

NSE4 Dumps

Fortinet Network Security Expert 4 Written Exam (400)

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



NEW QUESTION 1

Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.

```
config router static
edit 1
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 10
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 the static routing configuration provided above?

- A. The FortiGate evenly shares the traffic to 172.20.168.0/24 through both routes.
- B. The FortiGate shares the traffic to 172.20.168.0/24 through both routes, but the port2 route will carry approximately twice as much of the traffic.
- C. The FortiGate sends all the traffic to 172.20.168.0/24 through port1.
- D. Only the route that is using port1 will show up in the routing table.

Answer: C

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 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 4

A FortiGate administrator with the super_admin profile configures a virtual domain (VDM) for a new customer. After creating the VDM, the administrator is unable to reassign the dmz interface to the new VDM as the option is greyed out in the GUI in the management VDM. What would be a possible cause for this problem?

- A. The administrator does not have the proper permissions the dmz interface.
- B. The dmz interface is referenced in the configuration of another VDM.
- C. Non-management VDMs cannot reference physical interfaces
- D. The dmz interface is in PPPoE or DHCP mode.

Answer: B

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

For traffic that does match any configured firewall policy, what is the default action taken by the FortiGate?

- A. The traffic is allowed and no log is generated.
- B. The traffic is allowed and logged.
- C. The traffic is blocked and no log is generated.
- D. The traffic is blocked and logged.

Answer: C

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 is NOT true about source matching with firewall policies?

- A. A source address object must be selected in the firewall policy.
- B. A source user/group may be selected in the firewall policy.
- C. A source device may be defined in the firewall policy.
- D. A source interface must be selected in the firewall policy.
- E. A source user/group and device must be specified in the firewall policy.

Answer: E

NEW QUESTION 10

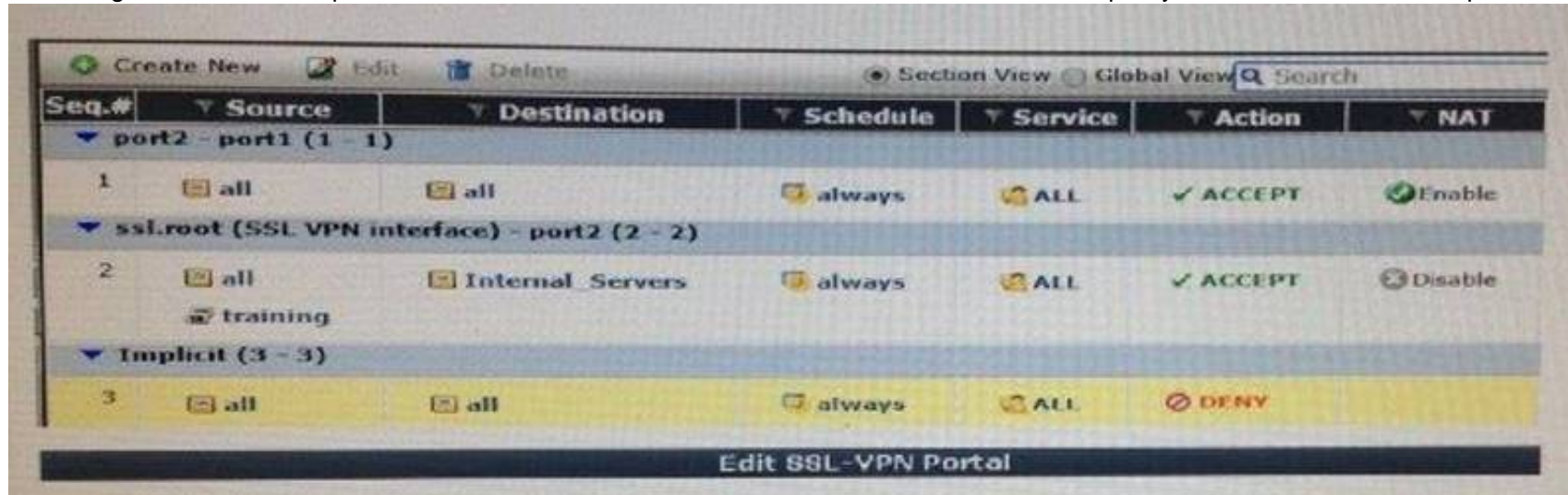
Which statements are correct for port pairing and forwarding domains? (Choose two.)

- 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 14

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

The order of the firewall policies is important. Policies can be re-ordered from either the GUI or the CLI. Which CLI command is used to perform this function?

- A. set order
- B. edit policy
- C. reorder
- D. move

Answer: D

NEW QUESTION 19

With FSSO DC-agent mode, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent.

If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

- A. The login event is sent to a collector agent.
- B. The FortiGate receives the user information directly from the receiving domain controller agent of the secondary domain controller.
- C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.
- D. The user cannot be authenticated with the FortiGate in this manner because each domain controller agent requires a dedicated collector agent.

Answer: AC

NEW QUESTION 20

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 25

Which action does the FortiGate take when link health monitor times out?

- A. All routes to the destination subnet configured in the link health monitor are removed from the routing table.
- B. The distance values of all routes using interface configured in the link health monitor are increased.
- C. The priority values of all routes using configured in the link health monitor are increased.
- D. All routes using the next-hop gateway configured in the link health monitor are removed from the routing table.

Answer: D

NEW QUESTION 29

The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.

Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web F
port2 - port1 (1 - 1)								
1	all	all	always	ALL	✓ ACCEPT	Enable		
Implicit (2 - 2)								
2	all	all	always	ALL	✗ DENY			

Based on the firewall configuration illustrated in the exhibit, which statement is correct?

- A. A user that has not authenticated can access the Internet using any protocol that does not trigger an authentication challenge.
- B. A user that has not authenticated can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP.
- C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access all Internet services.
- D. DNS Internet access is always allowed, even for users that have not authenticated.

Answer: D

NEW QUESTION 34

What is the maximum number of different virus databases a FortiGate can have?

- A. 5
- B. 2
- C. 3
- D. 4

Answer: B

NEW QUESTION 35

Which are valid replies from a RADIUS server to an ACCESS-REQUEST packet from a FortiGate? (Choose two.)

- A. ACCESS-CHALLENGE
- B. ACCESS-RESTRICT
- C. ACCESS-PENDING
- D. ACCESS-REJECT

Answer: AD

NEW QUESTION 39

Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of diagnose sys session stat for the STUDENT device. Exhibit B shows the command output of diagnose sys session stat for the REMOTE device.

Exhibit A:

