Fortinet.NSE4_FGT_AD-7.6.v2026-05-11.q39

Exam Code:	NSE4_FGT_AD-7.6
Exam Name:	Fortinet NSE 4 - FortiOS 7.6 Administrator
Certification Provider:	Fortinet
Free Question Number:	39
Version:	v2026-05-11
# of views:	122
# of Questions views:	390
https://www.freepdfdumps.com/Fortinet.NSE4_FGT_AD-7.6.v2026-05-11.q39.html	

NEW QUESTION: 1
You have configured an application control profile, set peer-o-peer traffic to Block under the Categories tab, and applied it to the firewall policy. However, you peer-to-peer traffic on known ports is passing through the FortiGate without being blocked. What FortiGate settings should you check to resolve this issue?
A. Replacement Messages for UDP-based Applications
B. Network Protocol Enforcement
C. Application and Filter Overrides
D. FortiGuard category ratings
Answer: C (LEAVE A REPLY)
"After the IPS engine examines the traffic stream for a signature match, FortiGate scans packets for matches, in this order, for the application control profile:
1. Application and filter overrides..."
"Because application overrides are applied first in the scan, these two applications are allowed and generate logs."
"The priority in which application and filter overrides are placed takes precedence." Technical Deep Dive:
The correct answer is C. Application and Filter Overrides.
If you already set the P2P category to Block, but some peer-to-peer traffic is still being allowed, the first thing to check is whether there is an application override or filter override that matches that traffic before the category action is applied. FortiGate processes Application and Filter Overrides before Categories, so any matching override set to Allow or Monitor will effectively bypass the category block.
Why the others are wrong:
A only affects user-facing block-page behavior for HTTP/HTTPS applications, not whether P2P is blocked.

B is for enforcing expected services on expected ports and for blocking applications on non-default ports. It is not the first place to look when a category block is being bypassed.
D concerns web categorization, not application-control category enforcement.
Operationally, this is a classic troubleshooting sequence: first inspect the override table, then the category action, then logs under Application Control to see which signature and action actually matched.

NEW QUESTION: 2
Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two answers)
A. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.
B. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
C. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP.
D. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.
Answer: A,D (LEAVE A REPLY)
"If SD-WAN is disabled, you can change the ECMP load balancing algorithm on the FortiGate CLI using the commands shown on this slide."
"When SD-WAN is enabled, FortiOS hides the v4-ecmp-mode setting and replaces it with the load-balance-mode setting under config system sdwan. That is, when you enable SD-WAN, you control the ECMP algorithm with the load-balance-mode setting."
"There are some differences between the two settings. The main difference is that load-balance-mode supports the volume algorithm, and v4-ecmp-mode does not."
"These routes are called equal cost multipath (ECMP) routes..."
Technical Deep Dive:
The correct answers are A and D.
A is correct because when SD-WAN is enabled, FortiOS no longer uses v4-ecmp-mode; it uses load-balance-mode under config system sdwan. That is the explicit SD-WAN control point for ECMP behavior.
D is correct because when SD-WAN is disabled, ECMP configuration is done in the regular system routing settings, not under SD-WAN. The study guide states that you change the ECMP algorithm on the FortiGate CLI when SD-WAN is disabled, which corresponds to the classic config system settings ECMP controls.
Why the others are wrong:
B is wrong because the guide explicitly says load-balance-mode supports volume, while v4-ecmp-mode does not. So you cannot set v4-ecmp-mode to volume-based.
C is wrong because ECMP requires equal-cost routes. If distance or priority differ, they are no longer ECMP candidates; FortiGate selects the preferred route instead. The concept of ECMP itself requires equal route cost attributes.
From an implementation standpoint, the common CLI patterns are:

config system settings
set v4-ecmp-mode source-ip-based
end
and, with SD-WAN enabled:
config system sdwan
set load-balance-mode source-ip-based
end
On hardware platforms, ECMP still affects session distribution at the routing decision stage before later security services are applied. NP offload can accelerate forwarding after route selection, but the ECMP decision itself is a FortiOS control-plane routing function.

NEW QUESTION: 3
Refer to the exhibits.

The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.
Based on the system performance output, what are the two possible outcomes? (Choose two.)
A. FortiGate drops new sessions.
B. Administrators can access FortiGate only through the console port.
C. Administrators can change the configuration.
D. FortiGate has entered conserve mode.
Answer: A,D (LEAVE A REPLY)
"Three different configurable thresholds define when FortiGate enters and exits conserve mode. If memory usage goes above the percentage of total RAM defined as the red threshold, FortiGate enters conserve mode."
"If memory usage keeps increasing, it might exceed the extreme threshold. While memory usage is above this highest threshold, all new sessions are dropped."

"What actions does FortiGate take to preserve memory while in conserve mode?
* FortiGate does not accept configuration changes, because they might increase memory usage."
"However, if the memory usage exceeds the extreme threshold, new sessions are always dropped, regardless of the FortiGate configuration." Technical Deep Dive:
The system performance output shows Memory: 2042076k total, 1837868k used (90%). The configured thresholds shown are:
green = 82
red = 88
extreme = 89
Because memory usage is 90%, it is:
Above the red threshold (88%) → so FortiGate has entered conserve mode
Above the extreme threshold (89%) → so all new sessions are dropped
That makes A and D correct.
Why the others are wrong:
B is not stated anywhere in the study guide as an automatic outcome of conserve mode.
C is the opposite of what the guide says. In conserve mode, FortiGate does not accept configuration changes.
A useful verification command is:
diagnose hardware sysinfo conserve
Operationally, once a FortiGate crosses the red threshold, it starts protecting itself by limiting behavior that could increase memory usage. Once it crosses the extreme threshold, it becomes more severe and drops new sessions to keep the system from becoming unstable.

NEW QUESTION: 4
Refer to the exhibit.

Refer to the exhibit.

Packet trace output

Time	Message
Packet Trace #1 14	
06:39:29	vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0 from port4. type=8, code=0, id=3, seq=168.
06:39:29	allocate a new session-00000ec6
06:39:29	in-[port4], out-[]
06:39:29	len=0
06:39:29	result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000
06:39:29	find a route: flag=00000000 gw-0.0.0.0 via port2
06:39:29	in-[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
06:39:29	gnum-100004, use addr/intf hash, len=1
06:39:29	check-gnum-100004 policy-0, ret-matched, act-accept
06:39:29	ret-matched
06:39:29	policy-0 is matched, act-drop
06:39:29	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
06:39:29	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
06:39:29	Denied by forward policy check (policy 0)

Why did the FortiGate device drop the packet?

A. It matched the default implicit firewall policy.

B. It failed the RPF check.

C. It matched an explicitly configured firewall policy with the action DENY.

D. It cannot reach the next-hop IP.

Answer: A (LEAVE A REPLY)

"FortiGate looks for the matching firewall policy from top-to-bottom and, if a match is found, the traffic is processed based on the firewall policy. If no match is found, the traffic is dropped by the default implicit deny firewall policy." Technical Deep Dive:

The debug flow output clearly points to the implicit deny:

ret-no-match

policy-0 is matched, act-drop

Denied by forward policy check (policy 0)

On FortiGate, policy 0 is the internal representation of the default implicit deny firewall policy. That means the packet did not match any user-defined forward firewall policy, so FortiGate dropped it automatically.

Why the other options are wrong:

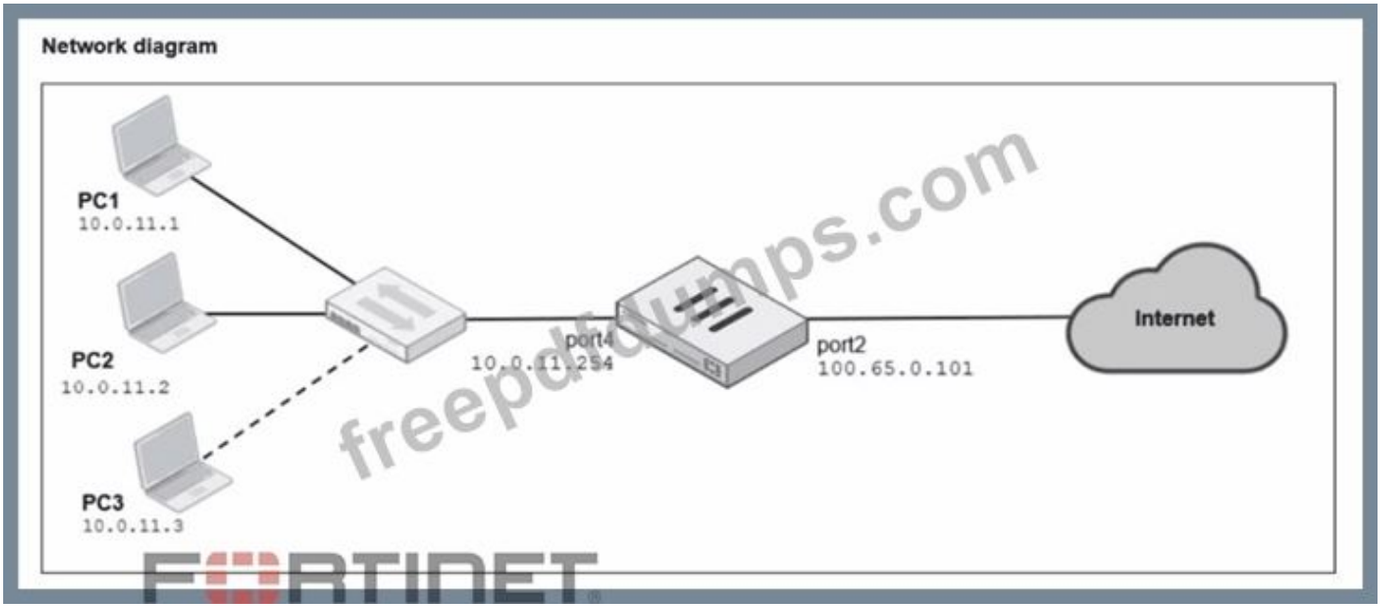
B is wrong because an RPF failure would show a reverse-path-related drop reason, not Denied by forward policy check (policy 0).

C is wrong because the trace does not show a matched explicit policy ID with deny action; it shows policy 0, which is the implicit rule.
D is wrong because the trace actually shows a route lookup result: find a route: ... gw-0.0.0.0 via port2. So this is not a next-hop reachability failure.
In packet-flow troubleshooting, this pattern is one of the most important to recognize. If you see policy 0 in FortiGate debug flow, the first things to verify are:
diagnose debug flow filter addr <src_or_dst_ip>
diagnose debug flow show function-name enable
diagnose debug enable
Then review whether a firewall policy exists with the correct incoming interface, outgoing interface, source, destination, schedule, and service. If any one of those does not match, FortiGate falls through to policy 0 and drops the session.

