



Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

NEW QUESTION 1
- (Exam Topic 1)
Refer to the exhibit.

Outgoing Interfaces

☐ Manual
Manually assign outgoing interfaces.

☒ Best Quality
The interface with the best measured performance is selected.

☐ Lowest Cost (SLA)
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

☐ Maximize Bandwidth (SLA)
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

port1

port2

port3

port4

Measured SLA

SLA_1

Quality criteria

Latency

Status

Enable

Disable

```
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

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Detect Viruses: **Block** Monitor

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

Inspected Protocols

HTTP ☒

SMTP ☒

POP3 ☒

IMAP ☒

FTP ☒

CIFS ☐

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ☒

Include Mobile Malware Protection ☒

Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database ☐

Use External Malware Block List ⓘ ☐

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

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

Answer: B


Explanation:

- "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
 - When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
- In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

NEW QUESTION 3

- (Exam Topic 1)

Refer to the exhibit.

HQ-FortiGate  Remote-FortiGate

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToRemote

Comments:

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal: Add

Encryption: AES128 Authentication: SHA1

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

Diffie-Hellman Group: ☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☒ 5 ☐ 2 ☐ 1

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Auto-negotiate: ☐

Autokey Keep Alive: ☐

Key Lifetime: Seconds 43200

Phase 2 Selectors

Name	Local Address	Remote Address
ToHQ	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToHQ

Comments:

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal: Add

Encryption: AES256 Authentication: SHA1

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

Diffie-Hellman Group: ☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☒ 5 ☒ 2 ☐ 1

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Auto-negotiate: ☒

Autokey Keep Alive: ☐

Key Lifetime: Seconds 14400

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)

An administrator wants to configure timeouts for users. Regardless of the user's behavior, the timer should start as soon as the user authenticates and expire after the configured value.

Which timeout option should be configured on FortiGate?

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

Answer: E

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221#:~:text=Hard%20timeout%3A%20User%20>

NEW QUESTION 5

- (Exam Topic 1)

Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiCache
- B. FortiSIEM
- C. FortiAnalyzer
- D. FortiSandbox
- E. FortiCloud

Answer: BCE

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview>

NEW QUESTION 6

- (Exam Topic 1)

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

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

Answer: CD

Explanation:

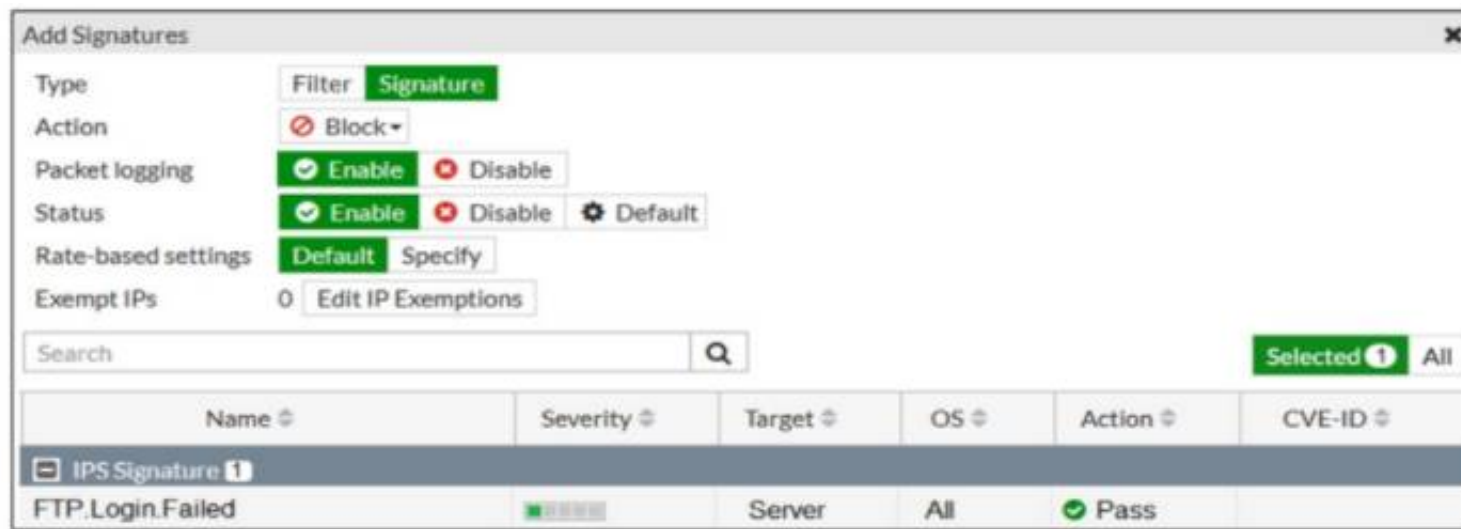
C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

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 7

- (Exam Topic 1)

Refer to the exhibit.



Name	Severity	Target	OS	Action	CVE-ID
FTP.Login.Failed	1	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:

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

NEW QUESTION 8

- (Exam Topic 1)

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:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD34906>

<https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1>

NEW QUESTION 9

- (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 10

- (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.



The screenshot shows the configuration for a performance SLA named 'SLA1'. The protocol is set to 'Ping'. The server list contains two entries: '4.2.2.2' and '4.2.2.1'. The participants are set to 'All SD-WAN Members'. Below this, there is a list of participants with 'port1' and 'port2' selected, each with a small green icon and a close button. At the bottom, the 'Enable probe packets' checkbox is checked.

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 11

- (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
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 13

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 14

- (Exam Topic 1)

Refer to the exhibit.



The screenshot shows the configuration page for the Administrator user. The 'Username' field is set to 'Administrator' and the 'Type' is set to 'Local User'. The 'Comments' field is empty with a character count of 0/255. The 'Administrator Profile' is set to 'prof_admin' and the 'Email Address' is 'admin@xyz.com'. Below these fields are four toggle switches, all of which are currently turned off: 'SMS', 'Two-factor Authentication', 'Restrict login to trusted hosts', and 'Restrict admin to guest account provisioning only'. A 'Change Password' button is located next to the Username field.

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

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

Answer: C

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD34502>

NEW QUESTION 17

- (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 21

- (Exam Topic 1)

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:

Reference: https://www.reddit.com/r/fortinet/comments/c7j6jg/recommended_ssl_cert/

NEW QUESTION 26

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 30

- (Exam Topic 1)

Which three statements about a flow-based antivirus profile are correct? (Choose three.)

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

Answer: BDE

Explanation:

Reference: <https://forum.fortinet.com/tm.aspx?m=192309>

NEW QUESTION 34

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 37

- (Exam Topic 1)

An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

- A. Add the support of NTLM authentication.
- B. Add user accounts to Active Directory (AD).
- C. Add user accounts to the FortiGate group filter.
- D. Add user accounts to the Ignore User List.

Answer: D

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828>

NEW QUESTION 38

- (Exam Topic 1)

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

NEW QUESTION 40

- (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 41

- (Exam Topic 1)

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 43

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:

https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-sslvpn-40-mr3.pdf

NEW QUESTION 47

- (Exam Topic 1)

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 originated.

Answer: D

Explanation:

Reference:

https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/300_System/303d_FortiG

NEW QUESTION 49

- (Exam Topic 1)

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 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 50

- (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 53

- (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?](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113)

[attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113](https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113)

NEW QUESTION 54

- (Exam Topic 2)

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

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

Answer: CD

Explanation:

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

NEW QUESTION 57

- (Exam Topic 2)

Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {
    if (shExpMatch (url, "*.fortinet.com/*")) {
        return "DIRECT";
    }
    if (isInNet (host, "172.25.120.0", "255.255.255.0")) {
        return "PROXY altproxy.corp.com: 8060";
    }
    return "PROXY proxy.corp.com: 8090";
}
```

