

Free PDF 2026 NSE8_812: Fortinet NSE 8 - Written Exam (NSE8_812) Perfect Latest Dumps Ppt

Download the latest PDF of NSE8_812 exam dumps for free at https://www.passcert.com/NSE8_812.html

Exam : NSE8_812

Title : Fortinet NSE 8 - Written Exam (NSE8_812)

https://www.passcert.com/NSE8_812.html

11/16

What's more, part of that GetValidTest NSE8_812 dumps now are free: https://drive.google.com/open?id=1JWO2Kki0udmpkQz5J4NXEyXEiw_cdkFc

In the era of information, everything around us is changing all the time, so do the NSE8_812 exam. But you don't need to worry it. We take our candidates' future into consideration and pay attention to the development of our NSE8_812 study training materials constantly. Free renewal is provided for you for one year after purchase, so the NSE8_812 Latest Questions won't be outdated. The latest NSE8_812 latest questions will be sent to you email, so please check then, and just feel free to contact with us if you have any problem. Our reliable NSE8_812 exam material will help pass the exam smoothly.

Provided you get the certificate this time with our NSE8_812 practice materials, you may have striving and excellent friends and promising colleagues just like you. It is also as obvious magnifications of your major ability of profession, so NSE8_812 practice materials may bring underlying influences with positive effects. The promotion or acceptance will be easy. So it is quite rewarding investment.

>> NSE8_812 Latest Dumps Ppt <<

Reliable NSE8_812 Exam Bootcamp | Exam Dumps NSE8_812 Zip

Fortinet NSE8_812 exams play a significant role to verify skills, experience, and knowledge in a specific technology. Enrollment in

the Fortinet NSE 8 - Written Exam (NSE8_812) NSE8_812 is open to everyone. Upon completion of Fortinet NSE 8 - Written Exam (NSE8_812) NSE8_812 Exam Questions' particular criteria. Participants in the NSE8_812 Dumps come from all over the world and receive the credentials for the Fortinet NSE 8 - Written Exam (NSE8_812) NSE8_812 Questions. They can quickly advance their careers in the fiercely competitive market and benefit from certification after earning the NSE8_812 Questions badge.

Fortinet NSE 8 - Written Exam (NSE8_812) Sample Questions (Q63-Q68):

NEW QUESTION # 63

Refer to The exhibit showing a FortiEDR configuration.



Based on the exhibit, which statement is correct?

- A. The presence of a cryptolocker malware at rest on the filesystem will be detected by the Ransomware Prevention security policy.
- B. FortiEDR Collector will not collect OS Metadata.
- C. If an unresolved file rule is triggered, by default the file is logged but not blocked.
- D. If a malicious file is executed and attempts to establish a connection it will generate duplicate events.

Answer: C

NEW QUESTION # 64

Refer to the exhibits, which show a topology and diagnostic commands.

Exhibit A

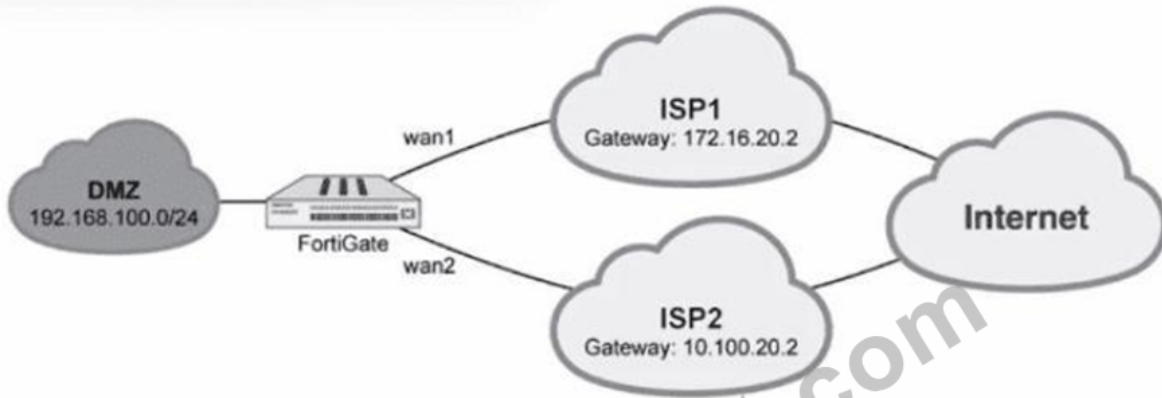


Exhibit B

```
FGT # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency),
link-cost-threshold(20), health-check(Default_Gmail)
Members(2):
  1: Seq_num(1 wan1), alive, latency: 200.177, selected
  2: Seq_num(2 wan2), alive, latency: 167.417, selected
Src address(1):
  192.168.100.0-192.168.100.255

Dst address(1):
  0.0.0.0-255.255.255.255

FGT # diagnose sys sdwan health-check
Health Check(Default_Gmail):
Seq(1 wan1): state(alive), packet-loss(2.000%) latency(200.564), jitter(1.277) sla_map=0x1
Seq(2 wan2): state(alive), packet-loss(0.000%) latency(167.877), jitter(1.060) sla_map=0x1

FGT # diagnose sys sdwan member
Member(1): interface: wan1, priority: 0, weight: 0
Member(2): interface: wan2, priority: 0, weight: 0
```

Which two statements about the path resolution are true? (Choose two.)