NEW QUESTION: 5
An administrator wanted to configure an IPS sensor to block traffic that triggers the signature set number of times during a specific time period. How can the administrator achieve the objective?
A. Use IPS group signatures, set rate-mode 60.
B. Use IPS packet logging option with periodical filter option.
C. Use IPS signatures, rate-mode periodical option.
D. Use IPS filter, rate-mode periodical option.
Answer: C (LEAVE A REPLY)
"Rate-based IPS signatures also allows you to detect anomalies, which are unusual behaviors in the network..."
"There are two ways to add predefined signatures to an IPS sensor. One way is to select the signatures individually... The second way to add a signature to a sensor is using filters."
"You can also add rate-based signatures to block specific traffic when the threshold is exceeded. On the CLI, If you set the command rate-mode to periodical, FortiGate triggers the action when the threshold is reached during the configured Duration time period." Technical Deep Dive:
The correct answer is C. Use IPS signatures, rate-mode periodical option.
The guide is explicit that this behavior belongs to rate-based IPS signatures. The question asks for blocking traffic when a signature is triggered a certain number of times within a defined interval. That is exactly what rate-mode periodical does: it evaluates the trigger count over the configured duration window and then applies the configured IPS action when the threshold is met.
Why the other options are wrong:
A is wrong because rate-mode 60 is not the documented syntax or method.
B is wrong because packet logging records packets; it does not implement threshold-based blocking logic.
D is wrong because the guide ties rate-mode periodical to rate-based signatures, not to IPS filters as the mechanism for this threshold behavior.
Operationally, this is used for anomaly-style detection, similar in concept to lightweight rate-based protection. A typical CLI pattern is along these lines:

config ips sensor
edit "custom-ips"
config entries
edit 1
set rule <signature_id>
set rate-mode periodical
set rate-count <threshold>
set rate-duration <seconds>
set action block
next
end
next
end
This works best when applied only to relevant protocols and signatures, because broad use of rate-based signatures can consume more resources and increase false-positive risk.

NEW QUESTION: 6
Refer to the exhibits.



Dynamic IP pool

A diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device are shown.

Two PCs. PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.
Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)
A. In the system settings, set Multiple Interface Policies to enable.
B. in the IP pool configuration, set end ipto 100.65.0.112.
C. In the firewall policy, set match-vip to enable using CLI.
D. In the IP pool configuration, set type to overload.
Answer: (SHOW ANSWER)
From the exhibits:
The firewall policy has NAT enabled and is configured to Use Dynamic IP Pool.
The selected IP pool (Internet-pool) is configured as:
Type: One-to-One
External IP Range: 100.65.0.110-100.65.0.111 (only two public IPs)
PC1 and PC2 can access the internet because each one-to-one NAT mapping consumes one public IP from the pool. When PC3 is added, there is no third public IP available in the pool, so FortiGate cannot allocate a one-to-one mapping for PC3 and the session fails.
FortiOS behavior here is standard: with one-to-one IP pools, the available pool size limits how many distinct internal sources can be translated concurrently (depending on allocation and sessions), and a pool with only two IPs will not reliably support three separate hosts needing translations.
Therefore, the administrator can fix this in two valid ways:
B . In the IP pool configuration, set end ip to 100.65.0.112.
This expands the pool by adding an additional public IP address, making three public IPs available (.110, .111, .112), so PC3 can be assigned an address for one-to-one NAT.
D . In the IP pool configuration, set type to overload.
Changing the pool type to overload enables PAT (many-to-one), allowing multiple internal hosts (PC1, PC2, PC3) to share the pool address(es) using different source ports. This removes the "one public IP per internal host" limitation inherent to one-to-one pools.
Why the other options are not correct:
A . Multiple Interface Policies is unrelated to IP pool exhaustion and does not solve NAT allocation limits.
C . match-vip affects VIP matching behavior for destination NAT/virtual IP usage and does not address the source NAT pool shortage causing PC3 to fail.

NEW QUESTION: 7
A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded. The administrator confirms that the

traffic matches the configured firewall policy. What are two reasons for the failed virus detection by FortiGate? (Choose two answers)

A. The selected SSL inspection profile has certificate inspection enabled.

B. The website is exempted from SSL inspection.

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

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

Answer: A,B (LEAVE A REPLY)

"The only security features you can apply using SSL certificate inspection mode are web filtering and application control... certificate inspection does not allow FortiGate to inspect the flow of encrypted data."

"For antivirus or IPS control, you should use a deep-inspection profile."

"Within the full SSL inspection profile, you can also specify which SSL sites, if any, you want to exempt from SSL inspection." Technical Deep Dive:

The correct answers are A and B.

A is correct because if the firewall policy uses certificate inspection, FortiGate can inspect certificate/SNI metadata only. It cannot decrypt the HTTPS payload, so the antivirus engine never sees the EICAR file contents. That means HTTPS malware scanning fails even though HTTP scanning works.

B is also correct because if the destination site is exempt from SSL inspection, FortiGate intentionally skips decryption for that HTTPS session. Again, no payload decryption means no antivirus content scan.

Why the others are wrong:

C is not the likely reason here, especially for EICAR, which is a very small test file.

D would usually cause browser certificate warnings or connection issues during deep inspection, not a clean download that bypasses AV inspection.

Operationally, HTTPS antivirus requires this chain to be true:

firewall policy match → SSL deep inspection active → site not exempted → AV profile applied.

If either certificate-inspection is used or the site is exempted, FortiGate cannot inspect the encrypted file body.

NEW QUESTION: 8

When configuring firewall policies which of the following is true regarding the policy ID? (Choose two.)

A. A firewall policy ID identifies the order of policy execution in firewall policies.

B. A policy ID cannot be modified once a policy is created.

C. You can create a policy in CLI with policy ID 0

D. It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.

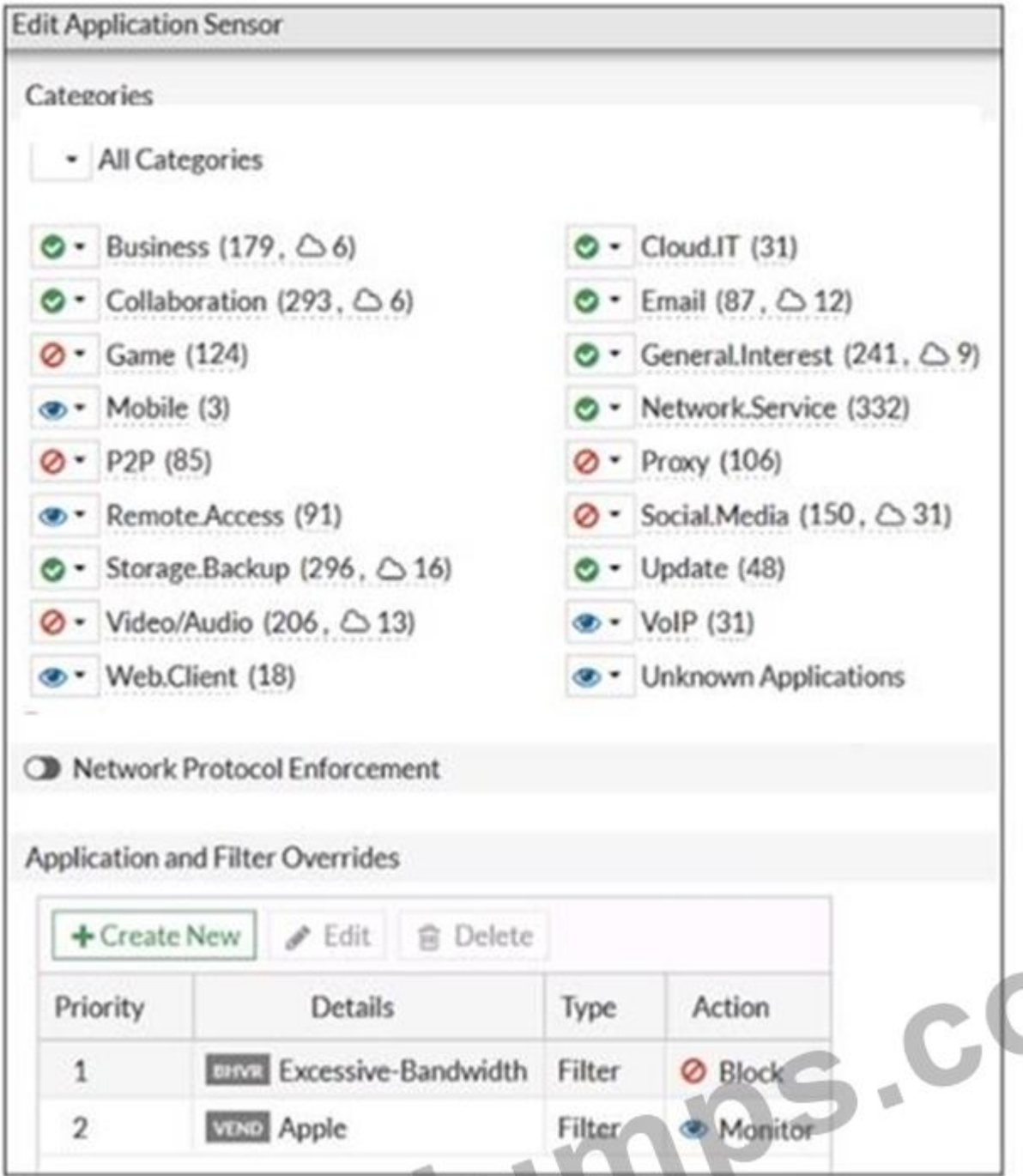
Answer: (SHOW ANSWER)

According to the FortiOS 7.6 Administration Guide, the firewall policy ID is a unique numerical identifier assigned to each policy for internal database tracking and management purposes. It is important to distinguish the policy ID from the policy sequence. While the FortiGate processes

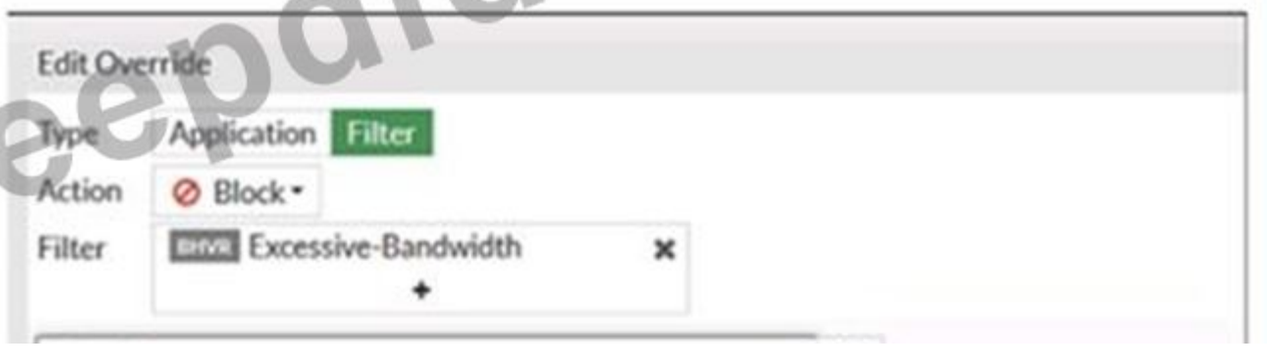
traffic based on a top-down approach (the sequence), the policy ID itself does not determine the order of execution (Statement A is incorrect).
In FortiOS, once a policy is committed to the configuration, the policy ID cannot be modified (Statement B). If an administrator needs to change a policy ID, they must either delete and recreate the policy or use the clone command in the CLI to copy the settings to a new ID.
Furthermore, the CLI provides a specific shortcut for policy creation: you can create a policy with ID 0 (Statement C). When the command edit 0 is used within the config firewall policy context, the FortiOS kernel automatically assigns the next available integer as the policy ID. This is a standard practice for efficient configuration via the command line. Statement D is incorrect because, while every policy must have an ID, the GUI automatically generates this value without requiring the user to manually provide or even see it during the initial creation process.

