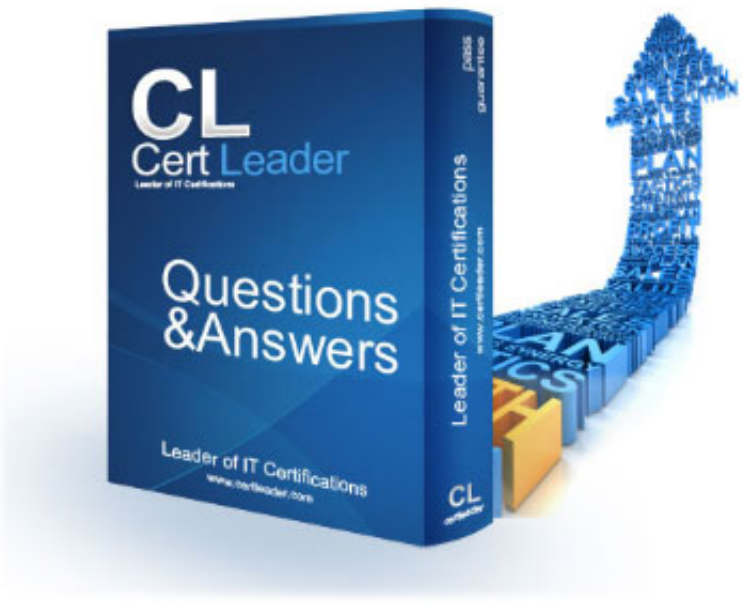
NSE4_FGT-6.4 Dumps

Fortinet NSE 4 - FortiOS 6.4

https://www.certleader.com/NSE4_FGT-6.4-dumps.html

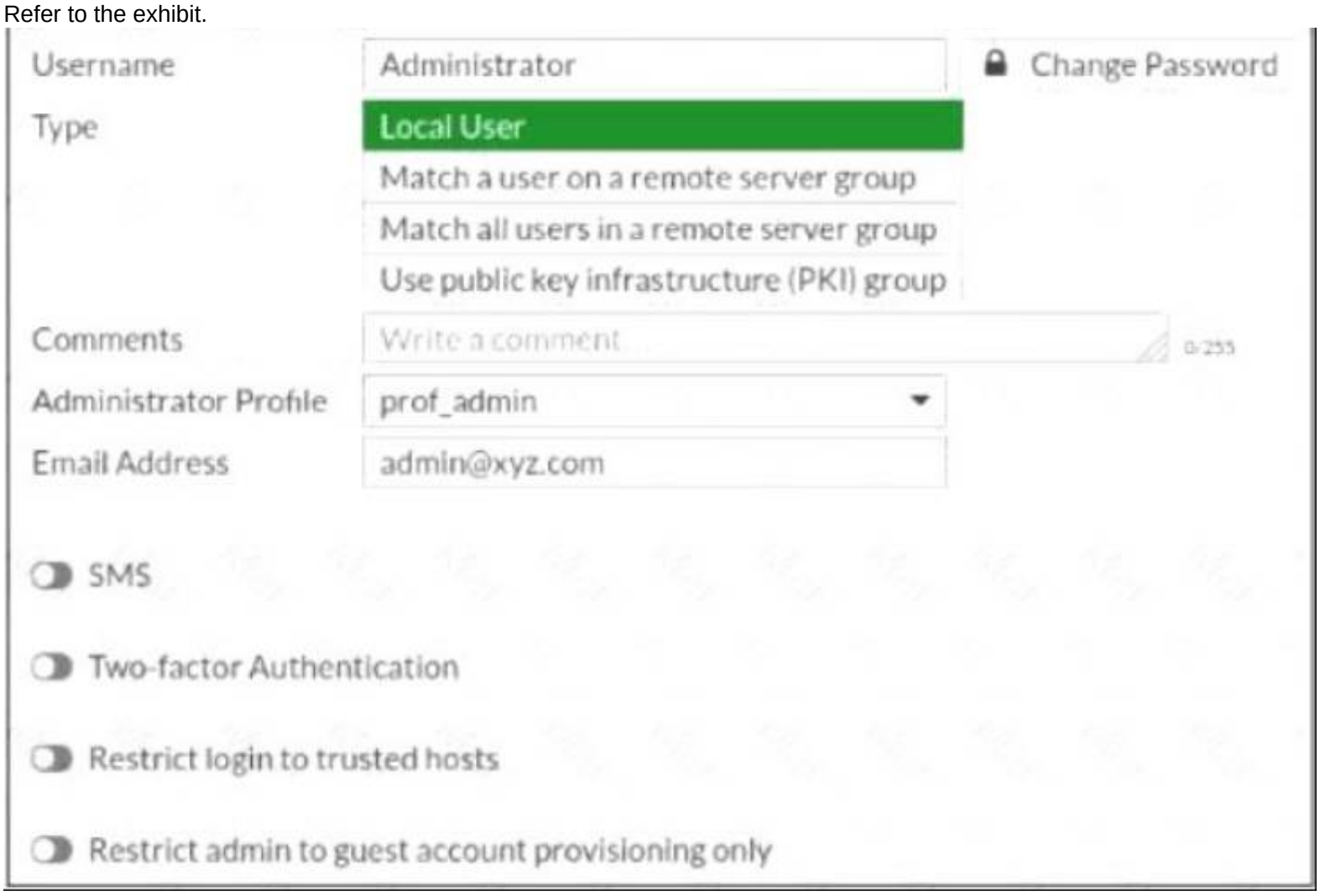


NEW QUESTION 1
Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
C. Virtual IP addresses are used to distinguish between cluster members.
D. The primary device in the clusteris always assigned IP address 169.254.0.1.

Answer: AB

NEW QUESTION 2
Refer to the exhibit.



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: D

NEW QUESTION 3
Which two statements ate true about the Security Fabric rating? (Choose two.)

A. It provides executive summaries of the four largest areas of security focus.
B. Many of the security issues can befixed immediately by click ng Apply where available.
C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
D. The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.

Answer: AC

NEW QUESTION 4
Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
B. An SA never expires.
C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
D. Phase 2 SA expiration can be time-based, volume-based, or both.
E. Both the phase 1 SA and phase 2 SA are bidirectional.

Answer: BCD

NEW QUESTION 5
NGFW mode allows policy-based configuration for most inspection rules. Which security profile’s configuration does not change when you enable policy-based inspection?

