

## Exam Questions NSE4\_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

[https://www.2passeasy.com/dumps/NSE4\\_FGT-7.2/](https://www.2passeasy.com/dumps/NSE4_FGT-7.2/)



### NEW QUESTION 1

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 Exhibit B

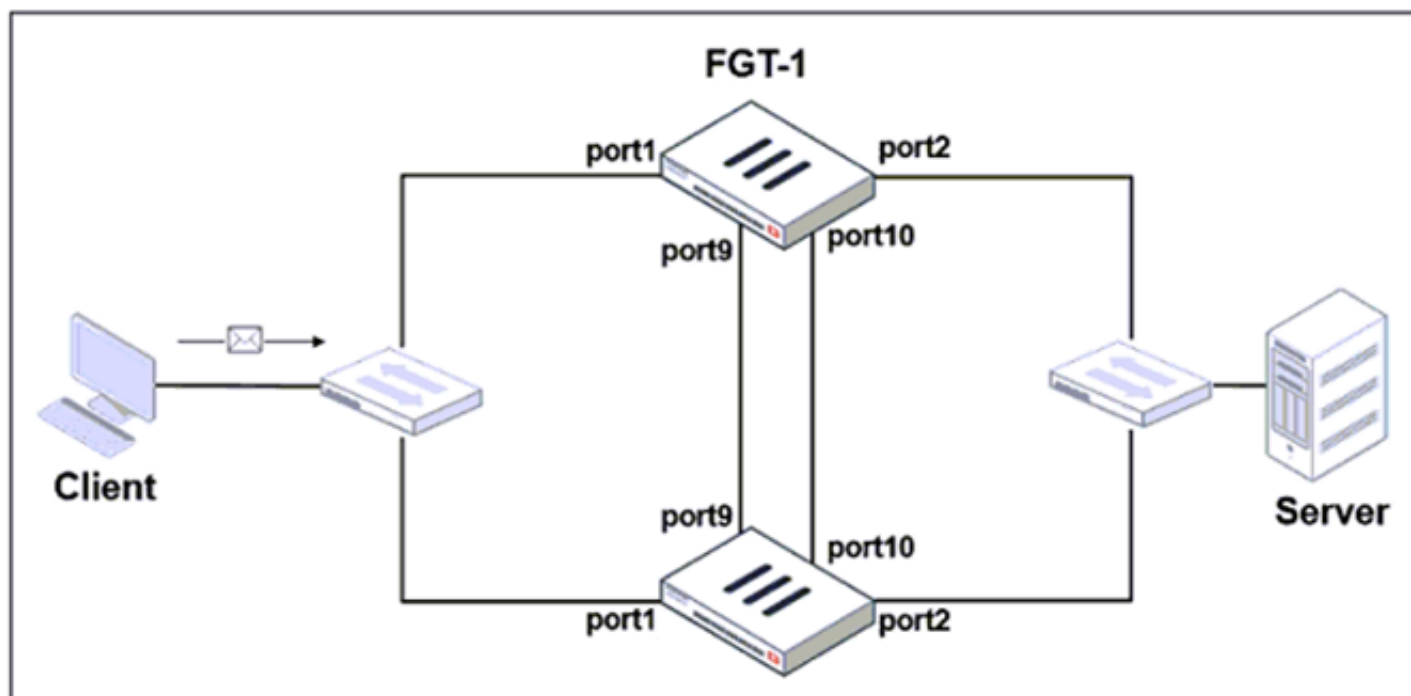


Exhibit A Exhibit B

```
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

# 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 2

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 3

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 4

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 5

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 6

An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192. 168. 1.0/24 and the remote quick mode selector is 192. 168.2.0/24.

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

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

**Answer:** C

#### Explanation:

For an IPsec VPN between site A and site B, the administrator has configured the local quick mode selector for site A as 192.168.1.0/24 and the remote quick mode selector as 192.168.2.0/24. This means that the VPN will allow traffic to and from the 192.168.1.0/24 subnet at site A to reach the 192.168.2.0/24 subnet at site B.

To complete the configuration, the administrator must configure the local quick mode selector for site B. To do this, the administrator must use the same subnet as the remote quick mode selector for site A, which is 192.168.2.0/24. This will allow traffic to and from the 192.168.2.0/24 subnet at site B to reach the 192.168.1.0/24 subnet at site A.

Therefore, the administrator must configure the local quick mode selector for site B as 192.168.2.0/24.

### NEW QUESTION 7

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 8

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 9

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 10

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

- A. It redirects the client request to the access proxy.
- B. It applies security profiles to protect traffic.
- C. It defines the access proxy.
- D. It enforces access control.

**Answer:** BD

#### Explanation:

A ZTNA rule is a policy that enforces access control and applies security profiles to protect traffic between the client and the access proxy<sup>1</sup>. A ZTNA rule defines the following parameters<sup>1</sup>:

- Incoming interface: The interface that receives the client request.
- Source: The address and user group of the client.
- ZTNA tag: The tag that identifies the domain that the client belongs to.
- ZTNA server: The server that hosts the access proxy.
- Destination: The address of the application that the client wants to access.
- Action: The action to take for the traffic that matches the rule. It can be accept, deny, or redirect.
- Security profiles: The security features to apply to the traffic, such as antivirus, web filter, application control, and so on.

