

Fortinet NSE 4 NSE4 FGT-6.4 Exam Updated Dumps

below, you can study them to prepare this NSE4_FGT-6.4 NSE 4 exam.

1.The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.

What order must FortiGate use when the web filter profile has features enabled, such as safe search?

- A. DNS-based web filter and proxy-based web filter
- B. Static URL filter, FortiGuard category filter, and advanced filters
- C. Static domain filter, SSL inspection filter, and external connectors filters
- D. FortiGuard category filter and rating filter

Answer: B

Explanation:

Reference: https://fortinet121.rssing.com/chan-67705148/all_p1.html

2.Refer to the exhibit.



Review the Intrusion Prevention System (IPS) profile signature settings.

Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.

Answer: D

3.View the exhibit.

Application Details

Name	Category	Technology	Popularity	Risk
Addicting Games	Game	Browser-Based	☆☆☆☆☆	Risk

Application Control Profile

Categories

- All Categories
- Business (149, 6)
- Email (80, 13)
- Industrial (1168)
- P2P (70)
- Social.Media (120, 31)
- Video/Audio (164, 14)
- Unknown Applications
- Cloud.IT (42)
- Game (83)
- Mobile (3)
- Proxy (148)
- Storage.Backup (175, 17)
- VoIP (27)
- Collaboration (274, 10)
- General.Interest (233, 6)
- Network.Service (325)
- Remote.Access (84)
- Update (49)
- Web.Client (22)

Application Overrides

Application Signature	Category	Action
Addicting Games	Game	Allow

Filter Overrides

Filter Details	Action
Risk (2304, 52)	Block

A user behind the FortiGate is trying to go to <http://www.addictinggames.com> (Addicting Games). Based on this configuration, which statement is true?

A. Addicting.Games is allowed based on the Application Overrides configuration.

B. Addicting.Games is blocked on the Filter Overrides configuration.

C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.

D. Addicting.Games is allowed based on the Categories configuration.

Answer: A

4.Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {
  if (shExpMatch (url, "*.fortinet.com/*")) {
    return "DIRECT";}
  if (isInNet (host, "172.25.120.0", "255.255.255.0")) {
    return "PROXY altproxy.corp.com: 8060";}
  return "PROXY proxy.corp.com: 8090";
}
```

Which of the following statements are true? (Choose two.)

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25.120.0/24 subnet is allowed to bypass the proxy.

C. All requests not made to Fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.

D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: A,D

5.To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

A. FortiManager

B. Root FortiGate

C. FortiAnalyzer

D. Downstream FortiGate

Answer: B

6.Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1, 10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)

A. The debug flow is of ICMP traffic.

B. A firewall policy allowed the connection.

C. A new traffic session is created.

D. The default route is required to receive a reply.

Answer: B

7.Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

A. To allow for out-of-order packets that could arrive after the FIN/ACK packets










B. To finish any inspection operations










C. To remove the NAT operation

D. To generate logs

Answer: A

8.View the exhibit.

Destination 	<div>Subnet Named Address Internet Service</div> <div>172.13.24.0/255.255.255.0 </div>
Interface	<div> TunnelB </div>
Administrative Distance 	<div>5</div>
Comments	<div></div> 0/255
Status	<div> Enabled  Disabled</div>
<div> Advanced Options</div>	
Priority 	<div>30</div>

Destination 	<div>Subnet Named Address Internet Service</div> <div>172.13.24.0/255.255.255.0 </div>
Interface	<div> TunnelA </div>
Administrative Distance 	<div>10</div>
Comments	<div></div> 0/255
Status	<div> Enabled  Disabled</div>
<div> Advanced Options</div>	
Priority 	<div>0</div>

Which of the following statements are correct? (Choose two.)

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
- D. This is a redundant IPsec setup.

Answer: C,D

9.An administrator must disable RPF check to investigate an issue.

Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

- A. Enable asymmetric routing, so the RPF check will be bypassed.
- B. Disable the RPF check at the FortiGate interface level for the source check.
- C. Disable the RPF check at the FortiGate interface level for the reply check.
- D. Enable asymmetric routing at the interface level.

Answer: D

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955>

10.Examine this FortiGate configuration:

```
config system global
    set av-failopen pass
end
```

Examine the output of the following debug command:

