EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 1 DISCUSSION

Refer to the exhibit.

FortiGate routing database

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
C    *> 172.16.100.0/24 is directly connected, port8
```

Which two statements are true about the routing entries in this database table? (Choose two.)

A. All of the entries in the routing database table are installed in the FortiGate routing table.

B. The port2 interface is marked as inactive.

C. Both default routes have different administrative distances.

D. The default route on port2 is marked as the standby route.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

by terminatoritsec at *Aug. 28, 2024, 1:48 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 10 DISCUSSION

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
All traffic must be routed through the primary tunnel when both tunnels are up. The secondary tunnel must be used only if the primary tunnel goes down. In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.
Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)

A. Enable Dead Peer Detection.

B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.

D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

Suggested Answer: *AC*

Community vote distribution

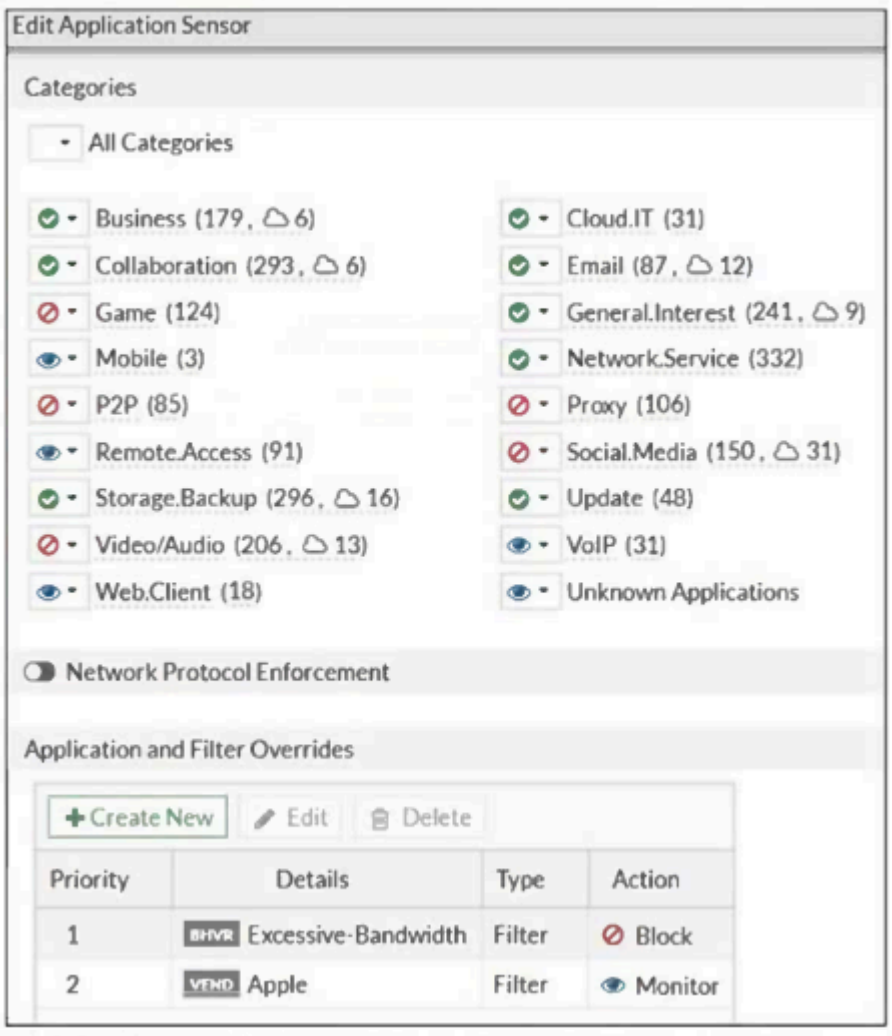
AC (100%)

by TIGERZ44 at *Sept. 1, 2024, 7:26 a.m.*

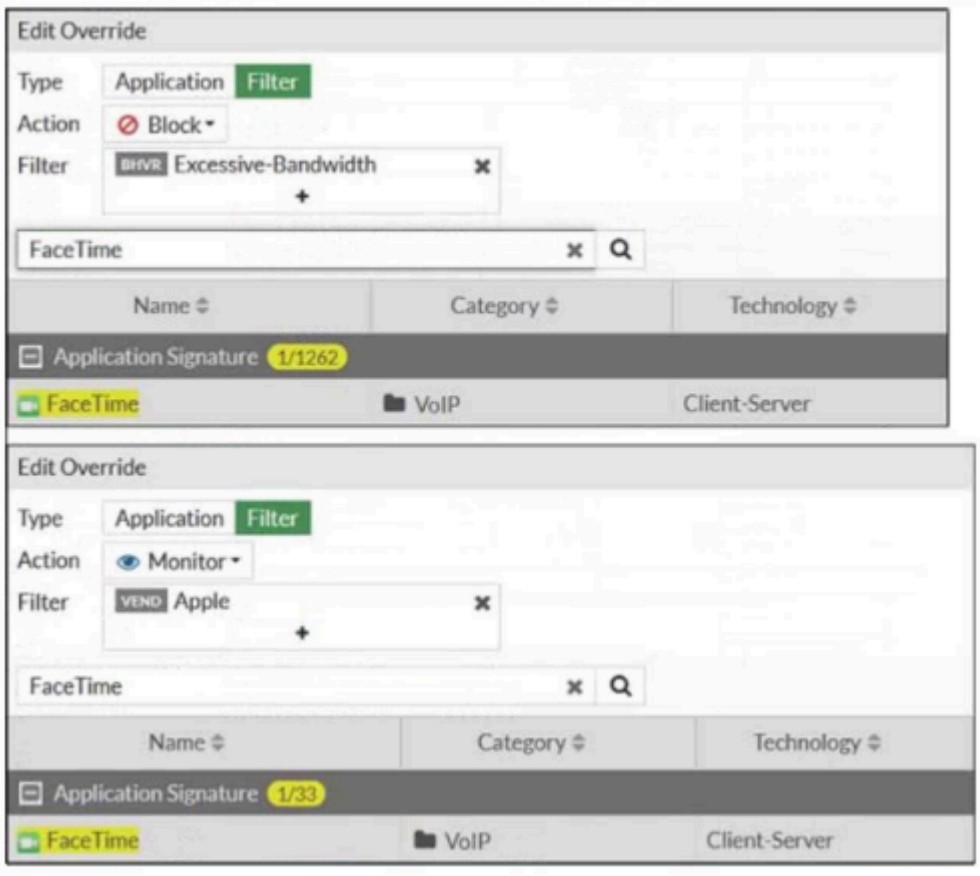
EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 11 DISCUSSION

Refer to the exhibits.

Application sensor configuration



Application and Filter override configuration



The exhibits show the application sensor configuration and the Excessive-Bandwidth and Apple filter details.

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

A. Apple FaceTime will be allowed, based on the Video/Audio category configuration.

B. Apple FaceTime will be allowed, based on the Apple filter configuration.

C. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

D. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.

Suggested Answer: *D*

Community vote distribution

D (82%)

B (18%)

by IBB90704 at *Sept. 5, 2024, 8:56 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 12 DISCUSSION

An employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

A. SSL VPN idle-timeout

B. SSL VPN login-timeout

C. SSL VPN dtls-hello-timeout

D. SSL VPN session-ttl

Suggested Answer: *C*

Community vote distribution

C (58%) B (42%)

by bob511 at *Sept. 2, 2024, 8:31 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 13 DISCUSSION

When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate.
Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

A. Allow & Warning

B. Trust & Allow

C. Allow

D. Block & Warning

E. Block

Suggested Answer: *BCE*

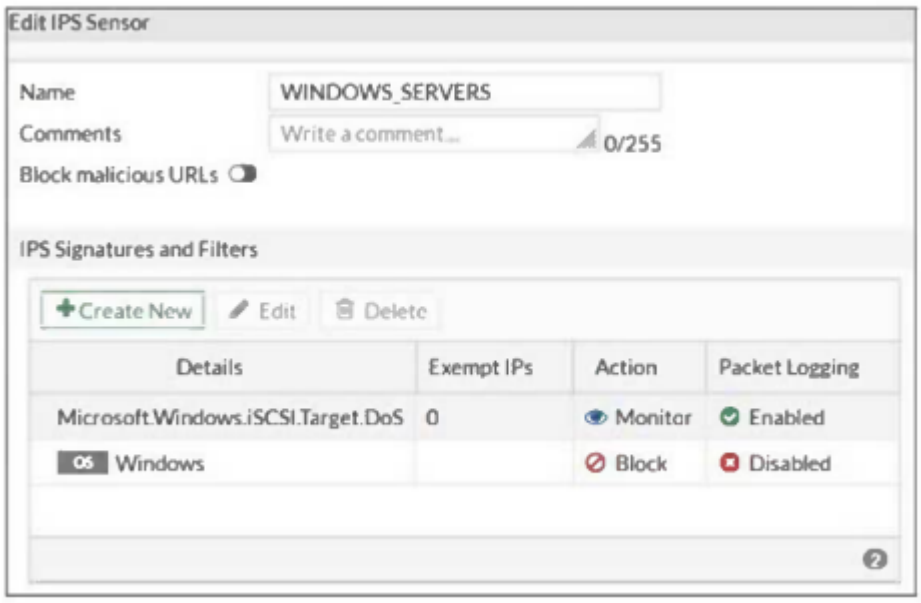
Community vote distribution

BCE (80%) ABE (20%)

by andres8h at *Aug. 30, 2024, 10:44 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 14 DISCUSSION

Refer to the exhibit, which shows the IPS sensor configuration.



If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will gather a packet log for all matched traffic.

B. The sensor will reset all connections that match these signatures.

C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.

D. The sensor will block all attacks aimed at Windows servers.

Suggested Answer: *CD*

Community vote distribution

CD (55%) AC (40%) 5%

by VirtuaTech at *Sept. 9, 2024, 7:39 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 15 DISCUSSION

Which statement is a characteristic of automation stitches?

A. They can be run only on devices in the Security Fabric.

B. They can be created only on downstream devices in the fabric.

C. They can have one or more triggers.

D. They can run multiple actions at the same time.

Suggested Answer: *D*

Community vote distribution

D (79%) C (21%)

by bob511 at *Sept. 1, 2024, 10:35 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 17 DISCUSSION

Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.

B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.

D. The client FortiGate requires a manually added route to remote subnets.

Suggested Answer: *AB*

Community vote distribution

AB (91%) 9%

by knoor at *Sept. 5, 2024, 7:39 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 18 DISCUSSION

Refer to the exhibit.

Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

Which statement about this firewall policy list is true?

A. The Implicit group can include more than one deny firewall policy.

B. The firewall policies are listed by ID sequence view.

C. The firewall policies are listed by ingress and egress interfaces pairing view.

D. LAN to WAN, WAN to LAN, and Implicit are sequence grouping view lists.

Suggested Answer: *D*

Community vote distribution

D (76%) C (24%)

by wsdeffwd at *Sept. 6, 2024, 5:16 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 19 DISCUSSION

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration

Based on the exhibit, which statement is true?

A. The underlay zone contains port1 and port2.

B. The d-wan zone contains no member.

C. The d-wan zone cannot be deleted.

D. The virtual-wan-link zone contains no member.

Suggested Answer: *B*

Community vote distribution

B (100%)

by Beatledrew at *Sept. 12, 2024, 4:46 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 2 DISCUSSION

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 host field in the HTTP header.

B. The server name indication (SNI) extension in the client hello message.

C. The subject alternative name (SAN) field in the server certificate.

D. The subject field in the server certificate.

E. The serial number in the server certificate.

Suggested Answer: *BCD*

Community vote distribution

BCD (100%)

by lenriquereyes at *Aug. 29, 2024, 10:27 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 20 DISCUSSION

Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.

B. The RPF check is run on the first reply packet of any new session.

C. The RPF check is run on the first sent and reply packet of any new session.

D. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

Suggested Answer: *AD*

Community vote distribution

AD (88%) 12%

by ShrekAlmighty at *Sept. 5, 2024, 6:56 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 21 DISCUSSION

Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three.)

A. Manual with load balancing

B. Lowest Cost (SLA) with load balancing

C. Best Quality with load balancing

D. Lowest Quality (SLA) with load balancing

E. Lowest Cost (SLA) without load balancing

Suggested Answer: *ABE*

Community vote distribution

ABE (69%) ABC (28%) 3%

by andres8h at *Aug. 30, 2024, 11 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 22 DISCUSSION

Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

A. Pre-shared key and certificate signature as authentication methods

B. Extended authentication (XAuth) to request the remote peer to provide a username and password

C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged

D. No certificate is required on the remote peer when you set the certificate signature as the authentication method

Suggested Answer: *AB*

Community vote distribution

AB (100%)

by ShrekAlmighty at *Sept. 5, 2024, 6:59 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 23 DISCUSSION

Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

A. Checksums of devices are compared against each other to ensure configurations are the same.

B. Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.

C. Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster.

D. Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

Suggested Answer: *AC*

Community vote distribution

AC (77%) AB (15%) 8%

by andres8h at *Aug. 31, 2024, 3:45 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 24 DISCUSSION

What are two features of the NGFW profile-based mode? (Choose two.)

A. NGFW profile-based mode can only be applied globally and not on individual VDOMs.

B. NGFW profile-based mode must require the use of central source NAT policy.

C. NGFW profile-based mode policies support both flow inspection and proxy inspection.

D. NGFW profile-based mode supports applying applications and web filtering profiles in a firewall policy.

Suggested Answer: *CD*

Community vote distribution

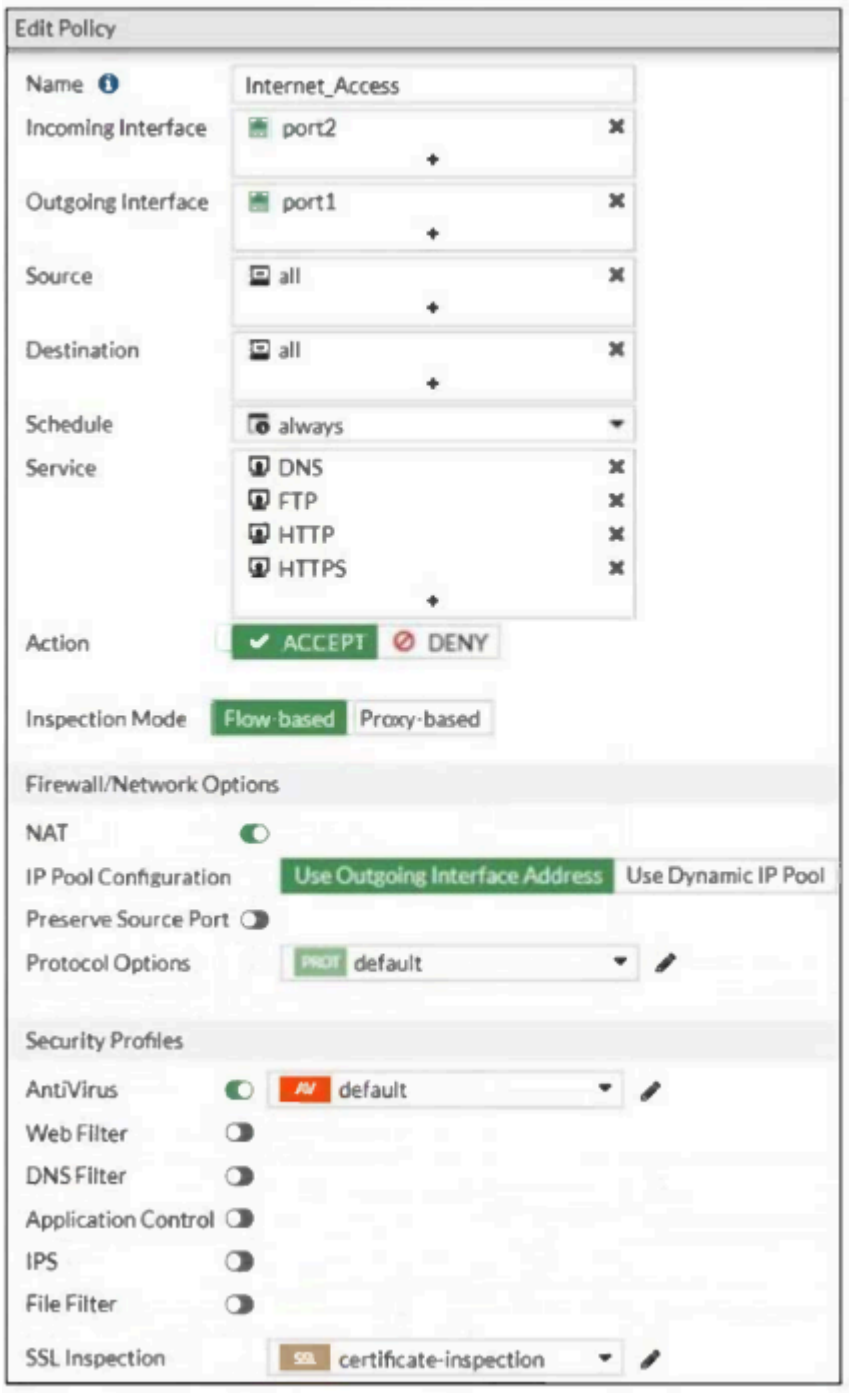
CD (100%)

by Beatledrew at *Sept. 12, 2024, 5:02 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 25 DISCUSSION

Refer to the exhibit to view the firewall policy.

Firewall policy configuration



Why would the firewall policy not block a well-known virus, for example eicar?

A. The action on the firewall policy is not set to deny.

B. The firewall policy is not configured in proxy-based inspection mode.

C. Web filter is not enabled on the firewall policy to complement the antivirus profile.

D. The firewall policy does not apply deep content inspection.

Suggested Answer: *D*

Community vote distribution

D (100%)

by Beatledrew at *Sept. 13, 2024, 3:35 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 26 DISCUSSION

Which inspection mode does FortiGate use for application profiles if it is configured as a profile-based next-generation firewall (NGFW)?

A. Full content inspection

B. Proxy-based inspection

C. Certificate inspection

D. Flow-based inspection

Suggested Answer: *D*

Community vote distribution

D (100%)

by andres8h at *Aug. 31, 2024, 4:36 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 27 DISCUSSION

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 Updated Time
173.243.141.16      -8   18    DI  0                    4          0          0 Thu Jun  9 11:26:24 2022
12.34.97.18         20   30        1                    1          0          0 Thu Jun  9 11:26:24 2022
210.7.96.18        160  305        9                    0          0          0 Thu Jun  9 11:26:24 2022
```