A ZTNA rule does not redirect the client request to the access proxy. That is the function of a policy route that matches the ZTNA tag and sends the traffic to the ZTNA server<sup>2</sup>.

A ZTNA rule does not define the access proxy. That is done by creating a ZTNA server object that specifies the IP address, port, and certificate of the access proxy<sup>3</sup>.

FortiGate Infrastructure 7.2 Study Guide (p.177): "A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic."

#### NEW QUESTION 10

Refer to the exhibit.



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

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

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

**Answer:** B

**Explanation:**

FortiGate\_Security\_6.4 page 155 . In one-to-one, PAT is not required.

**NEW QUESTION 12**

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. The collector agent uses a Windows API to query DCs for user logins.
- B. NetAPI polling can increase bandwidth usage in large networks.
- C. The collector agent must search security event logs.
- D. The NetSession Enum function is used to track user logouts.

**Answer:** D

**Explanation:**

FortiGate\_Infrastructure\_7.0 page 270: "NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows."

**NEW QUESTION 16**

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuaid update servers
- C. Operating mode
- D. NGFW mode

**Answer:** CD

**Explanation:**

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate\_Infrastructure\_6.4\_Study\_Guide

**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 25**

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

- A. By default, FortiGate uses WINS servers to resolve names.
- B. By default, the SSL VPN portal requires the installation of a client's certificate.
- C. By default, split tunneling is enabled.
- D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

**Answer:** D

### NEW QUESTION 26

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 29

Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.

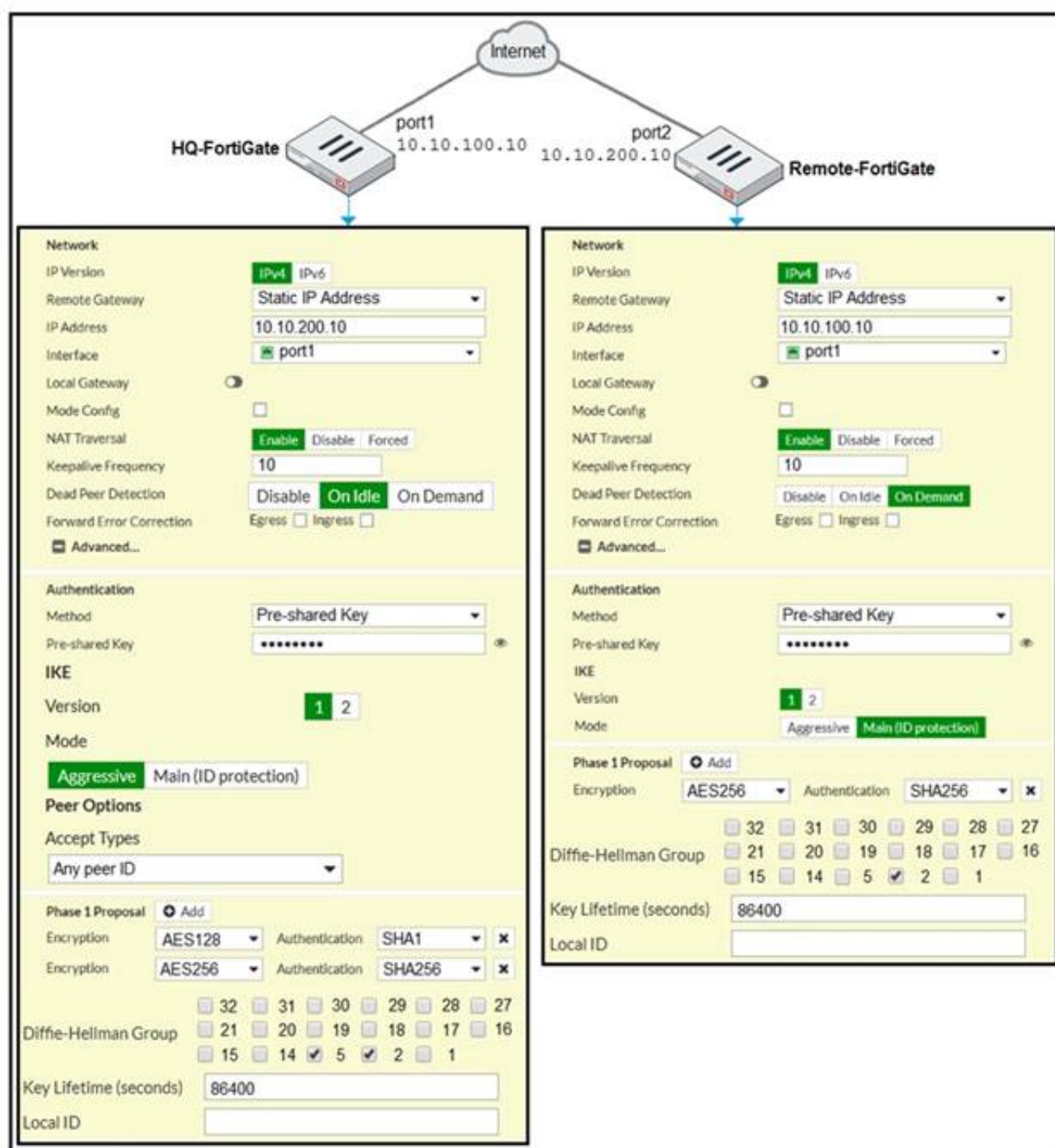
Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

- A. On HQ-FortiGate, enable Auto-negotiate.
- B. On Remote-FortiGate, set Seconds to 43200.
- C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
- D. On HQ-FortiGate, set Encryption to AES256.

Answer: D

### NEW QUESTION 30

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 34

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate points the collector agent to use a remote LDAP server.
- B. FortiGate uses the AD server as the collector agent.
- C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- D. FortiGate queries AD by using the LDAP to retrieve user group information.

**Answer:** CD

#### Explanation:

Fortigate Infrastructure 7.0 Study Guide P.272-273 <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

#### NEW QUESTION 37

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 VPNs12

\* 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 38

Refer to the exhibits.

#### Exhibit A Exhibit B

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 3 hours, 28 minutes
```

