

NSE4_FGT-7.0 Dumps

Fortinet NSE 4 - FortiOS 7.0

https://www.certleader.com/NSE4_FGT-7.0-dumps.html



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

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

Answer: BD

NEW QUESTION 3

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 4

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, which configuration change will bring phase 2 up?

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

Answer: B

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

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 7

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 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 Interfac
- C. Outgoing Interfac
- 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 attacks¹

* 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 performance²

NEW QUESTION 10

Refer to the exhibit.

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1					
FTP.Login.Failed	100	Server	All	Pass	

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

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

Answer: D

Explanation:

Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be 'Pass' for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be 'Default'.

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

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 proxy¹. A ZTNA rule defines the following parameters¹:

- 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 server2.

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 proxy3.

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 15

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 16

An administrator is running the following sniffer command:

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

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

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

Answer: ABD

NEW QUESTION 21

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

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

Answer: AB

NEW QUESTION 29

An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSL/TLS connection. Which FortiGate configuration can achieve this goal?

- A. SSL VPN bookmark
- B. SSL VPN tunnel
- C. Zero trust network access
- D. SSL VPN quick connection

Answer: B

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.198): "Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as fortissl to the user's PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated. The main advantage of tunnel mode over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel."

An SSL VPN tunnel allows remote users to establish a secure and encrypted Virtual Private Network (VPN) connection to the private network using the SSL/TLS protocol¹. An SSL VPN tunnel can provide access to network resources such as FTP servers, as well as external applications running on the user's PC¹.

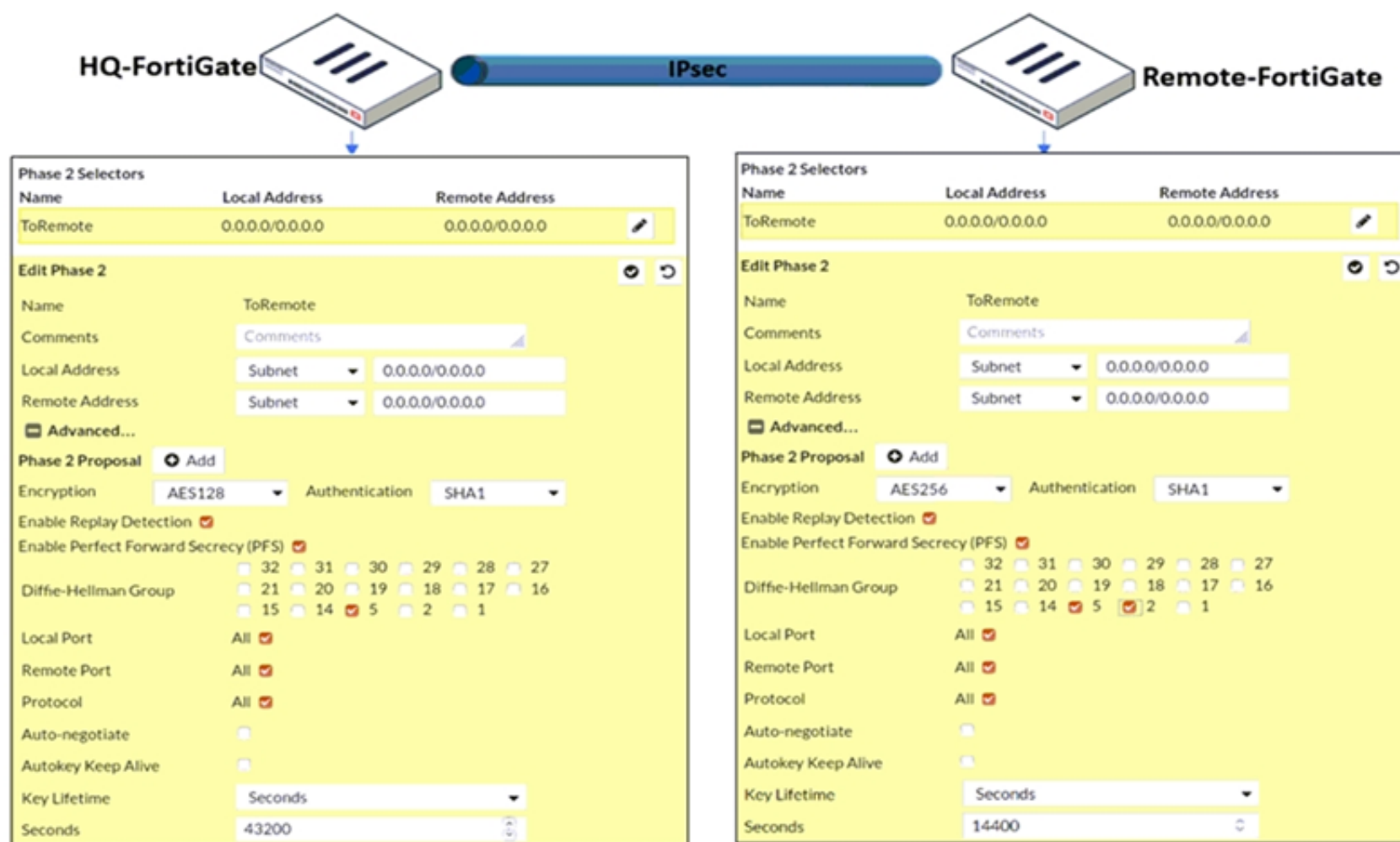
An SSL VPN bookmark is a web link that provides access to network resources through the SSL VPN web portal¹. It does not support external applications running on the user's PC.

