



## **Fortinet**

### **Exam Questions NSE4\_FGT-7.2**

Fortinet NSE 4 - FortiOS 7.2

**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**

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 3**

Refer to the exhibit.

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 configuration change will bring phase 2 up?

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

**Answer:** B

#### NEW QUESTION 4

What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

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

Answer: D

#### NEW QUESTION 5

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-Filter
Status      : Enable
License     : Contract

Num. of servers : 3
Protocol    : https
Port        : 443
Anycast     : Disable
Default servers : Included
-- Server List (Mon Jul 5 12:00:25 2021) --

IP           Weight  RTT  Flags  TZ  FortiGuard-requests  Curr  Lost  Total  Lost  Updated Time
173.243.138.210  10    350  DI    -8   29      0    0      0      0    Mon Jul 5 09:23:33 2021
12.34.97.18     20    30   -5    -5   25      0    0      0      0    Mon Jul 5 09:23:33 2021
210.7.96.18     160   605   9     9   25      0    0      0      0    Mon Jul 5 09:23:33 2021
```

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

- A. A local FortiManager is one of the servers FortiGate communicates with.
- B. One server was contacted to retrieve the contract information.
- C. There is at least one server that lost packets consecutively.
- D. FortiGate is using default FortiGuard communication settings.

Answer: BD

#### Explanation:

FortiGate Security 7.2 Study Guide (p.287-288): "Flags: D (IP returned from DNS), I (Contract server contacted), T (being timed), F (failed)" "By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. Other ports and protocols are available by disabling the FortiGuard anycast setting on the CLI."

#### NEW QUESTION 6

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 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**

Refer to the exhibit.



Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.

**Answer:** D

**Explanation:**

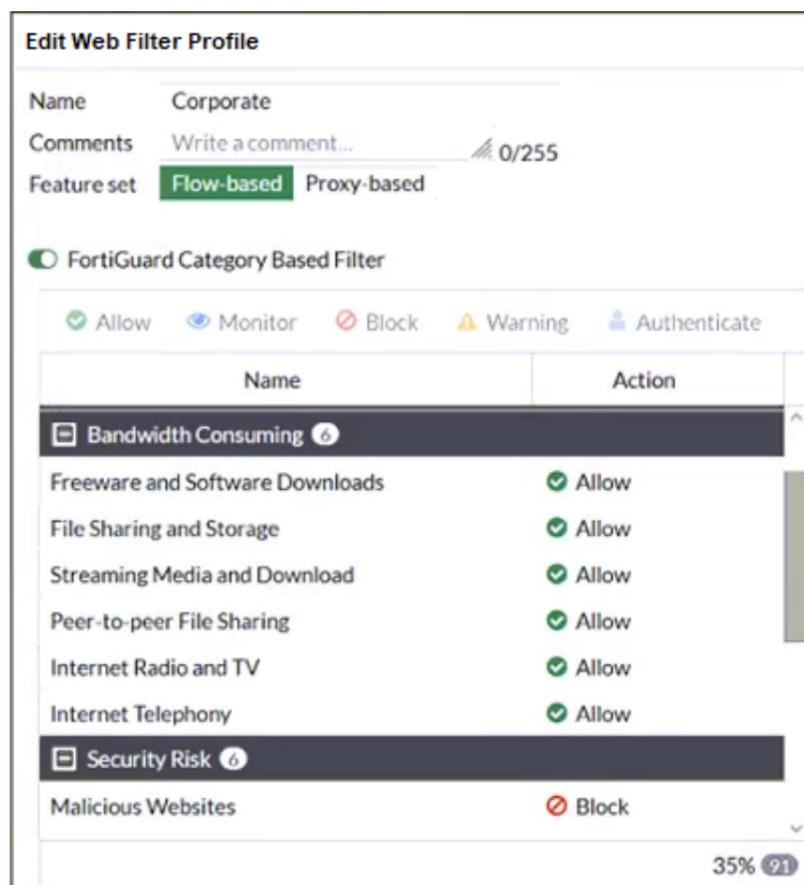
Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be 'Pass' for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be 'Default'. Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

**NEW QUESTION 10**

Refer to the exhibit.

The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.

An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.



What are two solutions for satisfying the requirement? (Choose two.)

- A. Configure a separate firewall policy with action Deny and an FQDN address object for \*.download.com as destination address.
- B. Configure a web override rating for download.com and select Malicious Websites as the subcategory.
- C. Set the Freeware and Software Downloads category Action to Warning.
- D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

**Answer:** BD

**Explanation:**

FortiGate Security 7.2 Study Guide (p.268-269): "If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. You can block a website that belongs to an allowed category." "Static URL filtering is another web filter feature. Configured URLs in the URL filter are checked against the visited websites. If a match is found, the configured action is taken. URL filtering has the same patterns as static domain filtering: simple, regular expressions, and wildcard."

\* B. Configure a web override rating for download.com and select Malicious Websites as the subcategory. This is true because a web override rating is a feature that allows the administrator to change the FortiGuard category of a specific website or domain, and apply a different action to it based on the web filter profile. By configuring a web override rating for download.com and selecting Malicious Websites as the subcategory, the administrator can block access to download.com, which belongs to the Freeware and Software Downloads category by default, without affecting other websites in the same category. The Malicious Websites category has the action Block in the web filter profile shown in the exhibit.

\* D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively. This is true because a static URL filter entry is a feature that allows the administrator to define custom rules for filtering specific URLs or domains, and apply an action to them based on the web filter profile. By configuring a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively, the administrator can block access to download.com and any subdomains or paths under it, without affecting other websites in the Freeware and Software Downloads category. The static URL filter entries have higher priority than the FortiGuard category based filter entries in the web filter profile.

**NEW QUESTION 10**

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 proxy<sup>1</sup>. A ZTNA rule defines the following parameters<sup>1</sup>:

- > 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 server<sup>2</sup>.

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 proxy<sup>3</sup>.

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 13

An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.12" 5
```

