PassQueen
a.k.a dumpsqueen.com

# FCPFortiGate 7.6 Administrator

## Fortinet FCP_FGT_AD-7.6

**Version Demo**

**Total Demo Questions: 15**

**Total Premium Questions: 150**

**Buy Premium PDF**

https://passqueen.com

support@passqueen.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Deployment and system configuration | 8 |
| Topic 2, Firewall policies and authentication | 39 |
| Topic 3, VPN | 22 |
| Topic 4, Content inspection | 33 |
| Topic 5, Routing | 18 |
| Topic 6, FortiGate infrastructure | 23 |
| Topic 7, Security Fabric | 6 |
| Topic 8, Mix Questions | 1 |
| Total | 150 |

QUESTION NO: 1

A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view.

Why is the policy order different in these two views?

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

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

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

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

**ANSWER: D**

**Explanation:**

Interface Pair View sorts and groups firewall policies according to their source and destination interface pair. This presentation helps an administrator manage and review policies that govern traffic between the same interfaces, such as policies from an internal LAN interface to a WAN interface. Because the display is organized around those interface relationships, its visual ordering does not necessarily match the global order in which FortiGate evaluates policies.

By Sequence View displays policies according to their configured sequence. FortiGate evaluates applicable IPv4 or IPv6 firewall policies in sequence order and uses the first policy that matches the traffic's relevant criteria. Therefore, By Sequence View is the appropriate view for verifying rule precedence and troubleshooting which policy is expected to handle a session. The difference is purely a matter of how the GUI presents the same policy set: interface-pair grouping for administration versus sequence order for policy evaluation. Fortinet documents these policy-list display modes in the FortiGate Administration Guide and further describes their behavior in this Fortinet Community technical tip.

**QUESTION NO: 2**

Refer to the exhibit.


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.** Move NOC_Access to the top of the list to ensure all profile settings take effect.

**B.** Increase the offline value of the Override Idle Timeout parameter in the NOC_Access admin profile.

**C.** Ensure that all NOC_Access users are assigned the super_admin role to guarantee access

**D.** Increase the admintimeout value under config system accprofile NOC_Access.

**ANSWER: B**

**Explanation:**

Increase the offline value of the Override Idle Timeout parameter in the NOC_Access admin profile. FortiGate administrative access profiles can override the globally configured administrator idle timeout for administrators who use that specific profile. This lets the administrator meet the NOC team's requirement without lengthening the idle-session duration for every FortiGate administrator.

The override includes separate values for management access types. The `offline` value applies to GUI and other non-console administrative sessions, so increasing it allows an authenticated NOC administrator to remain signed in for a longer period when no activity occurs. The override must be enabled in the `NOC_Access` access profile, and the offline timeout should be set to a value that conforms to the organization's operational and security requirements. This is more targeted than changing the system-wide administrator timeout because it affects only accounts assigned to `NOC_Access`.

Fortinet documents administrator access-profile configuration, including idle-timeout override settings, in the FortiGate 7.6 Administration Guide: Administrators. Related CLI configuration is documented in the FortiGate 7.6 CLI Reference: config system accprofile.

## QUESTION NO: 3

An administrator wants to analyze and manage digital certificates to prevent browser warnings when users connect to the SSL VPN portal.

Which two statements describe how to correctly do this? (Choose two.)

**A.** The administrator can rely on the default FortiGate self-signed certificate to prevent all security warnings in the browser.

**B.** The administrator must disable HTTPS administrative access entirely to avoid certificate warnings.

**C.** The administrator can use a publicly trusted certificate from a known certificate authority (CA) to stop browser warnings.

**D.** The administrator can import the FortiGate self-signed certificate into each user's browser as a trusted certificate.

**ANSWER: C D**

**Explanation:**

The administrator can use a publicly trusted certificate from a known certificate authority (CA) to stop browser warnings. The certificate installed and selected for the SSL VPN service should identify the hostname that users enter for the portal, either in its common name or subject alternative name. It must also be within its validity period and include any required intermediate CA certificates. Because browsers already contain trust anchors for established public CAs, they can validate this certificate chain and the portal identity without prompting users with an untrusted-certificate warning. FortiGate supports importing and managing local certificates for services such as SSL VPN; see the FortiGate 7.6 Administration Guide.

