



## **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**

Refer to the exhibit, which shows the IPS sensor configuration.

### Edit IPS Sensor

**Name** WINDOWS\_SERVERS

**Comments** Write a comment... 0/255

**Block malicious URLs**

#### IPS Signatures and Filters

+ Create New ✎ Edit 🗑 Delete

Details	Exempt IPs	Action	Packet Logging
Microsoft.Windows.iSCSI.Target.DoS	0	Monitor	Enabled
<span style="background-color: #333; color: white; padding: 2px 5px;">OS</span> Windows		Block	Disabled

2

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

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

**Answer:** AC

**Explanation:**

The IPS sensor configuration shows that:

➤ The Microsoft.Windows.iSCSI.Target.DoS signature is set to "Monitor" with packet logging enabled, meaning that while traffic matching this signature will be allowed, it will also be logged for further analysis.

➤ The generic Windows filter is set to "Block," meaning that all other attacks matching this filter will be blocked. However, the sensor will not reset connections or log packets unless specified.

Therefore, the sensor will allow attackers matching the specific DoS signature while blocking other attacks against Windows.

References:

➤ FortiOS 7.4.1 Administration Guide: IPS Configuration

**NEW QUESTION 2**

Which two statements describe how the RPF check is used? (Choose two.)

- A. The RPF check is run on the first sent packet of any new session.
- B. The RPF check is run on the first reply packet of any new session.
- C. The RPF check is run on the first sent and reply packet of any new session.
- D. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

**Answer:** AD

**Explanation:**

The Reverse Path Forwarding (RPF) check is run on the first sent packet of any new session to ensure that the packet arrives on a legitimate interface. This check protects the network from IP spoofing attacks by verifying that a return route exists from the receiving interface back to the source IP address. If the route is invalid or not found, the packet is discarded. Options B and C are incorrect because RPF checks are performed on the first sent packet, not the reply packet.

References:

➤ FortiOS 7.4.1 Administration Guide: Reverse Path Forwarding (RPF) Check

### 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

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.

