

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

https://www.2passeasy.com/dumps/NSE4_FGT-7.2/



NEW QUESTION 1

If Internet Service is already selected as Destination in a firewall policy, which other configuration object can be selected for the Destination field of a firewall policy?

- A. IP address
- B. No other object can be added
- C. FQDN address
- D. User or User Group

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.59): "When configuring your firewall policy, you can use Internet Service as the destination in a firewall policy, which contains all the IP addresses, ports, and protocols used by that service. For the same reason, you cannot mix regular address objects with ISDB objects, and you cannot select services on a firewall policy. The ISDB objects already have services information, which is hardcoded."

This is true because Internet Service is a special type of destination object that can only be used alone in a firewall policy. Internet Service is a feature that allows FortiGate to identify and filter traffic based on the internet service or application that it belongs to, such as Facebook, YouTube, Skype, etc. Internet Service uses a database of IP addresses and ports that are associated with each internet service or application, and updates it regularly from FortiGuard. When Internet Service is selected as the destination in a firewall policy, FortiGate will match the traffic to the corresponding internet service or application, and apply the appropriate action and security profiles to it. However, Internet Service cannot be combined with any other destination object, such as IP address, FQDN address, user or user group, etc., as this would create a conflict or ambiguity in the firewall policy. Therefore, no other object can be added if Internet Service is already selected as the destination in a firewall policy

NEW QUESTION 2

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

- A. Source defined as Internet Services in the firewall policy.
- B. Destination defined as Internet Services in the firewall policy.
- C. Highest to lowest priority defined in the firewall policy.
- D. Services defined in the firewall policy.
- E. Lowest to highest policy ID number.

Answer: ABD

Explanation:

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

- Incoming Interface
- Outgoing Interface
- Source: IP address, user, internet services
- Destination: IP address or internet services
- Service: IP protocol and port number
- Schedule: Applies during configured times

NEW QUESTION 3

Which two statements are correct about SLA targets? (Choose two.)

- A. You can configure only two SLA targets per one Performance SLA.
- B. SLA targets are optional.
- C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
- D. SLA targets are used only when referenced by an SD-WAN rule.

Answer: BD

NEW QUESTION 4

Which two statements explain antivirus scanning modes? (Choose two.)

- A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
- B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
- C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
- D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Answer: BC

Explanation:

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

FortiGate Security 7.2 Study Guide (p.350 & 352): "In flow-based inspection mode, the IPS engine reads the payload of each packet, caches a local copy, and forwards the packet to the receiver at the same time. Because the file is ransmitted simultaneously, flow-based mode consumes more CPU cycles than proxy-based." "Each protocol's proxy picks up a connection and buffers the entire file first (or waits until the oversize limit is reached) before scanning. The client must wait for the scanning to finish."

NEW QUESTION 5

Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.



Based on the phase 2 configuration shown in the exhibit, which configuration change will bring phase 2 up?

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

Answer: B

NEW QUESTION 6

What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

- A. Full Content inspection
- B. Proxy-based inspection
- C. Certificate inspection
- D. Flow-based inspection

Answer: D

NEW QUESTION 7

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

- A. Antivirus engine
- B. Intrusion prevention system engine
- C. Flow engine
- D. Detection engine

Answer: B

Explanation:

<http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control>

NEW QUESTION 8

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

- A. The IP version of the sources and destinations in a firewall policy must be different.
- B. The Incoming Interface
- C. Outgoing Interface
- D. Schedule, and Service fields can be shared with both IPv4 and IPv6.
- E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
- F. The IP version of the sources and destinations in a policy must match.
- G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: BDE

NEW QUESTION 9

Which two statements describe how the RPF check is used? (Choose two.)

- A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
- B. The RPF check is run on the first sent and reply packet of any new session.
- C. The RPF check is run on the first sent packet of any new session.
- D. The RPF check is run on the first reply packet of any new session.

Answer: AC

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.41): "The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table." "FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session."

* A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks1

* C. The RPF check is run on the first sent packet of any new session.

This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the session initiation. This reduces the processing overhead and improves performance2

NEW QUESTION 10

Refer to the exhibit.

```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000  4500 003c 2f8f 0000 8001 f020 0a00 0102  E.</.....
0x0010  0808 0808 0800 4d5a 0001 0001 6162 6364  .....MZ....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869  uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000  4500 003c 2f8f 0000 7f01 0106 0a38 f0e4  E.</.....8..
0x0010  0808 0808 0800 6159 ec01 0001 6162 6364  .....aY....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869  uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000  4500 003c 0000 0000 7501 3a95 0808 0808  E.<....u.:....
0x0010  0a38 f0e4 0000 6959 ec01 0001 6162 6364  .8....iY....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869  uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000  4500 003c 0000 0000 7401 2bb0 0808 0808  E.<....t.+....
0x0010  0a00 0102 0000 555a 0001 0001 6162 6364  .....UZ....abcd
0x0020  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efghijklmnopqrst
0x0030  7576 7761 6263 6465 6667 6869  uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit. Which three pieces of information are included in the sniffer output? (Choose three.)

- A. Interface name
- B. Ethernet header
- C. IP header
- D. Application header
- E. Packet payload

Answer: ACE

NEW QUESTION 10

An administrator is running the following sniffer command:

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

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

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

Answer: ABD

NEW QUESTION 12

An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

- A. Policy lookup will be disabled.
- B. By Sequence view will be disabled.
- C. Search option will be disabled
- D. Interface Pair view will be disabled.

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821>

NEW QUESTION 16

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

- A. The collector agent uses a Windows API to query DCs for user logins.
- B. NetAPI polling can increase bandwidth usage in large networks.
- C. The collector agent must search security event logs.
- D. The NetSession Enum function is used to track user logouts.

Answer: D

Explanation:

FortiGate_Infrastructure_7.0 page 270: "NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows."

NEW QUESTION 17

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. SSH
- B. HTTPS
- C. FTM
- D. FortiTelemetry

Answer: AB

NEW QUESTION 22

Examine this PAC file configuration.

Which of the following statements are true? (Choose two.)

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 24

Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

- A. diagnose sys top
- B. execute ping
- C. execute traceroute
- D. diagnose sniffer packet any
- E. get system arp

Answer: BCD

NEW QUESTION 29

What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

- A. FortiGate uses fewer resources.
- B. FortiGate performs a more exhaustive inspection on traffic.
- C. FortiGate adds less latency to traffic.
- D. FortiGate allocates two sessions per connection.

Answer: AC

NEW QUESTION 34

An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSL/TLS connection. Which FortiGate configuration can achieve this goal?

- A. SSL VPN bookmark
- B. SSL VPN tunnel
- C. Zero trust network access
- D. SSL VPN quick connection

Answer: B

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.198): "Tunnel mode requires FortiClient to connect to FortiGate. FortiClient adds a virtual network adapter identified as fortissl to the user's PC. This virtual adapter dynamically receives an IP address from FortiGate each time FortiGate establishes a new VPN connection. Inside the tunnel, all traffic is SSL/TLS encapsulated. The main advantage of tunnel mode over web mode is that after the VPN is established, any IP network application running on the client can send traffic through the tunnel."

An SSL VPN tunnel allows remote users to establish a secure and encrypted Virtual Private Network (VPN) connection to the private network using the SSL/TLS protocol1. An SSL VPN tunnel can provide access to network resources such as FTP servers, as well as external applications running on the user's PC1.

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

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

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

NEW QUESTION 39

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

Answer: B

Explanation:

Strict Reverse Path Forwarding (RPF) is a security feature that is used to detect and prevent IP spoofing attacks on a network. It works by checking the routing information for incoming packets to ensure that they are coming from the source address that is indicated in the packet's header. In strict RPF mode, the firewall will check the best route back to the source of the incoming packet using the incoming interface. If the packet's source address does not match the route back to the source, the packet is dropped. This helps to prevent attackers from spoofing their IP address and attempting to access the network.

NEW QUESTION 42

Which two types of traffic are managed only by the management VDOM? (Choose two.)

- A. FortiGuard web filter queries
- B. PKI
- C. Traffic shaping
- D. DNS

Answer: AD

NEW QUESTION 43

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate points the collector agent to use a remote LDAP server.
- B. FortiGate uses the AD server as the collector agent.
- C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- D. FortiGate queries AD by using the LDAP to retrieve user group information.

Answer: CD

Explanation:

Fortigate Infrastructure 7.0 Study Guide P.272-273 <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

NEW QUESTION 46

Which three statements explain a flow-based antivirus profile? (Choose three.)

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

Answer: ADE

NEW QUESTION 47

Refer to the exhibits.

Exhibit A Exhibit B

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 3 hours, 28 minutes
```

