

Fortinet.NSE4_FGT-7.2.vDec-2023.by.Jakmar.108q

Number: NSE4_FGT-7.2
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: NSE4_FGT-7.2
Exam Name: Fortinet NSE 4 - FortiOS 7.2

Exam A

QUESTION 1

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

Exhibit A

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

Exhibit B

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.

Correct Answer: B

Section:

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.

QUESTION 2

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.

Correct Answer: B, C

Section:

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.

QUESTION 3

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 4

Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

- A. Traffic between port2 and port2-vlan1 is allowed by default.
- B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- C. port1 is a native VLAN.
- D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Correct Answer: C, D

Section:

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf>
<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883>

QUESTION 5

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.

Correct Answer: B

Section:

QUESTION 6

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

Correct Answer: A, D

Section:

QUESTION 7

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'

Correct Answer: A

Section:

QUESTION 8

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.

Correct Answer: A, C

Section:

QUESTION 9

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.

Correct Answer: D

Section:

QUESTION 10

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.

Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN 0	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries	
Predefined Internet Services 1,635			
Facebook-Web	Destination	26,578	
IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80	TCP	Enabled
	443		
	8443		
1.9.91.17 - 1.9.91.18	443	UDP	Enabled
1.9.91.30	443	UDP	Enabled

Firewall Policies

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

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.

Correct Answer: B

Section:

Explanation:

We are looking for a policy that will allow or deny traffic from the source interface Port3 and source IP address 10.1.1.10 (LOCAL_CLIENT) to facebook.com TCP port 443 (HTTPS). There are only two policies that will match this traffic, policy ID 2 and 5. In FortiGate, firewall policies are evaluated from top to bottom. This means that the first policy that matches the traffic is applied, and subsequent policies are not evaluated. Based on the Policy Lookup criteria, Policy ID 5 will be highlighted

QUESTION 11

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.

Correct Answer: C, D

Section:

QUESTION 12

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.

Correct Answer: B

Section:

Explanation:

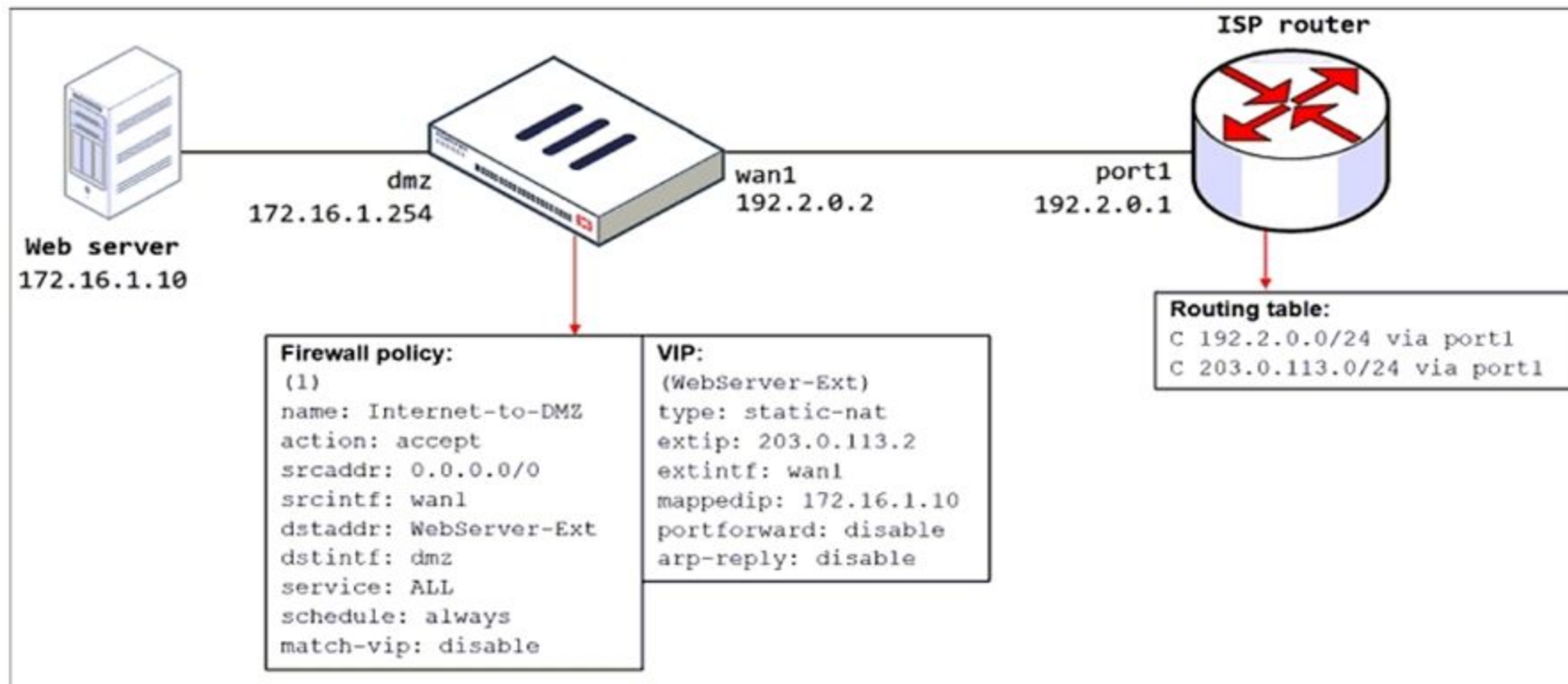
FortiGate Security 7.2 Study Guide (p.192): 'if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm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

QUESTION 13

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.

When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

- A. Configure a loopback interface with address 203.0.113.2/32.
- B. In the VIP configuration, enable arp-reply.
- C. Enable port forwarding on the server to map the external service port to the internal service port.
- D. In the firewall policy configuration, enable match-vip.

Correct Answer: B

Section:

Explanation:

FortiGate Security 7.2 Study Guide (p.115): 'Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled.'

QUESTION 14

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

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

Correct Answer: A, C

Section:

Explanation:

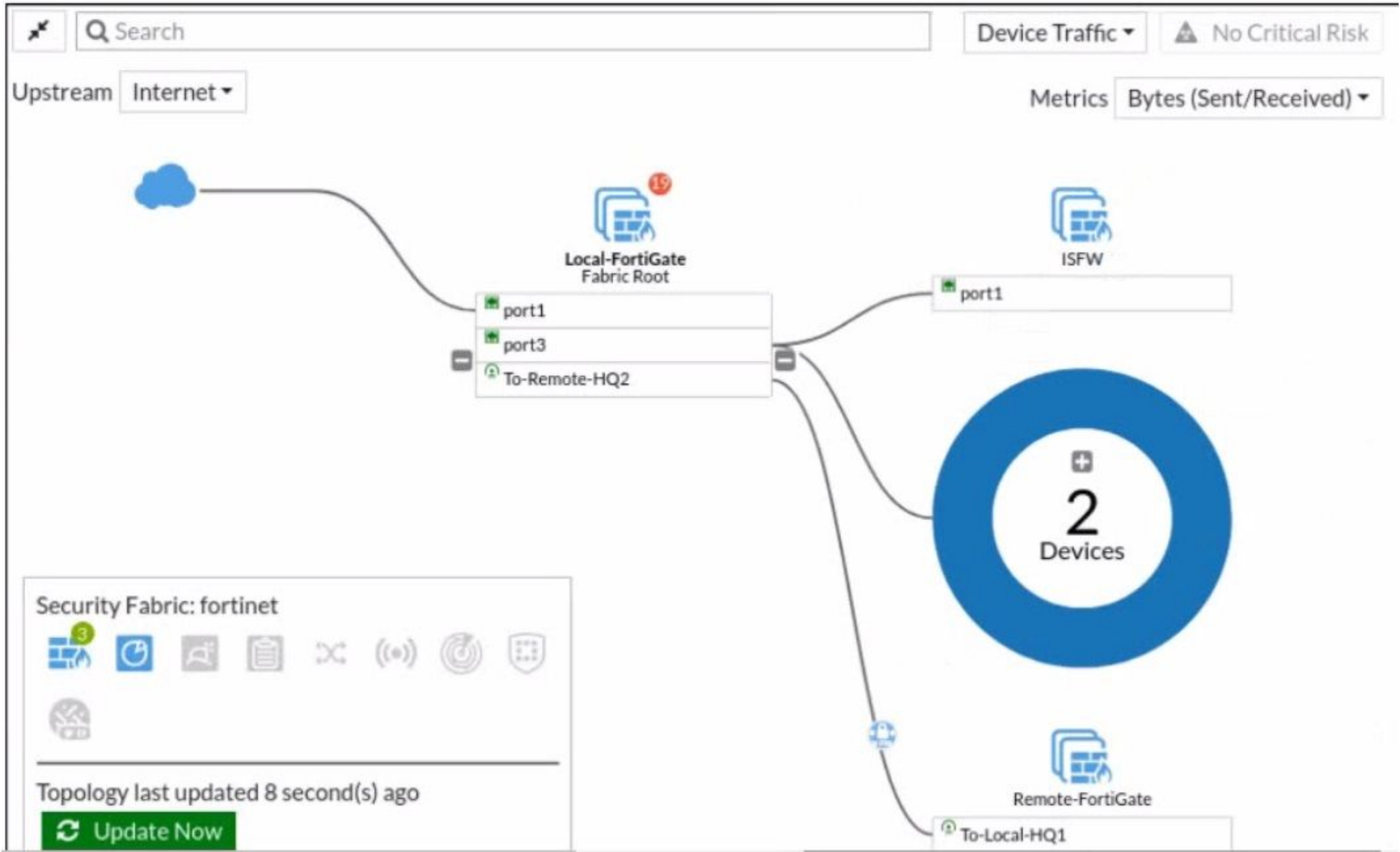
Flow-based inspection is a type of traffic inspection that is used by some firewall devices, including FortiGate, to analyze network traffic. It is designed to be more efficient and less resource-intensive than proxy-based inspection, and it offers several benefits over this approach.

