Free Questions for FCP_FGT_AD-7.4

Shared by Farrell on 04-10-2024
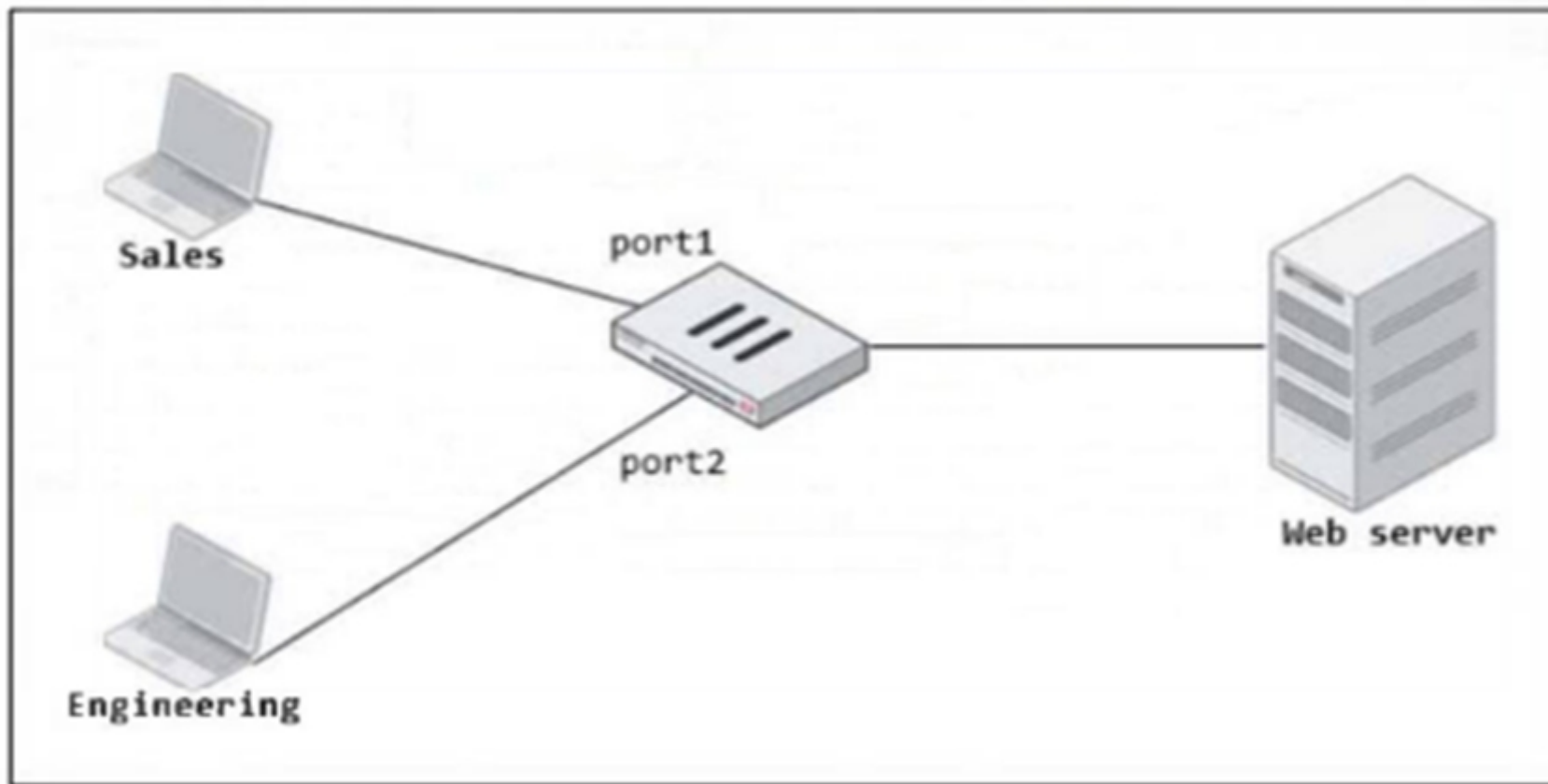
For More Free Questions and Preparation Resources

Question 1

Refer to the exhibit.

FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.

