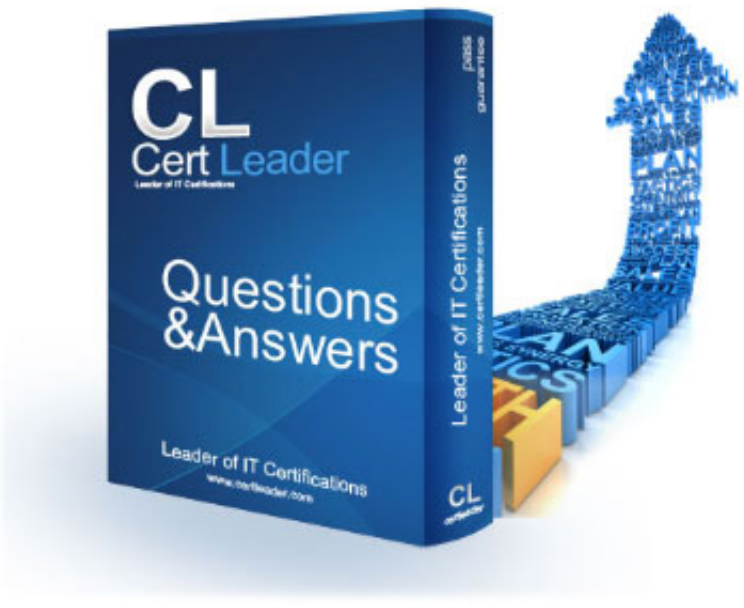
FCP_FGT_AD-7.4 Dumps

FCP - FortiGate 7.4 Administrator

https://www.certleader.com/FCP_FGT_AD-7.4-dumps.html



NEW QUESTION 1
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)"
```

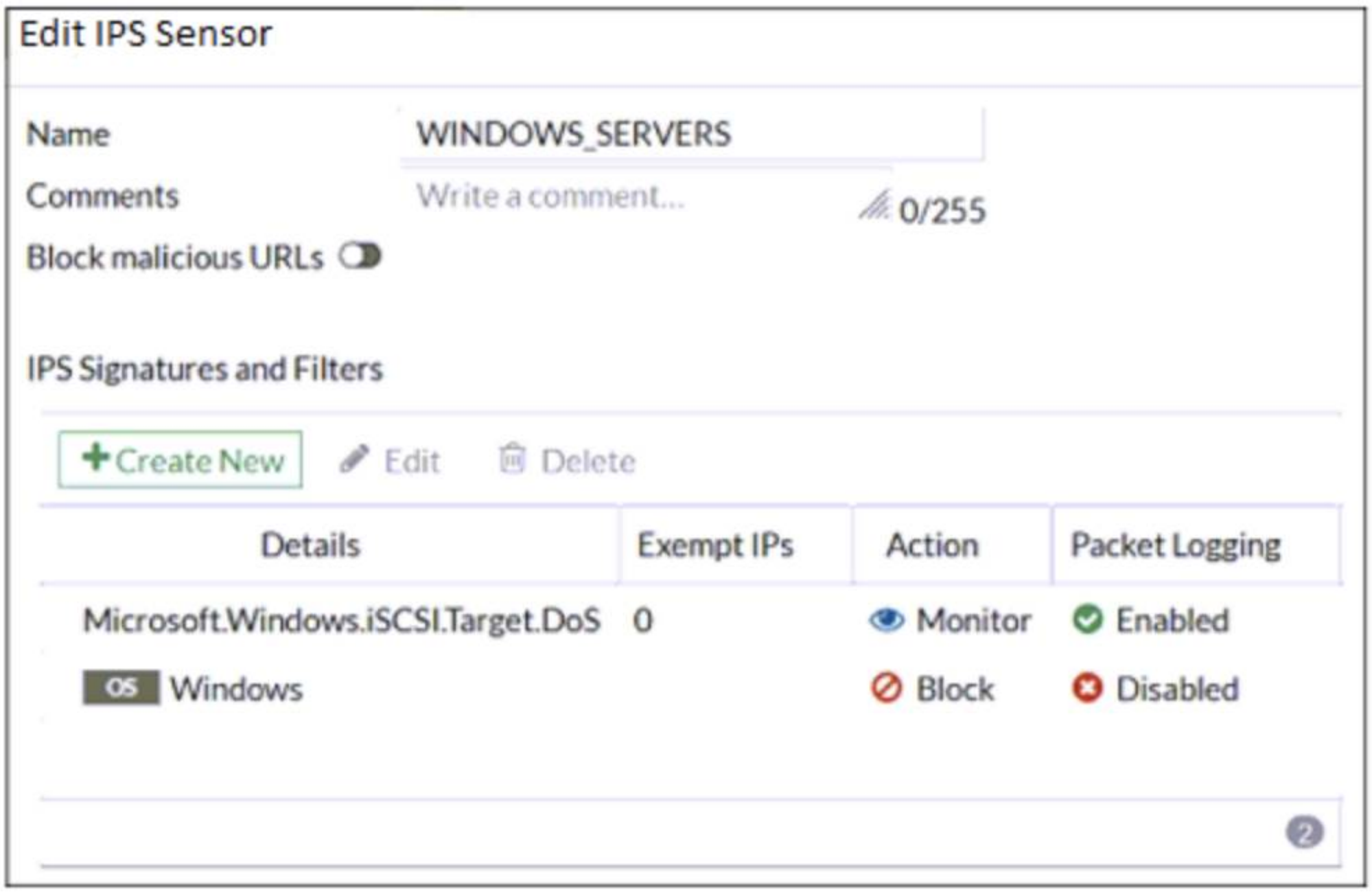
Why did FortiGate drop the packet?

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

Answer: D

Explanation:
The debug trace output shows that the packet was "Denied by forward policy check (policy 0)." In FortiGate, policy ID 0 corresponds to the default implicit deny policy. This means that if a packet does not match any configured firewall policies, it is denied by the default implicit policy.
