



Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

About ExamBible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Source defined as Internet Services in the firewall policy.
- B. Destination defined as Internet Services in the firewall policy.
- C. Highest to lowest priority defined in the firewall policy.
- D. Services defined in the firewall policy.
- E. Lowest to highest policy ID number.

Answer: ABD

Explanation:

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

- Incoming Interface
- Outgoing Interface
- Source: IP address, user, internet services
- Destination: IP address or internet services
- Service: IP protocol and port number
- Schedule: Applies during configured times

NEW QUESTION 2

Refer to the exhibits.

Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.

Exhibit A **Exhibit B**

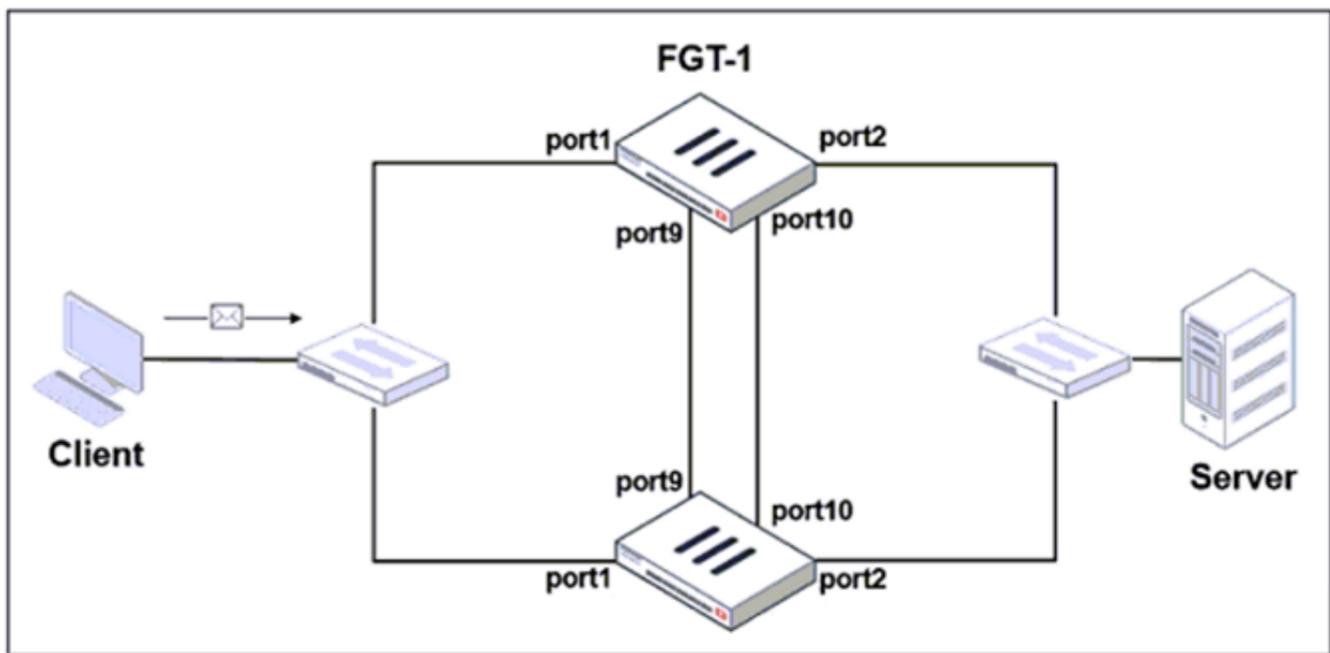


Exhibit A **Exhibit B**

```

set group-id 3
set group-name "NSE"
set mode a-a
set password *
set hbdev "port9" 50 "port10" 50
set session-pickup enable
set override disable
set monitor port3
end

# get system ha status
...
Primary      : FGT-2, FGVM010000065036, HA cluster index = 1
Secondary    : FGT-1, FGVM010000064692, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000065036, HA operating index = 1
Secondary: FGVM010000064692, HA operating index = 0
    
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

- A. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.
- B. The traffic sourced from the client and destined to the server is sent to FGT-1.
- C. The cluster can load balance ICMP connections to the secondary.
- D. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

Answer: AD

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.317 & p.320): "To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses." "The primary forwards the SYN packet to the selected secondary. (...) This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic."

NEW QUESTION 3

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 4

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 5

An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192. 168. 1.0/24 and the remote quick mode selector is 192. 168.2.0/24.

Which subnet must the administrator configure for the local quick mode selector for site B?

- A. 192. 168. 1.0/24
- B. 192. 168.0.0/24
- C. 192. 168.2.0/24
- D. 192. 168.3.0/24

Answer: C

Explanation:

For an IPsec VPN between site A and site B, the administrator has configured the local quick mode selector for site A as 192.168.1.0/24 and the remote quick mode selector as 192.168.2.0/24. This means that the VPN will allow traffic to and from the 192.168.1.0/24 subnet at site A to reach the 192.168.2.0/24 subnet at site B.

To complete the configuration, the administrator must configure the local quick mode selector for site B. To do this, the administrator must use the same subnet as the remote quick mode selector for site A, which is 192.168.2.0/24. This will allow traffic to and from the 192.168.2.0/24 subnet at site B to reach the 192.168.1.0/24 subnet at site A.

Therefore, the administrator must configure the local quick mode selector for site B as 192.168.2.0/24.

NEW QUESTION 6

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 7

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 8

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

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

Answer: AC

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.41): "The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table." "FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session."

* A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks¹

* C. The RPF check is run on the first sent packet of any new session.

This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the session initiation. This reduces the processing overhead and improves performance²

NEW QUESTION 9

What are two functions of the ZTNA rule? (Choose two.)

- A. It redirects the client request to the access proxy.
- B. It applies security profiles to protect traffic.
- C. It defines the access proxy.
- D. It enforces access control.

Answer: BD

Explanation:

A ZTNA rule is a policy that enforces access control and applies security profiles to protect traffic between the client and the access proxy¹. A ZTNA rule defines the following parameters¹:

- > Incoming interface: The interface that receives the client request.
- > Source: The address and user group of the client.
- > ZTNA tag: The tag that identifies the domain that the client belongs to.
- > ZTNA server: The server that hosts the access proxy.
- > Destination: The address of the application that the client wants to access.
- > Action: The action to take for the traffic that matches the rule. It can be accept, deny, or redirect.
- > Security profiles: The security features to apply to the traffic, such as antivirus, web filter, application control, and so on.

A ZTNA rule does not redirect the client request to the access proxy. That is the function of a policy route that matches the ZTNA tag and sends the traffic to the ZTNA server².

A ZTNA rule does not define the access proxy. That is done by creating a ZTNA server object that specifies the IP address, port, and certificate of the access proxy³.

FortiGate Infrastructure 7.2 Study Guide (p.177): "A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic."

NEW QUESTION 10

Refer to the exhibit.

