

Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)

<https://www.2passeasy.com/dumps/NSE4/>



NEW QUESTION 1

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 2

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 3

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 4

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 5

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 6

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

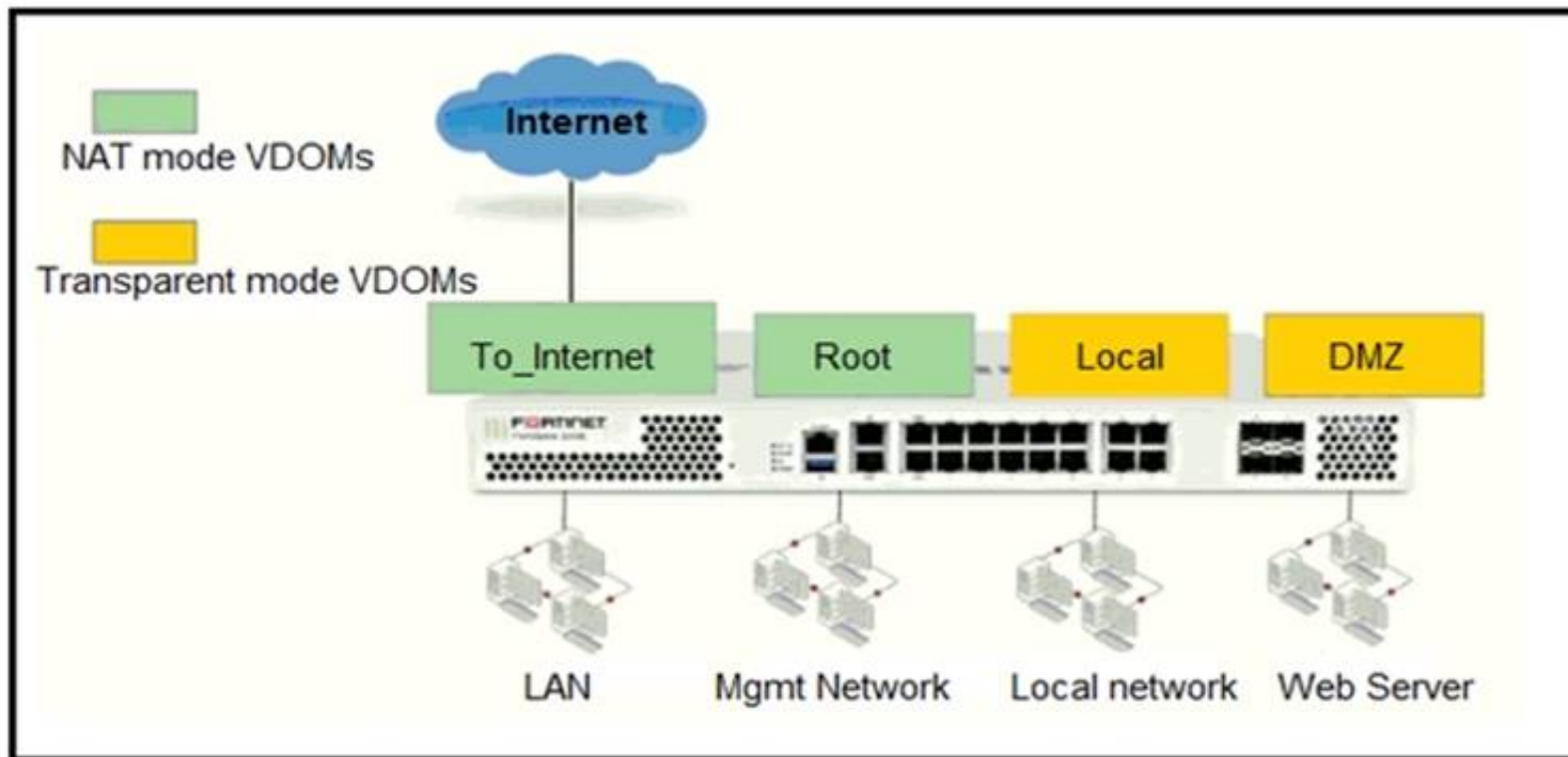
Answer: D

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 7

Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode. The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem .
 With this configuration, which statement is true?

- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
- B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

NEW QUESTION 8

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.

