

NSE4_FGT-6.4

Number: NSE4_FGT-6.4

Passing Score: 800

Time Limit: 120 min

File Version: 1

NSE4_FGT-6.4



Website: <https://vceplus.com> - <https://vceplus.co>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

Exam A

QUESTION 1

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



<https://vceplus.com/>

- 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.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Reference: [https://kb.fortinet.com/kb/viewAttachment.do?](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate%20Transparent%20Mode%20Technical%20Guide%20FortiOS%204.0%20version1.2.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%20Transparent%20Mode%20Technical%20Guide%20FortiOS%204.0%20version1.2.pdf&documentID=FD33113)

QUESTION 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.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 3

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 4

Refer to the exhibit, which contains a Performance SLA configuration.



The screenshot shows the Performance SLA configuration interface for SLA1. The configuration is as follows:

Name	SLA1		
Protocol	Ping	HTTP	DNS
Server	4.2.2.2	x	
	4.2.2.1	x	
Participants	All SD-WAN Members Specify		
	port1	x	
	port2	x	
	+		
Enable probe packets	<input type="checkbox"/>		

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic.

Why is FortiGate not generating any traffic for the performance SLA?

- A. There may not be a static route to route the performance SLA traffic.

- B. You need to turn on the **Enable probe packets** switch.
- C. The Ping protocol is not supported for the public servers that are configured.
- D. Participants configured are not SD-WAN members.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/478384/performance-sla-link-monitoring>

QUESTION 5

Refer to the exhibit to view the application control profile.



Edit Application Sensor

Categories

<input checked="" type="checkbox"/> Business (143, 6)	<input checked="" type="checkbox"/> Cloud.IT (47, 1)
<input checked="" type="checkbox"/> Collaboration (255, 10)	<input checked="" type="checkbox"/> Email (78, 12)
<input type="checkbox"/> Game (84)	<input checked="" type="checkbox"/> General.Interest (229, 7)
<input type="checkbox"/> Mobile (3)	<input checked="" type="checkbox"/> Network.Service (330)
<input type="checkbox"/> P2P (56)	<input type="checkbox"/> Proxy (168)
<input type="checkbox"/> Remote.Access (84)	<input type="checkbox"/> Social.Media (116, 31)
<input checked="" type="checkbox"/> Storage.Backup (162, 16)	<input checked="" type="checkbox"/> Update (49)
<input type="checkbox"/> Video/Audio (154, 14)	<input type="checkbox"/> VoIP (24)
<input type="checkbox"/> Web.Client (24)	<input type="checkbox"/> Unknown Applications

☐ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	<input type="checkbox"/> Block
2	VEND Apple	Filter	<input checked="" type="checkbox"/> Monitor

Users who use Apple FaceTime video conferences are unable to set up meetings.

In this scenario, which statement is true?

- A. Apple FaceTime belongs to the custom monitored filter.
- B. The category of Apple FaceTime is being monitored.
- C. Apple FaceTime belongs to the custom blocked filter.

D. The category of Apple FaceTime is being blocked.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 7

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: https://fortinet121.rssing.com/chan-67705148/all_p1.html

QUESTION 8

Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

- A. Denial of Service
- B. Web application firewall
- C. Antivirus
- D. Application control

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortiweb/6.3.3/administration-guide/60895/introduction>

QUESTION 9

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The subject field in the server certificate
- B. The serial number in the server certificate
- C. The server name indication (SNI) extension in the client hello message
- D. The subject alternative name (SAN) field in the server certificate
- E. The host field in the HTTP header

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://checkthefirewall.com/blogs/fortinet/ssl-inspection>

QUESTION 10

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

- A. SSH
- B. HTTPS

C. FTM

D. FortiTelemetry

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 11

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-Filter
Status      : Enable
License     : Contract

