

# Fortinet

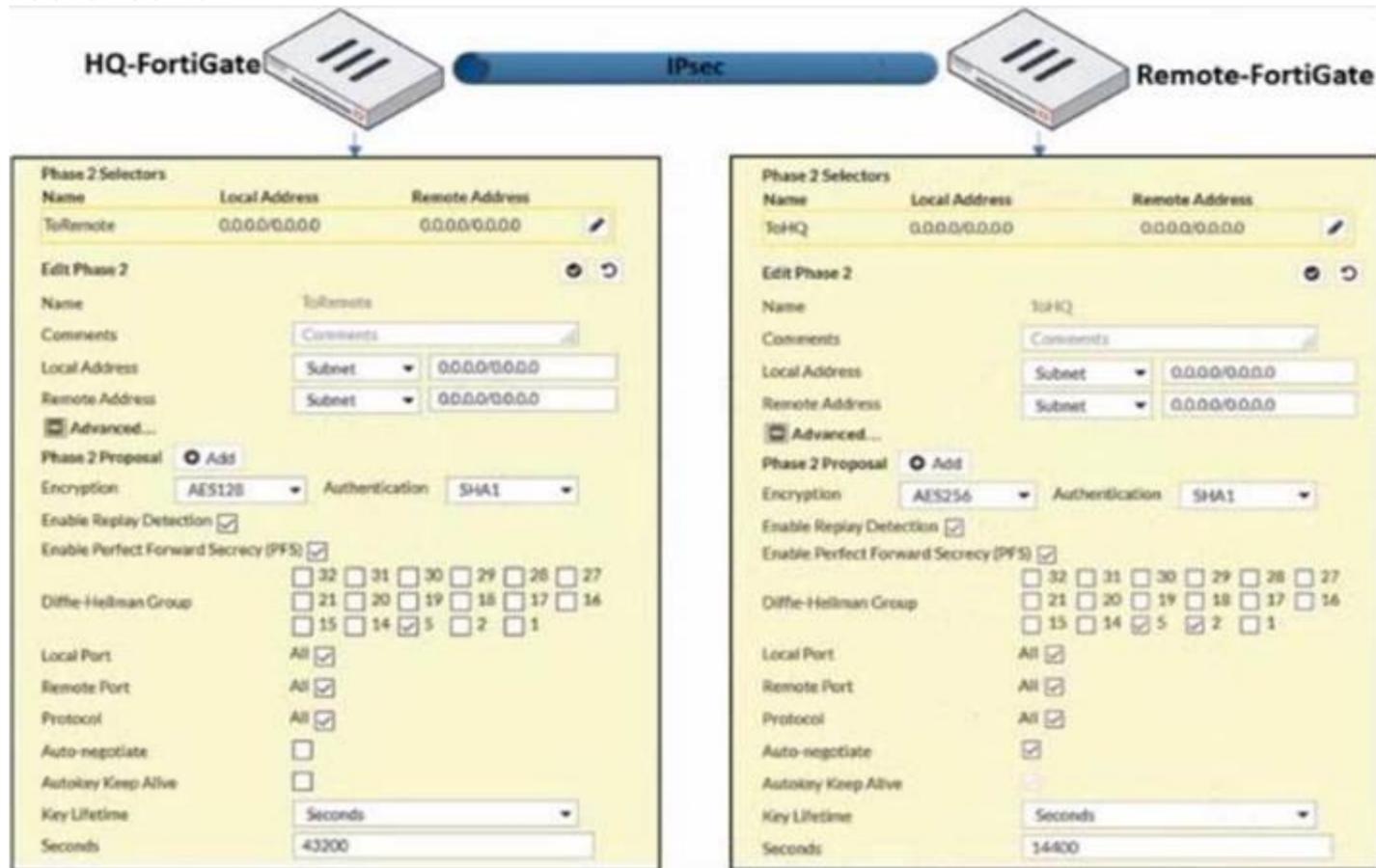
## Exam Questions NSE4\_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0



**NEW QUESTION 1**

- (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 to be successfully established.

