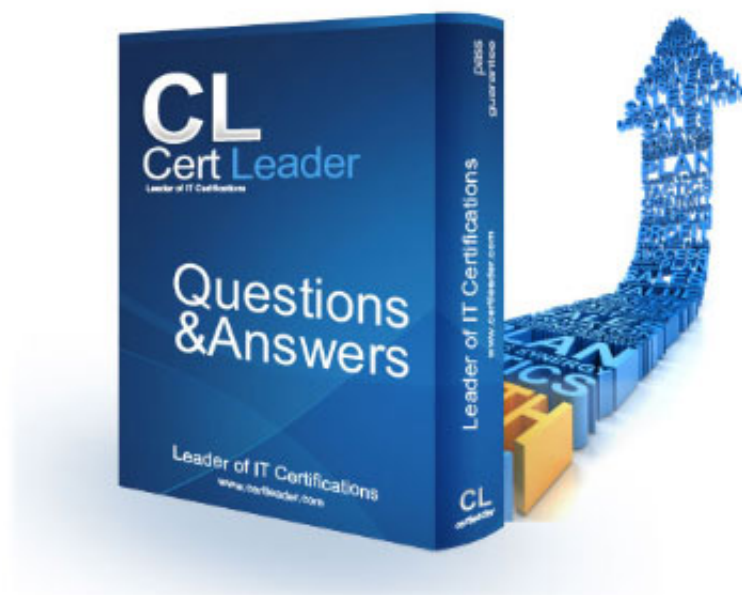


# NSE4\_FGT-7.2 Dumps

## Fortinet NSE 4 - FortiOS 7.2

[https://www.certleader.com/NSE4\\_FGT-7.2-dumps.html](https://www.certleader.com/NSE4_FGT-7.2-dumps.html)



### NEW QUESTION 1

Which two statements are correct about SLA targets? (Choose two.)

- A. You can configure only two SLA targets per one Performance SLA.
- B. SLA targets are optional.
- C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
- D. SLA targets are used only when referenced by an SD-WAN rule.

**Answer:** BD

### NEW QUESTION 2

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 3

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 4

Refer to the exhibit.

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1					
FTP.Login.Failed		Server	All	Pass	

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:

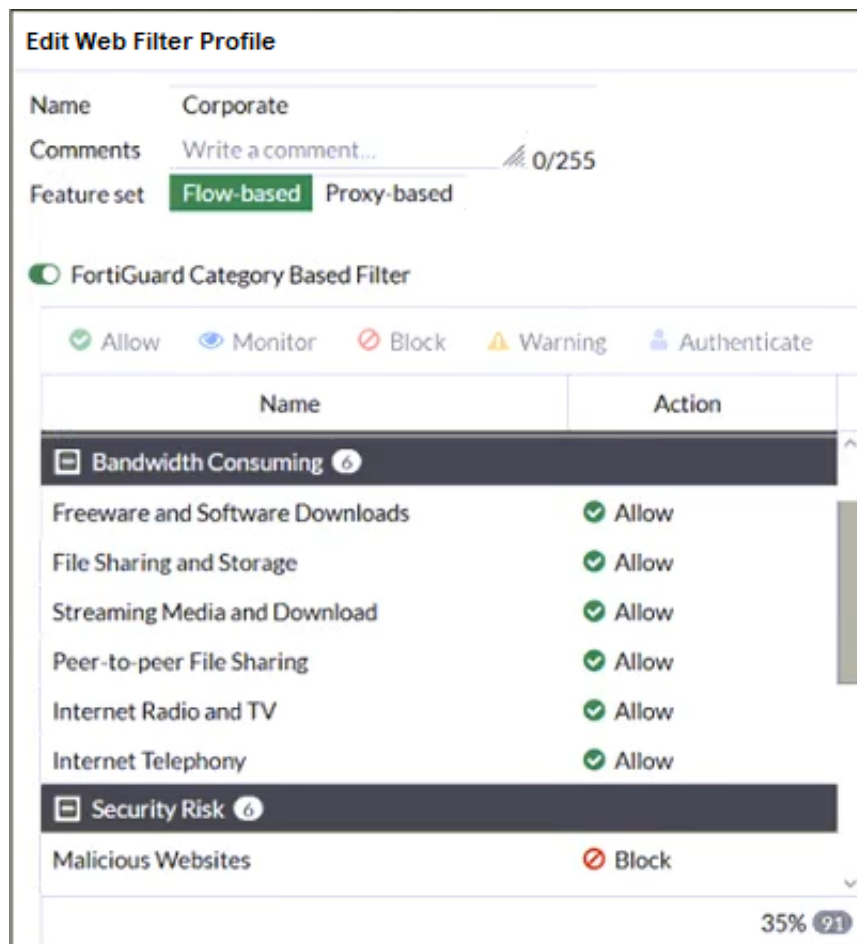
Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be 'Pass' for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be 'Default'. Action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

