

Fortinet.NSE4_FGT_AD-7.6-JPN.v2026-10-17.q41

試験コード :	NSE4_FGT_AD-7.6-JPN
試験名称 :	Fortinet NSE 4 - FortiOS 7.6 Administrator (NSE4_FGT_AD-7.6日本語版)
認証ベンダー :	Fortinet
無料問題の数 :	41
バージョン :	v2026-10-17
ページの閲覧量 :	105
問題集の閲覧量 :	410

https://www.jpnsnshiken.com/shiken/Fortinet.NSE4_FGT_AD-7.6-JPN.v2026-10-17.q41.html

質問: 1

FortiGateデバイスをFSSO用に構成しました。ユーザーはWindowsへのログインには成功しましたが、インターネットへのアクセスが拒否されました。管理者はまず何をチェックすべきでしょうか？(回答を1つ選択してください)

- A. ユーザーが正しい AD グループに割り当てられているかどうか。
- B. SSL復号化のためのFortiGateファイアウォールポリシー設定。
- C. ユーザーのIPアドレスに対応するFortiGate FSSOアクティブユーザーリスト。
- D. ログイン失敗時の Windows イベント ビューアー。

正解: C ([コメントを發表する](#))

"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.

質問: 2

展示資料を参照してください。

SD-WAN traffic log

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
YouTube	✓ Accept (8.08 kB / 27...	1 (DIA)	port2		
YouTube	✓ Accept (UTM Allowed)	1 (DIA)	port2		
Facebook	✓ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✓ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✓ Accept (3.33 kB / 10...	1 (DIA)	port1		
YouTube	✓ Accept (44.63 kB / 3...	1 (DIA)	port2		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port1		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port2		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port2		

管理者は SD-WAN ルールを設定し、FortiGate のトラフィック ログ ページに SD-WAN 固有の列 (SD-WAN 品質と SD-WAN ルール名) を表示するように設定しました。FortiGate は、一番上に配置されたポリシー ID 1 に従ってトラフィックを許可します。これは SD-WAN トラフィックを許可するポリシーです。これらの設定にもかかわらず、トラフィック ログには、これらのトラフィック フローを制御するために使用された SD-WAN ルールの名前が表示されません。原因は何でしょうか？

- A. SD-WANルール名はすぐには表示されません。管理者はページを更新する必要があります。
- B. ファイアウォール ポリシーにアプリケーション コントロール プロファイルが適用されていません。
- C. SD-WANルール内の宛先はアプリケーションごとに構成されていますが、機能の可視性は有効になっていません。
- D. FortiGate は暗黙の SD-WAN ルールに従ってトラフィックの負荷分散を行いました。

正解: (正解を表示します)

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.

質問: 3

FortiGateにおける等コストマルチパス(ECMP)構成に関する記述のうち、正しいものはどれですか？(2つ選択してください)

- A. SD-WANが有効になっている場合、load-balance-modeパラメータを使用してロードバランシングアルゴリズムを制御します。

- B.** SD-WANが無効になっている場合は、v4-ecmp-modeパラメータをボリュームベースに設定できます。
- C.** SD-WANが有効になっている場合、距離と優先度の値が異なるルートをECMPの一部として構成できます。
- D.** SD-WANが無効になっている場合は、構成システム設定でロードバランシングアルゴリズムを設定します。

正解: **A,D** ([コメントを发表する](#))

"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.

質問: **4**

HAオーバーライド設定が有効になっている場合、FortiGateの主要な選出プロセスは何ですか？(回答を1つ選択してください)

- A.** 接続されている監視対象ポート > 優先度 > HA稼働時間 > FortiGateシリアル番号
- B.** 監視対象ポート > 優先度 > システム稼働時間 > FortiGate シリアル番号
- C.** 接続されている監視対象ポート > HA稼働時間 > 優先度 > FortiGateシリアル番号
- D.** 監視対象ポート > システム稼働時間 > 優先度 > FortiGate シリアル番号

正解: **A** ([コメントを发表する](#))

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.

質問: 5

アプリケーション制御プロファイルを設定し、カテゴリー」タブでピアツーピアトラフィックを「ブロック」に設定しました。

そして、それをファイアウォールポリシーに適用しました。しかし、既知のポートでのピアツーピアトラフィックは、ブロックされることなくFortiGateを通過しています。

この問題を解決するには、FortiGateのどの設定を確認すればよいですか？

- A. UDPベースのアプリケーション向け置換メッセージ
- B. FortiGuardカテゴリ評価
- C. ネットワークプロトコルの強制
- D. アプリケーションとフィルタの上書き

正解: ([正解を表示します](#))

質問: 6

フローベースのウイルス対策プロファイルを説明する3つの記述はどれですか？(3つ選択してください)

- A. FortiGate はファイル全体をバッファリングしますが、同時にクライアントに送信します。
- B. フローベースの検査では、プロキシベースの検査で利用可能なスキャンモードのハイブリッドを使用します。
- C. ウイルスが検出された場合、最後のパケットがクライアントに配信されます。
- D. フローベースの検査は、プロキシベースの検査と比較してパフォーマンスを最適化します。
- E. IPS エンジン、プロセスをスタンドアロンとして処理します。

正解: **A,B,D** ([コメントを發表する](#))

According to the FortiOS 7.6 Study Guide and Parallel Path Processing documentation, flow-based antivirus inspection is designed to provide security with minimal impact on performance.

First, a defining characteristic of modern flow-based AV (specifically in its " hybrid " mode) is that FortiGate buffers the whole file but transmits to the client at the same time (Statement A). This behavior allows the client to start receiving data immediately to prevent session timeouts, while the FortiGate reassembles the file in memory to perform a signature check before the final packet is released.

Second, starting with recent FortiOS versions including 7.6, flow-based inspection uses a hybrid of the scanning modes (Statement B). Previously, flow mode offered " Quick " or " Full " scans; now, it combines these techniques to offer a balance between the speed of stream-based scanning and the thoroughness of archive inspection.

Third, the primary motivation for selecting this mode is that flow-based inspection optimizes performance compared to proxy-based inspection (Statement D). It processes traffic in a single pass using the IPS engine, avoiding the overhead associated with the WAD (proxy) process. Statement C is incorrect because if a virus is detected, the last packet is withheld and the connection is reset to prevent the file from being completed. Statement E is less accurate as the IPS engine loads the AV engine to perform the task rather than acting as a " standalone " entity in the context of file scanning.

質問: 7

管理者がFortiGate上で、add-routeを有効にしたダイヤルアップIPsec VPNを設定しました。しかし、静的ルートがルーティングテーブルに表示されません。この状況について正しい記述はどれですか？(2つ選択してください。)

- A. add-route が正しく機能するためには、管理者は静的ルートではなくポリシー ルートを使用する必要があります。
- B. 管理者はフェーズ2が正常に確立されていることを確認する必要があります。
- C. 管理者はフェーズ 2 セレクタでリモート ネットワークを正しく定義する必要があります。
- D. 管理者はダイヤルアップインターフェースで動的ルーティングプロトコルを有効にする必要があります。

正解: ([正解を表示します](#))

With a dialup IPsec VPN on FortiGate, when add-route is enabled, FortiGate will only install the corresponding route when it has enough negotiated information from the tunnel. In FortiOS 7.6, that means the route is tied to the Phase 2 (Quick Mode) selectors and is created dynamically when the IPsec SA is actually up.

B). The administrator must ensure phase 2 is successfully established

This is required. FortiGate does not install the add-route route just because Phase 1 exists or because the configuration is present. The route is added when the tunnel is effectively usable, which requires Phase 2 (IPsec SA) to be up. If Phase 2 is not established, there is no active SA and FortiGate will not inject the related route into the routing table.

So, if the static route is not showing, one correct explanation is that Phase 2 is not up.

C). The administrator must define the remote network correctly in the phase 2 selectors This is also required. For dialup tunnels, FortiGate derives what route to add from the remote subnet(s) defined in the Phase 2 selector (proxy ID). If the remote network in Phase 2 is missing, incorrect, or too broad

/too narrow in a way that prevents negotiation, the tunnel either won't come up (so no route), or the route that would be installed won't match what the administrator expects.

So, another correct explanation is that the Phase 2 remote network is not correctly defined, preventing the correct route from being created.

Why the other options are incorrect

A). Policy route instead of a static route

Add-route does not require policy routes. It is specifically a feature that injects a route (route-table entry) associated with the IPsec tunnel/SA and the Phase 2 selector networks.

D). Enable a dynamic routing protocol

Dynamic routing protocols (OSPF/BGP/RIP) are not required for add-route. Add-route is independent of dynamic routing and works by installing routes locally based on the negotiated selectors.

