

Exam Questions NSE7_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2

https://www.2passeasy.com/dumps/NSE7_SDW-7.2/



NEW QUESTION 1

Refer to the exhibits.

Exhibit A

```
branch1_fgt (3) # show
config service
  edit 3
    set name "Corp"
    set mode sla
    set dst "Corp-net"
    set src "LAN-net"
    config sla
      edit "VPN_PING"
        set id 1
      next
      edit "VPN_HTTP"
        set id 1
      next
    end
    set priority-members 3 4 5
    set gateway enable
  next
end
```

Exhibit B -

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
Members(2):
  1: Seq_num(5 T_MPLS_0), alive, sla(0x3), gid(0), cfg_order(2), cost(0), selected
  2: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  3: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), cost(0), selected
Src address(1):
  10.0.1.0-10.0.1.255

Dst address(1):
  10.0.0.0-10.255.255.255

branch1_fgt # get router info routing-table all | grep T_
S      10.0.0.0/8 [1/0] via T_INET_0_0 tunnel 100.64.1.1
      [1/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.201.1.254/32 [15/0] via T_INET_0_0 tunnel 100.64.1.1
S      10.202.1.254/32 [15/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.203.1.254/32 [15/0] via T_MPLS_0 tunnel 172.16.1.5

branch1_fgt # diagnose sys sdwan member | grep T_
Member(3): interface: T_INET_0_0, flags=0x4, gateway: 100.64.1.1, peer: 10.201.1.254,
priority: 0 1024, weight: 0
Member(4): interface: T_INET_1_0, flags=0x4, gateway: 100.64.1.9, peer: 10.202.1.254,
priority: 0 1024, weight: 0
Member(5): interface: T_MPLS_0, flags=0x4, gateway: 172.16.1.5, peer: 10.203.1.254,
priority: 0 1024, weight: 0
```

Exhibit A shows the configuration for an SD-WAN rule and exhibit B shows the respective rule status, the routing table, and the member status.

The administrator wants to understand the expected behavior for traffic matching the SD- WAN rule.

Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

- A. The traffic will be load balanced across all three overlays.
- B. The traffic will be routed over T_INET_0_0.
- C. The traffic will be routed over T_MPLS_0.
- D. The traffic will be routed over T_INET_1_0.

Answer: C

NEW QUESTION 2

Refer to the exhibit.