#### Exhibit A Exhibit B

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

- A. Administrators can access FortiGate only through the console port.
- B. FortiGate has entered conserve mode.
- C. FortiGate will start sending all files to FortiSandbox for inspection.
- D. Administrators cannot change the configuration.

**Answer:** BD

### 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 43

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 47

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 51

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 56

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:

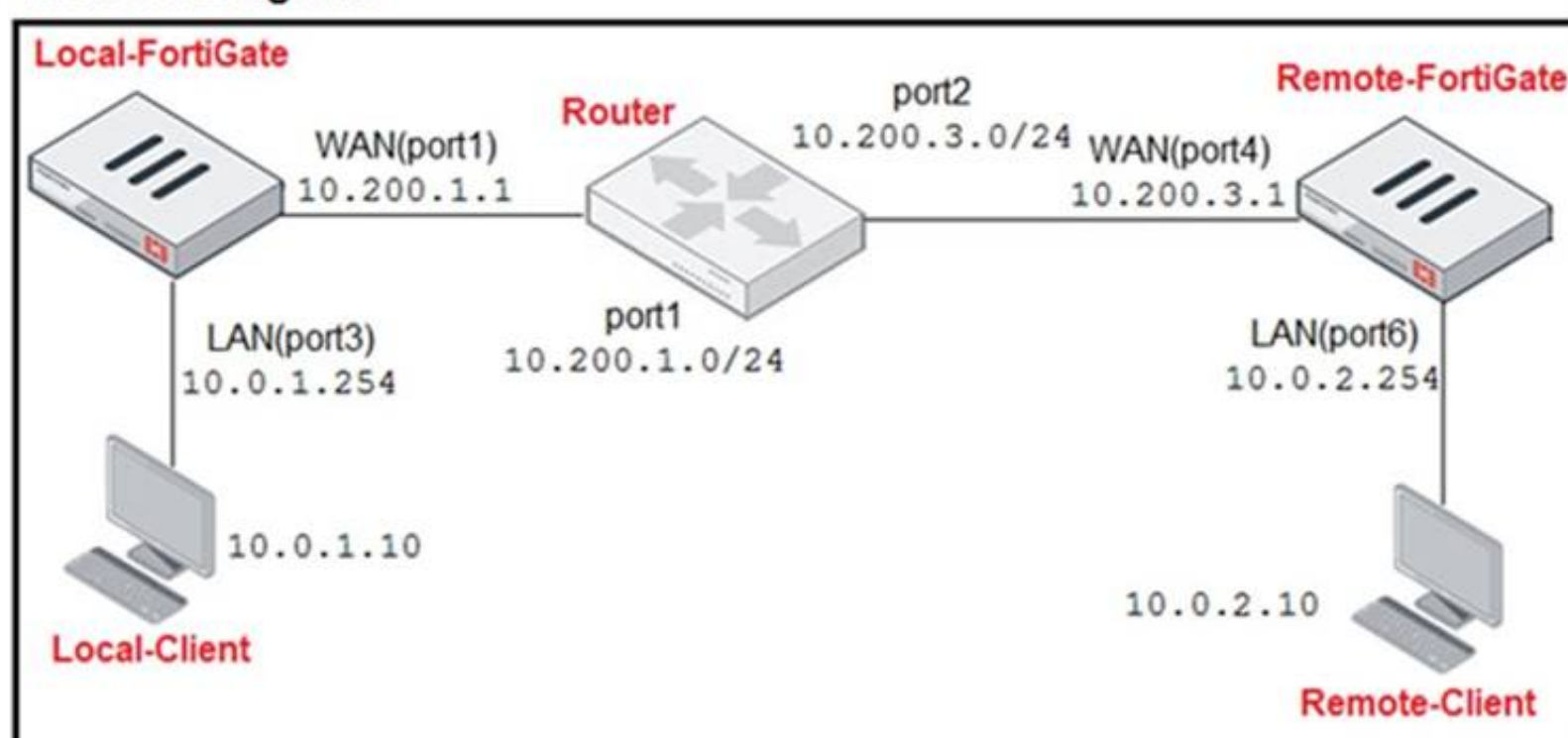
➤ The two VLAN subinterfaces must have different VLAN IDs. This is because the VLAN ID is used to tag the traffic with the appropriate VLAN information, and to separate the traffic into different VLANs<sup>2</sup>. If the two VLAN subinterfaces have the same VLAN ID, they will not be able to distinguish 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 58