質問: 8

サイトベースのリモートインターネットアクセス方式において、FortiExtenderはどのようにしてFortiSASEに接続するのですか？

- A. FortiExtenderはIPsec上の仮想拡張LAN(VXLAN)接続を使用します。
- B. FortiExtender は FortiClient を使用して安全な SSL 接続を確立します。
- C. FortiExtender は、まずセキュア Web ゲートウェイ (SWG) を介して FortiGate LAN 拡張機能に接続します。
- D. FortiExtender はプロキシ自動構成 <PAC) ファイルと明示的な Web プロキシを使用して接続します。

正解: ([正解を表示します](#))

In FortiSASE site-based (remote internet access) deployments, FortiExtender is used to onboard branch or remote sites without a local FortiGate.

According to FortiSASE and FortiExtender architecture documentation:

FortiExtender integrates with FortiSASE using a secure VXLAN-over-IPsec tunnel This tunnel:

Extends the site network to FortiSASE

Transparently forwards traffic for inspection

Preserves network segmentation and routing context

This design is similar to cloud-based LAN extension and is not proxy-based Why the other options are incorrect B: FortiClient is used for agent-based user access, not FortiExtender C: Secure Web Gateway (SWG) is a service, not a transport mechanism D: PAC files and explicit proxies are used in agentless / proxy-based access, not site-based FortiExtender deployments

質問: 9

FSSOコレクターエージェントのNetAPIポーリングモードを正しく説明しているのは、次のうちどれですか？

- A. コレクターエージェントは、Windows API を使用して DC にユーザーログインを照会します。

- B. NetSessionEnum 関数は、ユーザーのログアウトを追跡するために使用されます。
- C. NetAPI ポーリングは、大規模ネットワークで帯域幅の使用量を増加させる可能性があります。
- D. コレクターエージェントは、Windows アプリケーションイベントログを検索する必要があります。

正解: [\(正解を表示します\)](#)

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 from RAM, before the agent has a chance to poll and notify FG.

質問: 10

展示資料を参照してください。



事前定義された詳細検査プロファイルとカスタム詳細検査プロファイルでは、図に示すように、一部のウェブカテゴリがSSL検査から除外されています。これらのウェブカテゴリが除外される理由は次のうちどれですか？(2つ選択してください。)

- A. これらのウェブサイトは FortiGate の信頼済みドメイン リストに含まれているため、リソースの利用効率が最適化されています。
- B. この法的規制は、これらのウェブサイトのユーザーのプライバシーを優先し、機密情報を保護することを目的としています。
- C. これらのウェブサイトは、FortiGuard が管理する信頼できるドメイン名の許可リストに含まれています。
- D. FortiGate の一時証明書は、HTTP Strict Transport Security を使用する Web サイトへのブラウザのアクセスを拒否します。

正解: **B,D** ([コメントを发表する](#))

"You may need to exempt traffic from SSL inspection if it is causing problems with traffic, or for legal reasons."

"Performing SSL inspection on a site that is enabled with HTTP Strict Transport Security (HSTS), for example, can cause problems with traffic. Remember, the only way for FortiGate to inspect encrypted traffic is to intercept the certificate coming from the server and generate a temporary one. After FortiGate presents the temporary SSL certificate, browsers that use HSTS refuse to proceed."

"Laws protecting privacy might be another reason to bypass SSL inspection. For example, in some countries, it is illegal to inspect SSL bank-related traffic. Configuring an exemption for sites is simpler than setting up firewall policies for each individual bank. You can exempt sites based on their web category, such as Finance and Banking..."

"The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories-Finance and Banking, and Health and Wellness-and some FQDN addresses..." Technical Deep Dive:

The correct answers are B and D .

B is correct because the study guide explicitly says SSL inspection may be bypassed for legal reasons , especially where privacy laws restrict inspection of sensitive categories such as Finance and Banking . The same privacy rationale also explains why Health and Wellness is commonly exempted.

D is correct because some sites break under deep inspection due to HSTS . FortiGate must generate and present a temporary certificate during full SSL inspection, and browsers enforcing HSTS can reject that interception flow. That is why some sites are exempted from deep inspection.

Why the others are wrong:

* A is not stated in the guide.

* C refers to the separate Reputable websites option, which is a FortiGuard-maintained allowlist feature, not the reason the predefined categories shown in the exhibit are excluded.

From an operational standpoint, this is a classic balance between security visibility and application/legal compatibility . Deep inspection gives FortiGate payload visibility, but it can interfere with pinned-certificate

/HSTS behavior and can violate privacy policy for regulated content.

質問: 11

管理者はFGCPプロトコルを使用してHAクラスタを構築したいと考えています。管理者は、両方のメンバーが満たしていることを確認する必要がある2つの要件は何ですか？(2つ選択してください)

A. それらは同じ HA グループ ID を持っている必要があります。

B. ハートビートインターフェースは同じサブネット内になければなりません。

C. それらは同じ数の構成済み VDOM を持つ必要があります。

D. ハードドライブの構成が同じである必要があります。

正解: **A,D** ([コメントを發表する](#))

"To successfully form an HA cluster, you must ensure that the members have the same:

* Model: hardware model or VM model

* Firmware version

* Licensing: includes the FortiGuard license, virtual domain (VDOM) license, FortiClient license, and so on

* Hard drive configuration: the same number and size of drives and partitions

* Operating mode: the operating mode-NAT mode or transparent mode-of the management VDOM."

"From a configuration and setup point of view, you must ensure that the HA settings on each member have the same group ID , group name, password, and heartbeat interface settings. Try to place all heartbeat interfaces in the same broadcast domain , or for two-member clusters, connect them directly." Technical Deep Dive:

The correct answers are A and D .

A is correct because FGCP cluster formation requires matching HA parameters, and group ID is explicitly one of them. If the group ID differs, the units will not consider each other part of the same cluster during HA discovery and election.

D is correct because FortiGate HA expects hardware parity in critical platform characteristics, including hard drive configuration . If disk layout differs, the members do not satisfy the HA formation prerequisites.

B is incorrect because the study guide does not require heartbeat interfaces to be in the same IP subnet. The requirement is that heartbeat links be in the same broadcast domain , or directly connected in a two-node design. In practice, heartbeat links are Layer 2 adjacency links; IP subnet matching is not the stated requirement.

C is incorrect because the guide does not say both units must start with the same number of configured VDOMs. What must match is the licensing level and the operating mode of the management VDOM . After cluster formation, the primary synchronizes its configuration to the secondary.

A practical verification set before forming FGCP HA is:

get system status

show system ha

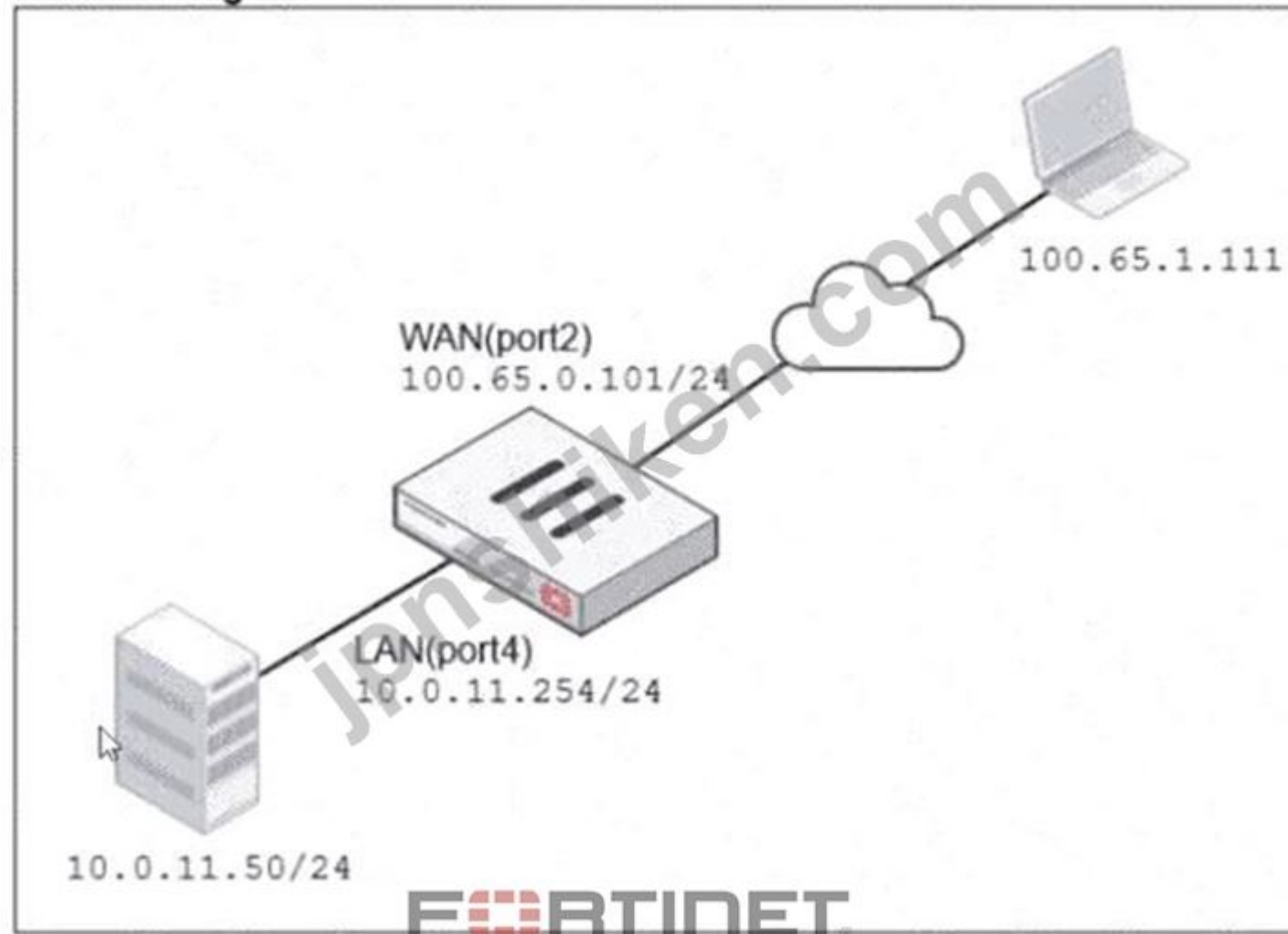
diagnose sys ha status

Operationally, FGCP then uses the heartbeat links for member discovery, health monitoring, election, and config/session synchronization. On supported hardware, session forwarding and HA processing can still benefit from FortiGate's ASIC-assisted architecture, but HA state, config sync, and election logic remain control-plane functions handled by FortiOS.

質問: 12

展示資料を参照してください。

Network diagram



Fortinet

Name: VIP-WEB-SERVER

Comments: Write a comment... 0/255

Color: Change

Network

Interface: WAN (port2)

Type: Static NAT

External IP address/range: 100.65.0.200

Map to:

IPv4 address/range: 10.0.11.50

☐ Optional Filters

☒ Port Forwarding

Protocol: ☒ TCP ☐ UDP ☐ SCTP ☐ ICMP

Port Mapping Type: ☒ One to one ☐ Many to many

External service port: 443

Map to IPv4 port: 4443

Firewall policies

	Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
☐	Internet (1)	LAN (port4)	WAN (port2)	all	all	always	ALL	✓ ACCEPT		✓ NAT
☐	Web_Server_Access (2)	WAN (port2)	LAN (port4)	all	VIP-WEB-SERVER	always	HTTPS	✓ ACCEPT		✗ Disabled

ネットワークVIPオブジェクトに接続されたFortiGateデバイスとファイアウォールポリシー構成の図を示します。

WAN(ポート2)インターフェースにはIPアドレスが割り当てられています。

100.65.0.101/24。

LAN(ポート4)インターフェースにはIPアドレスが割り当てられています。

10.0.11.254/24。

ホスト100.65.1.111がポート443でTCP SYNパケットを100.65.0.200に送信した場合、FortiGateがパケットを宛先に転送する時点で、パケットの送信元アドレス、宛先アドレス、および宛先ポートはどうなりますか？

- A. それぞれ 10.0.11.254、100.65.0.200、および 443
- B. それぞれ 10.0.11.254、10.0.15.50、および 4443。
- C. それぞれ 100.65.1. 111、10.0.11.50、および 4443。
- D. それぞれ 100.65.1.111、10.0.11.50、443。

正解: **C** ([コメントを發表する](#))

From the exhibits:

A VIP named VIP-WEB-SERVER is configured on WAN (port2) with:

External IP: 100.65.0.200

Mapped (internal) IP: 10.0.11.50

Port forwarding enabled (TCP)

External service port: 443

Map to IPv4 port: 4443

The inbound firewall policy Web_Server_Access is:

From WAN (port2) to LAN (port4)

Destination: VIP-WEB-SERVER

Service: HTTPS

NAT: Disabled (meaning no source NAT is applied)

What happens to the packet

A host 100.65.1.111 sends TCP SYN dst-port 443 to 100.65.0.200.

When FortiGate matches the VIP and forwards traffic to the internal server, FortiGate performs destination NAT (DNAT) based on the VIP:

Source IP is unchanged because policy NAT is disabled:

Source remains 100.65.1.111

Destination IP is translated by the VIP:

Destination becomes 10.0.11.50

Destination port is translated by the VIP port-forward:

Destination port becomes 4443

Therefore, at the time FortiGate forwards the packet to the destination (internal server), it will be:

Source address: 100.65.1.111

Destination address: 10.0.11.50

Destination port: 4443

質問: **13**

展示資料を参照してください。

Application and Filter Overrides

+ Create New Edit Delete FORTINET

Priority	Details	Type	Action
1	ABC.Com	Application	Allow
2	Excessive-Bandwidth	Filter	Block

2

管理者は、ABC.Com アプリケーション署名に対してアプリケーションオーバーライドを設定し、アクションを「許可」に設定しました。このアプリケーション制御プロファイルは、すべての送信トラフィックをスキャンするファイアウォールポリシーに適用されます。ファイアウォールポリシーではログ記録が有効になっています。設定をテストするために、管理者は ABC.Com Web サイトへ複数回アクセスしました。

ABC.Comのセキュリティログにログが生成されないのはなぜですか？

- A. ABC Com は「帯域幅過剰」のカテゴリに該当します。
- B. ABC.Com タイプがフィルターではなくアプリケーションに設定されています。
- C. ABC.Com はアプリケーション プロファイルの下に構成されており、これは Web フィルタ プロファイルとして構成する必要があります。
- D. ABC Com Action は「許可」に設定されています

正解: [\(正解を表示します\)](#)

In FortiOS 7.6 Application Control, security logs are generated primarily for actions such as Block or Monitor, not for Allow actions.

What is happening in the exhibit

An Application Override is configured for ABC.Com

Type: Application

Action: Allow

The application control profile is applied to a firewall policy

Logging is enabled on the firewall policy

Traffic to ABC.Com is successfully allowed

However, no security logs appear for ABC.Com.

Why no logs are generated

In FortiOS 7.6:

Application Control logs are written to Security Logs when:

An application is Blocked

An application is Monitored

When an application action is set to Allow:

The traffic is permitted silently

No application control security log is generated

Even if policy logging is enabled

This is expected and documented behavior.

To generate logs for allowed applications, the action must be set to Monitor, not Allow.

Why the other options are incorrect

A). ABC.Com is hitting the category Excessive-BandwidthIncorrect. ABC.Com has a higher-priority explicit override (priority 1), so it is not evaluated against the Excessive-Bandwidth filter.

B). The ABC.Com Type is set as Application instead of FilterIncorrect. Application-type overrides are valid and commonly used; this does not suppress logging.

C). The ABC.Com must be configured as a web filter profileIncorrect. This traffic is being evaluated by Application Control, not Web Filter.

質問: 14

展示資料を参照してください。

Edit Application Sensor

Categories

☒ Mixed ▾ All Categories☒ Business (157, ⬇ 6)☒ Collaboration (266, ⬇ 13)☒ Game (83)☒ Mobile (3)☐ Operational Technology☒ Proxy (189)☒ Social Media (113, ⬇ 29)☒ Update (48)☒ VoIP (23)☒ Unknown Applications☒ Cloud/IT (72, ⬇ 12)☒ Email (76, ⬇ 11)☒ General Interest (254, ⬇ 15)☒ Network Service (338)☒ P2P (55)☒ Remote Access (96)☒ Storage/Backup (150, ⬇ 20)☒ Video/Audio (148, ⬇ 17)☒ Web Client (24)☒ Network Protocol Enforcement

Application and Filter Overrides

[+ Create New](#) [Edit](#) [Delete](#)

Priority	Details	Type	Action
1	BNR Excessive-Bandwidth	Filter	☒ Block
2	VEND Google	Filter	☒ Monitor
2			

Firewall policy

Edit Policy

Firewall/Network Options

Inspection mode: Flow-based Proxy-based

NAT: ☒

IP pool configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve source port: ☐

Protocol options: PROXY default

Security Profiles

AntiVirus: ☐

Web filter: ☐

Video filter: ☐

OS Signatures: ☐

Application control: ☒ APP default

IPS: ☐

File filter: ☐

SSL inspection: SSL certificate-inspection

- 図に示すように、アプリケーションセンサーとそれに対応するファイアウォールポリシーを実装しました。Googleのアプリケーションには一切アクセスできませんが、www.fortinet.comにはアクセスできます。この問題を解決するために、あなたはどのような行動を2つ取りますか？(2つ選択してください。)
- A. SSL検査をディープコンテンツ検査に設定します。
 - B. アプリケーションとフィルタの上書きセクションでGoogleを上に移動して、その優先順位を設定します。
 - C. セキュリティプロファイルの URL カテゴリに "Google"..com を追加します。
 - D. 検査モードをフローベースに変更します
 - E. アプリケーションとフィルタの上書きセクションで、Google のアクションを 許可」に設定します。

正解: ([正解を表示します](#))

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.

