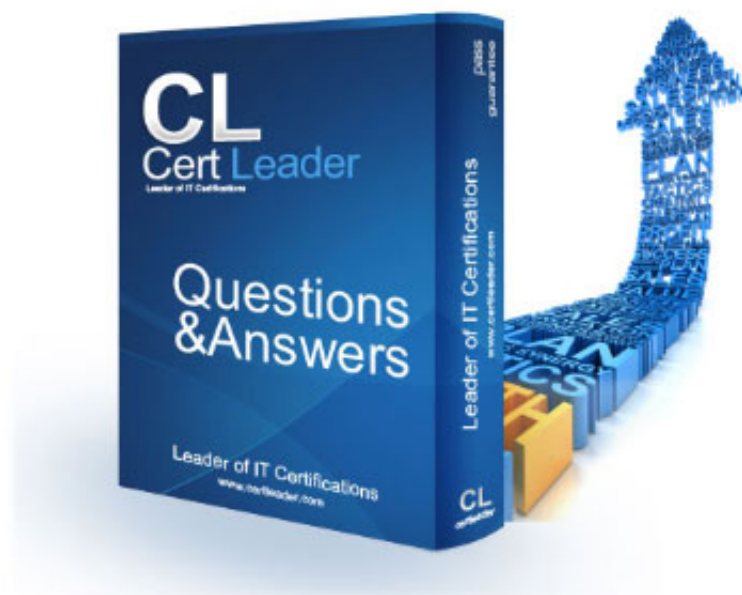


FCP_FGT_AD-7.6 Dumps

FCP - FortiGate 7.6 Administrator

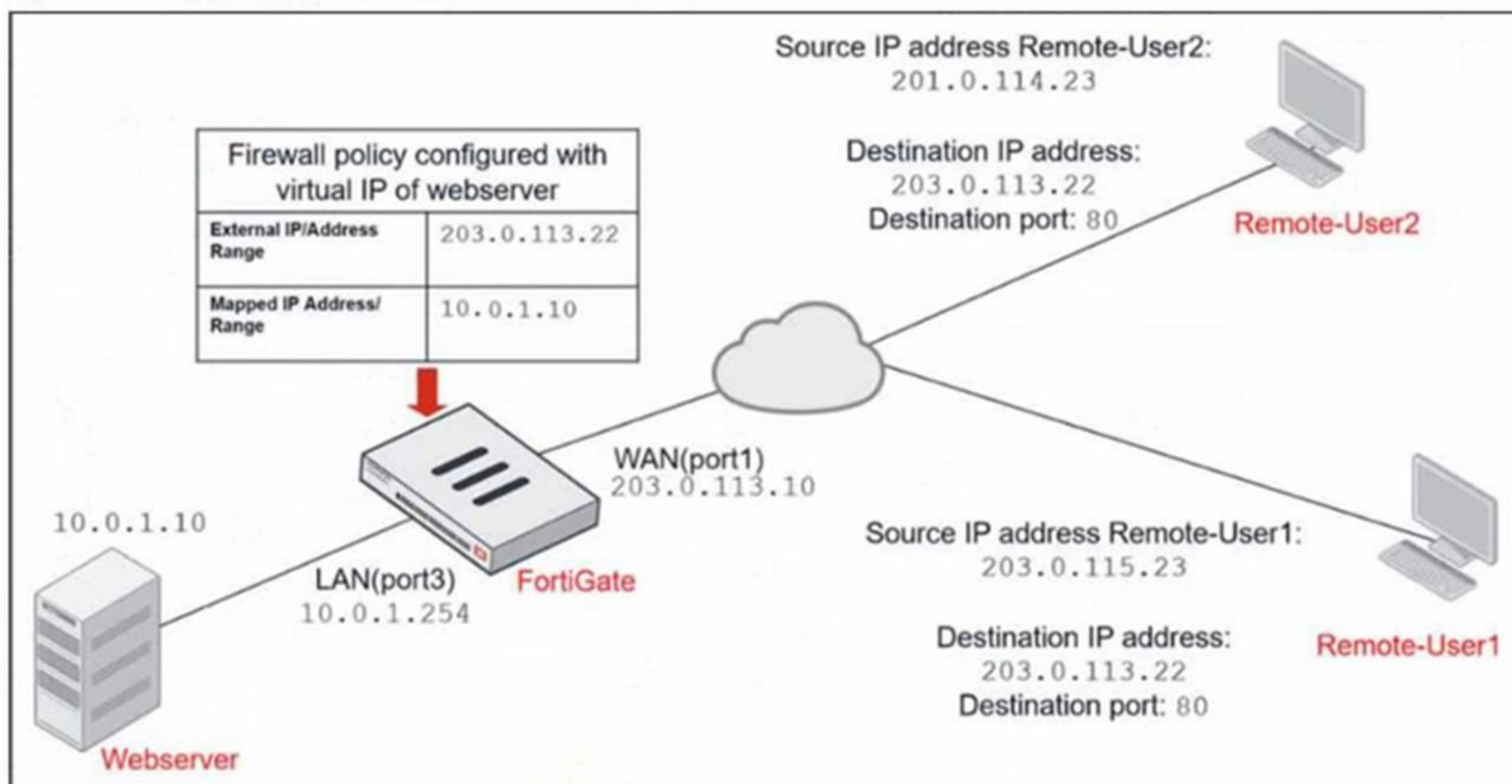
https://www.certleader.com/FCP_FGT_AD-7.6-dumps.html



