



Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Which three methods are used by the collector agent for AD polling? (Choose three.)

- A. WinSecLog
- B. WMI
- C. NetAPI
- D. FSSO REST API
- E. FortiGate polling

Answer: ABC

Explanation:

The Fortinet Single Sign-On (FSSO) Collector Agent supports three primary methods for Active Directory (AD) polling to collect user information:

- WinSecLog: Monitors Windows Security Event Logs for login events.
- WMI: Uses Windows Management Instrumentation to poll user login sessions.
- NetAPI: Utilizes the Netlogon API to query domain controllers for user session data.

These methods allow the FortiGate to gather user logon information and enforce user-based policies effectively.

References:

- FortiOS 7.4.1 Administration Guide: FSSO Configuration

NEW QUESTION 2

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 3

Refer to the exhibit, which shows a partial configuration from the remote authentication server.

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	 

Why does the FortiGate administrator need this configuration?

- A. To authenticate only the Training user group.
- B. To set up a RADIUS server Secret
- C. To authenticate and match the Training OU on the RADIUS server.
- D. To authenticate Any FortiGate user groups.

Answer: A

NEW QUESTION 4

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 1

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 5

Refer to the exhibit.

Edit Web Filter Profile

Name

Corporate

Comments

Write a comment...

0/255

Feature set

Flow-based

Proxy-based

FortiGuard Category Based Filter

Allow

Monitor

Block

Warning

Authenticate

Name	Action
<div><div></div>Bandwidth Consuming 6</div>	
Freeware and Software Downloads	<div><div></div>Allow</div>
File Sharing and Storage	<div><div></div>Allow</div>
Streaming Media and Download	<div><div></div>Allow</div>
Peer-to-peer File Sharing	<div><div></div>Allow</div>
Internet Radio and TV	<div><div></div>Allow</div>
Internet Telephony	<div><div></div>Allow</div>
<div><div></div>Security Risk 6</div>	
Malicious Websites	<div><div></div>Block</div>

35% 91

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. Set the Freeware and Software Downloads category Action to Warning

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

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

Answer: AD

Explanation:

To block access specifically to download.com while allowing other sites in the "Freeware and Software Downloads" category, you can create a separate firewall policy with a deny action specifically for the FQDN *.download.com. This approach allows blocking this particular site without affecting the other sites in the same category. Alternatively, configuring a static URL filter entry with the type set to Wildcard and action set to Block will also achieve the desired effect by directly blocking the specific URL without impacting other sites in the category.

References:

- FortiOS 7.4.1 Administration Guide: URL filter configuration

NEW QUESTION 6

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:

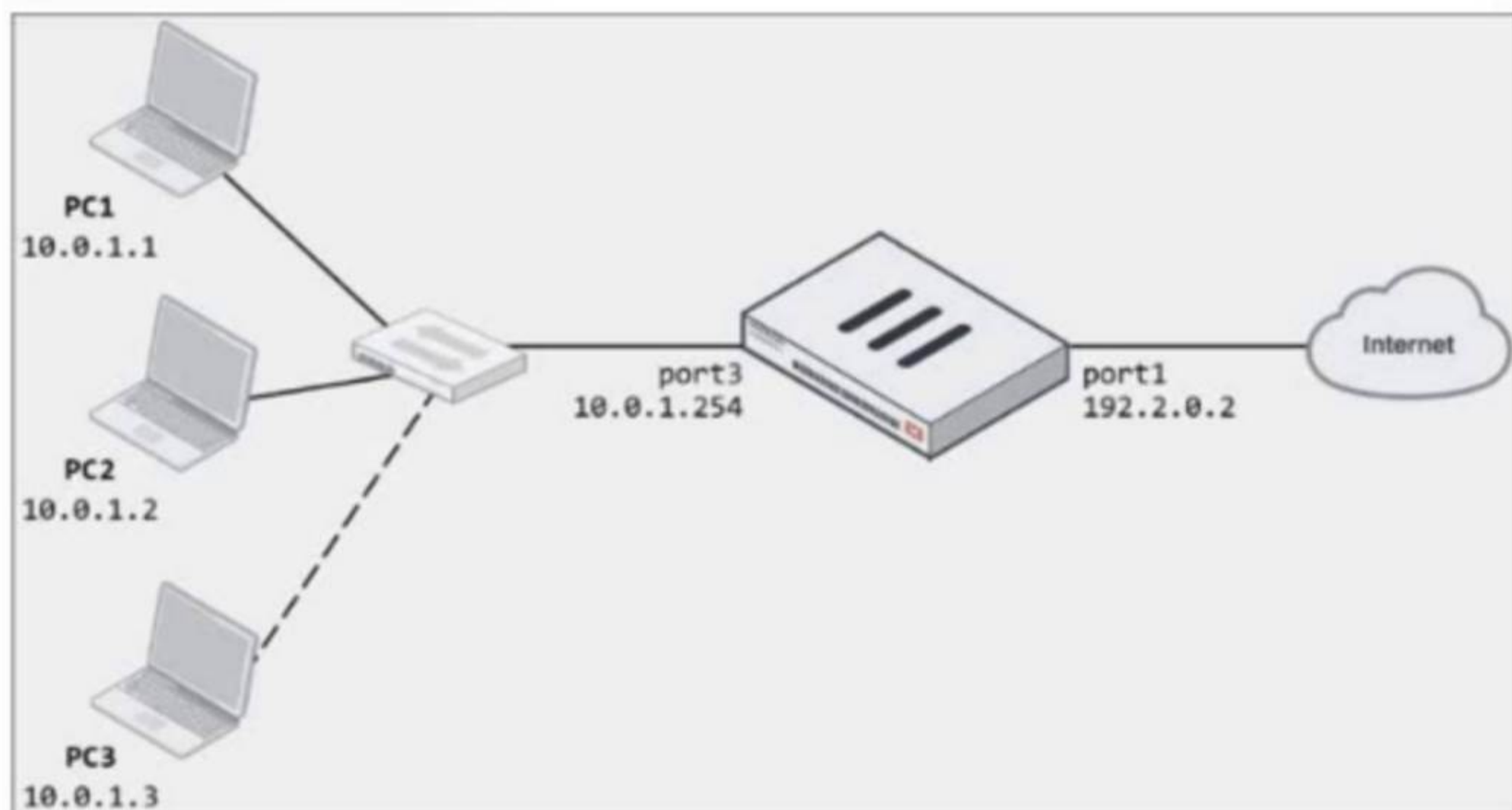


FortiOS 7.4.1 Administration Guide: Console connection

NEW QUESTION 7

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 	

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.