```
STUDENT # get system session list
```

PROTO	EXPIRE	SOURCE	SOURCE-NAT	DESTINATION	DESTINATION-NAT
tcp	3598	10.0.1.10:2706	10.200.1.6:2706	10.200.1.254:80	-
tcp	3598	10.0.1.10:2704	10.200.1.6:2704	10.200.1.254:80	-
tcp	3596	10.0.1.10:2702	10.200.1.6:2702	10.200.1.254:80	-
tcp	3599	10.0.1.10:2700	10.200.1.6:2700	10.200.1.254:443	-
tcp	3599	10.0.1.10:2698	10.200.1.6:2698	10.200.1.254:80	-
tcp	3598	10.0.1.10:2696	10.200.1.6:2696	10.200.1.254:443	-
udp	174	10.0.1.10:2694	-	10.0.1.254:53	-
udp	173	10.0.1.10:2690	-	10.0.1.254:53	-

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

- A. Destination NAT is disabled in the firewall policy.
- B. One-to-one NAT IP pool is used in the firewall policy.
- C. Overload NAT IP pool is used in the firewall policy.
- D. Port block allocation IP pool is used in the firewall policy.

Answer: B

Explanation:

FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

NEW QUESTION 10

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 14

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 collector agent must search security event logs.
- D. The NetSession Enum function is used to track user logouts.

Answer: D

Explanation:

FortiGate_Infrastructure_7.0 page 270: "NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows."

NEW QUESTION 17

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. SSH
- B. HTTPS
- C. FTM
- D. FortiTelemetry

Answer: AB

NEW QUESTION 21

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

- A. By default, FortiGate uses WINS servers to resolve names.
- B. By default, the SSL VPN portal requires the installation of a client's certificate.
- C. By default, split tunneling is enabled.
- D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 23

Examine this PAC file configuration.

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

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 26

Refer to the exhibit.



Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToRemote

Comments: [Text Field]

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal: Add

Encryption: AES128 Authentication: SHA1

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group:

 32 31 30 29 28 27

 21 20 19 18 17 16

 15 14 5 2 1

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds

Seconds: 43200

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToRemote

Comments: [Text Field]

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal: Add

Encryption: AES256 Authentication: SHA1

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group:

 32 31 30 29 28 27

 21 20 19 18 17 16

 15 14 5 2 1

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds

Seconds: 14400

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, what configuration change will bring phase 2 up?

- A. On HQ-FortiGate, enable Auto-negotiate.
- B. On Remote-FortiGate, set Seconds to 43200.
- C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
- D. On HQ-FortiGate, set Encryption to AES256.

Answer: D

NEW QUESTION 30

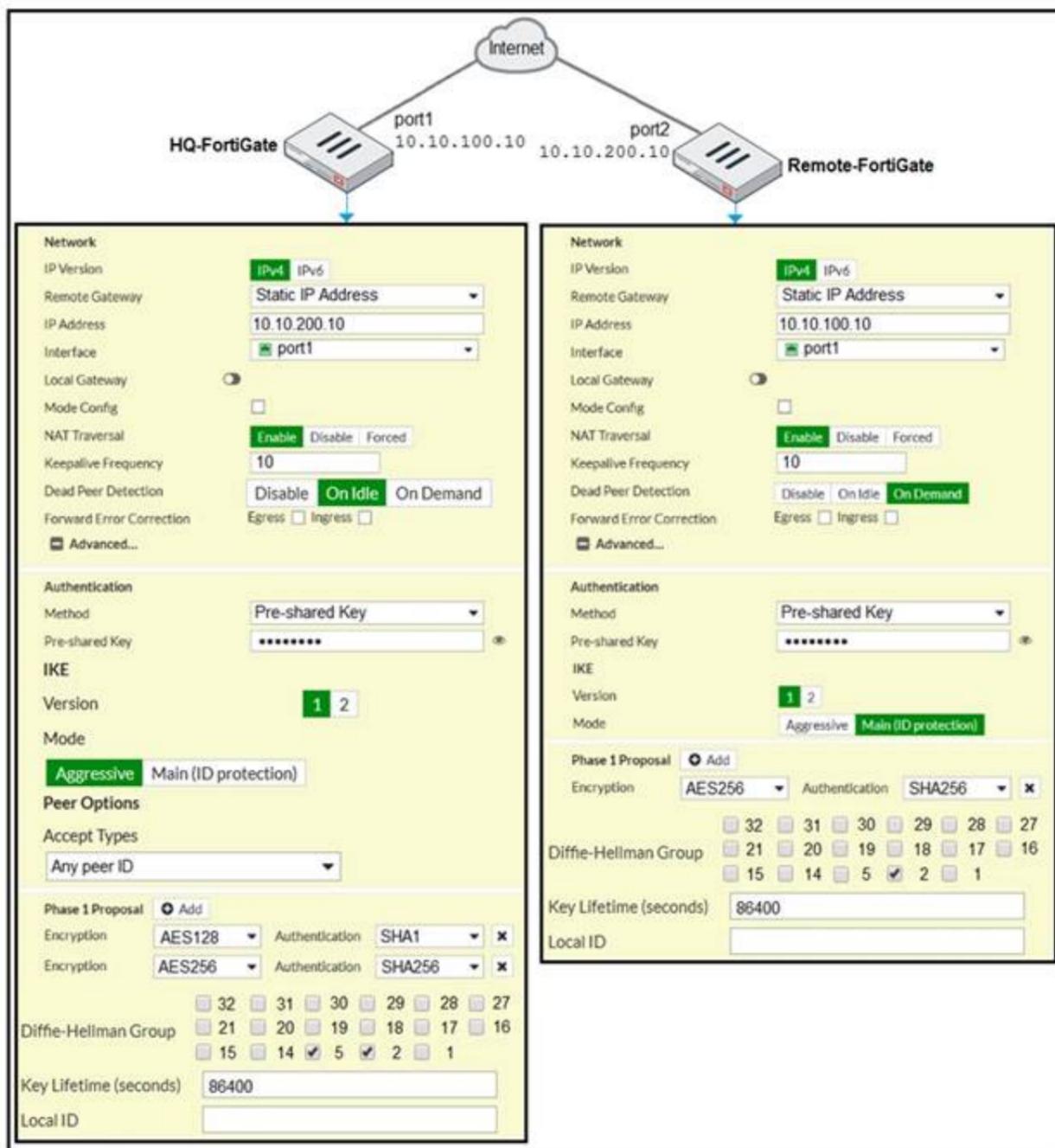
An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

- A. Add the support of NTLM authentication.
- B. Add user accounts to Active Directory (AD).
- C. Add user accounts to the FortiGate group filter.
- D. Add user accounts to the Ignore User List.

Answer: D

NEW QUESTION 34

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-Helman 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 38

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate points the collector agent to use a remote LDAP server.
- B. FortiGate uses the AD server as the collector agent.
- C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- D. FortiGate queries AD by using the LDAP to retrieve user group information.

Answer: CD

Explanation:

Fortigate Infrastructure 7.0 Study Guide P.272-273 <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

NEW QUESTION 40

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 42

Refer to the exhibits.

Exhibit A Exhibit B

