

Fortinet.NSE4_FGT_AD-7.6-JPN.v2026-09-01.q66

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：66
バージョン：v2026-09-01
ページの閲覧量：103
問題集の閲覧量：660

https://www.jpnsiken.com/shiken/Fortinet.NSE4_FGT_AD-7.6-JPN.v2026-09-01.q66.html

質問: 1

図を参照してください。図に示されているログメッセージを表示する方法は2つあります。

(2つ選択してください。)



- A. 暗黙の拒否ポリシーを右クリックする
- B. ログエントリ内のポリシーのユニバーサル意識別子 (UUID) とアプリケーション名をフィルタリングすることによって
- C. FortiGate CLIコマンドdiagnose log testを使用する
- D. 前方交通セクション

正解: (正解を表示します)

You can view log messages by filtering based on the policy UUID and application name in the log entry, and also in the Forward Traffic section, which displays logs related to allowed and denied traffic.

質問: 2

FortiGateがプロファイルベースの次世代ファイアウォール(NGFW)として構成されている場合、アプリケーションプロファイルに対してどの検査モードを使用しますか？

- A. 証明書検査
- B. フローベースの検査
- C. プロキシベースの検査
- D. 全内容検査

正解: (正解を表示します)

You can configure application control in proxy-based and flow-based firewall policies. However, because application control uses the IPS engine, which uses flow-based inspection, the INSPECTION is always flow-based.

質問: 3

従業員は、遅延の大きいインターネット接続を介してオフィスに接続する必要がある。

SSL VPNのネゴシエーション失敗を防ぐために、管理者はどのSSL VPN設定を調整すべきでしょうか？

- A. SSL VPN dtls-hello-timeout
- B. SSL VPNログインタイムアウト
- C. SSL VPNセッションTTL
- D. SSL VPN アイドルタイムアウト

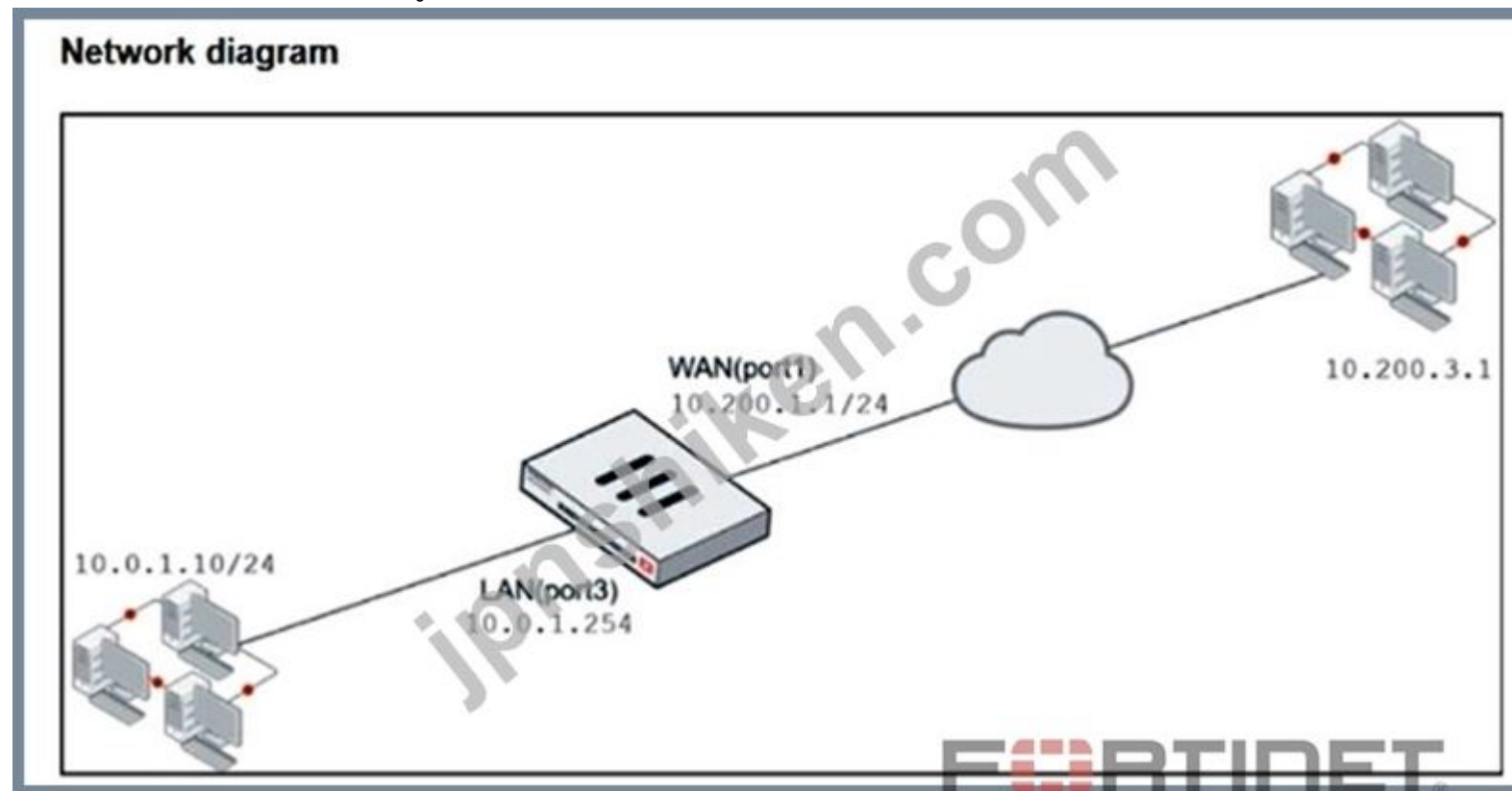
正解: **B** ([コメントを発表する](#))

When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under config vpn ssl settings have been added to address this.

The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN connections.

質問: 4

展示資料を参照してください。



VIP object configuration

Edit Virtual IP

Name

Webserver

Comments

Write a comment... 0/255

Color



Change

Network

Interface

WAN (port1)

Type

Static NAT

External IP address/range

10.200.1.200

Map to

IPv4 address/range

10.0.1.10

☐ Optional Filters

☒ Port Forwarding

Protocol

TCPUDP SCTP ICMP

Port Mapping Type

One to oneMany to many

External service port

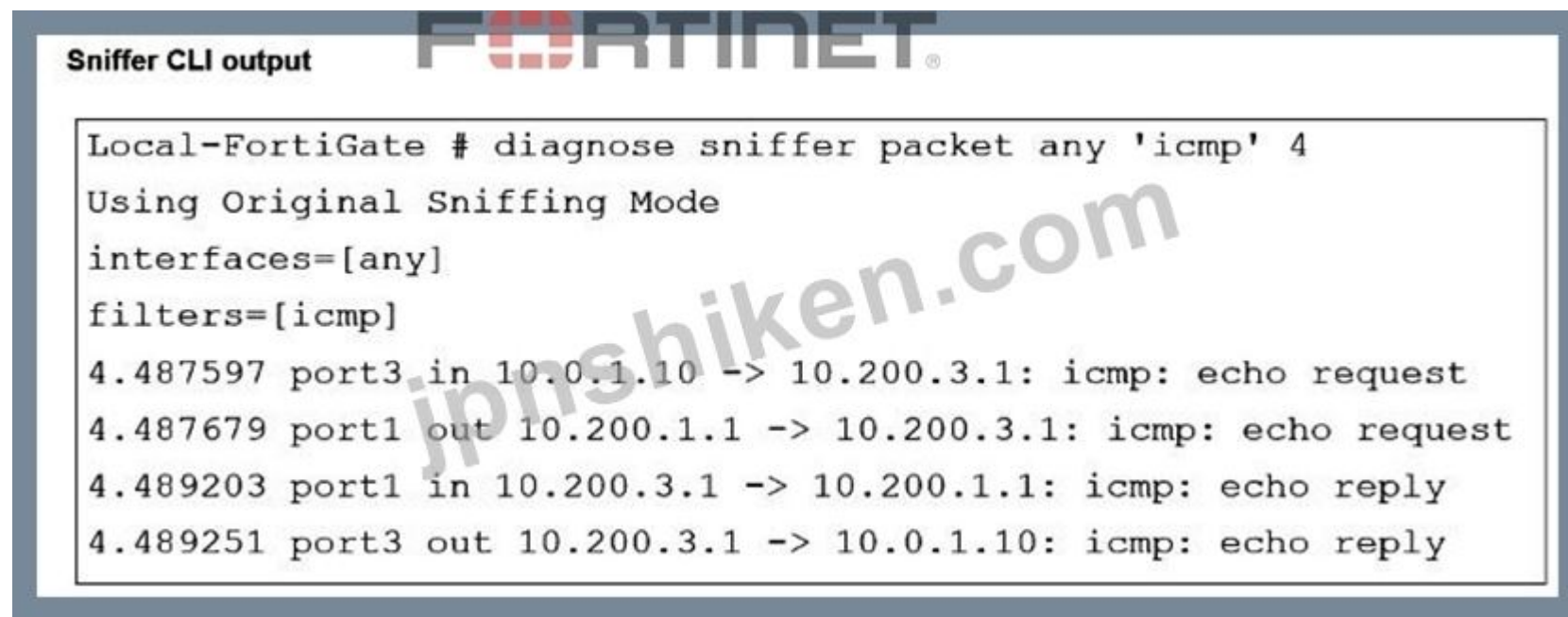
80

Map to IPv4 port

80

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port3) → WAN (port1) 1								
2	Internet_Access	all	all	always	ALL	✓ ACCEPT		✓ NAT
WAN (port1) → LAN (port3) 1								
3	Allow_access	all	Webserver	always	HTTP HTTPS	✓ ACCEPT		✗ Disabled



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、VIP構成、ファイアウォールポリシー、およびFortiGateデバイス上のスニファCLI出力が示されています。

WAN(ポート1)インターフェースのIPアドレスは10.200.1.1/24です。

LAN(ポート3)インターフェースのIPアドレスは10.0.1.254/24です。

ウェブサーバーホスト(10.0.1.10)は、リモートサーバー(10.200.3.1)にpingを実行する際に、VIP外部IPアドレスを送信元NAT(SNAT)として使用する必要があります。

この目標を達成するために有効な記述はどれですか？(2つ選択してください。)

- A. Allow_accessファイアウォールポリシーでNATを有効にします。
- B. Internet_AccessファイアウォールポリシーでNATを無効にします。
- C. VIPオブジェクトのポートフォワーディングを無効にします。
- D. WebサーバーのInternet_Accessの前に新しいファイアウォールポリシーを作成し、IPプールを適用します。

正解: ([正解を表示します](#))

The current VIP is configured with port forwarding, so it only applies to TCP/80 traffic. To use the VIP's external address (10.200.1.200) as the source for any outbound sessions (such as ICMP ping), the VIP must be a full static 1-to-1 NAT, which requires disabling port forwarding.

You then need a dedicated firewall policy for the webserver that is placed before the generic Internet_Access policy and that uses an IP pool with 10.200.1.200. Traffic from 10.0.1.10 will match this policy first and be SNATed to 10.200.1.200, so the remote server 10.200.3.1 sees the VIP external IP as the source.