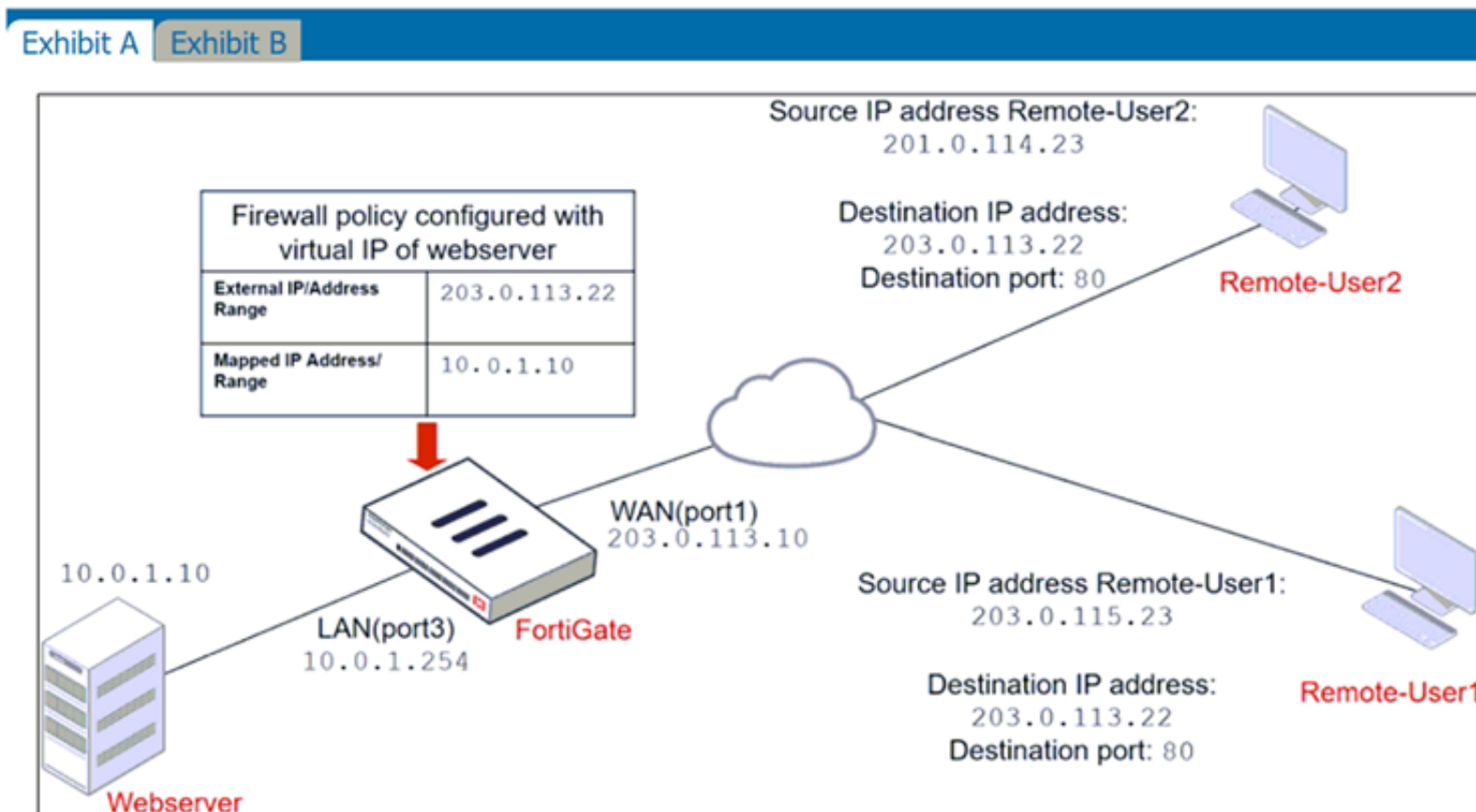


Exhibit A Exhibit B

Edit Address

Name

Deny_IP

Color

Change

Type

Subnet

IP/Netmask

201.0.114.23/32

Interface

WAN (port1)

Static route configuration

☐

Comments

Deny web server access. 23/255

Firewall address object

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: CD

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta>

NEW QUESTION 9

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 10

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 sourcesand 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 10

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.