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 58

- (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 60

- (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 62

- (Exam Topic 2)

View the exhibit.

Application Details

Name	Category	Technology	Popularity	Risk
Addicting Games	Game	Browser-Based	☆☆☆☆	Risk

Application Control Profile

Categories

All Categories

Business (149, 6)

Email (80, 13)

Industrial (1168)

P2P (70)

SocialMedia (120, 31)

Video/Audio (164, 14)

Unknown Applications

Cloud.IT (42)

Game (83)

Mobile (3)

Proxy (148)

Storage.Backup (175, 17)

VoIP (27)

Collaboration (274, 10)

GeneralInterest (233, 6)

Network.Service (325)

Remote.Access (84)

Update (49)

Web.Client (22)

Application Overrides

Add Signatures

Edit Parameters

Delete

Application Signature	Category	Action
Addicting Games	Game	Allow

Filter Overrides

Add Filter

Edit

Delete

Filter Details	Action
Risk (2304, 52)	Block

A user behind the FortiGate is trying to go to <http://www.addictinggames.com> (Addicting Games). Based on this configuration, which statement is true?

- A. Addicting.Games is allowed based on the Application Overrides configuration.
- B. Addicting.Games is blocked on the Filter Overrides configuration.
- C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
- D. Addcting.Games is allowed based on the Categories configuration.