質問: 5

新しい管理者が、DCエージェントモードを使用してFortiGate上でFSSO認証を設定しています。

想定されるプロセスに含まれていない手順はどれですか？

- A. DCエージェントはログインイベントデータをFortiGateに直接送信します。
- B. ユーザーがWindowsドメインにログインします。
- C. コレクターエージェントはログインイベントデータをFortiGateに転送します。
- D. FortiGate は、FSSO リスト内の IP アドレスに基づいてユーザー ID を決定します。

正解: ([正解を表示します](#))

In DC Agent mode, the DC agent installed on the Domain Controller captures the logon events (e.g., Event ID 4624) in real-time. It then pushes this information to the Collector Agent. The Collector Agent, which runs as a service on a dedicated machine, is responsible for consolidating this information and then forwarding it to the FortiGate firewall. The FortiGate receives this data and uses the user's IP address to apply appropriate security policies.

質問: 6

図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。

FortiGate web filter profile configuration

Edit Web Filter Profile

Name

Corporate

Comments

Write a comment...0/255

Feature set

Flow-based

Proxy-based

FortiGuard Category Based Filter

Allow

Monitor

Block

Warning

Authenticate

Name	Action
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Allow
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	
Malicious Websites	Block

35% 21

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ウェブサイトへのアクセスは許可する必要があります。

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.** アクションが拒否で、宛先アドレスとして *.download.com の FQDN アドレス オブジェクトを持つ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。

正解: ([正解を表示します](#))

You can create a web rating override to change the website category to someone that is blocked in the web filter profile You can enable the URL Filter in the Web Filter Profile and block the website.

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.** 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。
- B.** 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。
- C.** 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。
- D.** 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。

正解: ([正解を表示します](#))

The administrator must ensure phase 2 is successfully established → The static route for the dialup VPN is only added after Phase 2 negotiation completes successfully.

The administrator must define the remote network correctly in the phase 2 selectors → The add- route feature installs a route based on the Phase 2 selectors; if they are incorrect, no route will appear in the routing table.

質問: 8

FortiGate FSSOのエージェントレスポーリングモードの2つの特徴は何ですか？(2つ選択してください。)

- A.** FortiGate はコレクターエージェントにリモート LDAP サーバーを使用するように指示します。
- B.** FortiGate は SMB プロトコルを使用して、DC からイベント ビューア ログを読み取ります。
- C.** FortiGateはワークステーションチェックをサポートしていません。
- D.** FortiGate は AD サーバーをコレクター エージェントとして使用します。

正解: ([正解を表示します](#))

FortiGate FSSO agentless polling mode uses the SMB protocol to directly read event viewer logs from domain controllers (DCs), eliminating the need for external collector agents.

Workstation checks are not supported in this mode, as FortiGate polls only DC logs and lacks the additional verification features of agent-based modes.

質問: 9

図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？

Edit Address

Name	Fortinet
Color	 Change
Interface	 port2
Type	FQDN
FQDN	www.fortinet.com
Routing configuration	☒
Comments	Write a comment... 0/255

- 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。

正解: **D** ([コメントを发表する](#))

To use an FQDN-based address object as a destination in a static route, the "Routing configuration" option must be enabled in the firewall address settings. Without this, the address cannot be selected for routing.

質問: 10

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？

- 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: ([正解を表示します](#))

If Override DISABLED then: ports > HA Uptime > Priority > SN.

If Overrid ENABLED then: ports > Priority > HA Uptime > SN.

質問: 11

セキュリティファブリックの評価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. セキュリティ評価セクションのエグゼクティブサマリーを取得するにはライセンスが必要です。

- B. ルートFortiGateは、セキュリティファブリック内のすべてのFortiGateデバイスの概要を提供します。
- C. セキュリティ態勢カテゴリは、PCI準拠の結果を提供します。
- D. セキュリティ評価に関するインサイトは、セキュリティ評価ページでのみ利用可能です。

正解: **B,C** ([コメントを發表する](#))

The Security Rating section provides an executive summary of all the security rating checks. By default, it is available with a base set of free checks, otherwise a licensed set is available with a subscription service that requires a FortiGuard Security Rating Service subscription.

質問: 12

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. 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。
- B. 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。
- C. 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。
- D. 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。
- E. 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。

正解: **A,D,E** ([コメントを發表する](#))

Flow-based antivirus buffers the entire file while simultaneously transmitting data to the client to minimize latency.

Flow-based inspection combines multiple scanning techniques from proxy-based modes for efficient detection.

Flow-based inspection provides better performance by processing traffic on the fly without full proxy overhead.

質問: 13

図を参照してください。NOCチームは、NOC_Access管理者プロファイルを使用してFortiGate GUIに接続します。彼らは、非アクティブ時にGUIセッションが早すぎるタイミングで切断されないようにすることを要求しています。NOCチームからのこの特定の要求に応えるために、管理者は何を構成する必要がありますか？



- A. すべてのプロファイル設定が有効になるように、NOC_Access をリストの一番上に移動します。
- B. NOC_Access 管理者プロファイルの Override Idle Timeout パラメータのオフライン値を増やします。
- C. すべての NOC_Access ユーザーに super_admin ロールが割り当てられ、アクセスが保証されていることを確認してください。
- D. config system accprofile NOC_Access の下の admintimeout 値を増やします。

正解: ([正解を表示します](#))

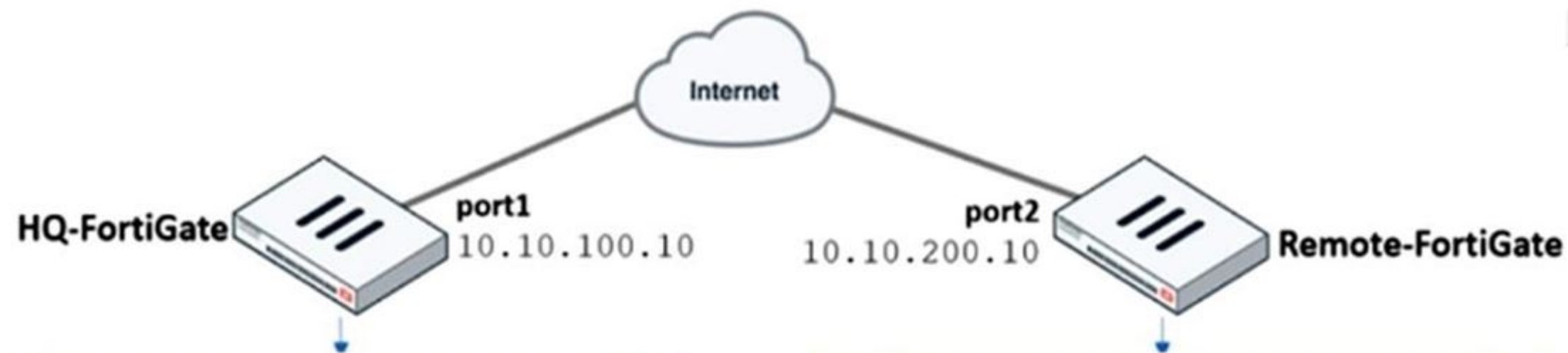
You can override the idle timeout setting per administrator profile using the Override Idle Timeout setting.

You can configure an administrator profile to increase inactivity timeout and facilitate use of the GUI for central monitoring. Then Override Idle Timeout setting allows the admintimeout value, under the config system accprofile, to be overridden per access profile..

質問: 14

展示資料を参照してください。

IPsec tunnel configuration



Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 10.10.200.10

Interface: port1

Local Gateway: ☐

Mode Config: ☐

NAT Traversal: ☒ Enable ☐ Disable ☐ Forced

Keepalive Frequency: 10

Dead Peer Detection: ☐ Disable ☒ On Idle ☐ On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress ☐ Ingress ☐

Advanced...

Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: ☒ 1 ☐ 2

Mode: ☒ Aggressive ☐ Main (ID protection)

Peer Options

Accept Types: Any peer ID

Phase 1 Proposal ☒ Add

Encryption: AES128 Authentication: SHA1

Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 10.10.100.10

Interface: port1

Local Gateway: ☐

Mode Config: ☐

NAT Traversal: ☒ Enable ☐ Disable ☐ Forced

Keepalive Frequency: 10

Dead Peer Detection: ☐ Disable ☐ On Idle ☒ On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress ☐ Ingress ☐

Advanced...

Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: ☒ 1 ☐ 2

Mode: ☒ Aggressive ☐ Main (ID protection)

Phase 1 Proposal ☒ Add

Encryption: AES256 Authentication: SHA256



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-FortiGate で、IKE モードを Main (ID 保護) に設定します。
- B. Remote-FortiGate で、ポート 2 をインターフェイスとして設定します。
- C. HQ-FortiGate で、Diffie-Helman グループ 2 を無効にします。
- 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)

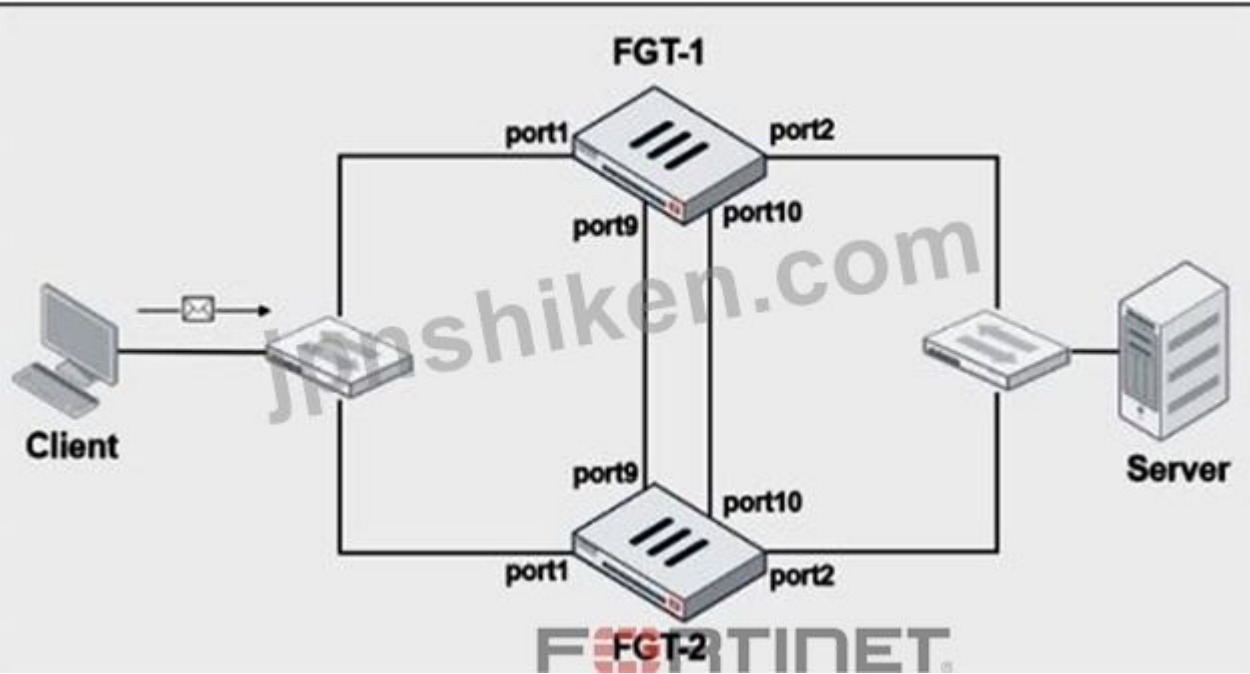
On the HQ-FortiGate the IKE phase 1 mode is set to Aggressive, while on the Remote-FortiGate it is set to Main (ID protection). Both sides must use the same IKE mode for phase 1 to come up, so changing HQ-FortiGate to Main mode resolves this mismatch.

On the Remote-FortiGate, the phase 1 Interface is configured as port1, but according to the diagram the WAN-facing interface with IP 10.10.200.10 is port2. The local interface in the IPsec configuration must match the physical WAN interface, so changing it to port2 is required for the tunnel to establish.