Two benefits of flow-based inspection compared to proxy-based inspection are:

FortiGate uses fewer resources: Flow-based inspection uses fewer resources than proxy-based inspection, which can help to improve the performance of the firewall device and reduce the impact on overall system performance.

FortiGate adds less latency to traffic: Flow-based inspection adds less latency to traffic than proxy-based inspection, which can be important for real-time applications or other types of traffic that require low latency.

QUESTION 15
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.

Correct Answer: C, D
Section:
Explanation:

<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>

QUESTION 16

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.

Correct Answer: A, C

Section:

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.

QUESTION 17

Refer to the exhibit.



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.

Correct Answer: D

Section:

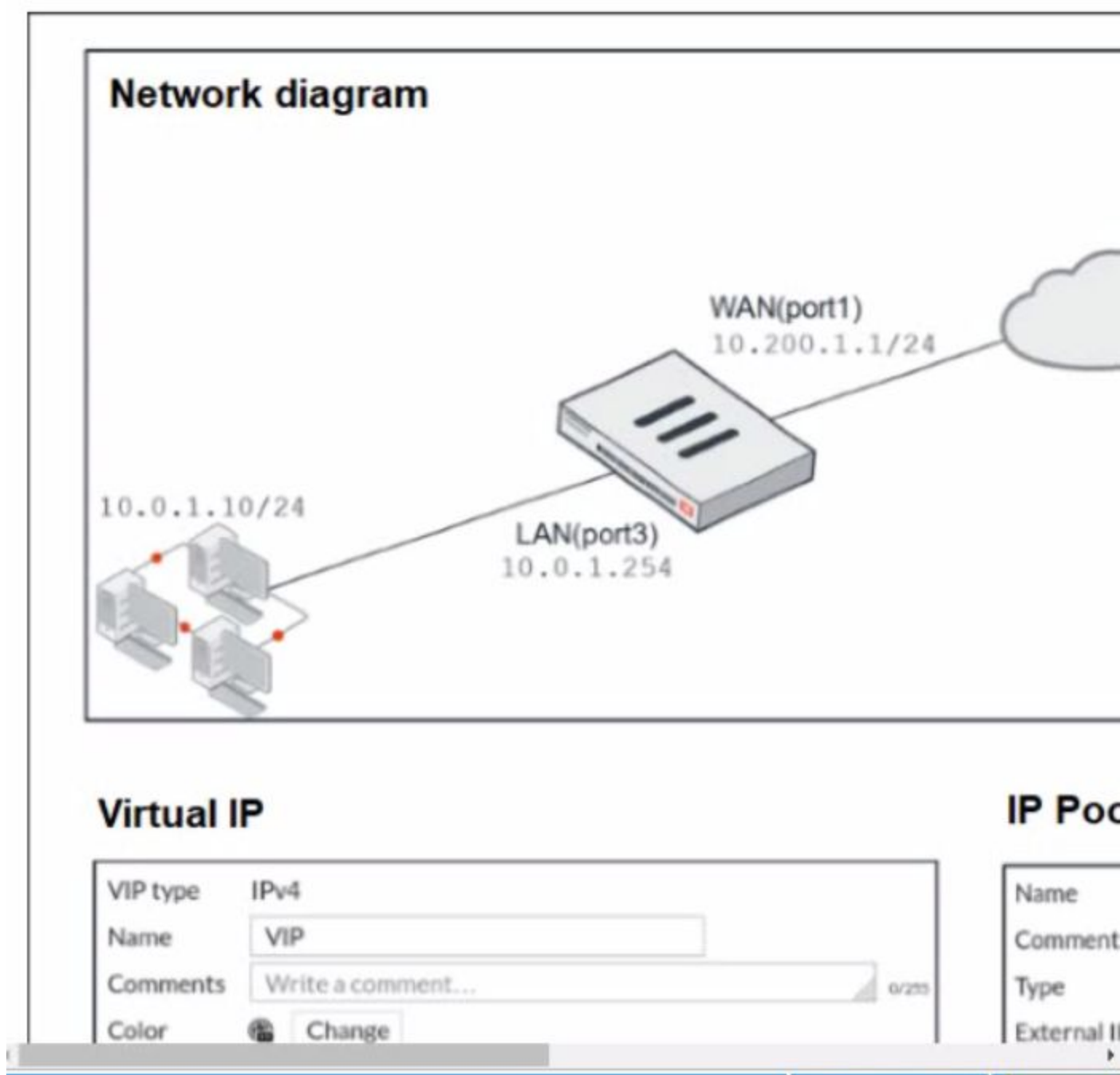
Explanation:

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.

QUESTION 18

Refer to the exhibit.



The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration.

The WAN (port1) interface has the IP address 10.200. 1. 1/24.

The LAN (port3) interface has the IP address 10 .0.1.254. /24.

The first firewall policy has NAT enabled using IP Pool.

The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0. 1. 10?

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 19
Refer to the exhibit.

Name

SLA_1

Protocol

Ping

HTTP

DNS

Servers

4.2.2.2

×

4.2.2.1

×

Participants

All SD-WAN Members

Specify

port1

×

port2

×

+

Enable probe packets

☐

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.

Correct Answer: B, D
Section:

QUESTION 20
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.

Correct Answer: B

Section:

Explanation:

FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

QUESTION 21

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

Correct Answer: B, C

Section:

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'.

QUESTION 22

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

Correct Answer: B

Section:

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.'

QUESTION 23

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

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.

D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: C, D

Section:

QUESTION 24

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.

Correct Answer: B, C

Section:

QUESTION 25

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

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

Correct Answer: D

Section:

QUESTION 26

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.

Correct Answer: C

Section:

QUESTION 27

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

Correct Answer: C, D

Section:

QUESTION 28

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
orgin->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.

Correct Answer: A

Section:

Explanation:

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

QUESTION 29

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.

Correct Answer: B, C

Section:

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.'

QUESTION 30

Refer to the exhibit.

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.

Correct Answer: A

Section:

QUESTION 31

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

Correct Answer: C, D

Section:

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'

QUESTION 32

An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value.