- A. wan2 is currently used as an outgoing interface.
- B. wan1 is currently used as an outgoing interface.
- C. Packet-loss is the quality criteria.
- D. Latency is the quality criteria.

Answer: D

NEW QUESTION # 65

Refer to the exhibits.

Exhibit A

```

vd: root/0
name: vpn-hub02-1
version: 2
interface: wan1 7
addr: 10.73.255.67:500 -> 10.73.255.82:500
tun_id: 10.73.255.82/::10.73.255.82
remote_location: 0.0.0.0
created: 82236s ago
peer-id: CN = fgtdc01.example.com
peer-id-auth: yes
Assigned IPv4 address: 192.168.73.67/255.255.255.224
auto-discovery: 2 receiver
PPK: no
IKE SA: created 1/1 established 1/1 time 50/50/50 ms
IPsec SA: created 1/2 established 1/2 time 0/25/50 ms
  id/spi: 1 e4f6465bbae7490f/2535d26ef1f21557
  direction: initiator
  status: established 82236-82236s ago = 50ms
  proposal: aes256-sha256
  child: no
  PPK: no
  message-id sent/rcv: 4/1
  lifetime/rekey: 86400/3863
  DPD sent/rcv: 00000000/00000000
  peer-id: CN = fgtdc01.example.com

```

Exhibit B

```

fgt01-branch01 # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=vpn-hub02-1 ver=2 serial=1 10.73.255.67:0->10.73.255.82:0 tun_id=10.73.255.82
tun_id6=:10.73.255.82 dst_mtu=1500 dpd-link=on weight=1
bound_if=7 lgwy=static/1 tun=tunnel/255 mode=auto/1 encap=none/535 options[0218]=npu create_dev frag
accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=0 olast=0 adr=r/2
stat: rxp=1 txp=1500326 rxb=73 txb=273040631
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vpn-hub02-1 proto=0 sa=1 ref=27 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=3844/0B replaywin=2048
seqno=b1d18 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=42902/43200
dec: spi=4da0c1a4 esp=aes key=32 6495048006963561c4c9b9d91e5e22c454446438480484a81e6bed9f9d3742ef
ah=sha256 key=32 7fb9fce764431ba10b6da88263cd0484d9f5824cc9d5bd268db2cfffca1a1d572
enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b88457e7bf29ee171779b556c83cf
ah=sha256 key=32 9e87bf36eca21c4732cf5af4ccdfe7f1dbc19e7e1afe17fe2a77475f2dd2b0fa
dec:pkts/bytes=0/0, enc:pkts/bytes=1456559/316245764
npu_flag=03 npu_rgwy=10.73.255.82 npu_lgwy=10.73.255.67 npu_selid=0 dec_npuid=1 enc_npuid=1

```

Exhibit C

```

config vpn ipsec phase1-interface
edit "vpn-hub02-1"
  set interface "wan1"
  set net-device enable
  set mode-cfg enable
  set proposal aes256-sha256
  set add-route disable
  set auto-discovery-receiver enable
  set remote-gw 10.73.255.82
next
end

```

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?

```
config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set ike-version 1
    set authmethod signature
    set certificate "BR01FGTLOCAL"
    set peer "vpn-hub02-1_peer"
  next
end
```

- A.

```
config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set ike-version 2
    set authmethod signature
    set npu-offload disable
    set certificate "BR01FGTLOCAL"
    set peer "vpn-hub02-1_peer"
  next
end
```

- B.

```
config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set ike-version 2
    set authmethod signature
    set certificate "BR01FGTLOCAL"
    set peer "vpn-hub02-1_peer"
  next
end
```

- C.

```
config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set ike-version 2
    set net-device enable
    set psksecret fortinet
  next
end
```

- D.

Answer: C

NEW QUESTION # 66

Review the following FortiGate-6000 configuration excerpt:

```

config load balance setting
    set nat-source-port chassis-slots
end

```

Based on the configuration, which statement is correct regarding SNAT source port partitioning behavior?

- A. It is the default SNAT configuration and preserves active sessions when an FPC or FPM goes down.
- **B. It dynamically distributes SNAT source ports to operating FPCs or FPMs.**
- C. It statically distributes SNAT source ports to operating FPCs or FPMs
- D. It equally distributes SNAT source ports across chassis slots.

Answer: B

Explanation:

The configuration excerpt shows that the SNAT source port partitioning behavior is set to dynamic. This means that the FortiGate will dynamically distribute SNAT source ports to operating FPCs or FPMs. This ensures that active sessions are not interrupted if an FPC or FPM goes down.

The other options are incorrect. Option B is incorrect because the default SNAT configuration is static. Option C is incorrect because the configuration excerpt does not specify that SNAT source ports are statically distributed. Option D is incorrect because the SNAT source ports are not evenly distributed across chassis slots.

