



Fortinet

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

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

If Internet Service is already selected as Destination in a firewall policy, which other configuration object can be selected for the Destination field of a firewall policy?

- A. IP address
- B. No other object can be added
- C. FQDN address
- D. User or User Group

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.59): "When configuring your firewall policy, you can use Internet Service as the destination in a firewall policy, which contains all the IP addresses, ports, and protocols used by that service. For the same reason, you cannot mix regular address objects with ISDB objects, and you cannot select services on a firewall policy. The ISDB objects already have services information, which is hardcoded." This is true because Internet Service is a special type of destination object that can only be used alone in a firewall policy. Internet Service is a feature that allows FortiGate to identify and filter traffic based on the internet service or application that it belongs to, such as Facebook, YouTube, Skype, etc. Internet Service uses a database of IP addresses and ports that are associated with each internet service or application, and updates it regularly from FortiGuard. When Internet Service is selected as the destination in a firewall policy, FortiGate will match the traffic to the corresponding internet service or application, and apply the appropriate action and security profiles to it. However, Internet Service cannot be combined with any other destination object, such as IP address, FQDN address, user or user group, etc., as this would create a conflict or ambiguity in the firewall policy. Therefore, no other object can be added if Internet Service is already selected as the destination in a firewall policy

NEW QUESTION 2

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager
- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

Answer: B

NEW QUESTION 3

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors. What is the reason for the certificate warning errors?

- A. The matching firewall policy is set to proxy inspection mode.
- B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
- C. The full SSL inspection feature does not have a valid license.
- D. The browser does not trust the certificate used by FortiGate for SSL inspection.

Answer: D

Explanation:

FortiGate Security 7.2 Study Guide (p.235): "If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser."

NEW QUESTION 4

Which statement about the policy ID number of a firewall policy is true?

- A. It is required to modify a firewall policy using the CLI.
- B. It represents the number of objects used in the firewall policy.
- C. It changes when firewall policies are reordered.
- D. It defines the order in which rules are processed.

Answer: A

NEW QUESTION 5

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

- A. Antivirus engine
- B. Intrusion prevention system engine
- C. Flow engine
- D. Detection engine

Answer: B

Explanation:

<http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control>

NEW QUESTION 6

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

- A. The IP version of the sources and destinations in a firewall policy must be different.
- B. The Incoming Interface
- C. Outgoing Interface
- D. Schedule, and Service fields can be shared with both IPv4 and IPv6.
- E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
- F. The IP version of the sources and destinations in a policy must match.
- G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: BDE

NEW QUESTION 7

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

- A. The Services field prevents SNAT and DNAT from being combined in the same policy.
- B. The Services field is used when you need to bundle several VIPs into VIP groups.
- C. The Services field removes the requirement to create multiple VIPs for different services.
- D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

Answer: C

NEW QUESTION 8

Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

- A. diagnose sys top
- B. execute ping
- C. execute traceroute
- D. diagnose sniffer packet any
- E. get system arp

Answer: BCD

NEW QUESTION 9

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

- A. The keyUsage extension must be set to keyCertSign.
- B. The common name on the subject field must use a wildcard name.
- C. The issuer must be a public CA.
- D. The CA extension must be set to TRUE.

Answer: AD

Explanation:

"In order for FortiGate to act in these roles, its CA certificate must have the basic constraints extension set to cA=True and the value of the keyUsage extension set to keyCertSign."

NEW QUESTION 10

What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

- A. FortiGate uses fewer resources.
- B. FortiGate performs a more exhaustive inspection on traffic.
- C. FortiGate adds less latency to traffic.
- D. FortiGate allocates two sessions per connection.