質問: 15

展示資料を参照してください。

FortiGate HA cluster topology



Current HA status

```
# get system ha status
...
Configuration Status:
  FGVM010000064692(updated 4 seconds ago): in-sync
  FGVM010000064692 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
  FGVM010000065036(updated 4 seconds ago): in-sync
  FGVM010000065036 chksum dump: 13 8b 52 c7 59 2a 9a 5c 5f
...
Primary      : FGT-1, FGVM010000064692, HA cluster index = 1
Secondary    : FGT-2, FGVM010000065036, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

New FortiGate HA configuration

```
FGT-1
#config system ha
  set group-id 3
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port9" 50 "port10" 50
  set session-pickup enable
  set override disable
  set priority 90
  set monitor port3

FGT-2
#config system ha
  set group-id 3
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port9" 50 "port10" 50
  set session-pickup enable
  set override enable
  set priority 110
  set monitor port3
```

FGT-1とFGT-2は、図に示すHA構成コマンドで更新されます。

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. FGT-2 はオーバーライド有効化設定を持ち、FGT-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. FGT-1 はオーバーライド無効化設定を FGT-2 と同期します。
- 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. FGT-2の優先順位が低いため、FGT-1がプライマリのままになります。

正解: (正解を表示します)

With override enabled, the primary unit with the highest device priority will always become the primary unit. Whenever an event occurs that may affect primary unit selection, the cluster negotiates. For example, when override is enabled a cluster renegotiates when you change the device priority of any cluster unit or when you add a new unit to a cluster.

Override and primary unit selection

Enabling override changes the order of primary unit selection. As shown below, if override is enabled, primary unit selection considers device priority before age and serial number. This means that if you set the device priority higher on one cluster unit, with override enabled this cluster unit becomes the primary unit even if its age and serial number are lower than other cluster units..

質問: 16

図を参照してください。この部分的な構成に基づくと、FortiGateが節約モードに入った場合に考えられる2つの結果は何ですか？(2つ選択してください。)

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

- A. 管理者は設定を変更できません。
- B. FortiGate は隔離アクションをスキップします。
- C. 管理者は新しいセッションを許可するために FortiGate を再起動する必要があります。
- D. FortiGate は検査が必要な新しいセッションを破棄します。

正解: (正解を表示します)

System configuration cannot be changed because of the IPS Global configuration "fail-open enabled" FortiGate skips quarantine actions - again because of the IPS Global configuration "fail-open enabled"

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。展示資料に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？

```
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"
```

- A. 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。
- B. 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。
- C. 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。
- D. 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。

正解: (正解を表示します)

The log message IPS session scan paused, enter fail open mode indicates that the IPS socket buffer is full, meaning the IPS engine does not have enough memory to process new sessions. As a result, FortiGate switches to fail-open mode, allowing traffic to pass (or temporarily dropping it) without full IPS scanning.

質問: 18

添付資料を参照してください。添付資料に示すように、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済みです。
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。)

Application sensor

Edit Application Sensor

FORTINET

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	BHVR Excessive-Bandwidth	Filter	Block
2	VEND Google	Filter	Monitor

2

Firewall policy

Edit Policy

Firewall/Network Options

Inspection mode

Flow-basedProxy-based

NAT

☒

IP pool configuration

Use Outgoing Interface AddressUse Dynamic IP Pool

Preserve source port

☐

Protocol options

PROTdefault

Security Profiles

AntiVirus

☐

Web filter

☐

Video filter

☐

DNS filter

☐

Application control

☒APPdefault

IPS

☐

File filter

☐

SSL inspection

SSLcertificate-inspection

- A. 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、優先度を 1 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 のアクションを「許可」に設定します。
- 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. SSL検査をディープコンテンツ検査に設定します。

正解: A,E ([コメントを发表する](#))

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

The "Excessive-Bandwidth" filter has a higher priority (1) and is configured to Block. Because Google applications generate significant bandwidth, they match this rule first and get blocked.

Moving the "Google" filter to priority 1 ensures that the monitor action for Google is applied before the block rule.

Set SSL inspection to deep-content inspection.

Google applications use HTTPS encryption, so the FortiGate cannot identify or control them unless SSL traffic is decrypted. Changing from certificate-inspection (which only inspects certificates) to deep-inspection allows FortiGate to fully analyze encrypted application traffic and properly apply the Application Control rules.

質問: 19

FortiGateファイアウォールポリシーはアクティブ認証で設定されていますが、ユーザーがWebサイトにアクセスする際に認証できません。ユーザーが認証できない場合でも、FortiGateはどのプロトコルを許可する必要がありますか？

A. LDAP

B. TACASC+

C. Kerberos

D. DNS

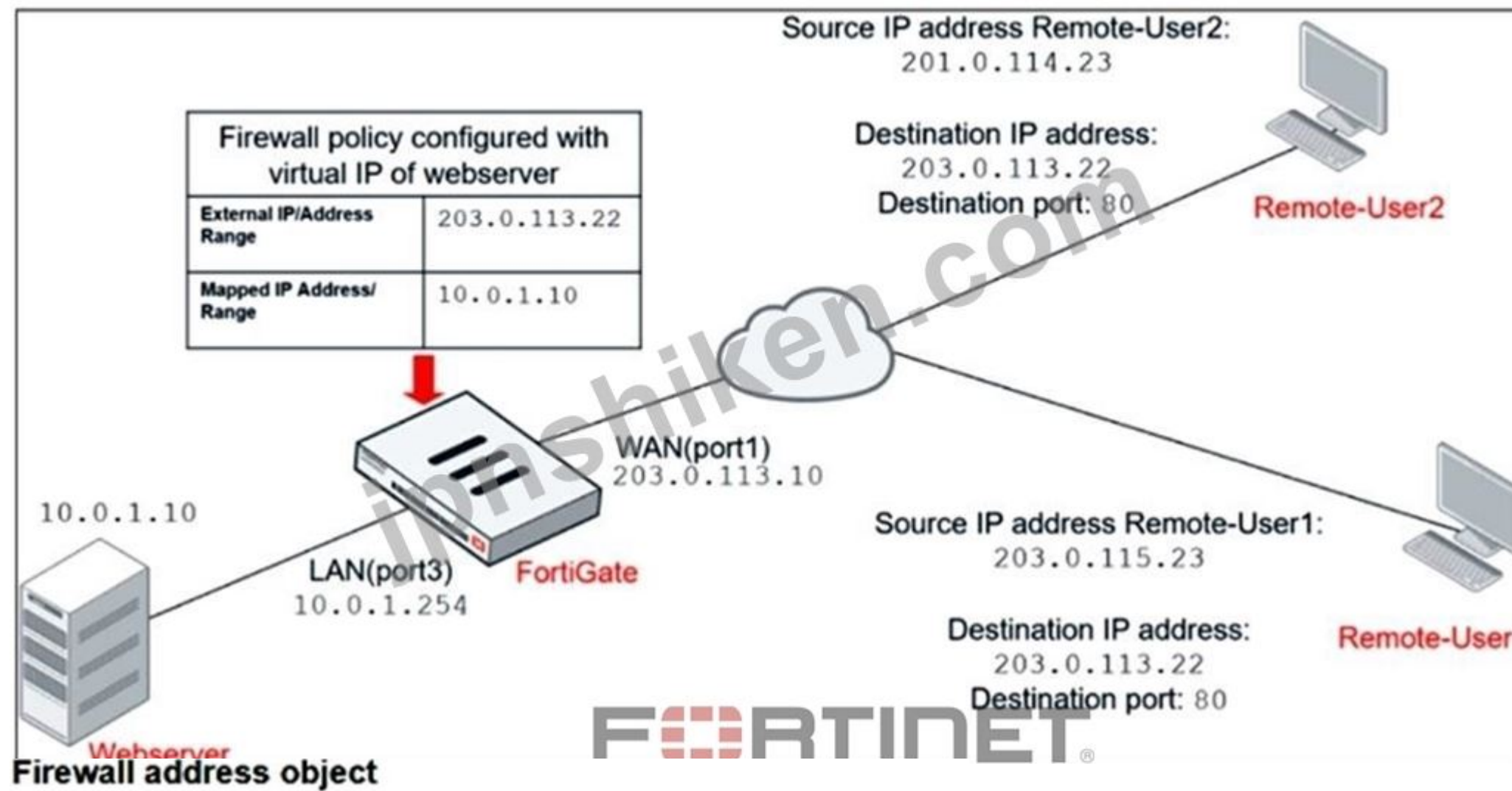
正解: ([正解を表示します](#))

A firewall policy must allow a protocol in order to show the authentication dialog that is used in active authentication (such as HTTP/HTTPS/FTP/Telnet) and DNS.

質問: 20

展示資料を参照してください。

Network diagram



Edit Address

Name Deny_IP

Color Change

Type Subnet

IP/Netmask 201.0.114.23/32

Interface WAN (port1)

Static route configuration ☐

Comments Deny web server access. 23/255

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

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、リモートユーザー1がWebサーバーにアクセスできる一方で、リモートユーザー2がWebサーバーにアクセスできないように機能するべきである。

管理者は、リモートユーザー2によるWebサーバーへのアクセスを拒否するために、ポリシーに対してどのような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. 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。

B. 拒否ポリシーでmatch-viを無効にします。

C. Allow_access ポリシーで宛先アドレスを Deny_IP に設定します。

D. 拒否ポリシーでmatch-viを有効にします。

正解: A,D (コメントを发表する)

In this scenario, the FortiGate uses a Virtual IP (VIP) to map the external IP 203.0.113.22 to the internal web server 10.0.1.10. When using VIPs, firewall policies must be configured carefully to match the translated destination address.

The external users (Remote-User1 and Remote-User2) connect to 203.0.113.22, which is the VIP for the web server.

By default, firewall policies match pre-NAT addresses (the original destination before VIP translation).

To make the deny policy recognize traffic destined for the VIP-mapped address, the match-vip option must be enabled.

The destination in the Deny policy should explicitly be the Webserver (the VIP object), so FortiGate correctly identifies the target.

質問: 21

SSL VPNユーザーの認証済みセッションが、VPNから切断された後もアクティブなままにならないようにする必要があります。

どの設定でこれが実現できますか？

- A. ファイアウォール認証セッションのタイムアウトを、SSL VPNセッションのタイムアウトよりも短く設定します。
- B. ユーザーが切断した後、アクティブなファイアウォール認証セッションを手動でクリアします。
- C. SSL VPNのアイドルタイムアウトを長くして、早期切断の可能性を減らします。
- D. SSL VPNセッション終了時にファイアウォール認証セッションを強制的に終了させる設定を有効にする

正解: (正解を表示します)

Firewall policy authentication session is associated with SSL VPN tunnel session.

Firewall policy authentication session is forced to end when SSL VPN tunnel session ends.

Prevents reuse of authenticated SSL VPN firewall sessions (not yet expired) by a different user, after the initial user terminates the SSL VPN tunnel session.

質問: 22

管理者は、一部のユーザーがSSL VPN接続を確立できない一方で、他のユーザーは問題なく接続できることに気づいた。

管理者はまず何をチェックすべきでしょうか？

- A. 影響を受けるユーザーが正しいポート番号を使用していることを確認してください。
- B. SSL VPNトンネルインターフェースでHTTPSサービスが有効になっていることを確認してください。
- C. すべてのトラフィックを SSL VPN 経由でルーティングするために、強制トンネリングが有効になっていることを確認してください。
- D. ユーザーのトラフィックがファイアウォールポリシーに当たっていることを確認します。

正解: ([正解を表示します](#))

質問: 23

FortiGate上で以下のコマンドを設定しました。

