

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

https://www.2passeasy.com/dumps/NSE4_FGT-7.0/



NEW QUESTION 1

- (Exam Topic 1)

Refer to the exhibit.

The screenshot shows the configuration for an SD-WAN Performance SLA. The 'Outgoing Interfaces' section has four options: 'Manual', 'Best Quality' (selected), 'Lowest Cost (SLA)', and 'Maximize Bandwidth (SLA)'. The 'Interface preference' list includes port1, port2, port3, and port4. The 'Measured SLA' is 'SLA_1' and the '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:

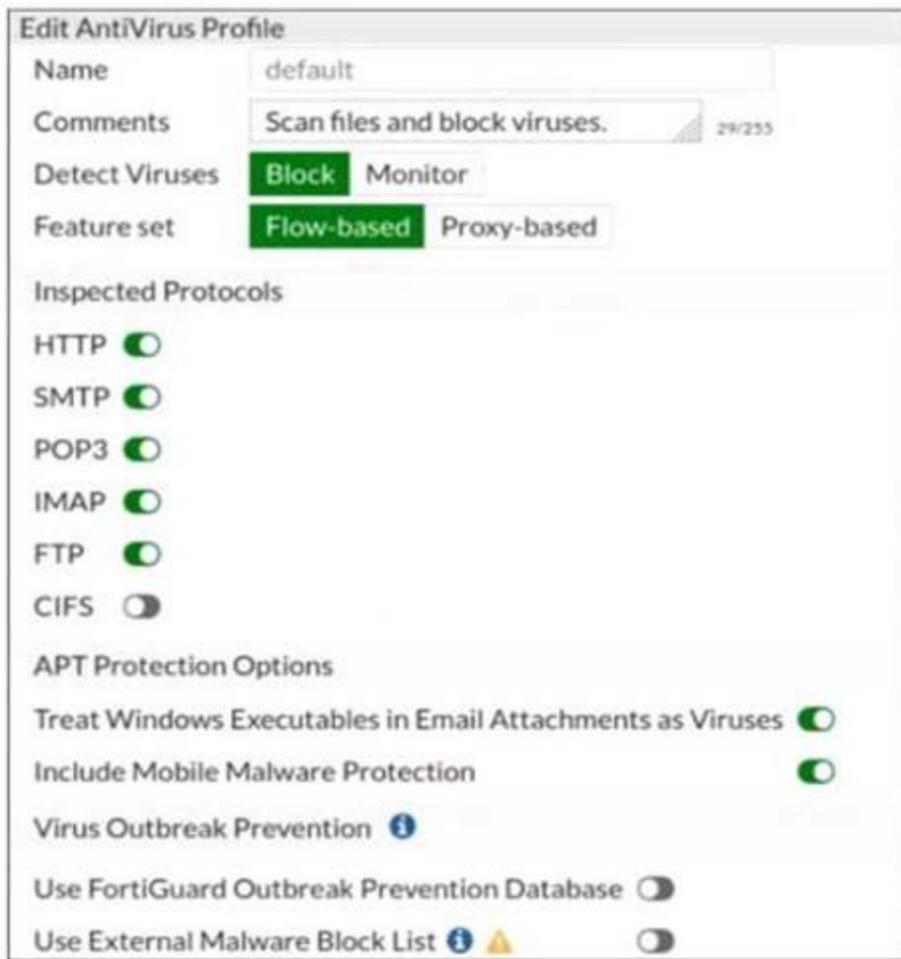
Port 1 shows the lowest latency.

NEW QUESTION 2

- (Exam Topic 1)

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

Exhibit B



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.

