

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FGT_AD-7.4/



NEW QUESTION 1

Refer to the exhibit.

```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.
0"
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw=10.200.1.254
via port1"
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (policy 0)"
```

Why did FortiGate drop the packet?

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

Answer: D

Explanation:

The debug trace output shows that the packet was "Denied by forward policy check (policy 0)." In FortiGate, policy ID 0 corresponds to the default implicit deny policy. This means that if a packet does not match any configured firewall policies, it is denied by the default implicit policy.

References:



FortiOS 7.4.1 Administration Guide: Firewall Policies

NEW QUESTION 2

Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

Edit Antivirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan  ☒ **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  ☒

Send files to FortiSandbox for inspection  ☐

Send files to FortiNDR for inspection  ☐

Include mobile malware protection ☒

Quarantine  ☐

Virus Outbreak Prevention

Use FortiGuard outbreak prevention database ☐

Use external malware block list ☐

Use EMS threat feed  ☐

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

- A. The intrusion prevention security profile must be enabled when using flow-based inspection mode.
- B. The option to send files to FortiSandbox for inspection is enabled.
- C. The firewall policy performs a full content inspection on the file.

D. Flow-based inspection is used, which resets the last packet to the user.

Answer: D

Explanation:

In flow-based inspection mode, FortiGate sends a reset (RST) packet to the client instead of providing a replacement message, which causes the block message not to be displayed.

NEW QUESTION 3

Which inspection mode does FortiGate use for application profiles if it is configured as a profile-based next- generation firewall (NGFW)?

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

Answer: D

Explanation:

When FortiGate is configured in NGFW profile-based mode, it primarily uses flow-based inspection for application profiles. Flow-based inspection provides faster processing and lower latency by inspecting traffic in real-time without buffering, making it suitable for scenarios where performance is a priority.

References:

> FortiOS 7.4.1 Administration Guide: Inspection Modes

NEW QUESTION 4

An administrator manages a FortiGate model that supports NTurbo. How does NTurbo enhance performance for flow-based inspection?

- A. NTurbo offloads traffic to the content processor.
- B. NTurbo creates two inspection sessions on the FortiGate device.
- C. NTurbo buffers the whole file and then sends it to the antivirus engine.
- D. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.

Answer: A

Explanation:

NTurbo enhances performance for flow-based inspection by offloading traffic to the content processor.

NEW QUESTION 5

Refer to the exhibit.

Add Signatures

Type

Filter

Signature

Action

Block

Packet logging

Enable

Disable

Status

Enable

Disable

Default

Rate-based settings

Default

Specify

Exempt IPs

0

Edit IP Exemptions

Search

Q

Selected

All

Name	Severity	Target	OS	Action
IPS Signature				
FTP.Login.Failed		Server	All	Pass

Review the intrusion prevention system (IPS) profile signature settings shown in the exhibit. What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

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

Answer: A

Explanation:

The exhibit shows that the "FTP.Login.Failed" IPS signature is set with the action "Pass" and packet logging enabled. This means that any traffic matching this signature will be allowed through the FortiGate, and the traffic details will be logged for monitoring and analysis purposes.

References:



FortiOS 7.4.1 Administration Guide: IPS Signature Actions

NEW QUESTION 6

A network administrator has configured an SSL/SSH inspection profile defined for full SSL inspection and set with a private CA certificate. The firewall policy that allows the traffic uses this profile for SSL inspection and performs web filtering. When visiting any HTTPS websites, the browser reports certificate warning errors. What is the reason for the certificate warning errors?

- A. The SSL cipher compliance option is not enabled on the SSL inspection profile.
- B. This setting is required when the SSL inspection profile is defined with a private CA certificate.
- C. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
- D. The browser does not recognize the certificate in use as signed by a trusted CA.
- E. With full SSL inspection it is not possible to avoid certificate warning errors at the browser level.

Answer: C

Explanation:

The certificate warning errors occur because the SSL inspection profile is configured to use a private CA certificate that is not recognized by the browser as being signed by a trusted CA. For the browser to trust the FortiGate's re-signed certificates, the CA certificate used by FortiGate for SSL inspection must be installed in the browser's trusted certificate store. Until the browser recognizes the certificate authority (CA) as trusted, it will continue to display warning errors when accessing HTTPS websites.

References:



FortiOS 7.4.1 Administration Guide: SSL/SSH Inspection Configuration

NEW QUESTION 7

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

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

Answer: BC

Explanation:

For SSL VPN to function correctly between two FortiGate devices, the following settings are required:



B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate must have a Certificate Authority (CA) certificate installed to authenticate and verify the certificate presented by the client FortiGate device.



C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate: The client FortiGate must have a client certificate that is signed by the same CA that the server FortiGate uses for verification. This ensures a secure SSL VPN connection between the two devices.

The other options are not directly necessary for establishing SSL VPN:



A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: This is incorrect as SSL VPN does not require a specific tunnel interface type; it typically uses an SSL VPN client profile.



D. The client FortiGate requires a manually added route to remote subnets: While routing may be necessary, it is not specifically required for the SSL VPN functionality between two FortiGates.

References



FortiOS 7.4.1 Administration Guide - Configuring SSL VPN, page 1203.



FortiOS 7.4.1 Administration Guide - SSL VPN Authentication, page 1210.