References:
FortiOS 7.4.1 Administration Guide: Firewall Policies

NEW QUESTION 2
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.

Answer: AC

Explanation:
The IPS sensor configuration shows that:
The Microsoft.Windows.iSCSI.Target.DoS signature is set to "Monitor" with packet logging enabled, meaning that while traffic matching this signature will be

allowed, it will also be logged for further analysis.

The generic Windows filter is set to "Block," meaning that all other attacks matching this filter will be blocked. However, the sensor will not reset connections or log packets unless specified.
Therefore, the sensor will allow attackers matching the specific DoS signature while blocking other attacks against Windows.
References:

FortiOS 7.4.1 Administration Guide: IPS Configuration

NEW QUESTION 3
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.

Answer: AD

Explanation:
The Reverse Path Forwarding (RPF) check is run on the first sent packet of any new session to ensure that the packet arrives on a legitimate interface. This check protects the network from IP spoofing attacks by verifying that a return route exists from the receiving interface back to the source IP address. If the route is invalid or not found, the packet is discarded. Options B and C are incorrect because RPF checks are performed on the first sent packet, not the reply packet.
References:

FortiOS 7.4.1 Administration Guide: Reverse Path Forwarding (RPF) Check

NEW QUESTION 4
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

Answer: ABC

Explanation:
The Fortinet Single Sign-On (FSSO) Collector Agent supports three primary methods for Active Directory (AD) polling to collect user information:

WinSecLog: Monitors Windows Security Event Logs for login events.

WMI: Uses Windows Management Instrumentation to poll user login sessions.

NetAPI: Utilizes the Netlogon API to query domain controllers for user session data.
These methods allow the FortiGate to gather user logon information and enforce user-based policies effectively.
References:

FortiOS 7.4.1 Administration Guide: FSSO Configuration

NEW QUESTION 5
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.

Answer: AD

Explanation:
Advanced mode allows for configuration as an LDAP client and supports group filtering directly on the FortiGate, as well as nested or inherited groups.

NEW QUESTION 6
Refer to the exhibit, which shows a partial configuration from the remote authentication server.

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	

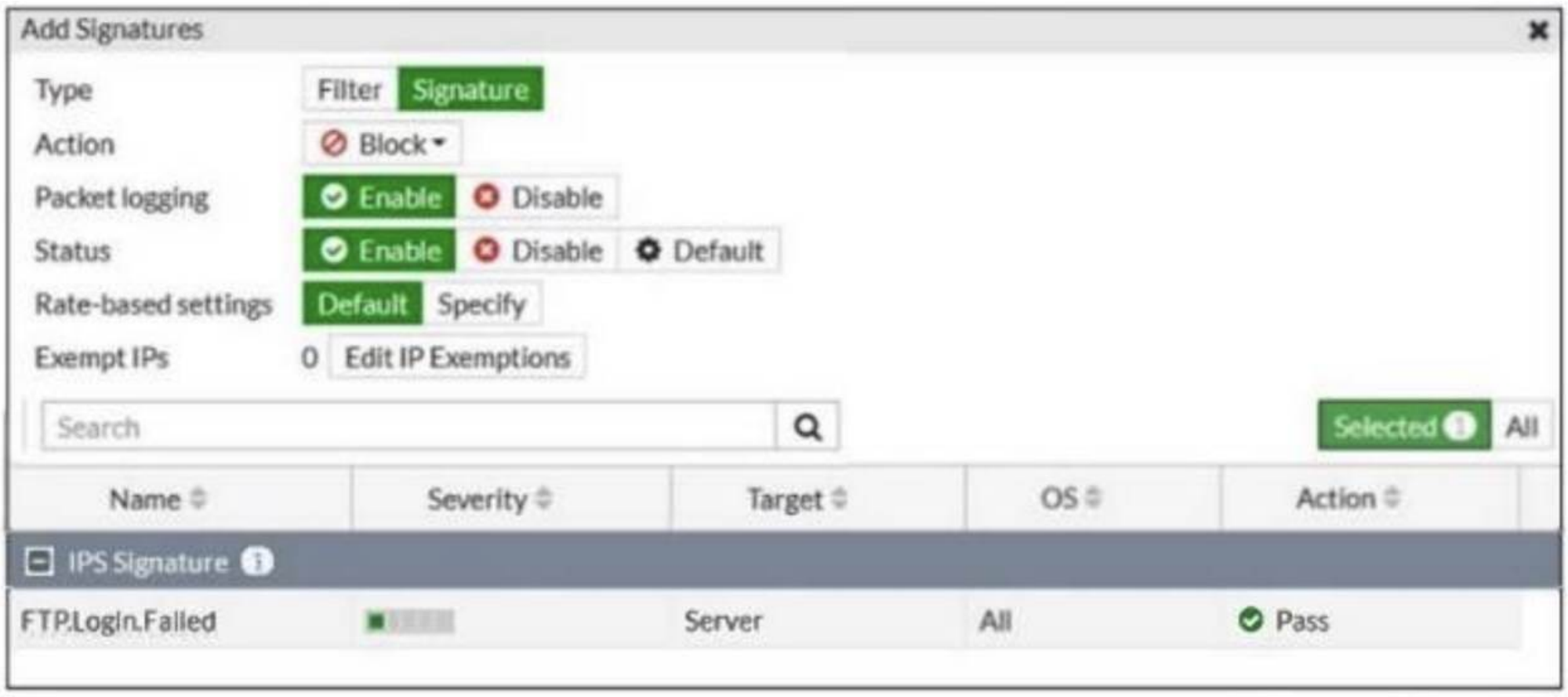
Why does the FortiGate administrator need this configuration?

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.

Answer: A

NEW QUESTION 7
Refer to the exhibit.



