

# NSE4\_FGT-7.0 Dumps

## Fortinet NSE 4 - FortiOS 7.0

[https://www.certleader.com/NSE4\\_FGT-7.0-dumps.html](https://www.certleader.com/NSE4_FGT-7.0-dumps.html)



**NEW QUESTION 1**

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

**NEW QUESTION 2**

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:** BD

**NEW QUESTION 3**

Which two statements describe how the RPF check is used? (Choose two.)

- A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
- B. The RPF check is run on the first sent and reply packet of any new session.
- C. The RPF check is run on the first sent packet of any new session.
- D. The RPF check is run on the first reply packet of any new session.

**Answer:** AC

**Explanation:**

FortiGate Infrastructure 7.2 Study Guide (p.41): "The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table." "FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session."

\* A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks<sup>1</sup>

\* C. The RPF check is run on the first sent packet of any new session.

This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the session initiation. This reduces the processing overhead and improves performance<sup>2</sup>

**NEW QUESTION 4**

An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.12" 5
```

Which three pieces of Information will be Included in me sniffer output? {Choose three.)

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

**Answer:** ABD

**NEW QUESTION 5**

An employee needs to connect to the office through a high-latency internet connection.

Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

- A. idle-timeout
- B. login-timeout
- C. udp-idle-timer
- D. session-ttl

**Answer:** B

**Explanation:**

FortiGate Infrastructure 7.2 Study Guide (p.222):

"When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under config vpn ssl settings have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN connections."

**NEW QUESTION 6**

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

- A. IP address
- B. Once Internet Service is selected, no other object can be added
- C. User or User Group
- D. FQDN address

**Answer:** B

#### NEW QUESTION 7

Examine this PAC file configuration.

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:** AD

#### NEW QUESTION 8

Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

- A. Shut down/reboot a downstream FortiGate device.
- B. Disable FortiAnalyzer logging for a downstream FortiGate device.
- C. Log in to a downstream FortiSwitch device.
- D. Ban or unban compromised hosts.

**Answer:** AB

#### NEW QUESTION 9

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.

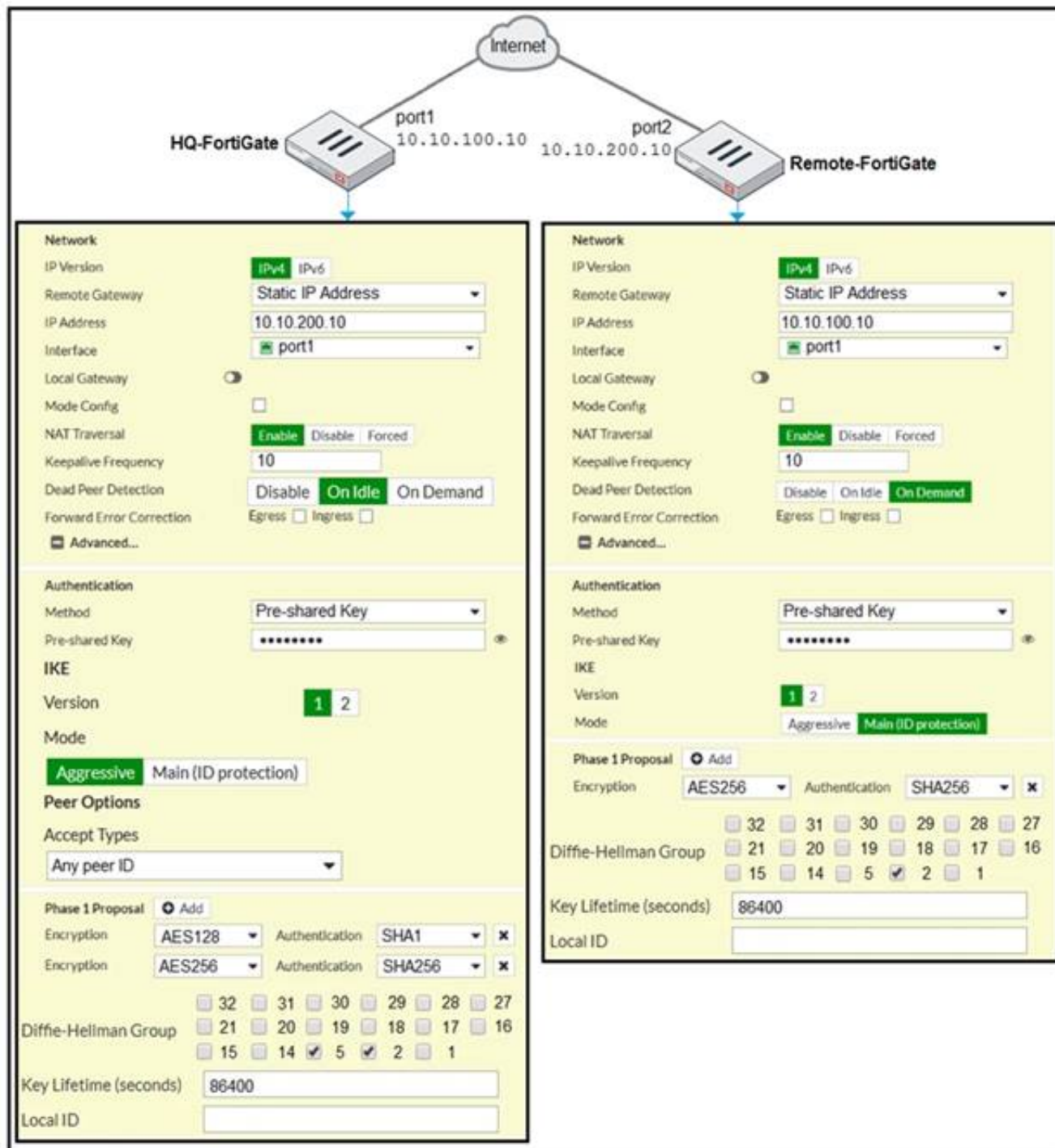
**Answer:** B

#### Explanation:

Strict Reverse Path Forwarding (RPF) is a security feature that is used to detect and prevent IP spoofing attacks on a network. It works by checking the routing information for incoming packets to ensure that they are coming from the source address that is indicated in the packet's header. In strict RPF mode, the firewall will check the best route back to the source of the incoming packet using the incoming interface. If the packet's source address does not match the route back to the source, the packet is dropped. This helps to prevent attackers from spoofing their IP address and attempting to access the network.