A. Web filtering
B. Antivirus
C. Web proxy
D. Application control

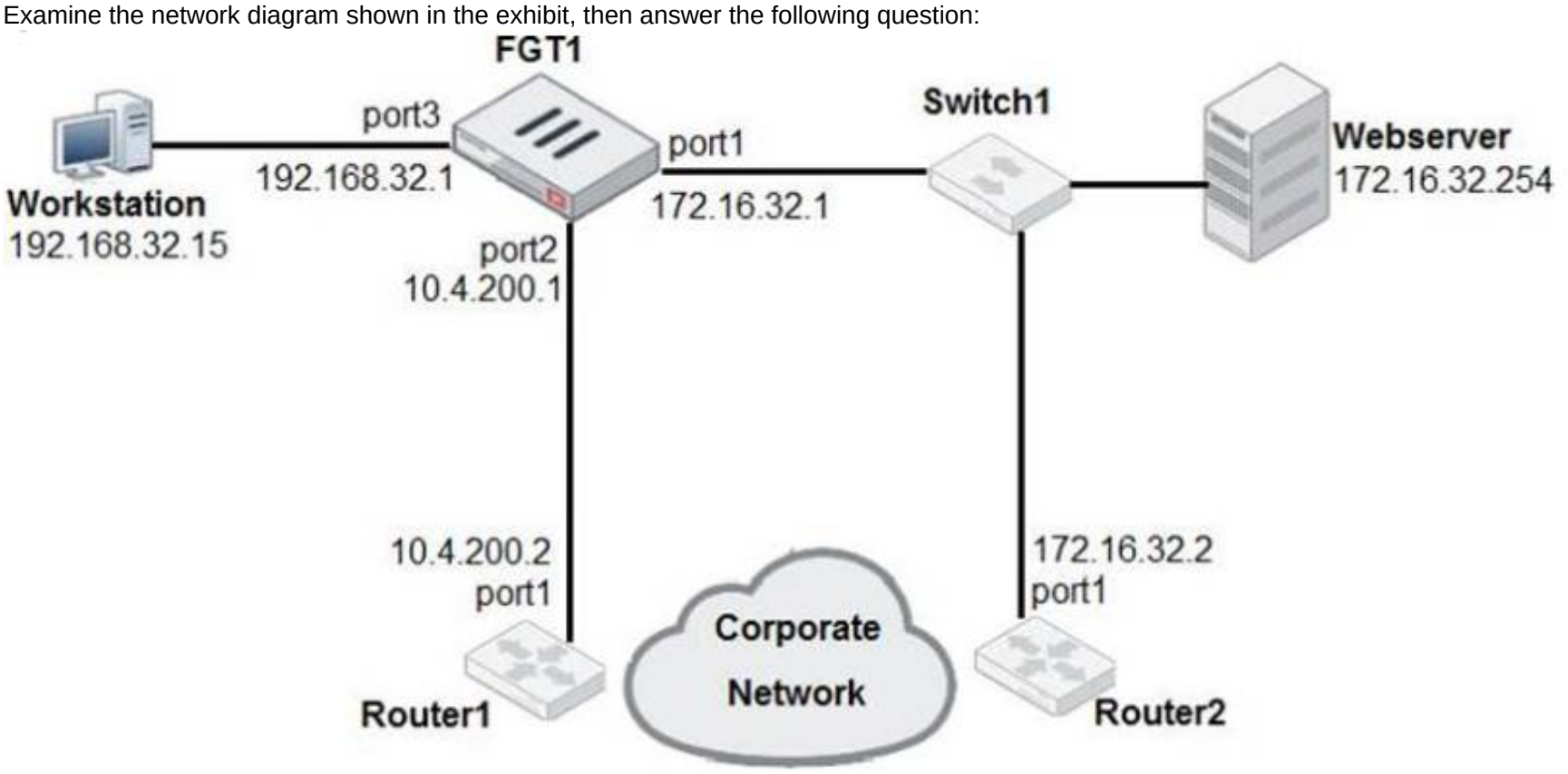
Answer: B

NEW QUESTION 6
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 7
Examine the network diagram shown in the exhibit, then answer the following question:



Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?

A. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
B. 0.0.0.0/0 [20/0] via 10.4.200.2, port2
C. 10.4.200.0/30 is directly connected, port2
D. 172.16.32.0/24 is directly connected, port1

Answer: D

NEW QUESTION 8
An administrator Is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A. the local quick mode selector is 192.160.1.0/24 and the remote quick mode selector is 192.168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

A. 192.168.1.0/24
B. 192.168.0.0/24
C. 192.168.2.0/24
D. 192.168.3.0/24

Answer: B

NEW QUESTION 9
Which three statements about a flow-based antivirus profile are correct? (Choose three.)

A. IPS engine handles the process as a standalone.
B. FortiGate buffers the whole file but transmits to the client simultaneously.
C. If the virus is detected, the last packet is delivered to the client.
D. Optimized performance compared to proxy-based inspection.
E. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