```
STUDENT # diagnose sys session stat
Misc info:      session_count=166 setup_rate=68 exp_count=0 clash=0
                memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
    8 in ESTABLISHED state
    3 in SYN_SENT state
    1 in FIN_WAIT state
   139 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
    syncqf=0 acceptqf=0 no-listener=2 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

STUDENT # _
```

Exhibit B:

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
Misc info:      session_count=11 setup_rate=0 exp_count=0 clash=4
                memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
    2 in ESTABLISHED state
    1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
    syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

Given the information provided in the exhibits, which of the following statements are correct? (Choose two.)

- A. STUDENT is likely to be the master device.
- B. Session-pickup is likely to be enabled.
- C. The cluster mode is active-passive.
- D. There is not enough information to determine the cluster mode.

Answer: AD

NEW QUESTION 41

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 46

What capabilities can a FortiGate provide? (Choose three)

- A. Mail relay
- B. Email filtering
- C. Firewall
- D. VPN gateway
- E. Mail server

Answer: BCD

NEW QUESTION 50

Which statement is correct concerning an IPsec VPN with the remote gateway setting configured as 'Dynamic DNS'?

- A. The FortiGate will accept IPsec VPN connection from any IP address.
- B. The FQDN resolution of the local FortiGate IP address where the VPN is terminated must be provided by a dynamic DNS provider.
- C. The FortiGate will Accept IPsec VPN connections only from IP addresses included on a dynamic DNS access list.
- D. The remote gateway IP address can change dynamically.

Answer: D

NEW QUESTION 53

Which of the following statements describes the objectives of the gratuitous ARP packets sent by an HA cluster?

- A. To synchronize the ARp tables in all the FortiGate Unis that are part of the HA cluster.
- B. To notify the network switches that a new HA master unit has been elected.
- C. To notify the master unit that the slave devices are still up and alive.
- D. To notify the master unit about the physical MAC addresses of the slave units.

Answer: B

NEW QUESTION 56

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 59

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 61

What is not true of configuring disclaimers on the FortiGate?

- A. Disclaimers can be used in conjunction with captive portal.
- B. Disclaimers appear before users authenticate.
- C. Disclaimers can be bypassed through security exemption lists.
- D. Disclaimers must be accepted in order to continue to the authentication login or originally intended destination.

Answer: C

NEW QUESTION 63

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 protocol.
- E. Otherwise, it does not respond.

Answer: B

NEW QUESTION 67

When configuring LDAP on the FortiGate as a remote database for users, what is not a part of the configuration?

- A. The name of the attribute that identifies each user (Common Name Identifier).
- B. The user account or group element names (user DN).
- C. The server secret to allow for remote queries (Primary server secret).
- D. The credentials for an LDAP administrator (password).

Answer: C

NEW QUESTION 68

Which of the following statements best describes what a Public Certificate Authority (CA) is?

- A. A service that provides a digital certificate each time a user is authenticating

- B. An entity that certifies that the information contained in a digital certificate is valid and true.
- C. The FortiGate process in charge of generating digital certificates on the fly for SSL inspection purposes
- D. A service that validates digital certificates for certificate-based authentication purposes

Answer: D

NEW QUESTION 70

Which of the following statement correct describes the use of the "diagnose sys ha reset- uptime" command?

- A. To force an HA failover when the HA override setting is disabled.
- B. To force an HA failover when the HA override setting is enabled.
- C. To clear the HA counters.
- D. To restart a FortiGate unit that is part of an HA cluster.

Answer: A

NEW QUESTION 75

Which of the following actions can be used with the FortiGuard quota feature? (Choose three.)

- A. Allow
- B. Block
- C. Monitor
- D. Warning
- E. Authenticate

Answer: CDE

NEW QUESTION 77

Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

- A. Split tunneling is supported.
- B. It requires the installation of a VPN client.
- C. It requires the use of an Internet browser.
- D. It does not support traffic from third-party network applications.
- E. An SSL VPN IP address is dynamically assigned to the client by the FortiGate unit.

Answer: ABE

NEW QUESTION 80

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 83

A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.

Which of the following statements are possible reasons for this?

A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received. Which of the following statements are possible reasons for this? (Select all that apply.)

- A. The external facing interface of the FortiGate unit is configured to use DHCP.
- B. The FortiGate unit has not been registered.
- C. There is a NAT device between the FortiGate unit and the FortiGuard Distribution Network and no override push IP is configured.
- D. The FortiGate unit is in Transparent mode which does not support push updates.

Answer: ABC

NEW QUESTION 84

Examine the following spanning tree configuration on a FortiGate in transparent mode:

```
config system interface edit <interface name> set stp-forward enable end
```

Which statement is correct for the above configuration?

- A. The FortiGate participates in spanning tree.
- B. The FortiGate device forwards received spanning tree messages.
- C. Ethernet layer-2 loops are likely to occur.
- D. The FortiGate generates spanning tree BPDU frames.

Answer: B

NEW QUESTION 86

Which best describes the mechanism of a TCP SYN flood?

- A. The attackers keeps open many connections with slow data transmission so that other clients cannot start new connections.
- B. The attackers sends a packets designed to sync with the FortiGate
- C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
- D. The attacker starts many connections, but never acknowledges to fully form them.

Answer: D

NEW QUESTION 88

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 93

Which of the following spam filtering methods are supported on the FortiGate unit? (Select all that apply.)

- A. IP Address Check
- B. Open Relay Database List (ORDBL)
- C. Black/White List
- D. Return Email DNS Check
- E. Email Checksum Check

Answer: ABCDE

NEW QUESTION 98

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 100

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 102

On your FortiGate 60D, you've configured firewall policies. They port forward traffic to your Linux Apache web server. Select the best way to protect your web server by using the IPS engine.

- A. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache application
- B. Configured DLP to block HTTP GET request with credit card numbers.
- C. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache application
- D. Configure DLP to block HTTP GET with credit card number
- E. Also configure a DoS policy to prevent TCP SYN floods and port scans.
- F. Non
- G. FortiGate 60D is a desktop model, which does not support IPS.
- H. Enable IPS signatures for Linux and windows servers with FTP, HTTP, TCP, and SSL protocols and Apache and PHP applications.

Answer: D

NEW QUESTION 106

Which is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying a FortiGate unit?

- A. MIB-based report uploads.
- B. SNMP access limited by access lists.
- C. Packet encryption.
- D. Running SNMP service on a non-standard port is possible.

Answer: C

NEW QUESTION 107

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 112

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 117

Which statement best describes what SSL VPN Client Integrity Check does?

- A. Blocks SSL VPN connection attempts from users that have been blacklisted.
- B. Detects the Windows client security applications running in the SSL VPN client's PCs.
- C. Validates the SSL VPN user credential.
- D. Verifies which SSL VPN portal must be presented to each SSL VPN user.
- E. Verifies that the latest SSL VPN client is installed in the client's PC.

Answer: B

NEW QUESTION 121

Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.

Phase 2 Selectors

Name	Local Address	Remote Address
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: remote

Comments: VPN: remote (Created by VPN wizard)

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

Encryption: AES256 Authentication: SHA512 Add

Enable Replay Detection: ☒

Enable Perfect Forward Secrecy (PFS): ☒

Diffie-Hellman Group: ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☒ 14 ☒ 5 ☐ 2 ☐ 1

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Autokey Keep Alive: ☒

Auto-negotiate: ☒

Key Lifetime: Seconds 43200

Which statements are correct regarding this configuration? (Choose two.)

- A. The Phase 2 will re-key even if there is no traffic.
- B. There will be a DH exchange for each re-key.
- C. The sequence number of ESP packets received from the peer will not be checked.
- D. Quick mode selectors will default to those used in the firewall policy.

Answer: AB

NEW QUESTION 124

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 128

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 available
- 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 key
- E. Asymmetric cryptography uses a pair of keys
- F. Asymmetric keys can be sent to the remote peer via digital certificate
- G. Symmetric keys cannot

Answer: CD

NEW QUESTION 130

An administrator has configured a route-based site-to-site IPsec VPN. Which statement is correct regarding this IPsec VPN configuration?

- A. The IPsec firewall policies must be placed at the top of the list.
- B. This VPN cannot be used as a part of a hub and spoke topology.
- C. Routes are automatically created based on the quick mode selectors.
- D. A virtual IPsec interface is automatically created after the Phase 1 configuration is completed.

Answer: D

NEW QUESTION 133

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

- A. SSL VPN creates a HTTPS connection
- 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 138

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 143

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 145

Which of the following statements are correct concerning the FortiGate session life support protocol? (Choose two)

- A. By default, UDP sessions are not synchronized.
- B. Up to four FortiGate devices in standalone mode are supported.
- C. only the master unit handles the traffic.
- D. Allows per-VDOM session synchronization.

Answer: AD

NEW QUESTION 147

Examine the static route configuration shown below; then answer the question following it.