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

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

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

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

D. FortiGate is using default FortiGuard communication settings.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

by fab1ccb at *Sept. 14, 2024, 3:54 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 28 DISCUSSION

Refer to the exhibit.

```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637
->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-00025d45, tun_id=0.0.0.
0"
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw-10.200.1.254
via port1"
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (policy 0)"
```

Why did FortiGate drop the packet?

A. It 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.

Suggested Answer: *D*

Community vote distribution

D (100%)

by fab1ccb at *Sept. 14, 2024, 3:57 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 29 DISCUSSION

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?

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

by fab1ccb at *Sept. 14, 2024, 4:12 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 3 DISCUSSION

Refer to the exhibit.

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Critical-DIA	LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 ✓ port2
2	Non-Critical-DIA	LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2 ✓
3	Default-Internet	LOCAL_SUBNET	REMOTE_SUBNET	Latency	port1 port2
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

A. All traffic from a source IP to a destination IP is sent to the same interface.

B. Traffic is sent to the link with the lowest latency.

C. Traffic is distributed based on the number of sessions through each interface.

D. All traffic from a source IP is sent to the same interface

Suggested Answer: *A*

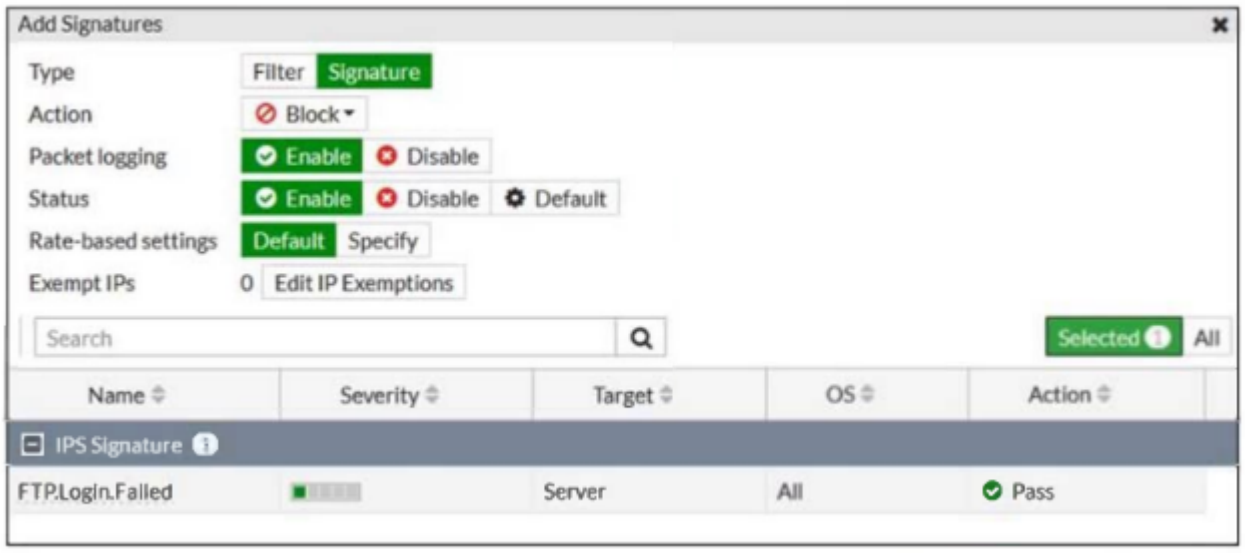
Community vote distribution

A (100%)

by gimy19 at *Aug. 29, 2024, 7:16 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 30 DISCUSSION

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?

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

by GopiChandMurari at *Sept. 13, 2024, 10:28 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 31 DISCUSSION

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?

