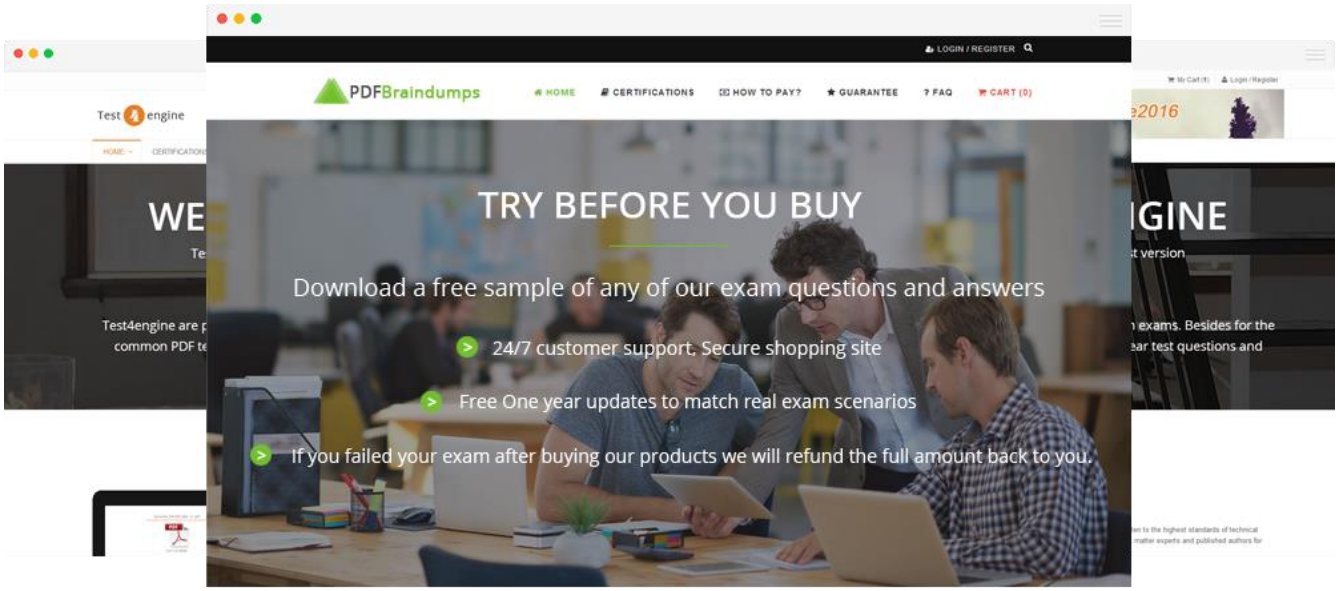
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **NSE4_FGT_AD-7.6-JPN**

Title : Fortinet NSE 4 - FortiOS 7.6 Administrator (NSE4_FGT_AD-7.6日本語版)

Vendor : Fortinet

Version : DEMO

QUESTION NO: 1
SD-
WANのパフォーマンスSLAに関する記述のうち、正しいものはどれですか？(3つ選択してください。)
A.セッションの損失とジッターに依存します。
B.FortiGate デバイスの状態を監視します。
C. すべてのSLAターゲットを設定できます。
D. これらはSD-WANルールの最低コスト戦略で適用されます。
E.能動的または受動的に測定できます。
Answer: C D E
Explanation:
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.

QUESTION NO: 2

エージェントレスのセキュアWebゲートウェイ(SWG)エンドポイントを導入し、セキュアインターネットアクセス(SIA)を実現しようとしています。ユーザーのWeb以外のトラフィックはどうなりますか？(回答を1つ選択してください)

A. Web以外のトラフィックはすべてFortiSASEをバイパスします。

B.エンドポイントはスプリットトンネリングを使用して、Web以外のトラフィックをFortiSASEにリダイレクトします。

C. FortiSASE はファイアウォール・アズ・ア・サービス (FWaaS) を使用して、Web 以外のトラフィックをリダイレクトします。

D. FortiSASE は SWG を使用して非 Web トラフィックを FortiExtender にリダイレクトします。

Answer: A

Explanation:

"In this use case, FortiSASE acts as an SWG and distributes a proxy auto-configuration (PAC) file to end users, enabling the FortiSASE SWG service as an explicit web proxy. SWG deployment secures only web traffic protocols, such as HTTP and HTTPS."