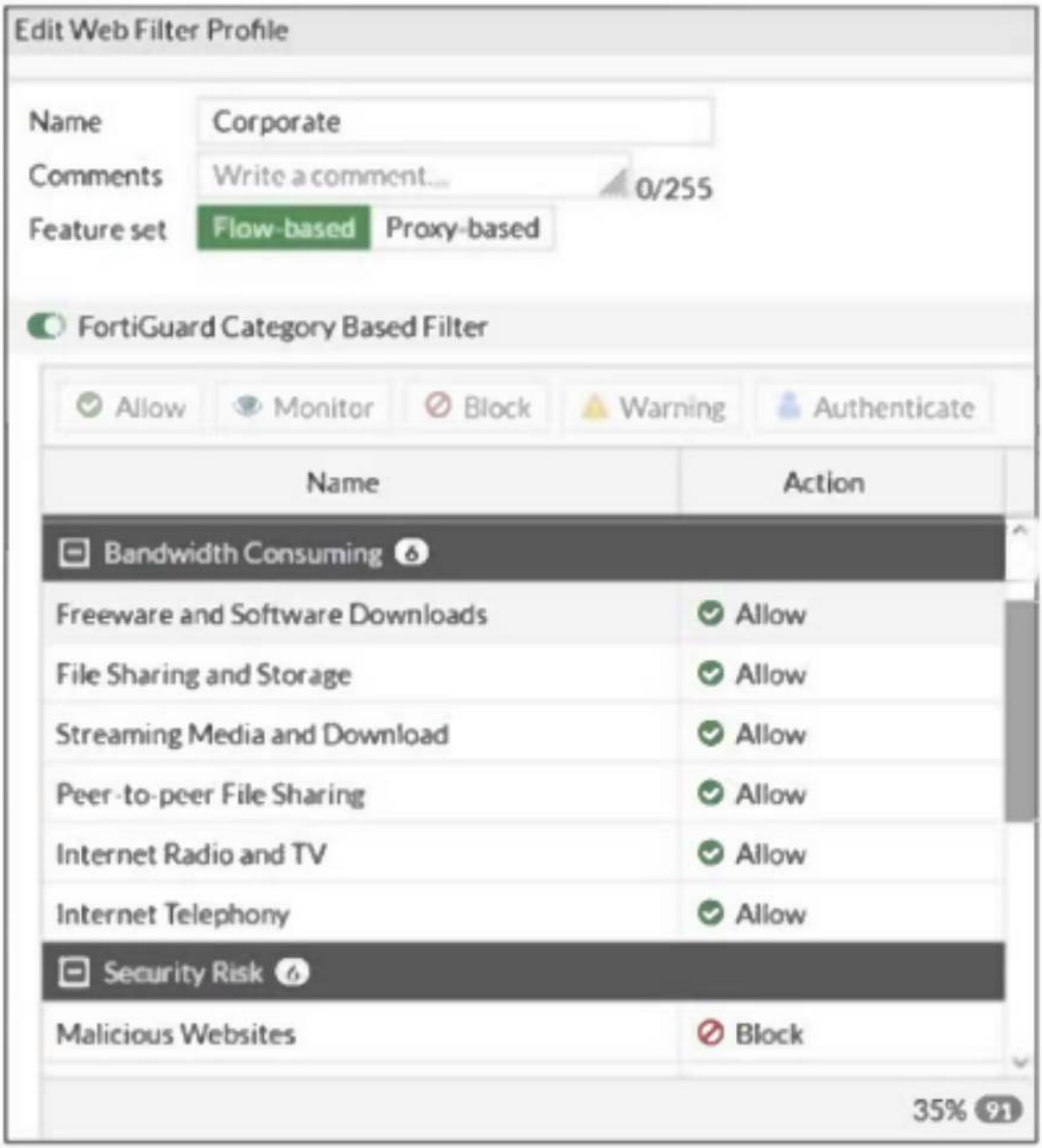
Review the intrusion prevention system (IPS) profile signature settings shown in the exhibit. What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

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.

Answer: A

Explanation:
The exhibit shows that the "FTP.Login.Failed" IPS signature is set with the action "Pass" and packet logging enabled. This means that any traffic matching this signature will be allowed through the FortiGate, and the traffic details will be logged for monitoring and analysis purposes.
References:
FortiOS 7.4.1 Administration Guide: IPS Signature Actions

NEW QUESTION 8
Refer to the exhibit.



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.

Answer: AD

Explanation:
To block access specifically to download.com while allowing other sites in the "Freeware and Software Downloads" category, you can create a separate firewall policy with a deny action specifically for the FQDN
*.download.com. This approach allows blocking this particular site without affecting the other sites in the same category. Alternatively, configuring a static URL filter entry with the type set to Wildcard and action set to Block will also achieve the desired effect by directly blocking the specific URL without impacting other sites in the category.
References:

FortiOS 7.4.1 Administration Guide: URL filter configuration

NEW QUESTION 9
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.

Answer: C

Explanation:
Automation stitches on FortiGate can have one or more triggers, which are conditions or events that activate the automation stitch. The trigger defines when the automation stitch should execute the defined actions. Actions within a stitch can be executed sequentially or in parallel, depending on the configuration.
References:
FortiOS 7.4.1 Administration Guide: Automation Stitches

NEW QUESTION 10
Which method allows management access to the FortiGate CLI without network connectivity?

A. SSH console
B. CLI console widget
C. Serial console
D. Telnet console

Answer: C

Explanation:
The serial console method allows management access to the FortiGate CLI without relying on network connectivity. This method involves directly connecting a computer to the FortiGate device using a serial cable (such as a DB-9 to RJ-45 cable or USB to RJ-45 cable) and using terminal emulation software to interact with the FortiGate CLI. This method is essential for situations where network-based access methods (such as SSH or Telnet) are not available or feasible.
References:
FortiOS 7.4.1 Administration Guide: Console connection

NEW QUESTION 10
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. LDAP server
B. RADIUS server
C. DHCP server
D. Windows server

Answer: A

Explanation:
To retrieve AD user group information in agentless polling mode, the administrator must add an LDAP server to the FortiGate device.

