

FCP_FGT_AD-7.4 Dumps

FCP - FortiGate 7.4 Administrator

https://www.certleader.com/FCP_FGT_AD-7.4-dumps.html



NEW QUESTION 1

When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate. Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

- A. Allow & Warning
- B. Trust & Allow
- C. Allow
- D. Block & Warning
- E. Block

Answer: ADE

Explanation:

When FortiGate performs SSL/SSH full inspection and detects an invalid certificate, there are three valid actions it can take:



Allow & Warning: This action allows the session but generates a warning.



Block & Warning: This action blocks the session and generates a warning.



Block: This action blocks the session without generating a warning.

Actions such as "Trust & Allow" or just "Allow" without additional configurations are not applicable in the context of handling invalid certificates.

References:



FortiOS 7.4.1 Administration Guide: Configuring SSL/SSH inspection profile

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

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 4

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 profil
- 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 5

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 6

Refer to the exhibit.

IPsec tunnel configuration

The diagram shows two FortiGate devices connected via the Internet. HQ-FortiGate is on the left with port1 (10.10.100.10) connected to the Internet. Remote-FortiGate is on the right with port2 (10.10.200.10) connected to the Internet.

Configuration Screenshots:

Left Screenshot (HQ-FortiGate):

- Network:** IP Version: IPv4, Remote Gateway: Static IP Address, IP Address: 10.10.200.10, Interface: port1, Local Gateway: ☒, Mode Config: ☐, NAT Traversal: Enable, Keepalive Frequency: 10, Dead Peer Detection: Disable, DPD retry count: 3, DPD retry interval: 20 s, Forward Error Correction: Egress ☐ Ingress ☐ Advanced...
- Authentication:** Method: Pre-shared Key, Pre-shared Key: [REDACTED], IKE: Version: 1 2, Mode: Aggressive Main (ID protection), Peer Options: Accept Types: Any peer ID
- Phase 1 Proposal:** Add, Encryption: AES128 Authentication: SHA1, Encryption: AES256 Authentication: SHA256, Diffie-Hellman Groups: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1, Key Lifetime (seconds): 86400, Local ID: [REDACTED]

Right Screenshot (Remote-FortiGate):

- Network:** IP Version: IPv4, Remote Gateway: Static IP Address, IP Address: 10.10.100.10, Interface: port1, Local Gateway: ☒, Mode Config: ☐, NAT Traversal: Enable, Keepalive Frequency: 10, Dead Peer Detection: Disable, DPD retry count: 3, DPD retry interval: 20 s, Forward Error Correction: Egress ☐ Ingress ☐ Advanced...
- Authentication:** Method: Pre-shared Key, Pre-shared Key: [REDACTED], IKE: Version: 1 2, Mode: Aggressive Main (ID protection)
- Phase 1 Proposal:** Add, Encryption: AES256 Authentication: SHA256, Diffie-Hellman Groups: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1, Key Lifetime (seconds): 86400, Local ID: [REDACTED]

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 failed to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match. Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes can the administrator make to bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, disable Diffie-Helman group 2.
- B. On Remote-FortiGate, set port2 as Interface.
- C. On both FortiGate devices, set Dead Peer Detection to On Demand.
- D. On HQ-FortiGate, set IKE mode to Main (ID protection).