### NEW QUESTION 5

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.



**Edit Web Filter Profile**

Name: Corporate

Comments: Write a comment... 0/255

Feature set: **Flow-based** Proxy-based

☒ FortiGuard Category Based Filter

Allow Monitor Block Warning Authenticate

Name	Action
<b>Bandwidth Consuming</b> 6	
Freeware and Software Downloads	✓ Allow
File Sharing and Storage	✓ Allow
Streaming Media and Download	✓ Allow
Peer-to-peer File Sharing	✓ Allow
Internet Radio and TV	✓ Allow
Internet Telephony	✓ Allow
<b>Security Risk</b> 6	
Malicious Websites	✗ Block

35% 91

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."

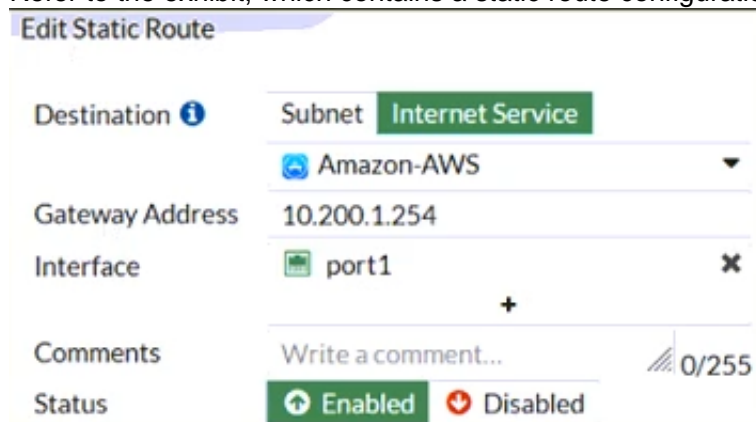
\* B. Configure a web override rating for download.com and select Malicious Websites as the subcategory. This is true because a web override rating is a feature that allows the administrator to change the FortiGuard category of a specific website or domain, and apply a different action to it based on 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 6**

Refer to the exhibit, which contains a static route configuration. An administrator created a static route for Amazon Web Services.



**Edit Static Route**

Destination: Subnet **Internet Service**

Gateway Address: 10.200.1.254

Interface: port1

Comments: Write a comment... 0/255

Status: **Enabled** Disabled

Which CLI command must the administrator use to view the route?

- A. get router info routing-table database
- B. diagnose firewall route list
- C. get internet-service route list
- D. get router info routing-table all