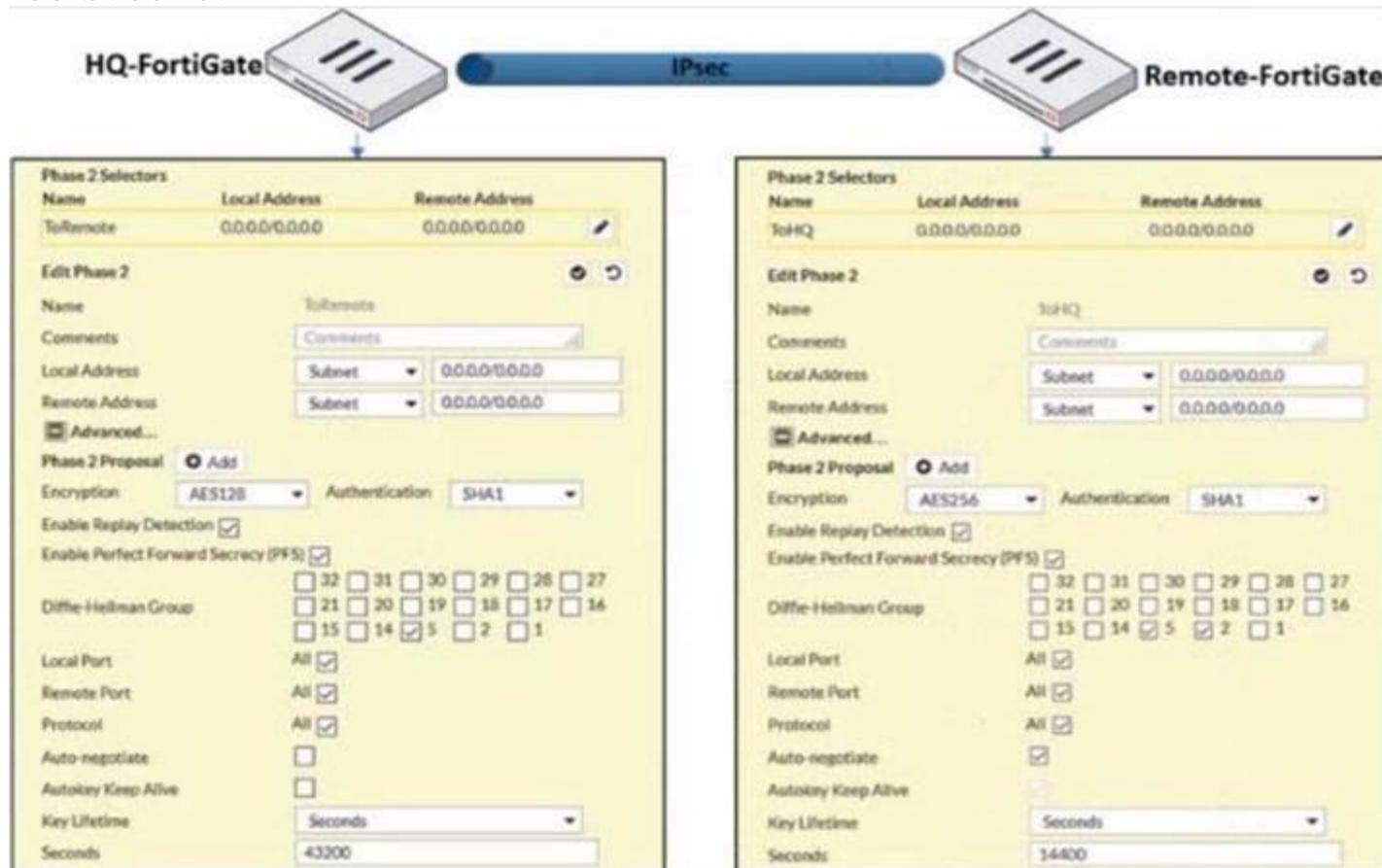
Answer: B

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 3

- (Exam Topic 1)
 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, what configuration change will bring phase 2 up?

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

Answer: D

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495>

Encryption and authentication algorithm needs to match in order for IPSEC be successfully established.

NEW QUESTION 4

- (Exam Topic 1)

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuard update servers
- C. Operating mode
- D. NGFW mode

Answer: CD

Explanation:

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

NEW QUESTION 5

- (Exam Topic 1)

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:

B - because the customer requires the tunnels to notify when a tunnel goes down. DPD is designed for that purpose. To send a packet over a firewall to determine a failover for the next tunnel after a specific amount of time of not receiving a response from its peer.

C - remember when it comes to choosing a route with regards to Administrative Distance. The route with the lowest distance for that particular route will be chosen. So, by configuring a lower routing distance on the primary tunnel, means that the primary tunnel will be chosen to route packets towards their destination.

NEW QUESTION 6

- (Exam Topic 1)

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: BD

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

NEW QUESTION 7

- (Exam Topic 1)

Which type of logs on FortiGate 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

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970>

NEW QUESTION 8

- (Exam Topic 1)

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 NTP.Spoofed.KoD.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 9

- (Exam Topic 1)

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 10

- (Exam Topic 1)

Refer to the exhibit.

