

Fortinet

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 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

Refer to the exhibits.

Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.

Exhibit A **Exhibit B**

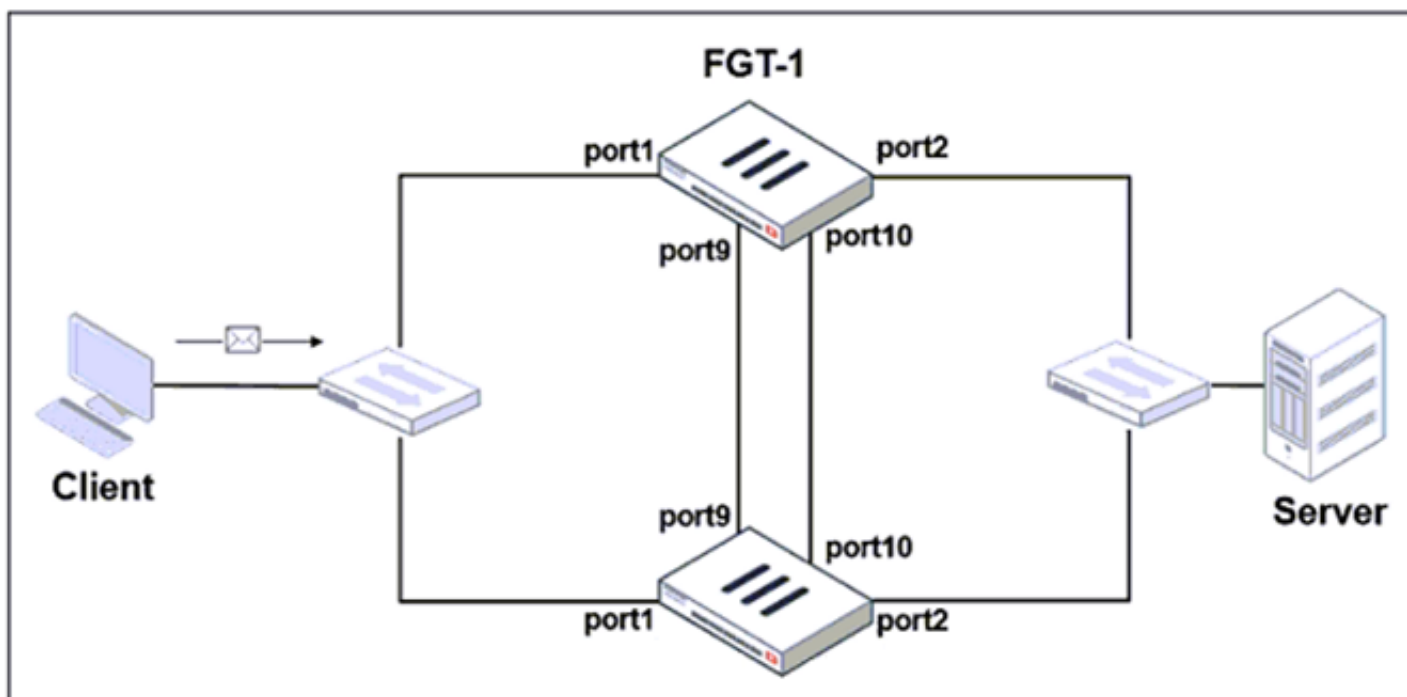


Exhibit A **Exhibit B**

```
set group-id 3
set group-name "NSE"
set mode a-a
set password *
set hbdev "port9" 50 "port10" 50
set session-pickup enable
set override disable
set monitor port3
end

# get system ha status
...
Primary      : FGT-2, FGVM010000065036, HA cluster index = 1
Secondary    : FGT-1, FGVM010000064692, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000065036, HA operating index = 1
Secondary: FGVM010000064692, HA operating index = 0
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

- A. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.
- B. The traffic sourced from the client and destined to the server is sent to FGT-1.
- C. The cluster can load balance ICMP connections to the secondary.
- D. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

Answer: AD

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.317 & p.320): "To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses." "The primary forwards the SYN packet to the selected secondary. (...) This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic."

NEW QUESTION 3

An administrator wants to simplify remote access without asking users to provide user credentials. Which access control method provides this solution?

- A. ZTNA IP/MAC filtering mode
- B. ZTNA access proxy
- C. SSL VPN
- D. L2TP

Answer: B

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.165): "ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs."

This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials. ZTNA access proxy uses a secure tunnel between the user's device and the FortiGate, and authenticates the user based on device identity and context. The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile. This simplifies remote access and enhances security by reducing the attack surface¹²

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

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 6

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 July 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		Mon Jul 5 09:23:33 2021
12.34.97.18	20	30		-5	25	0		0		Mon Jul 5 09:23:33 2021
210.7.96.18	160	605		9	25	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

Explanation:

FortiGate Security 7.2 Study Guide (p.287-288): "Flags: D (IP returned from DNS), I (Contract server contacted), T (being timed), F (failed)" "By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. Other ports and protocols are available by disabling the FortiGuard anycast setting on the CLI."

NEW QUESTION 7

An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192. 168. 1.0/24 and the remote quick mode selector is 192. 168.2.0/24. Which subnet must the administrator configure for the local quick mode selector for site B?

- A. 192. 168. 1.0/24
- B. 192. 168.0.0/24
- C. 192. 168.2.0/24
- D. 192. 168.3.0/24

Answer: C

Explanation:

For an IPsec VPN between site A and site B, the administrator has configured the local quick mode selector for site A as 192.168.1.0/24 and the remote quick mode selector as 192.168.2.0/24. This means that the VPN will allow traffic to and from the 192.168.1.0/24 subnet at site A to reach the 192.168.2.0/24 subnet at site B.

To complete the configuration, the administrator must configure the local quick mode selector for site B. To do this, the administrator must use the same subnet as the remote quick mode selector for site A, which is 192.168.2.0/24. This will allow traffic to and from the 192.168.2.0/24 subnet at site B to reach the 192.168.1.0/24 subnet at site A.

Therefore, the administrator must configure the local quick mode selector for site B as 192.168.2.0/24.

NEW QUESTION 8

Which statement about the policy ID number of a firewall policy is true?

- A. It is required to modify a firewall policy using the CLI.
- B. It represents the number of objects used in the firewall policy.
- C. It changes when firewall policies are reordered.
- D. It defines the order in which rules are processed.

Answer: A

NEW QUESTION 9

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 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 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 10

Refer to the exhibit.

Add Signatures

Type

Filter

Signature

Action

Block

Packet logging

Enable

Disable

Status

Enable

Disable

Default