NEW QUESTION 8

Which method allows management access to the FortiGate CLI without network connectivity?

- A. SSH console
- B. CLI console widget
- C. Serial console
- D. Telnet console

Answer: C

Explanation:

The serial console method allows management access to the FortiGate CLI without relying on network connectivity. This method involves directly connecting a computer to the FortiGate device using a serial cable (such as a DB-9 to RJ-45 cable or USB to RJ-45 cable) and using terminal emulation software to interact with the FortiGate CLI. This method is essential for situations where network-based access methods (such as SSH or Telnet) are not available or feasible.

References:

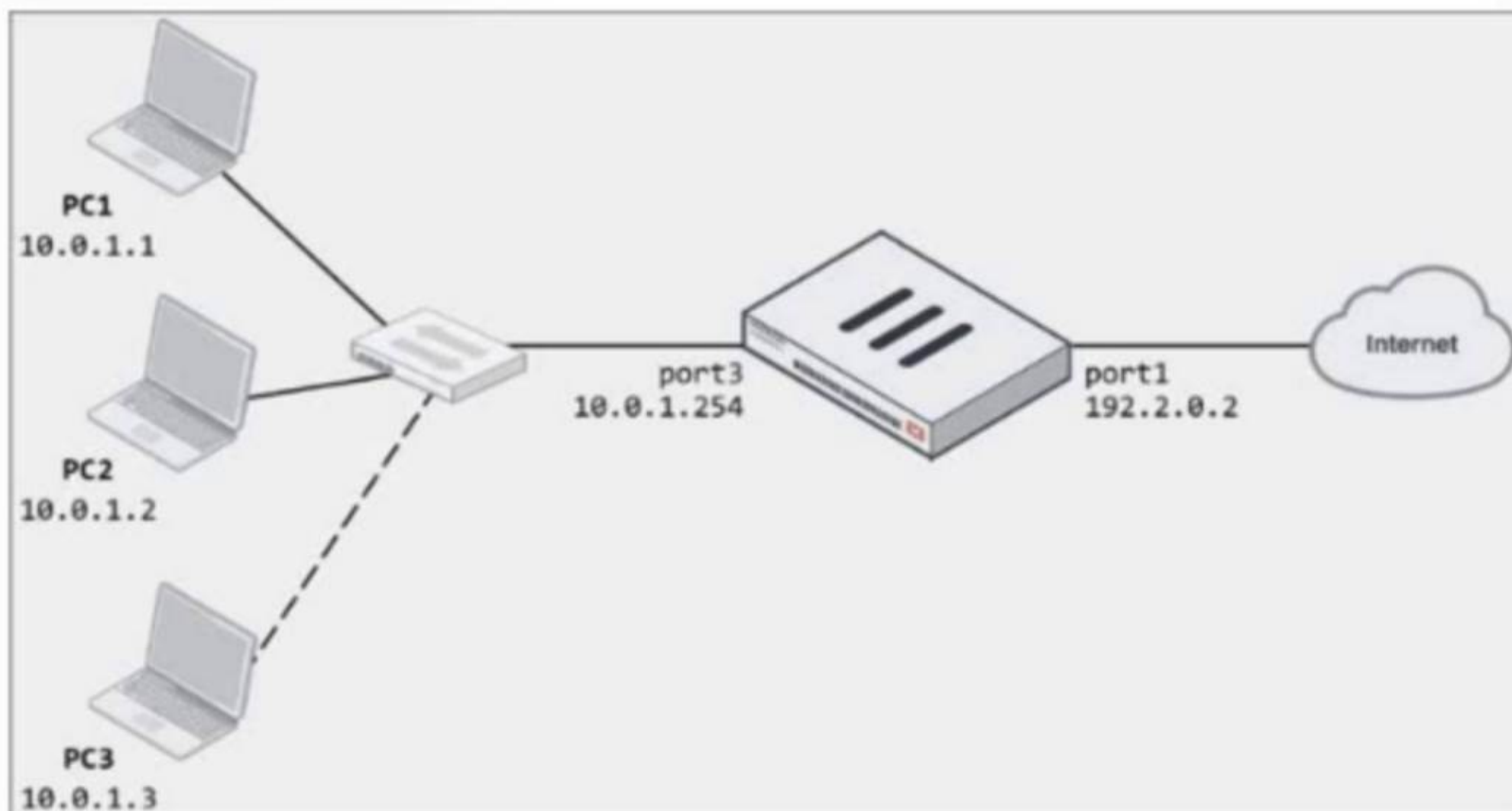


FortiOS 7.4.1 Administration Guide: Console connection

NEW QUESTION 9

Refer to the exhibits.

Network diagram



Dynamic IP pool

Edit Dynamic IP Pool

Name	internet-pool
Comments	Write a comment... 0/255
Type	One-to-One
External IP Range 	192.2.0.10-192.2.0.11
ARP Reply	<input checked="" type="checkbox"/>

Firewall policy

Edit Policy

Name

LAN-to-Internet

Incoming Interface

LAN (port3)

×

Outgoing Interface

WAN (port1)

×

Source

all

×

Destination

all

×

Schedule

always

▼

Service

ALL

×

Action

✓ ACCEPT

⊘ DENY

Inspection Mode

Flow-based

Proxy-based

Firewall/Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

internet-pool

×

Preserve Source Port

Protocol Options

PROT

default

The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device. Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.

Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

- A. In the firewall policy configuration, add 10.
- B. 3 as an address object in the source field.
- C. In the IP pool configuration, set endip to 192.2.0.12.
- D. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.
- E. In the IP pool configuration, set cype to overload.

Answer: BD

Explanation:

To resolve the issue of PC3 not being able to access the internet, the administrator needs to adjust the IP pool configuration or the firewall policy. The following two options will fix the connectivity issue:

- B. In the IP pool configuration, set the ending IP to 192.2.0.12: The current IP pool range is 192.2.0.10-192.2.0.11, which only provides two IP addresses for network address translation (NAT). To allow PC3 to access the internet, the IP pool should be expanded to include an additional IP address by changing the end of the range to 192.2.0.12.

Passing Certification Exams Made Easy

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

- D. In the IP pool configuration, set type to overload: Instead of using a one-to-one NAT, changing the type to overload will allow multiple internal addresses (such as PC1, PC2, and PC3) to share a single external IP address. This will solve the issue without needing additional public IP addresses. The other options are not suitable:
- A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field: This option is unnecessary since the firewall policy already allows all addresses from the source (LAN port3).
- C. Configure another firewall policy that matches only the address of PC3 as the source, and then place the policy on top of the list: This option is redundant and would not resolve the underlying issue with the IP pool configuration.

References

- FortiOS 7.4.1 Administration Guide - Configuring Firewall Policies, page 512.
- FortiOS 7.4.1 Administration Guide - Configuring NAT with IP Pools, page 518.

NEW QUESTION 10

An administrator configured a FortiGate to act as a collector for agentless polling mode.
What must the administrator add to the FortiGate device to retrieve AD user group information?

- A. LDAP server
- B. RADIUS server
- C. DHCP server
- D. Windows server

Answer: A

Explanation:

To retrieve AD user group information in agentless polling mode, the administrator must add an LDAP server to the FortiGate device.

NEW QUESTION 10

Refer to the exhibit to view the firewall policy.

Firewall policy configuration

Edit Policy

Name	Internet_Access	
Incoming Interface	port2	X
	+	
Outgoing Interface	port1	X
	+	
Source	all	X
	+	
Destination	all	X
	+	
Schedule	always	▼
Service	DNS	X
	FTP	X
	HTTP	X
	HTTPS	X
	+	
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY	
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based	

Firewall/Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

☐

Protocol Options

PROT default

✎

Security Profiles

AntiVirus

☒

AV default

✎

Web Filter

☐

DNS Filter

☐

Application Control

☐

IPS

☐

File Filter

☐

SSL Inspection

SSL certificate-inspection

✎

Why would the firewall policy not block a well-known virus, for example eicar?

- A. The action on the firewall policy is not set to deny.
- B. The firewall policy is not configured in proxy-based inspection mode.
- C. Web filter is not enabled on the firewall policy to complement the antivirus profile.
- D. The firewall policy does not apply deep content inspection.

Answer: B

Explanation:

The firewall policy shown in the exhibit is configured in flow-based inspection mode. In flow-based inspection, certain security features, such as deep content inspection, might not be as effective as in proxy-based mode. Proxy-based inspection is necessary for thorough content inspection, which includes identifying and blocking well-known viruses like EICAR.

References:



FortiOS 7.4.1 Administration Guide: Inspection Modes

NEW QUESTION 12

Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three.)

- A. Manual with load balancing
- B. Lowest Cost (SLA) with load balancing
- C. Best Quality with load balancing
- D. Lowest Quality (SLA) with load balancing
- E. Lowest Cost (SLA) without load balancing

Answer: ABC

Explanation:

FortiGate's SD-WAN rule strategies for member selection include the following:



Manual with load balancing: This strategy allows an administrator to manually configure which SD-WAN member interfaces to use for specific traffic.



Lowest Cost (SLA) with load balancing: This strategy prioritizes the link with the lowest cost that meets the SLA requirements.



Best Quality with load balancing: This strategy selects the link with the best performance metrics, such as latency, jitter, or packet loss.

Options D and E are incorrect because "Lowest Quality" is not a valid strategy, and "Lowest Cost without load balancing" contradicts the requirement for load balancing in the strategy name.

References:



FortiOS 7.4.1 Administration Guide: SD-WAN Rule Strategies

NEW QUESTION 13

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 must the administrator make on FortiGate to meet the requirements? (Choose two.)

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

Answer: AC

Explanation:

To configure redundant IPsec VPN tunnels on FortiGate with failover capability, the following two key configuration changes are required:



A. Enable Dead Peer Detection (DPD): Dead Peer Detection is crucial for detecting if the remote peer is unreachable. By enabling DPD, FortiGate can quickly detect a dead tunnel, ensuring a faster failover to the secondary tunnel when the primary tunnel goes down.



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: The static route with the lower distance (higher priority) will be used when both tunnels are operational. If the primary tunnel fails, the higher distance (lower priority) route for the secondary tunnel will take over, ensuring traffic is routed correctly.

The other options are not suitable:



B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels:

This option is not directly related to the requirements of failover between two IPsec VPN tunnels.



