ExamsIndex
Practice Materials & Tests

DEMO VERSION

Fortinet

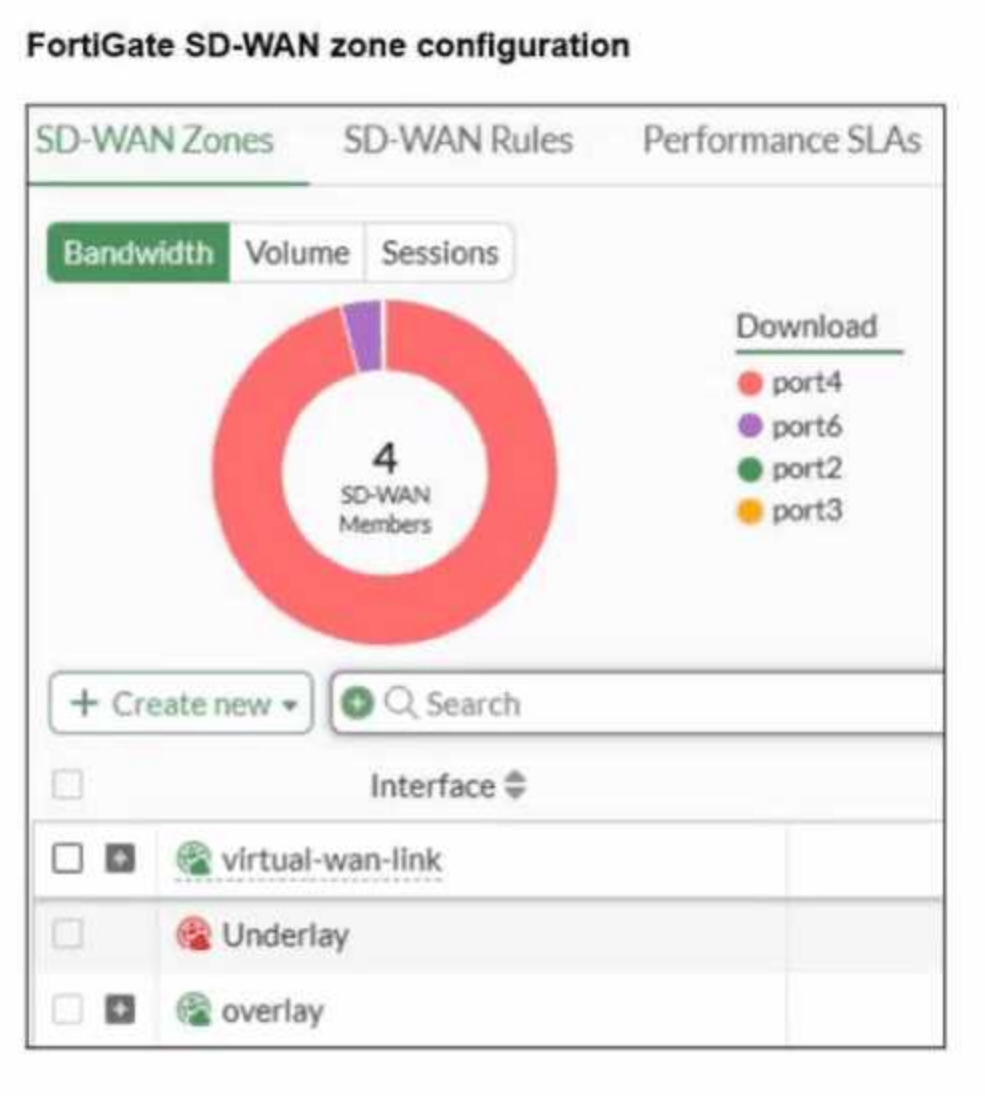
NSE4_FGT_AD-7.6 Exam

Fortinet NSE 4 - FortiOS 7.6 Administrator

Exam Latest Version: 6.1

Question 1. (Single Select)

Refer to the exhibit.



An SD-WAN zone configuration on the FortiGate GUI is shown. Based on the exhibit, which statement is true?

A: The Underlay zone contains no member.
B: The virtual-wan-link and overlay zones can be deleted
C: The Underlay zone is the zone by default.
D: port2 and port3 are not assigned to a zone.