```
config system settings
set strict-src-check enable
end

Config system interface
edit port1
set src-check disable
next
end
```

この構成はFortiGateにどのような影響を与えるでしょうか？

- A. FortiGate はすべてのインターフェースで厳密な RPF を有効にし、ポート 1 は非対称ルーティングを有効にします。
- B. FortiGate はすべてのインターフェースで厳格な RPF を有効にし、ポート 1 は RPF チェックから除外されます。
- C. Port1 はフレキシブル RPF が有効になり、その他のすべてのインターフェースは厳密 RPF が有効になります
- D. グローバル設定が優先され、FortiGate はすべてのインターフェイスで厳密な RPF を有効にします。

正解: ([正解を表示します](#))

The global setting enables strict source checking (RPF) on all interfaces by default. The per- interface setting disables the source check on port1, exempting it from strict RPF enforcement.

質問: 24

展示資料を参照してください。

Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
[-] LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
[-] WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
[-] Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

このファイアウォールポリシーリストに関する記述のうち、正しいものはどれですか？

- A. ファイアウォールポリシーはIDシーケンスビューで一覧表示されます。
- B. ファイアウォールポリシーは、入力インターフェースと出力インターフェースのペアビューで一覧表示されます。
- C. 暗黙グループには、複数の拒否ファイアウォールポリシーを含めることができます。
- D. LAN から WAN、WAN から LAN、および Implicit は、シーケンス グルーピング ビュー リストです。

正解: D (コメントを发表する)

The firewall policy list shown is displayed in the sequence grouping view, where policies are grouped based on their traffic direction - such as LAN to WAN, WAN to LAN, and Implicit. This view helps administrators quickly identify and manage policies according to their interface pairings and logical traffic flow, rather than by numerical ID order.

質問: 25

添付資料を参照してください。添付資料には、FortiGateデバイスにおける高メモリ使用量しきい値のシステムパフォーマンス出力とデフォルト設定が示されています。

System Performance output

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

Memory usage threshold settings

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

システムのパフォーマンス出力に基づくと、考えられる結果は次の2つです。(2つ選択してください。)

- A. FortiGate は省電力モードに入りました。
- B. 管理者はコンソールポート経由でのみFortiGateにアクセスできます。
- C. 管理者は設定を変更できます。
- D. FortiGate が新しいセッションをドロップします。

正解: ([正解を表示します](#))

FG enters conserve mode at 88% by default, at which point you can't make configuration changes. Also, without additional config, FG will drop sessions that require inspection. At 95%, all new sessions are dropped.

管理者は、デフォルト設定を使用してFortiGuardサーバーをFortiGate上のDNSサーバーとして構成します。
FortiGuardサーバーへのDNS接続について、正しいのはどれですか？

- A. DNS over TLSを使用します。
- B. HTTPS 上で DNS を使用します。
- C. UDP 8888を使用します。
- D. UDP 53 を使用します。

正解: (正解を表示します)

When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic. New FortiGuard DNS servers have been added as primary and secondary servers.

質問: 27

管理者は、NTurboをサポートするFortiGateモデルを管理します。
NTurboアクセラレーションは、どのようにウイルス対策ソフトのパフォーマンスを向上させるのでしょうか？

- A. プロキシベースの検査の場合、NTurbo はトラフィックをコンテンツプロセッサにオフロードします。
- B. フローベースの検査の場合、NTurboは専用のデータパスを確立し、IPSエンジンとFortiGateのイングレスおよびエグレスインターフェイス間のトラフィックをリダイレクトします。
- C. プロキシベースの検査の場合、NTurbo はファイル全体をバッファリングしてから、それをアンチウイルス エンジンに送信します。
- D. フローベースの検査の場合、NTurboはFortiGateデバイス上に2つの検査セッションを作成します。

正解: (正解を表示します)

NTurbo creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface.

質問: 28

ネットワーク管理者が、海外出張中の営業担当者向けにIPsec VPNトンネルを設定している。
管理者はどのIPsecウィザードテンプレートを適用する必要がありますか？

- A. ハブアンドスポーク
- B. サイト間
- C. リモートアクセス
- D. ダイアルアップユーザー

正解: C (コメントを发表する)

The Remote Access IPsec Wizard template is used for individual users connecting from remote locations, such as traveling employees. This template configures FortiGate to act as an IPsec VPN server, allowing remote clients (like FortiClient) to securely connect and access internal network resources while abroad.

質問: 29

展示資料を参照してください。

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port3 → port1 1									
1	Full_Access	Remote-users LOCAL_SUB...	all	always	HTTP HTTPS ALL ICMP	ACCEPT	NAT	Standard	Category_Monitor certificate-inspection

FortiGateはファイアウォール認証用に設定されています。外部ウェブサイトにアクセスしようとした際、ユーザーにログインプロンプトが表示されません。

この状況の最も可能性の高い原因は何ですか？

- A. ファイアウォール ポリシーでは、サービス DNS が必要です。
- B. ユーザーが間違ったユーザー名を使用しています。
- C. 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。
- D. リモートユーザーグループが宛先に追加されません。

正解: A ([コメントを發表する](#))

DNS traffic can be allowed if user has not authenticated yet.

Hostname resolution is often required by the application layer protocol (HTTP/HTTPS/FTP/Telnet) that is used to authenticate.

DNS service must be explicitly listed as a service in the policy.

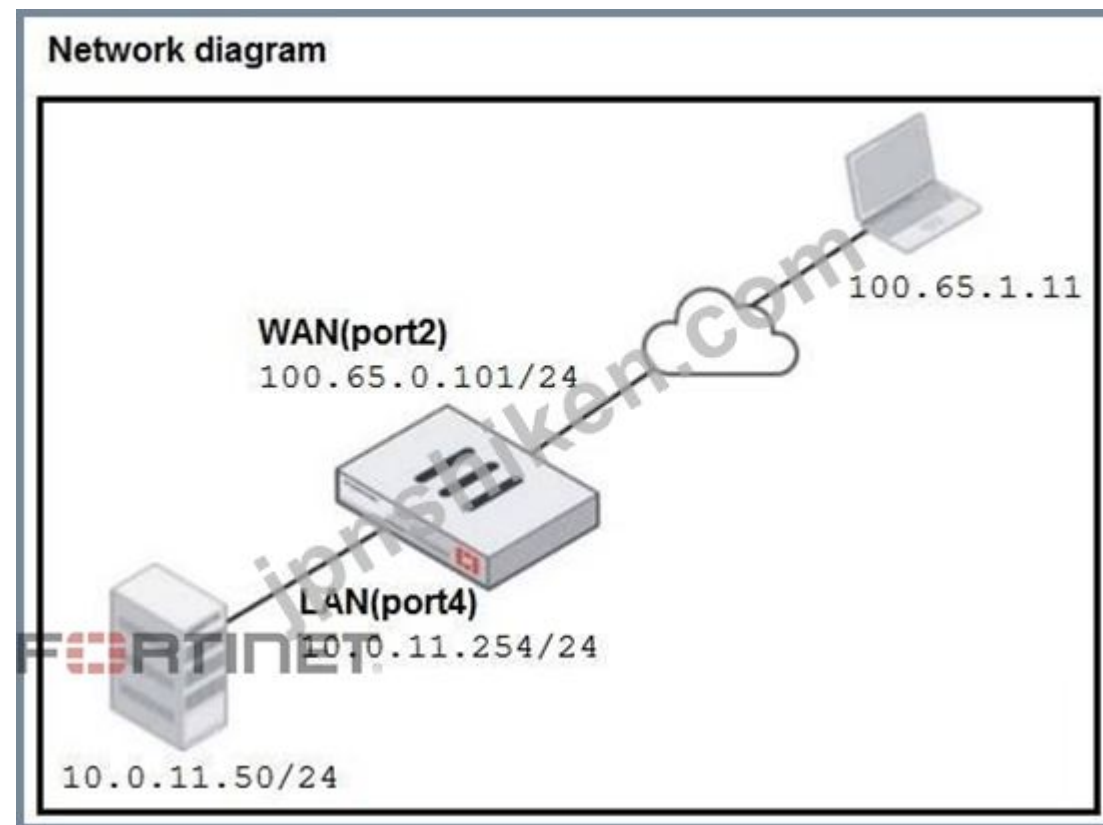
質問: 30

添付資料を参照してください。ネットワークVIPオブジェクトに接続されたFortiGateデバイスの図と、ファイアウォールポリシーの設定が示されています。

WAN(ポート2)インターフェースのIPアドレスは100.65.0.101/24です。

LAN(ポート4)インターフェースのIPアドレスは10.0.11.254/24です。

ホスト100.65.1.11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？



VIP object configuration

Edit Virtual IP

Name

Comments 0/255

Color 

Network

Interface 

Type

External IP address/range 

Map to

IPv4 address/range

☐ Optional Filters

☒ Port Forwarding

Protocol

Port Mapping Type

External service port 

Map to IPv4 port

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

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

正解: ([正解を表示します](#))

The VIP object maps the external IP 100.65.0.200:443 to the internal server 10.0.11.50:4443.

Since NAT is disabled on the firewall policy, the source IP is preserved.

So, when host 100.65.1.111 connects to 100.65.0.200:443:

- The source remains 100.65.1.111.
- The destination IP is translated to 10.0.11.50.
- The destination port is translated to 4443.

質問: **31**

添付資料を参照してください。添付資料には、アプリケーションセンサーの構成、および過剰帯域幅とAppleフィルターの詳細が示されています。

設定に基づくと、発信または着信の通話が少ない場合、Apple FaceTimeはどのようなのでしょうか？

Application sensor configuration

FORTINET

Edit Application Sensor

Categories

▼ All Categories

- ☒ Business (179, ☁ 6)
- ☒ Collaboration (293, ☁ 6)
- ☐ Game (124)
- ☐ Mobile (3)
- ☐ P2P (85)
- ☐ Remote.Access (91)
- ☒ Storage.Backup (296, ☁ 16)
- ☐ Video/Audio (206, ☁ 13)
- ☐ Web.Client (18)
- ☒ Cloud.IT (31)
- ☒ Email (87, ☁ 12)
- ☒ General.Interest (241, ☁ 9)
- ☒ Network.Service (332)
- ☐ Proxy (106)
- ☐ Social.Media (150, ☁ 31)
- ☒ Update (48)
- ☐ VoIP (30)
- ☐ Unknown Applications

☐ Network Protocol Enforcement

Application and Filter Overrides

+ Create New

✎ Edit

🗑 Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	☐ Block
2	VEND Apple	Filter	☐ Monitor

Application override configuration

Edit Override

Type

Application

Filter

Action

Block

Filter

BHVR

Excessive-Bandwidth

FaceTime

x

Q

Name

Category

Technology

Application Signature

1/1262

FaceTime

VoIP

Client-Server

Filter override configuration

Edit Override

Type

Application

Filter

Action

Monitor

Filter

VEND

Apple

FaceTime

x

Q

Name

Category

Technology

Application Signature

1/33

FaceTime

VoIP

Client-Server

- A. Apple Face Timeは、ビデオ/オーディオカテゴリの設定に基づいて許可されます。
- B. 過剰帯域幅フィルタの設定に基づき、Apple Face Time はブロックされます。
- C. Appleのフィルタ設定に基づいて、Apple Face Timeが許可されます。
- D. Apple Face Time は、[アプリケーションとフィルタの上書き] の Apple フィルタが [許可] に設定されている場合にのみ許可されます。

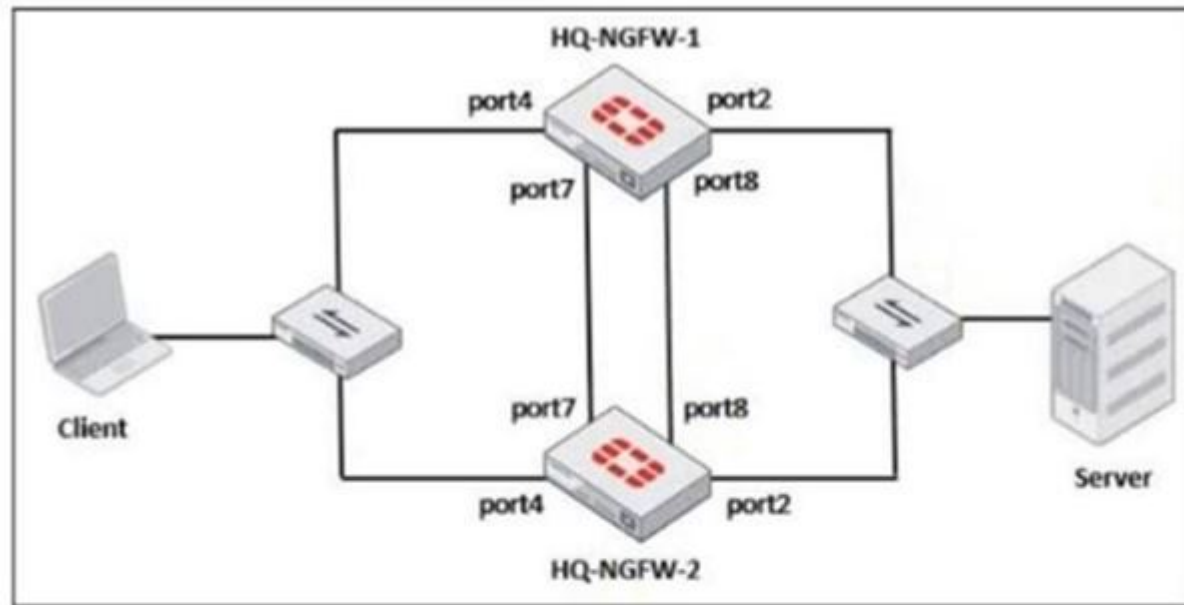
正解: (正解を表示します)

Apple FaceTime normally falls under Video/Audio and could be blocked by the Excessive- Bandwidth filter. However, in this configuration, an override is applied under the Apple vendor filter with Monitor action. Overrides take precedence over general filter actions. Therefore, FaceTime will not be blocked; instead, it will be monitored, and since only a few calls are made (not excessive bandwidth usage), it will be allowed based on the Apple filter configuration.

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」

図を参照してください。管理者は、現在のHAステータスに基づいて、図に示すようにHQ-NGFW-1とHQ-NGFW-2のオーバーライドパラメータと優先度パラメータを更新します。

FortiGate HA cluster topology



Current HA status

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

New FortiGate HA configuration

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

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

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-1 はオーバーライド無効化設定を HQ-NGFW-2 と同期します。
- B. 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。
- C. 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。
- D. 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。

正解: **B** ([コメントを発表する](#))

With override enabled on HQ-NGFW-2 and its higher priority (110 vs. 90), HQ-NGFW-2 will become the primary device, preempting HQ-NGFW-1 despite the current primary status.

質問: **33**

図を参照してください。管理者としてIPSプロファイルを作成しましたが、期待どおりに動作していません。テスト中に、図に示すような出力が得られました。展示されている診断結果の考えられる原因は何でしょうか？