Rate-based settings

Default

Specify

Exempt IPs

0

Edit IP Exemptions

Search

Q

Selected 1

All

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1					
FTP.Login.Failed		Server	All	Pass	

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.

Answer: D

Explanation:

Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be 'Pass' for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be 'Default'. Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

NEW QUESTION 12

Refer to the exhibit.
The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.
An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.

Edit Web Filter Profile

Name

Corporate

Comments

Write a comment...

0/255

Feature set

Flow-based

Proxy-based

FortiGuard Category Based Filter

Allow

Monitor

Block

Warning

Authenticate

Name	Action
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Allow
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	
Malicious Websites	Block

35% 91

What are two solutions for satisfying the requirement? (Choose two.)

- A. Configure a separate firewall policy with action Deny and an FQDN address object for *.download.com as destination address.
- B. Configure a web override rating for download.com and select Malicious Websites as the subcategory.
- C. Set the Freeware and Software Downloads category Action to Warning.
- D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

Answer: BD

Explanation:

FortiGate Security 7.2 Study Guide (p.268-269): "If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. You can block a website that belongs to an allowed category." "Static URL filtering is another web filter feature. Configured URLs in the URL filter are checked against the visited websites. If a match is found, the configured action is taken. URL filtering has the same patterns as static domain filtering: simple, regular expressions, and wildcard."
* B. Configure a web override rating for download.com and select Malicious Websites as the subcategory. This is true because a web override rating is a feature that allows the administrator to change the FortiGuard category of a specific website or domain, and apply a different action to it based on the web filter profile. By configuring a web override rating for download.com and selecting Malicious Websites as the subcategory, the administrator can block access to download.com, which belongs to the Freeware and Software Downloads category by default, without affecting other websites in the same category. The Malicious Websites category has the action Block in the web filter profile shown in the exhibit.

* D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

This is true because a static URL filter entry is a feature that allows the administrator to define custom rules for filtering specific URLs or domains, and apply an action to them based on the web filter profile. By configuring a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively, the administrator can block access to download.com and any subdomains or paths under it, without affecting other websites in the Freeware and Software Downloads category. The static URL filter entries have higher priority than the FortiGuard category based filter entries in the web filter profile.

NEW QUESTION 16

What are two functions of the ZTNA rule? (Choose two.)

- A. It redirects the client request to the access proxy.
- B. It applies security profiles to protect traffic.
- C. It defines the access proxy.
- D. It enforces access control.

Answer: BD

Explanation:

A ZTNA rule is a policy that enforces access control and applies security profiles to protect traffic between the client and the access proxy1. A ZTNA rule defines the following parameters1:

- Incoming interface: The interface that receives the client request.
- Source: The address and user group of the client.
- ZTNA tag: The tag that identifies the domain that the client belongs to.
- ZTNA server: The server that hosts the access proxy.
- Destination: The address of the application that the client wants to access.
- Action: The action to take for the traffic that matches the rule. It can be accept, deny, or redirect.
- Security profiles: The security features to apply to the traffic, such as antivirus, web filter, application control, and so on.

A ZTNA rule does not redirect the client request to the access proxy. That is the function of a policy route that matches the ZTNA tag and sends the traffic to the ZTNA server2.

A ZTNA rule does not define the access proxy. That is done by creating a ZTNA server object that specifies the IP address, port, and certificate of the access proxy3.