D. Configure a higher distance on the static route for the primary tunnel and a lower distance on the static route for the secondary tunnel: This would prioritize the secondary tunnel over the primary tunnel, which is opposite to the desired configuration.

References



FortiOS 7.4.1 Administration Guide - Configuring IPsec VPN, page 1320.



FortiOS 7.4.1 Administration Guide - Redundant VPN Configuration, page 1335.

NEW QUESTION 17

Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

- A. Pre-shared key and certificate signature as authentication methods
- B. Extended authentication (XAuth) to request the remote peer to provide a username and password
- C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
- D. No certificate is required on the remote peer when you set the certificate signature as the authentication method

Answer: AB

Explanation:

FortiGate supports both pre-shared key and certificate signature methods for IKEv1 authentication. These methods provide flexibility depending on the security requirements of the network. Additionally, FortiGate supports Extended Authentication (XAuth), which requests a username and password from the remote peer, enhancing security by adding an extra layer of authentication. The XAuth method does not necessarily make the authentication faster; it is an additional security measure.

References:



FortiOS 7.4.1 Administration Guide: IPsec VPN Configuration

NEW QUESTION 22

Refer to the exhibit.

FortiGate routing database

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S      0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C      *> 10.0.1.0/24 is directly connected, port3
C      *> 10.200.1.0/24 is directly connected, port1
C      *> 10.200.2.0/24 is directly connected, port2
C      *> 172.16.100.0/24 is directly connected, port8
```

Which two statements are true about the routing entries in this database table? (Choose two.)

- A. All of the entries in the routing database table are installed in the FortiGate routing table.
- B. The port2 interface is marked as inactive.
- C. Both default routes have different administrative distances.
- D. The default route on port2 is marked as the standby route.

Answer: CD

Explanation:

The routing table in the exhibit shows two default routes (0.0.0.0/0) with different administrative distances:



The default route through port2 has an

administrative distance of 20.



The default route through port1 has an administrative distance of 10.

Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of 10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2.

Regarding the statement that the port2 interface is marked as inactive, there is no indication in the routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.

References:



FortiOS 7.4.1 Administration Guide: Default route configuration



FortiOS 7.4.1 Administration Guide: Routing table

NEW QUESTION 26

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.

Which order must FortiGate use when the web filter profile has features such as safe search enabled?

- A. FortiGuard category filter and rating filter
- B. Static domain filter, SSL inspection filter, and external connectors filters
- C. DNS-based web filter and proxy-based web filter
- D. Static URL filter, FortiGuard category filter, and advanced filters

Answer: D

Explanation:

FortiGate applies web filters in the following order: Static URL filter, FortiGuard category filter, Web content filter, Web script filter, and Antivirus scanning.

NEW QUESTION 31

Refer to the exhibit.

Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

Which statement about this firewall policy list is true?

- A. The Implicit group can include more than one deny firewall policy.
- B. The firewall policies are listed by ID sequence view.
- C. The firewall policies are listed by ingress and egress interfaces pairing view.
- D. LAN to WA
- E. WAN to LA
- F. and Implicit are sequence grouping view lists.

Answer: C

Explanation:

The firewall policy list in the exhibit is arranged in the "Interface Pair View," where policies are grouped by their incoming (ingress) and outgoing (egress) interface pairs. Each section (LAN to WAN, WAN to LAN, etc.) groups policies based on these interface pairings. This view helps administrators quickly identify which policies apply to specific traffic flows between network interfaces. Options A and D are incorrect because the Implicit group typically does not include more than one deny policy, and there is no "sequence grouping view" in FortiGate. Option B is incorrect as the list is not displayed strictly by ID sequence.

References:

FortiOS 7.4.1 Administration Guide: Firewall Policy Views

NEW QUESTION 33

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. SSL VPN idle-timeout
- B. SSL VPN login-timeout
- C. SSL VPN dtls-hello-timeout
- D. SSL VPN session-ttl

Answer: C

Explanation:

For a high-latency internet connection, the SSL VPN setting that should be adjusted is:

* C. SSL VPN dtls-hello-timeout: This setting determines how long the FortiGate will wait for a DTLS hello message from the client. For high-latency connections, increasing this timeout will prevent SSL VPN negotiation failures caused by delays in receiving the DTLS hello message.

The other options are not suitable:

* A. SSL VPN idle-timeout: This setting controls the idle time allowed before a session is terminated, which is not relevant to the initial connection establishment.

* B. SSL VPN login-timeout: This setting controls the maximum time allowed for a user to log in, but does not affect connection negotiation.

* D. SSL VPN session-ttl: This setting controls the total time-to-live for an SSL VPN session but does not directly address issues caused by high latency.

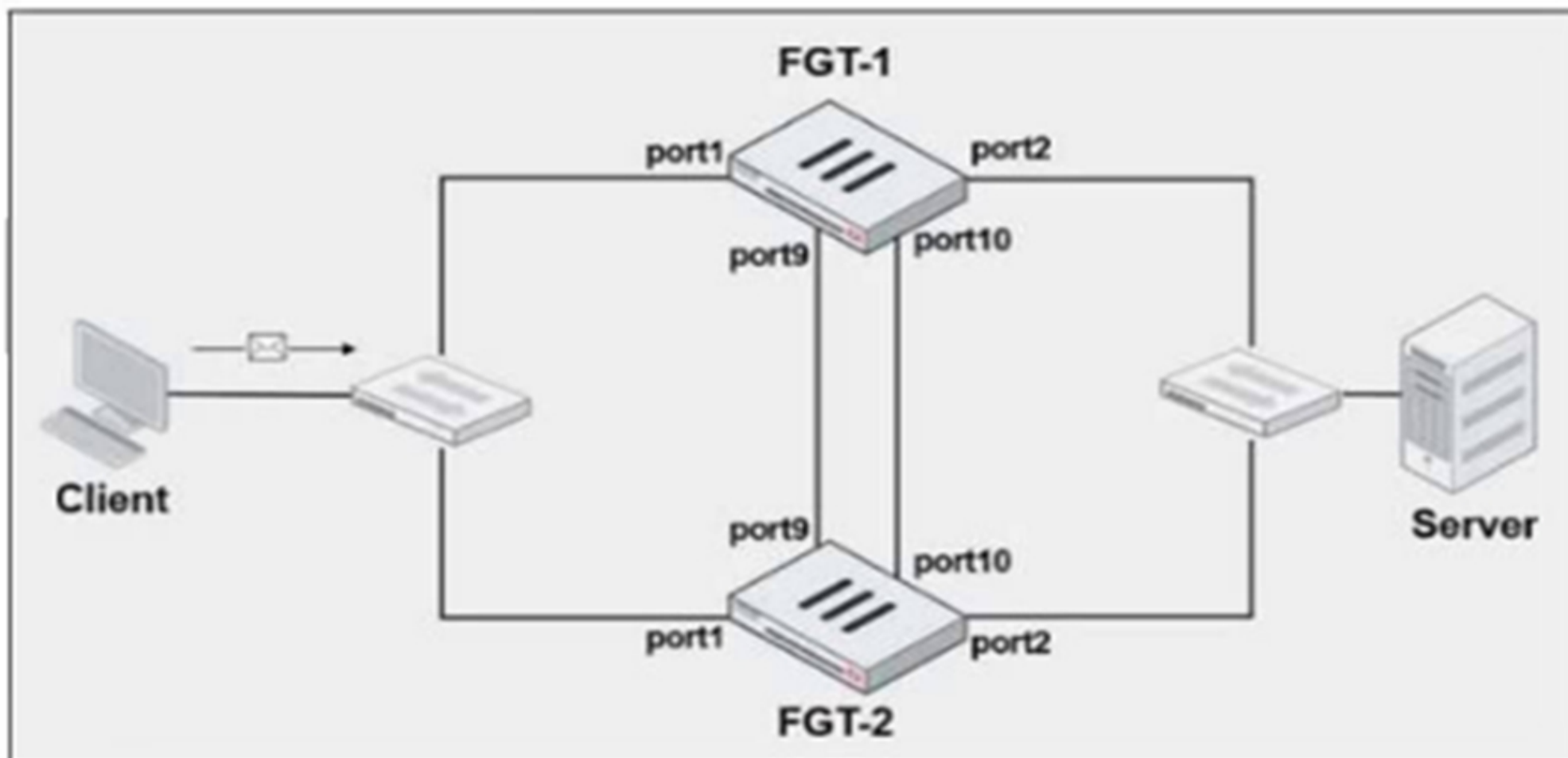
References

FortiOS 7.4.1 Administration Guide - SSL VPN Configuration, page 1415.

NEW QUESTION 38

Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