Answer: A

NEW QUESTION 65

- (Exam Topic 2)

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

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

Answer: AD

NEW QUESTION 70

- (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:

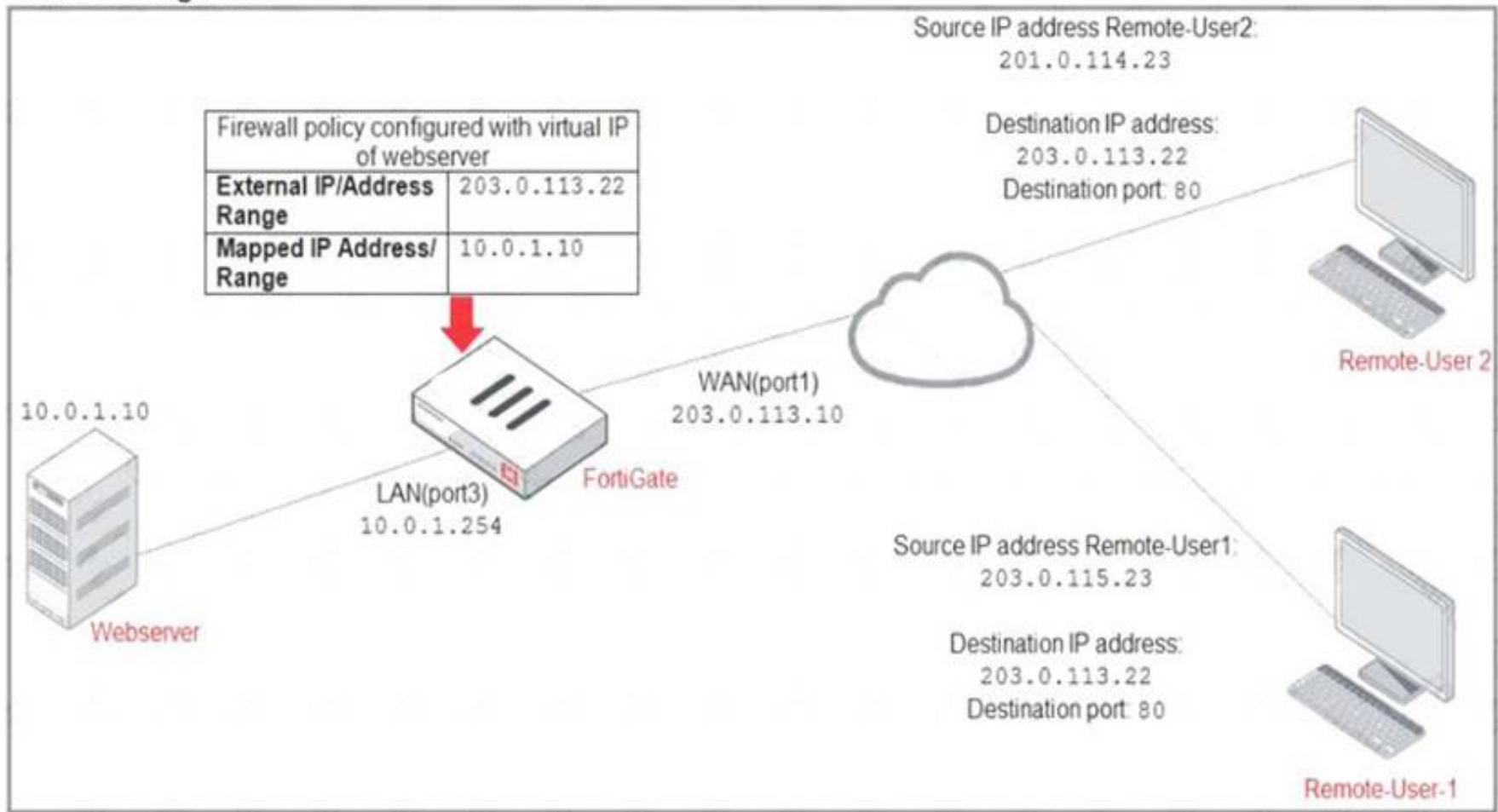
Reference: <https://checkthefirewall.com/blogs/fortinet/ssl-inspection>

NEW QUESTION 75

- (Exam Topic 2)

Refer to the exhibit.