Refer to the exhibit.

#### Network Diagram



## Central SNAT Policies Local-FortiGate

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

## IP Pool Local-FortiGate

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	Enabled

## Protocol Number Table

Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool 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.

A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.

Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0. 1. 10) pings the IP address of Remote-FortiGate (10.200.3. 1)?

- A. 10.200. 1. 149
- B. 10.200. 1. 1
- C. 10.200. 1.49
- D. 10.200. 1.99

**Answer:** D

### NEW QUESTION 61

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 overTLS.

**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 traffic1. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol2. 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.net1. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration1.

### NEW QUESTION 63

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 65

Which of the following SD-WAN load balancing method use interface weight value to distribute traffic? (Choose two.)

- A. Source IP
- B. Spillover
- C. Volume
- D. Session

**Answer:** CD

**Explanation:**

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing>

**NEW QUESTION 70**

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 74**

What are two characteristics of FortiGate HA cluster virtual IP addresses? (Choose two.)

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

**Answer:** AD

**Explanation:**

Fortigate Infrastructure 7.2 Study Guide page 301 FortiGate Infrastructure 7.2 Study Guide (p.301):

"FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number."

"A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster." "The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data." <https://networkinterview.com/fortigate-ha-high-availability/>

**NEW QUESTION 75**

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 80**

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scanning of application traffic to the DNS protocol only.
- B. It limits the scanning of application traffic to use parent signatures only.
- C. It limits the scanning of application traffic to the browser-based technology category only.
- D. It limits the scanning of application traffic to the application category only.

**Answer:** C

**Explanation:**

FortiGate Security 7.2 Study Guide (p.317): "You can configure the URL Category within the same security policy; however, adding a URL filter causes application control to scan applications in only the browser-based technology category, for example, Facebook Messenger on the Facebook website."

**NEW QUESTION 85**

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 87

Refer to the exhibit.



The screenshot shows the FortiGate SLA configuration page. The Name is SLA1. The Protocol is set to Ping. The Server field contains two entries: 4.2.2.2 and 4.2.2.1. The Participants field is set to All SD-WAN Members, with a Specify button. Below this, there are two entries: port1 and port2. The Enable probe packets checkbox is unchecked.

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic. Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

- A. The Detection Mode setting is not set to Passive.
- B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
- C. The configured participants are not SD-WAN members.
- D. The Enable probe packets setting is not enabled.

**Answer: BD**

### NEW QUESTION 90

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 92

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 95

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 98

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 100

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 105

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 109

On FortiGate, which type of logs record information about traffic directly to and from the FortiGate management IP addresses?

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

**Answer:** C

#### NEW QUESTION 111

Which timeout setting can be responsible for deleting SSL VPN associated sessions?

- A. SSL VPN idle-timeout
- B. SSL VPN http-request-body-timeout
- C. SSL VPN login-timeout
- D. SSL VPN dtls-hello-timeout

**Answer:** A

#### NEW QUESTION 112

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 117

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

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

**Answer:** B

#### Explanation:

FortiGate Security 7.2 Study Guide (p.67): "When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer."

#### NEW QUESTION 118

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 123

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 126

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 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0.0
FQDN 5	
facebook.com	facebook.com

### Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1,633		
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 129

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 133

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.

NameAllow\_Twitter

CommentsWrite a comment...0/255

Feature setFlow-basedProxy-based

FortiGuard Category Based Filter

AllowMonitorBlockWarningAuthenticate

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 NewEditDeleteSearch

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 134

By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

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

Answer: A

Explanation:

y default, "fortiguard-anycast" is enabled, and this setting only works with "set protocol https". To use udp (ie. "set protocol udp"), "fortiguard-anycast" must be disabled.

