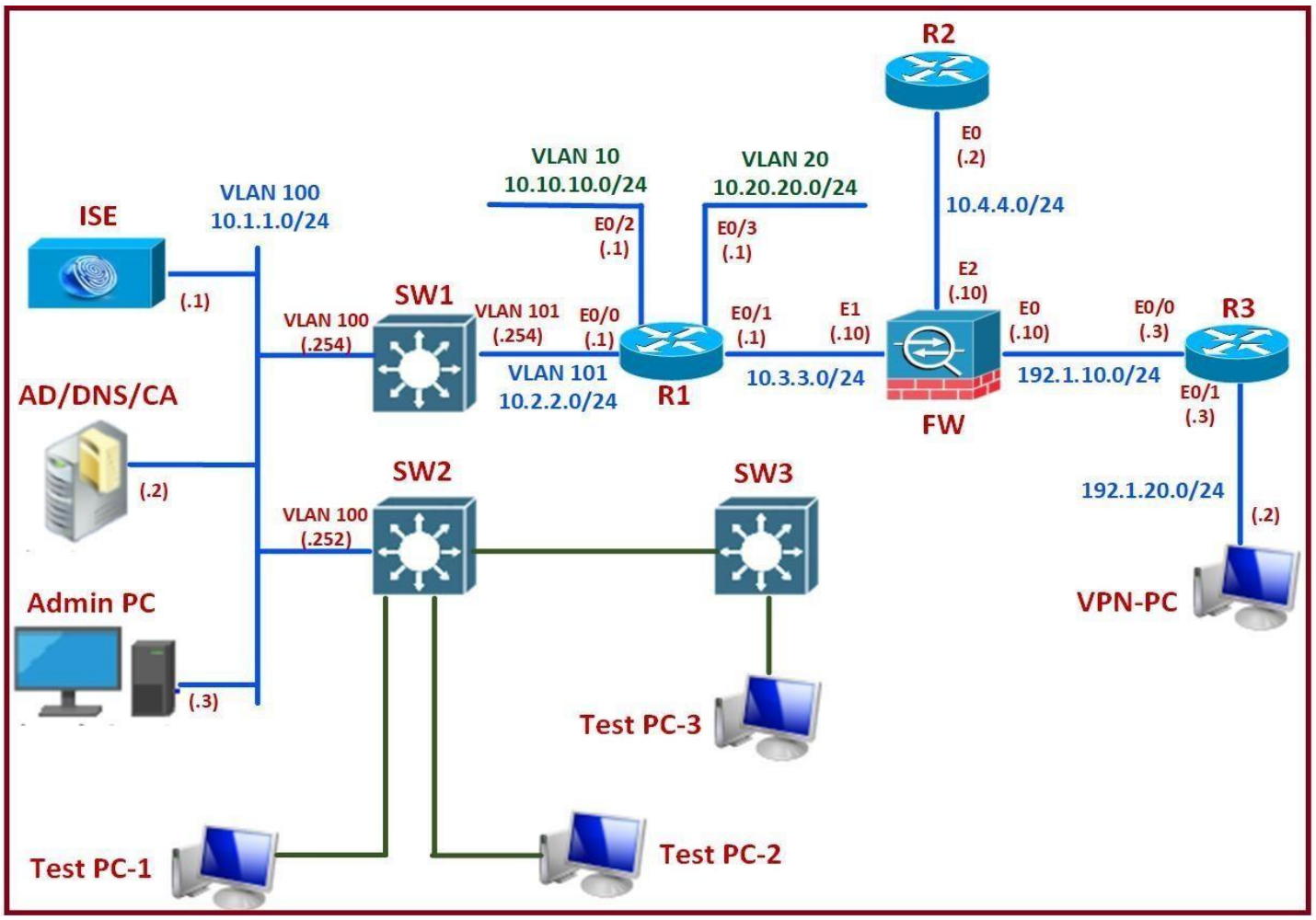
3. Click **Save.**

CCIE Security v6 – Identity Service Engine (ISE)

Module 2 – Configuring Wired 802.1x Authentication

Module 2 – Configuring Wired 802.1x Authentication

Lab 1 – Configuring ISE for Network Device Relationships



Lab Scenario:

- Configure Network Device Groups & Network Devices.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure Network Device Groups for Switches, Routers and Firewalls based on the following:

- Name: **Routers**
- Parent: All Device Types

- Name: **Switches**
- Parent: All Device Types

- Name: **Firewalls**
- Parent: All Device Types

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Administration -> Network Resources -> Network Device Groups -> Add"**

3. Create the Network Device Groups based on the above parameters.

4. Click **Save.**

Task 2

Configure the Switches based on the following parameters:

- Name: **SW1**
  - IP Address: **10.1.1.254/32**
  - Device Type: **Switches**
  - RADIUS: **Checked**
  - RADIUS Secret Password: **Cisco123***
  - TACACS+: **Checked**
  - TACACS+ Secret Password: **Cisco123***

- Name: **SW2**
  - IP Address: **10.1.1.252/32**
  - Device Type: **Switches**
  - RADIUS: **Checked**
  - RADIUS Secret Password: **Cisco123***
  - TACACS+: **Checked**
  - TACACS+ Secret Password: **Cisco123***

ISE

1. Browse to "**Administration -> Network Resources -> Network Devices -> Add**"

2. Create the Network Devices based on the above parameters.

3. Click **Save.**

Task 3

Configure the Routers based on the following parameters:

- Name: **R1**
  - IP Address: **10.2.1.1/32**
  - Device Type: **Routers**
  - TACACS+: **Checked**
  - TACACS+ Secret Password: **Cisco123***
- Name: **R2**
  - IP Address: **10.4.4.2/32**
  - Device Type: **Routers**
  - TACACS+: **Checked**
  - TACACS+ Secret Password: **Cisco123***

ISE

1. Browse to "**Administration -> Network Resources -> Network Devices -> Add**"

2. Create the Network Devices based on the above parameters.

3. Click **Save.**

Task 4

Configure the Firewall based on the following parameters:

- Name: **ASA-FW**
  - IP Address: **10.3.3.10/32**
  - Device Type: **Firewalls**
  - RADIUS: **Checked**
  - RADIUS Secret Password: **Cisco123***

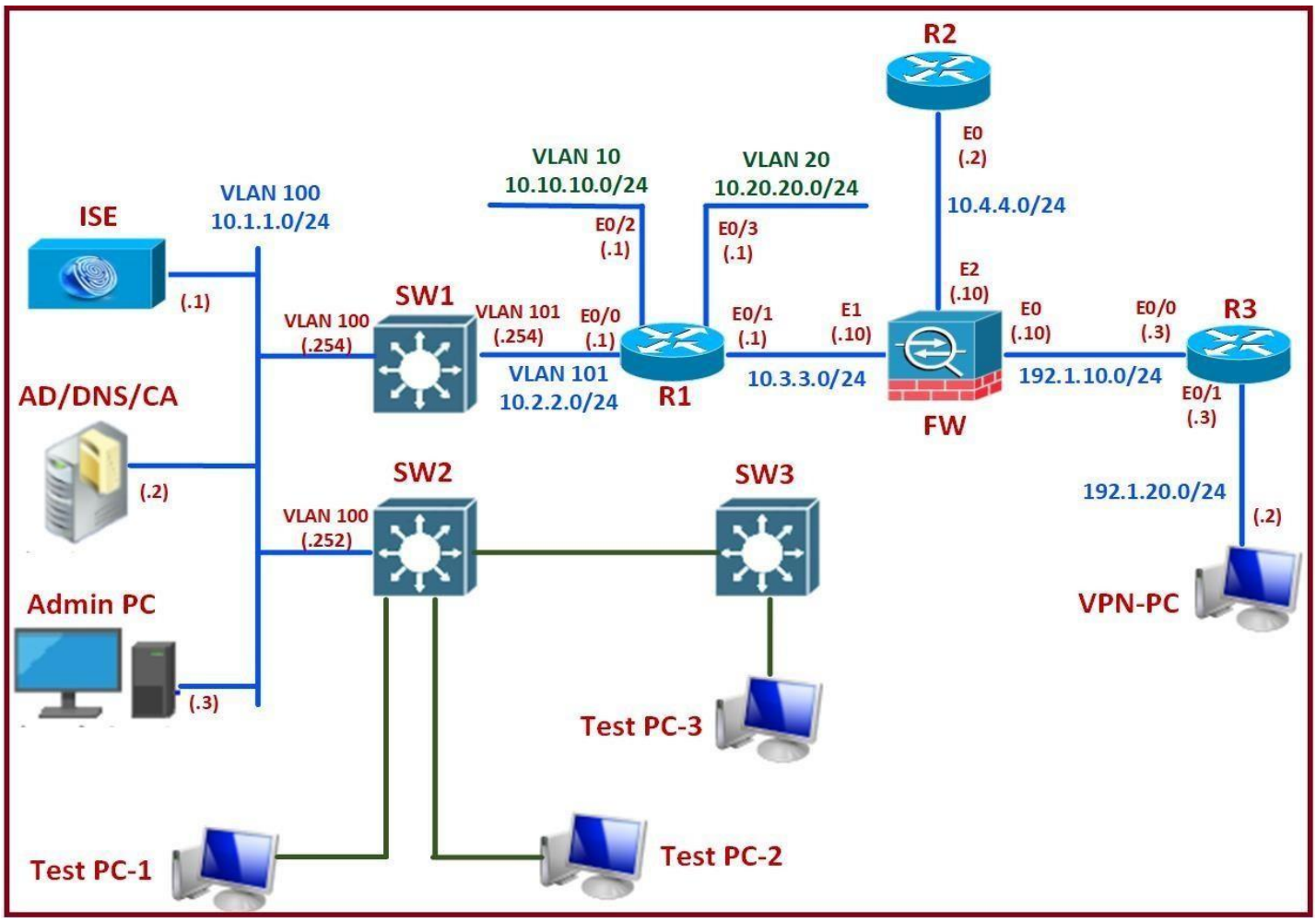
ISE

1. Browse to "**Administration -> Network Resources -> Network Devices -> Add**"

2. Create the Network Device based on the above parameters.

3. Click **Save.**

Lab 2 – Configuring Groups & Users in ISE



Lab Scenario:

- Configure User Identity Groups in ISE.
- Creating users (Identities) in ISE and assigning them to groups.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the following groups on ISE. They will be used for Dot1x Authenticatoin and Device Administrator Users.

- Name: **ISE-EMP**
- Name: **ISE-CON**
- Name: **SuperAdmins**
- Name: **RP-Admins**
- Name: **Switching-Admins**

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Administration -> Identity Management -> Groups -> User Identity Groups -> Create"**

3. Create the User Identity Groups based on the above Parameters.

4. Click **Save.**

Task 2

Create Users on ISE and assign them to the appropriate groups based on the following:

- Name: **ISE-1**
  - Password: **Cisco123***
  - Group: **ISE-EMP**
- Name: **ISE-2**
  - Password: **Cisco123***
  - Group: **ISE-CON**
- Name: **Admin1**
  - Password: **Cisco123***
  - Group: **SuperAdmins**
- Name: **Admin2**
  - Password: **Cisco123***
  - Group: **RP-Admins**
- Name: **Admin3**
  - Password: **Cisco123***
  - Group: **Switching-Admins**

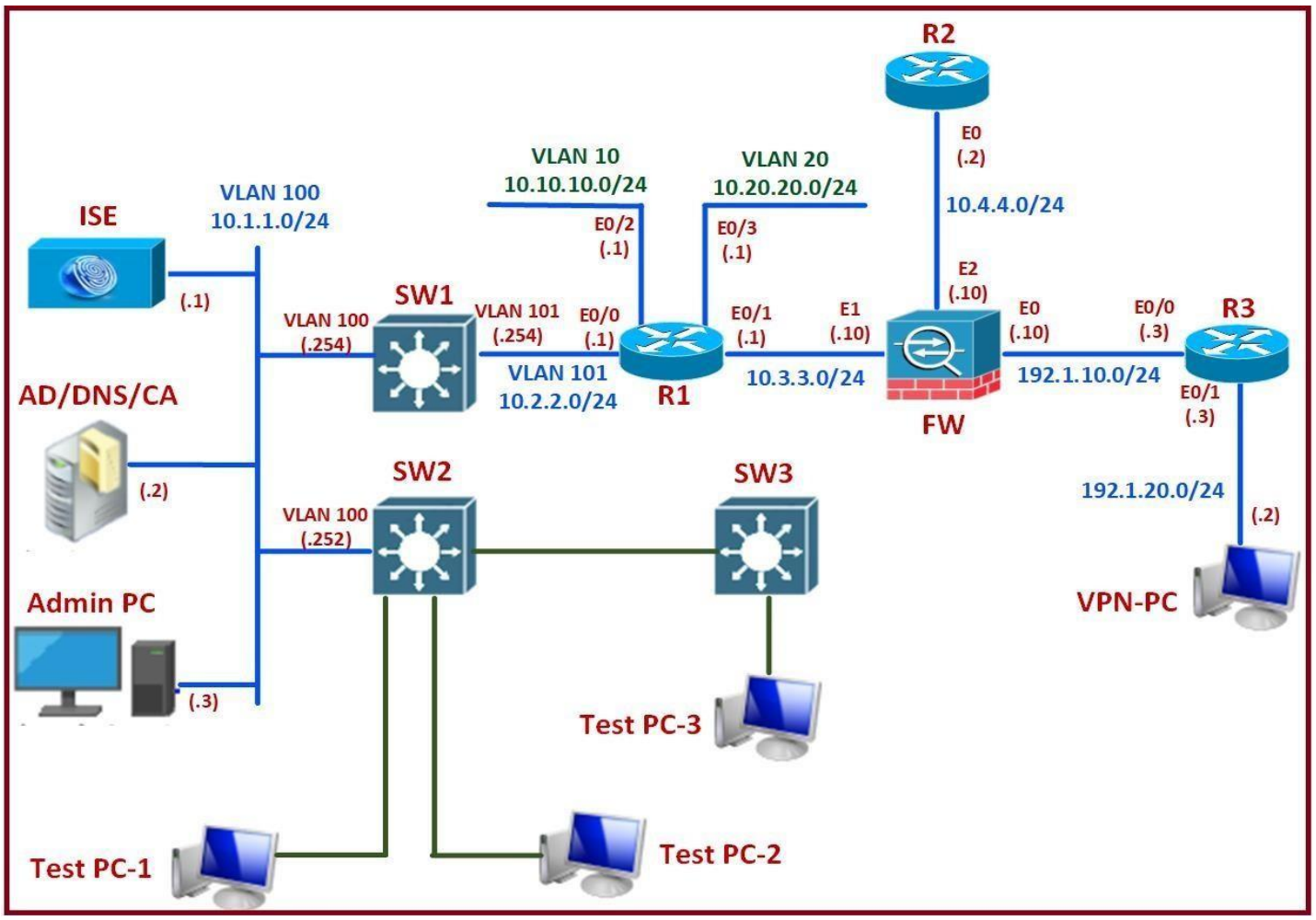
ISE

1. Browse to "**Administration -> Identity Management -> Identities -> Create"**

2. Create the Identities based on the above parameters.

3. Click **Save.**

Lab 3 – Configuring Dot1x Authentication Using the Windows Client



Lab Scenario:

- Configuring Policies.
- Configuring the Clients to authenticate using 802.1x authentication.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure authorization policies on ISE to provide access to the network based on successful authententication. Use the following to configure the Authorization Policies. Create them at the top of the Authorization Policies

- Name: **ISE-EMP-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-EMP**
    - Wired_802.1x
    - Network Device Group: **Switches**
  - Profile: **Permit Access**

- Name: **ISE-CON-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-CON**
    - Wired_802.1x
    - Network Device Group: **Switches**
  - Profile: **Permit Access**

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization -> Insert new Row Above"**

3. Create the Authorization Policies based on the above Parameters.

4. Click **Save.**

Task 2

Configure SW2 for Dot1x Authentication. Use basic 802.1x Authentication commands.

SW2

```
aaa new-model
!
username admin privilege 15 password admin
!
radius server ISE1
 address ipv4 10.1.1.1 auth-port 1812 acct-port 1813
 key Cisco123*
!
aaa group server radius ABC
 server name ISE1
!
aaa authentication dot1x default group ABC
aaa authorization network default group ABC
!
dot1x system-auth-control
!
interface range E0/1-2
 switchport access vlan 100
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

Task 3

Configure the Windows 802.1x Supplicant.

Test-PC1

- **Enable the WiredAutoConfig Services**
  - Click Start. Type and open Services.
  - Set the **WiredAutoConfig** to start Automatically.
  - Start the service.
- **Configure the Network Adapter**
  - Right-Click the Network Adapter and click Properties under Network & Sharing Center to configure Dot1x.
  - Click the Authentication Tab.
  - Click **Settings**.
  - Uncheck "**Validate Server Certificate".**
  - Click "Configure" to uncheck the "**Automatically use the Windows Logon**".
  - Click **OK** to back to the Authentication Page.
- **Configure Authentication Parameters**
  - Click the "**Additional Settings**" button on the Authentication Page
  - Select "**User Authentication**".
  - Configure the Username as **ISE-1** with a password of **Cisco123*.**
  - Click **OK** to go back to the Authentication Page.
  - Click **OK** twice to accept the settings.

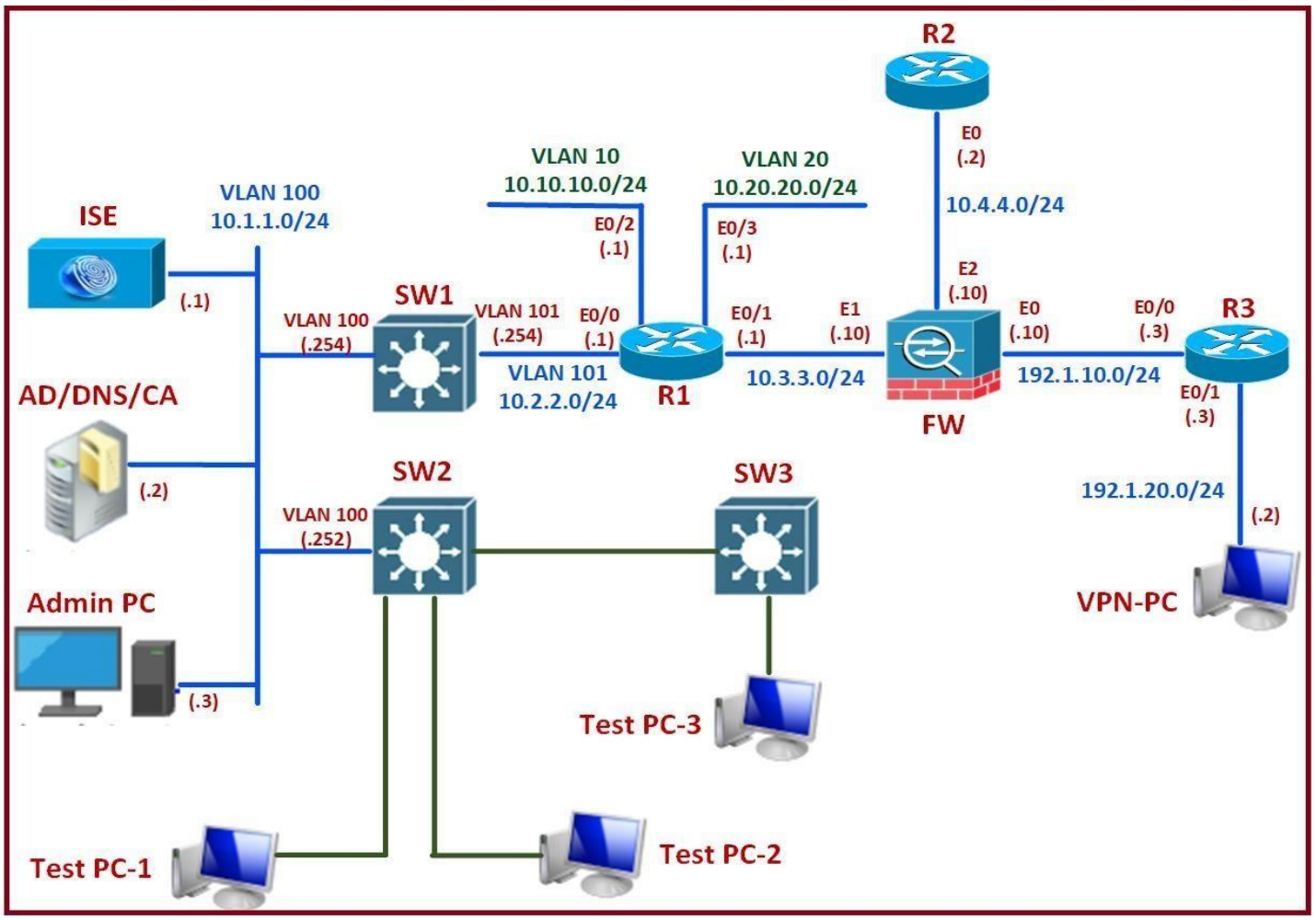
- You should be logged in with ISE-1 credentials.

- You can verify the credentials in ISE under the following:

  Operations -> RADIUS -> Live Logs

- Replace the credentials to ISE-2 on the Authentication -> Additional Settings Page and verify the RADIUS Log in ISE.

Lab 4 – Configuring Dot1x Authentication with VLAN Assignment



Lab Scenario:

- Configuring Per-User VLAN assignment.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure authorization profiles to assign ISE-EMP & ISE-CON users to vlans based on the following:

- Name: **ISE-EMP-PROFILE**
  - VLAN: **10**

- Name: **ISE-CON-PROFILE**
  - VLAN: **20**

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> Add"**

3. Create the Authorization Profiles based on the above Parameters.

4. Click **Save.**

Task 2

Re-configure authorization policies for ISE-EMP & ISE-CON users to use the appropriate Authorization Profile based on the following:

- Name: **ISE-EMP-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-EMP**
    - Wired_802.1x
    - Network Device Group: **Switches**
  - Profile: **ISE-EMP-PROFILE**

- Name: **ISE-CON-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-EMP**
    - Wired_802.1x
    - Network Device Group: **Switches**
  - Profile: **ISE-CON-PROFILE**

ISE

1. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy -> [Policy Name] -> Edit"**

2. Re-configure the Authorization Policies based on the above Parameters.

3. Click **Save.**

Task 3

Re-configure authorization policies for ISE-EMP & ISE-CON users to use the appropriate Authorization Profile based on the following:

- Name: **ISE-EMP-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-EMP**
    - Wired_802.1x
    - Network Device Group: **Switches**
  - Profile: **ISE-EMP-PROFILE**

- Name: **ISE-CON-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-EMP**
    - Wired_802.1x
    - Network Device Group: **Switches**
  - Profile: **ISE-CON-PROFILE**

ISE

1. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy -> [Policy Name] -> Edit"**

2. Re-configure the Authorization Policies based on the above Parameters.

3. Click **Save.**

Task 3

Re-login to verify the VLAN Assignment.

Test-PC1

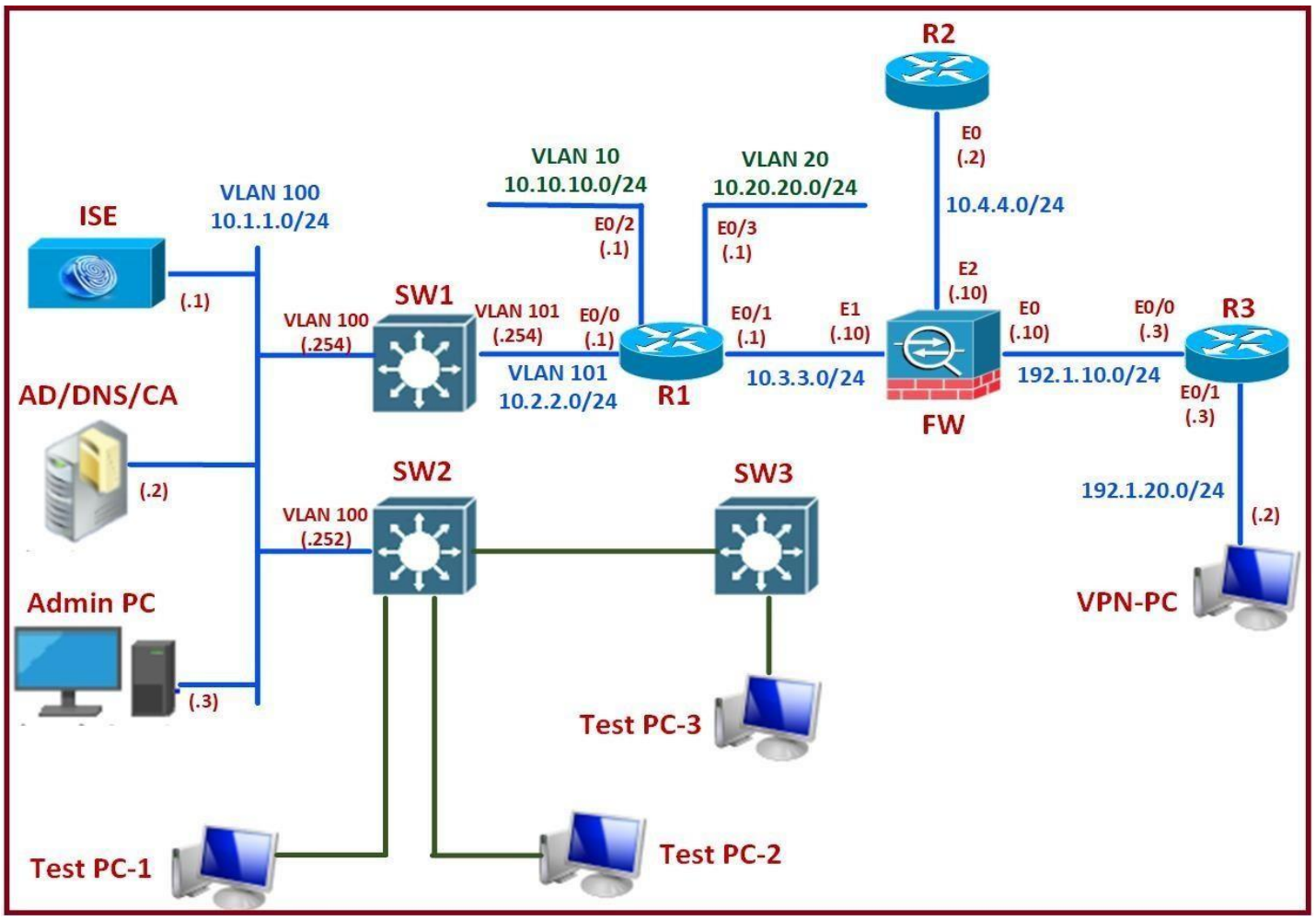
- Disable and re-enable the Network Adapter under Network & Sharing Center.
  - You should be logged in as ISE-2.
  - Verify that you are receiving an IP Address from VLAN 20 (10.20.20.0/24) using the "ipconfig" command.
  - Verify the RADIUS Log in ISE.

- Replace the credentials to ISE-1 on the Authentication -> Additional Settings Page and verify the IP Address and RADIUS Log in ISE.

- You can also verify the configuration on the Switch by using the following commands:

  - Show authentication session interface E0/1 details
  - Show VLAN

Lab 5 – Configuring Dot1x Authentication with Downloadable ACLs



Lab Scenario:

- Configuring Downloadable ACLs (DACL)

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure R1 for Telnet with a password of **Cisco123.**

R1

```
Line vty 0 4
 Password Cisco123
 Login
 Transport input telnet
```

Task 2

You should be logged in as ISE-1. Verify that you can telnet and ping R1 (10.10.10.1).

Task 3

Configure a Downloadable ACL (DACL) with the following content:

- **Deny tcp any any eq 23**
- **Permit ip any any**

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Downloadable ACLs -> Add"**

3. Configure the DACL based on the above parameters and **Save** it as **ISE-EMP-DACL**.

Task 4

Re-Configure the ISE-EMP-PROFILE authorization profiles to attach the DACL created in the previous step.

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> ISE-EMP-PROFILE"**

3. Configure the Authorization Profiles to include the DACL created in the previous task.

4. Click **Save.**

Task 3

Re-login to verify the DACL.

Test-PC1

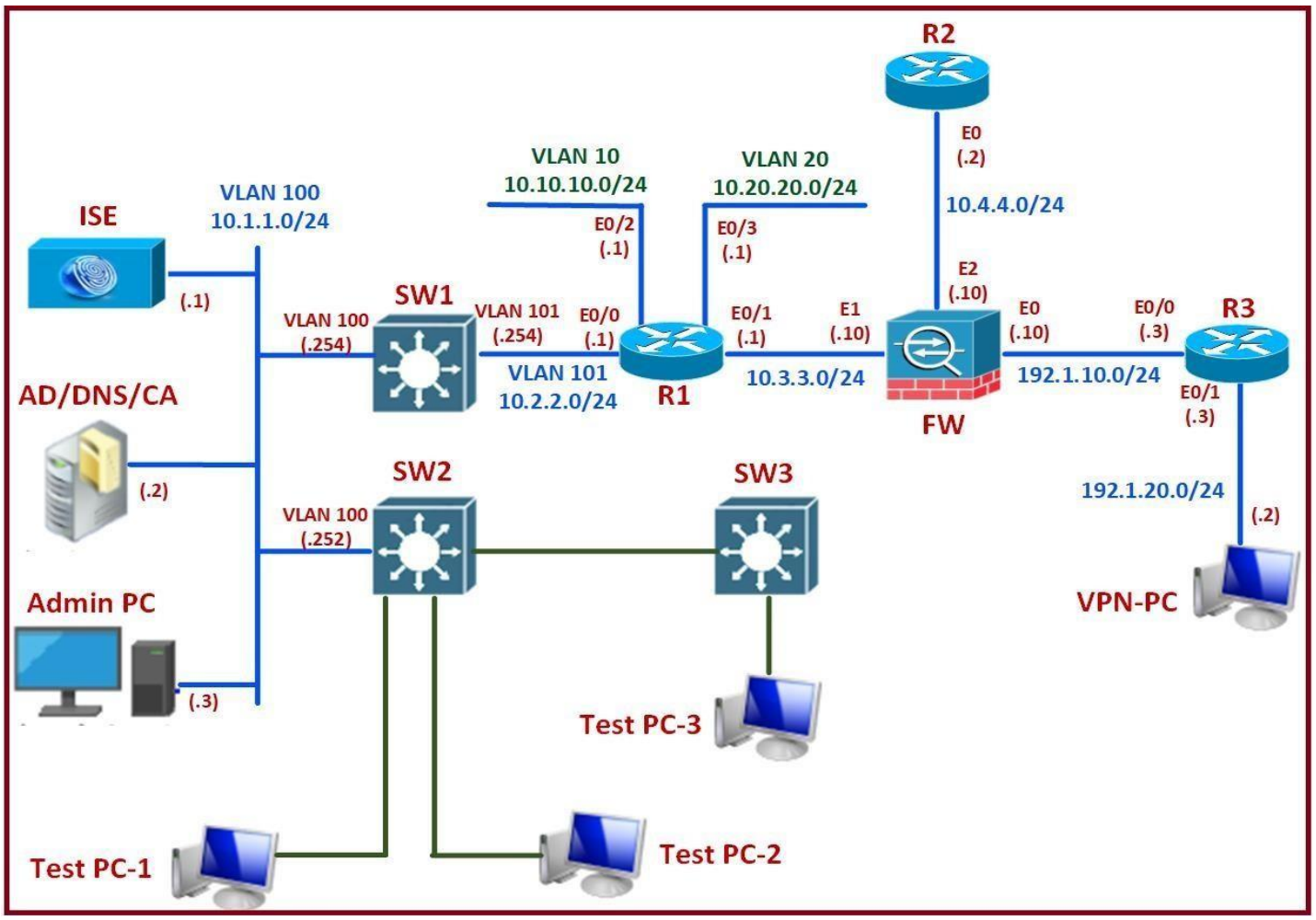
- Disable and re-enable the Network Adapter under Network & Sharing Center.
  - Telnet to 10.10.10.1. Are you successful?
  - Ping 10.10.10.1. You should still be successful.
  - You can verify the DACL on the SW2 by using the "**show authentication session Interface E0/1 detail"** command

CCIE Security v6 – Identity Service Engine (ISE)

Module 3 – Integrating ISE & Active Directory

Module 3 – Integrating ISE & Active Directory

Lab 1 – Integrating ISE with Microsoft Active Directory (AD)



Lab Scenario:

- Configure a relationship between ISE & Active Directory

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the relationship between ISE & AD based on the following:

- Join Point Name: **KBITS-AD**
- Active Directory Domain: **kbits.live**
- Administrator Username & Password: **Administrator/Kbits@123**

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Administration -> Identity Management -> External Identity Source -> Active Directory -> Add**"

3. Join the kbits.live domain using the parameters above.

Task 2

Pull down the groups listed below from AD to ISE:

- Kbits.live/users/Employees
- Kbits.live/users/Consultants
- Kbits.live/users/Domain Users

ISE

1. Browse to "**Administration -> Identity Management -> External Identity Source -> Active Directory -> KBITS-AD -> Groups**"

2. Add the groups specified above.

3. Click **Save.**

Task 3

Add the KBITS Identity in the Identity Source Sequence

- Kbits.live/users/Employees
- Kbits.live/users/Consultants
- Kbits.live/users/Domain Users

ISE

1. Browse to "**Administration -> Identity Management -> Identity Source Sequences -> All_Users_ID_Stores"**

2. Select **KBTIS-AD** from the Available Box under Authentication Search List & click the "**>**" button.

3. Move **KBITS-AD** to the 2nd spot in the search list.

4. Click **Save.**

Task 4

Configure ISE to support certificate-based authentication for AD objects.

ISE

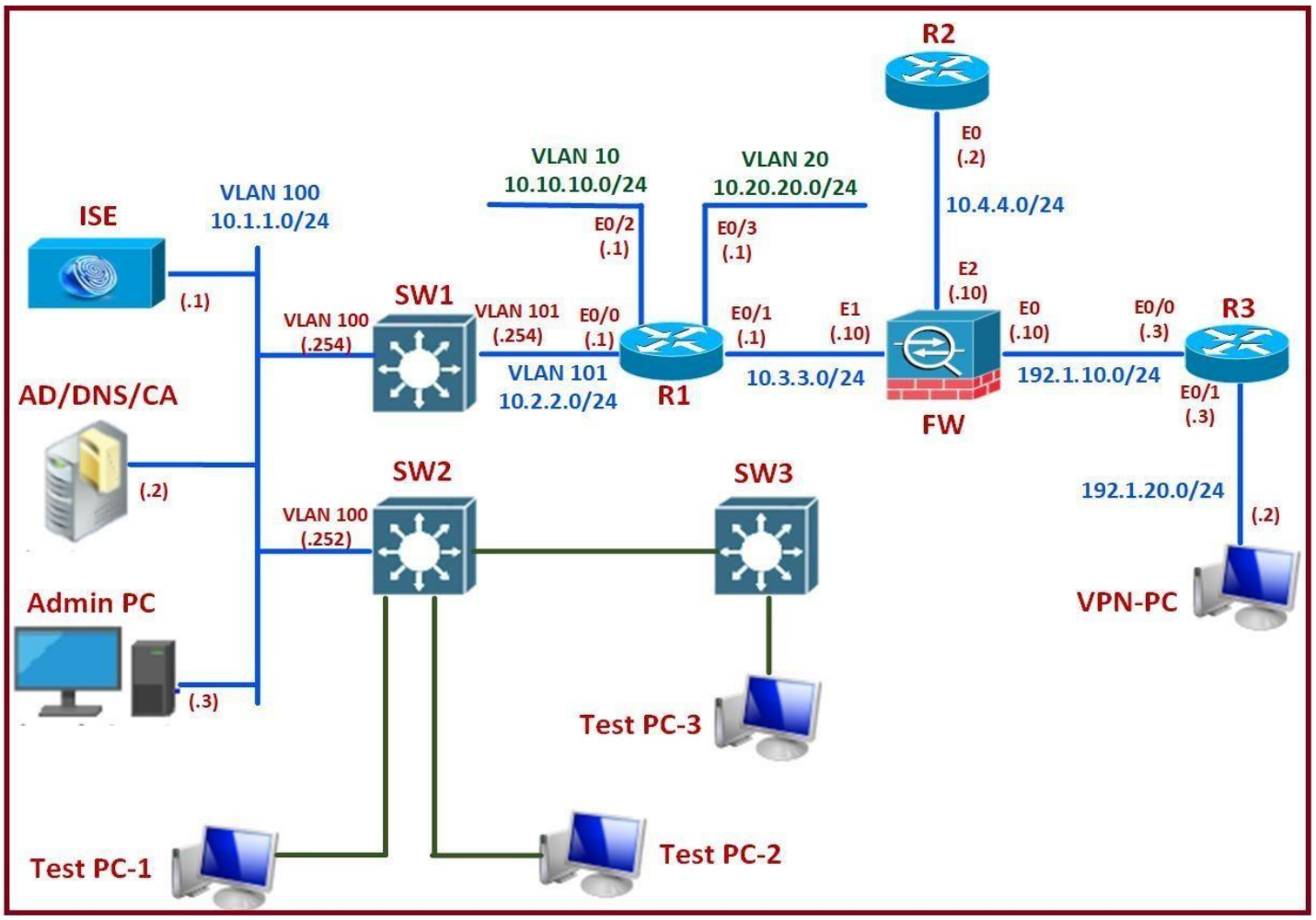
1. Browse to "**Administration -> Identity Management -> External Identity Sources -> Certificate Authentication Profile -> Preloaded-Certificate-Profile"**

2. Click the Drop-down box for Identity Store & select **KBITS-AD**.

3. Under Use Identity from, select the checkbox for "**Any Subject or alternate name Attributes in the certificate (for Active Directory Only)**"

4. Click **Save.**

Lab 2 – Authenticating Users using AD Username/Password



Lab Scenario:

- Configuring Authorization Profiles to be used in Policies for Active Directory (AD) users & groups.
- Coniguring Autorization Policies for AD users.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure 2 Authorization Profiles to assign AD Users to appropriate VLANs based on the following:

- Name: **AD-EMP-PROFILE**
- VLAN: **10**

- Name: **AD-CON-PROFILE**
- VLAN: **20**

ISE

1. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> Add"**

2. Configure the Authorization Profiles based on the above parameters.

3. Click **Save.**

Task 2

Configure authorization policies for Active Directory users based on the following:

- Name: **AD-EMP-POLICY**
  - Conditions:
    - KBITS:ExternalGroups: **kbits.live/Users/Employees**
    - **Wired_802.1x**
    - Network Device Group: **Switches**
  - Profile: **AD-EMP-PROFILE**

- Name: **AD-CON-POLICY**
  - Conditions:
    - KBITS:ExternalGroups: **kbits.live/Users/Consultants**
    - **Wired_802.1x**
    - Network Device Group: **Switches**
  - Profile: **AD-CON-PROFILE**

ISE

1. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy -> Insert Rule Above"**

2. Configure the Authorization Policies based on the above Parameters.

3. Click **Save.**

Task 3

Re-login using the Active Directory user credentials.

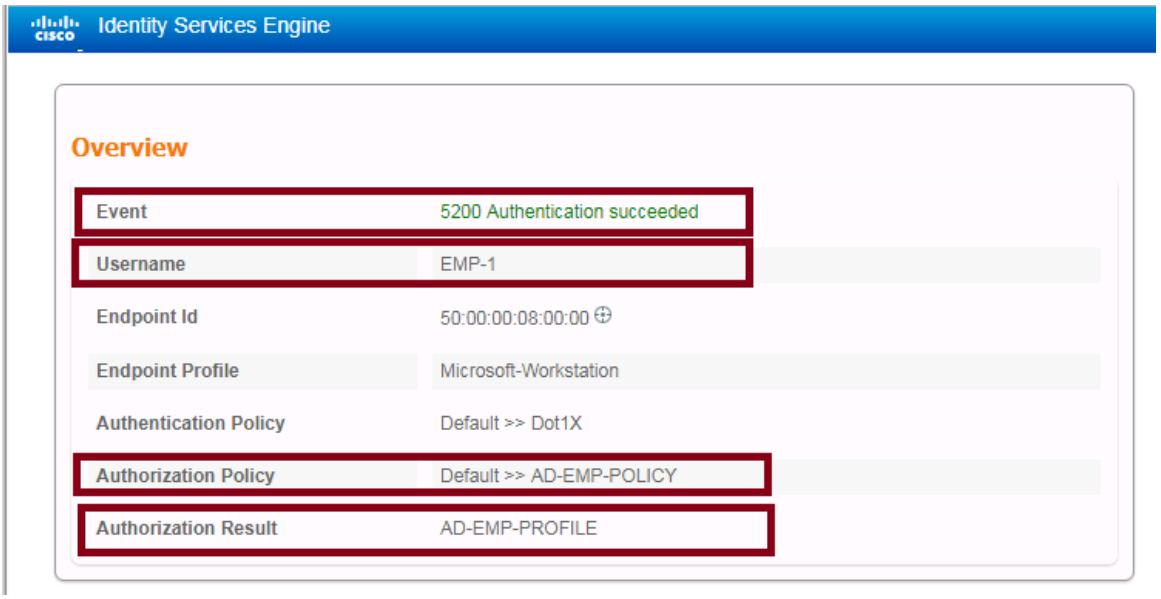
Test-PC1

- Under the Network Adapter under Network & Sharing Center, Replace the credentials to **EMP-1/Cisco123*** by clicking on the **Authentication -> Additional Settings** Page

- Verify the IP Address and RADIUS Log in ISE.

- You can also verify the configuration on the Switch by using the following commands:

  - **Show authentication session interface E0/1 details**
  - **Show VLAN**

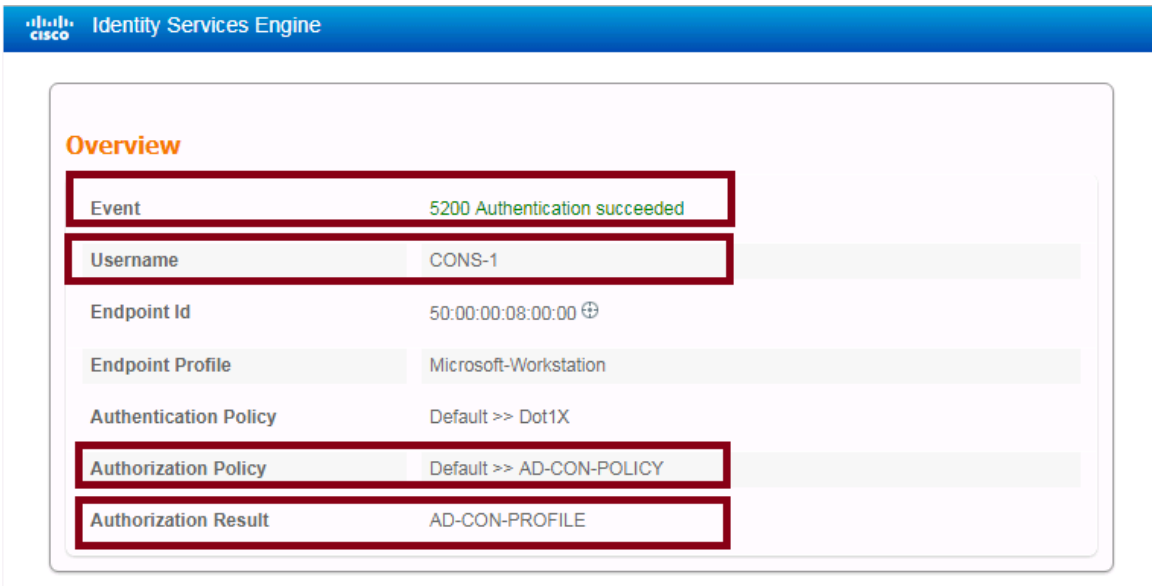


Task 4

Re-login using the Active Directory user credentials.

Test-PC1

- Under the Network Adapter under Network & Sharing Center, Replace the credentials to **CONS-1/Cisco123*** by clicking on the **Authentication -> Additional Settings** Page
- Verify the IP Address and RADIUS Log in ISE.
- You can also verify the configuration on the Switch by using the following commands:
  - **Show authentication session interface E0/1 details**
  - **Show VLAN**

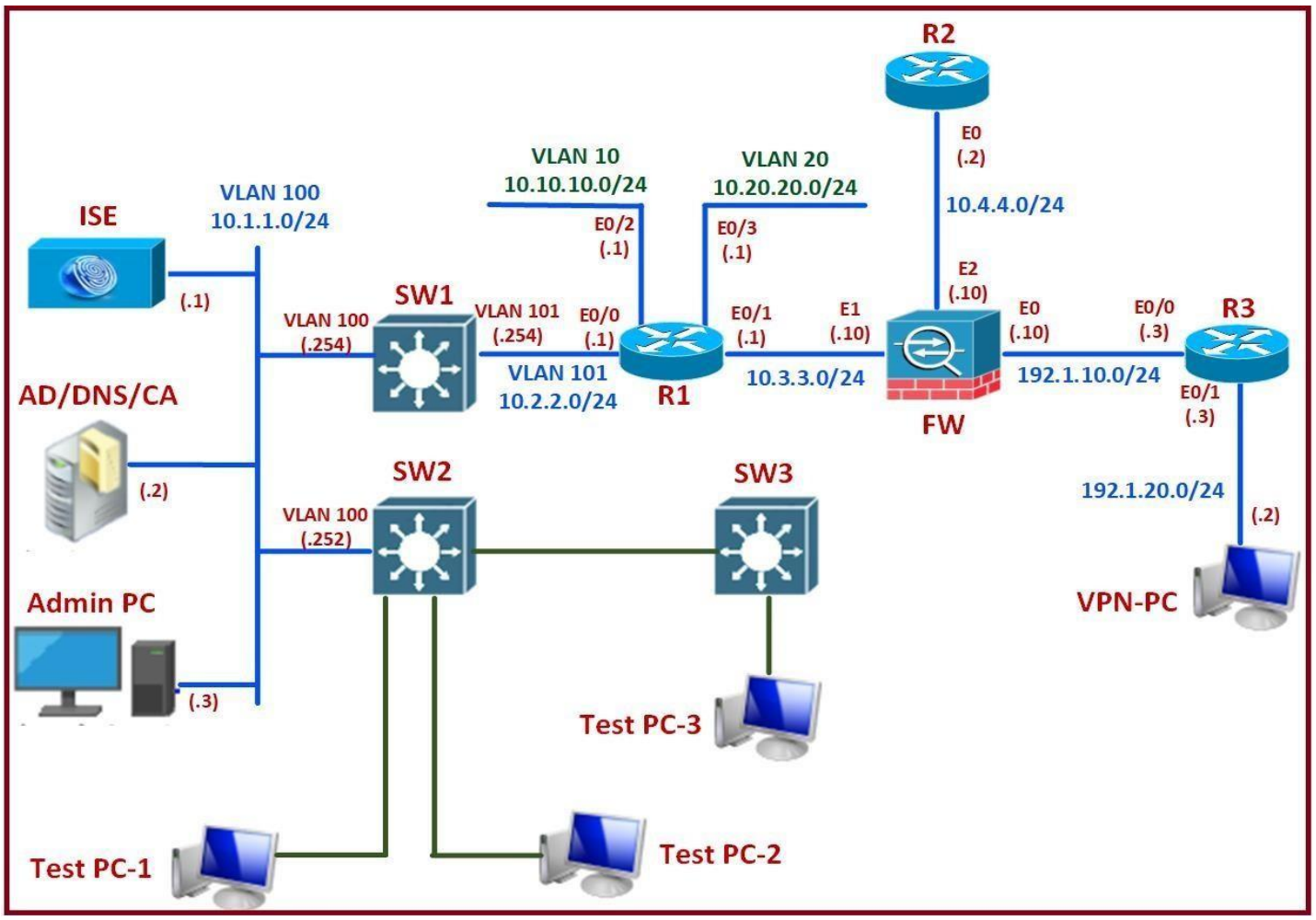


CCIE Security v6 – Identity Service Engine (ISE)

Module 4 – Authenticating VPN Connections using ISE

Module 4 – Authenticating VPN Connections using ISE

Lab 1 – Authenticating VPN Connections using ISE



Lab Scenario:

- Configure a Remote Access VPN on the ASA Firewall.
- It should use ISE for Authentication

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure ASA for ASDM Configuration. The ASA should allow ASDM access from the 10.1.1.0/24 network. Configure a local username of admin with a password of admin with a privilege of 15.

ASA