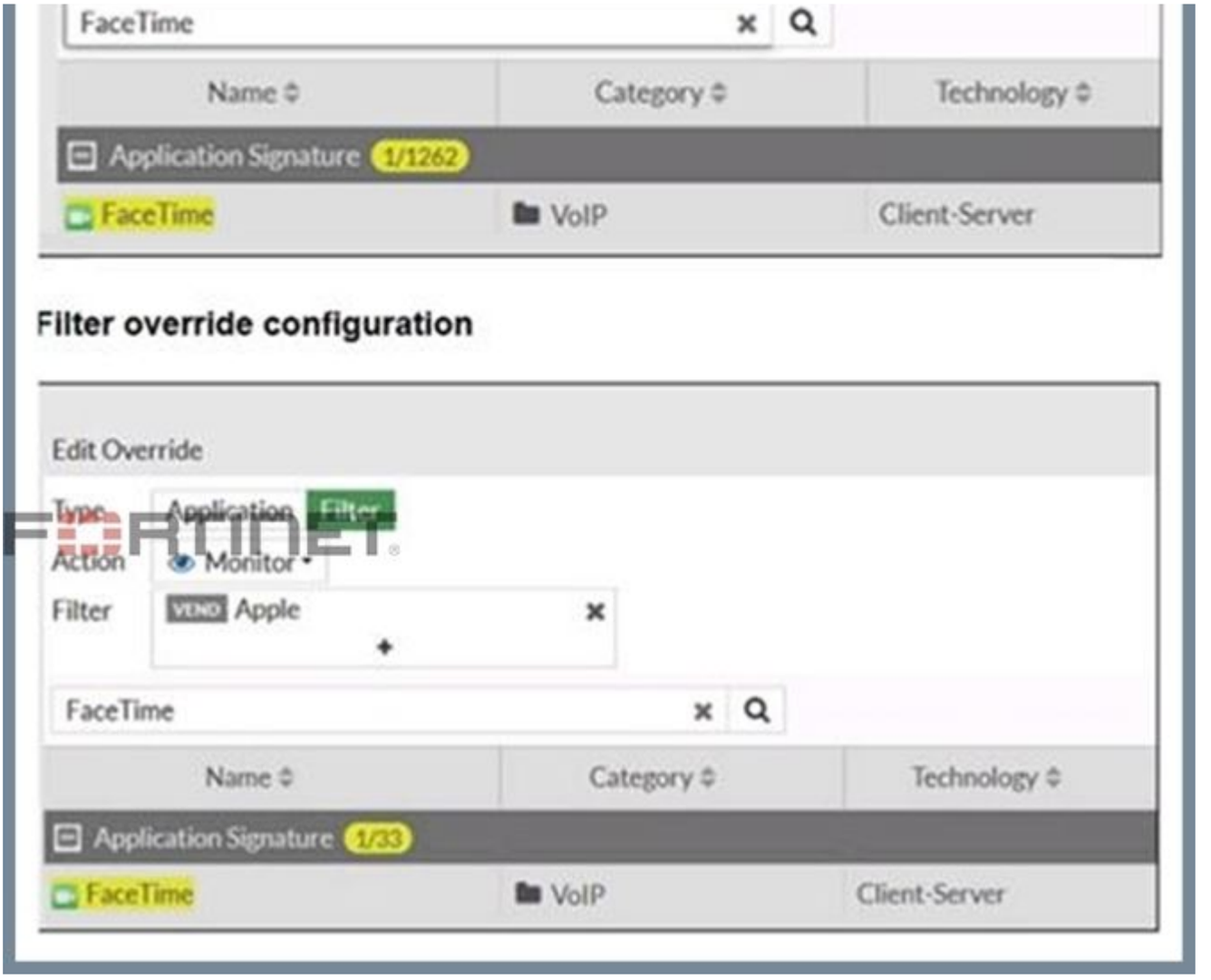
NEW QUESTION: 9
Refer to the exhibits.

Application sensor configuration



Application override configuration





The exhibits show the application sensor configuration and the Excessive-Bandwidth and Apple filter details. Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming? (Choose one answer)

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

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

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

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

Answer: (SHOW ANSWER)

According to the FortiOS 7.6 Administrator Study Guide, the Application Control engine processes traffic by evaluating the Application and Filter Overrides section first, using a top-down matching logic similar to firewall policies. In the provided exhibit, there are two override entries:
Priority 1: A behavior-based filter for Excessive-Bandwidth with the action set to Block.
Priority 2: A vendor-based filter for Apple with the action set to Monitor.
The exhibit titled "Application override configuration" explicitly shows that Apple FaceTime is one of the signatures included within the Excessive-Bandwidth behavior filter. When the FortiGate inspects FaceTime traffic, it matches the first entry (Priority 1) because the signature belongs to the "Excessive-Bandwidth" group. Since the action for this priority is Block, the traffic is dropped

immediately.
The phrase "only a few calls" is a common exam distractor; in this context, the "Excessive-Bandwidth" filter refers to the classification of the application (as one that typically consumes high bandwidth) rather than a real-time measurement of the specific session's throughput. Because the engine stops searching once a match is found in the overrides, it never reaches the Priority 2 "Monitor" rule or the general Category settings.

NEW QUESTION: 10
What are two features of collector agent advanced mode? (Choose two.)
A. In advanced mode, security profiles can be applied only to user groups, not individual users.
B. In advanced mode. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
C. Advanced mode uses the Windows convention-NetBios: Domain\Username.
D. Advanced mode supports nested or inherited groups.
Answer: B,D (LEAVE A REPLY)
"Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups." "In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent." Collector Agent Advanced Mode provides deeper integration between FortiGate, LDAP, and Active Directory, compared to standard mode.
Key features of Collector Agent Advanced Mode
B). FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
Correct
In advanced mode:
FortiGate directly queries LDAP/AD
User group filters are configured on FortiGate, not only on the Collector Agent This allows more flexible and scalable user/group-based policies D). Advanced mode supports nested or inherited groups.
Correct
Advanced mode supports:
Nested AD groups
Inherited group memberships
This is one of the primary reasons advanced mode is used in complex AD environments Why the other options are incorrect A). Security profiles only to user groups Incorrect.
Security profiles can be applied to users or groups, depending on policy configuration.
C). Uses NetBIOS Domain\Username format
Incorrect.
NetBIOS naming is associated with standard mode
Advanced mode typically uses LDAP DN-based identification

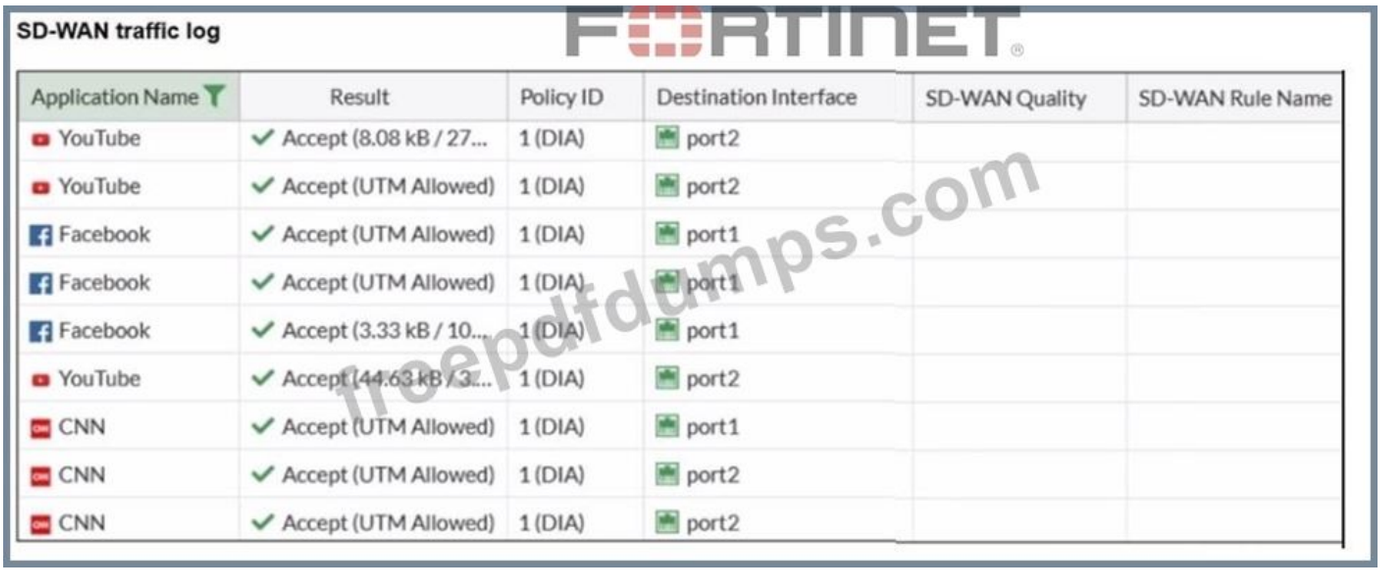
NEW QUESTION: 11
You have configured the FortiGate device for FSSO. A user is successful in log-in to Windows, but their access to the internet is denied. What should the administrator check first? (Choose one answer)
A. Whether the user is assigned to the correct AD group.
B. The FortiGate firewall policy settings for SSL decryption.
C. The FortiGate FSSO active users list for user's IP address.
D. The Windows event viewer for failed login attempts.
Answer: C (LEAVE A REPLY)
"FSSO is a software agent that enables FortiGate to identify network users for security policies or for VPN access, without asking for their username and password. When a user logs in to a directory service, the FSSO agent sends FortiGate the username, the IP address, and the list of groups that the user belongs to. FortiGate uses this information to maintain a local database of usernames, IP addresses, and group mappings."
"To display the list of FSSO users that are currently logged in, use the CLI command diagnose debug authd fsso list. For each user, the user name, user group, IP address, and the name of the workstation from which they logged in shows."
"You can monitor users who authenticate through your firewall policies using the Dashboard > Assets & Identities > Firewall Users page. It displays the user, user group, duration, IP address, traffic volume, and authentication method." Technical Deep Dive:
The first thing to verify is whether FortiGate has actually learned the user correctly in its FSSO active users table, especially the user-to-IP mapping. FSSO enforcement is identity-based, but the real-time match on live traffic still depends on FortiGate associating the traffic's source IP with the authenticated Windows user. If that mapping is missing, stale, or tied to the wrong IP because of DHCP changes, DNS update lag, or collector-agent timing, the firewall policy match can fail even though the user successfully logged in to Windows.
That is why C is the best first check.
A may be the next thing to verify if the user is present but still denied, but first you must confirm the user is even present in the FSSO table with the correct IP.
B is unrelated to the initial FSSO identity-mapping problem.
D is less likely because the Windows logon already succeeded.
Useful checks:
diagnose debug authd fsso list
diagnose debug authd fsso server-status
execute fsso refresh
These commands confirm whether FortiGate has the user, group, and IP mapping needed for policy matching.