FortiGate Infrastructure 7.2 Study Guide (p.177): "A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic."

NEW QUESTION 17

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 21

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 26

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 31

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 35

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

- A. The keyUsage extension must be set to keyCertSign.
- B. The common name on the subject field must use a wildcard name.
- C. The issuer must be a public CA.
- D. The CA extension must be set to TRUE.

Answer: AD

Explanation:

"In order for FortiGate to act in these roles, its CA certificate must have the basic constraints extension set to cA=True and the value of the keyUsage extension set to keyCertSign."

NEW QUESTION 36

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 39

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 44

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 46

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 47

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

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

Answer: CD

NEW QUESTION 50

Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
  pingsvr_flip_timeout/expire=3600s/2781s
  'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
  'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster. Which two statements are true? (Choose two.)

- A. FortiGate SN FGVM010000065036 HA uptime has been reset.
- B. FortiGate devices are not in sync because one device is down.
- C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- D. FortiGate SN FGVM010000064692 has the higher HA priority.

Answer: AD

Explanation:

* 1. Override is disable by default - OK
 * 2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary"
 The QUESTION NO: here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.
<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab>

NEW QUESTION 53

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

Answer: AC

NEW QUESTION 54

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

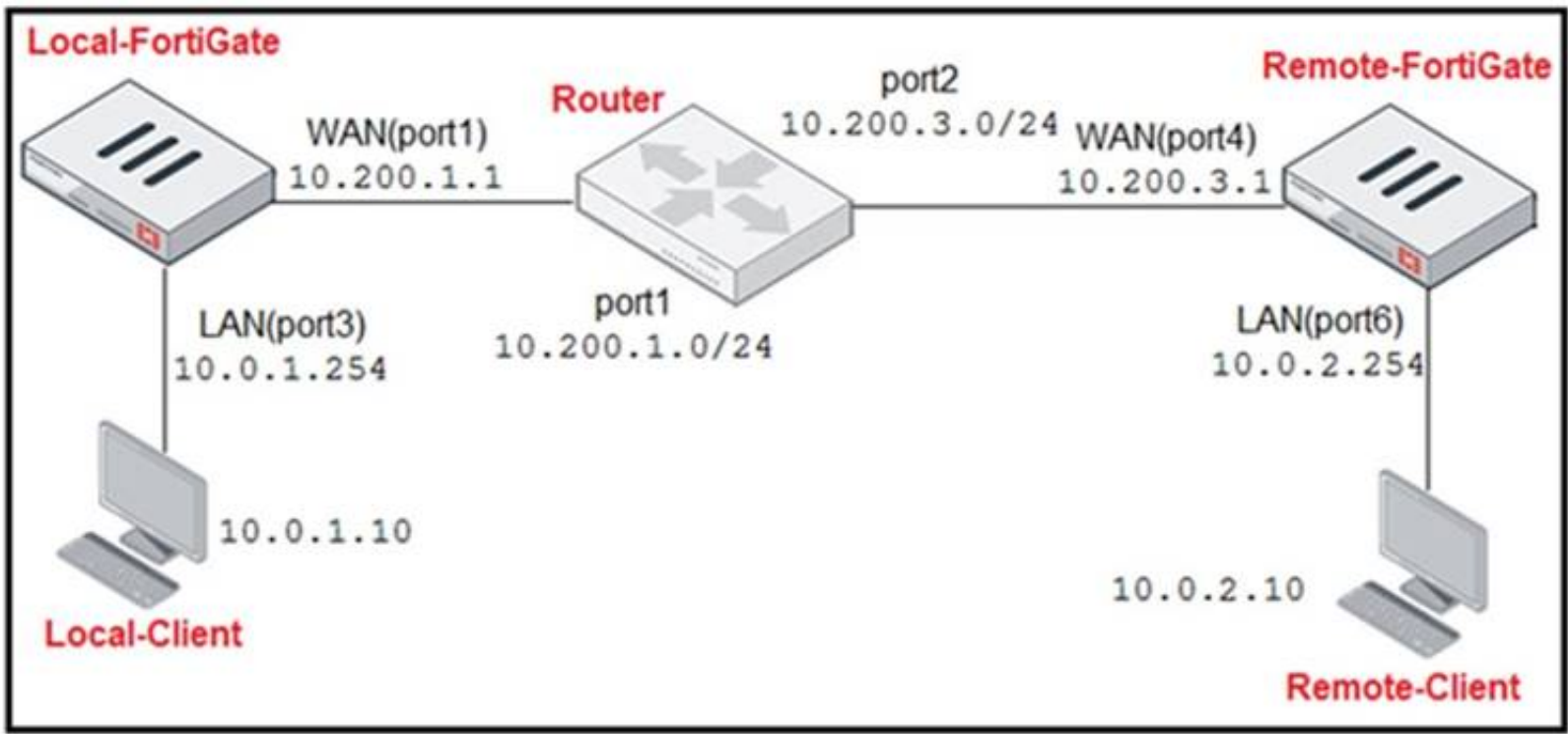
- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase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

Answer: AC

NEW QUESTION 59

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 63

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings. What is true about the DNS connection to a FortiGuard server?

A. It uses UDP 8888.
B. It uses UDP 53.
C. It uses DNS over HTTPS.
D. It uses DNS overTLS.

Answer: D

Explanation:

FortiGate Security 7.2 Study Guide (p.15): "When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic." When using FortiGuard servers for DNS, FortiOS defaults to using DNS over TLS (DoT) to secure the DNS traffic1. DNS over TLS is a protocol that encrypts and authenticates DNS queries and responses using the Transport Layer Security (TLS) protocol2. This prevents eavesdropping, tampering, and spoofing of DNS data by third parties. The default FortiGuard DNS servers are 96.45.45.45 and 96.45.46.46, and they use the hostname globalsdns.fortinet.net1. The FortiGate verifies the server hostname using the server-hostname setting in the system dns configuration1.

NEW QUESTION 68

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 73

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 75

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 76

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 80

Refer to the exhibit.



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 84

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

- A. To detect intermediary NAT devices in the tunnel path.
- B. To dynamically change phase 1 negotiation mode aggressive mode.
- C. To encapsulation ESP packets in UDP packets using port 4500.
- D. To force a new DH exchange with each phase 2 rekey.

Answer: AC

NEW QUESTION 87

An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192. 16. 1.0/24 and the remote quick mode selector is 192. 16.2.0/24. How must the administrator configure the local quick mode selector for site B?

- A. 192. 168.3.0/24
- B. 192. 168.2.0/24
- C. 192. 168. 1.0/24
- D. 192. 168.0.0/8

Answer: B

NEW QUESTION 88

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 91

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 95

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 97

Refer to the web filter raw logs.