Num. of servers : 1
Protocol     : https
Port        : 443
Anycast      : Enable
Default servers : Not included
-- Server List (Tue Feb 1 12:00:25 2020) --
IP           Weight  RTT  Flags  TZ      Packets  Curr Lost  Total Lost
173.243.138.210 10      85  DI     -8      868      0          0
96.45.33.68    10      270 -8      -8      868      0          0
173.243.138.211 10      340 -8      -8      859      0          0
```

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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

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



<https://vceplus.com/> D.

Intrusion prevention

Correct Answer: AC

Section: (none)

Explanation



Explanation/Reference:

QUESTION 13

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.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

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

Correct Answer: B

Section: (none)

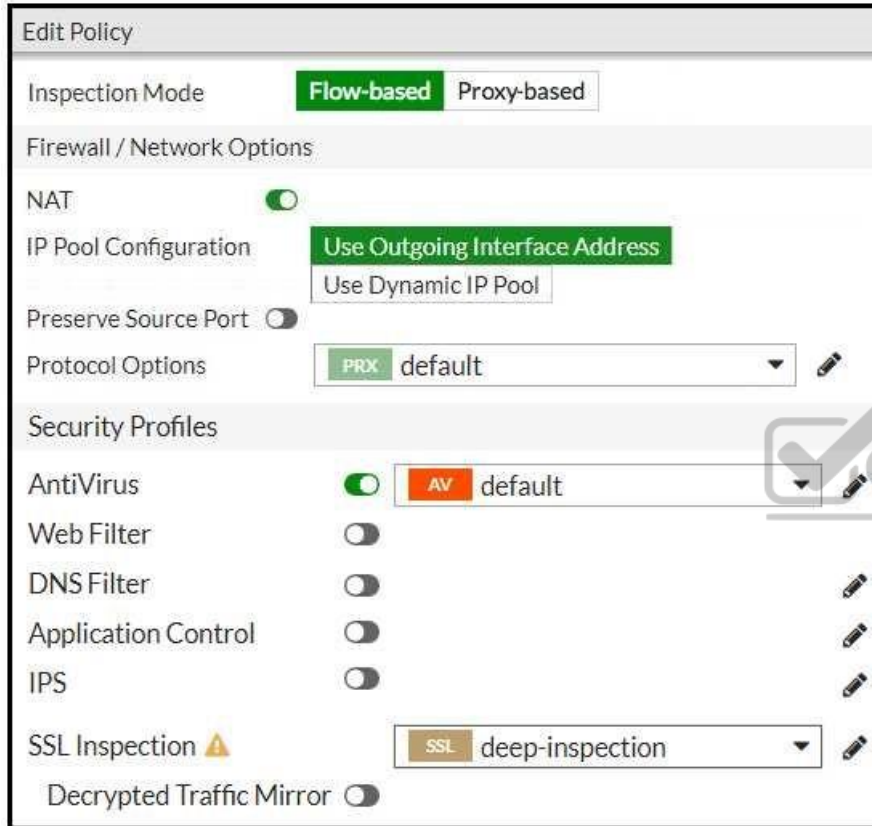
Explanation

Explanation/Reference:

QUESTION 15

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A



Edit Policy

Inspection Mode **Flow-based** Proxy-based

Firewall / Network Options

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address**
Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options **PRX** default

Security Profiles


AntiVirus ☒ **AV** default

Web Filter ☐

DNS Filter ☐

Application Control ☐

IPS ☐

SSL Inspection  **SSL** deep-inspection

Decrypted Traffic Mirror ☐

Exhibit B

Edit AntiVirus Profile

Name:

Comments: 29/255

Detect Viruses: **Block** Monitor

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

Inspected Protocols

HTTP ☒

SMTP ☒

POP3 ☒

IMAP ☒

FTP ☒

CIFS ☐

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ☒

Include Mobile Malware Protection ☒

Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database ☐

Use External Malware Block List ⓘ ⚠ ☐

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The volume of traffic being inspected is too high for this model of FortiGate.
- B. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.