```
# 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
```

Exhibit A Exhibit B

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

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

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

Answer: BD

NEW QUESTION 43

The IPS engine is used by which three security features? (Choose three.)

- A. Antivirus in flow-based inspection
- B. Web filter in flow-based inspection
- C. Application control
- D. DNS filter
- E. Web application firewall

Answer: ABC

Explanation:

FortiGate Security 7.2 Study Guide (p.385): "The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It's also responsible for application control, flow-based antivirus protection, web filtering, and email filtering."

NEW QUESTION 48

Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

- A. VDOMs without ports with connected devices are not displayed in the topology.
- B. Downstream devices can connect to the upstream device from any of their VDOMs.
- C. Security rating reports can be run individually for each configured VDOM.
- D. Each VDOM in the environment can be part of a different Security Fabric.

Answer: A

Explanation:

FortiGate Security 7.2 Study Guide (p.436): "When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric."

NEW QUESTION 52

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporarily disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 57

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Answer: AC

NEW QUESTION 59

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

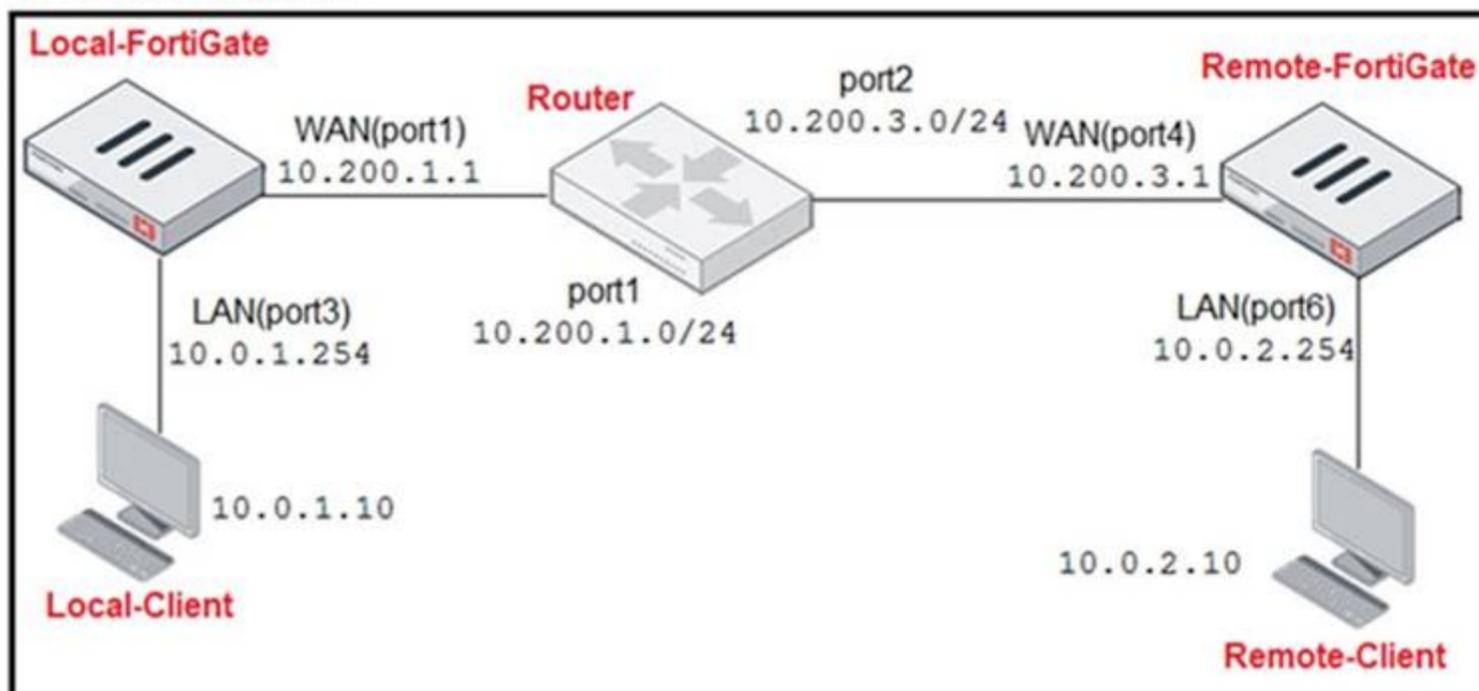
Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.73): "What about traffic originating from FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate. Traffic coming from FortiGate to those global services originates from the management VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM. It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate."

NEW QUESTION 63

Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

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

Protocol Number Table

Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. 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.

A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.

Which IP address will be used to source NAT 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. 149
- B. 10.200. 1. 1
- C. 10.200. 1.49
- D. 10.200. 1.99

Answer: D

NEW QUESTION 67

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 71

Refer to the exhibits.

Exhibit A shows the application sensor configuration. Exhibit B shows the Excessive-Bandwidth and Apple filter details.

Exhibit A Exhibit B

Edit Application Sensor

Categories

- All Categories
- Business (179, 6)
- Collaboration (293, 6)
- Game (124)
- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, 16)
- Video/Audio (206, 13)
- Web.Client (18)
- Cloud.IT (31)
- Email (87, 12)
- General.Interest (241, 9)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, 31)
- Update (48)
- VoIP (31)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

[+ Create New](#) [Edit](#) [Delete](#)

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	Block
2	VEND Apple	Filter	Monitor

Exhibit A Exhibit B

Edit Override

Type: Application **Filter**

Action: Block

Filter: **BHVR** Excessive-Bandwidth

FaceTime

Name	Category	Technology
Application Signature	1/1262	
FaceTime	VoIP	Client-Server

Edit Override

Type: Application **Filter**

Action: Monitor

Filter: **VEND** Apple

FaceTime

Name	Category	Technology
Application Signature	1/33	
FaceTime	VoIP	Client-Server

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

- A. Apple FaceTime will be allowed, based on the Categories configuration.
- B. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.
- C. Apple FaceTime will be allowed, based on the Apple filter configuration.
- D. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.310): "Then, FortiGate scans packets for matches, in this order, for the application control profile: 1. Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies. 2. Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories."

NEW QUESTION 72

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check .

Answer: D

NEW QUESTION 76

Refer to the exhibit.



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 79

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 80

Refer to the web filter raw logs.