NEW QUESTION 14
Refer to the exhibit to view the firewall policy.

Firewall policy configuration

Edit Policy

Name	Internet_Access
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	DNS FTP HTTP HTTPS
Action	ACCEPT / DENY
Inspection Mode	Flow-based / Proxy-based

Firewall/Network Options

NAT	
IP Pool Configuration	Use Outgoing Interface Address / Use Dynamic IP Pool
Preserve Source Port	
Protocol Options	default

Security Profiles

AntiVirus	default
Web Filter	
DNS Filter	
Application Control	
IPS	
File Filter	
SSL Inspection	certificate-inspection

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.

Answer: B

Explanation:
The firewall policy shown in the exhibit is configured in flow-based inspection mode. In flow-based inspection, certain security features, such as deep content inspection, might not be as effective as in proxy- based mode. Proxy-based inspection is necessary for thorough content inspection, which includes identifying and blocking well-known viruses like EICAR.
References:

FortiOS 7.4.1 Administration Guide: Inspection Modes

NEW QUESTION 15
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.

Answer: A

Explanation:
Firewall authentication generally requires the DNS service to be enabled in the firewall policy to correctly resolve hostnames during the authentication process. If DNS is not allowed in the firewall policy, the FortiGate cannot resolve external domains, and as a result, the user may not be presented with the login prompt when attempting to access an external website.
References:

FortiOS 7.4.1 Administration Guide: Firewall Authentication Configuration

NEW QUESTION 18
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 porc2 is marked as the standby route.

Answer: CD

Explanation:
The routing table in the exhibit shows two default routes (0.0.0.0/0) with different administrative distances:
- The default route through port2 has an administrative distance of 20.
- The default route through port1 has an administrative distance of 10.

Administrative distance determines the priority of the route; a lower value is preferred. Here, the route through port1 with an administrative distance of 10 is the preferred route. The route through port2 with an administrative distance of 20 acts as a standby or backup route. If the primary route (port1) fails or is unavailable, traffic will then be routed through port2.
Regarding the statement that the port2 interface is marked as inactive, there is no indication in the routing table that port2 is inactive. Similarly, all the routes displayed are not necessarily installed in the FortiGate routing table, as the table could include both active and backup routes.
References:
- FortiOS 7.4.1 Administration Guide: Default route configuration
- FortiOS 7.4.1 Administration Guide: Routing table

NEW QUESTION 22
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

Answer: D

Explanation:
FortiGate applies web filters in the following order: Static URL filter, FortiGuard category filter, Web content filter, Web script filter, and Antivirus scanning.

NEW QUESTION 26
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		

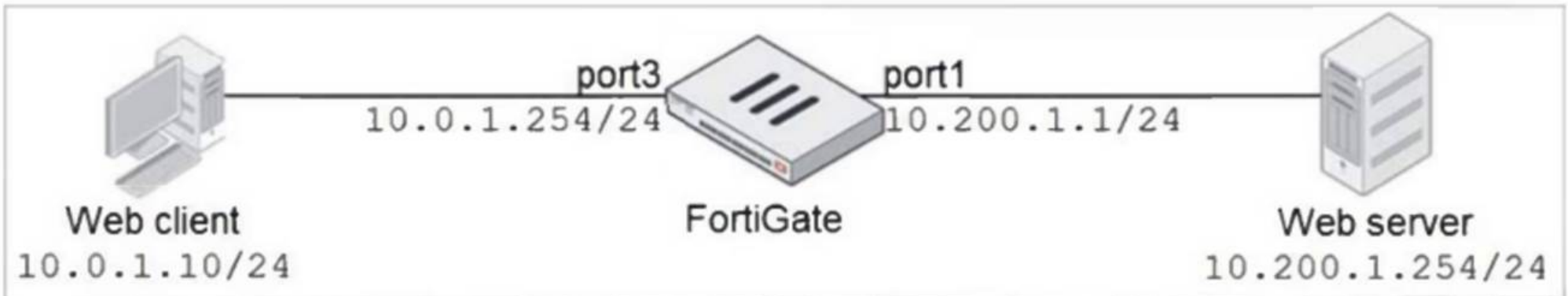
Which statement about this firewall policy list is true?

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 WA
E. WAN to LA
F. and Implicit are sequence grouping view lists.

Answer: C

Explanation:
The firewall policy list in the exhibit is arranged in the "Interface Pair View," where policies are grouped by their incoming (ingress) and outgoing (egress) interface pairs. Each section (LAN to WAN, WAN to LAN, etc.) groups policies based on these interface pairings. This view helps administrators quickly identify which policies apply to specific traffic flows between network interfaces. Options A and D are incorrect because the Implicit group typically does not include more than one deny policy, and there is no "sequence grouping view" in FortiGate. Option B is incorrect as the list is not displayed strictly by ID sequence.
References:
FortiOS 7.4.1 Administration Guide: Firewall Policy Views

NEW QUESTION 27
Refer to the exhibit.



