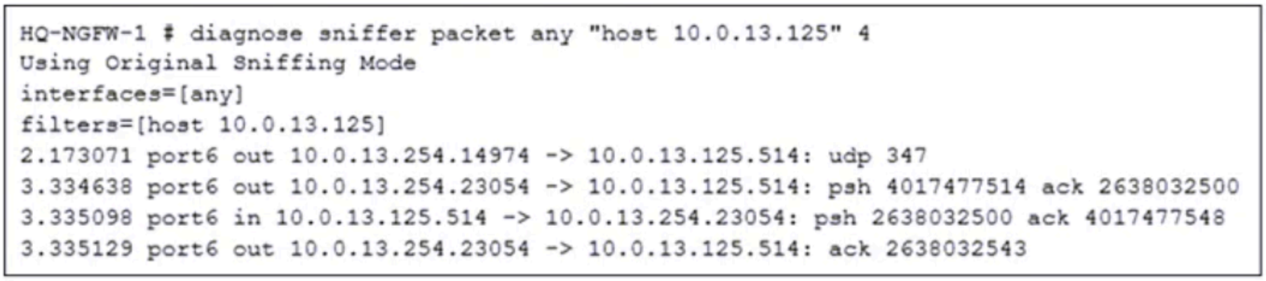
Question #1 *Topic 1*

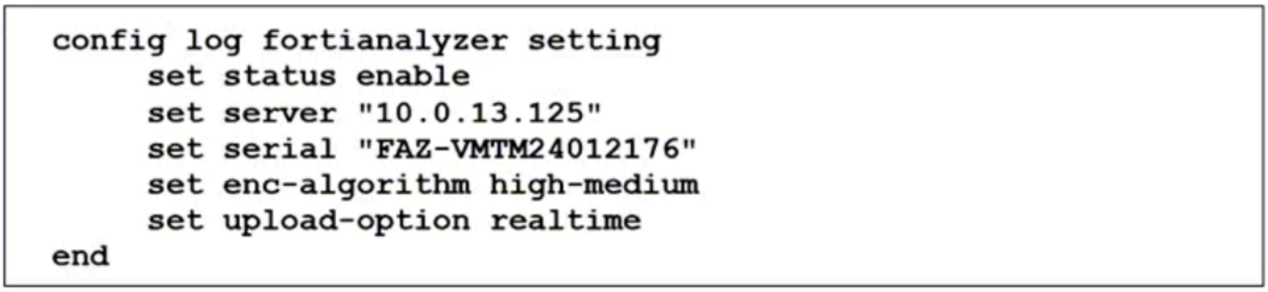
The FortiGate device HQ-NGFW-1 with the IP address 10.0.13.254 sends logs to the FortiAnalyzer device with the IP address 10.0.13.125. The administrator wants to verify that reliable logging is enabled on HQ-NGFW-1.
Which exhibit helps with the verification?

A.



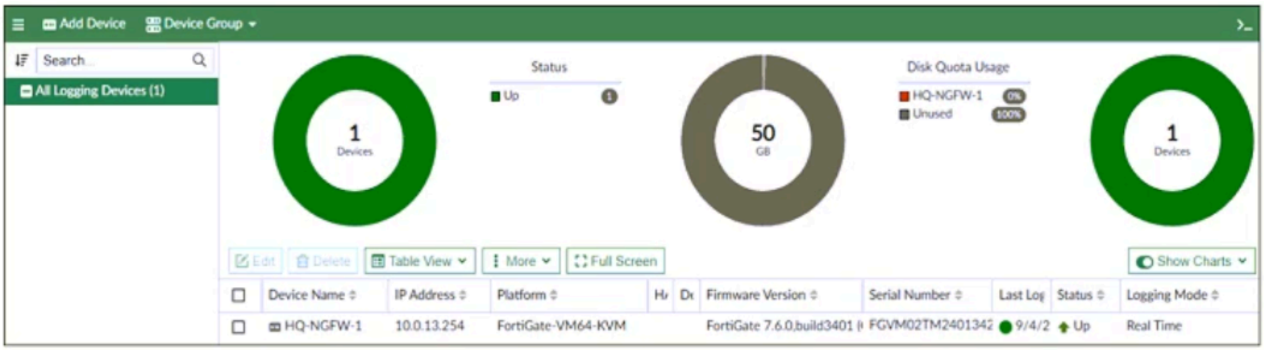
```
HQ-NGFW-1 # diagnose sniffer packet any "host 10.0.13.125" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.13.125]
2.173071 port6 out 10.0.13.254.14974 -> 10.0.13.125.514: udp 347
3.334638 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: psh 4017477514 ack 2638032500
3.335098 port6 in 10.0.13.125.514 -> 10.0.13.254.23054: psh 2638032500 ack 4017477548
3.335129 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: ack 2638032543
```

B.



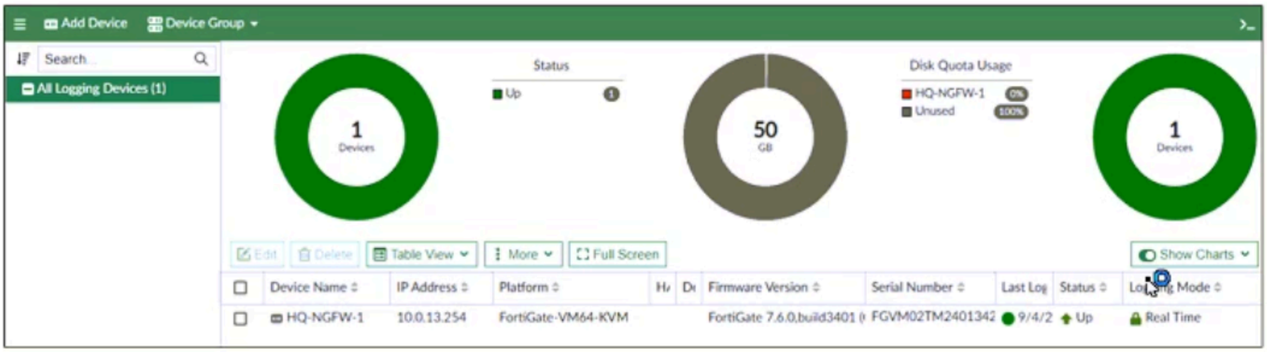
```
config log fortianalyzer setting
    set status enable
    set server "10.0.13.125"
    set serial "FAZ-VMTM24012176"
    set enc-algorithm high-medium
    set upload-option realtime
end
```

C.



□	Device Name	IP Address	Platform	H	D	Firmware Version	Serial Number	Last Log	Status	Logging Mode
□	HQ-NGFW-1	10.0.13.254	FortiGate-VM64-KVM			FortiGate 7.6.0,build3401 (	FGVM02TM2401342	● 9/4/2	Up	Real Time

D.