NEW QUESTION: 12
What is the primary FortiGate election process when the HA override setting is enabled? (Choose one answer)

A. Connected monitored ports > Priority > HA uptime > FortiGate serial number
B. Connected monitored ports > Priority > System uptime > FortiGate serial number
C. Connected monitored ports > HA uptime > Priority > FortiGate serial number
D. Connected monitored ports > System uptime > Priority > FortiGate serial number
Answer: A (LEAVE A REPLY)
According to the FortiOS 7.6 Study Guide and technical documentation regarding High Availability (HA), the FortiGate Clustering Protocol (FGCP) uses a specific set of rules to elect the primary unit in a cluster. By default, the election order follows: Connected Monitored Ports > HA Uptime > Priority > Serial Number.
However, when the HA override setting is enabled, the election logic is modified to prioritize the administrator-defined priority value over the uptime of the cluster members. In this specific configuration, the election process follows this sequence:
* Connected monitored ports: The unit with the most functioning monitored interfaces is preferred.
* Priority: The unit with the highest manually configured priority value (e.g., 255) is selected next.
* HA uptime: If monitored ports and priority are equal, the unit that has been up in the HA cluster the longest is chosen.
* FortiGate serial number: As a final tie-breaker, the unit with the higher serial number is elected.1
Statement A is correct because it reflects the shift where Priority is evaluated immediately after monitored ports, overriding the standard uptime advantage. Statements B and D are incorrect because the FGCP uses HA uptime, not system uptime, for its calculations.

NEW QUESTION: 13
You are onboarding an agentless, secure web gateway (SWG) endpoint for secure internet access (SIA). What will happen to the user's nonweb traffic? (Choose one answer)
A. All the nonweb traffic will bypass FortiSASE.
B. FortiSASE will use SWG to redirect nonweb traffic to FortiExtender.
C. FortiSASE will use Firewall-as-a-Service (FWaaS) to redirect nonweb traffic.
D. The endpoint will use split tunneling to redirect nonweb traffic to FortiSASE.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
Refer to the exhibit.



The administrator configured SD-WAN rules and set the FortiGate traffic log page to display SD-WAN-specific columns: SD-WAN Quality and SD-WAN Rule Name FortiGate allows the traffic according to policy ID 1 placed at the top. This is the policy that allows SD-WAN traffic. Despite these settings, the traffic logs do not show the name of the SD-WAN rule used to steer those traffic flows What could be the reason?

A. SD-WAN rule names do not appear immediately. The administrator must refresh the page.

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

C. Destinations in the SD-WAN rules are configured for each application, but feature visibility is not enabled.

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

Answer: D (LEAVE A REPLY)

In FortiOS 7.6, SD-WAN steering decisions are recorded in traffic logs only when traffic matches an explicit SD-WAN rule (SD-WAN service rule). When no configured SD-WAN rule matches a session, FortiGate uses the implicit (default) SD-WAN rule/behavior to select a member (often resulting in load-balancing or default selection based on the configured SD-WAN algorithm).

In the exhibit, traffic is permitted by firewall policy ID 1, and the Destination Interface alternates between port1 and port2, but SD-WAN Rule Name remains empty. This is consistent with the sessions being forwarded by the implicit SD-WAN rule, which does not populate a named rule in the log columns.

Why the other options are not correct:

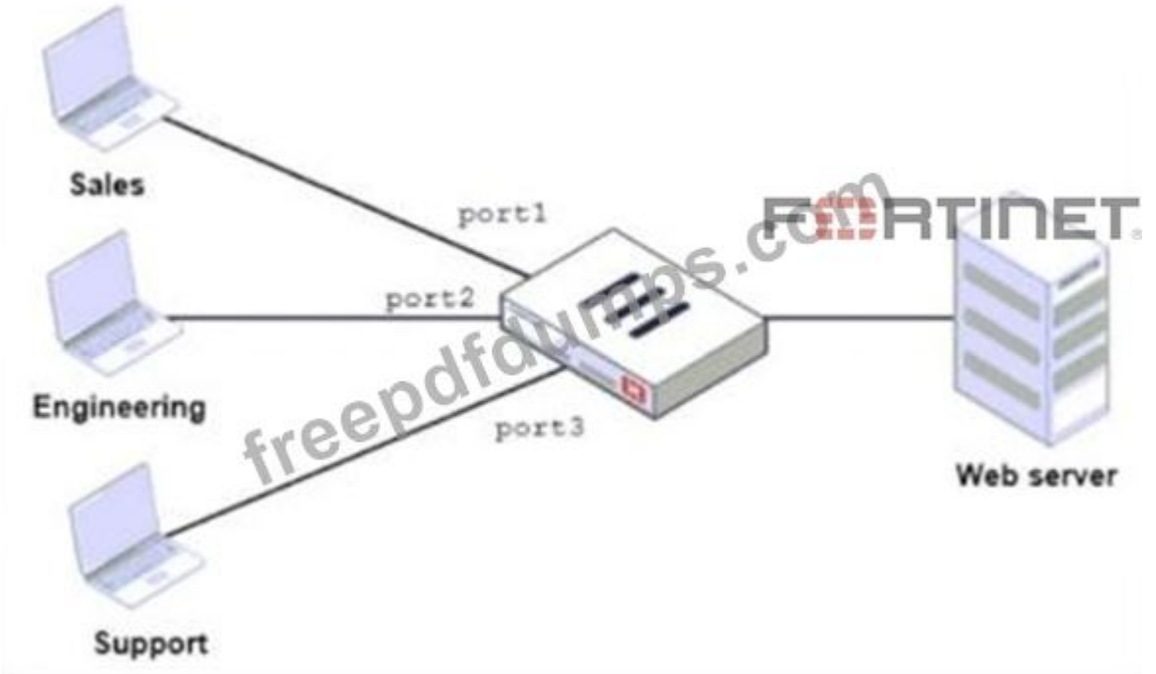
A: SD-WAN rule name logging is not a "delayed display" behavior requiring refresh; it is populated per-session when an explicit rule matches.

B: Application Control is not required for SD-WAN rule name to appear. Rule name logging depends on SD-WAN rule match, not on whether Application Control is enabled.

C: Feature visibility affects GUI display options, but the exhibit already shows the SD-WAN columns enabled; the issue is that no explicit SD-WAN rule is being hit.

NEW QUESTION: 15

Refer to the exhibit.



FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.

Which action must the administrator perform to consolidate the two policies into one?

A. Select port1 and port2 subnets in a single firewall policy.

B. Create an Aggregate interface that includes port1 and port2 to create a single firewall policy.

C. Replace port1 and port2 with the any interface in a single firewall policy.

D. Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy.

Answer: D (LEAVE A REPLY)

"By default, you can select only a single interface as the incoming interface and a single interface as the outgoing interface. This is because the option to select multiple interfaces, or any interface in a firewall policy, is disabled on the GUI. However, you can enable the Multiple Interface Policies option on the Feature Visibility page to disable the single interface restriction."

"You can also specify multiple interfaces, or use the any option, if you configure a firewall policy on the CLI, regardless of the default GUI setting." Technical Deep Dive:

The correct answer is D.

The policies are identical except for the incoming interface: one is for Sales and one is for Engineering. FortiGate GUI policy creation normally restricts you to one incoming interface per policy. To consolidate both into a single GUI policy, the administrator must enable Multiple Interface Policies so both port1 and port2 can be selected in the same rule.

Why the others are wrong:

A is not enough, because policy matching also includes the incoming interface, not just the source subnets.

B changes the network design and is unnecessary.

C would work too broadly by matching traffic from any interface, which is not the intended controlled consolidation.

A matching CLI-style concept would be:

config firewall policy
edit <id>
set srcintf "port1" "port2"
set dstintf "<server-interface>"
set srcaddr "Sales_Subnet" "Engineering_Subnet"
set dstaddr "<web-server>"
set service "HTTP" "HTTPS"
set action accept
next
end
That preserves a single policy while still being specific about which interfaces are allowed.

NEW QUESTION: 16
You have created a web filter profile named restrictmedia-profile with a daily category usage quota.
When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down.
What could be the reason?
A. The web filter profile is already referenced in another firewall policy.
B. The firewall policy is in no-inspection mode instead of deep-inspection.
C. The naming convention used in the web filter profile is restricting it in the firewall policy.
D. The inspection mode in the firewall policy is not matching with web filter profile feature set.
Answer: D (LEAVE A REPLY)
In FortiOS 7.6, web filter profiles are inspection-mode dependent. Certain advanced web filtering features-such as daily category usage quota-are only supported when the firewall policy is operating in proxy-based inspection mode.
Why the profile is not visible
The profile restrictmedia-profile includes a daily category usage quota.
Daily quotas are a proxy-based web filtering feature.
If the firewall policy is configured with:
Inspection mode: Flow-based
Then FortiGate will not display proxy-only web filter profiles in the Web Filter drop-down list.
FortiGate automatically filters the available profiles based on feature compatibility with the policy's inspection mode.
This behavior is explicitly documented in the FortiOS 7.6 Web Filtering and Inspection Mode Compatibility sections.
Why the other options are incorrect
A . Already referenced in another firewall policyWeb filter profiles can be reused across multiple policies. This does not hide them.
B . Firewall policy is in no-inspection mode instead of deep-inspectionSSL inspection depth affects HTTPS visibility, not whether a web filter profile appears in the drop-down list.

C . Naming convention restrictionFortiOS does not restrict profile selection based on naming conventions.

NEW QUESTION: 17
An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.
What is true about the DNS connection to a FortiGuard server?
A. It uses UDP 53.
B. It uses DNS over HTTPS.
C. It uses DNS over TLS.
D. It uses UDP 8888.
Answer: C (LEAVE A REPLY)
"When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic. New FortiGuard DNS servers have been added as primary and secondary servers." Technical Deep Dive:
The correct answer is C. It uses DNS over TLS.
This is a direct default-behavior question. If you configure FortiGuard servers as DNS servers and do not change anything else, FortiGate uses DoT rather than plain DNS. That means the DNS session is encrypted, which protects DNS queries from simple interception or tampering on the path.
Why the other options are wrong:
A is standard clear-text DNS behavior, not the FortiGuard DNS default stated in the guide.
B is incorrect because the guide specifically says DNS over TLS, not DNS over HTTPS.
D is incorrect; the guide does not describe UDP 8888 as the default transport for this DNS use case.
Operationally, this matters because FortiGate relies on DNS not only for client-facing services, but also for resolving objects and securely reaching cloud-based services. Using DoT improves confidentiality for those DNS lookups.

NEW QUESTION: 18
Which two statements are correct when FortiGate enters conserve mode? (Choose two answers)
A. FortiGate continues to run critical security actions, such as quarantine.