Correct Answer: A

Explanation:

According to the FortiOS 7.6 Administrator Guide and the specific behavior of the SD-WAN GUI, here is the technical breakdown:

SD-WAN Zone Hierarchy and UI Elements: In the FortiGate GUI, SD-WAN zones that contain member interfaces are displayed with a plus (+) icon next to the checkbox. This icon allows administrators to expand the zone and view the specific physical or logical interfaces assigned to it.

Analysis of the "Underlay" Zone: In the provided exhibit, the virtual-wan-link and overlay zones both feature the plus (+) expansion icon, indicating they have active members. The Underlay zone, however, lacks this icon and displays a red status icon. This is the visual indicator in FortiOS that the zone is currently empty and contains no member interfaces.

Mandatory Zone Membership: In FortiOS 7.x, every SD-WAN member interface must be assigned to a zone. It is not possible for an interface to be an "SD-WAN member" (as shown in the legend with port2 and port3) without being assigned to a zone. Since port2 and port3 are listed in the legend, they are indeed assigned to one of the other expanded zones (likely virtual-wan-link or overlay), making Option D incorrect.

Default Zone Behavior: While FortiOS 7.6 often creates default zones like virtual-wan-link, underlay, and overlay during certain configuration wizards or by default in newer versions, they are distinct entities. There is no single "default" zone that acts as a global catch-all in the way Option C suggests.

Immutability of System Zones: While certain system-defined zones have restrictions, the primary focus of this specific exhibit is the current membership state, which clearly shows the Underlay zone is empty.

Question 2. (Multi Select)

Refer to the exhibit.

```
FortiGate # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract
\
Num. of servers : 1
Protocol        : https
Port            : 8888
Anycast         : Disable
Default servers : Not included

--=- Server List (Wed Sep 20 09:22:42 2023) -=-

IP                     Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost            Updated Time
10.0.1.241               -244      2 I        0                   122          0          0 Wed Sep 20 09:21:55 2023
```

Which two statements about the FortiGuard connection are true? (Choose two.)

A: The weight increases as the number of failed packets rises
B: You can configure unreliable protocols to communicate with FortiGuard Server.
C: FortiGate identified the FortiGuard Server using DNS lookup.
D: FortiGate is using the default port for FortiGuard communication.

Correct Answer: A, D

Explanation:

Based on the diagnose debug rating output provided in the exhibit and the standard behavior of the FortiGuard connection mechanism in FortiOS 7.6:

Weight Calculation (Statement A is True):

In FortiOS, the rating server selection process uses a weight-based system.

According to official documentation, the weight increases with failed packets (lost responses) and decreases with successful packets.

This mechanism ensures that servers with poor reliability are penalized by having higher weights, effectively pushing them to the bottom of the preference list.

Default Port Communication (Statement D is True):

The exhibit explicitly shows the communication is using HTTPS on port 8888.

In FortiOS 7.6 (and legacy versions like 6.2/6.4), FortiGuard filtering supports specific protocols and ports: HTTPS on ports 443, 53, and 8888, where 8888 is considered a default port for FortiGuard queries.

Ports 53 and 8888 are standard for both UDP and TCP/HTTPS FortiGuard communications to avoid common firewall blocks on standard web ports.