**NEW QUESTION 2**

- (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 3**

- (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 4**

- (Exam Topic 1)  
 Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 5**

- (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

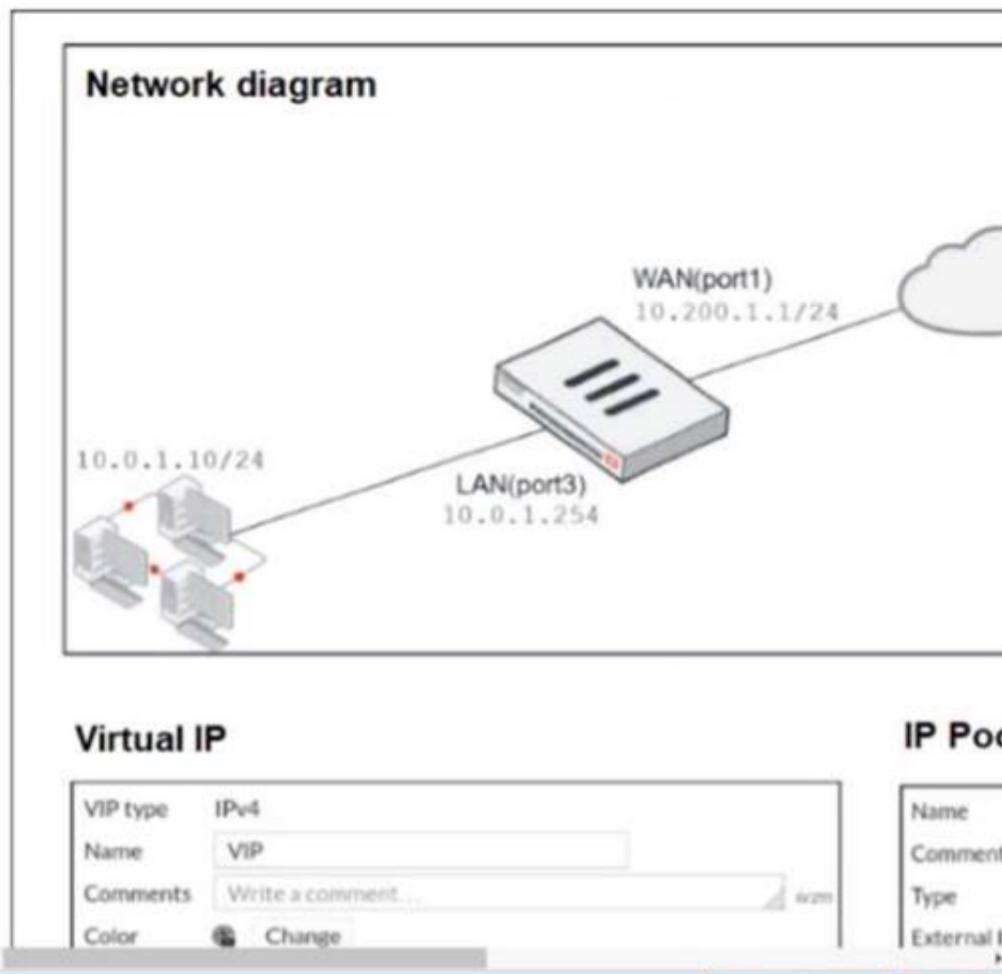
**Explanation:**

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 6**

- (Exam Topic 1)

Refer to the exhibit.



The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration. The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IP address 10.0.1.254/24. The first firewall policy has NAT enabled using IP Pool.

The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?

- A. 10.200.1.1
- B. 10.200.3.1
- C. 10.200.1.100
- D. 10.200.1.10

**Answer:** A

**Explanation:**

Reference:

<https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-firewall/Concepts%20-%20Firewall/Static%20N>