```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web" action="blocked"
reqtype="direct" url="https://twitter.com/" sentbyte=517
rcvdbyte=0 direction="outgoing" msg="URL belongs to a category
with warnings enabled" method="domain" cat=37 catdesc="Social
Networking"

date=2020-07-09 time=12:52:16 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313537024536428 tz="-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web"
action="passthrough" reqtype="direct" url="https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction="outgoing" msg="URL belongs to
a category with warnings enabled" method="domain" cat=37
catdesc="Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

- A. Social networking web filter category is configured with the action set to authenticate.
- B. The action on firewall policy ID 1 is set to warning.
- C. Access to the social networking web filter category was explicitly blocked to all users.
- D. The name of the firewall policy is all_users_web.

Answer: A

NEW QUESTION 98

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 101

FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.

Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

- A. www.example.com:443
- B. www.example.com
- C. example.com
- D. www.example.com/index.html

Answer: BC

Explanation:

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names - no URLs or wildcard characters are allowed.

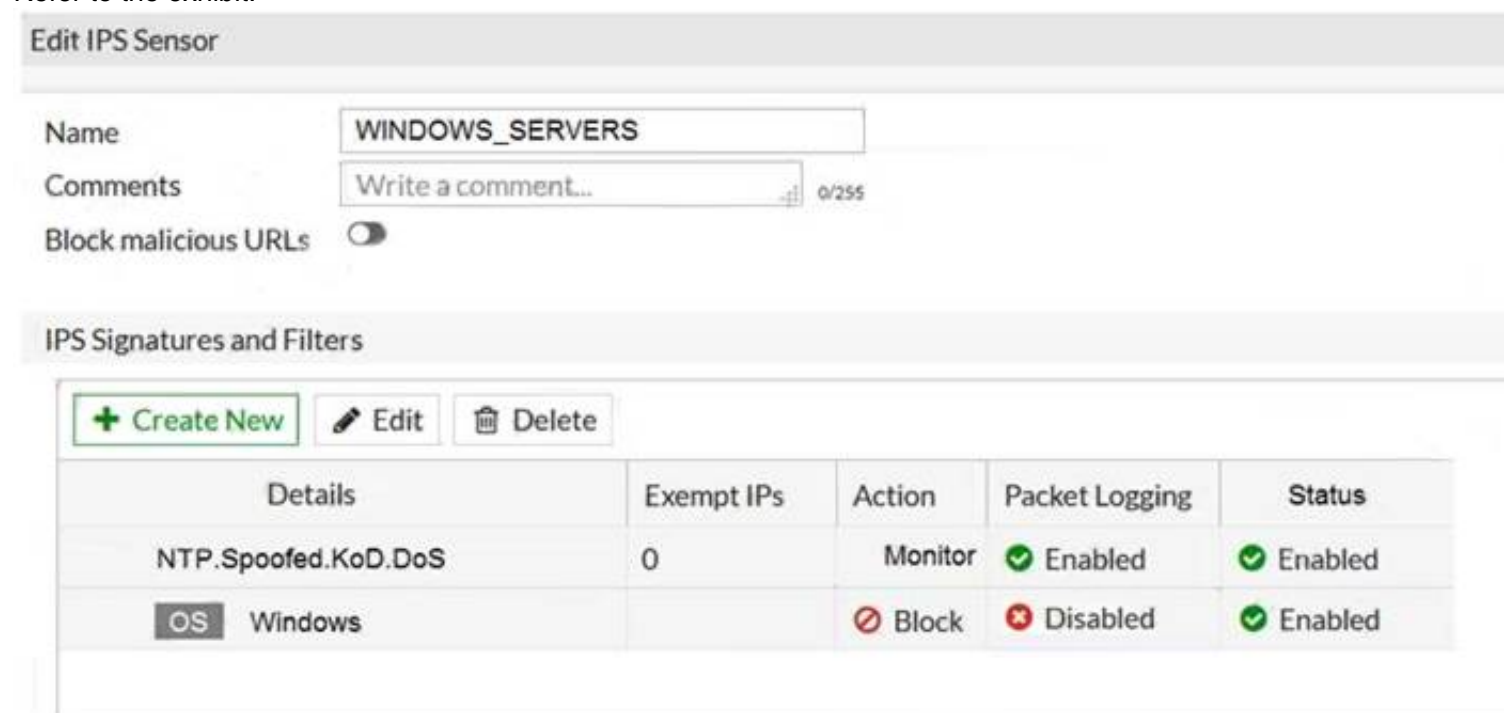
OK: google.com or www.google.com

NO OK: www.google.com/index.html or google.* FortiGate_Security_6.4 page 384

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names-- "no URLs or wildcard characters are allowed".