Which three pieces of Information will be Included in me sniffer output? {Choose three.}

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

**Answer:** ABD

### NEW QUESTION 17

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 19

An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

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

**Answer:** D

#### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821>

### NEW QUESTION 20

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuard update servers
- C. Operating mode
- D. NGFW mode

**Answer:** CD

#### Explanation:

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate\_Infrastructure\_6.4\_Study\_Guide

### NEW QUESTION 23

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

- A. IP address
- B. Once Internet Service is selected, no other object can be added
- C. User or User Group
- D. FQDN address

**Answer:** B

### NEW QUESTION 26

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 31

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 34**

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 38**

Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

- A. Shut down/reboot a downstream FortiGate device.
- B. Disable FortiAnalyzer logging for a downstream FortiGate device.
- C. Log in to a downstream FortiSwitch device.
- D. Ban or unban compromised hosts.

**Answer:** AB

**NEW QUESTION 40**

Refer to the exhibit.



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 44**

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 49**

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 53**

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

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

Answer: ADE

**NEW QUESTION 57**

Refer to the exhibits.

**SSL-VPN Settings**

**Connection Settings**

Listen on Interface(s): port1

Listen on Port: 10443

Web mode access will be listening at <https://10.200.1.1:10443>

Redirect HTTP to SSL-VPN:

Restrict Access:  Allow access from any host  Limit access to specific hosts

Idle Logout:

Inactive For: 300 Seconds

Server Certificate: Fortinet\_Factory

Require Client Certificate:

**Tunnel Mode Client Settings**

Address Range:  Automatically assign addresses  Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server:  Same as client system DNS  Specify

Specify WINS Servers:

**Authentication/Portal Mapping**

Users/Groups	Portal
sslvpn	tunnel-access
All Other Users/Groups	full-access



The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

- A. Change the SSL VPN port on the client.
- B. Change the Server IP address.
- C. Change the idle-timeout.
- D. Change the SSL VPN portal to the tunnel.

Answer: A

**NEW QUESTION 62**

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.

Exhibit A Exhibit B

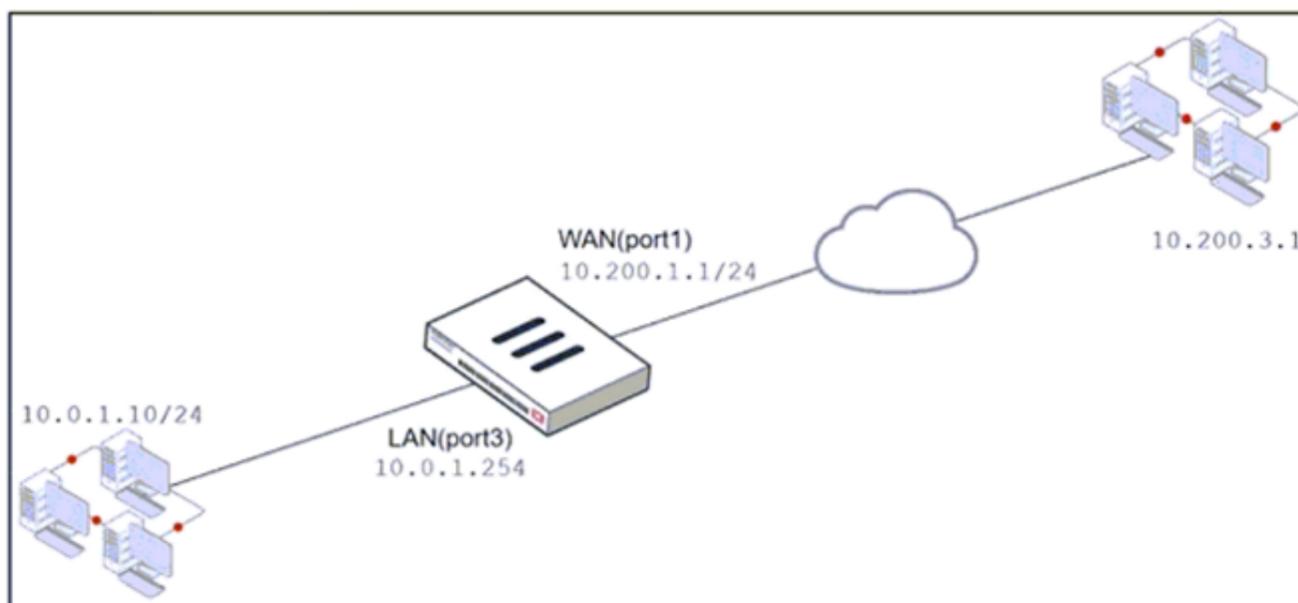


Exhibit A Exhibit B

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

**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

Optional Filters

Port Forwarding

Protocol: TCP UDP SCTP ICMP

Port Mapping Type: One to one Many to many

External service port: 10443  
 Map to IPv4 port: 443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

- A. 10.0.1.254, 10.0.1.10, and 443, respectively
- B. 10.0.1.254, 10.200.1.10, and 443, respectively
- C. 10.200.3.1, 10.0.1.10, and 443, respectively
- D. 10.0.1.254, 10.0.1.10, and 10443, respectively

**Answer: C**

**Explanation:**

The host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, which is the external IP address of the VIP object named VIP in Exhibit B1. The VIP object maps the external IP address and port to the internal IP address and port of the server 10.0.1.10 and 443, respectively. The VIP object also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface. The firewall policy ID 1 in Exhibit B allows traffic from WAN (port1) to LAN (port3) with the destination address of VIP and the service of HTTPS1. The policy also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface. Therefore, after FortiGate forwards the packet to the destination, the source address, destination address, and destination port of the packet will be 10.200.3.1, 10.0.1.10, and 443, respectively. You can find more information about VIP objects and firewall policies in the Fortinet Documentation

**NEW QUESTION 65**

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface. In this scenario, what are two requirements for the VLAN ID? (Choose two.)