Exhibit A Exhibit B

```
config system global
  set memory-use-threshold-red 88
  set memory-use-threshold-extreme 95
  set memory-use-threshold-green 82
end
```

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

- A. Administrators can access FortiGate only through the console port.
- B. FortiGate has entered conserve mode.
- C. FortiGate will start sending all files to FortiSandbox for inspection.
- D. Administrators cannot change the configuration.

Answer: BD

NEW QUESTION 51

The IPS engine is used by which three security features? (Choose three.)

- A. Antivirus in flow-based inspection
- B. Web filter in flow-based inspection
- C. Application control
- D. DNS filter
- E. Web application firewall

Answer: ABC

Explanation:

FortiGate Security 7.2 Study Guide (p.385): "The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It's also responsible for application control, flow-based antivirus protection, web filtering, and email filtering."

NEW QUESTION 56

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporarily disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 61

Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration. The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IP address 10.0.1.254/24.

Exhibit A Exhibit B

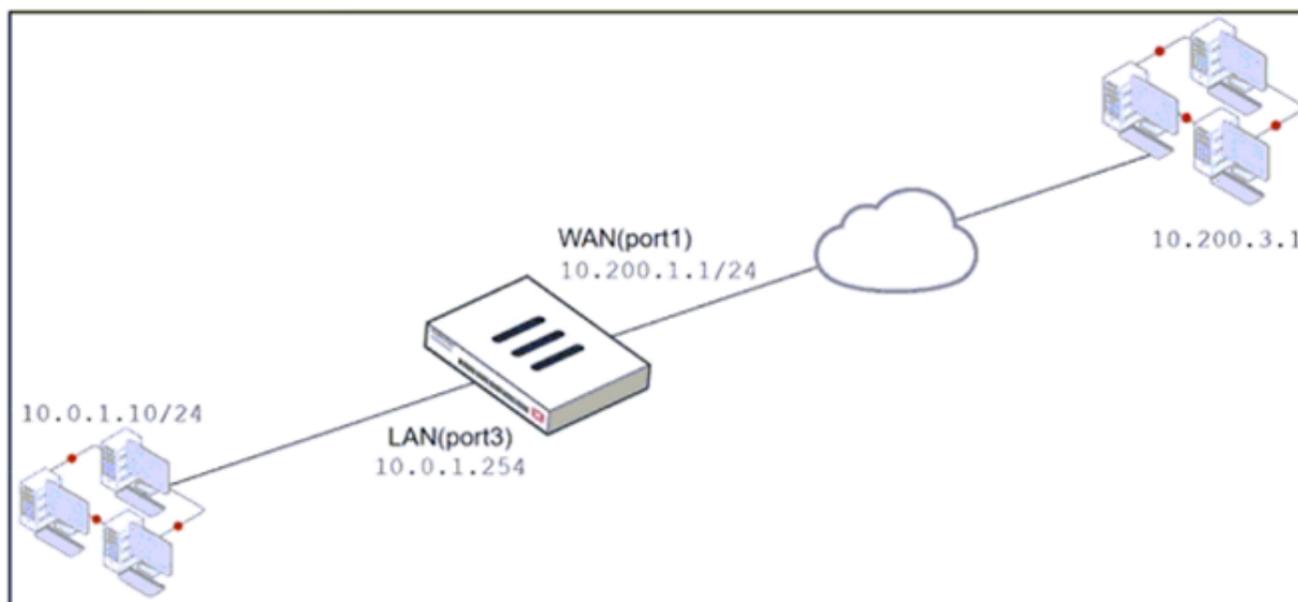


Exhibit A Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type: IPv4
 Name: VIP
 Comments: Write a comment... 0/255
 Color: Change

Network

Interface: WAN (port1)
 Type: Static NAT
 External IP address/range: 10.200.1.10
 Map to
 IPv4 address/range: 10.0.1.10

Optional Filters

Port Forwarding

Protocol: TCP UDP SCTP ICMP

Port Mapping Type: One to one Many to many

External service port: 10443
 Map to IPv4 port: 443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

- A. 10.0.1.254, 10.0.1.10, and 443, respectively
- B. 10.0.1.254, 10.200.1.10, and 443, respectively
- C. 10.200.3.1, 10.0.1.10, and 443, respectively
- D. 10.0.1.254, 10.0.1.10, and 10443, respectively

Answer: C

Explanation:

The host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, which is the external IP address of the VIP object named VIP in Exhibit B1. The VIP object maps the external IP address and port to the internal IP address and port of the server 10.0.1.10 and 443, respectively. The VIP object also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface. The firewall policy ID 1 in Exhibit B allows traffic from WAN (port1) to LAN (port3) with the destination address of VIP and the service of HTTPS1. The policy also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface. Therefore, after FortiGate forwards the packet to the destination, the source address, destination address, and destination port of the packet will be 10.200.3.1, 10.0.1.10, and 443, respectively. You can find more information about VIP objects and firewall policies in the Fortinet Documentation

NEW QUESTION 63

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

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

Answer: AC

NEW QUESTION 66

Which two types of traffic are managed only by the management VDOM? (Choose two.)