```
Fortinet
HQ-NGFW-1 # diagnose test application ipsmonitor 1
pid = 2044, engine count = 0 (+1)
0 - pid:2074:2074 cfg:1 master:0 run:1
```

- A. IPSセキュリティプロファイルが設定されたファイアウォールポリシーがありません。
- B. FortiGate が IPS フェイルオープン状態になりました。
- C. 管理者がコマンド diagnose test application ipsmonitor 5 を入力しました。
- D. 管理者がコマンド diagnose test application ipsmonitor 99 を入力しました。

正解: **A** ([コメントを発表する](#))

The output shows the IPS engine count as 0, indicating no active IPS engines are running. This typically means no firewall policy is referencing the IPS security profile, so the IPS profile is not being applied or triggered.

質問: **34**

管理者は、一部のユーザーがSSL VPN接続を確立できない一方で、他のユーザーは問題なく接続できることに気づいた。管理者はまず何をチェックすべきでしょうか？

- A. 影響を受けるユーザーが正しいポート番号を使用していることを確認してください。
- B. ユーザーのトラフィックがファイアウォールポリシーに当たっていることを確認します。
- C. すべてのトラフィックを SSL VPN 経由でルーティングするために、強制トンネリングが有効になっていることを確認してください。
- D. SSL VPNトンネルインターフェースでHTTPSサービスが有効になっていることを確認してください。

正解: (正解を表示します)

The key part of the question is some users can connect and some cannot, which strongly suggests a client-side connection issue rather than a firewall-policy issue (policy only applies after the tunnel is established). For SSL-VPN, the first thing to check when users fail to connect is whether they are using the correct connection settings (especially the port).

質問: 35

図を参照してください。このデータベーステーブルのルーティングエントリについて、正しい記述を2つ選択してください。

FortiGate routing database

Local-FortiGate # get router info routing-table database

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

V - BGP VPNv4

> - selected route, * - FIB route, p - stale info

Routing table for VRF=0

S 0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]

S *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]

C *> 10.0.1.0/24 is directly connected, port3

C *> 10.200.1.0/24 is directly connected, port1

C *> 10.200.2.0/24 is directly connected, port2

C *> 172.16.100.0/24 is directly connected, port8

- A. ルーティングデータベーステーブル内のすべてのエントリがFortiGateルーティングテーブルにインストールされます。
- B. port2インターフェースは非アクティブとしてマークされています。
- C. 両方のデフォルトルートは、管理距離が異なります。
- D. ポート2のデフォルトルートはスタンバイルートとしてマークされています。

正解: (正解を表示します)

The default route via port2 has the same prefix as the route via port1 but a higher administrative distance [20/0]vs[10/0] and is not marked with ">" or "*". This indicates it is kept as a standby/backup route, to be used only if the better route via port1 fails.

The two static default routes clearly show different administrative distances in the brackets: [20/0] for port2 and [10/0] for port1, confirming that their administrative distances are different.

質問: 36

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. 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。
- B. 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。
- C. 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。
- 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。

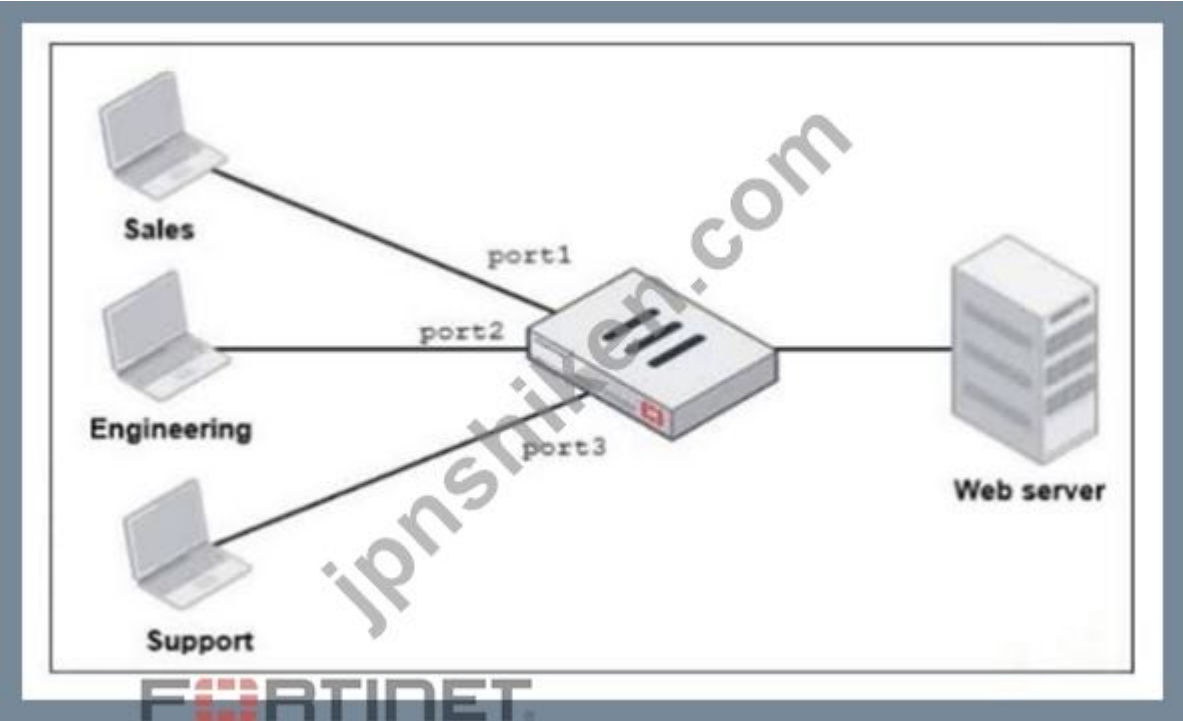
正解: A (コメントを發表する)

The browser presents a certificate warning when you attempt to access an HTTPS site that uses an untrusted certificate. Untrusted certificates include self-signed SSL certificates, unless the certificate is imported into the browser-trusted certificate store. FortiGate has its own configuration setting on the SSL/SSH Inspection profile, which includes options to Allow, Block, or Ignoreuntrusted SSL certificates.

質問: 37

図を参照してください。FortiGateには、営業部門とエンジニアリング部門が同じセキュリティプロファイルを使用して同じWebサーバーにアクセスできるように、それぞれ独立したファイアウォールポリシーが設定されています。

管理者は、2つのポリシーを1つに統合するために、どのような操作を行う必要がありますか？



- A. ポート1とポート2を含む集約インターフェースを作成し、単一のファイアウォールポリシーを作成します。
- B. 単一のファイアウォールポリシーでポート1とポート2のサブネットを選択します。
- C. 単一のファイアウォール ポリシーで、port1 と port2 を任意のインターフェースに置き換えます。
- D. 複数のインターフェイス ポリシーを有効にして、同じファイアウォール ポリシーでポート 1 とポート 2 を選択します。

正解: (正解を表示します)

Enabling Multiple Interface Policies allows you to select multiple interfaces (like port1 and port2) in a single firewall policy, consolidating access rules for both Sales and Engineering to the web server.

質問: 38

管理者は、同一インターフェース上でのSSL VPNとHTTPSによる管理アクセス間のポート競合を分析し、解決する必要があります。

これを実現するには、どのような方法が考えられますか？(2つ選択してください。)

- A. HTTPS 管理アクセスがどのインターフェースでもポート 443 を使用している場合、SSL VPN を無効にします。
- B. SSL VPNとHTTPS管理アクセス両方にポート443を同じインターフェースで問題なく使用できます。
- C. ポート443を使用して1つのインターフェースでSSL VPNを実行し、別のインターフェースで同じくポート443を使用してHTTPS管理アクセスを有効にします。
- D. SSL VPN サービスと HTTPS 管理サービスの両方が同じインターフェース上にある場合は、どちらかのポート番号を変更します。

正解: (正解を表示します)

You can keep port 443 for SSL VPN on one interface and also use port 443 for HTTPS admin access on a different interface. Since the services are bound to different interfaces, no conflict occurs. If both SSL VPN and HTTPS admin access are required on the same interface, you must change the port number for one of the services to avoid a port conflict.

質問: 39



このプロファイルを作成する際に、ウイルス対策スキャンスイッチがグレー表示されるのはなぜですか？

- A. このプロファイルでは、検査対象のプロトコルはどれも有効になっていません。
- B. FortiGate は、RAM が 2 GB 未満の場合、ウイルス対策スキャン機能をサポートしません。
- C. システム -> 機能の表示設定でウイルス対策スキャンが無効になっています。
- D. プロファイルの機能セットはフローベースですが、プロキシベースである必要があります。

正解: A (コメントを発表する)

Enable one or more protocols for inspection, then enable AntiVirus scan for the selected protocols with a specified action.

<https://docs.fortinet.com/document/fortigate/7.6.4/administration-guide/922096/inspection-mode- feature-comparison>

質問: 40

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

正解: (正解を表示します)

In agent-based mode, FortiSASE Secure Internet Access uses VPN policies for secure connectivity, and the FortiSASE Firewall-as-a-Service (FWaaS) component for enforcing security policies and filtering user traffic.

質問: 41

ネットワーク接続なしでFortiGate CLIへの管理アクセスを可能にする方法はどれですか？

- A. CLIコンソールウィジェット
- B. SSHコンソール
- C. Telnetコンソール
- D. シリアルコンソール

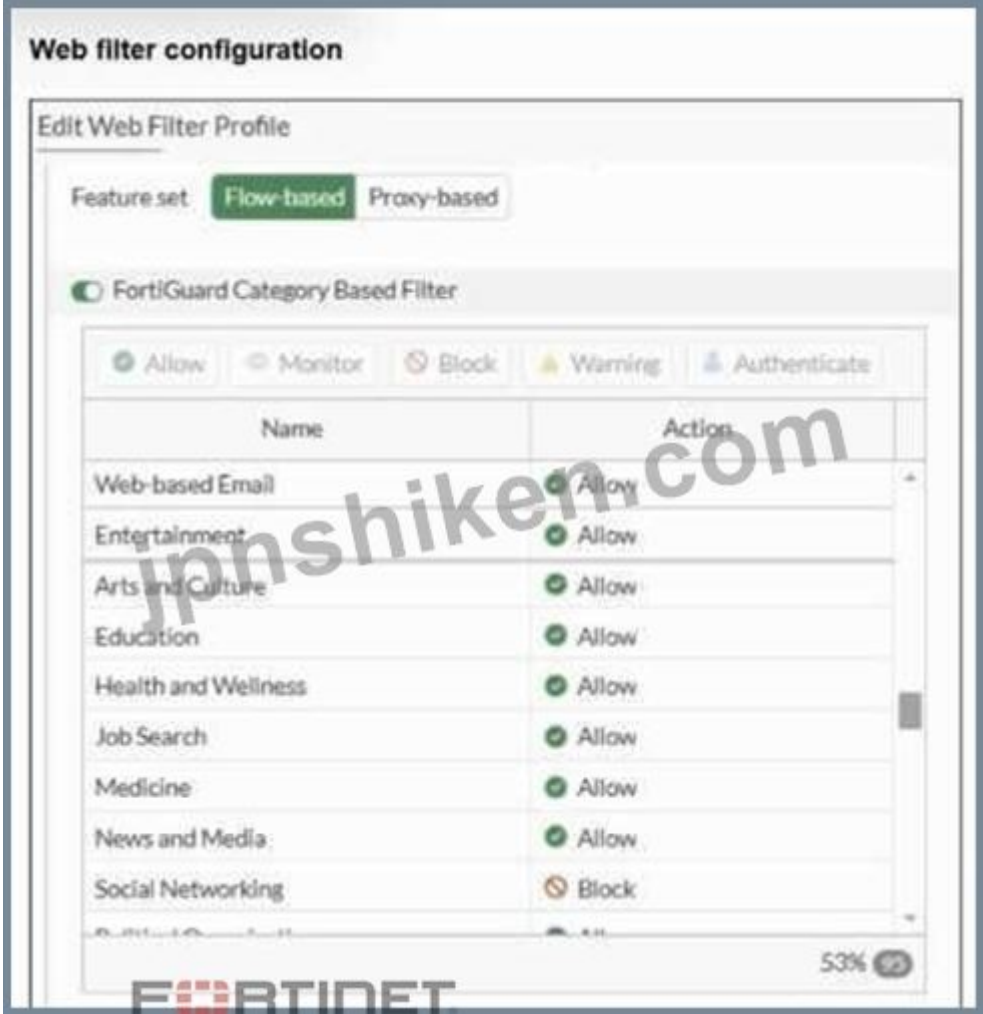
正解: (正解を表示します)

The serial console provides direct physical access to the FortiGate CLI without requiring any network connectivity. It connects via the FortiGate's console port using a serial cable, allowing administrators to perform initial configuration, recovery, or troubleshooting even if the network interfaces are down or misconfigured.

質問: 42

添付資料を参照してください。管理者は、Facebookを除く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と、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. www.facebook.com のアクションを除外設定する静的URLフィルター内。

- 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.** FortiGuard 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アクションを警告に設定します。
- D.** 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。

正解: ([正解を表示します](#))

質問: 43

FortiGateの管理者がポリシーでSSLディープインスペクションを有効にしましたが、ユーザーのブラウザで証明書の警告が表示されるという報告がありました。ディープインスペクションを有効にしたままこの問題を解決するための最も適切な手順は何でしょうか？

- A.** クライアントデバイスにFortiGate CA証明書をインストールします。
- B.** ポリシーでHTTPSスキャンを無効にする
- C.** ポリシー上のすべてのセキュリティ プロファイルを無効にする
- D.** ポリシーアクションを承認から拒否に変更します

正解: **A** ([コメントを发表する](#))

When FortiGate performs SSL deep inspection, it substitutes the original server certificate with one it generates on the fly, signed by its internal CA. If endpoints do not trust that CA, they report errors. Deploying the FortiGate CA as a trusted root certificate on client machines resolves the warnings while retaining the ability to inspect encrypted traffic for malware, policy violations, and suspicious behavior.

質問: 44

ウェブフィルタプロファイルで複数の機能が有効になっている場合、ウェブフィルタリングにおけるHTTP検査プロセスは特定の順序で実行されます。

ウェブフィルタプロファイルでセーフサーチなどの機能が有効になっている場合、FortiGateはどの順序で処理する必要がありますか？

- A.** DNSベースのWebフィルタとプロキシベースのWebフィルタ
- B.** 静的URLフィルタ、FortiGuardカテゴリフィルタ、および高度なフィルタ
- C.** FortiGuardカテゴリフィルタと評価フィルタ
- D.** 静的ドメインフィルタ、SSL検査フィルタ、および外部コネクタフィルタ

正解: ([正解を表示します](#))

Remember that the web filtering profile has several features. So, if you have enabled many of them, the inspection order flows as follows:

1. The local static URL filter
2. FortiGuard category filtering (to determine a rating)
3. Advanced filters (such as safe search or removing Active X components).

質問: 45

SSL証明書検査が有効になっている場合、FortiGateはSSLサーバーのホスト名を識別するために、どの3つの情報を使用しますか？(3つ選択してください。)

- A.** HTTP ヘッダーのホスト フィールド。
- B.** クライアントハローメッセージのサーバー名表示(SNI)拡張機能。
- C.** サーバー証明書のサブジェクト代替名 (SAN) フィールド。
- D.** サーバー証明書のサブジェクトフィールド。
- E.** サーバー証明書のシリアル番号。

正解: ([正解を表示します](#))

When using SSL certificate inspection, FortiGate is not decrypting the traffic. During the exchange of hello messages at the beginning of an SSL handshake, FortiGate parses the server name indication (SNI) from client Hello, which is an extension of the TLS protocol. The SNI tells FortiGate the hostname of the SSL server, which is validated against the DNS name before receipt of the server certificate. If there is no SNI exchanged, then FortiGate identifies the server by the value in the server by the value in the Subject field or SAN (Subject Alternative Name) field in the server certificate.

質問: 46

図を参照してください。FortiGuard接続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。)