Zero trust network access (ZTNA) is a security model that provides role-based application access to remote users without exposing the private network to the internet². It does not use SSL/TLS protocol, but rather a proprietary ZTNA protocol.

SSL VPN quick connection is a feature that allows users to connect to an SSL VPN tunnel without installing FortiClient or any other software on their PC³. It requires a web browser that supports Java or ActiveX. It does not support external applications running on the user's PC.

NEW QUESTION 34

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 36

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

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

Answer: B

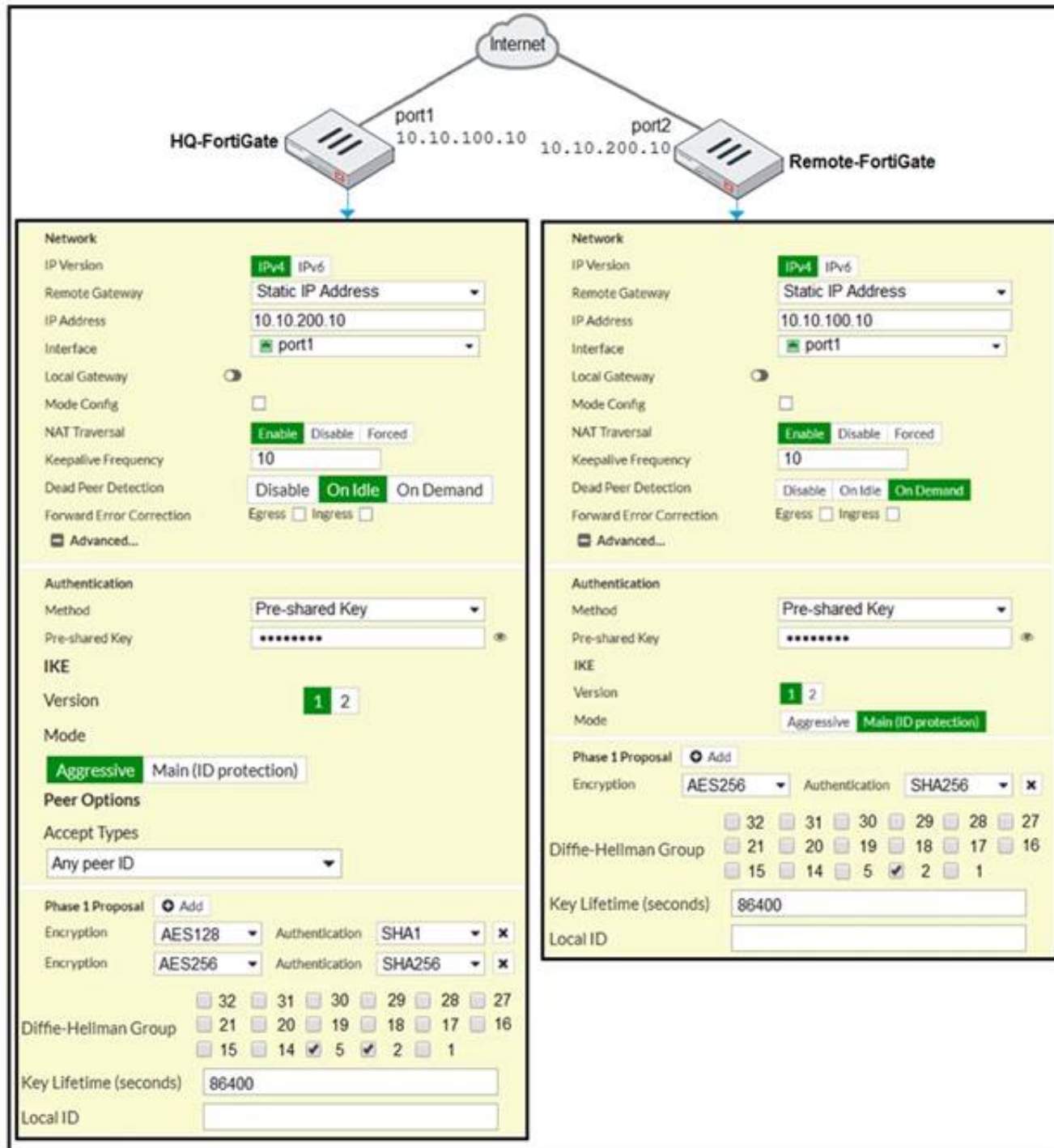
Explanation:

Strict Reverse Path Forwarding (RPF) is a security feature that is used to detect and prevent IP spoofing attacks on a network. It works by checking the routing

information for incoming packets to ensure that they are coming from the source address that is indicated in the packet's header. In strict RPF mode, the firewall will check the best route back to the source of the incoming packet using the incoming interface. If the packet's source address does not match the route back to the source, the packet is dropped. This helps to prevent attackers from spoofing their IP address and attempting to access the network.

NEW QUESTION 38

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 40

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 42

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

Edit Policy

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

Protocol Options

PRX default

Security Profiles

AntiVirus

AV default

Web Filter

DNS Filter

Application Control

IPS

SSL Inspection

SSL deep-inspection

Decrypted Traffic Mirror

Edit AntiVirus Profile

Name

default

Comments

Scan files and block viruses.

29/255

Detect Viruses

Block

Monitor

Feature set

Flow-based

Proxy-based

Inspected Protocols

HTTP

SMTP

POP3

IMAP

FTP

CIFS

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses

Include Mobile Malware Protection

Virus Outbreak Prevention

Use FortiGuard Outbreak Prevention Database

Use External Malware Block List

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 45

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 47

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

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

Answer: A

Explanation:

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

NEW QUESTION 49

Refer to the exhibits.

SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s) port1 + ×

Listen on Port 10443

Web mode access will be listening at <https://10.200.1.1:10443>

Redirect HTTP to SSL-VPN ☐

Restrict Access Allow access from any host Limit access to specific hosts

Idle Logout ☒

Inactive For 300 Seconds

Server Certificate Fortinet_Factory

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range Automatically assign addresses Specify custom IP ranges

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

DNS Server Same as client system DNS Specify

Specify WINS Servers ☐

Authentication/Portal Mapping ⓘ

+ Create New Edit Delete

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

Connection status

Connection: VPN

Server: <https://10.200.1.1:1443/>

Status: Connecting...

Duration: —

Bytes received: 0

Bytes sent: 0

Stop

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

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

Answer: A

NEW QUESTION 54

Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.

The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IP address 10.0.1.254/24.