- A. FortiGuard web filter queries
- B. PKI
- C. Traffic shaping
- D. DNS

Answer: AD

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.73): "What about traffic originating from FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate. Traffic coming from FortiGate to those global services originates from the management VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM. It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate."

NEW QUESTION 69

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface. In this scenario, what are two requirements for the VLAN ID? (Choose two.)

- A. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.
- B. The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs.
- C. The two VLAN subinterfaces must have different VLAN IDs.
- D. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

Answer: BC

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-use-vmac-vlan-to-share-the-same-VLAN/> When FortiGate is operating in NAT mode, it means that it uses network address translation (NAT) to modify the source or destination IP addresses of the traffic passing through it¹. NAT mode allows FortiGate to hide the IP addresses of the internal network from the external network, and to conserve IP addresses by using a single public IP address for multiple private IP addresses¹.

A virtual LAN (VLAN) subinterface is a logical interface that allows traffic from different VLANs to enter and exit the FortiGate unit². A VLAN subinterface is created by adding a VLAN ID to a physical interface or an aggregate interface². A VLAN ID is a numerical identifier that distinguishes one VLAN from another².

In this scenario, there are two requirements for the VLAN ID of the VLAN subinterfaces added to the same physical interface:

> The two VLAN subinterfaces must have different VLAN IDs. This is because the VLAN ID is used to tag the traffic with the appropriate VLAN information, and to separate the traffic into different VLANs². If the two VLAN subinterfaces have the same VLAN ID, they will not be able to distinguish the traffic from each other, and they will not be able to forward the traffic to the correct destination.

> The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs. This is because VDOMs are virtual instances of FortiGate that can have their own interfaces, policies, and routing tables³. Each VDOM operates independently from other VDOMs, and can have its own VLAN subinterfaces with different or identical VLAN IDs³. However, this requires inter-VDOM links to allow traffic between different VDOMs³.

NEW QUESTION 72

Refer to the exhibits.

The exhibits show a network diagram and firewall configurations.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.

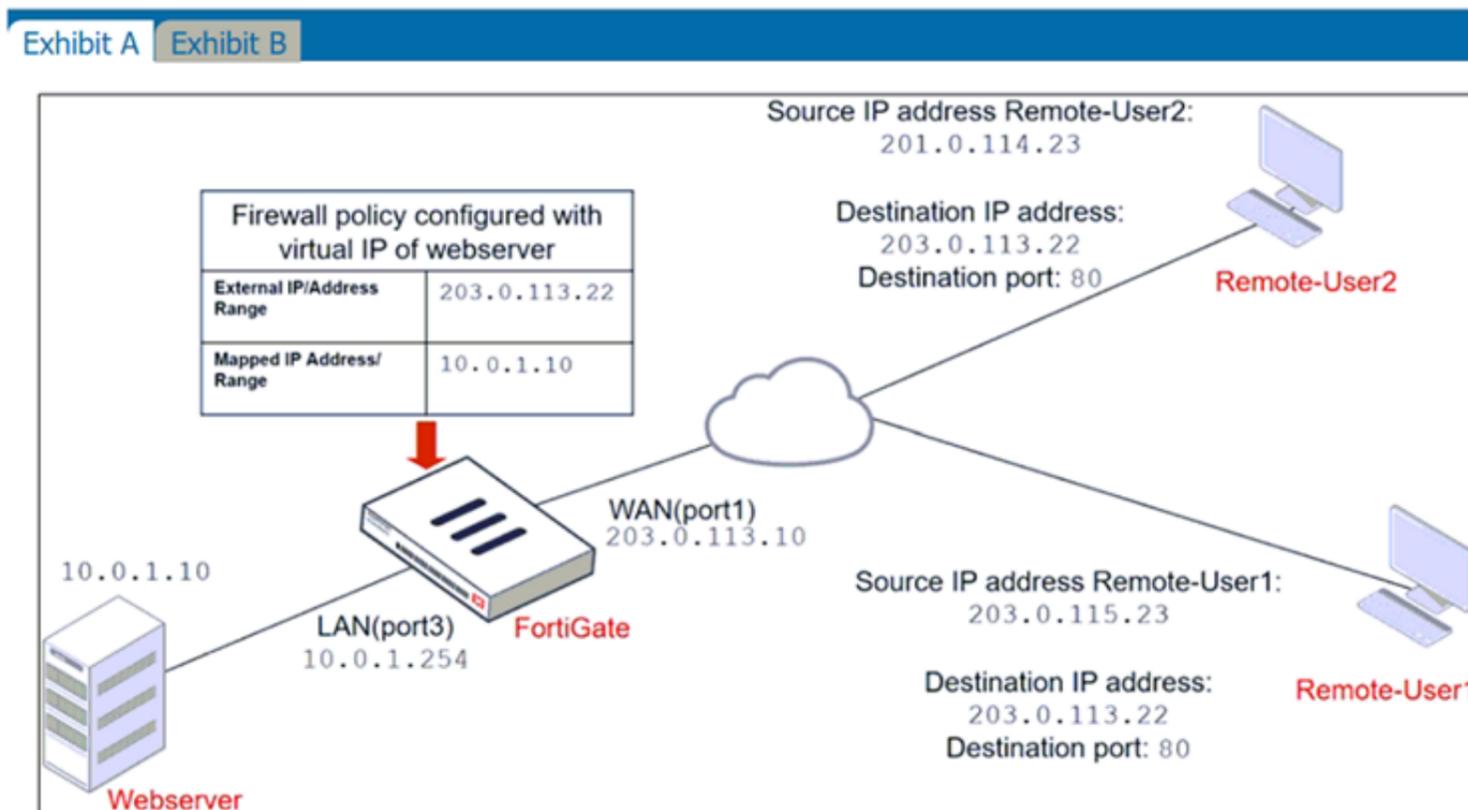


Exhibit A Exhibit B

The screenshot shows the 'Edit Address' configuration for 'Deny_IP' with the following details:

- Name: Deny_IP
- Color: Change
- Type: Subnet
- IP/Netmask: 201.0.114.23/32
- Interface: WAN (port1)
- Static route configuration: Off
- Comments: Deny web server access. 23/255

Below this is a table of Firewall policies:

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

- A. Disable match-vip in the Deny policy.
- B. Set the Destination address as Deny_IP in the Allow-access policy.
- C. Enable match vip in the Deny policy.
- D. Set the Destination address as Web_server in the Deny policy.

