NSE4 Dumps

Fortinet Network Security Expert 4 Written Exam (400)

https://www.certleader.com/NSE4-dumps.html

NEW QUESTION 1
Review the exhibit of an explicit proxy policy configuration.

If there is a proxy connection attempt coming from the IP address 10.0.1.5, and from a user that has not authenticated yet, what action does the FortiGate proxy take?

A. User is prompted to authenticat
B. Traffic from the user Student will be allowed by the policy #1. Traffic from any other user will be allowed by the policy #2.
C. User is not prompted to authenticat
D. The connection is allowed by the proxy policy #2.
E. User is not prompted to authenticat
F. The connection will be allowed by the proxy policy #1.
G. User is prompted to authenticat
H. Only traffic from the user Student will be allowe
I. Traffic from any other user will be blocked.

Answer: D

NEW QUESTION 2
Which of the following statements are true regarding DLP File Type Filtering? (Choose two.)

A. Filters based on file extension
B. Filters based on fingerprints
C. Filters based on file content
D. File types are hard coded in the FortiOS

Answer: BC

NEW QUESTION 3
Which of the following settings can be configured per VDOM? (Choose three)

A. Operating mode (NAT/route or transparent)
B. Static routes
C. Hostname
D. System time
E. Firewall Policies

Answer: ABE

NEW QUESTION 4
Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

A. SSH
B. Telnet
C. NTLM
D. HTTPS

Answer: AD

NEW QUESTION 5
Examine the exhibit; then answer the question below.

The Vancouver FortiGate initially had the following information in its routing table:
S 172.20.0.0/16 [10/0] via 172.21.1.2, port2
C 172.21.0.0/16 is directly connected, port2
C 172.11.11.0/24 is directly connected, port1
Afterwards, the following static route was added:
config router static edit 6
set dst 172.20.1.0 255.255.255.0
set priority 0
set device port1

set gateway 172.11.12.1 next
Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allow-subnet-overlap first.
B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.
C. The priority is 0, which means that the route will remain inactive.
D. The static route configuration is missing the distance setting.

Answer: B

NEW QUESTION 6
A new version of FortiOS firmware has just been released. When you upload new firmware, which is true?

A. If you upload the firmware image via the boot loader's menu from a TFTP server, it will not preserve the configuratio
B. But if you upload new firmware via the GUI or CLI, as long as you are following a supported upgrade path, FortiOS will attempt to convert the existing configuration to be valid with any new or changed syntax.
C. No settings are preserve
D. You must completely reconfigure.
E. No settings are preserve
F. After the upgrade, you must upload a configuration backup fil
G. FortiOS will ignore any commands that are not valid in the new O
H. In those cases, you must reconfigure settings that are not compatible with the new firmware.
I. You must use FortiConverter to convert a backup configuration file into the syntax required by the new FortiOS, then upload it to FortiGate.

Answer: A

NEW QUESTION 7
Which statement best describes what the FortiGate hardware acceleration processors main
task is?

A. Offload traffic processing tasks from the main CPU.
B. Offload management tasks from the main CPU.
C. Compress and optimize the network traffic.
D. Increase maximum bandwidth available in a FortiGate interface.

Answer: A

NEW QUESTION 8
Review to the network topology in the exhibit.

The workstation, 172.16.1.1/24, connects to port2 of the FortiGate device, and the ISP router, 172.16.1.2, connects to port1. Without changing IP addressing, which configuration changes are required to properly forward users traffic to the Internet? (Choose two)

A. At least one firewall policy from port2 to port1 to allow outgoing traffic.
B. A default route configured in the FortiGuard devices pointing to the ISP's router.
C. Static or dynamic IP addresses in both ForitGate interfaces port1 and port2.
D. The FortiGate devices configured in transparent mode.

Answer: AD

NEW QUESTION 9
Which statements are correct for port pairing and forwarding domains? (Choose two.)

A. They both create separate broadcast domains.
B. Port Pairing works only for physical interfaces.
C. Forwarding Domain only applies to virtual interfaces
D. They may contain physical and/or virtual interfaces.