NEW QUESTION 102

Refer to the exhibit.



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 107

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

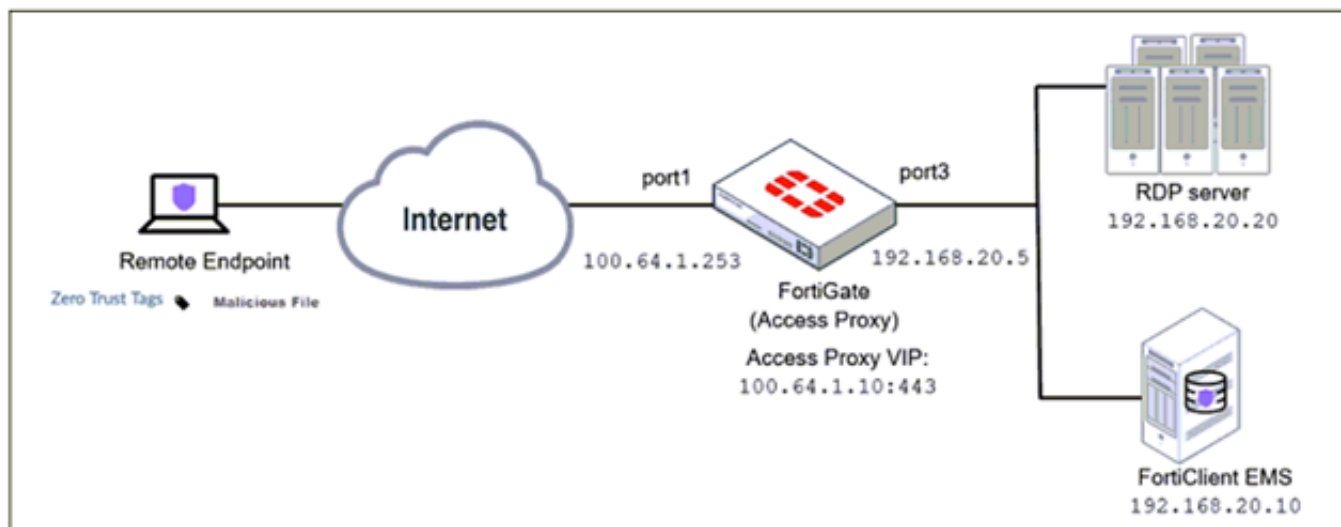
Answer: A

Explanation:

y 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 108

Refer to the exhibit.



Based on the ZTNA tag, the security posture of the remote endpoint has changed. What will happen to endpoint active ZTNA sessions?

- A. They will be re-evaluated to match the endpoint policy.
- B. They will be re-evaluated to match the firewall policy.
- C. They will be re-evaluated to match the ZTNA policy.
- D. They will be re-evaluated to match the security policy.

Answer: C

Explanation:

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-zt> FortiGate Infrastructure 7.2 Study Guide (p.182):
 "Endpoint posture changes trigger active ZTNA proxy sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy."

NEW QUESTION 111

Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

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

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=13900> <https://www.fortinetguru.com/2016/03/what-is-policy-id-0-and-why-lot-of-denied-traffic-on-this-policy/>

NEW QUESTION 112

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 115

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 116

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.