Answer: BC

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta> The exhibits show a network diagram and firewall configurations for a FortiGate unit that has two policies: Allow_access and Deny. The Allow_access policy allows traffic from the WAN (port1) interface to the LAN (port3) interface with the destination address of VIP and the service of HTTPS. The VIP object maps the external IP address 10.200.1.10 and port 10443 to the internal IP address 10.0.1.10 and port 443 of the Webserver. The Deny policy denies traffic from the WAN (port1) interface to the LAN (port3) interface with the source address of Deny_IP and the destination address of All. In this scenario, the administrator wants to deny Webserver access for Remote-User2, who has the IP address 10.200.3.2, which is included in the Deny_IP address object. Remote-User1, who has the IP address 10.200.3.1, must be able to access the Webserver. To achieve this goal, the administrator can make two changes to deny Webserver access for Remote-User2:

- > Set the Destination address as Webserver in the Deny policy. This will make the Deny policy more specific and match only the traffic that is destined for the Webserver's internal IP address, instead of any destination address.
- > Enable match-vip in the Deny policy. This will make the Deny policy apply to traffic that matches a VIP object, instead of ignoring it. This way, the Deny policy will block Remote-User2's traffic that uses the VIP object's external IP address and port.

NEW QUESTION 74

Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

- A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
- B. To finish any inspection operations
- C. To remove the NAT operation
- D. To generate logs

Answer: A

Explanation:

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

NEW QUESTION 78

Which scanning technique on FortiGate can be enabled only on the CLI?

- A. Heuristics scan
- B. Trojan scan
- C. Antivirus scan
- D. Ransomware scan

Answer: A

NEW QUESTION 82

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

- A. Source IP
- B. Spillover
- C. Volume

D. Session

Answer: CD

Explanation:

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing>

NEW QUESTION 87

In which two ways can RPF checking be disabled? (Choose two)

- A. Enable anti-replay in firewall policy.
- B. Disable the RPF check at the FortiGate interface level for the source check
- C. Enable asymmetric routing.
- D. Disable strict-arc-check under system settings.

Answer: CD

NEW QUESTION 91

What are two characteristics of FortiGate HA cluster virtual IP addresses? (Choose two.)

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

Answer: AD

Explanation:

Fortigate Infrastructure 7.2 Study Guide page 301 FortiGate Infrastructure 7.2 Study Guide (p.301):

"FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number."

"A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster." "The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data." <https://networkinterview.com/fortigate-ha-high-availability/>

NEW QUESTION 92

Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

- A. Proxy-based inspection
- B. Certificate inspection
- C. Flow-based inspection
- D. Full Content inspection

Answer: AC

NEW QUESTION 94

Refer to the exhibits.

Exhibit A shows the application sensor configuration. Exhibit B shows the Excessive-Bandwidth and Apple filter details.

Exhibit A Exhibit B

Edit Application Sensor

Categories

- All Categories
- Business (179, 6)
- Collaboration (293, 6)
- Game (124)
- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, 16)
- Video/Audio (206, 13)
- Web.Client (18)
- Cloud.IT (31)
- Email (87, 12)
- General.Interest (241, 9)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, 31)
- Update (48)
- VoIP (31)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

[+ Create New](#) [Edit](#) [Delete](#)

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	Block
2	Apple	Filter	Monitor

Exhibit A Exhibit B

Edit Override

Type: Application **Filter**

Action: Block

Filter: Excessive-Bandwidth

FaceTime

Name	Category	Technology
Application Signature 1/1262		
FaceTime	VoIP	Client-Server

Edit Override

Type: Application **Filter**

Action: Monitor

Filter: Apple

FaceTime

Name	Category	Technology
Application Signature 1/33		
FaceTime	VoIP	Client-Server

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

- A. Apple FaceTime will be allowed, based on the Categories configuration.
- B. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.
- C. Apple FaceTime will be allowed, based on the Apple filter configuration.
- D. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.310): "Then, FortiGate scans packets for matches, in this order, for the application control profile: 1. Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies. 2. Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories."

NEW QUESTION 98

Refer to the exhibit.

The screenshot shows the SD-WAN configuration interface. Under 'Outgoing interfaces', 'Best Quality' is selected. The 'Interface preference' list contains port1, port2, port3, and port4. The 'Measured SLA' is 'SLA_1' and 'Quality criteria' is 'Latency'. The status is 'Enable'.

```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check . Which interface will be selected as an outgoing interface?

- A. port2
- B. port4
- C. port3
- D. port1

Answer: D

Explanation:

Port 1 shows the lowest latency.

NEW QUESTION 101

Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

- A. Web filter in flow-based inspection
- B. Antivirus in flow-based inspection
- C. DNS filter
- D. Web application firewall
- E. Application control

Answer: ABE

Explanation:

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow>

NEW QUESTION 102

Which three statements are true regarding session-based authentication? (Choose three.)

- A. HTTP sessions are treated as a single user.
- B. IP sessions from the same source IP address are treated as a single user.
- C. It can differentiate among multiple clients behind the same source IP address.
- D. It requires more resources.
- E. It is not recommended if multiple users are behind the source NAT

Answer: ACD

NEW QUESTION 105

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

- A. Heartbeat interfaces have virtual IP addresses that are manually assigned.

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

Answer: BD

NEW QUESTION 107

Refer to the exhibit.

The screenshot shows the configuration for an SLA named 'SLA1'. The protocol is set to 'Ping', with 'HTTP' and 'DNS' also selected. Two servers are configured: 4.2.2.2 and 4.2.2.1. The participants are set to 'All SD-WAN Members', with 'Specify' also selected. Two ports, 'port1' and 'port2', are listed as participants. The 'Enable probe packets' checkbox is unchecked.

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic. Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

- A. The Detection Mode setting is not set to Passive.
- B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
- C. The configured participants are not SD-WAN members.
- D. The Enable probe packets setting is not enabled.

Answer: BD

NEW QUESTION 109

Refer to the exhibit.

The exhibit shows the output of a diagnose command.