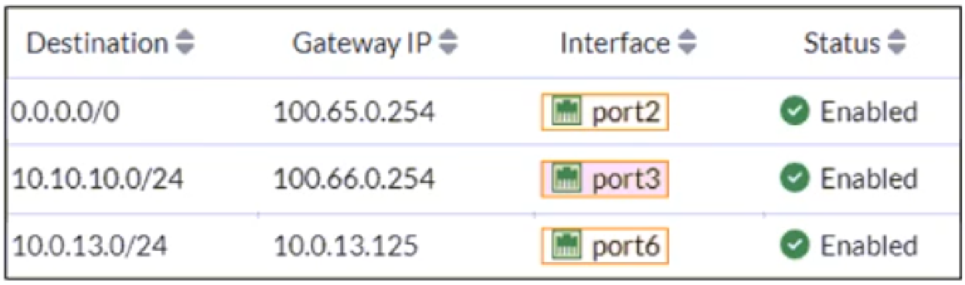
□	Device Name	IP Address	Platform	H	D	Firmware Version	Serial Number	Last Log	Status	Logging Mode
□	HQ-NGFW-1	10.0.13.254	FortiGate-VM64-KVM			FortiGate 7.6.0,build3401 (	FGVM02TM2401342	● 9/4/2	Up	🔒 Real Time

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Refer to the exhibit.



Destination	Gateway IP	Interface	Status
0.0.0.0/0	100.65.0.254	port2	✓ Enabled
10.10.10.0/24	100.66.0.254	port3	✓ Enabled
10.0.13.0/24	10.0.13.125	port6	✓ Enabled

Based on the routing table shown in the exhibit, which two statements are true? (Choose two.)

A. A packet with the source IP address 10.0.13.10 arriving on port2 is allowed if strict RPF is disabled.

B. A packet with the source IP address 10.100.110.10 arriving on port3 is allowed if strict RPF is disabled.

C. A packet with the source IP address 10.10.10.10 arriving on port2 is allowed if strict RPF is enabled.

D. A packet with the source IP address 10.100.110.10 arriving on port2 is allowed if strict RPF is enabled.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

A. They can be measured actively or passively.

B. They are applied in a SD-WAN rule lowest cost strategy.

C. They monitor the state of the FortiGate device.

D. All the SLA targets can be configured.

E. They rely on session loss and jitter.

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively.
Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

A. Both interfaces must have directly connected routes on the routing table.

B. Both interfaces must have IP addresses assigned.

C. Both interfaces must have DHCP enabled and interfaces set to LAN and DMZ roles assigned.

D. Both interfaces must have the interface role assigned.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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 matching firewall policy is set to proxy inspection mode.

B. The option invalid SSL certificates is set to allow on the SSL/SSH inspection profile.

C. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

D. The browser does not trust the certificate used by FortiGate for SSL inspection.

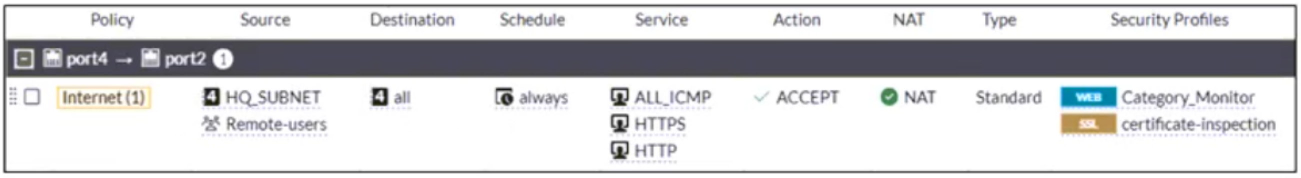
Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #6

Topic 1

Refer to the exhibit, which shows a firewall policy to enable active authentication.



Policy	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
⊟ port4 → port2								
□ Internet (1)	HQ_SUBNET Remote-users	all	always	ALL_ICMP HTTPS HTTP	✓ ACCEPT	● NAT	Standard	WEB Category_Monitor SSL certificate-inspection

When attempting to access an external website using an active authentication method, the user is not presented with a login prompt.

What is the most likely reason for this situation?

A. The Service DNS is required in the firewall policy.

B. The Remote-users group is not added to the Destination.

C. The Remote-users group must be set up correctly in the FSSO configuration.

D. No matching user account exists for this user.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view.
Why is the policy order different in these two views?

A. Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.

B. By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.

C. The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.

D. Policies in Interface Pair View are prioritized by security levels, while By Sequence View strictly follows the administrator's manual ordering.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #8

Topic 1

You have created a web filter profile named restrict_media-profile with a daily category usage quota.
When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down.
What could be the reason?

A. The inspection mode in the firewall policy is not matching with web filter profile feature set.

B. The web filter profile is already referenced in another firewall policy.

C. The naming convention used in the web filter profile is restricting it in the firewall policy.

D. The firewall policy is in no-inspection mode instead of deep-inspection.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.
Which DPD mode on FortiGate meets this requirement?

A. On Demand

B. Enabled

C. On Idle

D. Disabled

Suggested Answer: *C*

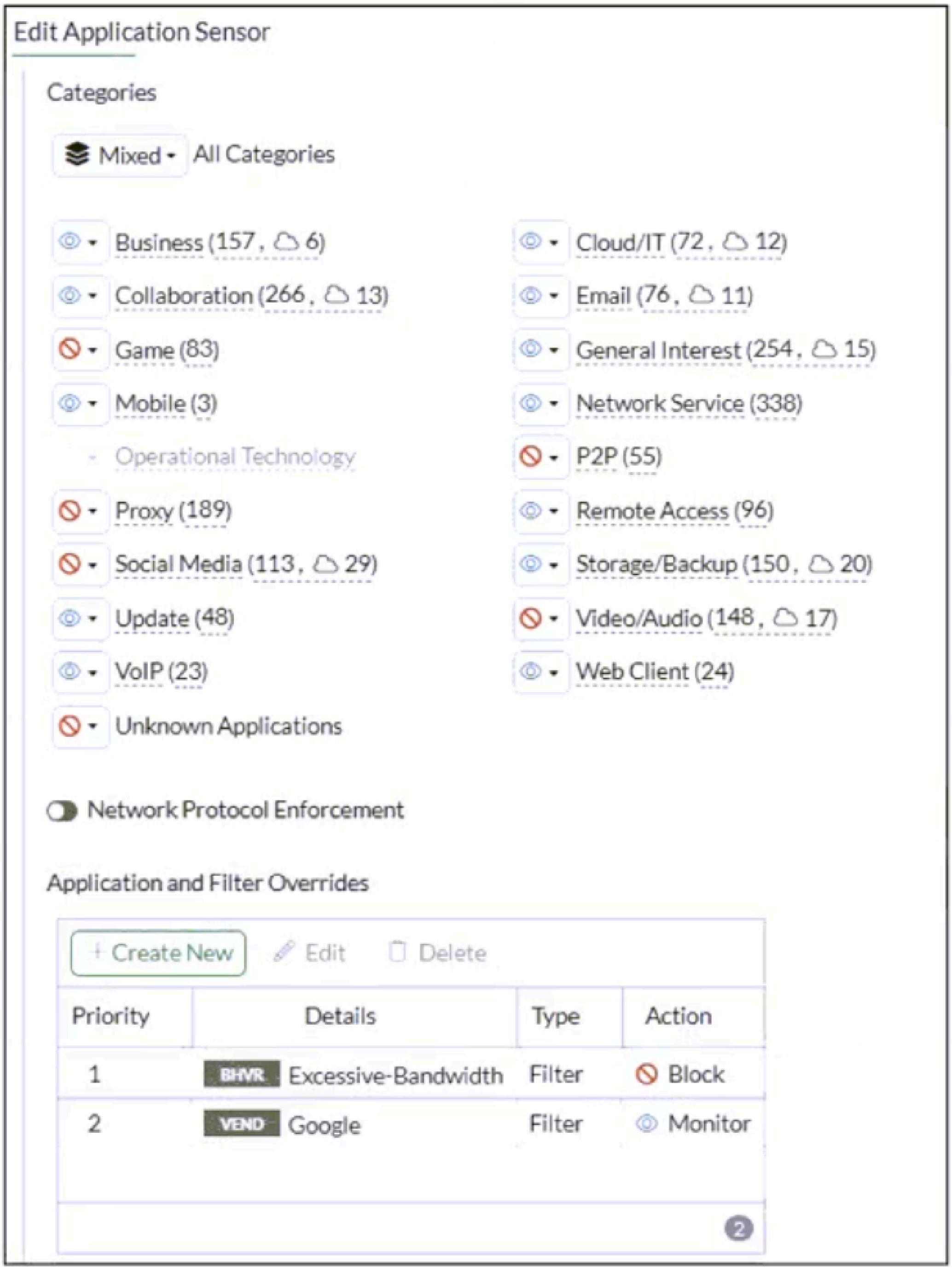
Currently there are no comments in this discussion, be the first to comment!

