# Fortinet

## Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

**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**
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

**Answer:** ADE

**Explanation:**
When FortiGate performs SSL/SSH full inspection and detects an invalid certificate, there are three valid actions it can take:

- Allow & Warning: This action allows the session but generates a warning.
- Block & Warning: This action blocks the session and generates a warning.
- Block: This action blocks the session without generating a warning.

Actions such as "Trust & Allow" or just "Allow" without additional configurations are not applicable in the context of handling invalid certificates.
References:

- FortiOS 7.4.1 Administration Guide: Configuring SSL/SSH inspection profile

**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 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

**Answer:** D

**Explanation:**
When FortiGate is configured in NGFW profile-based mode, it primarily uses flow-based inspection for application profiles. Flow-based inspection provides faster processing and lower latency by inspecting traffic in real-time without buffering, making it suitable for scenarios where performance is a priority.
References:

FortiOS 7.4.1 Administration Guide: Inspection Modes

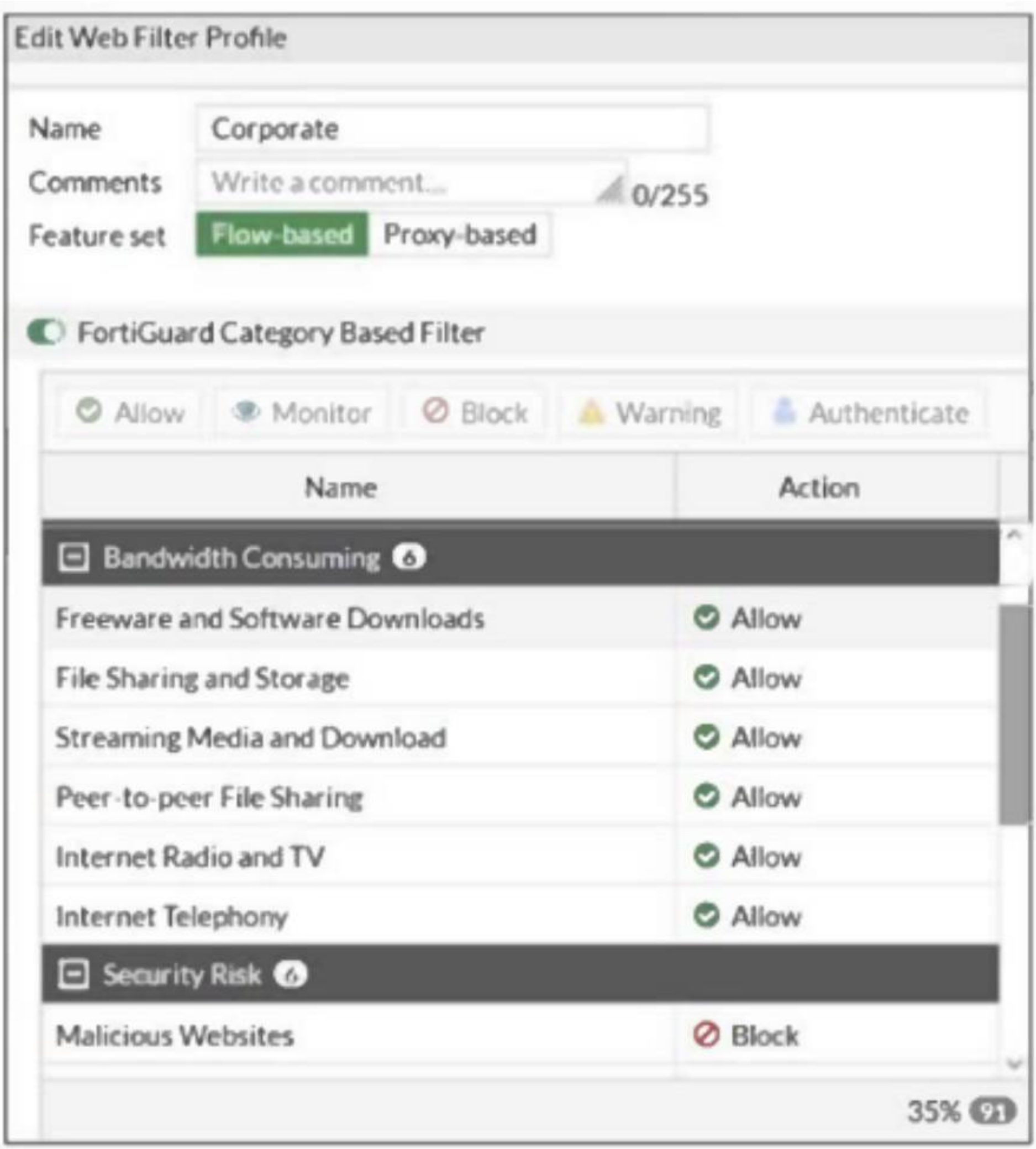
**NEW QUESTION 5**
Refer to the exhibit, which shows a partial configuration from the remote authentication server.