```
# diagnose firewall proute list
list route policy info(vf=root):
id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
```

What does the output reveal about the policy route?

- A. It is an ISDB route in policy route.
- B. It is a regular policy route.
- C. It is an ISDB policy route with an SDWAN rule.
- D. It is an SDWAN rule in policy route.

Answer: D

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.59): "ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the vwl_service field, and ISDB route entries don't."

NEW QUESTION 113

Which two statements are true when FortiGate is in transparent mode? (Choose two.)

- A. By default, all interfaces are part of the same broadcast domain.
- B. The existing network IP schema must be changed when installing a transparent mode.
- C. Static routes are required to allow traffic to the next hop.
- D. FortiGate forwards frames without changing the MAC address.

Answer: AD

NEW QUESTION 116

Which timeout setting can be responsible for deleting SSL VPN associated sessions?

- A. SSL VPN idle-timeout
- B. SSL VPN http-request-body-timeout
- C. SSL VPN login-timeout
- D. SSL VPN dtls-hello-timeout

Answer: A

NEW QUESTION 120

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile. What order must FortiGate use when the web filter profile has features enabled, such as safe search?

- A. DNS-based web filter and proxy-based web filter
- B. Static URL filter, FortiGuard category filter, and advanced filters
- C. Static domain filter, SSL inspection filter, and external connectors filters
- D. FortiGuard category filter and rating filter

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.285): "Remember that the web filtering profile has several features. So, if you have enabled many of them, the inspection order flows as follows: 1. The local static URL filter 2. FortiGuard category filtering (to determine a rating) 3. Advanced filters (such as safe search or removing Active X components)"

NEW QUESTION 125

An administrator configures outgoing interface any in a firewall policy. What is the result of the policy list view?

- A. Search option is disabled.
- B. Policy lookup is disabled.
- C. By Sequence view is disabled.
- D. Interface Pair view is disabled.

Answer: D

Explanation:

"If you use multiple source or destination interfaces, or the any interface in a firewall policy, you cannot separate policies into sections by interface pairs—some would be triplets or more. So instead, policies are then always displayed in a single list (By Sequence)."

NEW QUESTION 129

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

- A. Log ID
- B. Universally Unique Identifier
- C. Policy ID
- D. Sequence ID

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.67): "When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer."

NEW QUESTION 134

Which two statements are true about the Security Fabric rating? (Choose two.)

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

Answer: BC

NEW QUESTION 135

Refer to the exhibits.

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

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

Exhibit A Exhibit B

Address Object

Name	Details
IP Range/Subnet (10)	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN (1)	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries																		
Predefined Internet Services (1,633)																				
Facebook-Web	Destination	26,578																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>IP</th> <th>Port</th> <th>Protocol</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td rowspan="3">1.9.91.17 - 1.9.91.18</td> <td>80</td> <td rowspan="3">TCP</td> <td rowspan="3">Enabled</td> </tr> <tr> <td>443</td> </tr> <tr> <td>8443</td> </tr> <tr> <td>1.9.91.17 - 1.9.91.18</td> <td>443</td> <td>UDP</td> <td>Enabled</td> </tr> <tr> <td>1.9.91.30</td> <td>443</td> <td>UDP</td> <td>Enabled</td> </tr> </tbody> </table>			IP	Port	Protocol	Status	1.9.91.17 - 1.9.91.18	80	TCP	Enabled	443	8443	1.9.91.17 - 1.9.91.18	443	UDP	Enabled	1.9.91.30	443	UDP	Enabled
IP	Port	Protocol	Status																	
1.9.91.17 - 1.9.91.18	80	TCP	Enabled																	
	443																			
	8443																			
1.9.91.17 - 1.9.91.18	443	UDP	Enabled																	
1.9.91.30	443	UDP	Enabled																	

Firewall Policies

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

Exhibit A Exhibit B

Policy Lookup

Incoming Interface:

IP Version:

Protocol:

Source:

Source Port:

Destination:

Destination Port:

Which policy will be highlighted, based on the input criteria?

- A. Policy with ID 4.
- B. Policy with ID 5.
- C. Policies with ID 2 and 3.
- D. Policy with ID 4.

Answer: B

NEW QUESTION 139

Refer to the exhibit.

Edit IPS Sensor

Name:

Comments: 0/255

Block malicious URLs:

IPS Signatures and Filters

[+ Create New](#) [Edit](#) [Delete](#)

Details	Exempt IPs	Action	Packet Logging	Status
NTP.Spoofed.KoD.DoS	0	Monitor	✔ Enabled	✔ Enabled
OS Windows		⊘ Block	✘ Disabled	✔ Enabled

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

- A. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
- B. The sensor will block all attacks aimed at Windows servers.
- C. The sensor will reset all connections that match these signatures.
- D. The sensor will gather a packet log for all matched traffic.

Answer: AB

NEW QUESTION 143

An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.
 Which DPD mode on FortiGate will meet the above requirement?

- A. Disabled
- B. On Demand
- C. Enabled
- D. On Idle

Answer: D

NEW QUESTION 148

Which feature in the Security Fabric takes one or more actions based on event triggers?

- A. Fabric Connectors
- B. Automation Stitches
- C. Security Rating
- D. Logical Topology

Answer: B

NEW QUESTION 151

Which statement describes a characteristic of automation stitches?

- A. They can have one or more triggers.
- B. They can be run only on devices in the Security Fabric.
- C. They can run multiple actions simultaneously.
- D. They can be created on any device in the fabric.

Answer: C

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/351998/creating-automation-stitches>

NEW QUESTION 156

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
 * All traffic must be routed through the primary tunnel when both tunnels are up
 * The secondary tunnel must be used only if the primary tunnel goes down
 * In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover
 Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two.)

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

Answer: BC

Explanation:

Study Guide – IPsec VPN – IPsec configuration – Phase 1 Network.

When Dead Peer Detection (DPD) is enabled, DPD probes are sent to detect a failed tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same destination, and you want to failover to a backup connection when the primary connection fails to keep the connectivity between the sites up.

There are three DPD modes. On demand is the default mode. Study Guide – IPsec VPN – Redundant VPNs.

Add one phase 1 configuration for each tunnel. DPD should be enabled on both ends. Add at least one phase 2 definition for each phase 1.

Add one static route for each path. Use distance or priority to select primary routes over backup routes (routes for the primary VPN must have a lower distance or lower priority than the backup). Alternatively, use dynamic routing.

Configure FW policies for each IPsec interface.

NEW QUESTION 159

Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 164

View the exhibit.



Which of the following statements are correct? (Choose two.)

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote sit
- D. The TunnelA route is used only if the TunnelB VPN is down.
- E. This is a redundant IPsec setup.

Answer: CD

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundan>

NEW QUESTION 167

How does FortiGate act when using SSL VPN in web mode?

- A. FortiGate acts as an FDS server.
- B. FortiGate acts as an HTTP reverse proxy.
- C. FortiGate acts as DNS server.
- D. FortiGate acts as router.

Answer: B

NEW QUESTION 170

Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check .
- D. FortiGate directs the collector agent to use a remote LDAP server.

Answer: BC

Explanation:

You can deploy FSSO w/o installing an agent. FG polls the DCs directly, instead of receiving logon info indirectly from a collector agent.

Because FG collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.

Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FG uses the SMB protocol to read the event viewer logs from the DCs.

FG acts as a collector. It 's responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

NEW QUESTION 172

Examine the exhibit, which contains a virtual IP and firewall policy configuration.

Exhibit A Exhibit B

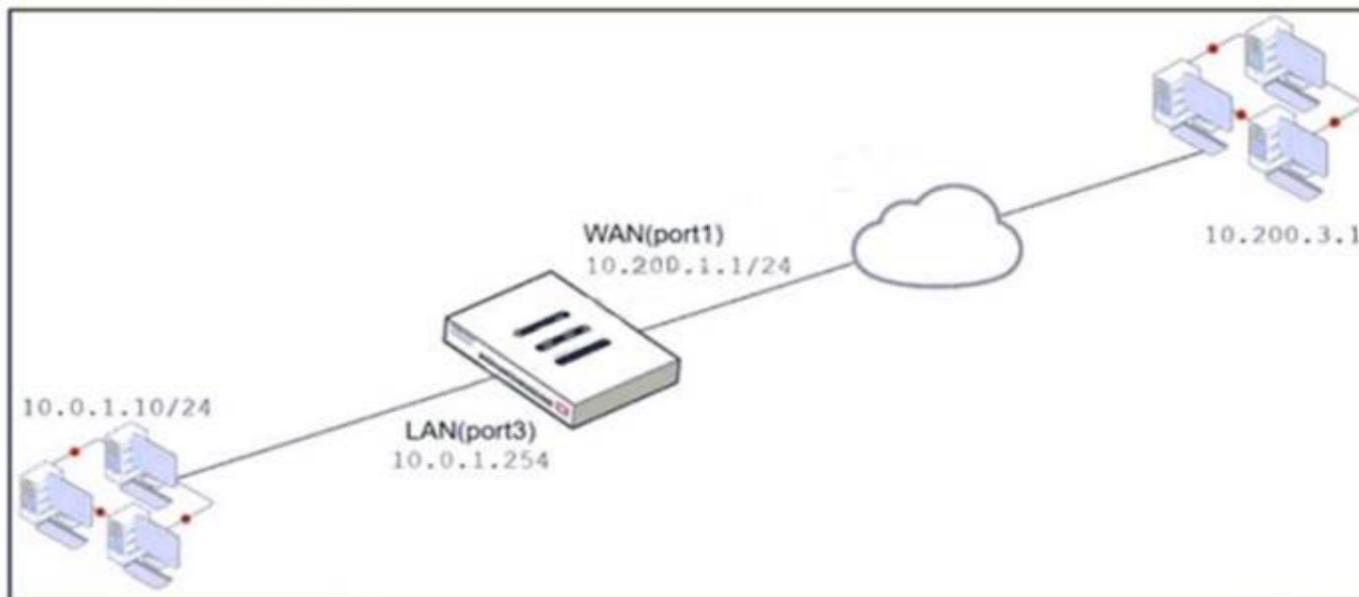


Exhibit A Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type: IPv4
 Name: VIP
 Comments: Write a comment... 0/255
 Color: Change

Network:
 Interface: WAN (port1)
 Type: Static NAT
 External IP address/range: 10.200.1.10
 Map to:
 IPv4 address/range: 10.0.1.10

Optional Filters

Port Forwarding

Protocol: TCP UDP SCTP ICMP
 Port Mapping Type: One to one Many to many
 External service port: 10443
 Map to IPv4 port: 443

The WAN (port1) interface has the IP address 10.200. 1. 1/24. The LAN (port2) interface has the IP address 10.0. 1.254/24. The first firewall policy has NAT enabled on the outgoing interface address. The second firewall policy is configured with a VIP as the destination address. Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0. 1. 10/24?

- A. 10.200. 1. 10
- B. Any available IP address in the WAN (port1) subnet 10.200. 1.0/24 66 of 108
- C. 10.200. 1. 1
- D. 10.0. 1.254

Answer: A

Explanation:

<https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs>.

NEW QUESTION 173

Refer to the exhibit.