#### NEW QUESTION 10

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-Hellman group 2.
- D. On Remote-FortiGate, set port2 as Interface.

**Answer: AD**

**Explanation:**

"In IKEv1, there are two possible modes in which the IKE SA negotiation can take place: main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel."

**NEW QUESTION 10**

Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

- A. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
- B. Extended authentication (XAuth) to request the remote peer to provide a username and password
- C. No certificate is required on the remote peer when you set the certificate signature as the authentication method
- D. Pre-shared key and certificate signature as authentication methods

**Answer: BD**

**Explanation:**

\* B. Extended authentication (XAuth) to request the remote peer to provide a username and password

This is true because extended authentication (XAuth) is a feature that allows FortiGate to request the remote peer to provide a username and password during the IPsec IKEv1 authentication process. XAuth is an extension of the IKEv1 protocol that adds an additional authentication step after the main mode or aggressive mode exchange. XAuth can be used with either pre-shared key or certificate signature as the primary authentication method, and it can provide stronger security and granular access control for IPsec VPNs.

\* D. Pre-shared key and certificate signature as authentication methods

This is true because pre-shared key and certificate signature are two authentication methods that are supported by FortiGate for IPsec IKEv1 VPNs. Pre-shared key is a method where both peers share a secret key that is used to authenticate each other during the IKEv1 exchange. Certificate signature is a method where both peers have digital certificates that are used to verify each other's identity and public key during the IKEv1 exchange. Both methods can be combined with XAuth for additional authentication.

**NEW QUESTION 15**

Which three statements explain a flow-based antivirus profile? (Choose three.)

- A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.

- B. If a virus is detected, the last packet is delivered to the client.
- C. The IPS engine handles the process as a standalone.
- D. FortiGate buffers the whole file but transmits to the client at the same time.
- E. Flow-based inspection optimizes performance compared to proxy-based inspection.

**Answer:** ADE

#### NEW QUESTION 18

Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

- A. VDOMs without ports with connected devices are not displayed in the topology.
- B. Downstream devices can connect to the upstream device from any of their VDOMs.
- C. Security rating reports can be run individually for each configured VDOM.
- D. Each VDOM in the environment can be part of a different Security Fabric.