質問: 15

コレクターエージェントのアドバンスモードの2つの特徴は何ですか？(2つ選択してください。)

A. 詳細モードでは、セキュリティプロファイルはユーザーグループにのみ適用でき、個々のユーザーには適用できません。

B. 詳細モードでは、FortiGate を LDAP クライアントとして構成したり、FortiGate 上でグループフィルタを構成したりすることができます。

C. 詳細モードでは、Windows の規則 NetBIOS: ドメイン\ユーザー名を使用します。

D. アドバンスモードでは、ネストされたグループまたは継承されたグループがサポートされます。

正解: **B,D** ([コメントを发表する](#))

" 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

質問: 16

HAクラスタについて正しい記述はどれですか？(2つ選択してください)

- A. HAクラスタは、インバンド管理インターフェイスとアウトオブバンド管理インターフェイスを同時に持つことはできません。
- B. 管理者がプライマリデバイスでインターフェイスをダウンさせると、リンクフェイルオーバーがトリガーされます。
- C. ハートビートインターフェイスをスニффイングする場合、管理者は IP アドレス 169.254.0.2 を確認する必要があります。
- D. HA の増分同期には、FIB エントリと IPsec SA が含まれます。

正解: ([正解を表示します](#))

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 8 can resume encrypted tunnels immediately after a failover without requiring a full 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.

有効的な**NSE4_FGT_AD-7.6-JPN**問題集はJPNTTest.com提供され、**NSE4_FGT_AD-7.6-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**NSE4_FGT_AD-7.6-JPN**試験問題集を提供します。JPNTTest.com NSE4_FGT_AD-7.6-JPN試験問題集はもう更新されました。ここで**NSE4_FGT_AD-7.6-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE4_FGT_AD-7.6-JPN-mondaishu **96**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

展示資料を参照してください。

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 a4f6yqY4iPexFmAnZgzDY
  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
```

FORTINET®

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
```

管理者は、HAクラスタのパフォーマンスステータス出力を55秒間監視しました。

プライマリのFortiGateはどれですか？

- A. HQ-NGFW-1、パラメータmemory-failover-flip-timeout設定
- B. パラメータ優先度設定付きHQ-NGFW-2
- C. パラメータオーバーライド設定付きのHQ-NGFW-1
- D. HQ-NGFW-2、パラメータmemory-failover-threshold設定

正解: ([正解を表示します](#))

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.

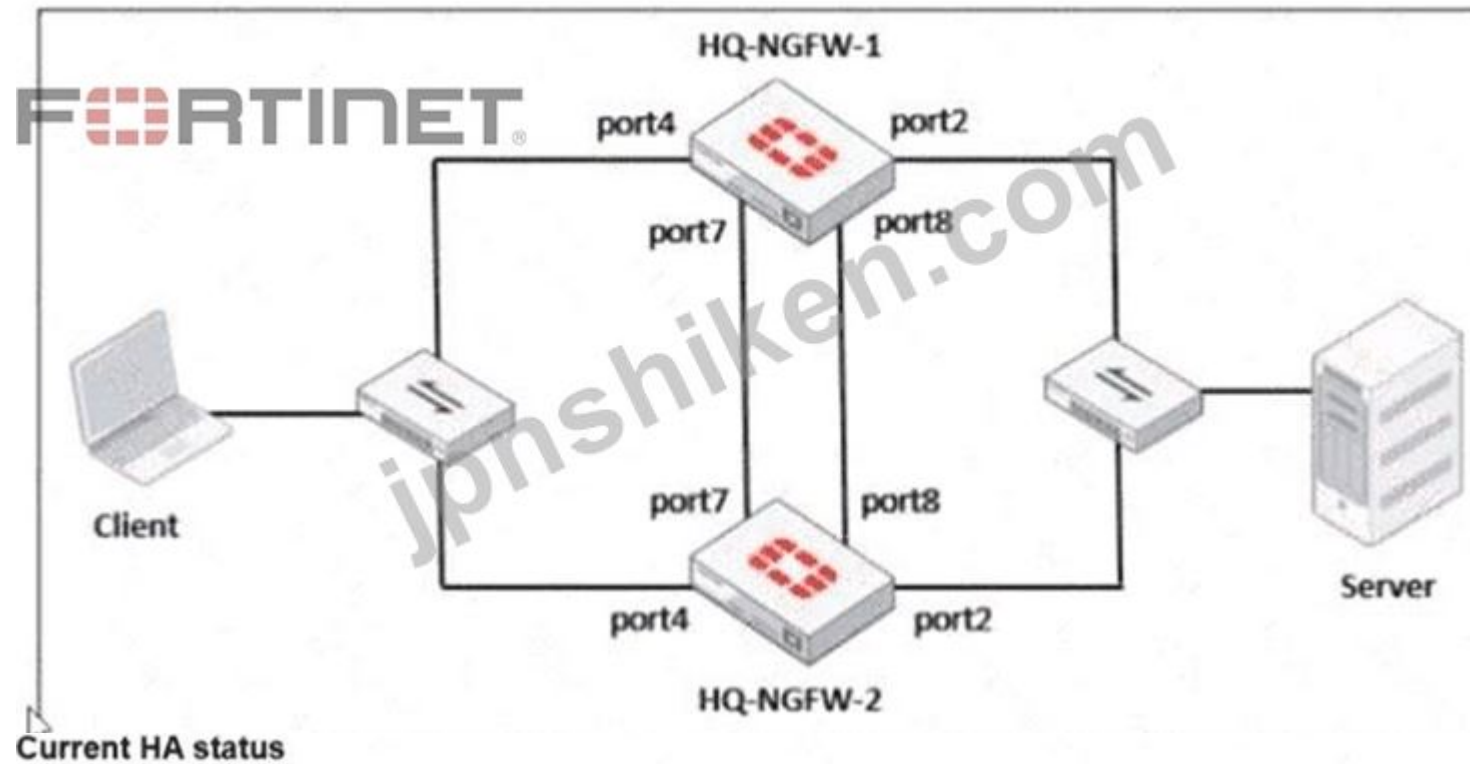
The administrator observed for 55 seconds, which is longer than 50 seconds, so the condition is met for long enough to trigger failover.

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.

質問: 18

展示資料を参照してください。

FortiGate HA cluster topology



```
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
Secondary: FGVM02TM24013501, HA operating index = 1
```

ew 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"
```

現在のHAステータスに基づいて、管理者は図に示すように、HQ-NGFW-1とHQ-NGFW-2のオーバーライドおよび優先度パラメータを更新します。HAクラスターではどのような結果が予想されるでしょうか？

- A. HQ-NGFW-2 はオーバーライド有効化設定を持ち、HQ-NGFW-1 よりも優先度が高いため、プライマリとして引き継ぎます。
- B. HQ-NGFW-2の優先度が低いため、HQ-NGFW-1がプライマリのままになります。
- C. オーバーライド設定はすべての HA メンバーで一致する必要があるため、HA クラスターは同期が取れなくなります。
- D. HQ-NGFW-1 はオーバーライド無効化設定を HQ-NGFW-2 と同期します。

正解: ([正解を表示します](#))

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.

質問: 19

展示資料を参照してください。