NEW QUESTION 15

By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

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

Answer: A

Explanation:

By default, "fortiguard-anycast" is enabled, and this setting only works with "set protocol https". To use udp (ie. "set protocol udp"), "fortiguard-anycast" must be disabled.

NEW QUESTION 17

Examine this FortiGate configuration:

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

Answer: D

Explanation:

"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

NEW QUESTION 18

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?

- A. The administrator can register the same FortiToken on more than one FortiGate.
- B. The administrator must use a FortiAuthenticator device
- C. The administrator can use a third-party radius OTP server.
- D. The administrator must use the user self-registration server.

Answer: B

NEW QUESTION 19

Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)

- A. Security policy
- B. SSL inspection and authentication policy CD

Answer: AB

NEW QUESTION 22

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 25

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 28

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.

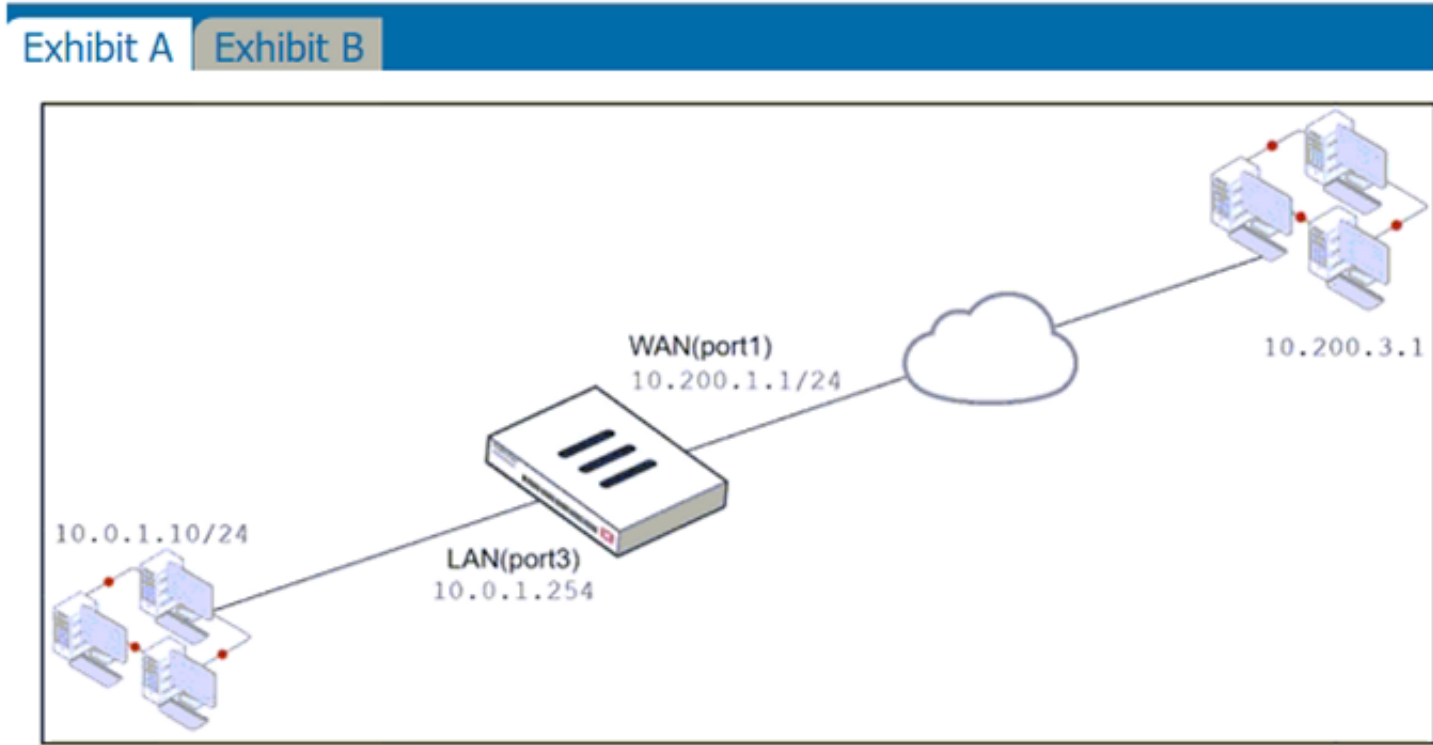


Exhibit B

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, 10.0.1.10, and 10443, respectively
- C. 10.200.3.1, 10.0.1.10, and 443, respectively

Answer: C

NEW QUESTION 32

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 34

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 37

Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

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

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

Answer: CD

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf>

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883>

NEW QUESTION 39

On FortiGate, which type of logs record information about traffic directly to and from the FortiGate management IP addresses?