NEW QUESTION 1

Refer to the exhibits.

Network diagram



Firewall address object

Edit Address

Name	Deny_IP
Color	Change
Type	Subnet
IP/Netmask	201.0.114.23/32
Interface	WAN (port1)
Static route configuration	☐
Comments	Deny web server access. 23/255

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.

The policy should work such that Remote-User1 must be able to access the Webserver while preventing

Remote-User2 from accessing the Webserver.

Which additional configuration can the administrator add to a deny firewall policy, beyond the default behavior, to block Remote-User2 from accessing the Webserver?

- A. Disable match-vip in the Allow_access policy
- B. Configure a One-to-One IP Pool object in a new policy.
- C. Set the Destination address as Webserver in the Deny policy.
- D. Set the Destination address as Deny_IP in the Allow_access policy.

Answer: C

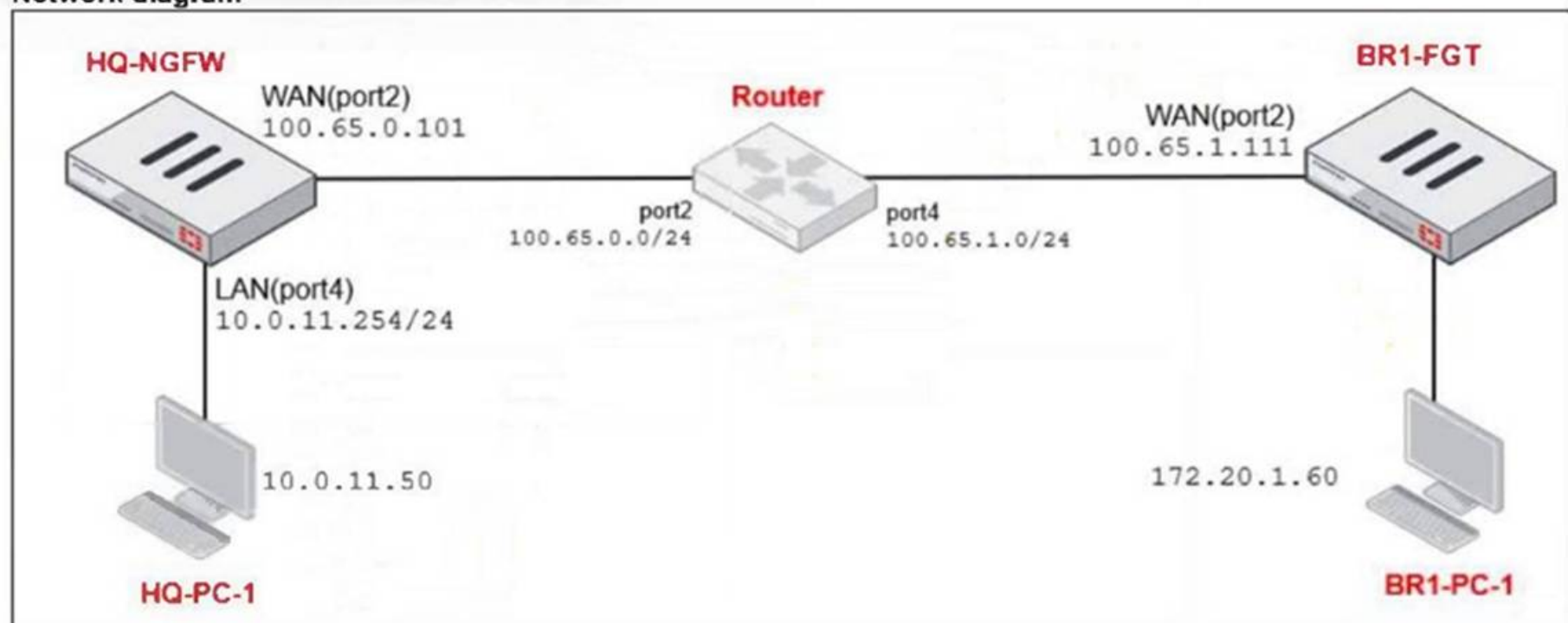
Explanation:

