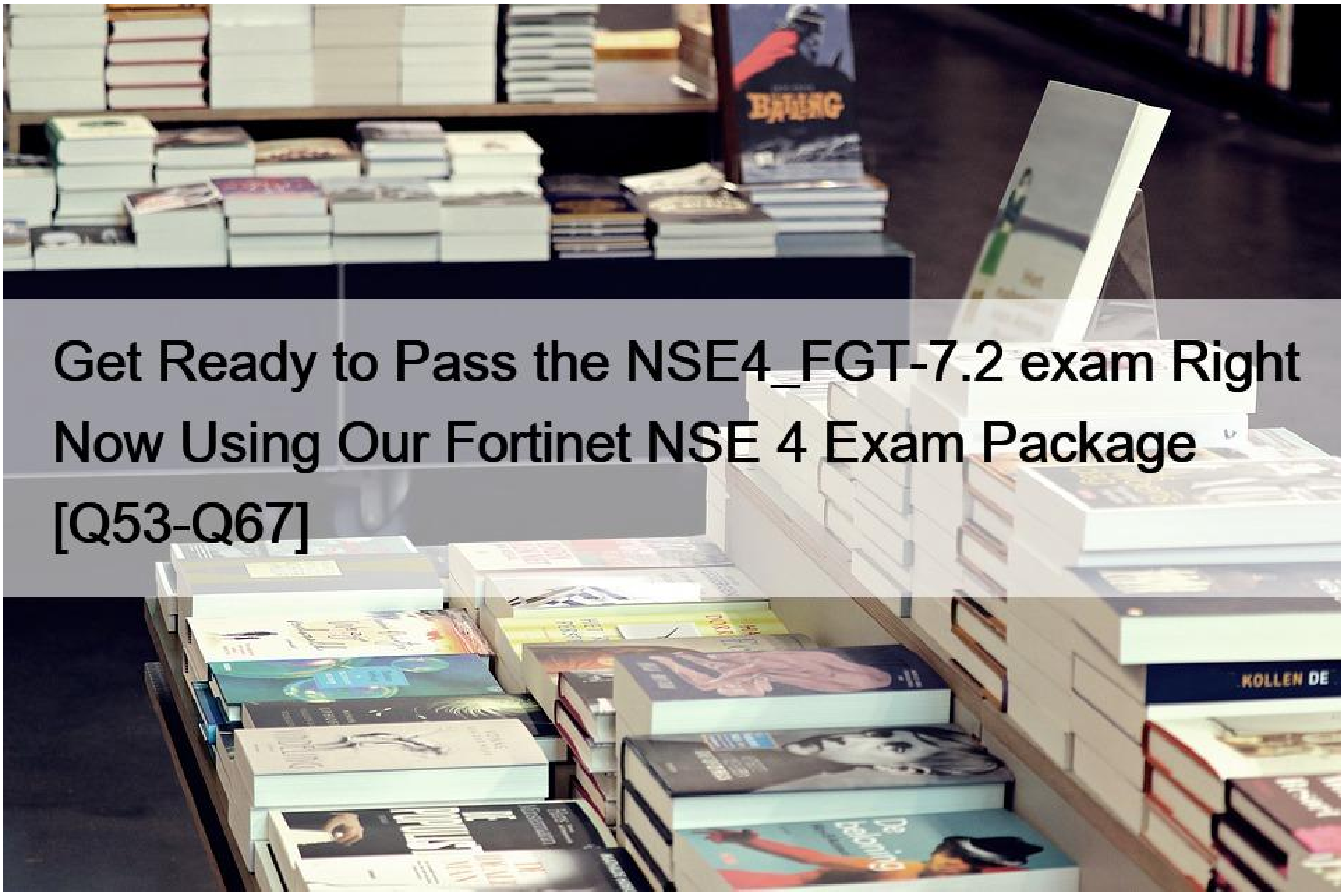
Get Ready to Pass the NSE4_FGT-7.2 exam Right Now Using Our Fortinet NSE 4 Exam Package [Q53-Q67



Get Ready to Pass the NSE4_FGT-7.2 exam Right Now Using Our Fortinet NSE 4 Exam Package Enhance Your Career With Available Preparation Guide for NSE4_FGT-7.2 Exam

Fortinet is one of the leading providers of network security solutions across the globe. With the increasing demand for cybersecurity professionals, the company offers a certification program known as the Fortinet Network Security Expert (NSE). The Fortinet NSE4_FGT-7.2 certification exam is a product of this program, and it is designed to test the knowledge and skills of professionals in Fortinet network security solutions.