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

Answer: C

NEW QUESTION 44

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.

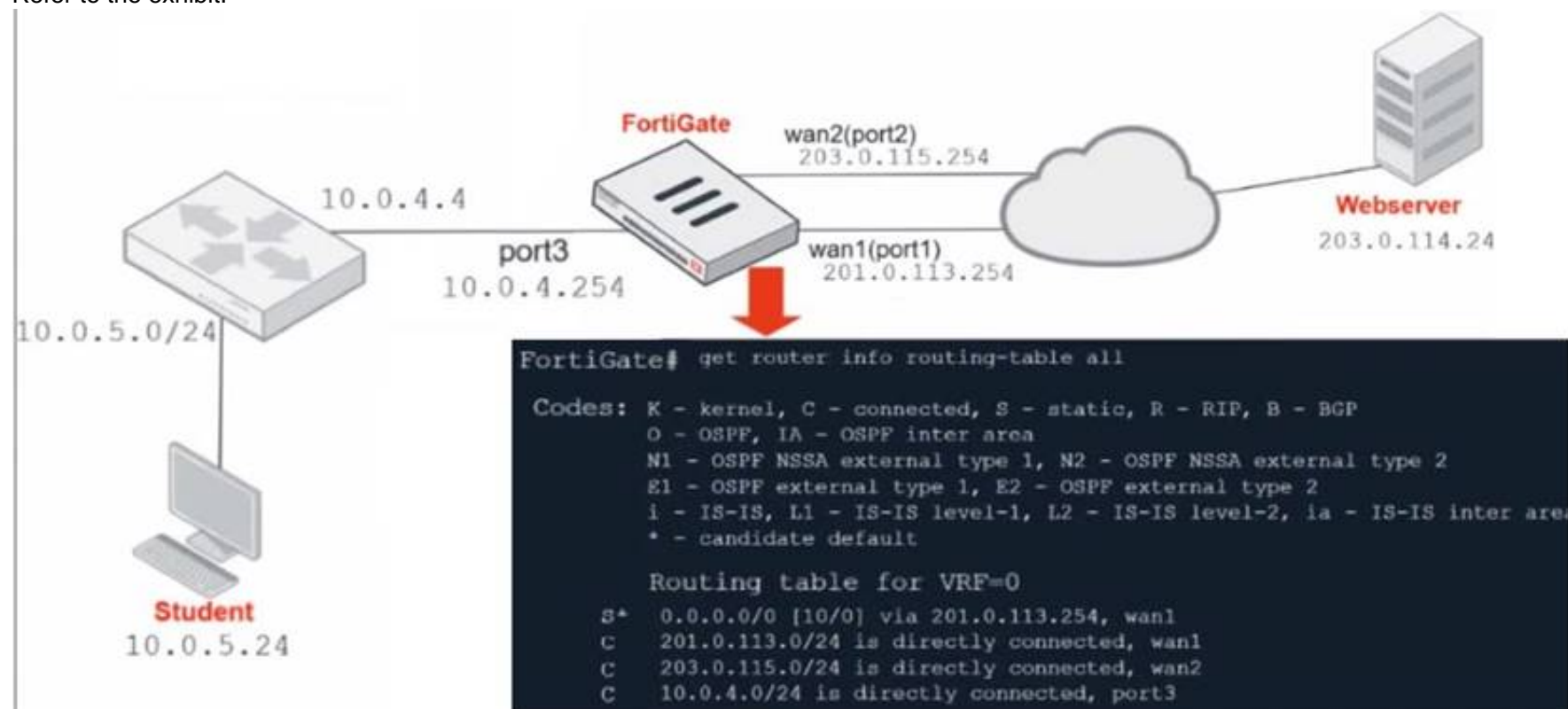
Answer: D

Explanation:

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

NEW QUESTION 47

Refer to the exhibit.