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

Suggested Answer: *D*

Community vote distribution

D (100%)

by wsdeffwd at *Sept. 10, 2024, 1:21 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 32 DISCUSSION

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?

A. Log ID

B. Policy ID

C. Sequence ID

D. Universally Unique Identifier

Suggested Answer: *D*

Community vote distribution

D (100%)

by andres8h at *Aug. 31, 2024, 3:42 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 33 DISCUSSION

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?

A. RADIUS server

B. DHCP server

C. Windows server

D. LDAP server

Suggested Answer: *D*

Community vote distribution

D (100%)

by DavidCA2024 at *Sept. 22, 2024, 11:21 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 34 DISCUSSION

An administrator manages a FortiGate model that supports NTurbo.
How does NTurbo enhance performance for flow-based inspection?

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.

Suggested Answer: *D*

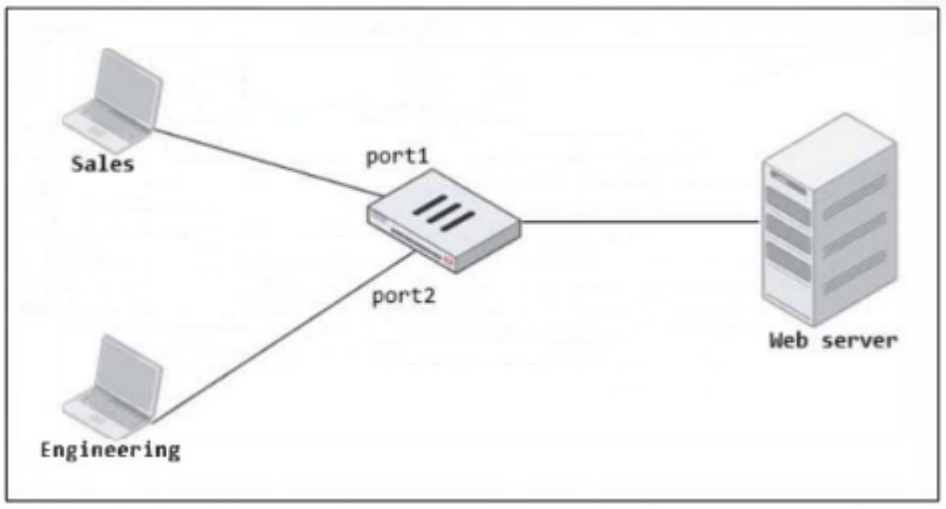
Community vote distribution

D (84%) A (16%)

by andres8h at *Aug. 31, 2024, 3:45 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 35 DISCUSSION

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?

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.

Suggested Answer: *A*

Community vote distribution

A (100%)

by andres8h at *Aug. 31, 2024, 4:15 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 36 DISCUSSION

Refer to the exhibit, which shows a partial configuration from the remote authentication server.

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	

Why does the FortiGate administrator need this configuration?

A. To authenticate only the Training user group.

B. To set up a RADIUS server Secret.

C. To authenticate and match the Training OU on the RADIUS server.

D. To authenticate Any FortiGate user groups.

Suggested Answer: *A*

Community vote distribution

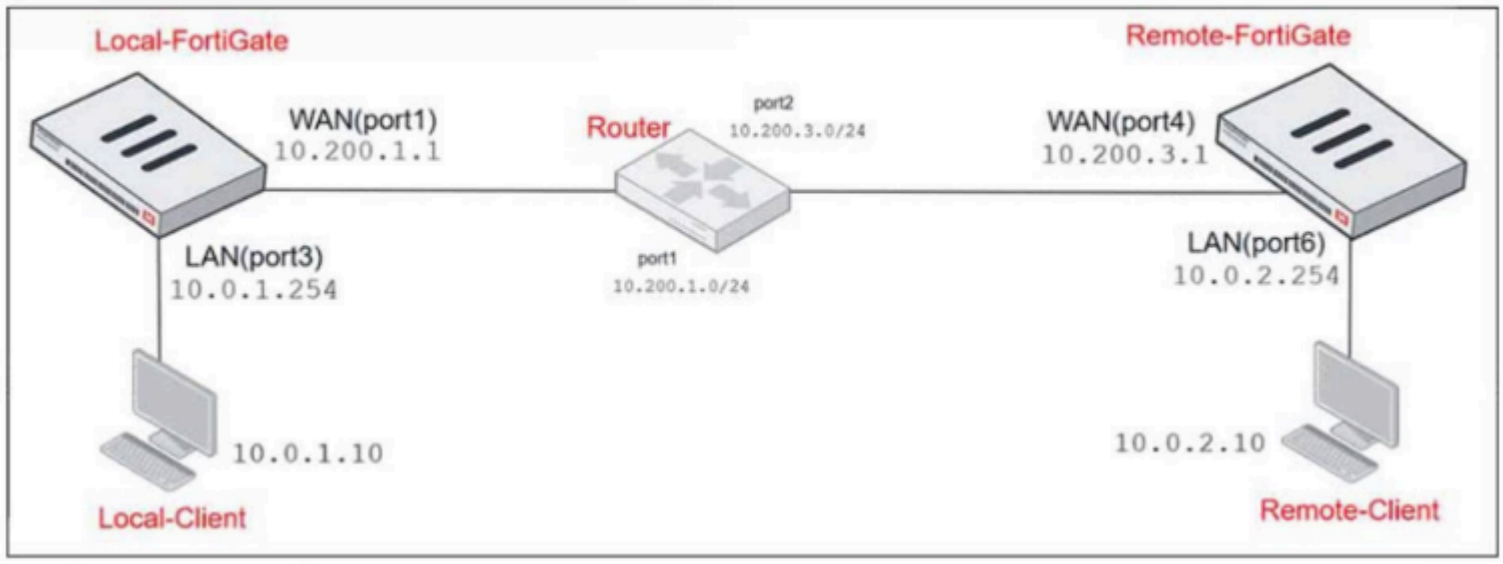
A (100%)

by knoor at *Sept. 5, 2024, 11:07 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 37 DISCUSSION

Refer to the exhibits.

Network diagram



NAT IP pool configuration

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

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port3) → WAN (port1)								
2	TCP traffic	all	REMOTE_FORTIGATE	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
6	PING traffic	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
7	IGMP traffic	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.
The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IPaddress 10.0.1.254/24.
Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

A. 10.200.1.1

B. 10.200.1.149

C. 10.200.1.99

D. 10.200.1.49

Suggested Answer: *C*

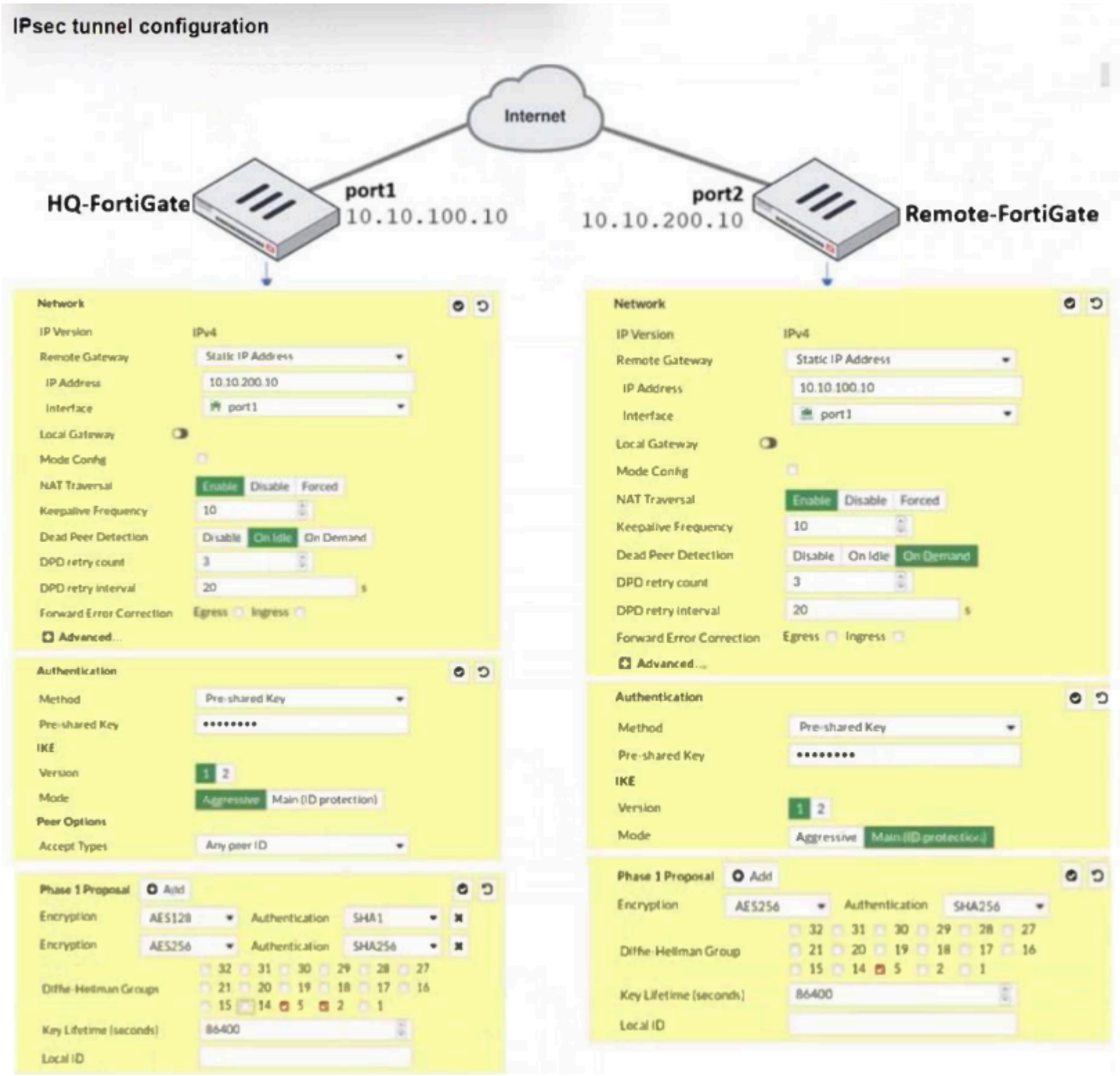
Community vote distribution

C (100%)

by Veritas007 at *Aug. 29, 2024, 11:16 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 38 DISCUSSION

Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 failed to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.

Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes can the administrator make to bring phase 1 up? (Choose two.)

A. On HQ-FortiGate, disable Diffie-Helman group 2.

B. On Remote-FortiGate, set port2 as Interface.

C. On both FortiGate devices, set Dead Peer Detection to On Demand.

D. On HQ-FortiGate, set IKE mode to Main (ID protection).

Suggested Answer: *BD*

Community vote distribution

BD (100%)

by ShrekAlmighty at *Sept. 5, 2024, 12:43 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 39 DISCUSSION

A network administrator has configured an SSL/SSH inspection profile defined for full SSL inspection and set with a private CA certificate. The firewall policy that allows the traffic uses this profile for SSL inspection and performs web filtering. When visiting any HTTPS websites, the browser reports certificate warning errors.
What is the reason for the certificate warning errors?