"All other nonweb traffic bypasses FortiSASE and is forwarded directly to the internet."

Technical Deep Dive:

The correct answer is A .

In agentless SWG-based SIA , FortiSASE is operating as an explicit web proxy using a PAC file . That model captures only web protocols , specifically HTTP and HTTPS . It does not create a full tunnel for the endpoint like agent-based FortiClient deployment does.

So the design implication is simple: nonweb traffic does not traverse FortiSASE in this onboarding model.

It goes directly to the internet from the endpoint.

Why the other options are wrong:

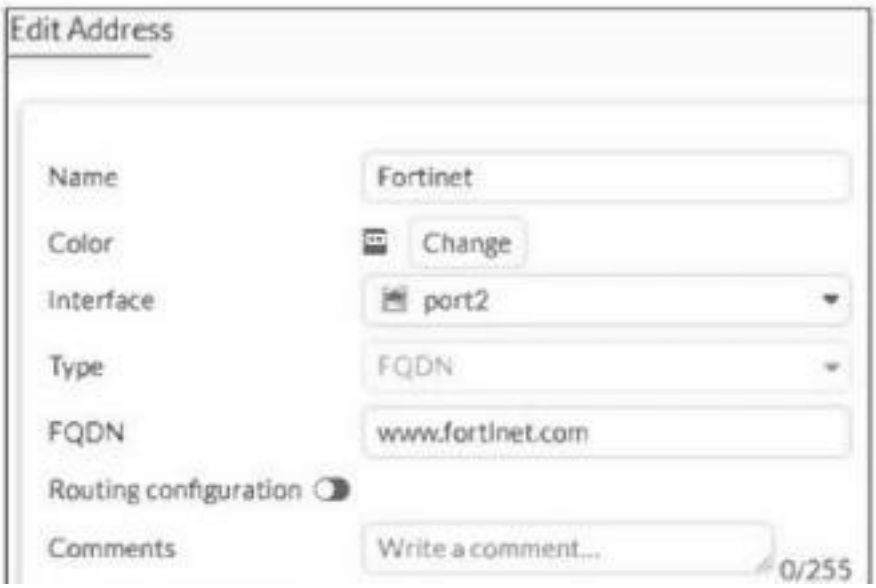
* B is wrong because this is not split-tunnel VPN behavior.
* C is wrong because FWaaS does not automatically capture nonweb traffic in the agentless SWG model.
* D is wrong because SWG does not redirect nonweb traffic to FortiExtender.

This is an important deployment distinction:

* Agent-based SIA can steer broader endpoint traffic through FortiSASE.
* Agentless SWG SIA secures only browser-based web traffic.

QUESTION NO: 3

展示資料を参照してください。



管理者が静的ルートの宛先として使用する新しいファイアウォールアドレスを作成しました。管理者が新しい静的ルートの宛先フィールドで新しいアドレスを選択できないのはなぜですか？(回答を1つ選択してください)

A. 新しい静的ルートでは、管理者は名前付きアドレスを選択する必要があります。

B. 新しいファイアウォールアドレスでは、まず FQDN
アドレスを解決する必要があります。

C.
新しい静的ルートでは、管理者はまずインターフェースをポート2に設定する必要があります。

D. 新しいファイアウォールアドレスでは、ルーティング設定を有効にする必要があります。

Answer: D

Explanation:

"If you create a firewall address object with the type Subnet or FQDN, you can use that firewall address as the destination of one or more static routes. First, enable Routing configuration in the firewall address configuration. After you enable it, the firewall address object becomes available for use in the Destination drop-down list for static routes with named addresses. " Technical Deep Dive:

The correct answer is D . The exhibit shows an FQDN address object (www.fortinet.com), but Routing configuration is disabled. FortiGate does not make that object available as a selectable destination for named static routes until this option is enabled.