- C. The firewall policy performs the full content inspection on the file.
- D. The flow-based inspection is used, which resets the last packet to the user.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srci ntfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dummytracker.org/"
sentbyte=517 rcvbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

- A. Traffic is blocked because **Action** is set to **DENY** in the firewall policy.
- B. Traffic belongs to the root VDOM.
- C. This is a security log.
- D. Log severity is set to `error` on FortiGate.

Correct Answer: AC

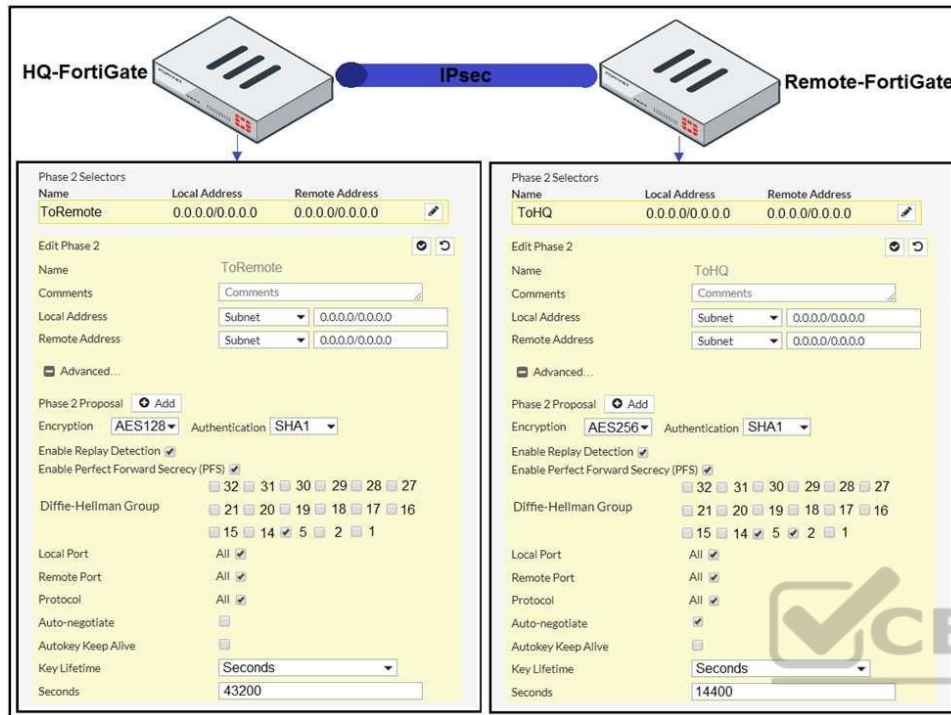
Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495>

QUESTION 18

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > System uptime > Priority > FortiGate Serial number
- B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
- C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
- D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <http://myitmicroblog.blogspot.com/2018/11/what-should-you-know-about-ha-override.html>

QUESTION 19

An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

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

Correct Answer: B

Section: (none)

Explanation

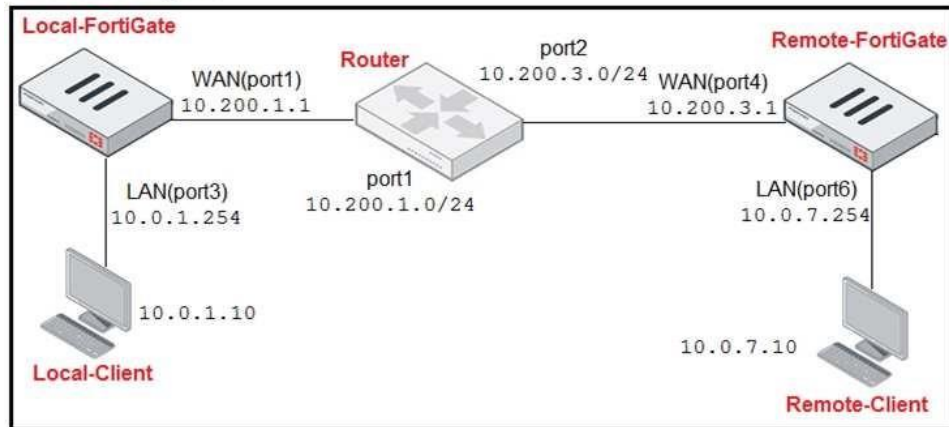
Explanation/Reference:

Reference: <https://forum.fortinet.com/tm.aspx?m=120324>

QUESTION 20

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 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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

Refer to the exhibit.

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

Why did FortiGate drop the packet?

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

Correct Answer: B

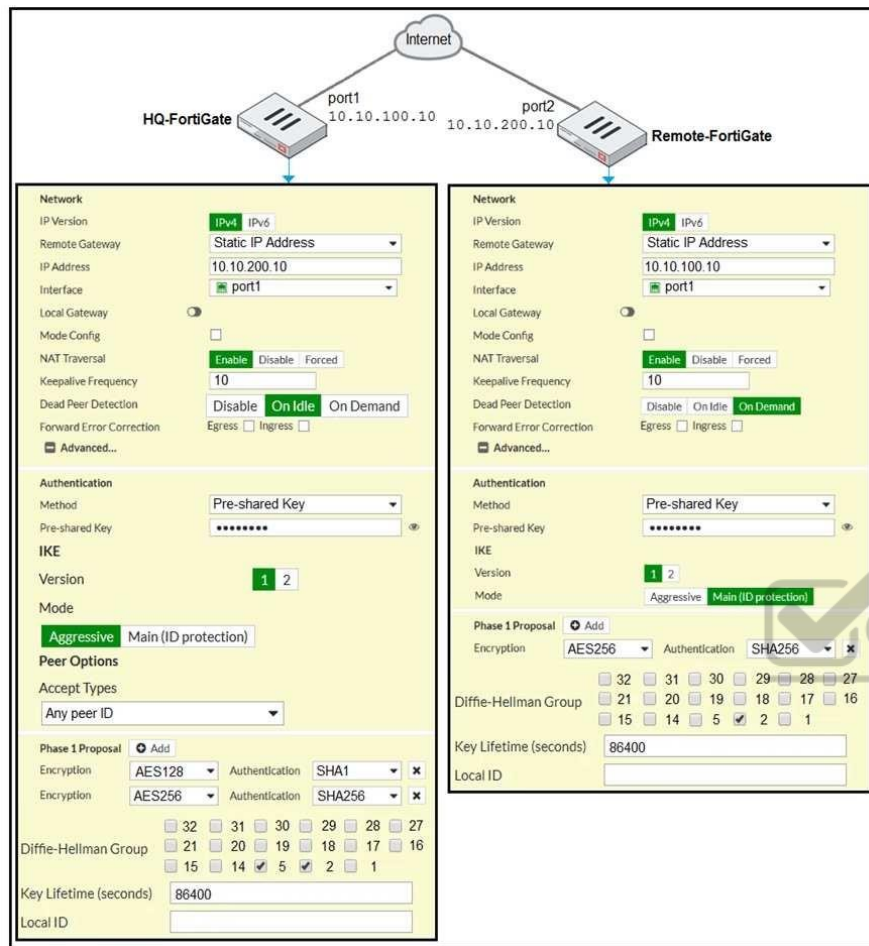
Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to **Main (ID protection)**.
- B. On both FortiGate devices, set **Dead Peer Detection** to **On Demand**.

- C. On HQ-FortiGate, disable **Diffie-Helman group 2**.
- D. On Remote-FortiGate, set **port2** as **Interface**.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