```
config router static edit 1
set dst 172.20.1.0 255.255.255.0
set device port1
set gateway 172.11.12.1
set distance 10
set weight 5 next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable set distance 5
set weight 10 next
end
```

Which of the following statements correctly describes the static routing configuration provided? (Choose two.)

- A. All traffic to 172.20.1.0/24 is dropped by the FortiGate.
- B. As long as port1 is up, all traffic to 172.20.1.0/24 is routed by the static route number 1. if the interface port1 is down, the traffic is routed using the blackhole route.
- C. The FortiGate unit does NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
- D. The FortiGate unit creates a session entry in the session table when the traffic is being routed by the blackhole route.

Answer: AC

NEW QUESTION 151

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 152

An administrator configures a FortiGate unit in Transparent mode on the 192.168.11.0 subnet. Automatic Discovery is enabled to detect any available FortiAnalyzers on the network.

Which of the following FortiAnalyzers will be detected?

- A. 192.168.11.100
- B. 192.168.11.251
- C. 192.168.10.100
- D. 192.168.10.251

Answer: AB

NEW QUESTION 155

Examine the following output from the diagnose sys session list command:


```
session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600 flags=00000000
sockflag=00000000 sockport=443 av_idx=9 use=5

origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps
reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps
state=redir local may_dirty ndr npu nlb os rs

statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3

orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.17.87.3/10.1.10.1
hook=post dir=org act=snat 192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)
hook=pre dir=reply act=dnat 74.201.86.29:443->172.17.87.16:57999(192.168.1.110:57999)
hook=post dir=reply act=noop 74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0)

misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0

npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0
```

Which statements are true regarding the session above? (Choose two.)

- A. Session Time-To-Live (TTL) was configured to 9 seconds.
- B. FortiGate is doing NAT of both the source and destination IP address on all packets coming from the 192.168.1.110 address.
- C. The IP address 192.168.1.110 is being translated to 172.17.87.16.
- D. The FortiGate is not translating the TCP port numbers of the packets in this session.

Answer: CD

NEW QUESTION 156

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 158

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 163

For FortiGate devices equipped with Network Processor (NP) chips, which are true? (Choose three.)

- A. For each new IP session, the first packet always goes to the CPU.
- B. The kernel does not need to program the NP
- C. When the NPU sees the traffic, it determines by itself whether it can process the traffic
- D. Once offloaded, unless there are errors, the NP forwards all subsequent packet
- E. The CPU does not process them.
- F. When the last packet is sent or received, such as a TCP FIN or TCP RST signal, the NP returns this session to the CPU for tear down.
- G. Sessions for policies that have a security profile enabled can be NP offloaded.

Answer: ACD

NEW QUESTION 165

In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

- A. The DC agents get each user IP address from the event logs and forward that information to the collector agent
- B. The collector agent does not know, and does not need, each user IP address
- C. Only workstation names are known by the collector agent.
- D. The collector agent frequently polls the AD domain controllers to get each user IP address.
- E. The DC agent learns the workstation name from the event logs and DNS is then used to translate those names to the respective IP addresses.

Answer: D

NEW QUESTION 168

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 173

Which statement is in advantage of using a hub and spoke IPsec VPN configuration instead of a fully-meshed set of IPsec tunnels?

- A. Using a hub and spoke topology provides full redundancy.
- B. Using a hub and spoke topology requires fewer tunnels.
- C. Using a hub and spoke topology uses stronger encryption protocols.
- D. Using a hub and spoke topology requires more routes.

Answer: B

NEW QUESTION 178

Which of the following traffic shaping functions can be offloaded to a NP processor? (Choose two.)

- A. Que prioritization
- B. Traffic cap (bandwidth limit)
- C. Differentiated services field rewriting
- D. Guarantee bandwidth

Answer: CD

NEW QUESTION 179

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 181

Which of the following email spam filtering features is NOT supported on a FortiGate unit?

- A. Multipurpose Internet Mail Extensions (MIME) Header Check
- B. HELO DNS Lookup
- C. Greylisting
- D. Banned Word

Answer: C

NEW QUESTION 185

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 188

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 193

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 195

Examine the following log message attributes and select two correct statements from the list below. (Choose two.)

hostname=www.youtube.com filetype="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 200

What are valid options for handling DNS requests sent directly to a FortiGate's interface IP? (Choose three.)

- A. Conditional-forward.
- B. Forward-only.
- C. Non-recursive.
- D. Iterative.
- E. Recursive.

Answer: BCE

NEW QUESTION 202

A FortiGate device is configured with two VDOMs. The management VDOM is 'root' , and is configured in transparent mode,'vdom1' is configured as NAT/route mode. Which traffic is generated only by 'root' and not 'vdom1'? (Choose three.)

- A. SNMP traps
- B. FortiGaurd
- C. ARP
- D. NTP
- E. ICMP redirect

Answer: ABD

NEW QUESTION 204

What information is synchronized between two FortiGate units that belong to the same HA cluster? (Choose three)

- A. IP addresses assigned to DHCP enabled interface.
- B. The master devices hostname.
- C. Routing configured and state.
- D. Reserved HA management interface IP configuration.
- E. Firewall policies and objects.

Answer: ACE

NEW QUESTION 207

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 211

Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

- A. The whole VDOM is a single broadcast domain even when multiple VLAN are used.
- B. Each VLAN is a separate broadcast domain.
- C. Interfaces configured with the same VLAN ID can belong to different broadcast domains.
- D. All the interfaces in the same broadcast domain must use the same VLAN ID.

Answer: BC

NEW QUESTION 213

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 215

Which of the following actions that can be taken by the Data Leak Prevention scanning? (Choose three.)

- A. Block
- B. Reject
- C. Tag
- D. Log only
- E. Quarantine IP address

Answer: ADE

NEW QUESTION 217

What configuration objects are automatically added when using the FortiGate's FortiClient VPN Configurations Wizard?(Choose two)

- A. Static route
- B. Phase 1
- C. Users group
- D. Phase 2

Answer: BD

NEW QUESTION 219

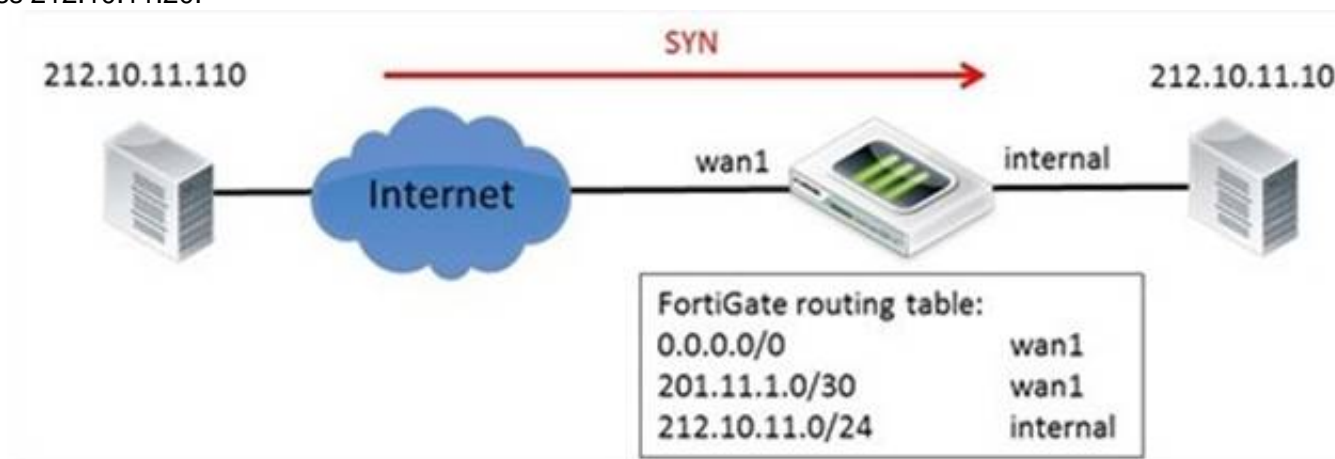
Which of the following statements are correct about the HA command diagnose sys ha reset-uptime? (Choose two.)

- A. The device this command is executed on is likely to switch from master to slave status if override is disabled.
- B. The device this command executed on is likely to switch from master to slave status if override is enabled.
- C. The command has no impact on the HA algorithm.
- D. This commands resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

Answer: AD

NEW QUESTION 220

Examine the network topology diagram in the exhibit; the workstation with the IP address 212.10.11.110 sends a TCP SYN packet to the workstation with the IP address 212.10.11.20.



Which of the following sentences best describes the result of the reverse path forwarding (RPF) check executed by the FortiGate on the SYN packets? (Choose two).

- A. Packets is allowed if RPF is configured as loose.