Answer: AC

NEW QUESTION 10

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

Answer: B

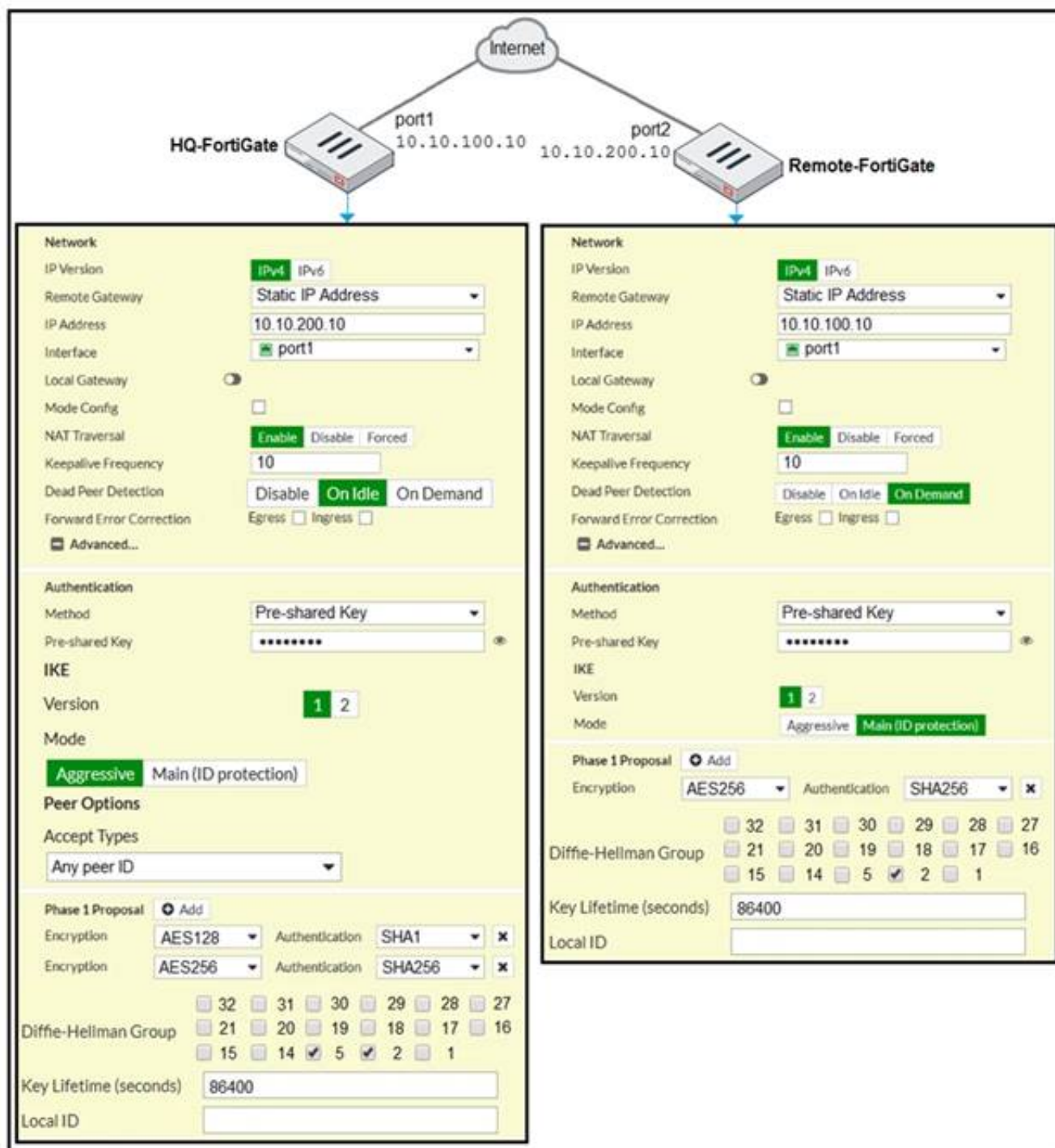
Explanation:

Strict Reverse Path Forwarding (RPF) is a security feature that is used to detect and prevent IP spoofing attacks on a network. It works by checking the routing information for incoming packets to ensure that they are coming from the source address that is indicated in the packet's header. In strict RPF mode, the firewall will check the best route back to the source of the incoming packet using the incoming interface. If the packet's source address does not match the route back to the source, the packet is dropped. This helps to prevent attackers from spoofing their IP address and attempting to access the network.

NEW QUESTION 12

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails 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 will bring phase 1 up? (Choose two.)