Name

Protocol Ping HTTP DNS

Server ✘
 ✘

Participants All SD-WAN Members Specify

port1 ✘
port2 ✘

+

Enable probe packets

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 10

- (Exam Topic 1)

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

- A. FortiGuard web filter cache
- B. FortiGate hostname
- C. NTP
- D. DNS

Answer: CD

NEW QUESTION 12

- (Exam Topic 1)

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
rcvbyte=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 rcvbyte=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 15

- (Exam Topic 1)

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) from 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) from 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

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/54688/debugging-the-packet-flow>

NEW QUESTION 20

- (Exam Topic 1)

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:

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

NEW QUESTION 25

- (Exam Topic 1)

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

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD48690>

NEW QUESTION 28

- (Exam Topic 1)

Refer to the exhibits.

SSL-VPN Settings

Connection Settings

Listen on Interface(s): port1

Listen on Port: 10443

Web mode access will be listening at <https://10.200.1.1:10443>

Redirect HTTP to SSL-VPN:

Restrict Access: Allow access from any host Limit access to specific hosts

Idle Logout:

Inactive For: 300 Seconds

Server Certificate: Fortinet_Factory

Require Client Certificate:

Tunnel Mode Client Settings

Address Range: Automatically assign addresses Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server: Same as client system DNS Specify

Specify WINS Servers:

Authentication/Portal Mapping

Users/Groups	Portal
sslvpn	tunnel-access
All Other Users/Groups	full-access



The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

- A. Change the SSL VPN port on the client.
- B. Change the Server IP address.
- C. Change the idle-timeout.
- D. Change the SSL VPN portal to the tunnel.

Answer: A

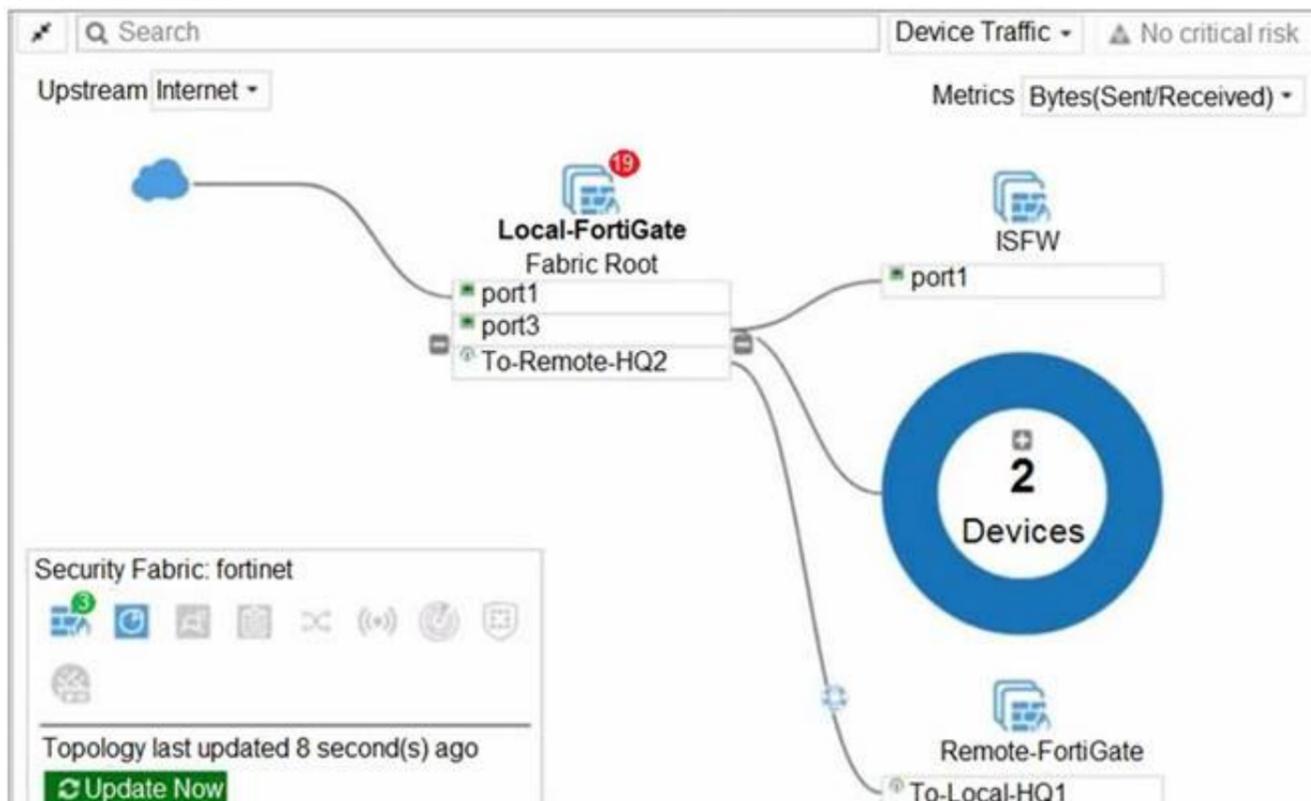
Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494>

NEW QUESTION 29

- (Exam Topic 1)

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 32

- (Exam Topic 1)

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

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/buildingsecurity-into-fortios>

NEW QUESTION 37

- (Exam Topic 1)

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:

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 42

- (Exam Topic 1)

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

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets>

NEW QUESTION 43

- (Exam Topic 1)

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 44

- (Exam Topic 1)

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:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD48294>

NEW QUESTION 49

- (Exam Topic 1)

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.