Answer: AD

NEW QUESTION 10
A user logs into a SSL VPN portal and activates the tunnel mode. The exhibit shows the firewall policy and the user's SSL VPN portal configuration:
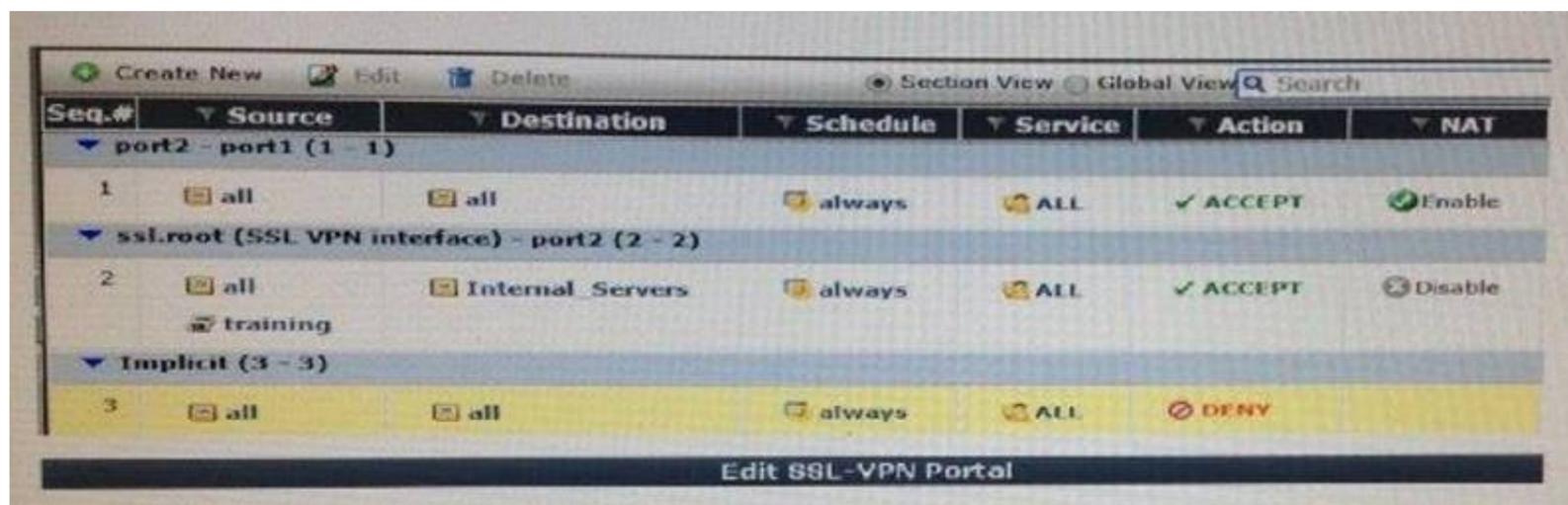
Given that the user authenticates against the SSL VPN policy shown in the image below, which statement below identifies the route that is added to the client's routing table.

A. A route to a destination subnet matching the Internal_Servers address object.
B. A route to the destination subnet configured in the tunnel mode widget.
C. A default route.
D. A route to the destination subnet configured in the SSL VPN global settings.

Answer: A

NEW QUESTION 10
A FortiGate is configured with the 1.1.1.1/24 address on the wan2 interface and HTTPS Administrative Access, using the default tcp port, is enabled for that interface. Given the SSL VPN settings in the exhibit.
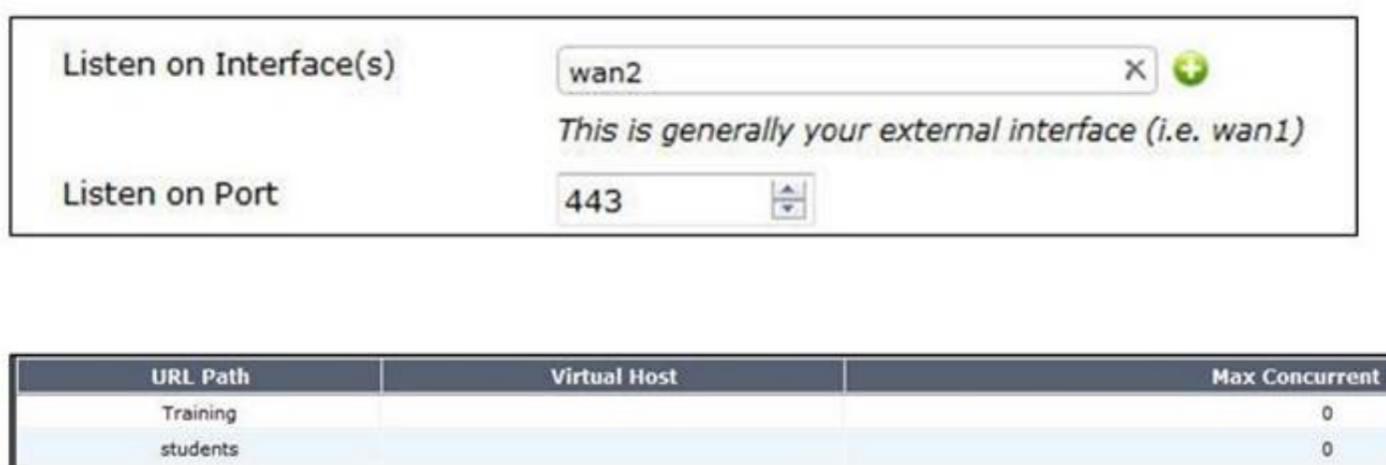
Which of the following SSL VPN login portal URLs are valid? (Choose two.)

A. http://1.1.1.1:443/Training
B. https://1.1.1.1:443/STUDENTS
C. https://1.1.1.1/login
D. https://1.1.1.1/

Answer: BD

NEW QUESTION 15
Which two statements are true regarding firewall policy disclaimers? (Choose two.)

A. They cannot be used in combination with user authentication.
B. They can only be applied to wireless interfaces.
C. Users must accept the disclaimer to continue.
D. The disclaimer page is customizable.

Answer: CD

NEW QUESTION 16
Which of the following fields contained in the IP/TCP/UDP headers can be used to make a routing decision when using policy-based routing? (Choose three)

A. Source IP address.
B. TCP flags
C. Source TCP/UDP ports
D. Type of service.
E. Checksum

Answer: ACD

NEW QUESTION 18
Which of the following protocols are defined in the IPsec Standard? (Choose two)

A. AH
B. GRE

C. SSL/TLS
D. ESP

Answer: AD

NEW QUESTION 22
Which of the following statements are true regarding application control? (Choose two.)