Your Partner of IT Exam

visit - <https://www.exambible.com>

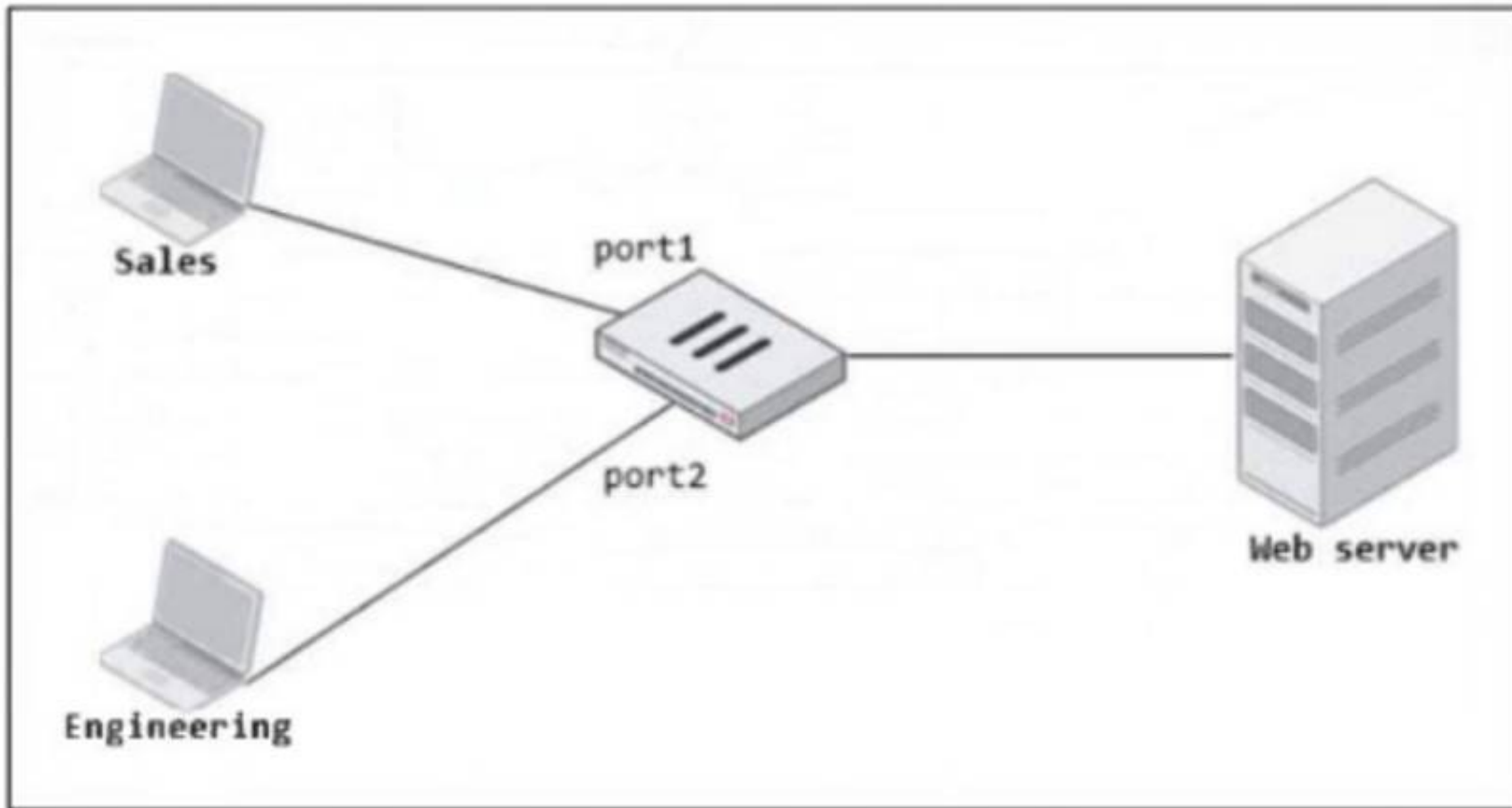
- D. In the IP pool configuration, set type to overload: Instead of using a one-to-one NAT, changing the type to overload will allow multiple internal addresses (such as PC1, PC2, and PC3) to share a single external IP address. This will solve the issue without needing additional public IP addresses. 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 8

Refer to the exhibit.



FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles. Which action must the administrator perform to consolidate the two policies into one?

- A. Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy
- B. Create an Interface Group that includes port1 and port2 to create a single firewall policy
- C. Select port1 and port2 subnets in a single firewall policy.
- D. Replace port1 and port2 with the any interface in a single firewall policy.

Answer: B

Explanation:

To consolidate the two separate firewall policies for Sales and Engineering departments accessing the same web server, you can create an Interface Group that includes both port1 (Sales) and port2 (Engineering). Once the Interface Group is created, you can use this group as a single incoming interface in a single firewall policy. This approach reduces the number of policies, making management more efficient.

References:

- FortiOS 7.4.1 Administration Guide: Firewall Policy Configuration

NEW QUESTION 9

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

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 10

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 11

Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

- A. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.
- B. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
- C. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP
- D. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.

Answer: AD

Explanation:

When SD-WAN is enabled on FortiGate, the load balancing algorithm for Equal-Cost Multi-Path (ECMP) is configured using the load-balance-mode parameter under SD-WAN settings. However, if SD-WAN is disabled, the ECMP load balancing algorithm can be configured under config system settings. This flexibility allows FortiGate to control traffic routing behavior based on the network configuration and requirements.

References:

- FortiOS 7.4.1 Administration Guide: ECMP Configuration

NEW QUESTION 15

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 18

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > Priority > System uptime > FortiGate serial number
- B. Connected monitored ports > System uptime > Priority > FortiGate serial number
- C. Connected monitored ports > Priority > HA uptime > FortiGate serial number
- D. Connected monitored ports > HA uptime > Priority > FortiGate serial number

Answer: A

Explanation:

When the HA override setting is disabled, FortiGate uses the primary election process based on the following criteria:



Connected monitored ports: The unit with the most monitored ports up is preferred.



Priority: The unit with the highest priority is preferred.



