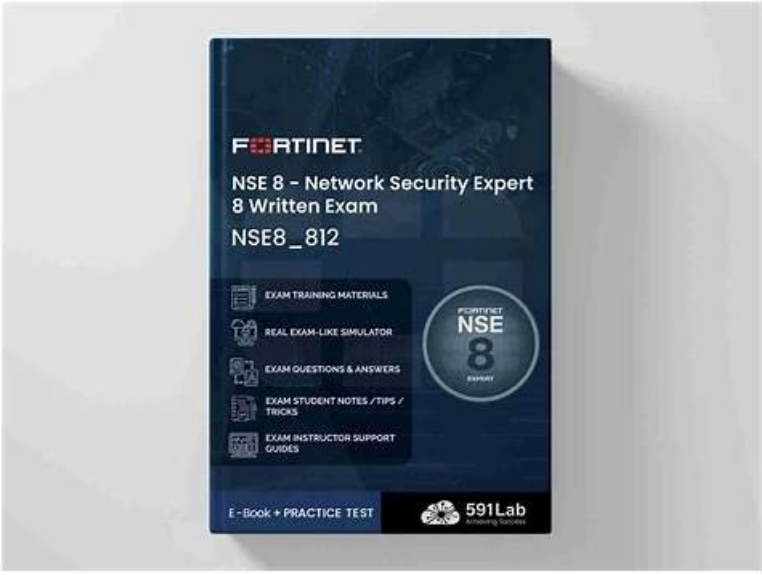
Training NSE8_812 Kit - NSE8_812 Exam Cram Review



P.S. Free 2026 Fortinet NSE8_812 dumps are available on Google Drive shared by Prep4sureGuide: https://drive.google.com/open?id=1dSFIkXJrcjs_UZWj5Z37xBUmWULXtm98

Prep4sureGuide are responsible in every aspect. After your purchase our NSE8_812 practice braindumps, the after sales services are considerate as well. We have considerate after sales services with genial staff. They are willing to solve the problems of our NSE8_812 Exam Questions 24/7 all the time. About the dynamic change of our NSE8_812 study guide, they will send the updates to your mailbox according to the trend of the exam.

Fortinet NSE8_812 exam covers a range of topics, including advanced security technologies, network security design, advanced threat protection, and security management. Candidates are required to demonstrate their knowledge of these topics through a series of multiple-choice questions and scenarios that test their ability to apply their knowledge in real-world situations. Passing NSE8_812 Exam is a testament to an individual's expertise in Fortinet security and can open up numerous career opportunities in the field.

>> Training NSE8_812 Kit <<

NSE8_812 Exam Cram Review - Latest NSE8_812 Training

Inlike other teaching platform, the Fortinet NSE 8 - Written Exam (NSE8_812) study question is outlined the main content of the calendar year examination questions didn't show in front of the user in the form of a long time, but as far as possible with extremely concise prominent text of NSE8_812 test guide is accurate incisive expression of the proposition of this year's forecast trend, and through the simulation of topic design meticulously. With a minimum number of questions and answers of NSE8_812 Test Guide to the most important message, to make every user can easily efficient learning, not to increase their extra burden, finally to let the NSE8_812 exam questions help users quickly to pass the exam.

Fortinet NSE8_812 Certification Exam covers a wide range of topics related to network security, including advanced threat protection, network design and architecture, and security operations and management. NSE8_812 exam also includes questions that test your ability to troubleshoot and optimize Fortinet solutions, as well as your understanding of emerging security trends and best practices. To pass the exam, you'll need to demonstrate a deep understanding of all these topics and be able to apply your knowledge to real-world scenarios.

Fortinet NSE 8 - Written Exam (NSE8_812) Sample Questions (Q42-Q47):

NEW QUESTION # 42
On a FortiGate Configured in Transparent mode, which configuration option allows you to control Multicast traffic passing through the?

A.
```
config system settings
    set multicast-skip-policy disable
end
```

B.
```
config system settings
    set multicast-forward enable
end
```

C.
```
config system settings
    set multicast-forward disable
end
```

D.
```
config system settings
    set multicast-skip-policy enable
end
```

- A. Option C
- B. Option B
- C. Option A
- D. Option D

Answer: C

Explanation:
When multicast-skip-policy is enabled, no check is performed based on multicast policy. A multicast packet received on an interface is flooded unconditionally to all interfaces (except the incoming interface) belonging to the same forwarding domain. Multicast packets are forwarded even when there is no multicast policy or the multicast policy is set to deny. To forward multicast traffic based on multicast policy, multicast-skip-policy must be disabled. In transparent mode, there is a per-VDOM configuration to skip policy check and forward all multicast traffic. This command is only available in transparent mode, and is disabled by default.