Question #10

Topic 1

Refer to the exhibits.

Application sensor



Edit Application Sensor

Categories

Mixed ▾ All Categories

- 👁 ▾ Business (157, ☁ 6)
- 👁 ▾ Collaboration (266, ☁ 13)
- 🚫 ▾ Game (83)
- 👁 ▾ Mobile (3)
- ▾ Operational Technology
- 🚫 ▾ Proxy (189)
- 🚫 ▾ Social Media (113, ☁ 29)
- 👁 ▾ Update (48)
- 👁 ▾ VoIP (23)
- 🚫 ▾ Unknown Applications
- 👁 ▾ Cloud/IT (72, ☁ 12)
- 👁 ▾ Email (76, ☁ 11)
- 👁 ▾ General Interest (254, ☁ 15)
- 👁 ▾ Network Service (338)
- 🚫 ▾ P2P (55)
- 👁 ▾ Remote Access (96)
- 👁 ▾ Storage/Backup (150, ☁ 20)
- 🚫 ▾ Video/Audio (148, ☁ 17)
- 👁 ▾ Web Client (24)

○ Network Protocol Enforcement

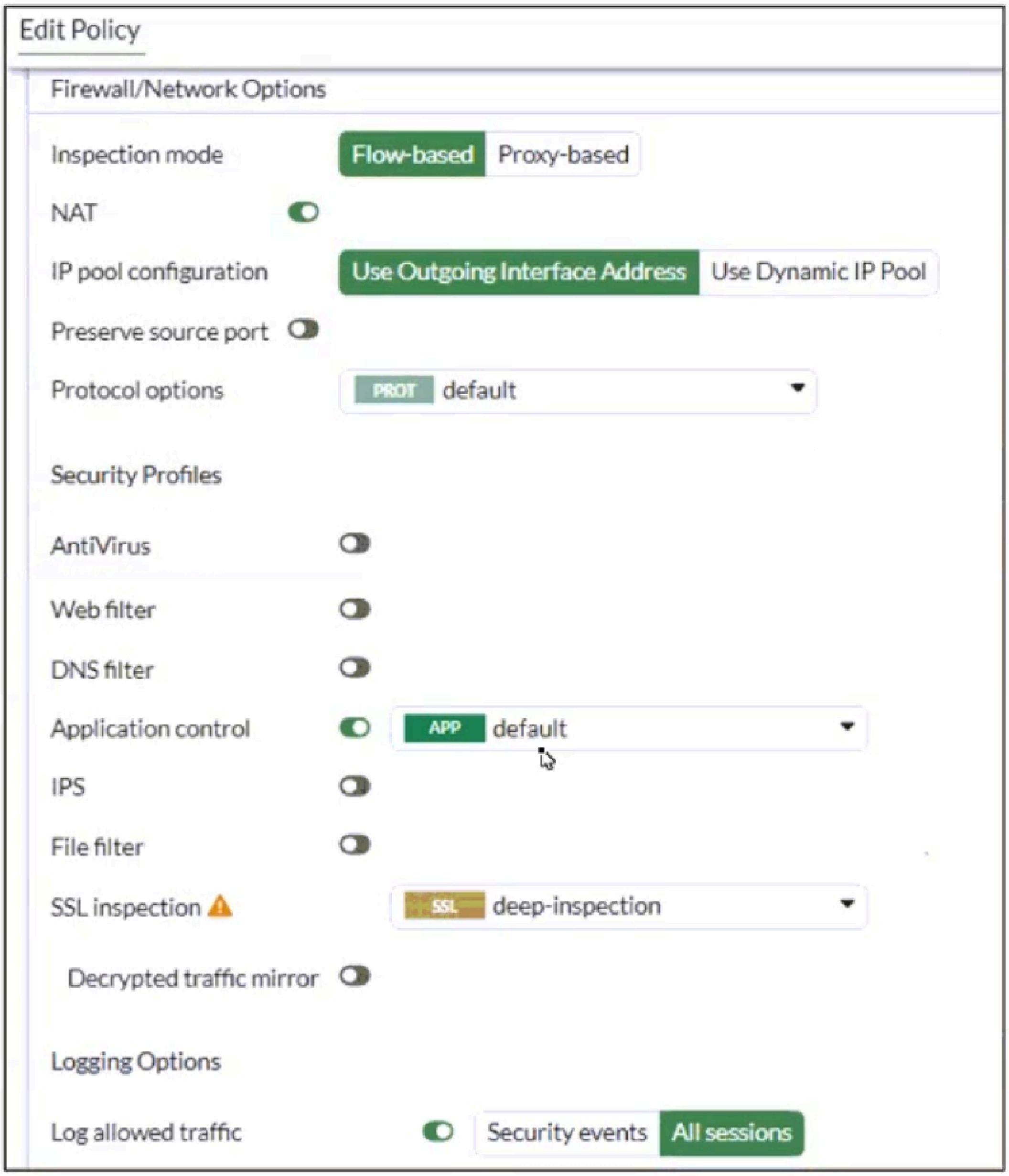
Application and Filter Overrides

+ Create New Edit Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	🚫 Block
2	VEND Google	Filter	👁 Monitor

2

Firewall policy


Edit Policy

Firewall/Network Options

Inspection mode [✓ Flow-based] Proxy-based

NAT ●

IP pool configuration [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Preserve source port ○

Protocol options PROT default

Security Profiles

AntiVirus ○

Web filter ○

DNS filter ○

Application control ● APP default

IPS ○

File filter ○

SSL inspection ⚠ SSL deep-inspection

Decrypted traffic mirror ○

Logging Options

Log allowed traffic ● Security events [✓ All sessions]

You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.
Which two factors can you observe from these configurations? (Choose two.)