A. Application control is based on TCP destination port numbers.
B. Application control is proxy based.
C. Encrypted traffic can be identified by application control.
D. Traffic shaping can be applied to the detected application traffic.

Answer: CD

NEW QUESTION 24
Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

A. More than one proxy is supported.
B. Can contain a list of destinations that will be exempt from the use of any proxy.
C. Can contain a list of URLs that will be exempted from the FortiGate web filtering inspection.
D. Can contain a list of users that will be exempted from the use of any proxy.

Answer: BC

NEW QUESTION 26
For data leak prevention, which statement describes the difference between the block and quarantine actions?

A. A block action prevents the transactio
B. A quarantine action blocks all future transactions, regardless of the protocol.
C. A block action prevents the transactio
D. A quarantine action archives the data.
E. A block action has a finite duratio
F. A quarantine action must be removed by an administrator.
G. A block action is used for known user
H. A quarantine action is used for unknown users.

Answer: A

NEW QUESTION 29
Which statements are true regarding local user authentication? (Choose two.)

A. Two-factor authentication can be enabled on a per user basis.
B. Local users are for administration accounts only and cannot be used to authenticate network users.
C. Administrators can create the user accounts in a remote server and store the user passwords locally in the FortiGate.
D. Both the usernames and passwords can be stored locally on the FortiGate.

Answer: AD

NEW QUESTION 32
Which of the following authentication methods can be used for SSL VPN authentication? (Choose three.)

A. Remote Password Authentication (RADIUS, LDAP)
B. Two-Factor Authentication
C. Local Password Authentication
D. FSSO
E. RSSO

Answer: ABC

NEW QUESTION 36
What log type would indicate whether a VPN is going up or down?

A. Event log
B. Security log
C. Forward log
D. Syslog

Answer: A

NEW QUESTION 39
Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

A. Proxy-based.
B. DNS-based.

C. Flow-based.
D. Man-in-the-middle.

Answer: C

NEW QUESTION 43
How do application control signatures update on a FortiGate device?

A. Through FortiGuard updates.
B. Upgrade the FortiOS firmware to a newer release.
C. By running the Application Control auto-learning feature.
D. Signatures are hard coded to the device and cannot be updated.

Answer: A

NEW QUESTION 45
Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit below.

Which statements are correct regarding this output (Choose two.)

A. The connecting client has been allocated address 172.20.1.1.
B. In the Phase 1 settings, dead peer detection is enabled.
C. The tunnel is idle.
D. The connecting client has been allocated address 10.200.3.1.

Answer: AB

NEW QUESTION 47
You are creating a custom signature. Which has incorrect syntax?

A. F-SBID(--attack_id 1842,--name "Ping.Death";--protocol icmp; --data_size>32000;)
B. F-SBID(--name "Block.SMTP.VRFY.CMD";--pattern "vrfy";-- service SMTP; --no_case;-- context header;)
C. F-SBID(--name "Ping.Death";--protocol icmp;--data_size>32000;)
D. F-SBID(--name "Block".HTTP.POST"; --protocol tcp;-- service HTTP;-- flow from_client;--pattern "POST"; -- context uri;--within 5,context;)

Answer: A

NEW QUESTION 51
When an administrator attempts to manage FortiGate from an IP address that is not a trusted host, what happens?

A. FortiGate will still subject that person's traffic to firewall policies; it will not bypass them.
B. FortiGate will drop the packets and not respond.
C. FortiGate responds with a block message, indicating that it will not allow that person to log in.
D. FortiGate responds only if the administrator uses a secure protoco
E. Otherwise, it does not respond

Answer: B

NEW QUESTION 54
A FortiGate unit has multiple VDOMs in NAT/route mode with multiple VLAN interfaces in each VDOM. Which of the following statements is correct regarding the IP addresses
assigned to each VLAN interface?

A. Different VLANs can share the same IP address as long as they have different VLAN IDs.
B. Different VLANs can share the same IP address as long as they are in different physical interface.
C. Different VLANs can share the same IP address as long as they are in different VDOMs.
D. Different VLANs can never share the same IP addresses.

Answer: C

NEW QUESTION 56

In "diag debug flow" output, you see the message "Allowed by Policy-1: SNAT". Which is true?

A. The packet matched the topmost policy in the list of firewall policies.
B. The packet matched the firewall policy whose policy ID is 1.
C. The packet matched a firewall policy, which allows the packet and skips UTM checks
D. The policy allowed the packet and applied session NAT.

Answer: B

NEW QUESTION 57
Which is not a FortiGate feature?

A. Database auditing
B. Intrusion prevention
C. Web filtering
D. Application control

Answer: A

NEW QUESTION 61
What attributes are always included in a log header? (Choose three.)

A. policyid
B. level
C. user
D. time
E. subtype
F. duration

Answer: BDE

NEW QUESTION 66
Which of the following statements best describes what a Certificate Signing Request (CSR) is?

A. A message sent by the Certificate Authority (CA) that contains a signed digital certificate.
B. An enquiry submitted to a Certificate Authority (CA) to request a root CA certificate
C. An enquiry submitted to a Certificate Authority (CA) to request a signed digital certificate
D. An enquiry submitted to a Certificate Authority (CA) to request a Certificate Revocation List (CRL)

Answer: B

NEW QUESTION 67
A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub-interfaces added to the same physical interface.
Which one of the following statements is correct regarding the VLAN IDs in this scenario?