**Answer:** B

**Explanation:**

ISDB static route will not create entry directly in routing-table. Reference: <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/1>

and here

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640>

FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take

precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

**NEW QUESTION 7**

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 8**

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 VPNs<sup>12</sup>

\* 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 9**

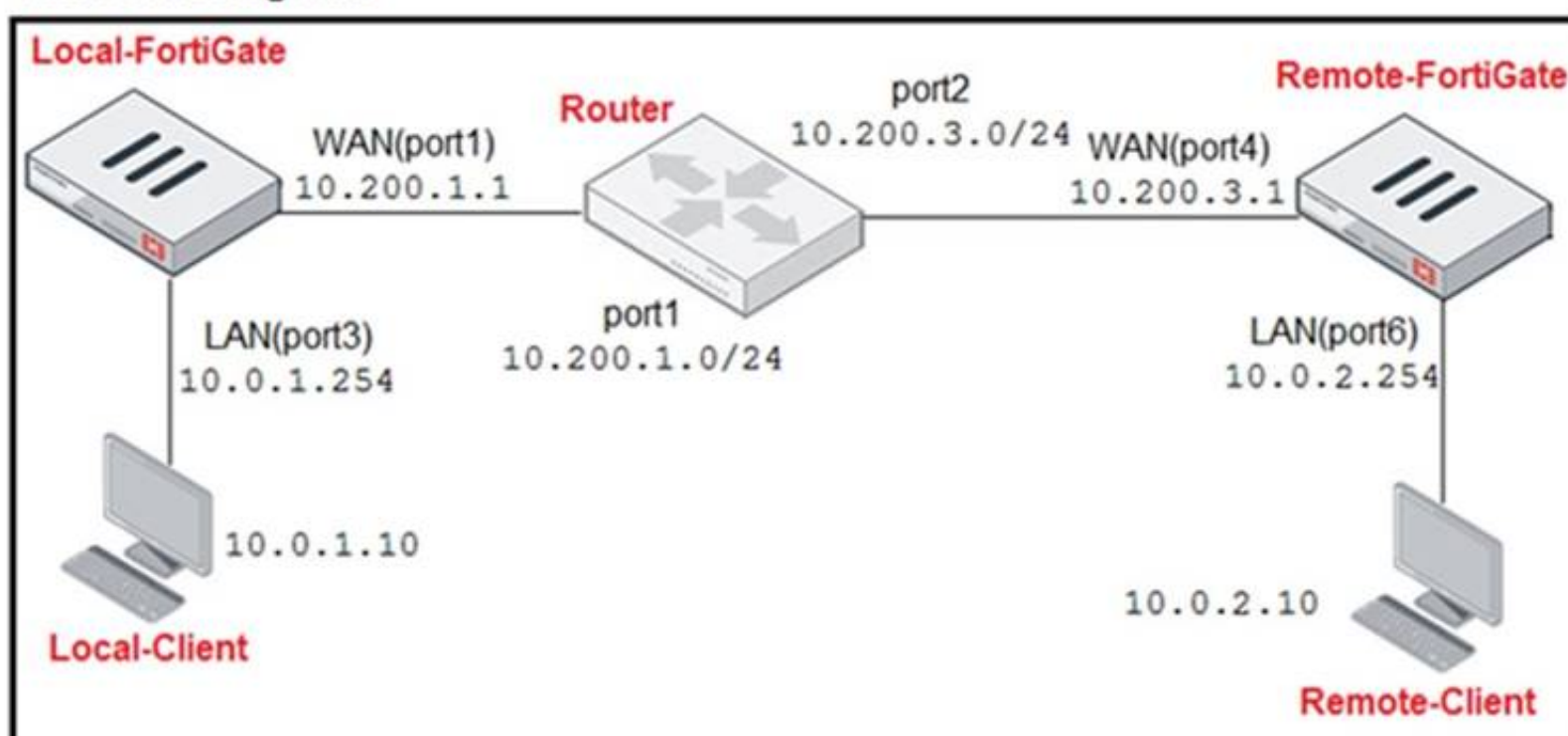
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- 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 10**

Refer to the exhibit.