**Answer:** A

#### Explanation:

FortiGate Security 7.2 Study Guide (p.436): "When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric."

#### NEW QUESTION 23

Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

- A. The public key of the web server certificate must be installed on the browser.
- B. The web-server certificate must be installed on the browser.
- C. The CA certificate that signed the web-server certificate must be installed on the browser.
- D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

**Answer:** C

#### NEW QUESTION 24

Which scanning technique on FortiGate can be enabled only on the CLI?

- A. Heuristics scan
- B. Trojan scan
- C. Antivirus scan
- D. Ransomware scan

**Answer:** A

#### NEW QUESTION 28

In which two ways can RPF checking be disabled? (Choose two )

- A. Enable anti-replay in firewall policy.
- B. Disable the RPF check at the FortiGate interface level for the source check
- C. Enable asymmetric routing.
- D. Disable strict-arc-check under system settings.

**Answer:** CD

#### NEW QUESTION 29

Which statement is correct regarding the use of application control for inspecting web applications?

- A. Application control can identify child and parent applications, and perform different actions on them.
- B. Application control signatures are organized in a nonhierarchical structure.
- C. Application control does not require SSL inspection to identify web applications.
- D. Application control does not display a replacement message for a blocked web application.

**Answer:** A

#### Explanation:

Application control is a feature that allows FortiGate to inspect and control the use of specific web applications on the network. When application control is enabled, FortiGate can identify child and parent applications, and can perform different actions on them based on the configuration.

#### NEW QUESTION 33

Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

- A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
- B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
- C. Virtual IP addresses are used to distinguish between cluster members.
- D. The primary device in the cluster is always assigned IP address 169.254.0.1.

**Answer:** BD



**NEW QUESTION 37**

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

- A. To detect intermediary NAT devices in the tunnel path.
- B. To dynamically change phase 1 negotiation mode aggressive mode.
- C. To encapsulation ESP packets in UDP packets using port 4500.
- D. To force a new DH exchange with each phase 2 rekey.

**Answer:** AC

**NEW QUESTION 38**

Which two statements are true when FortiGate is in transparent mode? (Choose two.)

- A. By default, all interfaces are part of the same broadcast domain.
- B. The existing network IP schema must be changed when installing a transparent mode.
- C. Static routes are required to allow traffic to the next hop.
- D. FortiGate forwards frames without changing the MAC address.

**Answer:** AD

**NEW QUESTION 43**

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:** BCE

**NEW QUESTION 44**

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

**Answer:** AC

**NEW QUESTION 48**

Refer to the web filter raw logs.

