

Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0



NEW QUESTION 1

- (Exam Topic 1)

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 2

- (Exam Topic 1)

Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

- A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
- B. To finish any inspection operations
- C. To remove the NAT operation
- D. To generate logs

Answer: A

Explanation:

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

NEW QUESTION 3

- (Exam Topic 1)

Refer to the exhibit.



The screenshot shows the FortiGate SLA configuration page for SLA1. The Name field is set to SLA1. The Protocol is set to Ping. The Server field has two entries: 4.2.2.2 and 4.2.2.1. The Participants field is set to All SD-WAN Members. The Enable probe packets checkbox is unchecked.

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

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

Answer: BD

NEW QUESTION 4

- (Exam Topic 1)

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

NEW QUESTION 5

- (Exam Topic 1)

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 6

- (Exam Topic 1)
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

☐ SMS

☐ Two-factor Authentication

☐ Restrict login to trusted hosts

☐ 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

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD34502>

NEW QUESTION 7

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 8

- (Exam Topic 1)

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 9

- (Exam Topic 1)

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 10

- (Exam Topic 1)

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

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD48690>

NEW QUESTION 10

- (Exam Topic 1)

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

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/buildingsecurity-into-fortios>

NEW QUESTION 13

- (Exam Topic 1)

FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.

Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

- A. www.example.com:443
- B. www.example.com

- C. example.com
- D. www.example.com/index.html

Answer: BC

Explanation:

FortiGate_Security_6.4 page 384

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names— "no URLs or wildcard characters are allowed".

NEW QUESTION 14

- (Exam Topic 1)

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 19

- (Exam Topic 1)

How does FortiGate act when using SSL VPN in web mode?

- A. FortiGate acts as an FDS server.
- B. FortiGate acts as an HTTP reverse proxy.
- C. FortiGate acts as DNS server.
- D. FortiGate acts as router.

Answer: B

Explanation:

Reference:

https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-sslvpn-40-mr3.pdf

NEW QUESTION 23

- (Exam Topic 1)

Refer to the exhibits.

Exhibit A.