Exhibit A Exhibit B

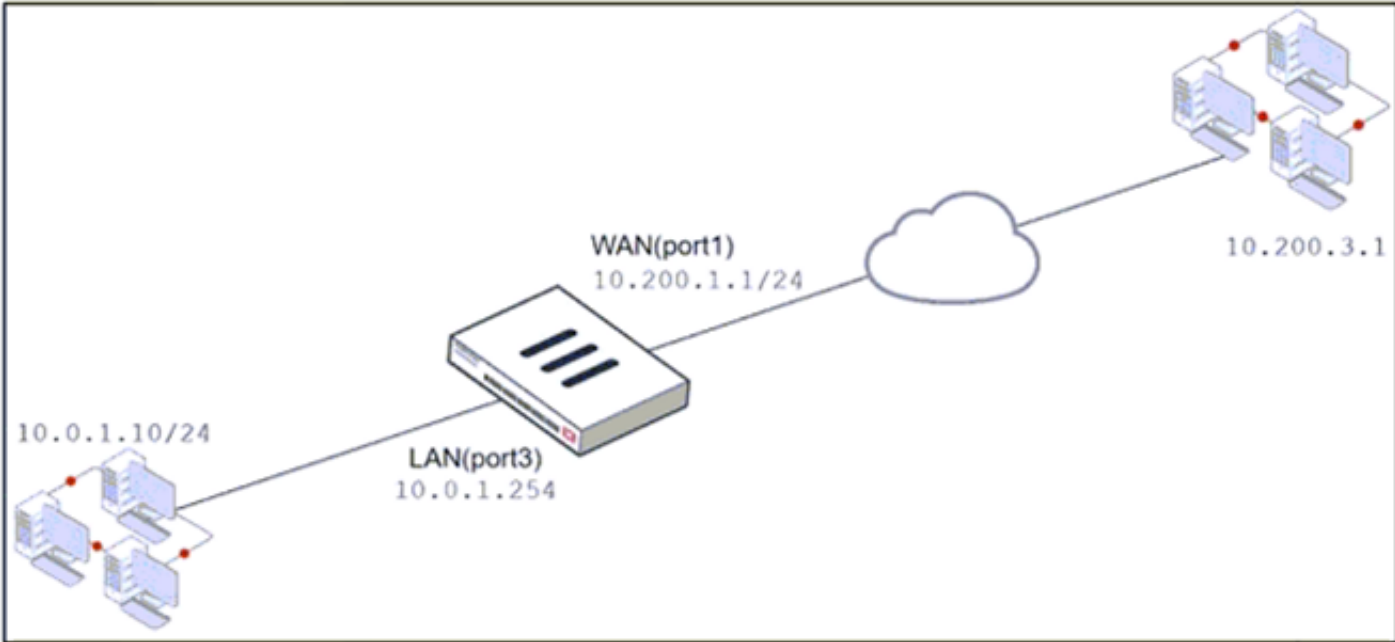


Exhibit A Exhibit B

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

Edit Virtual IP

VIP type

IPv4

Name

VIP

Comments

Write a comment...

0/255

Color

Change

Network

Interface

WAN (port1)

Type

Static NAT

External IP address/range

10.200.1.10

Map to

IPv4 address/range

10.0.1.10

Optional Filters

Port Forwarding

Protocol

TCP UDP SCTP ICMP

Port Mapping Type

One to one Many to many

External service port

10443

Map to IPv4 port

443

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

- A. 10.0.1.254, 10.0.1.10, and 443, respectively
- B. 10.0.1.254, 10.200.1.10, and 443, respectively
- C. 10.200.3.1, 10.0.1.10, and 443, respectively
- D. 10.0.1.254, 10.0.1.10, and 10443, respectively

Answer: C

Explanation:

The host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, which is the external IP address of the VIP object named VIP in Exhibit B1. The VIP object maps the external IP address and port to the internal IP address and port of the server 10.0.1.10 and 443, respectively1. The VIP object also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface2.

The firewall policy ID 1 in Exhibit B allows traffic from WAN (port1) to LAN (port3) with the destination address of VIP and the service of HTTPS1. The policy also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface2.

Therefore, after FortiGate forwards the packet to the destination, the source address, destination address, and destination port of the packet will be 10.200.3.1, 10.0.1.10, and 443, respectively.

You can find more information about VIP objects and firewall policies in the Fortinet Documentation

NEW QUESTION 57

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 60

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

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.73): "What about traffic originating from FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate. Traffic coming from FortiGate to those global services originates from the management VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM. It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate."

NEW QUESTION 61

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 it¹. 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 addresses¹.

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

and exit the FortiGate unit². A VLAN subinterface is created by adding a VLAN ID to a physical interface or an aggregate interface². A VLAN ID is a numerical identifier that distinguishes one VLAN from another².

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 VLANs². 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 tables³. Each VDOM operates independently from other VDOMs, and can have its own VLAN subinterfaces with different or identical VLAN IDs³. However, this requires inter-VDOM links to allow traffic between different VDOMs³.

NEW QUESTION 66

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 68

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 69

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 71

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 74

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 75

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 76

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

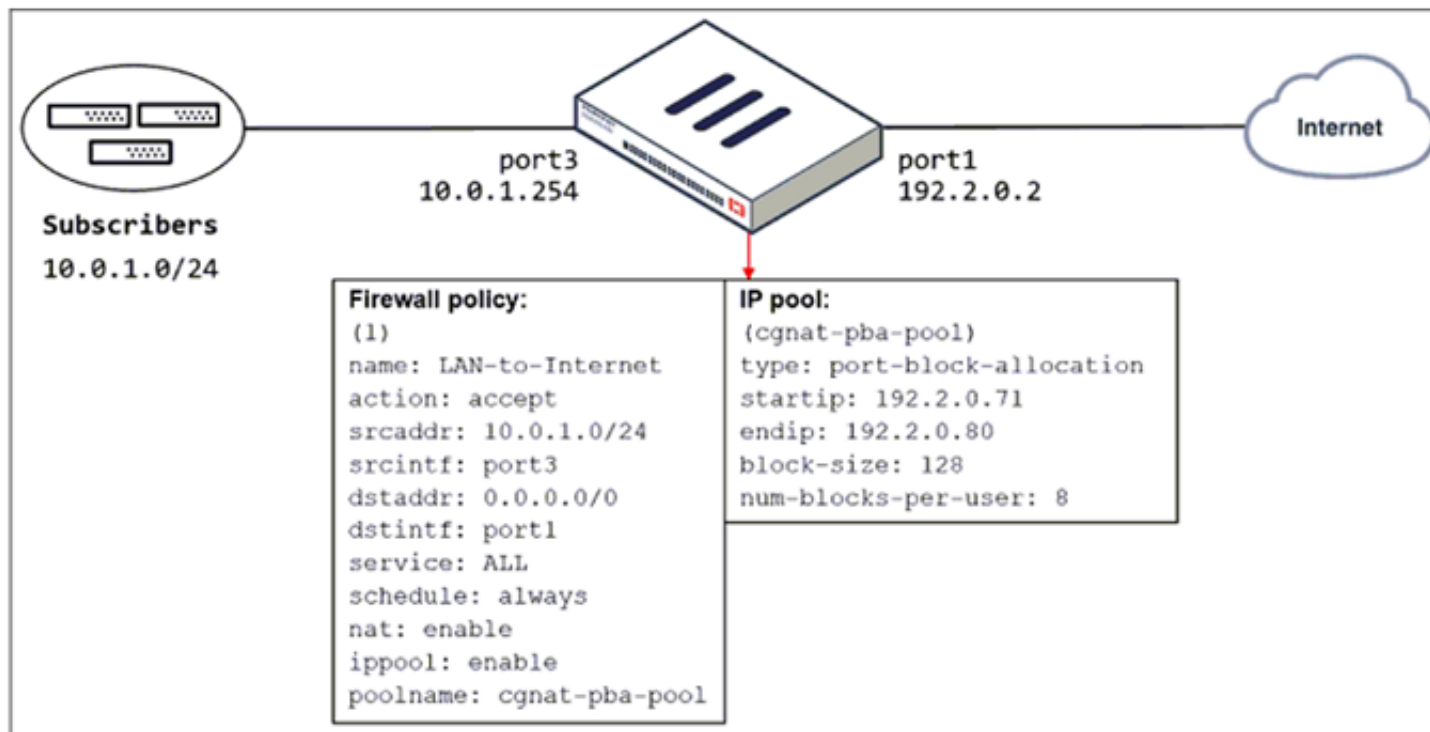
Explanation:

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 79

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 84

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 86

Refer to the exhibit.

The screenshot shows the FortiGate SLA configuration interface. The "Name" field is set to "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". The "Enable probe packets" checkbox is checked. The "Specify" button is highlighted.

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 91

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 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 96

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 102

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 107

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 112

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

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

Answer: BC

NEW QUESTION 117

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 118

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
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 119

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	Enabled	Enabled
<div>OS</div> Windows		Block	Disabled	Enabled

The exhibit shows the IPS sensor configuration.

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

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

Answer: AB

NEW QUESTION 122

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 124

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

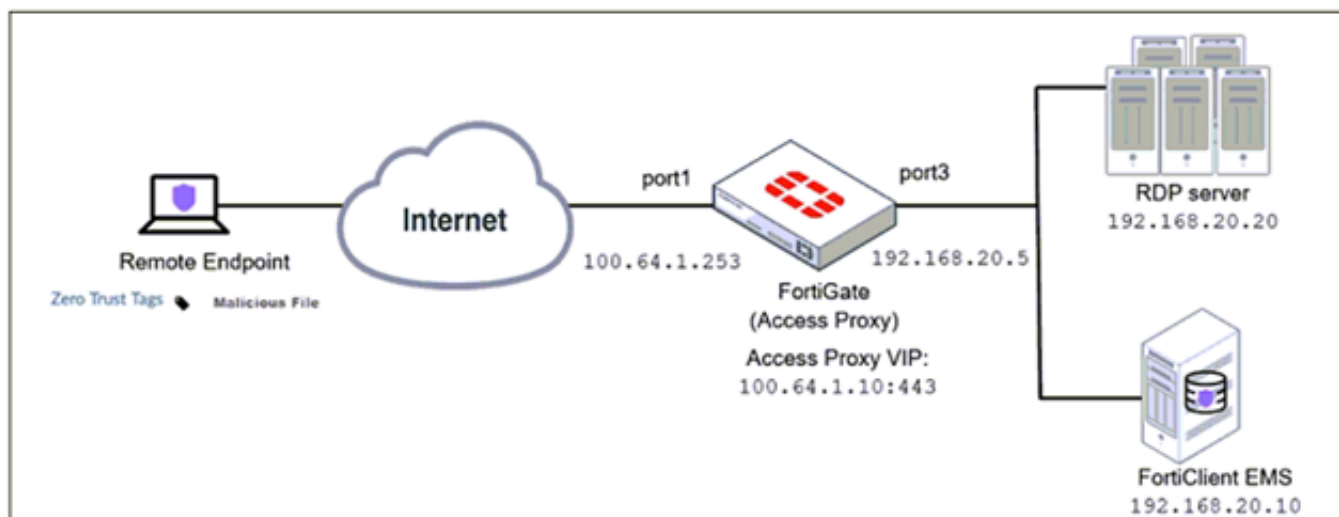
Answer: A

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 129

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 131

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 133

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.