Which timeout option should be configured on FortiGate?

- A. auth-on-demand
- B. soft-timeout
- C. idle-timeout
- D. new-session
- E. hard-timeout

Correct Answer: E

Section:

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Explanation-of-auth-timeout-types-for-Firewall/ta-p/189423>

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221#:~:text=Hard%20timeout%3A%20User%20>

QUESTION 33

Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

- A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
- B. To finish any inspection operations
- C. To remove the NAT operation
- D. To generate logs

Correct Answer: A

Section:

Explanation:

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

QUESTION 34

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

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

Correct Answer: A, B

Section:

Explanation:

<https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/buildingsecurity-into-fortios>

QUESTION 35

Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack .
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

Correct Answer: A

Section:

Explanation:

fortinet-fortigate-security-study-guide-for-fortios-72 page 417 If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

<https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshooting-high-cpu-usage>

QUESTION 36

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

Correct Answer: A

Section:

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.

'By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. Other ports and protocols are available by disabling the FortiGuard anycast setting on the CLI.'

QUESTION 37

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

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

Correct Answer: B

Section:

Explanation:

https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-sslvpn-40-mr3.pdf

QUESTION 38

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

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

Correct Answer: A, D, E

Section:

QUESTION 39

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.

Correct Answer: A, D

Section:

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>

QUESTION 40

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.

Correct Answer: A, D

Section:

Explanation:

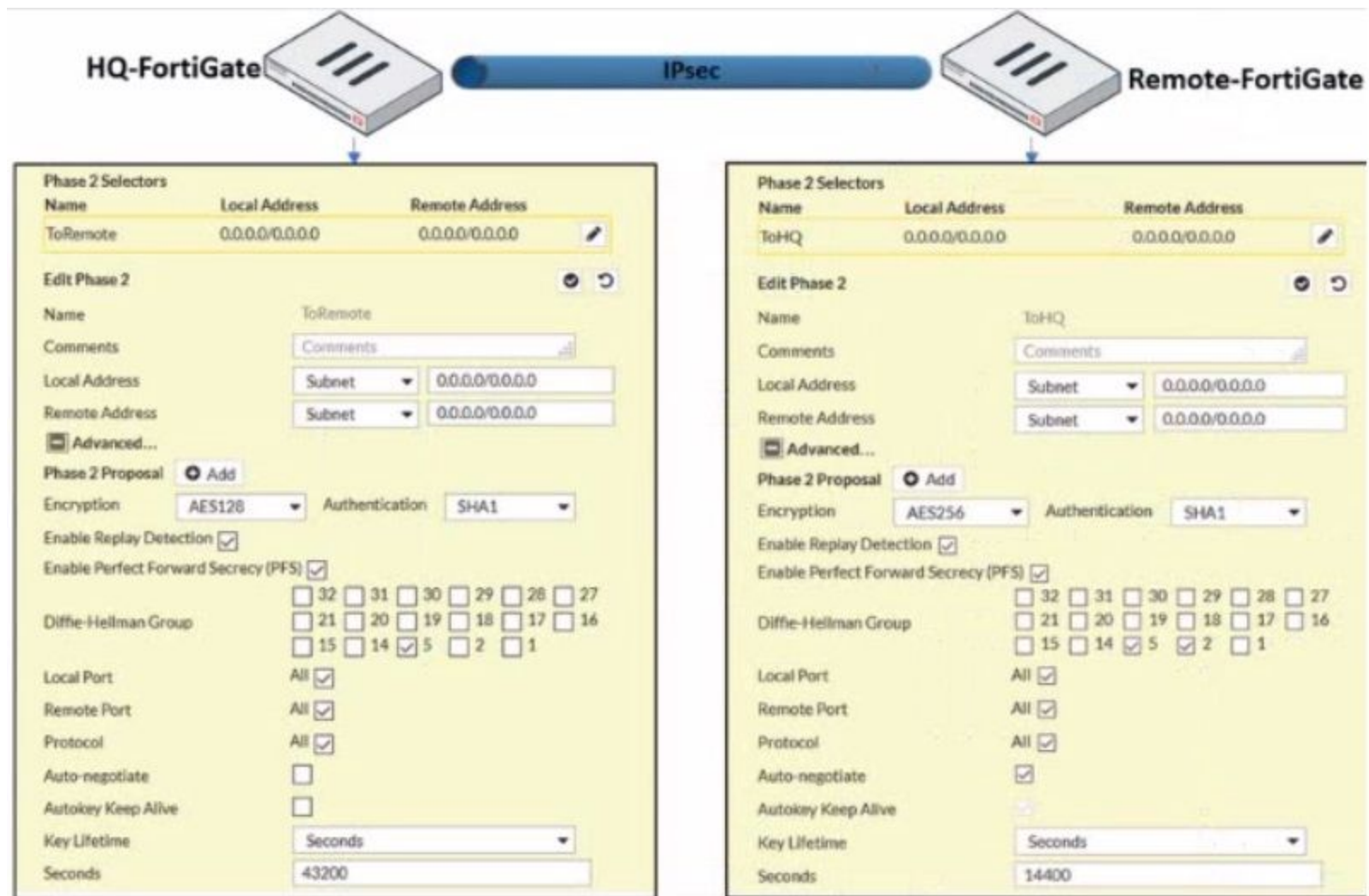
1. Override is disable by default - OK

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>

QUESTION 41

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.

Correct Answer: D

Section:

Explanation:

Encryption and authentication algorithm needs to match in order for IPSEC be successfully established.

QUESTION 42

Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiCache
- B. FortiSIEM
- C. FortiAnalyzer
- D. FortiSandbox
- E. FortiCloud

Correct Answer: B, C, E

Section:

Explanation:

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview>

QUESTION 43

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

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

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 44

An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

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

Correct Answer: D

Section:

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821>

QUESTION 45

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.

Correct Answer: D

Section:

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.'

<https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1>

QUESTION 46

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.

Correct Answer: C, D

Section:

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>

QUESTION 47

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

Correct Answer: D

Section:

QUESTION 48

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

Correct Answer: B, D, E

Section:

QUESTION 49

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

Correct Answer: A, C

Section:

QUESTION 50

Examine this FortiGate configuration:

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D

Section:

Explanation:

'What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting'