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD44529>

**NEW QUESTION 7**

- (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 8**

- (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 9**

- (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

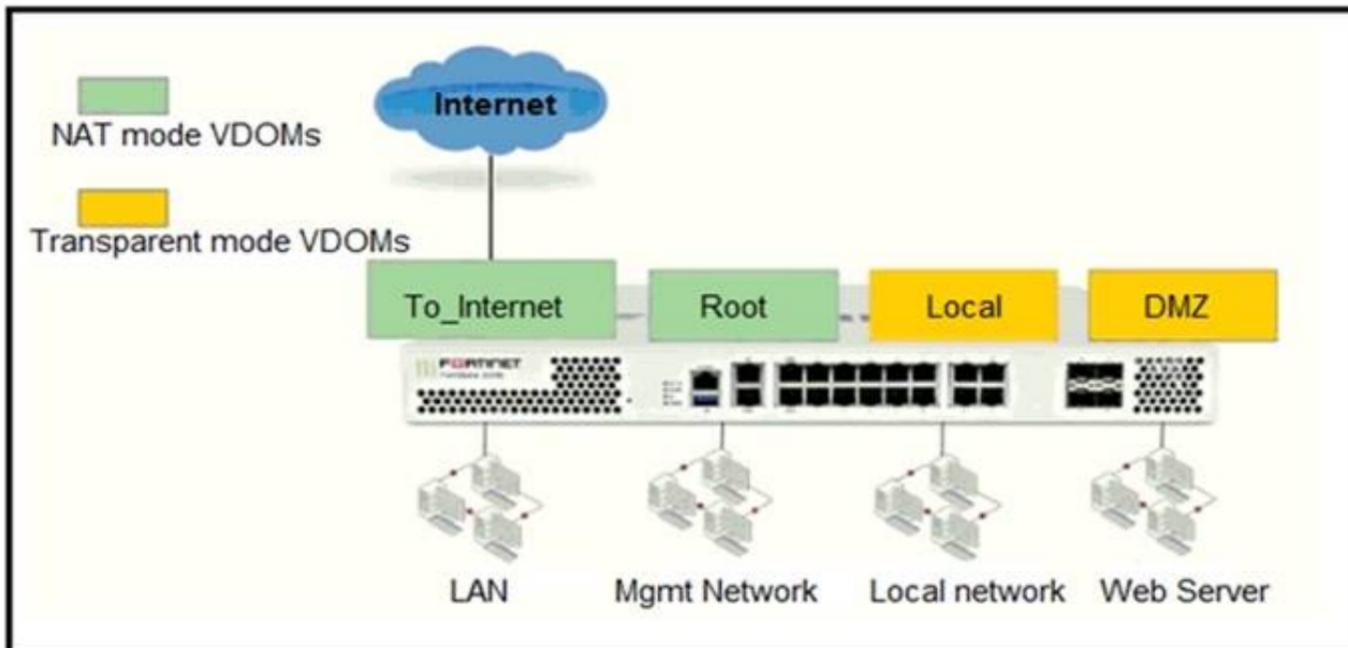
**Explanation:**

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

**NEW QUESTION 10**

- (Exam Topic 1)

Refer to the exhibit.



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

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

**Answer:** A

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46542>

**NEW QUESTION 10**

- (Exam Topic 1)