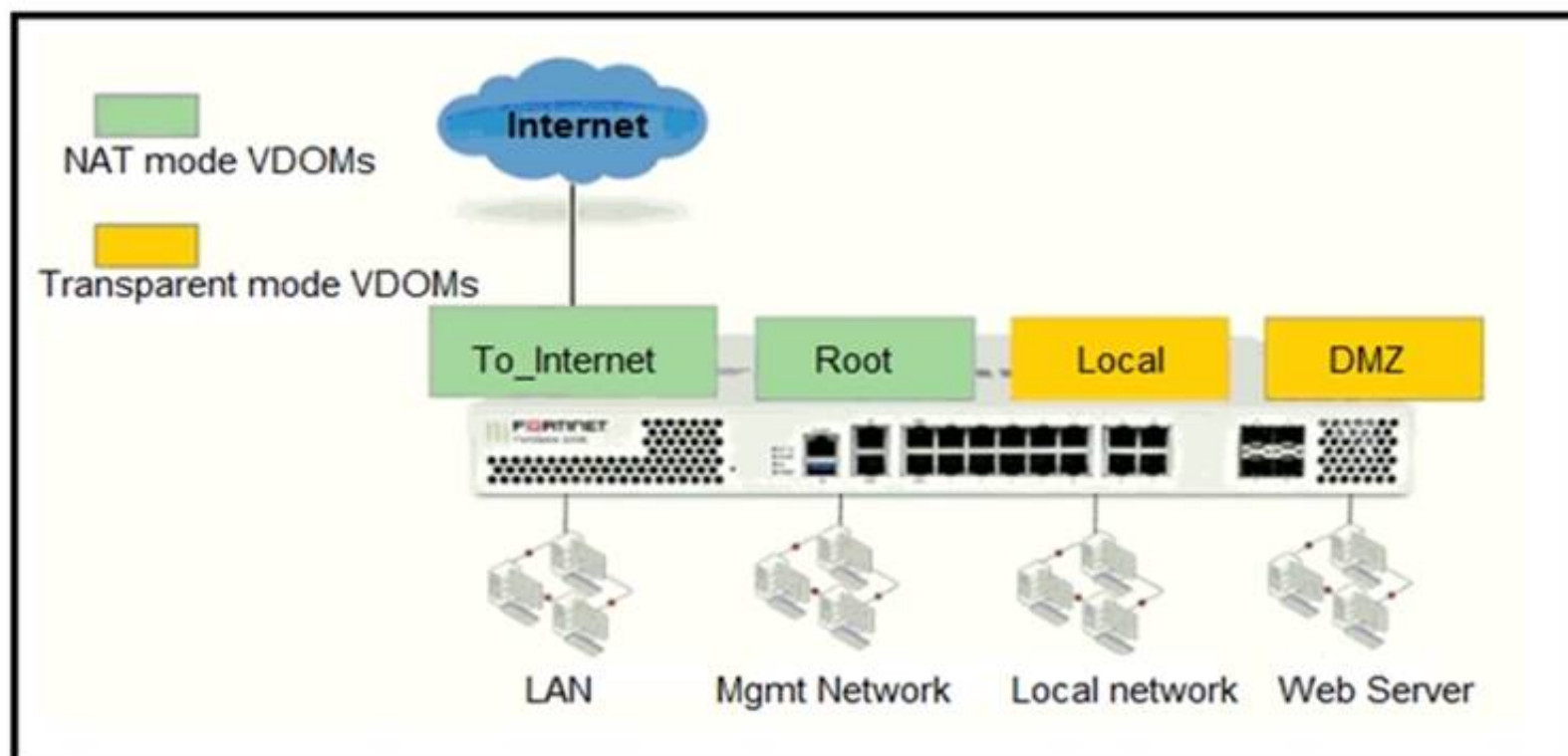
Add one phase 1 configuration for each tunnel. DPD should be enabled on both ends. Add at least one phase 2 definition for each phase 1.

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 135

Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.

The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem .

With this configuration, which statement is true?

- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.

- B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

NEW QUESTION 137

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]
        *>           [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 140

Refer to the exhibit.

Name Custom_Profile	
Comments	<input type="text"/> 0/255
Access Permissions	
Access Control	Permissions Set All ▾
Security Fabric	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
FortiView	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
User & Device	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
Firewall	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
Log & Report	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
Network	<input type="radio"/> None <input checked="" type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
System	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
Security Profile	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
VPN	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
WAN Opt & Cache	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
WiFi & Switch	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
Permit usage of CLI diagnostic commands <input type="checkbox"/>	
<input type="checkbox"/> 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 143

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 148

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 149

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 153

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

- A. IP tool references must be removed from existing firewall policies before enabling central NAT .
- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Answer: AB

NEW QUESTION 156

Refer to the exhibit.



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 161

In an explicit proxy setup, where is the authentication method and database configured?