```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web" action="blocked"
reqtype="direct" url="https://twitter.com/" sentbyte=517
rcvdbyte=0 direction="outgoing" msg="URL belongs to a category
with warnings enabled" method="domain" cat=37 catdesc="Social
Networking"

date=2020-07-09 time=12:52:16 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313537024536428 tz="-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web"
action="passthrough" reqtype="direct" url="https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction="outgoing" msg="URL belongs to
a category with warnings enabled" method="domain" cat=37
catdesc="Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

- A. Social networking web filter category is configured with the action set to authenticate.
- B. The action on firewall policy ID 1 is set to warning.
- C. Access to the social networking web filter category was explicitly blocked to all users.
- D. The name of the firewall policy is all\_users\_web.

**Answer:** A

#### NEW QUESTION 49

FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.

Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

- A. www.example.com:443
- B. www.example.com
- C. example.com
- D. www.example.com/index.html

**Answer:** BC

#### Explanation:

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names - no URLs or wildcard characters are allowed.

OK: google.com or www.google.com

NO OK: www.google.com/index.html or google.\* FortiGate\_Security\_6.4 page 384

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names-- "no URLs or wildcard characters are allowed".

#### NEW QUESTION 52

Refer to the exhibit.

**Edit IPS Sensor**

Name:

Comments:  0/255

Block malicious URLs: ☒

**IPS Signatures and Filters**

[+ Create New](#) [Edit](#) [Delete](#)

Details	Exempt IPs	Action	Packet Logging	Status
NTP.Spoofed.KoD.DoS	0	Monitor	Enabled	Enabled
<b>OS</b> Windows		Block	Disabled	Enabled

The exhibit shows the IPS sensor configuration.

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

- A. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
- B. The sensor will block all attacks aimed at Windows servers.
- C. The sensor will reset all connections that match these signatures.
- D. The sensor will gather a packet log for all matched traffic.

**Answer:** AB

#### NEW QUESTION 54

An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.

Which DPD mode on FortiGate will meet the above requirement?

- A. Disabled
- B. On Demand
- C. Enabled
- D. On Idle

**Answer:** D

#### NEW QUESTION 56

Refer to exhibit.

An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.

Name: Allow\_Twitter  
Comments: Write a comment... 0/255  
Feature set: **Flow-based** Proxy-based  
FortiGuard Category Based Filter  
Allow Monitor Block Warning Authenticate  

Name	Action
Medicine	Allow
News and Media	Allow
Social Networking	Block
Political Organizations	Allow
Reference	Allow
Global Religion	Allow
Shopping	Allow
Society and Lifestyles	Allow
Sports	Allow

Static URL Filter  
Block invalid URLs  
URL Filter  
+ Create New Edit Delete Search  

URL	Type	Action	Status
twitter.com	Wildcard	Allow	Enable

Block malicious URLs discovered by FortiSandbox  
Content Filter

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

- A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking
- B. On the Static URL Filter configuration, set Type to Simple
- C. On the Static URL Filter configuration, set Action to Exempt.
- D. On the Static URL Filter configuration, set Action to Monitor.

**Answer: C**

#### NEW QUESTION 59

Which feature in the Security Fabric takes one or more actions based on event triggers?

- A. Fabric Connectors
- B. Automation Stitches
- C. Security Rating
- D. Logical Topology

**Answer: B**

#### NEW QUESTION 60

Which two statements are true about the RPF check? (Choose two.)

- A. The RPF check is run on the first sent packet of any new session.
- B. The RPF check is run on the first reply packet of any new session.
- C. The RPF check is run on the first sent and reply packet of any new session.
- D. RPF is a mechanism that protects FortiGate and your network from IP spoofing attacks.

**Answer: AD**

#### NEW QUESTION 65

Examine the exhibit, which contains a virtual IP and firewall policy configuration.