```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web" action="blocked"
reqtype="direct" url="https://twitter.com/" sentbyte=517
rcvdbyte=0 direction="outgoing" msg="URL belongs to a category
with warnings enabled" method="domain" cat=37 catdesc="Social
Networking"

date=2020-07-09 time=12:52:16 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313537024536428 tz="-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web"
action="passthrough" reqtype="direct" url="https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction="outgoing" msg="URL belongs to
a category with warnings enabled" method="domain" cat=37
catdesc="Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

- A. Social networking web filter category is configured with the action set to authenticate.
- B. The action on firewall policy ID 1 is set to warning.
- C. Access to the social networking web filter category was explicitly blocked to all users.
- D. The name of the firewall policy is all_users_web.

Answer: A

NEW QUESTION 81

Which timeout setting can be responsible for deleting SSL VPN associated sessions?

- A. SSL VPN idle-timeout
- B. SSL VPN http-request-body-timeout
- C. SSL VPN login-timeout
- D. SSL VPN dtls-hello-timeout

Answer: A

NEW QUESTION 84

An administrator configures outgoing interface any in a firewall policy. What is the result of the policy list view?

- A. Search option is disabled.
- B. Policy lookup is disabled.
- C. By Sequence view is disabled.
- D. Interface Pair view is disabled.