```
# diagnose hardware sysinfo conserve
memory conserve mode: on
total RAM: 3040 MB
memory used: 2948 MB 97% of total RAM
memory freeable: 92 MB 3% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red: 2675 MB 88% of total RAM
memory used threshold green: 2492 MB 82% of total RAM
```

Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

- A. It is allowed, but with no inspection
- B. It is allowed and inspected as long as the inspection is flow based
- C. It is dropped.
- D. It is allowed and inspected, as long as the only inspection required is antivirus.

Answer: C

11.Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiCache
- B. FortiSIEM
- C. FortiAnalyzer
- D. FortiSandbox
- E. FortiCloud

Answer: B,C,E

12.Which two VDOMs are the default VDOMs created when FortiGate is set up in split VDOM mode? (Choose two.)

- A. FG-traffic
- B. Mgmt
- C. FG-Mgmt
- D. Root

Answer: A,D

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/758820/split-task-vdom-mode>

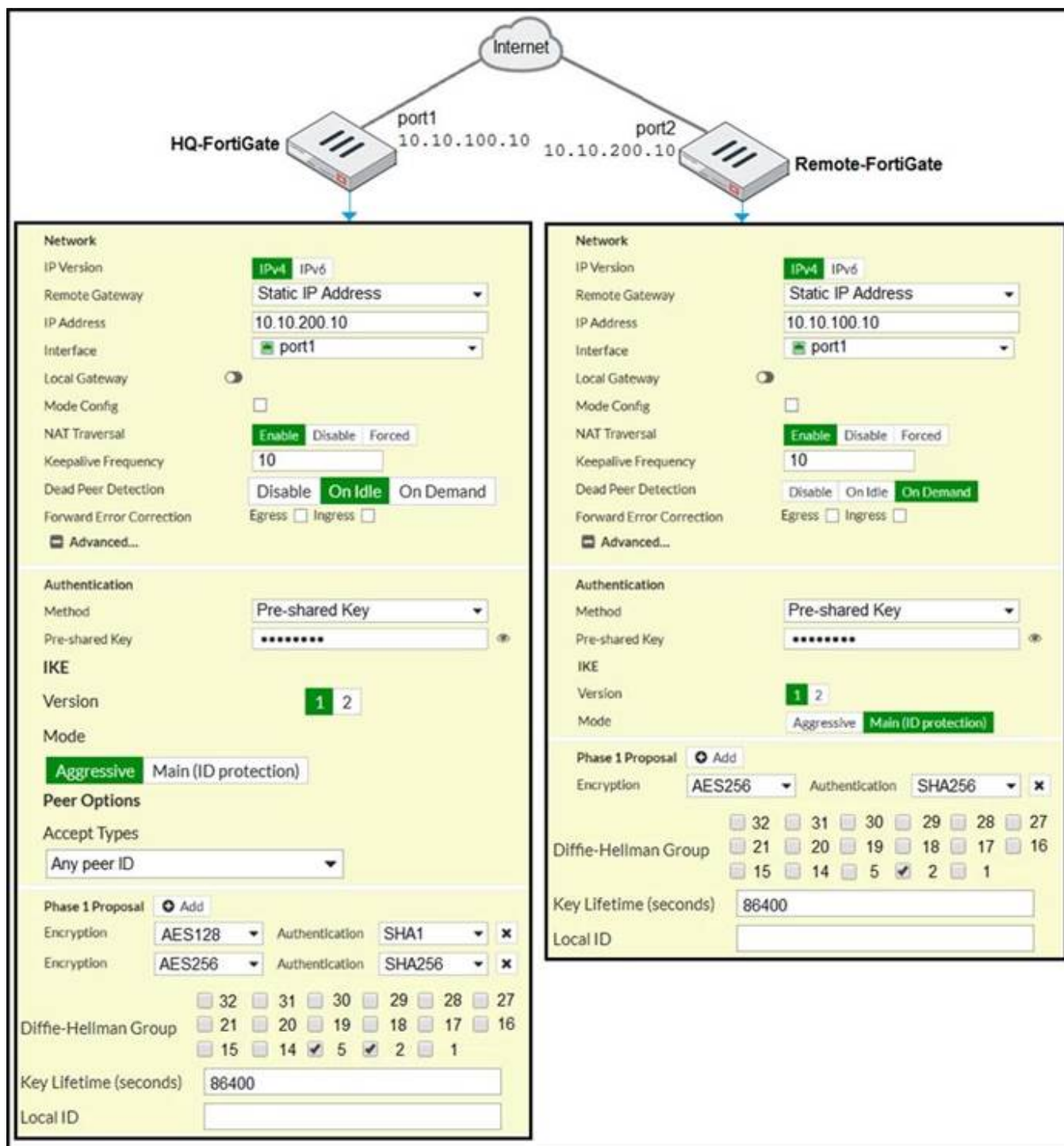
13.In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies.

Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

- A. The IP version of the sources and destinations in a firewall policy must be different.
- B. The Incoming Interface. Outgoing Interface. Schedule, and Service fields can be shared with both IPv4 and IPv6.
- C. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
- D. The IP version of the sources and destinations in a policy must match.
- E. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: A,C,E

14.Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to Main (ID protection).
- B. On both FortiGate devices, set Dead Peer Detection to On Demand.
- C. On HQ-FortiGate, disable Diffie-Helmann group 2.

D. On Remote-FortiGate, set port2 as Interface.

Answer: AD

15. Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

- A. FortiGuard web filter cache
- B. FortiGate hostname
- C. NTP
- D. DNS

Answer: C,D

16. Which two statements are correct about SLA targets? (Choose two.)

- A. You can configure only two SLA targets per one Performance SLA.
- B. SLA targets are optional.
- C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