```
http server enable
!
Username admin password admin privilege 15
!
http 10.1.1.0 255.255.255.0 inside
Aaa authentication http console LOCAL
```

Task 2

Open up ASDM on your device or browse to https://10.3.3.10 to download and install ASDM. Log into 10.3.3.10 using the username and password configured in the previous step.

Task 3

Configure a Remote access VPN on the ASA based on the following parameters:

- Connection Profile Name: AC-RemoteAccess
- Interface: Outside
- **Device Certificate**:
  - New Self-Signed
  - New TrustPointName: SELF-TP
  - Generate a New Self-Signed Identity Certificate using default Parameters.
- Add the existing Windows AnyConnect Image.
- **AAA Server Configuration**
  - Server Group Name: ISE
  - Authentication Protocol: RADIUS
  - Server IP: 10.1.1.1
  - Interface: Inside
  - Server secret key: Cisco123*
- **IPv4 Pool Configuration**
  - Pool Name: VPN-POOL
  - Range: 192.168.1.1-192.168.1.254
  - Subnet Mask: 255.255.255.0
- **Split-Tunnelling**
  - Only allow access to 10.4.4.0/24 (DMZ) network from Outside.

Admin-PC

1. Browse to "**Click on Configuration".**

2. Click on "**Wizard -> VPN Wizards -> AnyConect VPN Wizard**".

3. Configure the VPN parameters based on the above parameters.

4. Click **Apply.**

Task 4

Configure Authorization Profiles for ISE UsersKbits.live/users/Employees. Use **ISE-VPN-PROFILE** for the profile name. Configure an Authorization Profile to allow access to VPN Users. Although the profile will not have any parameters at this point, it will be populated later.

ISE

1. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> Add"**

2. Create an authorization profile name **ISE-VPN-PROFILE**.

3. Click **Save.**

Task 5

Configure a new Authorization Policies at the top based on the below parameters. The profile will be used for VPN Users:

- Name: **ISE-VPN-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-CON**
    - Network Device Group: **Firewalls**
  - Profile: **ISE-VPN-PROFILE**

ISE

1. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy -> Insert Rule Above"**

2. Configure the Authorization Policies based on the above Parameters.

3. Click **Save.**

Task 6

Configure R2 for Telnet using a Telnet password of **Cisco123**. Enable the HTPP Server. Configure an Enable password of **Cisco123**.

R2

```
Enable secret Cisco123
!
Ip http server
!
Line vty 0 4
 Password Cisco123
 Login
 Transport input all
```

Task 7

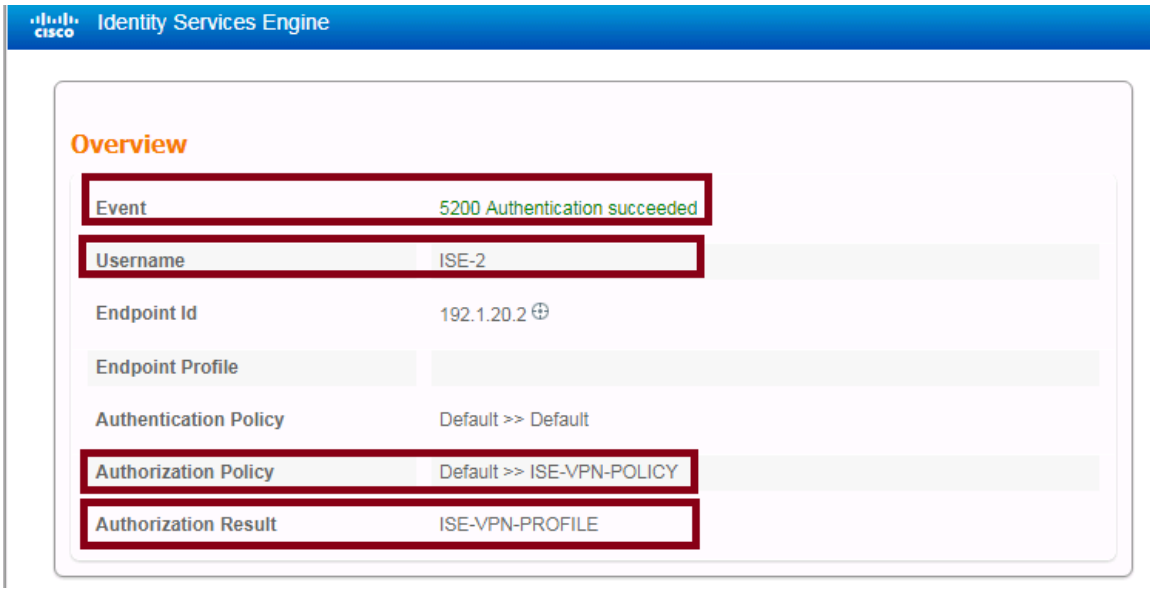
Connect to the Network using the VPN-PC as **ISE-2** with a password of **Cisco123***.

R2

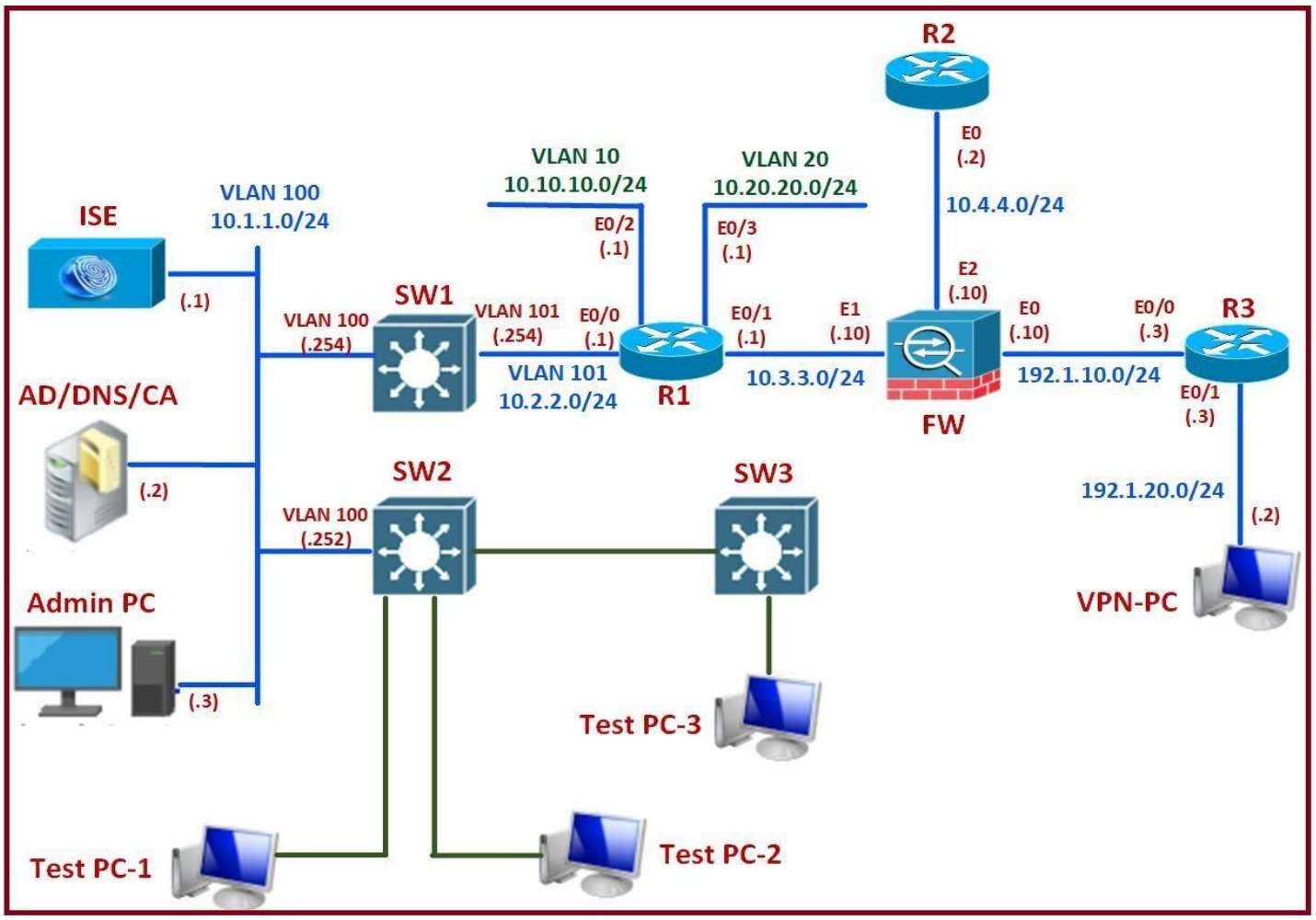
1. Connect to VPN-PC.
2. Open the Cisco AnyConnect Secure Mobility Client.
3. Connect to 192.1.10.10.
4. Accept the Certificate.
5. Specify **ISE-2** as the Username with a password of **Cisco123***.
6. You should successfully connect.
7. You can verify the credentials in ISE under the following:

   Operations -> RADIUS -> Live Logs

8. You should be able to **Ping**, **Telnet** & **Browse(Http)** to **R2**.



Lab 2 – Authenticating VPN Connections using ISE with DACL



Lab Scenario:

- Configuring a DACL for VPN Users.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure a Downloadable ACL (DACL) on ISE using the following parameters:

- Name: **ISE-VPN-DACL**
- Content:
  - Deny icmp any any
  - Permit ip any any

ISE

1. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> DACL -> Add**"

2. Configure the DACL based on the above parameters and **Save** it as **ISE-VPN-DACL**.

Task 2

Re-configure the ISE-VPN-PROFILE Authorization Profile to include the DACL created in the previous task.

ISE

1. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> ISE-VPN-PROFILE**"

2. Configure the Authorization Profiles to include the DACL created in the previous task.

3. Click **Save**.

Task 3

Re-login as ISE-2 to verify the DACL deployment.

ISE

1. Disconnect & reconnect to **192.1.10.10**.

2. Accept the Certificate.

3. Specify **ISE-2** as the Username with a password of **Cisco123***.

4. You should successfully connect.

5. You can verify the credentials in ISE under the following:

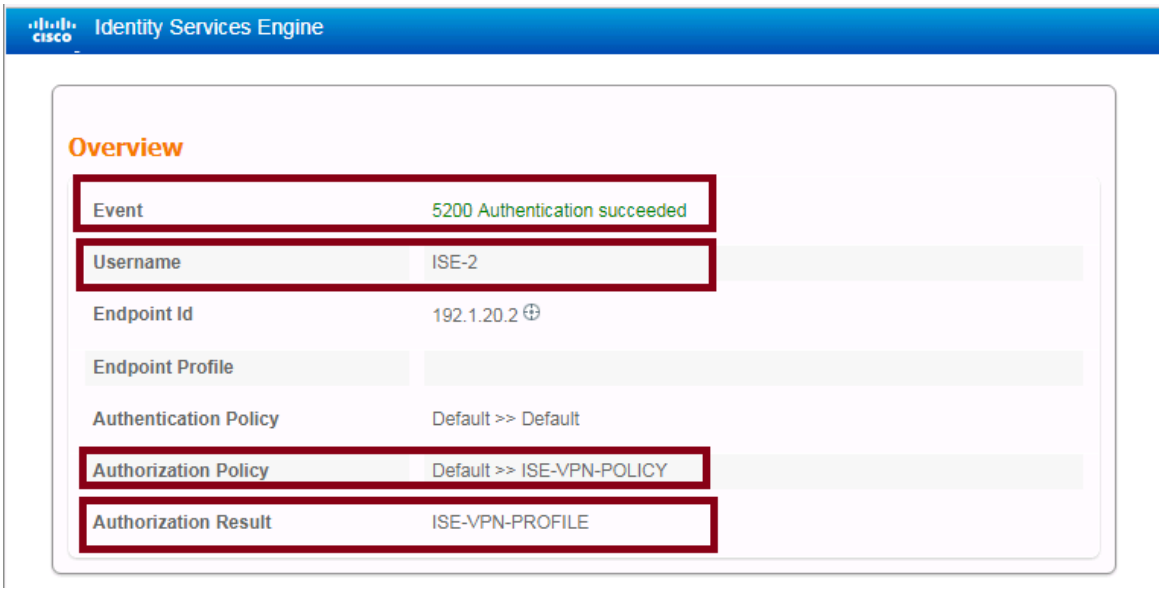
Operations -> RADIUS -> Live Logs

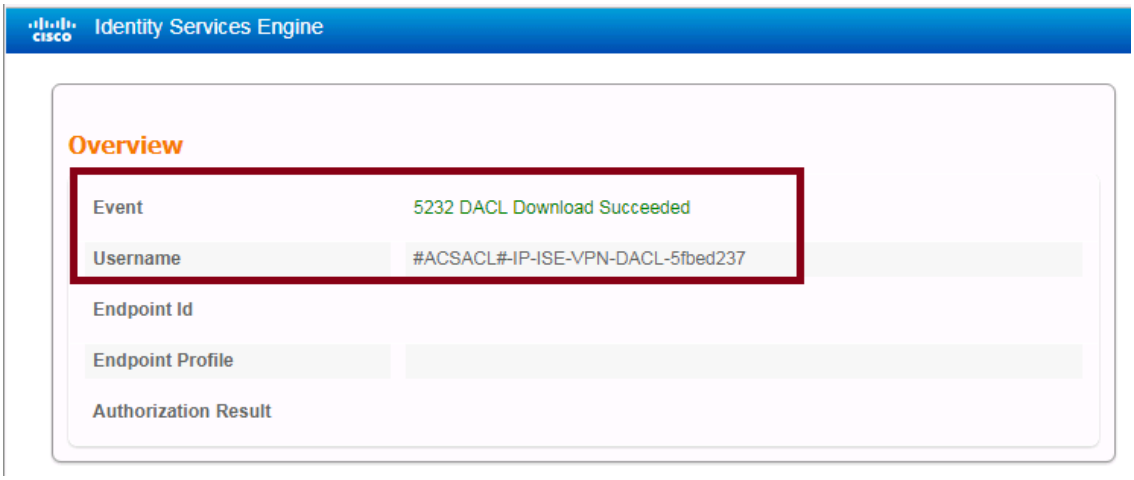
6. You could also verify the connection on the ASA by using the following 2 commands:

sh vpn-sessiondb anyconnect (Displays connection information)
sh access-list (Displays the DACL)

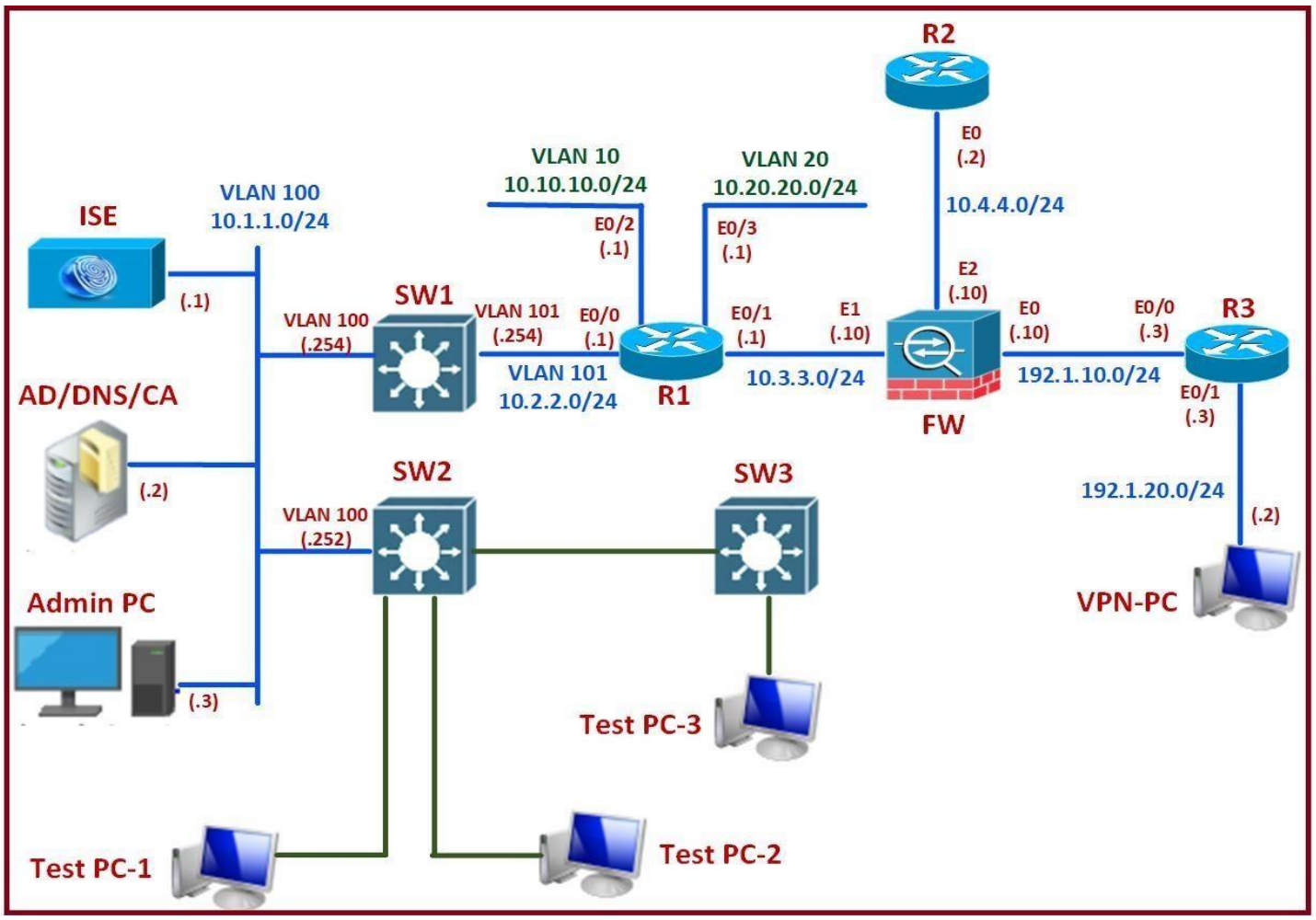
7. You should NOT be able to Ping R2.

8. You should continue to Telnet & Browse to R2.





Lab 3 – Authentication VPN Connections using AD with DACL



Lab Scenario:

- Configuring ISE to use AD for authenticating VPN Users.
- Assign the DACL to specified Users.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure 2 Authorization Profiles to assign AD Users to appropriate VLANs based on the following:

- Name: **AD-EMP-VPN-PROFILE**

- Name: **AD-CONS-VPN-PROFILE**
- DACL: **ISE-VPN-DACL**

ISE

1. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> Add"**

2. Configure the Authorization Profiles based on the above parameters.

3. Click **Save.**

Task 2

Configure authorization policies for Active Directory users based on the following:

- Name: **AD-EMP-VPN-POLICY**
  - Conditions:
    - KBITS:ExternalGroups: **kbits.live/Users/Employees**
    - Network Device Group: **Firewalls**
  - Profile: **AD-EMP-VPN-PROFILE**

- Name: **AD-CON-POLICY**
  - Conditions:
    - KBITS:ExternalGroups: **kbits.live/Users/Consultants**
    - Network Device Group: **Firewalls**
  - Profile: **AD-CONS-VPN-PROFILE**

ISE

1. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy -> Insert Rule Above"**

2. Configure the Authorization Policies based on the above Parameters.

3. Click **Save.**

Task 3
Re-login as ISE-1.

ISE

1. Disconnect & reconnect to **192.1.10.10**.

2. Accept the Certificate.

3. Specify **ISE-1** as the Username with a password of **Cisco123***.

4. You should successfully connect.

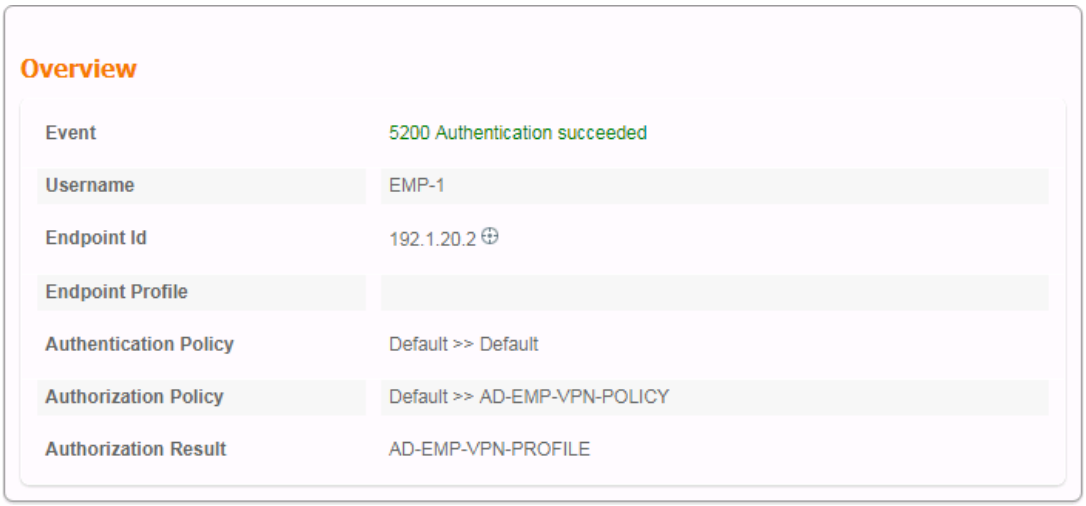
5. You can verify the credentials in ISE under the following:

   Operations -> RADIUS -> Live Logs

6. You could also verify the connection on the ASA by using the following 2 commands:

   sh vpn-sessiondb anyconnect (Displays connection information)
   sh access-list (Displays the DACL)

7. You should be able to Ping, Telnet & Browse to R2.



Task 4

Re-login as ISE-2.

ISE

1. Disconnect & reconnect to **192.1.10.10**.

2. Accept the Certificate.

3. Specify **ISE-2** as the Username with a password of **Cisco123***.

4. You should successfully connect.

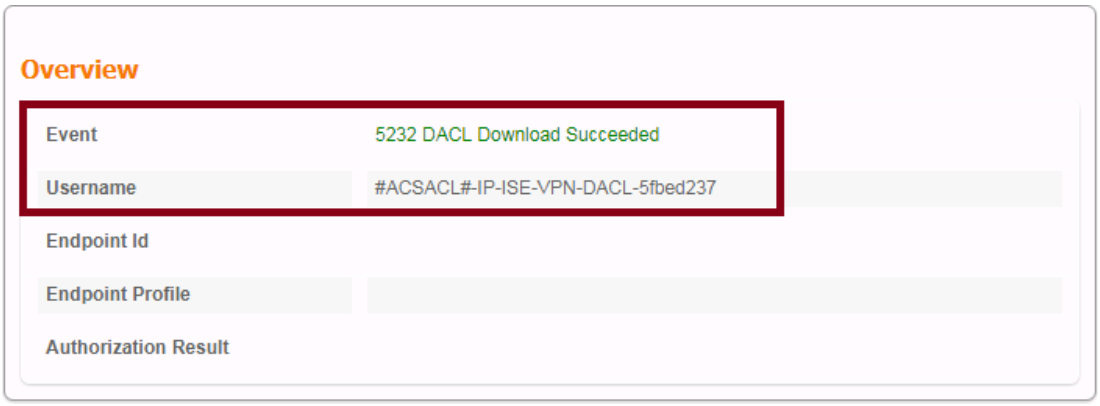
5. You can verify the credentials in ISE under the following:

   Operations -> RADIUS -> Live Logs

6. You could also verify the connection on the ASA by using the following 2 commands:

   sh vpn-sessiondb anyconnect (Displays connection information)
   sh access-list (Displays the DACL)

7. You should NOT be able to Ping R2. You should be able to Telnet & Browse to R2.

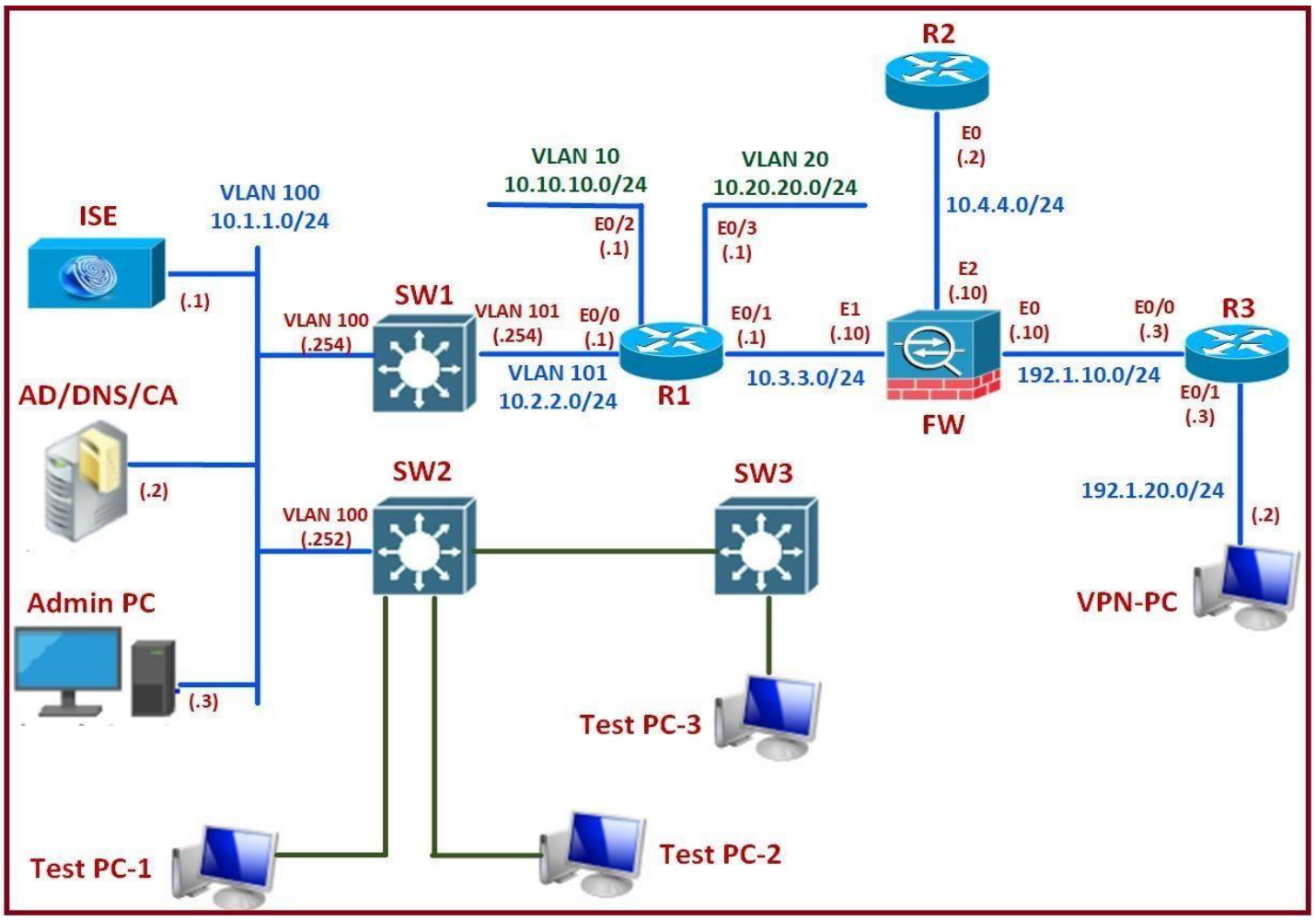


CCIE Security v6 – Identity Service Engine (ISE)

Module 5 – Configuring Device Admin. using TACACS+

Module 5 – Configuring Device Administration using TACACS+

Lab 1 – Configuring Authentication & Authorization on Routers / Switches



Lab Scenario:

- Configure the Autentication & Authorization Commands on the Routers & Switches.
- The Authentication & Authorization should be done based on ISE.
- ISE will be configured in a later lab.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure R1, R2, SW1 & SW2 to point towards ISE using TACACS+ as the protocol. Use ISE1-T as the server name and ISE-TAC as the Group Name. Configure the Secret Password as Cisco123*.

R1

```
Aaa new-model
!
Tacacs server ISE1-T
 Address ipv4 10.1.1.1
 Key Cisco123*
!
aaa group server tacacs+ ISE-TAC
 server name ISE1-T
```

R2

```
Aaa new-model
!
Tacacs server ISE1-T
 Address ipv4 10.1.1.1
 Key Cisco123*
!
aaa group server tacacs+ ISE-TAC
 server name ISE1-T
```

SW1

```
Aaa new-model
!
Tacacs server ISE1-T
 Address ipv4 10.1.1.1
 Key Cisco123*
!
aaa group server tacacs+ ISE-TAC
 server name ISE1-T
```

SW2

```
Aaa new-model
!
Tacacs server ISE1-T
 Address ipv4 10.1.1.1
```

```
 Key Cisco123*
!
aaa group server tacacs+ ISE-TAC
 server name ISE1-T
```

Task 2

Configure the ASA Firewall to allow communicatation from R2 to ISE for TACACS+.

ASA

```
Access-list DMZ permit tcp host 10.4.4.2 host 10.1.1.1 eq 49
!
Access-group DMZ in interface DMZ
```

Task 3

Configure R1, R2, SW1 & SW2 to use ISE for Telnet & SSH Authentication using the previously configured TACACS+ server. Use a Named-list.

R1

```
Ip domain-name kbits.live
!
Crypto key generate rsa modulus 1024
!
Aaa authentication login TAC-AUTHEN group ISE-TAC
!
Line vty 0 4
 Login authentication TAC-AUTHEN
 Transport input telnet ssh
```

R2

```
Ip domain-name kbits.live
!
Crypto key generate rsa modulus 1024
!
Aaa authentication login TAC-AUTHEN group ISE-TAC
!
Line vty 0 4
 Login authentication TAC-AUTHEN
 Transport input telnet ssh
```

SW1

```
Ip domain-name kbits.live
```

```
!
Crypto key generate rsa modulus 1024
!
Aaa authentication login TAC-AUTHEN group ISE-TAC
!
Line vty 0 4
 Login authentication TAC-AUTHEN
 Transport input telnet ssh
```

SW2

```
Ip domain-name kbits.live
!
Crypto key generate rsa modulus 1024
!
Aaa authentication login TAC-AUTHEN group ISE-TAC
!
Line vty 0 4
 Login authentication TAC-AUTHEN
 Transport input telnet ssh
```

Task 4

Configure R1, R2, SW1 & SW2 to use ISE for Telnet & SSH Exec and Command Authorization using the previously configured TACACS+ server. Comand Authorization should be done for Level 15 commands only. Use a Named-list.

R1

```
Aaa authorization config-commands
Aaa authorization exec TAC-AUTHOR group ISE-TAC
Aaa authorization command 15 TAC-AUTHOR group ISE-TAC
!
Line vty 0 4
 Authorization exec TAC-AUTHOR
 Authorization command 15 TAC-AUTHOR
```

R2

```
Aaa authorization config-commands
Aaa authorization exec TAC-AUTHOR group ISE-TAC
Aaa authorization command 15 TAC-AUTHOR group ISE-TAC
!
Line vty 0 4
 Authorization exec TAC-AUTHOR
 Authorization command 15 TAC-AUTHOR
```

SW1

```
Aaa authorization config-commands
Aaa authorization exec TAC-AUTHOR group ISE-TAC
Aaa authorization command 15 TAC-AUTHOR group ISE-TAC
!
Line vty 0 4
 Authorization exec TAC-AUTHOR
 Authorization command 15 TAC-AUTHOR
```

SW2

```
Aaa authorization config-commands
Aaa authorization exec TAC-AUTHOR group ISE-TAC
Aaa authorization command 15 TAC-AUTHOR group ISE-TAC
!
Line vty 0 4
 Authorization exec TAC-AUTHOR
 Authorization command 15 TAC-AUTHOR
```

Task 5

Configure a new Authorization Policies at the top based on the below parameters. The profile will be used for VPN Users:

- Name: **ISE-VPN-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-CON**
    - Network Device Group: **Firewalls**
  - Profile: **ISE-VPN-PROFILE**

ISE

1. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy -> Insert Rule Above"**

2. Configure the Authorization Policies based on the above Parameters.

3. Click **Save.**

Task 6

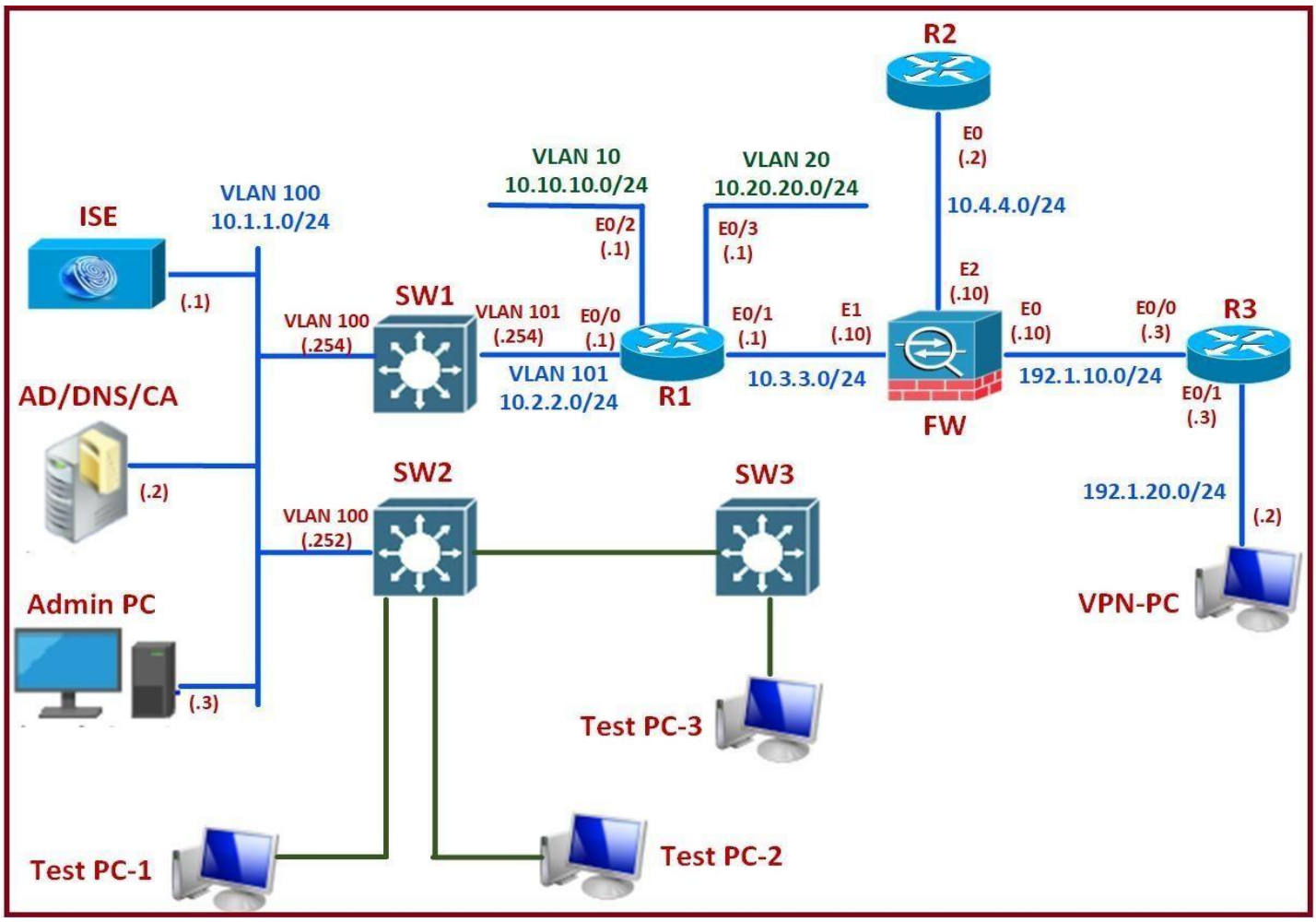
Configure R2 for Telnet using a Telnet password of **Cisco123**. Enable the HTPP Server. Configure an Enable password of **Cisco123**.

R2

```
Enable secret Cisco123
!
```

```
Ip http server
!
Line vty 0 4
 Password Cisco123
 Login
 Transport input all
```

Lab 2 – Configuring Accounting on Routers/Switches to send logs to ISE



Lab Scenario:

- Configure the Accounting Commands on the Routers & Switches.
- The Accounting should log to ISE.
- ISE will be configured in a later lab.

Initial Setup:

- **Based on the previous Lab**

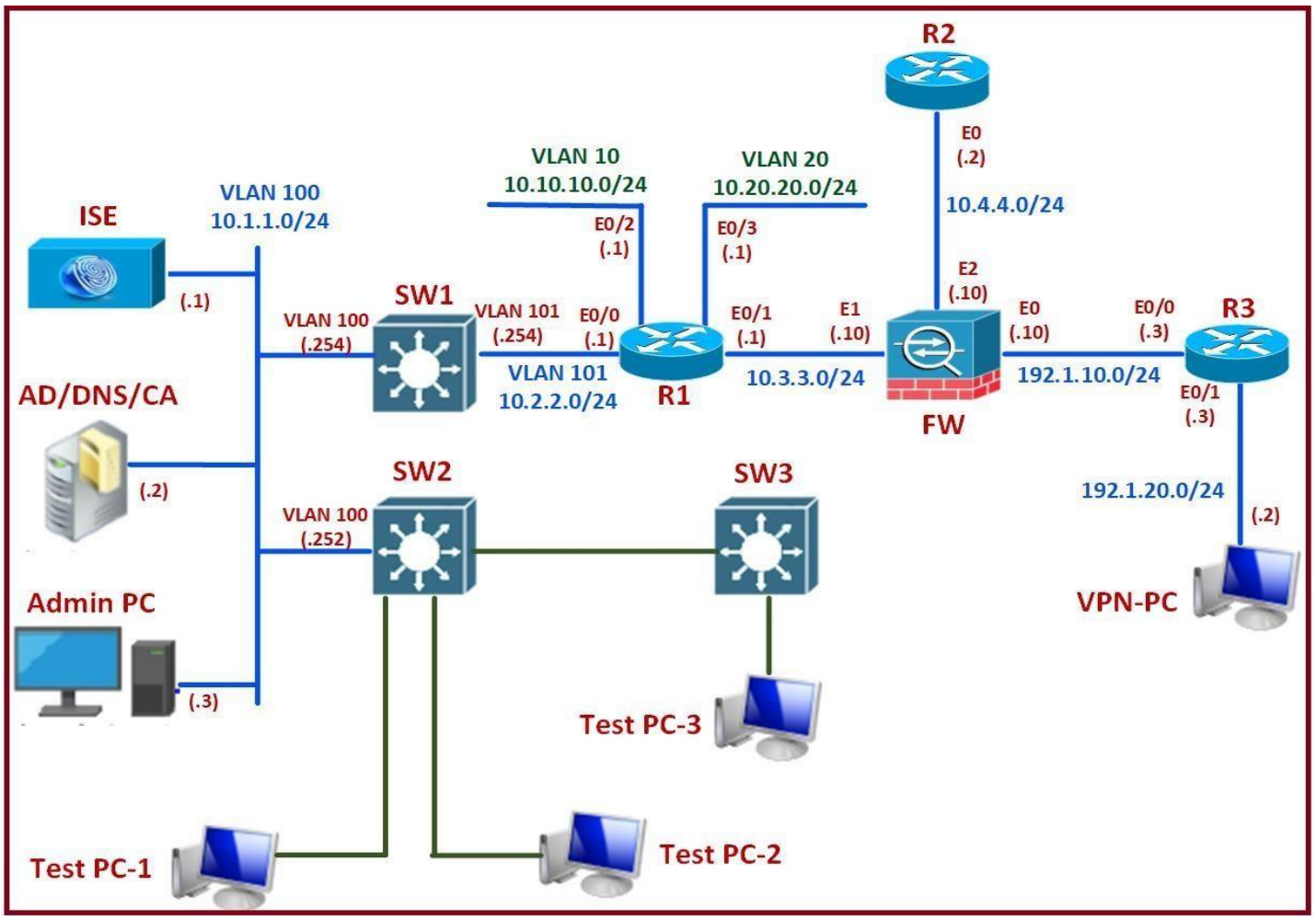
Lab Tasks:

Task 1

Configure R1, R2, SW1 & SW2 to use ISE for Exec Accounting (Login/Logouts). Configure R1, R2, SW1 & SW2 to use ISE for Command Level 15 Accounting (Command Accounting). Use a Named-list.

R1 Aaa accounting exec TAC-ACCT start-stop group ISE-TAC Aaa accounting command 15 TAC-ACCT start-stop group ISE-TAC ! Line vty 0 4 Accounting exec TAC-ACCT Accounting command 15 TAC-ACCT
R2 Aaa accounting exec TAC-ACCT start-stop group ISE-TAC Aaa accounting command 15 TAC-ACCT start-stop group ISE-TAC ! Line vty 0 4 Accounting exec TAC-ACCT Accounting command 15 TAC-ACCT
SW1 Aaa accounting exec TAC-ACCT start-stop group ISE-TAC Aaa accounting command 15 TAC-ACCT start-stop group ISE-TAC ! Line vty 0 4 Accounting exec TAC-ACCT Accounting command 15 TAC-ACCT
SW2 Aaa accounting exec TAC-ACCT start-stop group ISE-TAC Aaa accounting command 15 TAC-ACCT start-stop group ISE-TAC ! Line vty 0 4 Accounting exec TAC-ACCT Accounting command 15 TAC-ACCT Authorization command 15 TAC-AUTHOR

Lab 3 – Configuring Authentication & Authorization on ISE



Lab Scenario:

- Configuring Device Administration on ISE for Routers & Switches.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Pre-requisites:

1. **Device Admin** Service needs to be enabled. **(Module 1 – Lab 4).**

2. ISE-Network Device relationship for TACACS+. **(Module 2 – Lab 1).**

3. Groups & Admin Users. Create based on the following **(Module 2 – Lab 2)**

- Name: **Admin1**
  - Password: **Cisco123***
  - Group: **SuperAdmins**

- Name: **Admin2**
  - Password: **Cisco123***
  - Group: **RP-Admins**

- Name: **Admin3**
  - Password: **Cisco123***
  - Group: **Switching-Admins**

Task 1
Configure a TACACS+ Exec Authorization Profile to set the Exec Level to **15**. Name the Authorization Profile **PRIV_15**.

ISE

1. Browse to "**Work Centers -> Device Administration -> Policy Elements -> Results -> TACACS+ Profile -> Add"**

2. Configure the TACACS+ Profile based on the requirement.

3. Click **Save**.

Task 2

Configure TACACS+ Commad Sets based on the following parameters:

- Name: **Full-Access**
- Commands: **All**
  - Password: **Cisco123***
  - Group: **SuperAdmins**

- Name: **Routing-Protocol-CMDS**
- Commands:
  - Configure terminal
  - Router (All Protocols)
  - Network
  - Version
  - Router-id
  - Distribute-list
  - Redistribute
  - Access-list
  - Ip route

- Name: **Switching-Assistant-CMDS**
- Commands:
  - Configure terminal
  - VLAN
  - Interface
  - Switchport
  - Spanning-tree
  - Ip routing Ip route

ISE

1. Browse to "**Work Centers -> Device Administration -> Policy Elements -> Results -> TACACS+ Command Sets -> Add"**

2. Configure the TACACS+ commands based on the above requirements.

3. Click **Save**.

Task 3

Configure TACACS+ Device Admin Policies based on the following:

- Name: **SuperAdmins-Policy**
  - Conditions:
    - Identity Group Name: **SuperAdmins**
    - Network Device Group: **All Device Types**
  - Results
    - Exec Profile: **PRIV_15**
    - Commands Set: **Full-Access**

- Name: **RouterAdmins-Policy**
  - Conditions:
    - Identity Group Name: **RP-Admins**
    - Network Device Group: **Routers**
  - Results
    - Exec Profile: **PRIV_15**
    - Commands Set: **Routing-Protocols-CMDS**

- Name: **SwitchAdmins-Policy**
  - Conditions:
    - Identity Group Name: **Switching-Admins**
    - Network Device Group: **Switches**
  - Results
    - Exec Profile: **PRIV_15**
    - Commands Set: **Switching-Assistant-CMDS**

Admin-PC

Verifying Admin1 Authorizations

1. Telnet into R1 using **admin1/Cisco123*** username/password combination.

2. Are you able to login in?

3. Type Show Run. Are you successful?

4. In global configuration mode, try to enter the BGP Configuration mode by typing in **Router bgp 111**. Are you successful?

5. In global configuration mode, try to enter the Crypto ISAKMP Configuration mode by typing in **Crypto isakmp policy 10**. Are you successful?

Verifying Admin2 Authorizations

1. Telnet into R2 using **admin2/Cisco123*** username/password combination.

2. Are you able to login in?

3. Type **Show Run**. Are you successful?

4. In global configuration mode, try to enter the BGP Configuration mode by typing in **Router bgp 111**. Are you successful?

5. In global configuration mode, try to enter the Crypto ISAKMP Configuration mode by typing in **Crypto isakmp policy 10**. Are you successful?

6. Telnet into SW2 from SW1 using **admin2/Cisco123*** username/password combination.

7. Are you able to login in? Why or why not?

Verifying Admin3 Authorizations

1. Telnet into R2 using **admin3/Cisco123*** username/password combination.

2. Are you able to login in?

3. Type **Show Run**. Are you successful?

4. In global configuration mode, try to create a VLAN 199 using the **VLAN 199** command. Are you successful?

5. In global configuration mode, try to enter the BGP Configuration mode by typing in **Router bgp 111**. Are you successful?

Task 4

Configure a TACACS+ Exec Authorization Profile to set the Exec Level to **15**. Name the Authorization Profile **PRIV_15**.

ISE

1. Browse to "**Operations -> TACACS+ -> Live Logs"**

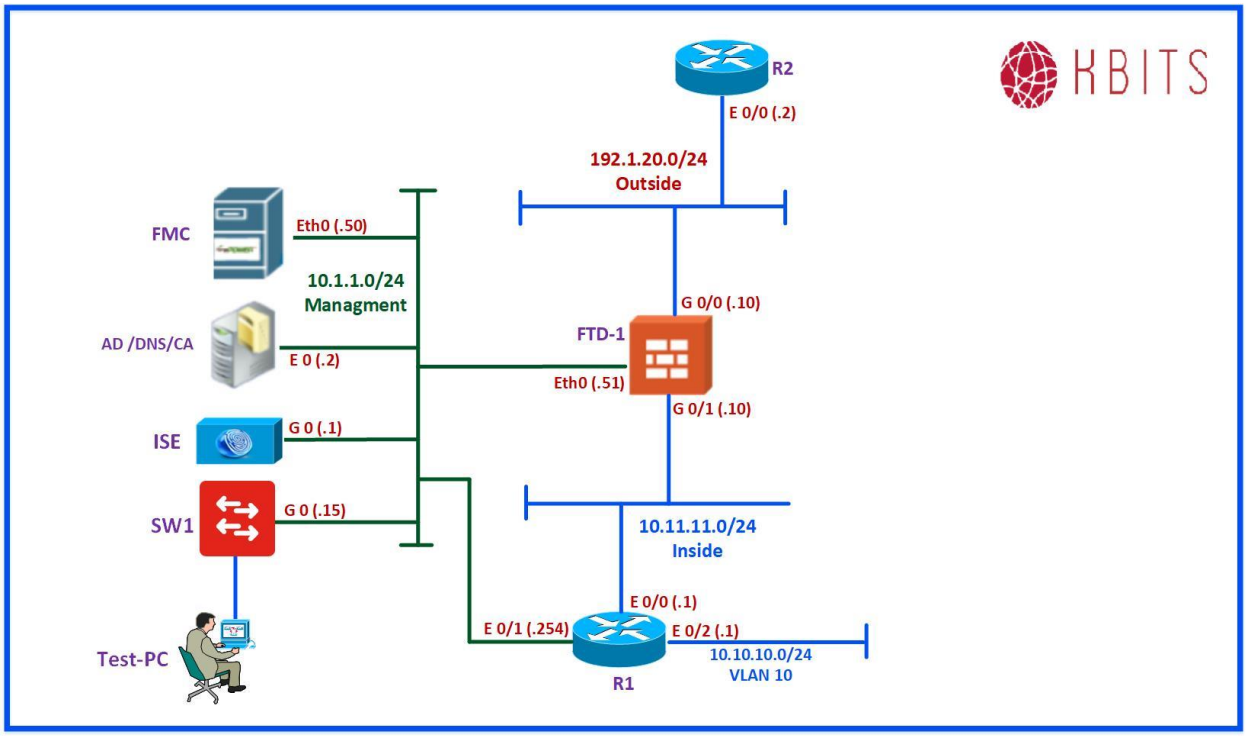
2. Verify that the Command and Logins are being recorded on ISE.

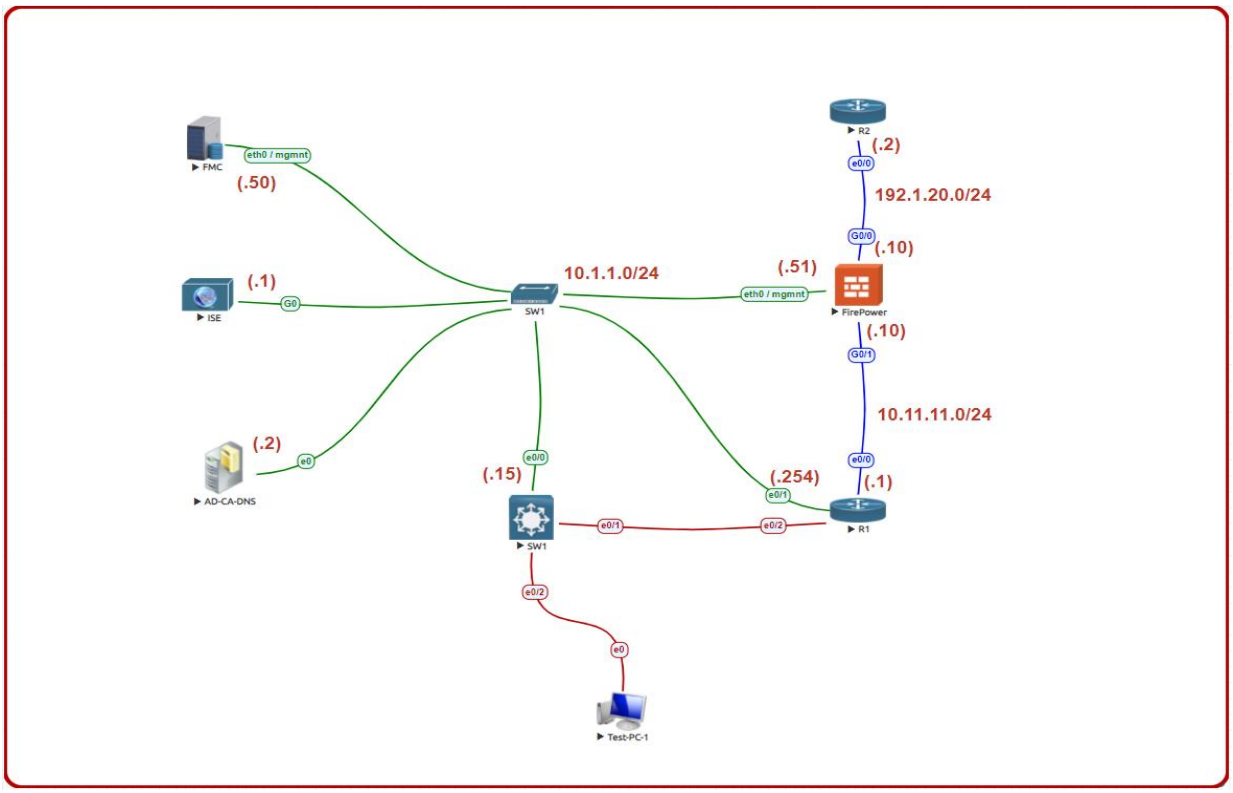
CCIE Security v6 – Identity Service Engine (ISE)

Module 6 – Integrating ISE with FMC & AD

Module 6 – Integrating ISE with FMC & AD

Lab 1 – Configure the network for Dot1x Authentication





Lab Scenario:

- Configuring the Base Network with VLANs, IP Addressing & Routing

Initial Setup:

- Not required.

Lab Tasks:

Task 1

Configure VLAN 10 on SW1. Configure the SW1 E0/0 as L3 port and assign it an IP Address of 10.1.1.15/24. Configure a static route back to 10.10.10.0/24 via 10.1.1.254 (R1).

SW1

```
VLAN 10
!
Ip routing
!
Interface E0/0
 No swichport
 Ip address 10.1.1.15 255.255.255.0
 No shut
!
Ip route 10.10.10.0 255.255.255.0 10.1.1.254
```

Task 2

Configure SW1 as a DHCP Server for VLANs 10.

Configuration parameters for VLAN 10 are:

- Range: 10.10.10.101 – 10.10.10.200
- Default Gateway: 10.10.10.1
- DNS-Server: 10.1.1.2

SW1

```
Ip dhcp excluded-address 10.10.10.1 10.10.10.100
Ip dhcp excluded-address 10.10.10.201 10.10.10.254
```

```
!
Ip dhcp pool VLAN10
 Network 10.10.10.0 /24
 Default-router 10.10.10.1
 Dns-server 10.1.1.2
```

Task 3

Configure R1 with IP Addresses based on the Logical Diagram. Configure a default gateway pointing towards the FTD (10.11.11.10). Configure R1 as a DHCP relay agent pointing towards SW1. SW1 will be configured as a DHCP Server.

R1

```
Interface E 0/0
 Ip address 10.11.11.1 255.255.255.0
 No shut
!
Interface E 0/1
 Ip address 10.1.1.254 255.255.255.0
 No shut
!
Interface E 0/2
 Ip address 10.10.10.1 255.255.255.0
 Ip helper-address 10.1.1.15
 No shut
!
Ip route 0.0.0.0 0.0.0.0 10.11.11.10
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

Task 4

Configure R2 with IP Address based on the Logical Diagram. Configure it with a default gateway pointing towards FTD (192.1.20.10). Enable Telnet using a password of Cisco123.