To block Remote-User2's access to the Webserver, the deny policy must explicitly specify the Webserver as the destination address; otherwise, it denies traffic to all destinations, which is not the desired behavior.

NEW QUESTION 2

Refer to the exhibits.

Network diagram



NAT IP pool configuration

	Name	External IP Range	Type	ARP Reply
☐	SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
☐	SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
☐	SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) 3							
☐ TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
☐ PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
☐ IGMP traffic (4)	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 (port2) interface has the IP address 100.65.0.101/24.

The LAN (port4) interface has the IP address 10.0.11.254/24.

Which IP address will be used to source NAT (SNAT) the traffic, if the user on HQ-PC-1 (10.0.11.50) pings the IP address of BR-FGT (100.65.1.111)

- A. 100.65.0.101
- B. 100.65.0.49
- C. 100.65.0.99
- D. 100.65.0.149

Answer: C

Explanation:

The ping traffic policy uses the IP pool named SNAT-Remote1, which has the external IP range 100.65.0.99. Therefore, traffic matching this policy (ping from HQ-PC-1 to BR1-FGT) will use 100.65.0.99 for source NAT.

NEW QUESTION 3

You have configured the below commands on a FortiGate.

```
config system settings
set strict-src-check enable
end
```

```
Config system interface
edit port1
set src-check disable
next
end
```

What would be the impact of this configuration on FortiGate?

- A. FortiGate will enable strict RPF on all its interfaces and port1 will be enabled for asymmetric routing.
- B. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
- C. Port1 will be enabled with flexible RPF, and all other interfaces will be enabled for strict RPF.
- D. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.

Answer: B

Explanation:

The global setting enables strict source checking (RPF) on all interfaces by default. The per-interface setting disables the source check on port1, exempting it from strict RPF enforcement.

NEW QUESTION 4

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. The collector agent uses a Windows API to query DCs for user logins.
- B. NetAPI polling can increase bandwidth usage in large networks.
- C. The NetSessionEnum function is used to track user logouts.
- D. The collector agent must search Windows application event logs.

Answer: B

Explanation:

NetAPI polling mode involves frequent queries to domain controllers, which can cause increased bandwidth usage, especially in large networks with many login events.

NEW QUESTION 5

You have configured the FortiGate device for FSSO. A user is successful in log-in to windows, but their access to the internet is denied. What should the administrator check first?

- A. Whether the user is assigned to the correct AD group.
- B. The FortiGate firewall policy settings for SSL decryption.
- C. The FortiGate FSSO active users list for user's IP address.
- D. The windows event viewer for failed login attempts.

Answer: C

Explanation:

Checking the active users list verifies if FortiGate correctly associates the user with their IP address, ensuring proper policy enforcement for internet access.

NEW QUESTION 6

A remote user reports slow SSL VPN performance and frequent disconnections. The user is located in an area with poor internet connectivity. What setting should the administrator adjust to improve the user's experience?

