NSE8_812 Testantworten & NSE8_812 Simulationsfragen

Übrigens, Sie können die vollständige Version der EchteFrage NSE8_812 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1X19SuNXYltb756sii6Pc3wjxu-3BLP-1

Unser EchteFrage ist eine fachliche Website, die Prüfungsmaterialien für zahlreiche Fortinet NSE8_812 Zertifizierungsprüfung bieten. Unser EchteFrage wird vielen IT-Fachleuten zum Berufsaufstieg verhelfen. Die Kraft unserer Eliteteams ist unglaublich. Sie können die Fortinet NSE8_812 Examensübungen-und antworten teilweise als Probe umsonst herunterladen, so dass Sie die Glaubwürdigkeit vom EchteFrage testen können.

Wir sollen im Leben nicht immer etwas von anderen fordern, wir sollen hingegen so denken, was ich für andere tun kann. In der Arbeit können Sie große Gewinne für den Boss bringen, legt der Boss natürlich großen Wert auf Ihre Position sowie Gehalt. Wenn wir ein kleiner Angestellte sind, werden wir sicher eines Tages ausrangiert. Wir sollen uns bemühen, die Fortinet NSE8_812 Zertifizierung zu bekommen und Schritt für Schritt nach oben gehen. Die Fragen und Antworten zur Fortinet NSE8_812 Zertifizierungsprüfung von EchteFrage helfen Ihnen, den Erfolg durch eine Abkürzung zu erlangen. Viele IT-Fachleute haben die Fragenkataloge zur Fortinet NSE8_812 Prüfung von EchteFrage gekauft.

>> NSE8_812 Testantworten <<

NSE8_812 Simulationsfragen - NSE8_812 Fragen Beantworten

Es ist unnötig für Sie, zu viel Zeit eine Prüfung vorzubereiten. Kaufen Sie bitte Fortinet NSE8_812 Dumps von EchteFrage. Mit diesen Dumps können Sie wissen, wie Fortinet NSE8_812 Prüfung hocheffektiv vorzubereiten. Das ist ein seltenes Gerät, das Ihnen helfen, sehr einfach die Fortinet NSE8_812 Prüfung zu bestehen. Sie werden bereuen, dass Sie diese Chance verlieren. So handeln Sie bitte schnell damit.

Die Fortinet NSE8_812 Prüfung ist eine Zertifizierungsprüfung, die die Kompetenz von Netzwerksicherheitsfachleuten in der Gestaltung, Implementierung und Verwaltung komplexer Sicherheitslösungen testet. Die Prüfung ist für Personen konzipiert, die ein tiefes Verständnis von Netzwerksicherheit haben und Erfahrung mit Fortinet-Produkten und -Lösungen haben. Die Prüfung soll ihre Expertise bei der Absicherung der Netzwerkinfrastruktur gegen fortschrittliche Cyberbedrohungen und Angriffe validieren.

Fortinet NSE 8 - Written Exam (NSE8_812) NSE8_812 Prüfungsfragen mit Lösungen (Q88-Q93):

88. Frage
A customer wants to use the FortiAuthenticator REST API to retrieve an SSO group called SalesGroup. The following API call is being made with the 'curl' utility:

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -X PUT -d '{"name":"SalesGroup"}' -H
'Content-Type: application/json' https://10.10.10.22/api/v1/ssogroup/100/
```

Which two statements correctly describe the expected behavior of the FortiAuthenticator REST API? (Choose two.)

- A. If the REST API web service access key is lost, it cannot be retrieved and must be changed.
- B. The syntax is incorrect because the API calls needs the get method.
- C. Only users with the "Full permission" role can access the REST API
- D. This API call will fail because it requires that API version 2

Antwort: B,D

Begründung:
To retrieve an SSO group called SalesGroup using the FortiAuthenticator REST API, the following issues need to be fixed in the API call:
The API version should be v2, not v1, as SSO groups are only supported in version 2 of the REST API.
The HTTP method should be GET, not POST, as GET is used to retrieve information from the server, while POST is used to create or update information on the server. Therefore, a correct API call would look like this: curl -X GET -H "Authorization: Bearer <token>" https://fac.example.com/api/v2/sso/groups/SalesGroup References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api-solution-guide/927310/introduction
https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api-solution-guide/927311/sso-groups

89. Frage
Which two types of interface have built-in active bypass in FortiDDoS devices? (Choose two.)

- A. LC
- B. Copper
- C. SFP+
- D. QSFP+
- E. SFP

Antwort: A,B

Begründung:
https://help.fortinet.com/fddos/4-3-0/FortiDDoS/Built_in_bypass.htm

90. Frage
Refer to the exhibits.
Exhibit A

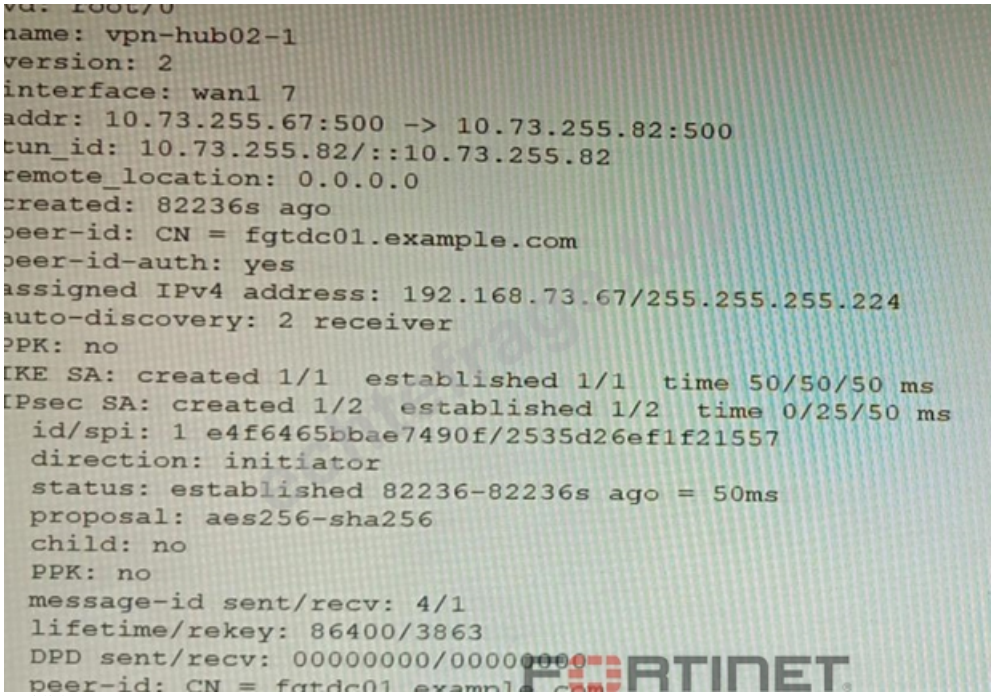


Exhibit B

```
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 ad=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 7fb9fce764431ba10b6da88263cd0484d9f5824cc9d5bd268db2cffca1a1d572
  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?

