

# Fortinet

## Exam Questions NSE4\_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2



### NEW QUESTION 1

If Internet Service is already selected as Destination in a firewall policy, which other configuration object can be selected for the Destination field of a firewall policy?

- A. IP address
- B. No other object can be added
- C. FQDN address
- D. User or User Group

**Answer: B**

#### Explanation:

FortiGate Security 7.2 Study Guide (p.59): "When configuring your firewall policy, you can use Internet Service as the destination in a firewall policy, which contains all the IP addresses, ports, and protocols used by that service. For the same reason, you cannot mix regular address objects with ISDB objects, and you cannot select services on a firewall policy. The ISDB objects already have services information, which is hardcoded." This is true because Internet Service is a special type of destination object that can only be used alone in a firewall policy. Internet Service is a feature that allows FortiGate to identify and filter traffic based on the internet service or application that it belongs to, such as Facebook, YouTube, Skype, etc. Internet Service uses a database of IP addresses and ports that are associated with each internet service or application, and updates it regularly from FortiGuard. When Internet Service is selected as the destination in a firewall policy, FortiGate will match the traffic to the corresponding internet service or application, and apply the appropriate action and security profiles to it. However, Internet Service cannot be combined with any other destination object, such as IP address, FQDN address, user or user group, etc., as this would create a conflict or ambiguity in the firewall policy. Therefore, no other object can be added if Internet Service is already selected as the destination in a firewall policy

### NEW QUESTION 2

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: ABD**

#### Explanation:

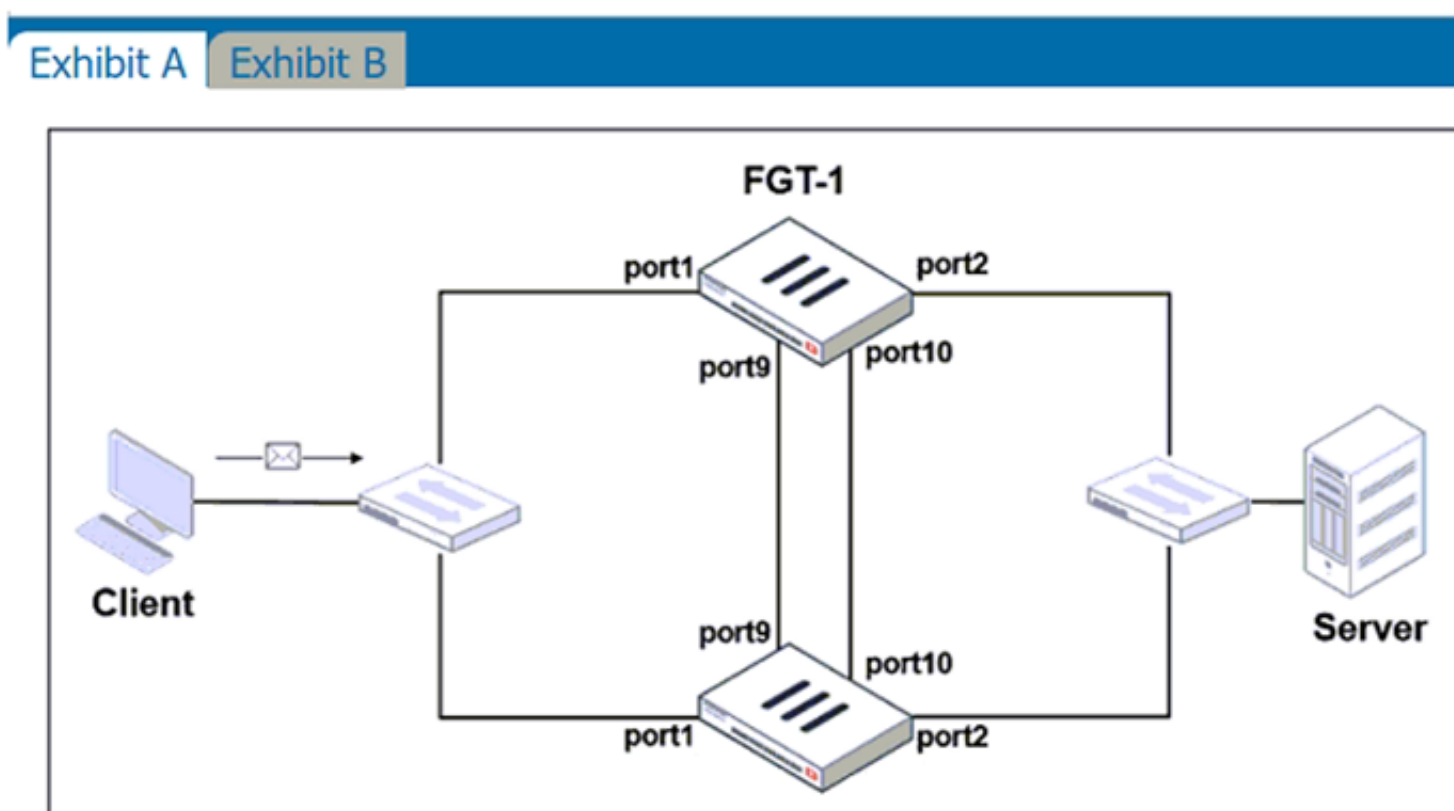
When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

- Incoming Interface
- Outgoing Interface
- Source: IP address, user, internet services
- Destination: IP address or internet services
- Service: IP protocol and port number
- Schedule: Applies during configured times

### NEW QUESTION 3

Refer to the exhibits.

Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.