Refer to the exhibit.

```
STUDENT # get system session list
PROTO  EXPIRE  SOURCE      SOURCE-NAT  DESTINATION  DESTINATION-NAT
tcp     3598     10.0.1.10:2706 10.200.1.6:2706 10.200.1.254:80 -
tcp     3598     10.0.1.10:2704 10.200.1.6:2704 10.200.1.254:80 -
tcp     3596     10.0.1.10:2702 10.200.1.6:2702 10.200.1.254:80 -
tcp     3599     10.0.1.10:2700 10.200.1.6:2700 10.200.1.254:443 -
tcp     3599     10.0.1.10:2698 10.200.1.6:2698 10.200.1.254:80 -
tcp     3598     10.0.1.10:2696 10.200.1.6:2696 10.200.1.254:443 -
udp     174      10.0.1.10:2694 -             10.0.1.254:53 -
udp     173      10.0.1.10:2690 -             10.0.1.254:53 -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

- A. Destination NAT is disabled in the firewall policy.
- B. One-to-one NAT IP pool is used in the firewall policy.
- C. Overload NAT IP pool is used in the firewall policy.
- D. Port block allocation IP pool is used in the firewall policy.

**Answer:** B

**Explanation:**

FortiGate\_Security\_6.4 page 155 . In one-to-one, PAT is not required.

**NEW QUESTION 15**

- (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 16**

- (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 20**

- (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 24**

- (Exam Topic 1)

Refer to the exhibits.

Exhibit A.

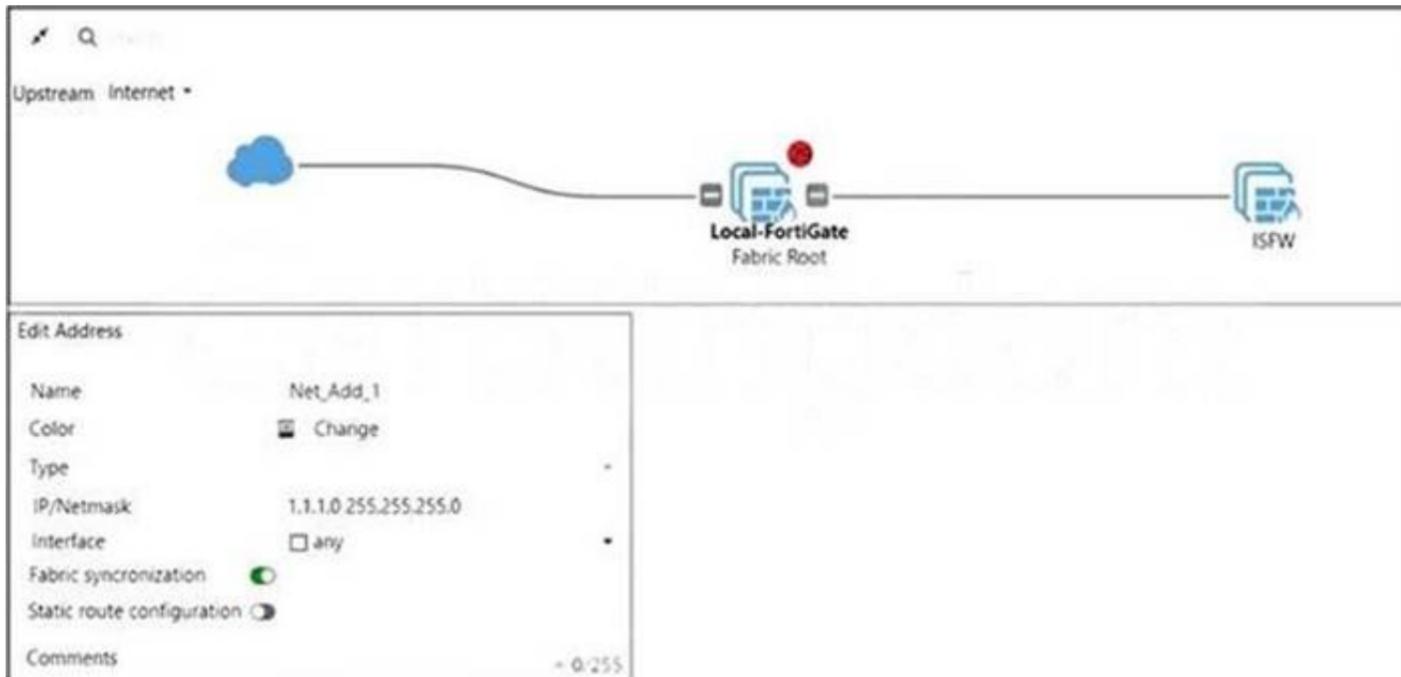


Exhibit B.

```

Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 0.0.0.0
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC X18CtzrcUBUq9yz9nryP+YfM16
    BJKv7S/trtoh2gYAe5CH8YMAa0GT18aX+/dKH/o5izw1ZEoN1QN2N
    FGLT4r5z2AyYI8i1PxutiLcsCplAdZadv1Cx0e66IdLX7I6o22J9P
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification local
    set saml-configuration-sync default

ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 10.0.1.254
    set upstream-port 8013
    set group-name ""
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync default
end