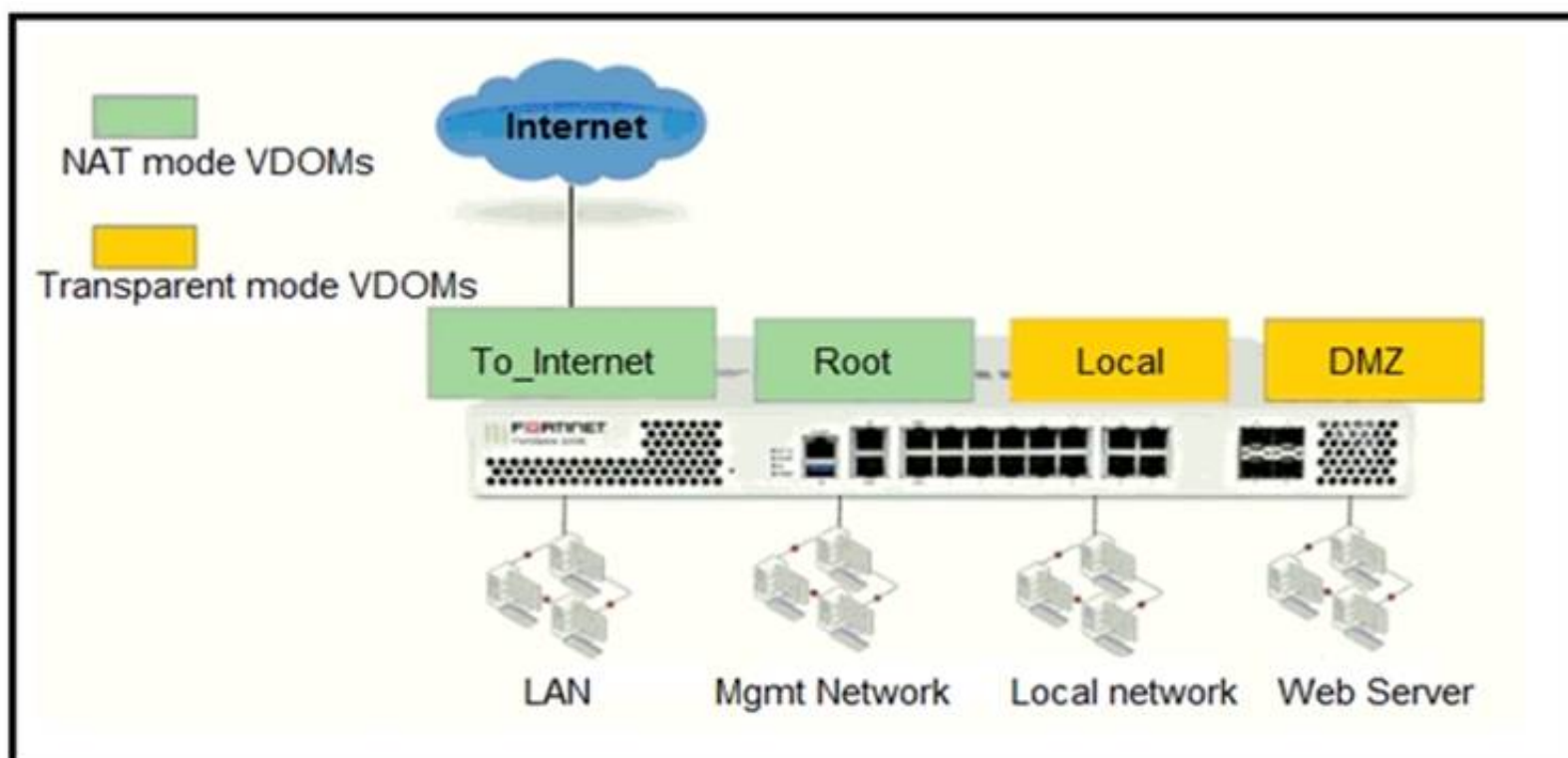
Answer: BC

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 118

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 121

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 125

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 128

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 132

Which of the following are valid actions for FortiGuard category based filter in a web filter profile in proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

Answer: AC

NEW QUESTION 134

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 139

Consider the topology:

Application on a Windows machine <--(SSL VPN) --> FGT --> Telnet to Linux server.

An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.

The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

- A. Set the maximum session TTL value for the TELNET service object.
- B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.
- C. Create a new service object for TELNET and set the maximum session TTL.
- D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Answer: CD

NEW QUESTION 142

An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

- A. VLAN interface
- B. Software Switch interface
- C. Aggregate interface
- D. Redundant interface

Answer: C

Explanation:

An aggregate interface is a logical interface that combines two or more physical interfaces into one virtual interface¹. An aggregate interface can increase network bandwidth and provide redundancy by distributing traffic across multiple physical interfaces using a load balancing algorithm¹. An aggregate interface can also support link aggregation control protocol (LACP) to negotiate the link aggregation settings with the connected device¹.

NEW QUESTION 143

Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack .
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

Answer: A

Explanation:

fortinet-fortigate-security-study-guide-for-fortios-72 page 417 If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

NEW QUESTION 147

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 150

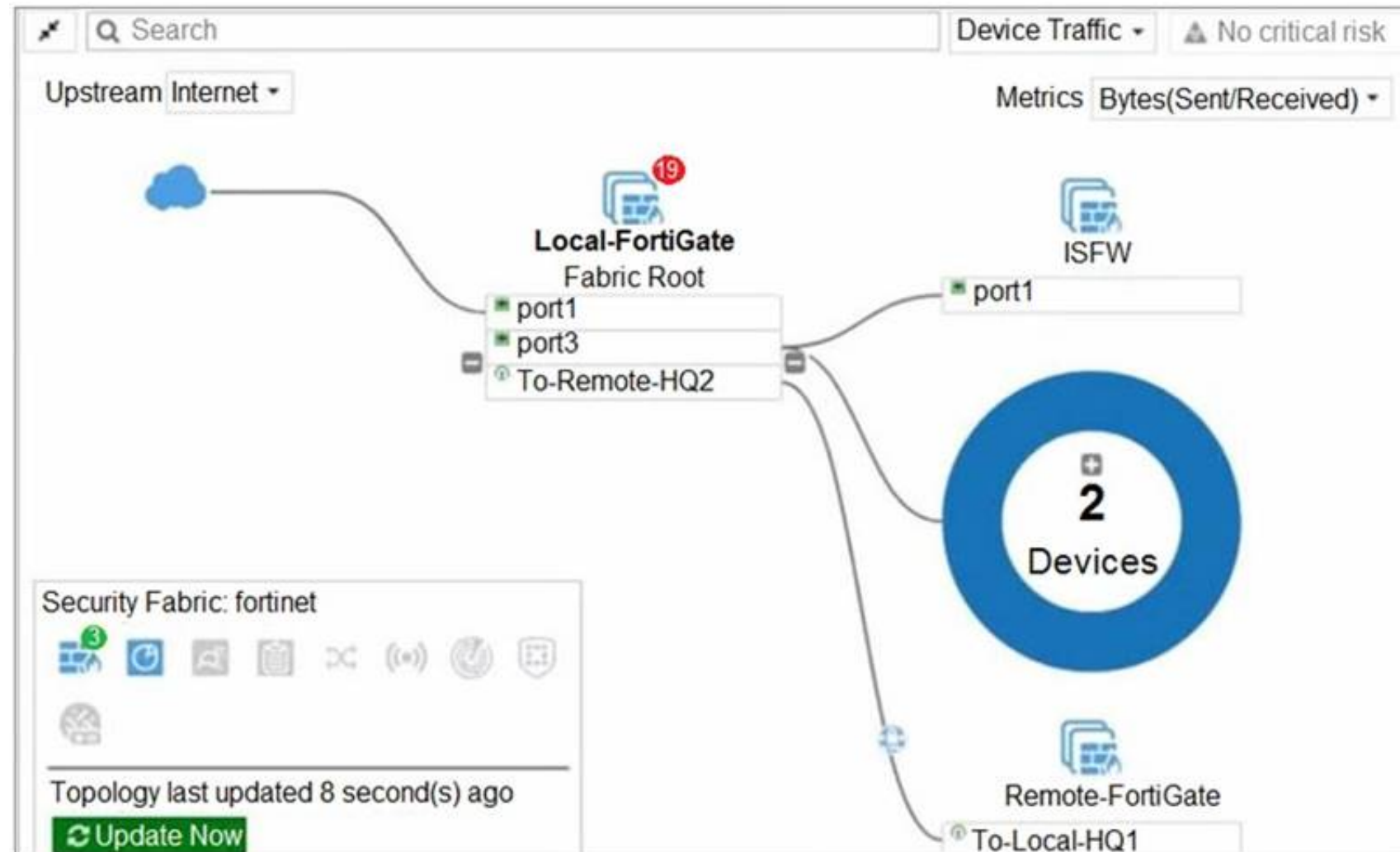
Which two statements are correct about NGFW Policy-based mode? (Choose two.)

