Test Fortinet NSE8_812 Simulator - Valid Exam NSE8_812 Braindumps

DOWNLOAD the newest TestBraindump NSE8_812 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1Yzoh1BmKyV5uOcXUYFUEcssH2NYLWelv

In order to make every customer to get the most suitable method to review NSE8_812 exam, we provide three versions of the NSE8_812 exam materials: PDF, online version, and test software. We believe that there is always a kind of method to best help your exam preparation. Each version has a free demo for you to try, and each version has the latest and most comprehensive NSE8_812 Exam Materials.

The NSE8_812 exam covers a wide range of topics, including advanced networking and security concepts, Fortinet security products and solutions, and best practices for designing and implementing complex security architectures. NSE8_812 exam is designed to test the candidate's ability to analyze complex security challenges, design effective solutions, and implement and manage them in real-world scenarios. Passing the NSE8_812 Exam requires a deep understanding of Fortinet technologies and a thorough understanding of networking and security principles.

>> Test Fortinet NSE8_812 Simulator <<

Valid Exam NSE8_812 Braindumps | NSE8_812 Valid Test Book

We present our Fortinet NSE8_812 real questions in PDF format. It is beneficial for those applicants who are busy in daily routines. The NSE8_812 PDF QUESTIONS contains all the exam questions which will appear in the real test. You can easily get ready for the examination in a short time by just memorizing NSE8_812 Actual Questions.

Fortinet NSE8_812 Exam is a challenging certification exam that tests the competency of network security professionals in designing, implementing, and managing complex security solutions. NSE8_812 exam covers a wide range of topics, including network security design, implementation, and management, cloud security, endpoint security, and threat intelligence. Fortinet NSE 8 - Written Exam (NSE8_812) certification is highly regarded in the network security industry and can help professionals advance their careers, increase their earning potential, and gain recognition for their expertise.

Fortinet NSE 8 - Written Exam (NSE8_812) Sample Questions (Q56-Q61):

NEW QUESTION # 56
An automation stitch was configured using an incoming webhook as the trigger named
'my_incoming_webhook'. The action is configured to execute the CLI Script shown:

```
config firewall address
    edit %%results.hostname%%
        set subnet %%results.ip.1%%/32
    next
end
config firewall addrgrp
    edit Bad-Hosts
        append member %%results.hostname%%
    next
end
```

The base Curl command starts with: curl -k -x POST -H 'Authorization: Bearer ' --data <data> <url> Which Curl command will successfully work with the configured automation stitch?

- A. data: '{ "hostname": "bad_host_1", "ip": "1.1.1.1"}'
  url: http://192.168.226.129/api/v2/monitor/system/automation-stitch/webhook/my_incoming_webhook
- B. data: '{ "hostname": "bad_host_1", "ip": "1.1.1.1"}'
  url: http://192.168.226.129/api/v2/cmdb/system/automation-stitch/webhook/my_incoming_webhook
- C. data: '{ "hostname": "bad_host_1", "ip": ["1.1.1.1"]}'
  url:
  http://192.168.226.129/api/v2/monitor/system/automation-stitch/webhook/my_incoming_webhook
- D. data: '{ "hostname": "bad_host_1", "ip": ["1.1.1.1"]}'
  url:
  http://192.168.226.129/api/v2/cmdb/system/automation-stitch/webhook/my_incoming_webhook

Answer: C

NEW QUESTION # 57
A customer with a FortiDDoS 200F protecting their fibre optic internet connection from incoming traffic sees that all the traffic was dropped by the device even though they were not under a DoS attack. The traffic flow was restored after it was rebooted using the GUI. Which two options will prevent this situation in the future? (Choose two)

- A. Create an HA setup with a second FortiDDoS 200F
- B. Replace with a FortiDDoS 1500F
- C. Move the internet connection from the SFP interfaces to the LC interfaces
- D. Change the Adaptive Mode.