- B. Packets is allowed if RPF is configured as strict.
- C. Packets is blocked if RPF is configured as loose.
- D. Packets is blocked if RPF is configured as strict.

Answer: AD

NEW QUESTION 224

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 225

How many packets are interchanged between both IPSec ends during the negotiation of a main-mode phase 1?

- A. 5
- B. 3
- C. 2
- D. 6

Answer: D

NEW QUESTION 229

You have configured the DHCP server on a FortiGate's port1 interface (or internal, depending on the model) to offer IPs in a range of 192.168.1.65-192.168.1.253. When the first host sends a DHCP request, what IP will the DHCP offer?

- A. 192.168.1.99
- B. 192.168.1.253
- C. 192.168.1.65
- D. 192.168.1.66

Answer: C

NEW QUESTION 230

Which web filtering inspection mode inspects DNS traffic?

- A. DNS-based.
- B. FQDN-based.
- C. Flow-based.
- D. URL-based.

Answer: A

NEW QUESTION 231

Which statement best describes what SSL.root is?

- A. The name of the virtual network adapter required in each user's PC for SSL VPN Tunnel mode.
- B. The name of a virtual interface in the root VDOM where all the SSL VPN user traffic comes from.
- C. A Firewall Address object that contains the IP addresses assigned to SSL VPN users.
- D. The virtual interface in the root VDOM that the remote SSL VPN tunnels connect to.

Answer: B

NEW QUESTION 232

Which statement concerning IPS is false?

- A. IPS packages contain an engine and signatures used by both IPS and other flow-based scans.
- B. One-arm topology with sniffer mode improves performance of IPS blocking.
- C. IPS can detect zero-day attacks.
- D. The status of the last service update attempt from FortiGuard IPS is shown on System>Config>FortiGuard and in output from 'diag autoupdate version'

Answer: D

NEW QUESTION 236

Which of the following statements are correct differences between NAT/route and transparent mode? (Choose two.)

- A. In transparent mode, interfaces do not have IP addresses.
- B. Firewall policies are only used in NAT/ route mode.
- C. Static routers are only used in NAT/route mode.
- D. Only transparent mode permits inline traffic inspection at layer 2.

Answer: AC

NEW QUESTION 240

Which type of conserve mode writes a log message immediately, rather than when the device exits conserve mode?

- A. Kernel
- B. Proxy
- C. System
- D. Device

Answer: B

NEW QUESTION 244

Which of the following regular expression patterns makes the terms “confidential data” case insensitive?

- A. [confidential data]

- B. /confidential data/i
- C. i/confidential data/
- D. “confidential data”

Answer: B

NEW QUESTION 245

Which of the following statements are characteristics of a FSSO solution using advanced access mode? (Choose three.)

- A. Protection profiles can be applied to both individual users and user groups
- B. Nested or inherited groups are supported
- C. Usernames follow the LDAP convention: CN=User, OU=Name, DC=Domain
- D. Usernames follow the Windows convention: Domain\username
- E. Protection profiles can be applied to user groups only.

Answer: BCE

NEW QUESTION 248

Which of the following statements are correct regarding FortiGate virtual domains (VDOMs)? (Choose two)

- A. VDOMs divide a single FortiGate unit into two or more independent firewall.
- B. A management VDOM handles SNM
- C. logging, alert email and FortiGuard updates.
- D. Each VDOM can run different firmware versions.
- E. Administrative users with a 'super_admin' profile can administrate only one VDOM.

Answer: AB

NEW QUESTION 250

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 253

What functions can the IPv6 Neighbor Discovery Protocol accomplish? (Choose two.)

- A. Negotiate the encryption parameters to use.
- B. Auto-adjust the MTU setting.
- C. Autoconfigure addresses and prefixes.
- D. Determine other nodes reachability.

Answer: CD

NEW QUESTION 255

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. Client - > slave FortiGate - > master FortiGate - > web server.
- B. Client - > slave FortiGate - > web server.
- C. Client - > master FortiGate - > slave FortiGate - > master FortiGate - > web server.
- D. Client - > master FortiGate - > slave FortiGate - > web server.

Answer: D

NEW QUESTION 257

Which of the following statements is true regarding the TCP SYN packets that go from a client, through an implicit web proxy (transparent proxy), to a web server listening at TCP port 80? (Choose three.)

- A. The source IP address matches the client IP address.
- B. The source IP address matches the proxy IP address.
- C. The destination IP address matches the proxy IP address.
- D. The destination IP address matches the server IP addresses.
- E. The destination TCP port number is 80.

Answer: ADE

NEW QUESTION 261

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 265

Which are the three different types of Conserve Mode that can occur on a FortiGate device? (Choose three.)

- A. Proxy
- B. Operating system
- C. Kernel
- D. System
- E. Device

Answer: ACD

NEW QUESTION 270

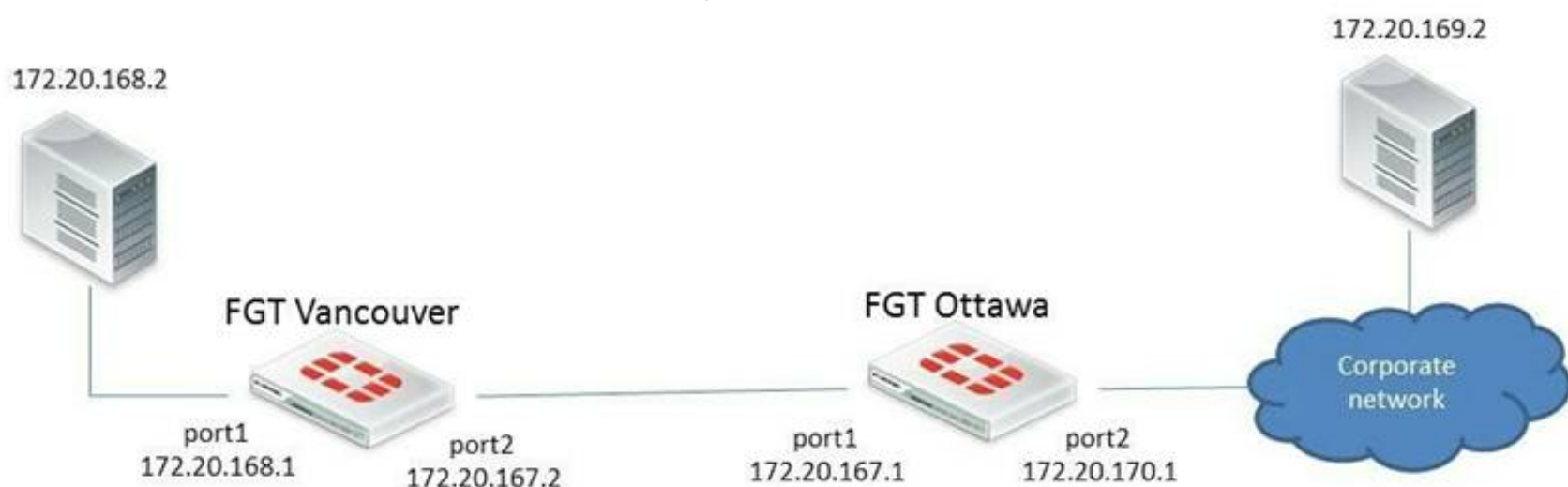
Which of the following sequences describes the correct order of criteria used for the selection of a master unit within a FortiGate high availability (HA) cluster when override is disabled?

- 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 272

Examine the exhibit below; then answer the question following it.



In this scenario. The FortiGate unit in Ottawa has the following routing table:

s*0.0.0.0/0 [10/0] via 172.20.170.254, port2

c172.20.167.0/24 is directly connected, port1 c172.20.170.0/24 is directly connected, port2

Sniffer tests show that packets sent from the source IP address 170.20.168.2 to the destination IP address 172.20.169.2 are being dropped by the FortiGate located in Ottawa.

Which of the following correctly describes the cause for the dropped packets?

- A. The forward policy check.
- B. The reserve path forwarding check.
- C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate's routing table.
- D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Answer: B

NEW QUESTION 275

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 276

Review the IKE debug output for IPsec shown in the exhibit below.