NEW QUESTION # 43
You must analyze an event that happened at 20:37 UTC. One log relevant to the event is extracted from FortiGate logs:

```
date=2022-07-11 time=10:37:08 eventtime=1657571829014946018 tz="-1000" logid="0000000022"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.100.91.12 srcport=51542
srcintf="port3" srcintfrole="lan" dstip=8.8.8.8 dstport=53 dstintf="port1" dstintfrole="wan"
srcuuid="2b4ee3fc-0124-51ed-7898-eae1b990b1ec" dstuuid="2b4ee3fc-0124-51ed-7898-eae1b990b1ec"
srccountry="Reserved" dstcountry="United States" sessionid=402530 proto=17 action="accept"
policyid=13 policytype="policy" poluuid="766bb040-0124-51ed-ca3a-eacce4ed289f" policyname="LAN to
Internet" service="DNS" trandisp="snat" transip=10.100.64.101 transport=51542 appid=16195 app="DNS"
appcat="Network.Service" apprisk="elevated" applist="default" duration=180 sentbyte=45 rcvdbyte=120
sentpkt=1 rcvdpkt=1 srchwvendor="Fortinet" devtype="Router" srcfamily="FortiGate" osname="FortiOS"
mastersrcmac="00:09:0f:00:03:01" srcmac="00:09:0f:00:03:01" srcserver=0
```

The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled
* The FortiGate is at GMT-1000.
* The FortiAnalyzer is at GMT-0800
* Your browser local time zone is at GMT-03.00
You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

- A. 20:37:08
- B. 12.37:08
- C. 10:37:08
- D. 17:37:08

Answer: D

Explanation:
To review this log on FortiAnalyzer GUI, the administrator should use the time filter that matches the local time zone of FortiAnalyzer, which is GMT-0800. Since the log was generated at 20:37 UTC (GMT+0000), the corresponding time in GMT-0800 is 20:37 - 8 hours = 12:37. However, since DST is disabled on FortiAnalyzer, the administrator should add one hour to account for daylight saving time difference, resulting in 12:37 + 1 hour = 13:37. Therefore, the time filter to use is 13:37:08.
References: https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/103664/time-zone-and-daylight-saving-time

NEW QUESTION # 44
Refer to the exhibits.
Exhibit A
Exhibit B
Exhibit C
A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration.
Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C
Referring to the exhibits, which configuration will restore VPN connectivity?

- A.
- B.
- C.
- D.

Answer: B

Explanation:
The output in Exhibit A shows that the VPN tunnel is not established because the peer IP address is incorrect.
The output in Exhibit B shows that the peer IP address is 192.168.1.100, but the baseline VPN configuration in Exhibit C shows that the peer IP address should be 192.168.1.101.
To restore VPN connectivity, you need to change the peer IP address in the VPN tunnel configuration to 192.168.1.101. The correct configuration is shown below:
config vpn ipsec phase1-interface
edit "wan"
set peer-ip 192.168.1.101
set peer-id 192.168.1.101
set dhgrp 1
set auth-mode psk
set psk SECRET_PSK
next
end
Option A is incorrect because it does not change the peer IP address. Option B is incorrect because it changes the peer IP address to 192.168.1.100, which is the incorrect IP address. Option D is incorrect because it does not include the necessary configuration for the VPN tunnel.

NEW QUESTION # 45
You must configure an environment with dual-homed servers connected to a pair of FortiSwitch units using an MCLAG.
Multicast traffic is expected in this environment, and you should ensure unnecessary traffic is pruned from links that do not have a multicast listener.
In which two ways must you configure the igmps-flood-traffic and igmps-flood-report settings? (Choose two.)

- A. enable on the ISL and FortiLink trunks
- B. enable on ICL trunks
- C. disable on the ISL and FortiLink trunks
- D. disable on ICL trunks

Answer: A,D

Explanation:
To ensure that unnecessary multicast traffic is pruned from links that do not have a multicast listener, you must disable IGMP flood traffic on the ICL trunks and enable IGMP flood reports on the ISL and FortiLink trunks.

Disabling IGMP flood traffic will prevent the FortiSwitch units from flooding multicast traffic to all ports on the ICL trunks. This will help to reduce unnecessary multicast traffic on the network.
Enabling IGMP flood reports will allow the FortiSwitch units to learn which ports are interested in receiving multicast traffic. This will help the FortiSwitch units to prune multicast traffic from links that do not have a multicast listener.

NEW QUESTION # 46
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 strip the ALPN header and forward the traffic.
- C. FortiGate will rewrite the ALPN header to request HTTP/1.
- D. FortiGate will reject all HTTP/2 ALPN headers.

Answer: B

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl- inspection

NEW QUESTION # 47
.....