**Exhibit A**

```
set group-id 3
set group-name "NSE"
set mode a-a
set password *
set hbdev "port9" 50 "port10" 50
set session-pickup enable
set override disable
set monitor port3
end
```

**Exhibit B**

```
# get system ha status
...
Primary      : FGT-2, FGVM010000065036, HA cluster index = 1
Secondary    : FGT-1, FGVM010000064692, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000065036, HA operating index = 1
Secondary: FGVM010000064692, HA operating index = 0
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

- A. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.
- B. The traffic sourced from the client and destined to the server is sent to FGT-1.
- C. The cluster can load balance ICMP connections to the secondary.
- D. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

**Answer:** AD

**Explanation:**

FortiGate Infrastructure 7.2 Study Guide (p.317 & p.320): "To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses." "The primary forwards the SYN packet to the selected secondary. (...) This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic."

**NEW QUESTION 4**

An administrator wants to simplify remote access without asking users to provide user credentials. Which access control method provides this solution?

- A. ZTNA IP/MAC filtering mode
- B. ZTNA access proxy
- C. SSL VPN
- D. L2TP

**Answer:** B

**Explanation:**

FortiGate Infrastructure 7.2 Study Guide (p.165): "ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs."

This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials. ZTNA access proxy uses a secure tunnel between the user's device and the FortiGate, and authenticates the user based on device identity and context. The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile. This simplifies remote access and enhances security by reducing the attack surface<sup>12</sup>

**NEW QUESTION 5**

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

- A. The matching firewall policy is set to proxy inspection mode.
- B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
- C. The full SSL inspection feature does not have a valid license.
- D. The browser does not trust the certificate used by FortiGate for SSL inspection.

**Answer:** D

**Explanation:**

FortiGate Security 7.2 Study Guide (p.235): "If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet\_CA\_SSL certificate and sends it to the browser. If the browser trusts the Fortinet\_CA\_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet\_CA\_SSL certificate into the trusted root CA certificate store of your browser."

**NEW QUESTION 6**

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.

FortiGate Security 7.2 Study Guide (p.350 & 352): "In flow-based inspection mode, the IPS engine reads the payload of each packet, caches a local copy, and forwards the packet to the receiver at the same time. Because the file is transmitted simultaneously, flow-based mode consumes more CPU cycles than proxy-based." "Each protocol's proxy picks up a connection and buffers the entire file first (or waits until the oversize limit is reached) before scanning. The client must wait for the scanning to finish."

**NEW QUESTION 7**

What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

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

**Answer:** D

**NEW QUESTION 8**

Which statement about the policy ID number of a firewall policy is true?

- A. It is required to modify a firewall policy using the CLI.
- B. It represents the number of objects used in the firewall policy.
- C. It changes when firewall policies are reordered.
- D. It defines the order in which rules are processed.

**Answer:** A

**NEW QUESTION 9**

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

- A. Antivirus engine
- B. Intrusion prevention system engine
- C. Flow engine
- D. Detection engine

**Answer:** B

**Explanation:**

<http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control>

**NEW QUESTION 10**

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**

Refer to the exhibit.



```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000  4500 003c 2f8f 0000 8001 f020 0a00 0102    E.</.....
0x0010  0808 0808 0800 4d5a 0001 0001 6162 6364    .....MZ....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374    efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869             uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000  4500 003c 2f8f 0000 7f01 0106 0a38 f0e4    E.</.....8..
0x0010  0808 0808 0800 6159 ec01 0001 6162 6364    .....aY....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374    efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869             uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000  4500 003c 0000 0000 7501 3a95 0808 0808    E.<....u.:....
0x0010  0a38 f0e4 0000 6959 ec01 0001 6162 6364    .8....iY....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374    efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869             uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000  4500 003c 0000 0000 7401 2bb0 0808 0808    E.<....t.+....
0x0010  0a00 0102 0000 555a 0001 0001 6162 6364    .....UZ....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374    efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869             uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.  
 Which three pieces of information are included in the sniffer output? (Choose three.)

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

**Answer:** ACE

#### NEW QUESTION 11

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

- A. The Services field prevents SNAT and DNAT from being combined in the same policy.
- B. The Services field is used when you need to bundle several VIPs into VIP groups.
- C. The Services field removes the requirement to create multiple VIPs for different services.
- D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

**Answer:** C

#### NEW QUESTION 16

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 20

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. SSH
- B. HTTPS
- C. FTM
- D. FortiTelemetry

**Answer:** AB

#### NEW QUESTION 23

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 27

Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

- A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
- B. The client FortiGate requires a manually added route to remote subnets.
- C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
- D. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

**Answer:** CD

#### Explanation:

<https://docs.fortinet.com/document/fortigate/7.0.9/administration-guide/508779/fortigate-as-ssl-vpn-client>

To establish an SSL VPN connection between two FortiGate devices, the following two settings are required:

The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate will use a CA (Certificate Authority) certificate to verify the client FortiGate certificate, ensuring that the client device is trusted and allowed to establish an SSL VPN connection.

The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: The client FortiGate must have an SSL VPN tunnel interface type configured in order to establish an SSL VPN connection. This interface type will be used to connect to the server FortiGate over the SSL VPN.