Answer: D

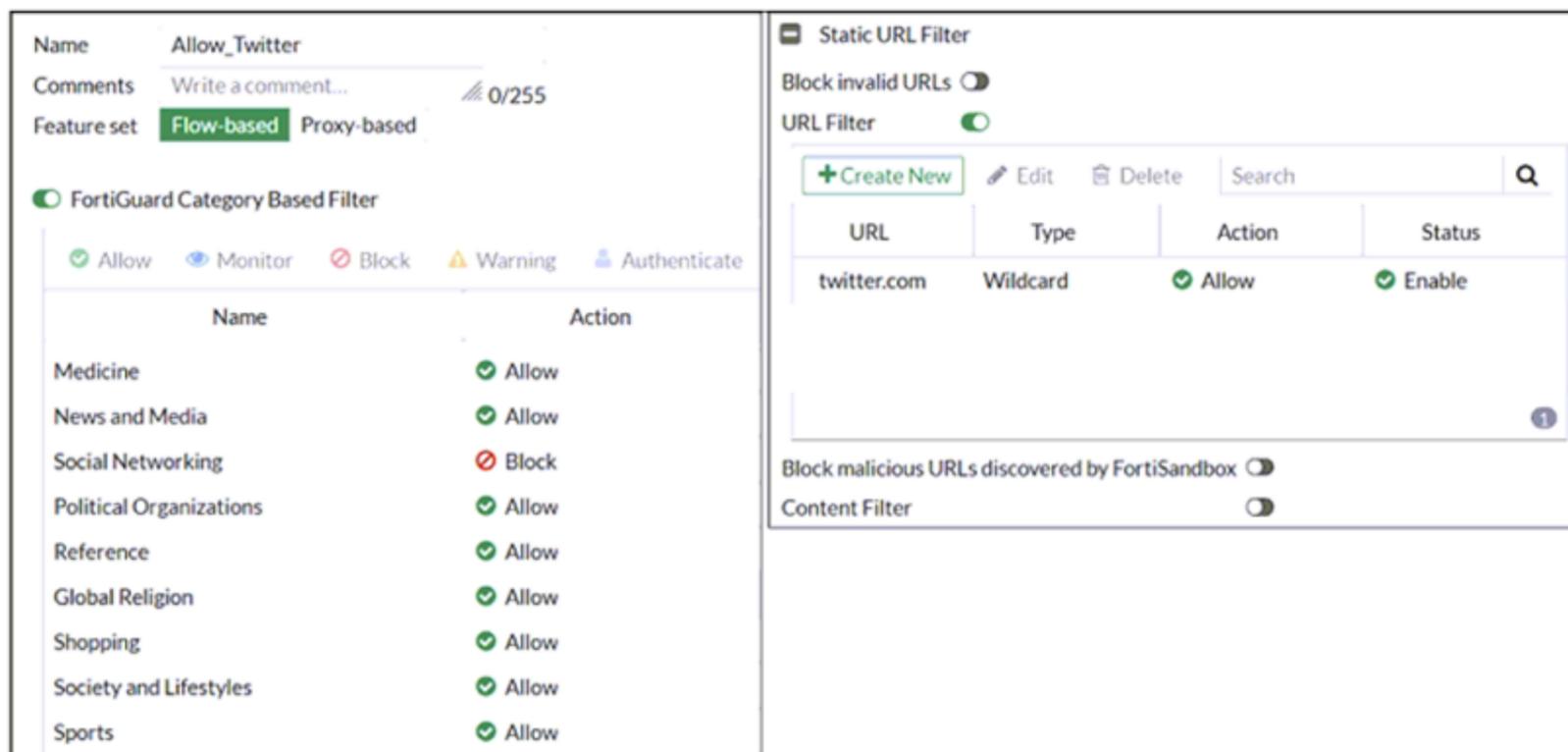
Explanation:

"If you use multiple source or destination interfaces, or the any interface in a firewall policy, you cannot separate policies into sections by interface pairs—some would be triplets or more. So instead, policies are then always displayed in a single list (By Sequence)."

NEW QUESTION 89

Refer to exhibit.

An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.



Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

- A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking
- B. On the Static URL Filter configuration, set Type to Simple
- C. On the Static URL Filter configuration, set Action to Exempt.
- D. On the Static URL Filter configuration, set Action to Monitor.

Answer: C

NEW QUESTION 93

Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

- A. The next-hop IP address is unreachable.
- B. It failed the RPF check .
- C. It matched an explicitly configured firewall policy with the action DENY.
- D. It matched the default implicit firewall policy.

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=13900> <https://www.fortinetguru.com/2016/03/what-is-policy-id-0-and-why-lot-of-denied-traffic-on-this-policy/>

NEW QUESTION 94

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 98

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 are needed on FortiGate to meet the design requirements? (Choose two,)

- A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
- B. Enable Dead Peer Detection.
- 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. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Answer: BC

Explanation:

Study Guide – IPsec VPN – IPsec configuration – Phase 1 Network.

When Dead Peer Detection (DPD) is enabled, DPD probes are sent to detect a failed tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same destination, and you want to failover to a backup connection when the primary connection fails to keep the connectivity between the sites up.

There are three DPD modes. On demand is the default mode. Study Guide – IPsec VPN – Redundant VPNs.

Add one phase 1 configuration for each tunnel. DPD should be enabled on both ends. Add at least one phase 2 definition for each phase 1.

Add one static route for each path. Use distance or priority to select primary routes over backup routes (routes for the primary VPN must have a lower distance or lower priority than the backup). Alternatively, use dynamic routing.

Configure FW policies for each IPsec interface.

NEW QUESTION 100

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 104

View the exhibit.

Destination: Subnet Named Address Internet Service 172.13.24.0/255.255.255.0 Interface: TunnelB Administrative Distance: 5 Status: Enabled Disabled Priority: 30	Destination: Subnet Named Address Internet Service 172.13.24.0/255.255.255.0 Interface: TunnelA Administrative Distance: 10 Status: Enabled Disabled Priority: 0
---	---

Which of the following statements are correct? (Choose two.)

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote sit
- D. The TunnelA route is used only if the TunnelB VPN is down.
- E. This is a redundant IPsec setup.

Answer: CD

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundan>

NEW QUESTION 107

Which two statements are true about the RPF check? (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. RPF is a mechanism that protects FortiGate and your network from IP spoofing attacks.

Answer: AD

NEW QUESTION 110

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not Which configuration option is the most effective way to support this request?

