NSE4_FGT-7.0 Q&As

Fortinet NSE 4 - FortiOS 7.0

Pass Fortinet NSE4_FGT-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse4_fgt-7-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

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.

Correct Answer: D

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

QUESTION 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

Correct Answer: D

QUESTION 3

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-preandandhook-out

C. diagnose wad session list | grep hook=preandandhook=out

D. diagnose wad session list | grep "hook=pre"and"hook=out"

Correct Answer: A

QUESTION 4

Refer to the exhibit.

Name	Type	IP/Netmask	VLAN ID
Physical Interface 14			
port1	Physical Interface	10.200.1.1/255.255.255.0	
port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
port10	Physical Interface	10.0.11.1/255.255.255.0	
port2	Physical Interface	10.200.2.1/255.255.255.0	
port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

A. Traffic between port2 and port2-vlan1 is allowed by default.

B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.

C. port1 is a native VLAN.

D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Correct Answer: CD

https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOMinterface/ta-p/197640?externalID=FD31639 https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

QUESTION 5

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale    : english

Service   : Web-Filter
Status    : Enable
License   : Contract

Num. of servers     : 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            868          0           0
173.243.138.211          10        340            -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: BD

QUESTION 6

Which of the following statements correctly describes FortiGates route lookup behavior when searching for a suitable gateway? (Choose two)

A. Lookup is done on the first packet from the session originator

B. Lookup is done on the last packet sent from the responder

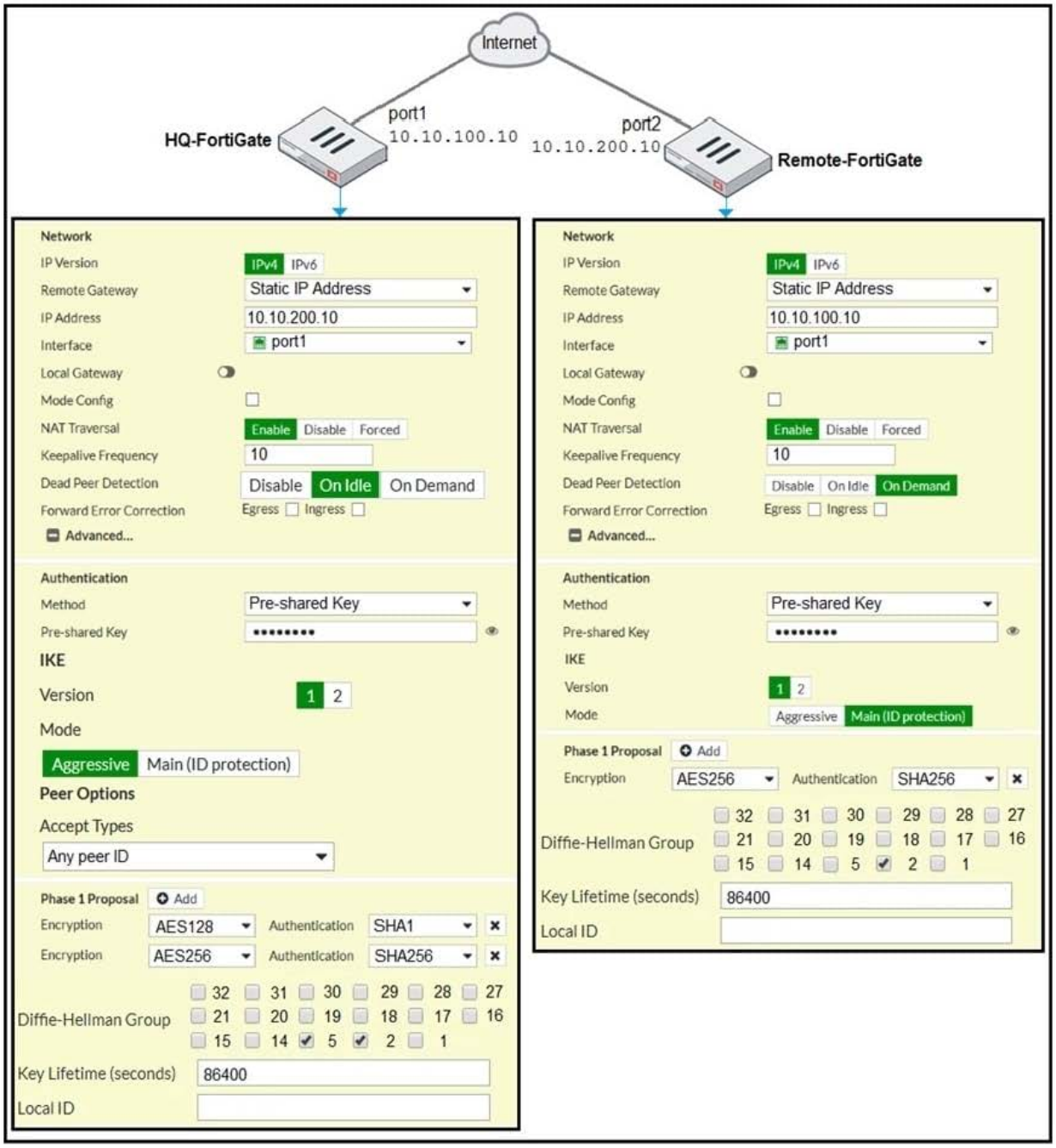
C. Lookup is done on every packet, regardless of direction