### NEW QUESTION 31

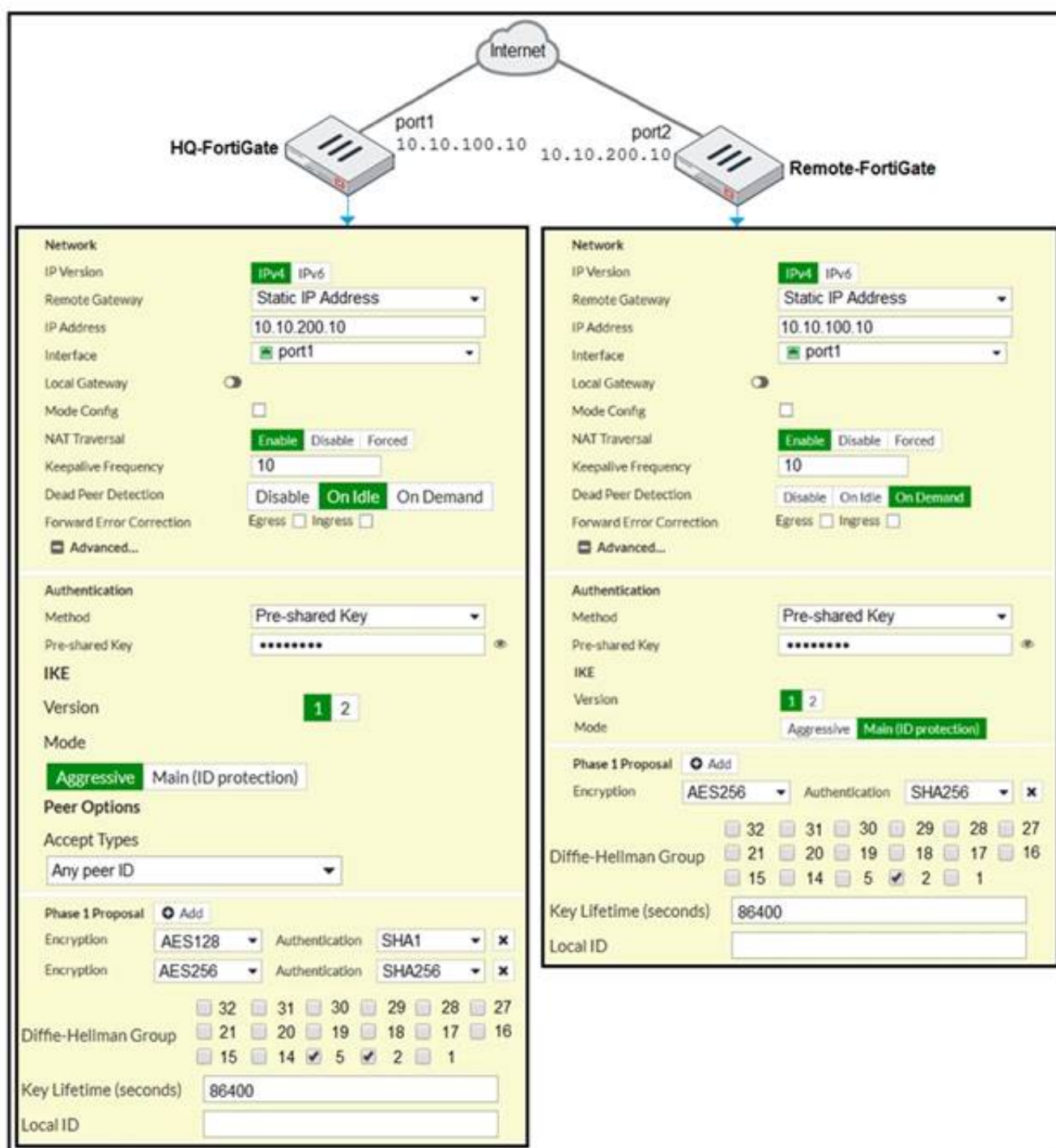
What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

- A. FortiGate uses fewer resources.
- B. FortiGate performs a more exhaustive inspection on traffic.
- C. FortiGate adds less latency to traffic.
- D. FortiGate allocates two sessions per connection.

**Answer:** AC

### NEW QUESTION 35

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-Helman 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 37**

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 38**

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

Comments
 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 39**

The IPS engine is used by which three security features? (Choose three.)

- A. Antivirus in flow-based inspection
- B. Web filter in flow-based inspection
- C. Application control
- D. DNS filter
- E. Web application firewall

**Answer:** ABC

**Explanation:**

FortiGate Security 7.2 Study Guide (p.385): "The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It's also responsible for application control, flow-based antivirus protection, web filtering, and email filtering."

**NEW QUESTION 41**

Refer to the exhibit.



```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
    pingsvr_flip_timeout/expire=3600s/2781s
    'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
    'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster. Which two statements are true? (Choose two.)

- A. FortiGate SN FGVM010000065036 HA uptime has been reset.
- B. FortiGate devices are not in sync because one device is down.
- C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- D. FortiGate SN FGVM010000064692 has the higher HA priority.

**Answer:** AD

**Explanation:**

\* 1. Override is disable by default - OK

\* 2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary"

The QUESTION NO: here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab>

**NEW QUESTION 46**

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.

In this scenario, what are two requirements for the VLAN ID? (Choose two.)

- A. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.
- B. The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs.
- C. The two VLAN subinterfaces must have different VLAN IDs.
- D. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

**Answer:** BC

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-use-vmac-vlan-to-share-the-same-VLAN/t> When FortiGate is operating in NAT mode, it means that it uses network address translation (NAT) to modify the source or destination IP addresses of the traffic passing through it<sup>1</sup>. NAT mode allows FortiGate to hide the IP addresses of the internal network from the external network, and to conserve IP addresses by using a single public IP address for multiple private IP addresses<sup>1</sup>.

A virtual LAN (VLAN) subinterface is a logical interface that allows traffic from different VLANs to enter

and exit the FortiGate unit<sup>2</sup>. A VLAN subinterface is created by adding a VLAN ID to a physical interface or an aggregate interface<sup>2</sup>. A VLAN ID is a numerical identifier that distinguishes one VLAN from another<sup>2</sup>.

In this scenario, there are two requirements for the VLAN ID of the VLAN subinterfaces added to the same physical interface:

➤ The two VLAN subinterfaces must have different VLAN IDs. This is because the VLAN ID is used to tag the traffic with the appropriate VLAN information, and to separate the traffic into different VLANs<sup>2</sup>. If the two VLAN subinterfaces have the same VLAN ID, they will not be able to distinguish the traffic from each other, and they will not be able to forward the traffic to the correct destination.

➤ The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs. This is because VDOMs are virtual instances of FortiGate that can have their own interfaces, policies, and routing tables<sup>3</sup>. Each VDOM operates independently from other VDOMs, and can have its own VLAN subinterfaces with different or identical VLAN IDs<sup>3</sup>. However, this requires inter-VDOM links to allow traffic between different VDOMs<sup>3</sup>.

**NEW QUESTION 49**

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

- A. It uses UDP 8888.
- B. It uses UDP 53.
- C. It uses DNS over HTTPS.
- D. It uses DNS over TLS.

**Answer:** D

**Explanation:**

FortiGate Security 7.2 Study Guide (p.15): "When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic."

When using FortiGuard servers for DNS, FortiOS defaults to using DNS over TLS (DoT) to secure the DNS traffic<sup>1</sup>. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol<sup>2</sup>. This prevents eavesdropping, tampering, and spoofing of DNS data by third parties.

The default FortiGuard DNS servers are 96.45.45.45 and 96.45.46.46, and they use the hostname globalsdns.fortinet.net<sup>1</sup>. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration<sup>1</sup>.

**NEW QUESTION 54**

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 57**

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 59**

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 64**

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

- A. Application control can identity 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 identity 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 66**

Refer to the exhibit.

Outgoing interfaces

☐ Manual  
Manually assign outgoing interfaces.

☒ Best Quality  
The interface with the best measured performance is selected.

☐ Lowest Cost (SLA)  
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

☐ Maximize Bandwidth (SLA)  
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

port1

port2

port3

port4

Measured SLA

SLA\_1

Quality criteria

Latency

Status

Enable

Disable

```

NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
  
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check . Which interface will be selected as an outgoing interface?