- A. Enable split tunneling to reduce VPN traffic.
- B. Change the SSL VPN port to a non-standard port.
- C. Increase the session timeout for inactive sessions.
- D. Configure the DTLS timeout to accommodate high-latency connections.

Answer: D

Explanation:

Adjusting the DTLS timeout helps maintain SSL VPN stability and performance in environments with poor or high-latency internet connectivity by allowing more time for packet retransmissions before dropping the connection.

NEW QUESTION 7

Refer to the exhibit.

FortiGate web filter profile configuration

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

35% 91

The exhibit shows theFortiGuard Category Based Filtersection of a corporate web filter profile.
An administrator must block access todownload.com, which belongs to theFreeware and Software Downloadscategory. The administrator must also allow other websites in the same category.
What are two solutions for satisfying the requirement? (Choose two.)

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

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

C. Configure a separate firewall policy with action Deny and an FQDN address object for*.download.com as destination address.

D. Set the Freeware and Software Downloads category Action to Warning.

Answer: AC

Explanation:

Creating a static URL filter to block download.com specifically allows blocking that site without affecting the entire category.
Using a separate firewall policy with a Deny action for an FQDN address object matching download.com can also block the site while allowing others in the same category.

The Leader of IT Certification

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

NEW QUESTION 8

A FortiGate firewall policy is configured with active authentication, however, the user cannot authenticate when accessing a website. Which protocol must FortiGate allow even though the user cannot authenticate?

- A. LDAP
- B. TACASC+
- C. Kerberos
- D. DNS

Answer: D

Explanation:

DNS traffic must be allowed so the user can resolve domain names and reach the authentication server or web resources, even if authentication initially fails.

NEW QUESTION 9

When configuring a FortiGate in a multi-WAN setup, why would an administrator enable session preservation on an interface?

- A. To allow the FortiGate to dynamically change interfaces for all active sessions when a WAN link fails
- B. To make sure all sessions without source NAT enabled always use the primary WAN link
- C. To improve security by forcing users to authenticate again when the WAN link changes
- D. To ensure that existing SSL VPN connections remain on the same interface even if route changes occur

Answer: D

Explanation:

Session preservation keeps active sessions, such as SSL VPNs, tied to the original interface to prevent disruption when WAN routes change.

NEW QUESTION 10

Refer to the exhibits.

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
  set group-id 5
  set group-name "Training"
  set mode a-p
  set password ENC a4fbyqY4iPexFmAnZgzDY
  set hbdev "port7" 0
  set session-pickup enable
  set override disable
  set priority 200
  set monitor "port1"
  set memory-based-failover enable
  set memory-failover-threshold 70
  set memory-failover-monitor-period 50
  set memory-failover-sample-rate 10
  set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # 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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # 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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32 kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds. Which FortiGate is the primary?

- A. HQ-NGFW-2 with the parameter memory-failover-threshold setting
- B. HQ-NGFW-2 with the parameter priority setting
- C. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting
- D. HQ-NGFW-1 with the parameter override setting

Answer: D

Explanation:

The HA configuration shows that override is disabled (set override disable), but despite this, HQ-NGFW-1 has the higher priority (200) and is acting as the primary, as indicated by its higher resource usage and uptime.

Override allows the device with higher priority to take over as primary, so HQ-NGFW-1 is the primary device.

NEW QUESTION 10

What are three key routing principles in SD-WAN? (Choose three.)

- A. By default
- B. SD-WAN rules are skipped if the included SD-WAN members do not have a valid route to the destination.
- C. SD-WAN rules have precedence over any other type of routes.
- D. Regular policy routes have precedence over SD-WAN rules.
- E. By default
- F. SD-WAN rules are skipped if only one route to the destination is available.
- G. By default
- H. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Answer: ABE

Explanation:

SD-WAN rules are skipped if none of the SD-WAN members have a valid route to the destination. SD-WAN rules take precedence over other route types. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member by default.

NEW QUESTION 12

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively. Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

- A. Both interfaces must have the interface role assigned.
- B. Both interfaces must have directly connected routes on the routing table.
- C. Both interfaces must have DHCP enabled and interfaces set to LAN and DMZ roles assigned.
- D. Both interfaces must have IP addresses assigned.