NEW QUESTION 136

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 140

Examine this output from a debug flow:

Passing Certification Exams Made Easy

visit - https://www.2PassEasy.com



```
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> <https://www.fortinetguru.com/2016/03/what-is-policy-id-0-and-why-lot-of-denied-traffic-on-this-policy/>

#### NEW QUESTION 144

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

- \* All traffic must be routed through the primary tunnel when both tunnels are up
- \* The secondary tunnel must be used only if the primary tunnel goes down
- \* In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two.)

- A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
- B. Enable Dead Peer Detection.
- C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
- D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

**Answer:** BC

**Explanation:**

Study Guide – IPsec VPN – IPsec configuration – Phase 1 Network.

When Dead Peer Detection (DPD) is enabled, DPD probes are sent to detect a failed tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same destination, and you want to failover to a backup connection when the primary connection fails to keep the connectivity between the sites up.

There are three DPD modes. On demand is the default mode. Study Guide – IPsec VPN – Redundant VPNs.

Add one phase 1 configuration for each tunnel. DPD should be enabled on both ends. Add at least one phase 2 definition for each phase 1.

Add one static route for each path. Use distance or priority to select primary routes over backup routes (routes for the primary VPN must have a lower distance or lower priority than the backup). Alternatively, use dynamic routing.

Configure FW policies for each IPsec interface.

#### NEW QUESTION 147

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

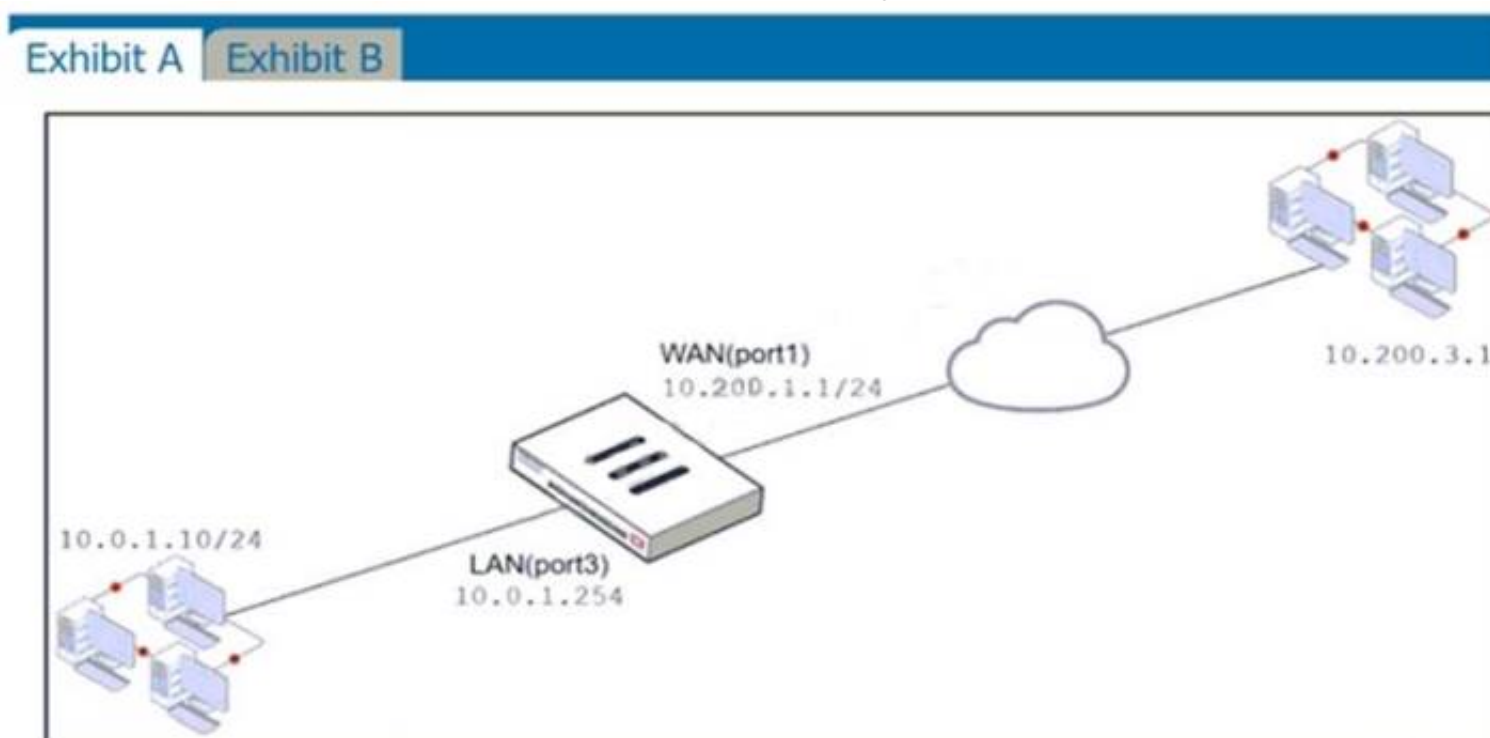


Exhibit A
Exhibit B

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 148

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