Network diagram



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

Firewall address object

Edit Address

Name

Deny_IP

Color

Change

Type

Subnet

IP/Netmask

201.0.114.23/32

Interface

WAN(port1)

Static route configuration

Comments

Deny webserver access. 22/255

The exhibit contains a network diagram, firewall policies, and a firewall address object configuration. An administrator created a Deny policy with default settings to deny Webserver access for Remote-user2. Remote-user2 is still able to access Webserver. Which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

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

Answer: CD

NEW QUESTION 78

- (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 79

- (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:

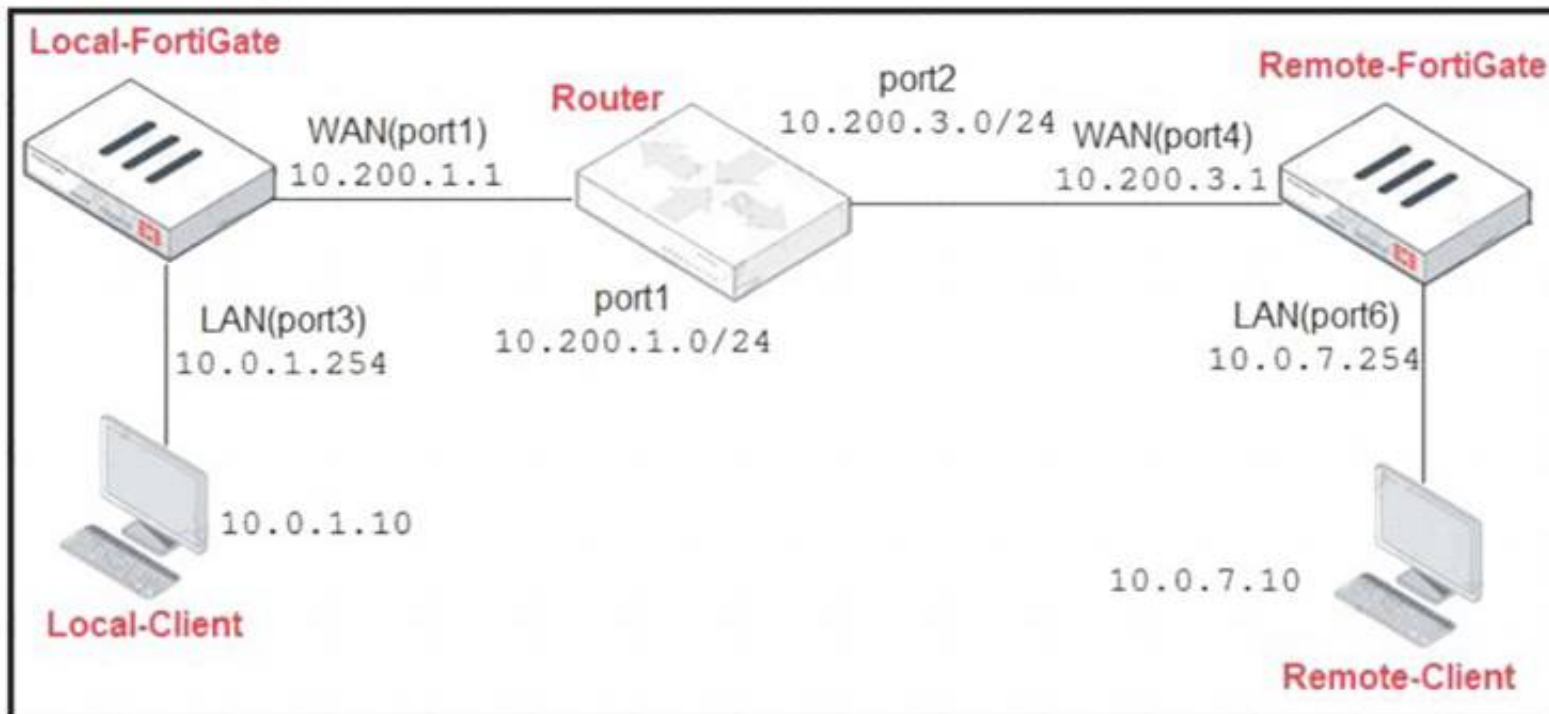
FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

NEW QUESTION 80

- (Exam Topic 2)

Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

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

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 84

- (Exam Topic 2)

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 89

- (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](#)

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	LOCAL_SUBNET Browser-CAT-1 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 94

- (Exam Topic 2)

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>

NEW QUESTION 96

- (Exam Topic 2)

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

A User or User Group

- A. IP address
- B. No other object can be added
- C. FQDN address

Answer: B

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy>

NEW QUESTION 97

- (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 101

- (Exam Topic 2)

Refer to the exhibit, which contains a radius server configuration.