What is the reason for the failed virus detection by FortiGate?

- A. Application control is not enabled
- B. SSL/SSH Inspection profile is incorrect
- C. Antivirus profile configuration is incorrect
- D. Antivirus definitions are not up to date

Answer: B

Explanation:

https traffic requires SSL decryption. Check the ssh inspection profile

NEW QUESTION 52

- (Exam Topic 1)

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:

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshooting-high-cpu-usage>

NEW QUESTION 55

- (Exam Topic 1)

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 57

- (Exam Topic 2)

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

Explanation:

Reference: https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

NEW QUESTION 61

- (Exam Topic 2)

Refer to the exhibit.



In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.

What should the administrator do next to troubleshoot the problem?

- A. Run a sniffer on the web server.
- B. Capture the traffic using an external sniffer connected to port1.
- C. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10"
- D. Execute a debug flow.

Answer: D

NEW QUESTION 66

- (Exam Topic 2)

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 69

- (Exam Topic 2)

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 71

- (Exam Topic 2)

What devices form the core of the security fabric?

- A. Two FortiGate devices and one FortiManager device
- B. One FortiGate device and one FortiManager device
- C. Two FortiGate devices and one FortiAnalyzer device
- D. One FortiGate device and one FortiAnalyzer device

Answer: C

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/425100/components>

NEW QUESTION 76

- (Exam Topic 2)

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk. What is the default behavior when the local disk is full?

- A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.
- B. No new log is recorded until you manually clear logs from the local disk.
- C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.

D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Answer: C

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/462620/log-disk-setting>

NEW QUESTION 78

- (Exam Topic 2)

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 81

- (Exam Topic 2)

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 84

- (Exam Topic 2)

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

- A. The subject field in the server certificate
- B. The serial number in the server certificate
- C. The server name indication (SNI) extension in the client hello message
- D. The subject alternative name (SAN) field in the server certificate
- E. The host field in the HTTP header

Answer: ACD

Explanation:

Reference: <https://checkthefirewall.com/blogs/fortinet/ssl-inspection>

NEW QUESTION 88

- (Exam Topic 2)

Which two statements are true about the RPF check? (Choose two.)

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

Answer: AD

Explanation:

Reference: <https://www.programmersought.com/article/16383871634/>

NEW QUESTION 89

- (Exam Topic 2)

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager
- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

Answer: B

NEW QUESTION 94

- (Exam Topic 2)

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check.

Answer: D

NEW QUESTION 97

- (Exam Topic 2)

A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface. Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

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

Answer: B

Explanation:

FortiGate_Infrastructure_6.0_Study_Guide_v2-Online.pdf -> page 147

"Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID"

NEW QUESTION 102

- (Exam Topic 2)

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 105

- (Exam Topic 2)

NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

- A. Web filtering
- B. Antivirus
- C. Web proxy
- D. Application control

Answer: B

NEW QUESTION 109

- (Exam Topic 2)