QUESTION 51

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

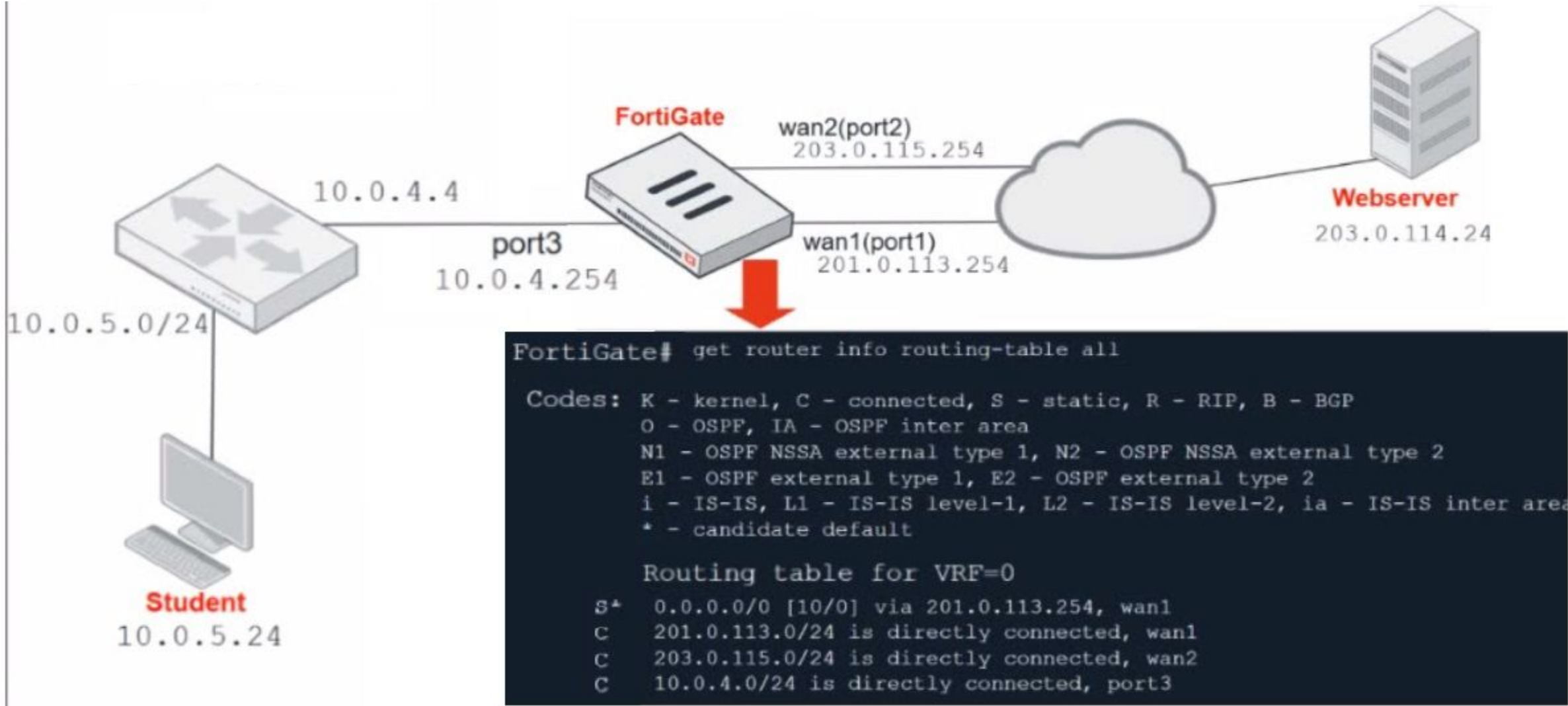
Correct Answer: A, D

Section:

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.'

QUESTION 52
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.

Correct Answer: D
Section:

QUESTION 53
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'

Correct Answer: A

Section:

QUESTION 54

Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Source defined as Internet Services in the firewall policy.
- B. Destination defined as Internet Services in the firewall policy.
- C. Highest to lowest priority defined in the firewall policy.
- D. Services defined in the firewall policy.
- E. Lowest to highest policy ID number.

Correct Answer: A, B, D

Section:

Explanation:

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

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

QUESTION 55

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

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

Correct Answer: A

Section:

QUESTION 56

Refer to the exhibit to view the application control profile.

The screenshot shows the FortiGate configuration for Application and Filter Overrides. The 'Excessive-Bandwidth' filter is set to 'Block' for priority 1. The 'Apple' filter is set to 'Monitor' for priority 2. The 'Application Signature' table shows 'FaceTime' categorized as 'VoIP' with a popularity of 5 stars.

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	Block
2	Apple	Filter	Monitor

Name	Category	Technology	Popularity
Application Signature 1/1659			
FaceTime	VoIP	Client-Server	★★★★★

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.

Correct Answer: A

Section:

QUESTION 57

An administrator must disable RPF check to investigate an issue.

Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

- A. Enable asymmetric routing, so the RPF check will be bypassed.
- B. Disable the RPF check at the FortiGate interface level for the source check.
- C. Disable the RPF check at the FortiGate interface level for the reply check .
- D. Enable asymmetric routing at the interface level.

Correct Answer: B

Section:

QUESTION 58

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

Correct Answer: B

Section:

QUESTION 59

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.

Correct Answer: A, B

Section:

QUESTION 60

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

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

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

Correct Answer: B

Section:

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.222):

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

QUESTION 61

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

Correct Answer: A, B, C

Section:

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

QUESTION 62

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

Correct Answer: A, C

Section:

QUESTION 63

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.

Correct Answer: C, D

Section:

Explanation:

Fortigate Infrastructure 7.0 Study Guide P.272-273

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

QUESTION 64

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.

Correct Answer: B

Section:

QUESTION 65

Examine this output from a debug flow:

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

Why did the FortiGate drop the packet?

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

Correct Answer: D

Section:

Explanation:

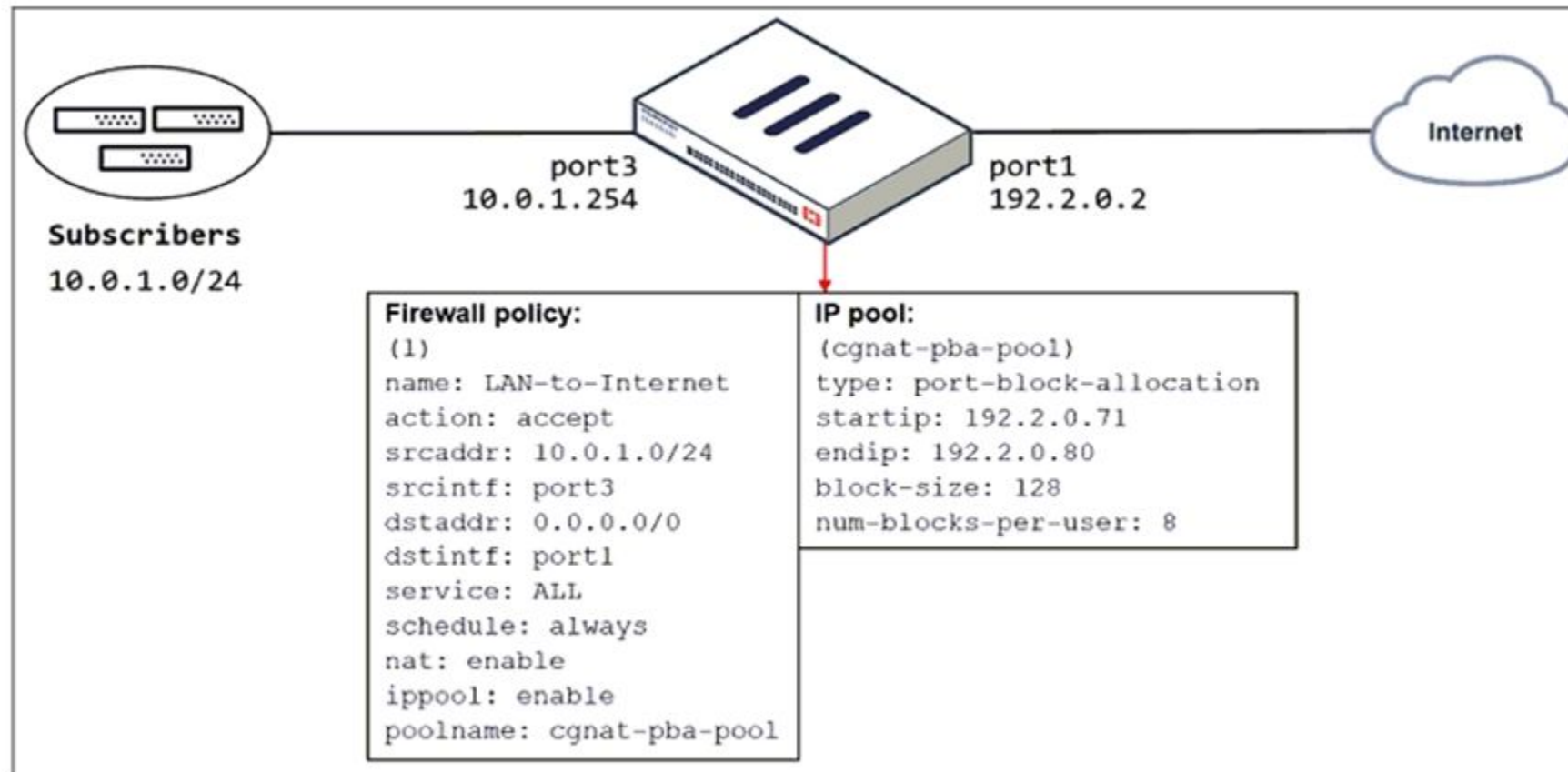
<https://kb.fortinet.com/kb/documentLink.do?externalID=13900>

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

QUESTION 66

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.

Correct Answer: B, C

Section:

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.'