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 if they are connected to different L2 IEEE 802.1Q compliant switches.

Answer: B

NEW QUESTION 72
Which changes to IPS will reduce resource usage and improve performance? (Choose three)

A. In custom signature, remove unnecessary keywords to reduce how far into the signature tree that FortiGate must compare in order to determine whether the packet matches.
B. In IPS sensors, disable signatures and rate based statistics (anomaly detection) for protocols, applications and traffic directions that are not relevant.
C. In IPS filters, switch from 'Advanced' to 'Basic' to apply only the most essential signatures.
D. In firewall policies where IPS is not needed, disable IPS.
E. In firewall policies where IPS is used, enable session start logs.

Answer: ABD

NEW QUESTION 77
Which of the following actions can be used to back up the keys and digital certificates in a FortiGate device? (Choose two.)

A. Taking a full backup of the FortiGate configuration
B. Uploading a PKCS#10 file to a USB drive
C. Manually uploading the certificate information to a Certificate authority (CA)
D. Uploading a PKCS#12 file to a TFTP server

Answer: AD

NEW QUESTION 82

Which TCP states does the global setting 'tcp-half-open-timer' applies to? (Choose two.)

A. SYN SENT
B. SYN & SYN/ACK
C. FIN WAIT
D. TIME WAIT

Answer: AD

NEW QUESTION 83
Which of the following items does NOT support the Logging feature?

A. File Filter
B. Application control
C. Session timeouts
D. Administrator activities
E. Web URL filtering

Answer: C

NEW QUESTION 84
In transparent mode, forward-domain is a CLI setting associated with .

A. a static route.
B. a firewall policy.
C. an interface.
D. a virtual domain.

Answer: C

NEW QUESTION 88
A backup file begins with this line:
#config-version=FGVM64-5.02-FW-build589-140613:opmode=0:vdom=0:user=admin
#conf_file_ver=3881503152630288414 #buildno=0589 #global_vdom=1
Can you restore it to a FortiWiFi 60D?

A. Yes
B. Yes, but only if you replace the "#conf_file_ver" line so that it contains the serial number of that specific FortiWiFi 60D.
C. Yes, but only if it is running the same version of FortiOS, or a newer compatible version.
D. No

Answer: D

NEW QUESTION 93
Which is the following statement are true regarding application control? (choose two)

A. Application control is based on TCP destination port numbers.
B. Application control is proxy based.
C. Encrypted traffic can be identified by application control.
D. Traffic Shaping can be applied to the detected application traffic.

Answer: CD

NEW QUESTION 97
Which statement best describes the objective of the SYN proxy feature available in SP processors?

A. Accelerate the TCP 3-way handshake
B. Collect statistics regarding traffic sessions
C. Analyze the SYN packet to decide if the new session can be offloaded to the SP processor
D. Protect against SYN flood attacks.

Answer: D

NEW QUESTION 99
Which statement describes what the CLI command diagnose debug authd fsso list is used for?

A. Monitors communications between the FSSO collector agent and FortiGate unit.
B. Displays which users are currently logged on using FSSO.
C. Displays are listing of all connected FSSO collector agents.
D. Lists all DC Agents installed on all domain controllers.

Answer: B

NEW QUESTION 100
Examine the exhibit; then answer the question below.
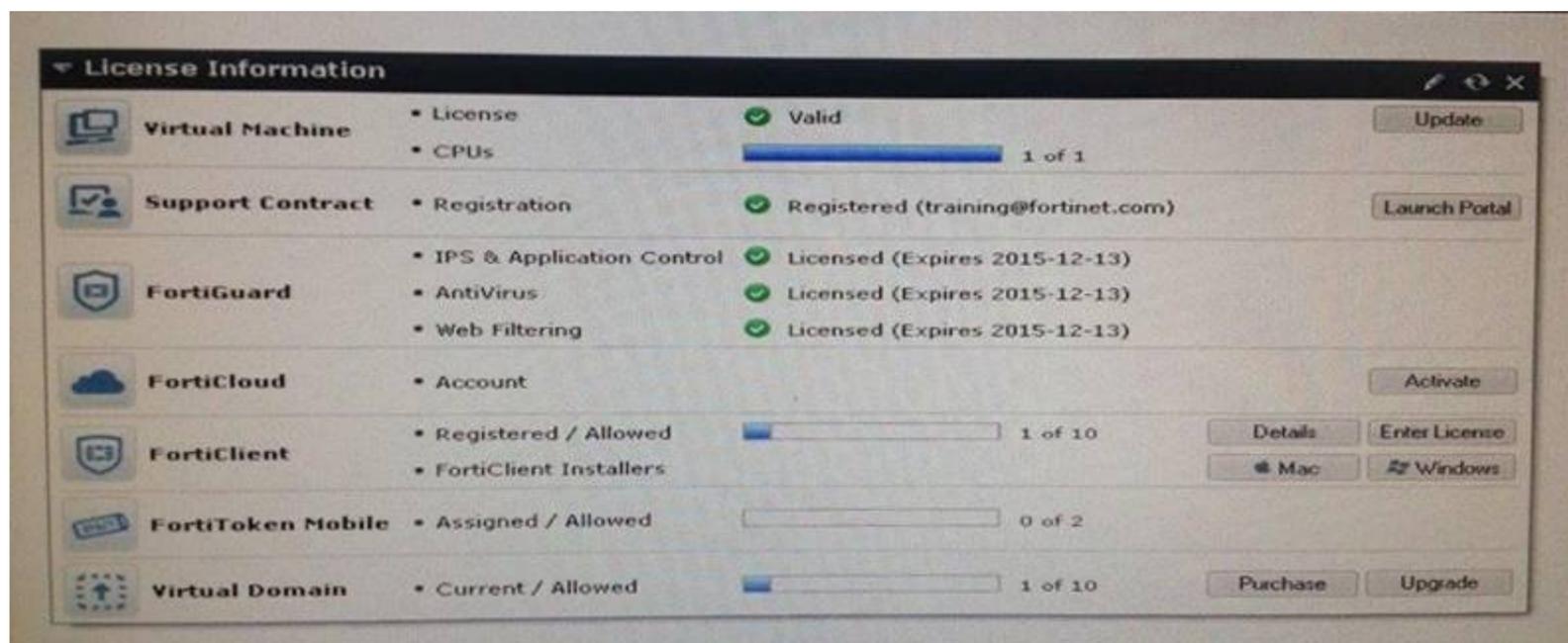
Which statement describes the green status indicators that appear next to the different FortiGuard Distribution Network services as illustrated in the exhibit?