Which contains a network diagram and routing table output. The Student is unable to access Webserver.

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 51

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

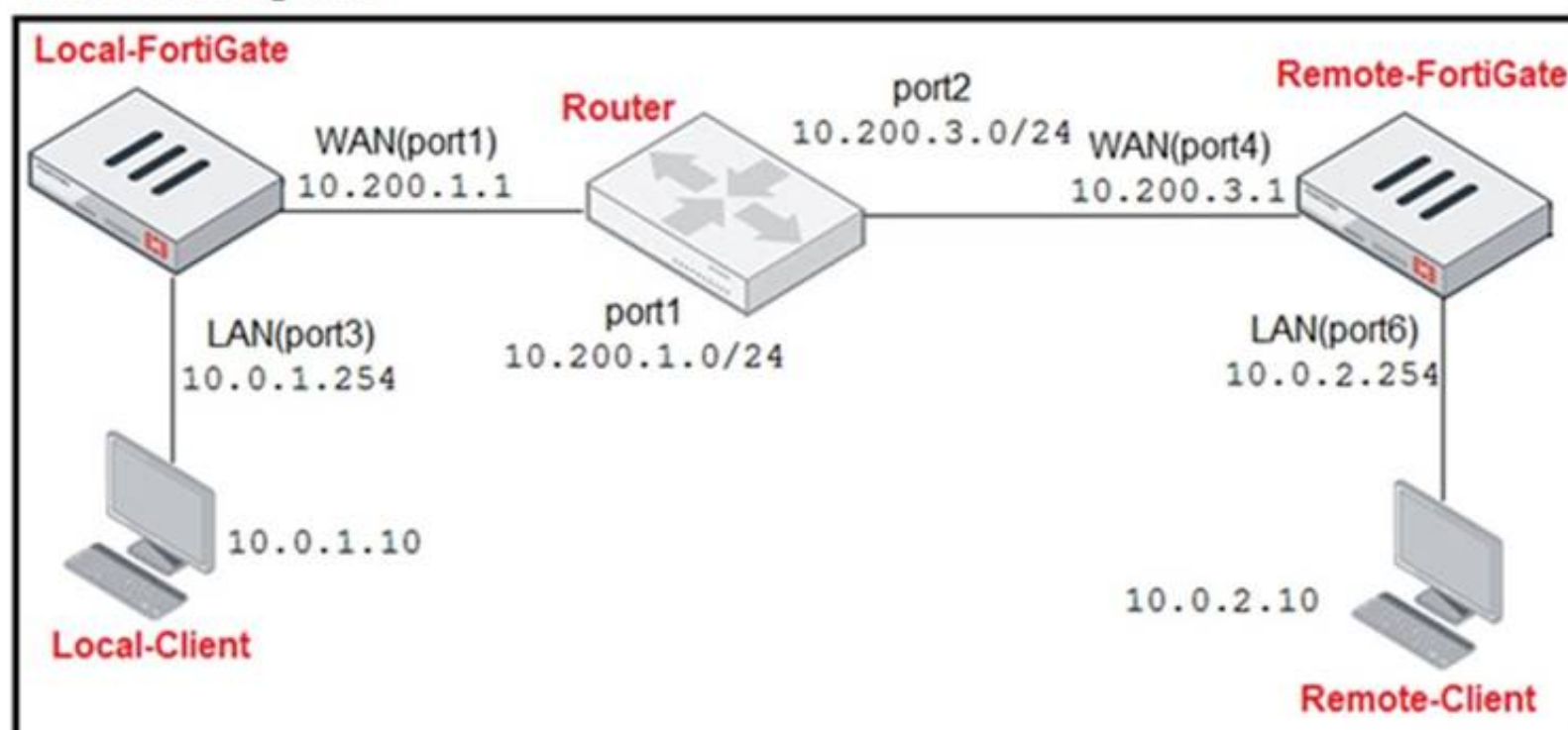
- A. IPS engine handles the process as a standalone.
- B. FortiGate buffers the whole file but transmits to the client simultaneously.
- C. If the virus is detected, the last packet is delivered to the client.
- D. Optimized performance compared to proxy-based inspection.
- E. Flow-based inspection uses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

Answer: BDE

NEW QUESTION 52

Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

+ Create New Edit Delete Search Q						
ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

+ Create New Edit Clone Delete Search Q			
Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	Enabled

Protocol Number Table

Protocol Number Table	
Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool 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. A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied. Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0. 1. 10) pings the IP address of Remote-FortiGate (10.200.3. 1)?