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

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

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

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

Answer: A

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/634373/authentication-servers>

NEW QUESTION 104

- (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 106

- (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

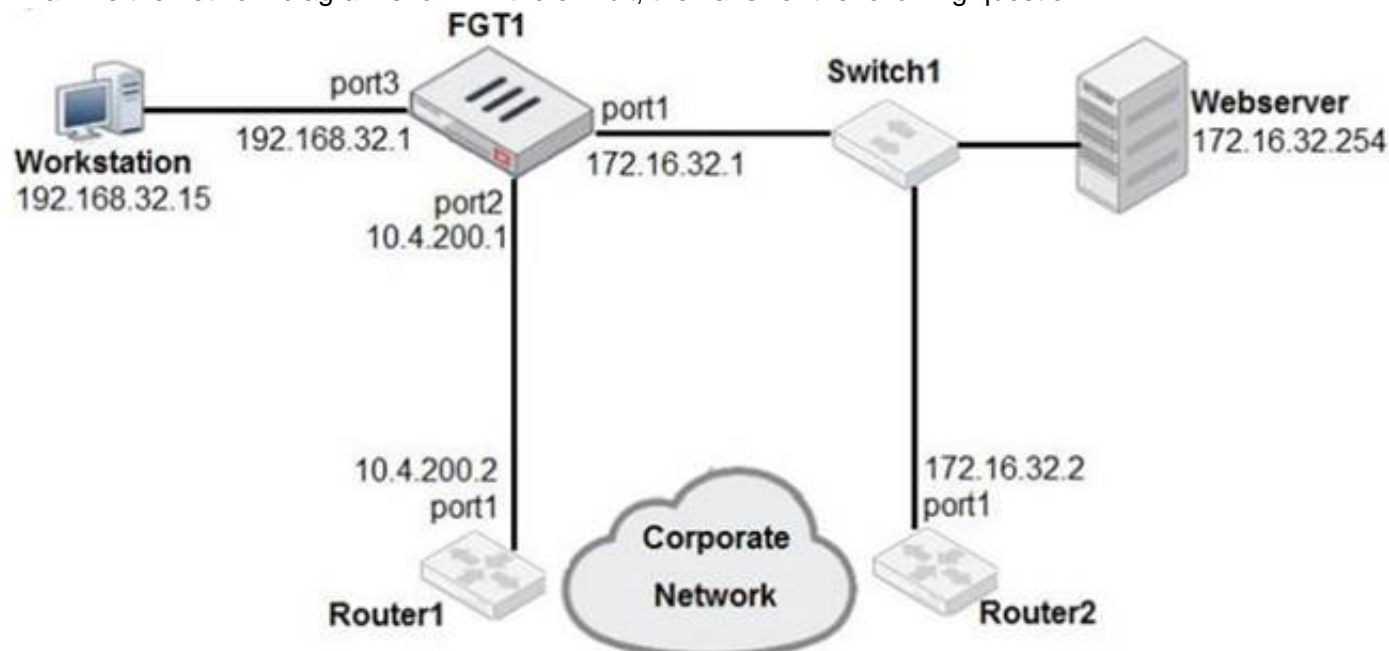
Explanation:

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

NEW QUESTION 110

- (Exam Topic 2)

Examine the network diagram shown in the exhibit, then answer the following question:



Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?

- A. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
- B. 0.0.0.0/0 [20/0] via 10.4.200.2, port2
- C. 10.4.200.0/30 is directly connected, port2
- D. 172.16.32.0/24 is directly connected, port1

Answer: D

NEW QUESTION 115

- (Exam Topic 2)

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

- A. IP tool references must be removed from existing firewall policies before enabling central NAT.
- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Answer: AB

NEW QUESTION 120

- (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 121

- (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 126

- (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.)

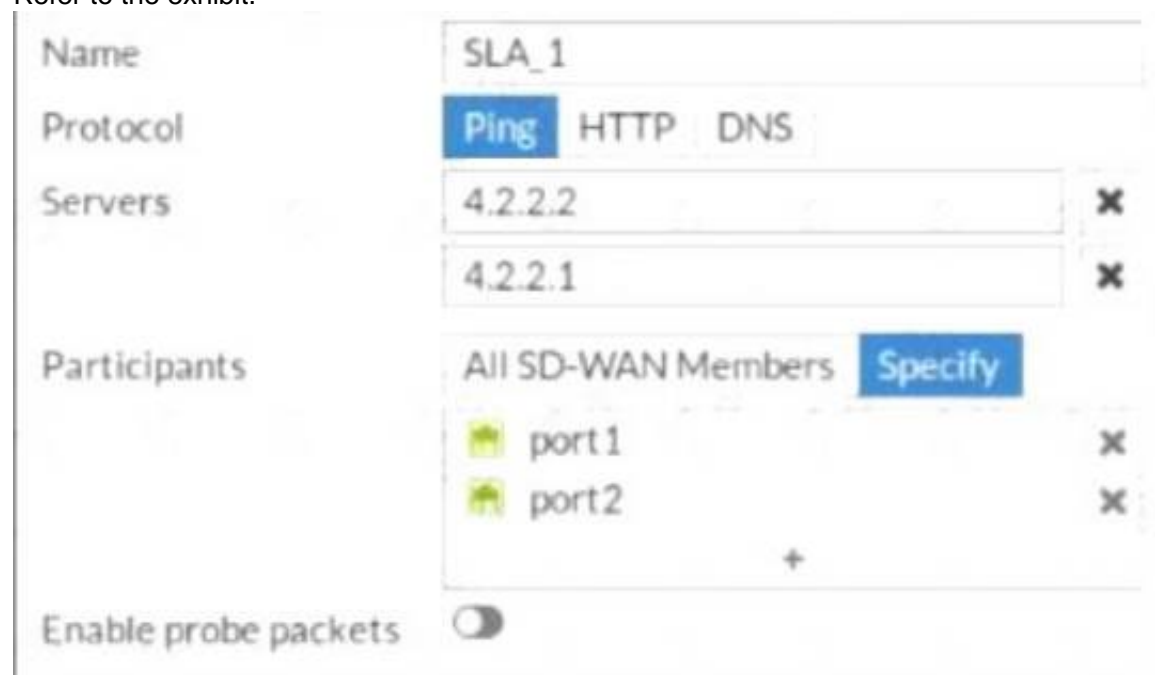
- A. DNS
- B. ping
- C. udp-echo
- D. TWAMP