QUESTION 67

Which statement about video filtering on FortiGate is true?

- A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.
- B. It does not require a separate FortiGuard license.
- C. Full SSL inspection is not required.
- D. its available only on a proxy-based firewall policy.

Correct Answer: D

Section:

Explanation:

FortiGate Security 7.2 Study Guide (p.279): 'To apply the video filter profile, proxy-based firewall polices currently allow you to enable the video filter profile. You must enable full SSL inspection on the firewall policy.'
<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/860867/filtering-based-on-fortiguard-categories>

QUESTION 68

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.

Correct Answer: C

Section:

Explanation:

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

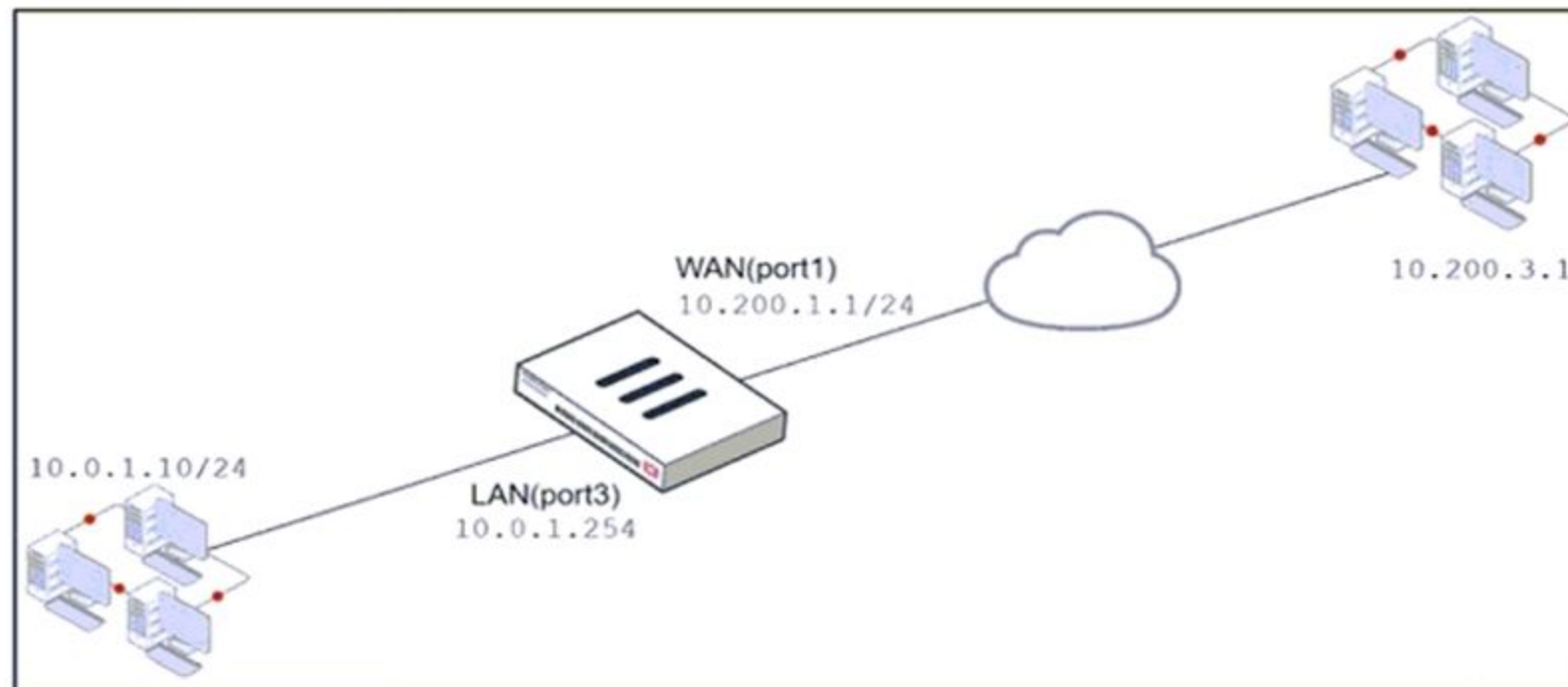
QUESTION 69

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.



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

Correct Answer: C

Section:

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

QUESTION 70

Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

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

Correct Answer: A, B, E

Section:

Explanation:

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow-mode>

QUESTION 71

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

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

Correct Answer: A, B

Section:

QUESTION 72

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.

Correct Answer: B

Section:

QUESTION 73

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.

Correct Answer: B

Section:

Explanation:

FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

QUESTION 74

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

Correct Answer: D
Section:

QUESTION 75

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

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

Correct Answer: A, C
Section:

QUESTION 76

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

Correct Answer: A, D
Section:

QUESTION 77

Refer to exhibit.

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

Name

Allow_Twitter

Comments

Write a comment... 0/255

Feature set

Flow-based

Proxy-based

FortiGuard Category Based Filter

Allow

Monitor

Block

Warning

Authenticate

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

Static URL Filter

Block invalid URLs

URL Filter

Create New

Edit

Delete

Search

URL	Type	Action	Status
twitter.com	Wildcard	Allow	Enable

Block malicious URLs discovered by FortiSandbox

Content Filter

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

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

Correct Answer: C

Section:

Explanation:

Based on the exhibit, the administrator has configured the FortiGuard Category Based Filter to block access to all social networking sites, and has also configured a Static URL Filter to block access to twitter.com. As a result, users are being redirected to a block page when they try to access twitter.com. To allow users to access twitter.com while blocking all other social networking sites, the administrator can make the following configuration change: On the Static URL Filter configuration, set Action to Exempt: By setting the Action to Exempt, the administrator can override the block on twitter.com that was specified in the FortiGuard Category Based Filter. This will allow users to access twitter.com, while all other social networking sites will still be blocked.

QUESTION 78

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.

Correct Answer: C, D

Section:

Explanation:

ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of 'never trust, always verify,' which means that all access to network resources is subject to strict verification and authentication.

Two functions of ZTNA are:

ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the device's software and hardware configurations, security settings, and the presence of malware.

ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

QUESTION 79

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

Correct Answer: A

Section:

Explanation:

The SSL VPN idle-timeout setting determines how long an SSL VPN session can be inactive before it is terminated. When an SSL VPN session becomes inactive (for example, if the user closes the VPN client or disconnects from the network), the session timer begins to count down. If the timer reaches the idle-timeout value before the user reconnects or sends any new traffic, the session will be terminated and the associated resources (such as VPN tunnels and virtual interfaces) will be deleted.

QUESTION 80

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.

Correct Answer: A

Section:

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.