- A. port2
- B. port4

- C. port3
- D. port1

**Answer:** D

**Explanation:**

Port 1 shows the lowest latency.

**NEW QUESTION 68**

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check .

**Answer:** D

**NEW QUESTION 72**

Which three statements are true regarding session-based authentication? (Choose three.)

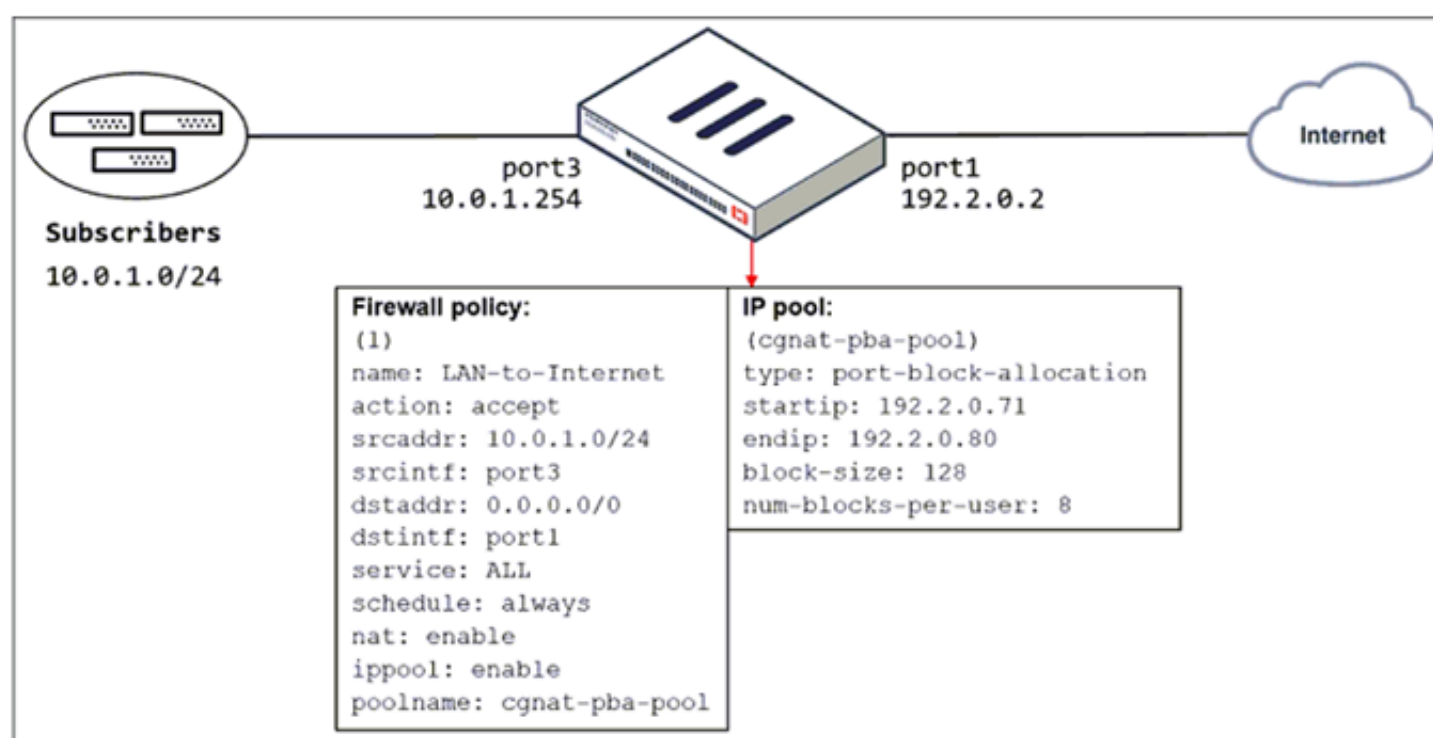
- A. HTTP sessions are treated as a single user.
- B. IP sessions from the same source IP address are treated as a single user.
- C. It can differentiate among multiple clients behind the same source IP address.
- D. It requires more resources.
- E. It is not recommended if multiple users are behind the source NAT

**Answer:** ACD

**NEW QUESTION 75**

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network and the firewall policy and IP pool configuration on the FortiGate device.



Which two actions does FortiGate take on internet traffic sourced from the subscribers? (Choose two.)

- A. FortiGate allocates port blocks per user, based on the configured range of internal IP addresses.
- B. FortiGate allocates port blocks on a first-come, first-served basis.
- C. FortiGate generates a system event log for every port block allocation made per user.
- D. FortiGate allocates 128 port blocks per user.

**Answer:** BC

**Explanation:**

FortiGate Security 7.2 Study Guide (p.109): "FortiGate allocates port blocks on a first-come, first-served basis." "For logging purposes, when FortiGate allocates a port block to a host, it generates a system event log to inform the administrator."

**NEW QUESTION 78**

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.

What is the reason for the failed virus detection by FortiGate?

- A. The website is exempted from SSL inspection.
- B. The EICAR test file exceeds the protocol options oversize limit.
- C. The selected SSL inspection profile has certificate inspection enabled.
- D. The browser does not trust the FortiGate self-signed CA certificate.



**Answer:** AC

**Explanation:**

SSL Inspection Profile, on the Inspection method there are 2 options to choose from, SSL Certificate Inspection or Full SSL Inspection. FG SEC 7.2 Studi Guide: Full SSL Inspection level is the only choice that allows antivirus to be effective.