Answer: CDE

NEW QUESTION 10
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

Answer: AD

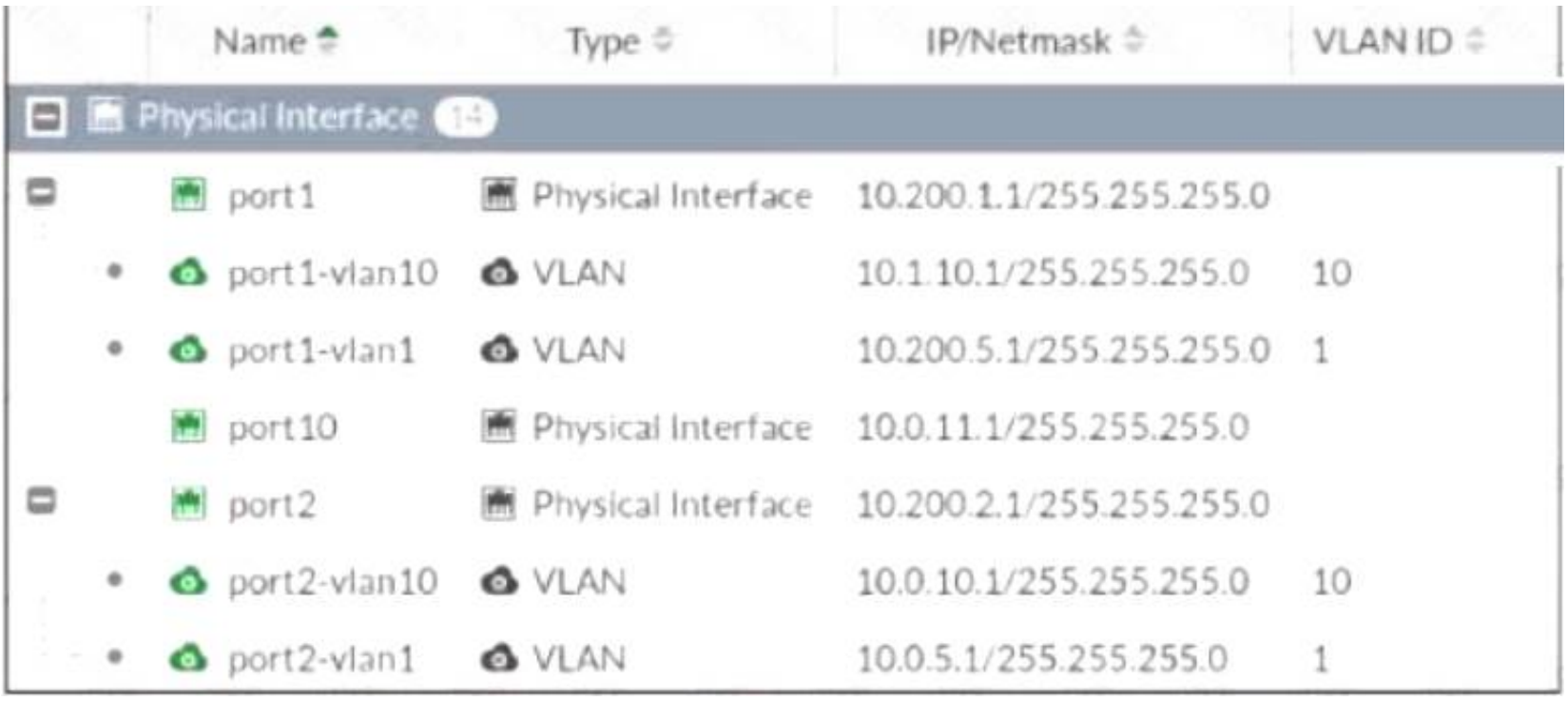
NEW QUESTION 10
Refer to the exhibit.

Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. This security fabric topology is a logical topology view.
B. There are 19 security recommendations for the security fabric.
C. There are five devices that are part of the security fabric.
D. Device detection is disabled on all FortiGate devices.

Answer: AD

NEW QUESTION 13
Refer to the exhibit.



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

A. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs
B. port1 is a native VLAN.
C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
D. Traffic between port2 and port2-vlan1 is allowed by default.

Answer: CD

NEW QUESTION 15
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.

Answer: BD

NEW QUESTION 18
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: B

NEW QUESTION 21
Which of statement is true about SSL VPN web mode?

A. The tunnel is up while the client is connected.
B. It supports a limited number of protocols.
C. The external network application sends data through the VPN.
D. It assigns a virtual IP address to the client.

Answer: C

NEW QUESTION 24
By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which two CLI commands will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering? (Choose two.)