B. FortiGate refuses to accept configuration changes.
C. FortiGate halts complete system operation and requires a reboot to regain available resources.
D. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.
Answer: B,D (LEAVE A REPLY)
According to the FortiOS 7.6 Study Guide and technical documentation, conserve mode is a protective state triggered when memory utilization reaches the Extreme Threshold (typically 95% by default). When this occurs, the FortiGate implements several measures to prioritize system stability over new functionality. One of the primary restrictions is that the FortiGate refuses to accept configuration changes (Statement B). This prevents the system from initiating new processes or allocating additional memory that could lead to a total system crash.
Regarding traffic handling, the behavior is determined by specific "fail-open" settings. For the IPS engine, if the fail-open global setting is enabled, the FortiGate continues to transmit packets without IPS inspection (Statement D). This ensures that network connectivity is maintained even when the system lacks the memory resources to perform deep packet inspection. In contrast, Statement A is incorrect because the system may skip non-essential actions to save memory. Statement C is incorrect because conserve mode is designed to avoid a system halt; the device remains operational and will automatically exit conserve mode once memory usage drops below the Release Threshold (typically 82%).

NEW QUESTION: 19
Refer to the exhibit.

```
config system global
    set av-failopen one-shot
end
config ips global
    set fail-open enable
end
```


Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)
A. Administrators must restart FortiGate to allow new sessions.
B. Administrators cannot change the configuration.
C. FortiGate skips quarantine actions.
D. FortiGate drops new sessions requiring inspection.
Answer: B,C (LEAVE A REPLY)

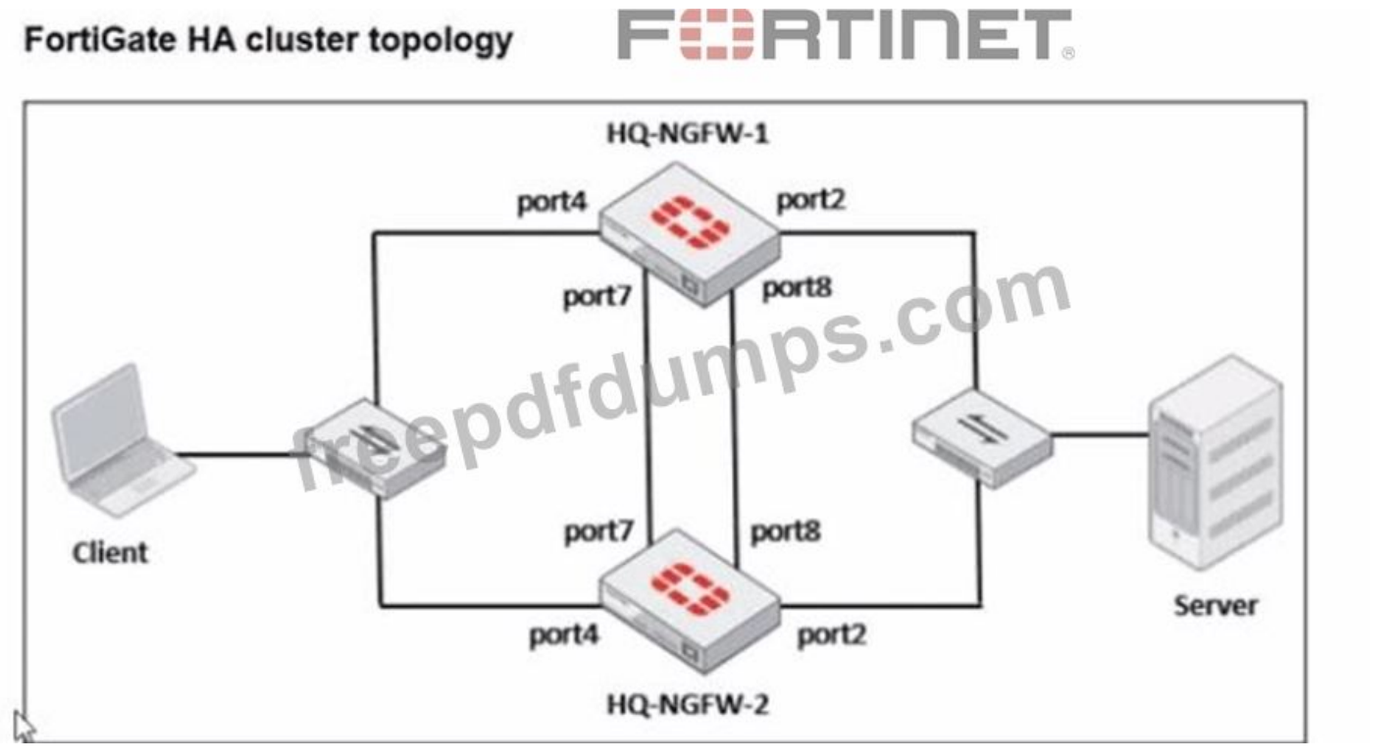
NEW QUESTION: 20
An administrator has configured the following settings.
config system settings

set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
What are the two results of this configuration? (Choose two.)
A. The number of logs generated by denied traffic is reduced.
B. A session for denied traffic is created.
C. Denied users are blocked for 30 minutes.
D. Session helpers are disabled for denied traffic.
Answer: (SHOW ANSWER)
"To reduce the number of log messages generated and improve performance, you can enable a session table entry of dropped traffic. This creates the denied session in the session table and, if the session is denied, all packets for that session are also denied. This ensures that FortiGate does not have to perform a policy lookup for each new packet matching the denied session, which reduces CPU usage and log generation."
"The CLI command is ses-denied-traffic. You can also set the duration for block sessions. This determines how long a session will be kept in the session table by setting block-session-timer in the CLI. By default, it is set to 30 seconds." Technical Deep Dive:
The correct answers are A and B.
When set ses-denied-traffic enable is configured, FortiGate creates a session-table entry for denied traffic. That means once traffic is denied, subsequent packets that belong to the same denied flow do not need a full policy lookup again. FortiGate can drop them immediately based on the existing denied-session entry. That directly confirms B.
Because FortiGate no longer re-evaluates every repeated denied packet in the same way, the device generates fewer logs and uses less CPU for repeated denied traffic. That is exactly why A is also correct.
Why the other two are wrong:
C is incorrect because block-session-timer 30 means 30 seconds, not 30 minutes. The denied session entry is kept in the session table for that duration.
D is incorrect because these settings do not disable session helpers. They only control how denied traffic is tracked in the session table.
In operational terms, this feature is useful when a host repeatedly retries traffic that FortiGate is already denying. Instead of doing a fresh lookup for every retry, FortiGate caches the denied decision temporarily and drops the repeated packets faster.

NEW QUESTION: 21
Which two statements are true about an HA cluster? (Choose two answers)
A. An HA cluster cannot have both in-band and out-of-band management interfaces at the same time.
B. Link failover triggers a failover if the administrator sets the interface down on the primary

device.
C. When sniffing the heartbeat interface, the administrator must see the IP address 169.254.0.2.
D. HA incremental synchronization includes FIB entries and IPsec SAs.
Answer: (SHOW ANSWER)
According to FortiOS 7.6 High Availability documentation, the FortiGate Cluster Protocol (FGCP) provides robust mechanisms for both link monitoring and stateful data synchronization. Link failover is a primary trigger for cluster renegotiation; if a monitored interface goes down-including when an administrator manually sets the interface to administratively down-the primary unit's priority is effectively reduced, triggering a failover to a secondary unit to ensure path continuity.5 This is a standard method for testing HA failover behavior.
Furthermore, to achieve a seamless stateful failover where active sessions are not dropped, the FortiGate performs incremental synchronization of critical runtime data.6 This specifically includes Forwarding Information Base (FIB) entries, which represent the compiled routing table, and IPsec Security Associations (SAs).7 By synchronizing IPsec SAs, the secondary unit 8can resume encrypted tunnels immediately after a failover without requiring a f9ull IKE re-negotiation.10 Statement A is incorrect because in-band and out-of-band management can coexist using reserved management interfaces and management-ip settings.11 Statement C is incorrect because while heartbeat interfaces use link-local IPs in the 169.254.0.x range, the specific IP .2 is not universally required for all heartbeats and depends on the number of cluster members and serial numbers.

NEW QUESTION: 22
Refer to the exhibits.



Current HA status

```
HQ-NGFW-1 # get system ha status
...
Configuration Status:
    FGVM02TM24013423(updated 0 seconds ago): in-sync
    FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
    FGVM02TM24013501(updated 4 seconds ago): in-sync
    FGVM02TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
...
number of member: 2
HQ-NGFW-1       , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2       , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
```

New FortiGate HA configuration

```
HQ-NGFW-1
# config system ha
     set group-id 5
     set group-name "Fortinet"
     set mode a-p
     set password *
     set hbdev "port7" 50 "port8" 60
     set session-pick enable
     set override disable
     set priority 90
     set monitor "port3"


HQ-NGFW-2
# config system ha
     set group-id 5
     set group-name "Fortinet"
     set mode a-p
     set password *
     set hbdev "port7" 50 "port8" 60
     set session-pick enable
     set override enable
     set priority 110
     set monitor "port3"
```


Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibits.

What would be the expected outcome in the HA cluster?

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

B. HQ-NGFW-1 will remain the primary because HQ-NGFW-2 has lower priority
C. The HA cluster will become out of sync because the override setting must match on all HA members.
D. HQ-NGFW-1 will synchronize the override disable setting with HQ-NGFW-2.
Answer: A (LEAVE A REPLY)
From the current HA status, HQ-NGFW-1 is the primary and HQ-NGFW-2 is the secondary.
The administrator then changes these HA parameters:
HQ-NGFW-1: set override disable, set priority 90
HQ-NGFW-2: set override enable, set priority 110
In FGCP (A-P mode), the override (preemption) feature controls whether a higher-priority unit is allowed to take over the primary role.
When override is enabled, the cluster will prefer (and can re-elect) the unit with the highest device priority to become primary (preempting a lower-priority primary when conditions trigger re-election behavior as defined by FGCP).
Here, HQ-NGFW-2 has:
override enabled
higher priority (110) than HQ-NGFW-1 (90)
Therefore, the expected result is that HQ-NGFW-2 becomes the primary.
Why the other options are incorrect:
B is incorrect because it claims HQ-NGFW-2 has lower priority (it is higher: 110 > 90).
C is incorrect because a mismatch in the override setting is not what causes the "configuration out of sync" condition shown in get system ha status (that is about synchronized configuration databases, not a requirement that override values must match to remain in-sync).
D is incorrect because HA settings like override/priority are not synchronized in the way regular configuration objects are; they are device-level HA parameters.

NEW QUESTION: 23
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?
A. The collector agent uses a Windows API to query DCs for user logins.
B. The NetSessionEnum function is used to track user logouts.
C. NetAPI polling can increase bandwidth usage in large networks.
D. The collector agent must search Windows application event logs.
Answer: B (LEAVE A REPLY)
NetAPI: Polls temporary sessions created on the DC when a user logs on or logs off and calls the NetSessionEnum function on Windows. It's faster than the WinSec and WMI methods; however, it can miss some logon events if a DC is under heavy system load. This is because sessions can be quickly created and purged form RAM, before the agent has a chance to poll and notify FG.

NEW QUESTION: 24
Refer to the exhibit
A firewall policy to enable active authentication is shown.

When attempting to access an external website using an active authentication method, the user is not presented with a login prompt. What is the most likely reason for this situation?