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

**Answer:** D

**Explanation:**

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

FortiGate Infrastructure 7.2 Study Guide (p.264): "...then FortiGate might drop interesting traffic because of the absence of active SAs. To prevent this, you can enable Auto-negotiate. When you do this, FortiGate not only negotiates new SAs before the current SAs expire, but it also starts using the new SAs right away." "Another benefit of enabling Auto-negotiate is that the tunnel comes up and stays up automatically, even when there is no interesting traffic. When you enable Autokey Keep Alive and keep Auto-negotiate disabled, the tunnel does not come up automatically unless there is interesting traffic. However, after the tunnel is up, it stays that way because FortiGate periodically sends keep alive packets over the tunnel. Note that when you enable Auto-negotiate, Autokey Keep Alive is implicitly enabled."

#### NEW QUESTION 150

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not Which configuration option is the most effective way to support this request?

- A. Implement a web filter category override for the specified website
- B. Implement a DNS filter for the specified website.
- C. Implement web filter quotas for the specified website
- D. Implement web filter authentication for the specified website.

**Answer:** D

#### NEW QUESTION 152

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 156

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 161

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
rpdb_link_id= 00000000 rpdb_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 163

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 165

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

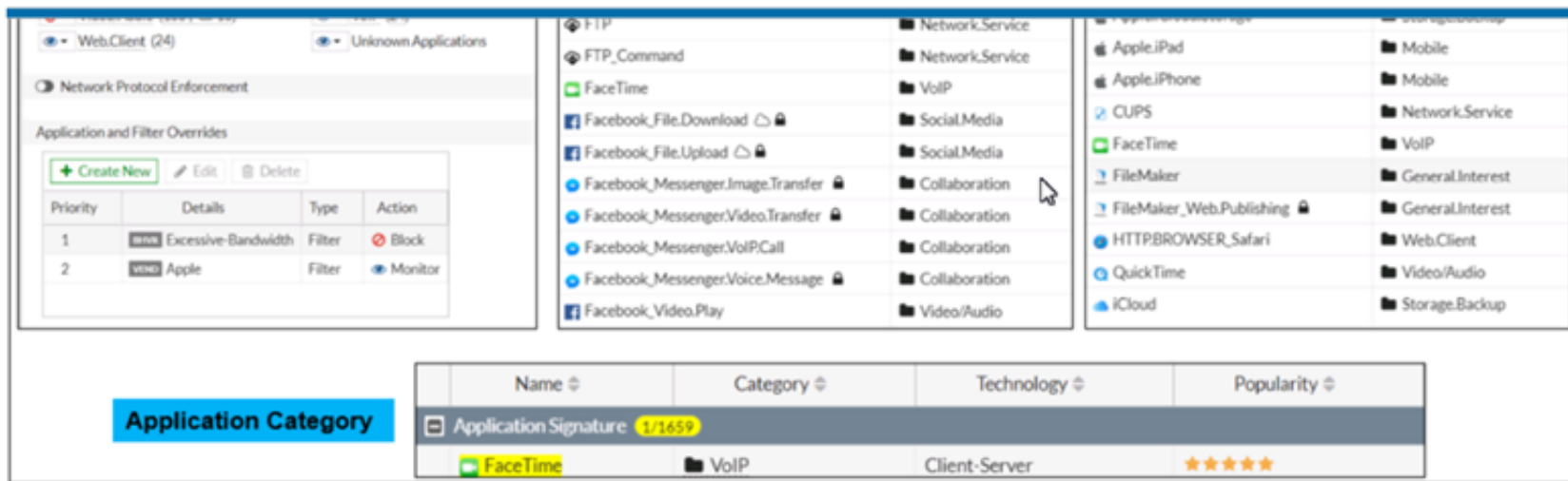


#### Explanation:

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 170

Refer to the exhibit to view the application control profile.



Based on the configuration, what will happen to Apple FaceTime?

- A. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration