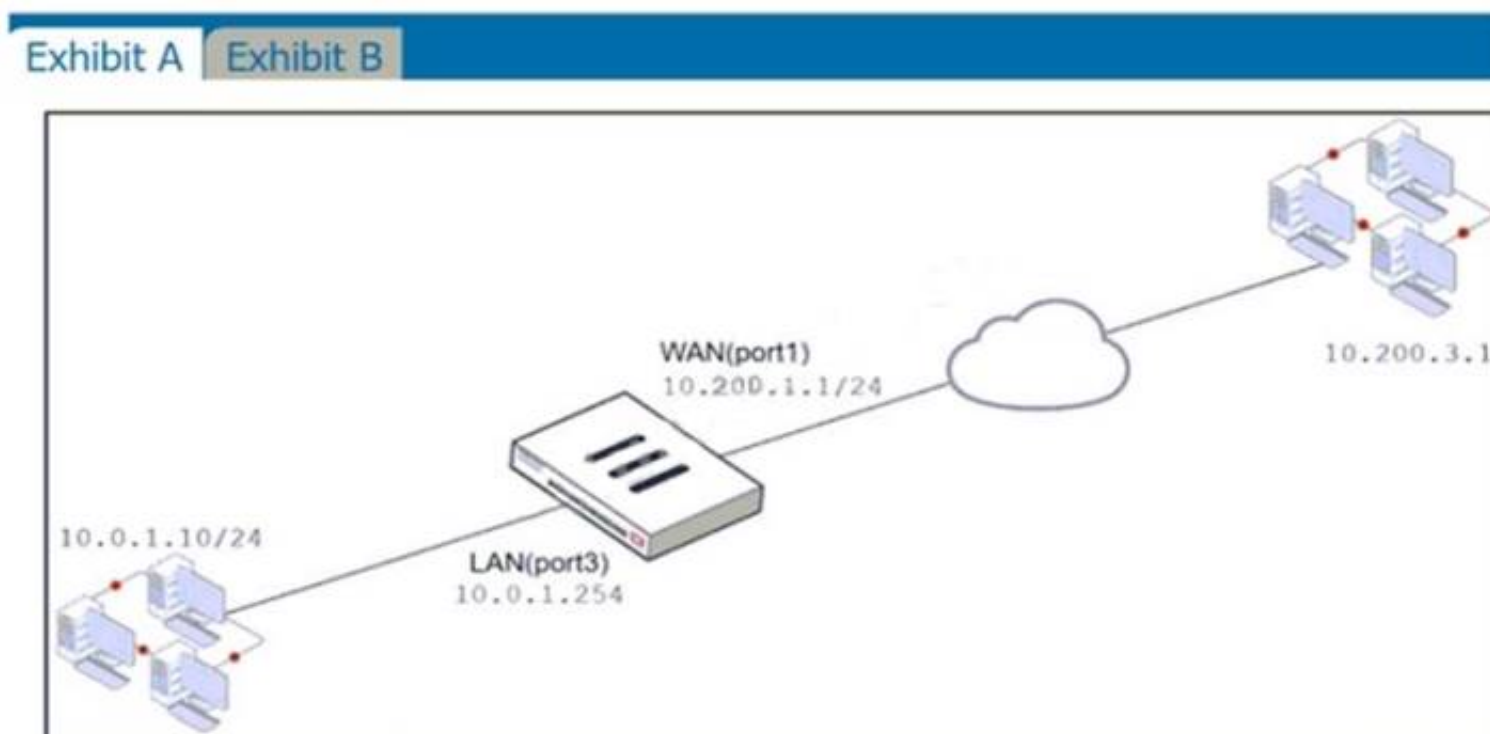




Exhibit A

Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type

IPv4

Name

VIP

Comments

Write a comment...

0/255

Color

Change

Network

Interface

WAN (port1)

Type

Static NAT

External IP address/range

10.200.1.10

Map to

IPv4 address/range

10.0.1.10

☐ Optional Filters

☒ Port Forwarding

Protocol

TCP

UDP

SCTP

ICMP

Port Mapping Type

One to one

Many to many

External service port

10443

Map to IPv4 port

443

The WAN (port1) interface has the IP address 10.200. 1. 1/24. The LAN (port2) interface has the IP address 10.0. 1.254/24. The first firewall policy has NAT enabled on the outgoing interface address. The second firewall policy is configured with a VIP as the destination address. Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0. 1. 10/24?

- A. 10.200. 1. 10
- B. Any available IP address in the WAN (port1) subnet 10.200. 1.0/24 66 of 108
- C. 10.200. 1. 1
- D. 10.0. 1.254

Answer: A

Explanation:

<https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs>.

NEW QUESTION 70

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: B

NEW QUESTION 75

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

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

Answer: AC

NEW QUESTION 80

Which two statements are correct about a software switch on FortiGate? (Choose two.)

- A. It can be configured only when FortiGate is operating in NAT mode
- B. Can act as a Layer 2 switch as well as a Layer 3 router
- C. All interfaces in the software switch share the same IP address
- D. It can group only physical interfaces

Answer: AC

NEW QUESTION 81

Refer to the exhibits.

Edit Policy

Name ⓘ

Facebook SSL Inspection

Incoming interface

port2

Outgoing interface

port1

Source

all

Destination

all

Service

ALL

Firewall/Network Options

ⓘ CentralNAT is enabled so NAT settings from matching Central SNAT policies will be applied

Security Profiles

SSL Inspection

SSL

 certificate-inspection

Edit Policy

Name ⓘ

Facebook Access

Incoming interface

port2

Outgoing interface

port1

Source

all

Destination

all

Schedule

always

Service

AppDefault

 Specify

Application

Facebook

Facebook\_Like.Button

Facebook\_Video.Play

URL Category

+

✓ ACCEPT

⊘ DENY

Firewall/Network Options

Protocol Options

IPsec

 default

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook . Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts. Which part of the policy configuration must you change to resolve the issue?