A. 10.200. 1. 149
B. 10.200. 1. 1
C. 10.200. 1.49
D. 10.200. 1.99

Answer: D

NEW QUESTION 55

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

A. The Services field prevents SNAT and DNAT from being combined in the same policy.
B. The Services field is used when you need to bundle several VIPs into VIP groups.
C. The Services field removes the requirement to create multiple VIPs for different services.
D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

Answer: C

NEW QUESTION 59

An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value. Which timeout option should be configured on FortiGate?

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

Answer: E

NEW QUESTION 63

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

NEW QUESTION 64

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Edit Policy

Inspection Mode **Flow-based** Proxy-based

Firewall / Network Options

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address**
Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options **PRX** default

Security Profiles

AntiVirus ☒ **AV** default

Web Filter ☐

DNS Filter ☐

Application Control ☐

IPS ☐

SSL Inspection **SSL** deep-inspection

Decrypted Traffic Mirror ☐

Edit AntiVirus Profile

Name default

Comments Scan files and block viruses. 29/255

Detect Viruses **Block** Monitor

Feature set **Flow-based** Proxy-based

Inspected Protocols

HTTP ☒

SMTP ☒

POP3 ☒

IMAP ☒

FTP ☒

CIFS ☐

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ☒

Include Mobile Malware Protection ☒

Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database ☐

Use External Malware Block List ⓘ ⚠ ☐

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: B

Explanation:

· "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately

· When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.

In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

NEW QUESTION 66

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 68

An administrator is running the following sniffer command:

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 72

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 73

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 77

An organization's employee needs to connect to the office through a high-latency internet connection. Which SSL VPN setting should the administrator adjust to prevent the SSL VPN negotiation failure?

- A. Change the session-ttl.
- B. Change the login timeout.
- C. Change the idle-timeout.
- D. Change the udp idle timer.

Answer: B

NEW QUESTION 79

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 83

Which statement is correct regarding the use of application control for inspecting web applications?

- A. Application control can identity child and parent applications, and perform different actions on them.
- B. Application control signatures are organized in a nonhierarchical structure.
- C. Application control does not require SSL inspection to identity web applications.
- D. Application control does not display a replacement message for a blocked web application.

Answer: A

Explanation:

Application control is a feature that allows FortiGate to inspect and control the use of specific web applications on the network. When application control is enabled, FortiGate can identify child and parent applications, and can perform different actions on them based on the configuration.

NEW QUESTION 85

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 86

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 90

Refer to the exhibit.



The screenshot shows the FortiGate SLA configuration interface. The Name field is set to SLA1. The Protocol is set to Ping. The Server field has two entries: 4.2.2.2 and 4.2.2.1. The Participants field is set to All SD-WAN Members. 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 95

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-Filter
Status      : Enable
License     : Contract

Num. of servers : 3
Protocol     : https
Port         : 443
Anycast      : Disable
Default servers : Included
-- Server List (Mon Jul 5 12:00:25 2021) --

IP           Weight  RTT  Flags  TZ  FortiGuard-requests  Curr  Lost  Total  Lost  Updated Time
173.243.138.210  10    350  DI    -8    29      0    0      0      0    Mon Jul 5 09:23:33 2021
12.34.97.18     20    30   -5    -5    25      0    0      0      0    Mon Jul 5 09:23:33 2021
210.7.96.18     160   605   9     9    25      0    0      0      0    Mon Jul 5 09:23:33 2021
```

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

- A. A local FortiManager is one of the servers FortiGate communicates with.
- B. One server was contacted to retrieve the contract information.
- C. There is at least one server that lost packets consecutively.
- D. FortiGate is using default FortiGuard communication settings.

Answer: BD

NEW QUESTION 97

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4 Product From:

<https://www.2passeasy.com/dumps/NSE4/>

Money Back Guarantee

NSE4 Practice Exam Features:

- * NSE4 Questions and Answers Updated Frequently
- * NSE4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year