- B. Apple FaceTime will be allowed, based on the Apple filter configuration.
- C. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn
- D. Apple FaceTime will be allowed, based on the Categories configuration.

Answer: A

#### NEW QUESTION 175

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 180

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 184

Which statement is correct regarding the security fabric?

- A. FortiManager is one of the required member devices.
- B. FortiGate devices must be operating in NAT mode.
- C. A minimum of two Fortinet devices is required.
- D. FortiGate Cloud cannot be used for logging purposes.

Answer: B

#### Explanation:

FortiGate Security 7.2 Study Guide (p.428): "You must have a minimum of two FortiGate devices at the core of the Security Fabric, plus one FortiAnalyzer or cloud logging solution. FortiAnalyzer Cloud or FortiGate Cloud can act as the cloud logging solution. The FortiGate devices must be running in NAT mode."

#### NEW QUESTION 186

Which two statements are correct about NGFW Policy-based mode? (Choose two.)

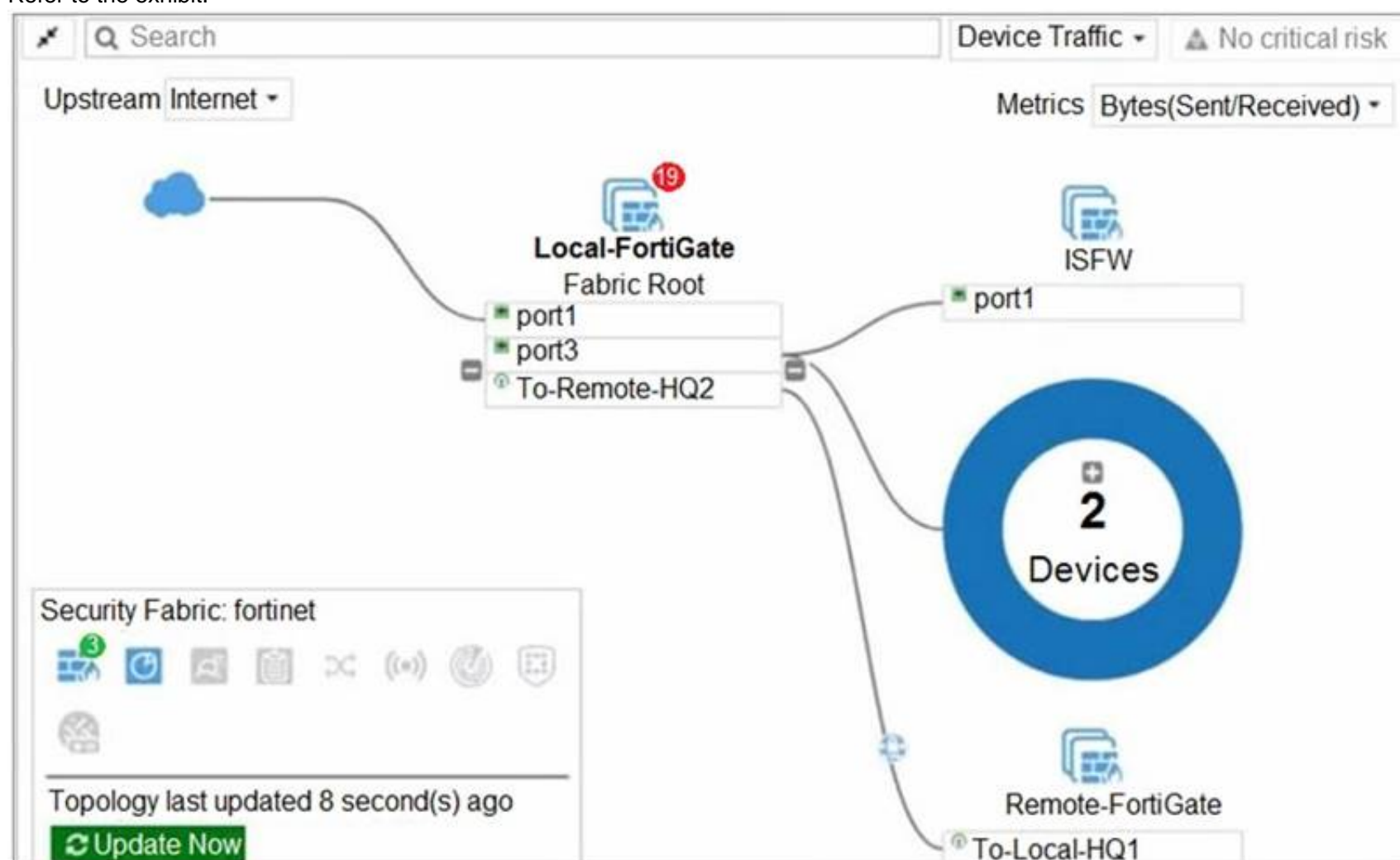
- A. NGFW policy-based mode does not require the use of central source NAT policy
- B. NGFW policy-based mode can only be applied globally and not on individual VDOMs
- C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
- D. NGFW policy-based mode policies support only flow inspection

Answer: CD



#### NEW QUESTION 191

Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

- A. There are five devices that are part of the security fabric.
- B. Device detection is disabled on all FortiGate devices.
- C. This security fabric topology is a logical topology view.
- D. There are 19 security recommendations for the security fabric.

**Answer:** CD

#### Explanation:

References: <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results>

<https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology>

#### NEW QUESTION 196

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 199