Answer: CD

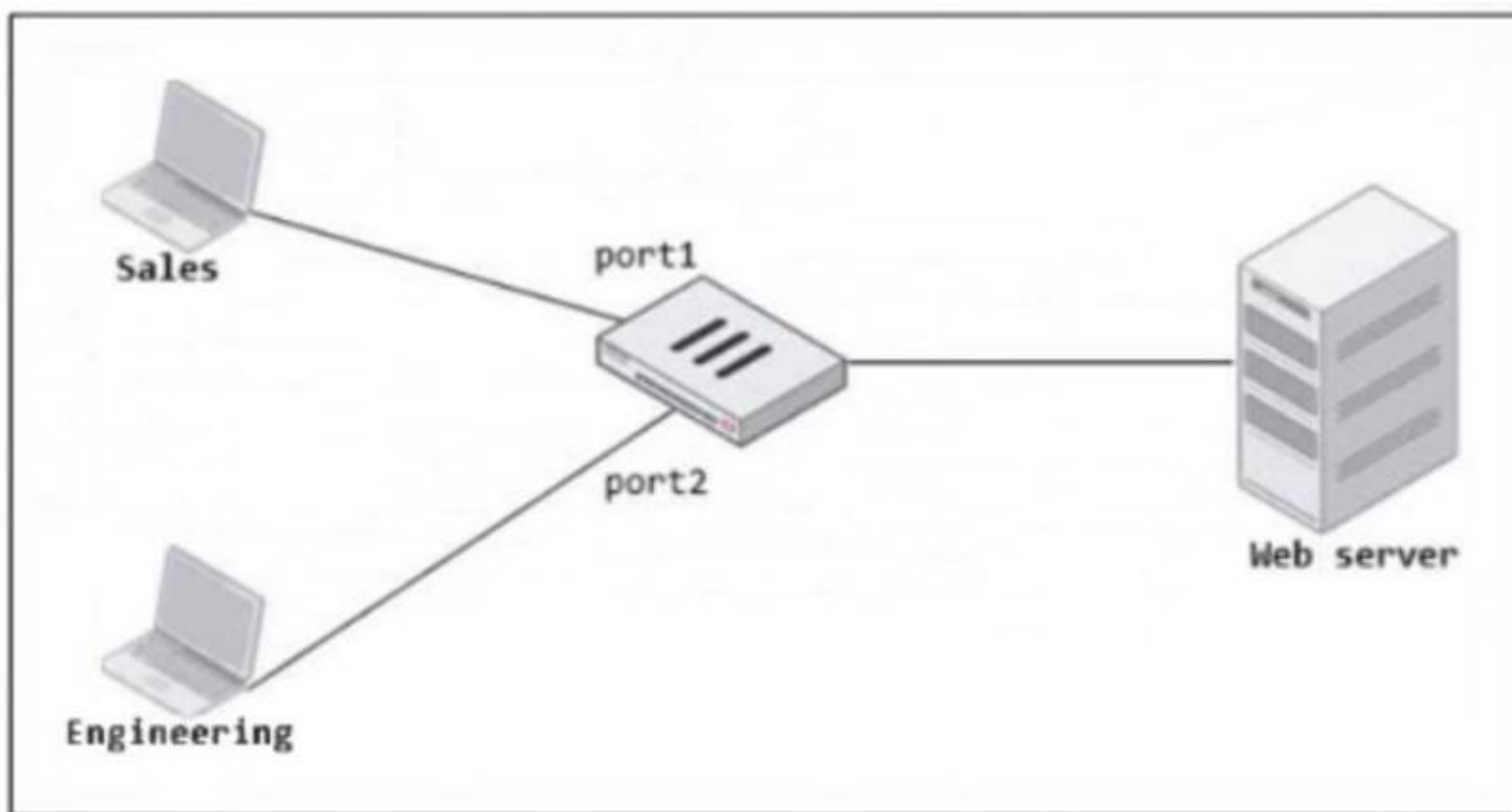
Explanation:

To bring Phase 1 up, the following changes can be made:

- A. On HQ-FortiGate, disable Diffie-Helman group 2: This is incorrect because Diffie-Hellman group 2 is already selected on both devices. Disabling it would not help.
 - B. On Remote-FortiGate, set port2 as Interface: This is incorrect as both sides should be consistent in their interface settings for the IPsec tunnel, and the interface is correctly set to port1 on both FortiGates in the IPsec configuration.
 - C. On both FortiGate devices, set Dead Peer Detection to On Demand: This is a valid option.
Setting Dead Peer Detection (DPD) to "On Demand" helps maintain the IPsec connection by checking if the peer is still available, which can help in some cases where the connection fails due to timeouts.
 - D. On HQ-FortiGate, set IKE mode to Main (ID protection): This is also a valid option because the Remote-FortiGate is already set to Main mode (ID protection). Ensuring that both ends use the same mode is crucial for successful phase 1 negotiation.
- Thus, the correct answers are: C. On both FortiGate devices, set Dead Peer Detection to On Demand. D. On HQ-FortiGate, set IKE mode to Main (ID protection).