Answer: CD

NEW QUESTION 127

- (Exam Topic 2)

Refer to the exhibit.



Name	SLA_1		
Protocol	Ping	HTTP	DNS
Servers	4.2.2.2	X	
	4.2.2.1	X	
Participants	All SD-WAN Members	Specify	
	port1	X	
	port2	X	
	+		
Enable probe packets	<input type="checkbox"/>		

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 128

- (Exam Topic 2)
Which two VDOMs are the default VDOMs created when FortiGate is set up in split VDOM mode? (Choose two.)

- A. FG-traffic
- B. Mgmt
- C. FG-Mgmt
- D. Root

Answer: AD

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/758820/split-task-vdom-mode>

NEW QUESTION 129

- (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 133

- (Exam Topic 2)
Refer to the exhibit.

NameCustom Profile

Comments

Access Permissions

Access Control

PermissionsSet All

Security Fabric	None	Read	Read/Write
FortiView	None	Read	Read/Write
User & Device	None	Read	Read/Write
Firewall	None	Read	Read/WriteCustom
Log & Report	None	Read	Read/WriteCustom
Network	None	Read	Read/WriteCustom
System	None	Read	Read/WriteCustom
Security Profile	None	Read	Read/WriteCustom
VPN	None	Read	Read/Write
WAN Opt & Cache	None	Read	Read/Write
WiFi & Switch	None	Read	Read/Write

Permit usage of CLI diagnostic commands

Override Idle Timeout

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

- A. Custom permission for Network
- B. Read/Write permission for Log & Report
- C. CLI diagnostics commands permission
- D. Read/Write permission for Firewall

Answer: C

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220>

NEW QUESTION 138

- (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 rcvdbyte=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 141

- (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 146

- (Exam Topic 2)

What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

- A. Traffic to botnetservers
- B. Traffic to inappropriate web sites
- C. Server information disclosure attacks
- D. Credit card data leaks
- E. SQL injection attacks

Answer: CDE

NEW QUESTION 150

- (Exam Topic 2)

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

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

Answer: BDE

Explanation:

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

NEW QUESTION 151

- (Exam Topic 2)

Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

- A. Fabric Coverage
- B. Automated Response
- C. Security Posture
- D. Optimization

Answer: C

Explanation:

Reference:

<https://www.fortinet.com/content/dam/fortinet/assets/support/fortinet-recommended-security-bestpractices.pdf>

NEW QUESTION 154

- (Exam Topic 2)

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

- A. The browser requires a software update.
- B. FortiGate does not support full SSL inspection when web filtering is enabled.
- C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
- D. There are network connectivity issues.

Answer: C

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD41394>

NEW QUESTION 155

- (Exam Topic 2)

Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

- A. This is known as many-to-one NAT.
- B. Source IP is translated to the outgoing interface IP.
- C. Connections are tracked using source port and source MAC address.
- D. Port address translation is not used.

Answer: BD

NEW QUESTION 159

- (Exam Topic 2)

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

- A. IP address
- B. Once Internet Service is selected, no other object can be added
- C. User or User Group
- D. FQDN address

Answer: B

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy>

NEW QUESTION 162

- (Exam Topic 2)

Refer to the exhibit.

config firewall policy	FIREWALL POLICIES	config firewall
<pre>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 ippool enable set poolname "ProxyPool" set nat enable next end</pre>		<pre>edit 1 set uuid 6491d126-c790-51ea-13f9-4ed04b543abe 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 818fb8b6-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>	PROXY ADDRESS	

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)

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 167

- (Exam Topic 2)

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

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

Answer: AB

NEW QUESTION 169

- (Exam Topic 2)

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.