```
# get system ha status
...
Configuration Status:
  FGVM010000064692(updated 4 seconds ago): in-sync
  FGVM010000064692 checksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
  FGVM010000065036(updated 4 seconds ago): in-sync
  FGVM010000065036 checksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary      : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary    : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```


New FortiGate HA configuration

```
FGT-1
#config system ha
  set group-id 3
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port9" 50 "port10" 50
  set session-pickup enable
  set override disable
  set priority 90
  set monitor port3
```

```
FGT-2
#config system ha
  set group-id 3
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port9" 50 "port10" 50
  set session-pickup enable
  set override enable
  set priority 110
  set monitor port3
```

FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.
What would be the expected outcome in the HA cluster?

- A. FGT-1 will remain the primary because FGT-2 has lower priority.
- B. FGT-2 will take over as the primary because it has the override enable setting and higher priority than FGT-1.
- C. FGT-1 will synchronize the override disable setting with FGT-2.
- D. The HA cluster will become out of sync because the override setting must match on all HA members.

Answer: B

NEW QUESTION 39

Refer to the exhibit.

```
FGT1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S      0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]
C      172.20.121.0/24 is directly connected, port1
C      172.20.168.0/24 is directly connected, port2
C      172.20.167.0/24 is directly connected, port3
S      10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
S      10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
S      10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
```

Which route will be selected when trying to reach 10.20.30.254?

- A. 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
- B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
- C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
- D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]

Answer: A

Explanation:

The correct route selected when trying to reach 10.20.30.254 is 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0].

Prefix Length: The routing process prioritizes routes with the most specific (longest) prefix. In this case, 10.20.30.0/24 has a shorter prefix than 10.20.30.0/26 (option C), but it still matches the target address 10.20.30.254. The /24 subnet includes all addresses from 10.20.30.0 to 10.20.30.255, so 10.20.30.254 falls within this range.