**NEW QUESTION 79**

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:** D

**Explanation:**

FortiGate Infrastructure 7.2 Study Guide (p.59): "ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the vwl\_service field, and ISDB route entries don't."

**NEW QUESTION 84**

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 86**

An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192. 16. 1.0/24 and the remote quick mode selector is 192. 16.2.0/24. How must the administrator configure the local quick mode selector for site B?

- A. 192. 168.3.0/24
- B. 192. 168.2.0/24
- C. 192. 168. 1.0/24
- D. 192. 168.0.0/8

**Answer:** B

**NEW QUESTION 87**

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 89**

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 94

A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.

What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

- A. Static IP Address
- B. Dialup User
- C. Dynamic DNS
- D. Pre-shared Key

**Answer:** B

#### Explanation:

Dialup user is used when the remote peer's IP address is unknown. The remote peer whose IP address is unknown acts as the dialup clien and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

#### NEW QUESTION 97

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:

FortiGate Security 7.2 Study Guide (p.285): "Remember that the web filtering profile has several features. So, if you have enabled many of them, the inspection order flows as follows: 1. The local static URL filter 2. FortiGuard category filtering (to determine a rating) 3. Advanced filters (such as safe search or removing Active X components)"

#### NEW QUESTION 100

An administrator configures outgoing interface any in a firewall policy. What is the result of the policy list view?

- A. Search option is disabled.
- B. Policy lookup is disabled.
- C. By Sequence view is disabled.
- D. Interface Pair view is disabled.

**Answer:** D

#### Explanation:

"If you use multiple source or destination interfaces, or the any interface in a firewall policy, you cannot separate policies into sections by interface pairs—some would be triplets or more. So instead, policies are then always displayed in a single list (By Sequence)."

#### NEW QUESTION 105

Which two statements are true about the FGCP protocol? (Choose two.)

- A. FGCP elects the primary FortiGate device.
- B. FGCP is not used when FortiGate is in transparent mode.
- C. FGCP runs only over the heartbeat links.
- D. FGCP is used to discover FortiGate devices in different HA groups.

**Answer:** AC

#### Explanation:

The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:

FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a variety of factors, such as the device's priority, to determine which device should be the primary.

FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices. FGCP does not run over other types of links, such as data links.

#### NEW QUESTION 108


Refer to the exhibits.

Exhibit A

Exhibit B

Search

Upstream Internet



Local-FortiGate Fabric Root

ISFW

Edit Address

Name

Net\_Add\_1

Color

Change

Type

Subnet

IP/Netmask

1.1.1.0 255.255.255.0

Interface

any

Fabric synchronization

☒

Static route configuration

☐

Comments

Write a comment...

0/255

Exhibit A

Exhibit B

Local-FortiGate # show full-configuration system csf

config system csf

set status enable

set upstream ''

set upstream-port 8013

set group-name "fortinet"

set group-password ENC Y9ynT+64RpCTpVdgSmoQH242mYSIzNNzLNvgzMXjyN9hSjIJE3KYJlo3XxygldvNxPI8T5xctBUSzy7rgIcHcA/qHrByXSXfPEeHC6ufkqlPJrW6GypwDUB5O3VFgPbASFYyteQesmwoJtGe84BLqa+hUcgunLD1z/97sBp+PLt5nrA==

set accept-auth-by-cert enable

set log-unification enable

set authorization-request-type serial

set fabric-workers 2

set downstream-access disable

set configuration-sync default

set fabric-object-unification default

set saml-configuration-sync default

ISFW # show full-configuration system csf

config system csf

set status enable

set upstream "10.0.1.254"

set upstream-port 8013

set group-name ''

set accept-auth-by-cert enable

set log-unification enable

set authorization-request-type serial

set fabric-workers 2

set downstream-access disable

set configuration-sync default

set saml-configuration-sync local

end

ISFW #

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).  
What must the administrator do to synchronize the address object?

- A. Change the csf setting on ISFW (downstream) to set configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to set authorization-request-type certificate.
- C. Change the csf setting on both devices to set downstream-access enable.
- D. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.

Answer: C

NEW QUESTION 109

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

NEW QUESTION 112

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
<b>IP Range/Subnet</b>	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
<b>FQDN</b>	
facebook.com	facebook.com

### Internet Service Object

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

### 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 114**

Refer to the exhibit.

Edit IPS Sensor

Name

WINDOWS\_SERVERS

Comments

Write a comment...

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	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
<div>OS</div> Windows		<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Disabled	<input checked="" type="checkbox"/> 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 117

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	<input checked="" type="checkbox"/> Allow
News and Media	<input checked="" type="checkbox"/> Allow
Social Networking	<input checked="" type="checkbox"/> Block
Political Organizations	<input checked="" type="checkbox"/> Allow
Reference	<input checked="" type="checkbox"/> Allow
Global Religion	<input checked="" type="checkbox"/> Allow
Shopping	<input checked="" type="checkbox"/> Allow
Society and Lifestyles	<input checked="" type="checkbox"/> Allow
Sports	<input checked="" type="checkbox"/> Allow

Static URL Filter

Block invalid URLs

☐

URL Filter

☒

+ Create New

Edit

Delete

Search

URL	Type	Action	Status
twitter.com	Wildcard	<input checked="" type="checkbox"/> Allow	<input checked="" type="checkbox"/> 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.