A. The SSL cipher compliance option is not enabled on the SSL inspection profile. This setting is required when the SSL inspection profile is defined with a private CA certificate.

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

C. The browser does not recognize the certificate in use as signed by a trusted CA.

D. With full SSL inspection it is not possible to avoid certificate warning errors at the browser level.

Suggested Answer: *C*

Community vote distribution

C (100%)

by wsdeffwd at *Sept. 6, 2024, 8:43 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 4 DISCUSSION

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad.
Which IPsec Wizard template must the administrator apply?

A. Remote Access

B. Site to Site

C. Dial up User

D. Hub-and-Spoke

Suggested Answer: *A*

Community vote distribution

A (92%) 8%

by andres8h at *Aug. 30, 2024, 7:53 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 40 DISCUSSION

Refer to the exhibit.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port3 → port1									
1	Full_Access	Remote-users LOCAL_SUB...	all	always	HTTP HTTPS ALL_ICMP	ACCEPT	NAT	Standard	WEB Category_Monitor SSL certificate-inspection

FortiGate is configured for firewall authentication. When attempting to access an external website, 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 user is using an incorrect user name.

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

D. No matching user account exists for this user.

Suggested Answer: *A*

Community vote distribution

A (96%) 4%

by bob511 at *Sept. 2, 2024, 1:25 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 41 DISCUSSION

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

A. WinSecLog

B. WMI

C. NetAPI

D. FSSO REST API

E. FortiGate polling

Suggested Answer: *ABC*

Community vote distribution

ABC (100%)

by terminatoritsec at *Aug. 28, 2024, 2:03 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 42 DISCUSSION

Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

A. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.

B. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.

C. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP

D. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

by andres8h at *Aug. 31, 2024, 4:35 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 43 DISCUSSION

What are two features of collector agent advanced mode? (Choose two.)

A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.

B. Advanced mode supports nested or inherited groups.

C. In advanced mode, security profiles can be applied only to user groups, not individual users.

D. Advanced mode uses the Windows convention —NetBios: Domain\Username.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

by bob511 at *Sept. 2, 2024, 1:40 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 44 DISCUSSION

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.
What is true about the DNS connection to a FortiGuard server?

A. It uses UDP 8888.

B. It uses DNS over HTTPS.

C. It uses DNS over TLS.

D. It uses UDP 53.

Suggested Answer: *C*

Community vote distribution

C (100%)

by bob511 at *Sept. 2, 2024, 1:48 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 45 DISCUSSION

Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

A. The intrusion prevention security profile must be enabled when using flow-based inspection mode.

B. The option to send files to FortiSandbox for inspection is enabled.

C. The firewall policy performs a full content inspection on the file.

D. Flow-based inspection is used, which resets the last packet to the user.

Suggested Answer: *D*

Community vote distribution

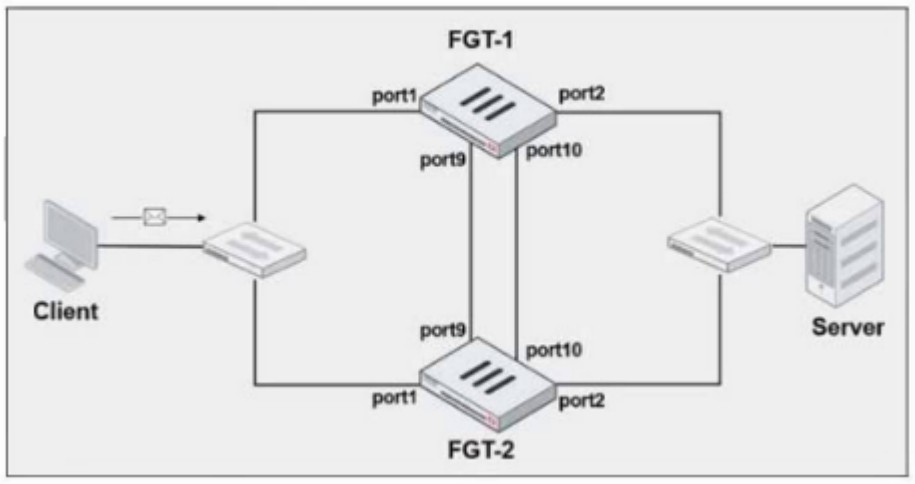
D (100%)

by TIGERZ44 at *Sept. 1, 2024, 4:02 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 46 DISCUSSION

Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

```
# get system ha status
...
Configuration Status:
    FGVM010000064692(updated 4 seconds ago): in-sync
    FGVM010000064692 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
    FGVM010000065036(updated 4 seconds ago): in-sync
    FGVM010000065036 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary     : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary   : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

New FortiGate HA configuration

```
FGT-1
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override disable
    set priority 90
    set monitor port3