A. set fortiguard anycast disable
B. set protocol udp
C. set webfilter-force-off disable
D. set webfilter-cache disable

Answer: AC

NEW QUESTION 27
Examine this output from a debug flow:

```
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 the FortiGate drop the packet?

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

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=13900

NEW QUESTION 32
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: A

NEW QUESTION 37
Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

A. The public key of the web servercertificate must be installed on the browser.
B. The web-server certificate must be installed on the browser.
C. The CA certificate that signed the web-server certificate must be installed on the browser.
D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Answer: C

NEW QUESTION 39
Which type of logs on FortiGate record information about traffic directly to and from the FortiGate management IP addresses?

A. System event logs
B. Forward traffic logs
C. Local traffic logs
D. Security logs

Answer: A

NEW QUESTION 42
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 43
An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.
B. This VPN cannot be used as part of a hub-and-spoke topology.
C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
D. The IPsec firewall policies must be placed at the top of the list.

Answer: C

Explanation:
In a route-based configuration, FortiGate automatically adds a virtual interface eith the VPN name (Infrastructure Study Guide, 206)

NEW QUESTION 46
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The collector agent must search security event logs.
D. The NetSessionEnum functionis user] to track user logouts.

Answer: A

NEW QUESTION 49
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 tunnelfailover
Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

A. Enable Dead Peer Detection.
B. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
C. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the state route for the secondary tunnel.

Answer: A

NEW QUESTION 50
How do you format the FortiGate flash disk?

A. Load a debug FortiOS image.
B. Load the hardware test (HQIP) image.
C. Execute the CLI command execute formatlogdisk.
D. Select the format boot device option from the BIOS menu.

Answer: D

NEW QUESTION 53

Refer to the exhibit.

```
STUDENT # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT       DESTINATION      DESTINATION-NAT
tcp     3598   10.0.1.10:2706  10.200.1.6:2706  10.200.1.254:80  -
tcp     3598   10.0.1.10:2704  10.200.1.6:2704  10.200.1.254:80  -
tcp     3596   10.0.1.10:2702  10.200.1.6:2702  10.200.1.254:80  -
tcp     3599   10.0.1.10:2700  10.200.1.6:2700  10.200.1.254:443 -
tcp     3599   10.0.1.10:2698  10.200.1.6:2698  10.200.1.254:80  -
tcp     3598   10.0.1.10:2696  10.200.1.6:2696  10.200.1.254:443 -
udp     174    10.0.1.10:2694  -                  10.0.1.254:53  -
udp     173    10.0.1.10:2690  -                  10.0.1.254:53  -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

A. Destination NAT is disabled in the firewall policy.
B. One-to-one NAT IP pool is used in the firewall policy.
C. Overload NAT IP pool is used in the firewall policy.
D. Port block allocation IP pool is used in the firewall policy.

Answer: A

NEW QUESTION 54
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 58
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 60
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 62
Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeou
B. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source IP.
C. It is a hard timeou
D. The FortiGate removes the temporary policy for a user’s source IP address after this timer has expired.
E. It is an idle timeou
F. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source MAC.
G. It is a hard timeou
H. The FortiGate removes the temporary policy for a user’s source MAC address after this timer has expired.

Answer: A

NEW QUESTION 67
An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?

A. A.-192.168.3.0/24B.192.168.2.0/24C.192.168.1.0/24D.192.168.0.0/8

Answer: B

NEW QUESTION 71
What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scope of application control to the browser-based technology category only.
B. It limits the scope of application control to scan application traffic based on application category only.
C. It limits the scope of application control to scan application traffic using parent signatures only
D. It limits the scope of application control to scan application traffic on DNS protocol only.