Answer: BD

Explanation:

Interfaces must have directly connected routes in the routing table to forward traffic correctly. Interfaces must have IP addresses assigned to communicate within their respective networks.

NEW QUESTION 17

Refer to the exhibit.



Phase 2 selectors

+ Create new Edit Delete

Search

Name	Local Address	Remote Address	Comments
ToBR1	10.0.11.0/255.255.255.0	172.20.1.0/255.255.255.0	

Edit Phase 2 Selector

Name: ToBR1

Comments: 0/255

Encapsulation: Tunnel Mode Transport Mode

IP version: IPv4 IPv6

Named address: ☐

Local address: IP Address Subnet Address IP Range
10.0.11.0 255.255.255.0

Remote address: IP Address Subnet Address IP Range
172.20.1.0 255.255.255.0

Advanced

Encryption - authentication: AES128 - SHA1

Replay detection: ☒ Enable ☐ Disable

Perfect forward secrecy (PFS): ☒ Enable ☐ Disable

Diffie-Hellman groups: ☐ 1 ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

Local port: All Specify

Remote port: All Specify

Protocol: All Specify

Auto-negotiate: ☒ Enable ☐ Disable

Autokey keep alive: ☒ Enable ☐ Disable

Key lifetime: Seconds Kilobytes Both
43200 second(s)

Phase 2 selectors

+ Create new Edit Delete

Search

Name	Local Address	Remote Address	Comments
ToHQ	172.20.1.0/255.255.255.0	10.11.0.0/255.255.255.0	

Edit Phase 2 Selector

Name: ToHQ

Comments: 0/255

Encapsulation: Tunnel Mode Transport Mode

IP version: IPv4 IPv6

Named address: ☐

Local address: IP Address Subnet Address IP Range
172.20.1.0 255.255.255.0

Remote address: IP Address Subnet Address IP Range
10.11.0.0 255.255.255.0

Advanced

Encryption - authentication: AES256 - SHA1

Replay detection: ☒ Enable ☐ Disable

Perfect forward secrecy (PFS): ☒ Enable ☐ Disable

Diffie-Hellman groups: ☐ 1 ☐ 2 ☒ 5 ☒ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 27 ☐ 28 ☐ 29 ☐ 30 ☐ 31 ☐ 32

Local port: All Specify

Remote port: All Specify

Protocol: All Specify

Auto-negotiate: ☒ Enable ☐ Disable

Autokey keep alive: ☒ Enable ☐ Disable

Key lifetime: Seconds Kilobytes Both
14400 second(s)

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.

Based on the phase 2 configuration shown in the exhibit, which two configuration changes will bring phase 2 up? (Choose two.)

- A. On BR1-FGT, set Seconds to 43200.
- B. On HQ-NGFW, enable Diffie-Hellman Group 2.
- C. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0
- D. On HQ-NGFW
- E. set Encryption to AES256

Answer: AC

Explanation:

The key lifetime (Seconds) must match on both sides; BR1-FGT is set to 14400, so setting it to 43200 matches HQ-NGFW.

The remote address on BR1-FGT should match the HQ-NGFW's local subnet (10.0.11.0/24), but it is currently set incorrectly as 172.20.1.0/24. Changing it to 10.0.11.0/255.255.255.0 will align the Phase 2 selectors.

NEW QUESTION 20

Which two statements are correct when FortiGate enters conserve mode? (Choose two.)

- A. FortiGate continues to run critical security actions, such as quarantine.
- B. FortiGate refuses to accept configuration changes.
- C. FortiGate halts complete system operation and requires a reboot to regain available resources.
- D. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.

Answer: BD

Explanation:

In conserve mode, FortiGate restricts configuration changes to preserve system stability.

When IPS fail-open is enabled, FortiGate continues forwarding traffic without IPS inspection during resource constraints (conserve mode).

NEW QUESTION 24

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

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

Answer: ABD

Explanation:

Flow-based antivirus buffers the entire file while simultaneously transmitting data to the client to minimize latency.

Flow-based inspection combines multiple scanning techniques from proxy-based modes for efficient detection. Flow-based inspection provides better performance by processing traffic on the fly without full proxy overhead.

NEW QUESTION 25

.....

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-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FGT_AD-7.6-dumps.html