FGT-2
#config system ha
    set group-id 3
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port9" 50 "port10" 50
    set session-pickup enable
    set override enable
    set priority 110
    set monitor port3
```

FGT-1 and FGT-2 are updated with HA configuration commands shown in the exhibit.

What would be the expected outcome in the HA cluster?

A. FGT-1 will remain the primary because FGT-2 has lower priority.

B. FGT-2 will take over as the primary because it has the override enable setting and higher priority than FGT-1.

C. FGT-1 will synchronize the override disable setting with FGT-2.

D. The HA cluster will become out of sync because the override setting must match on all HA members.

Suggested Answer: *B*

Community vote distribution

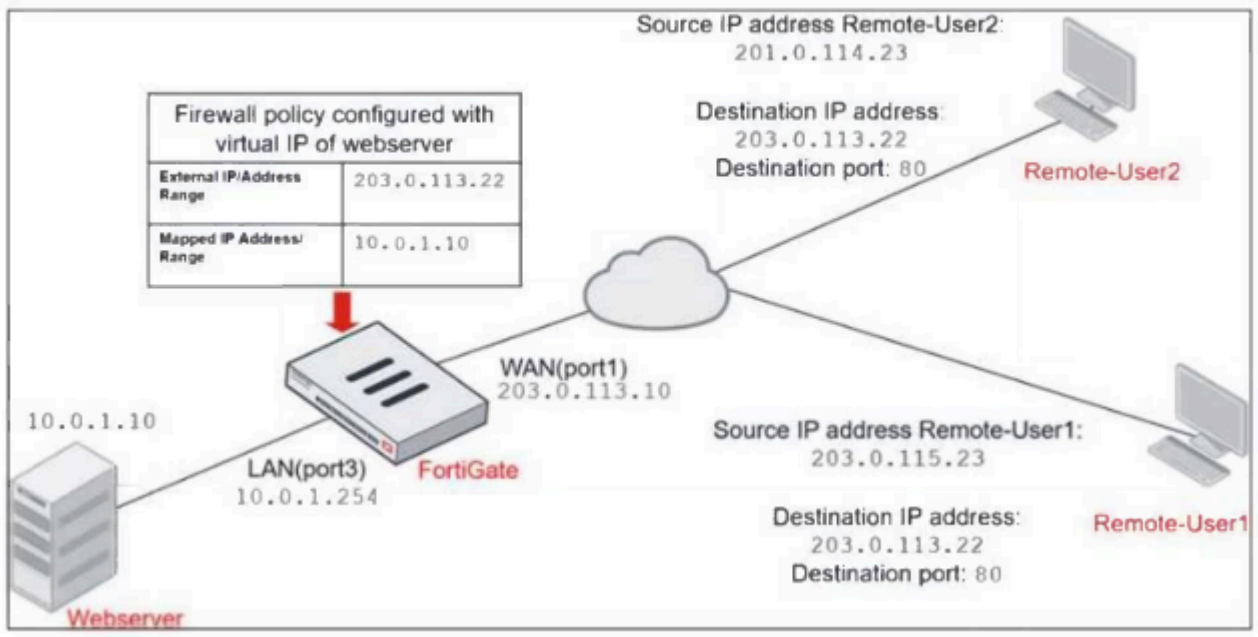
B (100%)

by Beatledrew at *Sept. 24, 2024, 12:35 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 47 DISCUSSION

Refer to the exhibits.

Network diagram



Firewall address object

Firewall policies

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

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.

The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.

Which two configuration changes can the administrator make to the policy to deny Webserver access for Remote-User2? (Choose two.)

A. Enable match-vip in the Deny policy.

B. Set the Destination address as Webserver in the Deny policy.

C. Disable match-vip in the Deny policy.

D. Set the Destination address as Deny_IP in the Allow_access policy.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

by 3101a6a at *Sept. 26, 2024, 4:53 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 48 DISCUSSION

Which two statements explain antivirus scanning modes? (Choose two.)

A. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

B. In flow-based inspection mode files bigger than the buffer size are scanned

C. In proxy-based inspection mode files bigger than the buffer size are scanned

D. In proxy-based inspection mode antivirus scanning buffers the whole file for scanning, before sending it to the client

Suggested Answer: *AD*

Community vote distribution

AD (100%)

by CharlieS8 at *Oct. 25, 2024, 4:46 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 5 DISCUSSION

Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.

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
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

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

A. FortiGate will start sending all files to FortiSandbox for inspection.

B. FortiGate has entered conserve mode.

C. Administrators cannot change the configuration.

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

Suggested Answer: *BC*

Community vote distribution

BC (100%)

by Qwerty379 at *Aug. 28, 2024, 11:27 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 50 DISCUSSION

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

A. Internet Service Database (ISDB) engine

B. Intrusion prevention system engine

C. Antivirus engine

D. Application control engine

Suggested Answer: *B*

Community vote distribution

B (100%)

by CharlieS8 at *Oct. 25, 2024, 4:48 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 51 DISCUSSION

A FortiGate administrator is required to reduce the attack surface on the SSL VPN portal.

Which SSL timer can you use to mitigate a denial of service (DoS) attack?

A. SSL VPN dtls-hello-timeout

B. SSL VPN http-request-header-timeout

C. SSL VPN login-timeout

D. SSL VPN idle-timeout

Suggested Answer: *B*

Community vote distribution

B (100%)

by sekanjiGuru at *Oct. 26, 2024, 12:26 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 52 DISCUSSION

A FortiGate firewall policy is configured with active authentication however, the user cannot authenticate when accessing a website.

Which protocol must FortiGate allow even though the user cannot authenticate?

A. ICMP

B. DNS

C. DHCP

D. LDAP

Suggested Answer: *B*

Community vote distribution

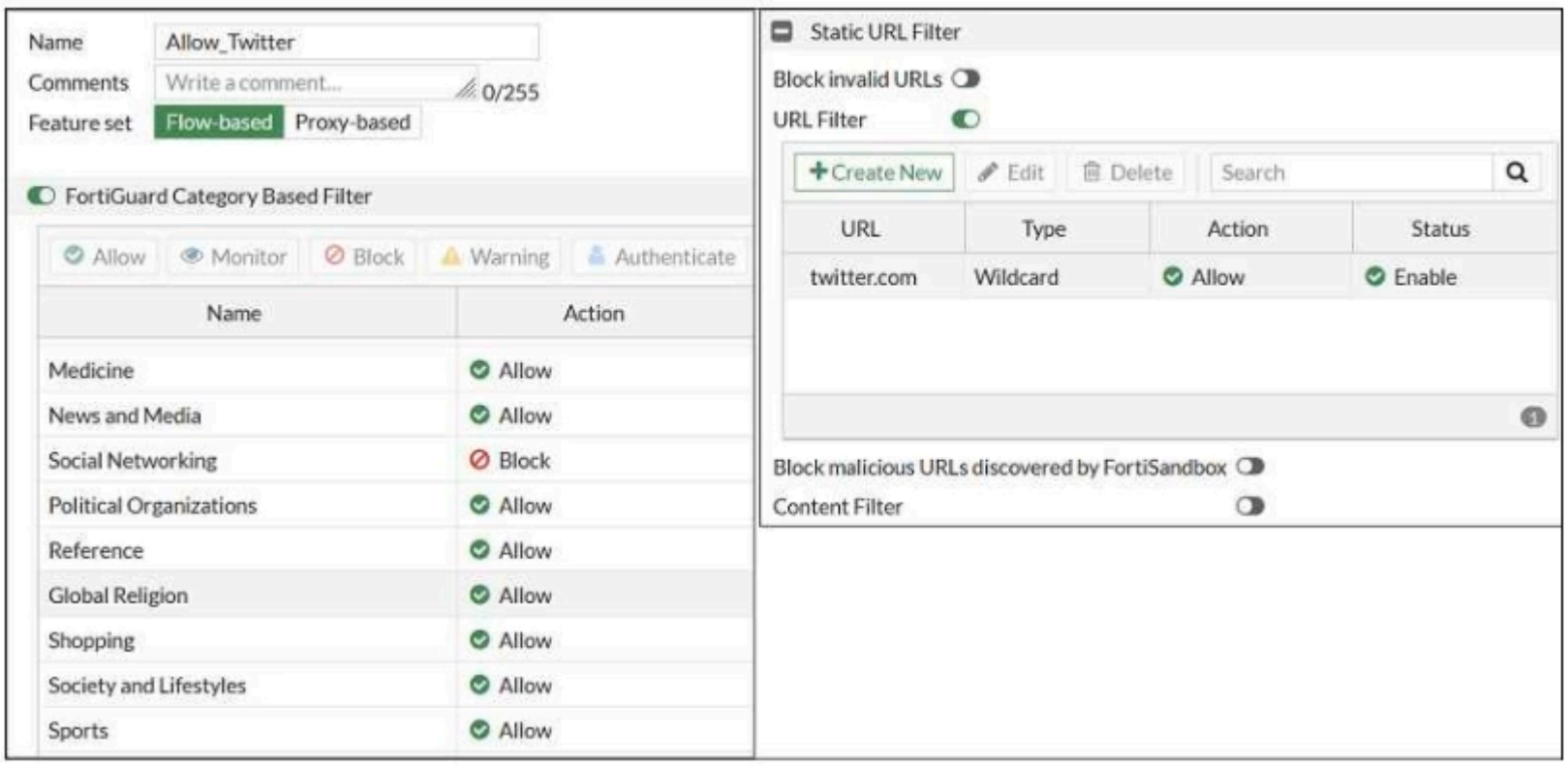
B (100%)

by CharlieS8 at *Oct. 29, 2024, 11:56 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 53 DISCUSSION

Refer to exhibit.

FortiGate web filter profile configuration



An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

A. On the Static URL Filter configuration set Type to Simple

B. On the FortiGuard Category Based Filter configuration set Action to Warning for Social Networking

C. On the Static URL Filter configuration set Action to Monitor

D. On the Static URL Filter configuration set Action to Exempt

Suggested Answer: *D*

Community vote distribution

D (100%)

by fa7474b at *Oct. 29, 2024, 10:58 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 54 DISCUSSION

There are multiple dial-up IPsec VPNs configured in aggressive mode on the HQ FortiGate. The requirement is to connect dial-up users to their respective department VPN tunnels.

Which phase 1 setting you can configure to match the user to the tunnel?

A. Peer ID

B. Local Gateway

C. Dead Peer Detection

D. IKE Mode Config

Suggested Answer: *A*

Community vote distribution

A (100%)

by CharlieS8 at *Oct. 25, 2024, 4:53 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 55 DISCUSSION

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. execute ping

B. execute traceroute

C. diagnose sys top

D. get system arp

E. diagnose sniffer packet any

Suggested Answer: *ABE*

Community vote distribution

ABE (100%)

by CharlieS8 at *Oct. 25, 2024, 2:07 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 56 DISCUSSION

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 outbound traffic but no response from the peer.

Which DPD mode on FortiGate meets this requirement?

A. On Demand

B. On Idle

C. Disabled

D. Enabled

Suggested Answer: *A*

Community vote distribution

A (100%)

by CharlieS8 at *Oct. 25, 2024, 2:10 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 57 DISCUSSION

Which two statements are correct when FortiGate enters conserve mode? (Choose two.)

A. FortiGate halts complete system operation and requires a reboot to regain available resources

B. FortiGate refuses to accept configuration changes

C. FortiGate continues to run critical security actions, such as quarantine.

D. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled

Suggested Answer: *BD*

Community vote distribution

BD (100%)

by 066c9f3 at *Oct. 28, 2024, 4:31 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 58 DISCUSSION

Which statement is correct regarding the use of application control for inspecting web applications?

A. Application control can identify child and parent applications, and perform different actions on them

B. Application control signatures are included in Fortinet Antivirus engine

C. Application control does not display a replacement message for a blocked web application

D. Application control does not require SSL Inspection to Identify web applications

Suggested Answer: *A*

Community vote distribution

A (100%)

by CharlieS8 at *Oct. 25, 2024, 4:56 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 59 DISCUSSION

What are three key routing principles in SD-WAN? (Choose three.)

A. By default, SD-WAN members are skipped if they do not have a valid route to the destination

B. By default, SD-WAN rules are skipped if only one route to the destination is available

C. By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member

D. SD-WAN rules have precedence over any other type of routes

E. Regular policy routes have precedence over SD-WAN rules

Suggested Answer: *ACE*

Community vote distribution

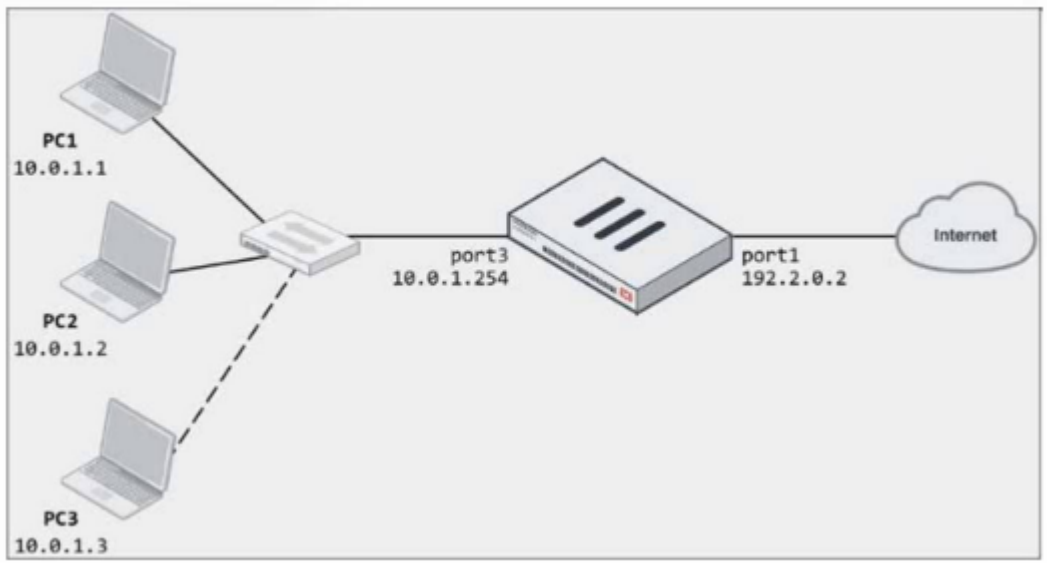
ACE (100%)

by CharlieS8 at *Oct. 25, 2024, 4:59 a.m.*

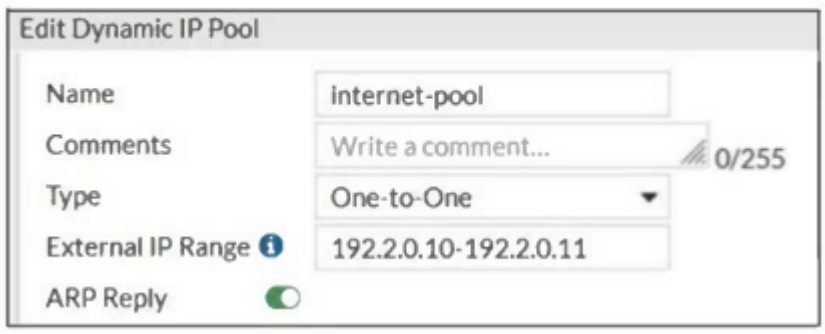
EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 6 DISCUSSION

Refer to the exhibits.

Network diagram



Dynamic IP pool



Firewall policy

The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device.

Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.

Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field.

B. In the IP pool configuration, set endip to 192.2.0.12.

C. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.

D. In the IP pool configuration, set type to overload.

Suggested Answer: *BD*

Community vote distribution

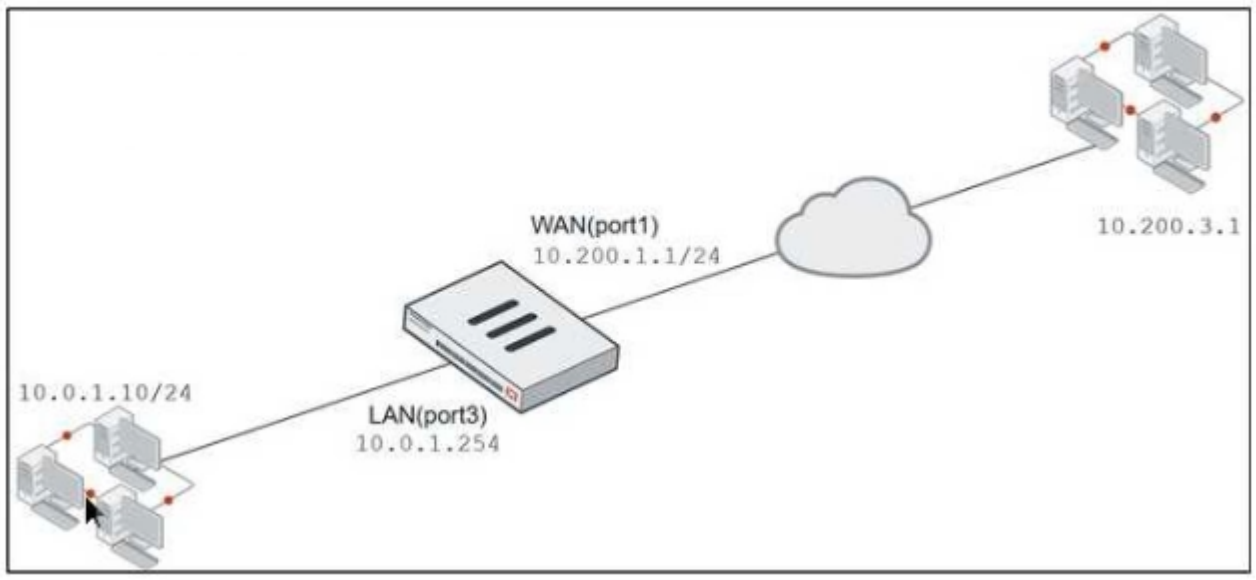
BD (100%)

by Qwerty379 at *Aug. 29, 2024, 4:58 a.m.*

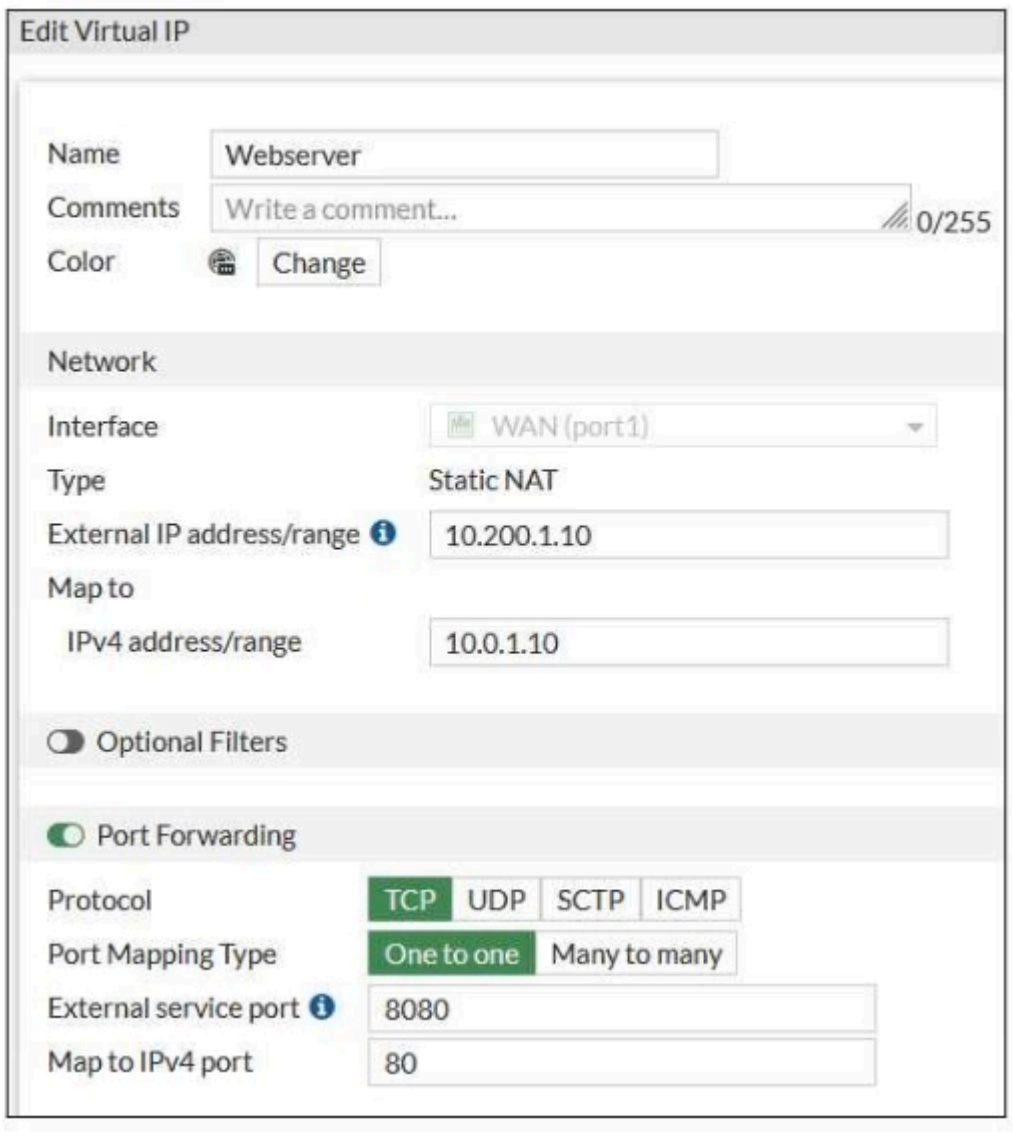
EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 60 DISCUSSION

Refer to the exhibits, which show a diagram of a FortiGate device connected to the network. VIP object configuration, and the firewall policy configuration.

Network diagram



VIP object configuration



Firewall policy configuration

Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
Internet_Access	LAN (port3)	WAN (port1)	all	all	always	ALL	ACCEPT		NAT
Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	HTTPS	ACCEPT		Disabled

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.

If the host 10.200.3.1 sends a TCP SYN packet on port 8080 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be at the time FortiGate forwards the packet to the destination?

A. 10.0.1.254, 10.200.1.10, and 8080, respectively

B. 10.0.1.254, 10.0.1.10, and 80, respectively

C. 10.200.3.1, 10.0.1.10, and 80, respectively

D. 10.200.3.1, 10.0.1.10, and 8080, respectively

Suggested Answer: *C*

Community vote distribution

C (64%) D (27%) 9%

by CharlieS8 at *Oct. 25, 2024, 4:59 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 61 DISCUSSION

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL inspection? (Choose two.)

A. The issuer must be a public CA

B. The CA extension must be set to TRUE

C. The Authority Key Identifier must be of type SSL

D. The keyUsage extension must be set to keyCertSign

Suggested Answer: *BD*

Community vote distribution

BD (100%)