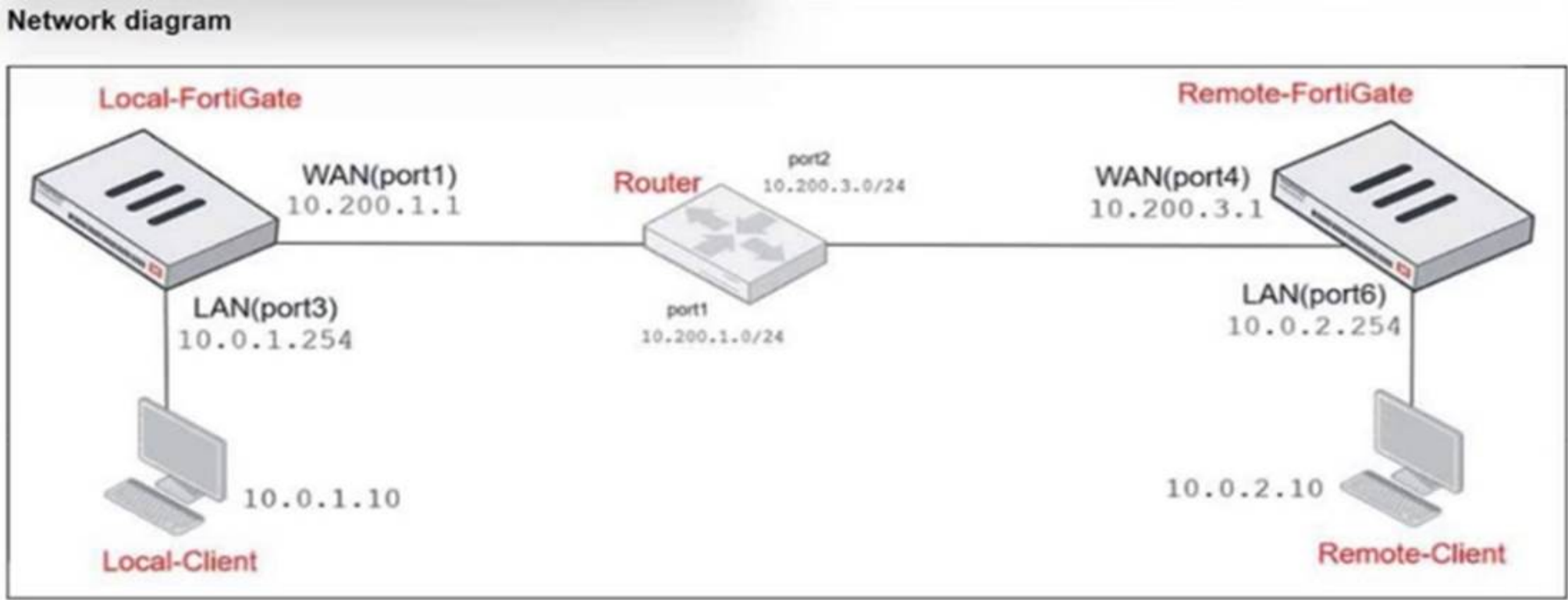
System uptime: The unit with the longest uptime is preferred.



FortiGate serial number: Used as the final criterion to break any remaining ties.

References:

NEW QUESTION 21
Refer to the exhibits.



NAT IP pool configuration

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

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port3) --> WAN (port1)								
2	TCP traffic	all	REMOTE_FORTIGATE	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
6	PING traffic	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
7	IGMP traffic	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects. 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. Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

- A. 10.200.1.1
- B. 10.200.1.149
- C. 10.200.1.99
- D. 10.200.1.49

Answer: C

Explanation:
The traffic from the user on Local-Client (10.0.1.10) pinging the IP address of Remote-FortiGate (10.200.3.1) will match the firewall policy with the service "PING traffic". According to the firewall policy:

Policy ID 6 is set for PING traffic and uses the NAT IP pool "SNAT-Remote1", which is defined as 10.200.1.99.