Fortinet NSE4_FGT-7.2 certification exam is an excellent way for network security professionals to validate their skills and knowledge. Fortinet NSE 4 - FortiOS 7.2 certification is recognized globally and can help professionals advance their careers. Fortinet NSE 4 - FortiOS 7.2 certification is also an excellent way for organizations to validate the expertise of their security professionals.

NO.53 Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

* It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
* ADVPN is only supported with IKEv2.
* Tunnels are negotiated dynamically between spokes.
* Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

NO.54 Which two statements explain antivirus scanning modes? (Choose two.)
* In proxy-based inspection mode, files bigger than the buffer size are scanned.
* In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
* In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
* In flow-based inspection mode, files bigger than the buffer size are scanned.
Explanation

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM&#8211;something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

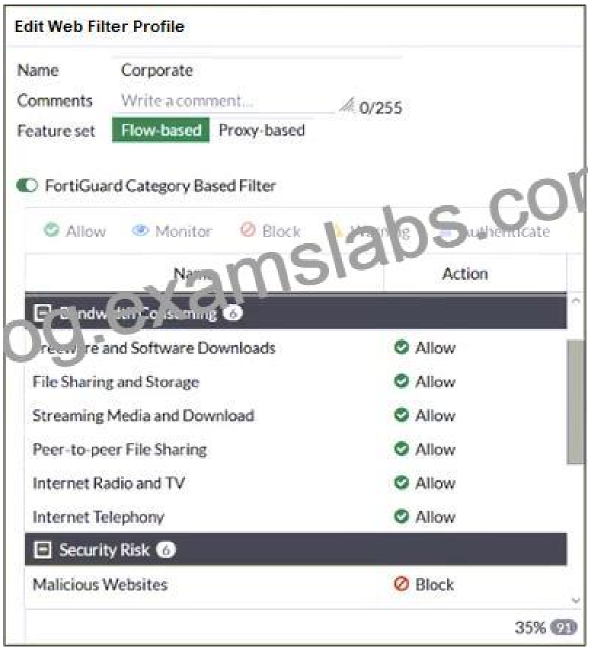
NO.55 What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?
* FortiGate automatically negotiates different local and remote addresses with the remote peer.
* FortiGate automatically negotiates a new security association after the existing security association expires.
* FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
* FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.
https://kb.fortinet.com/kb/documentLink.do?externalID=12069

FortiGate Infrastructure 7.2 Study Guide (p.264): &#8220;&#8230;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.&#8221; &#8220;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.&#8221;

NO.56 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

Name	Action
Bandwidth Consuming 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
Security Risk 6	
Malicious Websites	Block

35% 91

What are two solutions for satisfying the requirement? (Choose two.)
* Configure a separate firewall policy with action Deny and an FQDN address object for *.download.com as destination address.
* Configure a web override rating for download.com and select Malicious Websites as the subcategory.
* Set the Freeware and Software Downloads category Action to Warning.
* Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

FortiGate Security 7.2 Study Guide (p.268-269): &#8220;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.&#8221; &#8220;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.&#8221; 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.