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scope of application control to the browser-based technology category only.
- B. It limits the scope of application control to scan application traffic based on application category only.
- C. It limits the scope of application control to scan application traffic using parent signatures only
- D. It limits the scope of application control to scan application traffic on DNS protocol only.

**Answer:** B

#### NEW QUESTION 201

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 204

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 205

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 208

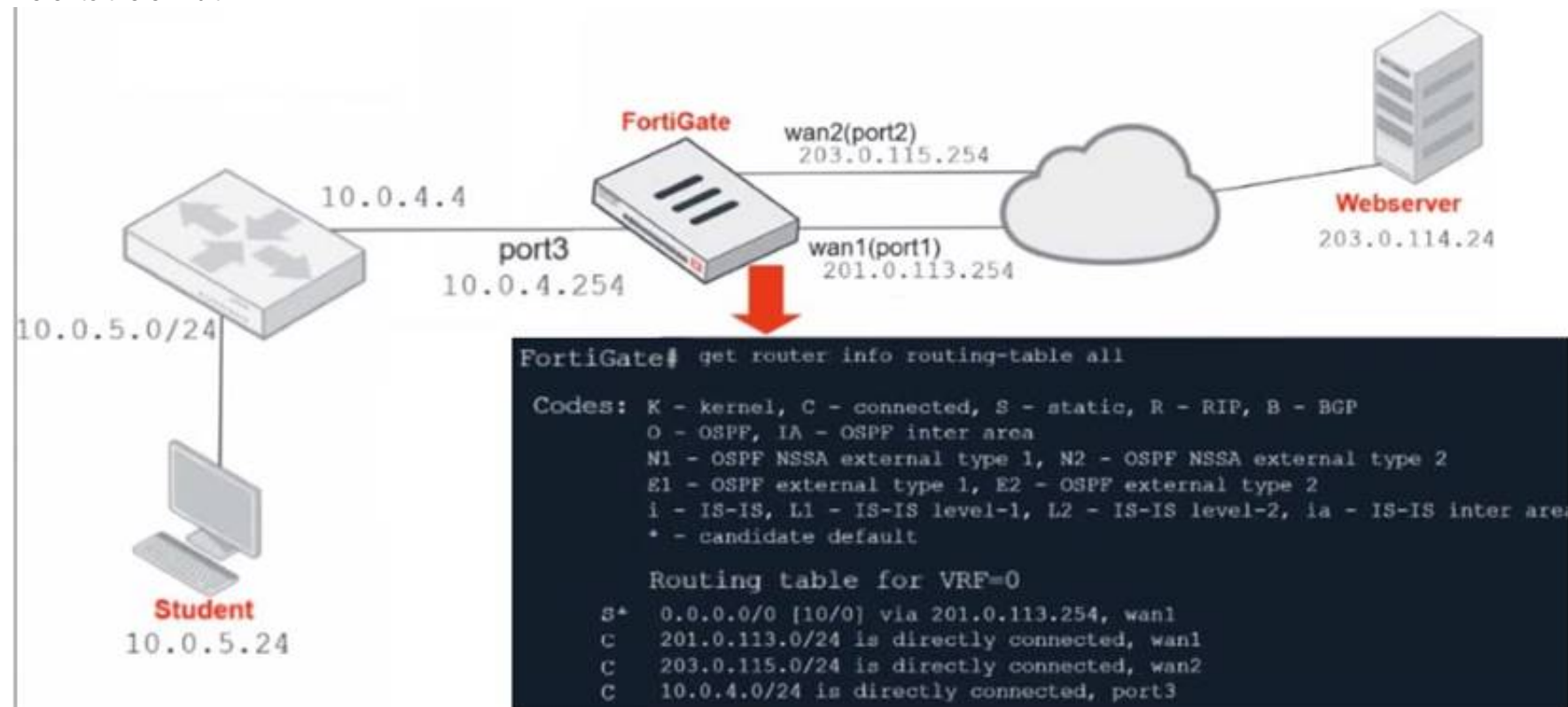
When configuring a firewall virtual wire pair policy, which following statement is true?

- 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 210

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 212

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) form 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) form local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

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

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

**Answer:** AC

#### NEW QUESTION 217

Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

- A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.
- B. The application signature database inspects traffic only from the original web application server.
- C. FortiGuard maintains only one signature of each web application that is unique.
- D. FortiGate can inspect sub-application traffic regardless where it was originate

**Answer:** D

#### NEW QUESTION 222

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 223

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4\_FGT-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4\_FGT-7.2 Product From:

[https://www.2passeasy.com/dumps/NSE4\\_FGT-7.2/](https://www.2passeasy.com/dumps/NSE4_FGT-7.2/)

## Money Back Guarantee

### 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