- D. SLA targets are used only when referenced by an SD-WAN rule.

Answer: B ,C

17. Refer to the exhibit, which contains a static route configuration.

Edit Static Route

Destination ⓘ Subnet Internet Service
Amazon-AWS

Gateway Address 10.200.1.254

Interface port1

Comments Write a comment... 0/255

Status Enabled Disabled

An administrator created a static route for Amazon Web Services. What CLI command must the administrator use to view the route?

- A. get router info routing-table all
- B. get internet service route list
- C. get router info routing-table database
- D. diagnose firewall proute list

Answer: A

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/latest/administration-guide/139692/routing-concepts>

18. An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site

A, the local quick mode selector is 192.160.1.0/24 and the remote quick mode selector is 192.168.2.0/24.

Which subnet must the administrator configure for the local quick mode selector for site B?

A. 192.168.1.0/24

B. 192.168.0.0/24

C. 192.168.2.0/24

D. 192.168.3.0/24

Answer: C

19. Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A

Edit Policy

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

☒

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

☐

Protocol Options

PRX

default

Security Profiles

AntiVirus

☒

AV

default

Web Filter

☐

DNS Filter

☐

Application Control

☐

IPS

☐

SSL Inspection

☒

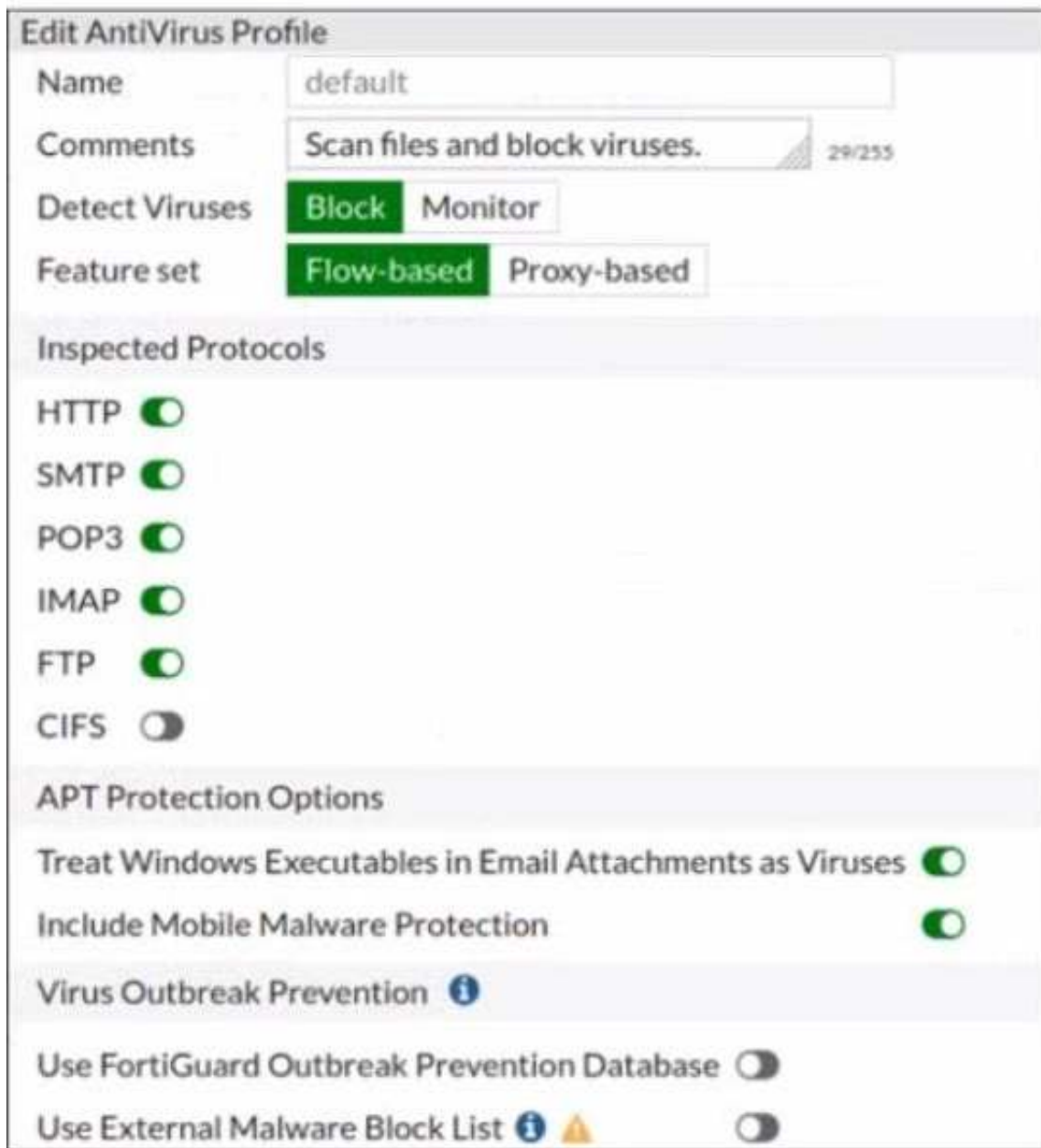
SSL

deep-inspection

Decrypted Traffic Mirror

☐

Exhibit B



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Detect Viruses: **Block** Monitor

Feature set: **Flow-based** Proxy-based

Inspected Protocols

- HTTP ☒
- SMTP ☒
- POP3 ☒
- IMAP ☒
- FTP ☒
- CIFS ☐

APT Protection Options

- Treat Windows Executables in Email Attachments as Viruses ☒
- Include Mobile Malware Protection ☒
- Virus Outbreak Prevention [i](#)
- Use FortiGuard Outbreak Prevention Database ☐
- Use External Malware Block List [i](#) [!](#) ☐

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: B

20. Which Security rating scorecard helps identify configuration weakness and