```
# get router info routing-table all
...
B      10.0.2.0/24 [200/0] via 10.201.1.2 [3] (recursive via VPN0 tunnel 100.64.1.1), 00:00:54
      [200/0] via 10.202.1.2 [3] (recursive via VPN1 tunnel 100.64.1.9), 00:00:54
      [200/0] via 10.203.1.1 [3] (recursive via VPN2 tunnel 172.16.1.5), 00:00:54
...
```

The device exchanges routes using IBGP.

Which two statements are correct about the IBGP configuration and routing information on the device? (Choose two.)

- A. Each BGP route is three hops away from the destination.
- B. ibgp-multipath is disabled.
- C. additional-path is enabled.
- D. You can run the get router info routing-table database command to display the additional paths.

Answer: CD

NEW QUESTION 3

What is a benefit of using application steering in SD-WAN?

- A. The traffic always skips the regular policy routes.
- B. You steer traffic based on the detected application.
- C. You do not need to enable SSL inspection.

D. You do not need to configure firewall policies that accept the SD-WAN traffic.

Answer: B

NEW QUESTION 4

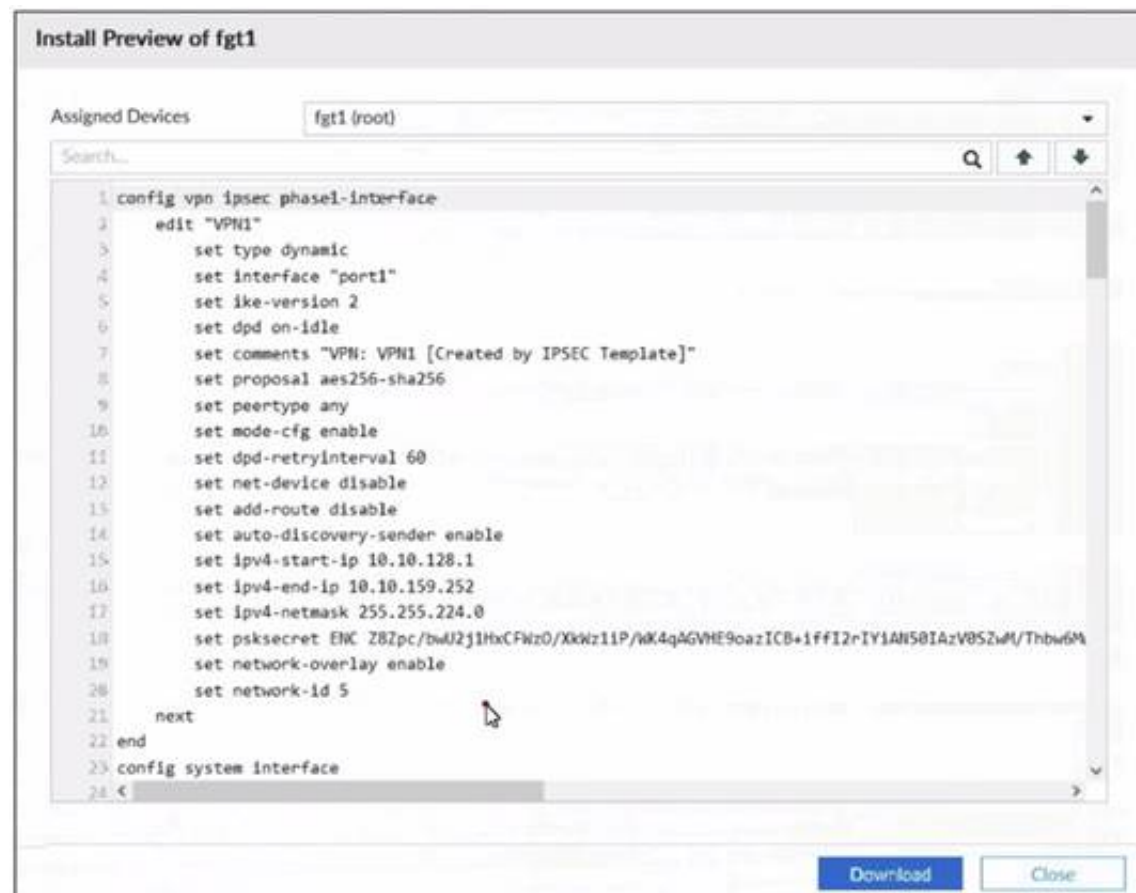
Which are two benefits of using CLI templates in FortiManager? (Choose two.)

- A. You can reference meta fields.
- B. You can configure interfaces as SD-WAN members without having to remove references first.
- C. You can configure FortiManager to sync local configuration changes made on the managed device, to the CLI template.
- D. You can configure advanced CLI settings.

Answer: AD

NEW QUESTION 5

Refer to the exhibit.



An administrator used the SD-WAN overlay template to prepare an IPsec configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the installation preview for one FortiGate device. In the exhibit, which statement best describes the configuration applied to the FortiGate device?

- A. It is a hub device
- B. It can send ADVPN shortcut offers.
- C. It is a spoke device that establishes dynamic IPsec tunnels to the hu
- D. The subnet range is 10.10.128.0/23.
- E. It is a spoke device that establishes dynamic IPsec tunnels to the hu
- F. It can send ADVPN shortcut requests.
- G. It is a hub device and will automatically discover the spoke devices that are in the SD- WAN topology.

Answer: C

Explanation:

According to the SD-WAN 7.2 Study Guide, the SD-WAN overlay template simplifies the configuration of IPsec tunnels in a hub-and-spoke topology. The template defines the following parameters:

- ? type: dynamic for spokes, static for hubs
 - ? interface: the WAN interface to use for the IPsec tunnel
 - ? network-overlay: enable for spokes, disable for hubs
 - ? network-id: a unique identifier for each spoke
 - ? auto-discovery-sender: enable for hubs, disable for spokes
 - ? auto-discovery-receiver: enable for spokes, disable for hubs
- Based on the exhibit, the FortiGate device has the following configuration:
- ? type: dynamic
 - ? interface: port1
 - ? network-overlay: enable
 - ? network-id: 5
 - ? auto-discovery-sender: disable
 - ? auto-discovery-receiver: enable

Therefore, the FortiGate device is a spoke that establishes dynamic IPsec tunnels to the hub. It also has the network-overlay and auto-discovery-receiver options enabled, which means it can send ADVPN shortcut requests to other spokes when it receives a shortcut offer from the hub

NEW QUESTION 6

Which three matching traffic criteria are available in SD-WAN rules? (Choose three.)

- A. Type of physical link connection
- B. Internet service database (ISDB) address object
- C. Source and destination IP address
- D. URL categories

E. Application signatures

Answer: BCE

NEW QUESTION 7

Which two settings can you configure to speed up routing convergence in BGP? (Choose two.)

- A. update-source
- B. set-route-tag
- C. holdtime-timer
- D. link-down-failover

Answer: CD

NEW QUESTION 8

Which diagnostic command can you use to show the member utilization statistics measured by performance SLAs for the last 10 minutes?

- A. diagnose sys sdwan sla-log
- B. diagnose ays sdwan health-check
- C. diagnose sys sdwan intf-sla-log
- D. diagnose sys sdwan log

Answer: A

NEW QUESTION 9

Refer to the exhibit.

Exhibit A