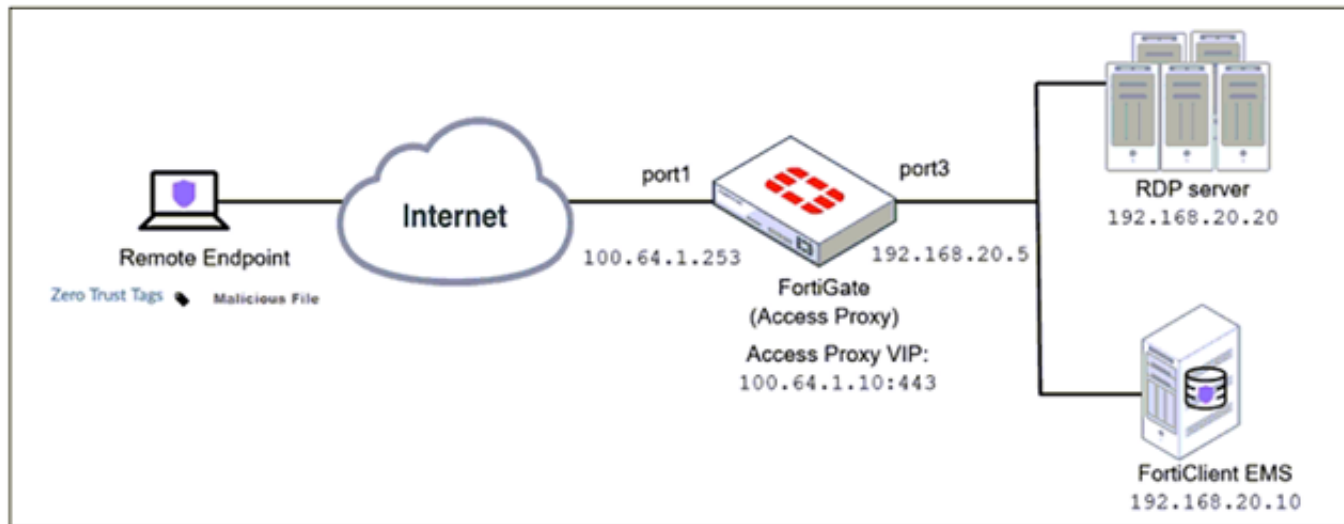
D. On the Static URL Filter configuration, set Action to Monitor.

Answer: C

NEW QUESTION 120

Refer to the exhibit.





Based on the ZTNA tag, the security posture of the remote endpoint has changed. What will happen to endpoint active ZTNA sessions?

- A. They will be re-evaluated to match the endpoint policy.
- B. They will be re-evaluated to match the firewall policy.
- C. They will be re-evaluated to match the ZTNA policy.
- D. They will be re-evaluated to match the security policy.

**Answer: C**

**Explanation:**

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-zt> FortiGate Infrastructure 7.2 Study Guide (p.182):  
 "Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy."

**NEW QUESTION 121**

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 124**

Which statement describes a characteristic of automation stitches?

- A. They can have one or more triggers.
- B. They can be run only on devices in the Security Fabric.
- C. They can run multiple actions simultaneously.
- D. They can be created on any device in the fabric.

**Answer: C**

**Explanation:**

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/351998/creating-automation-stitches>