A. They indicate that the FortiGate has the latest updates available from the FortiGuard Distribution Network.
B. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.
C. They indicate that the FortiGate is in the process of downloading updates from the FortiGuard Distribution Network.
D. They indicate that the FortiGate is able to connect to the FortiGuard Distribution Network.

Answer: D

NEW QUESTION 104
Which traffic can match a firewall policy's "Services" setting? (Choose three.)

A. HTTP
B. SSL
C. DNS
D. RSS
E. HTTPS

Answer: ACE

NEW QUESTION 108
A client can create a secure connection to a FortiGate device using SSL VPN in web-only mode. Which one of the following statements is correct regarding the use of web-only mode SSL VPN?

A. Web-only mode supports SSL version 3 only.
B. A Fortinet-supplied plug-in is required on the web client to use web-only mode SSL VPN.
C. Web-only mode requires the user to have a web browser that supports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client to be able to connect to a web-only mode SSL VPN.

Answer: C

NEW QUESTION 110
Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

A. In symmetric cryptography, the keys are publicly availabl
B. In asymmetric cryptography, the keys must be kept secret.
C. Asymmetric cryptography can encrypt data faster than symmetric cryptography
D. Symmetric cryptography uses one pre-shared ke
E. Asymmetric cryptography uses a pair or keys
F. Asymmetric keys can be sent to the remote peer via digital certificate
G. Symmetric keys cannot

Answer: CD

NEW QUESTION 115
Which two statements are true about IPsec VPNs and SSL VPNs? (Choose two.)

A. SSL VPN creates a HTTPS connectio
B. IPsec does not.
C. Both SSL VPNs and IPsec VPNs are standard protocols.
D. Either a SSL VPN or an IPsec VPN can be established between two FortiGate devices.
E. Either a SSL VPN or an IPsec VPN can be established between an end-user workstation and a FortiGate device.

Answer: AD

NEW QUESTION 120
Which of the following statements best describes the role of a DC agents in an FSSO DC?

A. Captures the login events and forward them to the collector agent.
B. Captures the user IP address and workstation name and forward that information to the FortiGate devices.
C. Captures the login and logoff events and forward them to the collector agent.
D. Captures the login events and forward them to the FortiGate devices.

Answer: C

NEW QUESTION 123
Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (choose three)

A. Irix
B. QNIX
C. Linux
D. Mac OS
E. BSD

Answer: CDE

NEW QUESTION 125
Which FSSO agents are required for a FSSO agent-based polling mode solution?

A. Collector agent and DC agents
B. Polling agent only
C. Collector agent only
D. DC agents only

Answer: A

NEW QUESTION 129
Which are outputs for the command 'diagnose hardware deviceinfo nic'? (Choose two.)

A. ARP cache
B. Physical MAC address
C. Errors and collisions
D. Listening TCP ports

Answer: BC

NEW QUESTION 130
There are eight (8) log severity levels that indicate the importance of an event. Not including Debug, which is only needed to log diagnostic data, what are both the lowest AND highest severity levels?

A. Notification, Emergency
B. Information, Critical
C. Error, Critical
D. Information, Emergency
E. Information, Alert

Answer: D

NEW QUESTION 134
Which of the following statements best describe the main requirements for a traffic session to be offload eligible to an NP6 processor? (Choose three.)

A. Session packets do NOT have an 802.1Q VLAN tag.
B. It is NOT multicast traffic.
C. It does NOT require proxy-based inspection.
D. Layer 4 protocol must be UDP, TCP, SCTP or ICMP.
E. It does NOT require flow-based inspection.

Answer: CDE

NEW QUESTION 137
Which of the following statements are correct concerning IPsec dialup VPN configurations for FortiGate devices? (Choose two)

A. Main mode mist be used when there is no more than one IPsec dialup VPN configured on the same FortiGate device.
B. A FortiGate device with an IPsec VPN configured as dialup can initiate the tunnel connection to any remote IP address.
C. Peer ID must be used when there is more than one aggressive-mode IPsec dialup VPN on the same FortiGate device.
D. The FortiGate will automatically add a static route to the source quick mode selector address received from each remote peer.