```
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"
```

展示されているログから、どのようなことが推測できますか？

- A. IPSソケットバッファがいっぱいです。IPSエンジンは新しいセッションを作成するためにより多くのメモリを必要としています。
- B. IPSソケットバッファがいっぱいで、IPSエンジンはパケットをデコードできません。
- C. IPS診断コマンドにより、バイパスモードオプション5でIPSスキャンが一時停止されます。
- D. ダーティフラグのため、IPSセッションスキャンが一時停止され、パケットが再評価されています。

正解: ([正解を表示します](#))

"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.

質問: 20

展示資料を参照してください。

部分的な雲のトポロジーを示す。



AWS上にFortiGateクラウドネイティブファイアウォール(CNF)をデプロイしました。

デプロイメント中に、FortiGate CNFはEC2インスタンスからのトラフィックを処理するために、どのコンポーネントを作成する必要がありますか？

- A. 顧客VPCとGWLB
- B. 顧客の仮想プライベートクラウド (VPC) 内のゲートウェイロードバランサーエンドポイント (GWLB)
- C. CNF VPC。顧客VPC。およびGWLB
- D. 顧客VPC内のGWLB、GWLB、およびインターネットゲートウェイ (IGW)

正解: ([正解を表示します](#))

In the FortiGate Cloud-Native Firewall (CNF) for AWS architecture, traffic from workloads (such as an EC2 instance) in the customer VPC is redirected to the security service (FortiGate CNF) using AWS Gateway Load Balancer (GWLB) technology.

The key AWS component that must exist inside the customer VPC to steer workload traffic to the GWLB is the:

Gateway Load Balancer Endpoint (GWLB)

This endpoint is what the customer VPC routes point to (for example, default route or subnet route entries), enabling transparent insertion of the FortiGate CNF inspection path for EC2 traffic.

Why the other options are not correct:

A: CNF does not "create the customer VPC" (that is customer-owned), and "GWLB" is the only relevant created item here, not the whole VPC.

C: Customer VPC is not created by CNF, and GWLB is typically part of the CNF service side; the question specifically asks what must be created to handle traffic from the EC2 instance (that requires GWLB in the customer VPC).

D: CNF does not create the Internet Gateway (IGW) in the customer VPC, and IGW is not the required CNF- created component for steering traffic to FortiGate CNF.

質問: 21

展示資料を参照してください。

IPsec tunnel configuration



ネットワーク管理者が、2台のFortiGateデバイス間のIPsecトンネルのトラブルシューティングを行っています。管理者は、フェーズ1が確立できなかったことを確認しました。また、両方のFortiGateデバイスに事前共有キーを再入力し、キーが一致していることを確認しました。

フェーズ1の構成と図表に基づいて、管理者はフェーズ1を起動するためにどの2つの構成変更を行うことができますか？(2つ選択してください。)

- A. HQ-NGFW で、Diffie-Hellman グループ 2 を無効にします。
- B. HQ-NGFW で、IKE モードを Main (ID 保護) に設定します。
- C. BR1-FGT で、ポート 2 をインターフェイスに設定します。
- D. 両方の FortiGate デバイスで、デッド ピア検出をオンデマンドに設定します。

正解: [\(正解を表示します\)](#)

Exact Extract:

"In IKEv1, there are two possible modes in which the IKE SA negotiation can take place: main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel."

"When both peers know each other 's IP address or FQDN, you may want to use main mode to take advantage of its more secure negotiation. In this case, FortiGate can identify the remote peer by its IP address and, as a result, associate it with the correct IPsec tunnel."

"FortiGate supports three DPD modes... The default DPD mode is On Demand ."

" Diffie-Hellman (DH) ... is used during IKE SA negotiation. The use of DH in phase 1 is mandatory and can't be disabled . You must select at least one DH group." Technical Deep Dive:

The correct answers are B and C .

B is correct because phase 1 fails when IKE mode settings do not match between peers. The study guide explicitly says phase 1 settings on both ends must agree. Since this is a static site-to-site tunnel and both peers know each other's IP addresses, Main (ID protection) is the appropriate mode.

C is correct based on the exhibit: BR1-FGT appears bound to the wrong physical interface. The screenshot shows Interface = port1 , while the diagram/answer choice indicates the tunnel should be using port2 . If the phase 1 is bound to the wrong WAN interface, FortiGate sends IKE packets out the wrong path and phase 1 will not come up.

Why the others are not the fix:

* A is not correct because DH is mandatory in phase 1. The issue is not "disable DH group 2" by itself; the real requirement is that the peers negotiate a compatible proposal. The option as written is not the proper corrective action from the guide.

* D is not correct because DPD does not determine whether phase 1 can initially establish. It is a tunnel health/failure-detection feature after negotiation behavior, and On Demand is already the default mode.

質問: 22

メンバー選択のための有効なSD-WANルール戦略はどれですか？(3つ選択してください)

- A. 負荷分散なしの最低コスト (SLA)
- B. 負荷分散による手動操作
- C. 負荷分散を伴う最低品質 (SLA)
- D. 負荷分散による最低コスト (SLA)
- E. ロードバランシングによる最高品質

正解: ([正解を表示します](#))

According to the FortiOS 7.6 Administrator Study Guide and official documentation, SD-WAN rules (services) determine the path selection for traffic matching specific criteria. Version 7.6 provides specific flexibility regarding how these strategies handle multiple member interfaces.

First, Manual with load balancing (Statement B) is a valid configuration. In the Manual strategy, the administrator orders interfaces by preference, but by enabling the Load balancing toggle, the FortiGate can distribute traffic across all members that are up.

Second, the Lowest Cost (SLA) strategy has been enhanced to support two modes. When the load balancing option is disabled, it acts as Lowest Cost (SLA) without load balancing (Statement A), selecting the single lowest-cost link that meets the SLA. Alternatively, by enabling the toggle, it functions as Lowest Cost (SLA) with load balancing (Statement D), where the FortiGate distributes traffic across all interfaces that satisfy the SLA target, regardless of their individual costs.

Statements C and E are incorrect because " Lowest Quality " is not a recognized SD-WAN strategy, and the Best Quality strategy is specifically a priority-based selection for a single " best " link, meaning the load balancing toggle is not available in the GUI when this mode is selected.

質問: 23

展示資料を参照してください。

Refer to the exhibit.

Packet trace output	
Time	Message
Packet Trace #1 04	
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	checked 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
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)

FortiGate デバイスはなぜパケットをドロップしたのですか？

- A. デフォルトの暗黙のファイアウォールポリシーに一致しました。
- B. RPFチェックに失敗しました。
- C. 明示的に設定されたファイアウォール ポリシーに一致し、アクションは DENY でした。
- D. ネクストホップIPに到達できません。

正解: [\(正解を表示します\)](#)

"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.

質問: 24
展示資料を参照してください。



Phase 2 selectors

[+ Create new](#) [Edit](#) [Delete](#)[+ Search](#)

Name	Local Address	Remote Address	Comments
ToBR1	10.0.11.0/255.255.255.0	172.20.1.0/255.255.255.0	

Edit Phase 2 Selector

Name ToBR1

Comments

0/255

Encapsulation **Tunnel Mode** Transport ModeIP version **IPv4** IPv6Named address ☐

Remote address IP Address Subnet Address IP Range

172.20.1.0 255.255.255.0

Advanced

Encryption - authentication AES128 SHA1

Replay detection ☒ Enable ☐ DisablePerfect forward secrecy (PFS) ☒ Enable ☐ Disable

Diffie-Hellman groups

☐ 1	☐ 2	☒ 5
☐ 14	☐ 15	☐ 16
☐ 17	☐ 18	☐ 19
☐ 20	☐ 21	☐ 27
☐ 28	☐ 29	☐ 30
☐ 31	☐ 32	

Local port **All** SpecifyRemote port **All** SpecifyProtocol **All** Specify

Phase 2 selectors

[+ Create new](#) [Edit](#) [Delete](#)[+ Search](#)

Name	Local Address	Remote Address	Comments
ToHQ	172.20.1.0/255.255.255.0	10.11.0.0/255.255.255.0	

Edit Phase 2 Selector

Name ToHQ

Comments

0/255

Encapsulation **Tunnel Mode** Transport ModeIP version **IPv4** IPv6Named address ☐

Remote address IP Address Subnet Address IP Range

10.11.0.0 255.255.255.0

Advanced

Encryption - authentication AES256 SHA1

Replay detection ☒ Enable ☐ DisablePerfect forward secrecy (PFS) ☒ Enable ☐ Disable

Diffie-Hellman groups

☐ 1	☐ 2	☒ 5
☒ 14	☐ 15	☐ 16
☐ 17	☐ 18	☐ 19
☐ 20	☐ 21	☐ 27
☐ 28	☐ 29	☐ 30
☐ 31	☐ 32	

Local port **All** SpecifyRemote port **All** SpecifyProtocol **All** Specify



ネットワーク管理者が、2台のFortiGateデバイス間のIPsecトンネルのトラブルシューティングを行っています。管理者は、フェーズ1の状態は正常であることを確認しましたが、フェーズ2が起動しないことが判明しました。

図に示されているフェーズ2の構成に基づいて、フェーズ2を起動させるには、どの2つの構成変更が必要ですか？(2つ選択してください。)

- A. BR1-FGT で、リモートアドレスを 10.0.11.0/255.255.255.0 に設定します。
- B. HQ-NGFW で、Diffie-Hellman グループ 2 を有効にします。
- C. BR1-FGTで、秒数を43200に設定します。
- D. HQ-NGFW で暗号化を AES256 に設定します。

正解: ([正解を表示します](#))

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 # does not match HQ's local subnet (10.0.11.0/24)

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 10.0.11.0/255.255.255.0.

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.

質問: 25

コレクターエージェントがADポーリングに使用する3つの方法はどれですか？(3つ選択してください)

- A. NetAPI

- B. WMI
- C. WinSecLog
- D. DNS逆引きルックアップ
- E. FSSO REST API

正解: ([正解を表示します](#))

"As previously stated, collector agent-based polling mode has three methods (or options) for collecting login information. The order on the slide from left to right shows most recommend to least recommended:

- * WMI ...
- * WinSecLog ...
- * NetAPI ..."

Technical Deep Dive:

The correct three AD polling methods are WMI, WinSecLog, and NetAPI . These are the collector-agent polling options FortiGate FSSO uses against Windows domain controllers. WMI is generally the most efficient because the DC returns requested login events directly. WinSecLog polls Windows Security Event Logs and is typically more reliable than NetAPI for not missing recorded logons. NetAPI can be faster, but it is more prone to missing events under load because it depends on temporary session information rather than persistent security logs.

Why the other options are wrong:

DNS reverse lookup is not one of the three AD polling methods. DNS is used by FSSO to resolve workstation names to IP addresses and to track IP changes, but it is not itself a polling method for collecting AD logon events. FSSO REST API is also not one of the documented collector-agent AD polling methods in the study guide.

From an operational standpoint, FSSO login collection and workstation verification are separate functions.

The collector agent may still rely on DNS and workstation checks after a login is learned, but the actual AD polling methods remain only WMI, WinSecLog, and NetAPI . On a FortiGate, when troubleshooting FSSO behavior, you would typically validate the collector feed and user cache with commands such as:

```
diagnose debug authd fsso list
```

```
diagnose debug authd fsso server-status
```

Those commands help confirm whether the users gathered by the collector through one of those three polling methods are reaching FortiGate correctly.

質問: **26**

展示資料を参照してください。

Web filter configuration

Edit Web Filter Profile

Feature set **Flow-based** Proxy-based

☒ FortiGuard Category Based Filter

☒ Allow

☐ Monitor

☐ Block

☐ Warning

☐ Authenticate

Name	Action
Web-based Applications	☒ Allow
Entertainment	☒ Allow
Arts and Culture	☒ Allow
Education	☒ Allow
Health and Wellness	☒ Allow
Job Search	☒ Allow
Medicine	☒ Allow
News and Media	☒ Allow
Social Networking	☐ Block

53% 95

☐ Allow users to override blocked categories

☒ Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ☐

☒ Static URL Filter

Block Invalid URLs ☐

URL Filter ☒

+ Create New

Edit

Delete

Search

URL	Type	Action	Status
www.facebook.com	Wildcard	☐ Monitor	☒ Enable



ウェブフィルタの設定が表示されます。

管理者は、Facebook以外のすべてのソーシャルネットワーキングサイトへのアクセスをブロックするようにWebフィルタプロファイルを設定しました。しかし、ユーザーがFacebook.comにアクセスしようとする、FortiGuardのWebフィルタリングブロックページにリダイレクトされます。

提示された資料に基づき、管理者はFacebookへのアクセスを許可しつつ、他のすべてのソーシャルネットワーキングサイトをブロックするために、どのような設定変更を行う必要がありますか？

- A. FortiGuardのカテゴリベースフィルタで、ソーシャルネットワーキングのアクションを警告に設定します。
- B. 静的URLフィルタセクションでタイプを「シンプル」に変更します。
- C. Webフィルタプロファイルの機能セットをプロキシベースに変更します。
- D. 静的URLフィルタで、www.facebook.comのアクションを「除外」に設定します。

正解: [\(正解を表示します\)](#)

The issue occurs because Facebook still belongs to the Social Networking category, and that category is configured with a Block action. A static URL filter entry with Monitor or Allow does not fully bypass later FortiGuard category filtering. In FortiOS web filtering, static URL filtering is evaluated before FortiGuard category filtering. The Exempt action is specifically used for trusted URLs that must bypass the remaining security inspections and category-based web filtering decisions. Therefore, to allow only Facebook while keeping the Social Networking category blocked, the administrator must configure the static URL filter entry for www.facebook.com with the action Exempt. Changing the entire Social Networking category to Warning would weaken the intended policy, and changing the URL type or feature set does not directly override the category block.

質問: 27

SD-WANにおける3つの重要なルーティング原則は何ですか？(3つ選択してください)

- A. デフォルトでは、含まれる SD-WAN メンバーが宛先への有効なルートを持っていない場合、SD-WAN ルールはスキップされます。
- B. SD-WAN ルールは、他のどのタイプのルートよりも優先されます。
- C. 通常のポリシー ルートは SD-WAN ルールよりも優先されます。
- D. デフォルトでは、宛先へのルートが 1 つしかない場合、SD-WAN ルールはスキップされます。
- E. デフォルトでは、宛先への最適なルートが SD-WAN メンバーでない場合、SD-WAN ルールはスキップされます。

正解: ([正解を表示します](#))

"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.

質問: 28

ネットワーク管理者がFortiGateでSSLのフルインスペクションとWebフィルタリングを有効にしました。HTTPSウェブサイトアクセスすると、ブラウザに証明書の警告エラーが表示されます。HTTPウェブサイトアクセスすると、ブラウザはエラーを報告しません。

証明書の警告エラーが発生する理由は何ですか？

A. SSL/SSH 検査プロファイルで、無効な SSL 証明書のオプションが許可されるように設定されています。

B. 一致するファイアウォールポリシーはプロキシ検査モードに設定されています。

C. ブラウザは、FortiGate が SSL 検査に使用する証明書を信頼していません。

D. FortiGate が SSL 検査に使用する証明書には、必要な証明書拡張機能が含まれていません。

正解: ([正解を表示します](#))

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

質問: 29

管理者は、特定の期間内に設定されたシグネチャに指定された回数だけ一致するトラフィックをブロックするようにIPSセンサーを設定したいと考えています。管理者はこの目的をどのように達成できるでしょうか？

- A. IPSグループ署名を使用し、レートモードを60に設定します。
- B. IPSパケットログオプションを定期フィルタオプションとともに使用します。
- C. IPS署名、レートモード定期オプションを使用します。
- D. IPSフィルタ、レートモード定期オプションを使用します。

正解: **C** ([コメントを发表する](#))

" 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.

質問: 30

展示資料を参照してください。

ルーティングテーブルが表示されます

Network ⇅	Gateway IP ⇅	Interfaces ⇅	Distance ⇅	Metric ⇅	Priority ⇅	Type ⇅
10.0.11.0/24	0.0.0.0	port4	0	0	0	Connected
10.0.12.0/24	0.0.0.0	port5	0	0	0	Connected
10.0.13.0/24	0.0.0.0	port6	0	0	0	Connected
10.0.14.0/24	0.0.0.0	port2	0	0	0	Connected
100.66.0.0/24	0.0.0.0	port3	0	0	0	Connected
172.20.1.0/24	100.66.0.254	port3	9	0	2	Static
192.168.0.0/16	0.0.0.0	port1	0	0	0	Connected

管理者は、サブネット 172.20.1.0/24 へのトラフィックがポート 2 のみを経由するように、新しい静的ルートを作成したいと考えています。この目的を達成するために管理者が使用できる 2 つの基準は何ですか？(2 つ選択してください。)

- A. 新しい静的ルートの優先度は 3 に設定する必要があります。
- B. 新しい静的ルートのメトリックは 1 に設定する必要があります。
- C. port3 を経由する既存の静的ルートの距離を 11 に設定する必要があります。
- D. 新しい静的ルートの距離は9に設定する必要があります

正解: [\(正解を表示します\)](#)

From the routing table in the exhibit, there is already a static route for 172.20.1.0/24 pointing out port3 with:

Distance = 9

Priority = 2

Type = Static

In FortiOS, route selection prefers (in order) the route with the lowest administrative distance to a destination.

Therefore, to make traffic to 172.20.1.0/24 go through port2 only, the administrator must ensure the port2 static route is more preferred than the existing port3 route.

Why C is correct

C). The existing static route through port3 must have the distance set to 11.

If the existing port3 route distance is increased to 11, then a new port2 route with distance 9 will be preferred (9 < 11). This makes the port3 route a backup route instead of the active one.

Why D is correct

D). The new static route must have the distance set to 9

Setting the new port2 route distance to 9 (and increasing the port3 route to 11 as in option C) ensures FortiGate selects the port2 route as the best route for 172.20.1.0/24.

Why A and B are not correct

A (priority 3): By itself it does not guarantee selection over the existing route, and FortiOS route choice is driven primarily by distance.

B (metric 1): Metric is not the primary selector for static route preference compared to administrative distance in this scenario.

So the two criteria that achieve the objective are:

Make the existing port3 route less preferred by increasing its distance (C) Ensure the new port2 route uses the preferred distance (D)

質問: 31

アプリケーション制御プロファイルを設定し、カテゴリータブでピアツーピアトラフィックを「ブロック」に設定して、ファイアウォールポリシーに適用しました。しかし、既知のポート上のピアツーピアトラフィックがブロックされずにFortiGateを通過しています。
この問題を解決するには、FortiGateのどの設定を確認すればよいですか？

- A. FortiGuardカテゴリ評価
- B. ネットワークプロトコルの強制
- C. UDPベースのアプリケーション用の置換メッセージ
- D. アプリケーションとフィルターのオーバーライド

正解: ([正解を表示します](#))

When the Application sensor receives traffic on that port, the protocol decoder will try to determine if the received data matches the HTTPS traffic In this case it will not match because it is P2P traffic, so this will class as violation and blocked The protocol decoder also try to determine what type of traffic it is, and even if it could not figure out it is P2P traffic, it still count as a violation because even though it does not know what it is, it knows for fact it is not HTTPS

有効的な**NSE4_FGT_AD-7.6-JPN**問題集はJPNTTest.com提供され、**NSE4_FGT_AD-7.6-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**NSE4_FGT_AD-7.6-JPN**試験問題集を提供します。JPNTTest.com NSE4_FGT_AD-7.6-JPN試験問題集はもう更新されました。ここで**NSE4_FGT_AD-7.6-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE4_FGT_AD-7.6-JPN-mondaishu **96**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **32**

FortiSASEのセキュアインターネットアクセス(SIA)エージェントベースモードを構成する2つのコンポーネントはどれですか？(2つ選択してください。)

- A. FortiSASE ファイアウォール・アズ・ア・サービス (FWaaS)
- B. プロキシ自動構成 (PAC) ファイル
- C. VPNポリシー
- D. FortiExtender

正解: ([正解を表示します](#))

In FortiSASE Secure Internet Access (SIA) agent-based mode, traffic steering and security enforcement rely on components integrated with the FortiClient agent.

Components used in SIA agent-based mode

A). FortiSASE Firewall-as-a-Service (FWaaS)

Correct.

FWaaS is a core security component of FortiSASE.

It enforces firewall policies, security inspection, and access control for agent-based users.

All user traffic tunneled by the agent is inspected by FWaaS.

C). VPN policies

Correct.

In agent-based mode, the FortiClient establishes a secure tunnel to FortiSASE.

VPN policies define:

Authentication

Access control

Traffic steering

These policies are fundamental to agent-based connectivity.

Why the other options are incorrect

B). Proxy auto-configuration (PAC) filePAC files are used in agentless or proxy-based modes, not agent-based SIA.

D). FortiExtenderFortiExtender is a WAN extension device and is unrelated to FortiSASE SIA agent-based architecture.

質問: 33

展示資料を参照してください

アクティブ認証を有効にするためのファイアウォールポリシーを示します。



有効な認証方法を使用して外部ウェブサイトにアクセスしようとした際に、ログイン画面が表示されない場合、最も可能性の高い原因は何でしょうか？

- A. このユーザーに一致するユーザーアカウントが存在しません。
- B. FSSO構成でRemote-usersグループが正しく設定されている必要があります。
- C. リモートユーザーグループが宛先に追加されていません
- D. ファイアウォール ポリシーでは、サービス DNS が必要です。

正解: (正解を表示します)

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.

質問: 34

FortiGateはFortiAnalyzerおよびFortiManagerと統合されています。

ファイアウォールポリシーを作成する際、FortiAnalyzerとFortiManagerの機能を強化し、ログ記録を有効にするために、管理者はどの属性を含める必要がありますか？

A. 普遍的に一意な識別子

B. ポリシーID

C. シーケンスID

D. ログID

正解: ([正解を表示します](#))

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.

質問: 35

ファイアウォールポリシーについては、添付資料を参照してください。



ファイアウォールポリシーが、例えばEICARのようなよく知られたウイルスをブロックしないのはなぜですか？(回答を1つ選択してください)

- A. ファイアウォール ポリシーのアクションが DENY に設定されていません。
- B. Webフィルタが有効になっていないため、ファイアウォールポリシーがウイルス対策プロファイルと連携しません。
- C. ファイアウォール ポリシーがプロキシ ベースの検査モードで構成されていません。
- D. ファイアウォール ポリシーでは、詳細なコンテンツ検査は適用されません。

正解: [\(正解を表示します\)](#)

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

"To perform SSL inspection on traffic flowing through the FortiGate device, you must allow the traffic with a firewall policy and apply an SSL inspection profile to the policy... For antivirus or IPS control, you should use a deep-inspection profile."

"When you use deep inspection, FortiGate impersonates the recipient of the originating SSL session, and then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient." Technical Deep Dive:

The exhibit shows that the policy is allowing HTTPS and the SSL/SSH inspection profile is certificate- inspection , not deep-inspection . That is the key issue. With certificate inspection, FortiGate can inspect only SSL metadata such as the certificate and SNI/hostname context; it cannot decrypt the HTTPS payload itself. Because EICAR is detected by antivirus through payload inspection, FortiGate must see the file contents. Without deep SSL inspection, the antivirus engine never gets the decrypted payload, so the file can pass even though the antivirus profile is attached.

Option A is incorrect because FortiGate firewall policies often use ACCEPT + security profile enforcement

; the session can still be blocked by antivirus after policy match. Option B is incorrect because web filter is not required for antivirus detection. Option C is incorrect because the real requirement is deep SSL inspection

, not specifically proxy-based mode; full SSL inspection is the deciding factor here.

In practice, to block EICAR over HTTPS, you would apply a deep-inspection SSL profile to the policy, for example:

config firewall policy

edit < policy-id >