The administrator can import the FortiGate self-signed certificate into each user's browser as a trusted certificate. This is appropriate for controlled environments where administrators manage endpoint trust stores, such as a corporate device fleet. By distributing the self-signed certificate, or preferably the organization's internal CA certificate when that CA issued the portal certificate, to the trusted certificate authorities store on client devices, the browser can establish trust in the SSL VPN server certificate. Fortinet's certificate-management guidance is available in the Certificate management documentation.

## QUESTION NO: 4

An administrator needs to capture a basic flow debug for traffic passing through FortiGate.

Which two commands are required to start the flow debug? (Choose two.)

**A.** diagnose debug flow trace start 100

**B.** diagnose debug enable

**C.** execute router restart

**D.** diagnose sniffer packet any "all" 4

**ANSWER: A B**

**Explanation:**

The command `diagnose debug flow trace start <count>` specifies how many packets or flow-trace entries FortiGate should capture. For example, `diagnose debug flow trace start 100` starts a trace limited to 100 entries.

The command `diagnose debug enable` activates debugging output. Without enabling debug output, FortiGate does not display the requested flow-trace information. Administrators can optionally configure flow filters before starting the trace to reduce output, and should disable debugging after collecting the required information. See the FortiGate Administration Guide for flow-debug troubleshooting commands.

## QUESTION NO: 5

Which two statements about HA session pickup are true? (Choose two.)

**A.** Session pickup can synchronize established TCP session state between HA members.

**B.** UDP and ICMP session synchronization requires session-pickup-connectionless.

**C.** Session pickup is supported only in active-active HA mode.

**D.** Session pickup eliminates the need for heartbeat interfaces.

**ANSWER: A B**

**Explanation:**

HA session pickup synchronizes session information from the primary FortiGate to the secondary FortiGate. When a failover occurs, the new primary can use this synchronized state to continue eligible established TCP sessions instead of requiring every connection to be created again.

TCP session pickup is enabled with the `session-pickup` setting. Connectionless protocols, such as UDP and ICMP, require the additional `session-pickup-connectionless` setting if their session state must also be synchronized. Session pickup can reduce interruption during failover, although the actual application experience also depends on the protocol and network environment. See the FortiGate Administration Guide for HA session synchronization information.

## QUESTION NO: 6

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

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

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

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

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

**ANSWER: A B**

**Explanation:**

NGFW profile-based mode uses traditional firewall-policy matching, including source and destination addresses, interfaces, schedules, and services. Security inspection capabilities are then enabled by attaching the appropriate security profiles to the individual firewall policy. Therefore, *NGFW profile-based mode supports applying applications and web filtering profiles in a firewall policy* is correct: Application Control and Web Filter are security-profile features that can be applied to policies operating in profile-based mode. This approach allows administrators to tailor security controls to the traffic handled by each policy.

*NGFW profile-based mode policies support both flow inspection and proxy inspection* is also correct. FortiGate supports both inspection methods in profile-based policy configurations. Flow-based inspection processes traffic as it passes through the device and is designed for efficiency, while proxy-based inspection can fully proxy supported traffic to enable deeper inspection behavior and features. The inspection mode can be selected as appropriate for the relevant policy and its security requirements. Fortinet documents the available inspection approaches in its inspection mode guide, and documents how security profiles are configured and applied in the security profiles documentation.

