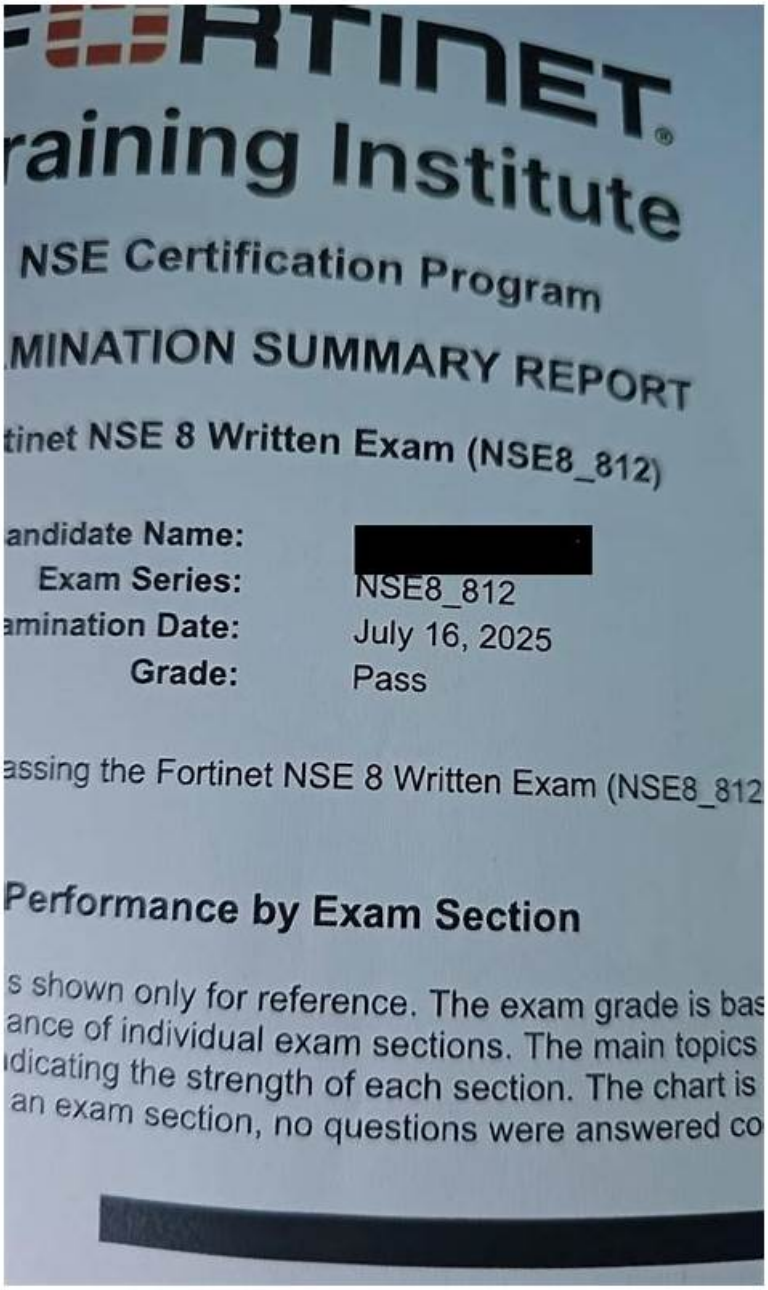
試験NSE8_812復習内容 &更新するNSE8_812トレーニング |大人気NSE8_812最新受験攻略



P.S. MogiExamがGoogle Driveで共有している無料かつ新しいNSE8_812ダンプ：https://drive.google.com/open?id=1xTgz_kW_ZgEtP-DU9tD3ji_VV0X4sFTp

MogiExam10年以上のビジネスエクスペリエンスを備えたFortinetのNSE8_812テストトレントは、顧客の購入エクスペリエンスを非常に重視しました。 電子製品の購入速度を心配する必要はありません。 弊社では、NSE8_812試験準備の信頼性を長期間にわたって評価および評価し、保証された購入スキームを提案するために尽力しています。 必要な場合は、NSE8_812テストトレントを使用するためのリモートオンラインガイダンスも利用できます。 通常、購入後数分でFortinet NSE 8 - Written Exam (NSE8_812)練習問題を効率よく取得できます。

Fortinet NSE8_812 認定試験は、ネットワークセキュリティ分野の知識やスキルを証明したい専門家を対象にした筆記試験です。この試験は、Fortinetのソリューションを使用して複雑なセキュリティインフラストラクチャを設計・実装・管理する経験を持つ人々を対象としています。