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

Answer: AD

Explanation:

"In IKEv1, there are two possible modes in which the IKE SA negotiation can take place: main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel."

NEW QUESTION 14

Which two types of traffic are managed only by the management VDOM? (Choose two.)

- A. FortiGuard web filter queries
- B. PKI
- C. Traffic shaping
- D. DNS

Answer: AD

NEW QUESTION 19

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

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

Answer: BD

Explanation:

* B. Extended authentication (XAuth) to request the remote peer to provide a username and password

This is true because extended authentication (XAuth) is a feature that allows FortiGate to request the remote peer to provide a username and password during the IPsec IKEv1 authentication process. XAuth is an extension of the IKEv1 protocol that adds an additional authentication step after the main mode or aggressive mode exchange. XAuth can be used with either pre-shared key or certificate signature as the primary authentication method, and it can provide stronger security

and granular access control for IPsec VPNs¹²

* D. Pre-shared key and certificate signature as authentication methods

This is true because pre-shared key and certificate signature are two authentication methods that are supported by FortiGate for IPsec IKEv1 VPNs. Pre-shared key is a method where both peers share a secret key that is used to authenticate each other during the IKEv1 exchange. Certificate signature is a method where both peers have digital certificates that are used to verify each other's identity and public key during the IKEv1 exchange. Both methods can be combined with XAuth for additional authentication

NEW QUESTION 21

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

Answer: AC

NEW QUESTION 23

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

Answer: D

Explanation:

FortiGate Security 7.2 Study Guide (p.15): "When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic."

When using FortiGuard servers for DNS, FortiOS defaults to using DNS over TLS (DoT) to secure the DNS traffic¹. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol². This prevents eavesdropping, tampering, and spoofing of DNS data by third parties.

The default FortiGuard DNS servers are 96.45.45.45 and 96.45.46.46, and they use the hostname globalsdns.fortinet.net¹. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration¹.

NEW QUESTION 24

In which two ways can RPF checking be disabled? (Choose two)

- A. Enable anti-replay in firewall policy.
- B. Disable the RPF check at the FortiGate interface level for the source check
- C. Enable asymmetric routing.
- D. Disable strict-arc-check under system settings.

Answer: CD

NEW QUESTION 26

Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

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

Answer: AC

NEW QUESTION 30

Refer to the exhibit.

Outgoing interfaces

☐ **Manual**
Manually assign outgoing interfaces.

☒ **Best Quality**
The interface with the best measured performance is selected.

☐ **Lowest Cost (SLA)**
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

☐ **Maximize Bandwidth (SLA)**
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

port1	X
port2	X
port3	X
port4	X

Measured SLA SLA_1

Quality criteria Latency

Status Enable Disable

```

NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
    
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check . Which interface will be selected as an outgoing interface?

- A. port2
- B. port4
- C. port3
- D. port1

Answer: D

Explanation:

Port 1 shows the lowest latency.

NEW QUESTION 34

Which three statements are true regarding session-based authentication? (Choose three.)

- A. HTTP sessions are treated as a single user.
- B. IP sessions from the same source IP address are treated as a single user.
- C. It can differentiate among multiple clients behind the same source IP address.
- D. It requires more resources.
- E. It is not recommended if multiple users are behind the source NAT

Answer: ACD

NEW QUESTION 38

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.

What is the reason for the failed virus detection by FortiGate?

- A. The website is exempted from SSL inspection.
- B. The EICAR test file exceeds the protocol options oversize limit.
- C. The selected SSL inspection profile has certificate inspection enabled.
- D. The browser does not trust the FortiGate self-signed CA certificate.

Answer: AC

Explanation:

SSL Inspection Profile, on the Inspection method there are 2 options to choose from, SSL Certificate Inspection or Full SSL Inspection. FG SEC 7.2 Studi Guide: Full SSL Inspection level is the only choice that allows antivirus to be effective.

NEW QUESTION 39

Refer to the exhibit.



The screenshot shows the FortiGate SLA configuration page for 'SLA1'. The 'Protocol' is set to 'Ping'. The 'Server' field contains two entries: '4.2.2.2' and '4.2.2.1'. The 'Participants' field is set to 'All SD-WAN Members'. The 'Enable probe packets' checkbox is unchecked. There are also fields for 'port1' and 'port2' under the 'Specify' button.

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic. Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

- A. The Detection Mode setting is not set to Passive.
- B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
- C. The configured participants are not SD-WAN members.
- D. The Enable probe packets setting is not enabled.

Answer: BD

NEW QUESTION 41

Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 44

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

- A. Log ID
- B. Universally Unique Identifier
- C. Policy ID
- D. Sequence ID

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.67): "When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer."

NEW QUESTION 47

Which statement describes a characteristic of automation stitches?

- A. They can have one or more triggers.
- B. They can be run only on devices in the Security Fabric.
- C. They can run multiple actions simultaneously.
- D. They can be created on any device in the fabric.

Answer: C

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/351998/creating-automation-stitches>

NEW QUESTION 51

Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 53

Refer to the exhibit.