A. YouTube search is allowed based on the Google Application and Filter override settings.

B. Facebook access is blocked based on the category filter settings.

C. Facebook access is allowed but you cannot play Facebook videos based on Video/Audio category filter settings.

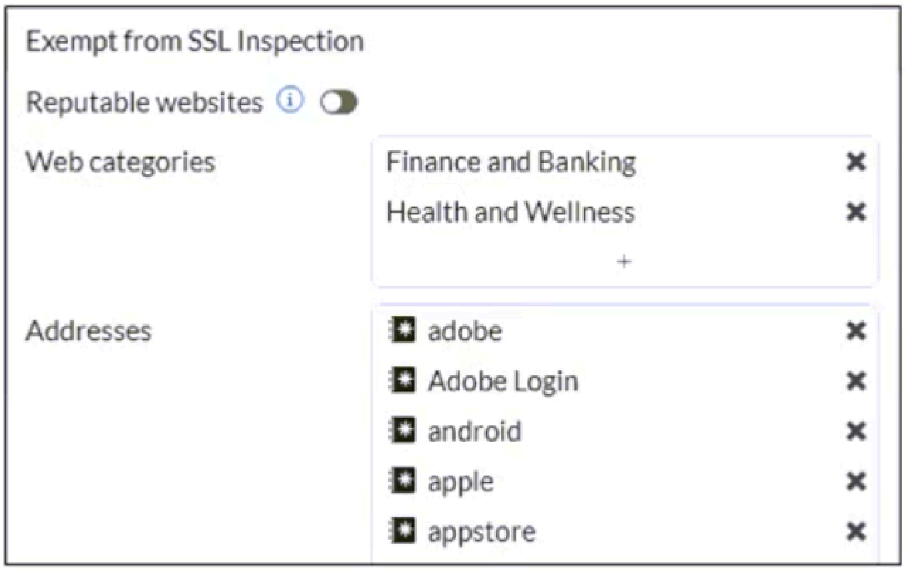
D. YouTube access is blocked based on Excessive-Bandwidth Application and Filter override settings.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Refer to the exhibit.



Exempt from SSL Inspection

Reputable websites ⓘ ○

Web categories	Finance and Banking ✕ Health and Wellness ✕ +
Addresses	adobe ✕ Adobe Login ✕ android ✕ apple ✕ appstore ✕

The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit.

For which two reasons are these web categories exempted? (Choose two.)

A. The FortiGate temporary certificate denies the browser’s access to websites that use HTTP Strict Transport Security.

B. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.

C. These websites are in an allowlist of reputable domain names maintained by FortiGuard.

D. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

What are two features of FortiGate FSSO agentless polling mode? (Choose two.)

A. FortiGate does not support workstation check.

B. FortiGate directs the collector agent to use a remote LDAP server.

C. FortiGate uses the AD server as the collector agent.

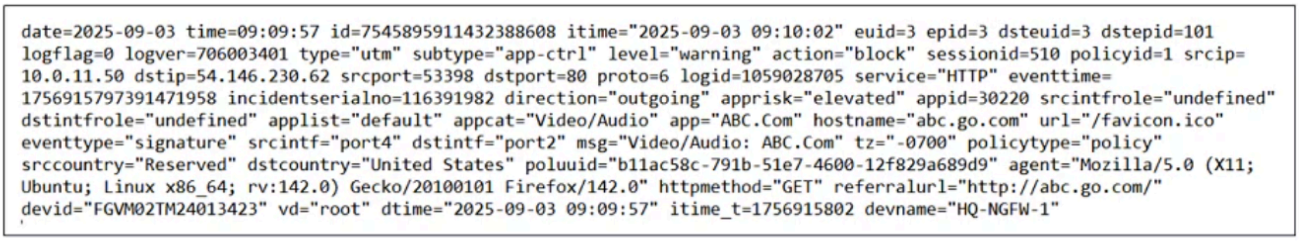
D. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Refer to the exhibit.



```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluuid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

Which two ways can you view the log messages shown in the exhibit? (Choose two.)

A. By right clicking the implicit deny policy

B. By filtering the policy universally unique identifier (UUID) and application name in the log entry

C. Using the FortiGate CLI command diagnose log test

D. In the Forward Traffic section

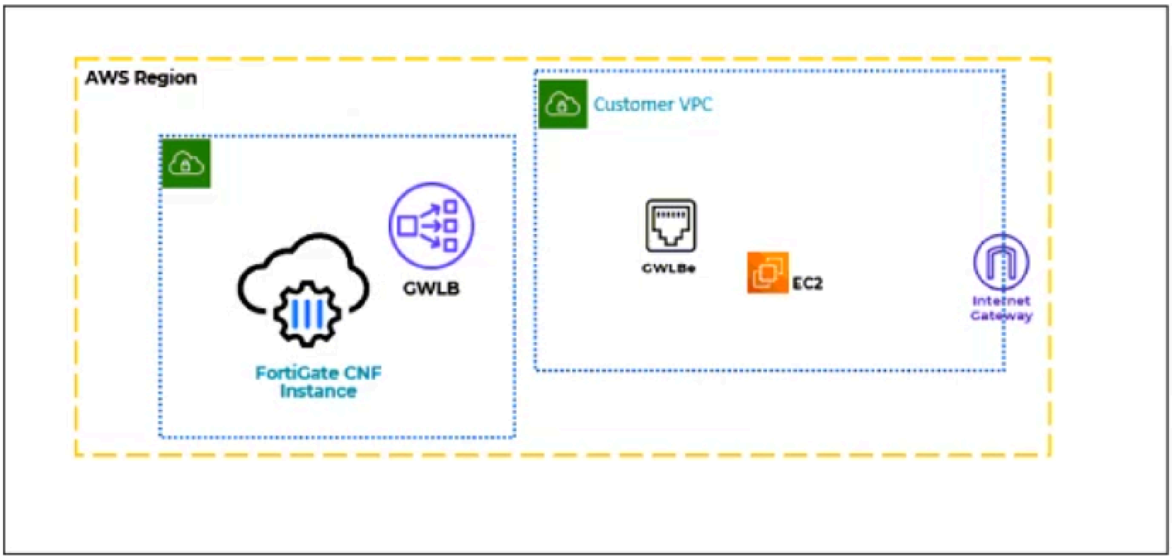
Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Refer to the exhibit.

A partial cloud topology is shown.



You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS.

During the deployment, which components must be FortiGate CNF create to handle traffic from the EC2 instance?

A. The GWLB, GWLBe, and the internet gateway (IGW) in the customer VPC

B. The CNF VPC, customer VPC, and GWLB

C. The customer VPC and GWLBe

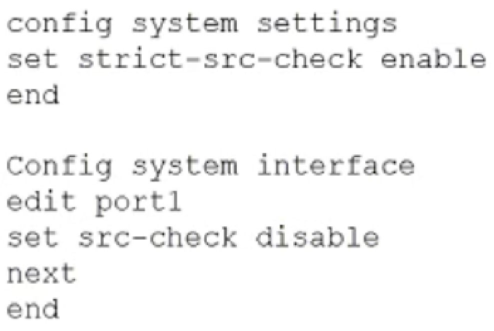
D. The gateway load balancer endpoint (GWLBe) in the customer virtual private cloud (VPC)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

You have configured the below commands on a FortiGate.