>> NSE8_812復習内容 <<

NSE8_812トレーニング & NSE8_812最新受験攻略

確かにFortinet　NSE8_812試験に準備する過程は苦しいんですけど、Fortinet　NSE8_812資格認定を手に入れるなり、IT業界で仕事のより広い将来性を持っています。あなたの努力を無駄にするのは我々MogiExamのすべきことです。MogiExamのレビューから見ると、弊社MogiExamは提供している質高い試験資料は大勢の顧客様の認可を受け取ったと考えられます。我々はあなたにFortinet　NSE8_812試験に合格させるために、全力を尽くします。

Fortinet NSE8_812試験は、ネットワークセキュリティーに関する幅広いトピックをカバーしています。ネットワークアーキテクチャ、セキュリティープロトコル、侵入防止、エンドポイントセキュリティー、クラウドセキュリティーなどが含まれます。この試験は、複雑な環境でネットワークセキュリティーの解決策を設計・実装する責任がある個人の知識とスキルをテストするために設計されました。

Fortinet NSE 8-筆記試験としても知られるFortinet NSE8_812は、Fortinet製品を使用して複雑なセキュリティソリューションの設計、実装、および管理における候補者の知識とスキルを検証するFortinetが提供する認定試験です。この試験は、すでにFortinet NSE 7認定を獲得しており、Fortinetのセキュリティファブリックと関連技術を深く理解している経験豊富な専門家向けに設計されています。

Fortinet NSE 8 - Written Exam (NSE8_812) 認定 NSE8_812 試験問題 (Q54-Q59):

質問 # 54
You are deploying a FortiExtender (FEX) on a FortiGate-60F. The FEX will be managed by the FortiGate. You anticipate high utilization. The requirement is to minimize the overhead on the device for WAN traffic.
Which action achieves the requirement in this scenario?

- A. Change connectivity between the FortiGate and the FortiExtender to use VLAN Mode
- B. Enable CAPWAP connectivity between the FortiGate and the FortiExtender.
- C. Add a VLAN under the FEX-WAN interface on the FortiGate.
- D. Add a switch between the FortiGate and FEX.

正解：B

解説：
The FortiExtender (FEX) is a device that provides wireless WAN connectivity for FortiGate devices by using 3G/4G/LTE cellular networks. The FEX can be managed by the FortiGate device that it connects to, or by a FortiManager device in a centralized management scenario. The FEX can use either Ethernet or CAPWAP connectivity to communicate with the FortiGate device. Ethernet connectivity means that the FEX uses a standard Ethernet connection to send and receive data packets from the FortiGate device. CAPWAP connectivity means that the FEX uses a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel to encapsulate data packets and send them over an IP network to the FortiGate device. If the requirement is to minimize the overhead on the device for WAN traffic, one option is to enable CAPWAP connectivity between the FortiGate and the FEX. This option can reduce the overhead on the device by offloading some of the processing tasks from the CPU to the NP6 processor, which can handle CAPWAP traffic more efficiently than Ethernet traffic. This option can also provide more flexibility and scalability for WAN traffic by allowing multiple FEX devices to connect to a single FortiGate device over an IP network. Reference:
https://docs.fortinet.com/document/fortigate/7.0.0/cookbook/19662/configuring-fortigate-with-fortiextender
https://docs.fortinet.com/document/fortigate/7.0.0/cookbook/19662/capwap-connectivity

質問 # 55
Refer to the exhibit.

```
FGT_3 # show router ospf
config router ospf
    set router-id 10.10.10.3
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "port2"
            set interface "port2"
            set network-type point-to-point
        next
    end
    config network
        edit 1
            set prefix 10.10.10.0 255.255.255.0
        next
    end
end
```

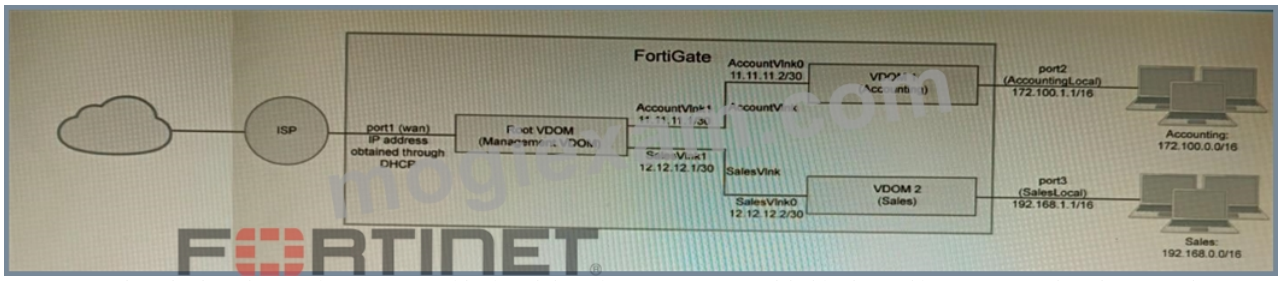
You are operating an internal network with multiple OSPF routers on the same LAN segment. FGT_3 needs to be added to the OSPF network and has the configuration shown in the exhibit. FGT_3 is not establishing any OSPF connection.
What needs to be changed to the configuration to make sure FGT_3 will establish OSPF neighbors without affecting the DR/BDR election?