## QUESTION NO: 7

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.** DNS-based web filter and proxy-based web filter

**B.** Static URL filter, FortiGuard category filter, and advanced filters

**C.** FortiGuard category filter and rating filter

**D.** Static domain filter, SSL inspection filter, and external connectors filters

## ANSWER: B

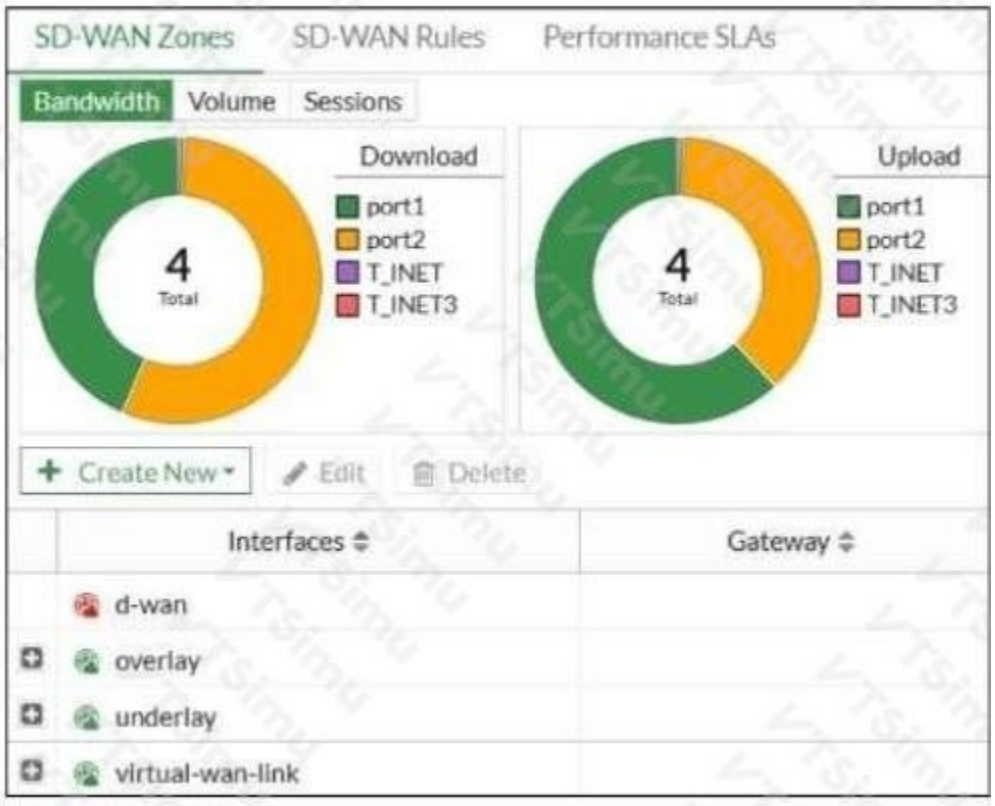
**Explanation:**

**Static URL filter, FortiGuard category filter, and advanced filters** is the required web-filter processing order for HTTP traffic. FortiGate first evaluates the static URL filter, which contains administrator-defined URL-pattern actions and therefore provides the most direct, explicit control over matching requests. It then performs FortiGuard category filtering, using FortiGuard's URL categorization information to apply the configured category actions. After those URL and category evaluations, FortiGate applies advanced web-filter capabilities. Safe Search enforcement is an advanced filter: for supported search engines, FortiGate modifies the HTTP request as needed to require the provider's safe-search behavior. Applying it after the core static and category filtering stages ensures that advanced request handling occurs within the documented web-filter inspection workflow. This sequence is relevant when more than one web-filter feature is enabled because the earlier URL and category decisions are processed before advanced filtering functions such as Safe Search, YouTube restrictions, and similar controls. Fortinet documents the web-filter feature set and its processing behavior in the FortiGate 7.6 Administration Guide. FortiGuard's categorization service, used during the category-filter stage, is described at FortiGuard Web Filtering.

## QUESTION NO: 8

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 d-wan zone cannot be deleted.

**B.** The underlay zone contains port1 and port2.

**C.** The d-wan zone contains no member.

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

**ANSWER: C**

**Explanation:**

The **d-wan zone contains no member** statement is correct. In the SD-WAN Zones view, FortiGate uses the zone status indicator to show whether a zone currently has member interfaces. The red indicator displayed for **d-wan** identifies it as an empty SD-WAN zone: the zone object has been created, but no SD-WAN member interface is assigned to it. A zone can therefore exist independently of its current membership and can later be selected when adding or moving an SD-WAN member interface.