```
config system settings
set strict-src-check enable
end

Config system interface
edit port1
set src-check disable
next
end
```

What would be the impact of this configuration on FortiGate?

A. FortiGate will enable strict RPF on all its interfaces and port1 will be enable for asymmetric routing.

B. Port1 will be enabled with flexible RPF, and all other interfaces will be enabled for strict RPF.

C. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.

D. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

FortiGate is integrated with FortiAnalyzer and FortiManager.
When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

A. Universally Unique Identifier

B. Log ID

C. Sequence ID

D. Policy ID

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

You have configured an application control profile, set peer-o-peer traffic to Block under the Categories tab, and applied it to the firewall policy. However, you peer-to-peer traffic on known ports is passing through the FortiGate without being blocked.
What FortiGate settings should you check to resolve this issue?

A. Replacement Messages for UDP-based Applications

B. Network Protocol Enforcement

C. Application and Filter Overrides

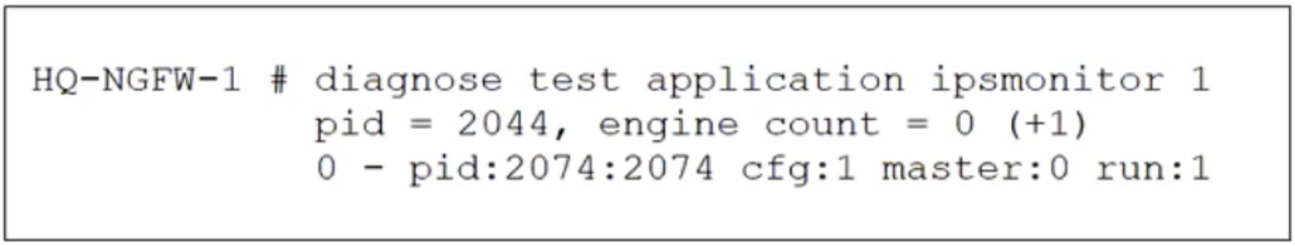
D. FortiGuard category ratings

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Refer to the exhibit.



```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
            pid = 2044, engine count = 0 (+1)
            0 - pid:2074:2074 cfg:1 master:0 run:1
```

As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit.
What could be the possible reason of the diagnose output shown in the exhibit?

A. There is no firewall policy configured with an IPS security profile.

B. Administrator entered the command diagnose test application ipsmonitor 5.

C. FortiGate entered into IPS fail open state.

D. Administrator entered the command diagnose test application ipsmonitor 99.

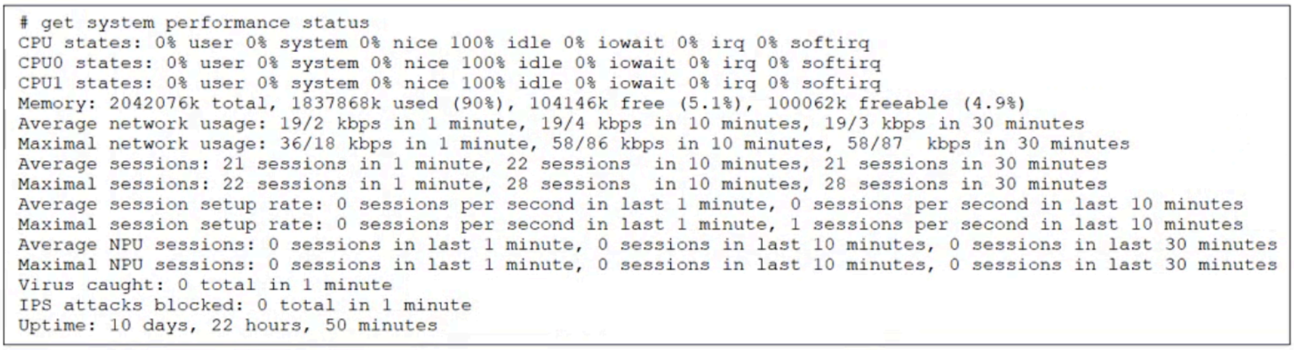
Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

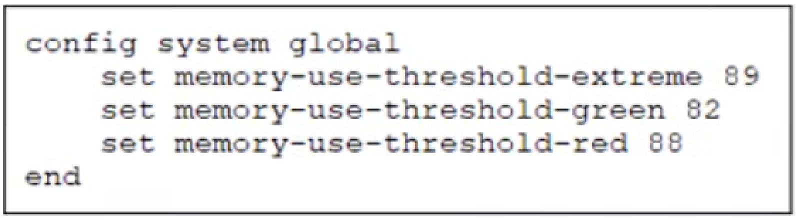
Refer to the exhibits.

System Performance output