```
FGT1 # 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
       > - selected route, * - FIB route, p - stale info

S      *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
      *>          [10/0] via 10.0.0.2, port2, [30/0]
S      0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C      *> 10.0.0.0/24 is directly connected, port2
S      172.13.24.0/24 [10.0] is directly connected, port4
C      *> 172.20.121.0/24 is directly connected, port1
S      *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C      *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

- A. The port3 default route has the lowest metric.
- B. The port1 and port2 default routes are active in the routing table.
- C. The ports default route has the highest distance.
- D. There will be eight routes active in the routing table.

Answer: BC

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-identify-Inactive-Routes-in-the-Routing/ta-p>

NEW QUESTION 58

An administrator must disable RPF check to investigate an issue.

Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

- A. Enable asymmetric routing, so the RPF check will be bypassed.
- B. Disable the RPF check at the FortiGate interface level for the source check.
- C. Disable the RPF check at the FortiGate interface level for the reply check .
- D. Enable asymmetric routing at the interface level.

Answer: B

NEW QUESTION 59

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeou
- B. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
- C. It is a hard timeou
- D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- E. It is an idle timeou
- F. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
- G. It is a hard timeou
- H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Answer: A

NEW QUESTION 62

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

Answer: AC

NEW QUESTION 63

Which of the following statements about central NAT are true? (Choose two.)

- A. IP tool references must be removed from existing firewall policies before enabling central NAT .
- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Answer: AB

NEW QUESTION 68

An administrator needs to increase network bandwidth and provide redundancy.
 What interface type must the administrator select to bind multiple FortiGate interfaces?

- A. VLAN interface
- B. Software Switch interface
- C. Aggregate interface
- D. Redundant interface

Answer: C

Explanation:

An aggregate interface is a logical interface that combines two or more physical interfaces into one virtual interface1. An aggregate interface can increase network bandwidth and provide redundancy by distributing traffic across multiple physical interfaces using a load balancing algorithm1. An aggregate interface can also support link aggregation control protocol (LACP) to negotiate the link aggregation settings with the connected device1.

NEW QUESTION 70

Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.
 Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack .
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