Why the others are wrong:

* A is incomplete. Even if the static route uses Named Address , the object still will not appear unless Routing configuration is enabled on the address object.
* B is not the first requirement from the study guide. DNS resolution matters operationally for FQDN objects, but the documented reason it does not appear in the drop-down is the missing Routing configuration setting.
* C is unrelated. The interface does not have to be set to port2 first just to make the address object selectable.

In practice, the fix is:

config firewall address

edit " Fortinet "
set type fqdn
set fqdn " www.fortinet.com "
set allow-routing enable
next
end
After that, the object becomes available in the static route Destination field when using a named address.

QUESTION NO: 4
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
Answer: C
Explanation:
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.

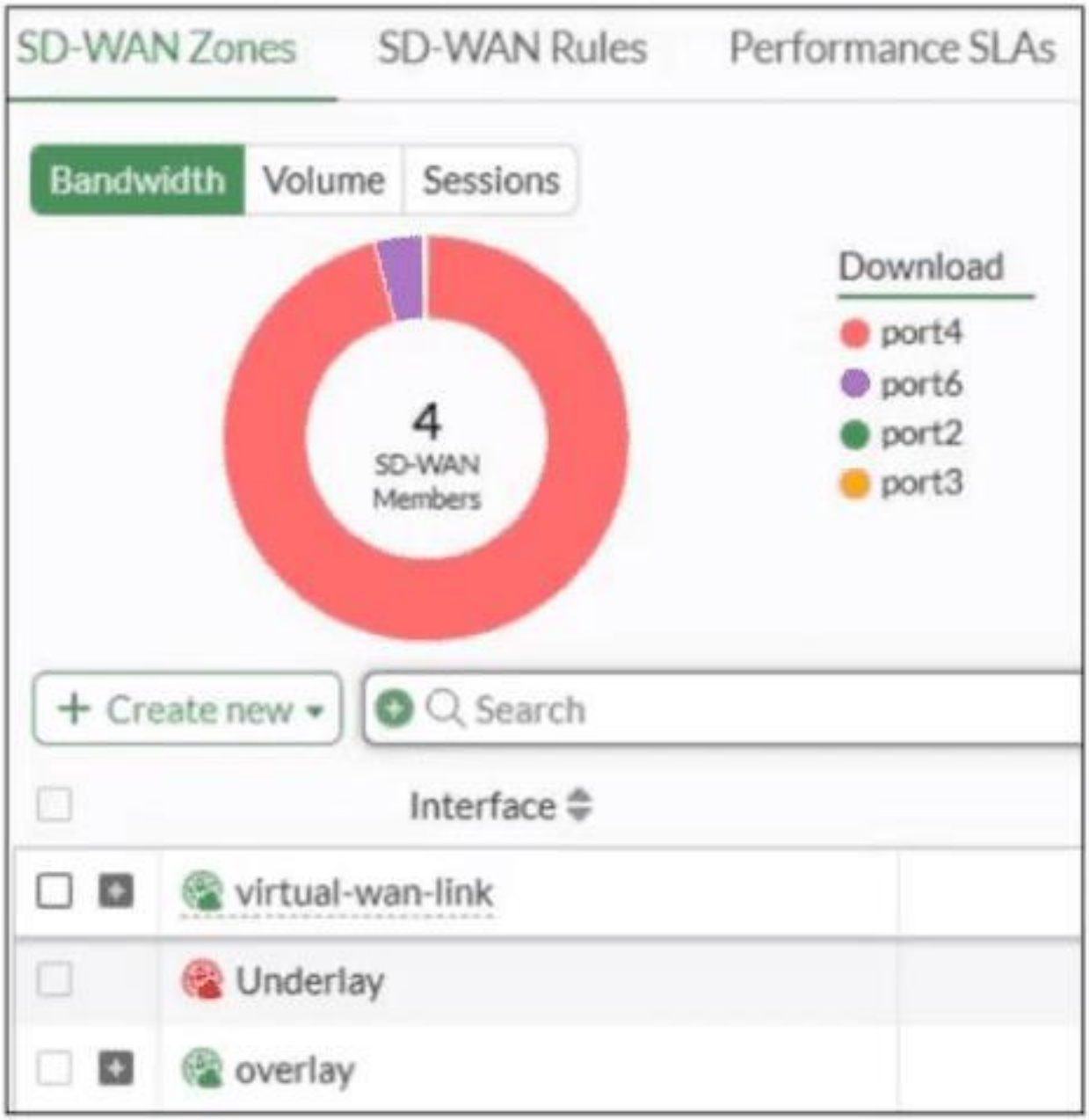
QUESTION NO: 5
HAオーバーライド設定が有効になっている場合、FortiGateの主要な選出プロセスは何ですか？(回答を1つ選択してください)
A. 接続されている監視対象ポート > 優先度 > HA稼働時間 > FortiGateシリアル番号
B. 監視対象ポート > 優先度 > システム稼働時間 > FortiGate シリアル番号
C. 接続されている監視対象ポート > HA稼働時間 > 優先度 > FortiGateシリアル番号
D. 監視対象ポート > システム稼働時間 > 優先度 > FortiGate シリアル番号
Answer: A
Explanation:
According 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.