```
fgt # show vpn ipsec phase1-interface T_INET_1
config vpn ipsec phase1-interface
edit "T_INET_1"
set type dynamic
set interface "port2"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256
set add-route disable
set auto-discovery-sender enable
set paksecret ENC MXtFGKOxLV+x4p3e9Xq2HGJoU+QOgg5YMqiXb2T73f2pSX5/
jv9oshWeQ1NEjOJEtuqqD8mAw7G22LTlsR3/ihAaAY4tvjveS+9CuTn00J2tuddoM9
uz4vaBTNbNrh3/KhbJytsCag==
next
end
```

Exhibit B

```
fgt # diag vpn tunnel list name T_INET_1_0
list ipsec tunnel by names in vd 0
-----
name=T_INET_1_0 ver=2 serial=a 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 tun_id6=:10.0.0.10
dst_mtu=0 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74408 options[122a8]=npu rgwy-chg
frag-rfc run_state=0 role=primary acc
ept_traffic=1 overlay_id=0
parent=T_INET_1 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=0 clast=42955943 ad=/0
stat: rxp=32 txp=0 rxh=1280 txh=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=T_INET_1_0 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255.0
dst: 0:10.0.1.0-10.0.1.255:0
SA: ref=3 options=20603 type=00 soft=0 mtu=1280 expire=1774/08 replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000021 qat=0 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1791/1800
dec: spi=7c176e24 esp=aes key=16 8547efb42d148c6692fb2af0d01ff12d
ah=shal key=20 f0d3ac8192d2e79fbbe29162f9ccf406flal6lb5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6alf9fe5ab38b953dd4782f
ah=shal key=20 d0182dfe827a4785d9493d46e3907d49465391fb
dec:pkts/bytes=64/2560, enc:pkts/bytes=0/0
npu_flag=00 npu_rgwy=192.2.0.9 npu_lgwy=100.64.1.9 npu_selid=6 dec_npuid=0 enc_npuid=0
```

Which two statements about the IPsec VPN configuration and the status of the IPsec VPN tunnel are true? (Choose two.)

- A. FortiGate does not install IPsec static routes for remote protected networks in the routing table
- B. Most Voted
- C. The phase 1 configuration supports the network-overlay setting
- D. Most Voted
- E. FortiGate facilitated the negotiation of the T_INET_1_0_0 ADVPN shortcut over T_INET_1_0.
- F. Dead peer detection is disabled.

Answer: AC

NEW QUESTION 10

Refer to the exhibit.