A. No matching user account exists for this user.

B. The Remote-users group must be set up correctly in the FSSO configuration.

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

D. The Service DNS is required in the firewall policy.

Answer: (SHOW ANSWER)

Based on the exhibit and FortiOS 7.6 Active Authentication (captive portal) behavior, the most likely reason the user is not presented with a login prompt is that DNS is missing from the firewall policy.

What the exhibit shows

The firewall policy configured for active authentication includes:

Source: HQ_SUBNET and Remote-users

Destination: all

Services:

HTTP

HTTPS

ALL_ICMP

Security Profiles: Web filter and SSL inspection enabled

Authentication: Active (user group referenced)

DNS is not included as a service in the policy.

Why DNS is required for active authentication

In FortiOS 7.6, active authentication (captive portal) works as follows:

The user attempts to access a website using a URL (for example, www.example.com).

The client must first perform a DNS lookup to resolve the domain name.

FortiGate intercepts the initial HTTP/HTTPS request and redirects the user to the authentication portal.

If DNS traffic is blocked or not allowed:

The hostname cannot be resolved.

The HTTP/HTTPS request never properly occurs.

FortiGate has nothing to intercept, so the login prompt is never triggered.

This is explicitly documented in the FortiOS 7.6 Authentication and Captive Portal requirements, which state that DNS must be permitted for captive portal-based authentication to function correctly.

Why the other options are incorrect

A . No matching user account exists for this user

Incorrect.

If the user account did not exist, the login page would still appear, but authentication would fail after credentials are entered.
B . The Remote-users group must be set up correctly in the FSSO configuration Incorrect.
This policy is using active authentication, not FSSO.
FSSO configuration is irrelevant for active authentication login prompts.
C . The Remote-users group is not added to the Destination
Incorrect.
User groups are applied in the Source field for authentication-based policies.
Destination does not accept user groups.

NEW QUESTION: 25
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.
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 26
Refer to the exhibit.

Why is the Antivirus scan switch grayed out when you are creating a new antivirus profile for FTP?

A. Antivirus scan is disabled under System -> Feature visibility

B. None of the inspected protocols are active in this profile.

C. The Feature Set for the profile is Flow-based but it must be Proxy-based

D. FortiGate. with less than 2 GB RAM. does not support the Antivirus scan feature.

Answer: B (LEAVE A REPLY)

In FortiOS 7.6, the Antivirus scan master switch in an antivirus profile becomes available only after at least one supported protocol is enabled for inspection.

What the exhibit shows

A new antivirus profile named FTP_AV_Profile

Feature set: Flow-based

Antivirus scan switch is grayed out

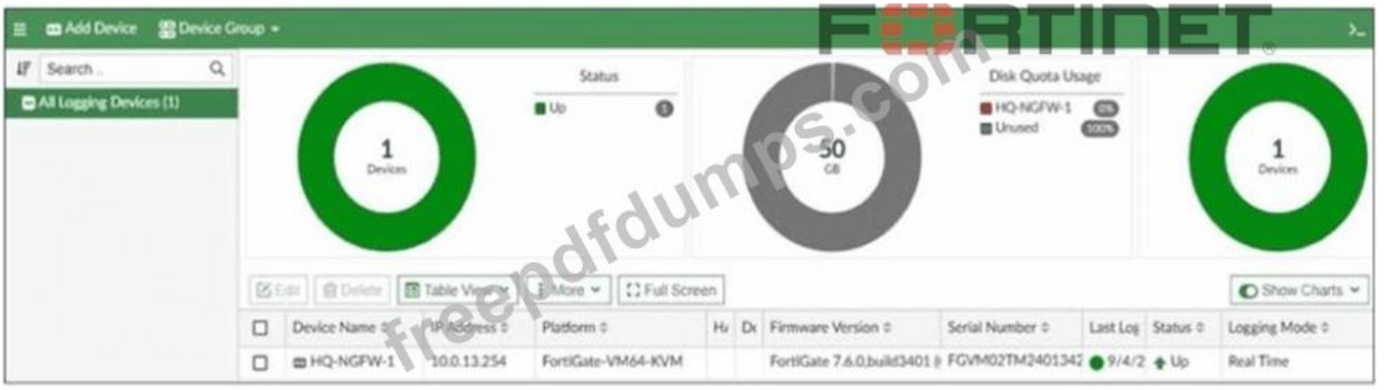
All Inspected Protocols (HTTP, SMTP, POP3, IMAP, FTP, CIFS) are currently disabled Why the Antivirus scan switch is grayed out In FortiOS antivirus profiles:

The Antivirus scan toggle is a dependent control

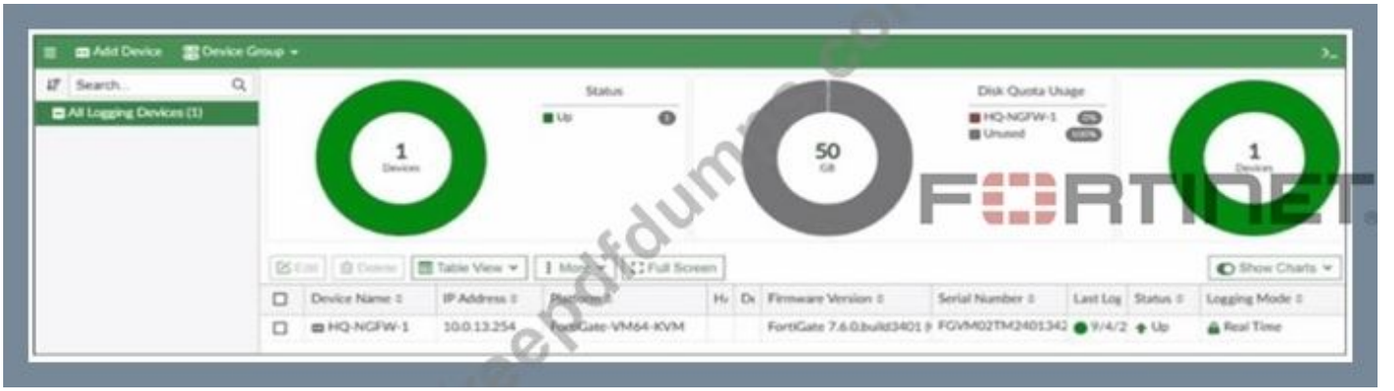
It cannot be enabled unless at least one inspected protocol is selected This prevents enabling AV scanning when there is no traffic type to scan This behavior is documented in the FortiOS 7.6 Antivirus Profile configuration section.

Once you enable a protocol (for example, FTP), the Antivirus scan switch becomes active and configurable.
Why option B is correct
B . None of the inspected protocols are active in this profile.
All protocol toggles are OFF
Therefore, FortiGate disables (grays out) the Antivirus scan option
This is expected and correct behavior
Why the other options are incorrect
A . Antivirus scan is disabled under Feature visibilityIncorrect. Feature Visibility controls whether Antivirus appears in the GUI, not whether the scan switch is enabled inside a profile.
C . Feature set must be Proxy-basedIncorrect. Antivirus scanning is supported in both flow-based and proxy-based modes.
D . Less than 2 GB RAM does not support Antivirus scanIncorrect. Memory size affects performance and offloading, not basic AV scan availability.

NEW QUESTION: 27
The FortiGate device HQ-NGFW-1 with the IP address 10.0.13.254 sends logs to the FortiAnalyzer device with the IP address 10.0.13.125. The administrator wants to verify that reliable logging is enabled on HQ-NGFW-1.
Which exhibit helps with the verification?
A.



B.



C.
```
config log fortianalyzer setting
      set status enable
      set server "10.0.13.125"
      set serial "FAZ-VMTM24012176"
      set enc-algorithm high-medium
      set upload-option realtime
end
```

D.
```
HQ-NGFW-1 # diagnose sniffer packet any "host 10.0.13.125" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.13.125]
2.173071 port6 out 10.0.13.254.14974 -> 10.0.13.125.514: udp 347
3.334638 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: psh 4017477514 ack 2638032500
3.335098 port6 in 10.0.13.125.514 -> 10.0.13.254.23054: psh 2638032500 ack 4017477548
3.335129 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: ack 2638032543
```

Answer: C (LEAVE A REPLY)

NEW QUESTION: 28

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

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

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

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

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

Answer: (SHOW ANSWER)

With full SSL inspection, FortiGate performs a man-in-the-middle process: it decrypts the HTTPS session, inspects it, then re-encrypts it. To do this, FortiGate presents a substitute certificate to the client, signed by the CA certificate configured in the SSL/SSH inspection profile (for example, Fortinet_CA_SSL or a custom enterprise CA).

Browsers will show certificate warning errors when the issuing CA is not trusted by the client device/browser trust store. This only happens for HTTPS because certificates are used in TLS; HTTP has no certificate exchange, so no warning appears.

Why the other options are incorrect:

A: Allowing invalid server certificates affects whether FortiGate blocks/permits connections to sites with bad certs; it does not fix the client warning about FortiGate's substituted cert.

B: Proxy vs flow inspection mode does not inherently cause certificate warnings; the warning is about trust of the signing CA.

D: Missing extensions is not the typical reason across "any HTTPS website"; the standard reason is the client does not trust the FortiGate inspection CA

NEW QUESTION: 29
An administrator wants to address shadow IT visibility challenges and prevent users from sending sensitive files outside the organization without proper approval. Which FortiSASE method should the administrator implement to achieve these goals? (Choose one answer)
A. Secure SD-WAN access (SSD-WAN)
B. Secure private access (SPA)
C. Secure SaaS access (SSA)
D. Secure internet access (SIA)
Answer: (SHOW ANSWER)
"FortiSASE provides secure access to remote users for the following use cases:
* SIA enables secure web browsing for remote users to protect from known and unknown threats
* SPA enables explicit application access under a zero-trust access or with SD-WAN integration to ensure secure application access
* SSA addresses shadow IT visibility challenges and safeguards data loss prevention"
"FortiCASB provides cloud-based and API-based features to enable deep inspection of SaaS applications to enable detailed monitoring, analysis, and reporting features... Data loss prevention (DLP) helps to identify, monitor, and protect organizational data at rest and in motion." Technical Deep Dive:
The correct answer is C. Secure SaaS access (SSA).
The question gives two very specific requirements:
Shadow IT visibility
Prevent sensitive files from leaving the organization without approval
The study guide maps both directly to SSA. In FortiSASE, SSA aligns with SaaS governance and CASB-style controls. That is the right architecture when you need visibility into sanctioned and unsanctioned SaaS usage, plus DLP controls for uploads, sharing, and file movement.
Why the other options are wrong:
SIA focuses on securing internet browsing and remote web traffic.
SPA is for explicit zero-trust access to private applications.
SSD-WAN is not the FortiSASE method for SaaS visibility/DLP control.
In practice, SSA is the choice because it combines SaaS visibility, activity monitoring, and DLP-style enforcement. That lets an administrator detect shadow SaaS usage and apply controls such as blocking uploads, monitoring sharing events, or restricting file transfers based on policy. This is a CASB-oriented use case, not just generic web security.