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 6**
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 7**
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 8**
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 9**
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

**Answer:** ABC

**Explanation:**
FortiGate's SD-WAN rule strategies for member selection include the following:

- Manual with load balancing: This strategy allows an administrator to manually configure which SD- WAN member interfaces to use for specific traffic.
- Lowest Cost (SLA) with load balancing: This strategy prioritizes the link with the lowest cost that meets the SLA requirements.
- Best Quality with load balancing: This strategy selects the link with the best performance metrics, such as latency, jitter, or packet loss.

Options D and E are incorrect because "Lowest Quality" is not a valid strategy, and "Lowest Cost without load balancing" contradicts the requirement for load balancing in the strategy name.
References:

- FortiOS 7.4.1 Administration Guide: SD-WAN Rule Strategies

**NEW QUESTION 10**
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:

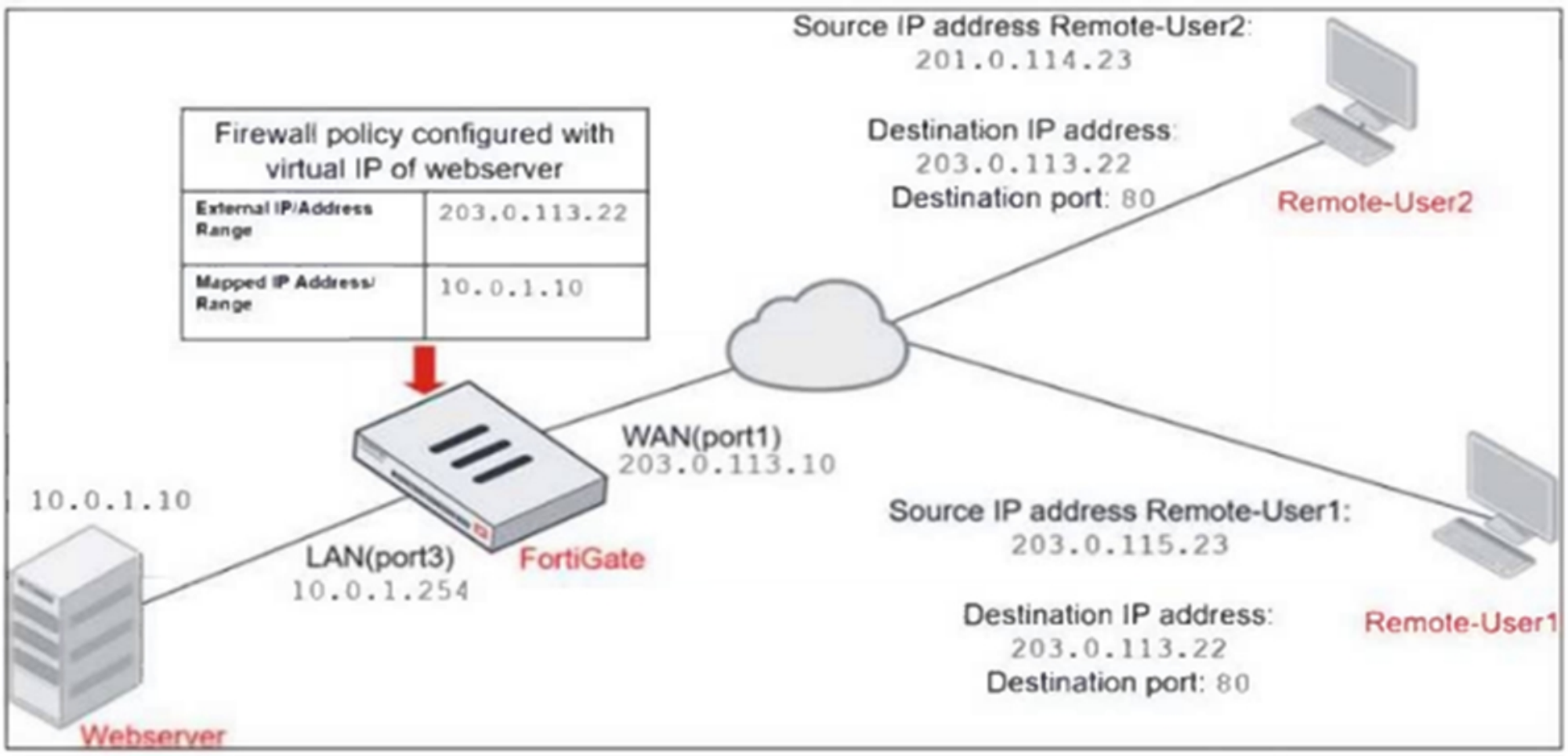
- The default route through port2 has an administrative distance of 20.
- The default route through port1 has an administrative distance of 10.