Answer: A,D

Explanation:
To prevent the situation where all the traffic was dropped by the FortiDDoS 200F even though there was no DoS attack, the following options can be considered:
Change the Adaptive Mode. The Adaptive Mode is a feature that allows the FortiDDoS 200F to automatically adjust its detection and prevention thresholds based on the traffic patterns and behavior. However, if the Adaptive Mode is not configured properly, it may cause false positives and drop legitimate traffic. Therefore, changing the Adaptive Mode settings or disabling it may help to avoid this situation.
Create an HA setup with a second FortiDDoS 200F. The HA setup is a feature that allows two FortiDDoS 200F devices to work together as a cluster and provide redundancy and load balancing. If one device fails or drops traffic, the other device can take over and continue to protect the network. Therefore, creating an HA setup with a second FortiDDoS 200F may help to avoid this situation. Reference: https://docs.fortinet.com/document/fortiddos-f/6.2.0/handbook/380639/understanding-fortiddos-adaptive-mode https://docs.fortinet.com/document/fortiddos-f/6.2.0/handbook/380639/configuring-fortiddos-ha

NEW QUESTION # 58
Review the VPN configuration shown in the exhibit.

```
config vpn ipsec fec
  edit "fecprofile"
    config mappings
      edit 1
        set base 8
        set redundant 2
        set packet-loss-threshold 10
      next
      edit 2
        set base 9
        set redundant 3
        set bandwidth-up-threshold 450000
      next
      edit 3
        set base 5
        set redundant 3
        bandwidth-bi-threshold 5000000
      next
    end
  next
end

config vpn ipsec phase1-interface
  edit "vd1-p1"
    set fec-health-check "1"
    set fec-mapping-profile "fecprofile"
    set fec-base 10
    set fec-redundant 1
  next
end
```

What is the Forward Error Correction behavior if the SD-WAN network traffic download is 500 Mbps and has 8% of packet loss in the environment?

- A. 3 redundant packet for every 9 base packets
- B. 3 redundant packet for every 5 base packets
- C. 2 redundant packet for every 8 base packets
- D. 1 redundant packet for every 10 base packets

Answer: B

Explanation:
Forward Error Correction (FEC) is a feature that can improve the quality of SD-WAN network traffic by adding redundant packets to the original packets. The ratio of redundant packets to base packets is determined by the FEC mode, which can be set to low, medium, or high. In low mode, the ratio is 1:10, in medium mode, the ratio is 2:8, and in high mode, the ratio is 3:5. The FEC mode can be configured manually or automatically based on the bandwidth and packet loss of the network. In this case, since the download bandwidth is 500 Mbps and the packet loss is 8%, the FEC mode is automatically set to high, which means that 3 redundant packets are added for every 5 base packets. Reference: https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan/19662/forward-error-correction-fec

NEW QUESTION # 59
You are migrating the branches of a customer to FortiGate devices. They require independent routing tables on the LAN side of the network.
After reviewing the design, you notice the firewall will have many BGP sessions as you have two data centers (DC) and two ISPs per DC while each branch is using at least 10 internal segments.
Based on this scenario, what would you suggest as the more efficient solution, considering that in the future the number of internal segments, DCs or internet links per DC will increase?

- A. Acquire a FortiGate model with more capacity, considering the next 5 years growth.
- B. No change in design is needed as even small FortiGate devices have a large memory capacity.
- C. Redesign the SD-WAN deployment to only use a single VPN tunnel and segment traffic using VRFs on BGP

- D. Implement network-id, neighbor-group and increase the advertisement-interval

Answer: C

Explanation:
Using multiple VPN tunnels and BGP sessions for each internal segment is not scalable and efficient, especially when the number of segments, DCs or internet links per DC increases. A better solution is to use a single VPN tunnel per branch and segment traffic using virtual routing and forwarding (VRF) instances on BGP. This way, each VRF can have its own routing table and BGP session, while sharing the same VPN tunnel. Reference: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/sd-wan-with-vrf-and-bgp

NEW QUESTION # 60
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 network-overlay id
- B. Change advpn2 to IKEv1
- C. Use peer-id
- D. Use local-id

Answer: A

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 # 61
......

Objectives

- pct.edu.pk, hazopsiltraining.com, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, ncon.edu.sa, www.stes.tyc.edu.tw, www.profidemy.com, www.stes.tyc.edu.tw, lms.ait.edu.za, Disposable vapes

What's more, part of that TestBraindump NSE8_812 dumps now are free: https://drive.google.com/open?id=1Yzoh1BmKyV5uOcXUYFUEcssH2NYLWelv