```

FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

S     *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
      *>                [10/0] via 10.0.0.2, port2, [30/0]
S     0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C     *> 10.0.0.0/24 is directly connected, port2
S     172.13.24.0/24 [10.0] is directly connected, port4
C     *> 172.20.121.0/24 is directly connected, port1
S     *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C     *> 192.168.15.0/24 is directly connected, port3
    
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

- A. The port3 default route has the lowest metric.
- B. The port1 and port2 default routes are active in the routing table.
- C. The ports default route has the highest distance.
- D. There will be eight routes active in the routing table.

Answer: BC

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-identify-Inactive-Routes-in-the-Routing/ta-p>

NEW QUESTION 178

What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

- A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
- B. FortiGate automatically negotiates a new security association after the existing security association expires.
- C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
- D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=12069>

FortiGate Infrastructure 7.2 Study Guide (p.264): "...then FortiGate might drop interesting traffic because of the absence of active SAs. To prevent this, you can enable Auto-negotiate. When you do this, FortiGate not only negotiates new SAs before the current SAs expire, but it also starts using the new SAs right away." "Another benefit of enabling Auto-negotiate is that the tunnel comes up and stays up automatically, even when there is no interesting traffic. When you enable Autokey Keep Alive and keep Auto-negotiate disabled, the tunnel does not come up automatically unless there is interesting traffic. However, after the tunnel is up, it stays that way because FortiGate periodically sends keep alive packets over the tunnel. Note that when you enable Auto-negotiate, Autokey Keep Alive is implicitly enabled."