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

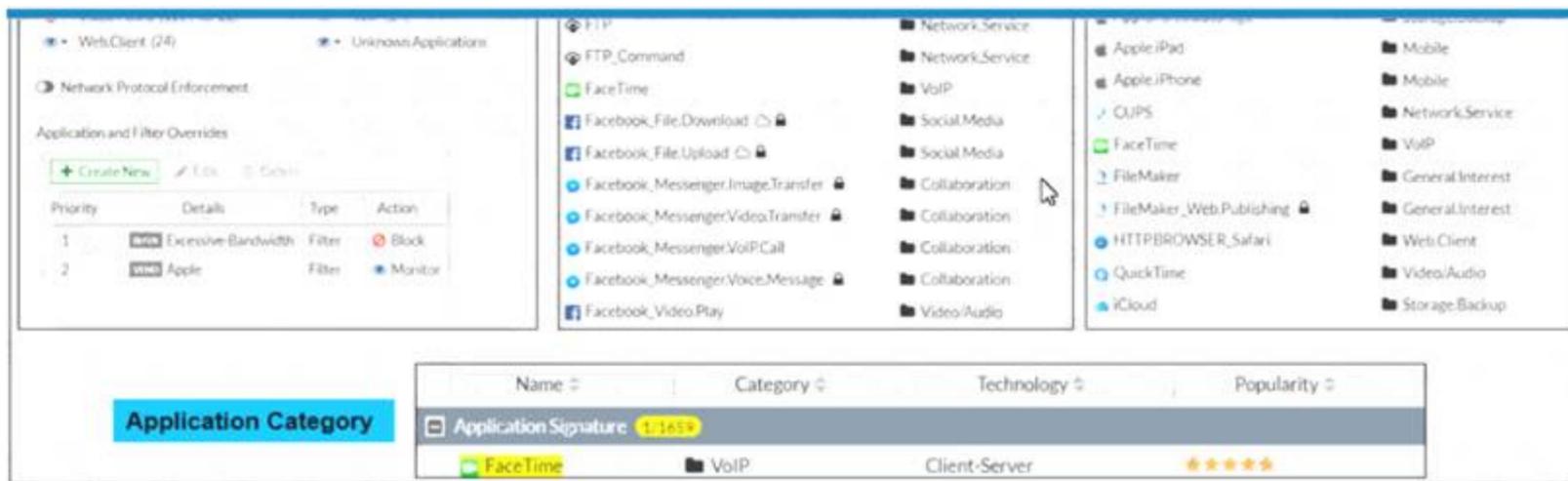
Explanation:

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

NEW QUESTION 112

- (Exam Topic 2)

Refer to the exhibit to view the application control profile.



Based on the configuration, what will happen to Apple FaceTime?

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

Answer: A

NEW QUESTION 116

- (Exam Topic 2)

Which two statements are true about collector agent standard access mode? (Choose two.)

- A. Standard mode uses Windows convention-NetBios: Domain\Username.
- B. Standard mode security profiles apply to organizational units (OU).
- C. Standard mode security profiles apply to user groups.
- D. Standard access mode supports nested groups.

Answer: AC

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso>

NEW QUESTION 121

- (Exam Topic 2)

Refer to the exhibit.

Authentication rule

Edit Rule Authentication rule

Name: WebproxyRule

Source Address: LOCAL_SUBNET

Protocol: HTTP

Authentication Scheme: Web-Proxy-Scheme

IP-based Authentication: Enable Disable

SSO Authentication Scheme:

Comments: Write a comment (0/1023)

Enable This Rule: Enable Disable

Users

+ Create New Edit Delete Search

Name	Type
User-A	LOCAL
User-B	LOCAL
User-C	LOCAL

Authentication scheme

Edit Authentication Scheme

Name: Web-Proxy-Scheme

Method: Form-based

User database: Local Other

Two-factor authentication:

Firewall address

Edit Address

Category: Address Proxy Address

Name: LOCAL_SUBNET

Color: Change

Type: Subnet

IP/Netmask: 10.0.1.0/24

Interface: any

Static route configuration:

Comments: Write a comment (0/255)

Proxy address

Edit Address

Category: Address Proxy Address

Name: Browser-CAT-1

Color: Change

Type: User Agent

Host: LOCAL_SUBNET

User Agent: Apple Safari, Google Chrome, Microsoft Internet Explorer or Spart

Comments: Write a comment (0/255)

Proxy address

Edit Address

Category: Address Proxy Address

Name: Browser-CAT-2

Color: Change

Type: User Agent

Host: LOCAL_SUBNET

User Agent: Mozilla Firefox

Comments: Write a comment (0/255)

Web proxy address

ID	Source	Destination	Schedule	Action
explicit-web proxy → port1				
1	Browser-CAT-2 LOCAL_SUBNET User-B	all	always	DENY
2	Browser-CAT-1 LOCAL_SUBNET User-A	all	always	ACCEPT
3	LOCAL_SUBNET	all	always	ACCEPT

The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address.

An explicit web proxy is configured for subnet range 10.0.1.0/24 with three explicit web proxy policies. The authentication rule is configured to authenticate HTTP requests for subnet range 10.0.1.0/24 with a form-based authentication scheme for the FortiGate local user database. Users will be prompted for authentication.

How will FortiGate process the traffic when the HTTP request comes from a machine with the source IP 10.1.1.10 to the destination http://www.fortinet.com? (Choose two.)