by CharlieS8 at *Oct. 25, 2024, 5 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 62 DISCUSSION

Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

What two conclusions can you make from the debug flow output? (Choose two.)

A. The debug flow is for ICMP traffic.

B. A firewall policy allowed the connection.

C. A new traffic session was created.

D. The default route is required to receive a reply.

Suggested Answer: *AC*

Community vote distribution

AC (100%)

by CharlieS8 at *Oct. 25, 2024, 5:01 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 63 DISCUSSION

Which three statements explain a flow-based antivirus profile? (Choose three.)

A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.

B. Flow-based inspection optimizes performance compared to proxy-based inspection.

C. FortiGate buffers the whole file but transmits to the client at the same time.

D. If a virus is detected, the last packet is delivered to the client.

E. The IPS engine handles the process as a standalone.

Suggested Answer: *ABC*

Community vote distribution

ABC (100%)

by CharlieS8 at *Oct. 25, 2024, 5:02 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 64 DISCUSSION

Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP is not used when FortiGate is in transparent mode

B. FGCP elects the primary FortiGate device

C. FGCP is used to discover FortiGate devices in different HA groups

D. FGCP runs only over the heartbeat links

Suggested Answer: *BD*

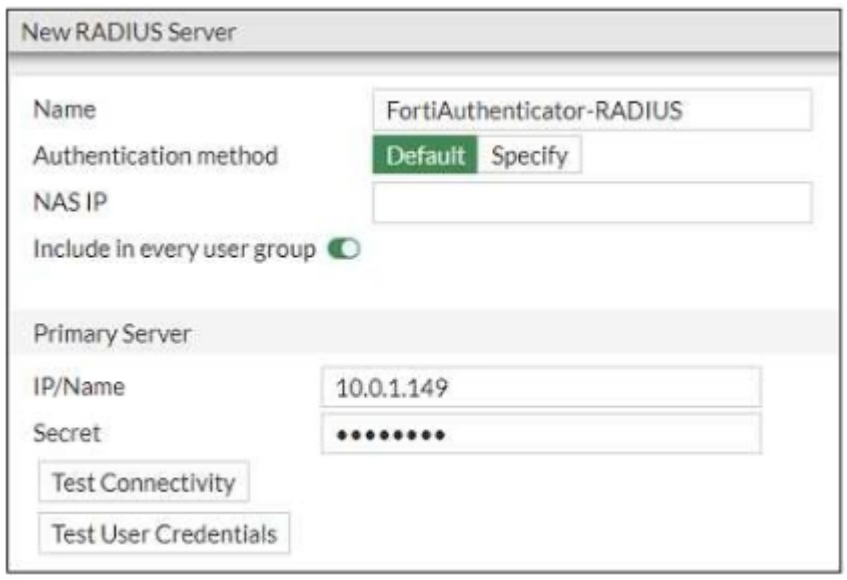
Community vote distribution

BD (100%)

by CharlieS8 at *Oct. 25, 2024, 5:02 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 65 DISCUSSION

Refer to the exhibit which contains a RADIUS server configuration.



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

What is the impact of using the 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 users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate

C. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case is FortiAuthenticator

D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group

Suggested Answer: *A*

Community vote distribution

A (100%)

by CharlieS8 at *Oct. 25, 2024, 5:03 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 66 DISCUSSION

Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

A. Downstream devices can connect to the upstream device from any of their VDOMs

B. Each VDOM in the environment can be part of a different Security Fabric

C. VDOMs without ports with connected devices are not displayed in the topology

D. Security rating reports can be run individually for each configured VDOM

Suggested Answer: *C*

Community vote distribution

C (82%) Other

by CharlieS8 at *Oct. 25, 2024, 5:04 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 67 DISCUSSION

Refer to the exhibit.

SD-WAN traffic log

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
YouTube	✓ Accept (8.08 kB / 27...	1 (DIA)	port2		
YouTube	✓ Accept (UTM Allowed)	1 (DIA)	port2		
Facebook	✓ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✓ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✓ Accept (3.33 kB / 10...	1 (DIA)	port1		
YouTube	✓ Accept (44.63 kB / 3....	1 (DIA)	port2		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port1		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port2		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port2		

The administrator configured SD-WAN rules and set the FortiGate traffic log page to display SD-WAN-specific columns: SD-WAN Quality and SD-WAN Rule Name.

FortiGate allows the traffic according to policy ID 1. This is the policy that allows SD-WAN traffic.

Despite these settings the traffic logs do not show the name of the SD-WAN rule used to steer those traffic flows.

What can be the reason?

A. FortiGate load balanced the traffic according to the implicit SD-WAN rule.

B. There is no application control profile applied to the firewall policy.

C. Destination in the SD-WAN rules are configured per application but the feature visibility is not enabled.

D. SD-WAN rule names do not appear immediately. The administrator needs to refresh the page.

Suggested Answer: *A*

Community vote distribution

A (100%)

by CharlieS8 at *Oct. 28, 2024, 8:59 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 68 DISCUSSION

FortiGuard categories can be overridden and defined in different categories. To create a web rating override for the example.com home page the override must be configured using a specific syntax.

Which two syntaxes are correct to configure a web rating override for the home page? (Choose two.)

A. www.example.com:443

B. www.example.com

C. www.example.com/index.hrml

D. example.com

Suggested Answer: *BD*

Community vote distribution

BD (100%)

by CharlieS8 at *Oct. 25, 2024, 5:06 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 69 DISCUSSION

An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

A. Denied users are blocked for 30 minutes.

B. A session for denied traffic is created.

C. The number of logs generated by denied traffic is reduced.

D. Device detection on all interfaces is enforced for 30 minutes.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

by CharlieS8 at *Oct. 25, 2024, 5:06 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 7 DISCUSSION

Which method allows management access to the FortiGate CLI without network connectivity?

A. CLI console widget

B. Serial console

C. Telnet console

D. SSH console

Suggested Answer: *B*

Community vote distribution

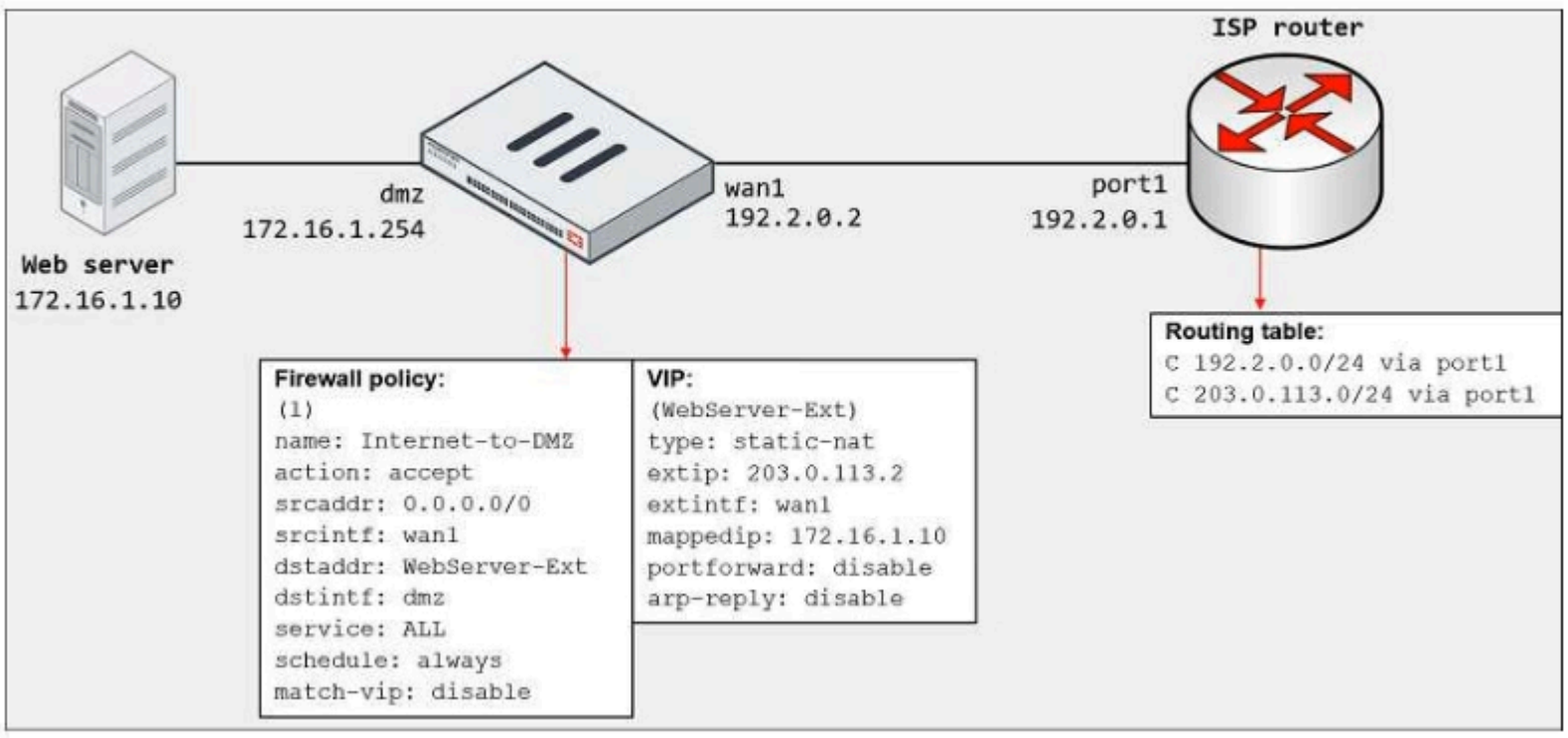
B (100%)

by Qwerty379 at *Aug. 29, 2024, 4:56 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 70 DISCUSSION

Refer to the exhibit.

FortiGate Firewall policy and VIP configuration



The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.

When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.

Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

A. Configure a loopback interface with address 203.0.113.2/32.

B. In the VIP configuration, enable arp-reply.

C. In the firewall policy configuration, enable match-vip.

D. Enable port forwarding on the server to map the external service port to the internal service port.

Suggested Answer: *B*

Community vote distribution

B (100%)

by CharlieS8 at *Oct. 25, 2024, 5:07 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 71 DISCUSSION

An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSUTLS connection.

Which FortiGate configuration can achieve this goal?

A. SSL VPN quick connection

B. SSL VPN tunnel

C. SSL VPN bookmark

D. Zero trust network access

Suggested Answer: *B*

Community vote distribution

B (100%)

by CharlieS8 at *Oct. 25, 2024, 5:08 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 72 DISCUSSION

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

A. An SD-WAN zone can contain physical and logical interfaces

B. You can use an SD-WAN zone in static route definitions

C. You can define up to three SD-WAN zones per FortiGate device

D. An SD-WAN zone must contains at least two members

E. An SD-WAN zone is a logical grouping of members

Suggested Answer: *ABE*

Community vote distribution

ABE (100%)

by CharlieS8 at *Oct. 30, 2024, 12:04 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 73 DISCUSSION

An administrator has configured a strict RPF check on FortiGate.

How does strict RPF check work?

A. Strict RPF checks the best route back to the source using the incoming interface.

B. Strict RPF allows packets back to sources with all active routes.

C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.

D. Strict RPF check is run on the first sent and reply packet of any new session.

Suggested Answer: *A*

Community vote distribution

A (86%) 14%

by CharlieS8 at *Oct. 25, 2024, 5:08 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 74 DISCUSSION

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

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

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

D. The matching firewall policy is set to proxy inspection mode

Suggested Answer: *B*

Community vote distribution

B (100%)

by CharlieS8 at *Oct. 25, 2024, 5:09 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 75 DISCUSSION

Refer to the exhibit.

Profile Name
Monitoring_Access
NOC_Access
prof_admin
super_admin

The NOC team connects to the FortiGate GUI with the NOC_Access admin profile. They request that their GUI sessions do not disconnect too early during inactivity.

What must the administrator configure to answer this specific request from the NOC team?

A. Enable the parameter Never Timeout in the admin profiles

B. Increase the admintimeout value under config system accprofile super_admin.

C. Increase the admintimeout value under config system global

D. Increase the offline value of the Override idle Timeout parameter in the NOC_Access admin profile

Suggested Answer: *D*

Community vote distribution

D (100%)

by CharlieS8 at *Oct. 28, 2024, 9:02 p.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 76 DISCUSSION

A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy.

When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the and does not block the file allowing it to be downloaded.

The administrator confirms that the traffic matches the configured firewall policy.

What are two reasons for the failed virus detection by FortiGate? (Choose two.)

A. The selected SSL inspection profile has certificate inspection enabled

B. The browser does not trust the FortiGate self-signed CA certificate

C. The EICAR test file exceeds the protocol options oversize limit

D. The website is exempted from SSL inspection

Suggested Answer: *AD*

Community vote distribution

AD (100%)

by CharlieS8 at *Oct. 25, 2024, 5:11 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 77 DISCUSSION

Refer to the exhibit.

IPS diagnostic output