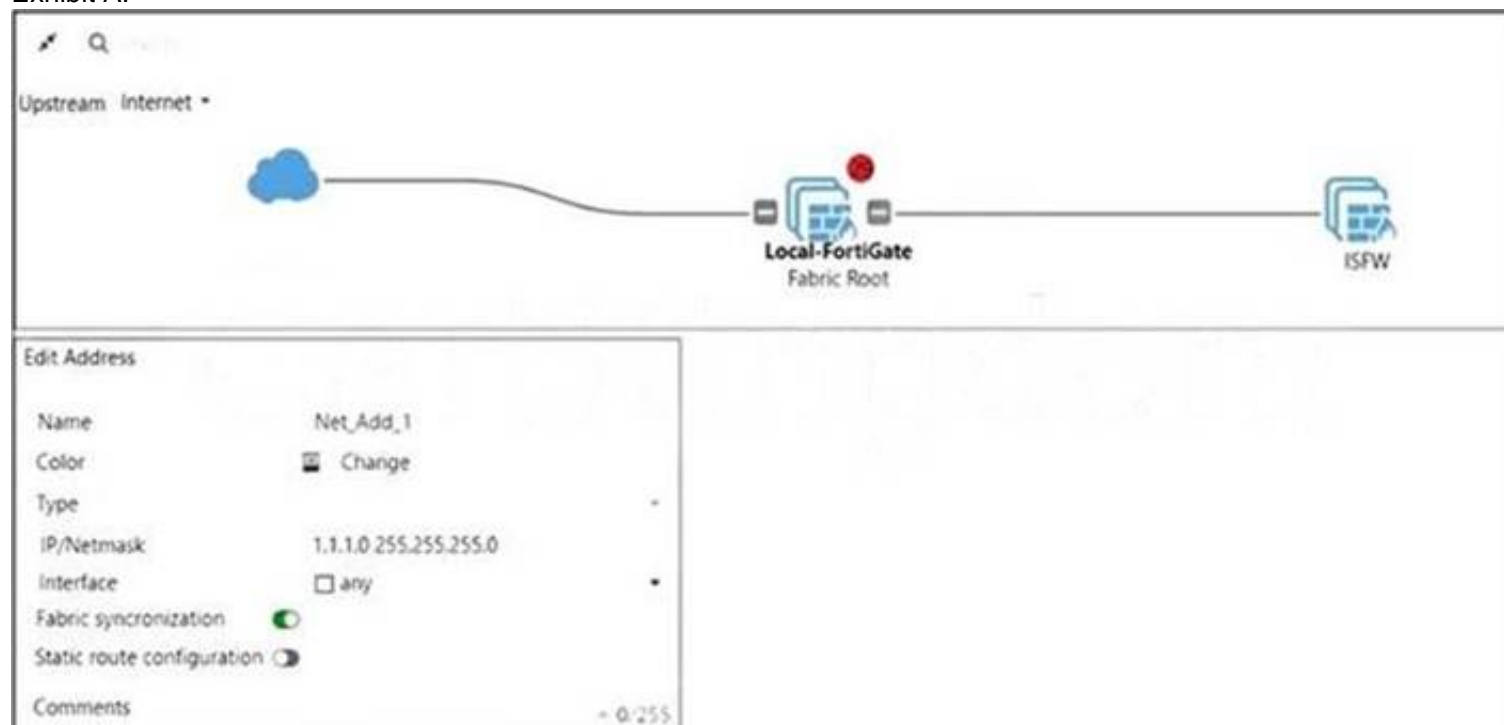


Exhibit B.



An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the

downstream FortiGate (ISFW).

What must the administrator do to synchronize the address object?

- A. Change the csf setting on Local-FortiGate (root) to sec configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to sec configuracion-sync local.
- C. Change the csf setting on Local-FortiGate (root) to sec fabric-objecc-unificacion defaultc.
- D. Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion defaultc.

Answer: A

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD43820>

NEW QUESTION 24

- (Exam Topic 1)

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 clien and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

NEW QUESTION 25

- (Exam Topic 1)

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 28

- (Exam Topic 1)

Refer to the exhibit.

```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000  4500 003c 2f8f 0000 8001 f020 0a00 0102      E..</.....
0x0010  0808 0808 0800 4d5a 0001 0001 6162 6364      .....MZ....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374      efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869                uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000  4500 003c 2f8f 0000 7f01 0106 0a38 f0e4      E..</.....8..
0x0010  0808 0808 0800 6159 ec01 0001 6162 6364      .....aY....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374      efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869                uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000  4500 003c 0000 0000 7501 3a95 0808 0808      E..<....u.:.....
0x0010  0a38 f0e4 0000 6965 ec01 0001 6162 6364      .8....iY....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374      efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869                uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000  4500 003c 0000 0000 7401 2bb0 0808 0808      E..<....t.+.....
0x0010  0a00 0102 0000 555a 0001 0001 6162 6364      .....UZ....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374      efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869                uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.

Which three pieces of information are included in the sniffer output? (Choose three.)

- A. Interface name
- B. Ethernet header

- C. IP header
- D. Application header
- E. Packet payload

Answer: ACE

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=11186>

NEW QUESTION 29

- (Exam Topic 2)

Which two statements are true when FortiGate is in transparent mode? (Choose two.)

- A. By default, all interfaces are part of the same broadcast domain.
- B. The existing network IP schema must be changed when installing a transparent mode.
- C. Static routes are required to allow traffic to the next hop.
- D. FortiGate forwards frames without changing the MAC address.

Answer: AD

Explanation:

Reference: [https://kb.fortinet.com/kb/viewAttachment.do?](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113)

[attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113)

NEW QUESTION 30

- (Exam Topic 2)

Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {  
    if (shExpMatch (url, "*.fortinet.com/*")) {  
        return "DIRECT";  
    }  
    if (isInNet (host, "172.25.120.0", "255.255.255.0")) {  
        return "PROXY altproxy.corp.com: 8060";  
    }  
    return "PROXY proxy.corp.com: 8090";  
}
```

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 33

- (Exam Topic 2)

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 35

- (Exam Topic 2)

Which two statements are true about the RPF check? (Choose two.)

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

Answer: AD

Explanation:

Reference: <https://www.programmersought.com/article/16383871634/>

NEW QUESTION 40

- (Exam Topic 2)

Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

- A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password

- B. FortiGate supports pre-shared key and signature as authentication methods.
- C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.
- D. A certificate is not required on the remote peer when you set the signature as the authentication method.