QUESTION NO: 6
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。
Answer: A
Explanation:
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

QUESTION NO: 7
展示資料を参照してください。

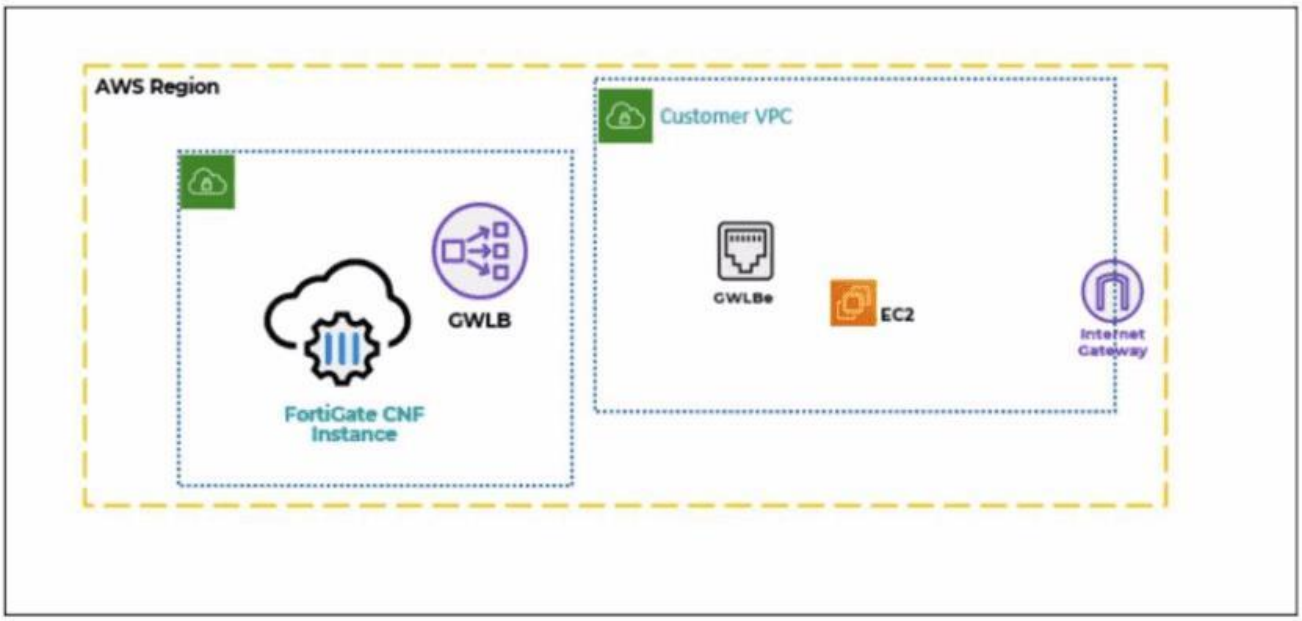
FortiGate SD-WAN zone configuration



FortiGate GUI上のSD-
WANゾーン設定が表示されています。この図に基づいて、正しい記述はどれですか？
A. アンダーレイゾーンにはメンバーが含まれていません。
B.仮想WANリンクとオーバーレイゾーンは削除できます
C. アンダーレイゾーンはデフォルトのゾーンです。
D. ポート2とポート3はゾーンに割り当てられていません。
Answer: A
Explanation:
According to the FortiOS 7.6 Administrator Guide and the specific behavior of the SD-WAN GUI, here is the technical breakdown:

SD-WAN Zone Hierarchy and UI Elements: In the FortiGate GUI, SD-WAN zones that contain member interfaces are displayed with a plus (+) icon next to the checkbox. This icon allows administrators to expand the zone and view the specific physical or logical interfaces assigned to it.
Analysis of the " Underlay " Zone: In the provided exhibit, the virtual-wan-link and overlay zones both feature the plus (+) expansion icon, indicating they have active members. The Underlay zone, however, lacks this icon and displays a red status icon. This is the visual indicator in FortiOS that the zone is currently empty and contains no member interfaces.
Mandatory Zone Membership: In FortiOS 7.x, every SD-WAN member interface must be assigned to a zone.
It is not possible for an interface to be an " SD-WAN member " (as shown in the legend with port2 and port3) without being assigned to a zone. Since port2 and port3 are listed in the legend, they are indeed assigned to one of the other expanded zones (likely virtual-wan-link or overlay), making Option D incorrect.
Default Zone Behavior: While FortiOS 7.6 often creates default zones like virtual-wan-link, underlay, and overlay during certain configuration wizards or by default in newer versions, they are distinct entities. There is no single " default " zone that acts as a global catch-all in the way Option C suggests.
Immutability of System Zones: While certain system-defined zones have restrictions, the primary focus of this specific exhibit is the current membership state, which clearly shows the Underlay zone is empty.

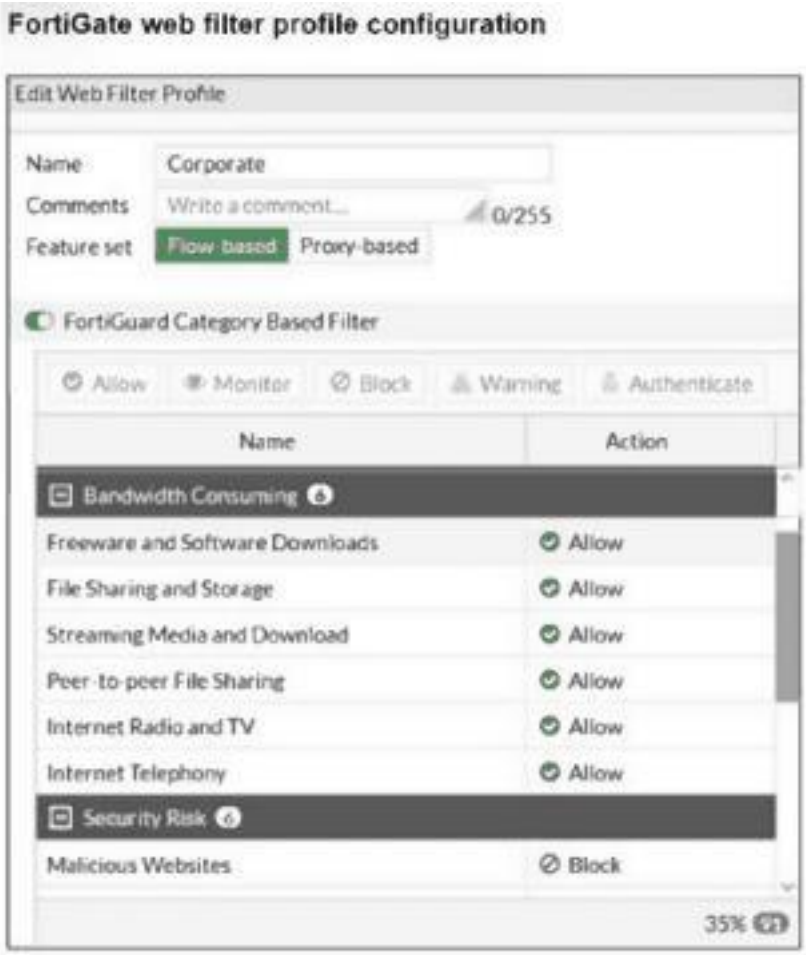
QUESTION NO: 8
展示資料を参照してください。
部分的な雲のトポロジーを示す。