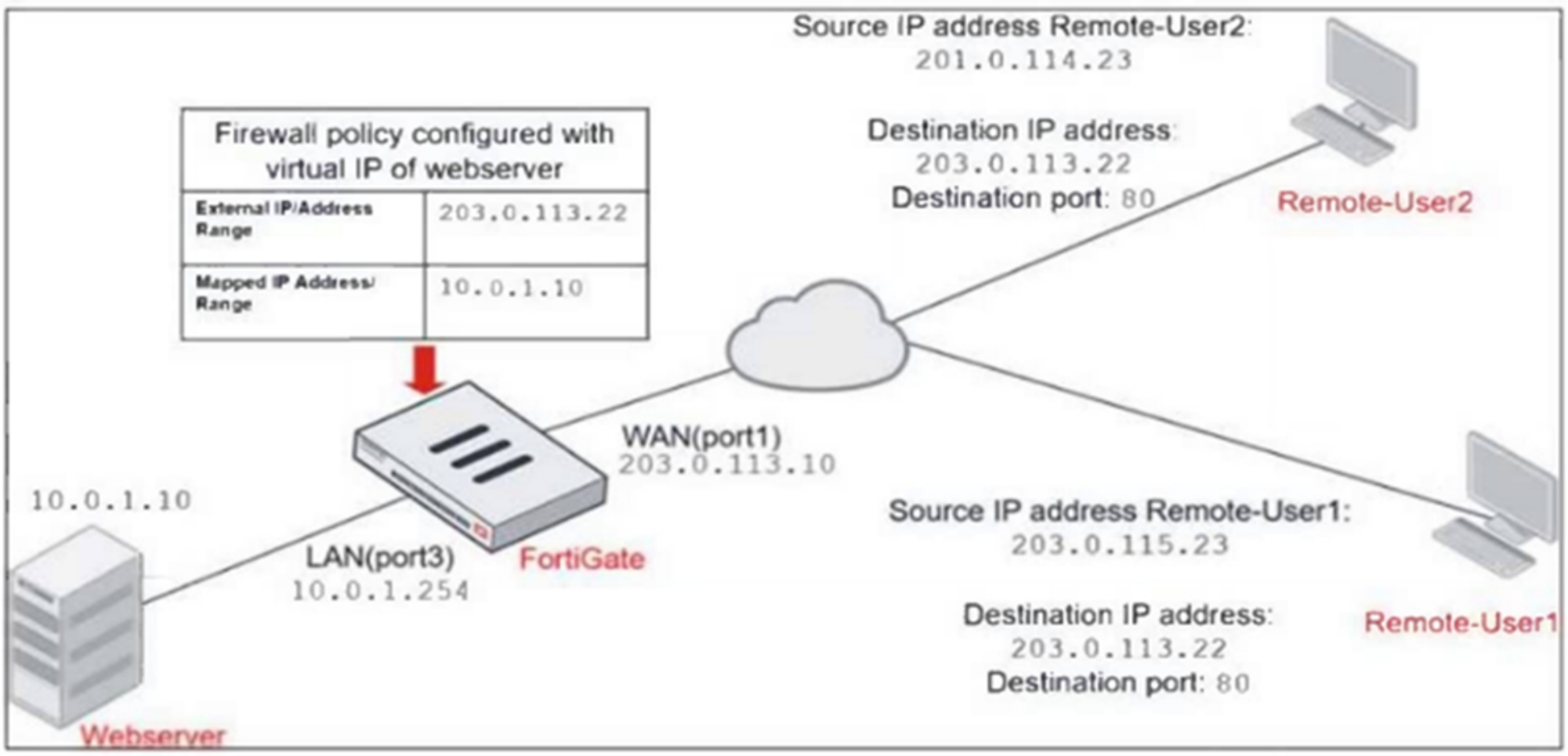
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.
What should the administrator do next, to troubleshoot the problem?

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.

Answer: A

NEW QUESTION 30
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.

Answer: AB

NEW QUESTION 35
Refer to the exhibit.

```
FGT1 # get router info routing-table all
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
       * - candidate default

Routing table for VRF=0
S       0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]
C       172.20.121.0/24 is directly connected, port1
C       172.20.168.0/24 is directly connected, port2
C       172.20.167.0/24 is directly connected, port3
S       10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
S       10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
S       10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
```

Which route will be selected when trying to reach 10.20.30.254?

A. 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]

Answer: A

Explanation:
The correct route selected when trying to reach 10.20.30.254 is 10.20.30.0/24 [10/0] via 172.20.167.254,
port3, [1/0].
Prefix Length: The routing process prioritizes routes with the most specific (longest) prefix. In this case, 10.20.30.0/24 has a shorter prefix than 10.20.30.0/26 (option C), but it still matches the target address 10.20.30.254. The /24 subnet includes all addresses from 10.20.30.0 to 10.20.30.255, so 10.20.30.254 falls within this range.
• Administrative Distance and Metric: In the exhibit, all routes have the same administrative distance (AD) and metric, meaning they are considered equal in terms of preference. Hence, the prefix length becomes the primary factor for route selection.
Why the other options are less appropriate:

B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
• This route is for a different subnet, 10.30.20.0/24, which does not include the target address 10.20.30.254. Therefore, it is not a valid match.

C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
• Although this has a more specific prefix (/26), which means it should cover a smaller range of addresses, the /26 subnet only includes addresses from 10.20.30.0 to 10.20.30.63. The target address 10.20.30.254 does not fall within this range, so this route will not be selected.

D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]
• This is a default route (0.0.0.0/0) used for any address that doesn??t match a more specific route.
Since 10.20.30.254 matches the 10.20.30.0/24 route (option A), the default route will not be selected.