best practice violations in your network?

- A. Fabric Coverage
- B. Automated Response
- C. Security Posture
- D. Optimization

Answer: A

Explanation:

Reference: <https://www.fortinet.com/content/dam/fortinet/assets/support/fortinet-recommended-security-bestpractices.pdf>

21. An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.

What must an administrator do to achieve this objective?

- A. The administrator can register the same FortiToken on more than one FortiGate.
- B. The administrator must use a FortiAuthenticator device.
- C. The administrator can use a third-party radius OTP server.
- D. The administrator must use the user self-registration server.

Answer: B

22. Which two statements about antivirus scanning mode are true? (Choose two.)

- A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
- B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
- C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
- D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Answer: B,C

23. Which of the following are valid actions for FortiGuard category based filter in a web filter profile in proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

Answer: A,C

24.D18912E1457D5D1DDCBD40AB3BF70D5D

What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

- A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
- B. FortiGate automatically negotiates a new security association after the existing security association expires.
- C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
- D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

Answer: B

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=12069>

25.Which type of logs on FortiGate record information about traffic directly to and from the FortiGate management IP addresses?

- A. System event logs
- B. Forward traffic logs
- C. Local traffic logs
- D. Security logs

Answer: A

26.Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

- A. This is known as many-to-one NAT.
- B. Source IP is translated to the outgoing interface IP.
- C. Connections are tracked using source port and source MAC address.
- D. Port address translation is not used.

Answer: A,B

27.Refer to the exhibit.