```
FortiGate # diagnose debug rating
Locale      : English

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

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

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

- A. FortiGate は FortiGuard との通信にデフォルト ポートを使用しています。
- B. FortiGate は DNS ルックアップを使用して FortiGuard サーバーを識別しました。
- C. 失敗したパケットの数が増えるにつれて重みが増加します。
- D. FortiGuard Serverとの通信に信頼性の低いプロトコルを設定できます。

正解: (正解を表示します)

FortiGuard web filtering, DNS filtering, and antispam service.fortiguard.net uses a proprietary protocol over UDP port 53 or 8888 securewf.fortiguard.net uses HTTPS over ports 443, 53, or 8888.

The weight value reflects server reliability. It decreases with good performance and increases as packet loss or failures rise, meaning higher weight indicates more failures.

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、**3 0 %ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 47

図を参照してください。管理者は、HAクラスタの両方のメンバーを同時に構成しました。1週間の監視後、管理者はHAフェイルオーバーのパフォーマンスを確認したいと考えています。管理者はどのようにしてフェイルオーバーを強制実行できますか？

HQ-NGFW-1 HA configuration

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

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

HQ-NGFW-2 HA configuration

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

- A. 管理者はHQ-NGFW-1のHA稼働時間をリセットする必要があります。
- B. 管理者は、HQ-NGFW-2 でパラメータオーバーライドを有効にするように設定する必要があります。
- C. 管理者は HQ-NGFW-2 の HA 優先度を上げる必要があります。
- D. 管理者は、HQ-NGFW-1 の監視対象ポートをダウンに設定する必要があります。

正解: ([正解を表示します](#))

Both FortiGates are in an active-passive (a-p) HA cluster with override disabled. This means failover is triggered only if the primary (HQ-NGFW-1) becomes unavailable or monitored interfaces fail. To test failover performance, the administrator can set the monitored interface (port1) down on HQ-NGFW-1, which will force a failover to HQ-NGFW-2.

質問: 48

添付資料を参照してください。管理者は、Facebookを除く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と、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？

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



- A. [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。
- B. FortiGuard 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アクションを警告に設定します。
- 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 FortiGuard category filter is blocking Social Networking, which includes Facebook. Although a static URL filter entry for www.facebook.com exists, its action is set to Monitor, so it does not override the category block. To allow Facebook while blocking other social networking sites, the action for www.facebook.com in the Static URL Filter must be set to Exempt. This explicitly bypasses category filtering for that URL.

質問: 49

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](#))

When you select Best Quality the "Load Balancing" toggle disappears from the UI. When you select Lowest Cost (SLA) you can choose to enable or disable load balancing.