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 FortiGuard and your network from IP spoofing attacks.

Correct Answer: AD

Section: (none)

Explanation



Explanation/Reference:


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

QUESTION 25


Refer to the exhibit.


Network interface configuration

Edit Interface

Name  LAN(port3)

Alias

Type  Physical Interface

Role 

Address


Addressing mode ☒ Manual ☐ DHCP


IP/Netmask


Secondary IP address ☐

Administrative Access


IPv4

<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
<input type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
<input checked="" type="checkbox"/> TELNET	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting
<input type="checkbox"/> Security Fabric		
<input type="checkbox"/> Connection 		

Receive LLDP  ☒ Use VDOM Setting ☐ Enable ☐ Disable


Transmit LLDP  ☒ Use VDOM Setting ☐ Enable ☐ Disable



Network


Device detection  ☐


Security mode ☒

Authentication portal ☒ Local ☐ External

User Access  ☒ Restricted to Groups ☐ Allow all

User Groups  

Exempt sources 

Exempt destinations/services 

Redirect after Captive Portal ☒ Original Request ☐ Specific URL

Enforce authentication on demand option enabled

```
Local-FortiGate # config user setting

Local-FortiGate (setting) # show
config user setting
    set auth-cert "Fortinet_Factory"
    set auth-on-demand always
end
```

Firewall policies

Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port3) → WAN(port1) 2						
Sales Users	Sales LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled
Auth-Users	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled

The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration.

How will FortiGate handle user authentication for traffic that arrives on the **LAN** interface?

- A. If there is a full-through policy in place, users will not be prompted for authentication.
- B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.
- C. Authentication is enforced at a policy level; all users will be prompted for authentication.
- D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>