```
set inspection-mode flow
set av-profile " default "
set ssl-ssh-profile " deep-inspection "
next
end
```

On real hardware, this also matters for performance design. Simple firewall/NAT sessions are often NP fast- pathed, but once you enable deep SSL inspection and content scanning, traffic is typically handed to CPU /WAD/content-inspection path for decryption and scanning, so throughput is lower than certificate-inspection or no-inspection.

質問: 36

ファイアウォールポリシーを設定する際、ポリシーIDに関して次のうちどれが正しいですか？(2つ選択してください。)

- A. ファイアウォールポリシーIDは、ファイアウォールポリシーにおけるポリシー実行の順序を識別します。
- B. ポリシーが作成されると、ポリシー ID は変更できません。
- C. CLIでポリシーID 0のポリシーを作成できます
- D. GUI または CLI に関係なく、ファイアウォール ポリシーを作成する際には、ポリシー ID を指定することが必須です。

正解: [\(正解を表示します\)](#)

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.

質問: 37

展示資料を参照してください。



Medicine	☒ Allow
News and Media	☒ Allow
Social Networking	☒ Allow
Political Organizations	☒ Allow
Reference	☒ Allow
Global Religion	☒ Allow
Shopping	☒ Allow
Society and Lifestyles	☒ Allow
58% 93	

☐ Allow users to override blocked categories

☐ Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ☐

☐ Static URL Filter

Block invalid URLs ☐

URL Filter ☒

+ Create New Edit Delete Search			
URL	Type	Action	Status
www.facebook.com	Simple	☒ Monitor	☒ Enable

Firewall policy configuration

Edit Policy

Firewall/Network Options

Inspection mode

Flow-based

Proxy-based

NAT



IP pool configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve source port



Protocol options

PROXY

default

Security Profiles

AntiVirus



Web filter



WEB

default

Video filter



DNS filter



Application control



IPS



File filter



SSL inspection

SSL

certificate-inspection

FortiGuard block page



ウェブフィルタプロファイルの設定とファイアウォールポリシーの設定が表示されます。

あなたはwww.facebook.comにアクセスしようとしていますが、FortiGuardのWebフィルタリングブロックページにリダイレクトされます。

展示物に基づいて、この問題の考えられる原因は何ですか？

- A. Webレーティングの上書き設定が正しくありません。
- B. Webフィルタプロファイル機能セットの設定が正しくありません。
- C. ファイアウォールポリシーの検査モードが正しくありません。
- D. www.facebook.com の URL フィルタの動作が正しくありません。

正解: ([正解を表示します](#))

From the exhibits:

The Web Filter profile is configured with Feature set = Flow-based.

The Firewall policy is configured with Inspection mode = Proxy-based and has Web Filter enabled.

In FortiOS 7.6, security profiles that have a feature set selection (Flow-based vs Proxy-based) must match the inspection mode used by the firewall policy. If the profile's feature set does not match the policy's inspection mode, the profile behavior will not align with what the administrator expects (and in many cases FortiOS will prevent correct use/selection, or the feature behavior will not apply as intended).

That mismatch explains why the configured URL filter entry for www.facebook.com (set to Monitor) is not producing the expected result, and instead the session is being evaluated by category rating and blocked (shown as Malicious Websites on the FortiGuard block page).

Why the other options are not the best fit:

A: A web rating override is not shown in the exhibits, and nothing indicates an override misconfiguration.

C: While the policy inspection mode could be changed, the root cause shown is the profile feature set mismatch (profile is Flow-based).

D: The URL filter action shown is Monitor, which would not produce a block page by itself.

質問: 38

本社FortiGateには、アグレッシブモードで設定された複数のダイヤルアップIPsec VPNが存在します。要件は、ダイヤルアップユーザーをそれぞれの部署のVPNトンネルに接続することです。ユーザーとトンネルをマッチングさせるために、フェーズ1のどの設定を構成できますか？

A. ローカルゲートウェイ

B. デッドピア検出

C. ピアID

D. IKEモード設定

正解: ([正解を表示します](#))

In FortiOS 7.6, when multiple dialup IPsec VPNs are configured on the same FortiGate-especially in Aggressive Mode-FortiGate must identify which Phase 1 configuration a connecting client should match.

How FortiGate selects a dialup IPsec tunnel

For dialup VPNs:

The remote peer (user or device) does not have a fixed IP address

Multiple Phase 1 interfaces may exist on the HQ FortiGate

FortiGate uses identifying information sent during IKE Phase 1 to select the correct tunnel Aggressive Mode behavior Aggressive mode sends ID information in clear text during Phase 1 This allows FortiGate to match incoming peers to the correct Phase 1 configuration Why Peer ID is the correct answer C). Peer ID Peer ID (also called IKE ID) is used to:

Identify the remote peer

Differentiate between multiple dialup tunnels

Common Peer ID formats:

FQDN

User FQDN

Key ID

FortiGate matches the received Peer ID against the Phase 1 configuration to select the correct tunnel This is the documented and recommended method for:

Mapping users to different department tunnels

Supporting multiple dialup IPsec VPNs in aggressive mode

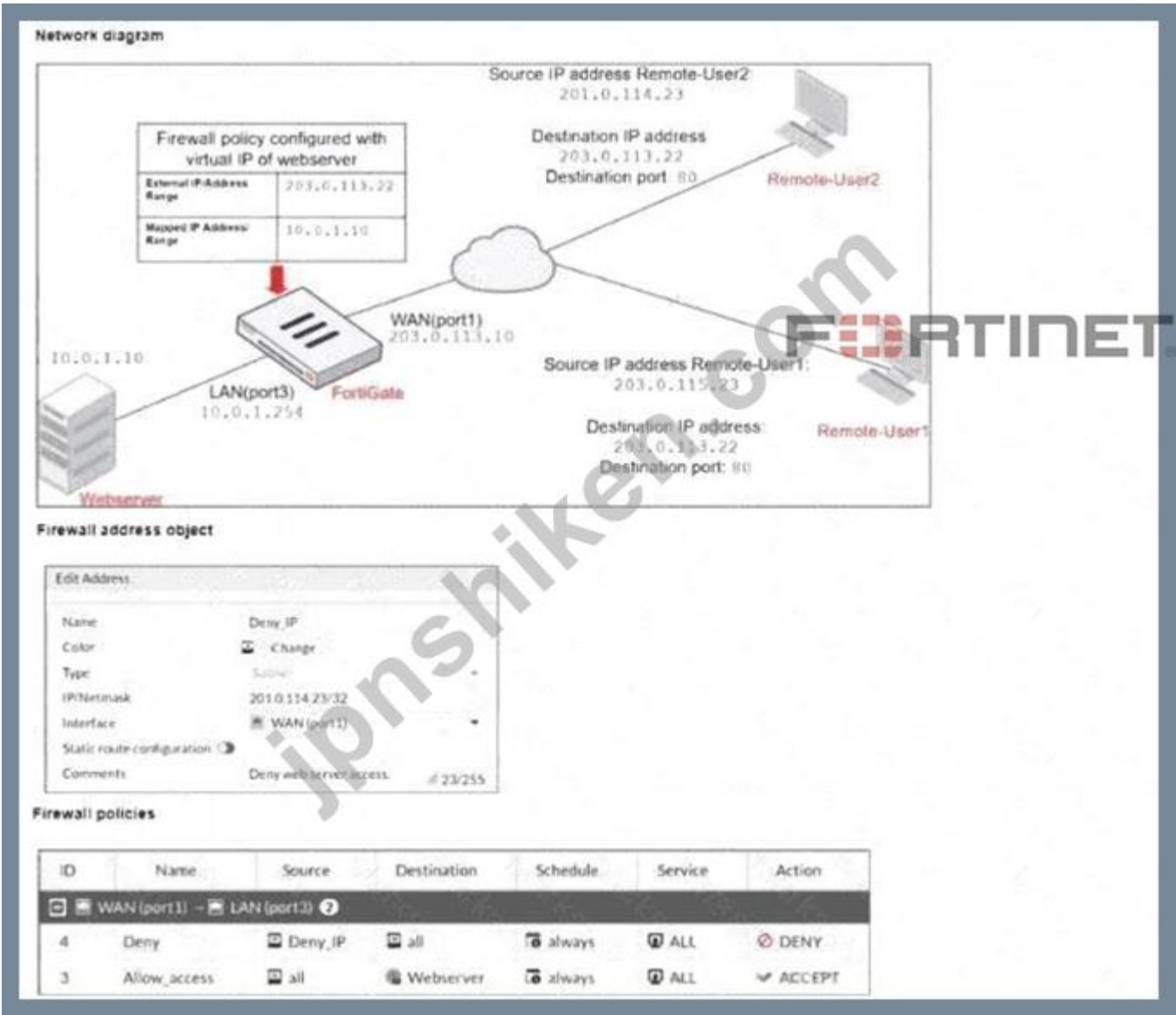
Why the other options are incorrect

A). Local GatewayIdentifies the local FortiGate interface/IP, not the remote user.

B). Dead Peer DetectionUsed only for tunnel health monitoring, not tunnel selection.

D). IKE Mode ConfigUsed for assigning IP addresses and pushing settings, not for selecting the Phase 1 tunnel.

質問: 39
展示資料を参照してください。



展示資料には、ネットワークに接続されたFortiGateデバイスの図と、ファイアウォールの設定図が示されている。
管理者は、Remote-User2 による Web サーバーへのアクセスを拒否するために、デフォルト設定の拒否ポリシーを作成しました。
このポリシーは、Remote-User1がWebサーバーにアクセスできる一方で、Remote-User2がWebサーバーにアクセスできないように動作する必要があります。管理者は、デフォルトの動作に加えて、拒否ファイアウォールポリシーにどのような追加設定を追加すれば、Remote-User2によるWebサーバーへのアクセスをブロックできるでしょうか？
(いずれか1つを選択してください)

A. Allow_access ポリシーで match-vip を無効にします。
B. 新しいポリシーで 1 対 1 IP プール オブジェクトを設定します。
C. 拒否ポリシーで宛先アドレスをWebサーバーに設定します。
D. Allow_access ポリシーで宛先アドレスを Deny_IP に設定します。

正解: C (コメントを发表する)

"The example on this slide shows how FortiGate handles two incoming connections to the same external address, but on different ports... Both connections match the firewall policy ID, which references two VIPs and firewall address objects are completely different. They are stored separately with no overlap. Starting in version 7.2.4, the parameter match-vip is enable by default and allows the firewall address objects to match VIPs."

"In the example shown on this slide, the destination of the first firewall policy is set to all . This means all destination addresses (0.0.0.0/0), by default, including the external addresses defined

B.



C.