NEW QUESTION 26
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 30

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:

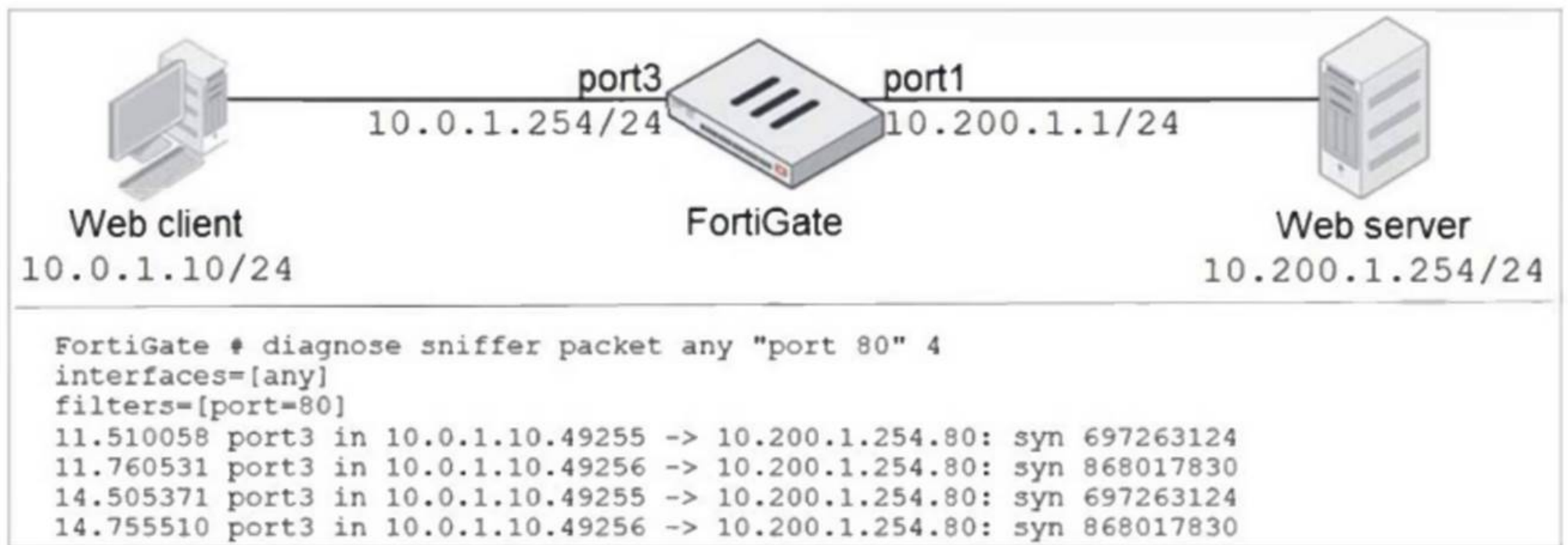
For a high-latency internet connection, the SSL VPN setting that should be adjusted is:
* C. SSL VPN dtls-hello-timeout: This setting determines how long the FortiGate will wait for a DTLS hello message from the client. For high-latency connections, increasing this timeout will prevent SSL VPN negotiation 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 34

Refer to the exhibit.



In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.

What should the administrator do next, to troubleshoot the problem?