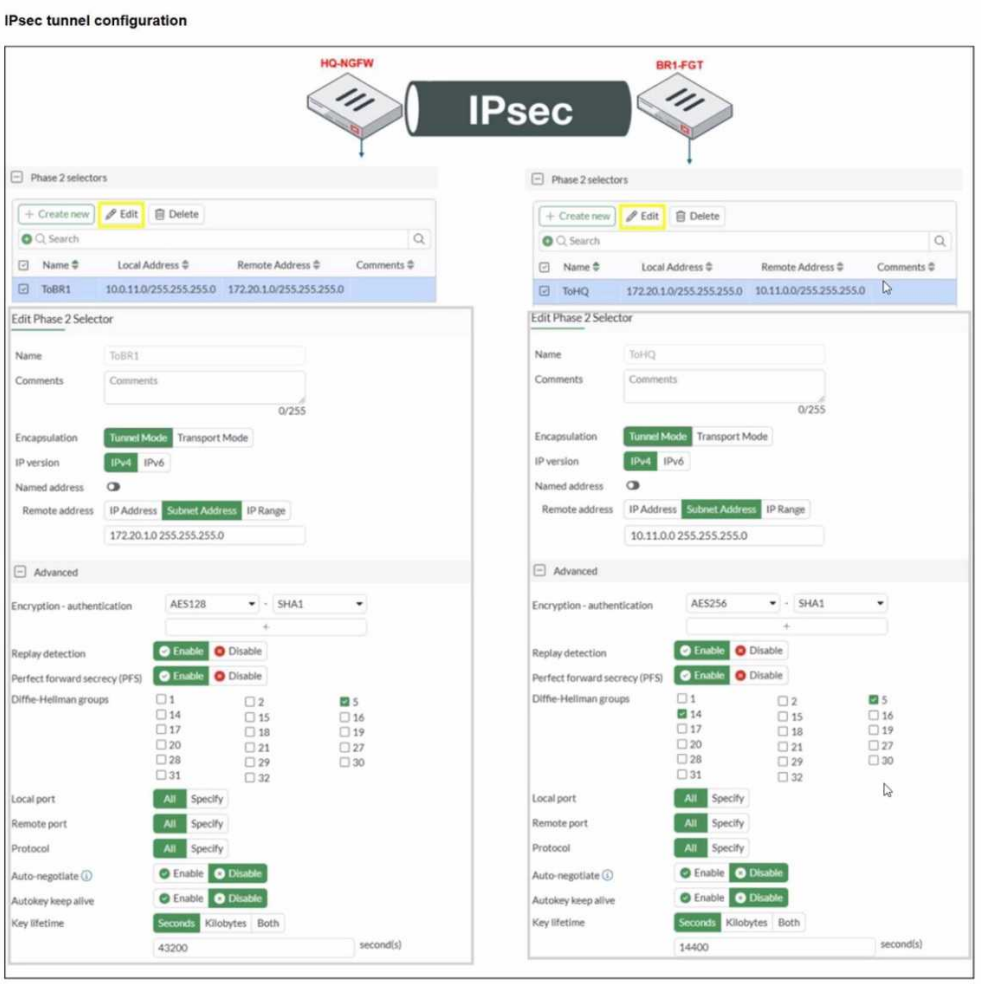
Why other options are incorrect:

Statement B (Unreliable protocols): While you can configure UDP (which is unreliable), the exhibit specifically shows HTTPS is being used, which is a reliable (TCP-based) protocol.

Statement C (DNS lookup): In the "Flags" column of the server list, a server found via DNS lookup would be marked with the "D" flag. The exhibit shows the flag as "I" (indicating the last INIT request was sent to this server) and a numeric "2," but the "D" flag is absent. Additionally, the IP 10.0.1.241 is a private address, suggesting it is a manually configured FortiManager or local override server rather than a public server found via global DNS lookup.

Question 3. (Multi Select)

Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up. Based on the phase 2 configuration shown in the exhibit, which two configuration changes will bring phase 2 up? (Choose two.)

A: On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0.
B: On HQ-NGFW. enable Diffie-Hellman Group 2.
C: On BR1-FGT. set Seconds to 43200
D: On HQ-NGFW. set Encryption to AES256.

Correct Answer: A, D

Explanation:

Phase 1 being up confirms the two FortiGate devices can authenticate and build the IKE SA. Phase 2 failing indicates the IPsec (Quick Mode) SA negotiation is failing due to mismatched Phase 2 parameters.

From the exhibit, the Phase 2 mismatches that would prevent SA establishment are:

1) Phase 2 selectors must mirror each other (Proxy IDs)

HQ-NGFW Phase 2 selector shows:

Local: 10.0.11.0/24

Remote: 172.20.1.0/24

BR1-FGT Phase 2 selector shows:

Local: 172.20.1.0/24

Remote: 10.11.0.0/24 'õ does not match HQ’s local subnet (10.0.

In FortiOS, Phase 2 comes up only when the peers’ selectors (proxy IDs) match as opposite pairs (local on one side = remote on the other).

' Fix: A. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.

2) Phase 2 proposal must match (encryption/authentication)

HQ-NGFW shows encryption AES128 (with SHA1)

BR1-FGT shows encryption AES256 (with SHA1)

For Phase 2 to establish, both peers must have at least one common proposal (same encryption and authentication settings). With one side set to AES128 and the other to AES256, there is no match.

' Fix: D. On HQ-NGFW, set Encryption to AES256.