D. Lookup is done on the trust reply packet from the responder

Correct Answer: AD

QUESTION 7

Refer to the exhibit.


Internet
HQ-FortiGate
port1
10.10.100.10
port2
10.10.200.10
Remote-FortiGate
Network
IP Version
IPv4 IPv6
Remote Gateway
Static IP Address
IP Address
10.10.200.10
Interface
port1
Local Gateway
Mode Config
NAT Traversal
Enable Disable Forced
Keepalive Frequency
10
Dead Peer Detection
Disable On Idle On Demand
Forward Error Correction
Egress Ingress
Advanced...
Authentication
Method
Pre-shared Key
Pre-shared Key
IKE
Version
1 2
Mode
Aggressive Main (ID protection)
Peer Options
Accept Types
Any peer ID
Phase 1 Proposal
Add
Encryption
AES128
Authentication
SHA1
Encryption
AES256
Authentication
SHA256
Diffie-Hellman Group
32 31 30 29 28 27
21 20 19 18 17 16
15 14 5 2 1
Key Lifetime (seconds)
86400
Local ID
Network
IP Version
IPv4 IPv6
Remote Gateway
Static IP Address
IP Address
10.10.100.10
Interface
port1
Local Gateway
Mode Config
NAT Traversal
Enable Disable Forced
Keepalive Frequency
10
Dead Peer Detection
Disable On Idle On Demand
Forward Error Correction
Egress Ingress
Advanced...
Authentication
Method
Pre-shared Key
Pre-shared Key
IKE
Version
1 2
Mode
Aggressive Main (ID protection)
Phase 1 Proposal
Add
Encryption
AES256
Authentication
SHA256
Diffie-Hellman Group
32 31 30 29 28 27
21 20 19 18 17 16
15 14 5 2 1
Key Lifetime (seconds)
86400
Local ID

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 preshared 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.