- 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 152

Refer to the exhibit.



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

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

Answer: CD

Explanation:

References: <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results>
<https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology>

NEW QUESTION 157

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

- A. Subject Key Identifier value
- B. SMMIE Capabilities value
- C. Subject value
- D. Subject Alternative Name value

Answer: A

NEW QUESTION 161

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 166

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.

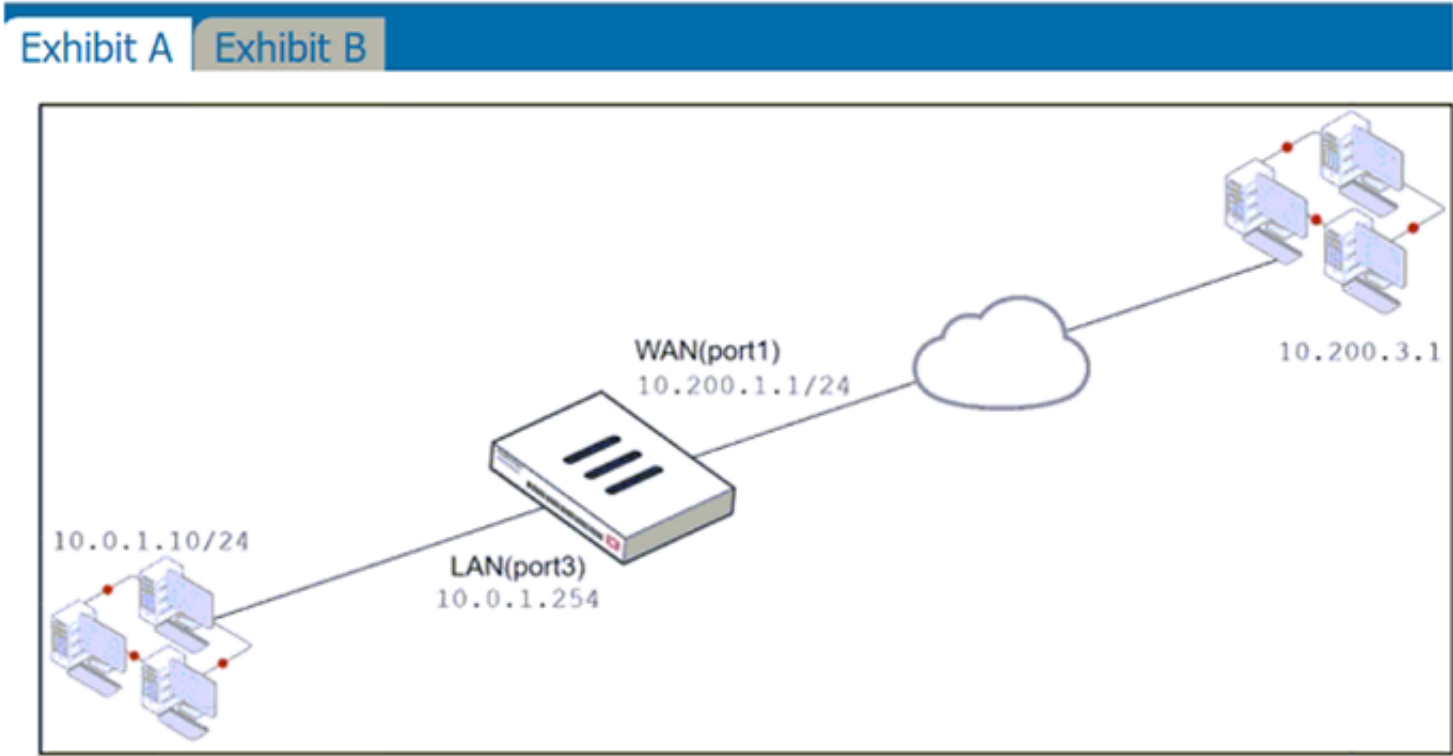


Exhibit A Exhibit B

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 167

Refer to the exhibit.