Answer: AB

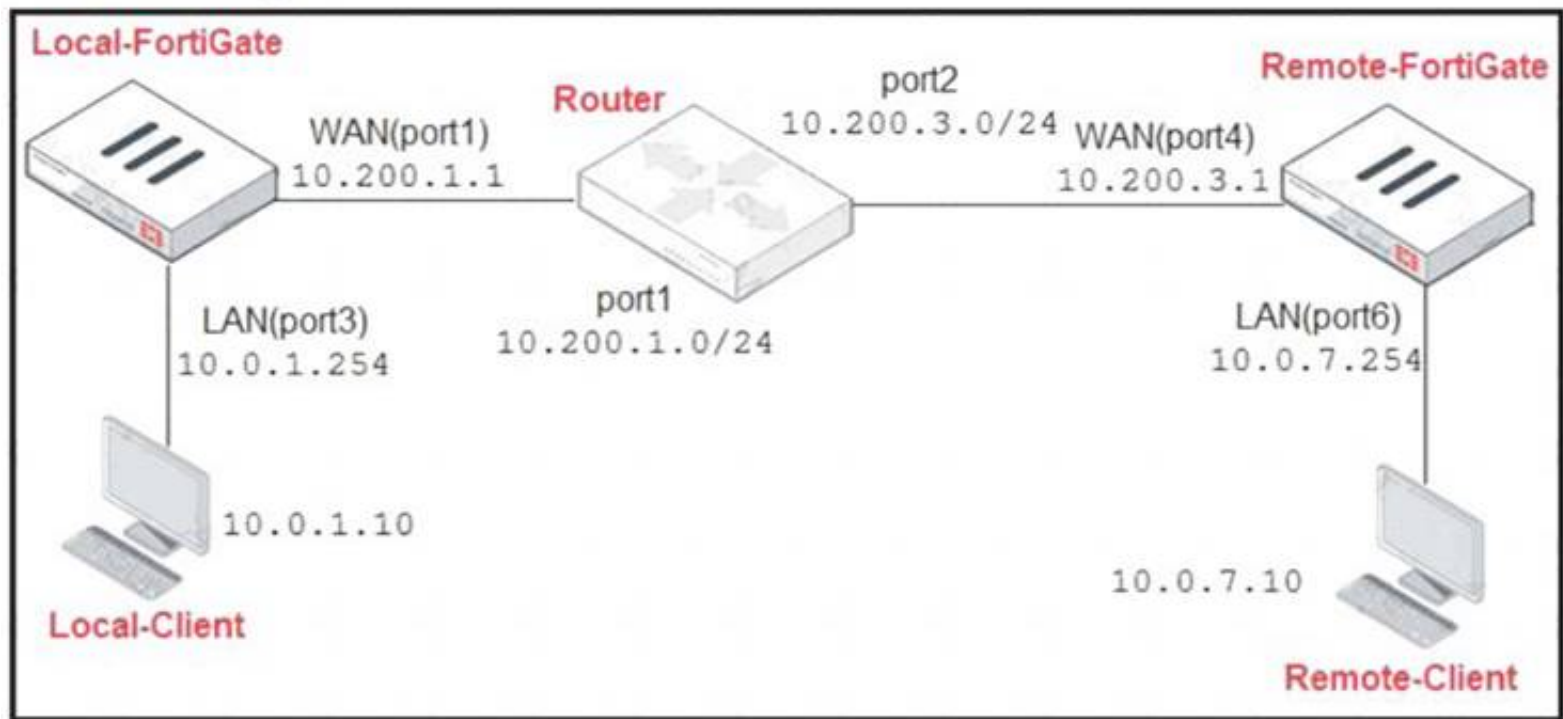
Explanation:

Reference:
<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticating-a-remote-fortigate>

NEW QUESTION 45

- (Exam Topic 2)
Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

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

IP Pool Local-FortiGate

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	Enabled

Protocol Number Table

Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IP address 10.0.1.254/24. A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied. Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

- A. 10.200.1.149
- B. 10.200.1.1
- C. 10.200.1.49
- D. 10.200.1.99

Answer: D

NEW QUESTION 48

- (Exam Topic 2)

View the exhibit.