NEW QUESTION 179

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not. Which configuration option is the most effective way to support this request?

- A. Implement a web filter category override for the specified website
- B. Implement a DNS filter for the specified website.
- C. Implement web filter quotas for the specified website
- D. Implement web filter authentication for the specified website.

Answer: D

NEW QUESTION 183

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface. In this scenario, which statement about VLAN IDs is true?

- A. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.
- B. The two VLAN subinterfaces must have different VLAN IDs.
- C. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.
- D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

Answer: CD

NEW QUESTION 186

Which of the following statements about central NAT are true? (Choose two.)

- A. IP tool references must be removed from existing firewall policies before enabling central NAT .

- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Answer: AB

NEW QUESTION 191

Which two statements are correct about a software switch on FortiGate? (Choose two.)

- A. It can be configured only when FortiGate is operating in NAT mode
- B. Can act as a Layer 2 switch as well as a Layer 3 router
- C. All interfaces in the software switch share the same IP address
- D. It can group only physical interfaces

Answer: AC

NEW QUESTION 193

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

- A. Antivirus scanning
- B. File filter
- C. DNS filter
- D. Intrusion prevention

Answer: AD

NEW QUESTION 195

In an explicit proxy setup, where is the authentication method and database configured?

- A. Proxy Policy
- B. Authentication Rule
- C. Firewall Policy
- D. Authentication scheme

Answer: D

NEW QUESTION 196

Refer to the exhibit.

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.

The screenshot shows the 'New RADIUS Server' configuration page. The 'Name' field is 'FortiAuthenticator-RADIUS'. The 'Authentication method' is set to 'Default'. The 'NAS IP' field is empty. The 'Include in every user group' checkbox is checked. The 'Primary Server' section shows 'IP/Name' as '10.0.1.149' and 'Secret' as a series of dots. There are buttons for 'Test Connectivity' and 'Test User Credentials'.

What is the impact of using the Include in every user group option in a RADIUS configuration?

- A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- C. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
- D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Answer: A

NEW QUESTION 200

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

Answer: D

Explanation:

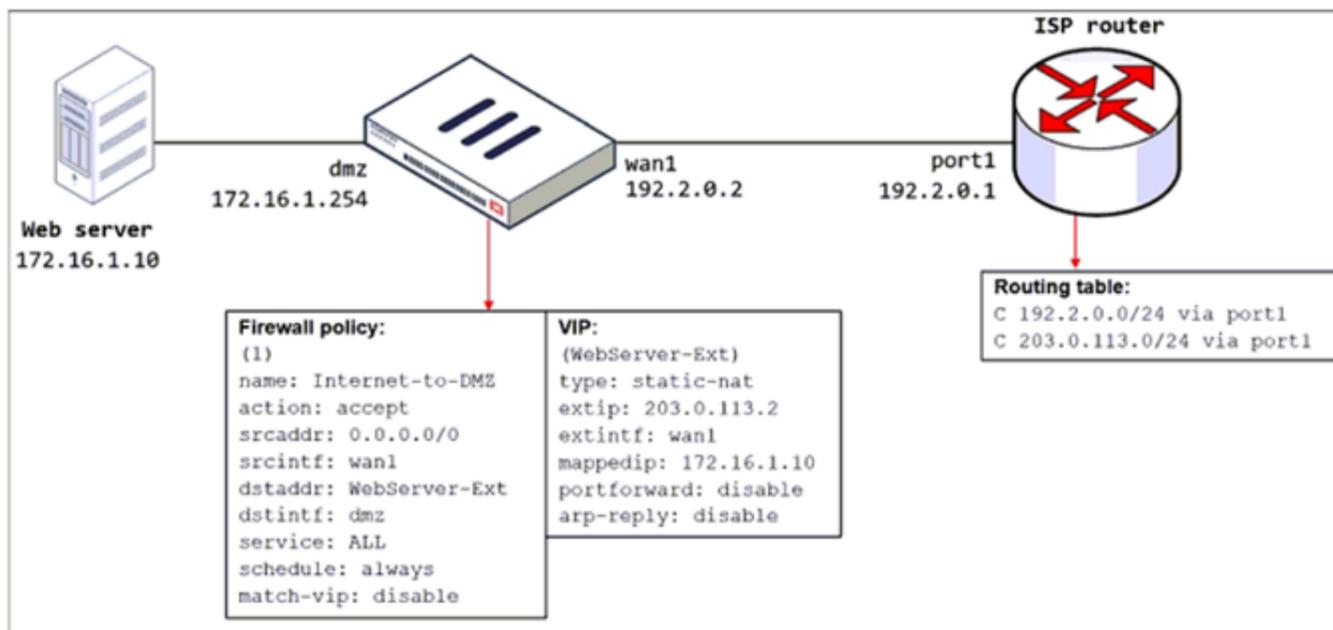
"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

NEW QUESTION 201

Refer to the exhibit.

The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.

When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.



Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

- A. Configure a loopback interface with address 203.0.113.2/32.
- B. In the VIP configuration, enable arp-reply.
- C. Enable port forwarding on the server to map the external service port to the internal service port.
- D. In the firewall policy configuration, enable match-vip.

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.115): "Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled."

NEW QUESTION 206

Which two statements are correct about NGFW Policy-based mode? (Choose two.)

- A. NGFW policy-based mode does not require the use of central source NAT policy
- B. NGFW policy-based mode can only be applied globally and not on individual VDOMs
- C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
- D. NGFW policy-based mode policies support only flow inspection

Answer: CD

NEW QUESTION 209

Refer to the exhibit.

Username	Administrator	<input type="button" value="Change Password"/>
Type	Local User Match a user on a remote server group Match all users in a remote server group Use public key infrastructure (PKI) group	
Comments	Write a comment... 0/255	
Administrator Profile	prof_admin	
Email Address	admin@xyz.com	
<input type="checkbox"/> SMS		
<input type="checkbox"/> Two-factor Authentication		
<input type="checkbox"/> Restrict login to trusted hosts		
<input type="checkbox"/> Restrict admin to guest account provisioning only		

The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

- A. Change password
- B. Enable restrict access to trusted hosts
- C. Change Administrator profile
- D. Enable two-factor authentication

Answer: C

NEW QUESTION 213

Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

- A. Log downloads from the GUI are limited to the current filter view
- B. Log backups from the CLI cannot be restored to another FortiGate
- C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
- D. Log downloads from the GUI are stored as LZ4 compressed files.