SD-WAN zones are logical groupings of member interfaces that simplify policy, routing, and service-rule configuration. Administrators can create custom zones to separate links by function, provider, transport type, or traffic requirements. The default **virtual-wan-link** zone is also an SD-WAN zone, but the display status for each zone must be interpreted from the individual row rather than inferred from its name. Here, the status shown specifically for **d-wan** is the evidence that it has no members. Fortinet documents the creation and management of SD-WAN zones and the assignment of members in the SD-WAN zones section of the FortiGate Administration Guide. See also Fortinet's SD-WAN overview for the role of members and zones in SD-WAN configuration.

**QUESTION NO: 9**

Which two statements describe characteristics of automation stitches? (Choose two.)

**A.** Actions involve only devices included in the Security Fabric.

**B.** An automation stitch can have multiple triggers.

**C.** Multiple actions can run in parallel.

**D.** Triggers can involve external connectors.

**ANSWER: C D**

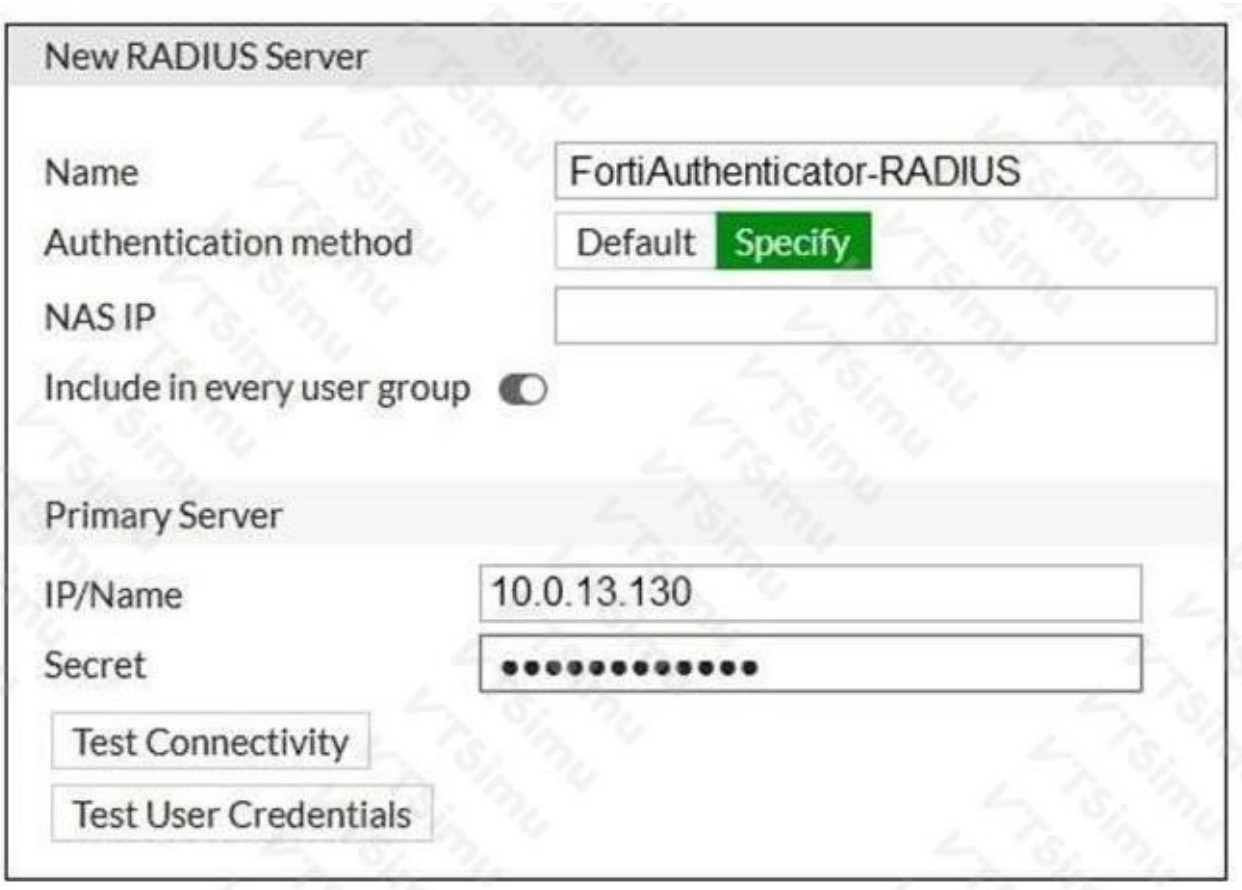
**Explanation:**

Automation stitches implement event-driven response workflows on FortiGate: a defined trigger starts one or more configured actions. **Multiple actions can run in parallel.** This lets an administrator associate several independent response tasks with the same event, such as sending a notification, creating a ticket through an integration, and applying a containment-oriented response. Parallel execution is useful when the outcome does not require one action to wait for another, helping FortiGate react promptly to security and operational events.

**Triggers can involve external connectors.** FortiGate automation integrates with Fabric connectors and other supported external services, allowing workflow initiation from connector-related events rather than limiting automation to locally generated events. This capability extends automated operations to connected cloud, collaboration, IT service-management, and Security Fabric environments. The trigger provides the event context, while the stitch coordinates the associated response actions. In practice, this enables organizations to combine FortiGate telemetry and integrated-service events in a consistent automated-response process, reducing manual intervention and improving response speed. Fortinet documents automation stitches, triggers, actions, and their configuration in the FortiGate Administration Guide.

**QUESTION NO: 10**

Refer to the exhibit, which contains a RADIUS server configuration.




An administrator added a configuration for a new RADIUS server.

While configuring, the administrator enabled Include in every user group.

What is the impact of enabling Include in every user group 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 the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