R2

```
Interface E 0/0
 Ip address 192.1.20.2 255.255.255.0
 No shut
!
Ip route 0.0.0.0 0.0.0.0 192.1.20.10
```

```
!
line vty 0 4
 Password Cisco123
 Login
 Transport input all
```

Task 5

Configure the ISE CLI Administrator password based on the following:

- The Default password on Eve-NG for ISE is Test123.
- It will prompt you to change the password.
- Change it to **Kbits@123**

ISE

```
ISE2-3 login: admin
Password:
You are required to change your password immediately (password aged)
Changing password for admin.
(current) UNIX password: Test123
Enter new UNIX password: Kbits@123
Retype new UNIX password: Kbits@123
```

Task 6

Reset the ISE GUI Admin password to **Kbits@123**.

ISE

```
ISE2-3/admin# application reset-passwd ise admin
Enter new password: Kbits@123
Confirm new password: Kbits@123

Password reset successfully.
```

Task 7

Configure/Verify ISE Network Parameters based on the following:

- IP Address: 10.1.1.1/24
- Default-Gateway: 10.1.1.254
- DNS Server (Name Server): 10.1.1.2
- Domain Name: kbits.live
- Hostname: ISE

ISE

```
Config t
!
hostname ISE1
!
ip domain-name Kbits.live
!
interface GigabitEthernet 0
 ip address 10.1.1.1 255.255.255.0
!
Ip default-gateway 10.1.1.254
!
no ip name-server 10.1.1.254
ip name-server 10.1.1.2
```

Note: It will prompt you to restart the ISE Application. Type "yes" to process. It will take a bit to come back.

Task 8

Configure RADIUS settings based on the following:

- Configure ISE to run the pxGrid services.
- We will be using pxGrid services for the ISE to FMC integration.

ISE

1. Browse to "**Administration -> System -> Deployment -> ISE1"**

2. Check to enable the pxGrid Services:

3. Click **Save.**

Task 9

Configure Network Device Group and Network Device for SW1 based on the following:

- Name: **SW1**
  - IP Address: **10.1.1.15/32**
  - Device Type: **Switches**
  - RADIUS: **Checked**
  - RADIUS Secret Password: **Cisco123***

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Administration -> Network Resources -> Network Device Groups -> Add**"

3. Create the Network Device Groups for **Switches** and click **Save.**

4. Browse to "**Administration -> Network Resources -> Network Devices -> Add**"

5. Create the SW1 based on the above parameters.

6. Click **Save.**

Task 10

Configure a Group on ISE. Name it **ISE-EMP**. Create a user **ISE-1** with a password of **Cisco123*.** Assign the user to the **ISE-EMP** group.

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Administration -> Identity Management -> Groups -> User Identity Groups -> Create**"

3. Create the ISE-EMP Group.

4. Click **Save.**

5. Browse to "**Administration -> Identity Management -> Identities -> Create**"

6. Create **ISE-1** based on the above parameters.

7. Click **Save.**

Task 11

Configure an authorization profile to assign **ISE-EMP** to **VLAN 10**. Assign it a name of **ISE-EMP-PROFILE**.

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles -> Add**"

3. Create the Authorization Profiles based on the above Parameters.

4. Click **Save.**

Task 12

Configure an authorization policy for ISE-EMP using the following paramters:

- Name: **ISE-EMP-POLICY**
  - Conditions:
    - Identity Group Name: **ISE-EMP**
    - Wired_802.1x
    - Network Device Group: **Switches**
  - Profile: **ISE-EMP-PROFILE**

ISE

1. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy -> <Insert at the top> -> Edit**"

2. Create the Authorization Policies based on the above Parameters.

3. Click **Save.**

Task 13

Configure **SW1** for Dot1x Authentication. Use basic 802.1x Authentication commands.

SW2

```
aaa new-model
!
username admin privilege 15 password admin
!
radius server ISE1
 address ipv4 10.1.1.1 auth-port 1812 acct-port 1813
 key Cisco123*
!
aaa group server radius ABC
 server name ISE1
!
aaa authentication dot1x default group ABC
```

```
aaa authorization network default group ABC
!
dot1x system-auth-control
!
interface E0/2
 switchport access vlan 100
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

Task 14

Configure the Windows 802.1x Supplicant.

Test-PC1

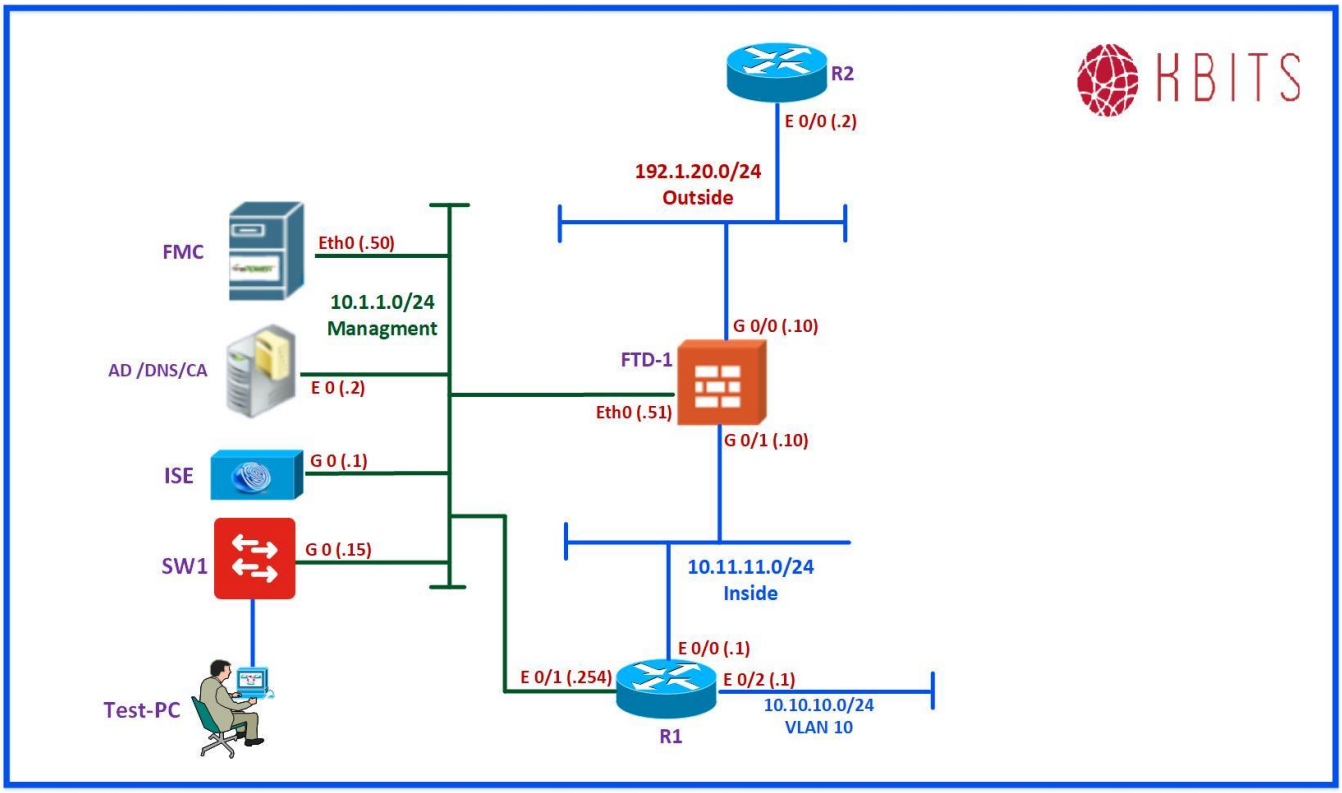
- **Enable the WiredAutoConfig Services**
  - Click Start. Type and open Services.
  - Set the **WiredAutoConfig** to start Automatically.
  - Start the service.
- **Configure the Network Adapter**
  - Right-Click the Network Adapter and click Properties under Network & Sharing Center to configure Dot1x.
  - Click the Authentication Tab.
  - Click **Settings**.
  - Uncheck "**Validate Server Certificate".**
  - Click "Configure" to uncheck the "**Automatically use the Windows Logon**".
  - Click **OK** to back to the Authentication Page.
- **Configure Authentication Parameters**
  - Click the "**Additional Settings**" button on the Authentication Page
  - Select "**User Authentication**".
  - Configure the Username as **ISE-1** with a password of **Cisco123*.**
  - Click **OK** to go back to the Authentication Page.
  - Click **OK** twice to accept the settings.

- You should be logged in with ISE-1 credentials.

- You can verify the credentials in ISE under the following:

  Operations -> RADIUS -> Live Logs

Lab 2 – Configuring Integrating ISE & AD for Dot1x Authentication



Lab Scenario:

- Integrate ISE & Active Directory.
- Authenticate Test-PC based on Active Directroy.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the relationship between ISE & AD based on the following:

- Join Point Name: **KBITS-AD**
- Active Directory Domain: **kbits.live**
- Administrator Username & Password: **Administrator/Kbits@123**

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Administration -> Identity Management -> External Identity Source -> Active Directory -> Add**"

3. Join the kbits.live domain using the parameters above.

Task 2

Pull down the groups listed below from AD to ISE:

- Kbits.live/users/Employees
- Kbits.live/users/Consultants
- Kbits.live/users/Domain Users

ISE

1. Browse to "**Administration -> Identity Management -> External Identity Source -> Active Directory -> KBITS-AD -> Groups**"

2. Add the groups specified above.

3. Click **Save.**

Task 3

Add the KBITS Identity in the Identity Source Sequence

ISE

1. Browse to "**Administration -> Identity Management -> Identity Source Sequences -> All_Users_ID_Stores"**

2. Select **KBTIS-AD** from the Available Box under Authentication Search List & click the "**>**" button.

3. Move **KBITS-AD** to the 2nd spot in the search list.

4. Click **Save.**

Task 4

Configure ISE to support certificate-based authentication for AD objects.

ISE

1. Browse to "**Administration -> Identity Management -> External Identity Sources -> Certificate Authentication Profile -> Preloaded-Certificate-Profile"**

2. Click the Drop-down box for Identity Store & select **KBITS-AD**.

3. Under Use Identity from, select the checkbox for "**Any Subject or alternate name Attributes in the certificate (for Active Directory Only)**"

4. Click **Save.**

Task 4

Configure 2 Authorization Profiles to assign AD Users to appropriate VLANs based on the following:

- Name: **AD-EMP-PROFILE**
- VLAN: **10**

- Name: **AD-CON-PROFILE**
- VLAN: **20**

ISE

1. Browse to "**Policy -> Policy Elements -> Results -> Authorization ->**

Authorization Profiles -> Add"

2. Configure the Authorization Profiles based on the above parameters.

3. Click **Save.**

Task 5

Configure authorization policies for Active Directory users based on the following:

- Name: **AD-EMP-POLICY**
  - Conditions:
    - KBITS:ExternalGroups: **kbits.live/Users/Employees**
    - **Wired_802.1x**
    - Network Device Group: **Switches**
  - Profile: **AD-EMP-PROFILE**

- Name: **AD-CON-POLICY**
  - Conditions:
    - KBITS:ExternalGroups: **kbits.live/Users/Consultants**
    - **Wired_802.1x**
    - Network Device Group: **Switches**
  - Profile: **AD-CON-PROFILE**

ISE

1. Browse to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy -> Insert Rule Above"**

2. Configure the Authorization Policies based on the above Parameters.

3. Click **Save.**

Task 6

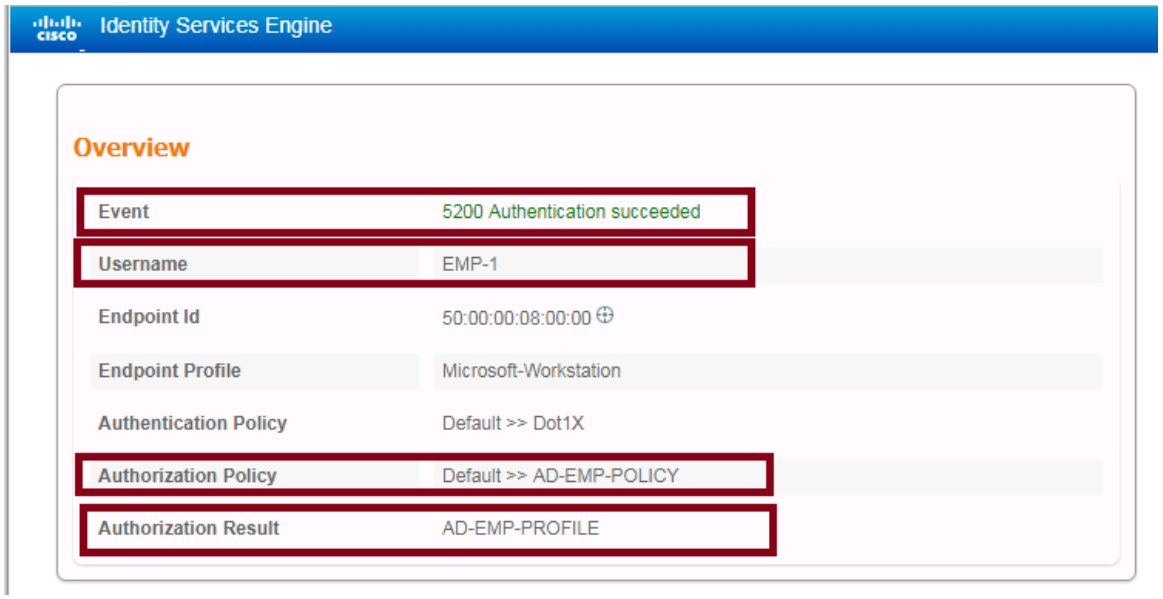
Re-login using the Active Directory user credentials.

Test-PC1

- Under the Network Adapter under Network & Sharing Center, Replace the credentials to **EMP-1/Cisco123*** by clicking on the **Authentication -> Additional Settings** Page

- Verify the IP Address and RADIUS Log in ISE.

- You can also verify the configuration on the Switch by using the following commands:
  - **Show authentication session interface E0/1 details**
  - **Show VLAN**

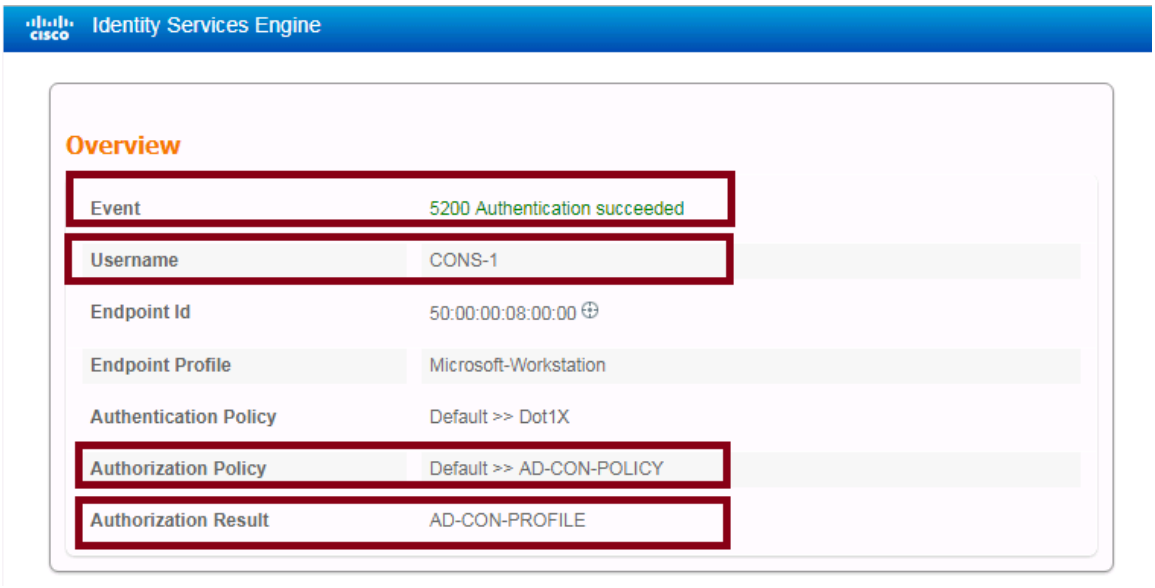


Task 7

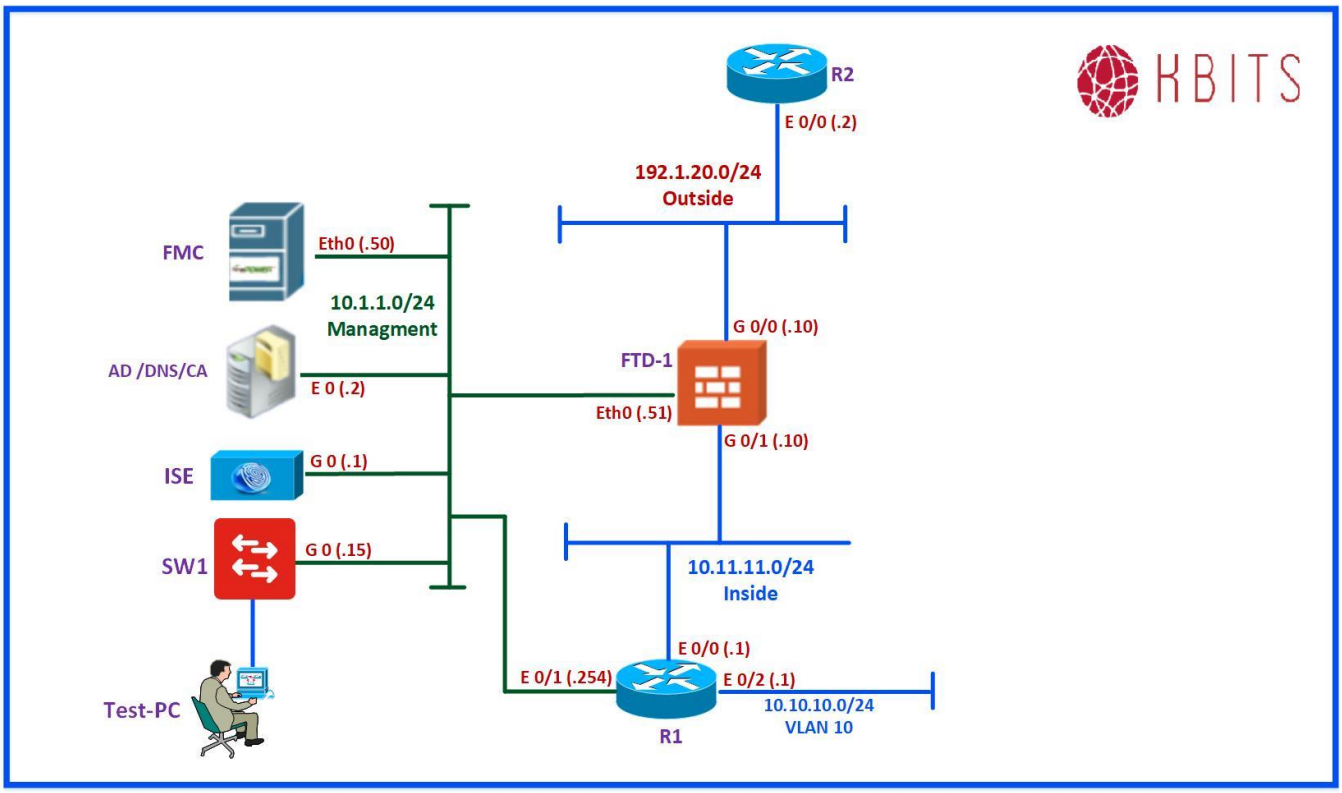
Re-login using the Active Directory user credentials.

Test-PC1

- Under the Network Adapter under Network & Sharing Center, Replace the credentials to **CONS-1/Cisco123*** by clicking on the **Authentication -> Additional Settings** Page
- Verify the IP Address and RADIUS Log in ISE.
- You can also verify the configuration on the Switch by using the following commands:
  - **Show authentication session interface E0/1 details**
  - **Show VLAN**



Lab 3 – Configuring Certificates for the FMC



Lab Scenario:

- Generating a CSR for FMC using the command line.
- Installing the CA Root Certificate on the FMC.

Initial Setup:

- **Pre-requisite: FMC & FTD Configured.**
- **Based on the previous Lab**

Lab Tasks:

Task 1

Generate a CSR and Key file on the FMC using the FMC command line.

SSH into the FMC. FMC is configured with a username of admin with a password of Kbits@123.

- Generate a Key for the Identity certificate using the following command:
- Active Directory Domain: **kbits.live**
- Administrator Username & Password: **Administrator/Kbits@123**

FMC

1. SSH into the FMC. FMC is configured with a username of **admin** with a password of **Kbits@123**.

2. Generate a Key for the Identity certificate using the following paramters:
   - Key Name: **FMC.key**
   - Size: **4096**

3. Use the "**openssl genrsa -out FMC.key 4096**" to generate the Key File.

4. Generate the CSR for the Identity Certificate using the Key created in the previous step. The CSR file should be named **FMC.csr**.

5. Use the "**openssl req -new -key FMC.key -out FMC.csr**" to generate the key.

Task 2

Download the files created in the previous step on the AD-DNS-CA device using WinSCP. Use SFTP to connect using a username of **admin** with a password of **Kbits@123**. Copy the FMC.key & FMC.csr files. They should be stored in the downloads folder by default.

Task 3

Download the Root Certificate from the CA Server. It will be uploaded to the FMC and ISE in later steps and Labs.

Admin-PC/AD-DNS-CA Devices

1. Browse to http://10.1.1.2/certsrv

2. Click "**Download Root Certificate**".

3. Select "**Base 64**".

4. Click “**Download CA Certificate**”.

5. Open Explorer and navigate to the downloads folder. Change the name of the Downloaded file “**certnew**” to “**RootCert**”.

Task 4

Enroll the FMC CSR to generate an Identity Certificate for the FMC.

Admin-PC/AD-DNS-CA Devices

1. Using Wordpad, open the “**FMC.csr**” file located in the downloads folder.

2. Copy by using **CTRL-A** and **CTRL-C.**

3. Browse to http://10.1.1.2/certsrv

4. Click “**Request a Certificate**”.

5. Select “**Advanced**”.

6. Paste the CSR in the box by using **CTRL-V**.

7. Select the “**pxGrid**” template from the Template drop-down and click Submit.

8. The Identity Certificate should be auto-enrolled.

9. Select “**Base 64**” and click “**Download**”.

10. Open Explorer and navigate to the downloads folder.

11. Change the name of the Downloaded file “**certnew**” to “**FMC-ID**”.

Task 5

Install the Root Certificate in FMC.

FMC

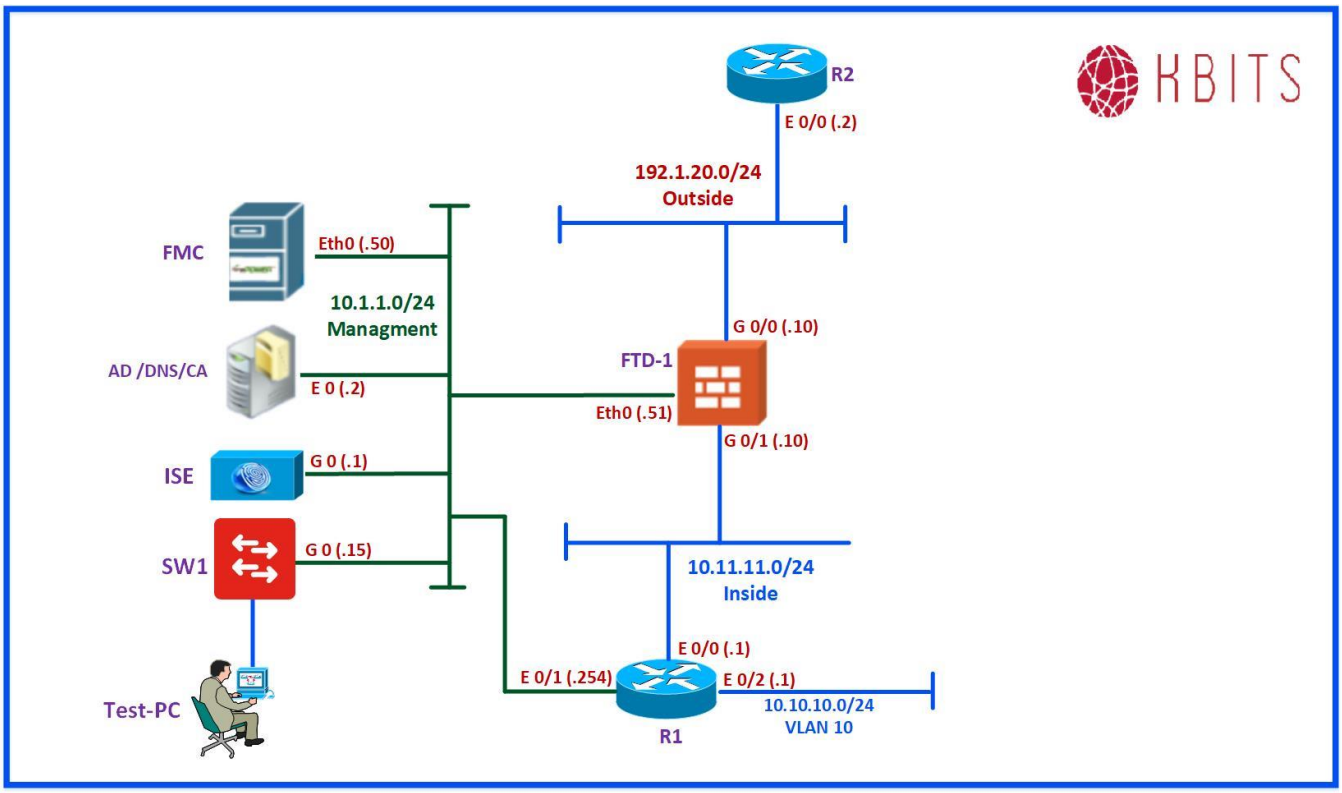
1. Log into **FMC** by browsing to https://10.1.1.50. Login using a Username of **admin** and a password of **Kbits@123**.

2. Navigate to "**Objects -> Object Management -> Trusted CAs and click Add Trusted CA**".

3. Assign the CA Server a name of "**KBITS-CA**". Use the "**RootCert.cer**" file in the download folder as the Root Certificate.

4. Click **Save**.

Lab 4 – Configuring Certificates and pxGrid on ISE



Lab Scenario:

- Generating a CSR and Installing Identity Certificate on ISE.
- Installing the CA Root Certificate on the ISE.
- Enabling the pxGrid Service.

Initial Setup:

- **Pre-requisite: FMC & FTD Configured.**
- **Based on the previous Lab**

Lab Tasks:

Task 1

Add the CA Server as a Trusted Certificate server in ISE.

ISE

1. Log into ISE using a Username of **admin** and a password of **Kbits@123**.

2. Browse to "**Administration -> System -> Certificates -> Trusted Certificates"**.

3. Add the CA Server as a Trusted Certificate Server by uploading the RootCert file from the Downloads folder. The name of the file is "RootCert.cer".

4. Allow this Certificate Server to be used for all authentications

5. Click **Save**.

Task 2

Generate a CSR on ISE. Configure it to be used for **pxGrid** Services. Name the file "**ISE-CSR**".Use defauts for all parameters.

ISE

1. Generate a Certificate Service Request by browsing to "**Administration -> System -> Certificates -> Certificate Signing Requests"**.

2. The CSR should be used for pxGrid services on the local node. Use the defaults for all the parameters.

3. Name the Export File "**ISE-CSR**". It will be stored in the Downloads folder as a .pem file.

Task 3

Enroll the ISE CSR to generate an Identity Certificate for the ISE.

ISE

1. Using Wordpad, open the "**ISE-CSR.pem**" file located in the downloads folder.

2. Copy by using **CTRL-A** and **CTRL-C.**

3. Browse to http://10.1.1.2/certsrv

4. Click "**Request a Certificate**".

5. Select "**Advanced**".

6. Paste the CSR in the box by using **CTRL-V**.

7. Select the "**pxGrid**" template from the Template drop-down and click Submit.

8. The Identity Certificate should be auto-enrolled.

9. Select "**Base 64**" and click "**Download**".

10. Open Explorer and navigate to the downloads folder.

11. Change the name of the Downloaded file "**certnew**" to "**ISE-ID**".

Task 4

Install the Identity Certificate downloaded from the CA Server on ISE.

ISE

1. Install the Identity Certificate by browsing to "**Administration -> System -> Certificates -> Certificate Signing Requests"**.

2. Select the checkbox for the CSR listed and click **Bind Certificate**.

3. Upload the "**ISE-ID.cer**" file from the Downloads folder. Check all boxes.

4. Click **Save**.

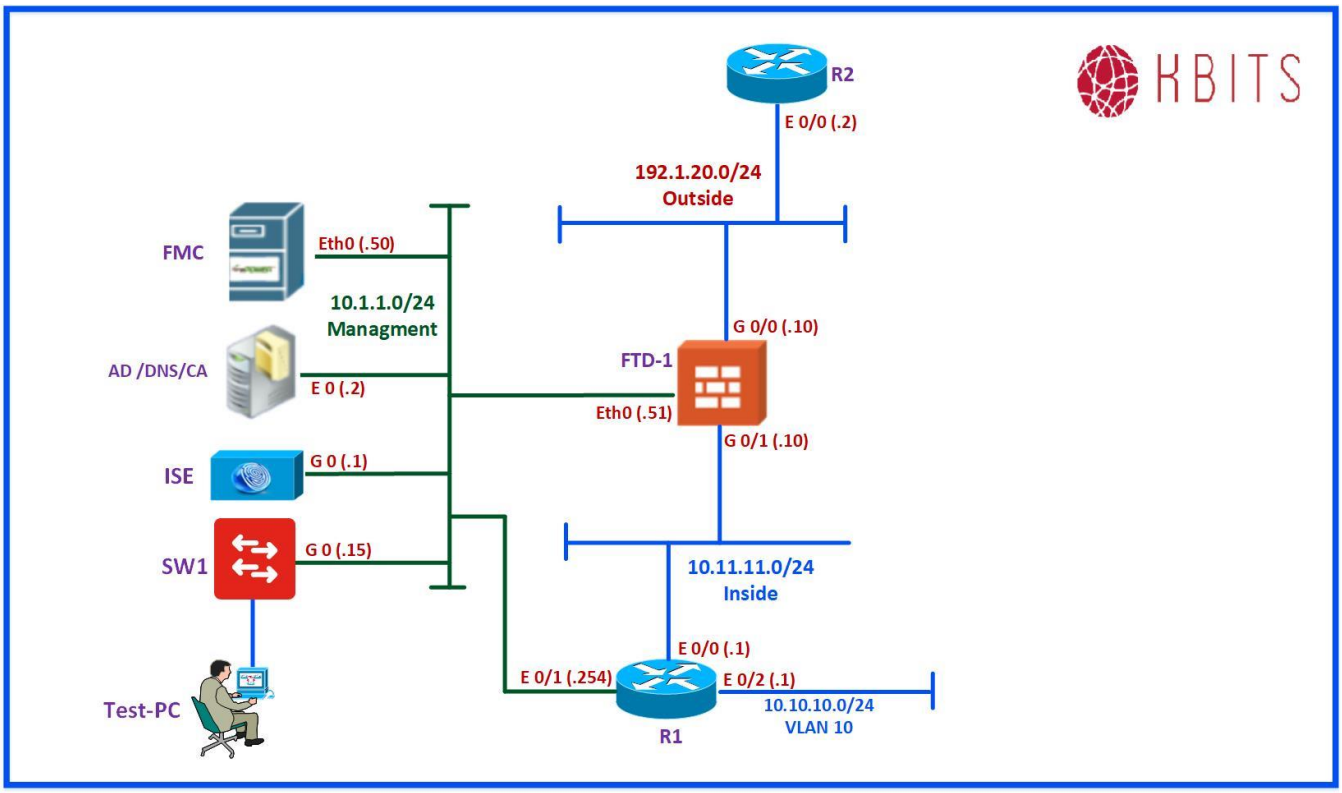
Task 5

Enable the pxGrid Service on ISE.

ISE

1. Browse to "**Administration -> System -> Deployment -> ISE1**".
2. Select the "**pxGrid**" Service and **submit**.
3. Verify the pxGrid Status by browsing to "**Administration -> pxGrid Services**".
4. Click **Settings** & select "**Automatically approve new accounts**".
5. Wait for pxGrid services to be online. It may take upto 5 minutes.

Lab 5 – Configuring FMC to Integrate with ISE & AD



Lab Scenario:

- Installing the FMC Identity Certificate on th FMC.
- Integrating FMC & ISE.
- Integrating FMC & AD.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure a relationship between FMC & ISE. Install the FMC certificate received from the CA Server. Use the following parameters for the integration:

- ISE IP Address: **10.1.1.1**
- pxGrid Server CA: **KBITS-CA**
- MNT Server CA: **KBITS-CA**
- FMC ID Certficate Name: **FMC-ID**
- FMC ID Certificate Filename: **FMC-ID.cer**.
- FMC Key Filename: **FMC.key**.

FMC

1. Log into FMC by browsing to https://10.1.1.50. Login using a Username of **admin** and a password of **Kbits@123**.

2. Navigate to "**System -> Integration -> Identity Sources**"

3. Click on "**Identity Services Engine**".

4. Configure ISE integration based on the parameters above.

5. Click **Save**.

Task 2

Configure the Integration between FMC & Active directory. Use the parameter below for the Integration.

- Name of the Realm: **KBITS-AD**
- Choose a type – **AD**
- Enter the AD primary domain: **kbits.live**
- Add the username: **administrator@kbits.live**
- Add the password: **Kbits@123**
- Base DN: **cn=Users,dc=kbits,dc=live**
- Group DN: **cn=Users,dc=kbits,dc=live**
- Group Attribute – **Member**

FMC

1. Navigate to "**System -> Integration -> Realms**".

2.Click on "**New Realms**".

3. Configure the Realm parameters based on the above parameters.

4. Click "**Save**".

Task 3

Add the Directory Services on FMC based on the following parameters:

- Hostname: **10.1.1.2**
- Port: **389**
- Encryption: **None**

FMC

1. Navigate to "**Directory**" Tab.

2. Click the "**Add Directory**" button towards the right.

3. Add the Directory based on the above parameters.

4. Click **OK.**

Task 4

Configure the Users/Groups that need to be download into FMC from the Active directory based on the following:

- **Employees**
- **Consultants**
- **Domain Users.**

FMC

1. Click the "**User Download Tab**".

2. Specify the Groups to be download based on the above information.

3. Click **Save.**

Task 5

Enable the realm and download the users that need to be download based on the previous configuration.

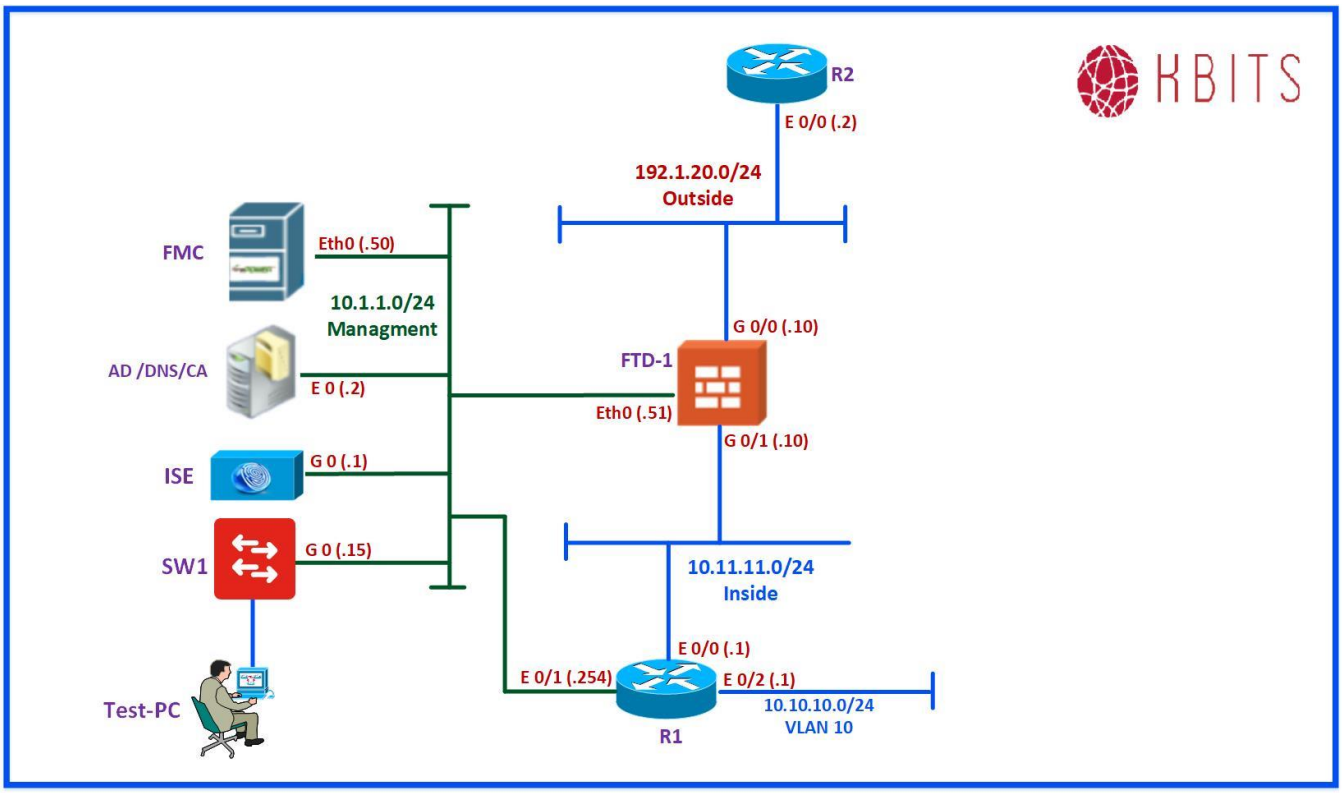
FMC

1. Navigate to "**System -> Integration -> Realms -> KBITS-AD**".

2. Enable the Realm by use the **slide-bar** under the "**State**" column.

3. Click the **Download Icon** next to the State to download the Users and groups from AD.

Lab 6 – Configuring FMC to use Identity Policies in ACP



Lab Scenario:

- Configuring an Identity Policy to use the KBITS-AD Realm.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Create an Identity Policy that will link the KBITS-AD Realm to be used in an Access Control Policy. Use the following parameters to configure the Identity Policy:

- Identity Policy Name: **ID-Policy-AD**
- Rule Name: **KBITS-AD**
- Realm Name: **KBITS-AD**

FMC

1. Navigate to "**Policies -> Access Control -> Identity**".
2. Click on "**New Policy**".
3. Name the Policy "**ID-Policy-AD**".
4. Click "**Add Rule**". Configure the Rule name as "**KBITS-AD**".
5. Click on "**Realm & Settings**".
6. Add the "**KBITS-AD**" realm
7. Click **Save**.
8. Click **Save** to save the Identity Policy.

Task 2

Configure the existing Access Control Policy (FTD1-ACP) to use the Identity Policy created in the previous task.

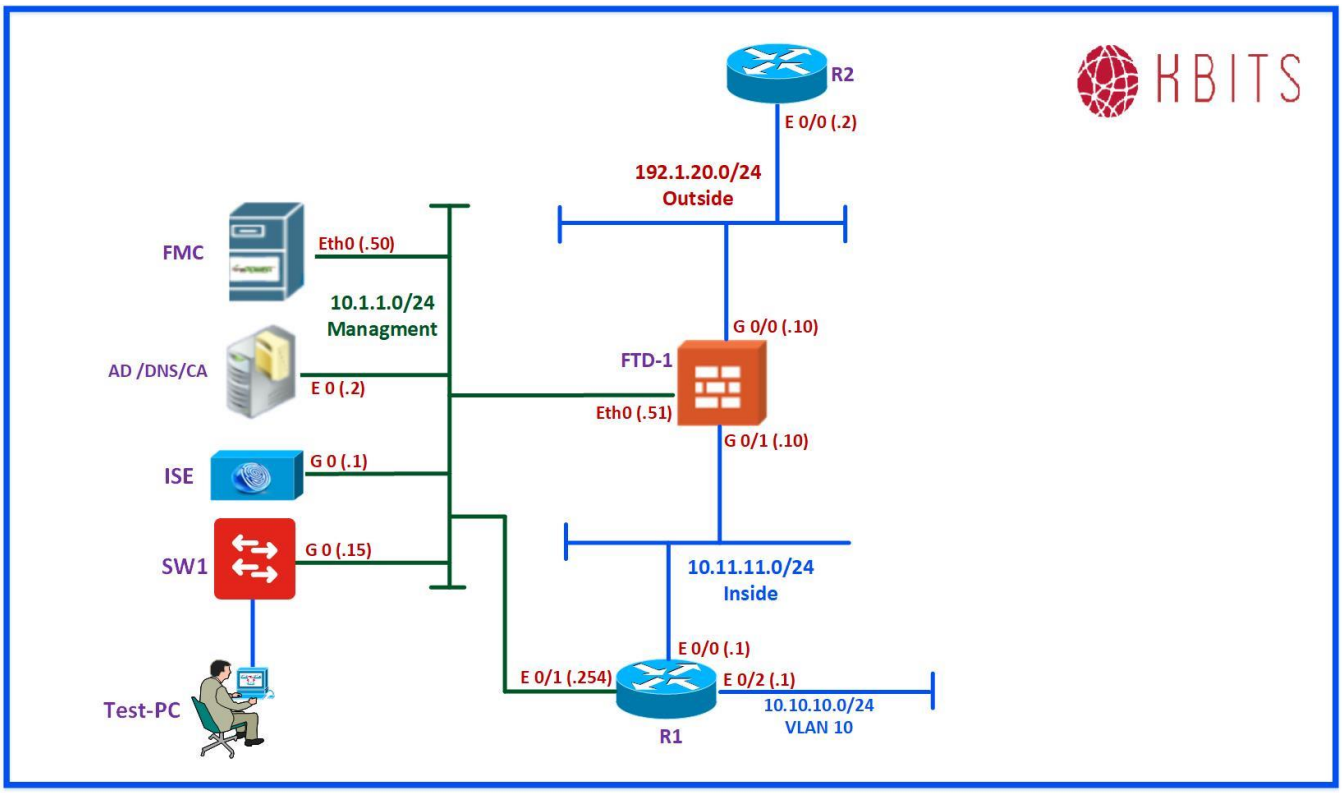
FMC

1. Navigate to "**Policies -> Access Control -> Access Control -> FTD1-ACP**"
2. Click **Edit**[Pencil].
3. Click the **Identity Policy link**.
4. Select the **ID-Policy-AD** policy as the Identity Policy.
5. Click the "**Advanced Settings**".

6. Configure the "**Transport/Network Layer Preprocessor**" Settings to "**Ignore the VLAN header when tracking connections**".

7. Click **Save** to save the Access Control Policy.

Lab 7 – Configuring FMC to use AD & ISE Attributes in ACP



Lab Scenario:

- Configure the ACP Rules to include Active Directory & ISE attributes.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure a new rule that will allow KBITS-AD/Employees full access from Inside Zone to Outside. Add the rule in the FTD1-ACP based on the following:

- Name: **INSIDE-2-OUTSIDE-AD**
- Action: **Allow**
- Source Zone: **INSIDE**
- Destination Zone: **OUTSIDE**
- Users: **KBITS-AD/Employees**

FMC

1. Navigate to "**Policies -> Access Control -> Access Control -> FTD1-ACP**"

2. Click **Edit** [Pencil].

3. Click on "**Add Rule**" to add a new rule at the top of the ACP based on the above parameters.

4. Click **Save** to save the rule.

Task 2

Configure a new rule that will allow ISE SGT/Employees full access from Inside Zone to Outside. Add the rule in the FTD1-ACP based on the following:

- Name: **INSIDE-2-OUTSIDE-ISE**
- Action: **Allow**
- Source Zone: **INSIDE**
- Destination Zone: **OUTSIDE**
- ISE/SGT Attribute: **SGT/Employees**

FMC

1. Navigate to "**Policies -> Access Control -> Access Control -> FTD1-ACP**"

2. Click **Edit** [Pencil].

3. Click on "**Add Rule**" to add a new rule at the top of the ACP based on the above parameters.

4. Click **Save** to save the rule.

Task 3

Re-Configure the ISE policy based on the following to assign the SGT besides the VLAN.

- Authorization Policy Name: **AD-EMP-POLICY**
- Result: **SGT -> Employees**

ISE

1. Log into ISE using a Username of **admin** and a password of **Kbits@123**.
2. Navigate to "**Policy -> Policy Sets -> Default -> ">" -> Authorization Policy**"
3. Re-configure the **AD-EMP-POLICY** based on the above requirement.
4. Click **Save** to save the rule.

Task 4

Log in on the Test-PC1 using the Active Directory user credentials.

Test-PC1

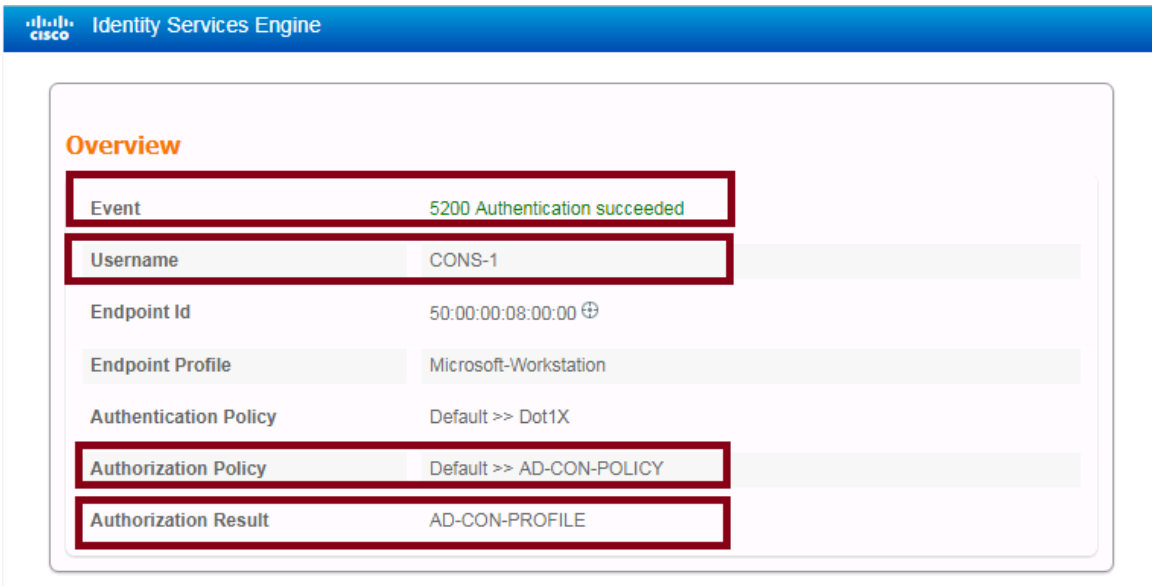
- Under the Network Adapter under Network & Sharing Center, Replace the credentials to EMP-1/Cisco123* by clicking on the **Authentication -> Additional Settings** Page
- **Telnet** and **Ping 192.1.20.2**. Are you successful?

Task 5

Re-login using the ISE user credentials.

Test-PC1

- Under the Network Adapter under Network & Sharing Center, Replace the credentials to **ISE-1/Cisco123*** by clicking on the **Authentication -> Additional Settings** Page
- **Telnet** and **Ping 192.1.20.2**. Are you successful?

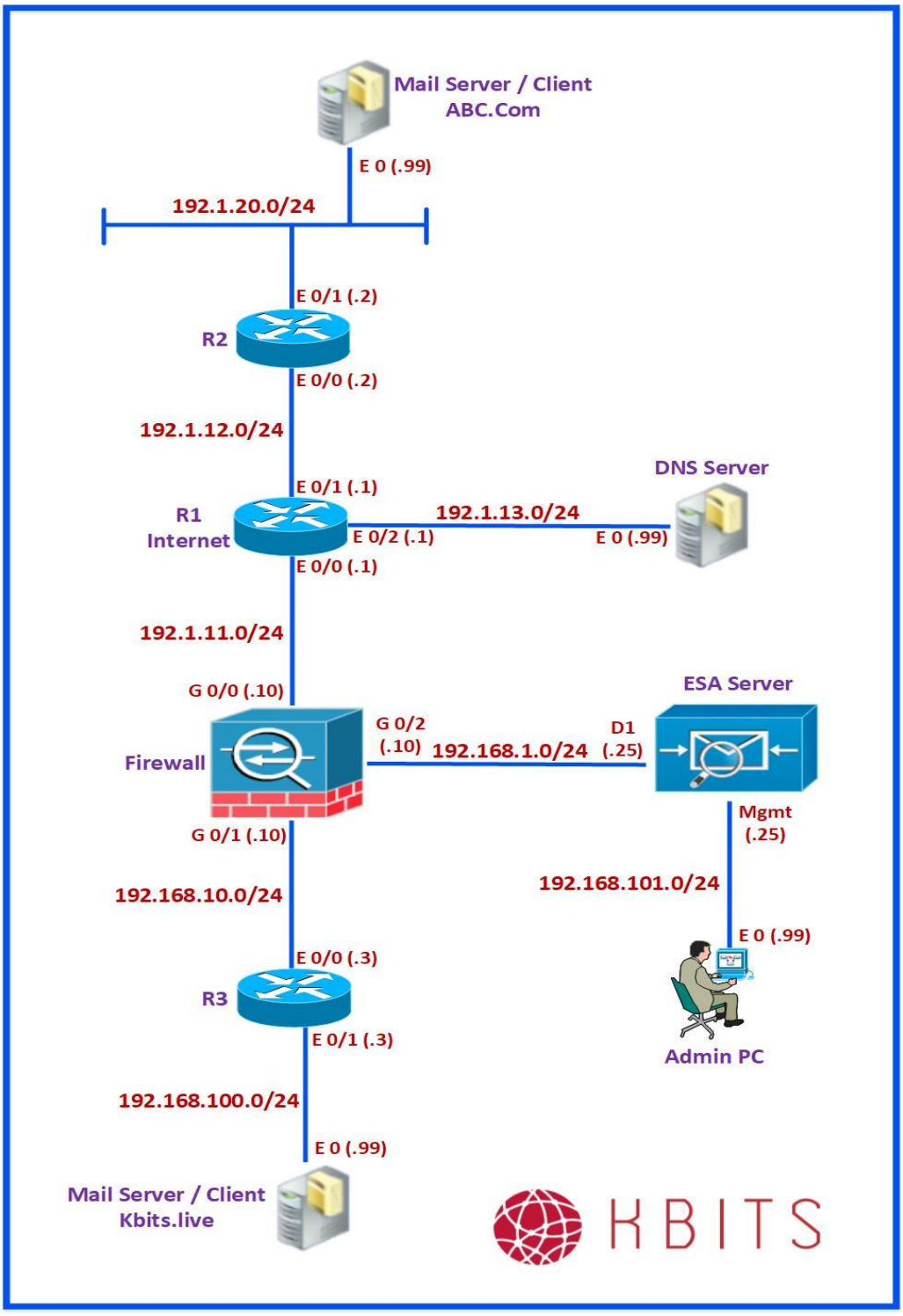


CCIE Security v6 – E-Mail Security Applicance (ESA)

Module 1 - Initial Configuration of the ESA

Module 1 – Initial Configuration of the ESA

Lab 1 – Initial E-Mail Server and Client Setup in the Network



Lab Scenario:

- Configuring the Base Network for E-Mail Exchange between 2 Domains.

Initial Setup:

- Not required.

Lab Tasks:

Task 1

Configure R1, R2 & R3 IP Addresses based on the network diagram. Configure a Default Route on R2 pointing towards R1. Configure a static route on R1 for the 192.1.20.0/24 network using R2 as the next hop. Enable the E 0/0 & E 0/1 interface under EIGRP 123 on R3. Also, configure a Default Route on R3 towards the ASA.

R1