Answer: AB

NEW QUESTION 214

Which of statement is true about SSL VPN web mode?

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

Answer: B

Explanation:

FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

NEW QUESTION 217

Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.

The WAN (port1) interface has the IP address 10.200.1.1/24.

The LAN (port3) interface has the IP address 10.0.1.254/24.

The administrator disabled the WebServer firewall policy.

Exhibit A Exhibit B

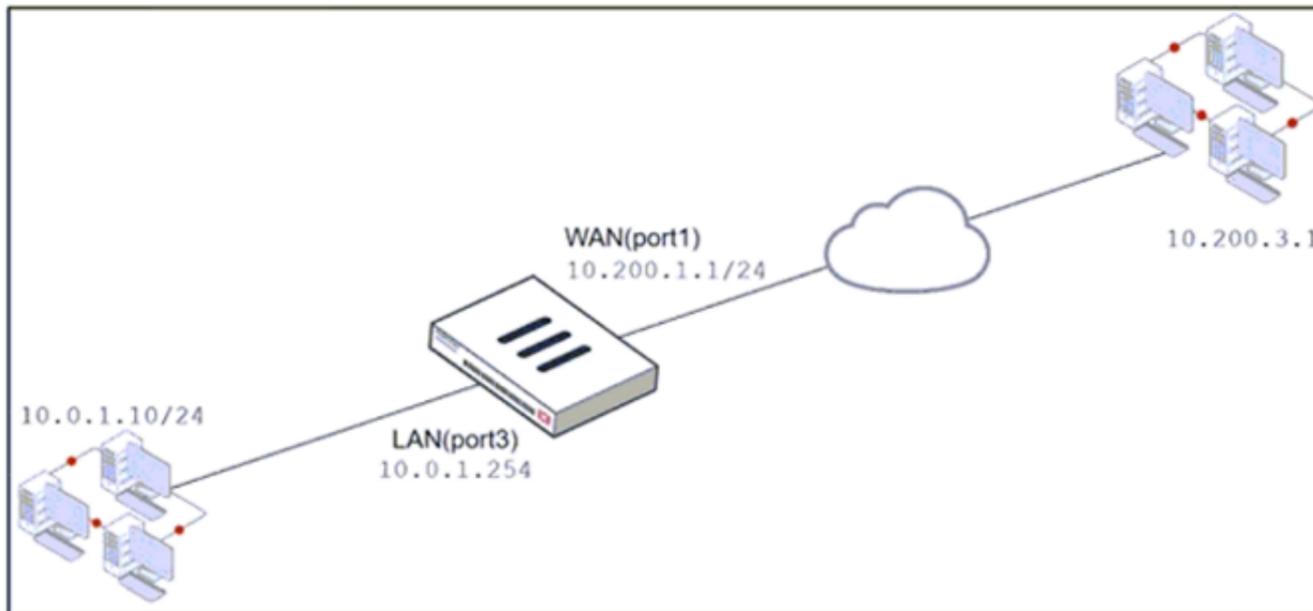


Exhibit A Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Full_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	ACCEPT	Enabled
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Disabled

Edit Virtual IP

VIP type: IPv4
 Name: VIP
 Comments: Write a comment... 0/255
 Color: Change

Network

Interface: WAN (port1)
 Type: Static NAT
 External IP address/range: 10.200.1.10
 Map to:
 IPv4 address/range: 10.0.1.10

Optional Filters
 Port Forwarding

Which IP address will be used to source NAT the traffic, if a user with address 10.0.1.10 connects over SSH to the host with address 10.200.3.1?

- A. 10.200.1.10
- B. 10.0.1.254
- C. 10.200.1.1
- D. 10.200.3.1

Answer: C

Explanation:

Traffic is coming from LAN to WAN, matches policy Full_Access which has NAT enable, so traffic uses source IP address of outgoing interface. Simple SNAT.

NEW QUESTION 220

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

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

Answer: B

NEW QUESTION 221

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A. A CRL
- B. A person
- C. A subordinate CA
- D. A root CA

Answer: D

NEW QUESTION 226

Which statement correctly describes the use of reliable logging on FortiGate?

- A. Reliable logging is enabled by default in all configuration scenarios.
- B. Reliable logging is required to encrypt the transmission of logs.
- C. Reliable logging can be configured only using the CLI.
- D. Reliable logging prevents the loss of logs when the local disk is full.

Answer: B

Explanation:

FortiGate Security 7.2 Study Guide (p.192): "if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the enc-algorithm setting on the CLI."

NEW QUESTION 230

Which statement about the IP authentication header (AH) used by IPsec is true?

- A. AH does not provide any data integrity or encryption.
- B. AH does not support perfect forward secrecy.
- C. AH provides data integrity but no encryption.
- D. AH provides strong data integrity but weak encryption.

Answer: C

NEW QUESTION 231

When configuring a firewall virtual wire pair policy, which following statement is true?

- A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
- B. Only a single virtual wire pair can be included in each policy.
- C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
- D. Exactly two virtual wire pairs need to be included in each policy.

Answer: A

NEW QUESTION 236

Refer to the exhibit.



Which contains a network diagram and routing table output. The Student is unable to access Webservice. What is the cause of the problem and what is the solution for the problem?

- A. The first packet sent from Student failed the RPF check. This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
- B. The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
- C. The first reply packet for Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.
- D. The first packet sent from Student failed the RPF check. This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

Answer: D

NEW QUESTION 239

Refer to the exhibit showing a debug flow output.

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

Which two statements about the debug flow output are correct? (Choose two.)

- A. The debug flow is of ICMP traffic.
- B. A firewall policy allowed the connection.
- C. A new traffic session is created.
- D. The default route is required to receive a reply.

Answer: AC

NEW QUESTION 244

Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

- A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.
- B. The application signature database inspects traffic only from the original web application server.
- C. FortiGuard maintains only one signature of each web application that is unique.
- D. FortiGate can inspect sub-application traffic regardless where it was originate

Answer: D

NEW QUESTION 247

Which three methods are used by the collector agent for AD polling? (Choose three.)

- A. FortiGate polling
- B. NetAPI
- C. Novell API
- D. WMI
- E. WinSecLog

Answer: BDE

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.127-128): "As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended: (WMI, WinSecLog, and NetAPI)"

NEW QUESTION 249

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4_FGT-7.2 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT-7.2/

Money Back Guarantee

NSE4_FGT-7.2 Practice Exam Features:

- * NSE4_FGT-7.2 Questions and Answers Updated Frequently
- * NSE4_FGT-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year