```
config system settings
set firewall-session-dirty check-new
end
```


Based on the exhibit, which two actions does FortiGate perform on sessions after a firewall policy change? (Choose two.)

- A. FortiGate flushes all sessions.
- B. FortiGate terminates the old sessions.
- C. FortiGate does not change existing sessions.
- D. FortiGate evaluates new sessions.

Answer: CD

Explanation:

FortiGate not to flag existing impacted session as dirty by setting firewall-session-dirty to check new. The results is that FortiGate evaluates only new session against the new firewall policy.

NEW QUESTION 10

Exhibit A –

#	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access
Physical (10)						
1	port1	Physical	port1	Manual	203.0.113.1/255.255.255.2	PING
2	port2	Physical	port2	Manual	203.0.113.9/255.255.255.2	PING
3	port3	Physical	port3	Manual	0.0.0.0/0.0.0.0	
4	port4	Physical	port4	Manual	172.16.0.9/255.255.255.24	PING
5	port5	Physical	port5	Manual	10.0.2.254/255.255.255.0	PING
6	port6	Physical	port6	Manual	0.0.0.0/0.0.0.0	
7	port7	Physical	port7	Manual	0.0.0.0/0.0.0.0	
8	port8	Physical	port8	Manual	0.0.0.0/0.0.0.0	
9	port9	Physical	port9	Manual	0.0.0.0/0.0.0.0	
10	port10	Physical	port10	Manual	192.168.0.32/255.255.255.	HTTPS, PING, SSH, HT
Aggregate (1)						
11	fortilink	Aggregate		Manual	169.254.1.1/255.255.255.0	PING, Security Fabric C
Tunnel (3)						
12	nat.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
13	l2t.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
14	ssl.root (SSL VPN interf	Tunnel		Manual	0.0.0.0/0.0.0.0	
EMAC VLAN (1)						
15	vt_lan_ts	EMAC VLAN		Manual	10.0.102.1/255.255.255.0	PING
SD-WAN Zone (2)						
16	virtual-wan link	SD-WAN Zone				
17	SASE	SD-WAN Zone				

#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
Static Route (2)								
1	1	0.0.0.0/0.0.0.0	203.0.113.2	port1	10	0	Enable	
2	2	0.0.0.0/0.0.0.0	203.0.113.10	port2	10	0	Enable	

Exhibit B –

#	Name	From	To	Source	Destination	Schedule	Service
1	Internet_Access	port5	port1	all	all	always	ALL
Implicit (2-2 / Total: 1)							
2	Implicit Deny	any	any	all	all	always	ALL

Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate.

Based on the FortiGate configuration shown in the exhibits, what issue might you encounter when creating an SD-WAN zone for port1 and port2?

- A. port1 is assigned a manual IP address.
- B. port1 is referenced in a firewall policy.
- C. port2 is referenced in a static route.
- D. port1 and port2 are not administratively down.

Answer: B

NEW QUESTION 11

Which SD-WAN setting enables FortiGate to delay the recovery of ADVPN shortcuts?

- A. hold-down-time
- B. link-down-failover
- C. auto-discovery-shortcuts
- D. idle-timeout

Answer: A

NEW QUESTION 15

Exhibit.

```
7: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.9 locip=192.2.0.9
rempart=500 locport=500 outintf="port2" cookies="773c72b48060051d/529ac435532959b6" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.202.1.1
vpntunnel="T_INET_1" tunnelip=N/A tunnelid=2595348112 tunneltype="ipsec" duration=3581
sentbyte=386431 rcvdbyte=387326 nextstat=600 advpnsc=0

9: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.0.9 locip=172.16.0.1
rempart=500 locport=500 outintf="port4" cookies="0624890597f0096d/ed1bd5247375c46f" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="T_MPLS_0"
tunnelip=0.0.0.0 tunnelid=2595348102 tunneltype="ipsec" duration=223 sentbyte=115040
rcvdbyte=345160 nextstat=600 advpnsc=1