NEW QUESTION: 30
Which three statements about SD-WAN performance SLAs are true? (Choose three.)
A. They rely on session loss and jitter.
B. They monitor the state of the FortiGate device.
C. All the SLA targets can be configured.
D. They are applied in a SD-WAN rule lowest cost strategy.
E. They can be measured actively or passively.

Answer: C,D,E (LEAVE A REPLY)

In FortiOS 7.6, SD-WAN Performance SLAs are used to measure link quality and influence SD-WAN rule decisions. The following three statements are true.

C). All the SLA targets can be configured.

True

SD-WAN Performance SLAs allow administrators to configure:

Latency

Jitter

Packet loss

Mean Opinion Score (MOS) (for voice)

Threshold values for these metrics are fully configurable per SLA.

This is explicitly documented in the SD-WAN Performance SLA configuration section.

D). They are applied in an SD-WAN rule lowest cost strategy.

True

Performance SLAs are commonly used with the Lowest Cost (SLA-based) strategy.

In this strategy:

FortiGate selects the lowest-cost link that meets the SLA requirements.

If a link violates the SLA, it is excluded from selection.

E). They can be measured actively or passively.

True

FortiOS supports:

Active probing (synthetic probes such as ping/HTTP)
Passive measurement (based on real traffic statistics)

Administrators can choose how SLAs are measured depending on the deployment and requirements.

Why the other options are incorrect

A). They rely on session loss and jitter.

Incorrect

SLAs measure packet loss, latency, and jitter.

Session loss is not an SLA metric in FortiOS.

B). They monitor the state of the FortiGate device.

Incorrect

Performance SLAs monitor link quality, not FortiGate system health or device state.

NEW QUESTION: 31

Refer to the exhibits.

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```


HQ-NGFW-1 System Performance output


```
HQ-NGFW-1 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32 kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds. Which FortiGate is the primary?

A. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting

B. HQ-NGFW-2 with the parameter priority setting

C. HQ-NGFW-1 with the parameter override setting

D. HQ-NGFW-2 with the parameter memory-failover-threshold setting

Answer: (SHOW ANSWER)

From the HA configuration shown for HQ-NGFW-1:

set memory-based-failover enable

set memory-failover-threshold 70

set memory-failover-monitor-period 50

set memory-failover-sample-rate 10

set memory-failover-flip-timeout 60

set override disable

set priority 200

From the performance status outputs:

HQ-NGFW-1 memory used is 90% (well above the configured threshold of 70%) HQ-NGFW-2 memory used is about 48.7% (well below the threshold) What happens in FortiOS 7.6 with memory-based failover When memory-based failover is enabled, FortiGate monitors memory utilization. If the unit's memory usage stays above the configured memory-failover-threshold for the configured memory-failover-monitor-period, the cluster triggers a failover away from the unit under memory pressure.

Threshold = 70%

HQ-NGFW-1 is at 90%, so it violates the threshold.

Monitor period = 50 seconds.

The administrator observed for 55 seconds, which is longer than 50 seconds, so the condition is met for long enough to trigger failover.

The memory-failover-flip-timeout 60 is used to prevent rapid back-and-forth role changes (flapping) after a failover decision; it does not prevent the initial failover from occurring once the threshold breach persists for the monitor period.

NEW QUESTION: 32
When configuring the connection between FortiGate and FortiAnalyzer, which option indicates that reliable traffic is enabled? (Choose one answer)
A. The connection status shows a green check icon
B. The interface status is set to up
C. A padlock icon appears in the connection settings
D. The logging mode is set to real-time
Answer: C (LEAVE A REPLY)
"When you enable reliable logging on FortiGate, the log transport delivery method changes from UDP to TCP. TCP provides reliable data transfer, guaranteeing that the transferred data remains intact and arrives in the same order in which it was sent."
"Optionally, if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecured network." Technical Deep Dive:
The correct answer is C. The study guide explicitly ties reliable logging to TCP transport and optionally to SSL-encrypted OFTP. Among the choices, the padlock icon is the only one that meaningfully indicates secure, reliable log transport behavior. A green check icon usually indicates that the FortiGate-FortiAnalyzer connection is simply up, not specifically that reliable logging is enabled. Interface status being up is unrelated, and real-time logging mode describes delivery behavior, not the reliable transport indicator itself.
So, exam-wise, the best answer is C.
From the CLI perspective, reliable logging changes the transport from UDP to TCP, and with encryption enabled it uses SSL-protected OFTP. That is why the GUI indicator associated with secure transport is the most relevant visual clue here.

NEW QUESTION: 33
What are three key routing principles in SD-WAN? (Choose three answers)
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 (LEAVE A REPLY)

"This slide shows the SD-WAN rule lookup process. SD-WAN rules are essentially policy routes."
"FortiGate performs a forwarding information base (FIB) lookup for the packet destination IP (dstip). If the resolved interface for the fib-best-match isn't an SD-WAN member, then FortiGate moves on to the next rule. This behavior follows the key routing principle: SD-WAN rules are skipped if the best route to the destination isn't an SD-WAN member."
"If the resolved interface is an SD-WAN member, then FortiGate looks for one or more acceptable members in the oif list... An acceptable member is an alive member that has a route to the destination. This behavior follows the key routing principle: SD-WAN rules are skipped if none of the configured members in the rule have a valid route to the destination."
"Because regular policy routes have precedence over any other routes..."
"Also note that policy routes have precedence over SD-WAN rules, and over any routes in the FIB." Technical Deep Dive:
The correct answers are A, C, and E.
A is correct because an SD-WAN rule is not enough by itself. A selected member must also be alive and have a valid route to the destination. If none of the members referenced by the rule can actually reach the destination, the rule is skipped.
C is correct because a regular policy route is evaluated before SD-WAN rules. This is a classic exam trap. FortiGate treats SD-WAN steering like policy-route logic, but standard policy routes still win if they match and are valid.
E is correct because FortiGate first checks the FIB best match. If that best route resolves to an interface that is not an SD-WAN member, FortiGate skips the SD-WAN rule and continues.
Why the others are wrong:
B is false because SD-WAN rules do not have precedence over everything; regular policy routes do.
D is false because the number of available routes is not the deciding rule. Even with only one route, SD-WAN can still steer traffic if the routing and member conditions are met.
Operationally, think of SD-WAN routing in this order: policy route check → SD-WAN rule lookup → standard FIB fallback. On FortiGate, the practical validation commands are:
get router info routing-table all
diagnose sys sdwan service
diagnose firewall proute list
That combination lets you confirm whether a packet is being captured by a policy route, whether an SD-WAN rule has acceptable members, and what the FIB currently resolves for the destination.

NEW QUESTION: 34

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

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

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

C. FortiGate does not support workstation check.
D. FortiGate directs the collector agent to use a remote LDAP server.
Answer: B,C (LEAVE A REPLY)
Based on the FortiOS 7.6 Administrator Guide regarding Fortinet Single Sign-On (FSSO) polling modes, the agentless polling mode has specific technical characteristics:
SMB Protocol Usage (Statement B is True):
In agentless polling mode, the FortiGate unit itself acts as the collector.
It establishes direct connections to the Windows Domain Controllers (DCs) using the SMB (Server Message Block) protocol, typically over TCP port 445, to read the Windows Security Event logs.
This allows FortiGate to parse login event IDs (such as 4768 and 4769) to identify users and their corresponding IP addresses without needing an external collector agent installed on a server.
Workstation Check Support (Statement C is True):
One of the primary limitations of the agentless polling mode compared to the agent-based mode is the lack of workstation verification.
In agentless mode, FortiGate does not perform "workstation checks" or "dead entry checks". This means it cannot proactively verify if a user is still logged into a specific workstation after the initial logon event is recorded, which can lead to stale entries if a user logs off without a corresponding event being captured.
Why other options are incorrect:
Option A: In agentless mode, FortiGate (the FSSO daemon) performs the collection itself; it does not use the AD server as a "collector agent" in the functional sense of FSSO architecture.
Option D: While FortiGate uses LDAP to retrieve group membership information once a user is identified, it does not "direct" a collector agent to a remote LDAP server, as there is no external collector agent involved in this specific mode.

NEW QUESTION: 35
Refer to the exhibits.

HQ-NGFW-1 HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
     set group-id 5
     set group-name "Training"
     set mode a-p
     set password ENC nmk7zGYiRrux1
     set hbdev "port7" 0
     set session-pickup enable
     set override disable
     set priority 200
     set monitor "port1"
end
```


HQ-NGFW-2 HA configuration

```
HQ-NGFW-2 (ha) # show
config system ha
     set group-id 5
     set group-name "Training"
     set mode a-p
     set password ENC n40G3dmn0K50s
     set hbdev "port7" 0
     set session-pickup enable
     set override disable
     set priority 100
     set monitor "port1"
end
```

An administrator configured both members of an HA cluster at the same time. After one week of monitoring, the administrator wants to verify the HA failover performance. How can the administrator force a failover? (Choose one answer)

A. The administrator must reset the HA uptime on HQ-NGFW-1.

B. The administrator must set the parameter override to enable on HQ-NGFW-2.

C. The administrator must increase the HA priority on HQ-NGFW-2.

D. The administrator must set the monitored port1 to down on HQ-NGFW-1.

Answer: A (LEAVE A REPLY)

"This slide shows the order when the HA override setting is disabled, which is the default behavior."

"1. The cluster compares the number of monitored interfaces that have a status of up. The member with the most available monitored interfaces becomes the primary.

2. The cluster compares the HA uptime of each member. The member with the highest HA uptime, by at least five minutes, becomes the primary.

3. The member with the highest priority becomes the primary."

"When HA override is disabled, the HA uptime has precedence over the priority setting. This means that if you must manually fail over to a secondary device, you can do so by reducing the HA uptime of the primary FortiGate. You can do this by running the diagnose sys ha reset-uptime command on the primary FortiGate, which resets its HA uptime to 0." Technical Deep Dive:

The correct answer is A.

Both HA members are configured with set override disable, so FGCP does not prefer the higher-priority unit first. With override disabled, the election order is based on monitored interfaces, then HA uptime, then priority, and finally serial number. Since the cluster has been running for one

week, the secondary unit will have a much higher HA uptime than a unit whose uptime is reset to zero. Therefore, if the administrator runs diagnose sys ha reset-uptime on the current primary HQ-NGFW-1, FGCP re-evaluates election and the other member can take over.
Option B is wrong because enabling override only on HQ-NGFW-2 does not by itself force an immediate clean failover in this scenario and also changes election behavior rather than performing the documented manual failover action. Option C is wrong because with override disabled, priority does not beat HA uptime. Option D can simulate a link failover, but the study guide's documented manual failover method for this exact override-disabled condition is to reset the primary's HA uptime.
Relevant CLI:
diagnose sys ha reset-uptime
get system ha status
diagnose sys ha status
This is the clean exam-aligned method to trigger a controlled HA role change.

NEW QUESTION: 36
Refer to the exhibits.