IPS Sensor

Edit IPS Sensor

WINDOWS_SERVER

Name

EMAIL-SERVER-IPS

[View IPS Signatures]

Comments

com

IPS Signatures

+ Add Signatures

Delete

Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce		High	Server	TCP_SMT	All	Block	

IPS Filters

+ Add Filter

Edit Filter

Delete

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	

Rate Based Signatures

Enable	Signature	Threshold	Duration(seconds)	Track By	Action	Block Duration(minutes)
<input checked="" type="checkbox"/>	IMAPLoginBruteForce	60	10	Source IP	Block	None
<input checked="" type="checkbox"/>	SMTPLoginBruteForce	60	10	Source IP	Block	None

Apply

DoS Policy

Incoming Interface

port1

Source Address

all

+

Destination Address

all

+

Services

ALL

+

L3 Anomalies

Name	Status	Logging	Pass	Block	Action
ip_src_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block	
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block	

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force
- C. ip_src_session
- D. Location: server Protocol: SMTP

Answer: B

NEW QUESTION 172

- (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 173

- (Exam Topic 2)

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.

Guaranteed success with Our exam guides

visit - https://www.certshared.com

IPS Sensor

Name

WINDOWS_SERVERS

Comments

[View IPS Signatures]

IPS Signatures

+ Add Signatures

Delete

Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

+ Add Filter

Edit Filter

Delete

Filter Details	Action	Packet Logging
Location:server OS:Windows	<div>Block</div>	<div></div>

Apply

Forward Traffic Logs

Add Filter

#		Date/Time	Source	Destination	Application Name	Result	Policy
1		10:09:03	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2		10:09:03	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3		10:09:02	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4		10:09:02	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5		10:09:01	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6		10:08:59	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7		10:08:57	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8		10:08:57	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9		10:08:57	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10		10:08:57	10.200.1.254	10.200.1.200	HTTPS	<div>✓</div> 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic. What is a possible reason for this?

- A. The IPS filter is missing the Protocol: HTTPS option.
- B. The HTTPS signatures have not been added to the sensor.
- C. A DoS policy should be used, instead of an IPS sensor.
- D. A DoS policy should be used, instead of an IPS sensor.
- E. The firewall policy is not using a full SSL inspection profile.

Answer: E

NEW QUESTION 177

- (Exam Topic 2)

Which two statements ate 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 alt FortiGate devices.

Answer: BC

Explanation:

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

NEW QUESTION 181

- (Exam Topic 2)

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 184

- (Exam Topic 2)

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

- A. It limits the scanning of application traffic to the DNS protocol only.
- B. It limits the scanning of application traffic to use parent signatures only.
- C. It limits the scanning of application traffic to the browser-based technology category only.
- D. It limits the scanning of application traffic to the application category only.

Answer: C

NEW QUESTION 188

- (Exam Topic 2)

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 192

- (Exam Topic 2)

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

Answer: ABC

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

NEW QUESTION 194

- (Exam Topic 2)

Which of the following statements correctly describes FortiGate's route lookup behavior when searching for a suitable gateway? (Choose two)

- A. Lookup is done on the first packet from the session originator
- B. Lookup is done on the last packet sent from the responder
- C. Lookup is done on every packet, regardless of direction
- D. Lookup is done on the trust reply packet from the responder

Answer: AD

NEW QUESTION 195

- (Exam Topic 2)

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

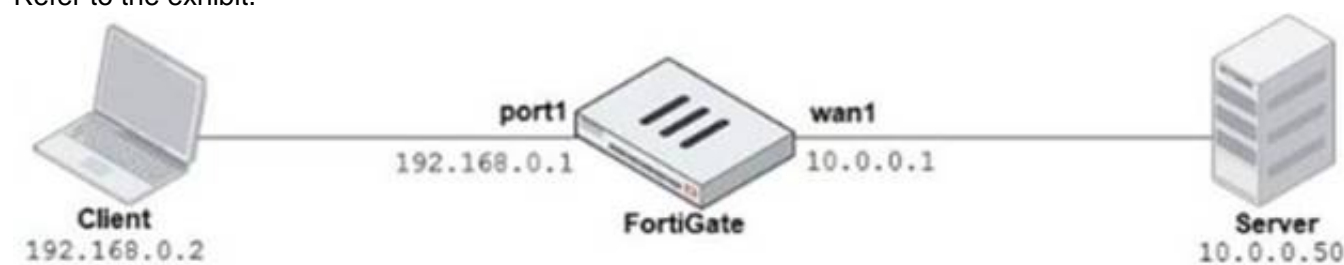
- A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
- B. An SA never expires.
- C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
- D. Phase 2 SA expiration can be time-based, volume-based, or both.
- E. Both the phase 1 SA and phase 2 SA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

Answer: ACD

NEW QUESTION 200

- (Exam Topic 2)

Refer to the exhibit.