```
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
```

D.

正解: (正解を表示します)

質問: 41

マルチWAN構成でFortiGateを設定する際、管理者はなぜインターフェースでセッション保持を有効にするのでしょうか？(回答を1つ選択してください)

- A. WANリンクが故障した際に、FortiGateがすべてのアクティブなセッションのインターフェースを動的に変更できるようにする。
- B. ソースNATが有効になっていないすべてのセッションが常にプライマリWANリンクを使用するようにする
- C. WANリンクが変更された際にユーザーに再度認証を強制することでセキュリティを向上させる
- D. ルート変更が発生した場合でも、既存のSSL VPN接続が同じインターフェース上に維持されるようにするため

正解: D (コメントを发表する)

A closely related routing principle from the guide is:

"For each session, FortiGate performs two route lookups... After completing these two lookups, FortiGate writes the routing information to its session table. Subsequent packets are routed according to the session table, not the routing table." Also, the guide notes an HA limitation that helps explain the same design principle for FortiGate-terminated sessions: "Enabling session pickup allows active sessions to be seamlessly handed picked up by the new primary in the event of an HA failover... Note that there are some limitations to this - for example, any sessions that terminate at the FortiGate itself (e.g. SSL VPN, proxy sessions) cannot be handed off to another FortiGate and must be restarted on the new primary." Technical Deep Dive: The correct answer is D .

In multi-WAN environments, session preservation is used so that traffic for sessions that are tightly bound to the FortiGate interface they terminate on-most notably SSL VPN and other FortiGate-terminated flows- does not suddenly switch to another egress interface just because the routing table changes. Those sessions are sensitive to interface consistency. If replies start leaving through a different WAN after a route recalculation, the remote peer may see an address/interface mismatch and the session can break.

That means:

- * A is the opposite of session preservation. Preservation is meant to avoid moving active sessions around.
- * B is not the purpose of the feature.
- * C is unrelated.

* D correctly describes why an administrator would enable it.

Operationally, this matters most for SSL VPN , management-plane flows, and other sessions that terminate on the FortiGate itself , not just ordinary transit traffic. Transit sessions are generally tracked in the session table and can often survive normal routing behavior more gracefully, but FortiGate-terminated sessions are much more sensitive to WAN/interface changes.

有効的な**NSE4_FGT_AD-7.6-JPN**問題集はJPNTest.com提供され、**NSE4_FGT_AD-7.6-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**NSE4_FGT_AD-7.6-JPN**試験問題集を提供します。JPNTest.com NSE4_FGT_AD-7.6-JPN試験問題集はもう更新されました。ここで**NSE4_FGT_AD-7.6-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/NSE4_FGT_AD-7.6-JPN-mondaishu **96**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」