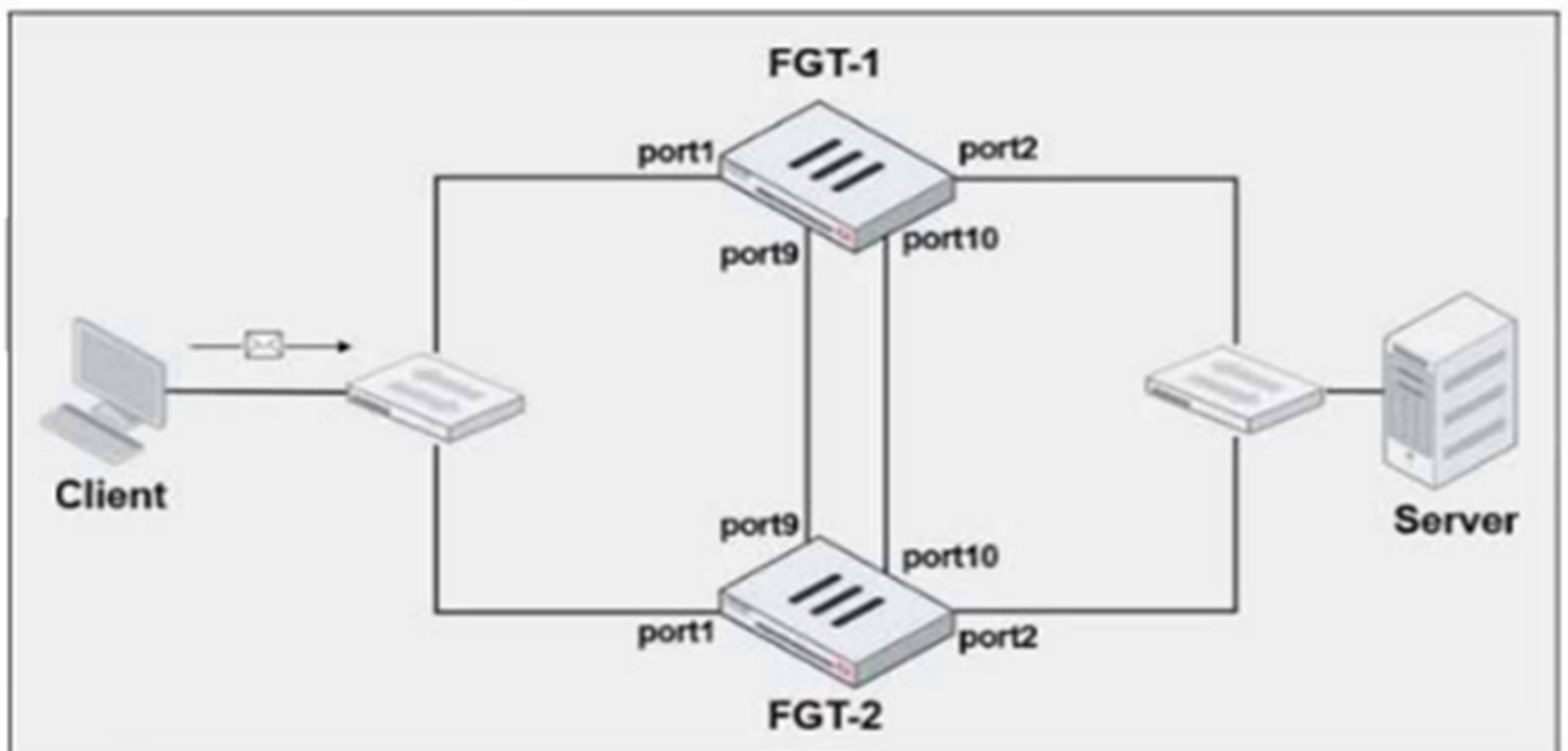
- A. Execute a debug flow.
- B. Capture the traffic using an external sniffer connected to port1.
- C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".
- D. Run a sniffer on the web server.

Answer: A

NEW QUESTION 35

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 37

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 39

Refer to the exhibit.



In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.

What should the administrator do next to troubleshoot the problem?

- A. Run a sniffer on the web server.
- B. Capture the traffic using an external sniffer connected to port1.
- C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??
- D. Execute a debug flow.

Answer: D

Explanation:

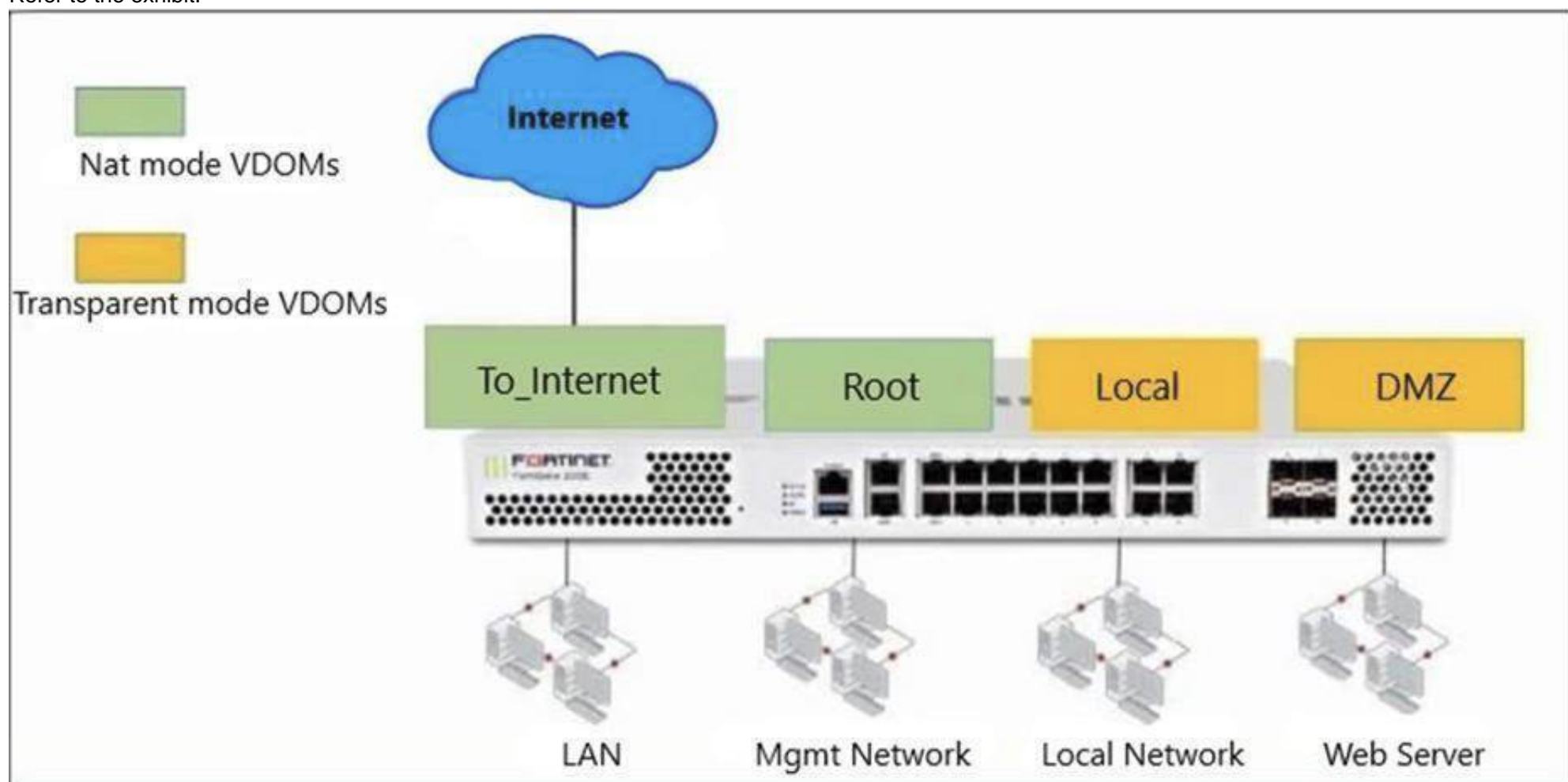
The next step for troubleshooting the problem would be to execute a debug flow on the FortiGate. The debug flow command provides detailed insights into how FortiGate handles the traffic, including whether the traffic is being dropped, allowed, or forwarded to the correct interface. It helps in identifying issues like firewall policy misconfigurations, routing issues, or NAT problems.

- A. Run a sniffer on the web server: While this might help diagnose server-side issues, the initial focus should be on the FortiGate, as the problem might lie in the firewall configuration or traffic handling.
- B. Capture the traffic using an external sniffer connected to port1: This may provide packetlevel information, but it's more useful to first analyze FortiGate's internal decision-making process with a debug flow.
- C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??: Running a sniffer on the specific host might give more packet details, but the debug flow provides more comprehensive information on how the firewall processes the packets.

Thus, using the debug flow will offer a more direct understanding of how the traffic is being processed or blocked within FortiGate.

NEW QUESTION 44

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 48

Consider the topology:

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

An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout. The administrator has already verified that the issue is not caused by the application or Linux server.

This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

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

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

Answer: CD

Explanation:

The issue with the idle session timing out after 90 minutes can be resolved by adjusting the session Time-To-Live (TTL) for the TELNET service used over the SSL VPN connection. Here's how the administrator

can address the problem:

- C. Create a new service object for TELNET and set the maximum session TTL:

By creating a new service object specifically for TELNET and setting a custom maximum session TTL, the administrator can ensure that the TELNET session does not time out prematurely. This way, the session will last longer or indefinitely, depending on the configured TTL.

- D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy:

Creating a dedicated firewall policy for SSL VPN traffic and placing it above the existing one allows the administrator to apply the new TELNET service object with a longer session TTL. This will ensure the new policy with the adjusted settings takes precedence for TELNET traffic.

Why the other options are less appropriate:

- A. Set the maximum session TTL value for the TELNET service object:

This would work if you were adjusting an existing TELNET service object. However, creating a new service object for TELNET and applying it in the firewall policy (as described in options C and D) is more granular and won't affect other services using the same TELNET object.