NEW QUESTION 38
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration

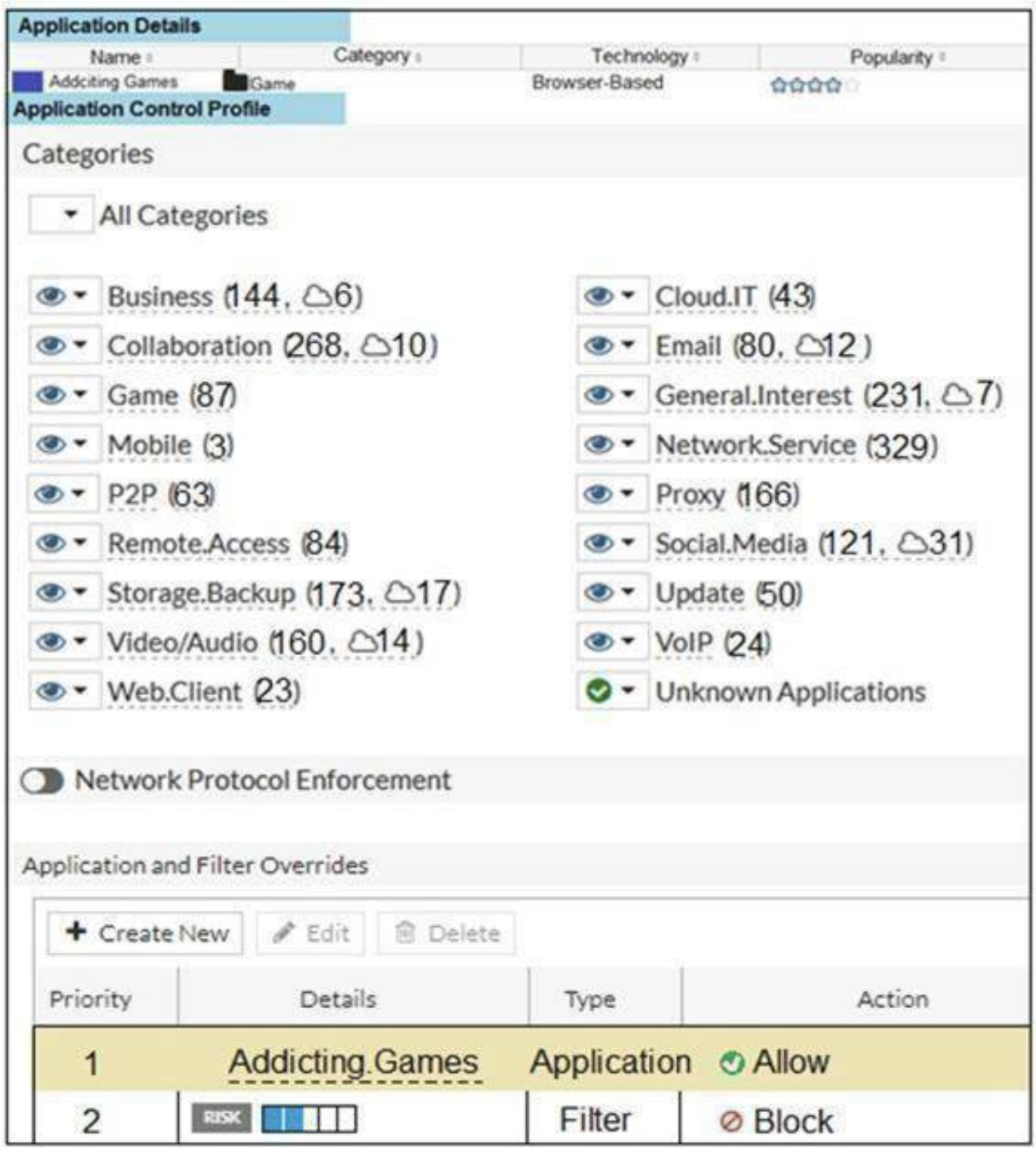
Based on the exhibit, which statement is true?

A. The underlay zone contains port1 and
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.

Answer: C

Explanation:
In FortiGate's SD-WAN configuration, the d-wan zone is a system default SD-WAN zone that is automatically created and cannot be deleted. This zone is used to manage dynamic WAN links for SD-WAN
traffic balancing and routing. It ensures that multiple WAN interfaces can be grouped and managed
effectively for WAN link optimization.
Why the other options are less appropriate:
• A. The underlay zone contains port1 and: There is no mention in the exhibit about an "underlay zone" containing port1.
• B. The d-wan zone contains no member: This statement is irrelevant since the focus is on the zone's deletion, not its members.
• D. The virtual-wan-link zone contains no member: This is unrelated to the core fact that the d-wan zone cannot be deleted.
Reference:
FortiOS 7.4.1 Administration Guide: SD-WAN Zone Configuration

NEW QUESTION 41
Refer to the exhibit.



A user located behind the FortiGate device is trying to go to http://www.addictinggames.com (Addicting.Games). The exhibit shows the application detains and application control profile.
Based on this configuration, which statement is true?

A. Addicting.Games will be blocked, based on the Filter Overrides configuration.
B. Addicting.Games will be allowed only if the Filter Overrides action is set to Learn.
C. Addicting.Games will be allowed, based on the Categories configuration.
D. Addicting.Games will be allowed, based on the Application Overrides configuration.

Answer: D

Explanation:
In the exhibit, it shows that the Application Overrides section is configured to allow the application Addicting.Games. The Application Control Profile gives priority to the application overrides, meaning that even if a category or filter would block it, the application control override would allow the specific application to proceed.
• A. Addicting.Games will be blocked, based on the Filter Overrides configuration:
This is incorrect because the Application Overrides take precedence over other filters.
• B. Addicting.Games will be allowed only if the Filter Overrides action is set to Learn:
This is not applicable as the action is based on Application Overrides, not filter overrides.
• C. Addicting.Games will be allowed, based on the Categories configuration:
This is not correct because the application is being allowed due to the Application Overrides, not the category settings.
Thus, the correct explanation is that Addicting.Games will be allowed due to the Application Overrides configuration.

NEW QUESTION 44
Refer to the exhibit.