**C.** This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.

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

**ANSWER: A**

**Explanation:**

"This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group." is correct. The *Include in every user group* setting makes the configured remote RADIUS authentication source available to all FortiGate user groups. As a result, a user successfully authenticated by that RADIUS server can satisfy the authentication requirement of a firewall policy, SSL VPN portal rule, or other feature that references a FortiGate user group, without the administrator having to explicitly add that RADIUS server to each individual group.

This setting is useful when the same RADIUS identity store is intended to provide authentication consistently across all FortiGate group-based access controls. It affects FortiGate's association of the remote authentication server with its local user-group objects; it does not alter group membership stored on the RADIUS server itself. Administrators should use it only when that broad availability is intended, because FortiGate user groups often provide the basis for applying differentiated access policies. Fortinet documents RADIUS as a remote authentication-server type and describes how remote servers are used with firewall user groups in the FortiGate Administration Guide and the FortiGate CLI Reference for RADIUS.

## QUESTION NO: 11

A FortiGate has learned the same destination prefix through OSPF and through a static route.

The OSPF route has an administrative distance of 110, and the static route has an administrative distance of 10.

Which route does FortiGate install in the routing table?

**A.** The static route, because it has the lower administrative distance.

**B.** The OSPF route, because dynamic routes always take precedence over static routes.

**C.** The OSPF route, because it has a lower route priority.

**D.** Both routes, because FortiGate automatically installs them as ECMP routes.

**ANSWER: A**

**Explanation:**

The static route is installed because FortiGate selects the route with the lowest administrative distance when routes have the same destination prefix length. Administrative distance represents the trustworthiness of a route source. A static route has a default distance of 10, while OSPF routes have a default distance of 110.

After FortiGate selects the best route source by administrative distance, it can use route priority as an additional tie-breaker when applicable. Longest-prefix matching is performed first when routes have different prefix lengths. See the FortiGate Administration Guide for routing concepts and static-route configuration.

## QUESTION NO: 12

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad.

Which IPsec Wizard template must the administrator apply?