Answer: CD

NEW QUESTION 140
Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

A. SMTP

B. WINS
C. HTTP
D. Telnet
E. SSH

Answer: CDE

NEW QUESTION 142
Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?

A. Policy-based only.
B. Route-based only.
C. Either policy-based or route-based VPN.
D. GRE-based only.

Answer: B

NEW QUESTION 146
Which of the following statements are correct concerning IKE mode config? (Choose two)

A. It can dynamically assign IP addresses to IPsec VPN clients.
B. It can dynamically assign DNS settings to IPsec VPN clients.
C. It uses the ESP protocol.
D. It can be enabled in the phase 2 configuration.

Answer: AB

NEW QUESTION 149
Which of the following statements best describes what the Document Fingerprinting feature is for?

A. Protects sensitive documents from leakage
B. Appends a fingerprint signature to all documents sent by users
C. Appends a fingerprint signature to all the emails sent by users
D. Validates the fingerprint signature in users' emails

Answer: A

NEW QUESTION 154
Which statement best describes what a Fortinet System on a Chip (SoC) is?

A. Low-power chip that provides general purpose processing power
B. Chip that combines general purpose processing power with Fortinet's custom ASIC technology
C. Light-version chip (with fewer features) of an SP processor
D. Light-version chip (with fewer features) of a CP processor

Answer: B

NEW QUESTION 157
In a high availability cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a slave unit?

A. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
B. Request: internal host; slave FortiGate; Internet; web server.
C. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
D. Request: internal host; master FortiGate; slave FortiGate; Internet; web server.

Answer: D

NEW QUESTION 158
Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type.
Which of the following are some of the available event types in Web Config?

A. Intrusion detected.
B. Successful firewall authentication.
C. Oversized file detected.
D. DHCP address assigned.
E. FortiGuard Web Filtering rating error detected.

Answer: A

NEW QUESTION 159
In FortiOS session table output, what are the two possible 'proto_state' values for a UDP session? (Choose two.)

A. 00
B. 11

C. 01
D. 05

Answer: AC

NEW QUESTION 160
Which of the following statements best describes how the collector agent learns that a user has logged off from the network?

A. The workstation fails to reply to the polls frequently done by the collector agent.
B. The DC agent captures the log off event from the event logs, which it forwards to the collector agent.
C. The work station notifies the DC agent that the user has logged off.
D. The collector agent gets the logoff events when polling the respective domain controller.

Answer: D

NEW QUESTION 163
Which define device identification? (Choose two.)

A. Device identification is enabled by default on all interfaces.
B. Enabling a source device in a firewall policy enables device identification on the source interfaces of that policy.
C. You cannot combine source user and source device in the same firewall policy.
D. FortiClient can be used as an agent based device identification technique.
E. Only agentless device identification techniques are supported.

Answer: BD

NEW QUESTION 164
Which statements are true regarding the factory default configuration? (Choose three.)

A. The default web filtering profile is applied to the first firewall policy.
B. The 'Port1' or 'Internal' interface has the IP address 192.168.1.99.
C. The implicit firewall policy action is ACCEPT.
D. The 'Port1' or 'Internal' interface has a DHCP server set up and enabled (on device models that support DHCP servers).
E. Default login uses the username: admin (all lowercase) and no password.

Answer: BDE

NEW QUESTION 166
What types of troubleshooting can you do when uploading firmware? (Choose two.)

A. Investigate corrupted firmware
B. Investigate current runtime state
C. Investigate damaged hardware
D. Investigate configuration history

Answer: AD

NEW QUESTION 168
Examine the following log message attributes and select two correct statements from the list below. (Choose two.)
hostname=www.youtube.com profiletype="Webfilter_Profile" profile="default" status="passthrough" msg="URL belongs to a category with warnings enabled"

A. The traffic was blocked.
B. The user failed authentication.
C. The category action was set to warning.
D. The website was allowed

Answer: CD

NEW QUESTION 170
Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)

Peer Options

Accept Types	This peer ID ▼
Peer ID	fortinet

Phase 1 Proposal ⊕ Add

Encryption [3DES ▼] Authentication [SHA1 ▼]

Diffie-Hellman Groups
☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16
☐ 15 ☑ 14 ☑ 5 ☐ 2 ☐ 1

Key Lifetime (seconds) [86400]

Local ID [   ]

XAUTH

Type [Disabled ▼]

Phase 2 Selectors ⊕ Add

Name	Local Address	Remote Address	
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	✎

A. The quick mode selector in the remote site must also be 0.0.0.0/0 for the source and destination addresses.
B. Only remote peers with the peer ID 'fortinet' will be able to establish a VPN.
C. The FortiGate device will automatically add a static route to the source quick mode selector address received from each remote VPN peer.
D. The configuration will work only to establish FortiClient-to-FortiGate tunnel
E. A FortiGate tunnel requires a different configuration.

Answer: CD

NEW QUESTION 173
You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using routebased mode. Users from either side must be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate already has a default route.
Which two configuration steps are required to achieve these objectives? (Choose two.)

A. Create one firewall policy.
B. Create two firewall policies.
C. Add a route to the remote subnet.
D. Add two IPsec phases 2.