- A. Implement a web filter category override for the specified website
- B. Implement a DNS filter for the specified website.
- C. Implement web filter quotas for the specified website
- D. Implement web filter authentication for the specified website.

Answer: D

NEW QUESTION 113

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 114

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 115

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

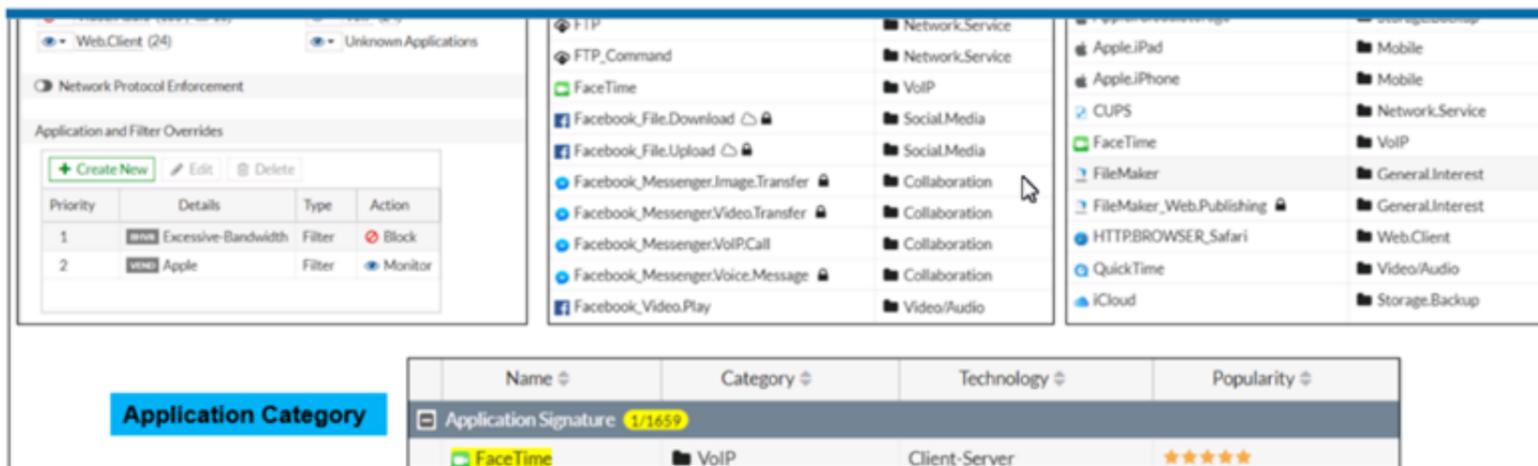
Answer: C

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 116

Refer to the exhibit to view the application control profile.



Based on the configuration, what will happen to Apple FaceTime?

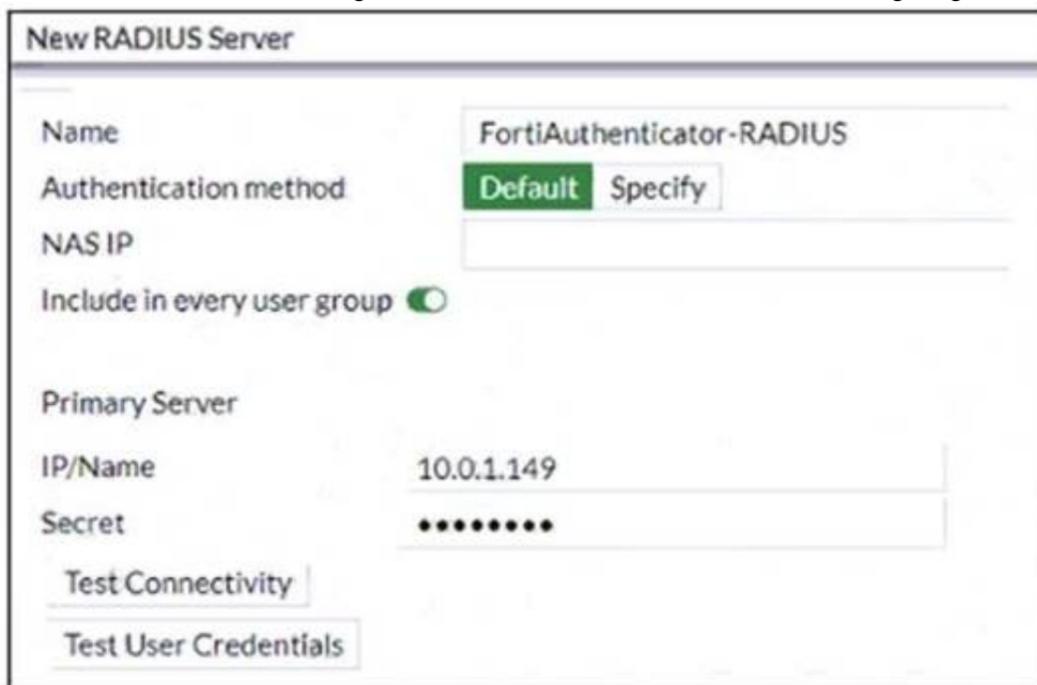
- A. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration
- B. Apple FaceTime will be allowed, based on the Apple filter configuration.
- C. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn
- D. Apple FaceTime will be allowed, based on the Categories configuration.

Answer: A

NEW QUESTION 118

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 122

An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value.

Which timeout option should be configured on FortiGate?