**A.** Hub-and-Spoke

**B.** Site to Site

**C.** Remote Access

**D.** Dial up User

**ANSWER: C**

**Explanation:**

The **Remote Access** template is the appropriate IPsec VPN Wizard choice for a sales employee travelling abroad. This template is designed for individual remote endpoint devices, such as a laptop running FortiClient, that must securely connect to resources behind a FortiGate from arbitrary and potentially changing Internet locations. The FortiGate is configured as the VPN gateway, while the employee's client initiates the IPsec connection when Internet access is available.

Remote-access deployments accommodate the realities of mobile users: the client commonly receives a dynamic public IP address, may connect through hotel, airport, or cellular networks, and needs authenticated access as a user rather than as an entire fixed branch network. The wizard builds the foundational configuration for this client-to-gateway scenario and supports the use of FortiClient as the remote IPsec peer. Fortinet documents Remote Access as one of the IPsec VPN Wizard templates specifically intended to create VPN connections for remote users. See the FortiGate 7.6 IPsec VPN Wizard documentation and the FortiClient IPsec VPN documentation.

## QUESTION NO: 13

An administrator enables central NAT on a FortiGate VDOM.

How should the administrator configure source NAT for IPv4 firewall policies in that VDOM?

**A.** Configure a central SNAT policy that matches the traffic.

**B.** Enable NAT in each matching IPv4 firewall policy.

**C.** Configure a VIP as the source address in the firewall policy.

**D.** Enable IP pools globally under system settings.

**ANSWER: A**

**Explanation:**

The administrator must configure a central SNAT policy. When central NAT is enabled, source NAT configuration is separated from the firewall policy. Firewall policies determine whether traffic is allowed, while central SNAT policies determine the source translation that FortiGate applies to matching traffic.

This model allows source NAT behavior to be managed independently of security policies and can simplify configurations where multiple firewall policies require the same translation behavior. The per-policy NAT setting is not used for source NAT when central NAT is enabled. Fortinet documents central SNAT configuration in the FortiGate Administration Guide.