- A. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.
- B. The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs.
- C. The two VLAN subinterfaces must have different VLAN IDs.
- D. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

**Answer: BC**

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-use-vmac-vlan-to-share-the-same-VLAN/t> When FortiGate is operating in NAT mode, it means that it uses network address translation (NAT) to modify the source or destination IP addresses of the traffic passing through it. NAT mode allows FortiGate to hide the IP addresses of the internal network from the external network, and to conserve IP addresses by using a single public IP address for multiple private IP addresses.

A virtual LAN (VLAN) subinterface is a logical interface that allows traffic from different VLANs to enter and exit the FortiGate unit. A VLAN subinterface is created by adding a VLAN ID to a physical interface or an aggregate interface. A VLAN ID is a numerical identifier that distinguishes one VLAN from another.

In this scenario, there are two requirements for the VLAN ID of the VLAN subinterfaces added to the same physical interface:

- > The two VLAN subinterfaces must have different VLAN IDs. This is because the VLAN ID is used to tag the traffic with the appropriate VLAN information, and to separate the traffic into different VLANs. If the two VLAN subinterfaces have the same VLAN ID, they will not be able to distinguish the traffic from each other, and they will not be able to forward the traffic to the correct destination.
- > The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs. This is because VDOMs are virtual instances of FortiGate that can have their own interfaces, policies, and routing tables. Each VDOM operates independently from other VDOMs, and can have its own VLAN subinterfaces with different or identical VLAN IDs. However, this requires inter-VDOM links to allow traffic between different VDOMs.

**NEW QUESTION 69**

Refer to the exhibits.

The exhibits show a network diagram and firewall configurations.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.

Exhibit A Exhibit B

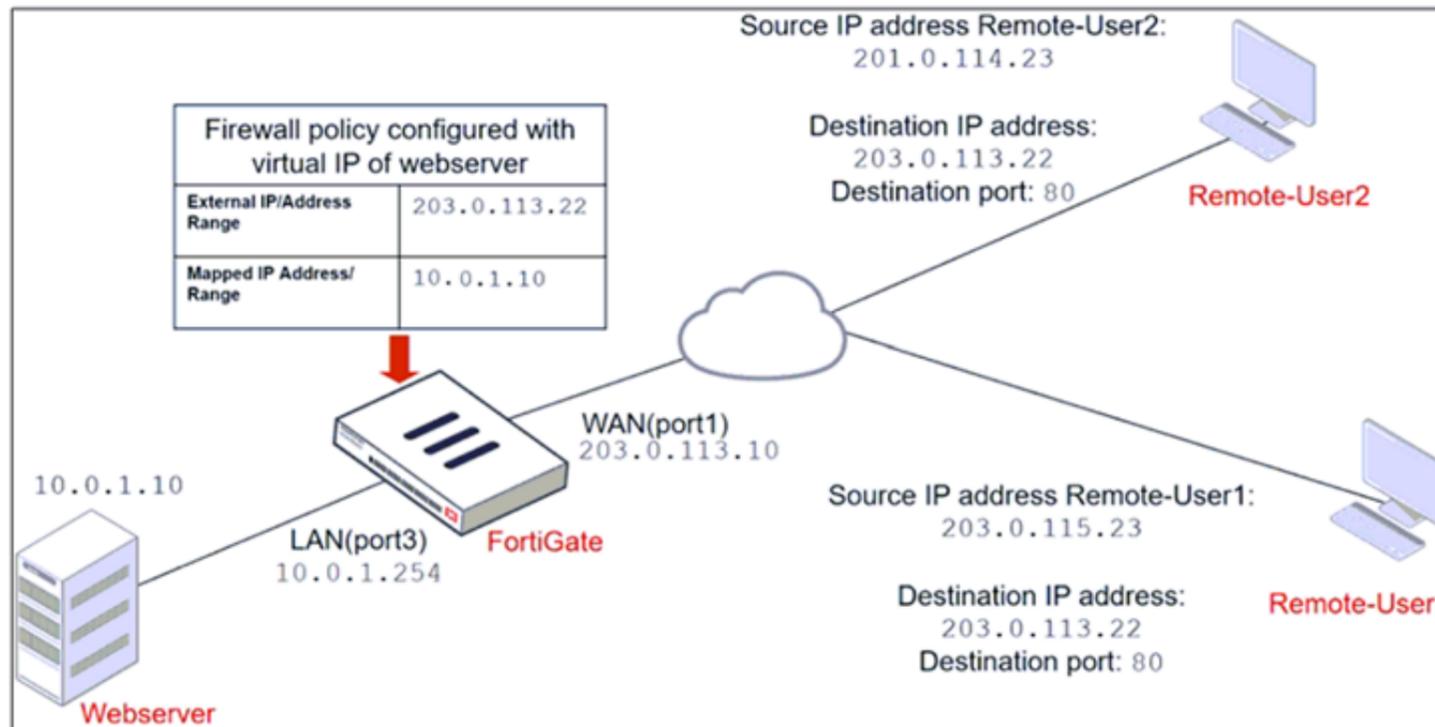


Exhibit A Exhibit B

**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 address object

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

In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

- A. Disable match-vip in the Deny policy.
- B. Set the Destination address as Deny\_IP in the Allow-access policy.
- C. Enable match vip in the Deny policy.
- D. Set the Destination address as Web\_server in the Deny policy.