• Administrative Distance and Metric: In the exhibit, all routes have the same administrative distance (AD) and metric, meaning they are considered equal in terms of preference. Hence, the prefix length becomes the primary factor for route selection.

Why the other options are less appropriate:

- B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
 - This route is for a different subnet, 10.30.20.0/24, which does not include the target address 10.20.30.254. Therefore, it is not a valid match.
- C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
 - Although this has a more specific prefix (/26), which means it should cover a smaller range of addresses, the /26 subnet only includes addresses from 10.20.30.0 to 10.20.30.63. The target address 10.20.30.254 does not fall within this range, so this route will not be selected.
- D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]
 - This is a default route (0.0.0.0/0) used for any address that doesn't match a more specific route. Since 10.20.30.254 matches the 10.20.30.0/24 route (option A), the default route will not be selected.

NEW QUESTION 44

Which of the following methods can be used to configure FortiGate to perform source NAT (SNAT) for outgoing traffic?

- A. Configure a static route pointing to the external interface.
- B. Enable the "Use Outgoing Interface Address" option in a firewall policy.
- C. Create a virtual server with an external IP address.
- D. Deploy an IPsec VPN tunnel with NAT enabled.

Answer: B

Explanation:

To configure source NAT (SNAT) for outgoing traffic on FortiGate, one of the most common methods is to enable the "Use Outgoing Interface Address" option in a firewall policy. This option ensures that the source IP address of packets leaving the FortiGate device is replaced by the IP address of the outgoing interface. This is typically done when traffic is exiting a private network to access the internet, requiring source NAT to translate the private IP addresses to a public IP.

Why the other options are less appropriate:

- * A. Configure a static route pointing to the external interface: A static route is used to direct traffic, but it does not configure SNAT. It determines where packets are sent but does not modify the source IP.
- C. Create a virtual server with an external IP address: Virtual servers are used to provide destination NAT (DNAT) for incoming traffic, not SNAT for outgoing traffic.
- D. Deploy an IPsec VPN tunnel with NAT enabled: While IPsec VPN tunnels can be configured with NAT traversal, this is not the typical method for configuring SNAT for general outgoing internet traffic.

NEW QUESTION 48

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.

IPS Sensor

Edit IPS Sensor
WINDOWS_SERVER
[View IPS Signatures]

Name: EMAIL-SERVER-IPS
Comments:

IPS Signatures

Add Signatures
Delete
Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce			Server	TCP_SMT	All	Block	

IPS Filters

Add Filter
Edit Filter
Delete

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
<input checked="" type="checkbox"/>	IMAPLoginBruteForce	60	10	Source IP	Block	None
<input type="checkbox"/>	Digiplex Asterisk SIP/TCP Connection Class DoS	5	1	Any	Block	None

Apply

DoS Policy

Incoming Interface
port1

Source Address
all

Destination Address
all

Services
ALL

L3 Anomalies

Name	Status	Logging	Pass	Block	Action
ip_src_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block	
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block	

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force
- C. ip_src_session
- D. Location: server Protocol: SMTP

Answer: B

Explanation:

When FortiGate evaluates potential attacks, the IPS sensor follows a specific processing order based on the configuration of filters, signatures, and anomaly thresholds. In this case:

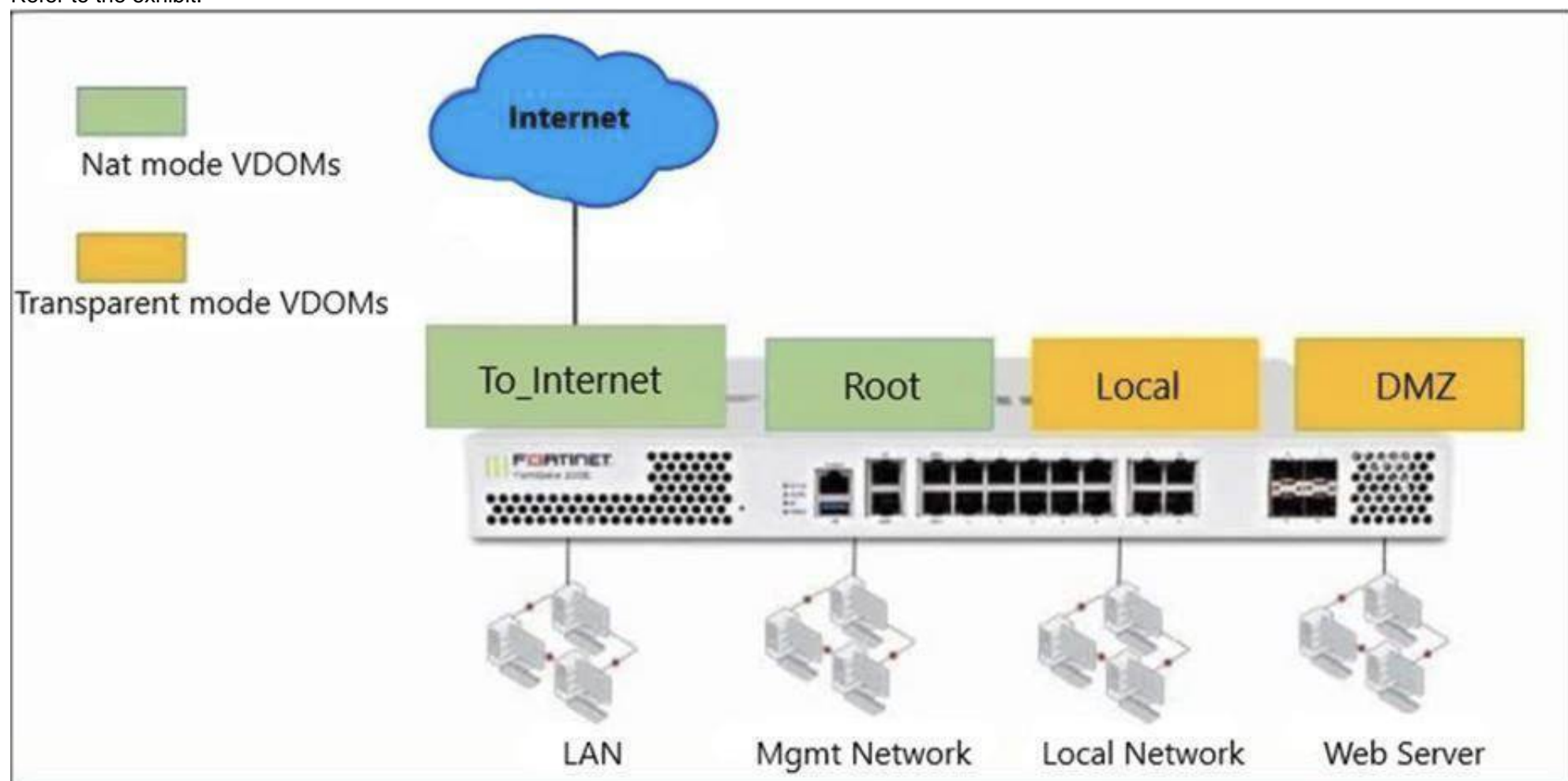
- The IPS sensor is configured with IMAP.Login.brute.Force, which comes first in the order of evaluation.
- FortiGate prioritizes based on signature definitions in the sensor, and since IMAP.Login.brute.Force appears higher in the configuration, it will be evaluated before the other signatures and anomalies.

Why the other options are less appropriate:

- A. SMTP.Login.Brute.Force: This would be evaluated after IMAP.Login.brute.Force, based on the sensor configuration hierarchy.
- C. ip_src_session: This is part of the DoS policy and does not come into play until after IPS signatures are evaluated.
- D. Location: server Protocol: SMTP: This appears to be part of the broader IPS sensor rule, but it is not the first item in the evaluation chain.

NEW QUESTION 53

Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode. The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem. With this configuration, which statement is true?

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

Answer: A

Explanation:

In this scenario, multiple Virtual Domains (VDOMs) are used, and each VDOM operates either in NAT mode or transparent mode:

- Root VDOM (management) and To_Internet VDOM are in NAT mode.
- DMZ VDOM and Local VDOM are in transparent mode.

To allow traffic between different VDOMs (e.g., Local and Root), inter-VDOM links must be configured.

Since Local VDOM is in transparent mode, it functions at Layer 2, meaning it requires an inter-VDOM link to pass traffic through the Root VDOM, which operates in NAT mode at Layer 3.

Why the other options are less appropriate:

- B. A default static route is not required on the To_Internet VDOM:

A default route is required on the To_Internet VDOM to send traffic from LAN users to the internet.

- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs:

Both Local and DMZ are in transparent mode and operate at Layer 2, so direct communication would require inter-VDOM links if passing through another VDOM.