Answer: B

NEW QUESTION 76
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

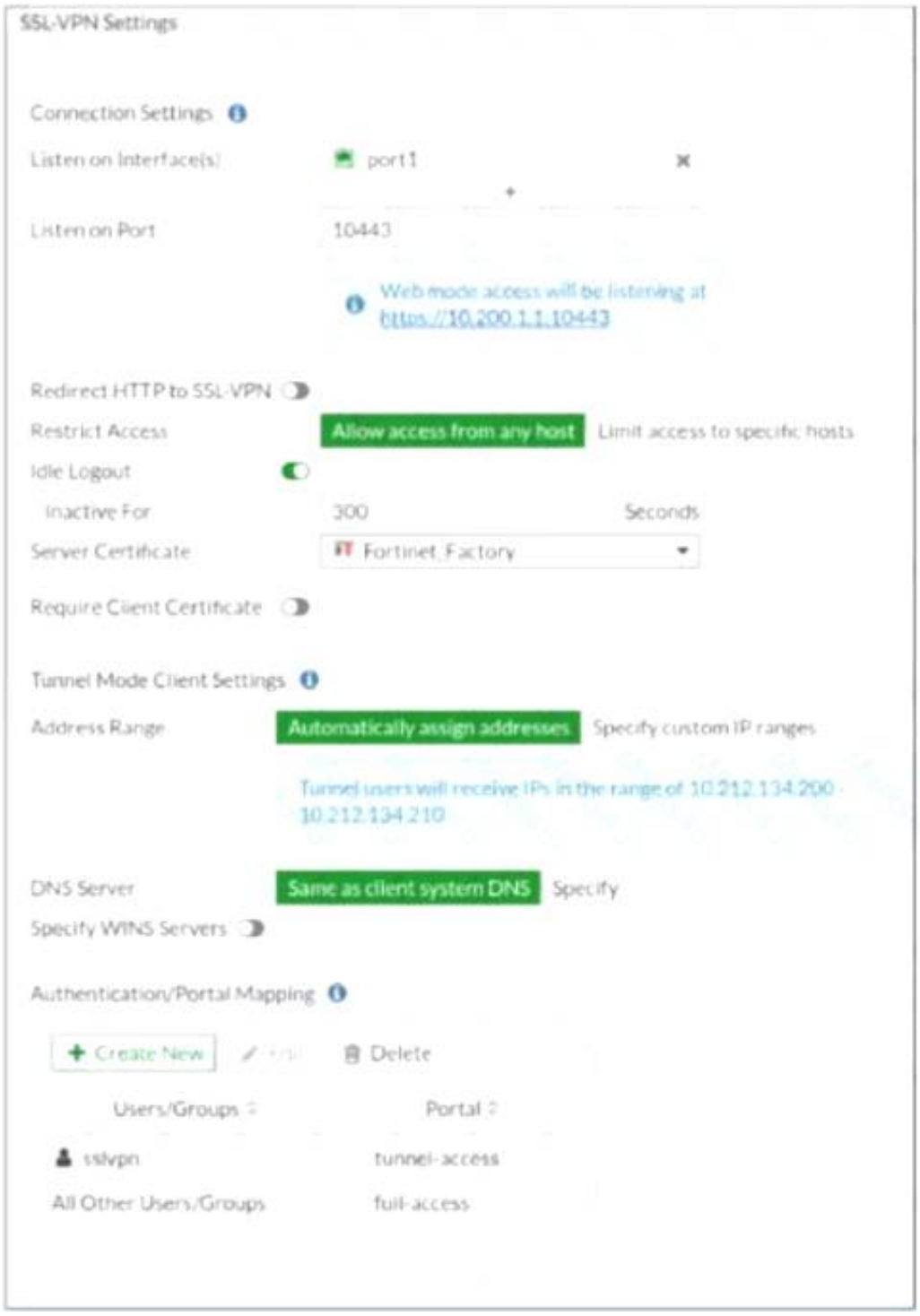
NEW QUESTION 77
Refer to the exhibit.

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

Answer: D

NEW QUESTION 82
Refer to the exhibits.



The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.
B. Change the Server IP address.
C. Change the idle-timeout.
D. Change the SSL VPN portal to the tunnel.

Answer: D

NEW QUESTION 86
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 91
Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

A. This is known as many-to-one NAT.
B. Source IP is translated to the outgoing interface IP.
C. Connections are tracked using source port and source MAC address.
D. Port address translation is not used.

Answer: AB

NEW QUESTION 93
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time
B. FortiGuaid update servers
C. Operating mode
D. NGFW mode

Answer: AD

NEW QUESTION 95
Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

A. hard-timeout
B. auth-on-demand
C. soft-timeout
D. new-session
E. Idle-timeout

Answer: ADE

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

NEW QUESTION 100
Which of the following SD-WAN load –balancing method use interface weight value to distribute traffic? (Choose two.)

A. Source IP
B. Spillover
C. Volume
D. Session

Answer: CD

NEW QUESTION 103
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 Interfac
C. Outgoing Interfac
D. Schedule, and Service fields can be shared with both IPv4and 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: ACE

NEW QUESTION 104
Refer to the exhibit.

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: B

NEW QUESTION 107
An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.
B. The interface is a member of a virtual wire pair.
C. The operation mode is transparent.
D. The interface is a member of a zone.
E. Captive portal is enabled in the interface.

Answer: ABC

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

NEW QUESTION 111
Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

A. Subject Key Identifiervalue
B. SMMIE Capabilitiesvalue
C. Subjectvalue
D. Subject Alternative Namevalue

Answer: C

NEW QUESTION 113
.....

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-6.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4_FGT-6.4-dumps.html