質問: 50

展示資料を参照してください。管理者は、セキュリティファブリックに HQ-ISFW-2 を追加したいと考えています。HQ-ISFW-2 は HQ-ISFW と同じサブネットにあります。HQ-ISFW でセキュリティファブリック設定を構成した後、
2. ステータスは保留のままです。

Security Fabric logical topology view

The diagram illustrates the Security Fabric logical topology. It shows a cloud icon connected to HQ-NGFW-1 Fabric Root. HQ-NGFW-1 is connected to HQ-ISFW-2 via port6 and port4. Below the diagram, two tables provide details for the interfaces involved:

FortiAnalyzer	
Interface	port6
Link	10 Gbps Full Duplex
Port Speed	Auto-Negotiation
Type	Physical Interface
IPv4 Addresses	10.0.13.254/24

HQ-ISFW-2	
Interface	port4
Link	10 Gbps Full Duplex
Port Speed	Auto-Negotiation
Type	Physical Interface
IPv4 Addresses	10.0.11.254/24

Security Fabric settings on HQ-ISFW-2

Security Fabric Settings

Security Fabric role

Standalone Serve as Fabric Root **Join Existing Fabric**

Allow other Security Fabric devices to join

☒ port6

Upstream FortiGate IP/FQDN

10.0.13.254

Allow downstream device REST API access ⓘ

☒

Management IP/FQDN ⓘ

Use WAN IP **Specify**

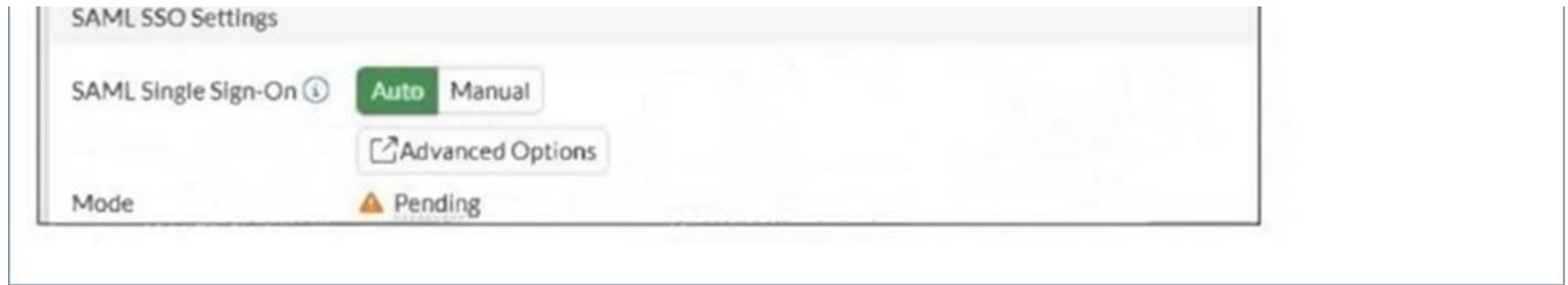
10.0.11.250

Management port

Use Admin Port **Specify**

443

FORTINET®



考えられる理由は2つあります。(2つ選択してください。)

- A. アップストリーム FortiGate IP は 10.0.11.254 に設定する必要があります。
- B. SAMLシングルサインオンは手動に設定する必要があります。
- C. HQ-ISFW-2 は HQ-ISFW で認証される必要があります。
- D. 管理IPは10.0.13.254に設定する必要があります。

正解: [\(正解を表示します\)](#)

The Upstream FortiGate IP should match the IP address of the Fabric Root interface, which is 10.0.11.254, not 10.0.13.254.

The new device (HQ-ISFW-2) must be authorized on the Fabric Root (HQ-ISFW) before it can join the Security Fabric, otherwise the status remains pending.

質問: 51

FortiGuard接続のデバッグ出力を示す図を参照してください。

FortiGuard connection debug output

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract

Service     : Antispam
Status      : Disable

Service     : Virus Outbreak Prevention
Status      : Disable

Num. of servers : 1
Protocol     : https
Port        : 443
Anycast     : Enable
Default servers : Included

-- Server List (Thu Jun  9 11:26:56 2022) --

IP           Weight  RTT  Flags  TZ  FortiGuard-requests  Curr  Lost  Total  Lost  Updated Time
173.243.141.16   -8    18   DI    0      4                0      0      0  Thu Jun  9 11:26:24 2022
12.34.97.18      20    30   1     1      1                0      0      0  Thu Jun  9 11:26:24 2022
210.7.96.18     160   305   9     9      0                0      0      0  Thu Jun  9 11:26:24 2022
```

出力結果に基づいて、管理者はFortiGuard接続についてどのような2つの事実を把握しているでしょうか？(2つ選択してください。)

- A. 契約情報を取得するために、1台のサーバーに接続しました。
- B. FortiGate はデフォルトの FortiGuard 通信設定を使用しています。
- C. 少なくとも1台のサーバーでパケットが連続して失われました。
- D. ローカルのFortiManagerは、FortiGateが通信するサーバーの1つです。

正解: (正解を表示します)

The output shows that one server was contacted to retrieve FortiGuard contract information, as indicated under "Service : Web-filter" with "License : Contract" and "Num. of servers : 1." The entry "Default servers : Included" confirms that FortiGate is using the default FortiGuard communication settings, meaning it communicates directly with Fortinet's public FortiGuard servers instead of a custom or local override.

質問: 52

SSL VPN環境において、中間デバイスがトラフィックをブロックすることによって引き起こされる接続問題を分析しています。

この問題を効果的に解決できる方法は、次のうちどれですか？(2つ選択してください。)

- A. IKEフラグメンテーションを無効にすると、大規模な証明書ネゴシエーションの問題を解決できます。
- B. フラグメントドロップや大規模な証明書交換の問題を解決するには、IPsecを使用する必要があります。
- C. SSL VPNトンネルモードを使用すると、ブロックされたESPおよびUDPポート(500または4500)の問題を回避できます。
- D. ハブアンドスポークトポロジをSSL VPNトンネルで構成して、ブロックされたUDPポートをバイパスできます。

正解: C,D (コメントを發表する)

The training is basically trying to point out the advantage of FortiGate's SSL VPN over IPSec VPN in situation where issues are caused by an intermediate device. IPsec uses ESP and UDP 500 and 4500, so where these are blocked, SSL VPN tunnel mode shines because it uses HTTPS (443) and TLS by default (both TCP). Again where UDP ports are blocked, SSL VPN shines (Tunnel mode Hub and Spoke) because it does not use UDP.

質問: **53**

FortiGateがSSL/SSHのフルインスペクションを実行する際、無効な証明書を検出した場合の対応方法を設定できます。

FortiGateが無効な証明書を検出した際に実行できる有効なアクションはどれですか？(3つ選択してください。)

- A. 許可する
- B. 信頼して許可する
- C. 許可と警告
- D. ブロック
- E. ブロックと警告

正解: ([正解を表示します](#))

When a certificate fails for any of the reasons above, you can configure any of the following actions:

* Keep Untrusted & Allow: FortiGate allows the website and lets the browser decide the action to take.

FortiGate takes the certificate as untrusted.

* Block: FortiGate blocks the content of the site.

* Trust & Allow: FortiGate allows the website and takes the certificate as trusted.

質問: **54**

自動化ステッチの特徴を説明しているのは、次のうちどれですか？(2つ選択してください。)

- A. アクションは、セキュリティファブリックに含まれるデバイスのみに関係します。
- B. 自動化ステッチには複数のトリガーを設定できます。
- C. 複数のアクションを並行して実行できます。
- D. トリガーには外部コネクタが関与する場合があります。

正解: **C,D** ([コメントを発表する](#))

Automation stitches can execute multiple actions concurrently (in parallel).

Triggers for automation stitches can come from external connectors beyond just Fortinet devices.

質問: **55**

図を参照してください。管理者は、図に示されているログメッセージをどのように閲覧できますか？

(2つ選択してください。)

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime t=1756915802 devname="HQ-NGFW-1"
```

- A. セキュリティイベントログページ経由
- B. FortiGate CLIコマンドdiagnose log testによる診断
- C. 暗黙の拒否ポリシーを右クリックする
- D. ログエントリでポリシーUUIDとアプリケーション名によるフィルタリング

正解: **A,D** ([コメントを发表する](#))

The log shown is a UTM application control log, which can be viewed through the Security Event log page. The administrator can also filter logs by the Policy UUID and Application Name to find specific entries like the one in the exhibit.

質問: 56

NGFWのプロファイルベースモードの2つの特徴は何ですか？(2つ選択してください。)

- A. NGFW プロファイルベースモードは、グローバルにのみ適用でき、個々の VDOM には適用できません。
- B. NGFW プロファイルベースモードでは、中央ソース NAT ポリシーの使用が必須となります。
- C. NGFW プロファイルベースモードポリシーは、フロー検査とプロキシ検査の両方をサポートします。
- D. NGFW プロファイルベースモードでは、ファイアウォールポリシーにアプリケーションおよび Web フィルタリング プロファイルを適用できます。

正解: ([正解を表示します](#))

NGFW (Next Generation Firewall) profile-based mode in FortiGate allows policies to use both flow- based and proxy-based inspection modes, providing flexibility depending on security and performance requirements. Additionally, profile-based mode supports applying applications and web filtering profiles directly in a firewall policy, allowing granular control over the traffic.

質問: 57

自動縫製の特徴として正しい記述はどれですか？

- A. トリガーは1つ以上持つことができます。
- B. ファブリック内の下流デバイスでのみ作成できます。
- C. 複数のアクションを同時に実行できます。
- D. これらはセキュリティファブリック内のデバイスでのみ実行できます。

正解: ([正解を表示します](#))

The stitch Action execution can be set to either Sequential or Parallel. In sequential execution, actions will execute one after another with a delay (if specified). If one action fails, then the action chain stops. This is the default setting. In parallel execution, all actions will execute immediately when the stitch is triggered.

質問: 58

デバッグフローの出力を示す図を参照してください。

Debug Flow output

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=5.

allocate a new session-00000721

in-[port4], out-[]

len=0

result:skb_flags-02000000, vid-0, ret no-match, act-accept, flag-00000000

find a route: flag=00000000 gw-0.0.0.0 via port2

in[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0

gnum-100004, use addr/intf hash, len=3

checked gnum-100004 policy-2, ret-matched. act-accept

ret-matched

gnum-4e20, check-fffffffa002c9c7

checked gnum-4e20 policy-6, ret-no-match, act-accept

gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000

policy-2 is matched, act-drop

after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-2

Denied by forward policy check (policy 2)

デバッグフローの出力から、どのような2つの結論を導き出せますか？(2つ選択してください。)

- A. デフォルトゲートウェイはポート2に設定されています。
- B. RPFチェックに失敗しました。
- C. デバッグフローはUDPトラフィック用です。
- D. 一致するファイアウォールポリシーにより、トラフィックが拒否されます。

正解: (正解を表示します)

The default gateway is configured on port2 → The debug output shows find a route:

flag=00000000 gw=0.0.0.0 via port2, which indicates that the default route (0.0.0.0/0) points out port2.

The matching firewall policy denies the traffic → The log line Denied by forward policy check (policy 2) confirms that policy 2 matched and explicitly dropped the traffic.

質問: 59

FortiGateデバイス間でSSL VPNを機能させるために必要な設定はどれですか？(2つ選択)

(2つ選択してください。)

- A. サーバーのFortiGateは、クライアントのFortiGate証明書を検証するためにCA証明書を必要とします。
- B. クライアント FortiGate は、リモートサブネットへのルートを手動で追加する必要があります。
- C. クライアント FortiGate は、サーバー FortiGate 上の CA によって署名されたクライアント証明書を必要とします。
- D. クライアント FortiGate は SSL VPN に接続するために SSL VPN トンネルインターフェイスタイプを必要とします。

正解: (正解を表示します)

The FortiGate can be configured as an SSL VPN client, using an SSL-VPN Tunnel interface type.

The FortiGate devices must have the proper CA certificate installed to verify the certificate chain to the root CA that signed the certificate.

質問: 60

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す図を参照してください。

Policy	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
[-] port4 → port2 1								
☐ Internet (1)	4 HQ SUBNET Remote-users	4 all	always	ALL ICMP HTTPS HTTP	✓ ACCEPT	✓ NAT	Standard	WEB Category Monitor SSL certificate-inspection

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場合、ユーザーにログインプロンプトが表示されません。

この状況の最も可能性の高い原因は何ですか？

- A. ファイアウォール ポリシーでは、サービス DNS が必要です。
- 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. 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。
- D. リモートユーザーグループが宛先に追加されません。

正解: A (コメントを發表する)

DNS is usually used by HTTP so that people can use domain names for websites, instead of their IP address. DNS is allowed because it is a base protocol and will most likely be required to initially see proper authentication protocol traffic... However, the DNS service must still be defined in the policy as allowed, in order for it to pass.