**Network Diagram**



Central SNAT Policies Local-FortiGate

<div><div>+ Create New</div><div>Edit</div><div>Delete</div><div>Search</div><div>Q</div></div>						
ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
<div><div></div><div></div></div>						
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

<div><div>+ Create New</div><div>Edit</div><div>Clone</div><div>Delete</div><div>Search</div><div>Q</div></div>			
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 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 10

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

A. It uses UDP 8888.

B. It uses UDP 53.

C. It uses DNS over HTTPS.

D. It uses DNS overTLS.

Answer: D

Explanation:

FortiGate Security 7.2 Study Guide (p.15): "When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic." When using FortiGuard servers for DNS, FortiOS defaults to using DNS over TLS (DoT) to secure the DNS traffic1. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol2. This prevents eavesdropping, tampering, and spoofing of DNS data by third parties. The default FortiGuard DNS servers are 96.45.45.45 and 96.45.46.46, and they use the hostname globalsdns.fortinet.net1. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration1.

NEW QUESTION 12

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 14

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)

Cloud.IT (31)

Collaboration (293, 6)

Email (87, 12)

Game (124)

General.Interest (241, 9)

Mobile (3)

Network.Service (332)

P2P (85)

Proxy (106)

Remote.Access (91)

Social.Media (150, 31)

Storage.Backup (296, 16)

Update (48)

Video/Audio (206, 13)

VoIP (31)

Web.Client (18)

Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Create New

Edit

Delete

Priority	Details	Type	Action
1	<div>BHVR</div> Excessive-Bandwidth	Filter	<div>Block</div>
2	<div>VEND</div> Apple	Filter	<div>Monitor</div>

Exhibit A

Exhibit B

Edit Override

Type

Application

Filter

Action

Block

Filter

BHVR

 Excessive-Bandwidth

FaceTime

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

Edit Override

Type

Application

Filter

Action

Monitor

Filter

VEND

 Apple

FaceTime

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

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 15

Refer to the exhibit.

The exhibit shows the output of a diagnose command.

```
# diagnose firewall proute list
list route policy info(vf=root):
id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
```

What does the output reveal about the policy route?

- A. It is an ISDB route in policy route.
- B. It is a regular policy route.
- C. It is an ISDB policy route with an SDWAN rule.
- D. It is an SDWAN rule in policy route.

**Answer: D**

#### Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.59): "ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the vwl\_service field, and ISDB route entries don't."

### NEW QUESTION 17

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

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

**Answer: AD**

### NEW QUESTION 19

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 24

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 25

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 30

What are two features of collector agent advanced mode? (Choose two.)

- A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
- B. In advanced mode, security profiles can be applied only to user groups, not individual users.
- C. Advanced mode uses the Windows convention—NetBios: Domain\Username.
- D. Advanced mode supports nested or inherited groups.

**Answer:** AD

#### Explanation:

\* A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.

This is true because advanced mode allows FortiGate to query the LDAP server directly for user information and group membership, without relying on the collector agent. This enables FortiGate to apply security policies based on LDAP group filters, which can be configured on FortiGate1

\* D. Advanced mode supports nested or inherited groups.

This is true because advanced mode can handle complex group structures, such as nested groups or inherited groups, where a user belongs to a group that is a member of another group. This allows FortiGate to apply security policies based on the effective group membership of a user, not just the direct group membership1