```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings



```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.

Based on the system performance output, what are the two possible outcomes? (Choose two.)

A. FortiGate drops new sessions.

B. Administrators can access FortiGate only through the console port.

C. Administrators can change the configuration.

D. FortiGate has entered conserve mode.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #20

Topic 1

What are two characteristics of HA cluster heartbeat IP addresses in an FortiGate device? (Choose two.)

A. Heartbeat IP addresses are used to distinguish between cluster members.

B. The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.

C. Heartbeat interfaces have virtual IP addresses that are manually assigned.

D. A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.

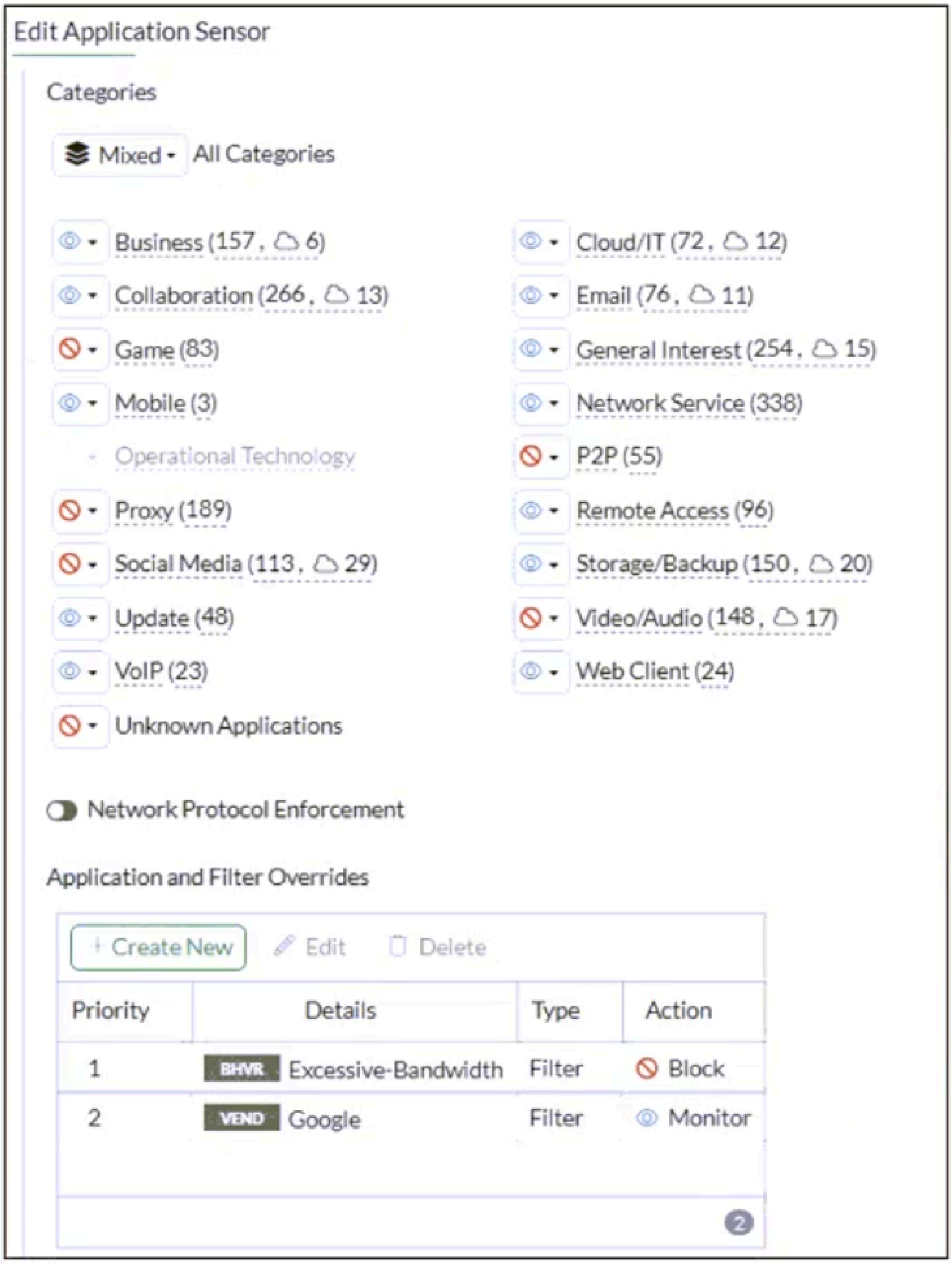
Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Refer to the exhibits.

Application sensor



Edit Application Sensor

Categories

Mixed ▾ All Categories

👁 ▾ Business (157, ☁ 6)

👁 ▾ Collaboration (266, ☁ 13)

🚫 ▾ Game (83)

👁 ▾ Mobile (3)

▾ Operational Technology

🚫 ▾ Proxy (189)

🚫 ▾ Social Media (113, ☁ 29)

👁 ▾ Update (48)

👁 ▾ VoIP (23)

🚫 ▾ Unknown Applications

👁 ▾ Cloud/IT (72, ☁ 12)

👁 ▾ Email (76, ☁ 11)

👁 ▾ General Interest (254, ☁ 15)

👁 ▾ Network Service (338)

🚫 ▾ P2P (55)

👁 ▾ Remote Access (96)

👁 ▾ Storage/Backup (150, ☁ 20)

🚫 ▾ Video/Audio (148, ☁ 17)

👁 ▾ Web Client (24)

○ Network Protocol Enforcement

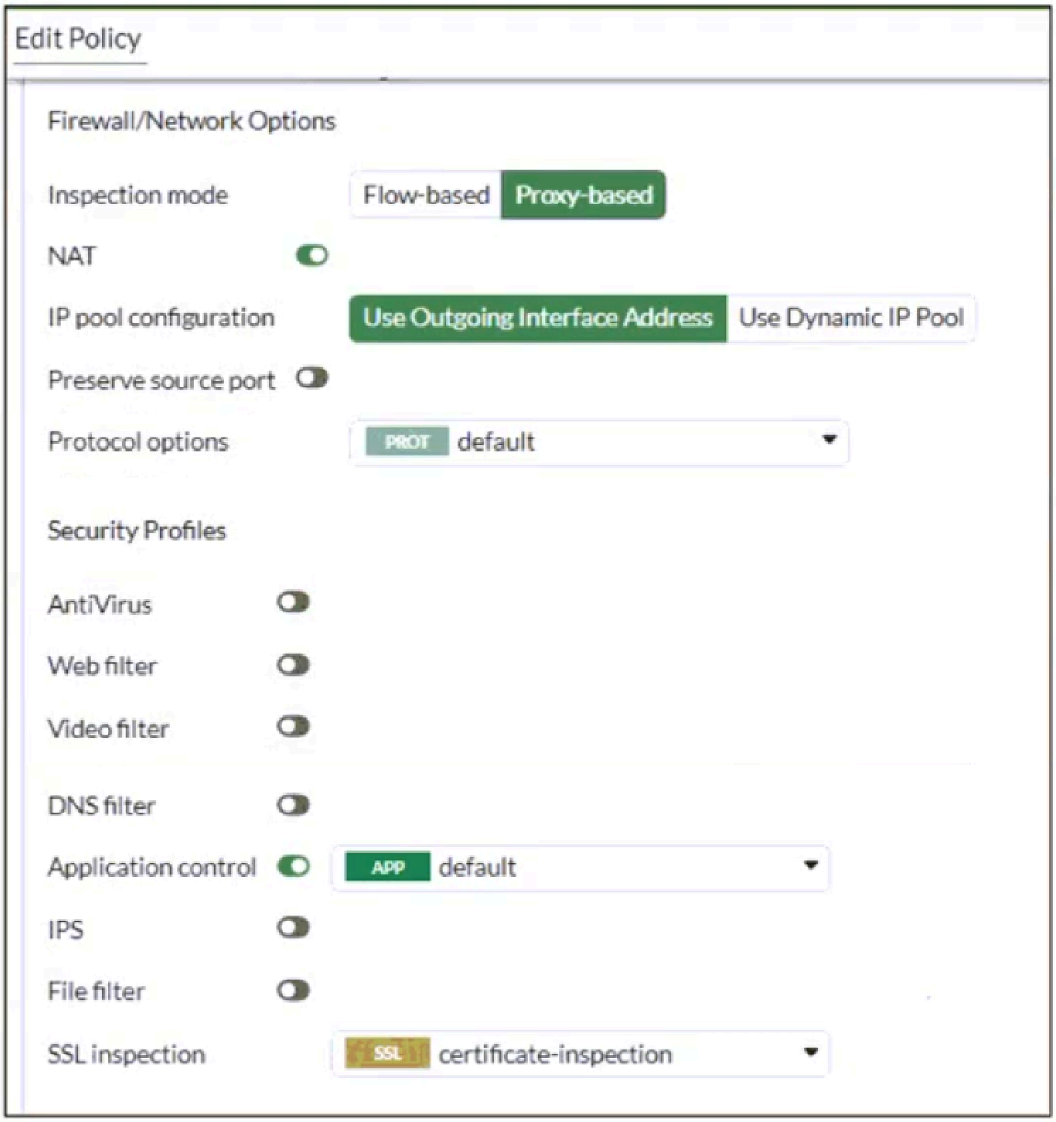
Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	🚫 Block
2	VEND Google	Filter	👁 Monitor

2

Firewall policy



Edit Policy

Firewall/Network Options

Inspection mode: Flow-based [✓ Proxy-based]

NAT ●

IP pool configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Preserve source port ○

Protocol options: PROT default

Security Profiles

AntiVirus ○

Web filter ○

Video filter ○

DNS filter ○

Application control ● APP default

IPS ○

File filter ○

SSL inspection: SSL certificate-inspection

You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.
You cannot access any of the Google applications, but you are able to access www.fortinet.com
Which two actions would you take to resolve the issue? (Choose two.)

A. Change the Inspection mode to Flow-based.

B. Set the action for Google in the Application and Filter Overrides section to Allow.

C. Add “Google”.com to the URL category in the security profile.

D. Set SSL inspection to deep-content inspection.

E. Move up Google in the Application and Filter Overrides section to set its priority to 1.

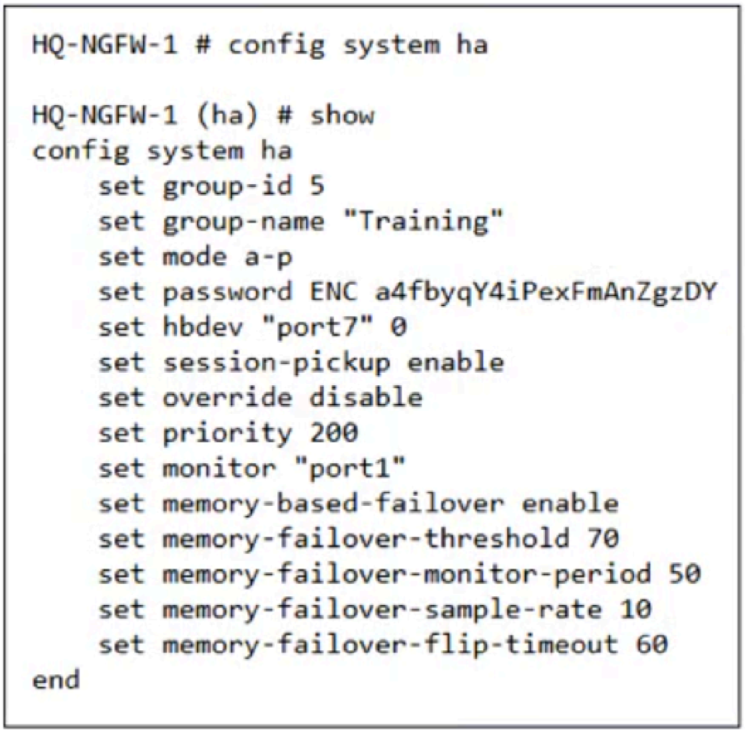
Suggested Answer: *BE*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

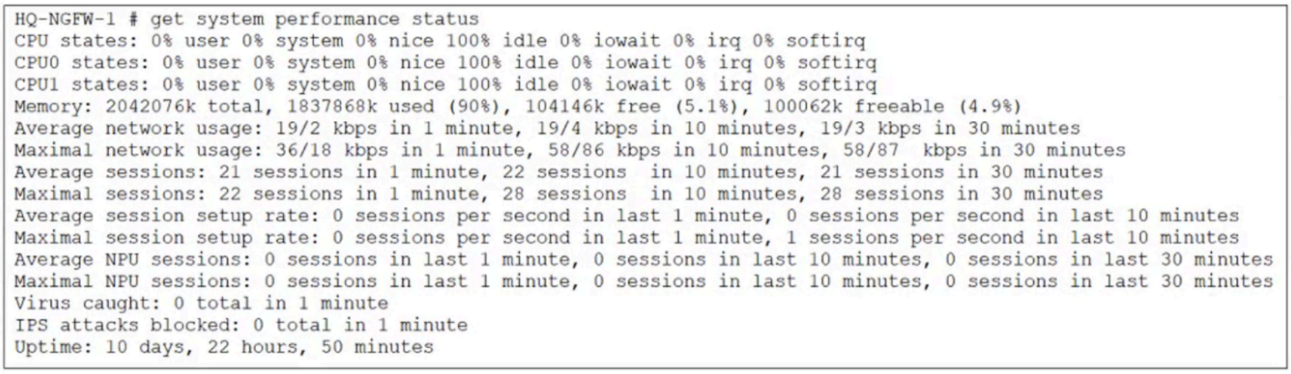
Refer to the exhibits.

HA configuration



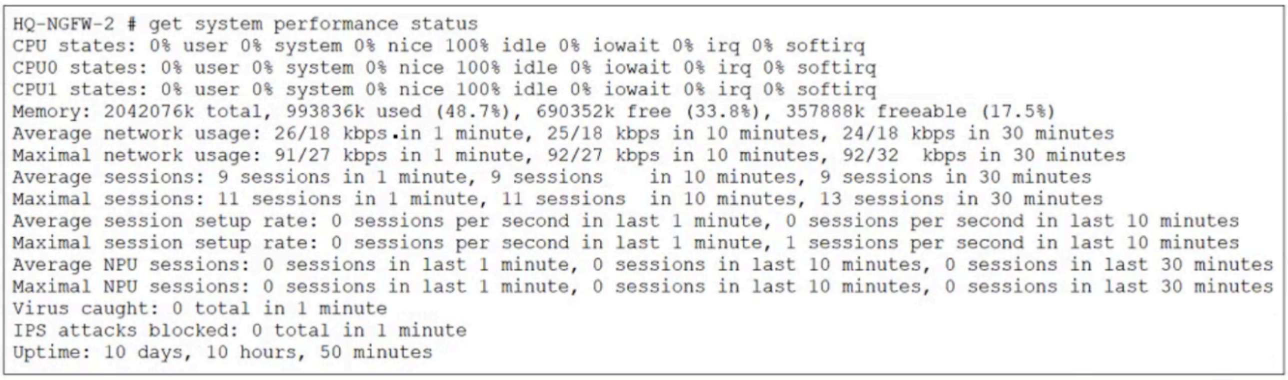
```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output



```
HQ-NGFW-1 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output