```
STUDENT # get system session list
PROTO  EXPIRE  SOURCE          SOURCE-NAT      DESTINATION      DESTINATION-NAT
tcp     3598     10.0.1.10:2706  10.200.1.6:2706 10.200.1.254:80 -
tcp     3598     10.0.1.10:2704  10.200.1.6:2704 10.200.1.254:80 -
tcp     3596     10.0.1.10:2702  10.200.1.6:2702 10.200.1.254:80 -
tcp     3599     10.0.1.10:2700  10.200.1.6:2700 10.200.1.254:443 -
tcp     3599     10.0.1.10:2698  10.200.1.6:2698 10.200.1.254:80 -
tcp     3598     10.0.1.10:2696  10.200.1.6:2696 10.200.1.254:443 -
udp     174      10.0.1.10:2694  -                10.0.1.254:53 -
udp     173      10.0.1.10:2690  -                10.0.1.254:53 -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

- A. Destination NAT is disabled in the firewall policy.
- B. One-to-one NAT IP pool is used in the firewall policy.
- C. Overload NAT IP pool is used in the firewall policy.
- D. Port block allocation IP pool is used in the firewall policy.

Answer: A

28.View the exhibit:

▼ Status	▼ Name	▼ VLAN ID	▼ Type	▼ IP/Netmask
Physical(12)				
⊞	port1		Physical Interface	10.200.1.1 255.255.255.0
└	port1-VLAN1	1	VLAN	10.200.5.1 255.255.255.0
└	port1-VLAN10	10	VLAN	10.0.10.1 255.255.255.0
⊞	port2		Physical Interface	10.200.2.1 255.255.255.0
└	port2-VLAN1	1	VLAN	10.0.5.1 255.255.255.0
└	port2-VLAN10	10	VLAN	10.0.20.254 255.255.255.0
⊞	port3		Physical Interface	10.0.1.254 255.255.255.0

Which the FortiGate handle web proxy traffic rue? (Choose two.)

- A. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.
- B. port-VLAN1 is the native VLAN for the port1 physical interface.
- C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
- D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Answer: A,C

29.What devices form the core of the security fabric?

- A. Two FortiGate devices and one FortiManager device

- B. One FortiGate device and one FortiManager device
- C. Two FortiGate devices and one FortiAnalyzer device
- D. One FortiGate device and one FortiAnalyzer device

Answer: C

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/425100/components>

30. An administrator has configured a strict RPF check on FortiGate.

Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

Answer: A

31. Refer to the exhibit.

Authentication rule

Edit Rule		Authentication rule	
Name	WebproxyRule		
Source Address	LOCAL_SUBNET		
Protocol	HTTP		
Authentication Scheme	Web-Proxy-Scheme		
IP-based Authentication	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable		
SSO Authentication Scheme	<input type="checkbox"/>		
Comments	Write a comment. 0/1023		
Enable This Rule	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable		

Users

+ Create New	Edit	Delete	Search
Name	Type		
User-A	LOCAL		
User-B	LOCAL		
User-C	LOCAL		

Authentication scheme

Edit Authentication Scheme	
Name	Web-Proxy-Scheme
Method	Form-based
User database	<input checked="" type="radio"/> Local <input type="radio"/> Other
Two-factor authentication	<input type="checkbox"/>

Firewall address

Edit Address	
Category	Address Proxy Address
Name	LOCAL_SUBNET
Color	Change
Type	Subnet
IP/Netmask	10.0.1.0/24
Interface	any
Static route configuration	<input type="checkbox"/>
Comments	Write a comment. 0/255

Proxy address

Edit Address	
Category	Address Proxy Address
Name	Browser-CAT-1
Color	Change
Type	User Agent
Host	LOCAL_SUBNET
User Agent	Apple Safari Google Chrome Microsoft Internet Explorer or Spart
Comments	Write a comment. 0/255

Proxy address

Edit Address	
Category	Address Proxy Address
Name	Browser-CAT-2
Color	Change
Type	User Agent
Host	LOCAL_SUBNET
User Agent	Mozilla Firefox
Comments	Write a comment. 0/255

Web proxy address

ID	Source	Destination	Schedule	Action
explicit-web proxy → port1				
1	Browser-CAT-2 LOCAL_SUBNET User-B	all	always	DENY
2	LOCAL_SUBNET Browser-CAT-1 User-A	all	always	ACCEPT
3	LOCAL_SUBNET	all	always	ACCEPT

The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address.