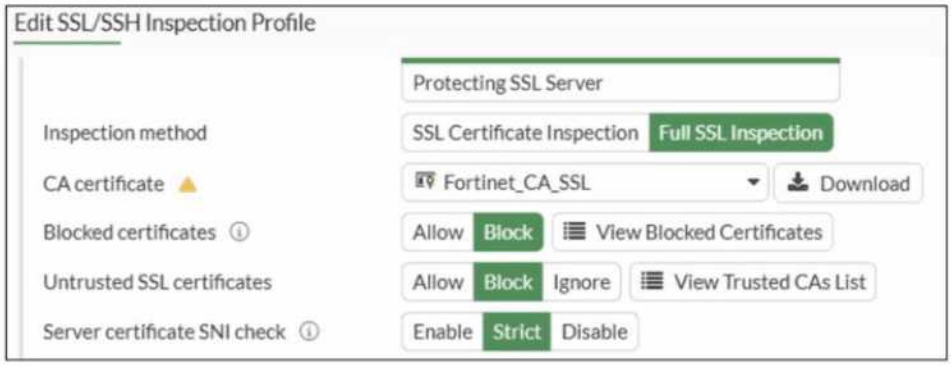
Why the other options are not correct

B . Enable Diffie-Hellman Group 2: The exhibit's mismatch is not resolved by adding DH group 2, and DH group must match when PFS is enabled. This option does not align the peers based on what's shown.

C . Set Seconds to 43200: Phase 2 lifetime mismatches typically do not prevent Phase 2 from coming up (the negotiated lifetime can be adjusted by the peers). The hard blockers here are the selectors and proposal mismatch.

Question 4. (Single Select)

Refer to the exhibit.



What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?

A: FortiGate will accept and use the CN in the server certificate for URL filtering if the SNI does not match the CN or SAN fields.

B: FortiGate will accept the connection with a warning if the SNI does not match the CN or SAN fields.
C: FortiGate will close the connection if the SNI does not match the CN or SAN fields.
D: FortiGate will close the connection if the SNI does not match the CN and SAN fields

Correct Answer: C

Explanation:

Based on the exhibit and the FortiOS 7.6 SSL/SSH Inspection documentation, the correct answer is C.

Understanding the Exhibit Configuration

In the SSL/SSH Inspection Profile, the following settings are shown:

Inspection method: Full SSL Inspection

Server certificate SNI check: Strict

This setting directly controls how FortiGate validates the Server Name Indication (SNI) provided by the client during the TLS handshake.

FortiOS 7.6 Behavior of “Server certificate SNI check”

FortiOS supports three modes for Server certificate SNI check:

Disable

No validation between SNI and server certificate.

Enable

FortiGate checks SNI against the certificate.

If mismatch occurs, FortiGate may still allow the session with reduced validation.

Strict

FortiGate enforces a strict match.

The SNI must match either the CN (Common Name) or one of the SAN (Subject Alternative Name) entries in the server certificate.

If the SNI does not match either CN or SAN, the TLS session is immediately terminated.

The exhibit clearly shows Strict selected.

Why Option C is Correct

With Strict enabled, FortiGate rejects the TLS connection when:

The SNI does not match the CN, and

The SNI does not match any SAN entry

This results in the connection being closed, not allowed with warnings or fallback behavior.

Therefore:

C . FortiGate will close the connection if the SNI does not match the CN or SAN fields is exactly the documented behavior.

Why the Other Options Are Incorrect

A: FortiGate does not fall back to using the CN for URL filtering when Strict is enabled.