## QUESTION NO: 14

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

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

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

**C.** Regular policy routes have precedence over SD-WAN rules.

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

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

**ANSWER: A C E**

**Explanation:**

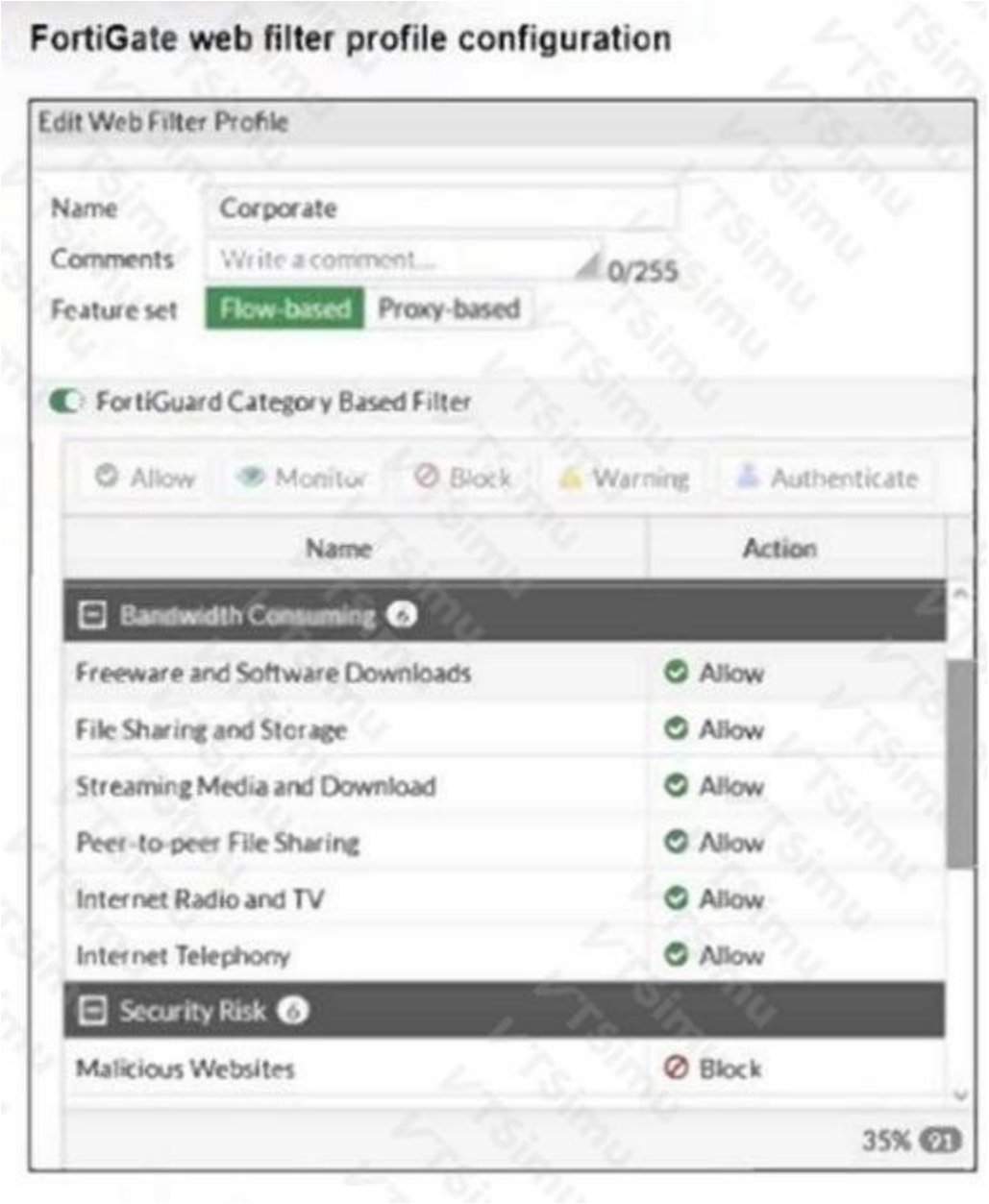
FortiGate SD-WAN steering operates within the overall routing decision process; it does not eliminate the requirement for a usable route. Therefore, “By default, SD-WAN rules are skipped if the included SD-WAN members do not have a valid route to the destination” is a key principle. For a rule to select an SD-WAN member, the member must be able to reach the destination according to the routing table. This ensures that SD-WAN does not steer traffic toward an unusable egress path.

“Regular policy routes have precedence over SD-WAN rules” is also correct. A matching policy route is processed before SD-WAN rule-based service steering, allowing explicitly configured policy-based forwarding to control the path for matching traffic.

Finally, “By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member” describes the default route lookup behavior. If the best matching route resolves through an interface outside the SD-WAN zone, FortiGate follows that normal routing result rather than applying SD-WAN rule processing. This behavior can be adjusted with SD-WAN configuration where appropriate, but it is the default routing principle. See the Fortinet SD-WAN rules documentation and policy routes documentation.

**QUESTION NO: 15**

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

respectively.

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

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

**D.** Set the Freeware and Software Downloads category Action to Warning.

**ANSWER: A B**

**Explanation:**

Configuring a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively, meets the requirement because URL filters are evaluated as specific website controls within the web filter profile. The Block action denies requests that match the configured domain pattern, while the category-based action for Freeware and Software Downloads can remain permissive for every other site assigned to that category. Using a wildcard-type entry also enables matching requests for the specified domain and relevant URL paths.

Configuring a web override rating for download.com and selecting Malicious Websites as the subcategory is also valid. A web rating override locally changes the FortiGuard category assigned to a particular URL or domain. If the web filter profile blocks the Malicious Websites category, FortiGate blocks download.com based on its overridden rating, without changing how the original Freeware and Software Downloads category is handled for other sites. This approach is useful when the administrator wants the exception managed through category-based filtering rather than through a URL-filter rule. Fortinet documents both URL filtering and local rating overrides as web-filter controls in the FortiGate administration documentation: URL filter and Web filter.