- A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.
- B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.
- C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.
- D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

Answer: BD

NEW QUESTION 125

- (Exam Topic 2)

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

NEW QUESTION 127

- (Exam Topic 2)

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 128

- (Exam Topic 2)

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 131

- (Exam Topic 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 132

- (Exam Topic 2)

Exhibit:

```
Fortigate # show authentication rule
config authentication rule
  edit "NTLM_rule"
    set srcaddr "all"
    set ip-based disable
    set web-auth-cookie enable
  next
end
```

Refer to the exhibit to view the authentication rule configuration. In this scenario, which statement is true?

- A. IP-based authentication is enabled
- B. Route-based authentication is enabled
- C. Session-based authentication is enabled.
- D. Policy-based authentication is enabled

Answer: C

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD45387>

NEW QUESTION 137

- (Exam Topic 2)

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 139

- (Exam Topic 2)

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

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955>

NEW QUESTION 144

- (Exam Topic 2)

Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

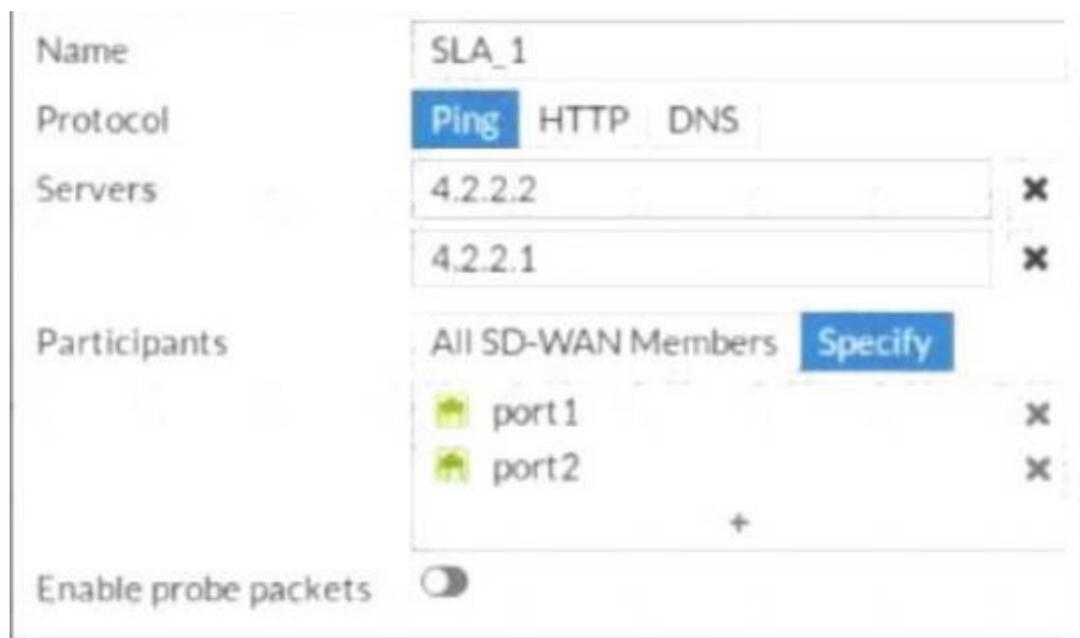
- A. DNS
- B. ping
- C. udp-echo
- D. TWAMP

Answer: CD

NEW QUESTION 145

- (Exam Topic 2)

Refer to the exhibit.



Which contains a Performance SLA configuration.

An administrator has configured a performance SLA on FortiGate. Which failed to generate any traffic. Why is FortiGate not generating any traffic for the performance SLA?

- A. Participants configured are not SD-WAN members.
- B. There may not be a static route to route the performance SLA traffic.
- C. The Ping protocol is not supported for the public servers that are configured.
- D. You need to turn on the Enable probe packets switch.

Answer: D

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/478384/performance-sla-linkmonitoring>

NEW QUESTION 148

- (Exam Topic 2)

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 150

- (Exam Topic 2)

Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srcintfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dummytracker.org/"
sentbyte=517 rcvbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

- A. Traffic is blocked because Action is set to DENY in the firewall policy.
- B. Traffic belongs to the root VDOM.
- C. This is a security log.
- D. Log severity is set to error on FortiGate.

Answer: AC

NEW QUESTION 155

- (Exam Topic 2)

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

- A. Firewall policy
- B. Policy rule
- C. Security policy
- D. SSL inspection and authentication policy

Answer: CD

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/38324/ngfw-policy-based-mode>

NEW QUESTION 160

- (Exam Topic 2)

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > System uptime > Priority > FortiGate Serial number
- B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
- C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
- D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Answer: B

Explanation:

Reference: <http://myitmicroblog.blogspot.com/2018/11/what-should-you-know-about-ha-override.html>

NEW QUESTION 161

- (Exam Topic 2)

Refer to the exhibit.

