

Fortinet

Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)



NEW QUESTION 1

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 2

An administrator needs to increase network bandwidth and provide redundancy.
What interface type must the administrator select to bind multiple FortiGate interfaces?

- A. VLAN interface
- B. Software Switch interface
- C. Aggregate interface
- D. Redundant interface

Answer: C

NEW QUESTION 3

Which two types of traffic are managed only by the management VDOM? (Choose two.)

- A. FortiGuard web filter queries
- B. PKI
- C. Traffic shaping
- D. DNS

Answer: AD

NEW QUESTION 4

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

Explanation:

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

NEW QUESTION 5

Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

- A. DNS
- B. ping
- C. udp-echo
- D. TWAMP

Answer: CD

NEW QUESTION 6

Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srcintfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reftype= "direct" url= "https://etp-experiment-1.dummytracker.org/"
sentbyte=517 rcvbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

- A. Traffic is blocked because Action is set to DENY in the firewall policy.
- B. Traffic belongs to the root VDOM.
- C. This is a security log.
- D. Log severity is set to error on FortiGate.

Answer: AC

NEW QUESTION 7

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 8

Which two types of traffic are managed only by the management VDOM? (Choose two.)

- A. FortiGuard web filter queries
- B. PKI
- C. Traffic shaping
- D. DNS

Answer: AD

NEW QUESTION 9

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

Answer: BDE

NEW QUESTION 10

Which two statements explain antivirus scanning modes? (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: BC

Explanation:

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM--something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

NEW QUESTION 10

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 15

What are two functions of ZTNA? (Choose two.)

- A. ZTNA manages access through the client only.
- B. ZTNA manages access for remote users only.
- C. ZTNA provides a security posture check.
- D. ZTNA provides role-based access.

Answer: CD

NEW QUESTION 18

How does FortiGate act when using SSL VPN in web mode?

- A. FortiGate acts as an FDS server.
- B. FortiGate acts as an HTTP reverse proxy.
- C. FortiGate acts as DNS server.
- D. FortiGate acts as router.

Answer: B

NEW QUESTION 21

Refer to the exhibits.
 Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.
 The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IP address 10.0.1.254/24.