**Answer: BC**

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta> The exhibits show a network diagram and firewall configurations for a FortiGate unit that has two policies: Allow\_access and Deny. The Allow\_access policy allows traffic from the WAN (port1) interface to the LAN (port3) interface with the destination address of VIP and the service of HTTPS. The VIP object maps the external IP address 10.200.1.10 and port 10443 to the internal IP address 10.0.1.10 and port 443 of the Webserver. The Deny policy denies traffic from the WAN (port1) interface to the LAN (port3) interface with the source address of Deny\_IP and the destination address of All.

In this scenario, the administrator wants to deny Webserver access for Remote-User2, who has the IP address 10.200.3.2, which is included in the Deny\_IP address object. Remote-User1, who has the IP address 10.200.3.1, must be able to access the Webserver.

To achieve this goal, the administrator can make two changes to deny Webserver access for Remote-User2:

- Set the Destination address as Webserver in the Deny policy. This will make the Deny policy more specific and match only the traffic that is destined for the Webserver's internal IP address, instead of any destination address.
- Enable match-vip in the Deny policy. This will make the Deny policy apply to traffic that matches a VIP object, instead of ignoring it. This way, the Deny policy will block Remote-User2's traffic that uses the VIP object's external IP address and port.

**NEW QUESTION 74**

Which scanning technique on FortiGate can be enabled only on the CLI?

- A. Heuristics scan
- B. Trojan scan
- C. Antivirus scan
- D. Ransomware scan

**Answer: A**

**NEW QUESTION 77**

Examine this FortiGate configuration:

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

**Answer: D**

**Explanation:**

"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

**NEW QUESTION 78**

Refer to the exhibit.

```
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 79**

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 80**

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

- A. To detect intermediary NAT devices in the tunnel path.
- B. To dynamically change phase 1 negotiation mode aggressive mode.
- C. To encapsulation ESP packets in UDP packets using port 4500.
- D. To force a new DH exchange with each phase 2 rekey.

**Answer:** AC

**NEW QUESTION 84**

An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192. 16. 1.0/24 and the remote quick mode selector is 192. 16.2.0/24. How must the administrator configure the local quick mode selector for site B?

- A. 192. 168.3.0/24
- B. 192. 168.2.0/24
- C. 192. 168. 1.0/24
- D. 192. 168.0.0/8

**Answer:** B

**NEW QUESTION 88**

Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

- A. DNS
- B. ping
- C. udp-echo
- D. TWAMP

**Answer:** CD

**NEW QUESTION 93**

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 95**

A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.

What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

- A. Static IP Address
- B. Dialup User
- C. Dynamic DNS
- D. Pre-shared Key

**Answer:** B

**Explanation:**

Dialup user is used when the remote peer's IP address is unknown. The remote peer whose IP address is unknown acts as the dialup client and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

**NEW QUESTION 99**

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
rcvbyte=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 rcvbyte=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 102**

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 107**

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile. What order must FortiGate use when the web filter profile has features enabled, such as safe search?

- A. DNS-based web filter and proxy-based web filter
- B. Static URL filter, FortiGuard category filter, and advanced filters
- C. Static domain filter, SSL inspection filter, and external connectors filters
- D. FortiGuard category filter and rating filter

**Answer: B**

**Explanation:**

FortiGate Security 7.2 Study Guide (p.285): "Remember that the web filtering profile has several features. So, if you have enabled many of them, the inspection order flows as follows: 1. The local static URL filter 2. FortiGuard category filtering (to determine a rating) 3. Advanced filters (such as safe search or removing Active X components)"

**NEW QUESTION 110**

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 111**

Which two statements are true about the FGCP protocol? (Choose two.)

- A. FGCP elects the primary FortiGate device.
- B. FGCP is not used when FortiGate is in transparent mode.
- C. FGCP runs only over the heartbeat links.
- D. FGCP is used to discover FortiGate devices in different HA groups.

**Answer:** AC

**Explanation:**

The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:  
 FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a variety of factors, such as the device's priority, to determine which device should be the primary.  
 FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices. FGCP does not run over other types of links, such as data links.

**NEW QUESTION 116**

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 119**

Which two statements are true about the Security Fabric rating? (Choose two.)

- A. It provides executive summaries of the four largest areas of security focus.