- A. auth-on-demand
- B. soft-timeout
- C. idle-timeout
- D. new-session
- E. hard-timeout

Answer: E

Explanation:

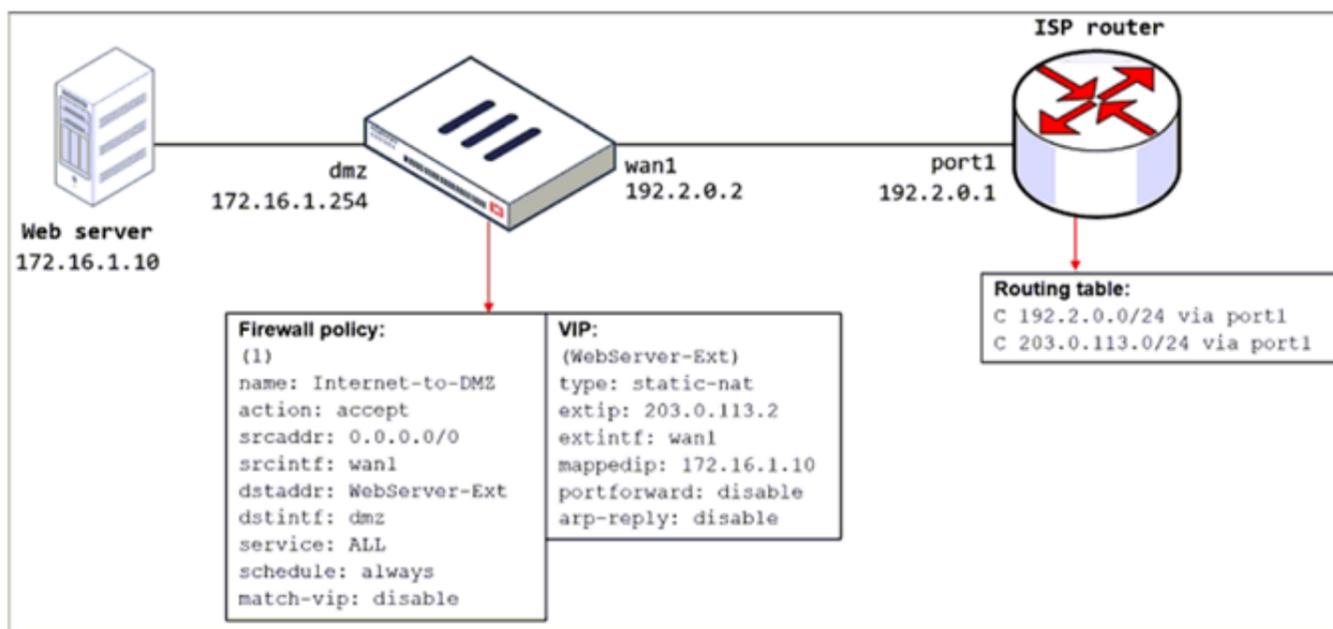
<https://community.fortinet.com/t5/FortiGate/Technical-TipExplanation:-of-auth-timeout-types-for-Firewall/ta-p/>

NEW QUESTION 125

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 128

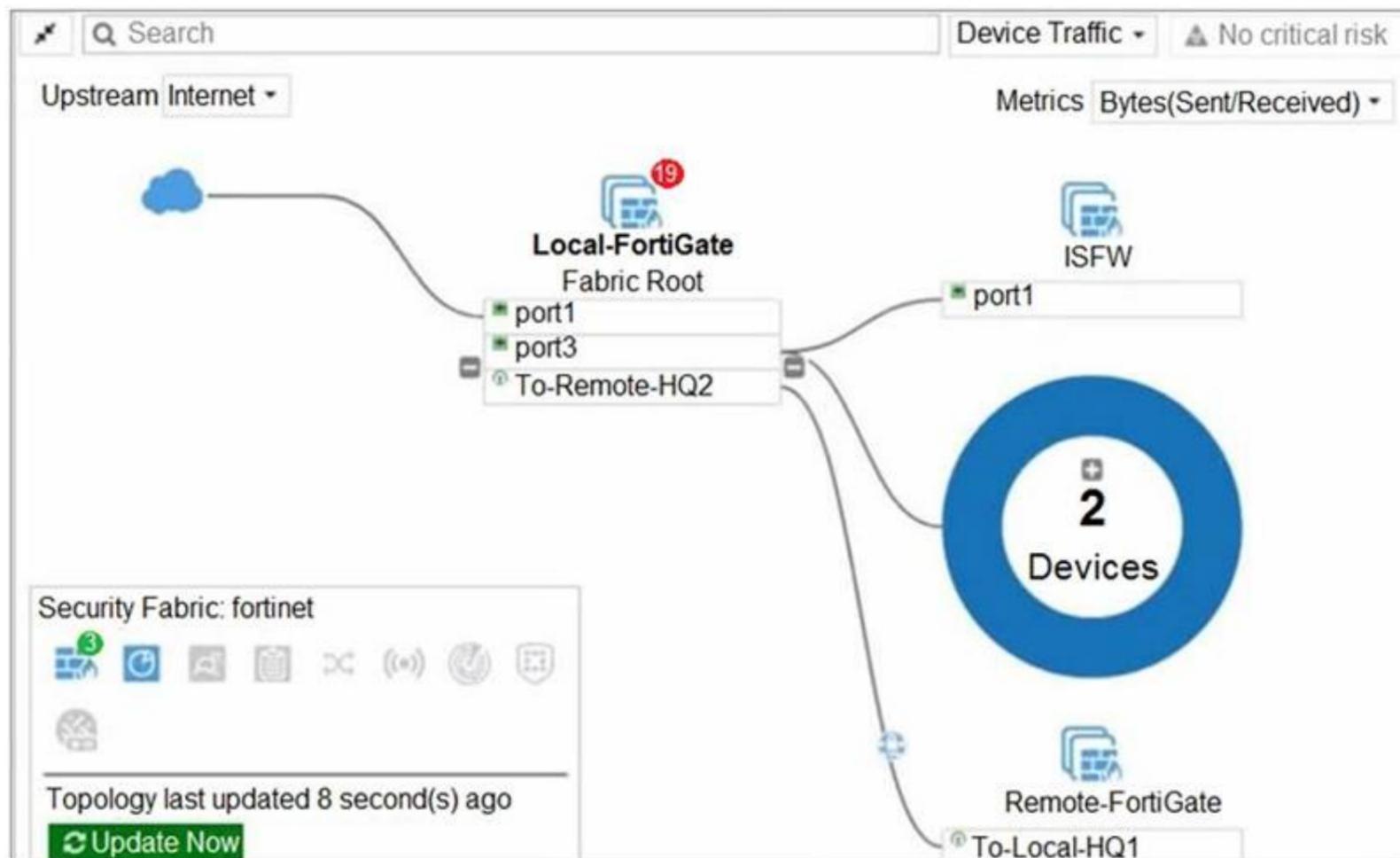
Which two statements are correct about NGFW Policy-based mode? (Choose two.)