```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps.in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32  kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions    in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions  in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds.
Which FortiGate is the primary?

A. HQ-NGFW-2 with the parameter memory-failover-threshold setting

B. HQ-NGFW-1 with the parameter override setting

C. HQ-NGFW-2 with the parameter priority setting

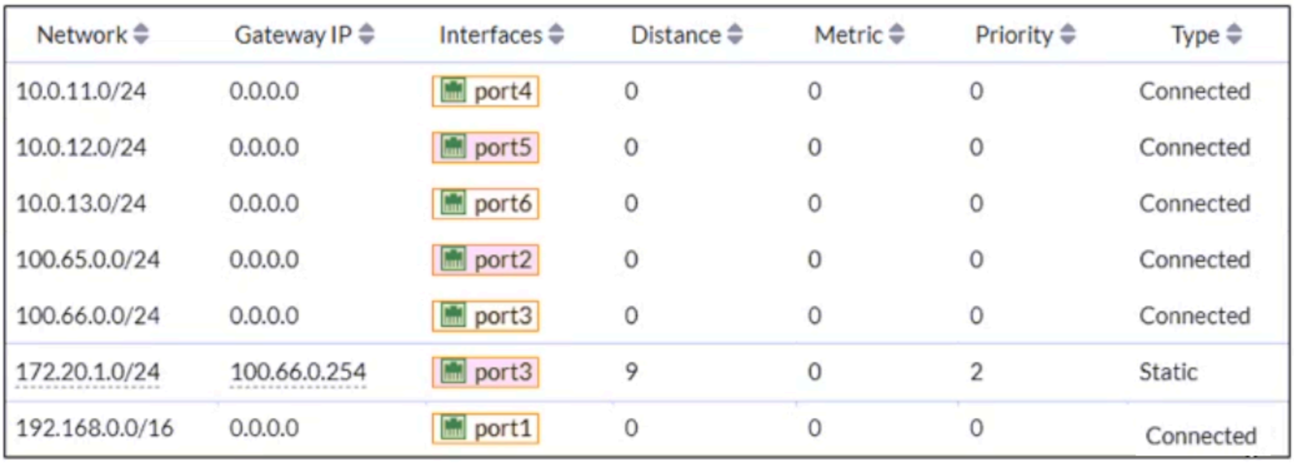
D. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Refer to the exhibit, which shows a routing table.



Network	Gateway IP	Interfaces	Distance	Metric	Priority	Type
10.0.11.0/24	0.0.0.0	port4	0	0	0	Connected
10.0.12.0/24	0.0.0.0	port5	0	0	0	Connected
10.0.13.0/24	0.0.0.0	port6	0	0	0	Connected
100.65.0.0/24	0.0.0.0	port2	0	0	0	Connected
100.66.0.0/24	0.0.0.0	port3	0	0	0	Connected
172.20.1.0/24	100.66.0.254	port3	9	0	2	Static
192.168.0.0/16	0.0.0.0	port1	0	0	0	Connected

An administrator wants to create a new static route so the traffic to the subnet 172.20.1.0/24 is routed through port2 only.
What are the two criteria that the administrator can use to achieve this objective? (Choose two.)