Answer: BC

NEW QUESTION 175
Which protocol can an Internet browser use to download the PAC file with the web proxy configuration?

A. HTTPS
B. FTP
C. TFTP
D. HTTP

Answer: D

NEW QUESTION 177
If you enable the option "Generate Logs when Session Starts", what effect does this have on the number of traffic log messages generated for each session?

A. No traffic log message is generated.
B. One traffic log message is generated.
C. Two traffic log messages are generated.
D. A log message is only generated if there is a security event.

Answer: C

NEW QUESTION 182
What is required in a FortiGate configuration to have more than one dialup IPsec VPN using aggressive mode?

A. All the aggressive mode dialup VPNs MUST accept connections from the same peer ID.
B. Each peer ID MUST match the FQDN of each remote peer.
C. Each aggressive mode dialup MUST accept connections from different peer ID.
D. The peer ID setting must NOT be used.

Answer: C

NEW QUESTION 187
Which statement correctly describes the output of the command diagnose ips anomaly list?

A. Lists the configured DoS policy.
B. List the real-time counters for the configured DoS policy.
C. Lists the errors captured when compiling the DoS policy.
D. Lists the IPS signature matches.

Answer: B

NEW QUESTION 188
In a FSSO agentless polling mode solution, where must the collector agent be?

A. In any Windows server
B. In any of the AD domain controllers
C. In the master AD domain controller
D. The FortiGate device polls the AD domain controllers

Answer: D

NEW QUESTION 190
Which authentication methods does FortiGate support for firewall authentication? (Choose two.)

A. Remote Authentication Dial in User Service (RADIUS)
B. Lightweight Directory Access Protocol (LDAP)
C. Local Password Authentication
D. POP3
E. Remote Password Authentication

Answer: AC

NEW QUESTION 191
A FortiGate is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root.
Which of the following settings will this administrator be able to configure? (Choose two.)

A. Firewall addresses
B. DHCP servers
C. FortiGuard Distribution Network configuration.
D. System hostname.

Answer: AB

NEW QUESTION 192
Which of the following statements is correct regarding FortiGate interfaces and spanning tree protocol? (Choose Two)

A. Only FortiGate switch interfaces Participate in spanning tree.
B. All FortiGate interfaces in transparent mode VDOMs participate in spanning tree.
C. All FortiGate interfaces in NAT/route mode VDOMs Participate in spanning tree.
D. All FortiGate interfaces in transparent mode VDOMs may block or forward BPDUs.

Answer: BD

NEW QUESTION 196
Which of the following IKE modes is the one used during the IPsec phase 2 negotiation?

A. Aggressive mode
B. Quick mode
C. Main mode
D. Fast mode

Answer: B

NEW QUESTION 201
Of the following information, what can be recorded by a Data Leak Prevention sensor configured to do a summary archiving? (Choose three.)

A. Visited URL (for the case of HTTP traffic)
B. Sender email address (for the case of SMTP traffic)
C. Recipient email address (for the case of SMTP traffic)
D. Attached file (for the case of SMTP traffic)
E. Email body (for the case of SMTP traffic)

Answer: BCE

NEW QUESTION 205

Which of the following statements are correct regarding logging to memory on a FortiGate unit?

A. When the system has reached its capacity for log messages, the FortiGate unit will stop logging to memory.
B. When the system has reached its capacity for log messages, the FortiGate unit overwrites the oldest messages.
C. If the FortiGate unit is reset or loses power, log entries captured to memory will be lost.
D. None of the above.

Answer: BC

NEW QUESTION 210
Which IPSec mode includes the peer id information in the first packet?

A. Main mode.
B. Quick mode.
C. Aggressive mode.
D. IKEv2 mode.

Answer: C

NEW QUESTION 214
Which of the following statements are correct regarding SSL VPN Web-only mode? (Choose two.)

A. It can only be used to connect to web services.
B. IP traffic is encapsulated over HTTPS.
C. Access to internal network resources is possible from the SSL VPN portal.
D. The standalone FortiClient SSL VPN client CANNOT be used to establish a Web-only SSL VPN.
E. It is not possible to connect to SSH servers through the VPN.

Answer: BC

NEW QUESTION 218
Which of the following sequences describes the correct order of criteria used for the selection of a master unit within a FortiGate high availability (HA) cluster when override is disabled?

A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number.
B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number.
C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number.
D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number.

Answer: B

NEW QUESTION 223
Which UTM feature sends a UDP query to FortiGuard servers each time FortiGate scans a packet (unless the response is locally cached)?

A. Antivirus
B. VPN
C. IPS
D. Web Filtering

Answer: D

NEW QUESTION 226
Bob wants to send Alice a file that is encrypted using public key cryptography.
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.
B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file.
C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.
D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.

Answer: C

NEW QUESTION 231
Which of the following combinations of two FortiGate device configurations (side A and side B), can be used to successfully establish an IPsec VPN between them? (choose two)

A. Side A:main mode, remote gateway as static IP address, policy based VP
B. Side B: aggressive mode, remote Gateway as static IP address policy-based VPN.
C. Side A:main mode, remote gateway as static IP address, policy based VP
D. Side B: main mode, remote gateway as static IP address, route-based VPN
E. Side A:main mode, remote gateway as static IP address, policy based VP
F. Side B: main mode, remote gateway as dialup, route-based VPN.
G. Side A: main mode, remote gateway as dialup policy based VPN, Side B: main mode, remote gateway as dialup, policy based VPN.