- A. NGFW policy-based mode does not require the use of central source NAT policy
- B. NGFW policy-based mode can only be applied globally and not on individual VDOMs
- C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
- D. NGFW policy-based mode policies support only flow inspection

Answer: CD

NEW QUESTION 132

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 137

Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

- A. Subject Key Identifier value
- B. SMMIE Capabilities value
- C. Subject value
- D. Subject Alternative Name value

Answer: A

NEW QUESTION 142

Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.

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.

The administrator disabled the WebServer firewall policy.

Exhibit A Exhibit B

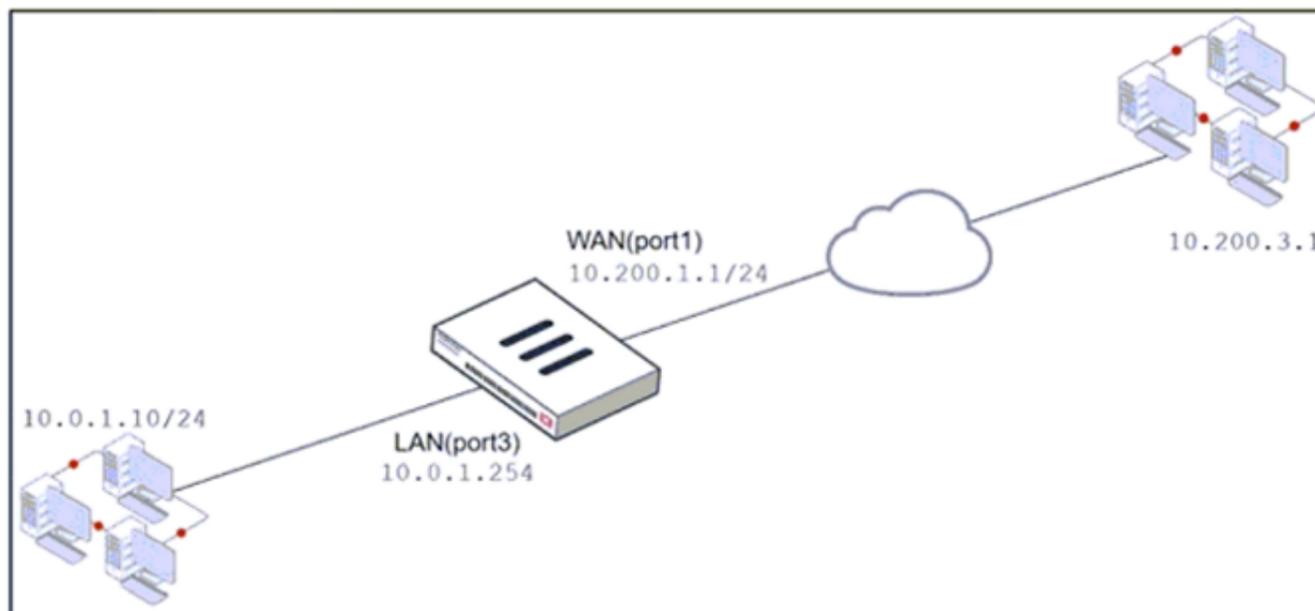


Exhibit A Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	ACCEPT	Enabled
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Disabled

Edit Virtual IP	
VIP type	IPv4
Name	VIP
Comments	Write a comment... 0/255
Color	Change
Network	
Interface	WAN (port1)
Type	Static NAT
External IP address/range	10.200.1.10
Map to	
IPv4 address/range	10.0.1.10
<input type="checkbox"/> Optional Filters	
<input type="checkbox"/> Port Forwarding	

Which IP address will be used to source NAT the traffic, if a user with address 10.0.1.10 connects over SSH to the host with address 10.200.3.1?

- A. 10.200.1.10
- B. 10.0.1.254
- C. 10.200.1.1
- D. 10.200.3.1

Answer: C

Explanation:

Traffic is coming from LAN to WAN, matches policy Full_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

NEW QUESTION 147

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 150

Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

- A. hard-timeout
- B. auth-on-demand
- C. soft-timeout
- D. new-session

E. Idle-timeout

Answer: ADE

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221>

NEW QUESTION 155

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

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

Answer: BDE

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.127-128): "As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended: (WMI, WinSecLog, and NetAPI)"

NEW QUESTION 156

.....

Relate Links

100% Pass Your NSE4_FGT-7.0 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-7.0-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/>