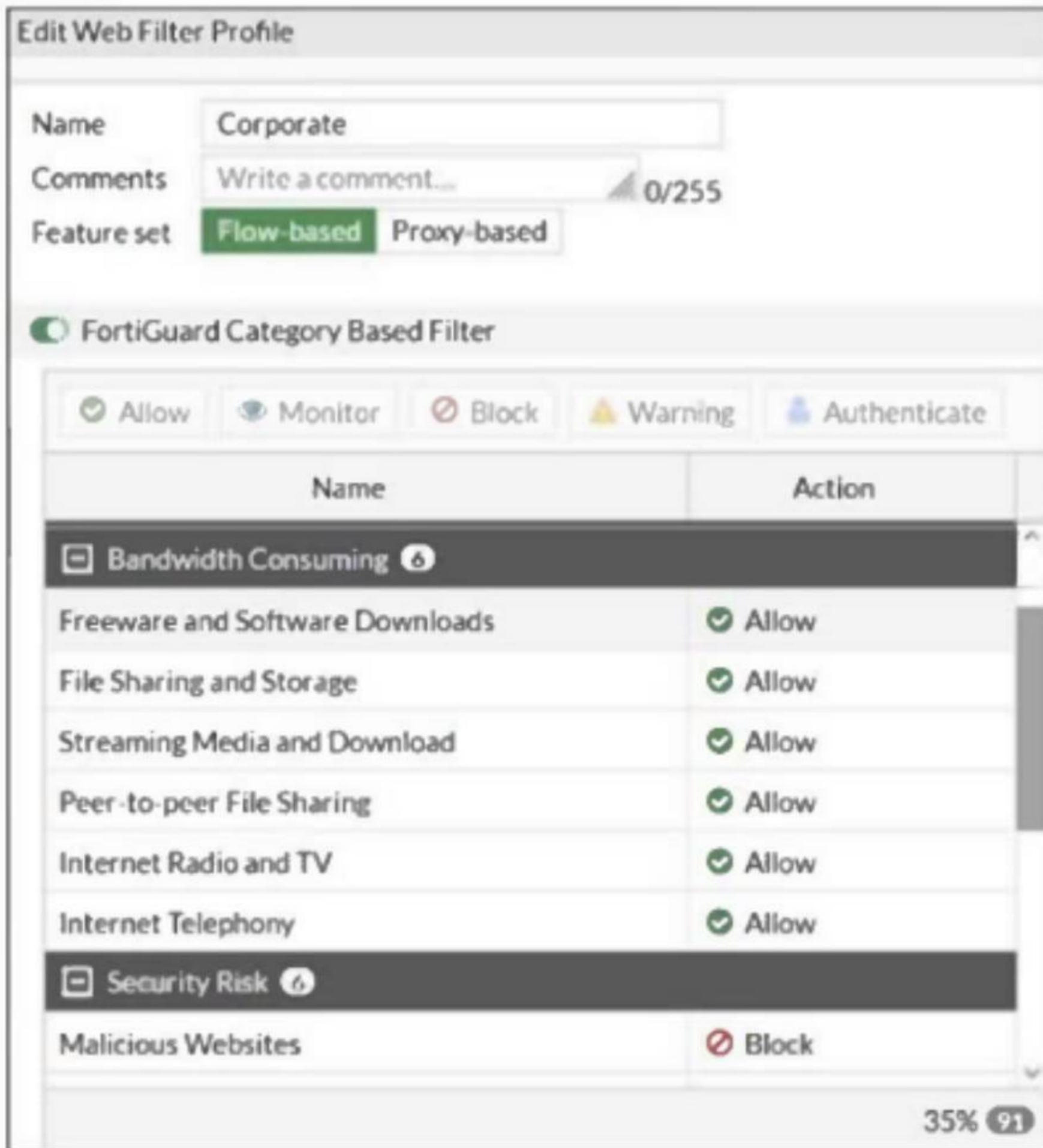
**Answer:** A

**Explanation:**

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

### NEW QUESTION 5

Refer to the exhibit.



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 two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

- A. Checksums of devices are compared against each other to ensure configurations are the same.
- B. Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.
- C. Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster
- D. Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

**Answer:** AB

#### Explanation:

In FortiGate HA (High Availability) configuration, checksums of device configurations are compared to ensure they are synchronized and identical across the cluster. Incremental synchronization can only happen from changes made on the primary device to ensure consistency and integrity across the cluster members. Changes made on non-primary devices do not initiate synchronization.

References:

- [FortiOS 7.4.1 Administration Guide: HA Configuration Synchronization](#)

### NEW QUESTION 7

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The host field in the HTTP header.
- B. The server name indication (SNI) extension in the client hello message.
- C. The subject alternative name (SAN) field in the server certificate.
- D. The subject field in the server certificate.
- E. The serial number in the server certificate.

**Answer:** BCD

#### Explanation:

When SSL certificate inspection is enabled on a FortiGate device, the system uses the following three pieces of information to identify the hostname of the SSL server:

- Server Name Indication (SNI) extension in the client hello message (B): The SNI is an extension in the client hello message of the SSL/TLS protocol. It indicates the hostname the client is attempting to connect to. This allows FortiGate to identify the server's hostname during the SSL handshake.
  - Subject Alternative Name (SAN) field in the server certificate (C): The SAN field in the server certificate lists additional hostnames or IP addresses that the certificate is valid for. FortiGate inspects this field to confirm the identity of the server.
  - Subject field in the server certificate (D): The Subject field contains the primary hostname or domain name for which the certificate was issued. FortiGate uses this information to match and validate the server's identity during SSL certificate inspection.
- The other options are not used in SSL certificate inspection for hostname identification:

- Host field in the HTTP header (A): This is part of the HTTP request, not the SSL handshake, and is not used for SSL certificate inspection.
- Serial number in the server certificate (E): The serial number is used for certificate management and revocation, not for hostname identification.

References:

- [FortiOS 7.4.1 Administration Guide - SSL/SSH Inspection, page 1802.](#)
- [FortiOS 7.4.1 Administration Guide - Configuring SSL/SSH Inspection Profile, page 1799.](#)

### NEW QUESTION 8

Which statement is a characteristic of automation stitches?

- A. They can be run only on devices in the Security Fabric.
- B. They can be created only on downstream devices in the fabric.
- C. They can have one or more triggers.
- D. They can run multiple actions at the same time.

**Answer:** C

#### Explanation:

Automation stitches on FortiGate can have one or more triggers, which are conditions or events that activate the automation stitch. The trigger defines when the automation stitch should execute the defined actions. Actions within a stitch can be executed sequentially or in parallel, depending on the configuration.

References:

- [FortiOS 7.4.1 Administration Guide: Automation Stitches](#)

### NEW QUESTION 9

Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.

## System Performance output

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

## Memory usage threshold settings

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

Based on the system performance output, what can be the two possible outcomes? (Choose two.)

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

**Answer:** BC

### Explanation:

Based on the system performance output provided, the memory usage on the FortiGate device is at 90%, which is above the green threshold (82%) but below the red threshold (88%). Given this high memory usage, the FortiGate device will enter "conserve mode" to prevent further resource exhaustion. In conserve mode:

- B. FortiGate has entered conserve mode: When the memory usage reaches or exceeds certain thresholds (in this case, the green and red thresholds), the FortiGate enters conserve mode to protect itself from running out of memory entirely. This mode limits some functionalities to reduce memory usage and avoid a potential system crash.
- D. Administrators can access FortiGate only through the console port: During conserve mode, administrative access might be restricted, and administrators may only be able to connect to the device via the console port. This restriction is in place to ensure that the FortiGate can be managed directly, even under low resource conditions.

The other options are not correct:

- A. FortiGate will start sending all files to FortiSandbox for inspection: This is unrelated to memory usage and conserve mode.
- C. Administrators cannot change the configuration: While access may be limited, configuration changes can still be made via the console port.

### References

- FortiOS 7.4.1 Administration Guide - Monitoring System Resources and Performance, page 325.
- FortiOS 7.4.1 Administration Guide - Conserve Mode, page 330.