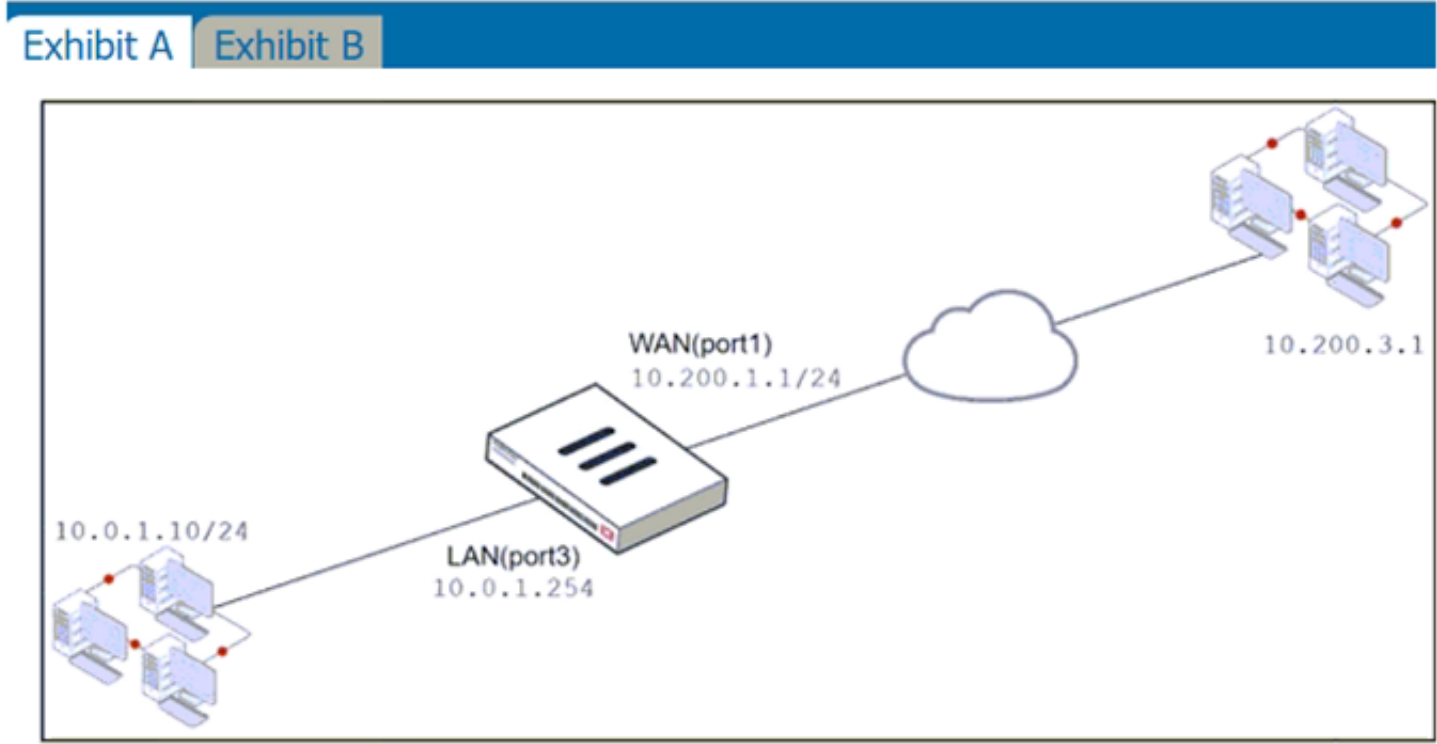


Exhibit A

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

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

- A. 10.0.1.254, 10.0.1.10, and 443, respectively
- B. 10.0.1.254, 10.0.1.10, and 10443, respectively
- C. 10.200.3.1, 10.0.1.10, and 443, respectively

Answer: C

NEW QUESTION 26

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: AD

NEW QUESTION 27

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: BCD

NEW QUESTION 31

Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

- A. The next-hop IP address is unreachable.
- B. It failed the RPF check .
- C. It matched an explicitly configured firewall policy with the action DENY.
- D. It matched the default implicit firewall policy.

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=13900>

NEW QUESTION 34

Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

- A. Proxy-based inspection
- B. Certificate inspection
- C. Flow-based inspection
- D. Full Content inspection

Answer: AC

NEW QUESTION 38

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

NEW QUESTION 40

Refer to the exhibit.

The exhibit shows the output of a diagnose command.


```
# diagnose firewall proute list
list route policy info(vf=root):
id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
```

What does the output reveal about the policy route?

- A. It is an ISDB route in policy route.
- B. It is a regular policy route.
- C. It is an ISDB policy route with an SDWAN rule.
- D. It is an SDWAN rule in policy route.

Answer: C

NEW QUESTION 42

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 46

Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 49

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 50

Which three methods are used by the collector agent for AD polling? (Choose three.)

- A. FortiGate polling
- B. NetAPI
- C. Novell API
- D. WMI
- E. WinSecLog

Answer: BDE

NEW QUESTION 54

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

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

☐

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

?

Use FortiGuard Outbreak Prevention Database

☐

Use External Malware Block List

? *!*
☐

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

Explanation:

- "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
- When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.

In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

NEW QUESTION 58

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 59

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 63

An organization's employee needs to connect to the office through a high-latency internet connection. Which SSL VPN setting should the administrator adjust to prevent the SSL VPN negotiation failure?

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

Answer: B

NEW QUESTION 67

Refer to the exhibits.

The exhibits show the firewall policies and the objects used in the firewall policies.

The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Exhibit A Exhibit B

Address Object

Name	Details
IP Range/Subnet	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services		
Facebook-Web	Destination	26.578
IP	Port	Protocol
1.9.91.17 - 1.9.91.18	80	TCP
	443	
	8443	
1.9.91.17 - 1.9.91.18	443	UDP
1.9.91.30	443	UDP

Firewall Policies

ID	From	To	Source	Destination	Schedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	✓ ACCEPT	Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	✓ ACCEPT	Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	✓ ACCEPT	Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	✓ ACCEPT	Enabled
2	port3	port1	all	all	always	ALL	✓ ACCEPT	Enabled

Exhibit A Exhibit B

Policy Lookup

Incoming Interface

port3

IP Version

IPv4

Protocol

TCP

Source

10.0.1.10

Source Port

Optional (1-65535)

Destination

facebook.com

Destination Port

443

Search

Close

Which policy will be highlighted, based on the input criteria?

- A. Policy with ID 4.
- B. Policy with ID 5.
- C. Policies with ID 2 and 3.
- D. Policy with ID 4.

Answer: B

NEW QUESTION 68

Refer to the exhibits.

SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s)

port1

+

×

Listen on Port

10443

Web mode access will be listening at

<https://10.200.1.1:10443>

Redirect HTTP to SSL-VPN

☐

Restrict Access

Allow access from any host

Limit access to specific hosts

Idle Logout

☒

Inactive For

300

Seconds

Server Certificate

Fortinet_Factory

▼

Require Client Certificate

☐

Tunnel Mode Client Settings ⓘ

Address Range

Automatically assign addresses

Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server

Same as client system DNS

Specify

Specify WINS Servers

☐

Authentication/Portal Mapping ⓘ

+ Create New

Edit

Delete

Users/Groups ⌵	Portal ⌵
sslvpn	tunnel-access
All Other Users/Groups	full-access

Connection status

Connection:

VPN

Server:

<https://10.200.1.1:1443/>

Status:

Connecting...

Duration:

—

Bytes received:

0

Bytes sent:

0

Stop

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

- A. Change the SSL VPN port on the client.
- B. Change the Server IP address.
- C. Change the idle-timeout.
- D. Change the SSL VPN portal to the tunnel.

Answer: A

NEW QUESTION 73

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: ADE

Explanation:

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

NEW QUESTION 77

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE4 Practice Exam Features:

- * NSE4 Questions and Answers Updated Frequently
- * NSE4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4 Practice Test Here](#)