Answer: A

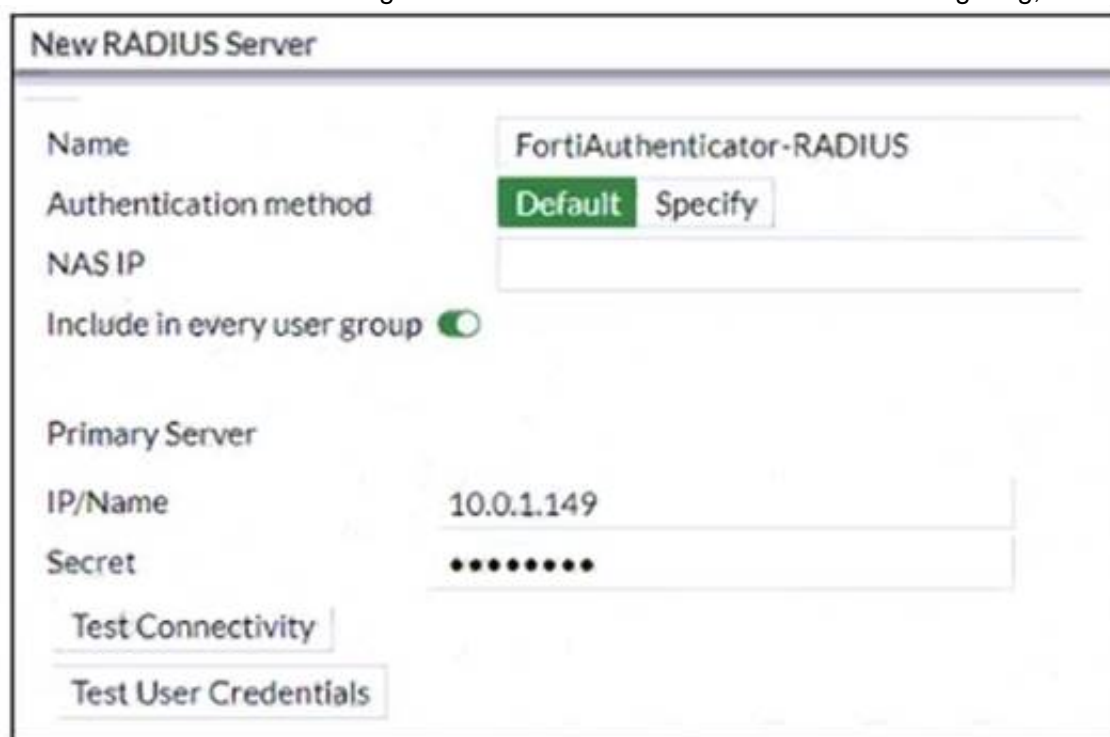
Explanation:

fortinet-fortigate-security-study-guide-for-fortios-72 page 417 If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

NEW QUESTION 71

Refer to the exhibit.

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.



What is the impact of using the Include in every user group option in a RADIUS configuration?

- A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- C. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
- D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Answer: A

NEW QUESTION 76

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

Answer: D

Explanation:

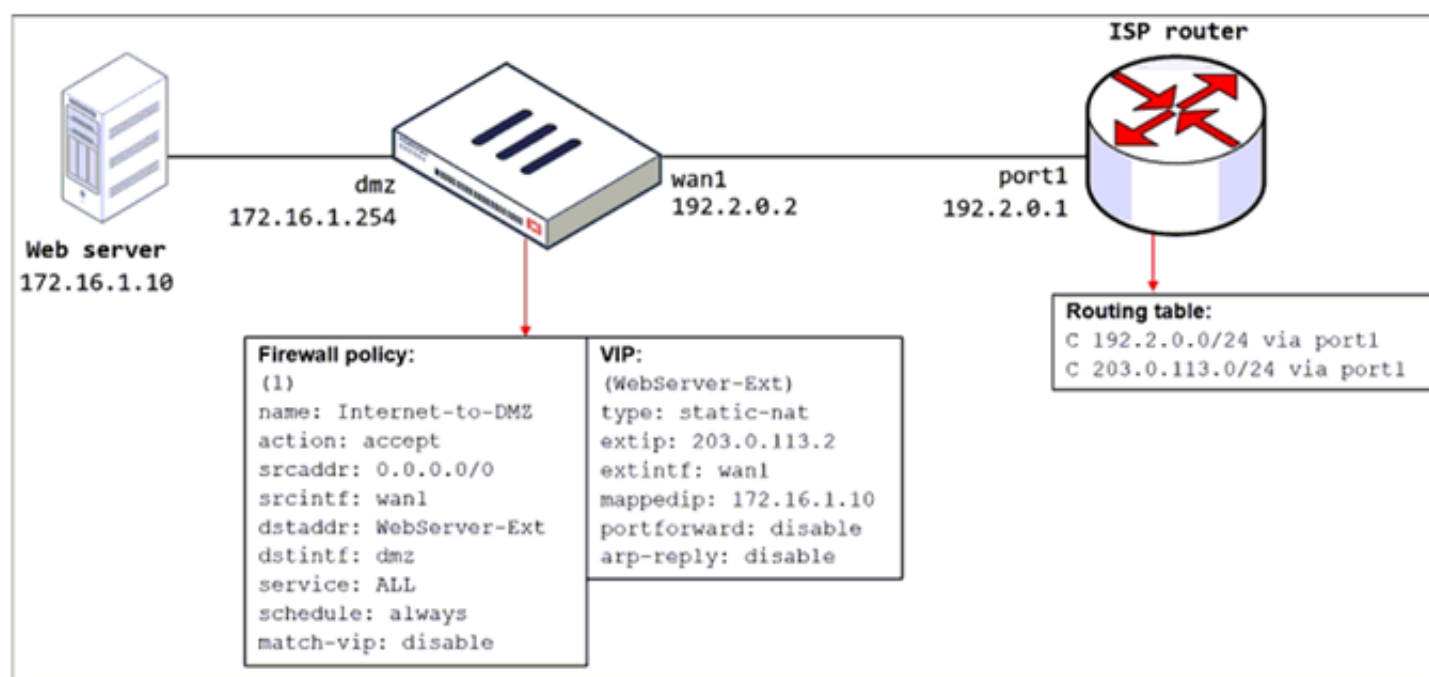
"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