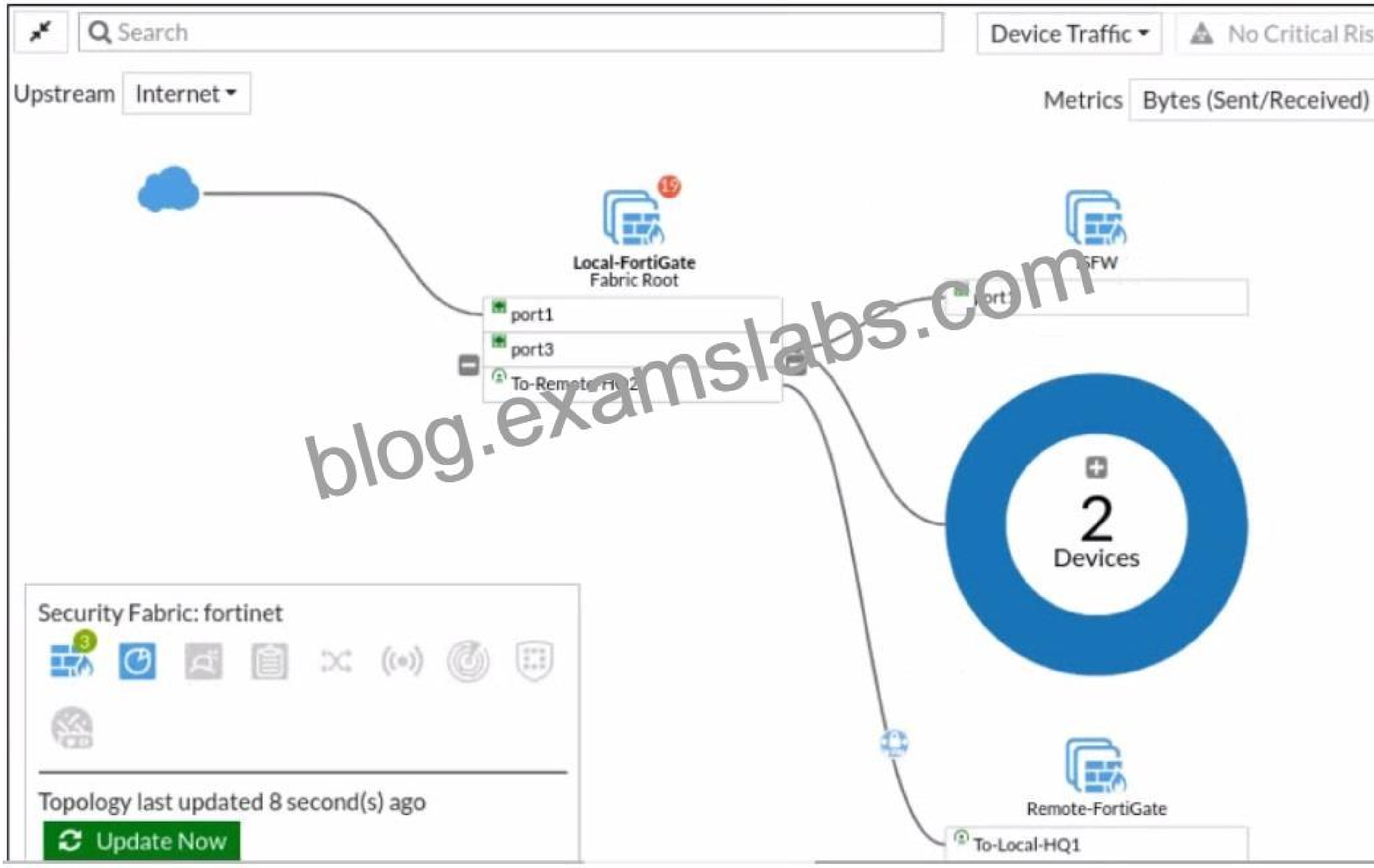
D) Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

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.

NO.57 Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?
* VDOMs without ports with connected devices are not displayed in the topology.
* Downstream devices can connect to the upstream device from any of their VDOMs.
* Security rating reports can be run individually for each configured VDOM.

* Each VDOM in the environment can be part of a different Security Fabric.
FortiGate Security 7.2 Study Guide (p.436): &#8220;When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric.&#8221;

NO.58 Refer to the exhibit.