QUESTION 81

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

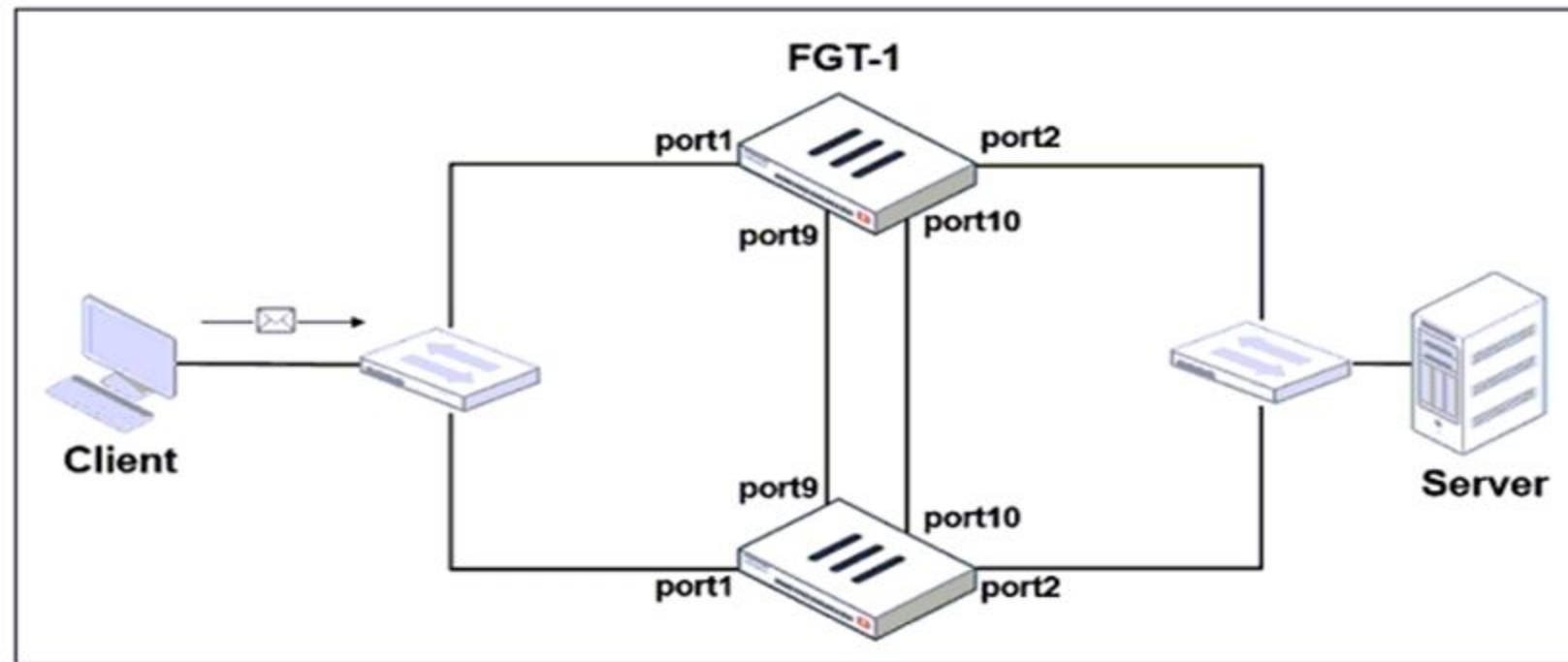


Exhibit A Exhibit B

```
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.

Correct Answer: A, D

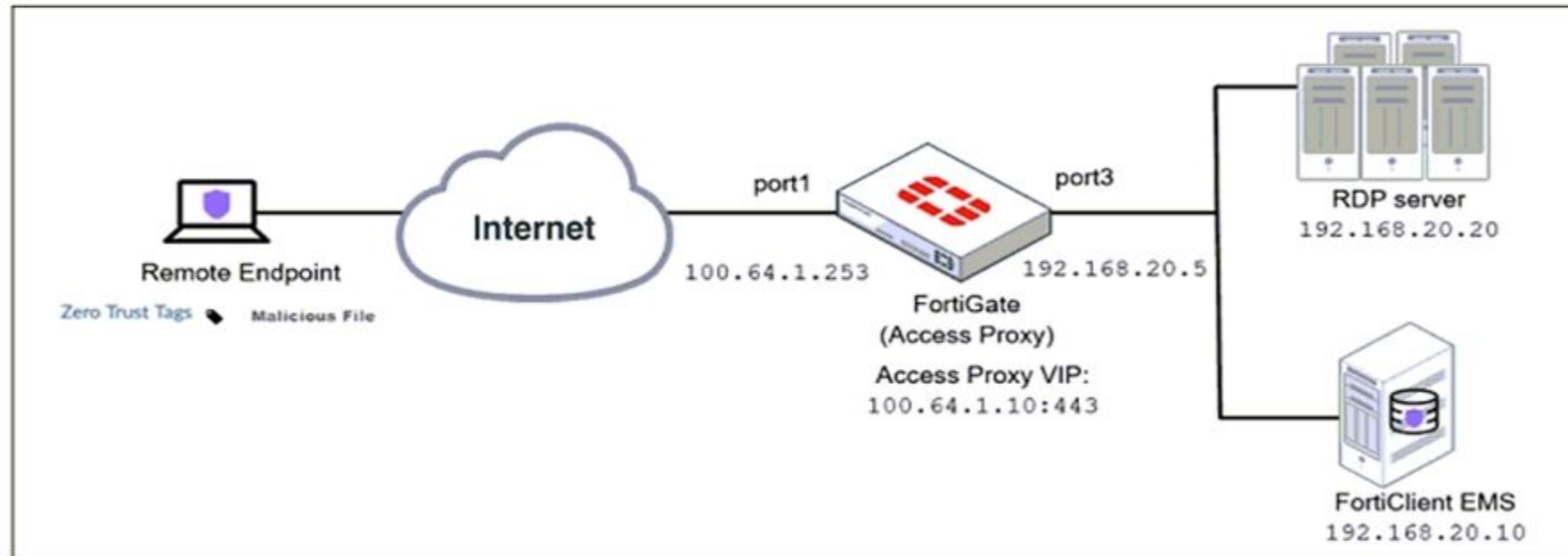
Section:

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.'

QUESTION 82

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.

Correct Answer: C

Section:

Explanation:

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-ztna-proxy-session-7-0-2>

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.'

QUESTION 83

What are two features of collector agent advanced mode? (Choose two.)

- A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
- B. In advanced mode, security profiles can be applied only to user groups, not individual users.
- C. Advanced mode uses the Windows convention---NetBios: Domain\Username.
- D. Advanced mode supports nested or inherited groups.

Correct Answer: A, D

Section:

Explanation:

A) In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.

This is true because advanced mode allows FortiGate to query the LDAP server directly for user information and group membership, without relying on the collector agent. This enables FortiGate to apply security policies based on LDAP group filters, which can be configured on FortiGate1

D) Advanced mode supports nested or inherited groups.

This is true because advanced mode can handle complex group structures, such as nested groups or inherited groups, where a user belongs to a group that is a member of another group. This allows FortiGate to apply security policies based on the effective group membership of a user, not just the direct group membership1

FortiGate Infrastructure 7.2 Study Guide (p.146): 'Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups.' 'In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent.'

QUESTION 84

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

Correct Answer: B

Section:

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 surface12

QUESTION 85

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.

Correct Answer: A, D

Section:

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/>

QUESTION 86

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

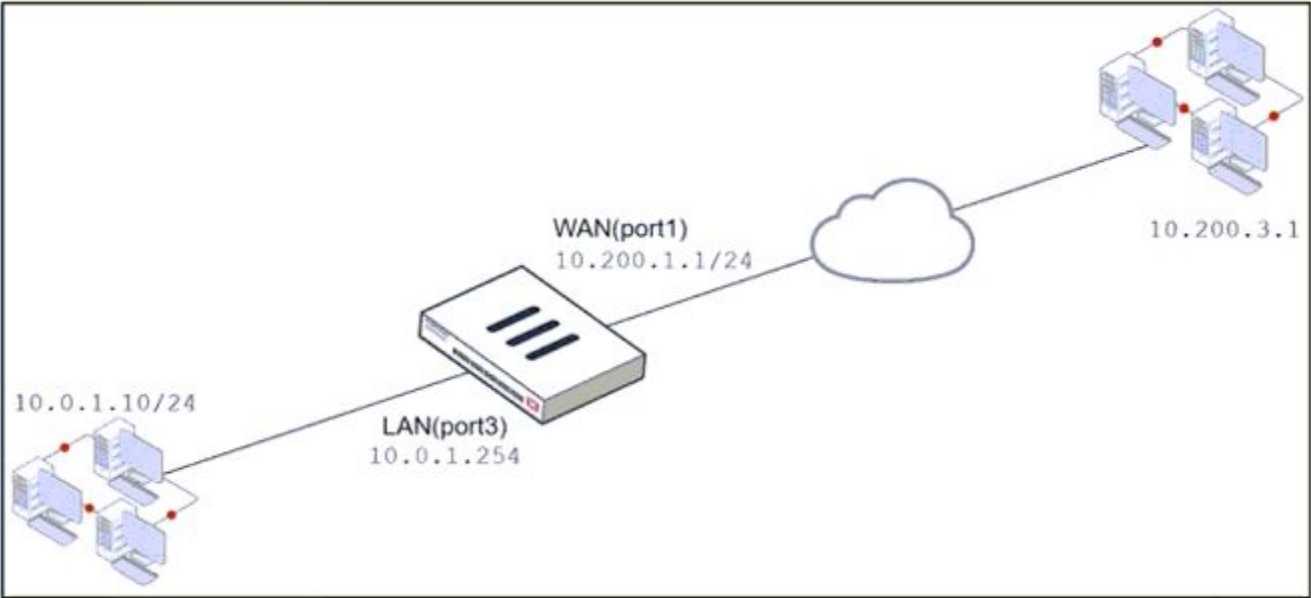


Exhibit A

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

Correct Answer: C

Section:

Explanation:

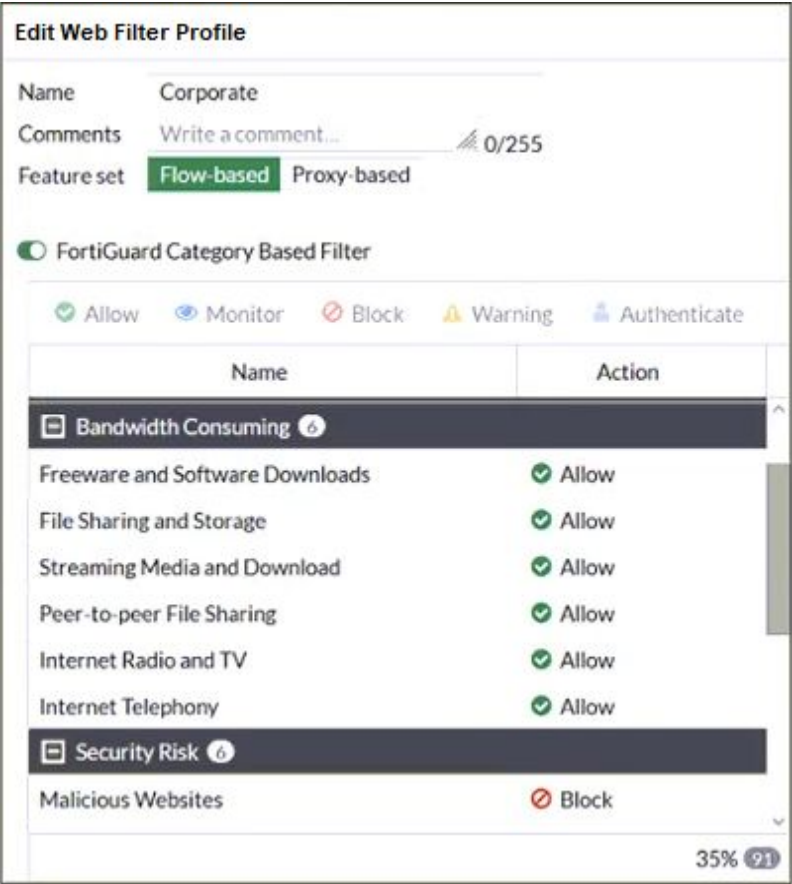
Traffic is coming from LAN to WAN, matches policy Full_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

QUESTION 87

Refer to the exhibit.

The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.

An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.



What are two solutions for satisfying the requirement? (Choose two.)

- A. Configure a separate firewall policy with action Deny and an FQDN address object for *.download.com as destination address.
- B. Configure a web override rating for download.com and select Malicious Websites as the subcategory.
- C. Set the Freeware and Software Downloads category Action to Warning.
- D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

Correct Answer: B, D

Section:

Explanation:

FortiGate Security 7.2 Study Guide (p.268-269): 'If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. You can block a website that belongs to an allowed category.' 'Static URL filtering is another web filter feature. Configured URLs in the URL filter are checked against the visited websites. If a match is found, the configured action is taken. URL filtering has the same patterns as static domain filtering: simple, regular expressions, and wildcard.'

B) Configure a web override rating for download.com and select Malicious Websites as the subcategory.

This is true because a web override rating is a feature that allows the administrator to change the FortiGuard category of a specific website or domain, and apply a different action to it based on the web filter profile. By

configuring a web override rating for download.com and selecting Malicious Websites as the subcategory, the administrator can block access to download.com, which belongs to the Freeware and Software Downloads category by default, without affecting other websites in the same category. The Malicious Websites category has the action Block in the web filter profile shown in the exhibit.

D) Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

This is true because a static URL filter entry is a feature that allows the administrator to define custom rules for filtering specific URLs or domains, and apply an action to them based on the web filter profile. By configuring a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively, the administrator can block access to download.com and any subdomains or paths under it, without affecting other websites in the Freeware and Software Downloads category. The static URL filter entries have higher priority than the FortiGuard category based filter entries in the web filter profile.

QUESTION 88
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.

Correct Answer: A
Section:
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.'

QUESTION 89
View the exhibit.

Destination

Subnet

Named Address

Internet Service

172.13.24.0/255.255.255.0

Interface

TunnelB

Administrative Distance

5

Comments

0/255

Status

Enabled

Disabled

Advanced Options

Priority

30

Destination

Subnet

Named Address

Internet Service

172.13.24.0/255.255.255.0

Interface

TunnelA

Administrative Distance

10

Comments

0/255

Status

Enabled

Disabled

Advanced Options

Priority

0

- Which of the following statements are correct? (Choose two.)
- A. This setup requires at least two firewall policies with the action set to IPsec.
 - B. Dead peer detection must be disabled to support this type of IPsec setup.
 - C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
 - D. This is a redundant IPsec setup.

Correct Answer: C, D
Section:

Explanation:

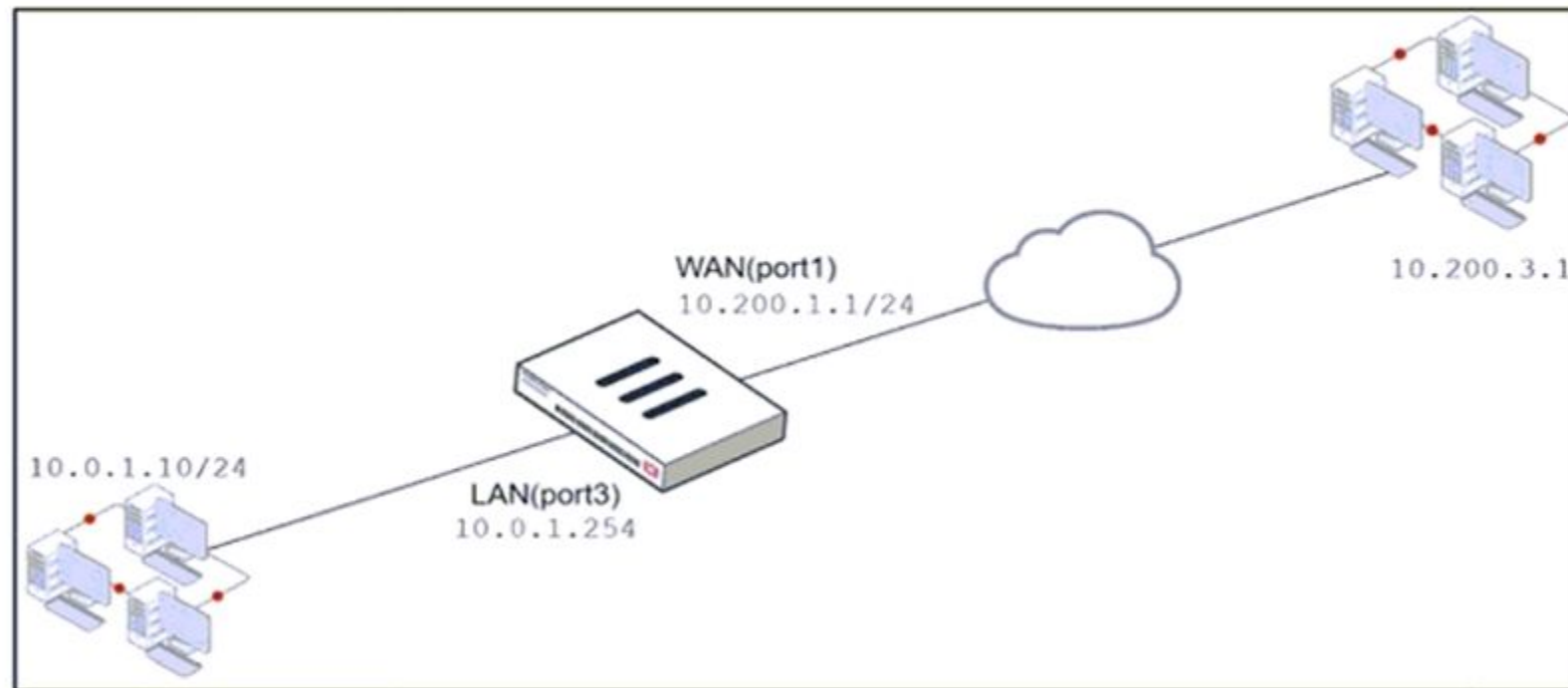
<https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundancy>

QUESTION 90

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

Exhibit A

Exhibit B



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

Edit Virtual IP

VIP type

IPv4

Name

VIP

Comments

Write a comment...

0/255

Color

Change

Network

Interface

WAN (port1)

Type

Static NAT

External IP address/range

10.200.1.10

Map to

IPv4 address/range

10.0.1.10

Optional Filters

Port Forwarding

Protocol

TCP UDP SCTP ICMP

Port Mapping Type

One to one Many to many

External service port

10443

Map to IPv4 port

443

The WAN (port1) interface has the IP address 10.200. 1. 1/24. The LAN (port2) interface has the IP address 10.0. 1.254/24.

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

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 91

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.

Correct Answer: A, B

Section:

QUESTION 92

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

Correct Answer: A, B, C

Section:

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.'

QUESTION 93

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

Correct Answer: B

Section:

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.

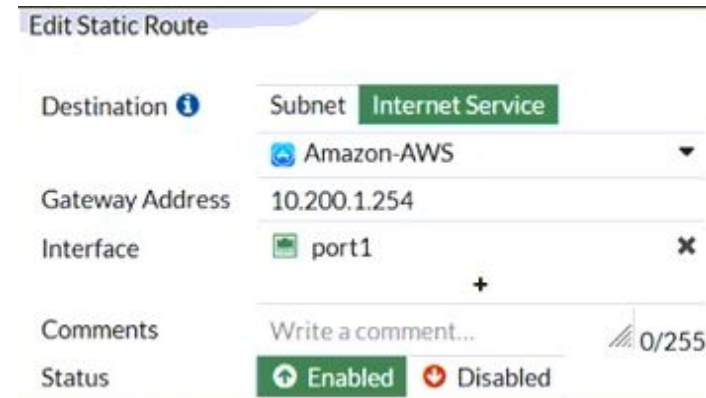
An SSL VPN bookmark is a web link that provides access to network resources through the SSL VPN web portal¹. It does not support external applications running on the user's PC.

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.

QUESTION 94

Refer to the exhibit, which contains a static route configuration.
An administrator created a static route for Amazon Web Services.



The screenshot shows the 'Edit Static Route' configuration page in FortiGate. The 'Destination' field is set to 'Subnet' with a value of 'Internet Service'. The 'Gateway Address' is '10.200.1.254'. The 'Interface' is 'port1'. The 'Status' is 'Enabled'. There is a comment field with the text 'Write a comment...' and a character count '0/255'.

Which CLI command must the administrator use to view the route?

- A. get router info routing-table database
- B. diagnose firewall route list
- C. get internet-service route list
- D. get router info routing-table all

Correct Answer: B

Section:

Explanation:

ISDB static route will not create entry directly in routing-table.

Reference: <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/198756>

and here <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640>

FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): 'Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table.' 'FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command.'