Answer: BC

NEW QUESTION 233
What is the default criteria for selecting the HA master unit in a HA cluster?

A. port monitor, priority, uptime, serial number
B. Port monitor, uptime, priority, serial number
C. Priority, uptime, port monitor, serial number
D. uptime, priority, port monitor, serial number

Answer: B

NEW QUESTION 237
The exhibit shoes three static routes.

```
config router static
    edit 1
        set dst 172.20.168.0 255.255.255.0
        set distance 10
        set priority 10
     set device port1
    next
    edit 2
        set dst 172.20.0.0 255.255.0.0
        set distance 5
        set priority 20
        set device port2
    next
    edit 3
        set dst 172.20.0.0 255.255.0.0
        set distance 5
        set priority 20
        set device port3
    next
end
```

Which routes will be used to route the packets to the destination IP address 172.20.168.1?

A. The route with the ID number 2 and 3.
B. Only the route with the ID number 3.
C. Only the route with the ID number 2.
D. Only the route with the ID number 1.

Answer: D

NEW QUESTION 238
In which order are firewall policies processed on a FortiGate unit?

A. From top to bottom, according with their sequence number.
B. From top to bottom, according with their policy ID number.
C. Based on best match.
D. Based on the priority value.

Answer: A

NEW QUESTION 242
What are two requirements for DC-agent mode FSSO to work properly in a Windows AD environment? (Choose two.)

A. DNS server must properly resolve all workstation names
B. The remote registry service must be running in all workstations
C. The collector agent must be installed in one of the Windows domain controllers
D. A same user cannot be logged in into two different workstations at the same time

Answer: AB

NEW QUESTION 245
Which of the following statements best describe what a FortiGate does when packets match a black hole route?

A. Packets are dropped.
B. Packets are routed based on the information in the policy-based routing table.
C. An ICMP error message is sent back to the originator.
D. Packet are routed back to the originator.

Answer: A

NEW QUESTION 250
What actions are possible with Application Control? (Choose three.)

A. Warn
B. Allow
C. Block
D. Traffic Shaping
E. Quarantine

Answer: BCD

NEW QUESTION 254
A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the antivirus and email filter profiles applied to this policy.
Exhibit A

Exhibit B:

What is the correct behavior when the email attachment is detected as a virus by the FortiGate antivirus engine?

A. The FortiGate unit will remove the infected file and deliver the email with a replacement message to alert the recipient that the original attachment was infected.
B. The FortiGate unit will reject the infected email and the sender will receive a failed delivery message.
C. The FortiGate unit will remove the infected file and add a replacement messag
D. Both sender and recipient are notified that the infected file has been removed.
E. The FortiGate unit will reject the infected email and notify the sender.

Answer: B

NEW QUESTION 256
In the debug command output shown in the exhibit, which of the following best described the MAC address 00:09:0f:69:03:7e ?

```
# diagnose ip arp list
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e
state=00000004 use=4589 confirm=4589 update=2422 ref=1
```

A. It is one of the secondary MAC addresses of the port1 interface.
B. It is the primary MAC address of the port interface.
C. It is the MAC address of another network devices located in the same LAN segment as the FortiGate unit's port1 interface.
D. It is the HA virtual MAC address.

Answer: C

NEW QUESTION 258
An administrator wants to create an IPsec VPN tunnel between two FortiGate devices.
Which three configuration steps must be performed on both units to support this scenario? (Choose three.)

A. Create firewall policies to allow and control traffic between the source and destination IP addresses.
B. Configure the appropriate user groups to allow users access to the tunnel.
C. Set the operating mode to IPsec VPN mode.
D. Define the phase 2 parameters.
E. Define the Phase 1 parameters.

Answer: ADE

NEW QUESTION 262
Which of the following options best defines what Diffie-Hellman is?

A. A symmetric encryption algorithm.
B. A "key-agreement" protocol.
C. A "Security-association-agreement" protocol.
D. An authentication algorithm.

Answer: B

NEW QUESTION 267
To which remote device can the FortiGate send logs? (Choose three.)

A. Syslog
B. FortiAnalyzer
C. Hard drive
D. Memory
E. FortiCloud

Answer: ABE

NEW QUESTION 268
The exhibit shows two static routes to the same destinations subnet 172.20.168.0/24.

```
#config router static
    edit 1
        set dst 172.20.168.0 255.255.255.0
        set distance 10
         set priority 20
        set device port1
    next
    edit 2
        set dst 172.20.168.0 255.255.255.0
        set distance 20
        set priority 20
        set device port2
    next
end
```

Which of the following statements correctly describes this static routing configuration? (choose two)

A. Both routes will show up in the routing table.
B. The FortiGate unit will evenly share the traffic to 172.20.168.0/24 between routes.
C. Only one route will show up in the routing table.
D. The FortiGate will route the traffic to 172.20.168.0/24 only through one route.

Answer: CD

NEW QUESTION 272
What are the ways FortiGate can monitor logs? (Choose three.)

A. MIB
B. SMS
C. Alert Emails
D. SNMP
E. FortiAnalyzer
F. Alert Message Console

Answer: CDF

NEW QUESTION 277
......

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 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4-dumps.html