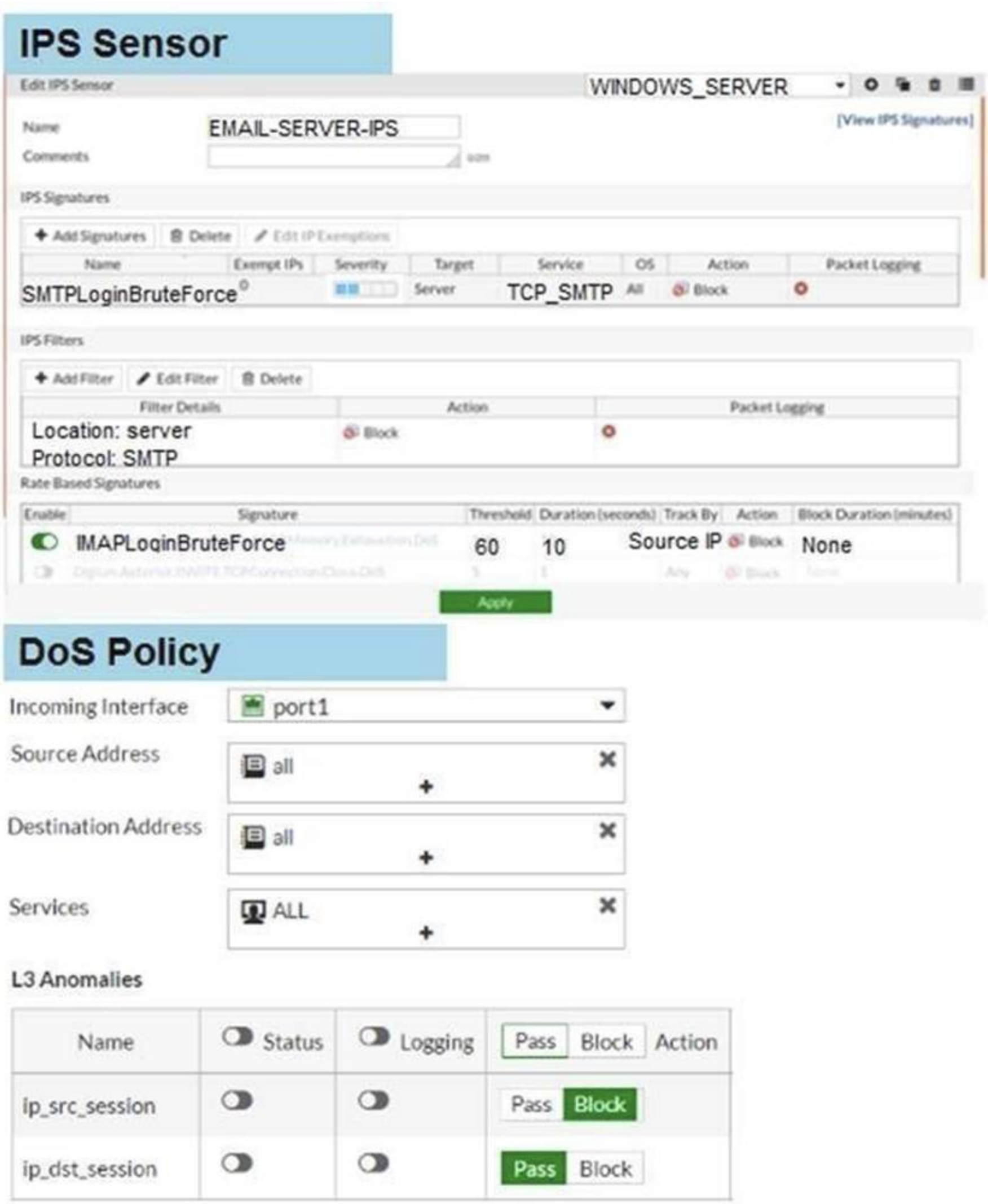
In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

A. Run a sniffer on the web server.
B. Capture the traffic using an external sniffer connected to port1.
C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??
D. Execute a debug flow.

Answer: D

Explanation:
The next step for troubleshooting the problem would be to execute a debug flow on the FortiGate. The debug flow command provides detailed insights into how FortiGate handles the traffic, including whether the traffic is being dropped, allowed, or forwarded to the correct interface. It helps in identifying issues like firewall policy misconfigurations, routing issues, or NAT problems.
• A. Run a sniffer on the web server: While this might help diagnose server-side issues, the initial focus should be on the FortiGate, as the problem might lie in the firewall configuration or traffic handling.
• B. Capture the traffic using an external sniffer connected to port1: This may provide packetlevel information, but it's more useful to first analyze FortiGate's internal decision-making process with a debug flow.
• C. Execute another sniffer in the FortiGate, this time with the filter ??host 10.0.1.10??: Running a sniffer on the specific host might give more packet details, but the debug flow provides more comprehensive information on how the firewall processes the packets.
Thus, using the debug flow will offer a more direct understanding of how the traffic is being processed or
blocked within FortiGate.

NEW QUESTION 46
Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



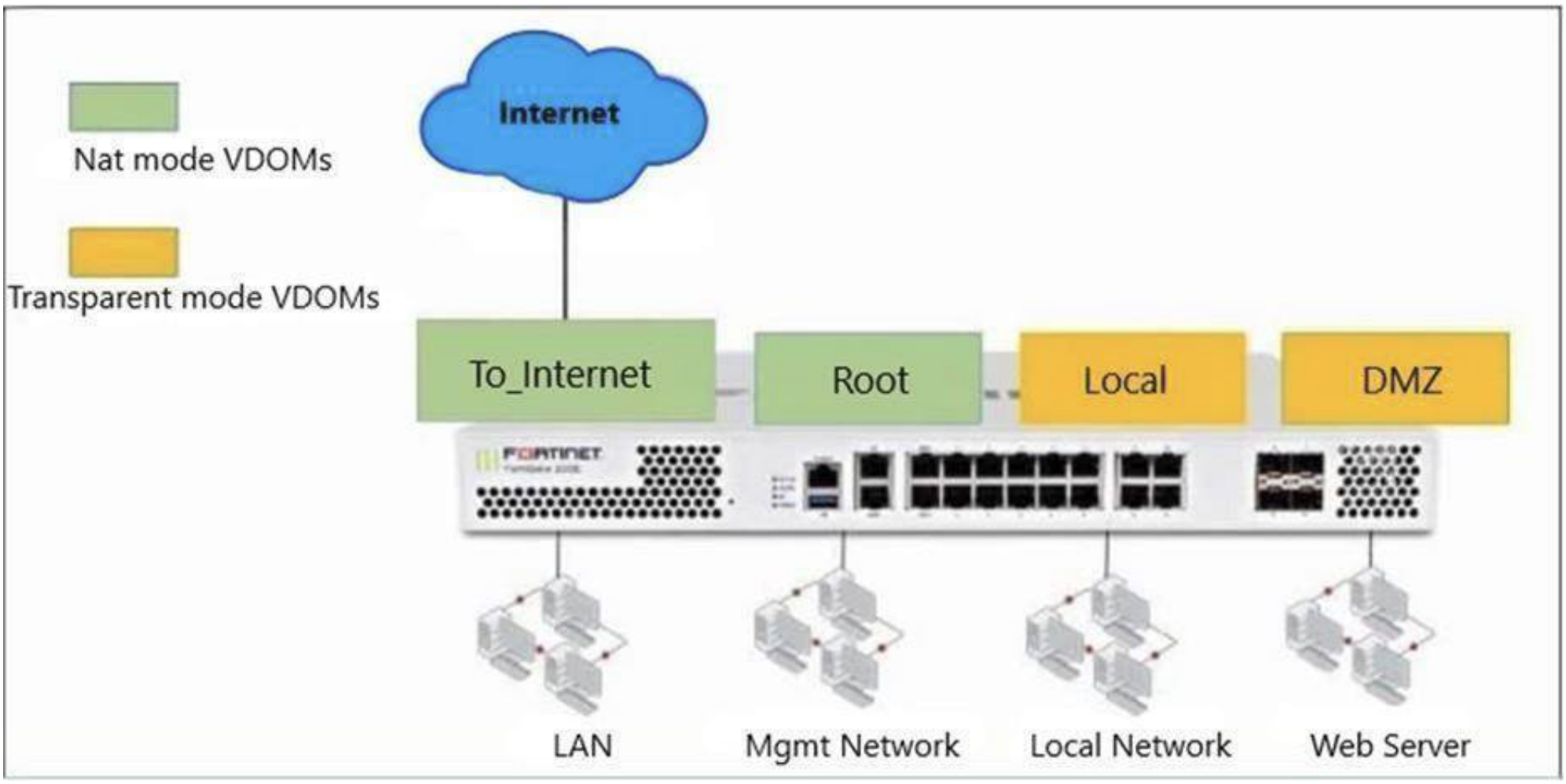
When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

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

Answer: B

Explanation:
When FortiGate evaluates potential attacks, the IPS sensor follows a specific processing order based on the configuration of filters, signatures, and anomaly thresholds. In this case:
• The IPS sensor is configured with IMAP.Login.brute.Force, which comes first in the order of evaluation.
• FortiGate prioritizes based on signature definitions in the sensor, and since IMAP.Login.brute.Force appears higher in the configuration, it will be evaluated before the other signatures and anomalies.
Why the other options are less appropriate:
• A. SMTP.Login.Brute.Force: This would be evaluated after IMAP.Login.brute.Force, based on the sensor configuration hierarchy.
• C. ip_src_session: This is part of the DoS policy and does not come into play until after IPS signatures are evaluated.
• D. Location: server Protocol: SMTP: This appears to be part of the broader IPS sensor rule, but it is not the first item in the evaluation chain.

NEW QUESTION 47
Refer to the exhibit.



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

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

Answer: A

Explanation:
In this scenario, multiple Virtual Domains (VDOMs) are used, and each VDOM operates either in NAT mode or transparent mode:
• Root VDOM (management) and To_Internet VDOM are in NAT mode.
• DMZ VDOM and Local VDOM are in transparent mode.