9: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.1 locip=192.2.0.1
rempart=500 locport=500 outintf="port1" cookies="747b432459497188/6616a969a6937853" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.201.1.1
vpntunnel="T_INET_0" tunnelip=N/A tunnelid=2595348115 tunneltype="ipsec" duration=3580
sentbyte=388020 rcvdbyte=387994 nextstat=600 advpnsc=0
```

The exhibit shows VPN event logs on FortiGate. In the output shown in the exhibit, which statement is true?

- A. There are no IPsec tunnel statistics log messages for ADVPN cuts.
- B. There is one shortcut tunnel built from master tunnel T_MPLS_0.
- C. The VPN tunnel T_MPLS_0 is a shortcut tunnel.
- D. The master tunnel T_INET_0 cannot accept the ADVPN shortcut.

Answer: B

Explanation:

VPN event logs record the status of VPN tunnels, such as the establishment, termination, or failure of a tunnel. The output includes the following information:

- ? logid: the log ID number
 - ? type: the log type, either traffic or event
 - ? subtype: the log subtype, either vpn or ipsec
 - ? level: the log level, either error, warning, or notice
 - ? vd: the virtual domain name
 - ? logdesc: the log description
 - ? msg: the log message
 - ? action: the log action, such as tunnel-up, tunnel-down, or tunnel-stats
 - ? remip: the remote IP address
 - ? locip: the local IP address
 - ? remport: the remote port number
 - ? locport: the local port number
 - ? outintf: the outgoing interface name
 - ? cookies: the IKE SA cookies
 - ? user: the user name
 - ? group: the user group name
 - ? useralt: the alternative user name
 - ? xauthuser: the XAuth user name
 - ? authgroup: the XAuth user group name
 - ? assignip: the assigned IP address
 - ? vpntunnel: the VPN tunnel name
 - ? tunnelip: the tunnel loopback IP address
 - ? tunnelid: the tunnel ID number
 - ? tunneltype: the tunnel type, either ipsec or ssl
 - ? duration: the tunnel duration in seconds
 - ? sentbyte: the number of bytes sent
 - ? rcvdbyte: the number of bytes received
 - ? nextstat: the next statistics interval in seconds
 - ? advpnsc: the ADVPN shortcut flag, either 0 or 1
- Based on the exhibit, the following statement is true:

? There is one shortcut tunnel built from master tunnel T_MPLS_0. This means that the VPN tunnel T_MPLS_0 is a master tunnel that can send ADVPN shortcut offers to other spokes, and the VPN tunnel T_MPLS_0_0 is a shortcut tunnel that is built from the master tunnel T_MPLS_01. In the exhibit, the log action for T_MPLS_0 is tunnel-up, and the log action for T_MPLS_0_0 is shortcut-up. The advpnsc flag for T_MPLS_0 is 0, indicating that it is not a shortcut tunnel, while the advpnsc flag for T_MPLS_0_0 is 1, indicating that it is a shortcut tunnel.

NEW QUESTION 20

Which components make up the secure SD-WAN solution?

- A. Application, antivirus, and URL, and SSL inspection
- B. Datacenter, branch offices, and public cloud
- C. FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy
- D. Telephone, ISDN, and telecom network.

Answer: C

NEW QUESTION 22

What are two benefits of using the Internet service database (ISDB) in an SD-WAN rule? (Choose two.)

- A. The ISDB is dynamically updated and reduces administrative overhead.
- B. The ISDB requires application control to maintain signatures and perform load balancing.
- C. The ISDB applies rules to traffic from specific sources, based on application type.
- D. The ISDB contains the IP addresses and port ranges of well-known internet services.

Answer: AD

NEW QUESTION 25

Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

- A. Encapsulating Security Payload (ESP)
- B. Secure Shell (SSH)
- C. Internet Key Exchange (IKE)
- D. Security Association (SA)

Answer: AC

NEW QUESTION 29

In the default SD-WAN minimum configuration, which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two)

- A. Traffic has matched none of the FortiGate policy routes.
- B. Matched traffic failed RPF and was caught by the rule.
- C. The FIB lookup resolved interface was the SD-WAN interface.
- D. An absolute SD-WAN rule was defined and matched traffic.

Answer: AC

NEW QUESTION 33

Refer to the exhibit.