```
interface Ethernet0/0
 ip address 192.1.11.1 255.255.255.0
 no shut
!
interface Ethernet0/1
 ip address 192.1.12.1 255.255.255.0
no shut
!
interface Ethernet0/2
 ip address 192.1.13.1 255.255.255.0
no shut
!
Ip route 192.1.20.0 255.255.255.0 192.1.12.2
```

R2

```
interface Ethernet0/0
 ip address 192.1.12.2 255.255.255.0
 no shut
!
interface Ethernet0/1
 ip address 192.1.20.2 255.255.255.0
 no shut
!
```

```
Ip route 0.0.0.0 0.0.0.0 192.1.12.1
```

R3

```
interface Ethernet0/0
 ip address 192.168.10.3 255.255.255.0
 no shut
!
interface Ethernet0/1
ip address 192.168.100.3 255.255.255.0
 no shut
!
Router eigrp 123
 Network 192.168.10.0
 Network 192.168.100.0
!
ip route 0.0.0.0 0.0.0.0 192.168.10.10
```

Task 2

Configure ASA Firewall IP Addresses based on the following:

- Gig 0/0
  - Name: **Outside**
  - Security-Level: **0**
  - IP Address: **192.1.11.10/24**
- Gig 0/1
  - Name: **Inside**
  - Security-Level: **100**
  - IP Address: **192.168.10.10/24**
- Gig 0/2
  - Name: **DMZ**
  - Security-Level: **50**
  - IP Address: **192.168.1.10/24**

ASA

```
Interface Gig0/0
 Nameif Outside
 Ip address 192.1.11.10
 No shut
!
Interface Gig0/1
 Nameif Inside
```

```
 Ip address 192.168.10.10
 No shut
!
Interface Gig0/2
 Nameif DMZ
 Security-level 50
 Ip address 192.168.1.10
 No shut
```

Task 3

Configure ASA Firewall with a Default Route towards R1. Also enable EIGRP in AS 123 on the Inside Interface.

ASA

```
Router eigrp 123
 Network 192.168.10.0
!
Route outside 0 0 192.1.11.1
```

Task 4

Translate the Kbits.live Mail-Server located at 192.168.100.99 as 192.1.11.25 on the Outside. Allow SMTP Access to this server from Outside.

ASA

```
Object network Mail
 Host 192.168.100.99
 Nat (Inside,Outside) static 192.1.11.25
!
access-list OUTSIDE permit tcp any host 192.168.100.99 eq 25
Access-group OUTSIDE in interface Outside
```

Task 5

Configure the DNS Server with 2 Zones for ABC.com & Kbits.live based on the following:

- Domain: **Kbits.live**
  - Zone Type: **Primary Zone**
  - Zone Name: **kbits.live**
  - Zone Filename: **kbits.live.dns**
  - Dynamic Updates: **No**

- Domain: **Abc.com**

- Zone Type: **Primary Zone**
- Zone Name: **abc.com**
- Zone Filename: **abc.com.dns**
- Dynamic Updates: **No**

DNS

1. RDP into the DNS Server using **administrator/Test123** as the username/password combination.

2. Open **Server Manager** and navigate to "**Server Manager -> Roles -> DNS Server -> DNS -> SRV -> Forward Lookup Zones**".

3. Right-Click to create "**New Zone**".

4. Create 2 zones based on the above parameters.

Task 6

Configure the DNS Records A Record for the mail servers in ABC.com & Kbits.live based on the following:

- Domain: **Kbits.live**
  - Record Type: **A Record**
  - Record Name: **mail**
  - FQDN: **mail.kbits.live**
  - IP Address: **192.1.11.25**

- Domain: **abc.com**
  - Record Type: **A Record**
  - Record Name: **mail**
  - FQDN: **mail.abc.com**
  - IP Address: **192.1.20.99**

DNS

1. Navigate to "**Server Manager -> Roles -> DNS Server -> DNS -> SRV -> Forward Lookup Zones -> [Zone Name]**".

2. Right-Click to create "**New Host (A or AAAA)**".

3. Create Host (A) Records for the Mail Servers for Kbits.live & Abc.com based on the above parameters:

Task 7

Configure the DNS Records MX Record for ABC.com & Kbits.live pointing to the respective Mail Servers based on the following:

- Domain: **Kbits.live**
  - Record Type: **MX Record**
  - FQDN: **mail.kbits.live**

- Domain: **Kbits.live**
  - Record Type: **MX Record**
  - FQDN: **mail.abc.com**

DNS

1. Navigate to "Server Manager -> Roles -> DNS Server -> DNS -> SRV -> Forward Lookup Zones -> [Zone Name]"

2. Right-Click to create "**New Mail Exchanger (MX)**".

3. Browse to the appropriate Mail Server for the FQDN and Click **OK**.

Task 8

2 Accounts are configured on the Thunderbird Client on the Mail Server/Client Device – Kbits.live. We will use these accounts to send and receive Messages. **(Info Only).**

- Name: **Kbits One**
- Account: kbits1@kbits.live
- Password: Cisco123*
- Mail & SMTP Servers: 192.168.100.99

- Name: **Kbits Two**
- Account: kbits2@kbits.live
- Password: Cisco123*

Task 9

2 Accounts are configured on the Thunderbird Client on the Mail Server/Client Device – Abc.com. We will use these accounts to send and receive Messages. **(Info Only).**

- Name: **Abc One**
- Account: Abc1@kbits.live
- Password: Cisco123*
- Mail & SMTP Servers: mail.abc.com

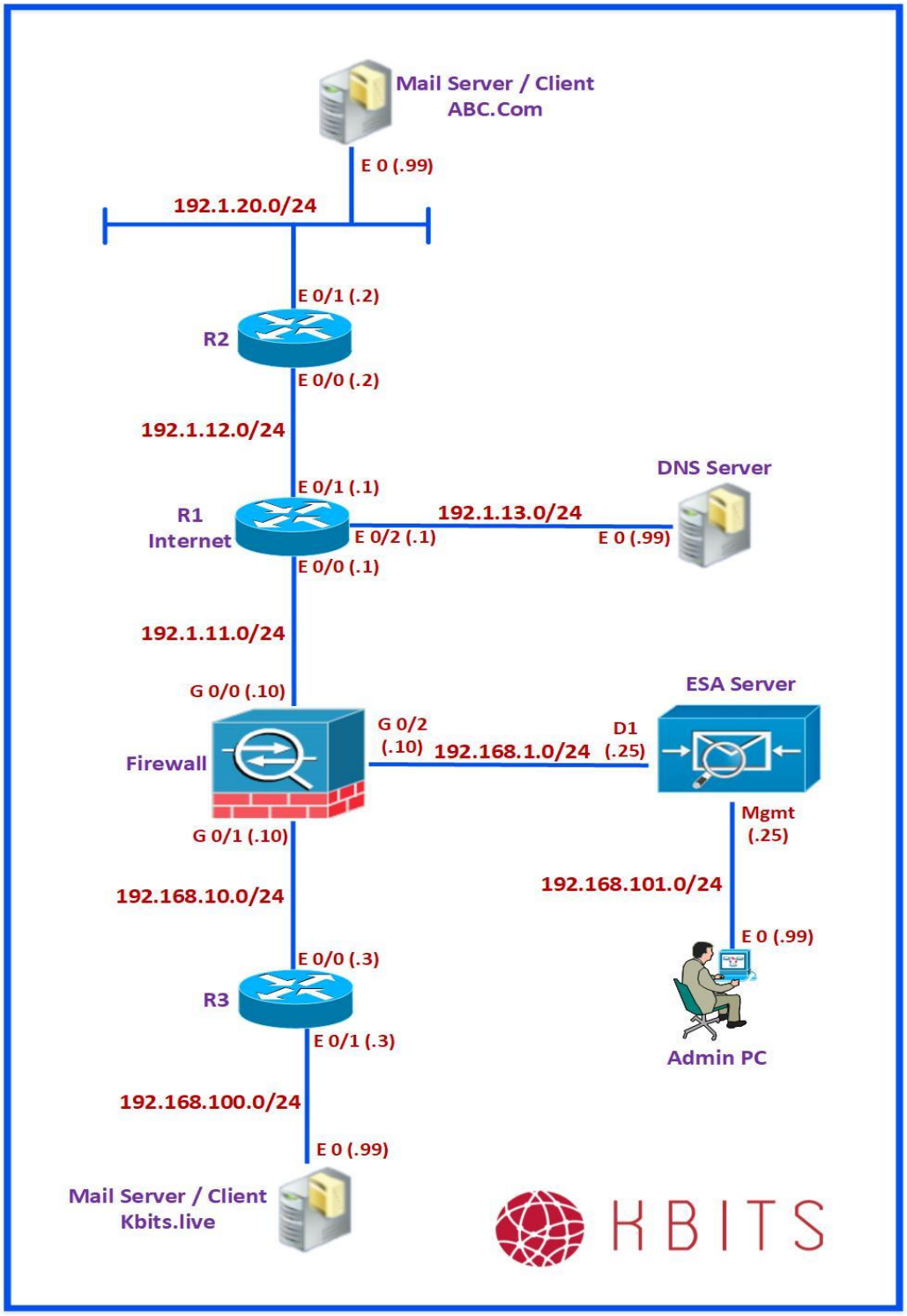
- Name: **Abc Two**

- Account: Abc2@kbits.live
- Password: Cisco123*
- Mail & SMTP Servers: mail.abc.com

Task 10

Verify the E-mail configuration by sending and receiving E-mail between the Users on the 2 domains.

Lab 2 – Initializing the ESA Appliance from CLI



Lab Scenario:

- Initialize the ESA from the Command Line.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Initialize the ESA from the CLI using the following parameters:

- Management Interface configuration:
  - Name: **MgmtData**
  - IP Address: **192.168.101.25/24**
  - Hostname: **ESA.KBITS.LIVE**
  - Protocols: **SSH, FTP, HTTP & HTTPS**
- Rest of the Parameters: **Default**

ESA

1. Log into ESA from the CLI Using the default Username and password (**admin/ironport**).

2. Type **interfaceconfig** and following the prompts:

Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: esa.kbits.live)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):

[Management]> **MgmtData**

Would you like to configure an IPv4 address for this interface (y/n)? [Y]> y

IPv4 Address (Ex: 192.168.1.2):
[192.168.42.42]> **192.168.101.51**

Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> **255.255.255.0**

Would you like to configure an IPv6 address for this interface (y/n)? [N]> **n**

Ethernet interface:
1. Data 1
2. Data 2
3. Management
[3]> **3**

Hostname:
[esa.ironport.com]> **mgmt.Kbits.live**

Do you want to enable SSH on this interface? [Y]> **y**

Which port do you want to use for SSH?
[**22**]**>**

Do you want to enable FTP on this interface? [Y]> **y**

Which port do you want to use for FTP?
[**21**]>

Do you want to enable Cluster Communication Service on this interface? [N]>

Do you want to enable HTTP on this interface? [Y]> **y**

Which port do you want to use for HTTP?
[**80**]>

Do you want to enable HTTPS on this interface? [Y]> **y**

Which port do you want to use for HTTPS?
[**443**]>

Do you want to enable Spam Quarantine HTTP on this interface? [N]>

Do you want to enable Spam Quarantine HTTPS on this interface? [N]>

Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [N]>

Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface? [N]>

The "Cisco ESA Certificate" certificate is currently configured. You may use "Cisco ESA Certificate", but this will not be secure. To assure privacy, run "certconfig" first.

Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the secure service? [**Y**]> **y**

Updating SNMP agent interface referencing the old interface name "Management"
to the new interface name "**MgmtData**".

Take default for everything

Task 2

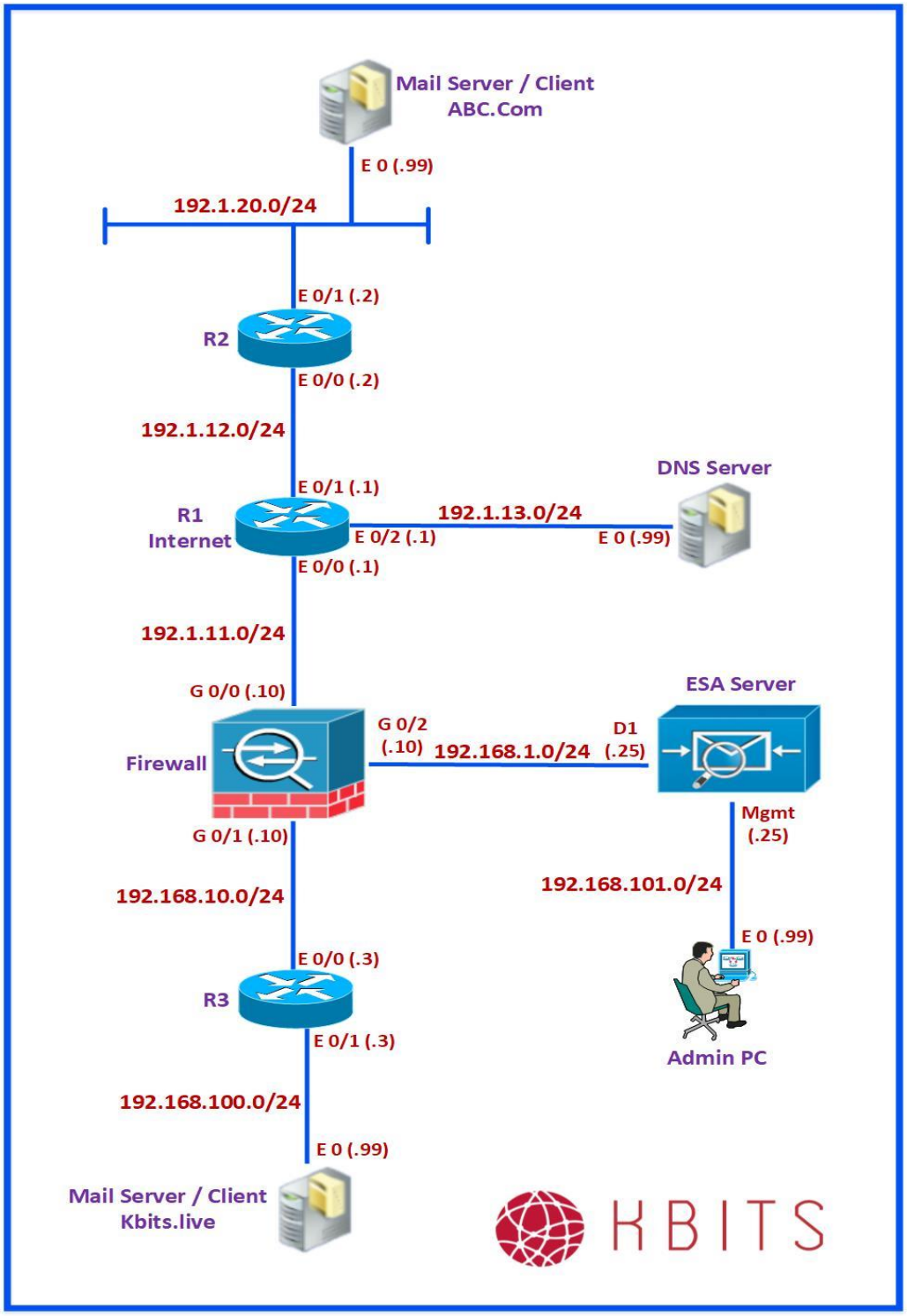
Verify Graphical access to the ESA.

Admin PC

1. Browse to **192.168.101.25**.

2. Log in using the default username & Password of **admin/ironport**.

Lab 3 – Running the System Setup Wizard on ESA



Lab Scenario:

- Initializing the ESA using the System Setup Wizard.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Run the System Wizard to finalize the initial setup. Verify/Re-configure the ESA Networking with the following Parameters:

- System Configuration:
  - System Name: **ESA.Kbits.live**
  - Alert E-Mail: **kb@kbits.live**
  - Administrator Passphrase: **Kbits@123**

- Network Integration:
  - IPv4 Default Gatway: **192.168.1.10**
  - DNS Server: **192.1.13.99**

- Interface Configuration – Data 1:
  - Data1: **Enabled**
  - Name: **Internet**
  - IP Address: **192.168.1.25/24**
  - Hostname: **esa.Kbits.live**
  - Accept Incoming E-Mail: **Checked**
    - Domain: **Kbits.live**
    - Destination: **192.168.100.99**

ESA

1. Browse to **192.168.101.25**.

2. Log in using the default username & Password of **admin/ironport**.

3. Browse to "**System Administration -> System Setup -> System Setup**

Wizard".

4. Configure the parameters in the wizard based on the parameters provided above:

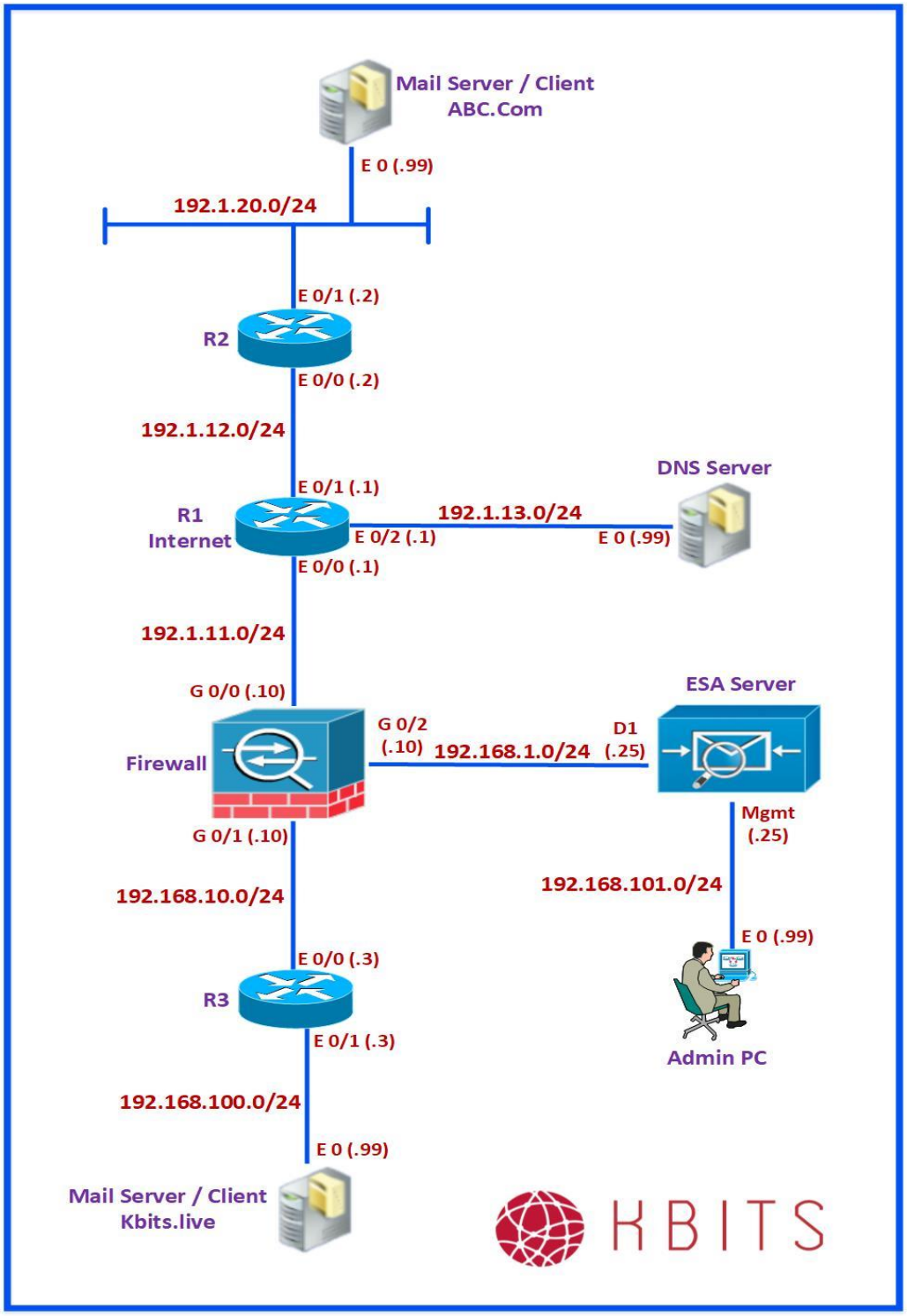
5. Take default values for values not provided.

6. Click "**Install this Configuration**".

7. Click "**Install**".

8. Click "**Cancel**" to cancel the Wizard and complete the setup wizard.

Lab 4 – Configuring E-mail Communication using ESA as SMTP Relay Agent



Lab Scenario:

- Configuring ESA to Relay Messages on behalf of the Kbits.live Mail Server located at 192.168.100.99.
- Configure the DNS MX Record for Kbits.live to use ESA as the SMTP Server.
- Re-Configure the ASA ACL to allow SMTP traffic towards the ESA
- Verify the configuration use the Tail – Mail Logs.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure a Mail Flow Policy for Relaying messages on the ESA using the following parameters:

- Mail Flow Policy
  - Policy Name: **RELAYED**
  - Connection behavior: **Relay**
  - Remaing Parameters: **Use Default**

ESA

1. Browse to **192.168.101.25**.

2. Log in using the default username & Password of **admin/ironport**.

3. Browse to "**Mail Policies -> Host Access Table (HAT) -> Mail Flow Policies -> Add Policy**".

4. Configure the Mail Flow Policy based on the parameters provided above.

5. Click "**Submit**".

6. Commit the changes by clicking the "**Commit Changes**" button.

Task 2

Configure a Sender Group to use the Mail Flow Policy created in the previous task for the Mail Server for Kbits.live:

- HAT
  - Policy Name: **RELAY LIST**
  - Order: **1**
  - Policy: **RELAYED**
  - Send Group: **RELAYED**

Admin PC

1. Browse to "**Mail Policies -> Host Access Table (HAT) -> HAT Overview -> Add Sender Group**".

2. Configure the Sender Group based on the parameters provided above.

3. Click "**Submit & Add Senders**".

4. Configure the Sender IP as "**192.168.100.99**" and click **Submit**.

5. Commit the changes by clicking the "**Commit Changes**" button.

Task 3

Translate the Kbits.live ESA located at 192.168.1.25 as 192.1.11.30 on the Outside. Allow SMTP Access to this server from Outside. Remove the previous ACL entry allowing access to the Kbits.live Mail Server. Also, create an ACL to allow the ESA communication to the Kbits.Live Mail Server. Apply this ACL to the ESA Interface.

ASA