Which action must the administrator perform to consolidate the two policies into one?

Options:

A- Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy

B- Create an Interface Group that includes port1 and port2 to create a single firewall policy

C- Select port1 and port2 subnets in a single firewall policy.

D- Replace port1 and port2 with the any interface in a single firewall policy.

Answer:

A

Question 2

Question Type: **MultipleChoice**

An administrator manages a FortiGate model that supports NTurbo.

How does NTurbo enhance performance for flow-based inspection?

Options:

A- NTurbo offloads traffic to the content processor.

B- NTurbo creates two inspection sessions on the FortiGate device.

C- NTurbo buffers the whole file and then sends it to the antivirus engine.

D- NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.

Answer:

A

Question 3

Question Type: MultipleChoice

An administrator configured a FortiGate to act as a collector for agentless polling mode.

What must the administrator add to the FortiGate device to retrieve AD user group information?

Options:

A- LDAP server

B- RADIUS server

C- DHCP server

D- Windows server

Answer:

D

Question 4

Question Type: MultipleChoice

FortiGate is integrated with FortiAnalyzer and FortiManager.

When a firewall policy is created, which attribute is added to the policy to improve functionality and to support recording logs to FortiAnalyzer or FortiManager?

Options:

A- Log ID

B- Policy ID

C- (Sequence ID

D- Universally Unique Identifier

Answer:

D

Question 5

Question Type: MultipleChoice

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.

Which order must FortiGate use when the web filter profile has features such as safe search enabled?

Options:

A- FortiGuard category filter and rating filter

B- Static domain filter, SSL inspection filter, and external connectors filters

C- DNS-based web filter and proxy-based web filter

D- Static URL filter, FortiGuard category filter, and advanced filters

Answer:

D

Question 6

Refer to the exhibit.

Review the intrusion prevention system (IPS) profile signature settings shown in the exhibit.

What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

Options:

A- Traffic matching the signature will be allowed and logged.

B- The signature setting uses a custom rating threshold.

C- The signature setting includes a group of other signatures.

D- Traffic matching the signature will be silently dropped and logged.

Answer:

D

Question 7

Question Type: **MultipleChoice**

An administrator must enable a DHCP server on one of the directly connected networks on FortiGate. However, the administrator is unable to complete the process on the GUI to enable the service on the interface.

In this scenario, what prevents the administrator from enabling DHCP service?

Options:

A- The role of the interface prevents setting a DHCP server.

B- The DHCP server setting is available only on the CLI.

C- Another interface is configured as the only DHCP server on FortiGate.

D- The FortiGate model does not support the DHCP server.

Answer:

A

Question 8

Refer to the exhibit.

```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025
0"
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=0400000
via port1"
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (p
```

Why did FortiGate drop the packet?

Options:

A- 11 matched an explicitly configured firewall policy with the action DENY

B- It failed the RPF check.

C- The next-hop IP address is unreachable.

D- It matched the default implicit firewall policy

Answer:

D

Question 9

Question Type: MultipleChoice

Refer to the exhibit showing a FortiGuard connection debug output.

FortiGuard connection debug output

```
FortiGate # diagnose debug rating
Locale        : english

Service       : Web-filter
Status        : Enable
License       : Contract

Service       : Antispam
Status        : Disable

Service       : Virus Outbreak Prevention
Status        : Disable

Num. of servers : 1
Protocol      : https
Port          : 443
Anycast       : Enable
Default servers : Included

-=- Server List (Thu Jun  9 11:26:56 2022) -=-

IP                Weight  RTT Flags TZ  FortiGuard-requests  Curr Lost Total Lost Upda
173.243.141.16        -8   18    DI  0                    4            0          0 Thu
12.34.97.18           20   30        1                    1            0          0 Thu
210.7.96.18          160  305        9                    0            0          0 Thu
```

Based on the output, which two facts does the administrator know about the FortiGuard connection? (Choose two.)

Options:

A- One server was contacted to retrieve the contract information.

B- There is at least one server that lost packets consecutively.

C- A local FortiManaqer is one of the servers FortiGate communicates with.

D- FortiGate is using default FortiGuard communication settings.

Answer:

A, D