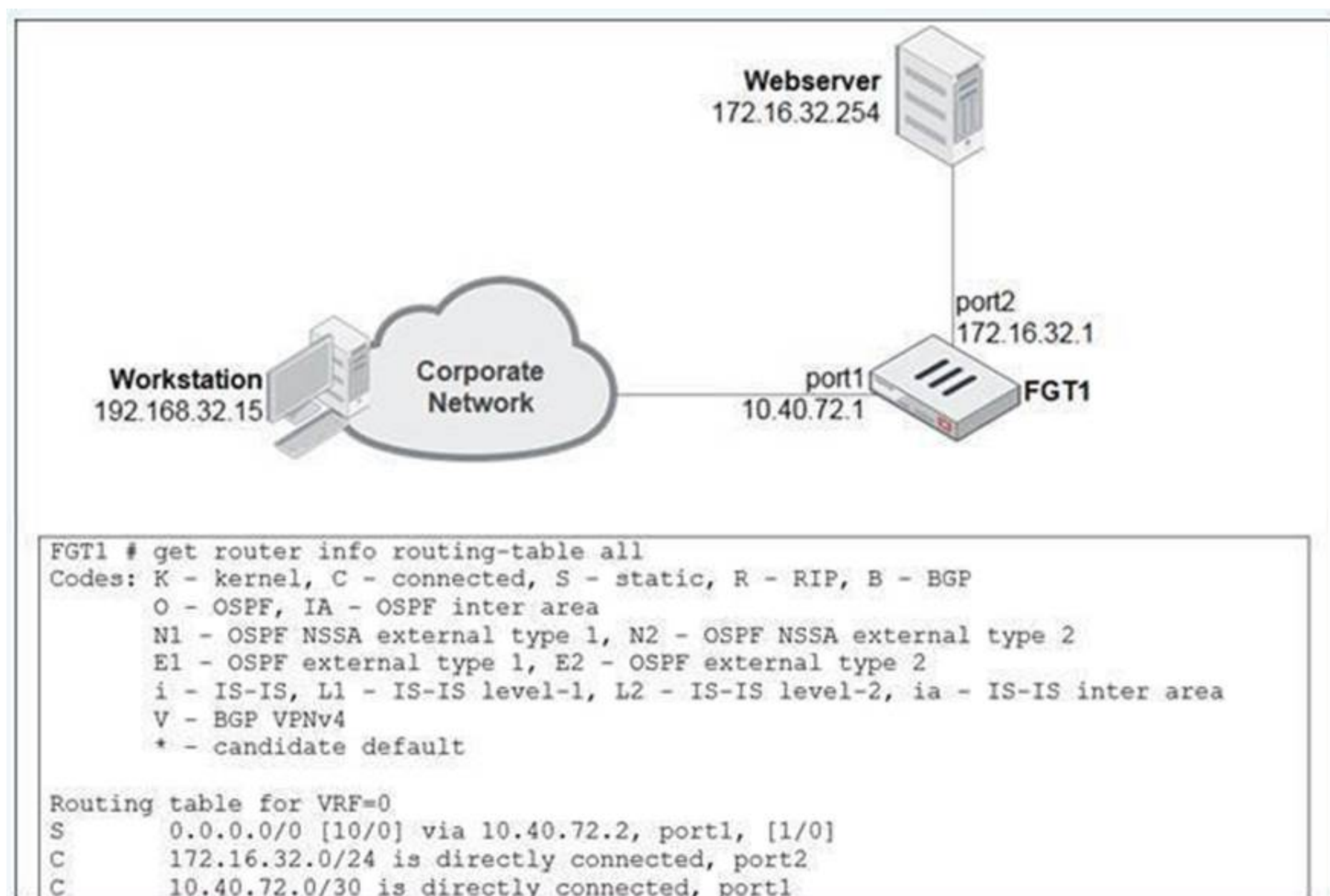
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs:

Even if the Root VDOM is only used for management, it still requires inter-VDOM links to communicate with other VDOMs (like To_Internet) in the Security Fabric.

NEW QUESTION 57

View the exhibit.

A user at 192.168.32.15 is trying to access the web server at 172.16.32.254.



Which two statements best describe how the FortiGate will perform reverse path forwarding (RPF) checks on this traffic? (Choose two.)

- A. Strict RPF check will deny the traffic.
- B. Loose RPF check will allow the traffic.
- C. Strict RPF check will allow the traffic.
- D. Loose RPF check will deny the traffic.

Answer: BC

Explanation:

When FortiGate performs reverse path forwarding (RPF) checks, it can operate in two modes: Strict RPF and Loose RPF. Here's how these two checks work:

In strict RPF, FortiGate checks whether the best route back to the source IP of the packet (in this case, 192.168.32.15) goes through the same interface on which the packet was received. If the best return path uses a different interface, the packet is denied. Based on the scenario:

o C. Strict RPF check will allow the traffic:

If the return path for 192.168.32.15 matches the interface where the traffic was received, the strict RPF check will allow the traffic.

• Loose RPF Check:

In loose RPF, FortiGate only checks if there is any route back to the source IP of the packet, regardless of the interface. This is a more permissive check, and if a route exists, the packet will be allowed.

o B. Loose RPF check will allow the traffic:

Since loose RPF requires only that a valid route to the source exists, the traffic is allowed.

Why the other options are less appropriate:

• A. Strict RPF check will deny the traffic:

This would only happen if the return route didn't match the incoming interface, which is not indicated here.

• D. Loose RPF check will deny the traffic:

Loose RPF is more permissive, so it will not deny the traffic as long as a valid route to the source IP exists.

NEW QUESTION 59

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

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

Answer: ACE

Explanation:

• A. Services defined in the firewall policy: FortiGate uses the service specified in the firewall policy to match traffic. Services define the types of traffic (like HTTP, FTP) that the policy will apply to.

- C. Destination defined as Internet Services in the firewall policy: Policies can be matched based on the destination being categorized as Internet Services, allowing specific handling of such traffic.
 - E. Source defined as Internet Services in the firewall policy: Similarly, traffic from sources categorized as Internet Services can be matched and processed according to the policy configuration.
- Why the other options are less relevant:
- B. Highest to lowest priority defined in the firewall policy: Policies are processed from top to bottom, not by priority. The highest priority policy is processed first, but this is about the order of policy processing rather than criteria for matching traffic.
 - D. Lowest to highest policy ID number: Policies are processed from the top of the list (the lowest policy ID) to the bottom (the highest policy ID), which is about the processing order rather than matching criteria.

NEW QUESTION 62

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FGT_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FGT_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FGT_AD-7.4/

Money Back Guarantee

FCP_FGT_AD-7.4 Practice Exam Features:

- * FCP_FGT_AD-7.4 Questions and Answers Updated Frequently
- * FCP_FGT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FGT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FGT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year