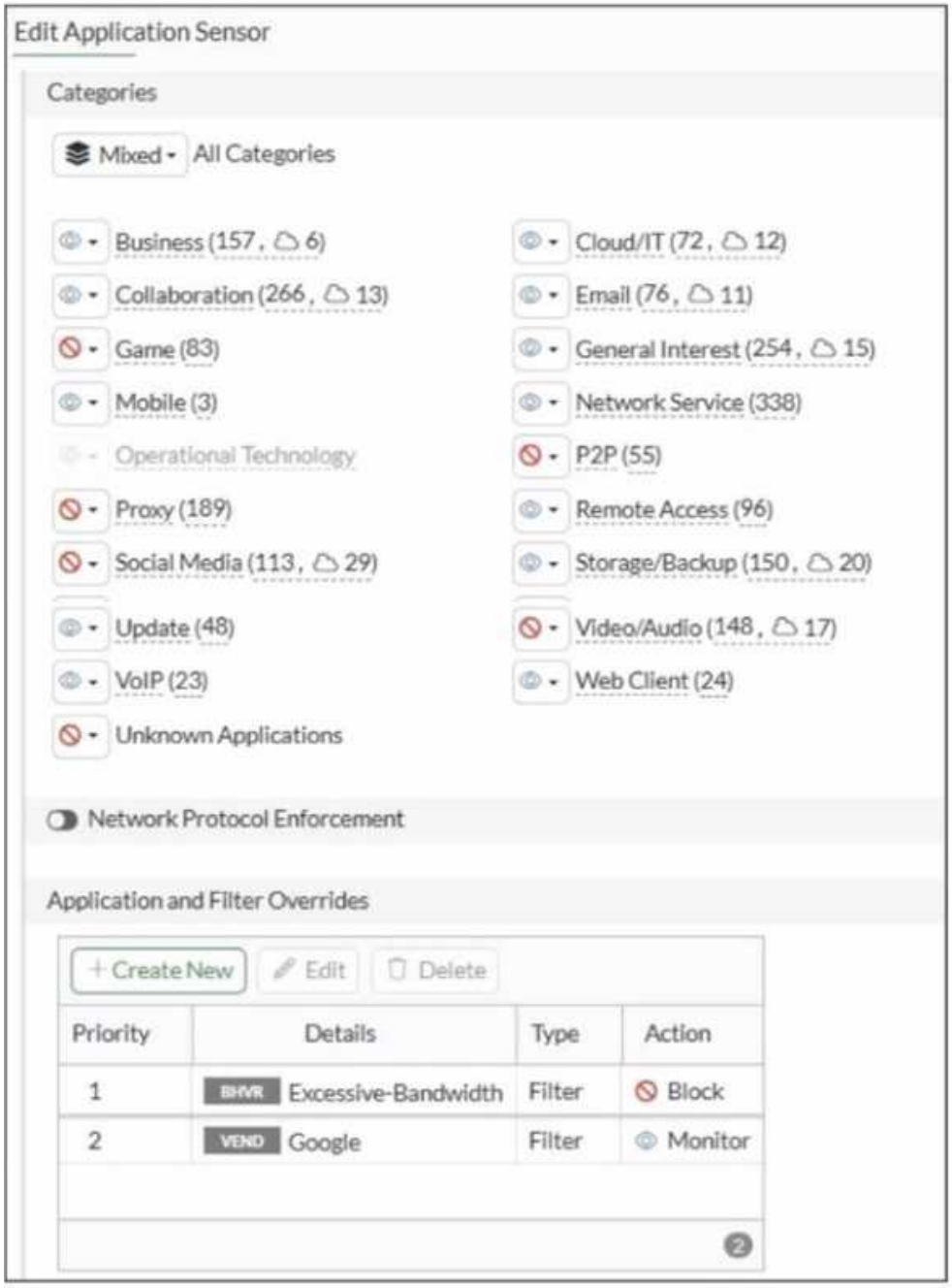
B: There is no “accept with warning” behavior in Strict mode.

D: Incorrect logical condition. FortiGate does not require mismatch with both CN and SAN simultaneously; a mismatch with either valid field set is sufficient to close the connection.