ISFW #
ISFW #
    
```

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).

What must the administrator do to synchronize the address object?

- A. Change the csf setting on Local-FortiGate (root) to sec configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to sec configuracion-sync local.
- C. Change the csf setting on Local-FortiGate (root) to sec fabric-objecc-unificacion default.
- D. Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion default.

**Answer:** A

**Explanation:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD43820>

**NEW QUESTION 29**

- (Exam Topic 1)

Refer to the exhibits.

### Exhibit A

**Edit Policy**

Name  Facebook SSL Inspection

Incoming Interface  port2

Outgoing Interface  port1

Source  all

Destination  all

Service  ALL

**Firewall / Network Options**

 Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied

**Security Profiles**

SSL Inspection  certificate-inspection

### Exhibit B

**Edit Policy**

Name  Facebook Access

Incoming Interface  port2

Outgoing Interface  port1

Source  all

Destination  all

Schedule  always

Service **App Default** Specify

Application Facebook

Application Facebook\_Like.Button 

Application Facebook\_Video.Play

URL Category +

Action  ACCEPT  DENY

**Firewall / Network Options**

Protocol Options  default

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook. Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

- A. The SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

**Answer:** A

**Explanation:**

The lock logo behind Facebook\_like.Button indicates that SSL Deep Inspection is Required.

**NEW QUESTION 32**

- (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 33**

- (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 38**

- (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 43**

- (Exam Topic 2)

An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?

- A. 192.168.3.0/24
- B. 192.168.2.0/24
- C. 192.168.1.0/24
- D. 192.168.0.0/8

**Answer: B**

**NEW QUESTION 46**

- (Exam Topic 2)

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-Filter
Status      : Enable
License     : Contract

Num. of servers : 1
Protocol    : https
Port        : 443
Anycast     : Enable
Default servers : Not included
-- Server List (Tue Feb 1 12:00:25 2020) --
```

IP	Weight	RTT	Flags	TZ	Packets	Curr Lost	Total Lost
173.243.138.210	10	85	DI	-8	868	0	0
96.45.33.68	10	270		-8	868	0	0
173.243.138.211	10	340		-8	859	0	0

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

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

**Answer: BD**

**NEW QUESTION 47**

- (Exam Topic 2)

An administrator must disable RPF check to investigate an issue.

Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

- A. Enable asymmetric routing, so the RPF check will be bypassed.
- B. Disable the RPF check at the FortiGate interface level for the source check.
- C. Disable the RPF check at the FortiGate interface level for the reply check.
- D. Enable asymmetric routing at the interface level.

**Answer: B**

**Explanation:**

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

**NEW QUESTION 52**

- (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 56**

- (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 60**

- (Exam Topic 2)

View the exhibit.

The screenshot shows the 'Application Control Profile' configuration for 'Addicting Games'. The application is categorized as 'Game' and 'Browser-Based'. Under 'Application Overrides', there is a table with one entry: 'Addicting Games' (Category: Game) with an 'Allow' action. Under 'Filter Overrides', there is a table with one entry: 'Risk' (2304) with a 'Block' action.

Application Signature	Category	Action
Addicting Games	Game	Allow

Filter Details	Action
Risk (2304)	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. Addicting.Games is allowed based on the Categories configuration.

**Answer:** A

**NEW QUESTION 62**

- (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 63**

- (Exam Topic 2)

An administrator is running the following sniffer command:

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

Which three pieces of Information will be Included in the sniffer output? (Choose three.)

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

**Answer:** ABD

#### **NEW QUESTION 64**

- (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 66**

- (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 71**

- (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	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 76**

- (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 78**

- (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 80**

- (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 81**

- (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 84**

- (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 87**

- (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 91**

- (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?