<pre>config firewall policy edit 1 set name "INTERNET" set uuid b11ac58c-791b-51e7-4600-12f829a689d9 set srcintf "port3" set dstintf "port1" set srcaddr "LOCAL_SUBNET" set dstaddr "all" set action accept set schedule "always" set service "ALL" set utm-status enable set inspection-mode proxy set http-policy-redirect enable set ssl-ssh-profile "certificate-inspection" set av-profile "default" set logtraffic all set logtraffic-start enable set ipool enable set poolname "ProxyPool" set nat enable next end</pre>	<p>FIREWALL POLICIES</p>	<pre>config firewall edit 1 set uuid 6491d126-c790-51ea-13f9-4ed04b543afe set proxy transparent-web set srcintf "port3" set dstintf "port1" set srcaddr "all" set dstaddr "EICAR" set service "webproxy" set action accept set schedule "always" set logtraffic all set utm-status enable set ssl-ssh-profile "certificate-inspection" set av-profile "default" next edit 2 set uuid 6a1c74c6-c794-51ea-e646-4f70ae2bc5f9 set proxy transparent-web set srcintf "port2" set dstintf "port1" set srcaddr "all" set dstaddr "all" set service "webproxy" set action accept set status disable set schedule "always" set logtraffic disable set ssl-ssh-profile "certificate-inspection" next edit 3 set uuid 018fb8b6-c797-51ea-d848-a7c2952ceea9 set proxy transparent-web set srcintf "port3" set dstintf "port1" set srcaddr "all" set dstaddr "all" set service "webproxy" set action accept set status disable set schedule "always" set logtraffic all set utm-status enable set ssl-ssh-profile "certificate-inspection" set av-profile "default" next end</pre>
<pre>config firewall proxy-address edit "EICAR" set uuid 5a24bdaa-c792-51ea-2c89-a9f79e2bdc96 set type host-regex set host-regex ".*eicar\\.org" next end</pre>	<p>PROXY ADDRESS</p>	

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses. How does FortiGate process the traffic sent to <http://www.fortinet.com>?

- A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.
- B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.
- C. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 1.
- D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

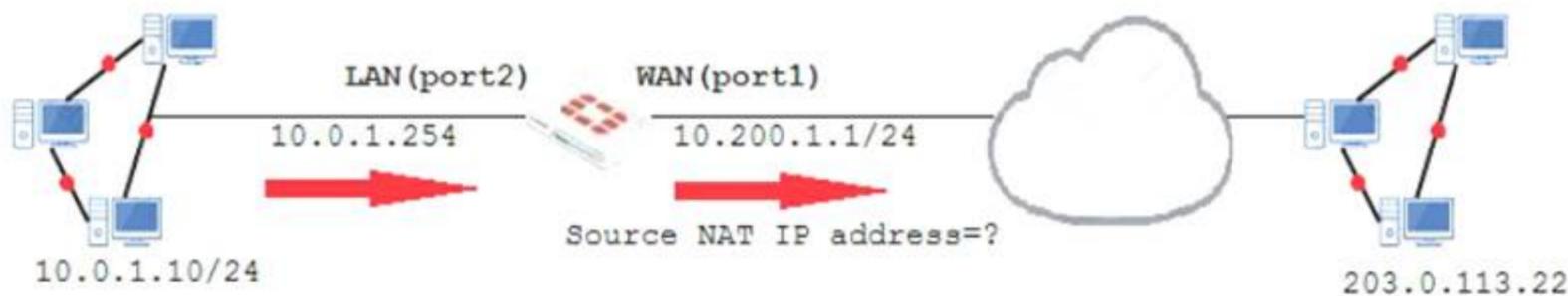
Answer: D

NEW QUESTION 165

- (Exam Topic 2)

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

Network Diagram



Name: 0/255

Comments:

Color:

Network

Interface:

Type:

External IP Address/Range: -

Mapped IP Address/Range: -

Optional Filters:

Port Forwarding:

ID	Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port2) → WAN(port1)							
1	Full_Access	all	all	always	ALL	ACCEPT	Enabled
LAN(port1) → WAN(port2)							
2	WebServer	all	VIP	always	ALL	ACCEPT	Disabled

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
- 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 170

- (Exam Topic 2)

Which two statements are true about collector agent advanced mode? (Choose two.)