- 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
```

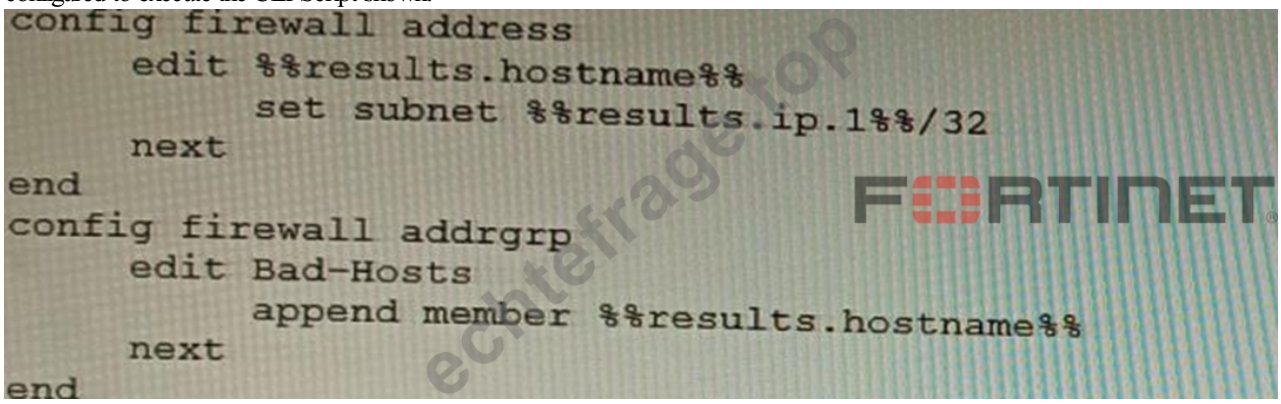
- B.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set npu-offload disable
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```
- C.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set net-device enable
        set psksecret fortinet
    next
end
```
- D.
```
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
```

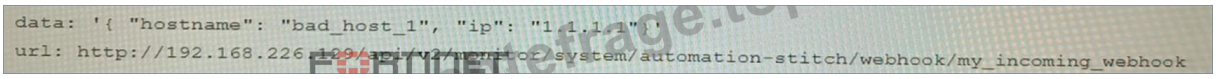
Antwort: B

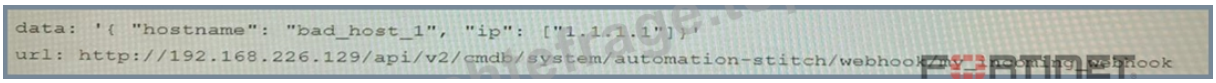
Begründung:
The output in Exhibit A shows that the VPN tunnel is not established because the peer IP address is incorrect. The output in Exhibit B shows that the peer IP address is 192.168.1.100, but the baseline VPN configuration in Exhibit C shows that the peer IP address should be 192.168.1.101.
To 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.

91. Frage
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:



- A.


- B.


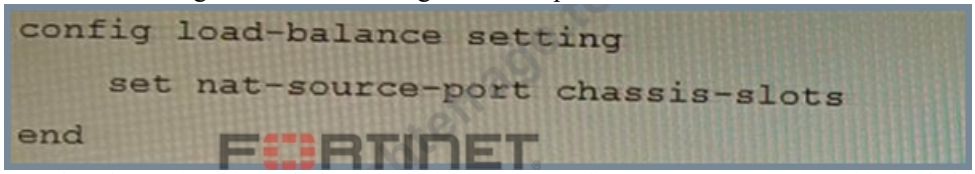
- C.


- D.


Antwort: C

Begründung:
The CLI script in option A will send the log message to the webhook server. The webhook server can then be configured to take any desired action, such as storing the log message in a database or sending an email notification.
The other options are incorrect. Option B will not send the log message to the webhook server because it does not contain the curl command. Option C will send the log message to the webhook server, but it will also include the FortiGate's IP address and MAC address. This information is not necessary, and it could be used by an attacker to identify the FortiGate. Option D will not send the log message to the webhook server because it does not contain the webhook action.
References:
Automation webhook stitches: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/989735/webhook-action
Webhooks: https://en.wikipedia.org/wiki/Webhook

92. Frage
Review the following FortiGate-6000 configuration excerpt:



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

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

Antwort: C

Begründung:
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.

93. Frage
.....

Disposable vapes

BONUS!!! Laden Sie die vollständige Version der EchteFrage NSE8_812 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1X19SuNXYltb756sii6Pc3wjxu-3BLP-1