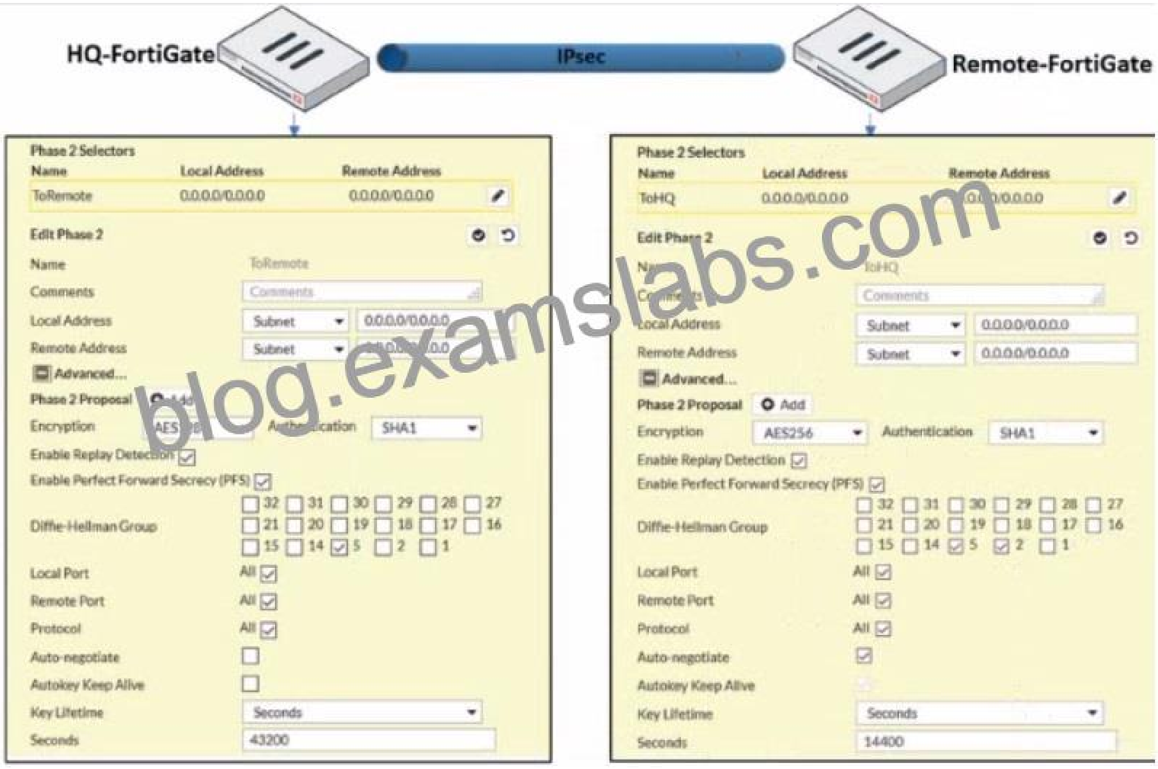
Topology last updated 8 second(s) ago

Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)
* There are five devices that are part of the security fabric.
* Device detection is disabled on all FortiGate devices.
* This security fabric topology is a logical topology view.
* There are 19 security recommendations for the security fabric.
Reference:

https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results

https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology

NO.59 Refer to the exhibit.



HQ-FortiGate

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToRemote
Comments: Comments
Local Address: Subnet 0.0.0.0/0.0.0.0
Remote Address: Subnet 0.0.0.0/0.0.0.0
Advanced...
Phase 2 Proposal: Add
Encryption: AES[illegible] Authentication: SHA1
Enable Replay Detection ☑
Enable Perfect Forward Secrecy (PFS) ☑
Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 □ 2 □ 1
Local Port: All ☑
Remote Port: All ☑
Protocol: All ☑
Auto-negotiate □
Autokey Keep Alive □
Key Lifetime: Seconds
Seconds: 43200

Remote-FortiGate

Phase 2 Selectors

Name	Local Address	Remote Address
ToHQ	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToHQ
Comments: Comments
Local Address: Subnet 0.0.0.0/0.0.0.0
Remote Address: Subnet 0.0.0.0/0.0.0.0
Advanced...
Phase 2 Proposal: Add
Encryption: AES256 Authentication: SHA1
Enable Replay Detection ☑
Enable Perfect Forward Secrecy (PFS) ☑
Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 ☑ 2 □ 1
Local Port: All ☑
Remote Port: All ☑
Protocol: All ☑
Auto-negotiate ☑
Autokey Keep Alive □
Key Lifetime: Seconds
Seconds: 14400

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?
* On HQ-FortiGate, enable Auto-negotiate.
* On Remote-FortiGate, set Seconds to 43200.
* On HQ-FortiGate, enable Diffie-Hellman Group 2.
* On HQ-FortiGate, set Encryption to AES256.
Reference:

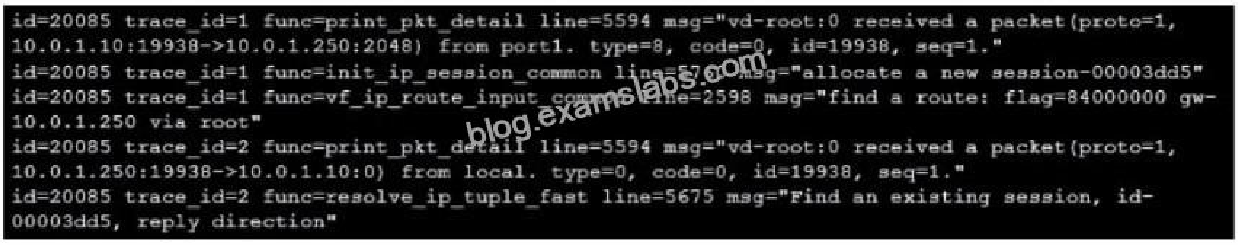
Encryption and authentication algorithm needs to match in order for IPSEC be successfully established.