```
Object network ESA
 Host 192.168.1.25
 Nat (DMZ,Outside) static 192.1.11.30
!
access-list OUTSIDE permit tcp any host 192.168.1.25 eq 25
No access-list OUTSIDE permit tcp any host 192.168.100.99 eq 25
!
Access-list DMZ permit ip host 192.168.1.25 any
Access-group DMZ in interface DMZ
```

Task 4

Configure an "A" Record for the ESA in ABC.com & Kbits.live based on the following:

- Domain: **Kbits.live**
  - Record Type: **A Record**
  - Record Name: **smtp**
  - FQDN: **smtp.kbits.live**
  - IP Address: **192.1.11.30**

DNS

1. RDP into the DNS Server using **administrator/Test123** as the username/password combination.

2. Open **Server Manager** and navigate to "**Server Manager -> Roles -> DNS Server -> DNS -> SRV -> Kbits.live**".

3. Right-Click to create "**New Host (A or AAAA)**".

4. Create Host (A) Record for the ESA for Kbits.live based on the above parameters.

Task 5

Configure the DNS Records MX Record for Kbits.live pointing to the ESA based created in the previous task.

DNS

1. Navigate to "**Server Manager -> Roles -> DNS Server -> DNS -> SRV -> Forward Lookup Zones -> Kbits.live"**

2. Re-configure the existing MX record.

3. Browse to the ESA for the FQDN and Click **Apply**.

Task 6

Configure Kbits.live Mail Server to use the ESA as the SMTP Relay Agent.

Kbits.live Mail Server

1. Open **hMail Administrator** on the **Kbits.live Server**.

2. Click "**Connect**" and specify the password as **Kbits@123**.

3. Click "**Settings -> Protocols -> SMTP -> Delivery of e-mail**".

4. Specify the SMTP Relayer as **192.168.1.25**.

5. Click **Save**.

Task 7

Open the ESA SSH Console. Type "**Tail**" on the command promot. Type **19** to start the log/debug for Mail messages.

Task 8

Open the Command Prompt on the ABC.com, Kbits.live and DNS Servrs. Type "**ipconfig /flushdns**". This will clear any older DNS entries.

Task 9

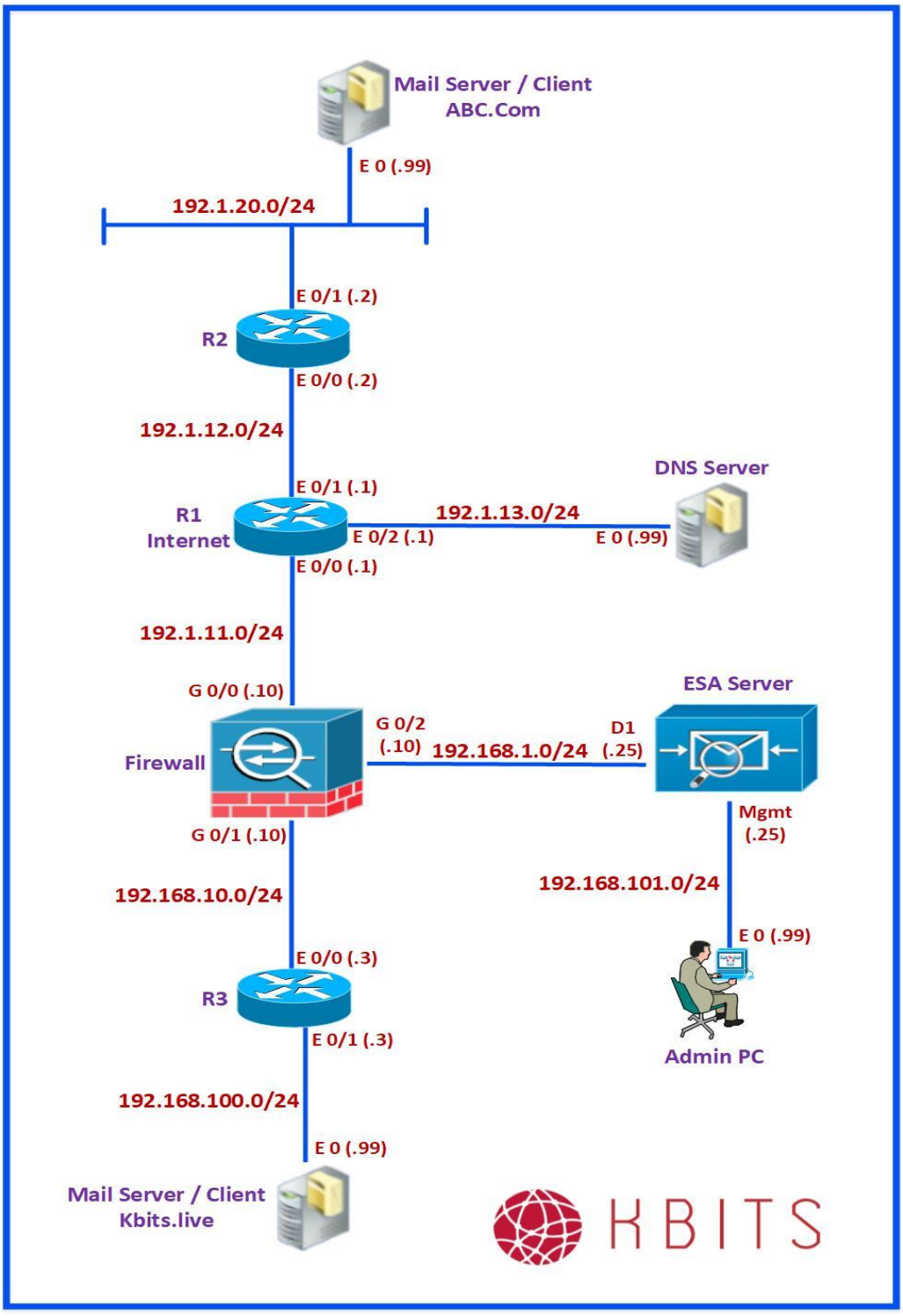
Verify the E-mail configuration by sending and receiving E-mail between the Users on the 2 domains. Also, check the logs on the ESA console to make sure the messages are getting forward thru the ESA.

CCIE Security v6 – E-Mail Security Applicance (ESA)

Module 2 – Configuring Incoming Filters Using ESA

Module 2 – Configuring Incoming Filters Using ESA

Lab 1 – Configuring Incoming Filter – Blocking E-Mails with Strings



Lab Scenario:

- Configure an Incoming Filter that blocks E-Mails with specified String

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure an Incoming Content Filter that blocks E-Mails based on the following parameters:

- Incoming Content Filter Name: **IC-BOMB**
  - Condition:
    - Message Body containg "**BOMB**"
  - Action:
    - **Drop**

ESA

1. Browse to **192.168.101.25**.

2. Log in using the default username & Password of **admin/ironport**.

3. Browse to "**Mail Policies -> Incoming Content Filter -> Add Filter".**

4. Configure the Incoming Content Filter based on the parameters provided above.

5. Click "**Submit**".

6. Commit the changes by clicking the "**Commit Changes**" button.

Task 2

Configure an Incoming Mail Policy that uses the Filter created in the previous task to block All E-Mails.

- Incoming Mail Policy Name: **IC-Mail-Policy**
  - Users:
    - Sender: **Any**
    - Recipient: **Any**
  - Content Filters:
    - **IC-BOMB**

ESA

1. Browse to "**Mail Policies -> Incoming Mail Policies -> Add Policy".**
2. Configure the Incoming Mail Policy based on the parameters provided above.
3. Click "**Submit**".
4. Commit the changes by clicking the "**Commit Changes**" button.

Task 3

Open the ESA SSH Console. Type "**Tail**" on the command promot. Type **19** to start the log/debug for Mail messages.

Task 4

Verify the filter by sending an e-mail from Abc1@abc.com to kbits1@kbits.live using the following:

- From: **Abc1@abc.com**
- To: **kbits1@kbits.live**
- Subject: **BOOOOOOOOOOOOMB**
- Message Body:

  Hello Kbits One,

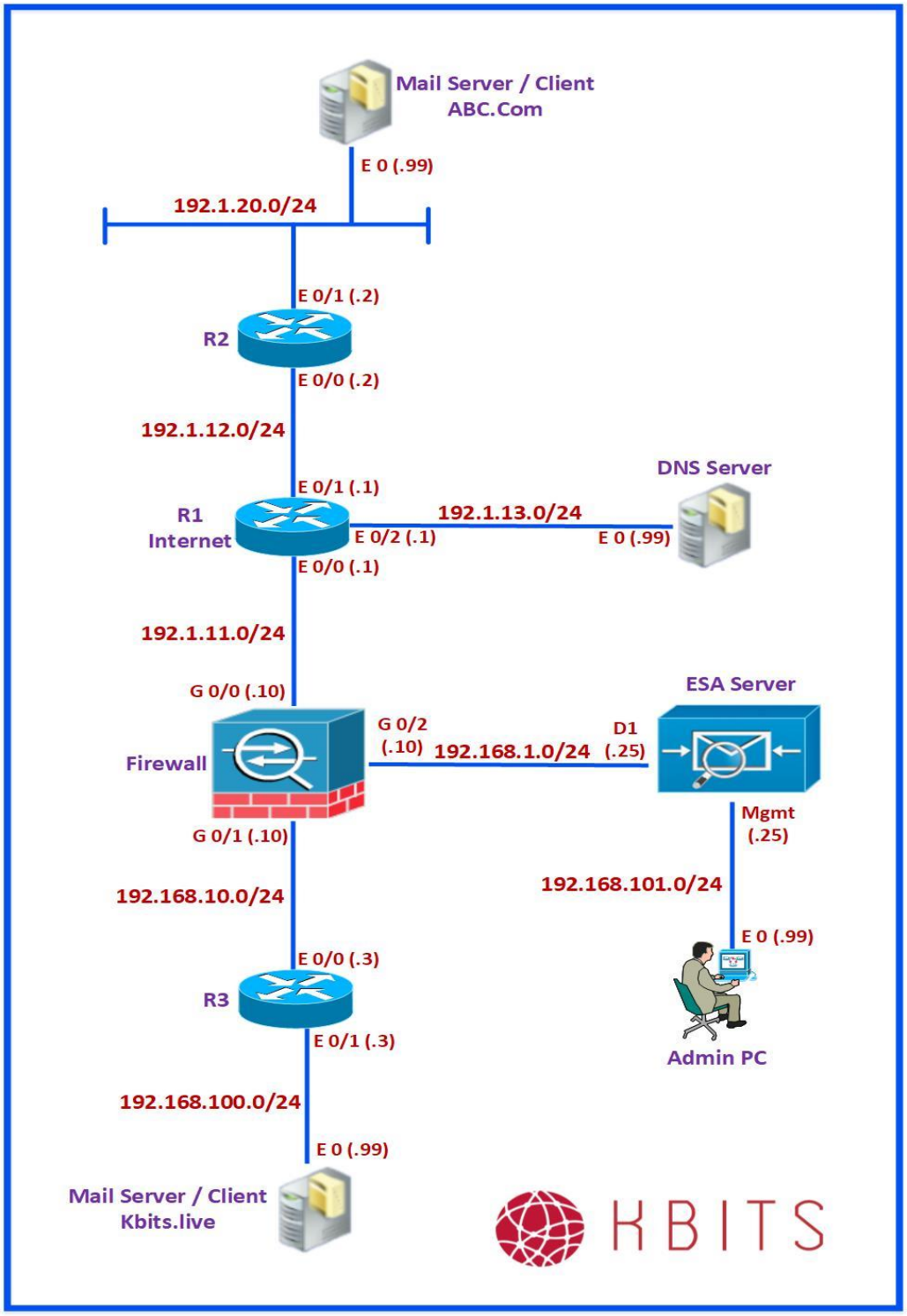
  BOMB is diffused.

  Regards
  ABC One

Task 5

Verify that the message is getting dropped by the Filter.

Lab 2 – Configuring Incoming Filter – Blocking E-Mails based on Message Size



Lab Scenario:

- Configure an Incoming Filter that strip attachments exceeding a specificied size.

Initial Setup:

- **Based on the previous Lab**

Task 1

Configure an Incoming Content Filter that blocks E-Mails based on the following parameters:

- Incoming Content Filter Name: **IC-File-Size**
  - Condition:
    - Message Size: greater than: "**3000000**"
  - Action:
    - Strip Attachment by File Info: File Size >: "**3000000**"
    - Replacement Message: **Attachment Dropped. Exceeded the Company Policy for Message Size!!!!!**

ESA

1. Browse to "**Mail Policies -> Incoming Content Filter -> Add Filter".**

2. Configure the Incoming Content Filter based on the parameters provided above.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 2
Edit the **IC-Mail-Policy** Filter to include the **IC-File-Size** Content Filter created in the previous task.

ESA

1. Browse to "**Mail Policies -> Incoming Mail Policies -> IC-Mail-Policy".**

2. Click the checkbox to select the **IC-File-Size** Filter.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 3
Open the ESA SSH Console. Type "**Tail**" on the command promot. Type **19** to start the log/debug for Mail messages.

Task 4
Verify the filter by sending an e-mail from Abc2@abc.com to kbits2@kbits.live using the following:

- From: **Abc2@abc.com**
- To: **kbits2@kbits.live**
- Subject: **Mail Server**
- Attachment: **Any File greater than 3 MB (HmailServer.exe)**
- Message Body:
  Hi Kbits Two,

  I have attached the Hmail Server file you had requested.

  Abc Two

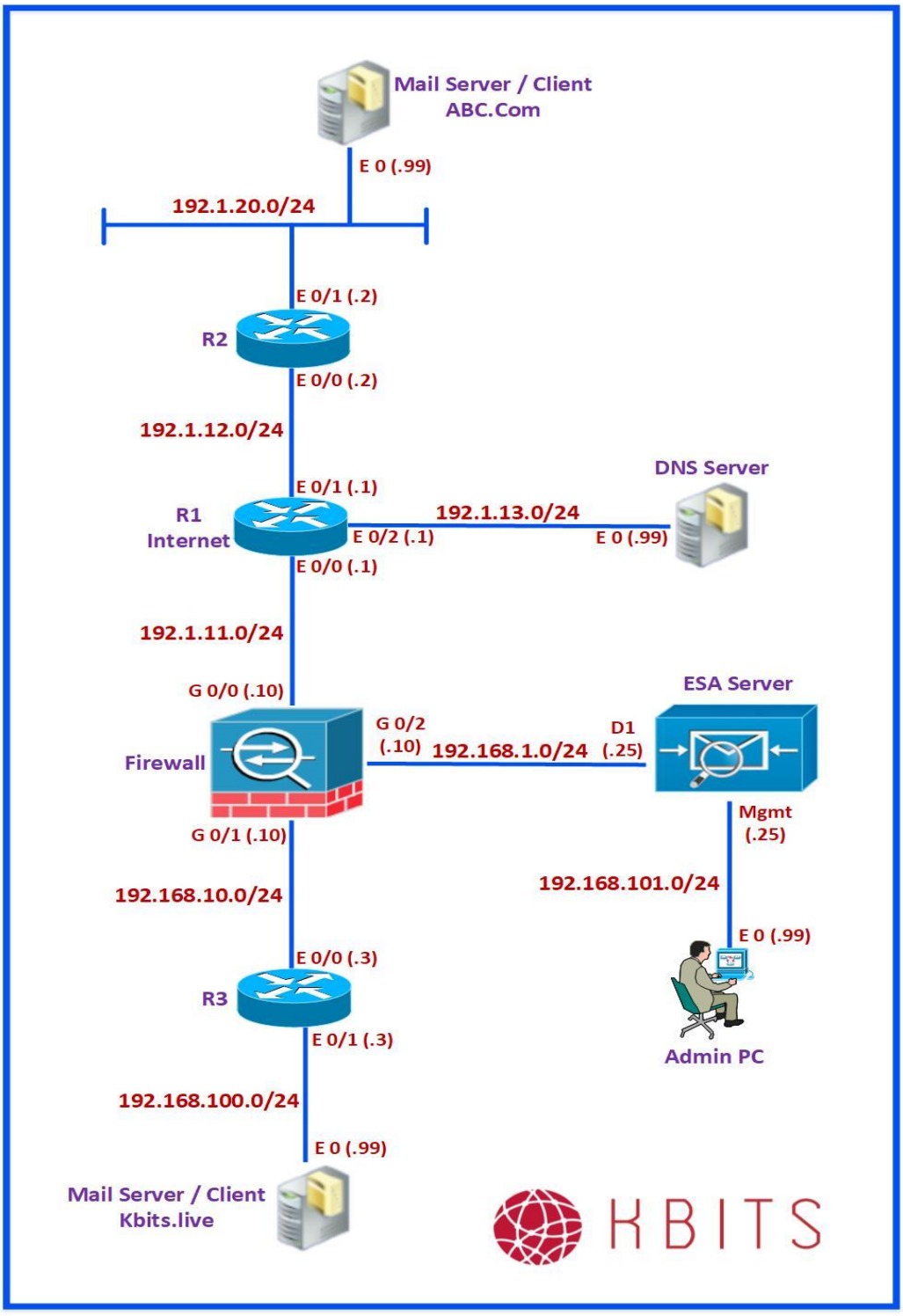
Task 5
Verify that the ESA is stripping the File and inserting the replacement message.

CCIE Security v6 – E-Mail Security Applicance (ESA)

Module 3 – Configuring Outgoing Filters Using ESA

Module 3 – Configuring Outgoing Filters Using ESA

Lab 1 – Configuring Outgoing Filters – Block E-Mails with Smart Filters



Lab Scenario:

- Configure an Outgoing Filter that blocks E-Mails with SSN with a notification to the Sender.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure a Text Resource that will be used for Notifications in Content Filters based on the following:

- Text Resource Name: **SSN-Notification**
- Type: **Notification Template**
- Type: **Notification Template**
- Text: "**SSN should not be sent in an e-mail**"

ESA

1. Browse to **192.168.101.25**.
2. Log in using the default username & Password of **admin/ironport**.
3. Browse to "**Mail Policies -> Text Resources -> Add Text Resource".**
4. Configure the Text Resource based on the parameters provided above.
5. Click "**Submit**".
6. Commit the changes by clicking the "**Commit Changes**" button.

Task 2

Configure an Outgoing Content Filter that blocks E-Mails based on the following parameters:

- Outgoing Content Filter Name: **OG-SSN**
  - Condition:
    - Message Body contains "**Contains smart identifier**": "**SSN**"
  - Action:
    - **Notify:** Report the Message to the "**Sender**" with the "**SSN-Notifcation**" text message created in the previous task.
    - **Drop**

ESA

1. Browse to "**Mail Policies -> Outgoing Content Filter -> Add Filter".**

2. Configure the Outgoing Content Filter based on the parameters provided above.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 3

Configure an Outgoingt Mail Policy that uses the Filter created in the previous task to block All E-Mails.

- Incoming Mail Policy Name: **OG-Mail-Policy**
  - Users:
    - Sender: **Any**
    - Recipient: **Any**
  - Content Filters:
    - **OG-SSN**

ESA

1. Browse to "**Mail Policies -> Outgoing Mail Policies -> Add Policy".**

2. Configure the Outgoing Mail Policy based on the parameters provided above.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 4

Open the ESA SSH Console. Type "**Tail**" on the command promot. Type **19** to start the log/debug for Mail messages.

Task 5

Verify the filter by sending an e-mail from kbits2@kbits.live to Abc2@abc.com using the following:

- From: **kbits2@kbits.live**
- To: **Abc2@abc.com**
- Subject: **Application Processing**
- Message Body:
-

  Hi Abc Two,

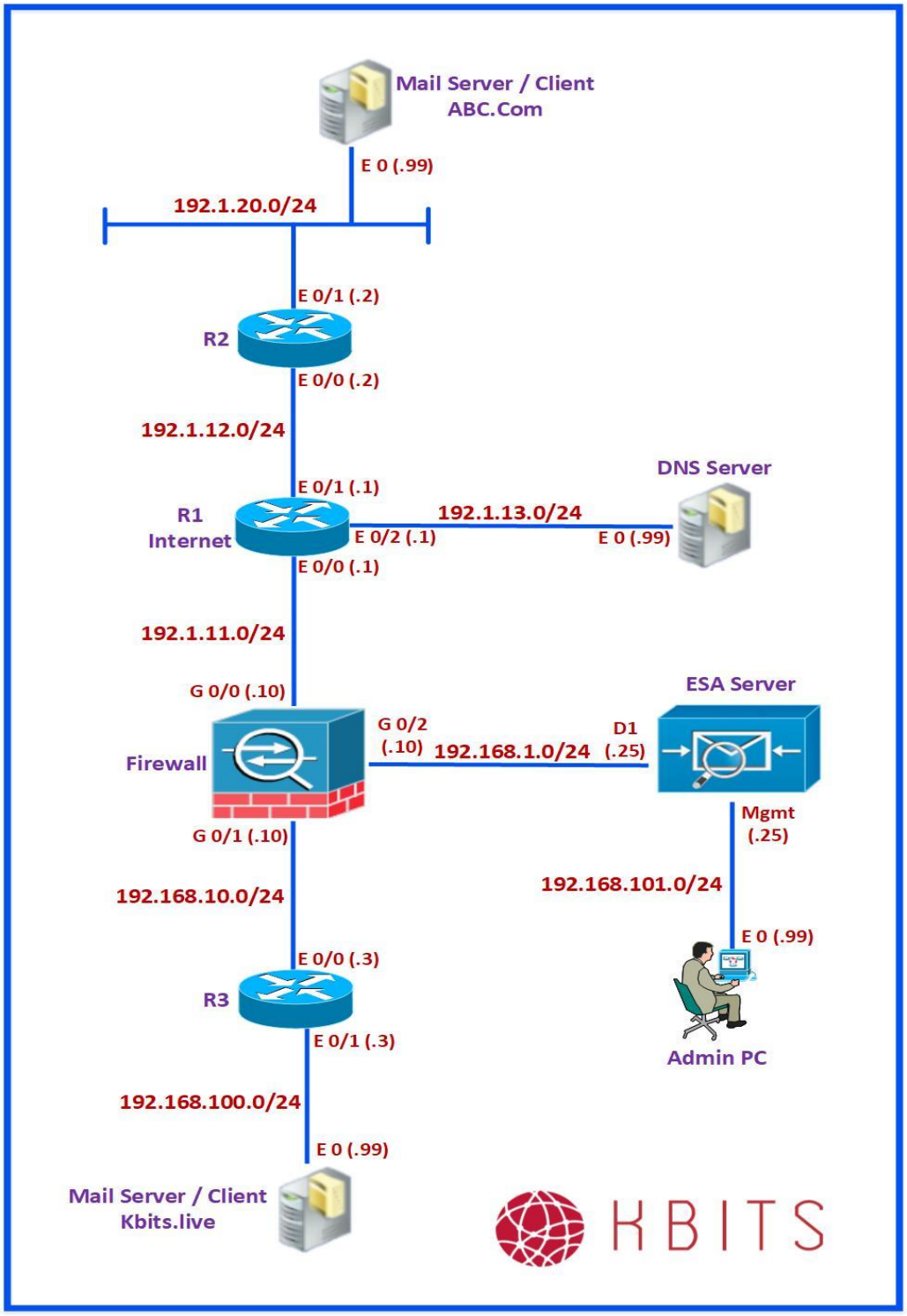
  My SSN is: 615-56-1234. Please process the application.

  Kbits Two

Task 6

Verify that the message is getting dropped by the Filter and Sender is getting an e-mail with Notification Text.

Lab 2 – Configuring Outgoing Filters – Block E-mails based on File Types



Lab Scenario:

- Configure an Incoming Filter that strip attachments exceeding a specificied size.

Initial Setup:

- **Based on the previous Lab**

Task 1

Configure an Outgoing Content Filter that blocks E-Mails based on the following parameters:

- Outgoing Content Filter Name: **OG-File-Type**
  - Condition:
    - File Type is : "**-- exe**"
  - Action:
    - **Drop**

ESA

1. Browse to "**Mail Policies -> Outgoing Content Filter -> Add Filter".**

2. Configure the Outgoing Content Filter based on the parameters provided above.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 2

Edit the **OG-Mail-Policy** Filter to include the **OG-File-Type** Content Filter created in the previous task.

ESA

1. Browse to "**Mail Policies -> Outgoing Mail Policies -> OG-Mail-Policy".**

2. Click the checkbox to select the **OG-File-Type** Filter.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 3

Open the ESA SSH Console. Type "**Tail**" on the command promot. Type **19** to start the log/debug for Mail messages.

Task 4

Verify the filter by sending an e-mail from kbits1@kbits.live to Abc1@abc.com using the following:

- From: **kbits1@kbits.live**
- To: **Abc1@abc.com**
- Subject: **TFTP Server Attached**
- Message Body:
- Attachment: **Any Exe file (tftpd64.exe)**

  Hi Abc One,

  I have attached the TFTP Server File that you had requested.

  Kbits One

Task 5

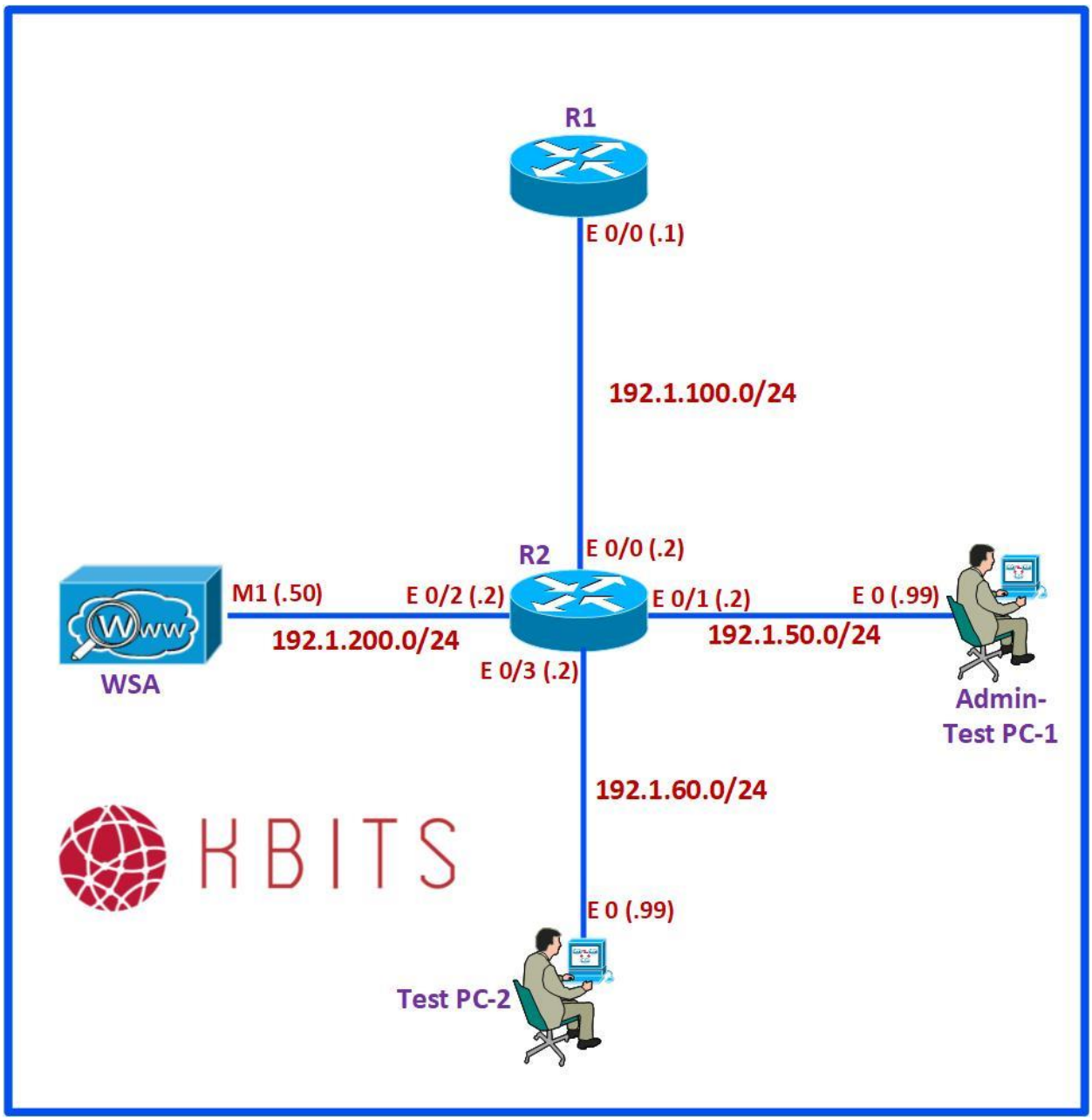
Verify that the message is getting dropped by the Filter.

CCIE Security v6 – Web Security Applicance (WSA)

Module 1 – Initial Configuration of the WSA

Module 1 – Initial Configuration of the WSA

Lab 1 – Basic Network Setup for Web Access



Lab Scenario:

- Configuring the Base Network for Web Communications

Initial Setup:

- Not required.

Lab Tasks:

Task 1

Configure R1 & R2 IP Addresses based on the network diagram. Configure a Default Route on R2 pointing towards R1. Configure a static route on R1 for the 192.1.50.0/24, 192.1.60.0/24 & 192.1.200.0/24 networks using R2 as the next hop.

R1

```
interface Ethernet0/0
 ip address 192.1.12.1 255.255.255.0
 no shut
!
Ip route 192.1.50.0 255.255.255.0 192.1.100.2
Ip route 192.1.60.0 255.255.255.0 192.1.100.2
Ip route 192.1.200.0 255.255.255.0 192.1.100.2
```

R2

```
interface Ethernet0/0
 ip address 192.1.100.2 255.255.255.0
 no shut
!
interface Ethernet0/1
 ip address 192.1.50.2 255.255.255.0
 no shut
!
interface Ethernet0/2
 ip address 192.1.200.2 255.255.255.0
 no shut
!
interface Ethernet0/3
 ip address 192.1.60.2 255.255.255.0
 no shut
```

```
!
Ip route 0.0.0.0 0.0.0.0 192.1.100.1
```

Task 2

Configure R1 as a Web Server. Configure it with an enable secret password of Cisco123. Configure a Loopback Interface (Loopback1) with an IP Address of 1.1.1.1/8.

R1

```
Ip http server
!
enable secret Cisco123
!
Interface Loopback1
 Ip address 1.1.1.1 255.0.0.0
```

Task 3

Configure R2 as a DNS Server. Configure the following mappings:

- www.espn.com - 192.1.100.1
- www.cnn.com - 192.1.100.1
- www.gamble.com - 192.1.100.1
- www.xxx.com - 192.1.100.1
- www.kbits.live - 192.1.100.1
- www.cisco.com - 192.1.100.1

R2

```
Ip dns server
!
ip host www.espn.com 192.1.100.1
ip host www.cnn.com 192.1.100.1
ip host www.gamble.com 192.1.100.1
ip host www.xxx.com 192.1.100.1
ip host www.kbits.live 192.1.100.1
ip host www.cisco.com 192.1.100.1
```

Task 4

Verify that the Admin/Test-PC-1 & Test-PC-2 are configured with the following Network Configurations:

Admin-PC/Test-PC-1

- IP Address: **192.1.50.99**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.1.50.2**
- DNS Server: **192.1.50.2**

Test-PC-2

- IP Address: **192.1.60.99**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.1.60.2**
- DNS Server: **192.1.60.2**

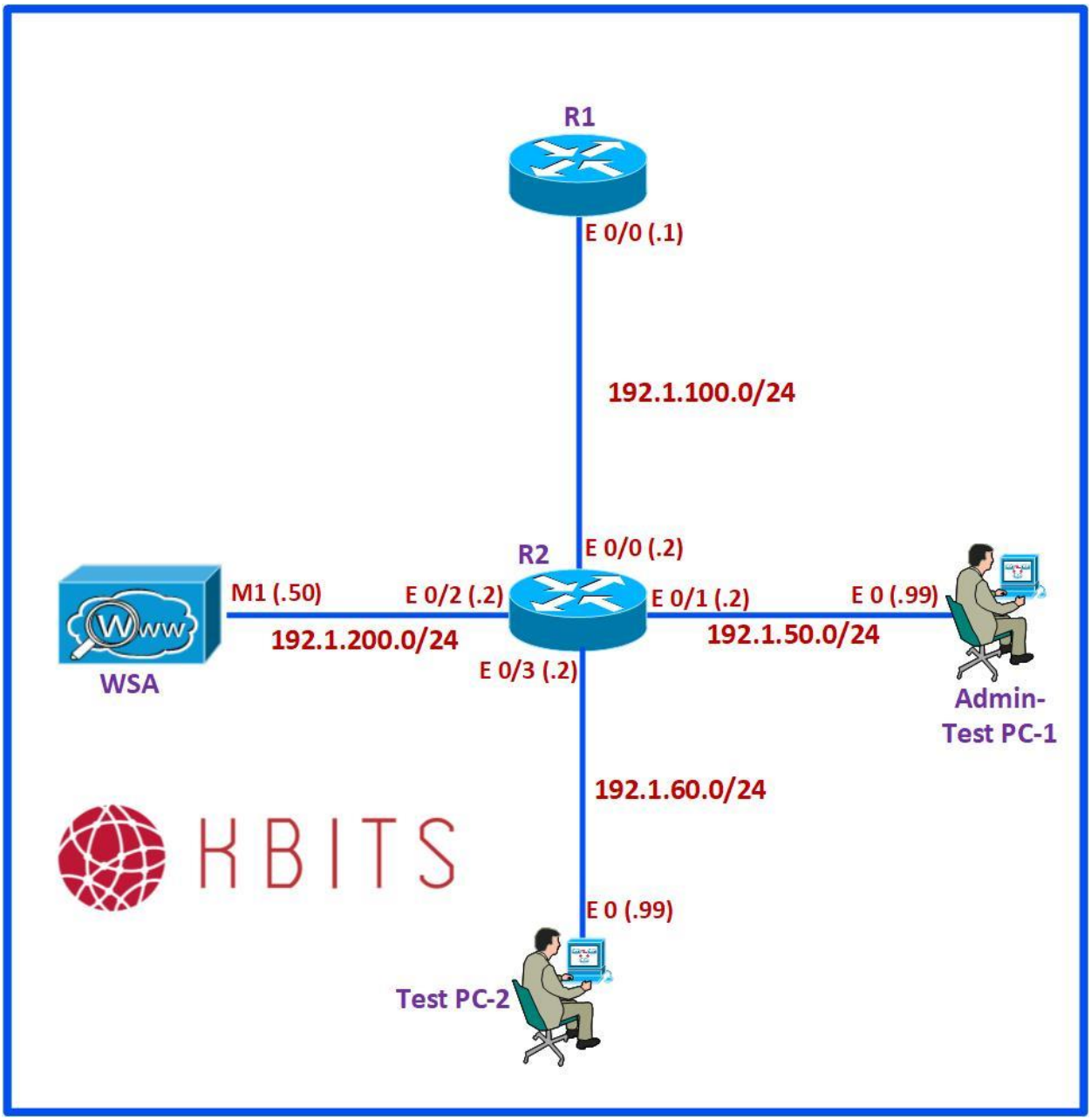
Task 5

Verify you can browse to some of the above websites from both the PC's/

Task 6

Verify the Remote IP's accessing the Web Server on R1 using "**Show ip http server history**" command. The Remote-IP should be **192.1.50.99 and/or 192.1.60.99**.

Lab 2 – Initializing the WSA Appliance from CLI



Lab Scenario:

- Initialize the WSA from the Command Line.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Initialize the WSA from the CLI using the following parameters:

- Management Interface configuration:
  - IP Address: **192.1.200.50/24**
  - Default Gateway: **192.1.200.2**
  - Hostname: **WSA.KBITS.LIVE**
  - Protocols: **SSH, HTTP & HTTPS**
- Rest of the Parameters: **Default**

WSA

1. Log into ESA from the CLI Using the default Username and password (**admin/ironport**).

2. Type **interfaceconfig** and following the prompts:

Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: ironport.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]> **edit**

Enter the number of the interface you wish to edit.
[]> **1**

Would you like to configure an IPv4 address for this interface (y/n)? [Y]> y

IPv4 Address (Ex: 192.168.1.2):
[192.168.42.42]> **192.1.200.50**

Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> **255.255.255.0**

Would you like to configure an IPv6 address for this interface (y/n)? [N]> **n**

Hostname:
[ironport.example.com]> **wsa.kbits.live**

Do you want to enable FTP on this interface? [N]> **n**

Do you want to enable SSH on this interface? [Y]> **y**

Which port do you want to use for SSH?
[22]> **22**

Do you want to enable HTTP on this interface? [Y]> **Y**

Which port do you want to use for HTTP?
[8080]> **8080**

Do you want to enable HTTPS on this interface? [Y]> **Y**

Which port do you want to use for HTTPS?
[8443]> **8443**

You have not entered an HTTPS certificate. To assure privacy, run "certconfig" first. You may use the demo, but this will not be secure.
Do you really wish to use a demo certificate? [Y]> **y**

Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the secure service? [Y]> **y**

Currently configured interfaces:
1. Management (192.1.200.50/24 on Management: wsa.kbits.live)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.

[]> **[Enter]**

Please run System Setup Wizard at http://192.1.200.50:8080
ironport.example.com> **commit**

Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.

Warning: Processing of network configuration changes might
cause a brief interruption in network availability.

Please enter some comments describing your changes:
[]> **[Enter]**

Changes committed: Tue Oct 20 23:40:02 2020 GMT
Please run System Setup Wizard at http://192.1.200.50:8080
ironport.example.com> **setgateway**

Warning: setting an incorrect default gateway may cause the current
connection to be interrupted when the changes are committed.
Set the default gateway for:
1. IPv4
2. IPv6
[1]> **1**

Enter new default gateway:
[]> **192.1.200.2**

Please run System Setup Wizard at http://192.1.200.50:8080
ironport.example.com> **commit**

Please enter some comments describing your changes:
[]>

Changes committed: Tue Oct 20 23:40:21 2020 GMT
Please run System Setup Wizard at http://192.1.200.50:8080

Task 2

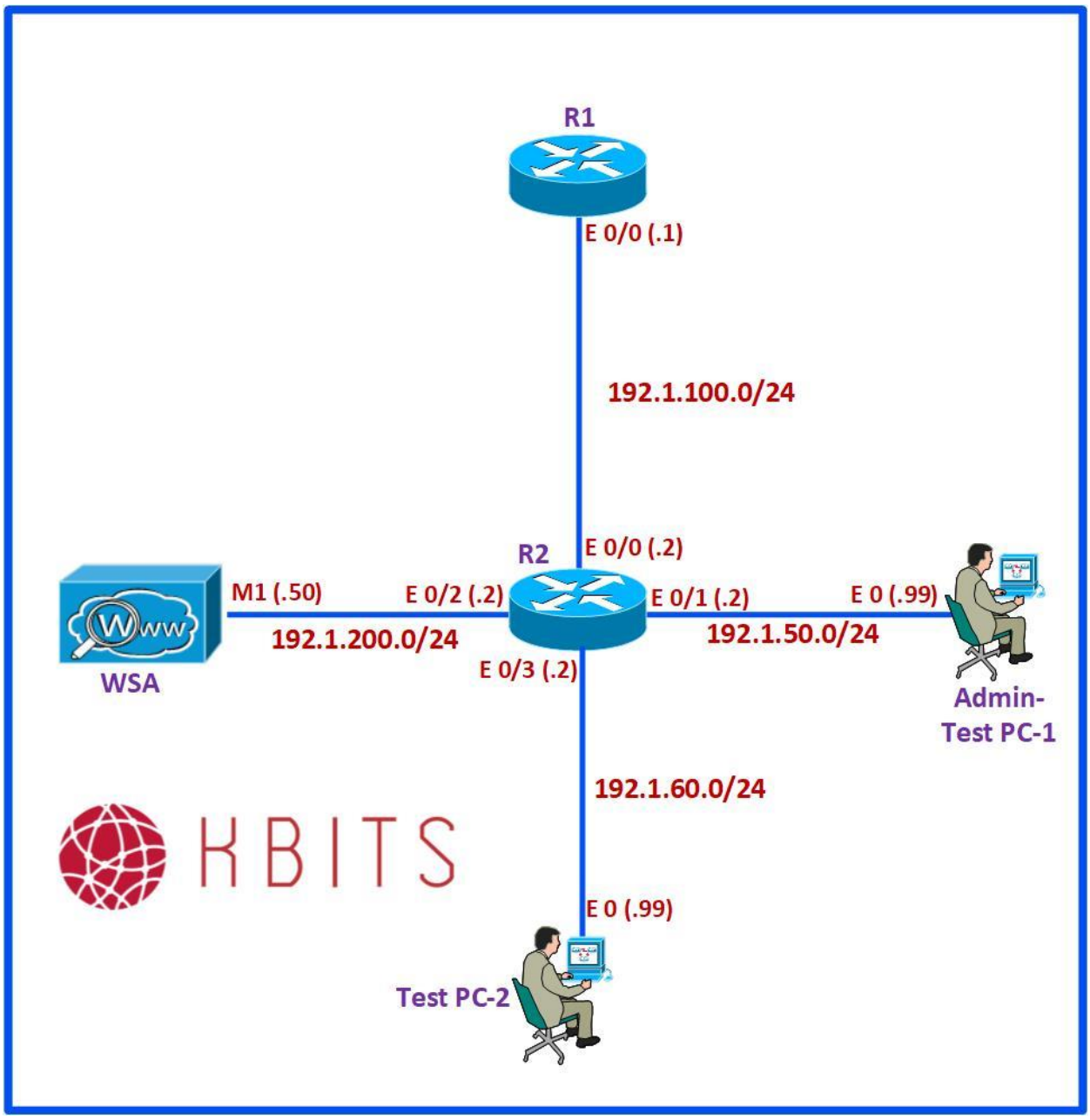
Verify Graphical access to the WSA.

Admin PC

1. Browse to **192.1.200.50:8080**

2. Log in using the default username & Password of **admin/ironport**.

Lab 3 – Initializing the WSA Appliance from GUI Using the System Setup Wizard



Lab Scenario:

- Initializing the WSA using the System Setup Wizard.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Run the System Wizard to finalize the initial setup. Verify/Re-configure the ESA Networking with the following Parameters:

- System Configuration:
  - System Name: **WSA.Kbits.live**
  - DNS Server: **192.1.200.2**
  - NTP Server: **Delete and leave it blank**

- Network Content:
  - Proxy Server: **No**

- Network Interfaces & Wiring:
  - M1 IP: **192.1.200.50/24**
  - M1 Hostname: **wsa.kbits.live**

- L4 Traffic Monitor:
  - **Take the default**

- IPv4 Routes for Management:
  - Default Gateway: **192.1.200.2**

- Transparent Connection Settings:
  - **Take the default**

- Administrative Settings:
  - Admin Password: **Kbits@123**
  - System Alerts E-mail: Khawarb@kbits.live
  - SMTP Server: **192.1.200.25**

- Security Settings:
  - **Take the defaults**

WSA

1. Browse to **http://192.1.200.50:8080**.

2. Log in using the default username & Password of **admin/ironport**.

3. Browse to "**System Administration -> System Setup -> System Setup Wizard**".

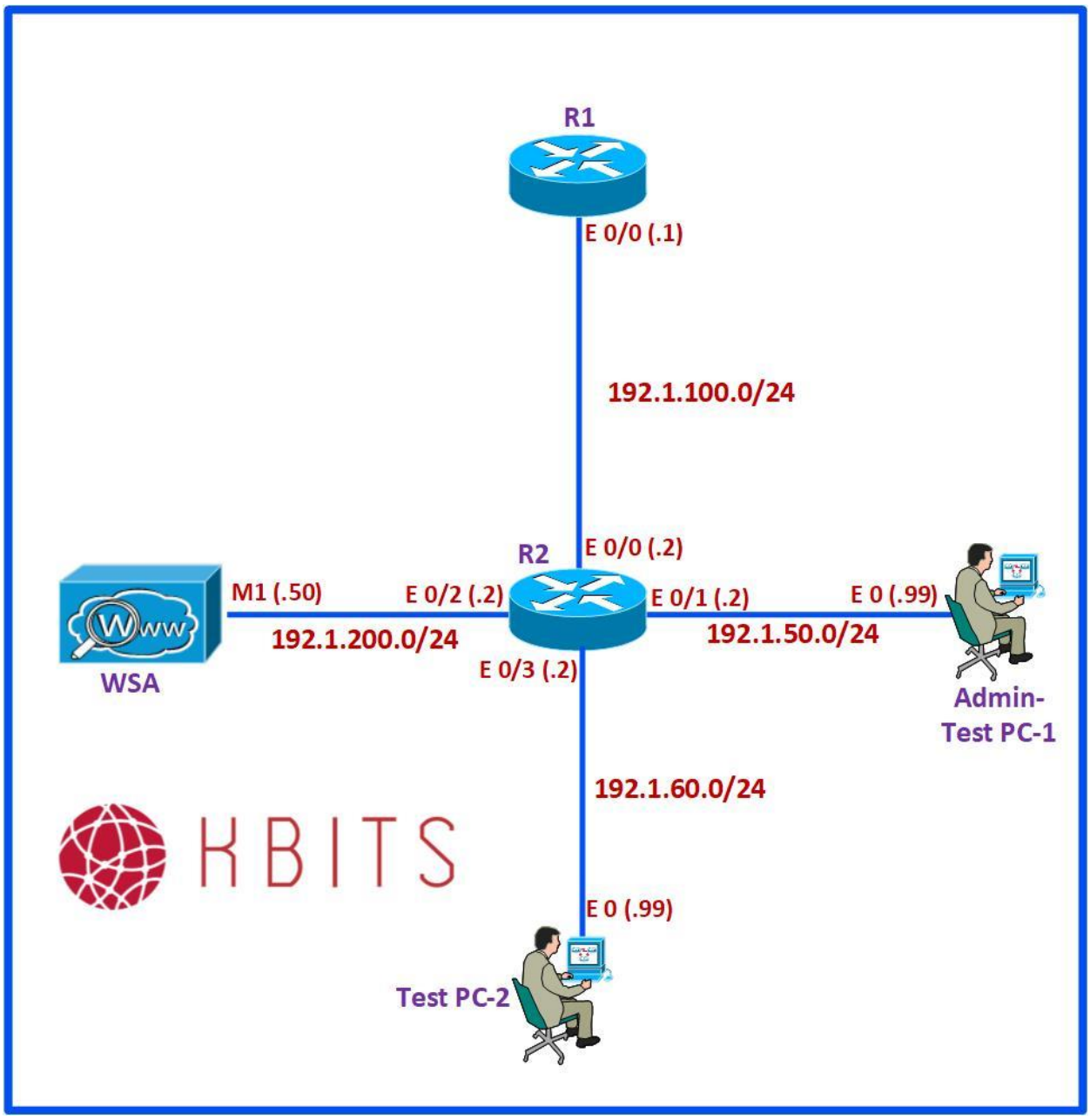
4. Configure the parameters in the wizard based on the parameters provided above:

5. Take default values for values not provided.

6. Click "**Install this Configuration**".

7. Browse to **http://192.1.200.50:8080** as you will loose the connection to the devices.

Lab 4 – Configuring the Router – WSA Relationship for WCCP



Lab Scenario:

- Configure WCCP on the WSA to establish the WCCP Relationship for transparent proxy.
- Configure WCCP on R2.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure WCCP Transparent Redirection on the WSA based on the following parameters:

- Service Profile Name: **R2**
- Dynamic Service ID: **55**
- Port Numbers: **80**
- Router IP Address: **192.1.200.2**
- Password: **cisco**

WSA

1. Browse to **https://192.1.200.50:8443.**

2. Log in using the default username & Password of **admin/Kbits@123**.

3. Browse to "**Network -> Transparent Redirection -> Edit Device -> WCCP Version 2 -> Submit -> Add Service**".

4. Configure Transparent redirection based on the above parameters.

5. Click "**Submit**".

6. Commit the changes by clicking the "**Commit Changes**" button.

Task 2

Configure WCCP on R2 based on the following parameters:

- WCCP Version: **2**
- WSA IP Address: **192.1.200.2**
- Traffic flow ACL: permit tcp any any eq 80
- Dynamic Service ID: **55**
- Password: **cisco**
- Redirection Interfaces: **E 0/1 & E 0/3**

R2