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 10**
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 12**
Which two IP pool types are useful for carrier-grade NAT deployments? (Choose two.)

A. Port block allocation
B. Fixed port range
C. One-to-one
D. Overload

**Answer:** AB

**Explanation:**
In carrier-grade NAT (CGNAT) deployments, specific IP pool types are used to manage large-scale NAT translations efficiently. The correct IP pool types for CGNAT are:
• A. Port block allocation: This type of IP pool allocates a block of ports from a single public IP to multiple clients. It allows efficient use of a limited number of public IPs by distributing port ranges among users, which is crucial for carrier-grade NAT environments where a large number of users need access to the internet.
• B. Fixed port range: In this type, each client is assigned a fixed range of ports, ensuring that the same public IP and port range are used consistently. This helps in reducing the complexity and overhead of managing dynamic port assignments, which is particularly useful in large-scale CGNAT setups.
Why the other options are less appropriate:
• C. One-to-one: One-to-one NAT is used for mapping a single private IP address to a single public IP address. This is not efficient for carrier-grade NAT because CGNAT is designed to allow multiple clients to share a smaller number of public IPs.
• D. Overload: Overload, also known as PAT (Port Address Translation), maps multiple private IPs to a single public IP by differentiating connections based on port numbers. While commonly used in regular NAT setups, CGNAT benefits more from port block allocation and fixed port range due to th

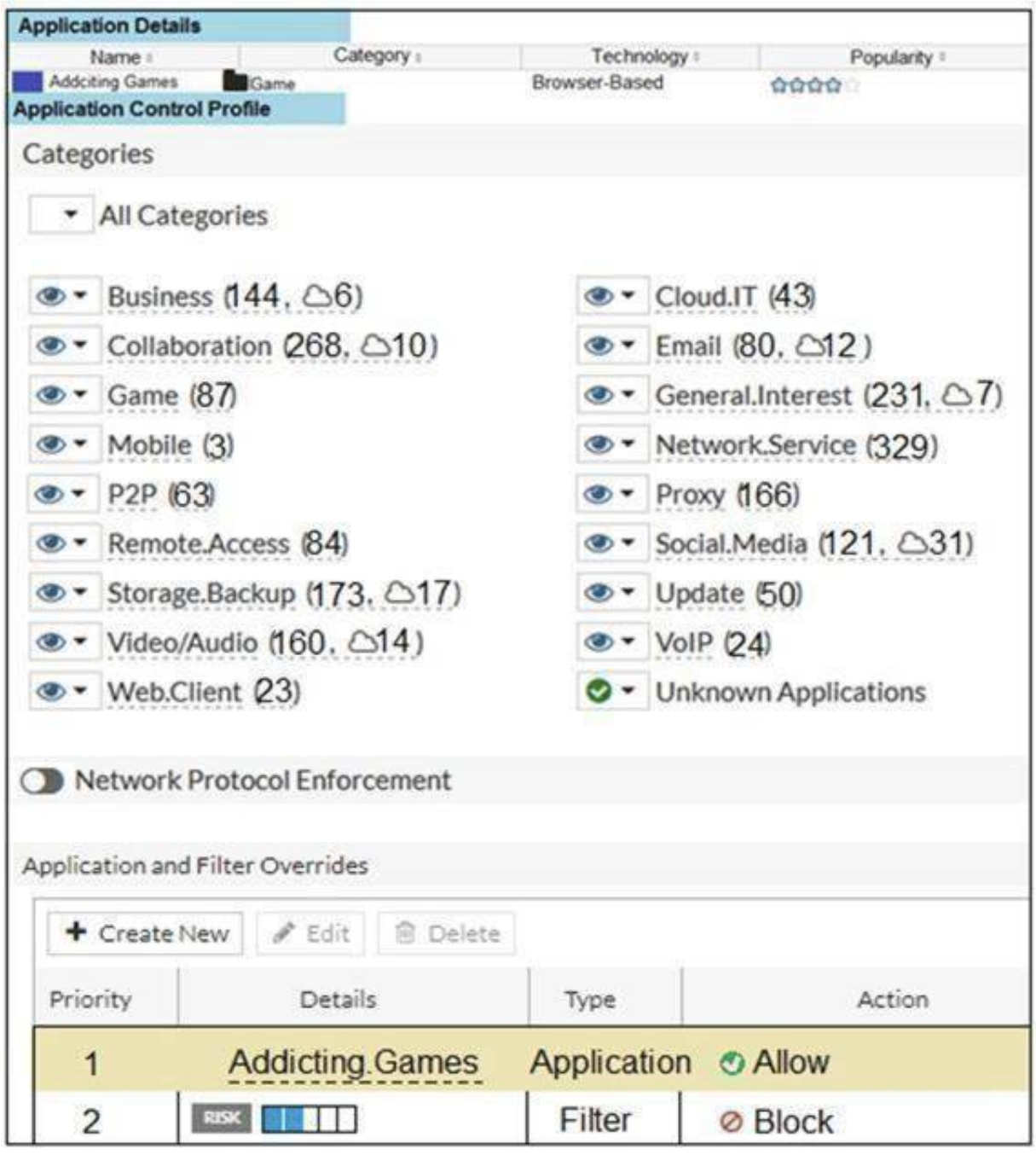
**NEW QUESTION 15**
Which of the following methods can be used to configure FortiGate to perform source NAT (SNAT) for outgoing traffic?