### NEW QUESTION 10

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 DNS over HTTPS.
- C. It uses DNS over TLS.
- D. It uses UDP 53.

**Answer:** D

### Explanation:

By default, DNS queries to FortiGuard servers use UDP port 53.

### 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 11**

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 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**

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 19**

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:

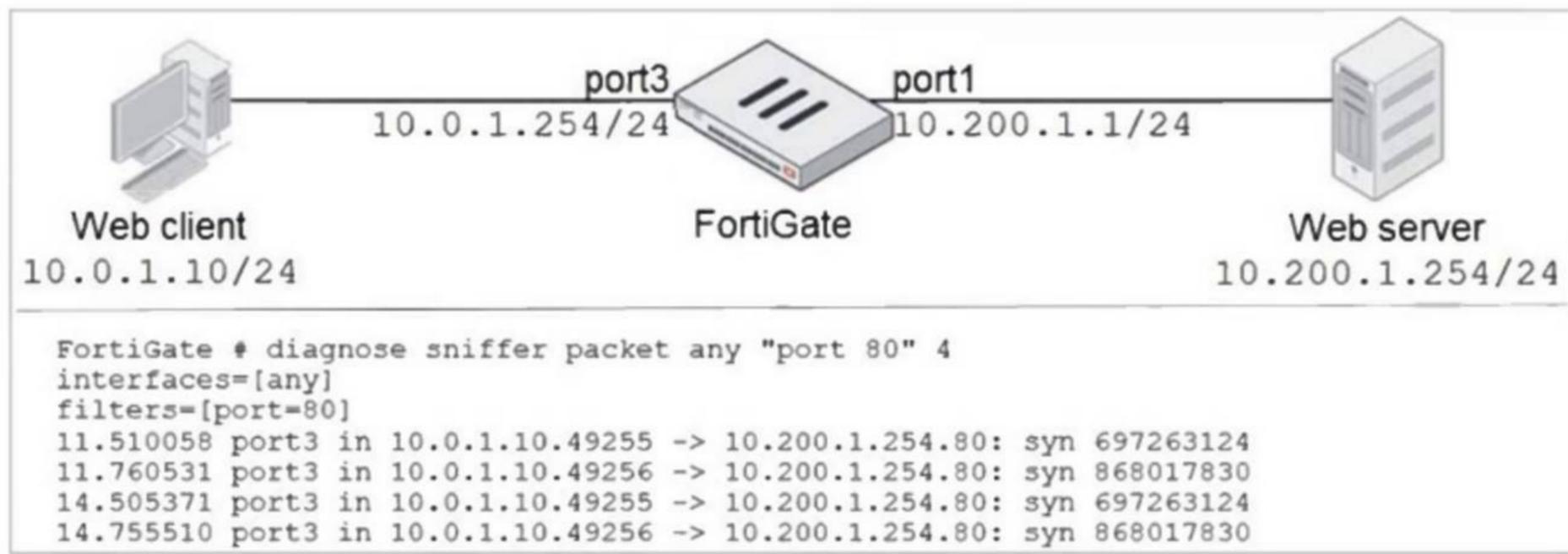
- Connected monitored ports: The unit with the most monitored ports up is preferred.
- Priority: The unit with the highest priority is preferred.
- System uptime: The unit with the longest uptime is preferred.
- FortiGate serial number: Used as the final criterion to break any remaining ties.

References:

- FortiOS 7.4.1 Administration Guide: HA election process

**NEW QUESTION 21**

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 25**

Which two IP pool types are useful for carrier-grade NAT deployments? (Choose two.)

- A. Port block allocation
- B. Fixed port range
- C. One-to-one
- D. Overload

**Answer:** AB

**Explanation:**

In carrier-grade NAT (CGNAT) deployments, specific IP pool types are used to manage large-scale NAT translations efficiently. The correct IP pool types for CGNAT are:

- A. Port block allocation: This type of IP pool allocates a block of ports from a single public IP to multiple clients. It allows efficient use of a limited number of public IPs by distributing port ranges among users, which is crucial for carrier-grade NAT environments where a large number of users need access to the internet.
  - B. Fixed port range: In this type, each client is assigned a fixed range of ports, ensuring that the same public IP and port range are used consistently. This helps in reducing the complexity and overhead of managing dynamic port assignments, which is particularly useful in large-scale CGNAT setups.
- Why the other options are less appropriate:
- C. One-to-one: One-to-one NAT is used for mapping a single private IP address to a single public IP address. This is not efficient for carrier-grade NAT because CGNAT is designed to allow multiple clients to share a smaller number of public IPs.
  - D. Overload: Overload, also known as PAT (Port Address Translation), maps multiple private IPs to a single public IP by differentiating connections based on port numbers. While commonly used in regular NAT setups, CGNAT benefits more from port block allocation and fixed port range due to th

**NEW QUESTION 29**

.....

## Relate Links

**100% Pass Your FCP\_FGT\_AD-7.4 Exam with Exambible Prep Materials**

[https://www.exambible.com/FCP\\_FGT\\_AD-7.4-exam/](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/>