NEW QUESTION 7

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 8

Refer to the exhibit to view the firewall policy.

Firewall policy configuration

Edit Policy

Name	Internet_Access	
Incoming Interface	<div> port2 </div> <div>+</div>	✕
Outgoing Interface	<div> port1 </div> <div>+</div>	✕
Source	<div> all </div> <div>+</div>	✕
Destination	<div> all </div> <div>+</div>	✕
Schedule	<div> always </div> <div>▼</div>	
Service	<div> <div> DNS </div> <div>✕</div> </div> <div> <div> FTP </div> <div>✕</div> </div> <div> <div> HTTP </div> <div>✕</div> </div> <div> <div> HTTPS </div> <div>✕</div> </div> <div>+</div>	
Action	<div> <div> ACCEPT </div> <div> DENY </div> </div>	
Inspection Mode	<div> <div>Flow-based</div> <div>Proxy-based</div> </div>	

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

default

▼

✎

Web Filter

DNS Filter

Application Control

IPS

File Filter

SSL Inspection

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 9

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 10

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 10

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

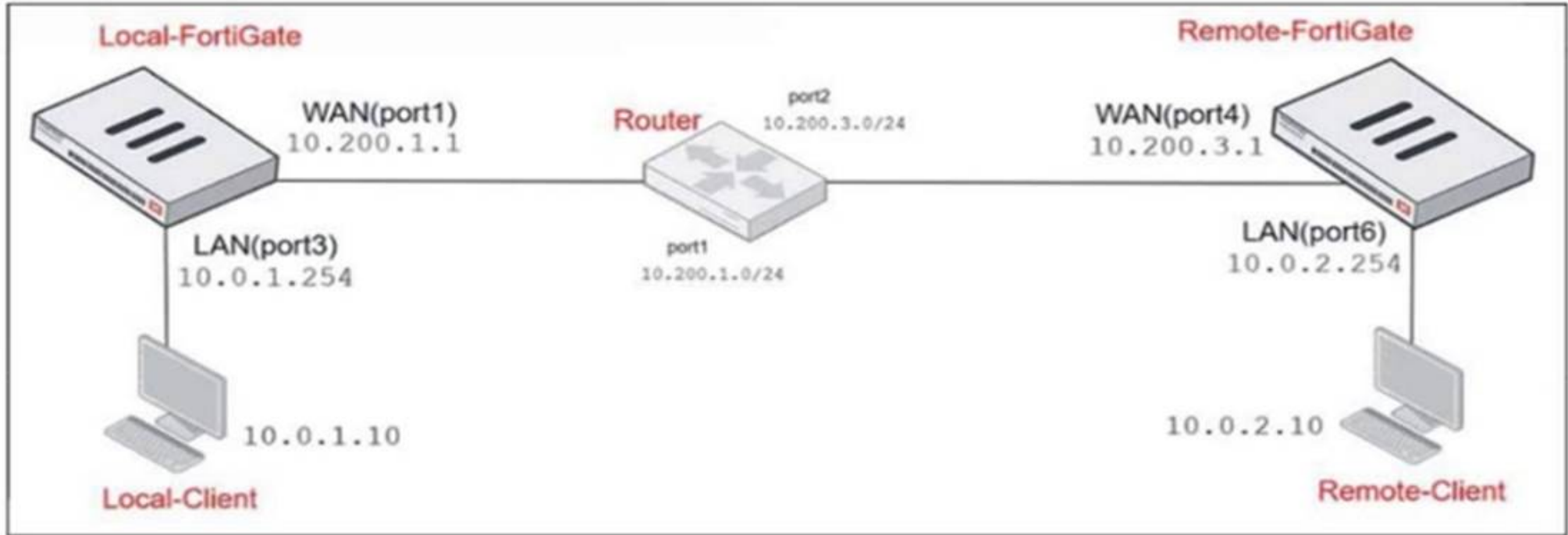
Explanation:

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 11

Refer to the exhibits.