- A.
```
config router ospf
   config ospf-interface
      edit "port2"
         set priority 0
         set network-type point-to-multipoint
      next
   end
end
```
- B.
```
config router ospf
   config ospf-interface
      edit "port2"
         set priority 0
         set network-type broadcast
      next
   end
end
```
- C.
```
config router ospf
   config ospf-interface
      edit "port2"
         set priority 255
         set network-type broadcast
      next
   end
end
```
- D.

正解：B

解説：
The OSPF configuration shown in the exhibit is using the default priority value of 1 for the interface port1. This means that FGT_3 will participate in the DR/BDR election process with the other OSPF routers on the same LAN segment. However, this is not desirable because FGT_3 is a new device that needs to be added to the OSPF network without affecting the existing DR/BDR election. Therefore, to make sure FGT_3 will establish OSPF neighbors without affecting the DR/BDR election, the priority value of the interface port1 should be changed to 0. This will prevent FGT_3 from becoming a DR or BDR and allow it to form OSPF adjacencies with the current DR and BDR. Option B shows the correct configuration that changes the priority value to 0. Option A is incorrect because it does not change the priority value. Option C is incorrect because it changes the network type to point-to-point, which is not suitable for a LAN segment with multiple OSPF routers. Option D is incorrect because it changes the area ID to 0.0.0.1, which does not match the area ID of the other OSPF routers on the same LAN segment. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/358640/basic-ospf-example

質問 # 56
Refer to the exhibit.



A customer has deployed a FortiGate 300E with virtual domains (VDOMs) enabled in the multi-VDOM mode. There are three VDOMs: Root is for management and internet access, while VDOM 1 and VDOM 2 are used for segregating internal traffic. AccountVInk and SalesVInk are standard VDOM links in Ethernet mode.
Given the exhibit, which two statements below about VDOM behavior are correct? (Choose two.)

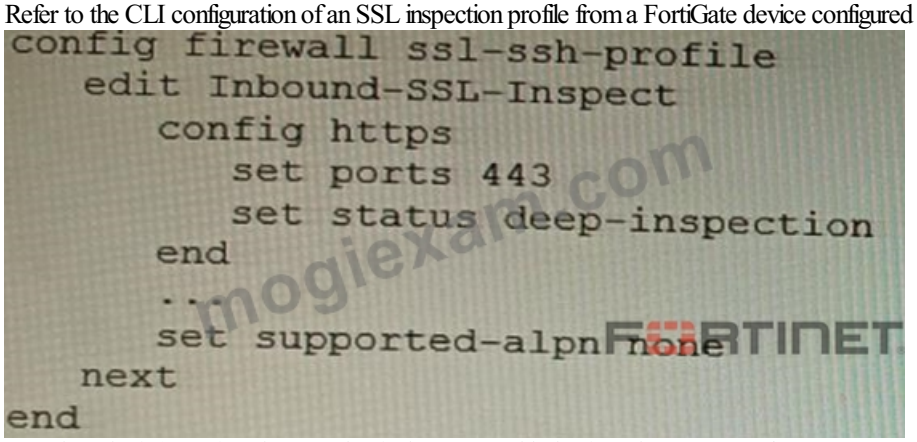
- A. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides.
- B. Traffic on AccountVInk and SalesVInk will not be accelerated.
- C. Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs.
- D. OSPF routing can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVInk
- E. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode

正解：C、E

解説：
a) You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode. This is because VDOM links can be configured in either PPP or Ethernet mode, and OSPF routing can be configured on both types of links.
d) Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs. This is because the Root VDOM is the default VDOM, and it is used for management and internet access. VDOM 1 and VDOM 2 are traffic type VDOMs,

which are used for segregating internal traffic.
The other options are not correct.
b) Traffic on AccountVInk and SalesVInk will not be accelerated. This is because VDOM links are not accelerated by default. However, you can configure acceleration on VDOM links if you want.
c) The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides. This is not necessarily true. The VDOM links could be in PPP mode even if they have IP addresses assigned on both sides.
e) OSPF routing can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVInk. This is correct. OSPF routing can be configured between any two VDOMs, even if they are not directly connected. In this case, the OSPF routing would be configured on the AccountVInk link.