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GWLBe

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 (GWLBe)
C. CNF VPC。顧客VPC。およびGWLB
D. 顧客VPC内のGWLB、GWLBe、およびインターネットゲートウェイ(IGW)
Answer: B
Explanation:
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 (GWLBe)
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 "GWLBe" 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 GWLBe 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.

QUESTION NO: 9
展示資料を参照してください。



この図は、企業向けWebフィルタプロファイルのFortiGuardカテゴリベースフィルタセクションを示しています。管理者は、フリーウェアおよびソフトウェアダウンロードカテゴリに属するdownload.comへのアクセスをブロックする必要があります。また、同じカテゴリに属する他のWebサイトへのアクセスは許可する必要があります。この要件を満たすための解決策を2つ挙げてください。(2つ選択してください)

A. タイプとアクションをそれぞれワイルドカードとブロックに設定して、download.comの静的 URL フィルタエントリを設定します。

B. download.com の Web オーバーライド評価を設定し、サブカテゴリとして悪意のあるWeb サイトを選択します。

C. *.download.com を宛先アドレスとする FQDN アドレス オブジェクトとアクション Denyを指定した別のファイアウォール ポリシーを設定します。

D. フリーウェアとソフトウェアのダウンロードカテゴリのアクションを警告に設定します。

Answer: A B

Explanation:

"In FortiOS, there are three main components of web filtering:

* Web content filtering...

* URL filtering: uses URLs and URL patterns to block or exempt web pages from specific sources ...

* FortiGuard Web Filtering service..."

"In the web filter profile, Fortiguard category filtering enhances the web filter features. Rather than block or allow websites individually, it looks at the category that a website has been

rated with. Then, FortiGate takes action based on that category, not based on the URL."
"If you consider that a particular URL does not have the correct category, you can ask to re-evaluate the rating in the Fortinet URL Rating Submission website. You can also override a web rating for an exceptional URL in the FortiGate configuration. "
"Static URL filtering is another web filter feature, which provides more granularity. Configured URLs in the URL filter are checked from top to bottom against the visited websites. If FortiGate finds a match, it applies the configured action."
"To find the exact match, URL filtering has three pattern types: Simple, Regular Expressions, and Wildcard
."
"So, with these different features, what is the inspection order? If you have enabled many of them, the inspection order flows as follows:
* The local static URL filter
* FortiGuard category filtering..."
Technical Deep Dive:
The correct answers are A and B .
A is correct because a static URL filter gives per-URL granularity. Since the category Freeware and Software Downloads is currently allowed in the profile, adding a local static URL filter entry for download.
com with Block lets FortiGate deny only that site while continuing to allow the rest of the category. This also aligns with the documented inspection order, where the local static URL filter is checked before FortiGuard category filtering .
B is also correct because a web rating override can reclassify a specific exceptional URL. If download.com is re-rated into a blocked category such as Malicious Websites , it will be blocked by the profile while other sites in Freeware and Software Downloads remain allowed.
Why the others are wrong:
C is not the intended web-filter solution. A firewall policy with an FQDN object operates at policy/routing resolution level, not as a category-aware web filtering exception.
D is wrong because changing the whole category to Warning affects all sites in that category, not just download.com.
In production, the cleaner design is usually: keep the category allowed, then add a local URL-filter exception or a web-rating override for the specific site . For HTTPS traffic, remember FortiGate still needs enough SSL inspection visibility to identify the hostname correctly. A representative CLI approach for URL filtering is:

```
config webfilter urlfilter
edit 1
config entries
edit 1
set url " download.com "
set type wildcard
set action block
next
end
next
end
```

This is the most deterministic way to block one site without penalizing the rest of the category.

QUESTION NO: 10
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ッフィングする場合、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。
Answer: B D
Explanation:
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 f 9 ull 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.