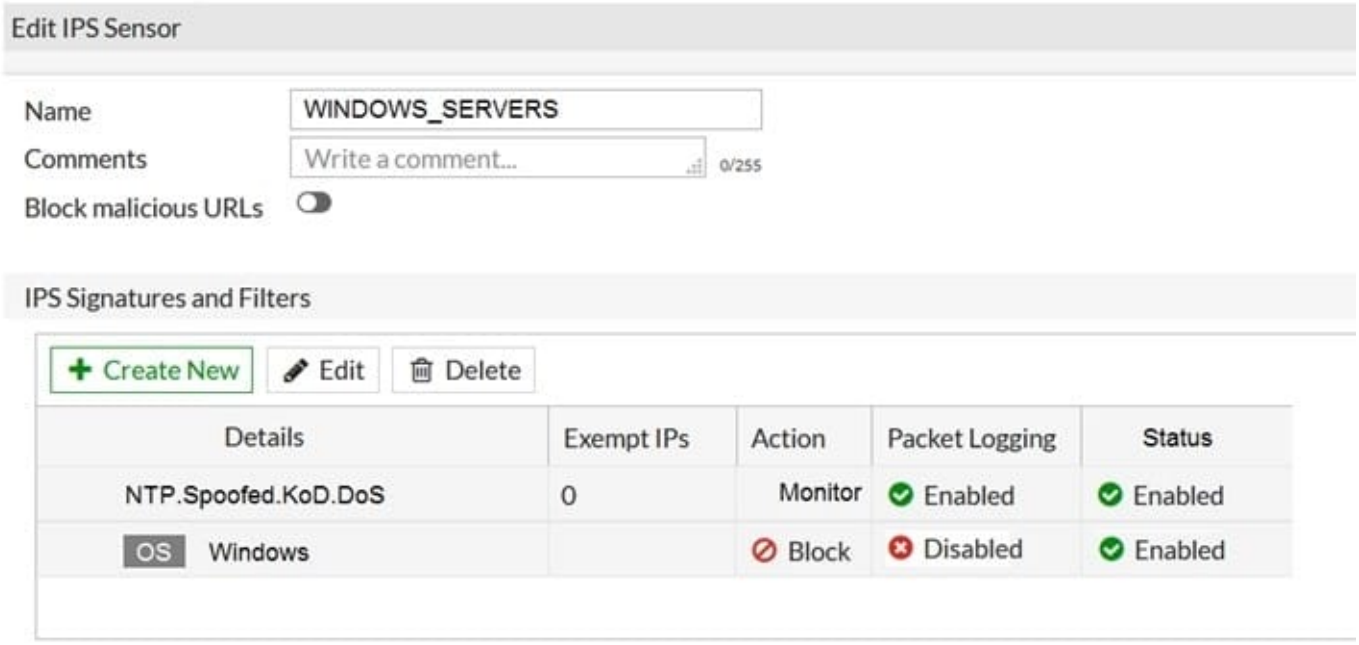
C. On HQ-FortiGate, disable Diffie-Helman group 2.

D. On Remote-FortiGate, set port2 as Interface.

Correct Answer: AD

QUESTION 8

Refer to the exhibit.



The exhibit shows the IPS sensor configuration.

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

A. The sensor will allow attackers matching the NTP.Spoofed.KoD.DoS signature.

B. The sensor will block all attacks aimed at Windows servers.

C. The sensor will reset all connections that match these signatures.

D. The sensor will gather a packet log for all matched traffic.

Correct Answer: AB

QUESTION 9

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: B

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

QUESTION 10

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

A. Source defined as Internet Services in the firewall policy.

B. Destination defined as Internet Services in the firewall policy.

C. Highest to lowest priority defined in the firewall policy.

D. Services defined in the firewall policy.

E. Lowest to highest policy ID number.

Correct Answer: ABD

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47435

QUESTION 11

A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface.

Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

B. The two VLAN sub interfaces must have different VLAN IDs.

C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.

D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

Correct Answer: B

FortiGate_Infrastructure_6.0_Study_Guide_v2-Online.pdf ?gt; page 147 "Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID"

QUESTION 12

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

A. The keyUsage extension must be set to keyCertSign.

B. The common name on the subject field must use a wildcard name.

C. The issuer must be a public CA.

D. The CA extension must be set to TRUE.

Correct Answer: AD

Reference: https://www.reddit.com/r/fortinet/comments/c7j6jg/recommended_ssl_cert/

QUESTION 13

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.

Correct Answer: B

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

QUESTION 14

An administrator is running the following sniffer command:

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

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

A. Interface name

B. Packet payload

C. Ethernet header

D. IP header

E. Application header

Correct Answer: ABD

QUESTION 15

What devices form the core of the security fabric?

A. Two FortiGate devices and one FortiManager device

B. One FortiGate device and one FortiManager device

C. Two FortiGate devices and one FortiAnalyzer device

D. One FortiGate device and one FortiAnalyzer device

Correct Answer: C

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/425100/components