Network diagram



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

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 16

Refer to the exhibit.

Application Details

NameAddicting Games

CategoryGame

TechnologyBrowser-Based

Popularity☆☆☆☆

Application Control Profile

Categories

All Categories

Business (144, △6)

Collaboration (268, △10)

Game (87)

Mobile (3)

P2P (63)

Remote.Access (84)

Storage.Backup (173, △17)

Video/Audio (160, △14)

Web.Client (23)

Cloud.IT (43)

Email (80, △12)

General.Interest (231, △7)

Network.Service (329)

Proxy (166)

Social.Media (121, △31)

Update (50)

VoIP (24)

Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New

Edit

Delete

Priority	Details	Type	Action
1	Addicting Games	Application	Allow
2	RISK <div><div></div><div></div><div></div><div></div></div>	Filter	Block

A user located behind the FortiGate device is trying to go to <http://www.addictinggames.com> (Addicting.Games). The exhibit shows the application details and application control profile.
Based on this configuration, which statement is true?

- A. Addicting.Games will be blocked, based on the Filter Overrides configuration.
- B. Addicting.Games will be allowed only if the Filter Overrides action is set to Learn.
- C. Addicting.Games will be allowed, based on the Categories configuration.
- D. Addicting.Games will be allowed, based on the Application Overrides configuration.

Answer: D

Explanation:

In the exhibit, it shows that the Application Overrides section is configured to allow the application Addicting.Games. The Application Control Profile gives priority to the application overrides, meaning that even if a category or filter would block it, the application control override would allow the specific application to proceed.

- A. Addicting.Games will be blocked, based on the Filter Overrides configuration:
This is incorrect because the Application Overrides take precedence over other filters.
- B. Addicting.Games will be allowed only if the Filter Overrides action is set to Learn:
This is not applicable as the action is based on Application Overrides, not filter overrides.
- C. Addicting.Games will be allowed, based on the Categories configuration:
This is not correct because the application is being allowed due to the Application Overrides, not the category settings.

Thus, the correct explanation is that Addicting.Games will be allowed due to the Application Overrides configuration.

NEW QUESTION 20

Which two statements correctly describe the differences between IPsec main mode and IPsec aggressive mode? (Choose two.)

- A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not.
- B. Main mode cannot be used for dialup VPNs, while aggressive mode can.
- C. Aggressive mode supports XAuth, while main mode does not.
- D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode.

Answer: AD

Explanation:

The differences between IPsec main mode and IPsec aggressive mode are mainly in the number of packets exchanged and the level of security provided during the negotiation process. Here's the breakdown:

- A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not:
In aggressive mode, the peer's identity is sent in the first packet, making the process faster but less secure because the peer's identity is not encrypted. In main mode, the peer's identity is protected and only exchanged after the encryption is established, offering more security.
- D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode:
Main mode involves a more detailed negotiation process, requiring the exchange of six packets. Aggressive mode, on the other hand, reduces this to three packets, speeding up the connection but sacrificing some security in the process.

Why the other options are less appropriate:

- B. Main mode cannot be used for dialup VPNs, while aggressive mode can:

This is incorrect. Main mode can be used for dialup VPNs as long as the peer's IP is known or configured in advance.

- C. Aggressive mode supports XAuth, while main mode does not:

Both main mode and aggressive mode can support XAuth (eXtended Authentication) if needed.

NEW QUESTION 23

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FGT_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FGT_AD-7.4-dumps.html