```
ip wccp version 2
!
access-list 1 permit host 192.1.200.50
!
access-list 101 permit tcp any any eq 80
!
ip wccp 55 group-list 1 redirect-list 101 password cisco
!
Interface E 0/1
 ip wccp 55 redirect in
!
Interface E 0/3
 ip wccp 55 redirect in
```

Task 3

Verify the relationship between the WSA & the router by using the "**Show ip wccp 55 view**" command on R2. You should see the WSA IP, **192.1.200.50**, listed as an active client.

Task 4

Verify you can browse to www.cnn.com or www.espn.com from the Admin/Test-PC-1 or Test-PC-2.

Task 5

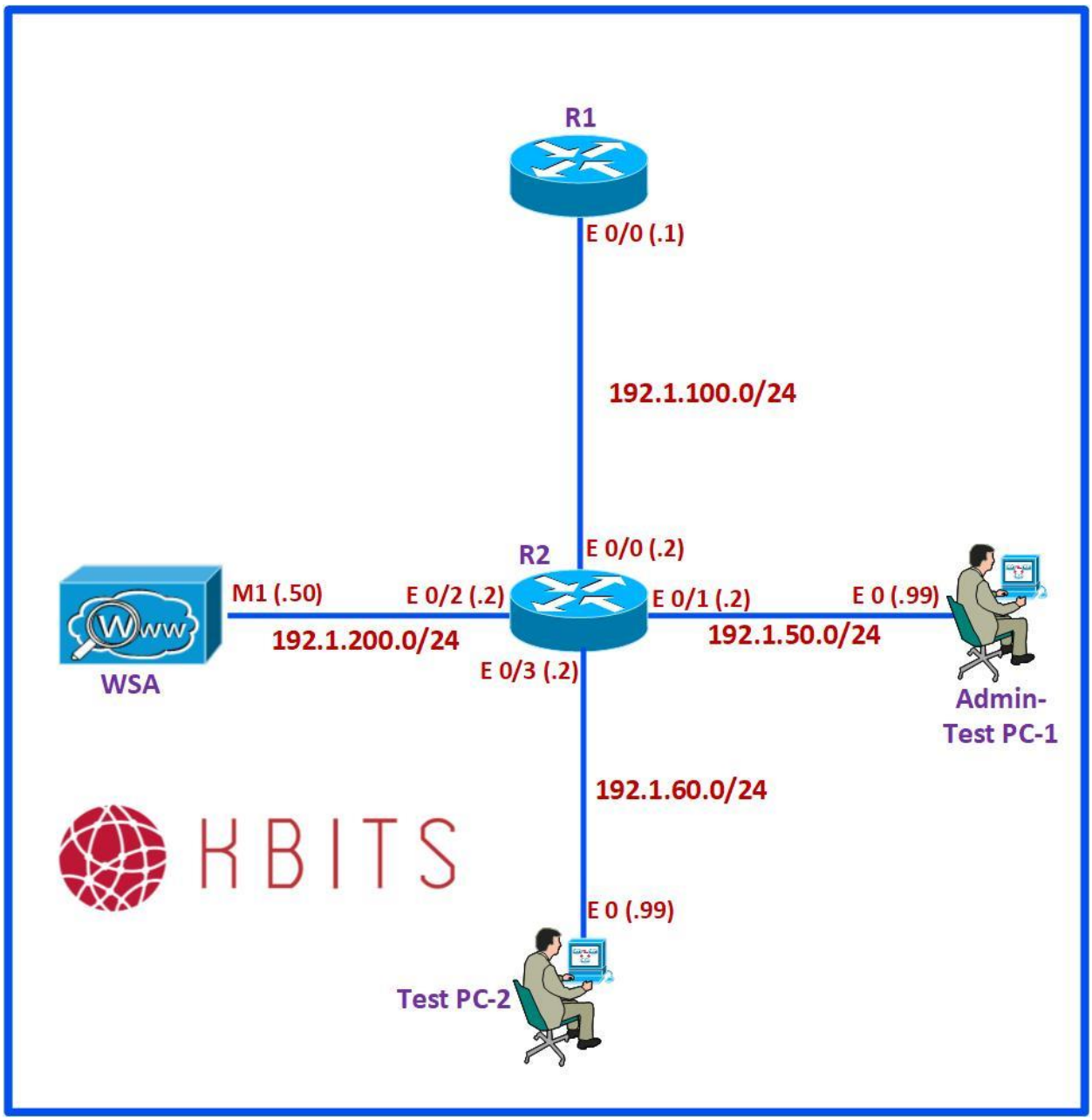
Verify the Client IP's accessing the Web Server on R1 using "**Show ip http server history**" command. The Clients IP should now be pointing towards **192.1.200.50**, the WSA IP.

CCIE Security v6 – Web Security Applicance (WSA)

Module 2 – Configuring Web Filtering Using WSA

Module 2 – Configuring Web Filtering Using WSA

Lab 1 – Creating Identities Used for Web Filtering



Lab Scenario:

- Creating the Identities for Web Filtering.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the following Identities on the WSA:

- Name: **Network 50** Subnet: **192.1.50.0/24**
- Name: **Network 60** Subnet: **192.1.60.0/24**
- Name: **Execs** Range: **192.1.50.91 – 192.1.50.100**

WSA

1. Browse to **https://192.1.200.50:8443.**

2. Log in using the default username & Password of **admin/Kbits@123**.

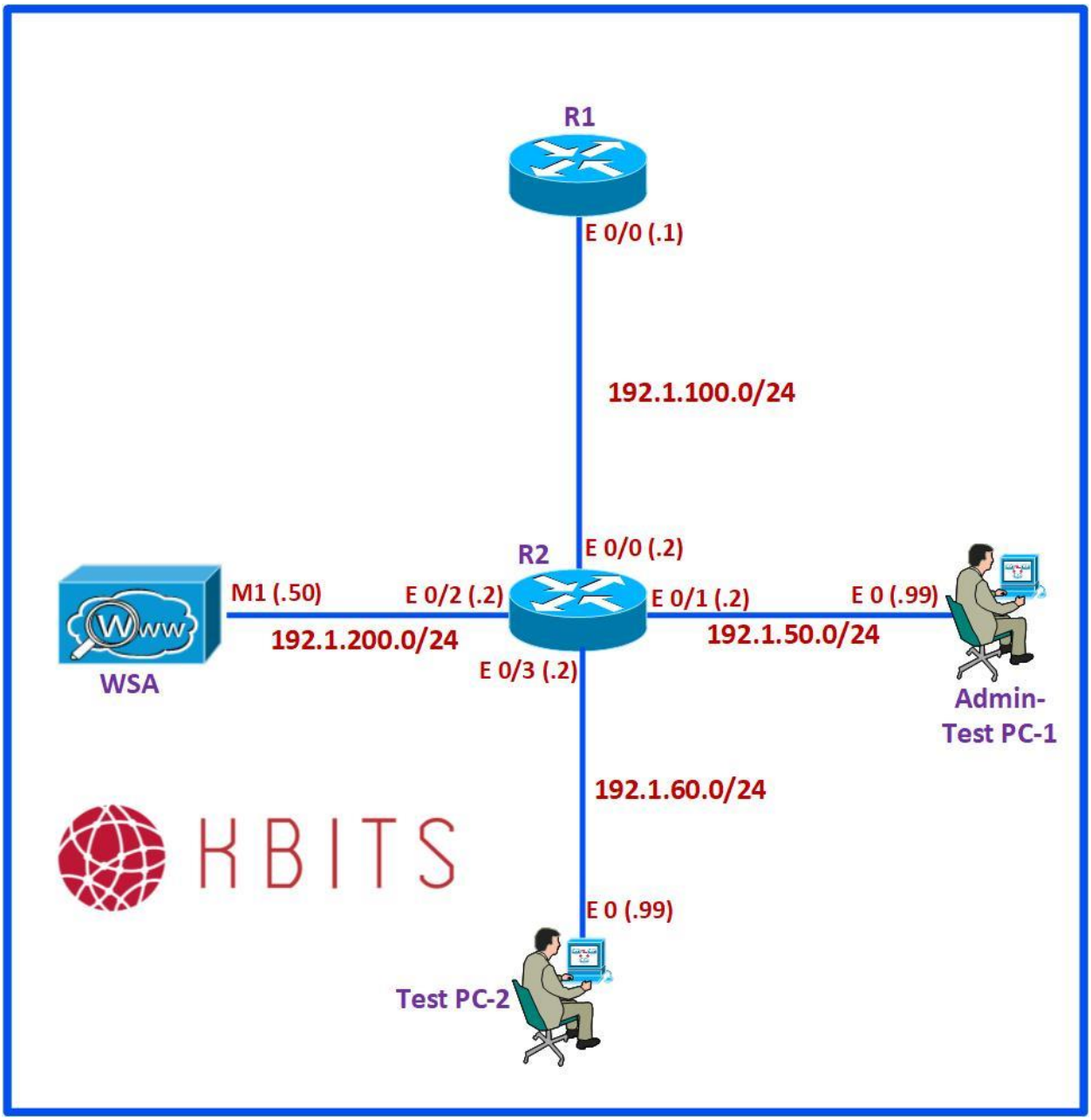
3. Browse to "**Web Security Manager -> Authentication -> Identification Profiles -> Add Identification Profiles**".

4. Create the Identities based on the above parameters.

5. Click "**Submit**".

6. Commit the changes by clicking the "**Commit Changes**" button.

Lab 2 – Category Based Blocking on the WSA



Lab Scenario:

- Blocking Websites based on Categories.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the Global Policy to filter the following websites categories:

- Adult
- Gambling
- Pornography
- Social Networking
- Sports & recreation

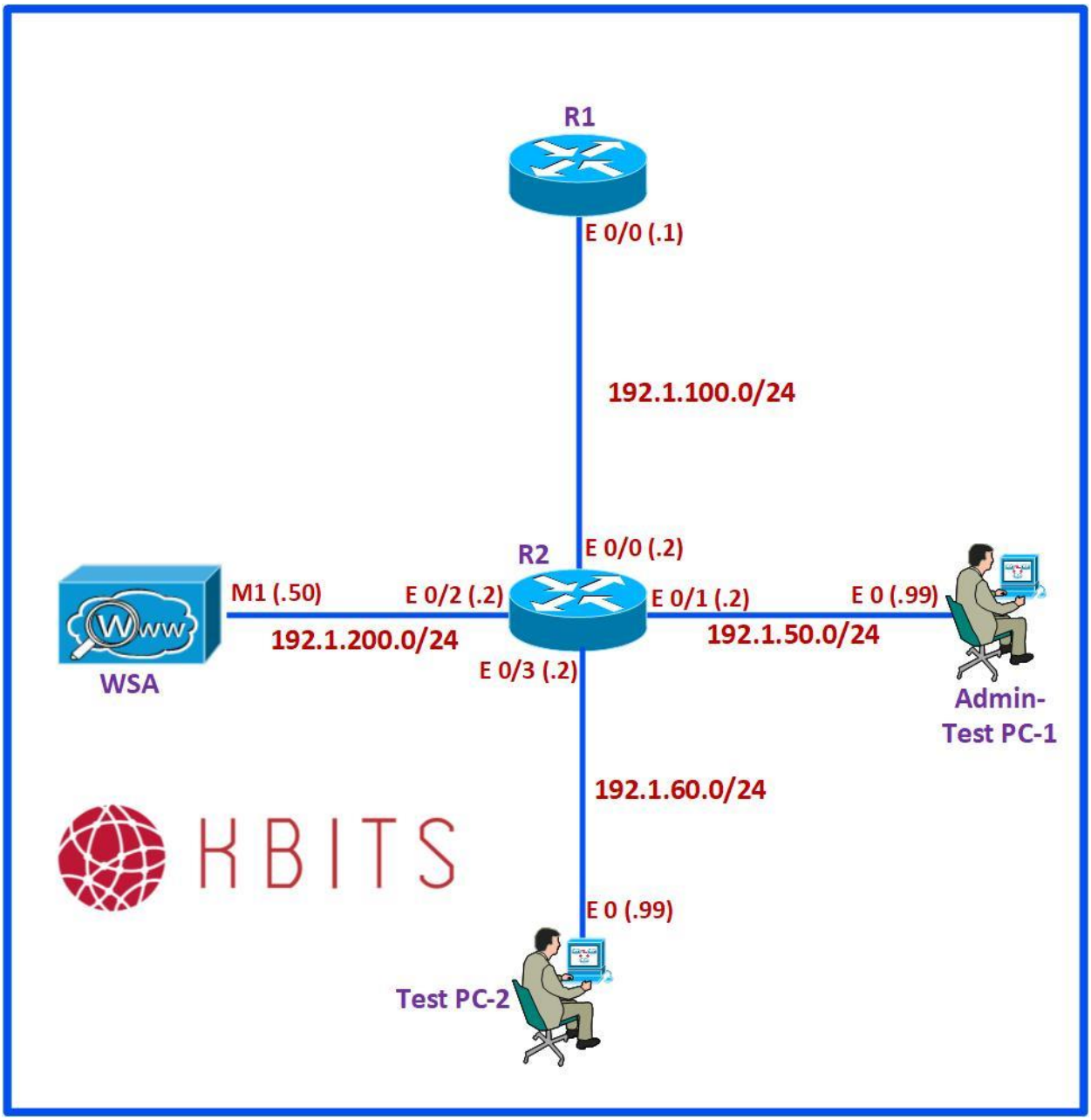
WSA

1. Browse to "**Web Security Manager -> Web Policies -> Access Policies**".
2. Create "**Monitor**"" under "**URL Filtering**" for the "**Global Policy**".
3. Block the Categories listed above.
4. Click "**Submit**".
5. Commit the changes by clicking the "**Commit Changes**" button.

Task 2

Verify you cannot browse to www.espn.com from the Admin/Test-PC-1 or Test-PC-2. You should still be able to browse to www.cnn.com.

Lab 3 – Configuring Identity Specific Policies



Lab Scenario:

- Configuring Web Access Policies for specific Identities.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure an Access Policy for the **Execs** Identity to filter the websites categories listed below. The name of the policy should be **Execs Policy**.

- Adult
- Gambling
- Pornography

WSA

1. Browse to "**Web Security Manager -> Web Policies -> Access Policies -> Add Policy**".

2. Create the Access Policy for **Execs** based on the list above.

3. Block the Categories listed above.

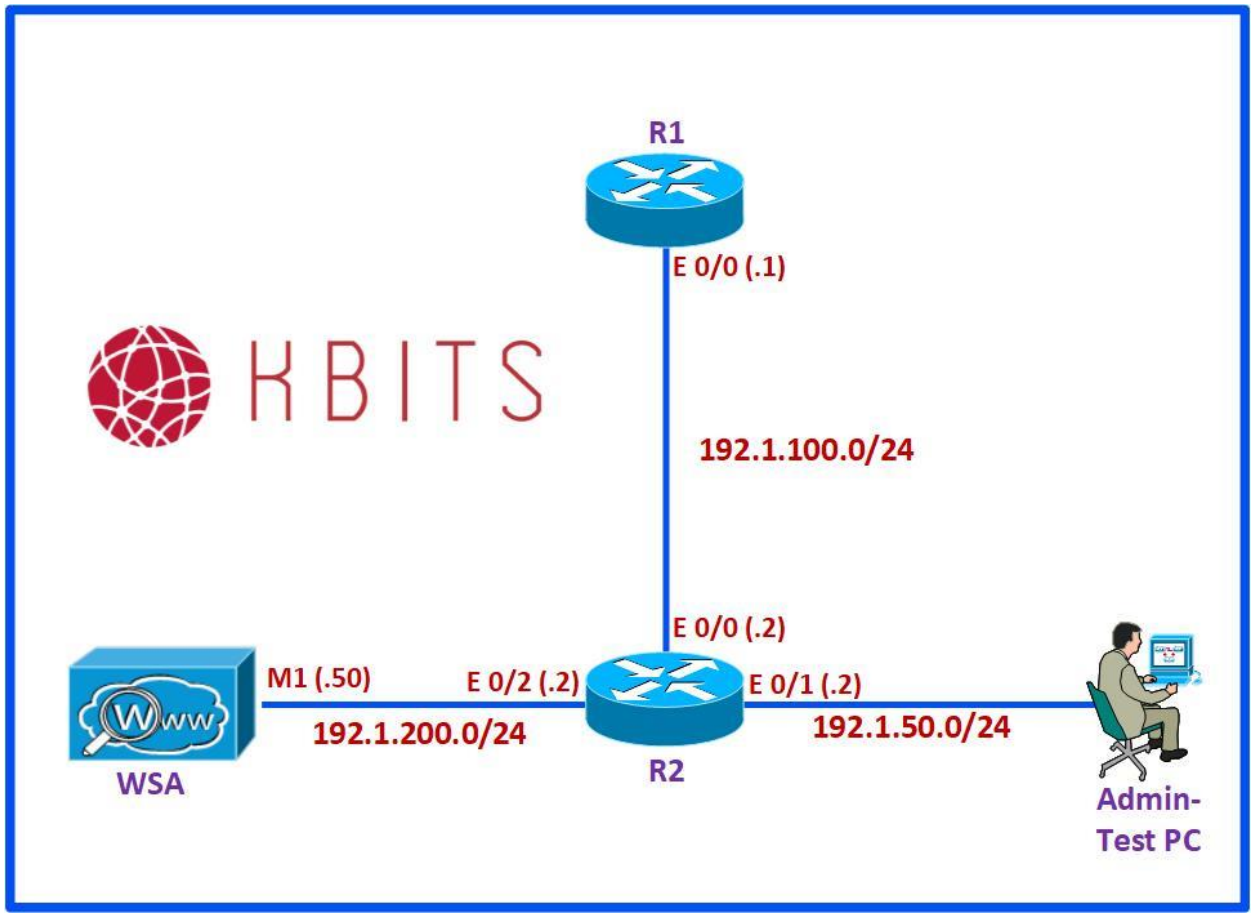
4. Click "**Submit**".

5. Commit the changes by clicking the "**Commit Changes**" button.

Task 2

Verify you can browse to www.espn.com from the Admin/Test-PC-1. You should not be able to browse to the same website from Test-PC-2.

Lab 4 – Configuring Custom URL Policies



Lab Scenario:

- Configuring Custom URLs.
- Using Custom URLs in Policy.

Initial Setup:

- **Based on the previous Lab**

Lab Tasks:

Task 1

Configure Custom URLs based on the following:

- Name: **Allow List**
  - URLs: www.espn.com, .espn.com
- Name: **Deny List**
  - URLs: www.cnn.com, .cnn.com

WSA

1. Browse to "**Web Security Manager -> Custom Policy Elements -> Custom & External URL Categories -> Add Category**".

2. Create the 2 Custom Categories based on the above parameters.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 2

Configure **Execs Policy** to include the 2 Custom Categories in the policy. The Action for the **Allow List** should be to **Allow** and for the **Deny List** should be to **block**.

WSA

1. Browse to "**Web Security Manager -> Web Policies -> Access Policies -> Execs Policy**".

2. Click the **URL Filtering** link and "Select the Custom Categories". Specify the the action based on the task requirement.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 3

Configure **Global Policy** to include the 2 Custom Categories in the policy. The Action for the **Allow List** should be to **Allow** and for the **Deny List** should be to **block**.

WSA

1. Browse to "**Web Security Manager -> Web Policies -> Access Policies -> Global Policy**".

2. Click the **URL Filtering** link and "Select the Custom Categories". Specify the the action based on the task requirement.

3. Click "**Submit**".

4. Commit the changes by clicking the "**Commit Changes**" button.

Task 4

Verify you can browse to www.espn.com from both of the PC's.

Task 5

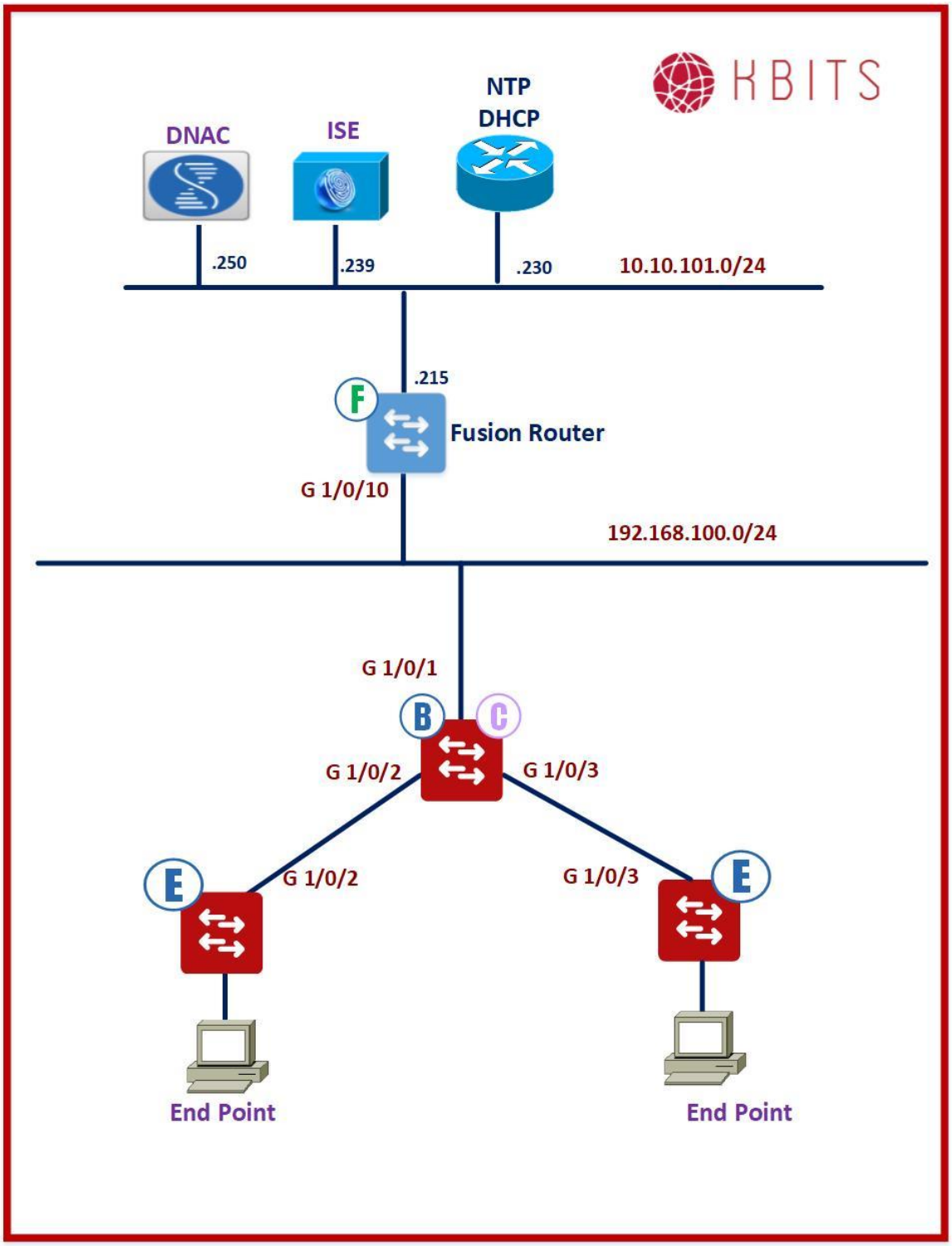
Verify you cannot browse to www.cnn.com from the either of the PC's.

CCIE Security v6 – Software Defined Access (SDA)

Module 1 – Configuring the Non-SDA Components

Module 1 – Configuring the Non-SDA Components

Lab 1 – Configuring DNAC & ISE Integration



Task 1
Configure the following RADIUS settings on ISE:

- Uncheck “Reject RADIUS requests from clients with repeated failures”.
- Uncheck “Suppress repeated failed clients”.
- Uncheck “Suppress repeated successful authentications”

ISE

1. Browse to **https://10.10.101.239.**

2. Log in using the username & Password of **admin/Kbits@123**.

3. Browse to “**Administration -> System -> Settings -> Protocols -> RADIUS**”.

4. Configure the RADIUS Settings based on the above parameters.

5. Click **Save**

Task 2
Configure the following ERS settings on ISE:

- Check Enable ERS for Read/Write

ISE

1. Browse to “**Administration -> System -> Settings -> ERS Settings**”.

2. Configure the ERS Settings based on the above parameter.

3. Click **Save**

Task 3
Enable the pxGrid Service.

ISE

1. Browse to “**Administration -> System -> Deployment -> DNAC-ISE**”.

2. Check to enable the **pxGrid** service.

3. Click **Save**. Wait for the pxGrid Services to come online before proceeding.

Task 4

Configure DNAC to communicate to ISE using the following parameters:

- Server IP Address: **10.10.101.239**
- Shared Secret: **Cisco@123**
- Cisco ISE Server: **Slide to Enable**
- Username: **admin**
- Password: **Cisco@123**
- FQDN: **dnac-ise.kbits.local**
- Subsriber Name: **DNAC-KBITS**

DNAC

1. Browse to **https://10.10.101.250.**

2. Log in using the username & Password of **admin/Cisco@123**.

3. Browse to "**Settings (Icon) -> System Settings -> Settings -> Authentication & Policy Servers -> Add**".

4. Configure the ISE Integration based on the the above parameters.

5. Click **Apply**.

Task 5

Approve the Pending requests on ISE to allow DNAC to integrate with ISE.

ISE

1. Browse to "**Administration -> pxGrid Services**".

2. Click on Total Pending and "**Approve All**".

Note: Need to see "Connected via XMPP dna-ise.kbits.local"

Task 5

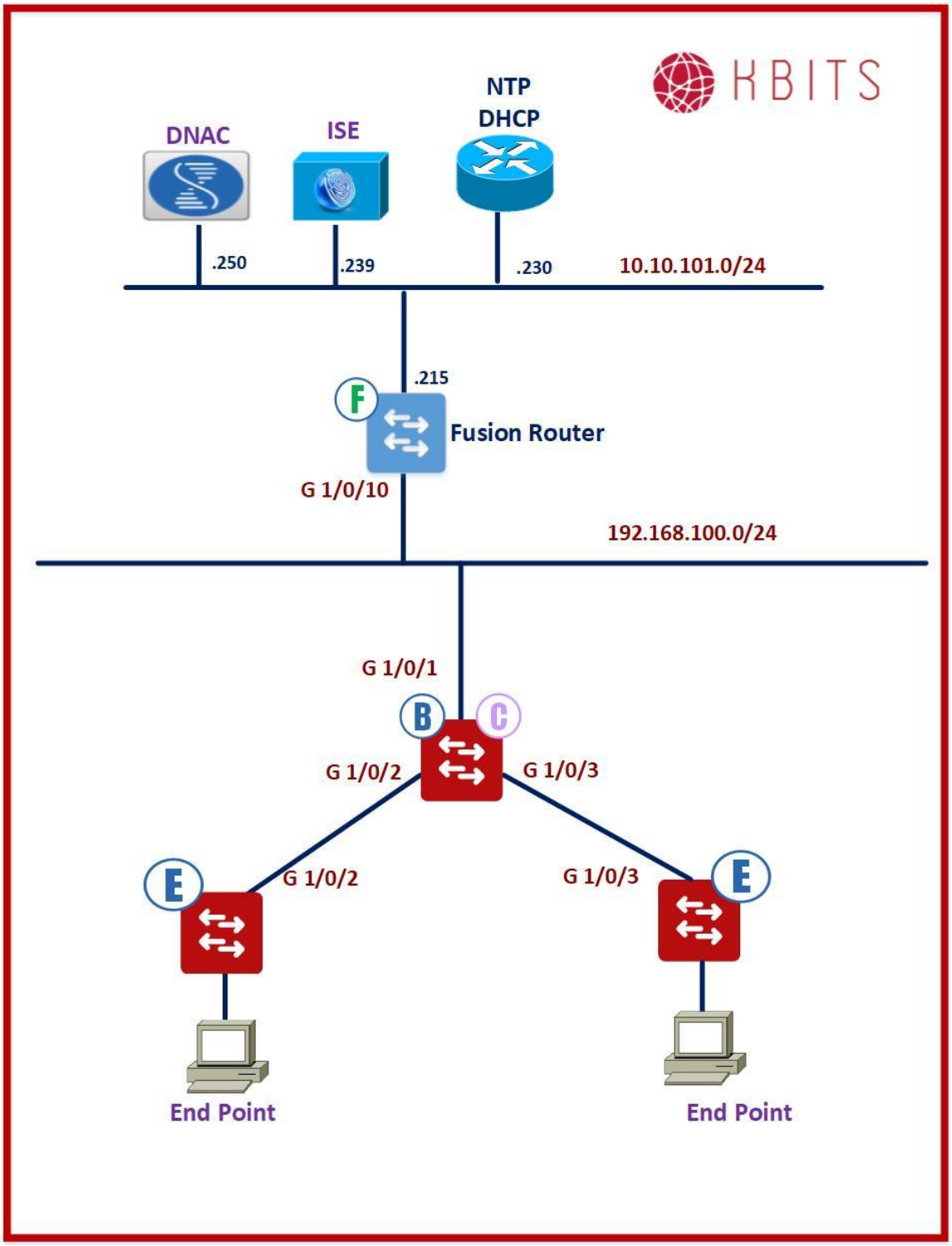
Migrate Policy Data from ISE to DNAC. This will bring over the existing ISE SGT's into DNAC.

DNAC

1. Browse to "**Policy -> Group-Based Access Control -> Scalable Groups -> Start Migration (In Message)**".

2. Click "**Yes**" to accept to iniate the migration.

Lab 2 – Configuring Border Switch Initial Configuration



Task 1

Configure the 9300CB device with a hostname of **9300CB**. Configure the Gig 1/0/1 interface as a trunk towards the Fusion Router. Create a vlan **199** and an SVI for **VLAN 199** with an ip address of **192.168.100.2/24**. Configure a default route towards the Fusion Router (**192.168.100.1**).

9300CB

```
no ip domain lookup
!
line con 0
 logg sync
 no exec-timeout
!
hostname 9300CB
!
Interface Gig 1/0/1
 switchport mode trunk
!
vlan 199
!
ip routing
!
interface VLAN 199
 ip address 192.168.100.2 255.255.255.0
 no shut
!
ip route 0.0.0.0 0.0.0.0 192.168.100.1
```

Task 2

Configure a username **kbits** with a password of **Cisco@123**. It should have a privilege of **15**. Configure the vty lines (0 4) to authenticate based on the local DB.

9300CB

```
username kbits privilege 15 secret Cisco@123
!
line vty 0 4
 login local
```

Task 3 – Configure SNMP Parameters for RO & RW Communities

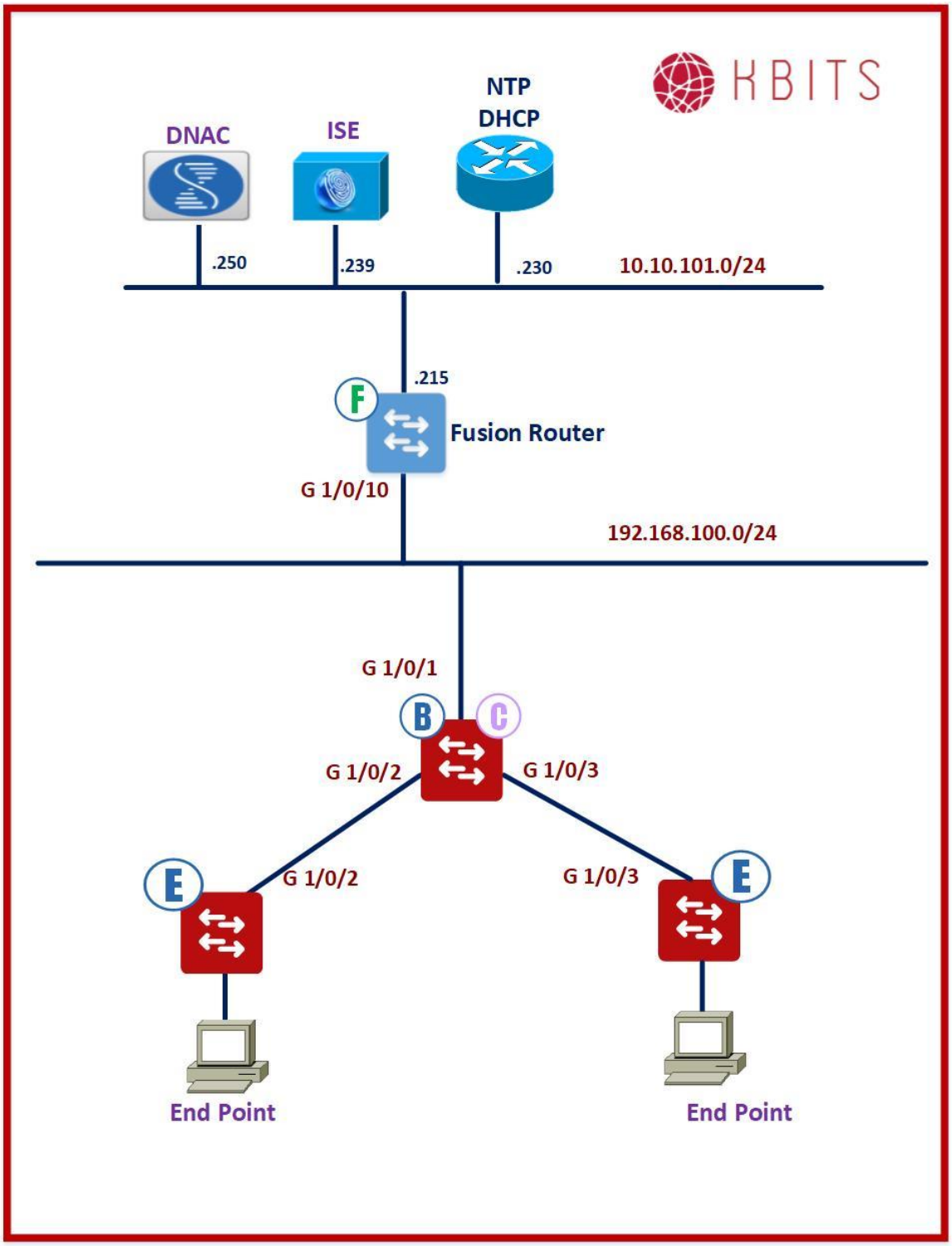
Task 2

Configure the snmp community for **Read-Only** as **public**. Configure the snmp community for **Read-Write** as **private**.

9300CB

