Trustworthy Fortinet NSE8_812 Pdf & Certification NSE8_812 Training

DOWNLOAD the newest VCE4Plus NSE8_812 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1pOngGRgYZ8H1owO7MJmI8uAqm_D1TAXn

As for Fortinet NSE8_812 exam, it is the most difficult to pass. But, as long as you believe in VCE4Plus, everything is ok. VCE4Plus Fortinet NSE8_812 exam simulations contain the most accurate questions and answers. If you don't believe our Fortinet NSE8_812 certification training, you can go to our VCE4Plus. You can find pdf real questions and answers and download it. And the purchase rate is unbelievably high every day. By choosing it, pass rate is 100%. Hurry up! Don't hesitate to add our Fortinet NSE8_812 Dumps Torrent to your shopping cart.

Fortinet NSE8_812 exam is an advanced-level certification exam that is designed to validate the skills and expertise of network security professionals. NSE8_812 exam is intended for those who have significant experience in designing, implementing, and managing complex network security solutions. The Fortinet NSE8_812 certification exam covers a wide range of topics, including advanced routing and switching, dynamic routing protocols, secure VPNs, advanced firewall policies, and advanced threat protection. NSE8_812 Exam is based on practical scenarios and real-world challenges that network security professionals may face in their day-to-day operations.

>> Trustworthy Fortinet NSE8_812 Pdf <<

Certification NSE8_812 Training & NSE8_812 Test King

The Fortinet NSE 8 - Written Exam (NSE8_812) NSE8_812 exam is a valuable credential that will assist you to advance your career. To pass the NSE8_812 exam is not an easy job. It always gives tough times to their candidates. The best NSE8_812 Exam

Preparation strategy along with the VCE4Plus NSE8_812 exam practice test questions can help you to crack the Fortinet NSE8_812 exam easily.

Passing the Fortinet NSE8_812 exam is a crucial step towards becoming a certified Fortinet expert. Fortinet NSE 8 - Written Exam (NSE8_812) certification is recognized globally and is highly respected in the cybersecurity industry. Fortinet NSE 8 - Written Exam (NSE8_812) certification is an endorsement of the candidates' skills and knowledge in developing and implementing effective security solutions using Fortinet products and services. It is also a testament to their commitment to continuous learning and development.

The NSE8_812 Exam covers a wide range of topics related to network security, including network design and topology, security protocols, VPN technologies, intrusion prevention, and web filtering. Candidates are required to have a deep understanding of these topics in order to pass the exam.

Fortinet NSE 8 - Written Exam (NSE8_812) Sample Questions (Q66-Q71):

NEW QUESTION # 66
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 net-device disable
- B. set ike-version 1
- C. set add-route enable
- D. set mode-cfg-allow-client-selector enable
- E. set mode-cfg enable

Answer: C,D,E

Explanation:
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

NEW QUESTION # 67
Refer to the exhibit, which shows a Branch1 configuration and routing table.
In the SD-WAN implicit rule, you do not want the traffic load balance for the overlay interface when all members are available.
In this scenario, which configuration change will meet this requirement?

- A. Change the load-balance-mode to source-ip-based.
- B. Create a new static route with the internet sdwan-zone only
- C. Configure the priority in each overlay member to 10.
- D. Configure the cost in each overlay member to 10.

Answer: C

Explanation:
The default load balancing mode for the SD-WAN implicit rule is source IP based. This means that traffic will be load balanced evenly between the overlay members, regardless of the member's priority.
To prevent traffic from being load balanced, you can configure the priority of each overlay member to 10. This will make the member ineligible for load balancing.
The other options are not correct. Changing the load balancing mode to source-IP based will still result in traffic being load balanced. Creating a new static route with the internet sdwan-zone only will not affect the load balancing of the overlay interface. Configuring the cost in each overlay member to 10 will also not affect the load balancing, as the cost is only used when the implicit

rule cannot find a match for the destination IP address.

NEW QUESTION # 68
Refer to the exhibits.
The exhibits show a diagram of a requested topology and the base IPsec configuration.
A customer asks you to configure ADVPN via two internet underlays. The requirement is that you use one interface with a single IP address on DC FortiGate.
In this scenario, which feature should be implemented to achieve this requirement?

- A. Use peer-id
- B. Use network-overlay id
- C. Change advpn2 to IKEv1
- D. Use local-id

Answer: B

Explanation:
A is correct because using network-overlay id allows you to configure multiple ADVPN tunnels on a single interface with a single IP address on the DC FortiGate. This is explained in the FortiGate Administration Guide under ADVPN > Configuring ADVPN > Configuring ADVPN on the hub. Reference: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn/978794/configuring-advpn

NEW QUESTION # 69
Refer to the exhibit.
You are deploying a FortiGate 6000F. The device should be directly connected to a switch. In the future, a new hardware module providing higher speed will be installed in the switch, and the connection to the FortiGate must be moved to this higher-speed port. You must ensure that the initial FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port speed is defined.
How should the initial connection be made?

- A. Connect the switch on any interface between ports 5 to 8.
- B. Connect the switch on any interface between ports 25 to 28
- C. Connect the switch on any interface between ports 21 to 24
- D. Connect the switch on any interface between ports 1 to 4

Answer: D

Explanation:
The FortiGate 6000F has 24 1/10/25-Gbps SFP28 data network interfaces (1 to 24). These interfaces are divided into the following interface groups: 1 to 4, 5 to 8, 9 to 12, 13 to 16, 17 to 20, and 21 to 24. The ports 25 to 28 are 40/100-Gbps QSFP28 data network interfaces.
The initial connection should be made to any interface between ports 1 to 4. This is because the ports 21 to 24 are part of the same interface group, and changing the speed of one of these ports will affect the speeds of all of the ports in the group. The ports 5 to 8 are also part of the same interface group, so they should not be used for the initial connection.
The new hardware module that will be installed in the switch will provide higher speed ports. When this module is installed, the speed of the ports 21 to 24 will be increased. However, this will not affect the ports 1 to 4, because they are not part of the same interface group.
Therefore, the initial connection should be made to any interface between ports 1 to 4, in order to ensure that the FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port speed is defined.
Reference:
FortiGate 6000F Front Panel Interfaces: https://docs.fortinet.com/document/fortigate-6000/hardware/fortigate-6000f-system-guide/827055/front-panel-interfaces

NEW QUESTION # 70
Refer to the exhibit showing FortiGate configurations
FortiManager VM high availability (HA) is not functioning as expected after being added to an existing deployment.
The administrator finds that VRRP HA mode is selected, but primary and secondary roles are greyed out in the GUI The managed

devices never show online when FMG-B becomes primary, but they will show online whenever the FMG-A becomes primary. What change will correct HA functionality in this scenario?

- A. Change the priority of FMG-A to be numerically lower for higher preference
- B. Make the monitored IP to match on both FortiManager devices.
- C. Change the FortiManager IP address on the managed FortiGate to 10.3.106.65.
- D. Unset the primary and secondary roles in the FortiManager CLI configuration so VRRP will decide who is primary.

Answer: C

Explanation:
https://community.fortinet.com/t5/FortiManager/Technical-Tip-FortiManager-VRRP-HA-configuration-in- Azure-Public/ta-p/267503 https://community.fortinet.com/t5/FortiManager/Technical-Tip-FortiManager-HA- setup-and-troubleshooting/ta-p/222998

NEW QUESTION # 71
.....

P.S. Free 2026 Fortinet NSE8_812 dumps are available on Google Drive shared by VCE4Plus: https://drive.google.com/open?id=1pOngGRgYZ8H1owO7MJmI8uAqm_D1TAXn