```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500, ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C26E2A7EC8461AC15E9BB0705B6C1F667A41957AED11F87003C07A1
07B0934D038E1A2074348E08FD6B39146C618525C6EC51E2F26885B68B8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C08000018E281874EECF170EB522216A4E3A027C71-
00000C0200000000101108D269E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540B0000181C047F014CBEF1B0EC8DA915F3B18AEB00
A0000C0200000000101108D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AAE79C1BE712B84255
EB84E5FA7A9677FE99C7B731057FF33728BB42AA983E79C919DA9B64EBC087EFOA02666C1FB02C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3ab31
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

Which statements is correct regarding this output?

- A. The output is a phase 1 negotiation.
- B. The output is a phase 2 negotiation.
- C. The output captures the dead peer detection messages.
- D. The output captures the dead gateway detection packets.

Answer: C

NEW QUESTION 279

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 281

Which of the following are considered log types? (Choose three.)

- A. Forward log
- B. Traffic log
- C. Syslog
- D. Event log
- E. Security log

Answer: BDE

NEW QUESTION 285

Which statements are true regarding IPv6 anycast addresses? (Choose two.)

- A. Multiple interfaces can share the same anycast address.
- B. They are allocated from the multicast address space.
- C. Different nodes cannot share the same anycast address.
- D. An anycast packet is routed to the nearest interface.

Answer: AD

NEW QUESTION 290

Which of the following statements must be true for a digital certificate to be valid? (Choose two.)

- A. It must be signed by a “trusted” CA
- B. It must be listed as valid in a Certificate Revocation List (CRL)
- C. The CA field must be “TRUE”
- D. It must be still within its validity period

Answer: AD

NEW QUESTION 294

Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

- A. Asymmetric Keys
- B. CA root digital certificates
- C. RSA signature
- D. Pre-shared keys

Answer: CD

NEW QUESTION 298

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 300

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

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

Answer: BCD

NEW QUESTION 303

Which of the following statements are true about Man-in-the-middle SSL Content Inspection? (Choose three.)

- A. The FortiGate device “re-signs” all the certificates coming from the HTTPS servers
- B. The FortiGate device acts as a sub-CA
- C. The local service certificate of the web server must be installed in the FortiGate device
- D. The FortiGate device does man-in-the-middle inspection.
- E. The required SSL Proxy certificate must first be requested to a public certificate authority (CA).

Answer: BCE

NEW QUESTION 308

What are the advantages of FSSO DC mode over polling mode?