Exhibit A Exhibit B

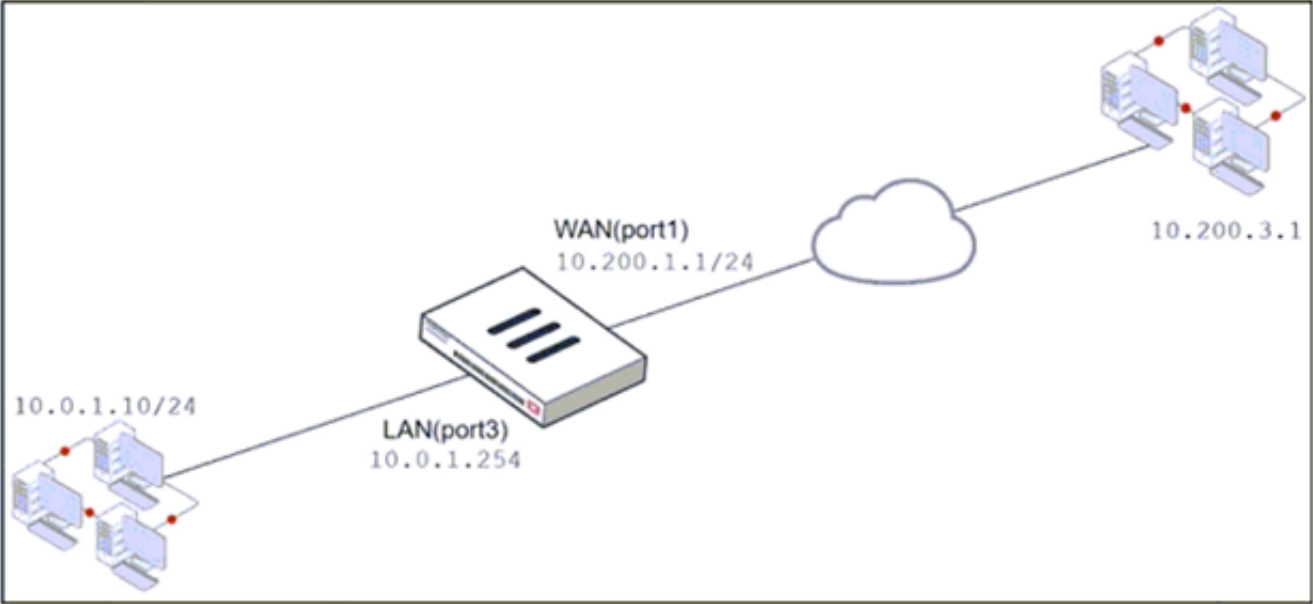


Exhibit AExhibit B

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

Edit Virtual IP

VIP type

IPv4

Name

VIP

Comments

Write a comment...

Color

Change

Network

Interface

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

TCPUDP SCTP ICMP

Port Mapping Type

One to oneMany to many

External service port

443

Map to IPv4 port

443

Edit Dynamic IP Pool

Name

IP Pool

Comments

Write a comment...

Type

OverloadOne-to-OneFixed Port RangePort Block Allocation

External IP address/range

10.200.1.100-10.200.1.100

NAT64

ARP Reply

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies 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 first firewall policy has NAT enabled using IP Pool. 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?

- A. 10.200. 1. 1
- B. 10.200.3. 1
- C. 10.200. 1. 100
- D. 10.200. 1. 10

Answer: C

Explanation:

Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

NEW QUESTION 169

An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

- A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
- B. Create a new service object for HTTP service and set the session TTL to never
- C. Set the TTL value to never under config system-ttl
- D. Set the session TTL on the HTTP policy to maximum

Answer: BC

NEW QUESTION 171

Which statement about video filtering on FortiGate is true?

- A. Full SSL Inspection is not required.
- B. It is available only on a proxy-based firewall policy.
- C. It inspects video files hosted on file sharing services.
- D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Answer: B

NEW QUESTION 172

Which statement about video filtering on FortiGate is true?

- A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.
- B. It does not require a separate FortiGuard license.
- C. Full SSL inspection is not required.
- D. its available only on a proxy-based firewall policy.

Answer: D

Explanation:

FortiGate Security 7.2 Study Guide (p.279): "To apply the video filter profile, proxy-based firewall policies currently allow you to enable the video filter profile. You must enable full SSL inspection on the firewall policy."

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/860867/filtering-based-on-fortiguard-cat>

NEW QUESTION 175

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 177

Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53->10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

- A. The session is a UDP unidirectional state.
- B. The session is in TCP ESTABLISHED state.
- C. The session is a bidirectional UDP connection.
- D. The session is a bidirectional TCP connection.

Answer: C

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 180

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 183

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

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

Answer: ADE

Explanation:

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

NEW QUESTION 186

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT-7.2 Practice Test Here](#)