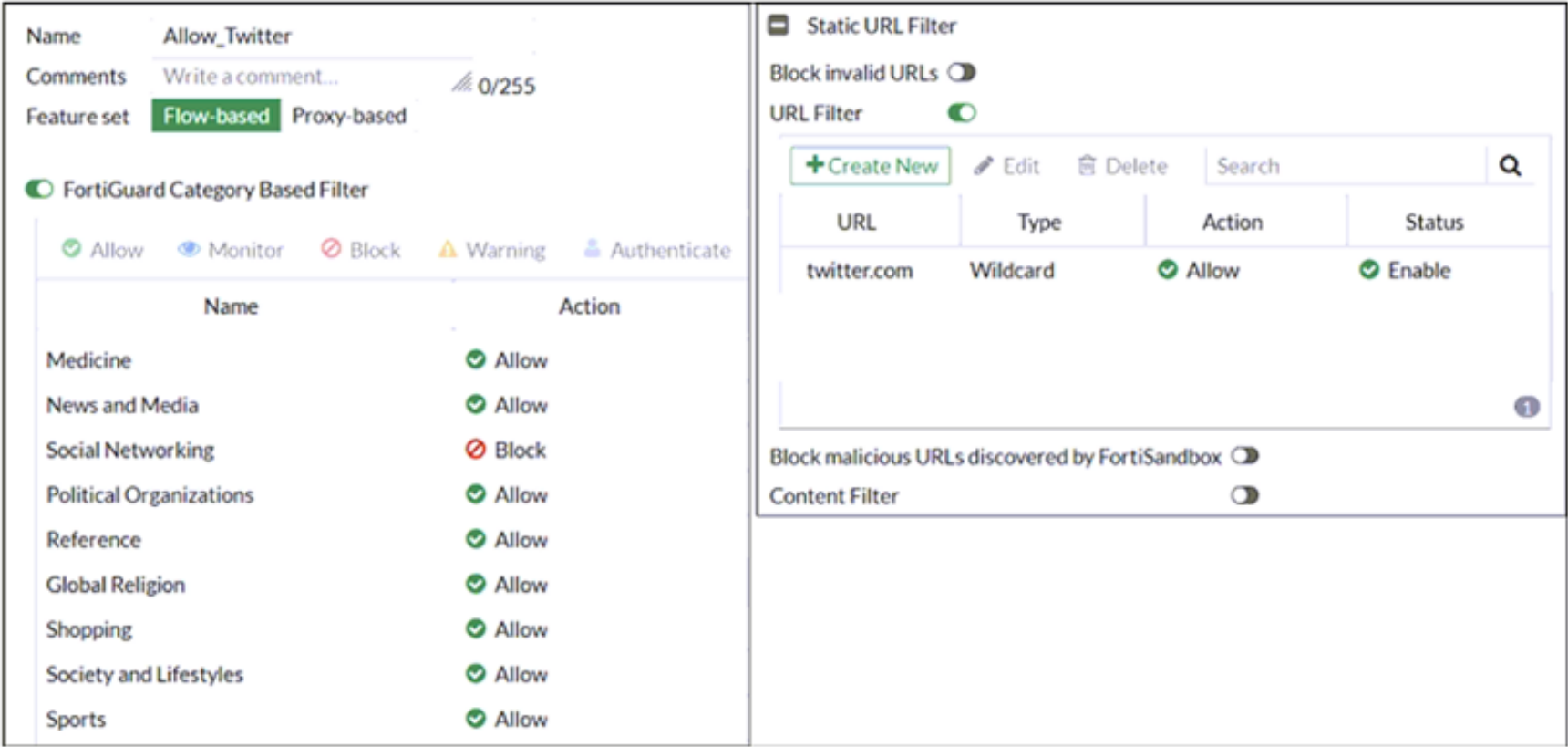
FortiGate Infrastructure 7.2 Study Guide (p.146): "Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups." "In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent."