- A. Make SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Get the additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

Answer: A

Explanation:

They can play video (tick) content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts. This indicate that the rule are partially working as they can watch video but cant react, i.e. liking the content. So must be an issue with the SSL inspection rather then adding an app rule.

NEW QUESTION 82

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: CD

**Explanation:**

In the 7.2 Infrastructure Guide (page 306) the list of configuration settings that are NOT synchronized includes both 'FortiGate host name' and 'Cache'

**NEW QUESTION 83**

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

**Answer:** D

**Explanation:**

"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

**NEW QUESTION 87**

Which of statement is true about SSL VPN web mode?

- A. The tunnel is up while the client is connected.
- B. It supports a limited number of protocols.
- C. The external network application sends data through the VPN.
- D. It assigns a virtual IP address to the client.

**Answer:** B

**Explanation:**

FortiGate\_Security\_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

**NEW QUESTION 90**

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A. A CRL
- B. A person
- C. A subordinate CA
- D. A root CA

**Answer:** D

**NEW QUESTION 91**

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"
```

What two conclusions can you make from the debug flow output? (Choose two.)

- A. The debug flow is for ICMP traffic.
- B. The default route is required to receive a reply.
- C. A new traffic session was created.
- D. A firewall policy allowed the connection.

**Answer:** AC

**Explanation:**

The debug flow output shows the result of a diagnose command that captures the traffic flow between the source and destination IP addresses1. The debug flow output reveals the following information about the traffic flow1:

➤ The protocol is 1, which means that the traffic uses ICMP protocol2. ICMP is a protocol that is used to send error messages and test connectivity between devices2.

➤ The session state is 0, which means that a new traffic session was created3. A session is a data structure that stores information about a connection between two devices3.

➤ The policy ID is 1, which means that the traffic matched the firewall policy with ID 14. A firewall policy is a rule that defines how FortiGate processes traffic based on the source, destination, service, and action parameters4.

➤ The action is 0, which means that the traffic was allowed by the firewall policy. An action is a parameter that specifies what FortiGate does with the traffic that matches a firewall policy.

Therefore, two conclusions that can be made from the debug flow output are:

➤ The debug flow is for ICMP traffic.



➤ A new traffic session was created.

#### NEW QUESTION 94

Which statement correctly describes the use of reliable logging on FortiGate?

- A. Reliable logging is enabled by default in all configuration scenarios.
- B. Reliable logging is required to encrypt the transmission of logs.
- C. Reliable logging can be configured only using the CLI.
- D. Reliable logging prevents the loss of logs when the local disk is full.

**Answer: B**

#### Explanation:

FortiGate Security 7.2 Study Guide (p.192): "if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm setting on the CLI."

#### NEW QUESTION 97

Which statement about the IP authentication header (AH) used by IPsec is true?

- A. AH does not provide any data integrity or encryption.
- B. AH does not support perfect forward secrecy.
- C. AH provides data integrity but no encryption.
- D. AH provides strong data integrity but weak encryption.

**Answer: C**

#### NEW QUESTION 98

Refer to the exhibit.



Which contains a network diagram and routing table output. The Student is unable to access Webserver.

What is the cause of the problem and what is the solution for the problem?

- A. The first packet sent from Student failed the RPF check. This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
- B. The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
- C. The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.
- D. The first packet sent from Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

**Answer: D**

#### NEW QUESTION 101

You have enabled logging on a FortiGate device for event logs and all security logs, and you have set up logging to use the FortiGate local disk. What is the default behavior when the local disk is full?

- A. No new log is recorded after the warning is issued when log disk use reaches the threshold of 95%.
- B. No new log is recorded until you manually clear logs from the local disk.
- C. Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.
- D. Logs are overwritten and the only warning is issued when log disk use reaches the threshold of 95%.

**Answer: C**

#### Explanation:

config log disk setting

set diskfull [ overwrite | nolog ]

Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full. (default --> overwrite)

config log memory global-setting



set full-first-warning-threshold {integer}

Log full first warning threshold as a percent. (default --> 75)

#### **NEW QUESTION 106**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your NSE4\_FGT-7.0 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/NSE4\\_FGT-7.0-dumps.html](https://www.certleader.com/NSE4_FGT-7.0-dumps.html)