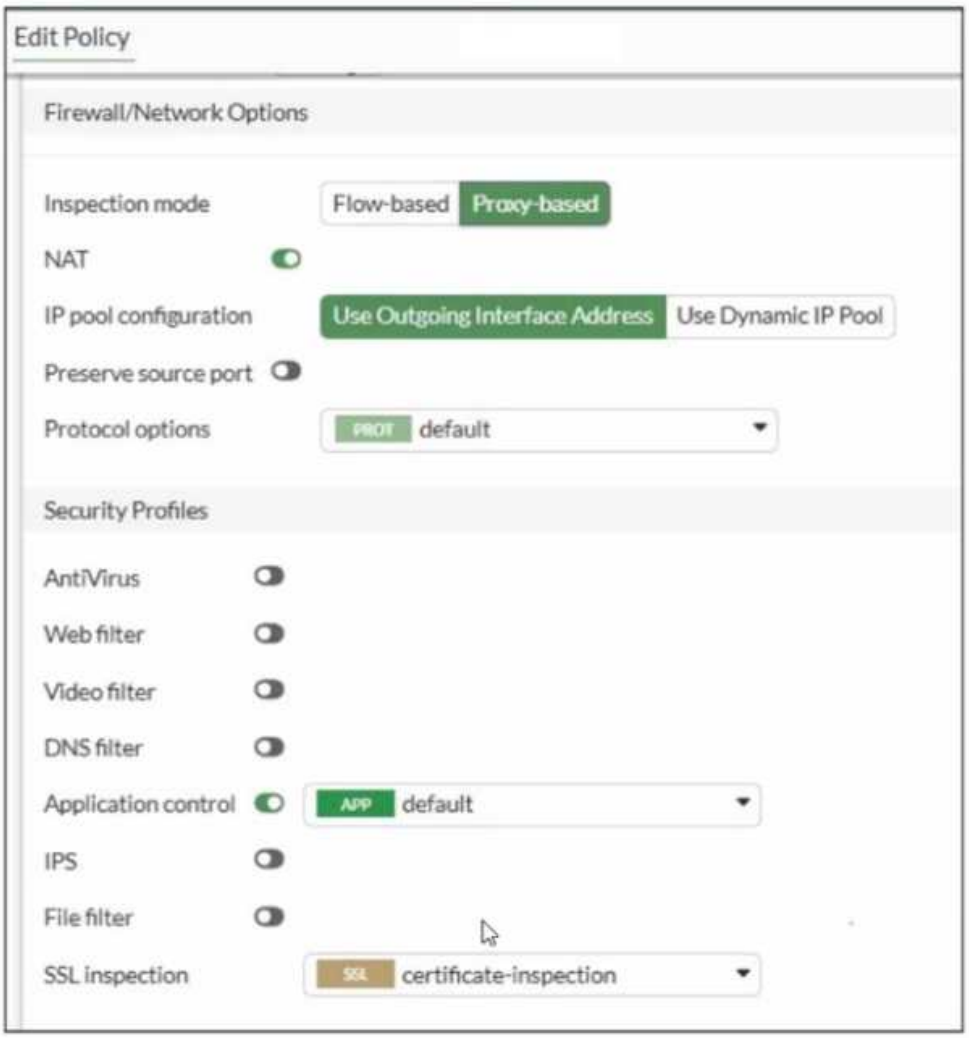
Question 5. (Multi Select)

Refer to the exhibits.

Application sensor



Firewall policy



You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access www.fortinet.com. Which two actions would you take to resolve the issue? (Choose two.)

A: Set SSL inspection to deep-content inspection.
B: Move up Google in the Application and Filter Overrides section to set its priority lot
C: Add "Google".com to the URL category in the security profile.
D: Change the Inspection mode to Flow-based
E: Set the action for Google in the Application and Filter Overrides section to Allow

Correct Answer: B, E

Explanation:

From the exhibits:

The firewall policy has Application Control enabled and uses certificate-inspection for SSL inspection.

The application sensor has Application and Filter Overrides with the following order (priority):

Excessive-Bandwidth with action Block

Google (vendor filter) with action Monitor

In FortiOS, Application and Filter Overrides are evaluated by priority (top-down). The first matching override is applied. If traffic matches an earlier override with Block, it will be blocked even if a later override would Monitor/Allow it.

Why Google apps fail while www.fortinet.com works:

Many Google applications can be detected as (or can trigger) the Excessive-Bandwidth behavior/signature depending on the specific service and traffic pattern.

Because Excessive-Bandwidth (Block) is above Google (Monitor), Google-related traffic may match the first rule and be blocked before the Google override is evaluated.

Access to www.fortinet.com works because that traffic is not matching the Excessive-Bandwidth override.

Therefore, to resolve:

B . Move up Google in the Application and Filter Overrides section to set its priority higher

This ensures Google matches the Google override before any broader blocking override is applied.

E . Set the action for Google in the Application and Filter Overrides section to Allow

This explicitly permits Google applications once the higher-priority match occurs (stronger than Monitor for troubleshooting and ensuring access).

Why the other options are not the best fit here:

A (deep-content inspection) can help identify more HTTPS applications, but the exhibit already shows a specific Google override configured; the immediate issue is the override evaluation order and action.

C relates to Web Filter URL categories, but the problem is occurring under Application Control behavior/vendor overrides.

D (flow-based) is not required to fix an override priority/action conflict.

ExamsIndex

Demo PDF Complete

Your NSE4_FGT_AD-7.6 Demo (5 Questions)