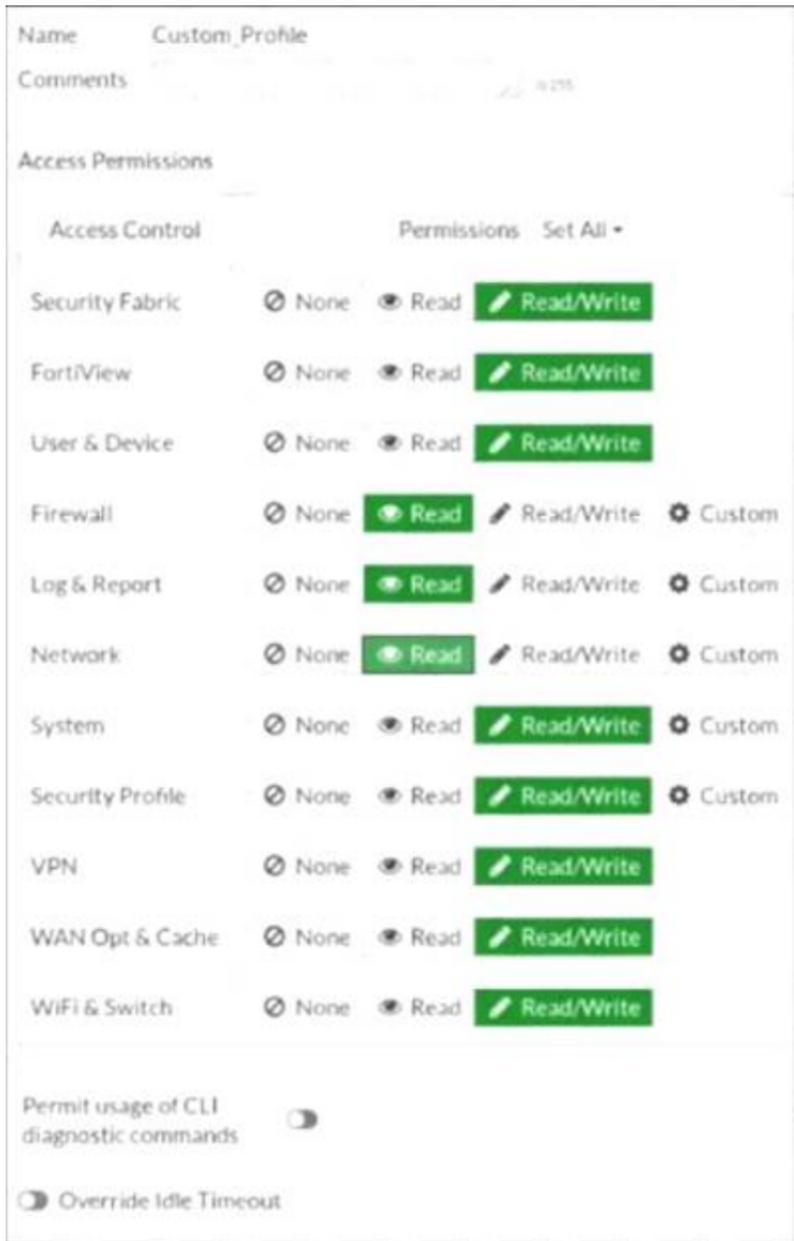
- A. Change the session-ttl.
- B. Change the login timeout.
- C. Change the idle-timeout.
- D. Change the udp idle timer.

**Answer:** B

**NEW QUESTION 92**

- (Exam Topic 2)

Refer to the exhibit.



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 95**

- (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 98**

- (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 102**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 106**

- (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 107**

- (Exam Topic 2)

An administrator needs to increase network bandwidth and provide redundancy.

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

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

**Answer:** C

**Explanation:**

Reference: <https://forum.fortinet.com/tm.aspx?m=120324>

**NEW QUESTION 111**

- (Exam Topic 2)

Refer to the exhibit.

```

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 ippool enable
set poolname "ProxyPool"
set nat enable
next
end

config firewall proxy-address
edit "EICAR"
set uuid 5a24bdaa-c792-51ea-2c89-a9f79e2bdc96
set type host-regex
set host-regex ".*eicar\\.org"
next
end

FIREWALL POLICIES

config firewall
edit 1
set uuid 6491d126-c790-51ea-1319-4ed04b543abe
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
    
```

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 114**

- (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 118**

- (Exam Topic 2)

Consider the topology:

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

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

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

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

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

**Answer: CD**

**NEW QUESTION 120**

- (Exam Topic 2)

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

**IPS Sensor**

Name: **WINDOWS\_SERVERS** [View IPS Signatures]

Comments:  0 / 255

**IPS Signatures**

+ Add Signatures Delete Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
<b>No matching entries found</b>							

**IPS Filters**

+ Add Filter Edit Filter Delete

Filter Details	Action	Packet Logging
Location:server OS:Windows	Block	<input checked="" type="checkbox"/>

Apply

**Forward Traffic Logs**

#	Date/Time	Source	Destination	Application Name	Result	Policy
1	10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2	10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3	10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4	10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5	10:09:01	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6	10:08:59	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10	10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 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 125**

- (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 129**

- (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 132**

- (Exam Topic 2)

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

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

**Answer:** CD

**NEW QUESTION 137**

- (Exam Topic 2)

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

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

**Answer:** ACD

**NEW QUESTION 140**

- (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 143**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 144**

- (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 149**

.....

## **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](#)**