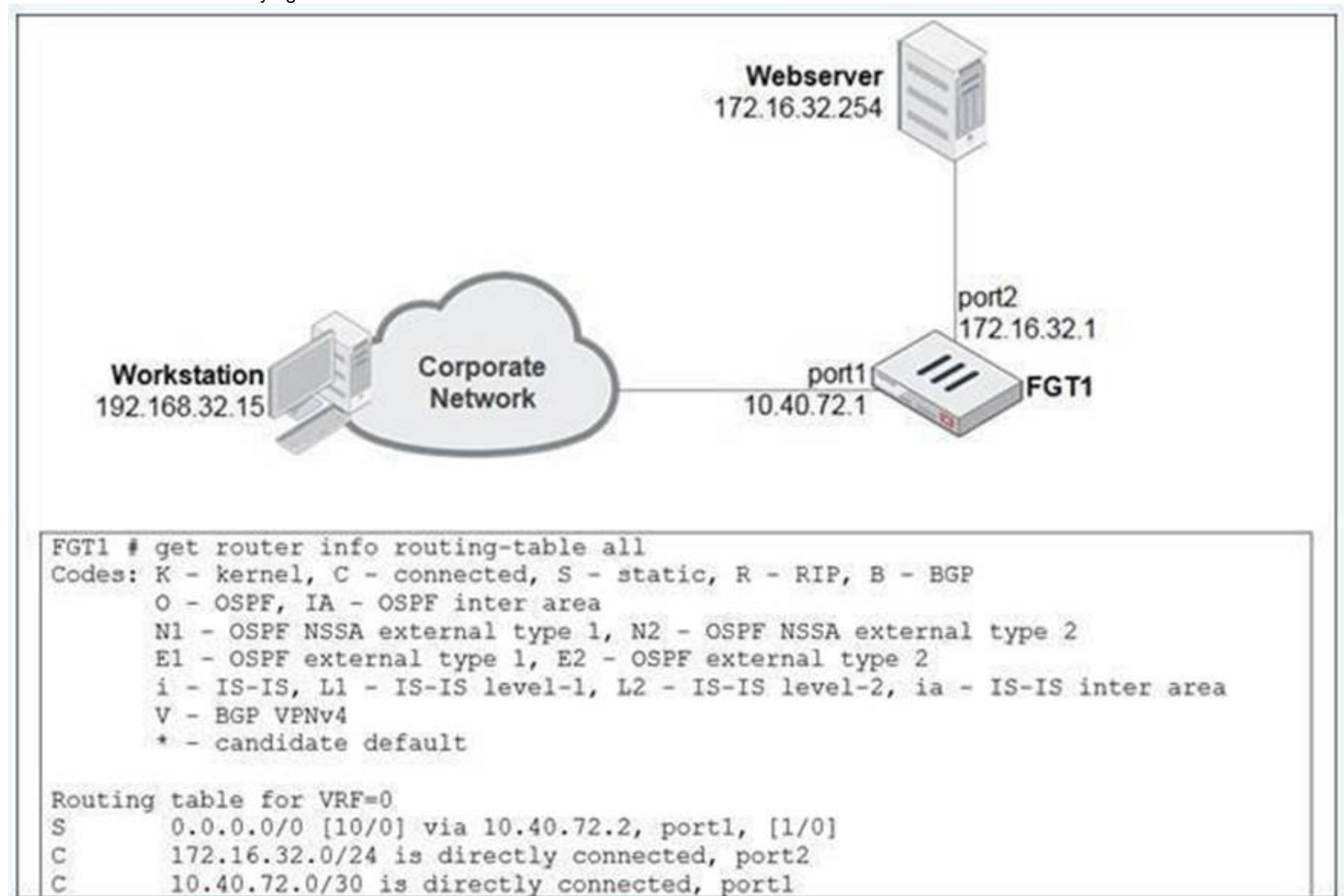
- B. Set the session TTL on the SSLVPN policy to maximum:

While this would extend the session timeout for the entire SSL VPN traffic, it could affect other services running through the SSL VPN, which may not be desirable. This option would lack the necessary specificity for only the TELNET traffic.

NEW QUESTION 49

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 52

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 56

.....

Relate Links

100% Pass Your FCP_FGT_AD-7.4 Exam with Exam Bible Prep Materials

https://www.exambible.com/FCP_FGT_AD-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>