```
# 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
6: Submit attack characteristics now
10: IPS queue length
11: Clear IPS queue length
12: IPS L7 socket statistics
13: IPS session list
14: IPS NTurbo statistics
15: IPSA statistics
...
97: Start all IPS engines
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command shown in the exhibit.

If option 5 is used with the IPS diagnostic command and the outcome is a decrease in the CPU usage, what is the correct conclusion?

A. The IPS engine is blocking all traffic.

B. The IPS engine is inspecting a high volume of traffic.

C. The IPS engine is unable to prevent an intrusion attack.

D. The IPS engine will continue to run in a normal state.

Suggested Answer: *B*

Community vote distribution

B (100%)

by CharlieS8 at *Oct. 25, 2024, 5:11 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 78 DISCUSSION

How can you disable RPF checking?

A. Disable src-check on the interface level settings

B. Unset fail-alert-interfaces on the interface level settings.

C. Disable fail-detect on the interface level settings.

D. Disable strict-src-check under system settings.

Suggested Answer: *A*

Community vote distribution

A (100%)

by CharlieS8 at *Oct. 25, 2024, 5:12 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 79 DISCUSSION

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. 192.168.3.0/24

B. 192.168.0.0/8

C. 192.168.2.0/24

D. 192.168.1.0/24

Suggested Answer: *C*

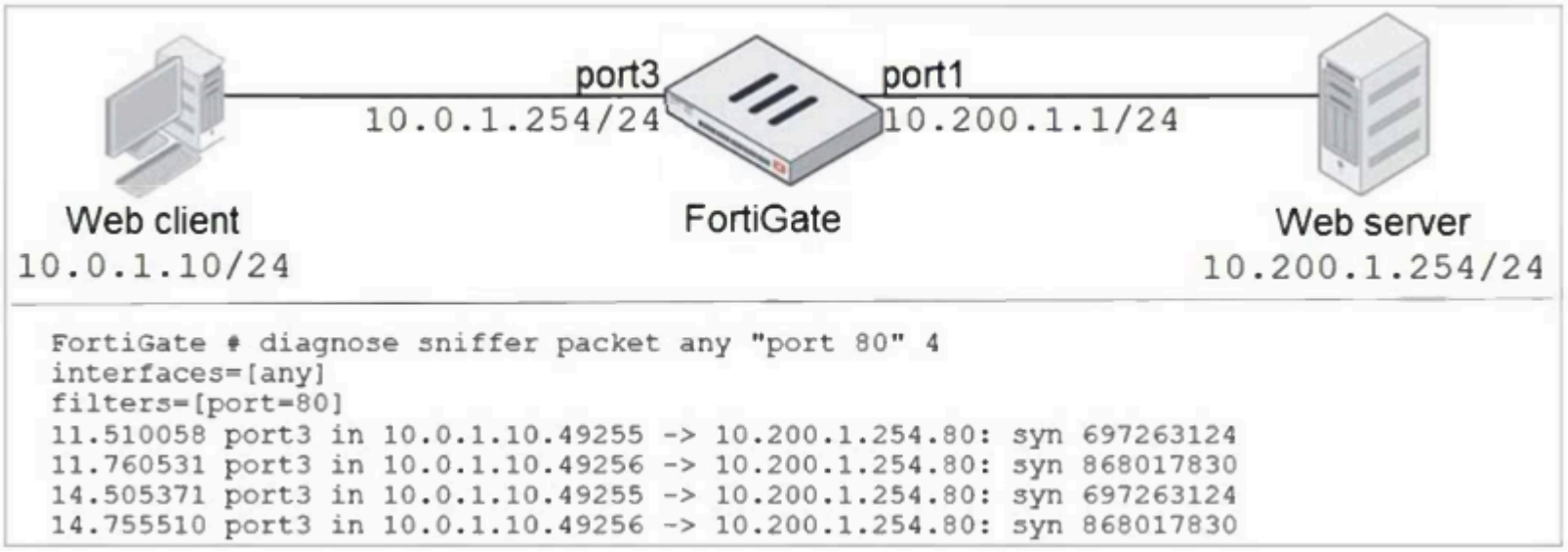
Community vote distribution

C (85%) B (15%)

by CharlieS8 at *Oct. 25, 2024, 5:12 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 8 DISCUSSION

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 shown in the exhibit.