NO.60 What are two features of collector agent advanced mode? (Choose two.)
* In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
* In advanced mode, security profiles can be applied only to user groups, not individual users.
* Advanced mode uses the Windows convention-NetBios: DomainUsername.
* Advanced mode supports nested or inherited groups.
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): &#8220;Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups.&#8221; &#8220;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.&#8221;

NO.61 Refer to the exhibit showing a debug flow output.



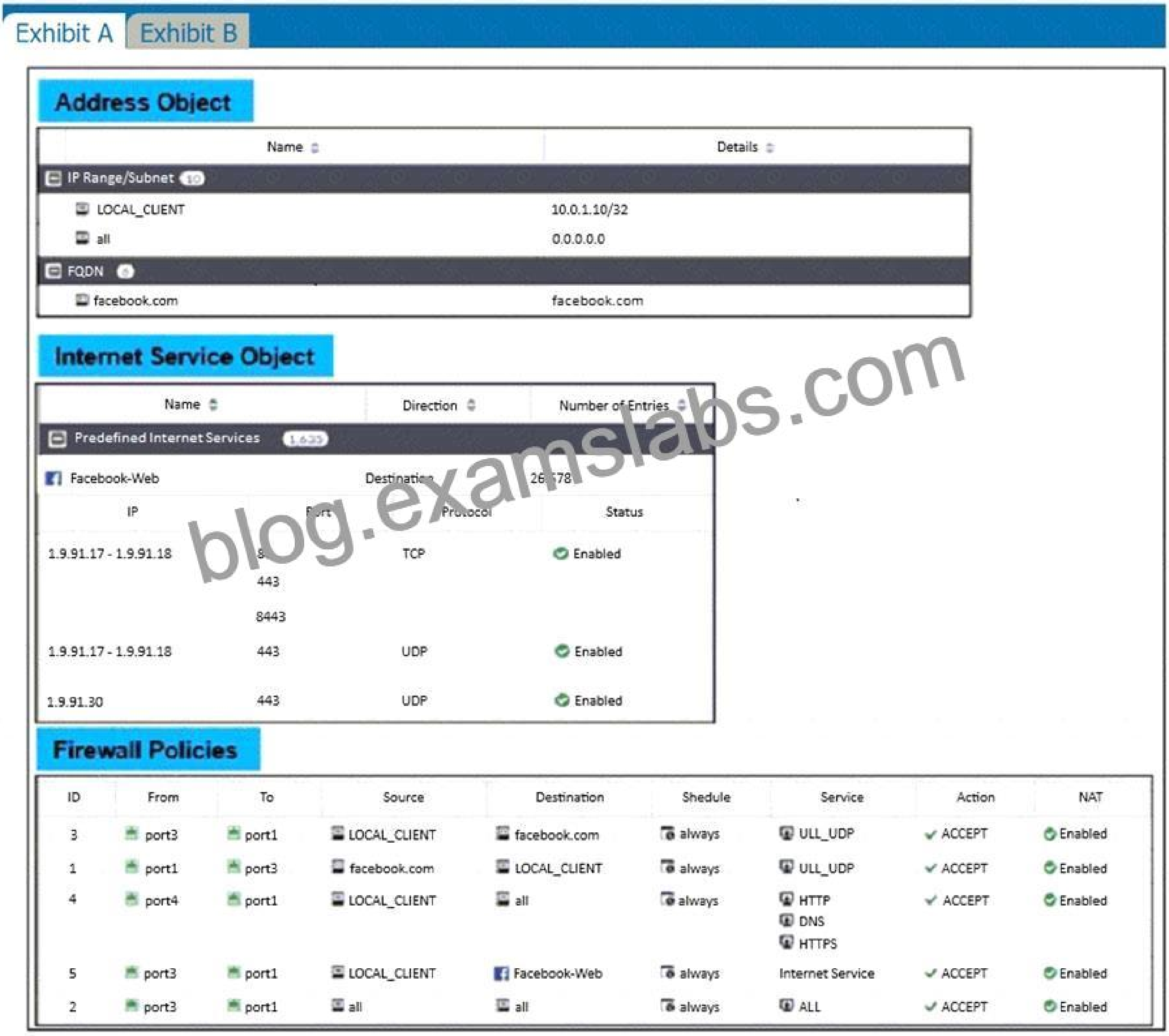
```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)
* The debug flow is of ICMP traffic.
* A firewall policy allowed the connection.
* A new traffic session is created.
* The default route is required to receive a reply.

NO.62 Refer to the exhibits.

The exhibits show the firewall policies and the objects used in the firewall policies.

The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.



Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN 6	
facebook.com	facebook.com

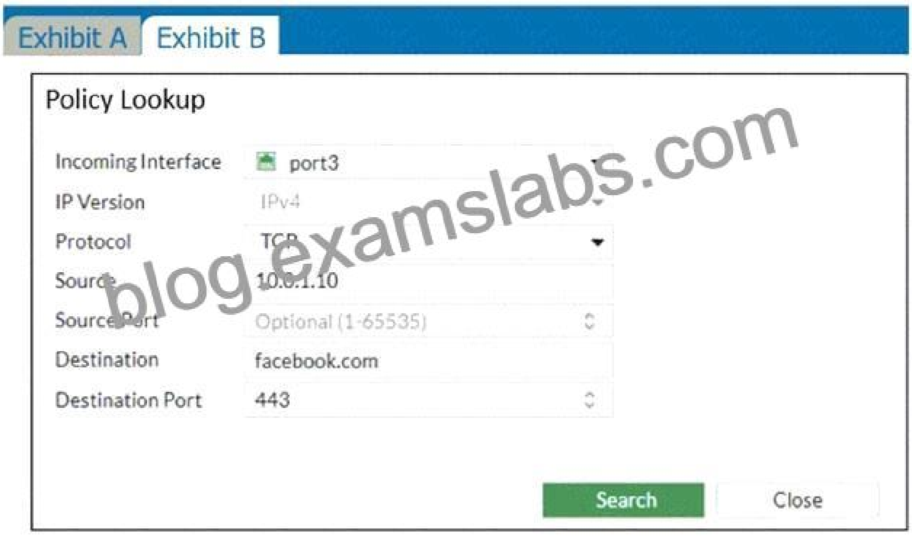
Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1,635		
Facebook-Web	Destination	26578

IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80 443 8443	TCP	Enabled
1.9.91.17 - 1.9.91.18	443	UDP	Enabled
1.9.91.30	443	UDP	Enabled

Firewall Policies

ID	From	To	Source	Destination	Shedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	✓ ACCEPT	Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	✓ ACCEPT	Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	✓ ACCEPT	Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	✓ ACCEPT	Enabled