Here are some additional details about SNAT source port partitioning behavior:

SNAT source port partitioning behavior can be set to dynamic or static.

The default SNAT configuration is static.

Dynamic SNAT source port partitioning ensures that active sessions are not interrupted if an FPC or FPM goes down.

Static SNAT source port partitioning can improve performance by reducing the number of SNAT lookups.

NEW QUESTION # 67

Refer to the exhibits.

Exhibit A

```

vd: root/0
name: vpn-hub02-1
version: 2
interface: wan1 7
addr: 10.73.255.67:500 -> 10.73.255.82:500
tun_id: 10.73.255.82/::10.73.255.82
remote_location: 0.0.0.0
created: 82236s ago
peer-id: CN = fgtdc01.example.com
peer-id-auth: yes
assigned IPv4 address: 192.168.73.67/255.255.255.224
auto-discovery: 2 receiver
PPK: no
IKE SA: created 1/1 established 1/1 time 50/50/50 ms
IPsec SA: created 1/2 established 1/2 time 0/25/50 ms
  id/spi: 1 e4f6465bbae7490f/2535d26ef1f21557
  direction: initiator
  status: established 82236-82236s ago = 50ms
  proposal: aes256-sha256
  child: no
  PPK: no
  message-id sent/rcv: 4/1
  lifetime/rekey: 86400/3863
  DPD sent/rcv: 00000000/00000000
  peer-id: CN = fgtdc01.example.com

```

Exhibit B

```

rft01-branch01 # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=vpn-hub02-1 ver=2 serial=1 10.73.255.67:0->10.73.255.82:0 tun_id=10.73.255.82
tun_id6::10.73.255.82 dst_mtu=1500 dpd-link=on weight=1
bound_if=7 lgwy=static/1 tun=tunnel/255 mode=auto/1 encap=none/536 options[0218]=npu create_dev frag
accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=0 olast=0 adr=r/2
stat: rxp=1 txp=1500326 rxb=73 txb=273040631
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vpn-hub02-1 proto=0 sa=1 ref=27 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=3844/0B replaywin=2048
seqno=b1d18 esn=0 replaywin lastseq=00000000 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=42902/43200
dec: spi=4da0c1a4 esp=aes key=32 6495048006963561c4c9b9d91e5e22c454446438480484a81e6bed9f9d3742ef
ah=sha256 key=32 7fb9fce764431ba10b6da88263cd0484d9f5824cc9d5bd268db2cfffca1ald572
enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b88457e7bf29ee1711779b556c83cf
ah=sha256 key=32 9e87bf36eca21c4732cf5af4ccdfef1d1bc19e7e1afe17fe2a77475f2dd2b0fa
dec:pkts/bytes=0/0, enc:pkts/bytes=1456559/316245764
npu_flag=03 npu_rgwy=10.73.255.82 npu_lgwy=10.73.255.67 npu_selid=0 dec_npuid=1 enc_npuid=1

```

Exhibit C

```

config vpn ipsec phase1-interface
edit "vpn-hub02-1"
set interface "wan1"
set net-device enable
set mode-cfg enable
set proposal aes256-sha256
set add-route disable
set auto-discovery-receiver enable
set remote-gw 10.73.255.82
next
end

```

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?

```

config vpn ipsec phase1-interface
edit "vpn-hub02-1"
set ike-version 2
set net-device enable
set psksecret fortinet
next
end

```

- A.

```

config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set ike-version 1
    set authmethod signature
    set certificate "BR01FGTLOCAL"
    set peer "vpn-hub02-1_peer"
  next
end

```

- B.

```

config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set ike-version 2
    set authmethod signature
    set npu-offload disable
    set certificate "BR01FGTLOCAL"
    set peer "vpn-hub02-1_peer"
  next
end

```

- C.

```

config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set ike-version 2
    set authmethod signature
    set certificate "BR01FGTLOCAL"
    set peer "vpn-hub02-1_peer"
  next
end

```

- D.

Answer: A

Explanation:

The VPN configuration shown in Exhibit C is a baseline VPN configuration that uses IKEv2 with pre-shared keys and AES256 encryption for both IKE and ESP phases. However, this configuration does not match the output shown in Exhibit A and B, which indicate that IKEv1 is used with RSA signatures and AES128 encryption for both IKE and ESP phases. Therefore, to restore VPN connectivity, the configuration needs to be modified to match these parameters. Option B shows the correct configuration that matches these parameters. Option A is incorrect because it still uses IKEv2 instead of IKEv1. Option C is incorrect because it still uses pre-shared keys instead of RSA signatures. Option D is incorrect because it still uses AES256 encryption instead of AES128 encryption. Reference: <https://docs.fortinet.com/document/fortigate/7.0.0/cookbook/19662/ipsec-vpn-with-forticlient>

NEW QUESTION # 68

.....

The Fortinet NSE8_812 questions certificates are the most sought-after qualifications for those looking to further their careers in the

What's more, part of that GetValidTest NSE8_812 dumps now are free: https://drive.google.com/open?id=1JWO2Kki0udmpkQz5J4NXEyXEiw_cdkFc