- A. Redundancy in the collector agent.
- B. Allows transparent authentication.
- C. DC agents are not required in the AD domain controllers.
- D. Scalability

Answer: C

NEW QUESTION 312

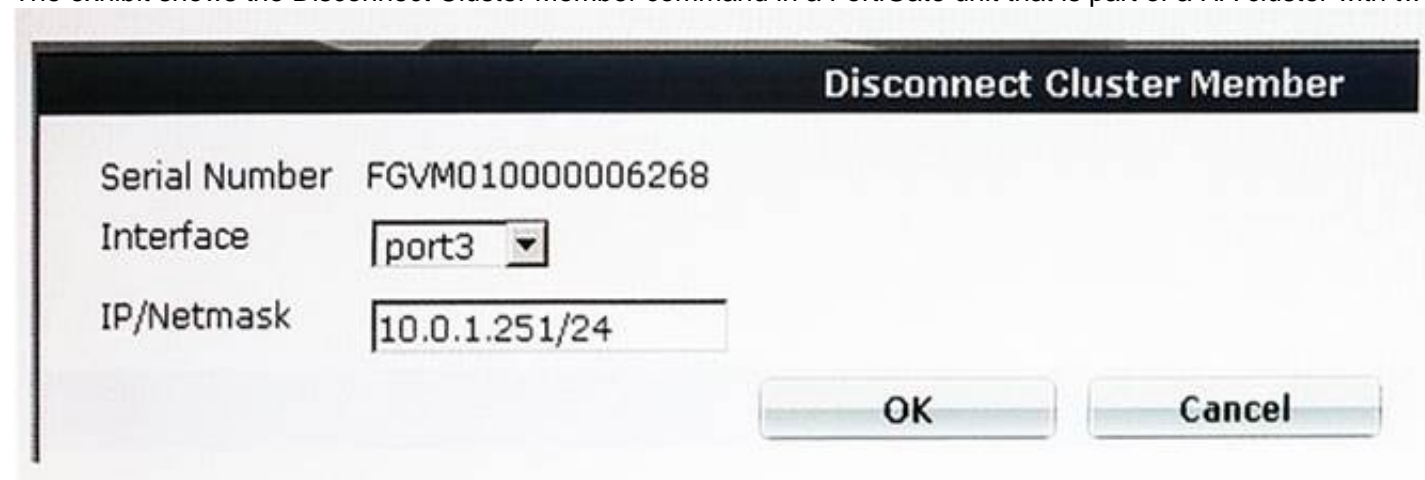
When creating FortiGate administrative users, which configuration objects specify the account rights?

- A. Remote access profiles.
- B. User groups.
- C. Administrator profiles.
- D. Local-in policies.

Answer: C

NEW QUESTION 317

The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA members.



What is the effect of the Disconnect Cluster Member command as given in the exhibit. (Choose two.)

- A. Port3 is configured with an IP address management access.
- B. The firewall rules are purged on the disconnected unit.
- C. The HA mode changes to standalone.
- D. The system hostname is set to the unit serial number.

Answer: AC

NEW QUESTION 320

Which of the following Fortinet products can receive updates from the FortiGuard Distribution Network?

- A. FortiGate
- B. FortiClient
- C. FortiMail
- D. FortiAnalyzer

Answer: ABC

NEW QUESTION 324

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 327

Which correctly define "Section View" and "Global View" for firewall policies? (Choose two.)

- A. Section View lists firewall policies primarily by their interface pairs.
- B. Section View lists firewall policies primarily by their sequence number.
- C. Global View lists firewall policies primarily by their interface pairs.
- D. Global View lists firewall policies primarily by their policy sequence number.
- E. The 'any' interface may be used with Section View.

Answer: AD

NEW QUESTION 331

Which of the following statements is true regarding the differences between route-based and policy-based IPsec VPNs? (Choose two.)

- A. The firewall policies for policy-based are bidirectiona
- B. The firewall policies for route- based are unidirectional.
- C. In policy-based VPNs the traffic crossing the tunnel must be routed to the virtual IPsec interfac
- D. In route-based, it does not.
- E. The action for firewall policies for route-based VPNs may be Accept or Deny, for policy- based VPNs it is Encrypt.
- F. Policy-based VPN uses an IPsec interface, route-based does not.

Answer: AC

NEW QUESTION 332

An administrator has formed a high availability cluster involving two FortiGate units.

[Multiple upstream Layer 2 switches] – [FortiGate HA Cluster] – [Multiple downstream Layer 2 Switches]

The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster.

Which of the following options describes the best step the administrator can take? The administrator should

- A. Increase the number of FortiGate units in the cluster and configure HA in active-active mode.
- B. Enable monitoring of all active interfaces.
- C. Set up a full-mesh design which uses redundant interfaces.
- D. Configure the HA ping server feature to allow for HA failover in the event that a path is disrupted.

Answer: C

NEW QUESTION 334

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 338

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 343

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 345

What are required to be the same for two FortiGate units to form an HA cluster? (Choose two)

- A. Firmware.
- B. Model.
- C. Hostname.
- D. System time zone.

Answer: AB

NEW QUESTION 346

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 351

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 352

What is valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

- A. Users are required to manually enter their credentials each time they connect to a different web site.
- B. Proxy users are authenticated via FSSO.
- C. There are multiple users sharing the same IP address.

D. Proxy users are authenticated via RADIUS.

Answer: C

NEW QUESTION 353

Which of the following statements are true about PKI users created in a FortiGate device? (Choose two.)

- A. Can be used for token-based authentication
- B. Can be used for two-factor authentication
- C. Are used for certificate-based authentication
- D. Cannot be members of user groups

Answer: AB

NEW QUESTION 355

.....

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>