A. Configure a static route pointing to the external interface.
B. Enable the "Use Outgoing Interface Address" option in a firewall policy.
C. Create a virtual server with an external IP address.
D. Deploy an IPsec VPN tunnel with NAT enabled.

**Answer:** B

**Explanation:**
To configure source NAT (SNAT) for outgoing traffic on FortiGate, one of the most common methods is to enable the "Use Outgoing Interface Address" option in a firewall policy. This option ensures that the source IP address of packets leaving the FortiGate device is replaced by the IP address of the outgoing interface. This is typically done when traffic is exiting a private network to access the internet, requiring source NAT to translate the private IP addresses to a public IP.
Why the other options are less appropriate:
* A. Configure a static route pointing to the external interface: A static route is used to direct traffic, but it does not configure SNAT. It determines where packets are sent but does not modify the source IP.
• C. Create a virtual server with an external IP address: Virtual servers are used to provide destination NAT (DNAT) for incoming traffic, not SNAT for outgoing traffic.
• D. Deploy an IPsec VPN tunnel with NAT enabled: While IPsec VPN tunnels can be configured with NAT traversal, this is not the typical method for configuring SNAT for general outgoing internet traffic.

**NEW QUESTION 17**
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 19**
Which two statements correctly describe the differences between IPsec main mode and IPsec aggressive mode? (Choose two.)

A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not.
B. Main mode cannot be used for dialup VPNs, while aggressive mode can.
C. Aggressive mode supports XAuth, while main mode does not.
D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode.

**Answer:** AD

**Explanation:**
The differences between IPsec main mode and IPsec aggressive mode are mainly in the number of packets exchanged and the level of security provided during the negotiation process. Here's the breakdown:
• A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not:
In aggressive mode, the peer's identity is sent in the first packet, making the process faster but less secure because the peer's identity is not encrypted. In main mode, the peer's identity is protected and only exchanged after the encryption is established, offering more security.
• D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode:
Main mode involves a more detailed negotiation process, requiring the exchange of six packets. Aggressive mode, on the other hand, reduces this to three packets, speeding up the connection but sacrificing some security in the process.

Why the other options are less appropriate:
• B. Main mode cannot be used for dialup VPNs, while aggressive mode can:
This is incorrect. Main mode can be used for dialup VPNs as long as the peer's IP is known or configured in advance.
• C. Aggressive mode supports XAuth, while main mode does not:
Both main mode and aggressive mode can support XAuth (eXtended Authentication) if needed.

**NEW QUESTION 24**
.....

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## FCP_FGT_AD-7.4 Practice Exam Features:

* FCP_FGT_AD-7.4 Questions and Answers Updated Frequently

* FCP_FGT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FGT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FGT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year