質問 # 57
Refer to the CLI configuration of an SSL inspection profile from a FortiGate device configured to protect a web server:



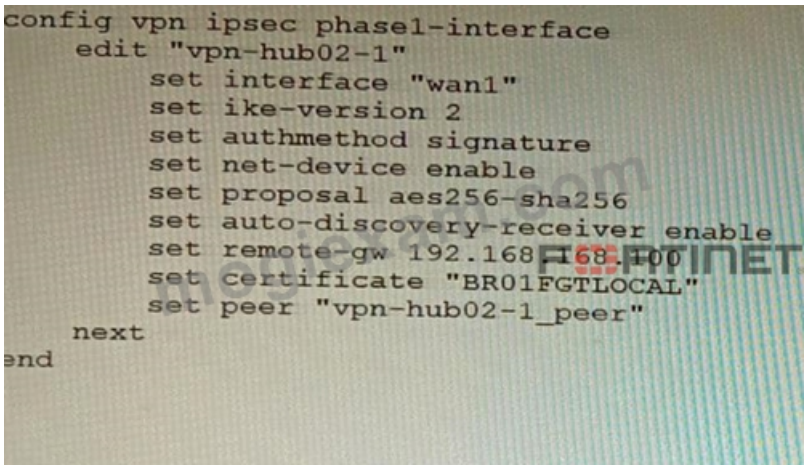
Based on the information shown, what is the expected behavior when an HTTP/2 request comes in?

- A. FortiGate will forward the traffic without modifying the ALPN header.
- B. FortiGate will rewrite the ALPN header to request HTTP/1.
- C. FortiGate will reject all HTTP/2 ALPN headers.
- D. FortiGate will strip the ALPN header and forward the traffic.

正解：C

解説：
The supported-alpn parameter is set to http1.1 in the SSL inspection profile. This means that the FortiGate will only accept HTTP/1.1 traffic. Any HTTP/2 traffic will be rejected.
The following is the relevant documentation from Fortinet:
The supported-alpn parameter specifies the list of ALPN protocols that the FortiGate will accept. If the client requests a protocol that is not in this list, the FortiGate will reject the connection.
The default value for the supported-alpn parameter is all. This means that the FortiGate will accept any ALPN protocol that the client requests.
To reject all HTTP/2 traffic, set the supported-alpn parameter to http1.1.
Source: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl-inspection

質問 # 58
Refer to the exhibit.



To facilitate a large-scale deployment of SD-WAN/ADVPN with FortiGate devices, you are tasked with configuring the FortiGate devices to support injecting of IKE routes on the ADVPN shortcut tunnels.
Which three commands must be added or changed to the FortiGate spoke config vpn ipsec phasei-interface options referenced in the exhibit for the VPN interface to enable this capability? (Choose three.)

- A. set mode-cfg-allow-client-selector enable
- B. set net-device disable
- C. set ike-version 1
- D. set mode-cfg enable
- E. set add-route enable

正解：A、D、E

解説：
* B must be set to enable mode-cfg, which is required for injecting IKE routes on the ADVPN shortcut tunnels.
* D must be set to enable add-route, which is the command that actually injects the IKE routes.
* E must be set to enable mode-cfg-allow-client-selector, which allows custom phase 2 selectors to be configured.
The other options are incorrect. Option A is incorrect because net-device disable is not required for injecting IKE routes on the ADVPN shortcut tunnels. Option C is incorrect because IKE version 1 is not supported for ADVPN.
References:
* Phase 2 selectors and ADVPN shortcut tunnels | FortiGate / FortiOS 7.2.0
* Configuring SD-WAN/ADVPN with FortiGate | FortiGate / FortiOS 7.2.0

質問 # 59
.....

- NSE8_812資格取得講座 □ NSE8_812復習教材 □ NSE8_812的中問題集 □ ▶ www.xhs1991.com ◀を開いて □ NSE8_812 □を検索し、試験資料を無料でダウンロードしてくださいNSE8_812関連日本語内容
- ユニークなNSE8_812復習内容一回合格-素晴らしいNSE8_812トレーニング □ “ www.goshiken.com ”には無料の【 NSE8_812 】問題集がありますNSE8_812日本語版対策ガイド
- NSE8_812日本語版対策ガイド □ NSE8_812復習問題集 □ NSE8_812日本語版受験参考書 □ 今すぐ □ www.xhs1991.com □で（ NSE8_812 ）を検索して、無料でダウンロードしてくださいNSE8_812資格取得講座
- academy.myabove.ng, socialmediastore.net, selfbizdirectory.com, haleemahphc393841.blogacep.com, bookmarkity.com, bookmarkdistrict.com, ezylinkdirectory.com, tetrabookmarks.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, elodiecmjm773268.wikikarts.com, Disposable vapes

2026年MogiExamの最新NSE8_812 PDFダンプおよびNSE8_812試験エンジンの無料共有：https://drive.google.com/open?id=1xTgz_kW_ZgEtP-DU9tD3ji_VV0X4sFTp