Destination	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0		
Interface	TunnelB		
Administrative Distance	5		
Comments			
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled		
<input type="checkbox"/> Advanced Options			
Priority	30		

Destination	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0		
Interface	TunnelA		
Administrative Distance	10		
Comments			
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled		
<input type="checkbox"/> Advanced Options			
Priority	0		

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

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

Answer: CD

NEW QUESTION 50

- (Exam Topic 2)

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

- (Exam Topic 2)

Exhibit:

```
Fortigate # show authentication rule
config authentication rule
  edit "NTLM_rule"
    set srcaddr "all"
    set ip-based disable
    set web-auth-cookie enable
  next
end
```

Refer to the exhibit to view the authentication rule configuration In this scenario, which statement is true?

- A. IP-based authentication is enabled
- B. Route-based authentication is enabled
- C. Session-based authentication is enabled.
- D. Policy-based authentication is enabled

Answer: C

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD45387>

NEW QUESTION 56

- (Exam Topic 2)

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.

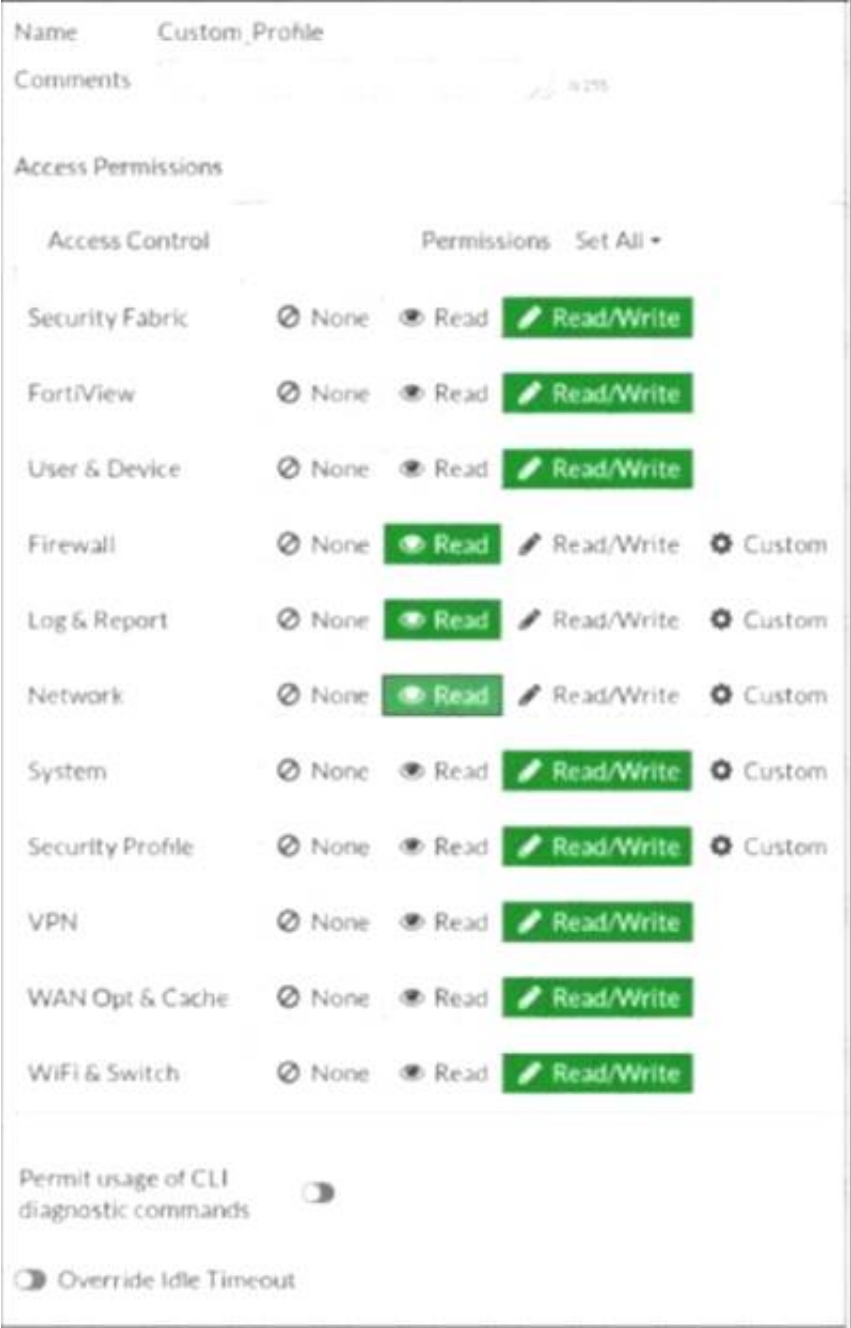
D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Answer: AB