**NEW QUESTION 125**

Refer to the exhibit.

```
FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

S      *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
S      *>          [10/0] via 10.0.0.2, port2, [30/0]
S      0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C      *> 10.0.0.0/24 is directly connected, port2
S      172.13.24.0/24 [10.0] is directly connected, port4
C      *> 172.20.121.0/24 is directly connected, port1
S      *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C      *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

- A. The port3 default route has the lowest metric.
- B. The port1 and port2 default routes are active in the routing table.
- C. The ports default route has the highest distance.
- D. There will be eight routes active in the routing table.

**Answer:** BC

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-identify-Inactive-Routes-in-the-Routing/ta-p>

**NEW QUESTION 130**

Refer to the exhibit.

NameCustom\_Profile

Comments0/255

Access Permissions

Access Control	Permissions	Set All
Security Fabric	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
FortiView	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
User & Device	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
Firewall	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
Log & Report	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
Network	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
System	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
Security Profile	<div><div>None</div><div>Read</div><div>Read/Write</div><div>Custom</div></div>	
VPN	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
WAN Opt & Cache	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	
WiFi & Switch	<div><div>None</div><div>Read</div><div>Read/Write</div></div>	

Permit usage of CLI diagnostic commands

Override Idle Timeout

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

- A. Custom permission for Network
- B. Read/Write permission for Log & Report
- C. CLI diagnostics commands permission
- D. Read/Write permission for Firewall

**Answer:** C

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220>

**NEW QUESTION 133**

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 137**

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.  
In this scenario, which statement about VLAN IDs is true?

- A. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.
- B. The two VLAN subinterfaces must have different VLAN IDs.
- C. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.
- D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

**Answer:** CD

#### NEW QUESTION 140

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\_SENT 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:** A

#### Explanation:

Indicates TCP (proto=6) session in SYN\_SENT state (proto=state=2) <https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

#### NEW QUESTION 142

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 144

Consider the topology:

Application on a Windows machine <--(SSL VPN)--> FGT --> Telnet to Linux server.

An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.

The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

- A. Set the maximum session TTL value for the TELNET service object.
- B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.
- C. Create a new service object for TELNET and set the maximum session TTL.
- D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

**Answer:** CD

#### NEW QUESTION 149

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



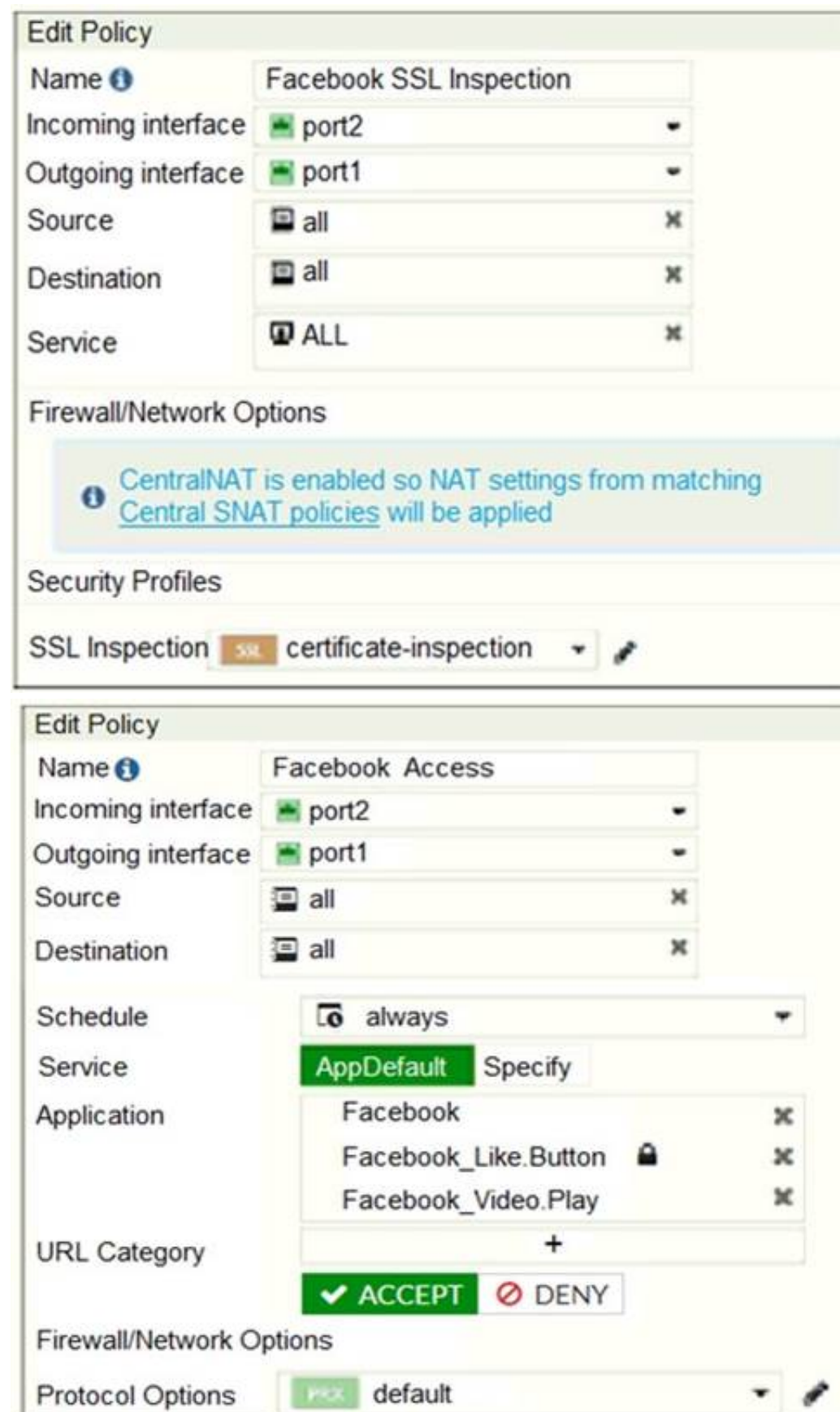
**Answer:** C

**Explanation:**

An aggregate interface is a logical interface that combines two or more physical interfaces into one virtual interface<sup>1</sup>. An aggregate interface can increase network bandwidth and provide redundancy by distributing traffic across multiple physical interfaces using a load balancing algorithm<sup>1</sup>. An aggregate interface can also support link aggregation control protocol (LACP) to negotiate the link aggregation settings with the connected device<sup>1</sup>.

**NEW QUESTION 152**

Refer to the exhibits.



**Exhibit A: Edit Policy (Facebook SSL Inspection)**

Field	Value
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

**Exhibit B: Edit Policy (Facebook Access)**

Field	Value
Name	Facebook Access
Incoming interface	port2
Outgoing interface	port1
Source	all
Destination	all
Schedule	always
Service	AppDefault
Application	Facebook, Facebook_Like.Button, Facebook_Video.Play
URL Category	ACCEPT
Protocol Options	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 than adding an app rule.