QUESTION 95

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.

Correct Answer: A, D

Section:

Explanation:

attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

QUESTION 96

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

Correct Answer: B, C, D

Section:

QUESTION 97

Examine this PAC file configuration.

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

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

Correct Answer: A, D

Section:

QUESTION 98

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

Correct Answer: D

Section:

QUESTION 99

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

Correct Answer: A, C, D

Section:

QUESTION 100

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeout. The FortiGate considers a user to be 'idle' if it does not see any packets coming from the user's source IP.
- B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- C. It is an idle timeout. The FortiGate considers a user to be 'idle' if it does not see any packets coming from the user's source MAC.
- D. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Correct Answer: A

Section:

QUESTION 101

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.

Correct Answer: B, D

Section:

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.'

QUESTION 102

An administrator configures outgoing interface any in a firewall policy.

What is the result of the policy list view?

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 103

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.

Correct Answer: A, C

Section:

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.

QUESTION 104

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

Correct Answer: B, D, E

Section:

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)'

QUESTION 105

Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

- A. hard-timeout
- B. auth-on-demand
- C. soft-timeout
- D. new-session
- E. Idle-timeout

Correct Answer: A, D, E

Section:

QUESTION 106

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.

Correct Answer: D

Section:

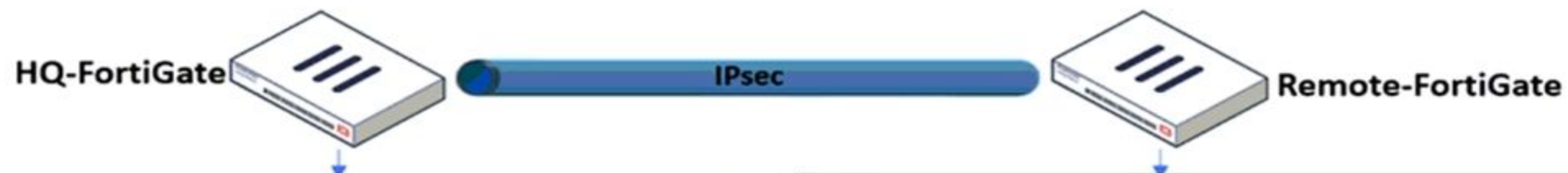
Explanation:

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.'

QUESTION 107

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.



Phase 2 Selectors		
Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2	
Name	ToRemote
Comments	Comments
Local Address	Subnet 0.0.0.0/0.0.0.0
Remote Address	Subnet 0.0.0.0/0.0.0.0
Advanced...	
Phase 2 Proposal	Add
Encryption	AES128
Authentication	SHA1
Enable Replay Detection	<input checked="" type="checkbox"/>
Enable Perfect Forward Secrecy (PFS)	<input checked="" type="checkbox"/>
Diffie-Hellman Group	<input type="checkbox"/> 32 <input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input type="checkbox"/> 14 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 2 <input type="checkbox"/> 1
Local Port	All <input checked="" type="checkbox"/>
Remote Port	All <input checked="" type="checkbox"/>
Protocol	All <input checked="" type="checkbox"/>
Auto-negotiate	<input type="checkbox"/>
Autokey Keep Alive	<input type="checkbox"/>
Key Lifetime	Seconds
Seconds	43200

Phase 2 Selectors		
Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2	
Name	ToRemote
Comments	Comments
Local Address	Subnet 0.0.0.0/0.0.0.0
Remote Address	Subnet 0.0.0.0/0.0.0.0
Advanced...	
Phase 2 Proposal	Add
Encryption	AES256
Authentication	SHA1
Enable Replay Detection	<input checked="" type="checkbox"/>
Enable Perfect Forward Secrecy (PFS)	<input checked="" type="checkbox"/>
Diffie-Hellman Group	<input type="checkbox"/> 32 <input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input type="checkbox"/> 14 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 1
Local Port	All <input checked="" type="checkbox"/>
Remote Port	All <input checked="" type="checkbox"/>
Protocol	All <input checked="" type="checkbox"/>
Auto-negotiate	<input type="checkbox"/>
Autokey Keep Alive	<input type="checkbox"/>
Key Lifetime	Seconds
Seconds	14400

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.

Correct Answer: B

Section:

QUESTION 108

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

- A. It uses UDP 8888.
- B. It uses UDP 53.

- C. It uses DNS over HTTPS.
- D. It uses DNS over TLS.

Correct Answer: D

Section:

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.