NEW QUESTION 61

- (Exam Topic 2)

Refer to the exhibit.



Access Control	Permissions	Set All
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 checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
Log & Report	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
Network	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
System	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom	
Security Profile	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" 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 ☐

☐ 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 65

- (Exam Topic 2)

Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)

- A. Firewall policy
- B. Policy rule
- C. Security policy
- D. SSL inspection and authentication policy

Answer: CD

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/38324/ngfw-policy-based-mode>

NEW QUESTION 67

- (Exam Topic 2)

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 68

- (Exam Topic 2)

Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

- A. Root VDOM
- B. FG-traffic VDOM
- C. Customer VDOM
- D. Global VDOM

Answer: A

NEW QUESTION 73

- (Exam Topic 2)

Which two statements are true about collector agent advanced mode? (Choose two.)

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

Answer: BC

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso>

NEW QUESTION 76

- (Exam Topic 2)

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.

IPS Sensor

Name

WINDOWS_SERVERS

[View IPS Signatures]

Comments

0 / 255

IPS Signatures

+ Add Signatures

Delete

Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

+ Add Filter

Edit Filter

Delete

Filter Details	Action	Packet Logging
Location:server OS:Windows	Block	

Apply

Forward Traffic Logs

#	Date/Time	Source	Destination	Application Name	Result	Policy
1	10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2	10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3	10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4	10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5	10:09:01	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6	10:08:59	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic. What is a possible reason for this?

- A. The IPS filter is missing the Protocol: HTTPS option.
- B. The HTTPS signatures have not been added to the sensor.
- C. A DoS policy should be used, instead of an IPS sensor.
- D. A DoS policy should be used, instead of an IPS sensor.
- E. The firewall policy is not using a full SSL inspection profile.

Answer: E

NEW QUESTION 79

- (Exam Topic 2)

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

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

Answer: AC

NEW QUESTION 80

- (Exam Topic 2)

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?

- A. The administrator can register the same FortiToken on more than one FortiGate.
- B. The administrator must use a FortiAuthenticator device.
- C. The administrator can use a third-party radius OTP server.
- D. The administrator must use the user self-registration server.

Answer: B

NEW QUESTION 81

- (Exam Topic 2)

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

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

Answer: CD

NEW QUESTION 83

- (Exam Topic 2)

Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

- A. To remove the NAT operation.
- B. To generate logs
- C. To finish any inspection operations.
- D. To allow for out-of-order packets that could arrive after the FIN/ACK packets.

Answer: D

NEW QUESTION 88

- (Exam Topic 2)

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

- A. remote user's public IP address
- B. The public IP address of the FortiGate device.
- C. The remote user's virtual IP address.
- D. The internal IP address of the FortiGate device.

Answer: D

Explanation:

Source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address

NEW QUESTION 91

- (Exam Topic 2)

Examine the two static routes shown in the exhibit, then answer the following question.

<div> + Create New Edit Clone Delete </div>				
Destination	Gateway	Interface	Priority	Distance
172.20.168.0/24	172.25.1 76.1	port1	10	20
172.20.168.0/24	172.25.1 78.1	port2	20	20

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

- A. FortiGate will load balance all traffic across both routes.
- B. FortiGate will use the port1 route as the primary candidate.
- C. FortiGate will route twice as much traffic to the port2 route
- D. FortiGate will only actuate the port1 route in the routing table

Answer: B

Explanation:

“If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path.”

NEW QUESTION 94

.....

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-7.0 Practice Exam Features:

- * NSE4_FGT-7.0 Questions and Answers Updated Frequently
- * NSE4_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT-7.0 Practice Test Here](#)