What should the administrator do next, to troubleshoot the problem?

A. Execute a debug flow.

B. Capture the traffic using an external sniffer connected to port1.

C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".

D. Run a sniffer on the web server.

Suggested Answer: *A*

Community vote distribution

A (100%)

by Qwerty379 at *Aug. 29, 2024, 4:55 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 80 DISCUSSION

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively.

Which two statements are true about the requirements of connected physical interfaces on FortiGate? (Choose two.)

A. Both interfaces must have the interface role assigned

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

C. Both interfaces must have DHCP enabled

D. Both interfaces must have IP addresses assigned

Suggested Answer: *BD*

Community vote distribution

BD (77%) AD (23%)

by CharlieS8 at *Oct. 30, 2024, 12:10 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 81 DISCUSSION

Which two pieces of information are synchronized between FortiGate HA members? (Choose two.)

A. OSPF adjacencies

B. IPsec security associations

C. BGP peerings

D. DHCP leases

Suggested Answer: *BD*

Community vote distribution

BD (100%)

by CharlieS8 at *Oct. 25, 2024, 5:14 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 82 DISCUSSION

Refer to the exhibit.

```
FGT1 # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S    *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
S    *>           [10/0] via 10.0.0.2, port2, [30/0]
S       0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C    *> 10.0.0.0/24 is directly connected, port2
S       172.13.24.0/24 [10/0] is directly connected, port4, [1/0]
C    *> 172.20.121.0/24 is directly connected, port1
S    *> 192.168.1.0/24 [10/0] via 10.0.0.2, port2, [1/0]
C    *> 192.168.15.0/24 is directly connected, port3
```

Based on the routing database shown in the exhibit which two conclusions can you make about the routes? (Choose two.)

A. There will be eight routes active in the routing table

B. The port1 and port2 default routes are active in the routing table

C. The port3 default route has the highest distance

D. The port3 default route has the lowest metric

Suggested Answer: *BC*

Community vote distribution

BC (100%)

by CharlieS8 at *Oct. 30, 2024, 12:11 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 83 DISCUSSION

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

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

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

C. FortiGate does not support workstation check.

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

Suggested Answer: *BC*

Community vote distribution

BC (100%)

by CharlieS8 at *Oct. 25, 2024, 5:14 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 84 DISCUSSION

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The NetSessionEnum function is used to track user logouts.

B. NetAPI polling can increase bandwidth usage in large networks.

C. The collector agent must search Windows application event logs.

D. The collector agent uses a Windows API to query DCs for user logins.

Suggested Answer: *A*

Community vote distribution

A (82%) Other

by CharlieS8 at *Oct. 25, 2024, 5:15 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 85 DISCUSSION

Refer to the exhibits.

Security Fabric physical topology view

Security Fabric configuration on Local-FortiGate

```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream ''
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC Y9ynT+64RpCTpVdgSmoQHZ42mYSIzNNzLNvgzMXjyN
9hSjIJE3KYJlo3Xxyg1dvNxPId8T5xctBUszy7rgIcHcA/qHrByXSXfPEeHC6ufkqlPJr
W6GypwDUb5O3VFgPbASFYYteQesmwoJtGe84BLqa+hUcgunLD1z/97sBp+PLt5nrA==
    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
```

Security Fabric configuration on ISFW

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream "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 local
end

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 set fabric-object-unification default.

B. Change the csf setting on both devices to set downstream-access enable.

C. Change the csf setting on ISFW (downstream) to set authorization-request-type certificate.

D. Change the csf setting on ISFW (downstream) to set configuration-sync local.

Suggested Answer: *A*

Community vote distribution

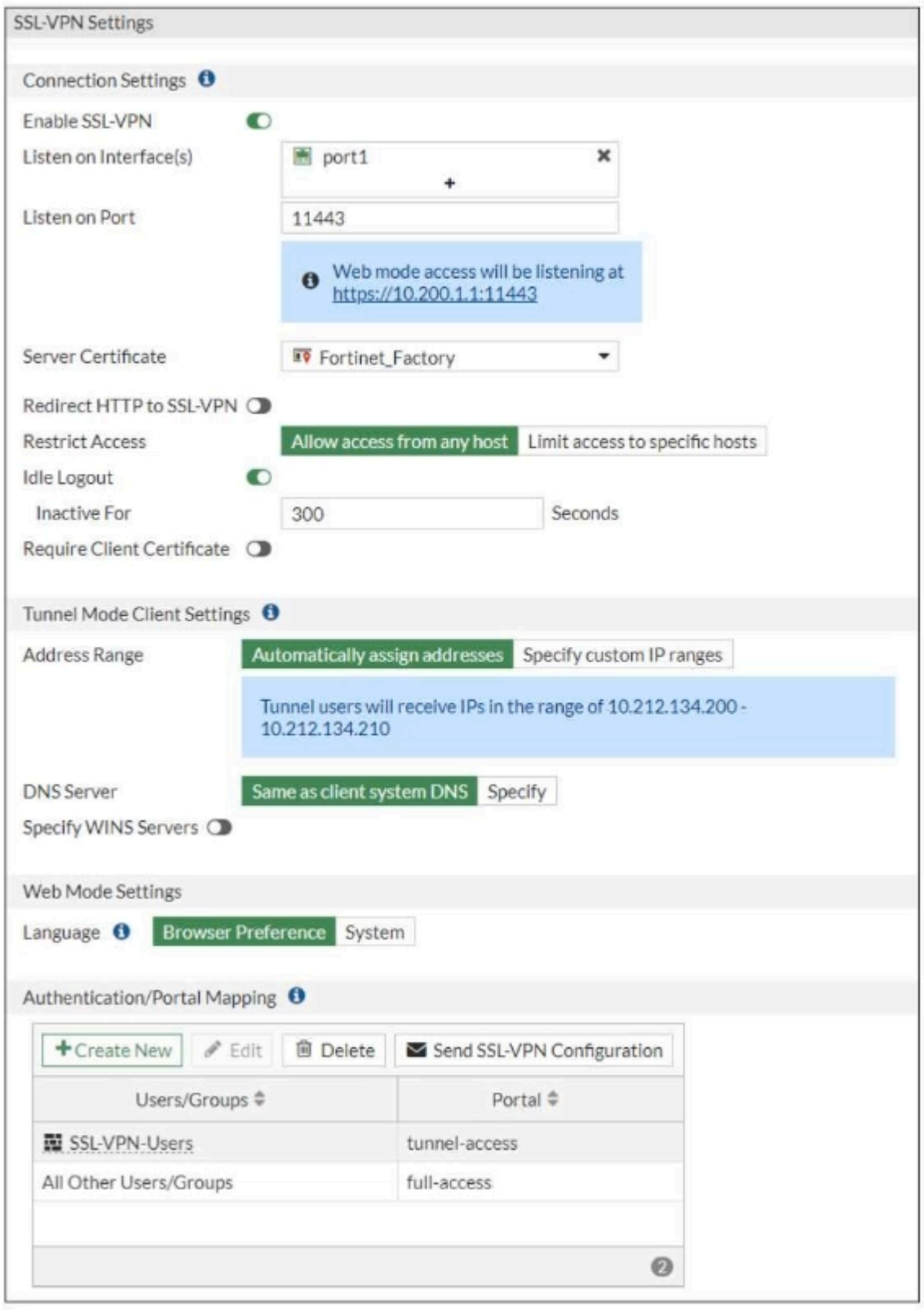
A (88%) 13%

by CharlieS8 at *Oct. 25, 2024, 5:18 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 86 DISCUSSION

Refer to the exhibits.

SSL-VPN settings



VPN connection status

The SSL VPN connection fails when a user attempts to connect to it.

What should the user do to successfully connect to the SSL VPN?

A. Change the SSL VPN portal to the tunnel.

B. Change the idle timeout.

C. Change the server IP address.

D. Change the SSL VPN port on the client.

Suggested Answer: *D*

Community vote distribution

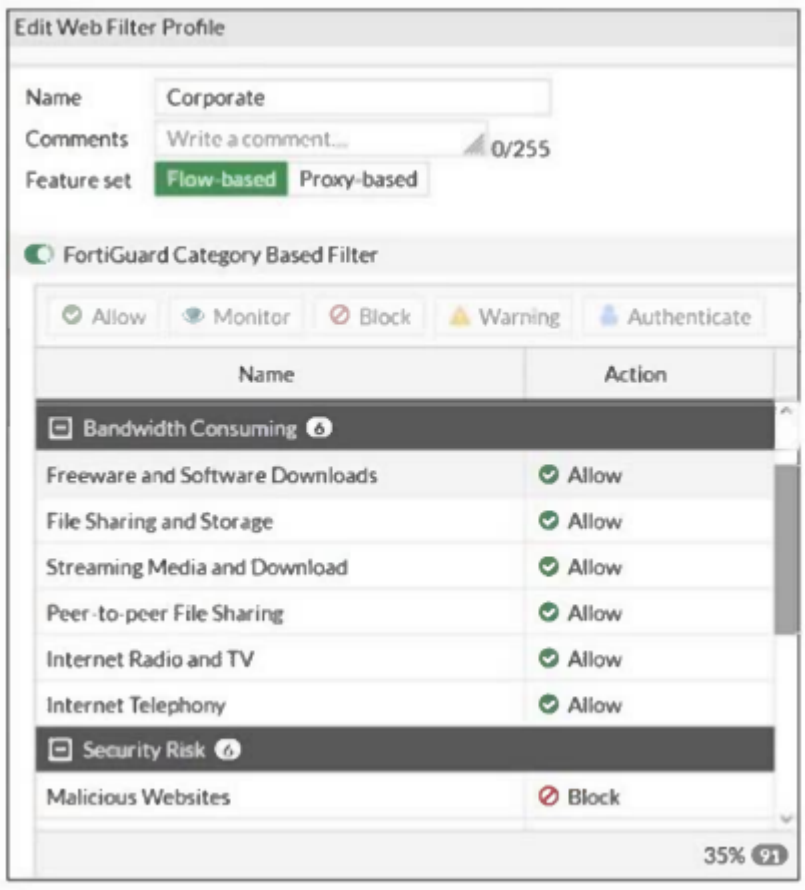
D (100%)

by CharlieS8 at *Oct. 25, 2024, 5:19 a.m.*

EXAM FCP_FGT_AD-7.4 TOPIC 1 QUESTION 9 DISCUSSION

Refer to the exhibit.

FortiGate web filter profile configuration



The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.

An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.

What are two solutions for satisfying the requirement? (Choose two.)

A. Configure a separate firewall policy with action Deny and an FQDN address object for *.download.com as destination address.

B. Set the Freeware and Software Downloads category Action to Warning.

C. Configure a web override rating for download.com and select Malicious Websites as the subcategory.

D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

by andres8h at *Aug. 30, 2024, 10:34 p.m.*