NEW QUESTION 80

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.

When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

- A. Configure a loopback interface with address 203.0.113.2/32.
- B. In the VIP configuration, enable arp-reply.
- C. Enable port forwarding on the server to map the external service port to the internal service port.
- D. In the firewall policy configuration, enable match-vip.

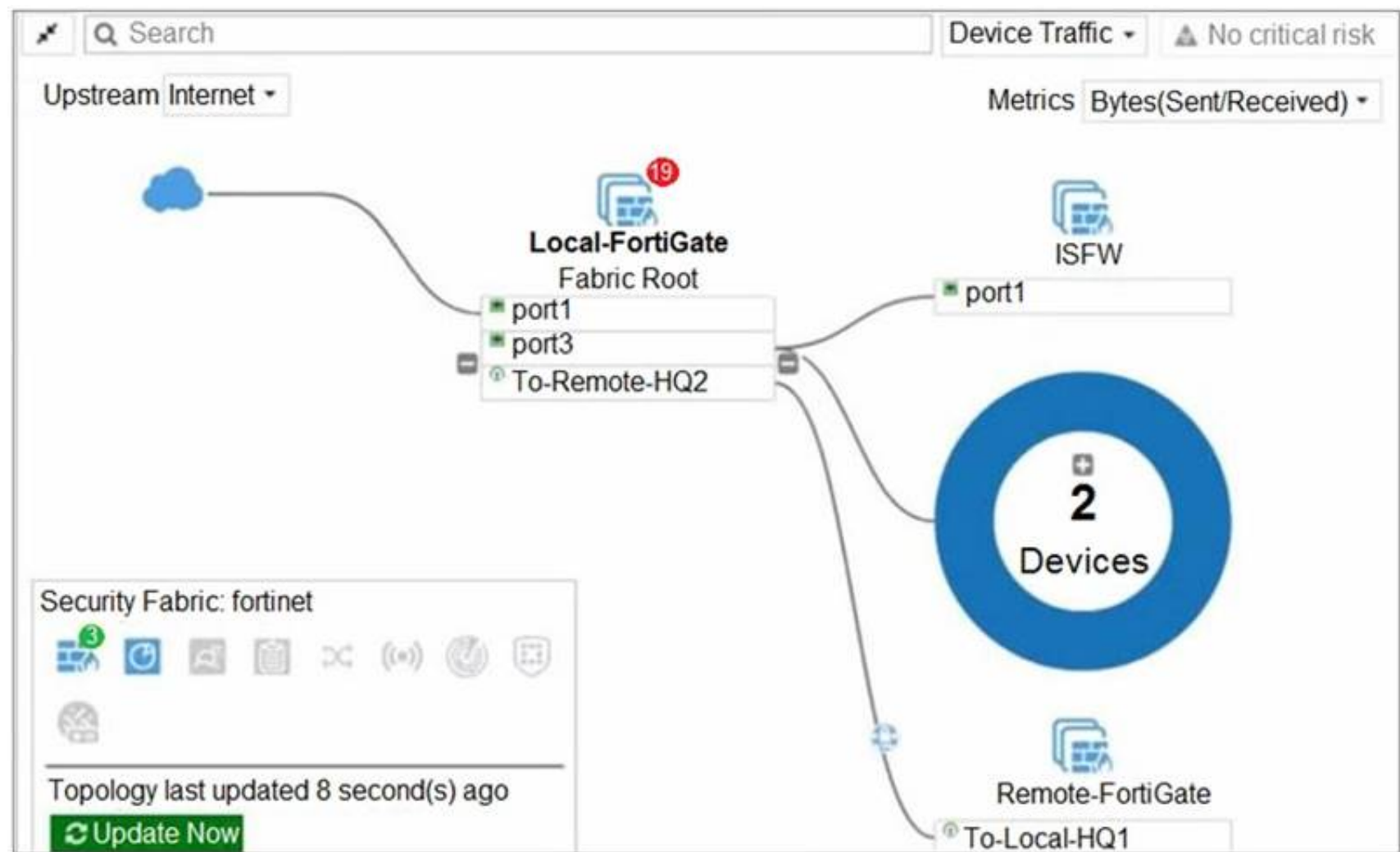
Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.115): "Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled."