System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

The system performance output and default configuration of high memory usage thresholds on a FortiGate device are shown.
Based on the system performance output, what are the two possible outcomes? (Choose two.)
A. Administrators can access FortiGate only through the console port.
B. FortiGate has entered conserve mode.
C. FortiGate drops new sessions.
D. Administrators can change the configuration.
Answer: B,D (LEAVE A REPLY)
From the exhibits:
System performance output
Memory used: 90%

Free memory: ~5%
Default memory thresholds (FortiOS 7.6)
memory-use-threshold-green 82%
memory-use-threshold-red 88%
memory-use-threshold-extreme 89%
Because memory usage (90%) exceeds the extreme threshold (89%), the FortiGate enters conserve mode.
Effects of conserve mode (FortiOS 7.6 - verified)
B . FortiGate has entered conserve mode.
Correct
When memory usage exceeds the red/extreme threshold, FortiGate automatically enters conserve mode.
This is exactly the condition shown in the system performance output.
D . Administrators can change the configuration.
Correct
Even in conserve mode:
Administrators can still log in (GUI, SSH, console)
Configuration changes are allowed
FortiGate does not lock configuration access during conserve mode.
This behavior is explicitly documented in the FortiOS 7.6 Conserve Mode section.
Why the other options are incorrect
A . Administrators can access FortiGate only through the console port.
Incorrect
Network access (GUI/SSH) is still available in conserve mode unless otherwise restricted.
Console-only access is not a conserve-mode requirement.
C . FortiGate drops new sessions.
Incorrect (as a general statement)
FortiGate may drop or bypass new inspection-required sessions depending on fail-open/fail-close settings.
It does not universally drop all new sessions, so this statement is not always true.

NEW QUESTION: 37
Refer to the exhibit.

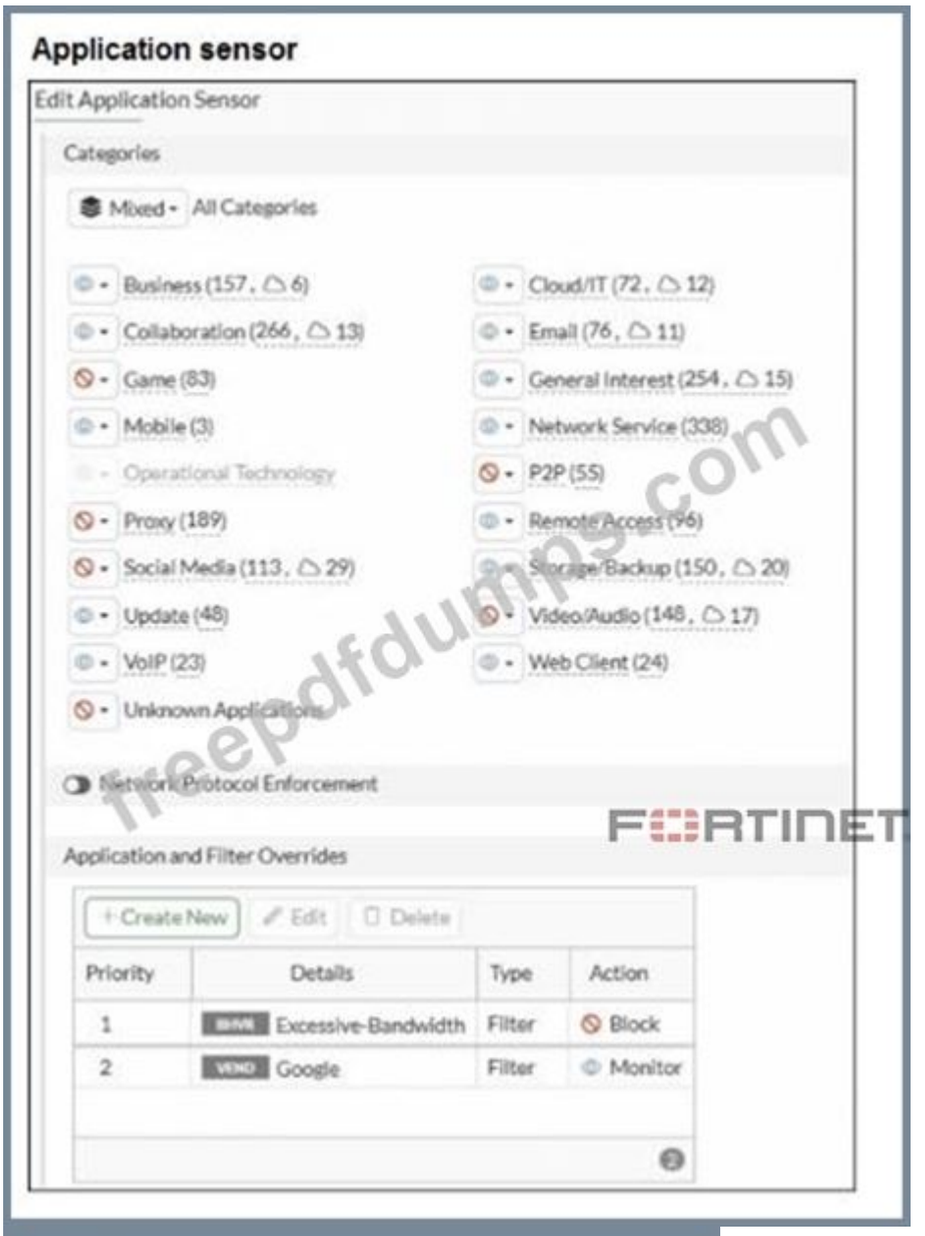
```
date=2025-02-4 time=09:07:59 logid=0100022700 type=event subtype=system level=critical
 vd="root" logdesc="IPS session scan paused" action="drop" msg="IPS session scan, enter fail open mode"
```

What can you conclude from the log shown in the exhibit?
A. The IPS socket buffer is full and IPS engine needs more memory to create new sessions.
B. The IPS socket buffer is full and IPS engine cannot decode a packet.
C. The IPS scan is paused by the IPS diagnostic command with bypass mode option 5.
D. The IPS session scan is paused and reevaluating the packet because of a dirty flag.
Answer: A (LEAVE A REPLY)

"You can configure the fail-open setting under config ips global to control how the IPS engine behaves when the IPS socket buffer is full."
"If the IPS engine does not have enough memory to build more sessions, the fail-open setting determines whether the FortiGate should drop the sessions or bypass the sessions without inspection."
"It is important to understand that the IPS fail-open setting is not just for conserve mode-it kicks in whenever IPS fails. Most failures are due to a high CPU issue or a high memory (conserve mode) issue." Technical Deep Dive:
The correct answer is A.
The log text says:
logdesc="IPS session scan paused"
action="drop"
msg="IPS session scan, enter fail open mode"
That combination indicates an IPS failure condition, specifically the condition described in the guide where the IPS socket buffer is full and the IPS engine lacks enough memory/resources to build additional sessions. In that state, FortiGate applies the configured IPS fail-open behavior. Since the log shows action="drop", the device is not bypassing those new sessions; it is dropping them.
Why the other choices are wrong:
B is wrong because the guide ties fail-open to socket buffer/resource exhaustion, not packet decode failure.
C is wrong because this is not evidence of a manual diagnostic pause.
D is wrong because the study guide does not associate this log with dirty-flag packet reevaluation.
Operationally, this usually points to high memory, high CPU, or conserve-mode pressure affecting the IPS engine. Useful checks are:
get system performance status
diagnose hardware sysinfo conserve
diagnose sys top
Those help confirm whether the IPS issue is being driven by memory pressure or CPU exhaustion.

NEW QUESTION: 38
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.

Application sensor



Firewall policy

You cannot access any of the Google applications, but you are able to access www.fortinet.com. What would you do to resolve this issue?

A. Change the Inspection mode to Proxy-based.

B. Set SSL inspection to deep-content-inspection.

C. Move up Google in the Application and Filter Overrides section to set its priority to 1.

D. Add Google.com to the URL category in the security profile.

Answer: C (LEAVE A REPLY)

"With these multiple filters, which one has the priority? After the IPS engine examines the traffic stream for a signature match, FortiGate scans packets for matches, in this order, for the application control profile:

1. Application and filter overrides..."

"Next, the scan checks for application and filter overrides. Because a filter override is configured to block applications that use excessive bandwidth, it blocks all applications using excessive bandwidth, regardless of other categories that allow these applications."

"In this scenario, the filter override (Excessive-Bandwidth) is blocked and, since Dailymotion falls under the excessive bandwidth category, Dailymotion is blocked even though it is set to Monitor in the Application and Filter Overrides section. The priority in which application and filter overrides are placed takes precedence."

"To allow web filtering, DNS filtering, or application control for HTTPS traffic, you must select an SSL inspection profile with certificate inspection or a deep inspection enabled." Technical Deep Dive:

The problem is not flow-based mode and not the SSL profile. Your firewall policy already has certificate-inspection, and the study guide explicitly says that application control for HTTPS traffic works with certificate inspection or deep inspection. So option B is unnecessary, and option A is unrelated.

The real issue is the override order inside the application sensor:

Priority 1: Filter = Excessive-Bandwidth, Action = Block

Priority 2: Vendor = Google, Action = Monitor

FortiGate evaluates overrides from top to bottom and applies the first match. Many Google applications match the Excessive-Bandwidth filter, so they are blocked before the later Google/Monitor override is ever reached. That is why Google apps fail while www.fortinet.com still works.

So the correct fix is to move the Google override above the Excessive-Bandwidth filter, making Google the first match.

A representative CLI-style logic would be:

```
config application list
edit "default"
config entries
edit 1
set vendor "Google"
set action monitor
```

next
edit 2
set filter "Excessive-Bandwidth"
set action block
next
end
next
end
That preserves the bandwidth block for other apps while allowing Google applications to match the higher-priority override first.

NEW QUESTION: 39
FortiGate is integrated with FortiAnalyzer and FortiManager.
When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?
A. Universally Unique Identifier
B. Policy ID
C. Sequence ID
D. Log ID
Answer: A (LEAVE A REPLY)
In FortiOS 7.6, when FortiGate is integrated with FortiAnalyzer and FortiManager, firewall policies rely on a Universally Unique Identifier (UUID) to ensure proper policy tracking, synchronization, and log correlation across devices.
Why the UUID is required
Every firewall policy in FortiOS has a UUID.
FortiManager uses the UUID to:
Track policies across managed FortiGate devices
Maintain policy consistency during installs and revisions
FortiAnalyzer uses the UUID to:
Correlate logs accurately to the correct firewall policy
Preserve log association even if policy order or policy ID changes
Without a UUID:
Policy-to-log mapping can break
FortiManager cannot reliably manage or synchronize policies
FortiAnalyzer log analysis becomes inconsistent
This is explicitly documented in Fortinet administration and logging architecture references.
Why the other options are incorrect
B). Policy IDPolicy ID can change when policies are moved and is not reliable for long-term correlation across FortiManager and FortiAnalyzer.
C). Sequence IDSequence ID reflects GUI ordering only and has no role in log correlation.
D). Log IDLog ID is generated per log event, not per firewall policy.

Valid NSE4_FGT_AD-7.6 Dumps shared by Actual4test.com for Helping Passing NSE4_FGT_AD-7.6 Exam! Actual4test.com now offer the **newest NSE4_FGT_AD-7.6 exam dumps**, the Actual4test.com NSE4_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NSE4_FGT_AD-7.6 dumps with Test Engine here: https://www.actual4test.com/NSE4_FGT_AD-7.6_examcollection.html (**95** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)