- B. Many of the security issues can be fixed immediately by clicking Apply where available.
- C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
- D. The Security Fabric rating is a free service that comes bundled with all FortiGate devices.

**Answer:** BC

**NEW QUESTION 121**

Refer to the exhibit.

**Edit IPS Sensor**

Name:

Comments:  0/255

Block malicious URLs:

**IPS Signatures and Filters**

Details	Exempt IPs	Action	Packet Logging	Status
NTP.Spoofed.KoD.DoS	0	Monitor	Enabled	Enabled
<b>OS</b> Windows		Block	Disabled	Enabled

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

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

Answer: AB

**NEW QUESTION 126**

By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

- A. set fortiguard-anycast disable
- B. set webfilter-force-off disable
- C. set webfilter-cache disable
- D. set protocol tcp

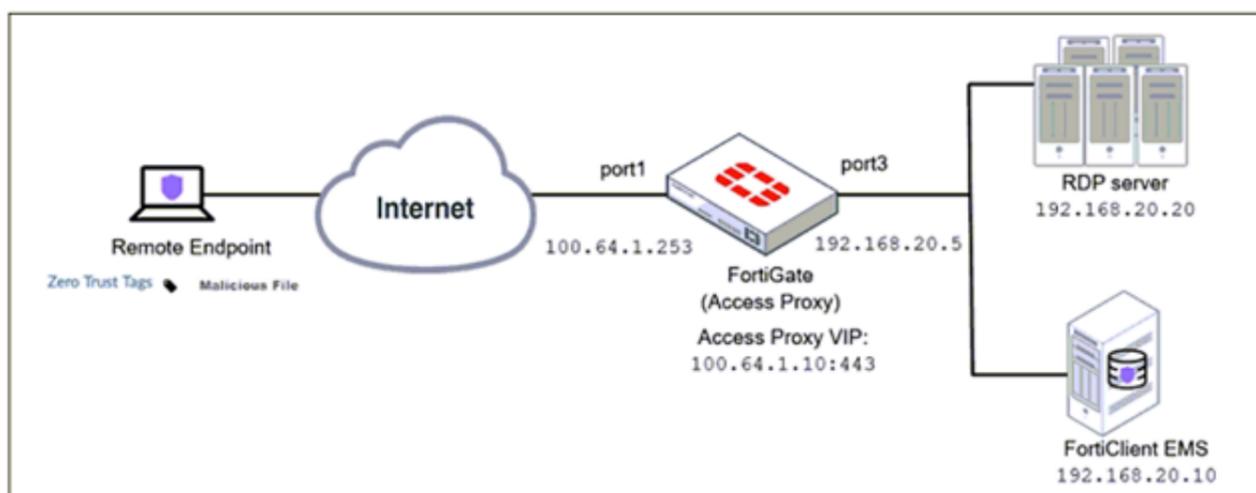
Answer: A

**Explanation:**

By default, "fortiguard-anycast" is enabled, and this setting only works with "set protocol https". To use udp (ie. "set protocol udp"), "fortiguard-anycast" must be disabled.

**NEW QUESTION 128**

Refer to the exhibit.



Based on the ZTNA tag, the security posture of the remote endpoint has changed. What will happen to endpoint active ZTNA sessions?

- A. They will be re-evaluated to match the endpoint policy.
- B. They will be re-evaluated to match the firewall policy.
- C. They will be re-evaluated to match the ZTNA policy.
- D. They will be re-evaluated to match the security policy.

Answer: C

**Explanation:**

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-zt> FortiGate Infrastructure 7.2 Study Guide (p.182):

"Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy."

**NEW QUESTION 129**

Which feature in the Security Fabric takes one or more actions based on event triggers?

- A. Fabric Connectors
- B. Automation Stitches
- C. Security Rating
- D. Logical Topology

Answer: B

**NEW QUESTION 130**

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 131**

Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check .
- D. FortiGate directs the collector agent to use a remote LDAP server.

**Answer:** BC

**Explanation:**

You can deploy FSSO w/o installing an agent. FG polls the DCs directly, instead of receiving logon info indirectly from a collector agent.

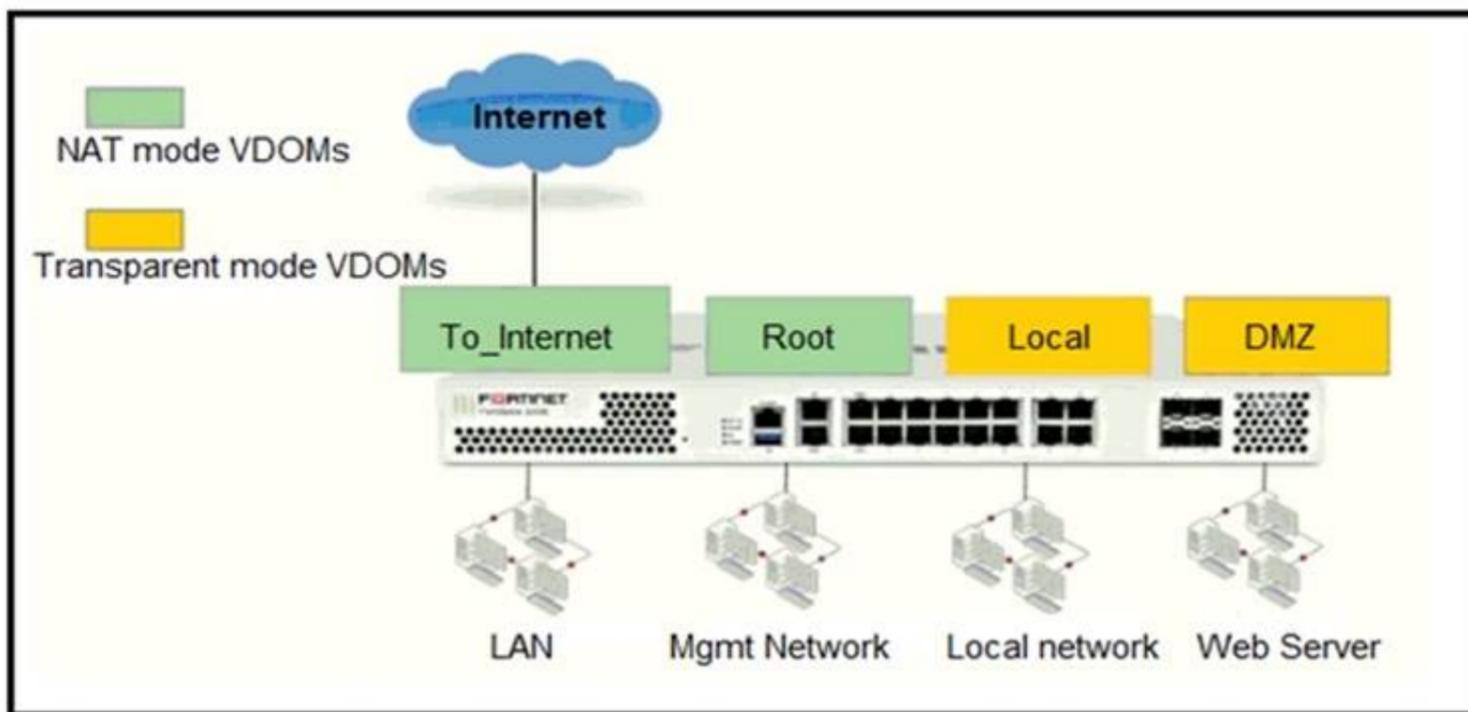
Because FG collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.

Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FG uses the SMB protocol to read the event viewer logs from the DCs.

FG acts as a collector. It 's responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

**NEW QUESTION 134**

Refer to the exhibit.



The Root and To\_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.

The Root VDOM is the management VDOM. The To\_Internet VDOM allows LAN users to access the internet. The To\_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem .

With this configuration, which statement is true?

- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
- B. A static route is required on the To\_Internet VDOM to allow LAN users to access the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
- D. Inter-VDOM links are not required between the Root and To\_Internet VDOMs because the Root VDOM is used only as a management VDOM.

**Answer:** A

**NEW QUESTION 139**

Examine the exhibit, which contains a virtual IP and firewall policy configuration.

Exhibit A Exhibit B

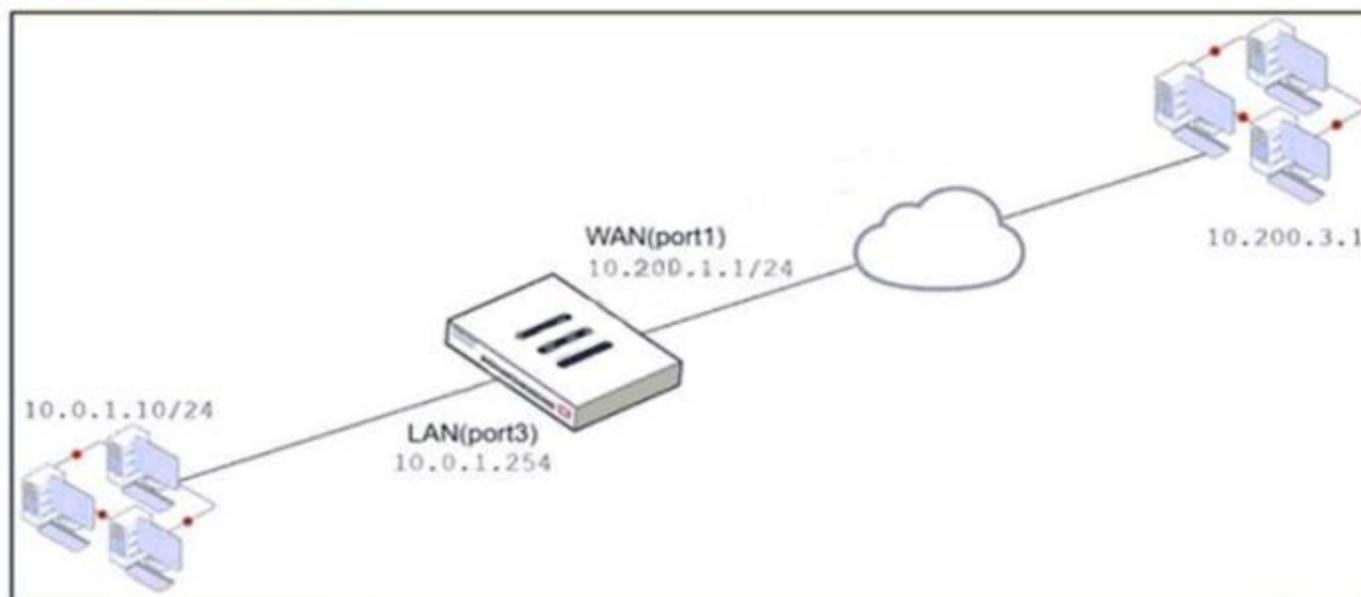


Exhibit A Exhibit B

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

**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

Optional Filters

Port Forwarding

Protocol:  TCP  UDP  SCTP  ICMP  