```
snmp-server community RO ro public
snmp-server community RW rw private
```

Lab 3 – Configure the Fusion Router to communicate to SDA Fabric via the Border



Task 1

Configure the Gig 1/0/10 interface as a trunk towards the 9300CB Router. Create a vlan **199** and an SVI for **VLAN 199** with an ip address of **192.168.100.1/24**.

Fusion Router

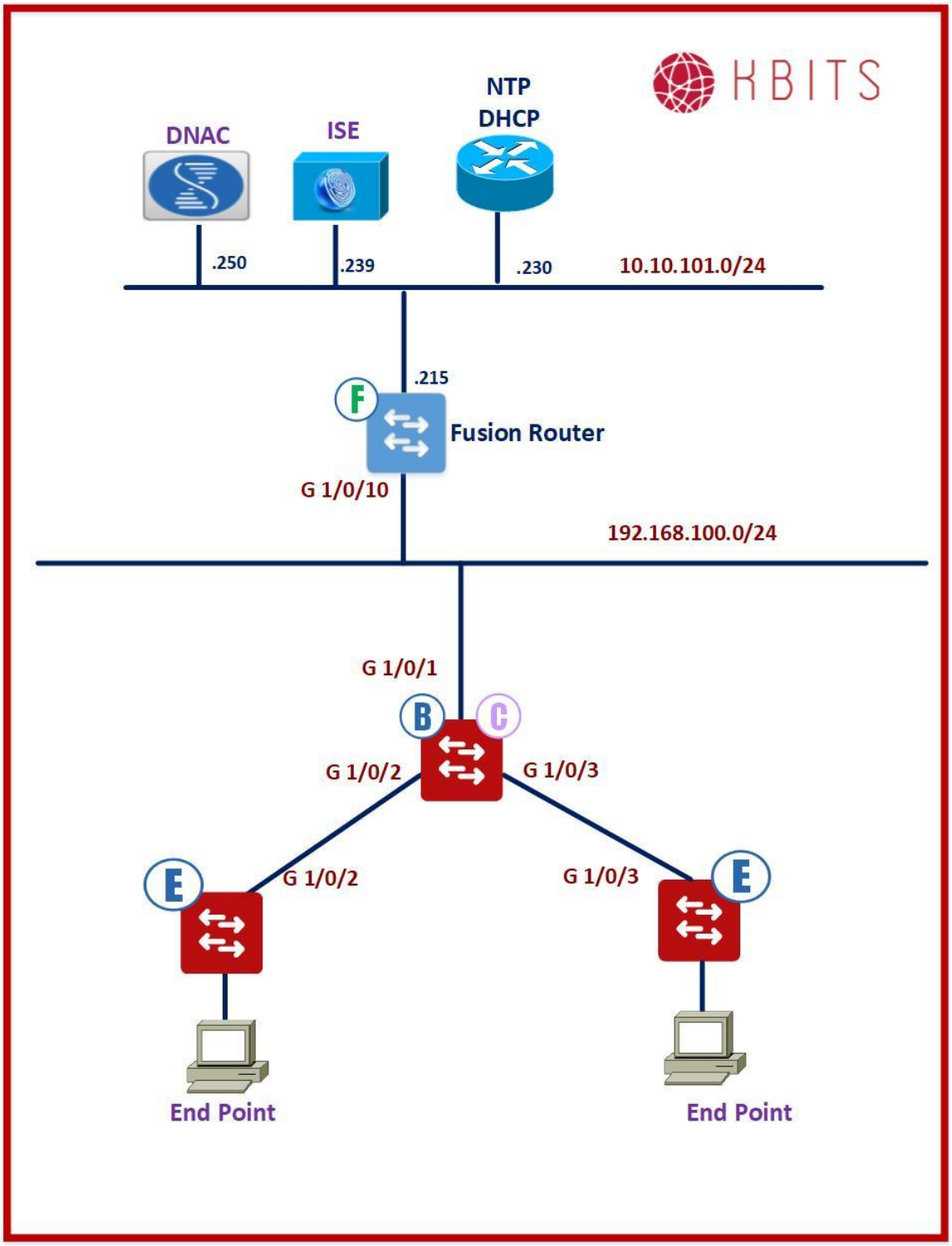
```
hostname Fusion
!
Interface Gig 1/0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
vlan 199
!
ip routing
!
interface VLAN 199
 ip address 192.168.100.1 255.255.255.0
 no shut
```

CCIE Security v6 – Software Defined Access (SDA)

Module 2 – Configuring the DNAC Design Components

Module 2 – Configuring the DNAC Design Components

Lab 1 – DNAC Design - Network Hierarchy – Site & Building



Task 1

Create an Area named **Los Angeles** under **Global**.

DNAC

1. Browse to **https://10.10.101.250.**
2. Log in using the username & Password of **admin/Cisco@123**.
3. Browse to "**Desgin -> Network Hierarchy -> Add Site -> Add Area**".
4. Create the Area based on the above requirements.
5. Click **Save**

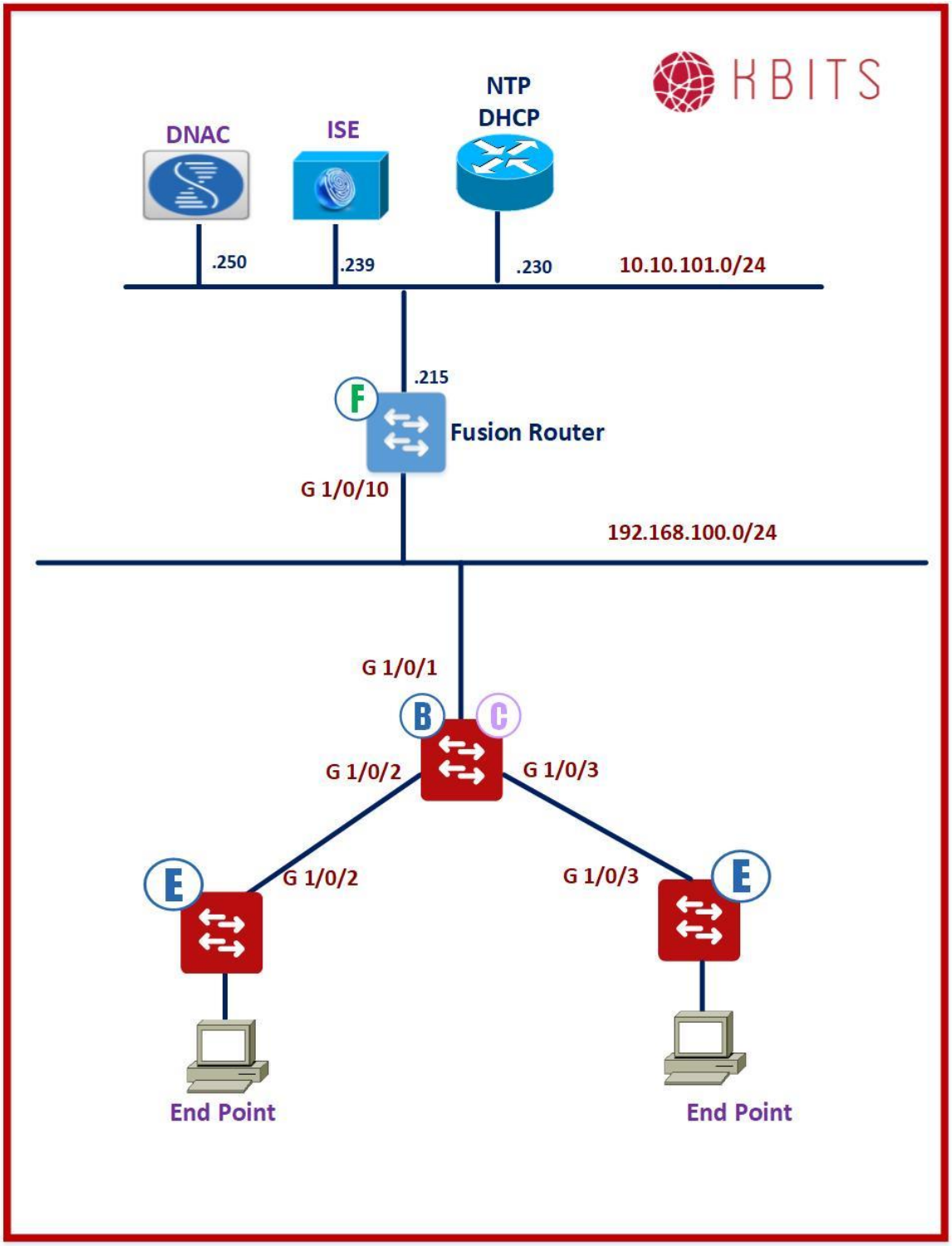
Task 2

Add a Building under the area **Los Angeles**. Name the building **HQ**. Configure the address as "**2640 Main Street, Irvine, California 92614, US**".

DNAC

1. Browse to "**Desgin -> Network Hierarchy -> Add Site -> Add Building**".
2. Create the building based on the above requirements.
3. Click **Save**

Lab 2 – DNAC Design – Server Configuration – AAA, NTP etc



Task 1

Add the following Servers under the Network Settings:

- ISE (**Client/Endpoint**):
  - Protocols: **RADIUS**
  - Client/Endpoint: **10.10.101.239 (Select from Drop-Down)**
  - IP Address (Pri): **10.10.101.239 (Select from Drop-Down)**

- DHCP Server:
  - IP Address: **10.10.101.230**

- NTP Server:
  - IP Address: **10.10.101.230**

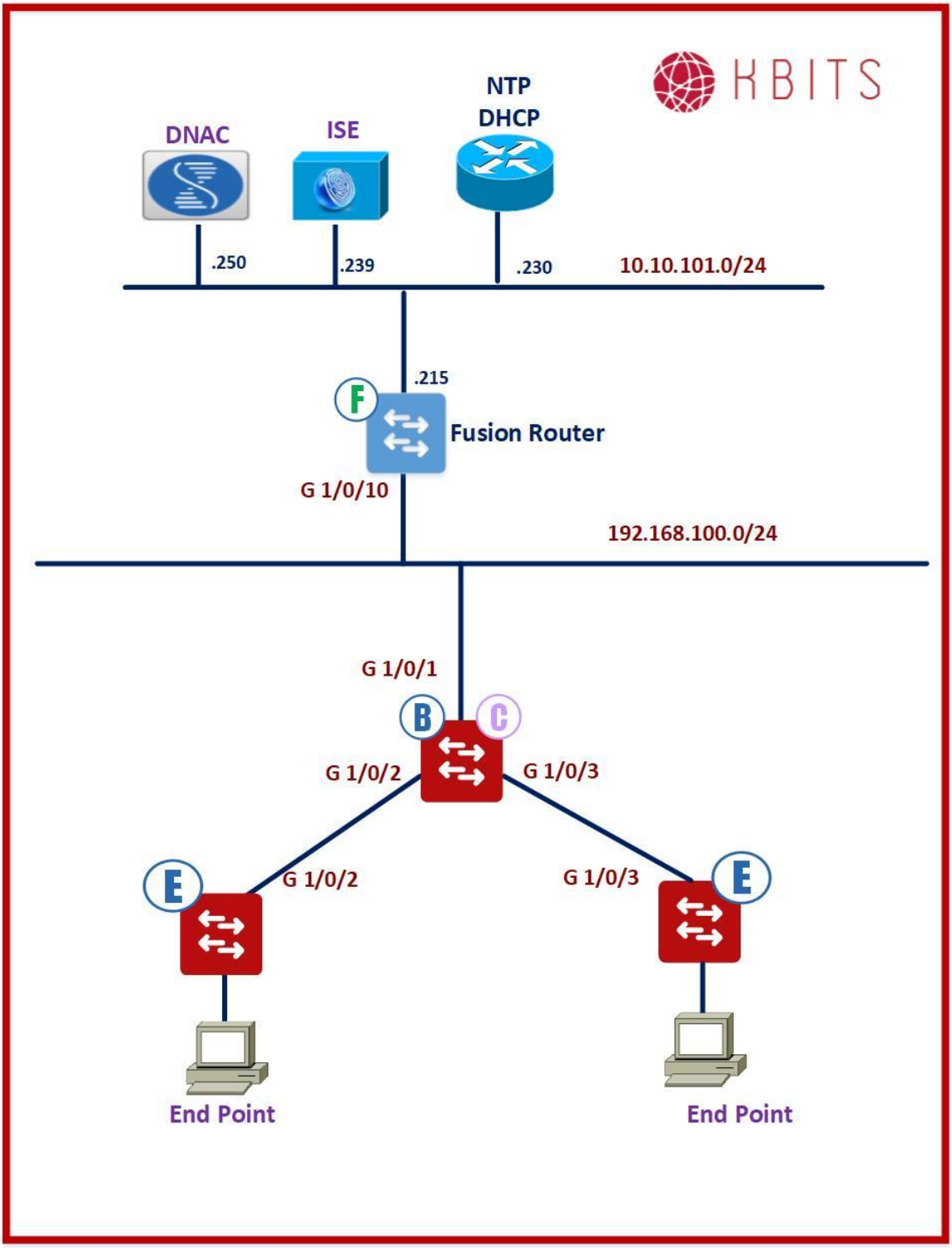
DNAC

1. Browse to "**Desgin -> Network Settings -> Network -> Add**".

2. Configure the Servers based on the above parameters.

3. Click **Save**

Lab 3 – DNAC Design - Device Credentials



Task 1

Configure the following Device Credentials for Telnet/SSH & SNMP:

- **CLI Credentials:**
  - Name: **FabricAdmin**
  - Username: **kbits**
  - Password: **Cisco@123**
  - Enable Password: **Cisco@123**

- **SNMPv2C Credentials – Read:**
  - Type: **SNMPv2C**
  - Community Type: **Read**
  - Name: **RO**
  - Community: **public**

- **SNMPv2C Credentials – Read/Write:**
  - Type: **SNMPv2C**
  - Community Type: **Read/Write**
  - Name: **RW**
  - Community: **private**

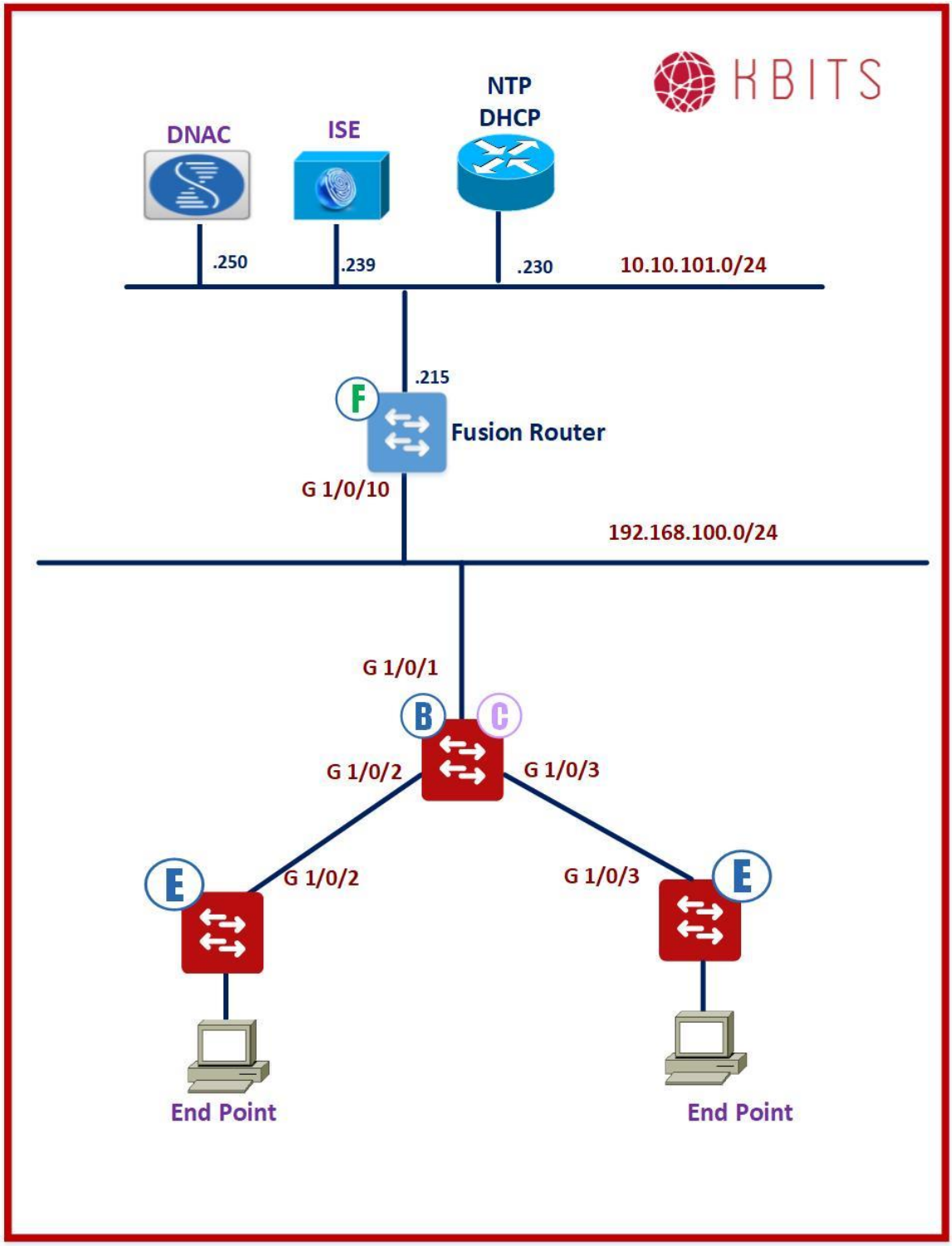
DNAC

1. Browse to "**Design -> Network Settings -> Device Credentials**".

2. Configure the Device Credentials based on the above parameters.

3. Click **Save**

Lab 4 – DNAC Design - IP Address Pools



Task 1

Configure the following Pools:

- Name: **LA_OVERLAY_POOL**
  - Type: **Generic**
  - IP Addres Space: **(IPv4)**
  - Subnet: **172.16.0.0**
  - Prefix-length: **/16**

- Name: **LA_UNDERLAY_POOL**
  - Type: **Generic**
  - IP Addres Space: **(IPv4)**
  - Subnet: **172.20.0.0**
  - Prefix-length: **/16**

DNAC

1. Browse to "**Design -> Network Settings -> IP Address Pools -> Global**".

2. Click **Add** to create the Pools based on the above parameters.

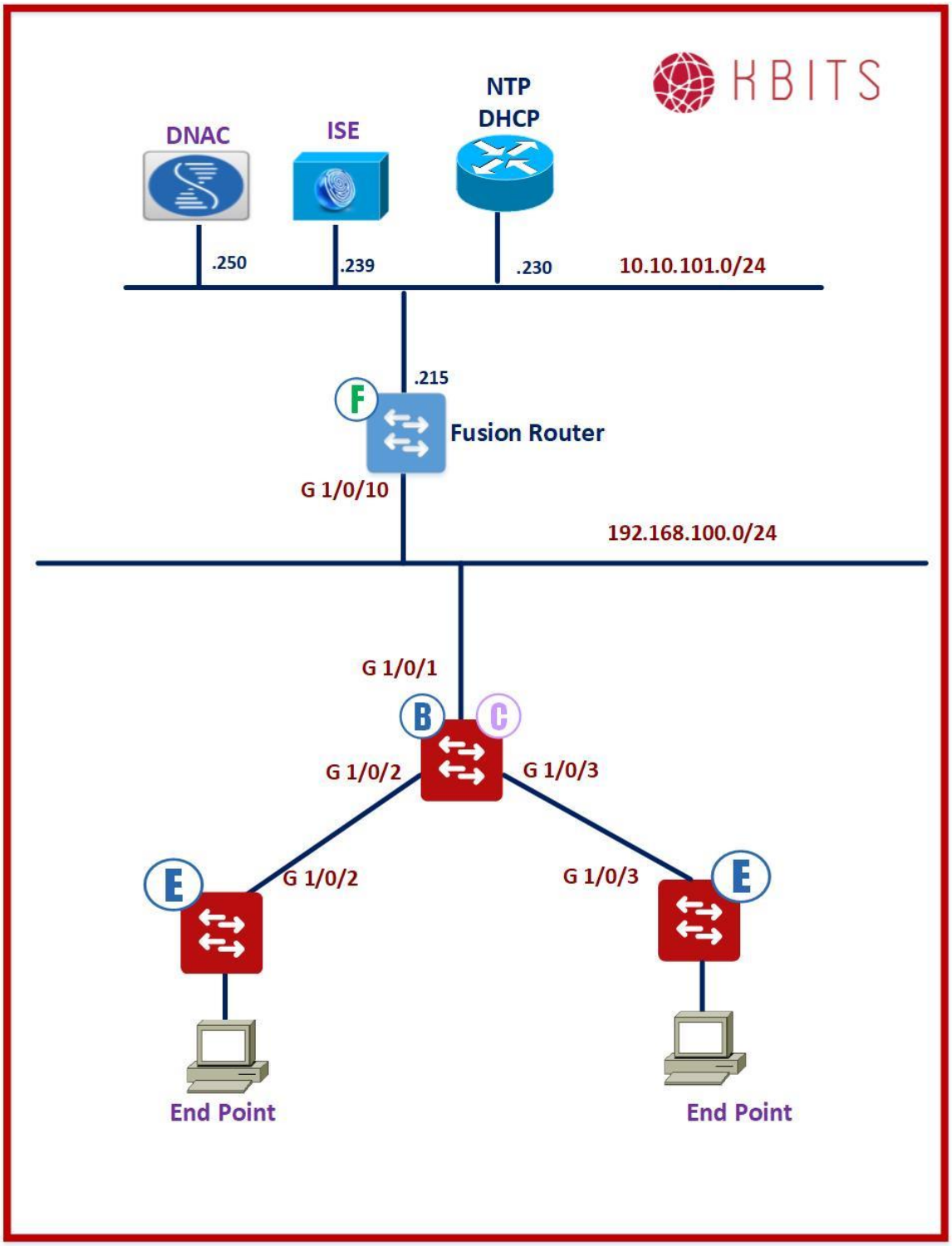
3. Click **Save**

CCIE Security v6 – Software Defined Access (SDA)

Module 3 – Using LAN Automation to discover the devices

Module 3 – Using LAN Automation to discover the devices

Lab 1 – DNAC Discovery – Discover the Seed Device (Border)



Task 1

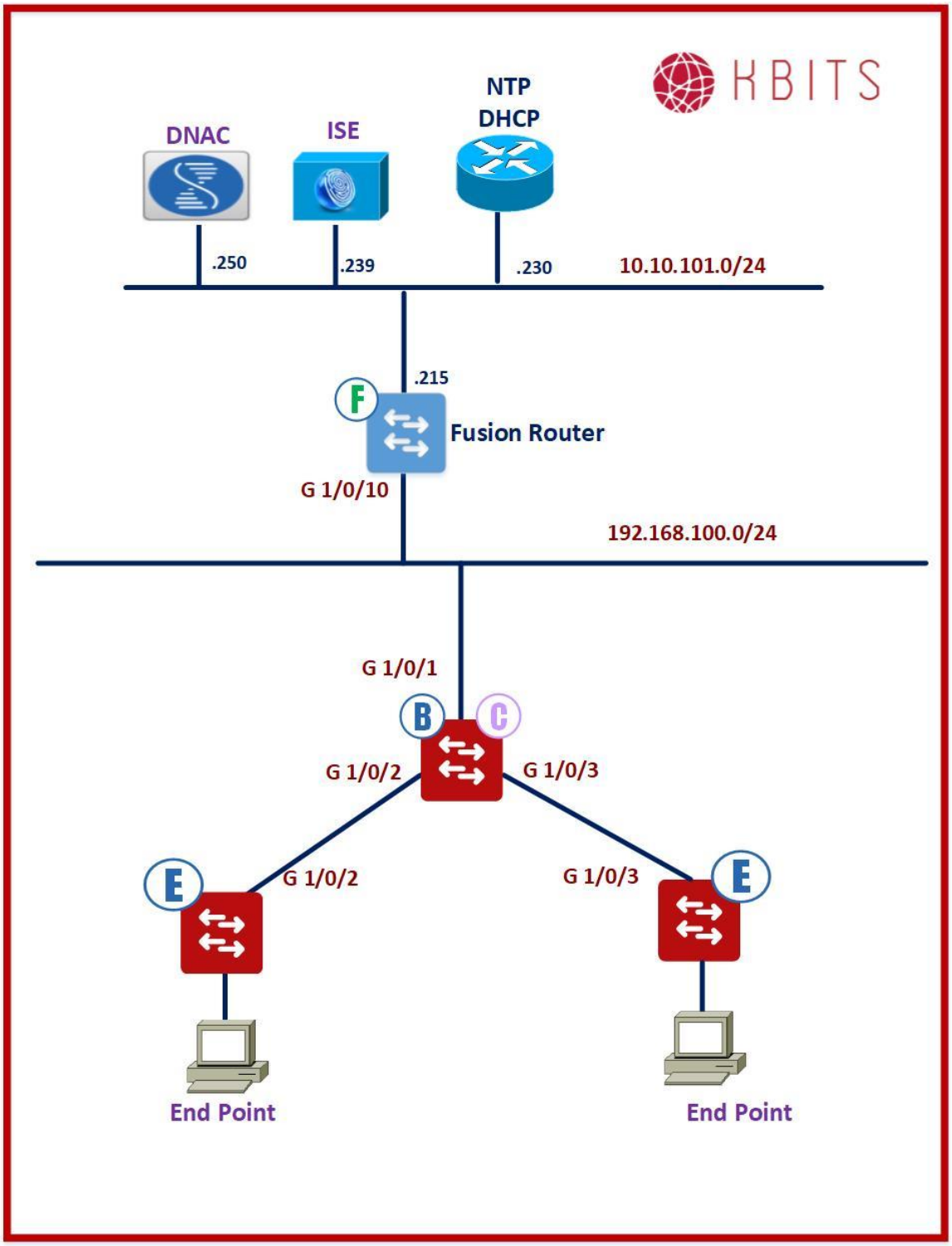
Configure a Discovery based on the following parameters:

- Discovery Name: **SEED-DEVICE**
  - IP Address Range: **192.168.100.2-192.168.100.2**
  - CLI Credentials: **FabricAdmin**
  - SNMP-Read: **RO**
  - SNMP-Write: **RW**

DNAC

1. Browse to **https://10.10.101.250.**
2. Log in using the username & Password of **admin/Cisco@123**.
3. Browse to "**Tools -> Discovery -> Add Discovery**".
4. Run a Discovery based on the above parameters.
5. Wait for the 9300CB to be discovered.

Lab 2 – DNAC Provisioning - Assign Seed Device to Building



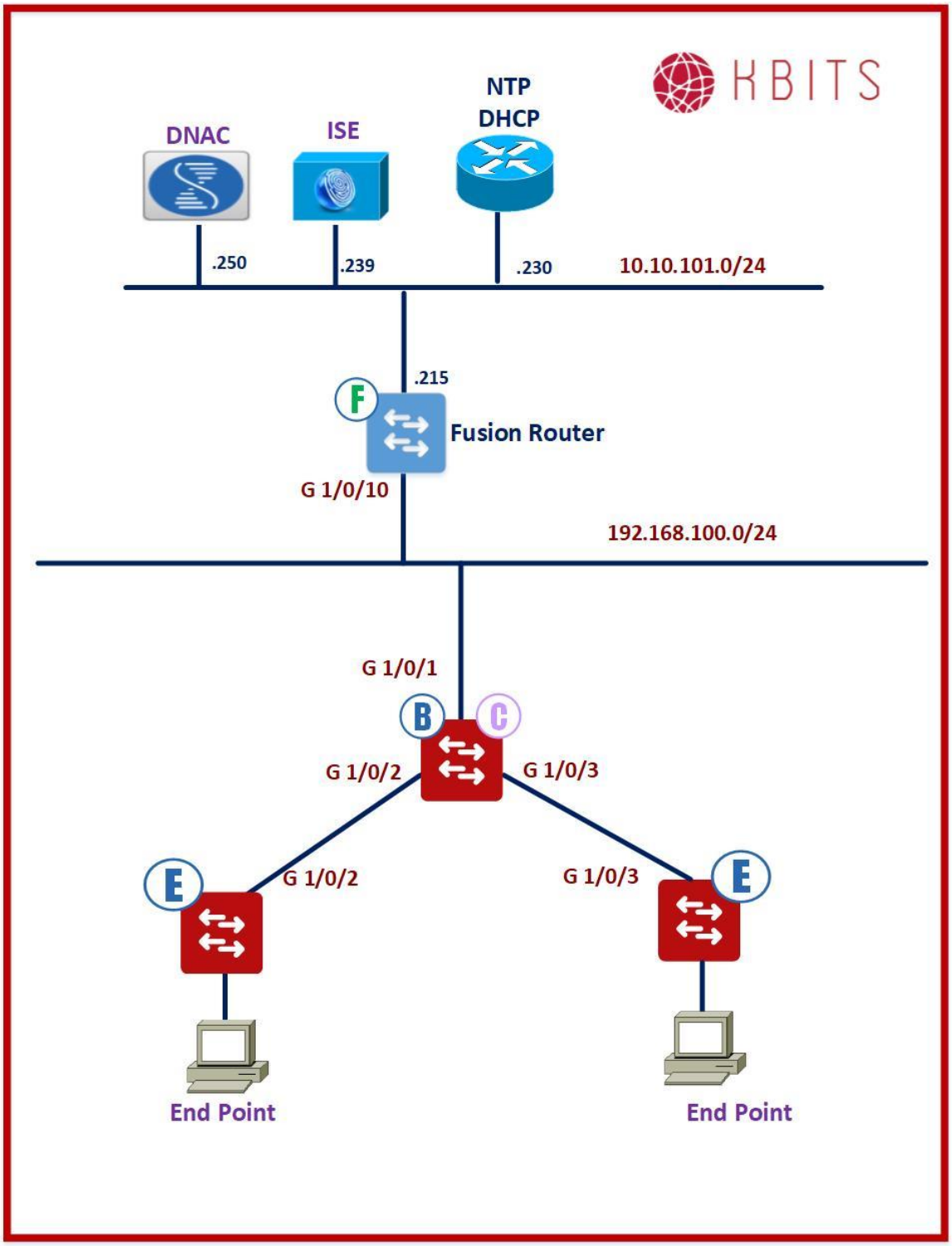
Task 1

Assign the discovered device, **9300CB** to the HQ building under **Los Angeles**.

DNAC

1. Browse to "**Provision -> Unassigned Devices -> Inventory**".
2. Select the **9300CB** switch.
3. Click "**Actions -> Provision -> Assign Device to Site**".
4. Select "**Global -> Los Angeles -> HQ**".
5. Click **Assign**.
6. The Switch will move under HQ.

Lab 3 – DNAC Provisioning – Enable LAN Automation to Discover the Fabric



Task 1

Reserve a pool for Lan Automation using the following parameters:

- Address Pool Name: **LAN_AUTO_HQ**
  - Type: **LAN**
  - IPv4 Global Pool: 172.20.0.0/24
  - Global Pool: **LA_UNDERLAY_POOL**
  - Prefix Length: **/24**
  - IPv4 Subnet: **172.20.0.0**

DNAC

1. Browse to "**Design -> Network Settings -> IP Address Pools -> Global -> Los Angeles -> HQ**".

2. Click **Reserve**.

3. Reservce the LAN Automation Pool based on the parameters above.

4. Click **Save**.

Task 2

Assign the Device Credentials for the HQ Site/Building using the following information:

- CLI Credentials: **FabricAdmin**
- SNMP Credentials: SNMPV2C Read: **RO**
- SNMP Credentials: SNMPV2C Write: **RW**

DNAC

1. Browse to "**Design -> Network Settings -> Device Credentials -> Global -> Los Angeles -> HQ**".

2. Select the Device Credentials based on the above information.

3. Click **Save**.

Task 3

Configure the Fusion Router with a Static Route for the LAN Automation Pool pointing towards the Seed/Border Device.

Fusion Router

Ip route 172.20.0.0 255.255.0.0 192.168.100.2

Task 4

Initiate the LAN Automation process for the HQ Site based on the parameters below:

- Primary Site: **Global/Los Angeles/HQ**
- Primary Device: **9300CB**
- Selected Ports of Primary Device: **Gig1/0/2 & Gig1/0/3**
- Discoverd Device Site: **HQ**
- IP Pool: **LAN_AUTO_HQ**
- IS-IS Domain Password: **Cisco@123**

DNAC

1. Browse to "**Provision -> Inventory -> Action -> Provision -> LAN AUTOMATION -> Start**".

2. Select the LAN Automation parameters based on the above information.

3. Click **Save** to initiate LAN Automation.

Task 5

Wait for both the Fabric Edge Switches to be discovered. The switches should show up as **Managed** in the Inventory window.

DNAC

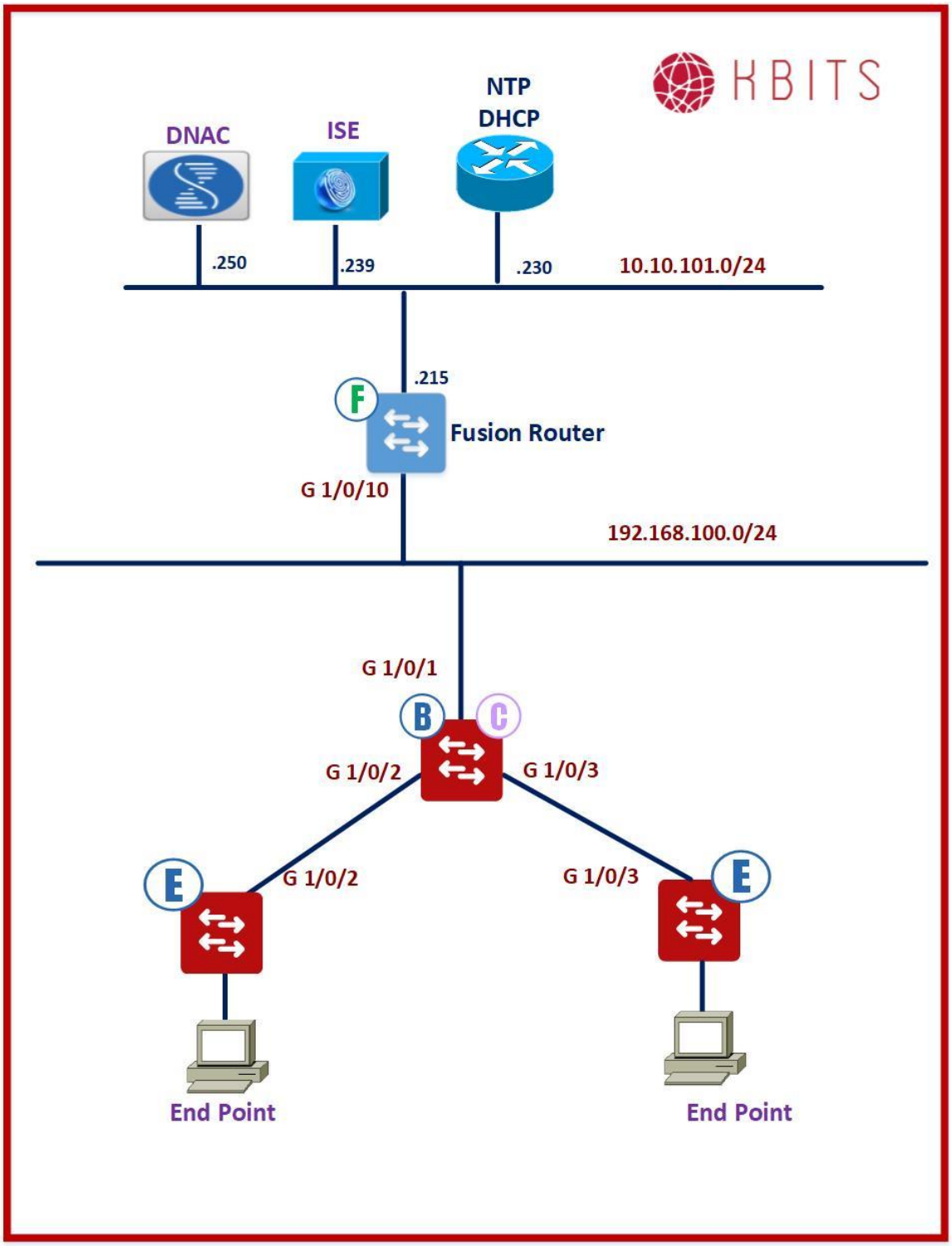
1. Check the Status of the LAN Automation Process in the inventory Page. Wait until it discovers the 2 devices and shows the status as "**Managed**".

2. Browse to "**Provision -> Inventory -> Action -> Provision -> LAN AUTOMATION Status**".

3. Click **Stop** to stop the LAN Automation Process.

4. Change the Switch type of the Fabric Edge Devices as **Access**.

Lab 4 – Provision the devices to HQ Site



Task 1

Provision the Devices to the Los Angeles -> HQ Building. This will initialize the switches with base configuration including the ISE, NTP and DHCP Server parameters configured earlier in the Design section.

DNAC

1. Browse to "**Provision -> Global -> Los Angeles -> HQ**".

2. Select "All" the devices

3. Click **Action -> Provision -> Provision** the device

4. Select "**Global -> Los Angeles -> HQ**".

5. Click "**Apply to all devices**".

6. Click **Assign**.

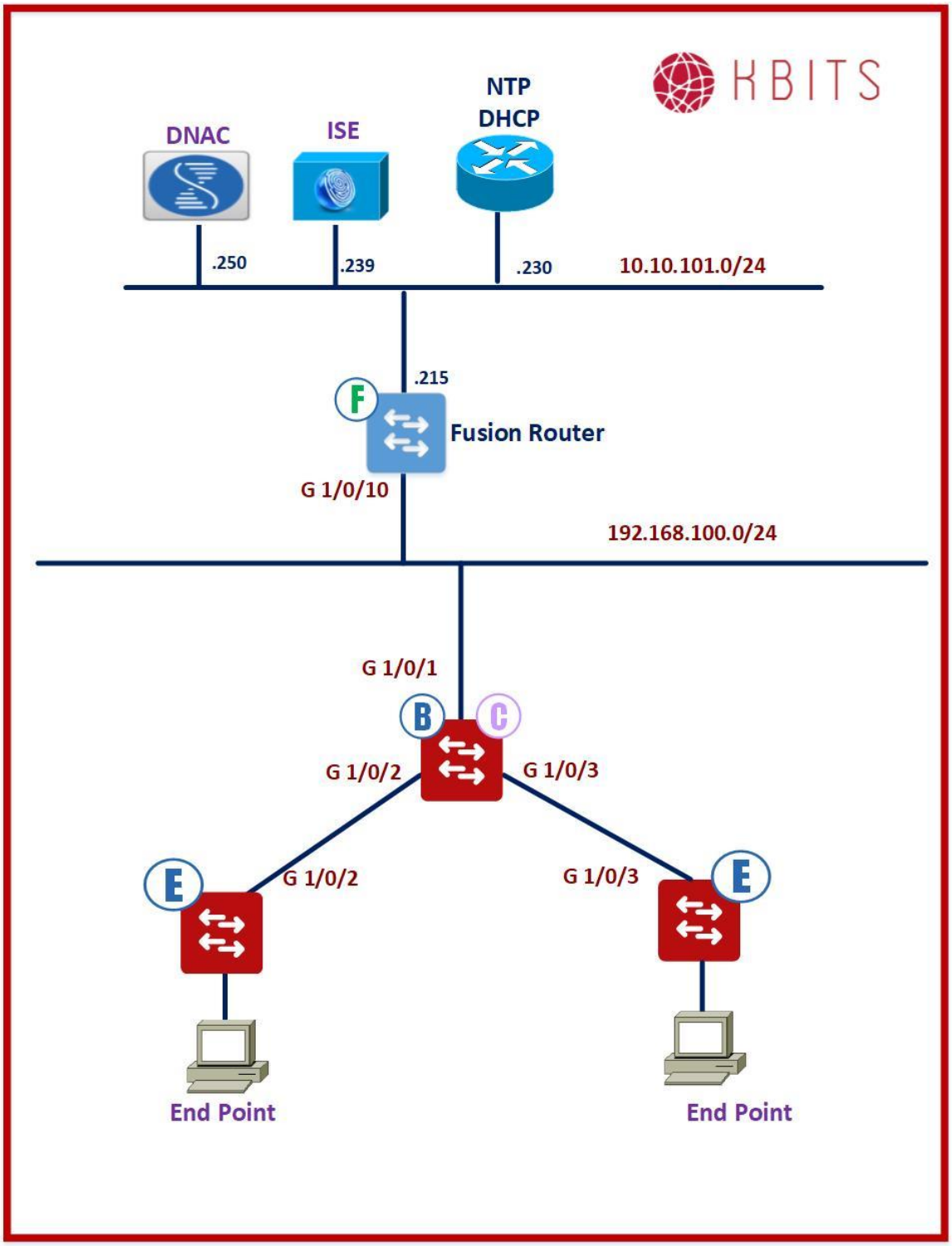
7. The devices should now be available for Device Role Assignment under the HQ Fabric

CCIE Security v6 – Software Defined Access (SDA)

Module 4 – Creating & Configuring the Fabric & L3Handoff

Module 4 – Creating & Configuring the Fabric & L3Handoff

Lab 1 – Reserve the IP Pools for HQ Site for Overlay & Underlay



Task 1

Reserve the Pools for the IT Department/VN using the **LA_OVERLAY_POOL** using the Parameters below:

- Name: **IT-DATA-1-POOL**
  - Prefix Length**: /24**
  - IPv4 Subnet: **172.16.1.0**
  - Default GW: **172.16.1.254**
  - DHCP Server: **10.10.101.230**

- Name: **IT-DATA-2-POOL**
  - Prefix Length**: /24**
  - IPv4 Subnet: **172.16.2.0**
  - Default GW: **172.16.2.254**
  - DHCP Server: **10.10.101.230**

- Name: **IT-VOICE-1-POOL**
  - Prefix Length**: /24**
  - IPv4 Subnet: **172.16.101.0**
  - Default GW: **172.16.101.254**
  - DHCP Server: **10.10.101.230**

DNAC

1. Browse to **https://10.10.101.250.**

2. Log in using the username & Password of **admin/Cisco@123**.

3. Browse to "**Network Settings -> IP Address Pools -> HQ**".

4. Click **Reserve**.

5. Reserve the pools for **IT** using the parameters above.

Task 2

Reserve the Pools for the SALES Department/VN using the **LA_OVERLAY_POOL** using the Parameters below:

- Name: **SALES-DATA-1-POOL**
  - Prefix Length**: /24**
  - IPv4 Subnet: **172.16.3.0**
  - Default GW: **172.16.3.254**
  - DHCP Server: **10.10.101.230**

- Name: **SALES-DATA-2-POOL**
  - Prefix Length**: /24**
  - IPv4 Subnet: **172.16.4.0**
  - Default GW: **172.16.4.254**
  - DHCP Server: **10.10.101.230**

- Name: **SALES-VOICE-1-POOL**
  - Prefix Length**: /24**
  - IPv4 Subnet: **172.16.102.0**
  - Default GW: **172.16.102.254**
  - DHCP Server: **10.10.101.230**

DNAC

1. Browse to "**Network Settings -> IP Address Pools -> HQ**".

2. Click **Reserve**.

3. Reserve the pools for **SALES** using the parameters above.

Task 3

Reserve the Pool for the L3Handoff Link using the **LA_UNDERLAY_POOL** using the Parameters below:

- Name: **L3HANDOFF-POOL**
  - Prefix Length**: /24**
  - IPv4 Subnet: **172.20.1.0**
  - Default GW: **172.16.3.254**

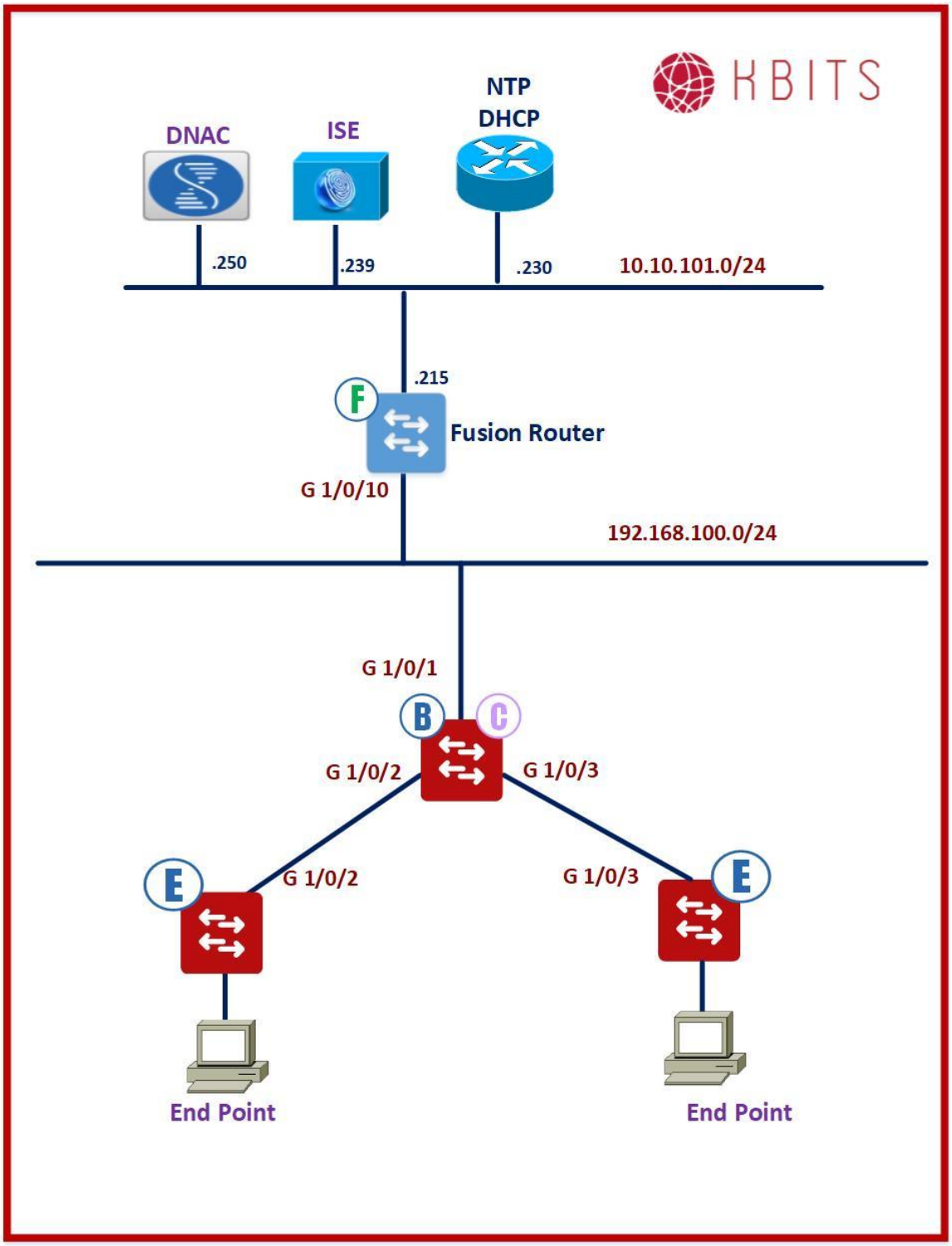
DNAC

1. Browse to "**Network Settings -> IP Address Pools -> HQ**".

2. Click **Reserve**.

3. Reserve the pools for **SALES** using the parameters above.

Lab 2 – Create VNs for the Fabric



Task 1

Create the following VNs for the HQ Fabric:

- Name: **IT_VN**
- Name: **SALES_VN**

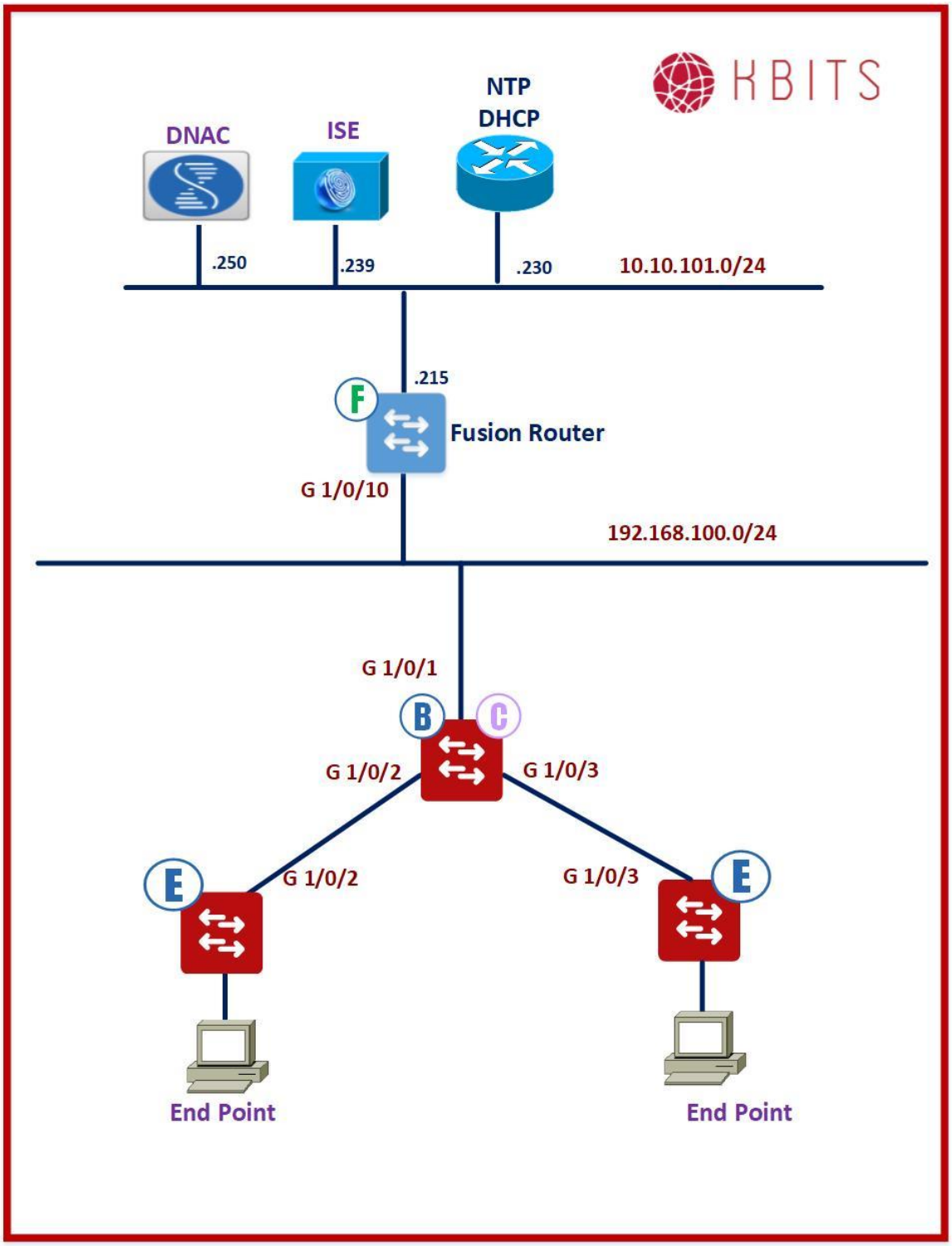
DNAC

1. Browse to "**Policy -> Virtual Network -> Add**".

2. Create the VNs based on the information above.

3. Click **Save**.

Lab 3 – Create the Transit Network (L3HANDOFF)



Task 1

Configure a L3 Handoff between the Border and Fusion. Specify the parameters for the Fusion based on the following:

- Name: **L3HANDOFF**
  - Transit/Type: **IP-Based**
  - Protocol: **BGP**
  - Type: **ASPlain**
  - AS #: **65001**

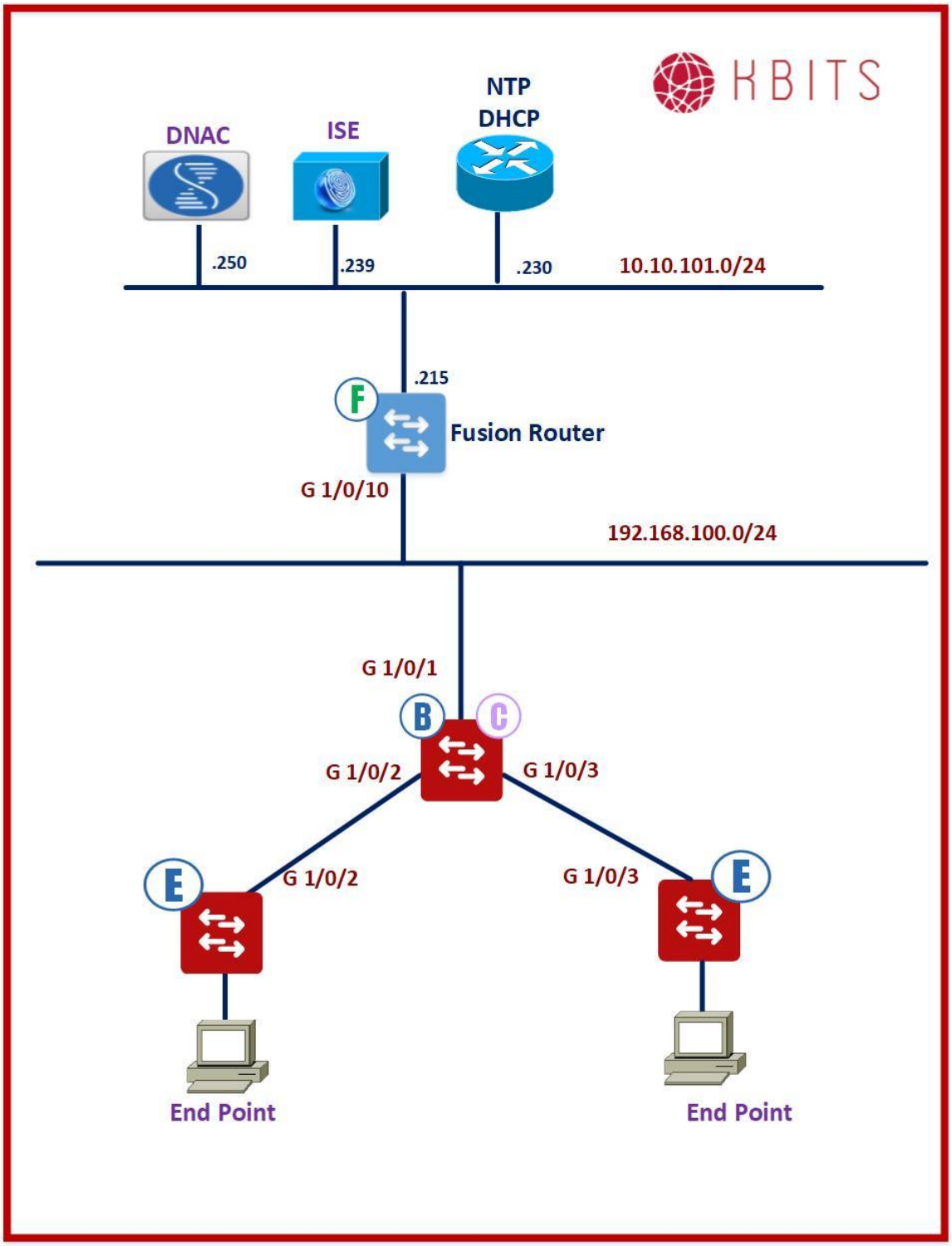
DNAC

1. Browse to "**Provision -> Fabric -> Add Transit/Peer Network**".

2. Create a L3 Handoff based on the parameters above.

3. Click **Save**.

Lab 4 – Configure Host Onboarding



Task 1

Configure the HQ Fabric. Name the fabric **HQ_Fabric**. Add the **INFRA**, **IT** & **SALES** VNs to the Fabric.

DNAC

1. Browse to "**Provision -> Fabric -> Add Fabric**".

2. Create the HQ Fabric based on the Task requirement.

3. Click **Add**.

Task 2

Configuring Host Onboarding based on the following parameters:

- **Authentication Template**
  - Select "**Closed Authentication**"
  - Click to set it as the "**Default**"

- **Virtual Network – IT_VN**

  - IP Address Pool: **IT-DATA-1-POOL**
  - Authentication Policy: **IT-DATA-1**
  - Traffic Type: **Data**

  - IP Address Pool: **IT-DATA-2-POOL**
  - Authentication Policy: **IT-DATA-2**
  - Traffic Type: **Data**

  - IP Address Pool: **IT-VOICE-1-POOL**
  - Authentication Policy: **IT-VOICE-1**
  - Traffic Type: **Data**

- **Virtual Network – SALES_VN**

  - IP Address Pool: **SALES-DATA-1-POOL**
  - Authentication Policy: **SALES-DATA-1**
  - Traffic Type: **Data**

  - IP Address Pool: **SALES-DATA-2-POOL**
  - Authentication Policy: **SALES-DATA-2**
  - Traffic Type: **Data**

  - IP Address Pool: **SALES-VOICE-1-POOL**

- Authentication Policy: **SALES-VOICE-1**
- Traffic Type: **Data**

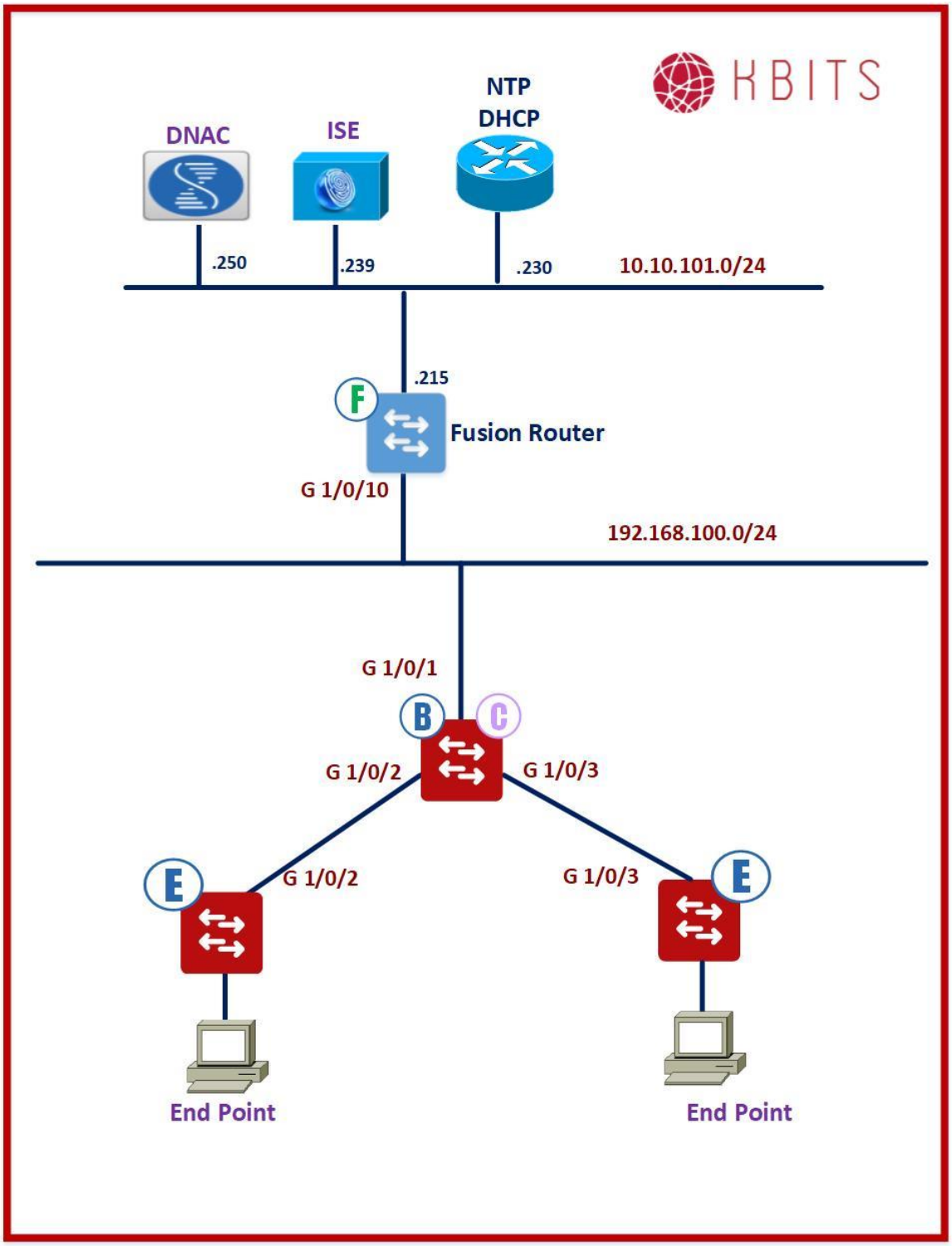
DNAC

1. Browse to "**Provision -> Fabric -> HQ-FABRIC -> Los Angeles -> HQ**".

2. Create the IT & SALES VNs with the Authentication Template and Pools based on the parameters above.

3. Click **Save**.

Lab 5 – Provision the Control/Border Device



Task 1

Provision the **9300CB** device as the **Control** & **Border** Device. Use the following information to complete the task:

- **Border L3Handoff Configuration Parameters**:
  - Select Type **ASPLAIN**
  - Local AS: **65002**

DNAC

1. Browse to "**Fabric -> HQ_FABRIC -> Los Angeles -> HQ**".

2. Select **9300CB.**

3. Slide the "**Control Slide-Bar**" to select the device as a Control Device

4. Slide the "**Border Slide-Bar**" to select the device as a Border Device

5. Configure the L3 Handoff Parameters based on the above information. Border L3Handoff Configuration Parameters:

6. Configure the device as a "**Anywhere Border**" by clicking on "**Default to all Virtual Networks**" and Unchecking "**Do not import External Routes**".

7. Configure the L3 Handoff pool as "**L3HANDOFF-POOL**" and click "**Add**".

8. Select "**L3HANDOFF**" and Click "**Add**" to add the Interface "**G 1/0/1**" as the transit interface towards the Fusion Router.

9. Select all the VNs (**INFRA_VN, IT_VN,SALES_VN**)

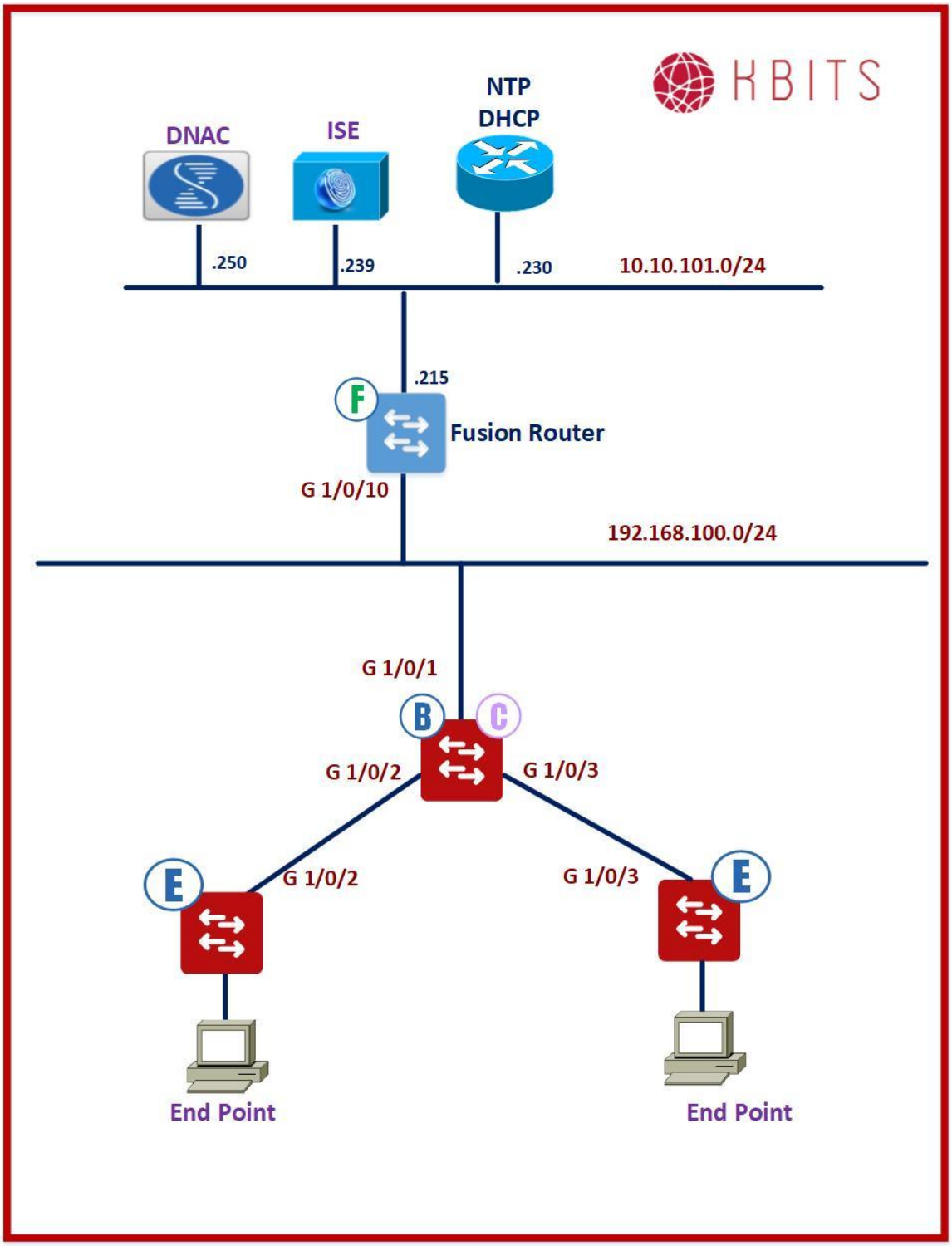
10. Click **Save** & **Add**.

11. Click **Add**.

12. Click **Save**.

13. The Device should turn **Blue** indicating that it is in the Fabric

Lab 6 – Provision the Edge Devices



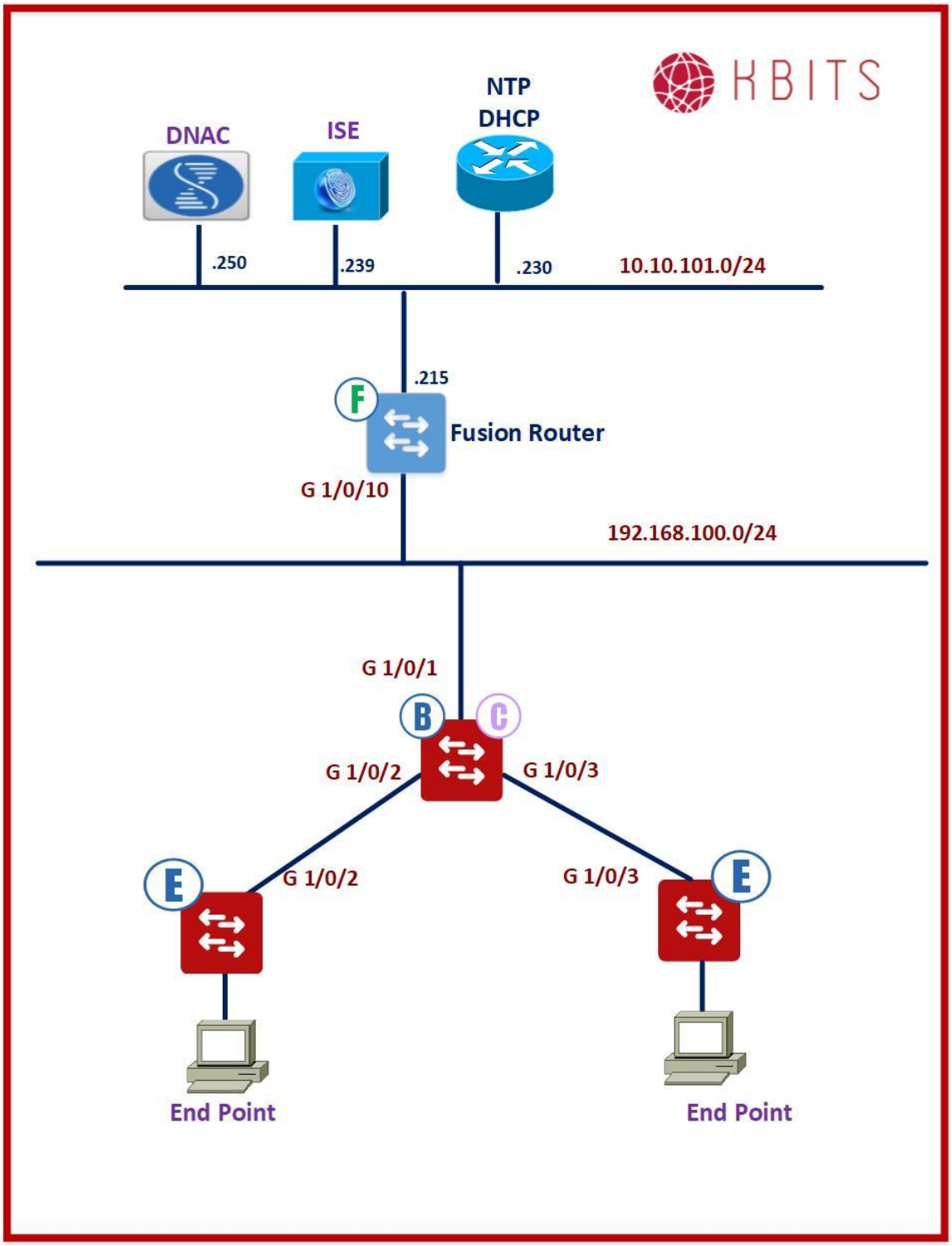
Task 1

Provision the **9300E1** & **9300E2** devices as the **Fabric Eges** Devices.

DNAC

1. Browse to "**Fabric -> HQ_FABRIC -> Los Angeles -> HQ**".
2. Select **9300E1**.
3. Slide the "**Edge Slide-Bar**" to select the device as an Edge Device
4. Click **Add**.
5. Select **9300E2**.
6. Slide the "**Edge Slide-Bar**" to select the device as an Edge Device
7. Click **Add**.
8. Click **Save**.
9. The Device should turn **Blue** indicating that it is in the Fabric

Lab 7 – Configure the Fusion Router to match the border configuration



Task 1

Configure the VRFs on the Fusion Router to match the Border Interfaces.

Fusion Router

```
vrf definition IT_VN
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family

!
vrf definition SALES_VN
 rd 1:4100
 !
 address-family ipv4
  route-target export 1:4100
  route-target import 1:4100
 exit-address-family
```

Task 2

Create the VLANs (**3001-3003**) and SVI to match the information of the Border Device. Make sure to change the IP Addresses to match Border BGP configuration regarding neighbor commands for BGP.

Fusion Router

```
vlan 3001-3003
!!! You need to enable VTP Transparent Mode to make it work
!
interface Vlan3001
 description vrf interface to External router
 ip address 172.20.1.2 255.255.255.252
 no shut
!
interface Vlan3002
 description vrf interface to External router
 vrf forwarding IT_VN
 ip address 172.20.1.6 255.255.255.252
 no shut
!
interface Vlan3003
 description vrf interface to External router
 vrf forwarding SALES_VN
 ip address 172.20.1.10 255.255.255.252
 no shut
```

Task 3

Create BGP on the Fusion Router to reciprocate the BGP Configuration on the Border. Fusion needs to advertise the **10.10.101.0/24** network and default gateway in the **Global** Routing Table, **IT_VN** and the **SALES_VN** VRF.

Fusion Router

```
router bgp 65001
 neighbor 172.20.1.1 remote-as 65002
 neighbor 172.20.1.1 update-source Vlan3001
 !
 address-family ipv4
  neighbor 172.20.1.1 activate
  neighbor 172.20.1.1 default-originate
  network 10.10.101.0 mask 255.255.255.0
!
 address-family ipv4 vrf SALES_VN
  neighbor 172.20.1.9 remote-as 65002
  neighbor 172.20.1.9 update-source Vlan3003
  neighbor 172.20.1.9 activate
  neighbor 172.20.1.9 default-originate
  network 10.10.101.0 mask 255.255.255.0
!
address-family ipv4 vrf IT_VN
  neighbor 172.20.1.5 remote-as 65002
  neighbor 172.20.1.5 update-source Vlan3002
  neighbor 172.20.1.5 activate
  neighbor 172.20.1.5 default-originate
  network 10.10.101.0 mask 255.255.255.0
```

Task 4

Configure Route Leaking to leaking the **10.10.101.0/24** Global Routing Table route into the **IT_VN** & **SALES_VN** VRFs.

Fusion Router