2	port3	port1	all	all	always	ALL	✓ ACCEPT	Enabled

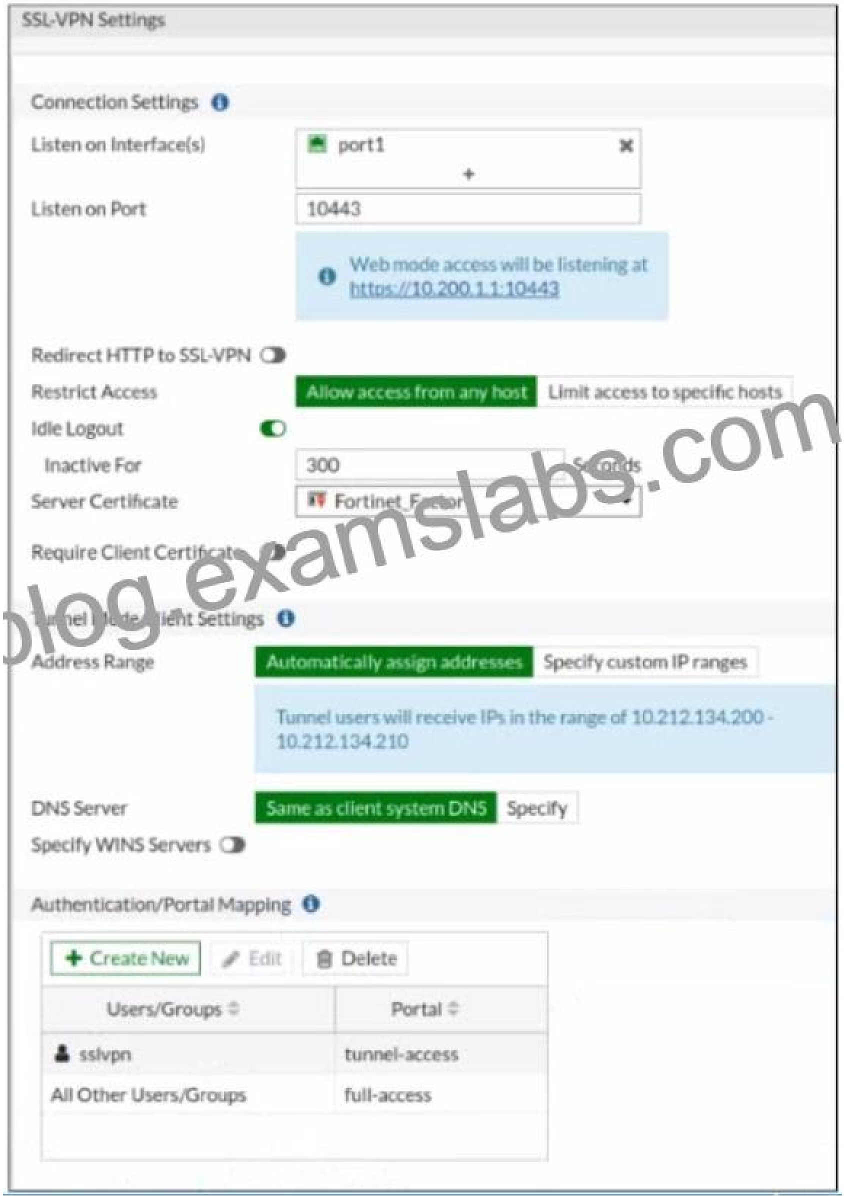


Policy Lookup

Incoming Interface	port3
IP Version	IPv4
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	facebook.com
Destination Port	443

Which policy will be highlighted, based on the input criteria?
* Policy with ID 4.
* Policy with ID 5.
* Policies with ID 2 and 3.
* Policy with ID 4.

NO.63 Refer to the exhibits.



SSL-VPN Settings

Connection Settings

Listen on Interface(s): port1

Listen on Port: 10443

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

Redirect HTTP to SSL-VPN: ○

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

Idle Logout: ●

Inactive For: 300 Seconds

Server Certificate: Fortinet_Factory

Require Client Certificate: ○

Tunnel Mode Client Settings

Address Range: [✓ Automatically assign addresses] Specify custom IP ranges

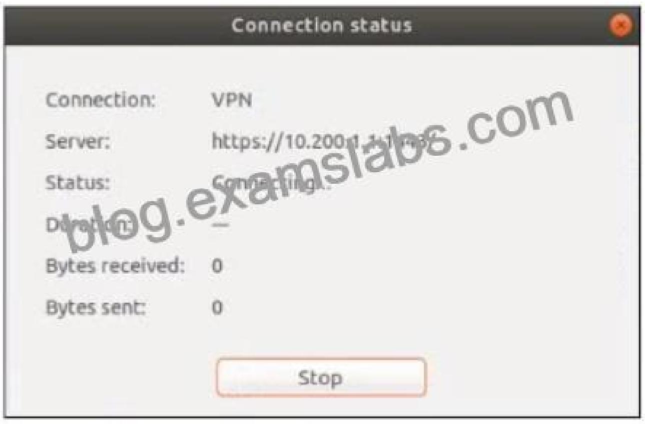
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server: [✓ Same as client system DNS] Specify

Specify WINS Servers: ○

Authentication/Portal Mapping

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



Connection: VPN
Server: https://10.200.1.1:443
Status: Connecting...
Duration: —
Bytes received: 0
Bytes sent: 0

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?
* Change the SSL VPN port on the client.
* Change the Server IP address.
* Change the idle-timeout.
* Change the SSL VPN portal to the tunnel.

NO.64 An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSL/TLS connection.