A. The new static route must have the priority set to 3.

B. The existing static route through port 3 must have the distance set to 11.

C. The new static route must have the distance set to 9.

D. The new static route must have the metric set to1.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which two components are part of the secure internet access (SIA) agent-based mode on FortiSASE? (Choose two.)

A. FortiExtender

B. VPN policies

C. The proxy auto-configuration (PAC) file

D. FortiSASE Firewall-as-a-Service (FWaaS)

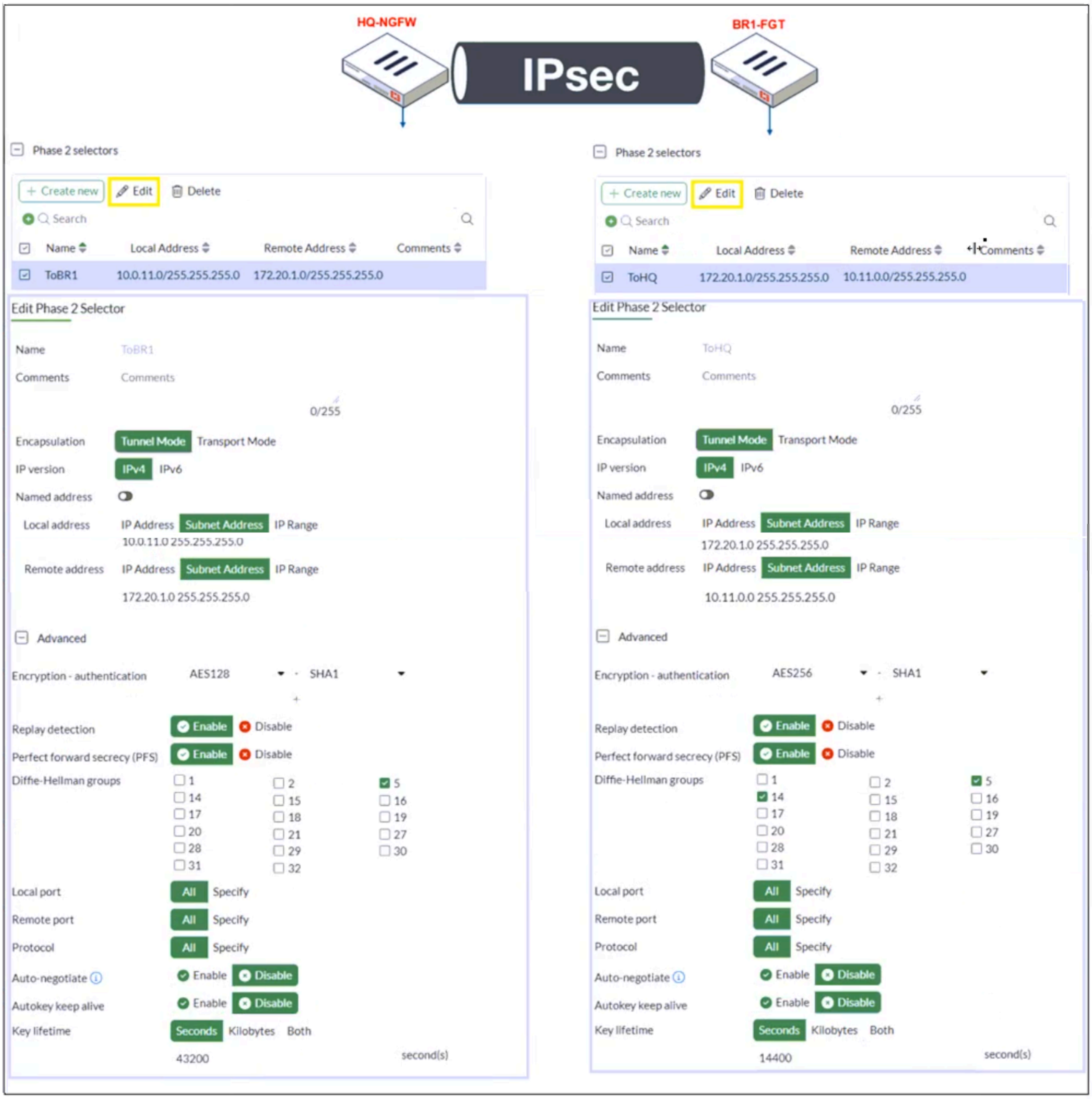
Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Refer to the exhibit.

IPsec tunnel configuration



HQ-NGFW

⊟ Phase 2 selectors

+ Create new | Edit | Delete

Search

☑	Name	Local Address	Remote Address	Comments
☑	ToBR1	10.0.11.0/255.255.255.0	172.20.1.0/255.255.255.0	

Edit Phase 2 Selector

Name: ToBR1

Comments: Comments 0/255

Encapsulation: [✓ Tunnel Mode] Transport Mode

IP version: [✓ IPv4] IPv6

Named address: ○

Local address: IP Address [✓ Subnet Address] IP Range
10.0.11.0 255.255.255.0

Remote address: IP Address [✓ Subnet Address] IP Range
172.20.1.0 255.255.255.0

⊟ Advanced

Encryption - authentication: AES128 - SHA1

Replay detection: [✓ Enable] Disable

Perfect forward secrecy (PFS): [✓ Enable] Disable

Diffie-Hellman groups:
□ 1 □ 2 ☑ 5
□ 14 □ 15 □ 16
□ 17 □ 18 □ 19
□ 20 □ 21 □ 27
□ 28 □ 29 □ 30
□ 31 □ 32

Local port: [✓ All] Specify

Remote port: [✓ All] Specify

Protocol: [✓ All] Specify

Auto-negotiate: Enable [✓ Disable]

Autokey keep alive: Enable [✓ Disable]

Key lifetime: [✓ Seconds] Kilobytes Both
43200 second(s)

BR1-FGT

⊟ Phase 2 selectors

+ Create new | Edit | Delete

Search

☑	Name	Local Address	Remote Address	Comments
☑	ToHQ	172.20.1.0/255.255.255.0	10.11.0.0/255.255.255.0	

Edit Phase 2 Selector

Name: ToHQ

Comments: Comments 0/255

Encapsulation: [✓ Tunnel Mode] Transport Mode

IP version: [✓ IPv4] IPv6

Named address: ○

Local address: IP Address [✓ Subnet Address] IP Range
172.20.1.0 255.255.255.0

Remote address: IP Address [✓ Subnet Address] IP Range
10.11.0.0 255.255.255.0

⊟ Advanced

Encryption - authentication: AES256 - SHA1

Replay detection: [✓ Enable] Disable

Perfect forward secrecy (PFS): [✓ Enable] Disable

Diffie-Hellman groups:
□ 1 □ 2 ☑ 5
☑ 14 □ 15 □ 16
□ 17 □ 18 □ 19
□ 20 □ 21 □ 27
□ 28 □ 29 □ 30
□ 31 □ 32

Local port: [✓ All] Specify

Remote port: [✓ All] Specify

Protocol: [✓ All] Specify

Auto-negotiate: Enable [✓ Disable]

Autokey keep alive: Enable [✓ Disable]

Key lifetime: [✓ Seconds] Kilobytes Both
14400 second(s)

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, which two configuration changes will bring phase 2 up? (Choose two.)

A. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0

B. On BR1-FGT, set Seconds to 43200.

C. On HQ-NGFW, set Encryption to AES256.

D. On HQ-NGFW, enable Diffie-Hellman Group 2.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!