 Port Mapping Type:  One to one  Many to many  
 External service port: 10443  
 Map to IPv4 port: 443

The WAN (port1) interface has the IP address 10.200. 1. 1/24. The LAN (port2) interface has the IP address 10.0. 1.254/24. The first firewall policy has NAT enabled on the outgoing interface address. The second firewall policy is configured with a VIP as the destination address. Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0. 1. 10/24?

- A. 10.200. 1. 10
- B. Any available IP address in the WAN (port1) subnet 10.200. 1.0/24 66 of 108
- C. 10.200. 1. 1
- D. 10.0. 1.254

**Answer:** A

**Explanation:**

<https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs>.

**NEW QUESTION 140**

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

**Answer:** ABC

**Explanation:**

[https://help.fortinet.com/fo50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top\\_VirtualWirePair.htm](https://help.fortinet.com/fo50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm)

**NEW QUESTION 141**

Refer to the exhibit.

The screenshot shows the 'Access Permissions' section of a FortiGate administrator profile. The profile name is 'Custom\_Profile'. Below the 'Access Control' column, there is a table of permissions for various system components. The 'Permissions' column has a 'Set All' dropdown menu. The permissions are as follows:

Access Control	Permissions
Security Fabric	None, Read, Read/Write
FortiView	None, Read, Read/Write
User & Device	None, Read, Read/Write
Firewall	None, Read, Read/Write, Custom
Log & Report	None, Read, Read/Write, Custom
Network	None, Read, Read/Write, Custom
System	None, Read, Read/Write, Custom
Security Profile	None, Read, Read/Write, Custom
VPN	None, Read, Read/Write
WAN Opt & Cache	None, Read, Read/Write
WiFi & Switch	None, Read, Read/Write

At the bottom of the permissions section, there are two toggle switches: 'Permit usage of CLI diagnostic commands' (which is currently turned off) and 'Override Idle Timeout' (which is currently turned on).

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

- A. Custom permission for Network
- B. Read/Write permission for Log & Report
- C. CLI diagnostics commands permission
- D. Read/Write permission for Firewall

**Answer:** C

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220>

**NEW QUESTION 146**

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 151**

Refer to the exhibits.

**Edit Policy**

Name **Facebook SSL Inspection**

Incoming interface **port2**

Outgoing interface **port1**

Source **all**

Destination **all**

Service **ALL**

**Firewall/Network Options**

**CentralNAT is enabled so NAT settings from matching Central SNAT policies will be applied**

**Security Profiles**

SSL Inspection **certificate-inspection**

**Edit Policy**

Name **Facebook Access**

Incoming interface **port2**

Outgoing interface **port1**

Source **all**

Destination **all**

Schedule **always**

Service **AppDefault** Specify

Application **Facebook**, **Facebook\_Like.Button**, **Facebook\_Video.Play**

URL Category **ACCEPT** **DENY**

**Firewall/Network Options**

Protocol Options **default**

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook . Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

- A. Make SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Get the additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

**Answer:** A

**Explanation:**

They can play video (tick) content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts. This indicate that the rule are partially working as they can watch video but cant react, i.e. liking the content. So must be an issue with the SSL inspection rather than adding an app rule.