- A. Advanced mode uses Windows convention—NetBios: Domain\Username.
- B. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate
- C. Advanced mode supports nested or inherited groups
- D. Security profiles can be applied only to user groups, not individual users.

Answer: BC

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso>

NEW QUESTION 171

- (Exam Topic 2)

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

- A. By default, FortiGate uses WINS servers to resolve names.

- B. By default, the SSL VPN portal requires the installation of a client's certificate.
- C. By default, split tunneling is enabled.
- D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 174

- (Exam Topic 2)

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 176

- (Exam Topic 2)

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeout
- B. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
- C. It is a hard timeout
- D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- E. It is an idle timeout
- F. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
- G. It is a hard timeout
- H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Answer: A

NEW QUESTION 181

- (Exam Topic 2)

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 186

- (Exam Topic 2)

An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

- A. A phase 2 configuration is not required.
- B. This VPN cannot be used as part of a hub-and-spoke topology.
- C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
- D. The IPsec firewall policies must be placed at the top of the list.

Answer: C

Explanation:

In a route-based configuration, FortiGate automatically adds a virtual interface with the VPN name (Infrastructure Study Guide, 206)

NEW QUESTION 189

- (Exam Topic 2)

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

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/292634/security-rating>

NEW QUESTION 194

- (Exam Topic 2)

Which three authentication timeout types are available 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 196

- (Exam Topic 2)

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>

NEW QUESTION 200

- (Exam Topic 2)

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

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/567568/enabling-scanning>

NEW QUESTION 202

- (Exam Topic 2)

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 206

- (Exam Topic 2)

Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

- A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
- B. An SA never expires.
- C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
- D. Phase 2 SA expiration can be time-based, volume-based, or both.
- E. Both the phase 1 SA and phase 2 SA are bidirectional.

Answer: ACD

NEW QUESTION 207

- (Exam Topic 2)

Refer to the exhibit to view the application control profile.

Edit Application Sensor

Categories

- All Categories
- Business (143, 6)
- Collaboration (255, 10)
- Game (84)
- Mobile (3)
- P2P (56)
- Remote.Access (84)
- Storage.Backup (162, 16)
- Video/Audio (154, 14)
- Web.Client (24)
- Cloud.IT (47, 1)
- Email (78, 12)
- General.Interest (229, 7)
- Network.Service (330)
- Proxy (168)
- Social.Media (116, 31)
- Update (49)
- VoIP (24)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New Edit Delete

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

Users who use Apple FaceTime video conferences are unable to set up meetings. In this scenario, which statement is true?

- A. Apple FaceTime belongs to the custom monitored filter.
- B. The category of Apple FaceTime is being monitored.
- C. Apple FaceTime belongs to the custom blocked filter.
- D. The category of Apple FaceTime is being blocked.

Answer: C

NEW QUESTION 209

- (Exam Topic 2)

Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

- A. Shut down/reboot a downstream FortiGate device.
- B. Disable FortiAnalyzer logging for a downstream FortiGate device.
- C. Log in to a downstream FortiSwitch device.
- D. Ban or unban compromised hosts.

Answer: AB

NEW QUESTION 212

- (Exam Topic 2)

Examine the following web filtering log.

```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked reqtype=direct url= "/" sentbyte=286 rcvbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

Which statement about the log message is true?

- A. The action for the category Games is set to block.
- B. The usage quota for the IP address 10.0.1.10 has expired
- C. The name of the applied web filter profile is default.
- D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

Answer: C

NEW QUESTION 215

- (Exam Topic 2)

How do you format the FortiGate flash disk?

- A. Load a debug FortiOS image.
- B. Load the hardware test (HQIP) image.
- C. Execute the CLI command execute formatlogdisk.
- D. Select the format boot device option from the BIOS menu.

Answer: D

NEW QUESTION 218

- (Exam Topic 2)

Examine the two static routes shown in the exhibit, then answer the following question.

Destination	Gateway	Interface	Priority	Distance
172.20.168.0/24	172.25.1 76.1	port1	10	20
172.20.168.0/24	172.25.1 78.1	port2	20	20

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

- A. FortiGate will load balance all traffic across both routes.
- B. FortiGate will use the port1 route as the primary candidate.
- C. FortiGate will route twice as much traffic to the port2 route
- D. FortiGate will only actuate the port1 route in the routing table

Answer: B

Explanation:

"If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path."

NEW QUESTION 220

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT-7.0 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-7.0 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT-7.0/

Money Back Guarantee

NSE4_FGT-7.0 Practice Exam Features:

- * NSE4_FGT-7.0 Questions and Answers Updated Frequently
- * NSE4_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year