**NEW QUESTION 156**

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

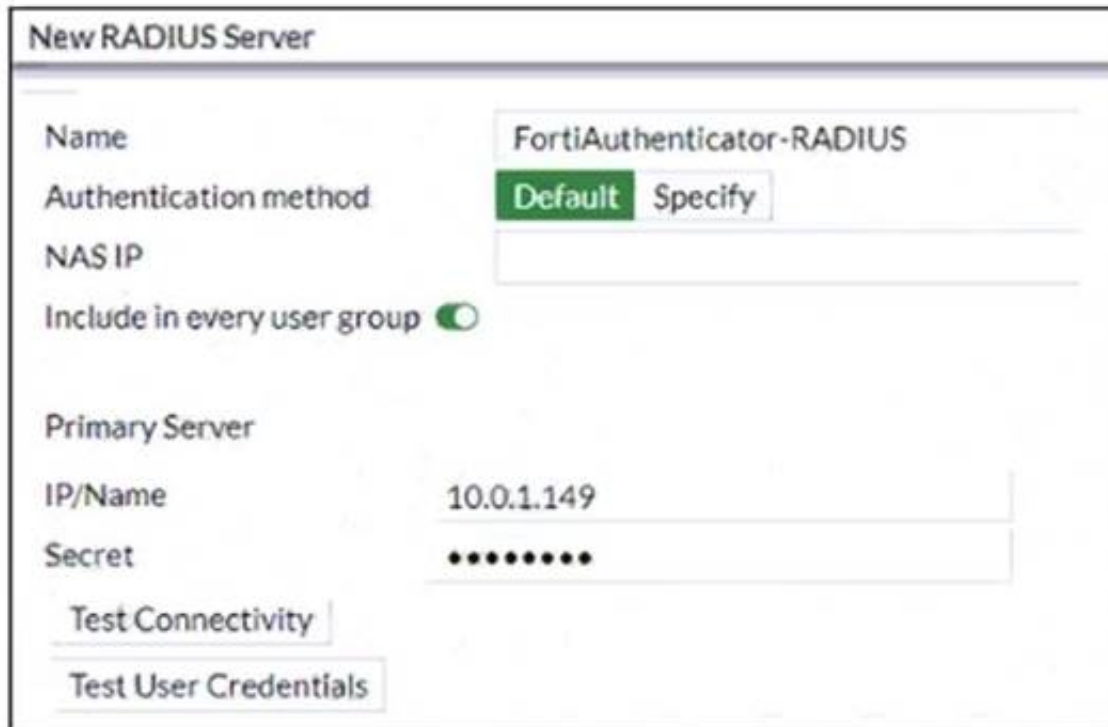
**Explanation:**

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 159**

Refer to the exhibit.

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.



What is the impact of using the Include in every user group option in a RADIUS configuration?

- A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- C. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
- D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

**Answer:** A

**NEW QUESTION 163**

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 166**

Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

- A. Log downloads from the GUI are limited to the current filter view
- B. Log backups from the CLI cannot be restored to another FortiGate
- C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
- D. Log downloads from the GUI are stored as LZ4 compressed files.

**Answer:** AB

**NEW QUESTION 170**

Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

- A. Subject Key Identifier value
- B. SMMIE Capabilities value
- C. Subject value
- D. Subject Alternative Name value

**Answer:** A

**NEW QUESTION 175**

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 176**

Refer to the exhibit.

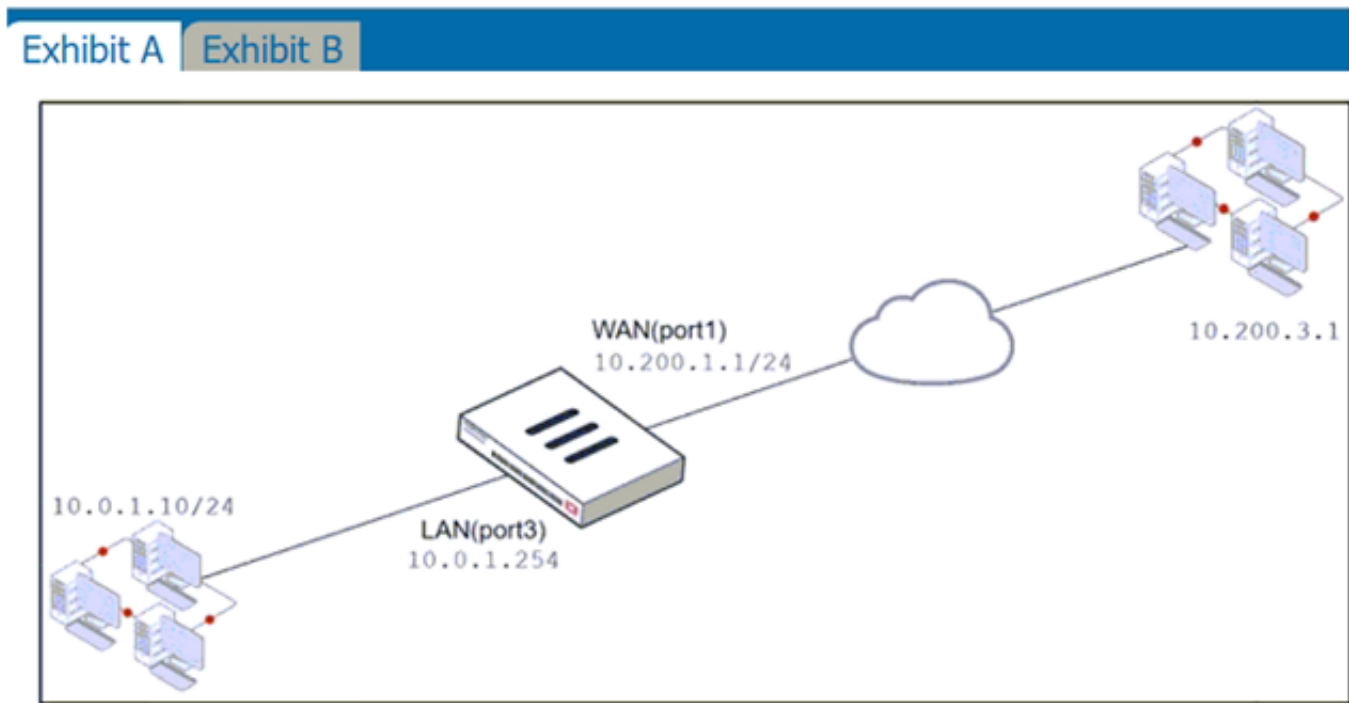


Exhibit A

Exhibit B

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

**Edit Virtual IP**

VIP type: IPv4

Name: VIP

Comments: Write a comment... 0/255

Color: Change

Network:

Interface: 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: 443

Map to IPv4 port: 443

**Edit Dynamic IP Pool**

Name: IP Pool

Comments: Write a comment... 0/255

Type: Overload One-to-One Fixed Port Range Port Block Allocation

External IP address/range: 10.200.1.100-10.200.1.100

NAT64: ☐

ARP Reply: ☒

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies 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. The first firewall policy has NAT enabled using IP Pool. 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?

- A. 10.200. 1. 1
- B. 10.200.3. 1
- C. 10.200. 1. 100
- D. 10.200. 1. 10

**Answer:** C

**Explanation:**

Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

#### NEW QUESTION 181

An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

- A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
- B. Create a new service object for HTTP service and set the session TTL to never
- C. Set the TTL value to never under config system-ttl
- D. Set the session TTL on the HTTP policy to maximum

**Answer: BC**

#### NEW QUESTION 183

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 188

Which statement about video filtering on FortiGate is true?

- A. Full SSL Inspection is not required.
- B. It is available only on a proxy-based firewall policy.
- C. It inspects video files hosted on file sharing services.
- D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

**Answer: B**

#### NEW QUESTION 192

When configuring a firewall virtual wire pair policy, which following statement is true?

- A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
- B. Only a single virtual wire pair can be included in each policy.
- C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
- D. Exactly two virtual wire pairs need to be included in each policy.

**Answer: A**

#### NEW QUESTION 193

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 197**

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 199**

Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 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=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53->10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

- A. The session is a UDP unidirectional state.
- B. The session is in TCP ESTABLISHED state.
- C. The session is a bidirectional UDP connection.
- D. The session is a bidirectional TCP connection.

**Answer: C**

**Explanation:**

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

**NEW QUESTION 204**

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 208**

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**

**Explanation:**

FortiGate Infrastructure 7.2 Study Guide (p.127-128): "As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended: (WMI, WinSecLog, and NetAPI)"



## NEW QUESTION 211

.....

## 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\_FGT-7.2 Practice Exam Features:

- \* NSE4\_FGT-7.2 Questions and Answers Updated Frequently
- \* NSE4\_FGT-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE4\_FGT-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE4\_FGT-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE4\\_FGT-7.2 Practice Test Here](#)**