- A. Proxy Policy
- B. Authentication Rule
- C. Firewall Policy
- D. Authentication scheme

Answer: D

NEW QUESTION 162

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 166

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.

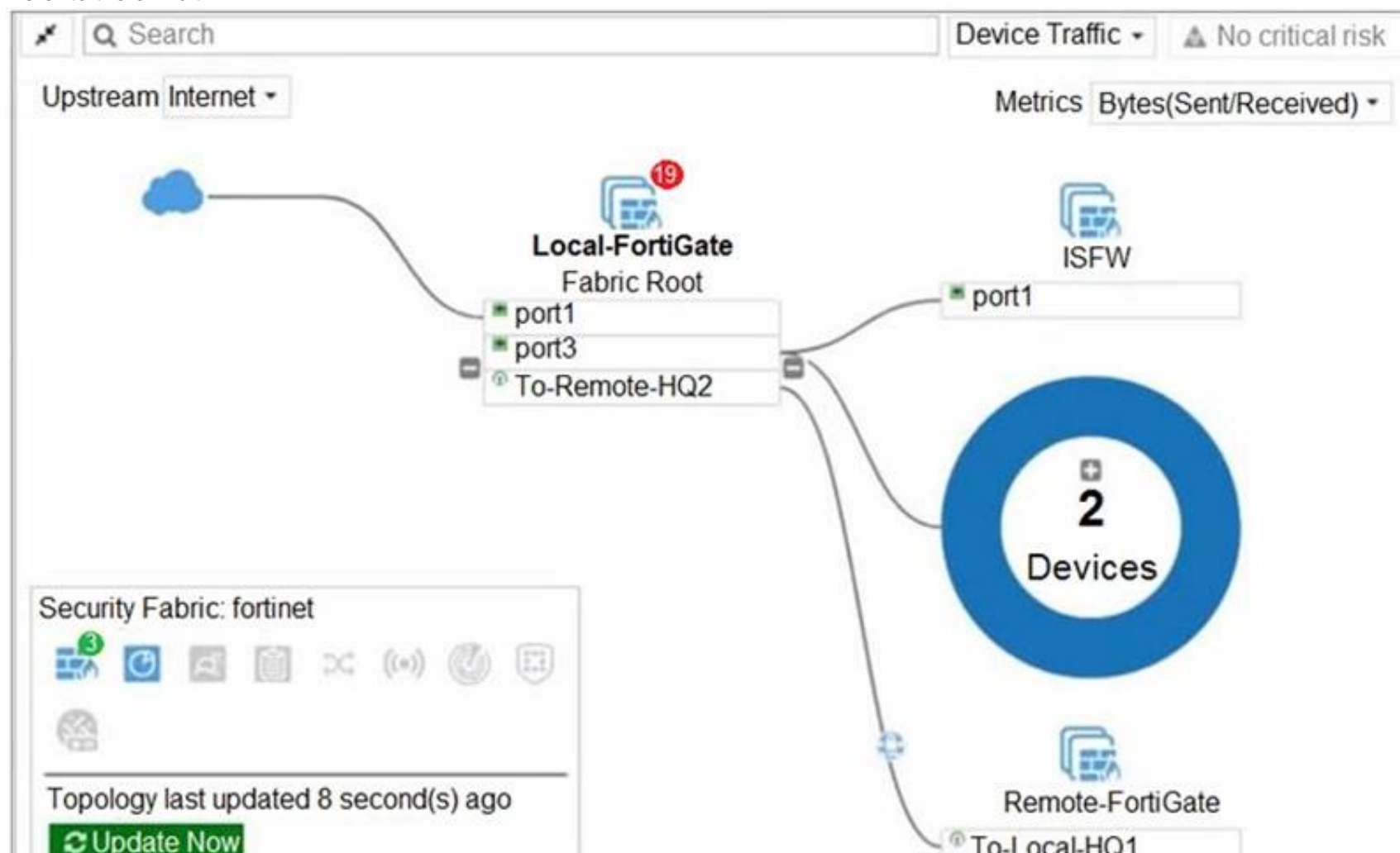
Answer: B

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 170

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 171

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

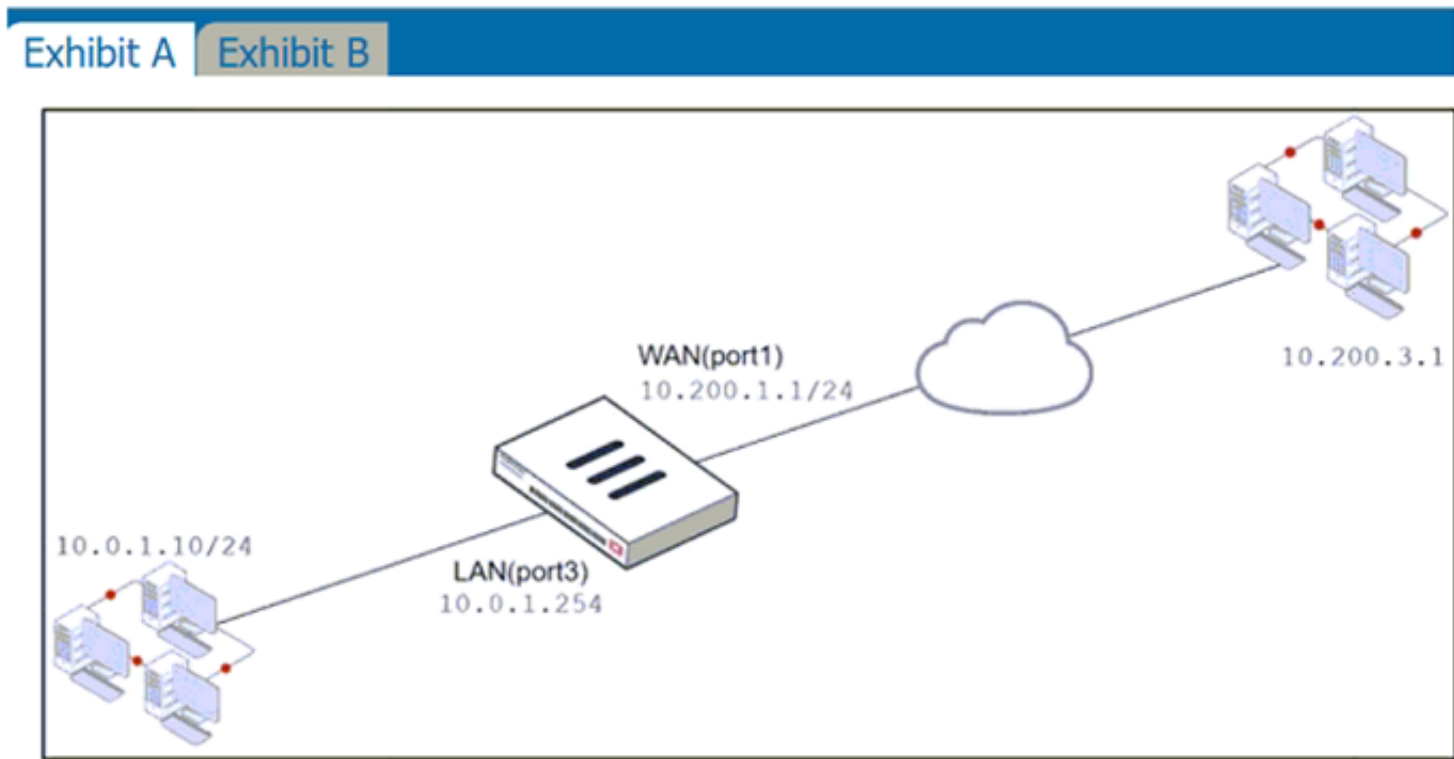


Exhibit A

Exhibit B

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

Which IP address will be used to source NAT the traffic, if a user with address 10.0.1.10 connects over SSH to the host with address 10.200.3.1?

- A. 10.200.1.10
- B. 10.0.1.254
- C. 10.200.1.1
- D. 10.200.3.1

Answer: C

Explanation:

Traffic is coming from LAN to WAN, matches policy Full_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

NEW QUESTION 174

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 175

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 180

Refer to the exhibit showing a debug flow output.

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

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

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

Answer: AC

Explanation:

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

- The protocol is 1, which means that the traffic uses ICMP protocol². ICMP is a protocol that is used to send error messages and test connectivity between devices².
- The session state is 0, which means that a new traffic session was created³. A session is a data structure that stores information about a connection between two devices³.
- The policy ID is 1, which means that the traffic matched the firewall policy with ID 14. A firewall policy is a rule that defines how FortiGate processes traffic based on the source, destination, service, and action parameters⁴.
- The action is 0, which means that the traffic was allowed by the firewall policy. An action is a parameter that specifies what FortiGate does with the traffic that matches a firewall policy.

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

- The debug flow is for ICMP traffic.
- A new traffic session was created.

NEW QUESTION 184

An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. A session for denied traffic is created.
- D. The number of logs generated by denied traffic is reduced.

Answer: CD

Explanation:

ses-denied-traffic

Enable/disable including denied session in the session table. <https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/20620/config-system-settings-block-session-timer>

Duration in seconds for blocked sessions . integer

Minimum value: 1 Maximum value: 300

30

<https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/1620/config-system-global>

NEW QUESTION 186

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

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

Answer: B

Explanation:

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

NEW QUESTION 190

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 194

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 196

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4_FGT-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4_FGT-7.0-dumps.html