質問: 61

展示資料を参照してください。

SSL VPN settings

FORTINET

SSL-VPN Settings

Connection Settings ⓘ

Enable SSL-VPN ☒

Listen on Interface(s)

port1

+

x

Listen on Port

11443

Web mode access will be listening at <https://10.200.1.1:11443>

Server Certificate

Fortinet_Factory

Redirect HTTP to SSL-VPN ☐

Restrict Access

Allow access from any host Limit access to specific hostsIdle Logout ☒

Inactive For

300

Seconds

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range

Automatically assign addresses Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server

Same as client system DNS SpecifySpecify WINS Servers ☐

Web Mode Settings

Language ⓘ

Browser Preference System

Authentication/Portal Mapping ⓘ

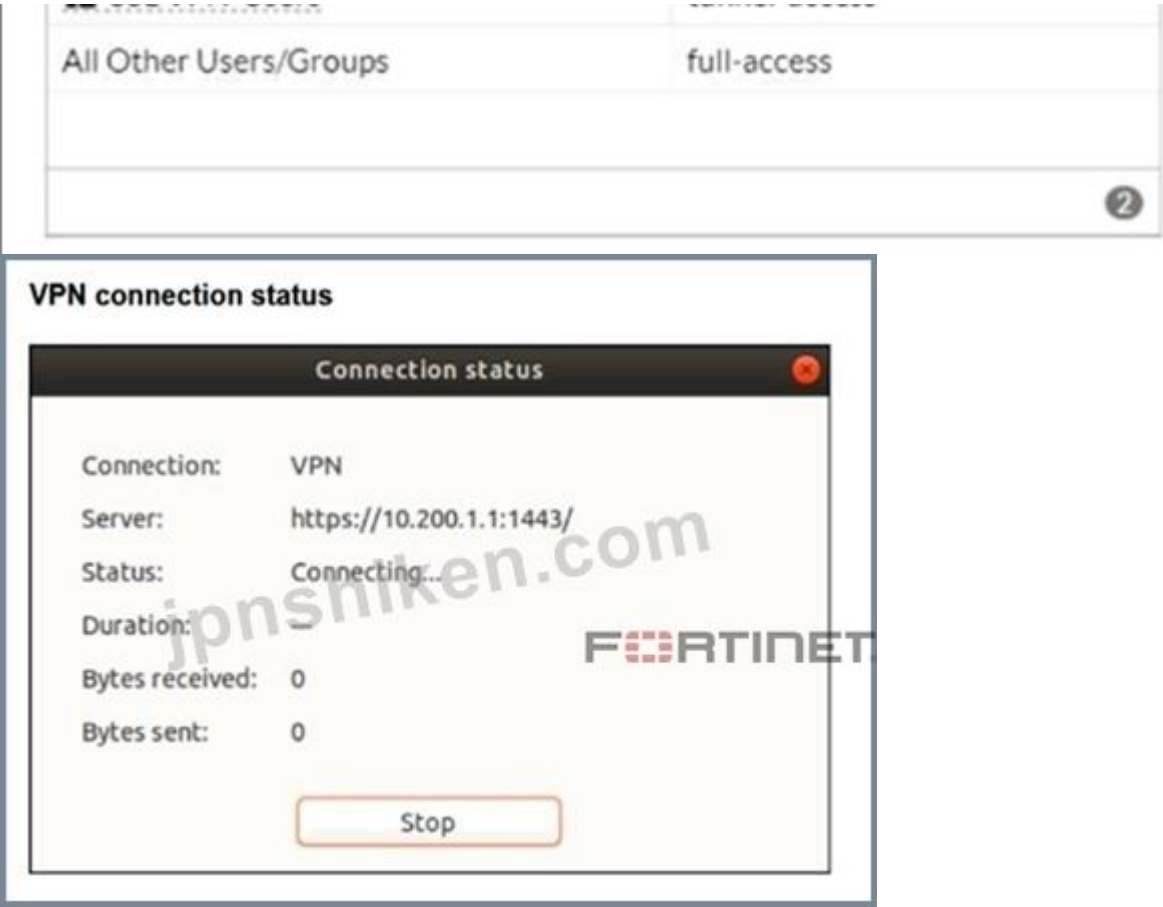
[+ Create New](#)[Edit](#)[Delete](#)[Send SSL-VPN Configuration](#)

Users/Groups ⇅

Portal ⇅

SSL-VPN-Users

tunnel-access



- ユーザーがSSL VPNに接続しようとする、接続が失敗します。
- ユーザーがSSL VPNに正常に接続するには、どのような操作を行うべきですか？
- A. クライアントの SSL VPN ポートを変更します。
 - B. SSL VPNポータルをトンネルに変更します。
 - C. サーバーのIPアドレスを変更します。
 - D. アイドルタイムアウトを変更します。

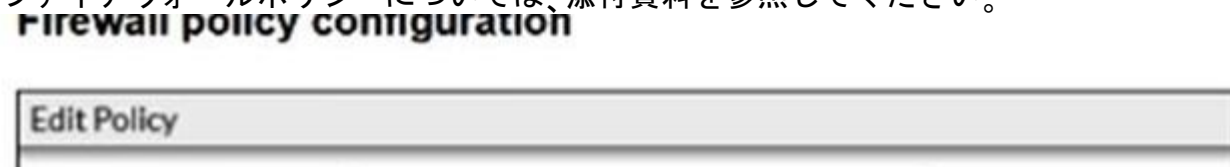
正解: ([正解を表示します](#))

In the FortiGate SSL-VPN settings, the VPN is configured to listen on port 11443, as shown in the "Listen on Port" field. However, the VPN client is attempting to connect to https://10.200.1.1:443/, which uses the default HTTPS port (443) instead of the configured port. To successfully connect, the user must change the SSL VPN port on the client to 11443 so that it matches the listening port defined on the FortiGate device.

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: 62

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。



Name Internet_Access

Incoming Interface port2 + ×

Outgoing Interface port1 + ×

Source all + ×

Destination all + ×

Schedule always ▼

Service DNS ×
FTP ×
HTTP ×
HTTPS ×
+

Action ✓ ACCEPT ✗ DENY

Inspection Mode Flow-based Proxy-based

Firewall/Network Options

NAT ☒

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options PROT default ✎

Security Profiles

AntiVirus ☒ AV default ✎

Web Filter ☐

DNS Filter ☐

Application Control ☐

IPS ☐

File Filter ☐

SSL Inspection SSL certificate-inspection ✎

なぜファイアウォールポリシーは、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でしょうか？

- A. 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。
- B. ファイアウォール ポリシーで Web フィルタが有効になっていないため、ウイルス対策プロファイルが補完されません。
- 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のアクションが拒否に設定されていません。

正解: **A** ([コメントを発表する](#))

The firewall policy uses certificate-inspection under SSL inspection and flow-based inspection mode. Certificate inspection does not decrypt HTTPS traffic; it only checks the certificate fields. Because of this, FortiGate cannot perform deep content inspection, which is required for antivirus to detect and block threats such as the EICAR test virus within encrypted HTTPS sessions.

質問: 63

FortiGateはNATモードで動作しており、LANネットワークとDMZネットワークにそれぞれ接続された2つの物理インターフェースを備えています。

FortiGateの接続された物理インターフェースの要件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. 両方のインターフェースにインターフェースロールが割り当てられている必要があります。
- B. 両方のインターフェースは、ルーティングテーブル上で直接接続されたルートを持っている必要があります。
- C. 両方のインターフェースでDHCPが有効になっており、インターフェースにLANおよびDMZの役割が割り当てられている必要があります。
- D. 両方のインターフェースにIPアドレスが割り当てられている必要があります。

正解: ([正解を表示します](#))

In NAT mode, FortiGate routes packets based on layer 3, like a router. Each of its logical network interfaces has an IP address, and FortiGate determines the outgoing or egress interface based on the destination IP address and entries in its routing tables.

質問: 64

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)

(2つ選択してください。)

- A. 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。
- B. 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。
- C. 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。
- D. 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。

正解: **C,D** ([コメントを発表する](#))

SD-WAN is enabled: v4-ecmp-mode is hide and you control the ECMP algorithm with the load- balance-mode setting.

SD-WAN is disabled: ECMP algorithm is set on the CLI: config system settings.

<https://docs.fortinet.com/document/fortigate/7.4.6/administration-guide/25967/equal-cost-multi- path>

質問: 65

管理者は、シャドウITの可視性に関する課題に対処し、ユーザーが適切な承認なしに機密ファイルを組織外に送信することを防止したいと考えています。これらの目標を達成するために、管理者はどのFortiSASEメソッドを導入すべきでしょうか？

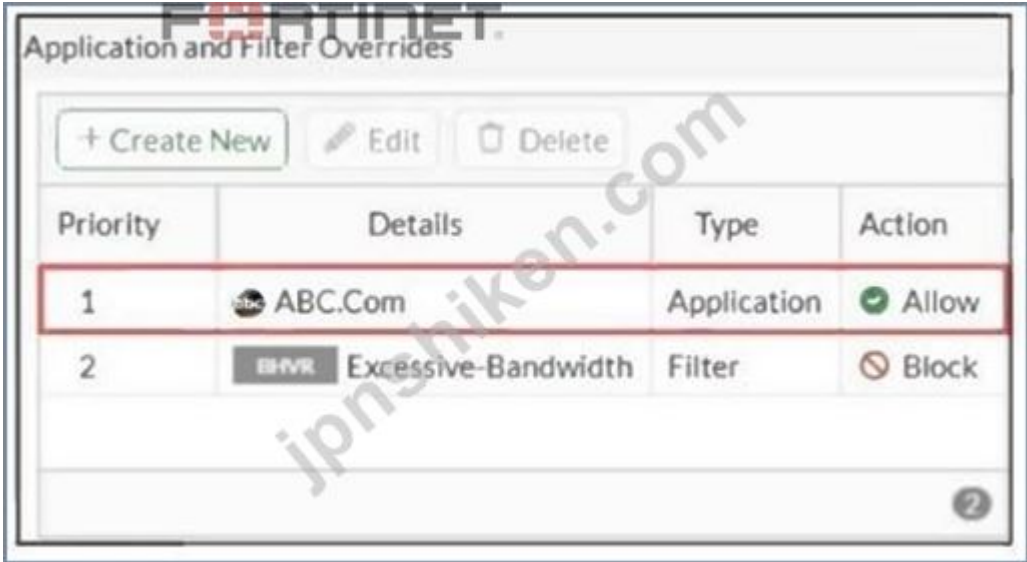
- A. セキュア インターネット アクセス (SIA)
- B. セキュアプライベートアクセス (SPA)
- C. セキュアなSaaSアクセス(SSA)
- D. セキュアSD-WANアクセス(SSD-WAN)

正解: ([正解を表示します](#))

Secure SaaS Access (SSA) provides visibility into shadow IT and allows control over SaaS applications, including enforcing policies to prevent sensitive files from being uploaded or shared without proper approval.

質問: 66

図を参照してください。管理者は、ABC.Comアプリケーションの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のWebサイトに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 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。
- B. 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。
- C. ABC.Com アクションは 許可」に設定されています。
- D. ABC.Com は 帯域幅過剰」のカテゴリに該当します。

正解: (正解を表示します)

When the action is set to Allow in an application override, traffic matching this override is allowed without generating security logs because it bypasses deeper inspection and blocking.

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」