NEW QUESTION 82

Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

- A. There are five devices that are part of the security fabric.
- B. Device detection is disabled on all FortiGate devices.
- C. This security fabric topology is a logical topology view.
- D. There are 19 security recommendations for the security fabric.

Answer: CD

Explanation:

References: <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results>
<https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology>

NEW QUESTION 87

Refer to the exhibit.



The image shows the configuration form for a FortiGate Administrator account. The form has the following fields and options:

- Username:** Administrator
- Type:** Local User (selected), Match a user on a remote server group, Match all users in a remote server group, Use public key infrastructure (PKI) group
- Comments:** Write a comment... (0/255 characters)
- Administrator Profile:** prof_admin (selected)
- Email Address:** admin@xyz.com
- Options (all are disabled):**
 - SMS
 - Two-factor Authentication
 - Restrict login to trusted hosts
 - Restrict admin to guest account provisioning only
- Change Password:** (button)

The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

- A. Change password
- B. Enable restrict access to trusted hosts
- C. Change Administrator profile
- D. Enable two-factor authentication

Answer: C

NEW QUESTION 90

Which of statement is true about SSL VPN web mode?

- A. The tunnel is up while the client is connected.
- B. It supports a limited number of protocols.
- C. The external network application sends data through the VPN.
- D. It assigns a virtual IP address to the client.

Answer: B

Explanation:

FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

NEW QUESTION 91

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scope of application control to the browser-based technology category only.
- B. It limits the scope of application control to scan application traffic based on application category only.
- C. It limits the scope of application control to scan application traffic using parent signatures only
- D. It limits the scope of application control to scan application traffic on DNS protocol only.

Answer: B

NEW QUESTION 95

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A. A CRL
- B. A person
- C. A subordinate CA
- D. A root CA

Answer: D

NEW QUESTION 99

Which statement about video filtering on FortiGate is true?

- A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.
- B. It does not require a separate FortiGuard license.
- C. Full SSL inspection is not required.
- D. its available only on a proxy-based firewall policy.

Answer: D

Explanation:

FortiGate Security 7.2 Study Guide (p.279): "To apply the video filter profile, proxy-based firewall policies currently allow you to enable the video filter profile. You must enable full SSL inspection on the firewall policy."

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/860867/filtering-based-on-fortiguard-cat>

NEW QUESTION 103

Which statement correctly describes the use of reliable logging on FortiGate?

- A. Reliable logging is enabled by default in all configuration scenarios.
- B. Reliable logging is required to encrypt the transmission of logs.
- C. Reliable logging can be configured only using the CLI.
- D. Reliable logging prevents the loss of logs when the local disk is full.

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.192): "if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm setting on the CLI."

NEW QUESTION 105

.....

Relate Links

100% Pass Your NSE4_FGT-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-7.2-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/>