An explicit web proxy is configured for subnet range 10.0.1.0/24 with three explicit web proxy policies.

The authentication rule is configured to authenticate HTTP requests for subnet range 10.0.1.0/24 with a form-based authentication scheme for the FortiGate local user database.

Users will be prompted for authentication.

How will FortiGate process the traffic when the HTTP request comes from a machine with the source IP 10.0.1.10 to the destination <http://www.fortinet.com>? (Choose two.)

- A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.
- B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.
- C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.
- D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

Answer: A,D

32.Refer to the exhibit.

Username	Administrator	Change Password
Type	<div>Local User</div> <div>Match a user on a remote server group</div> <div>Match all users in a remote server group</div> <div>Use public key infrastructure (PKI) group</div>	
Comments	Write a comment... 0/255	
Administrator Profile	prof_admin ▼	
Email Address	admin@xyz.com	
<input type="checkbox"/> SMS		
<input type="checkbox"/> Two-factor Authentication		
<input type="checkbox"/> Restrict login to trusted hosts		
<input type="checkbox"/> Restrict admin to guest account provisioning only		

The global settings on a FortiGate device must be changed to align with company security policies.

What does the Administrator account need to access the FortiGate global settings?

- A. Change password
- B. Enable restrict access to trusted hosts
- C. Change Administrator profile
- D. Enable two-factor authentication

Answer: D

33. Which two statements are true about the Security Fabric rating? (Choose two.)

- A. It provides executive summaries of the four largest areas of security focus.
- B. Many of the security issues can be fixed immediately by clicking Apply where available.
- C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
- D. The Security Fabric rating is a free service that comes bundled with all FortiGate devices.

Answer: B,C

34.Refer to the exhibit.

```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
origin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id= 00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output.

Which statement is true about the session diagnostic output?

- A. The session is in SYN_SEXT state.
- B. The session is in FIN_ACK state.
- C. The session is in FTN_WAIT state.
- D. The session is in ESTABLISHED state.

Answer: D

35.Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Source defined as Internet Services in the firewall policy.
- B. Destination defined as Internet Services in the firewall policy.
- C. Highest to lowest priority defined in the firewall policy.
- D. Services defined in the firewall policy.
- E. Lowest to highest policy ID number.

Answer: A,B,D

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47435>

36.By default, FortiGate is configured to use HTTPS when performing live web

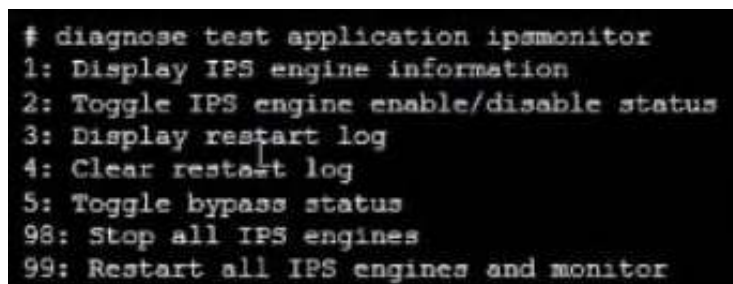
filtering with FortiGuard servers.

Which two CLI commands will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering? (Choose two.)

- A. set fortiguard anycast disable
- B. set protocol udp
- C. set webfilter-force-off disable
- D. set webfilter-cache disable

Answer: A,C

37.Refer to the exhibit.



```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack.
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

Answer: C

38.Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

- A. hard-timeout
- B. auth-on-demand
- C. soft-timeout
- D. new-session
- E. Idle-timeout

Answer: A,D,E

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221>

39. FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention

Answer: A,C

40. When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

- A. Log ID
- B. Universally Unique Identifier
- C. Policy ID
- D. Sequence ID

Answer: B

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies>

41. Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The subject field in the server certificate
- B. The serial number in the server certificate
- C. The server name indication (SNI) extension in the client hello message
- D. The subject alternative name (SAN) field in the server certificate
- E. The host field in the HTTP header

Answer: ACD

Explanation:

Reference: <https://checkthefirewall.com/blogs/fortinet/ssl-inspection>

42. Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

- A. diagnose sys top
- B. execute ping
- C. execute traceroute

D. diagnose sniffer packet any

E. get system arp

Answer: A,B, C