#### NEW QUESTION 33

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 38

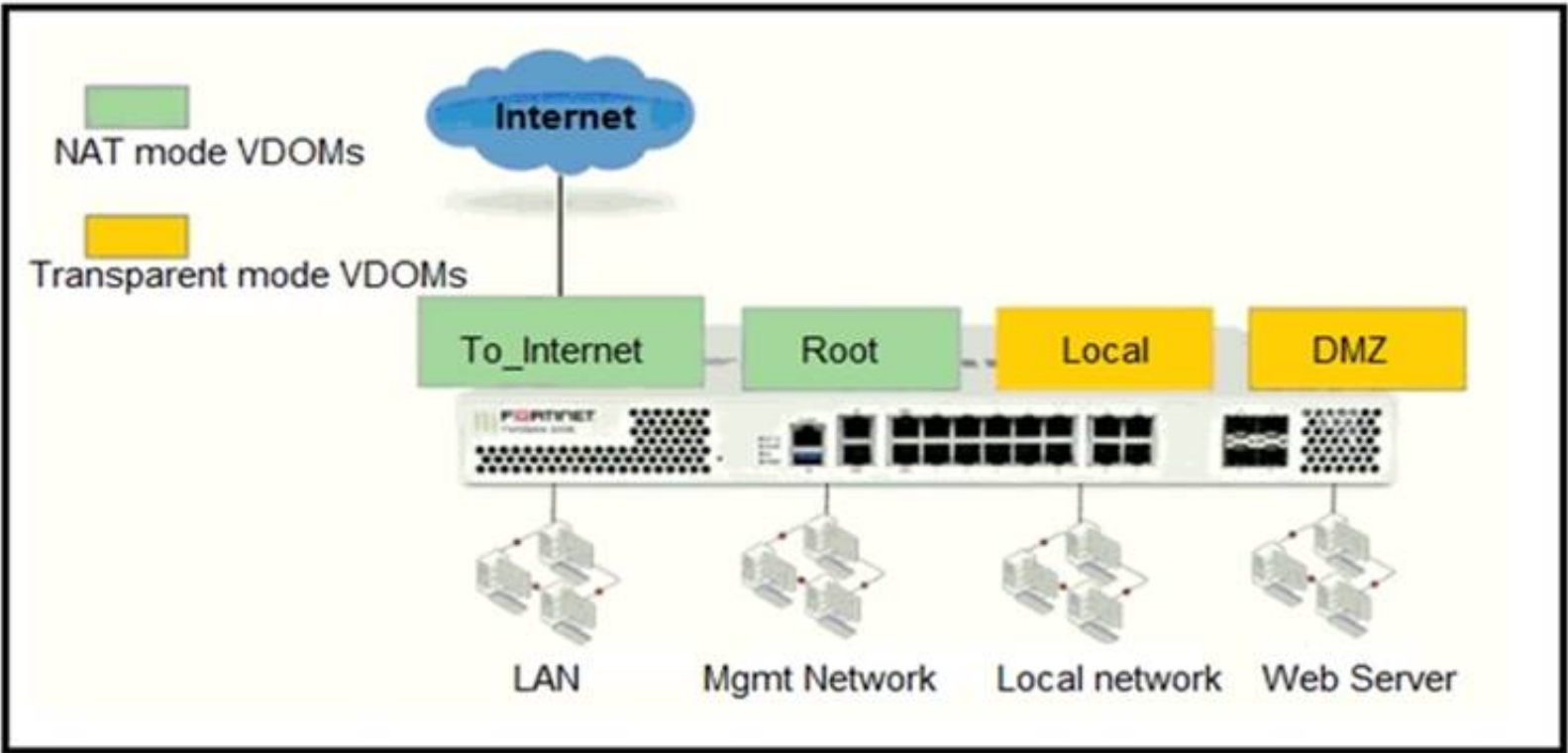
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- 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 41

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 43**

Refer to the exhibit.

Name	Custom_Profile		
Comments	<input type="text"/> 0/255		
Access Permissions			
Access Control	Permissions <span>Set All ▾</span>		
Security Fabric	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
FortiView	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
User & Device	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
Firewall	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write <input type="radio"/> Custom
Log & Report	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write <input type="radio"/> Custom
Network	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write <input type="radio"/> Custom
System	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
Security Profile	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
VPN	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
WAN Opt & Cache	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
WiFi & Switch	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Read/Write
Permit usage of CLI diagnostic commands <input type="checkbox"/>			
<input type="checkbox"/> Override Idle Timeout			

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 44**

What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

- A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
- B. FortiGate automatically negotiates a new security association after the existing security association expires.
- C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
- D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

**Answer:** D

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=12069>

FortiGate Infrastructure 7.2 Study Guide (p.264): "...then FortiGate might drop interesting traffic because of the absence of active SAs. To prevent this, you can enable Auto-negotiate. When you do this, FortiGate not only negotiates new SAs before the current SAs expire, but it also starts using the new SAs right away."