Which FortiGate configuration can achieve this goal?
* SSL VPN bookmark
* SSL VPN tunnel
* Zero trust network access
* SSL VPN quick connection

FortiGate Infrastructure 7.2 Study Guide (p.198): &#8220;Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as fortissl to the user&#8217;s PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated. The main advantage of tunnel mode over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel.&#8221; An SSL VPN tunnel allows remote users to establish a secure and encrypted Virtual Private Network (VPN) connection to the private network using the SSL/TLS protocol1. An SSL VPN tunnel can provide access to network resources such as FTP servers, as well as external applications running on the user&#8217;s PC1.

An SSL VPN bookmark is a web link that provides access to network resources through the SSL VPN web portal1. It does not support external applications running on the user&#8217;s PC.

Zero trust network access (ZTNA) is a security model that provides role-based application access to remote users without exposing the private network to the internet2. It does not use SSL/TLS protocol, but rather a proprietary ZTNA protocol.

SSL VPN quick connection is a feature that allows users to connect to an SSL VPN tunnel without installing FortiClient or any other software on their PC3. It requires a web browser that supports Java or ActiveX. It does not support external applications running on the user&#8217;s PC.

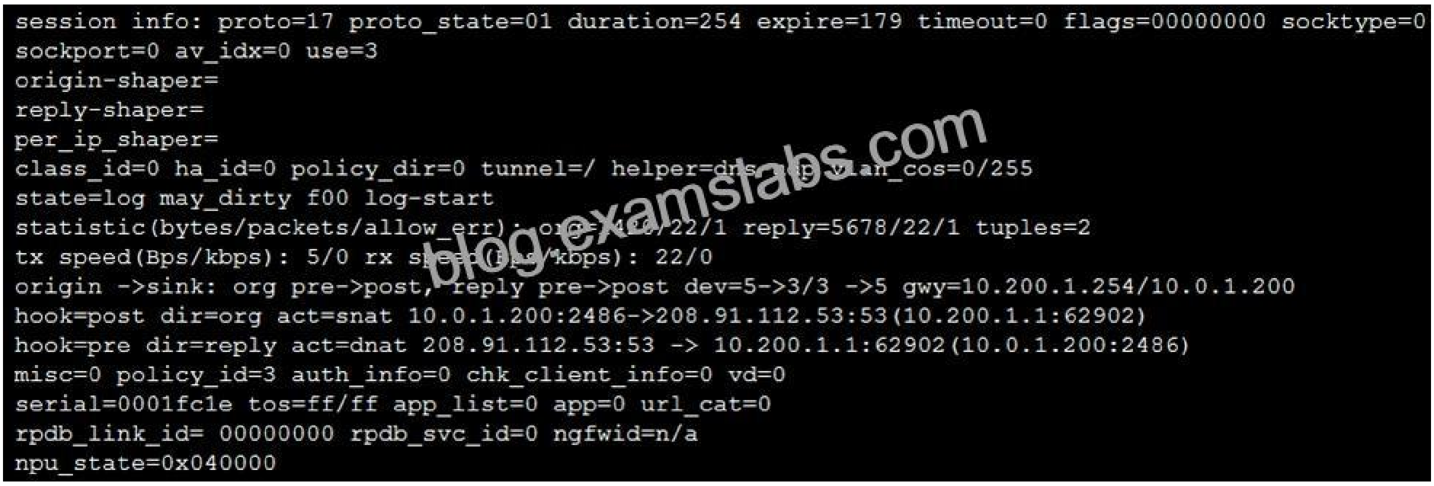
NO.65 Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)
* FortiGate points the collector agent to use a remote LDAP server.
* FortiGate uses the AD server as the collector agent.

* FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
* FortiGate queries AD by using the LDAP to retrieve user group information.
Explanation

Fortigate Infrastructure 7.0 Study Guide P.272-273

https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

NO.66 Refer to the exhibit, which contains a session diagnostic output.



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

Which statement is true about the session diagnostic output?
* The session is a UDP unidirectional state.
* The session is in TCP ESTABLISHED state.
* The session is a bidirectional UDP connection.
* The session is a bidirectional TCP connection.
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

NO.67 An administrator wants to simplify remote access without asking users to provide user credentials.

Which access control method provides this solution?
* ZTNA IP/MAC filtering mode
* ZTNA access proxy
* SSL VPN
* L2TP
FortiGate Infrastructure 7.2 Study Guide (p.165): &#8220;ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs.&#8221; This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials. ZTNA access proxy uses a secure tunnel between the user&#8217;s device and the FortiGate, and authenticates the user based on device identity and context. The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile. This simplifies remote access and enhances security by reducing the attack surface12

Get Special Discount Offer of NSE4_FGT-7.2 Certification Exam Sample Questions and Answers: https://www.examslabs.com/Fortinet/Fortinet-NSE-4/best-NSE4_FGT-7.2-exam-dumps.html]