Explicit Proxy

☒ Explicit Web Proxy

Listen on Interfaces

port1

+

×

HTTP Port

8080

-

8080

HTTPS Port

Use HTTP Port

Specify

FTP over HTTP

☐

Proxy auto-config (PAC)

☐

Proxy FQDN

default.fqdn

Max HTTP request length

8

KB

Max HTTP message length

32

KB

Unknown HTTP version

Best Effort

Reject

Realm

default

Default Firewall Policy Action

Accept

Deny

The exhibits show a network diagram and the explicit web proxy configuration.
In the command diagnose sniffer packet, what filter can you use to capture the traffic between the client and the explicit web proxy?

- A. 'host 192.168.0.2 and port 8080'
- B. 'host 10.0.0.50 and port 80'
- C. 'host 192.168.0.1 and port 80'
- D. 'host 10.0.0.50 and port 8080'

Answer: A

NEW QUESTION 205

- (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	<input type="checkbox"/> Block
2	VEND Apple	Filter	<input checked="" type="checkbox"/> 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.

Guaranteed success with Our exam guides

visit - https://www.certshared.com

Answer: C

NEW QUESTION 210

- (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 214

- (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 rcvdbyte=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 218

- (Exam Topic 2)

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

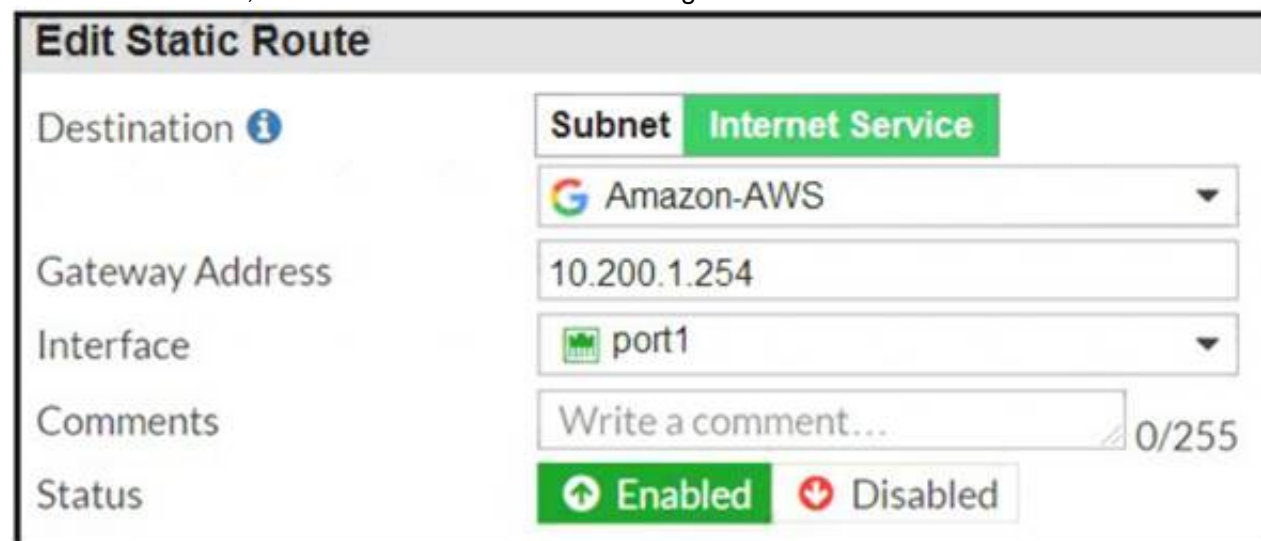
- A. Full Content inspection
- B. Proxy-based inspection
- C. Certificate inspection
- D. Flow-based inspection

Answer: D

NEW QUESTION 222

- (Exam Topic 2)

Refer to the exhibit, which contains a static route configuration.



An administrator created a static route for Amazon Web Services. What CLI command must the administrator use to view the route?

- A. get router info routing-table all
- B. get internet service route list
- C. get router info routing-table database
- D. diagnose firewall proute list

Answer: D

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/latest/administration-guide/139692/routing-concepts>

NEW QUESTION 225

.....

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-7.0 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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT-7.0 Practice Test Here](#)