"Another benefit of enabling Auto-negotiate is that the tunnel comes up and stays up automatically, even when there is no interesting traffic. When you enable Autokey Keep Alive and keep Auto-negotiate disabled, the tunnel does not come up automatically unless there is interesting traffic. However, after the tunnel is up, it stays that way because FortiGate periodically sends keep alive packets over the tunnel. Note that when you enable Auto-negotiate, Autokey Keep Alive is implicitly enabled."

**NEW QUESTION 47**

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 51

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 53

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 58

Refer to the exhibit.

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

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct? If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 60

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 SSL 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 PROX 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 then adding an app rule.

**NEW QUESTION 63**

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

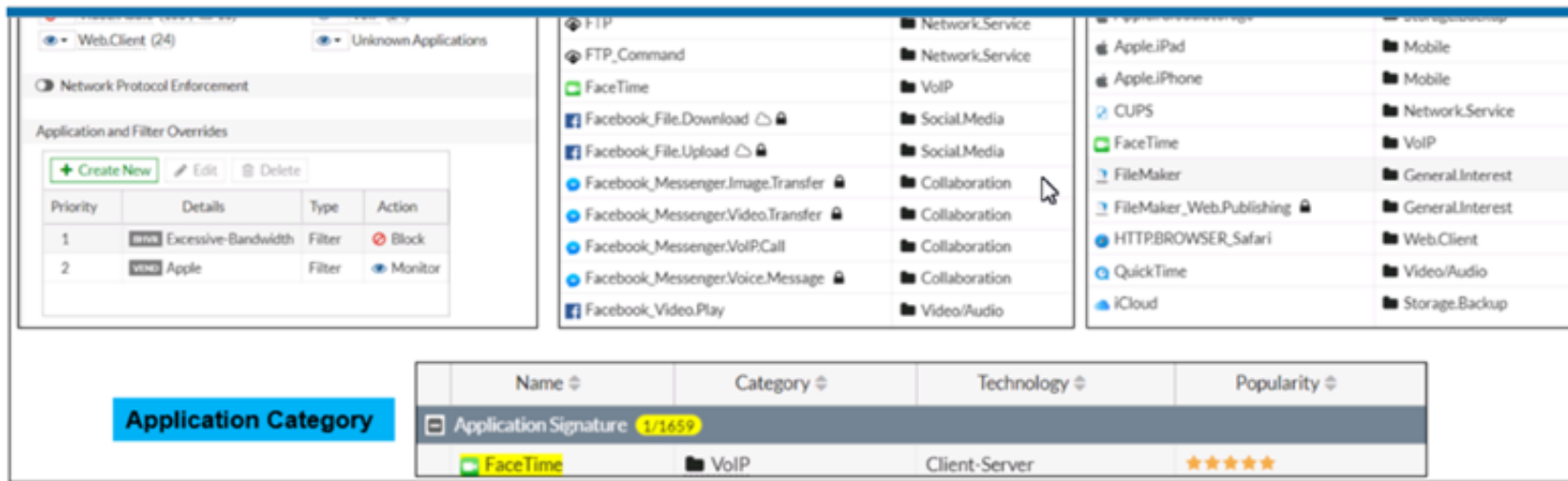
**Explanation:**

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 68**



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 73

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention

**Answer: AD**

### NEW QUESTION 75

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 78

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:**

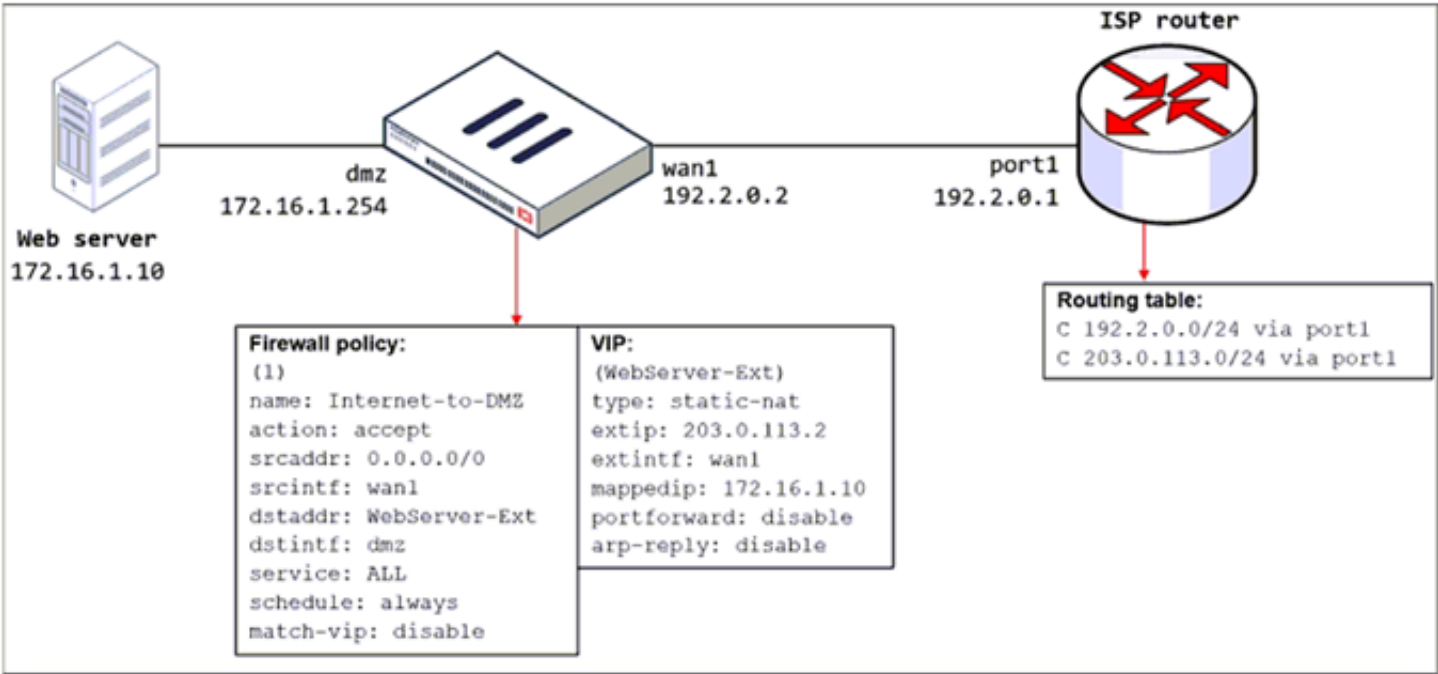
"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

**NEW QUESTION 79**

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 80**

Refer to the exhibit.

Username	Administrator	Change Password
Type	Local User	
	Match a user on a remote server group	
	Match all users in a remote server group	
	Use public key infrastructure (PKI) group	
Comments	Write a comment... 0/255	
Administrator Profile	prof_admin	
Email Address	admin@xyz.com	
<input type="checkbox"/> SMS		
<input type="checkbox"/> Two-factor Authentication		
<input type="checkbox"/> Restrict login to trusted hosts		
<input type="checkbox"/> Restrict admin to guest account provisioning only		

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

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

**Answer:** C

**NEW QUESTION 84**

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 85**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 87**

When configuring a firewall virtual wire pair policy, which following statement is true?

- A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
- B. Only a single virtual wire pair can be included in each policy.
- C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
- D. Exactly two virtual wire pairs need to be included in each policy.

**Answer:** A

**NEW QUESTION 92**

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 97**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your NSE4\_FGT-7.2 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/NSE4\\_FGT-7.2-dumps.html](https://www.certleader.com/NSE4_FGT-7.2-dumps.html)