```
ip prefix-list GLOBAL seq 5 permit 10.10.101.0/24
!
route-map GLOBAL permit 10
 match ip address prefix-list GLOBAL
!
vrf definition IT_VN
 address-family ipv4
  import ipv4 unicast map GLOBAL
!
vrf definition SALES_VN
 address-family ipv4
  import ipv4 unicast map GLOBAL
```

Task 5

Use static routing to leak the VRF Routes for the **IT_VN** & **SALES_VN** VRFs into the Global Routing Table.

Fusion Router

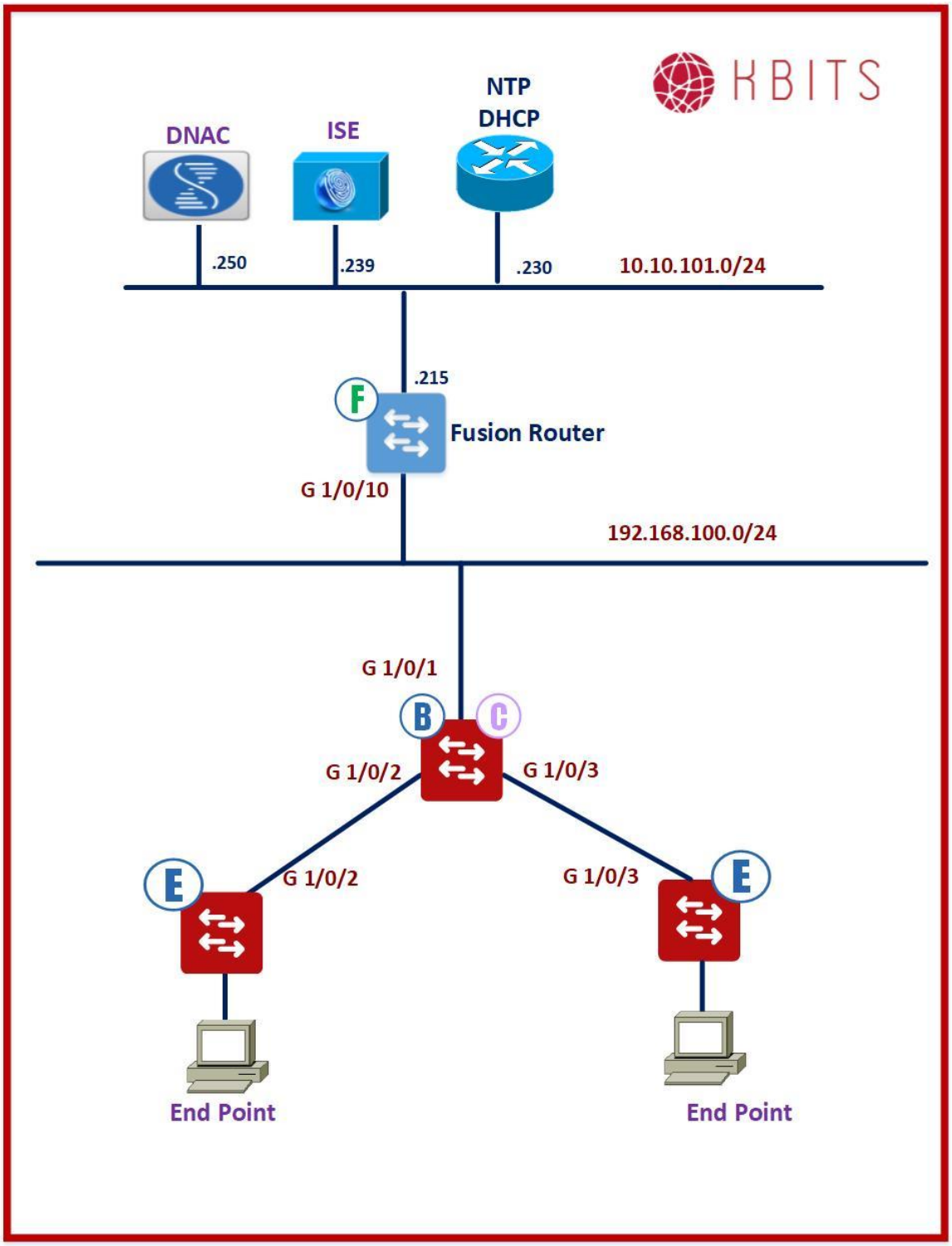
```
ip route 172.16.1.0 255.255.255.0 Vlan3002
ip route 172.16.2.0 255.255.255.0 Vlan3002
ip route 172.16.101.0 255.255.255.0 Vlan3002
ip route 172.20.1.4 255.255.255.252 Vlan3002
!
ip route 172.16.3.0 255.255.255.0 Vlan3003
ip route 172.16.4.0 255.255.255.0 Vlan3003
ip route 172.16.102.0 255.255.255.0 Vlan3003
ip route 172.20.1.8 255.255.255.252 Vlan3003
```

CCIE Security v6 – Software Defined Access (SDA)

Module 5 – Configuring ISE for SDA

Module 5 – Configuring ISE for SDA

Lab 1 – Configure User & Groups on ISE



Task 1

Configure the following User Identity groups on ISE.

- Name: **IT-DATA-1**
- Name: **IT-DATA-2**
- Name: **IT-VOICE**
- Name: **SALES-DATA-1**
- Name: **SALES-DATA-2**
- Name: **SALES-VOICE**

ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Administration -> Identity Management -> Groups -> User Identity Groups -> Create"**

3. Create the User Identity Groups based on the above Parameters.

4. Click **Save.**

Task 2

Create Users on ISE and assign them to the appropriate groups based on the following:

- Name: **IT1**
  - Password: **Cisco@123**
  - Group: **IT-DATA-1**

- Name: **IT2**
  - Password: **Cisco@123**
  - Group: **IT-DATA-2**

- Name: **SALES1**
  - Password: **Cisco@123**
  - Group: **SALES-DATA-1**

- Name: **SALES2**
  - Password: **Cisco@123**
  - Group: **SALES-DATA-2**

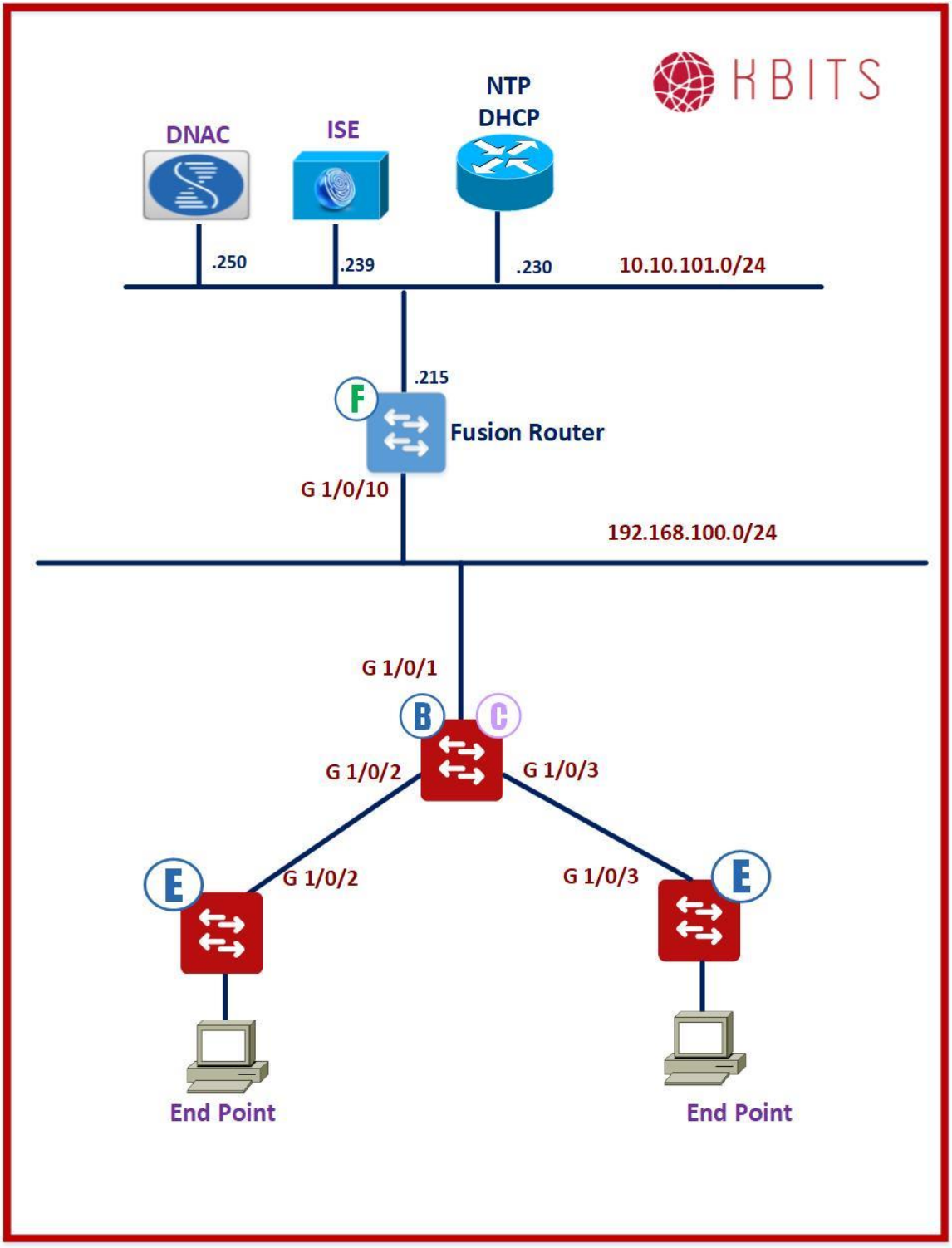
ISE

1. Browse to "**Administration -> Identity Management -> Identities -> Create**"

2. Create the Identities based on the above parameters.

3. Click **Save.**

Lab 2 – Configure Authorization Profiles for the DNAC VNs



Task 1

Configure the Authorization Profiles on ISE to link the Authorization Profile name in DNAC for the VNs & Pools. Use the following information for the creation of the Authorization Profiles.

- Name: **IT-DATA-1-PROF**
- VLAN: **IT-DATA-1** (**Copy from DNAC**)

- Name: **IT-DATA-2-PROF**
- VLAN: **IT-DATA-2** (**Copy from DNAC**)

- Name: **SALES-DATA-1-PROF**
- VLAN: **SALES-DATA-1** (**Copy from DNAC**)

- Name: **SALES-DATA-2-PROF**
- VLAN: **SALES-DATA-2** (**Copy from DNAC**)

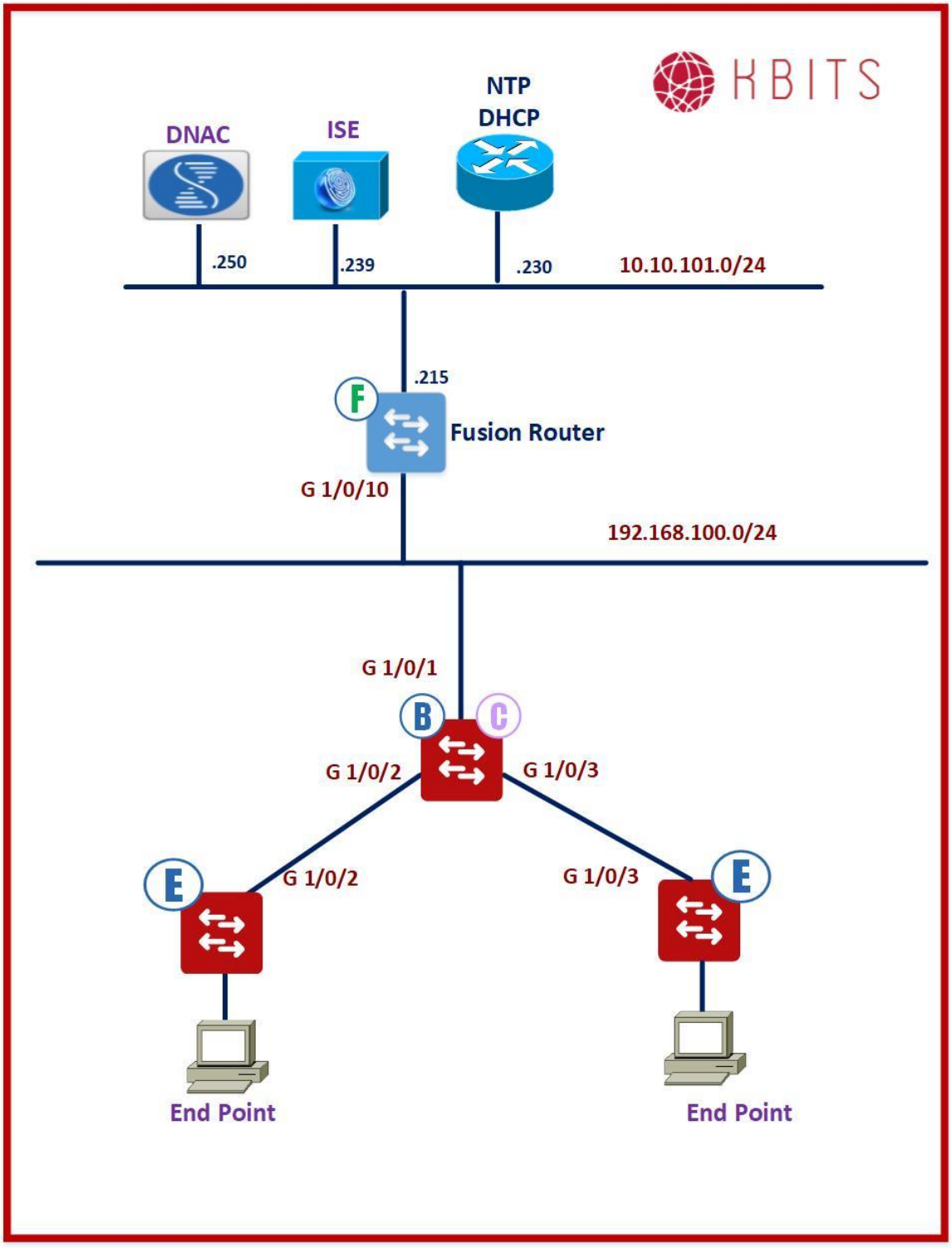
ISE

1. Browse to "**Policy -> Policy Elements -> Results -> Authorization -> Authorization Profile -> Create**"

2. Create the Authorization Profiles based on the above parameters.

3. Click **Save.**

Lab 3 – Configure Authorization Policies for the DNAC VNs



Task 1

Configure the Authorization Policies on ISE to link the Authorization Profile to the the Identity Groups for the Users for 802.1x authentication. Use the following information for the creation of the Authorization Policies.

- Name: **IT-DATA-1-POLICY**
- Identity Group: **IT-DATA-1**
- Authentication Method: **Wired_802.1x**
- Permission: **IT-DATA-1-PROF**

- Name: **IT-DATA-2-POLICY**
- Identity Group: **IT-DATA-2**
- Authentication Method: **Wired_802.1x**
- Permission: **IT-DATA-2-PROF**

- Name: **SALES-DATA-1-POLICY**
- Identity Group: **SALES-DATA-1**
- Authentication Method: **Wired_802.1x**
- Permission: **SALES-DATA-1-PROF**

- Name: **SALES-DATA-2-POLICY**
- Identity Group: **SALES-DATA-2**
- Authentication Method: **Wired_802.1x**
- Permission: **SALES-DATA-2-PROF**

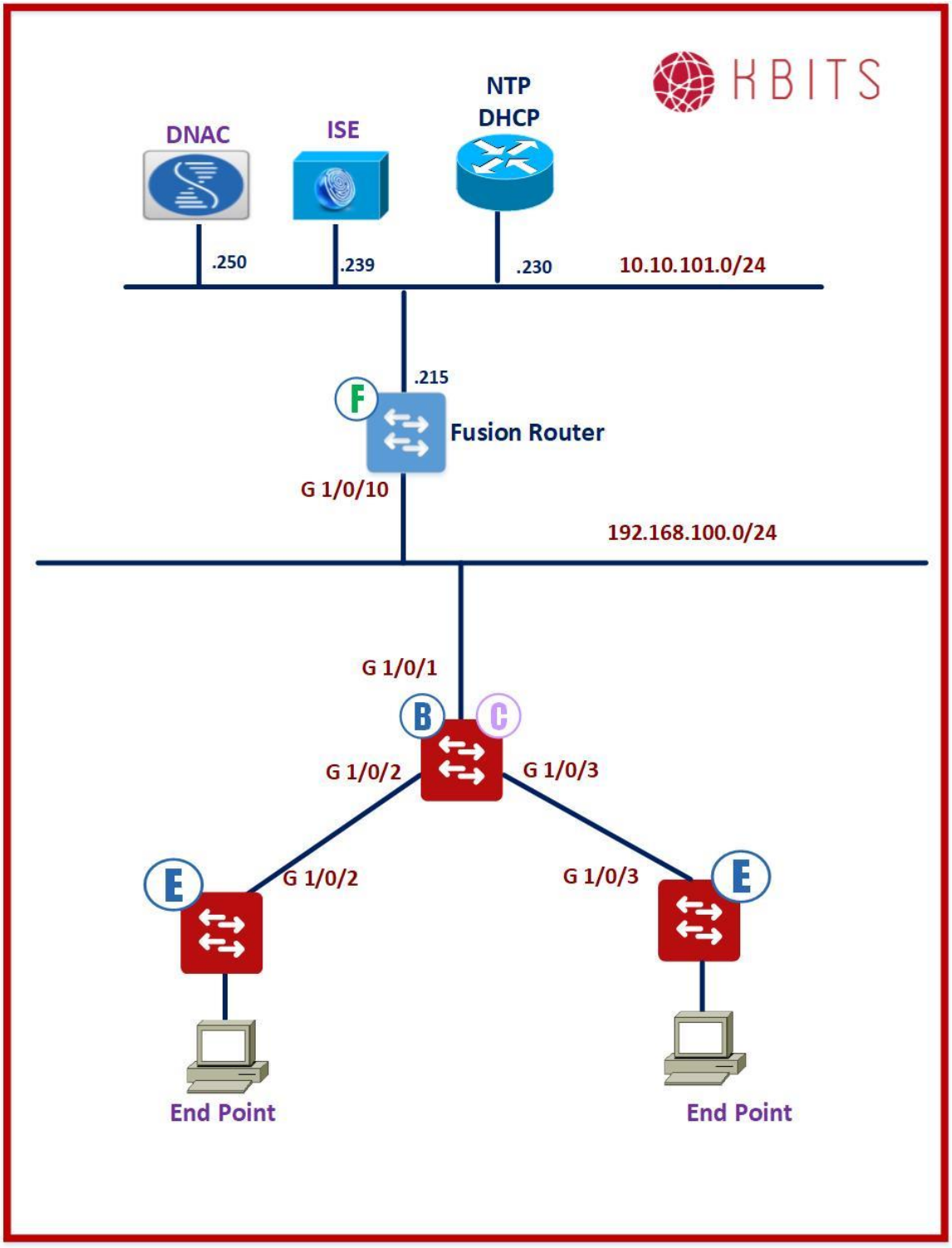
ISE

1. Browse to "**Policy -> Policy Sets -> default -> Authorization Policies -> Insert at the Top"**

2. Create the Authorization Policies based on the above parameters.

3. Click **Save.**

Lab 4 – Configure the DHCP Server to provide IP Configuration to Clients



Task 1

Configure the Access Server as a DHCP Server for the Clients. Configure the Pools based on the following parameters:

- Name: **IT_DATA1**
- Exclusions: **172.16.1.1-172.16.1.100 & 172.16.1.254**
- Network: **172.16.1.0 /24**
- Default Router: **172.16.1.254**

- Name: **IT_DATA2**
- Exclusions: **172.16.2.1-172.16.2.100 & 172.16.2.254**
- Network: **172.16.2.0 /24**
- Default Router: **172.16.2.254**

- Name: **SALES_DATA1**
- Exclusions: **172.16.3.1-172.16.3.100 & 172.16.3.254**
- Network: **172.16.3.0 /24**
- Default Router: **172.16.3.254**

- Name: **SALES_DATA2**
- Exclusions: **172.16.4.1-172.16.4.100 & 172.16.4.254**
- Network: **172.16.4.0 /24**
- Default Router: **172.16.4.254**

Access Server

```
ip dhcp excluded-address 172.16.1.1 172.16.1.100
ip dhcp excluded-address 172.16.2.1 172.16.2.100
ip dhcp excluded-address 172.16.3.1 172.16.3.100
ip dhcp excluded-address 172.16.4.1 172.16.4.100
!
 ip dhcp pool IT_DATA1
   network 172.16.1.0 255.255.255.0
   default-router 172.16.1.254
!
ip dhcp pool IT_DATA2
   network 172.16.2.0 255.255.255.0
   default-router 172.16.2.254
!
ip dhcp pool SALES_DATA1
   network 172.16.3.0 255.255.255.0
   default-router 172.16.3.254
!
ip dhcp pool SALES_DATA2
   network 172.16.4.0 255.255.255.0
   default-router 172.16.4.254
```

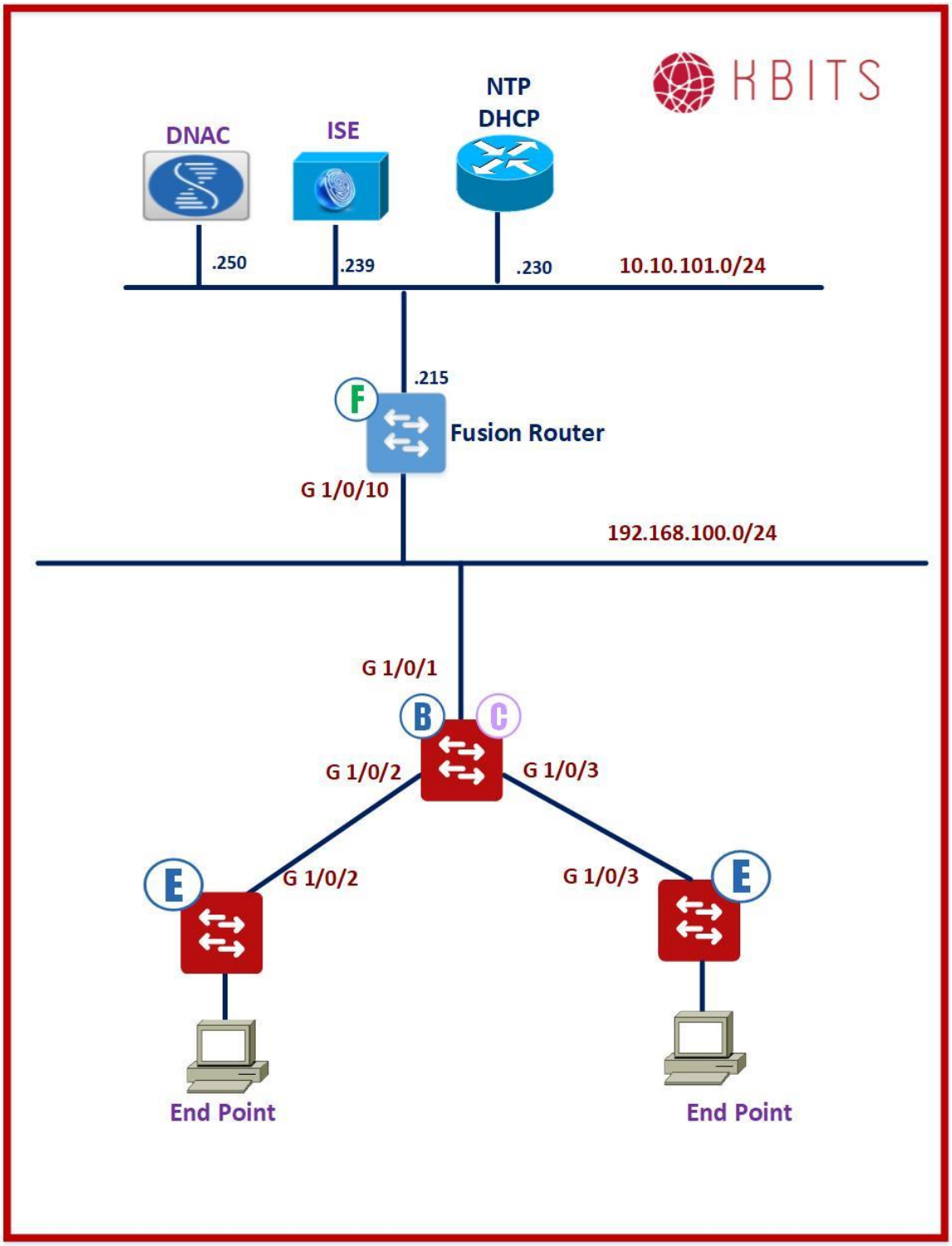
Task 2

Configure Static Routers on the Access Server to Access the 2 Fabric Networks, 172.16.0.0/16 & 172.16.20.0/24.

Access Server

```
ip route 172.16.0.0 255.255.0.0 10.10.101.215
ip route 172.20.0.0 255.255.0.0 10.10.101.215
```

Lab 5 – Verifying Macro Segmentation



Task 1

Log into End-Point # 1 & End-Point # 2 using IT1 & IT2 users respectively. The 2 Endpoints should be able to communicate to each other as they are in the same VN.

End Point # 1 1. Configure the Native Windows supplicant on **End Point # 1** to log in using **IT1/Cisco@123** credentials.
End Point # 2 1. Configure the Native Windows supplicant on **End Point # 2** to log in using **IT2/Cisco@123** credentials.
Verification: They should be in 2 different subnets but should be able to communicate to each other. Use Ipconfig to figure out the IPs. Use Ping to verify connectivity.

Task 2

Log into End-Point # 2 using SALES1 user. The 2 Endpoints should NOT be able to communicate to each other as they are in 2 different VNs.

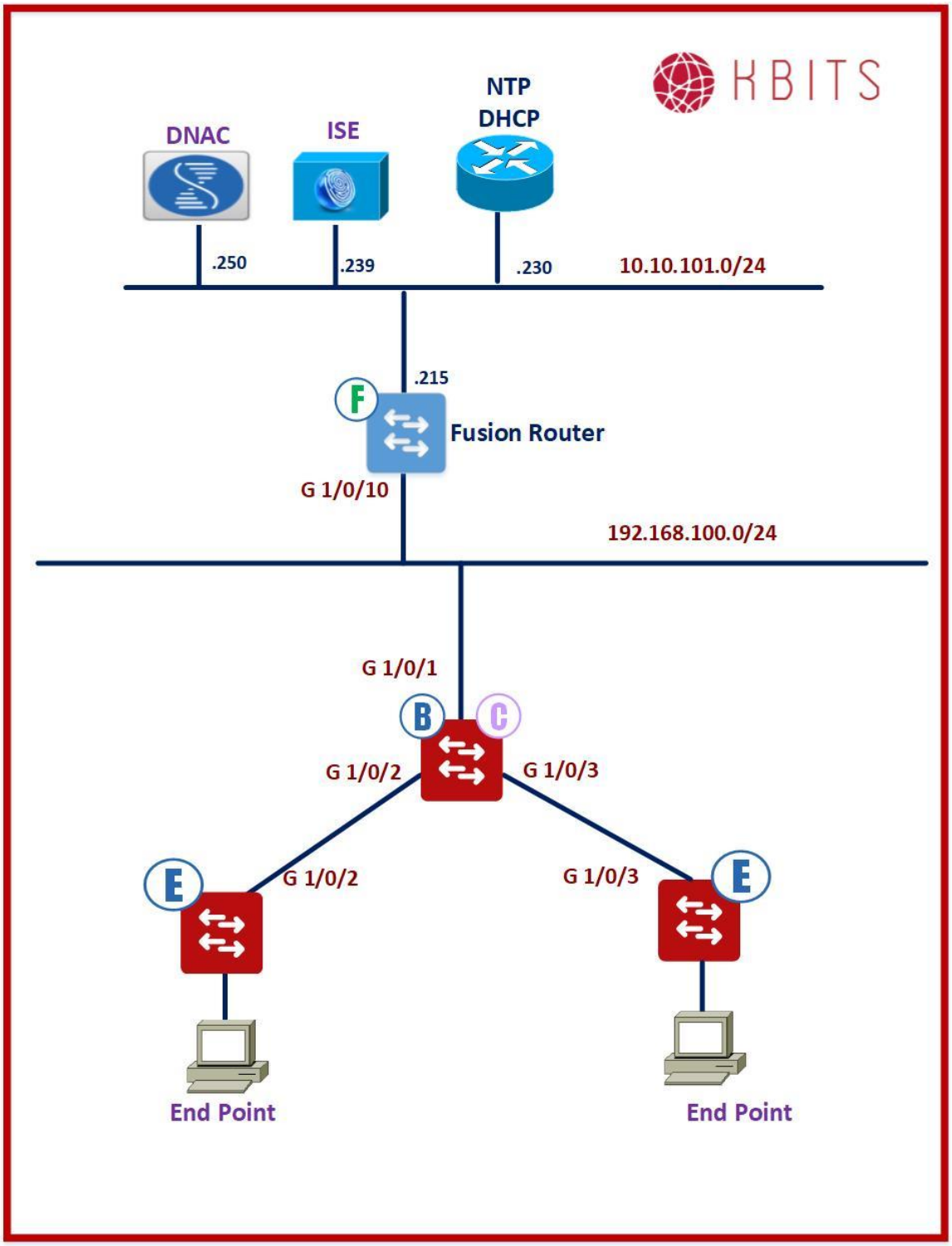
End Point # 2 1. Configure the Native Windows supplicant on **End Point # 2** to log in using **SALES1/Cisco@123** credentials.
Verification: They should be in 2 VNs. They should NOT be able to communicate to each other. Use Ipconfig to figure out the IPs. Use Ping to verify that they are not communicating to each other.

CCIE Security v6 – Software Defined Access (SDA)

Module 6 – Configuring Micro-Segmentation

Module 6 – Configuring Micro-Segmentation

Lab 1 – Create the SGTs



Task 1

Create 2 Security Group Tags (SGT) that will be used for IT-DATA-1 & IT-DATA-2 subnets. Create the SGTs based on the following:

- Name: **IT-DATA-1**
- SGT: **6001**
- VN: **IT_VN**

- Name: **IT-DATA-2**
- SGT: **6002**
- VN: **IT_VN**

DNAC

1. Log into DNAC using the **admin/Cisco@123** as the credentials.

2. Browse to "**Policy -> Group Based Access Control -> Scalabe Groups -> Create"**

3. Create the SGTs based on the above parameters.

4. Click **Save.**

Task 2

Verify the propagation of the SGTs to ISE.

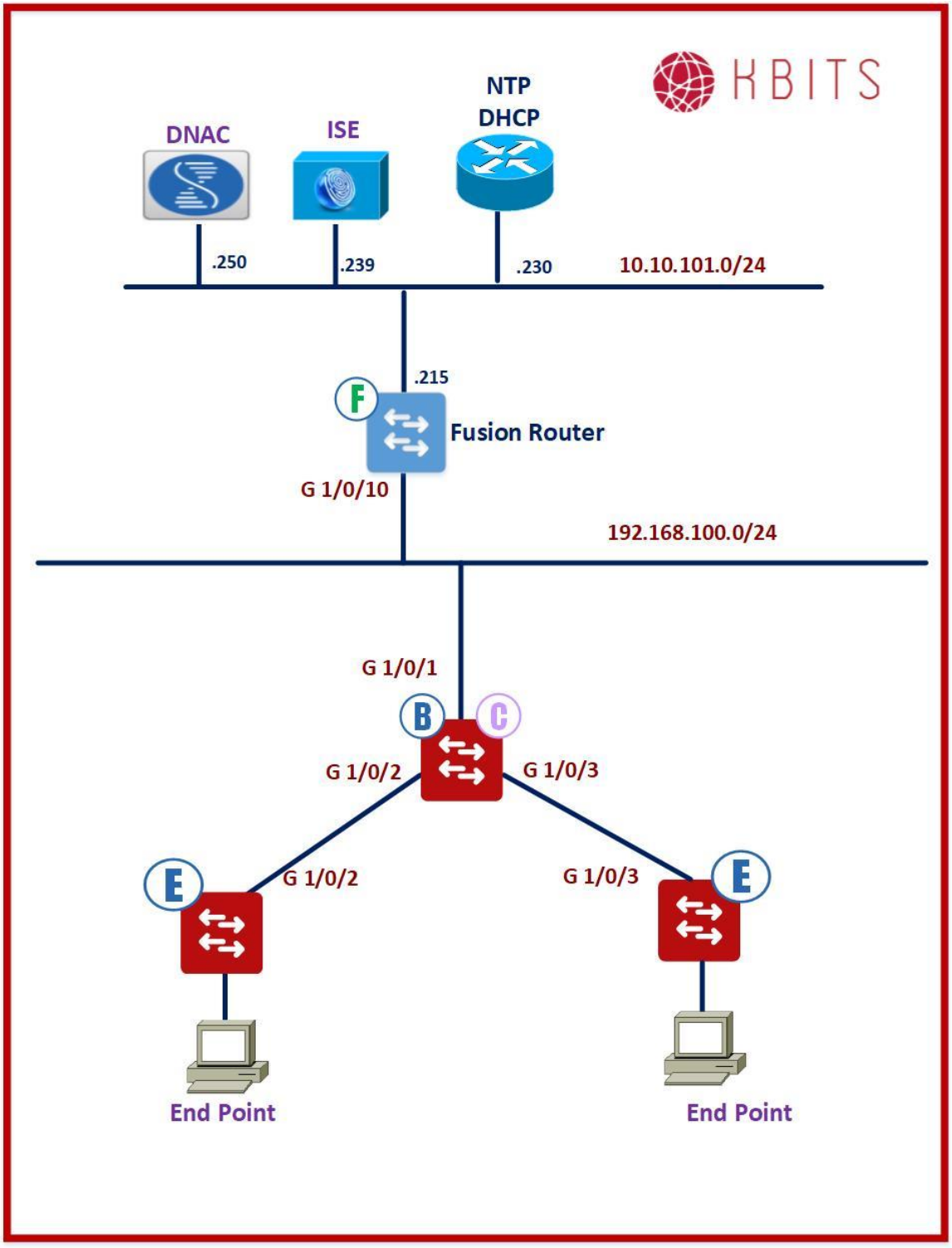
ISE

1. Log into ISE using the **admin/Kbits@123** as the credentials.

2. Browse to "**Work Centers -> TrustSe -> Components -> Security Groups**".

3. The **IT-DATA-1** & **IT-DATA-2** SGTs should be available in ISE

Lab 2 – Re-configure ISE Authorization Policies to use SGTs



Task 1

Re-configure the Authorization Policies to assign the IT-DATA-1 & IT-DATA-2 Groups appropriate SGT in addition to the Authorization profiles.

- Name: **IT-DATA-1-POLICY**
- Identity Group: **IT-DATA-1**
- Authentication Method: **Wired_802.1x**
- Permission: **IT-DATA-1-PROF**
- Security Group: **IT-DATA-1**

- Name: **IT-DATA-2-POLICY**
- Identity Group: **IT-DATA-2**
- Authentication Method: **Wired_802.1x**
- Permission: **IT-DATA-2-PROF**
- Security Group: **IT-DATA-2**

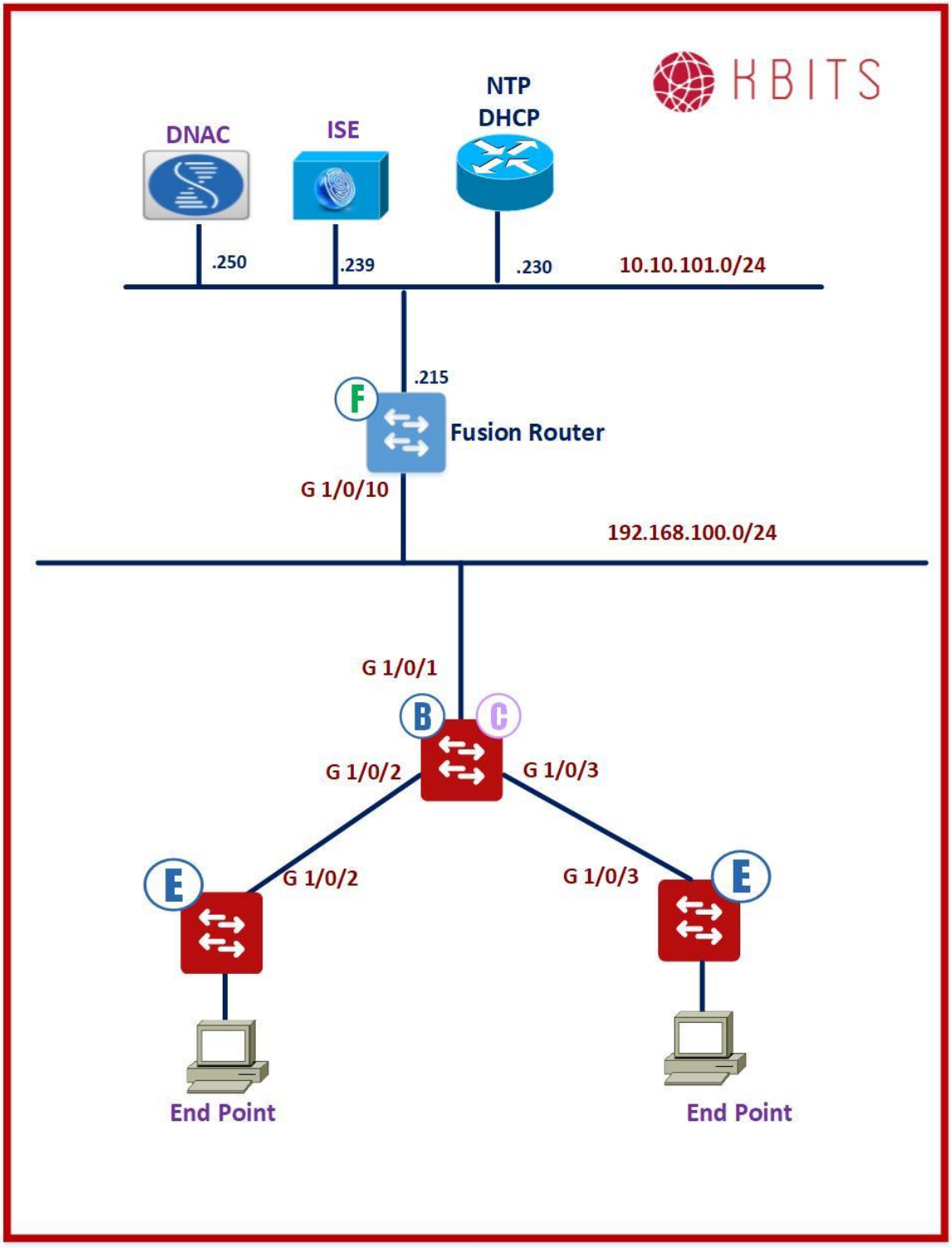
ISE

1. Browse to "**Policy -> Policy Sets -> default -> Authorization Policies"**

2. Edit the above policies and add the SGTs.

3. Click **Save**.

Lab 3 – Using a default contract to block all communications between SGTs



Task 1

Configure the SG Access Contract such that all traffic from **IT-DATA-1** to **IT-DATA-2** gets denied using the built-in Deny IP contract.

- Name: **IT-DATA-1-POLICY**
- Identity Group: **IT-DATA-1**
- Authentication Method: **Wired_802.1x**
- Permission: **IT-DATA-1-PROF**
- Security Group: **IT-DATA-1**

- Name: **IT-DATA-2-POLICY**
- Identity Group: **IT-DATA-2**
- Authentication Method: **Wired_802.1x**
- Permission: **IT-DATA-2-PROF**
- Security Group: **IT-DATA-2**

DNAC

1. Browse to "**Policy -> Group-Based Access Control -> Access Contracts -> Create Access Contact**".

2. Click on the "**Policy Matrix**" box that intersects **IT-DATA-1** & **IT-DATA-2**.

3. Click "**Change Contract**".

4. Select "**Deny IP**".

5. Click "**Change**".

6. Click **Save**.

7. Click **Đeploy** to implement the policy.

Task 2

Log into End-Point # 1 & End-Point # 2 using IT1 & IT2 users respectively. The 2 Endpoints should NOT to be able to communicate to each other although they are part of the same VN (IT_VN).

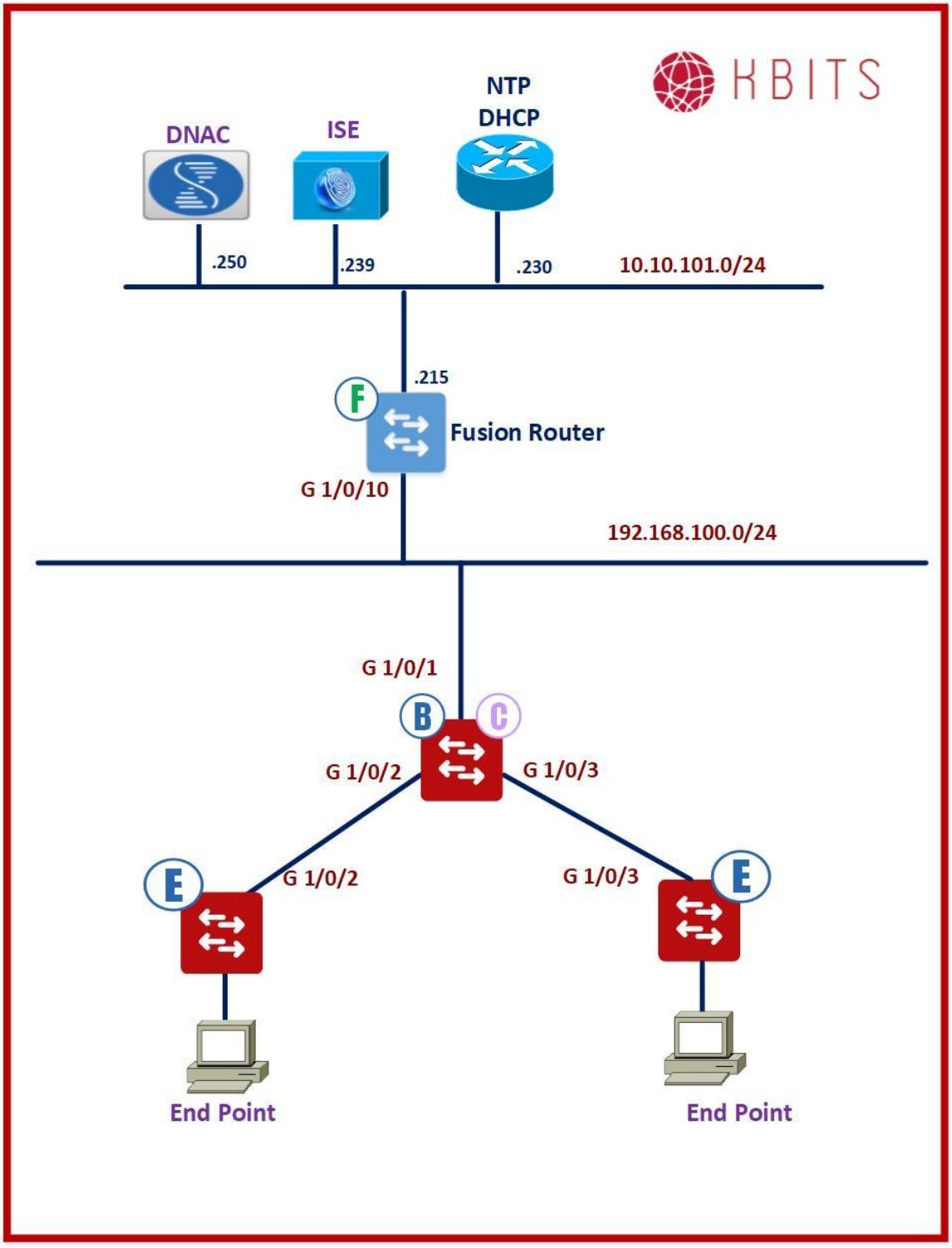
End Point # 1

1. Configure the Native Windows supplicant on **End Point # 1** to log in using **IT1/Cisco@123** credentials.

End Point # 2

1. Configure the Native Windows supplicant on **End Point # 2** to log in using **IT2/Cisco@123** credentials.
Verification: 1. Verify that the SG ACL is applied on the Egress Switch (9300E2) using the "**show cts role-based-permissions**" command. 2. Ping **ES2** from **ES1**. The ping should not work.

Lab 4 – Creating a Custom SG ACL Contracts to Control Traffic



Task 1

Remove the Contract between IT-DATA1 & IT-DATA2 by setting it back to default.

DNAC

1. Browse to "**Group-Based Access Control -> Policies**".

2. Click on the "**Policy Matrix**" box that intersects **IT-DATA-1** & **IT-DATA-2**.

3. Click "**Set it Default:Permit IP**"

4. Click **Change**.

5. Click **Save**.

6. Click **Ðeploy** to implement the policy.

Task 2

Create a Custom SG ACL (Access Contract) to block the following traffic from IT-DATA1 to IT-DATA2 based on the following:

- Name: **IT-DATA-1-TO-IT-DATA-2**
- Rules:
  - Permit – **TCP/80**
  - Permit – **TCP/443**
  - Permit – **CIFS**
  - Default Action: **Deny**

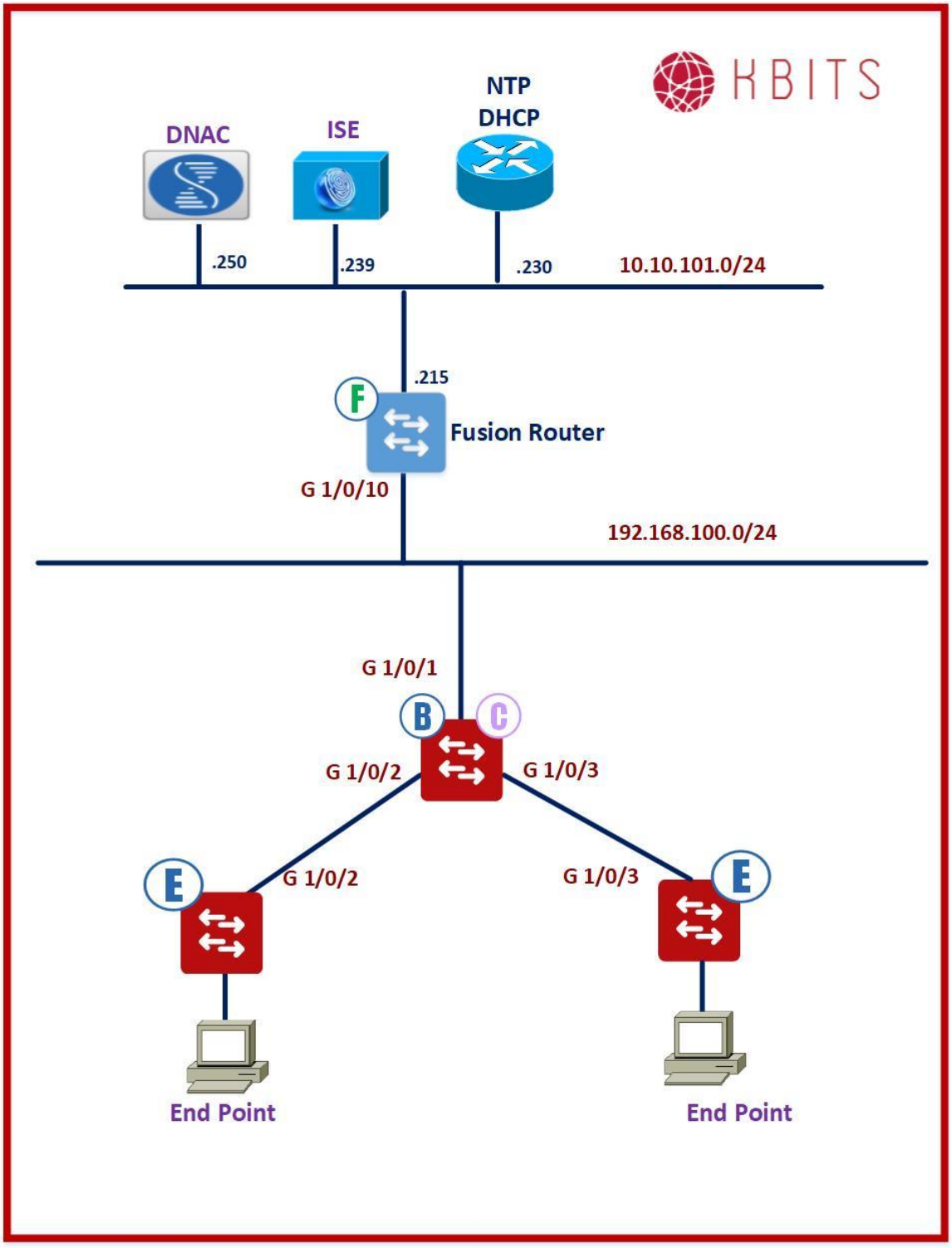
DNAC

1. Browse to "**Policy -> Group-Based Access Control -> Access Contracts -> Create Access Contracts**".

2. Create a SG ACL (Access Contract) based on the above parameters.

3. Click **Save**.

Lab 5 – Applying and verifying a Custom SG ACL- Contract



Task 1

Assign the SG Access Contract created in the previous lab to control traffic between the IT-DATA-1 & IT-DATA-2 SGTs.

DNAC
1. Browse to "**Group-Based Access Control -> Policies**". 2. Click on the "**Policy Matrix**" box that intersects **IT-DATA-1** & **IT-DATA-2**. 3. Click on "**Change Contract**" 4. Select "**IT-DATA-1-TO-IT-DATA-2**" contract. 5. Click **Change**. 6. Click **Ðeploy** to implement the policy.

Task 2

Log into End-Point # 1 & End-Point # 2 using IT1 & IT2 users respectively. Make sure that the IT1 can access IT2's shared folder. They should not be able to Ping each other.

End Point # 1
1. Configure the Native Windows supplicant on **End Point # 1** to log in using **IT1/Cisco@123** credentials.
End Point # 2
1. Configure the Native Windows supplicant on **End Point # 2** to log in using **IT2/Cisco@123** credentials.
Verification: 1. Verify that the **SG ACL** is applied on the Egress Switch (9300E2) using the "**show cts role-based-permissions**" command. 2. Ping **ES2** from **ES1**. The ping should not work. 3. Browse to a shared folder on **ES2**. It should work.