**NEW QUESTION 155**

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

- A. FortiGuard web filter cache
- B. FortiGate hostname
- C. NTP
- D. DNS

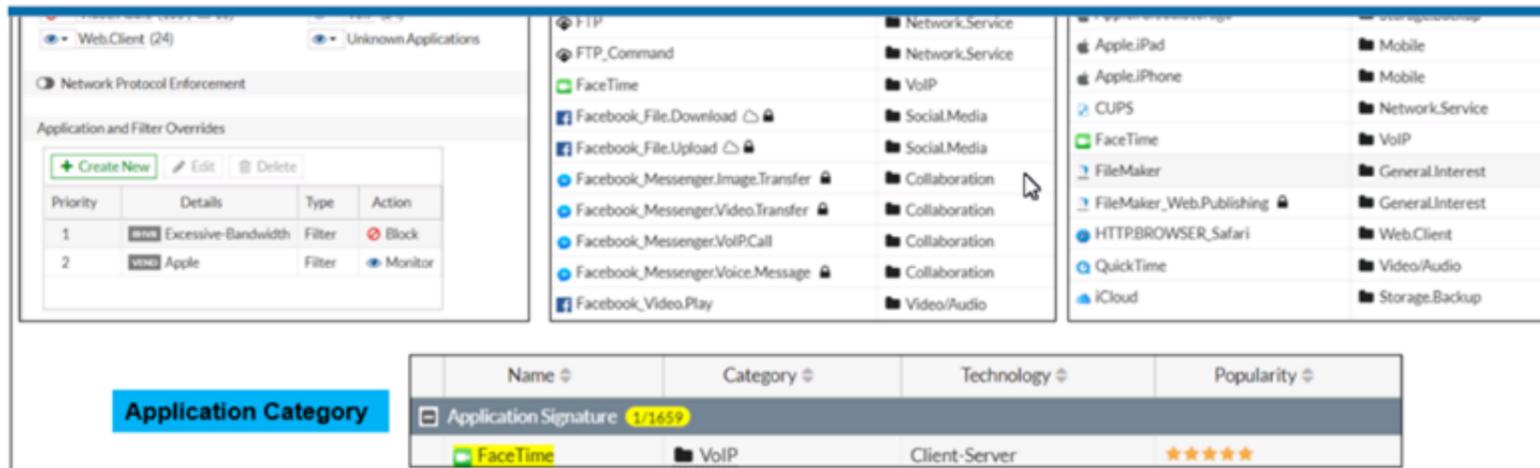
**Answer:** CD

**Explanation:**

In the 7.2 Infrastructure Guide (page 306) the list of configuration settings that are NOT synchronized includes both 'FortiGate host name' and 'Cache'

**NEW QUESTION 160**

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 163**

In an explicit proxy setup, where is the authentication method and database configured?

- A. Proxy Policy
- B. Authentication Rule
- C. Firewall Policy
- D. Authentication scheme

Answer: D

**NEW QUESTION 165**

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 166**

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 168**

Which statement is correct regarding the security fabric?

- A. FortiManager is one of the required member devices.
- B. FortiGate devices must be operating in NAT mode.
- C. A minimum of two Fortinet devices is required.
- D. FortiGate Cloud cannot be used for logging purposes.

Answer: B

**Explanation:**

FortiGate Security 7.2 Study Guide (p.428): "You must have a minimum of two FortiGate devices at the core of the Security Fabric, plus one FortiAnalyzer or cloud logging solution. FortiAnalyzer Cloud or FortiGate Cloud can act as the cloud logging solution. The FortiGate devices must be running in NAT mode."

**NEW QUESTION 170**

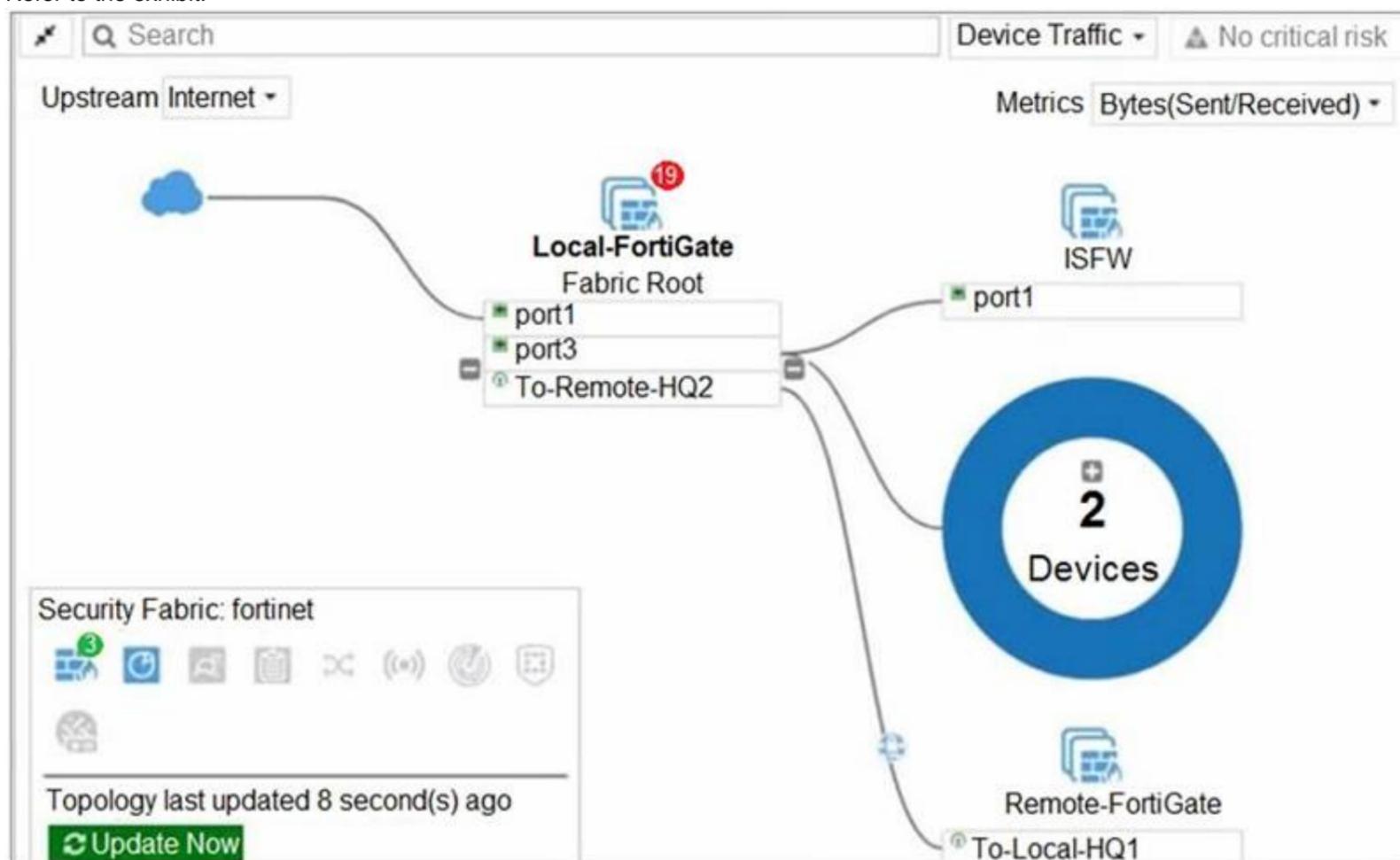
Which two statements are correct about NGFW Policy-based mode? (Choose two.)

- 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 173**

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 176**

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 180**

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 181

An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. A session for denied traffic is created.
- D. The number of logs generated by denied traffic is reduced.

**Answer:** CD

#### Explanation:

ses-denied-traffic

Enable/disable including denied session in the session table. <https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/20620/config-system-settings-block-session-timer>

Duration in seconds for blocked sessions . integer

Minimum value: 1 Maximum value: 300

30

<https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/1620/config-system-global>

### NEW QUESTION 185

Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53->10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

- A. The session is a UDP unidirectional state.
- B. The session is in TCP ESTABLISHED state.
- C. The session is a bidirectional UDP connection.
- D. The session is a bidirectional TCP connection.

**Answer:** C

#### Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

### NEW QUESTION 190

Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

- A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.
- B. The application signature database inspects traffic only from the original web application server.
- C. FortiGuard maintains only one signature of each web application that is unique.
- D. FortiGate can inspect sub-application traffic regardless where it was originate

**Answer:** D

### NEW QUESTION 192

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 195**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE4\_FGT-7.2 Practice Exam Features:

- \* NSE4\_FGT-7.2 Questions and Answers Updated Frequently
- \* NSE4\_FGT-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE4\_FGT-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE4\_FGT-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
[Order The NSE4\\_FGT-7.2 Practice Test Here](#)