To allow traffic between different VDOMs (e.g., Local and Root), inter-VDOM links must be configured.
Since Local VDOM is in transparent mode, it functions at Layer 2, meaning it requires an inter-VDOM link to pass traffic through the Root VDOM, which operates in NAT mode at Layer 3.
Why the other options are less appropriate:
• B. A default static route is not required on the To_Internet VDOM:
A default route is required on the To_Internet VDOM to send traffic from LAN users to the internet.
• C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs:
Both Local and DMZ are in transparent mode and operate at Layer 2, so direct communication
would require inter-VDOM links if passing through another VDOM.
• D. Inter-VDOM links are not required between the Root and To_Internet VDOMs:
Even if the Root VDOM is only used for management, it still requires inter-VDOM links to communicate with other VDOMs (like To_Internet) in the Security Fabric.

NEW QUESTION 49
View the exhibit.
A user at 192.168.32.15 is trying to access the web server at 172.16.32.254.


```
FGT1 # get router info routing-table all
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
       * - candidate default

Routing table for VRF=0
S       0.0.0.0/0 [10/0] via 10.40.72.2, port1, [1/0]
C       172.16.32.0/24 is directly connected, port2
C       10.40.72.0/30 is directly connected, port1
```

Which two statements best describe how the FortiGate will perform reverse path forwarding (RPF) checks on this traffic? (Choose two.)

A. Strict RPF check will deny the traffic.
B. Loose RPF check will allow the traffic.
C. Strict RPF check will allow the traffic.
D. Loose RPF check will deny the traffic.

Answer: BC

Explanation:
When FortiGate performs reverse path forwarding (RPF) checks, it can operate in two modes: Strict RPF and Loose RPF. Here??s how these two checks work:
In strict RPF, FortiGate checks whether the best route back to the source IP of the packet (in this case, 192.168.32.15) goes through the same interface on which the packet was received. If the best return path uses a different interface, the packet is denied. Based on the scenario:
o C. Strict RPF check will allow the traffic:
If the return path for 192.168.32.15 matches the interface where the traffic was received, the strict RPF check will allow the traffic.
• Loose RPF Check:
In loose RPF, FortiGate only checks if there is any route back to the source IP of the packet, regardless of the interface. This is a more permissive check, and if a route exists, the packet will be allowed.
o B. Loose RPF check will allow the traffic:
Since loose RPF requires only that a valid route to the source exists, the traffic is allowed.
Why the other options are less appropriate:
• A. Strict RPF check will deny the traffic:
This would only happen if the return route didn??t match the incoming interface, which is not indicated here.
• D. Loose RPF check will deny the traffic:
Loose RPF is more permissive, so it will not deny the traffic as long as a valid route to the source IP exists.

NEW QUESTION 54
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FGT_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FGT_AD-7.4-dumps.html