```
config system sdwan
  set fail-detect enable
  set fail-alert-interfaces "port5"
  config health-check
    edit "Level3_DNS"
      set update-cascade-interface enable
      set members 1 2
    next
    edit "HQ"
      set update-cascade-interface enable
      set members 3
    next
  end
end
```

Based on the exhibit, which action does FortiGate take?

- A. FortiGate bounces port5 after it detects all SD-WAN members as dead.
- B. FortiGate fails over to the secondary device after it detects all SD-WAN members as dead.
- C. FortiGate brings up port5 after it detects all SD-WAN members as alive.
- D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

Answer: A

NEW QUESTION 38

Which CLI command do you use to perform real-time troubleshooting for ADVPN negotiation?

- A. get router info routing-table all
- B. diagnose debug application ike
- C. diagnose vpn tunnel list
- D. get ipsec tunnel list

Answer: B

Explanation:

IKE real-time debug - useful when debugging ADVPN shortcut messages and spoke-to-spoke negotiations.

- diagnose debug console timestamp enable
- diagnose vpn ike log filter clear
- diagnose vpn ike log filter mdst-addr4 <ip.of.hub> <ip.of.spoke>
- diagnose debug application ike -1
- diagnose debug enable

NEW QUESTION 42

Refer to the exhibit.


```
config vpn ipsec phase1-interface
edit "FIRST_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes128-sha256 aes256-sha38
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "first-group"
    set psksecret fortinet1
next
edit "SECOND_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes128-sha256 aes256-sha38
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "second-group"
    set psksecret fortinet2
next
edit
```

FortiGate has multiple dial-up VPN interfaces incoming on port1 that match only FIRST_VPN.

Which two configuration changes must be made to both IPsec VPN interfaces to allow incoming connections to match all possible IPsec dial-up interfaces? (Choose two.)

- A. Specify a unique peer ID for each dial-up VPN interface.
- B. Use different proposals are used between the interfaces.
- C. Configure the IKE mode to be aggressive mode.
- D. Use unique Diffie Hellman groups on each VPN interface.

Answer: AC

NEW QUESTION 47

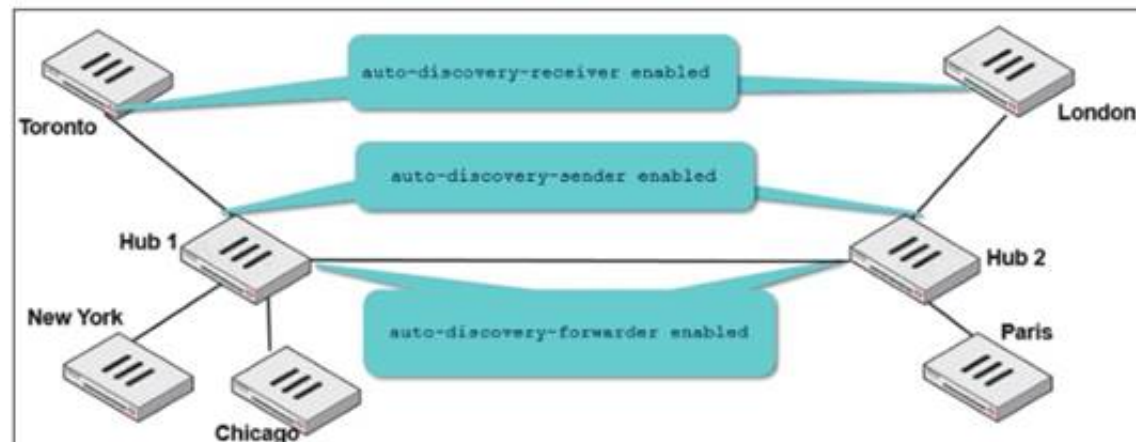
Which two interfaces are considered overlay links? (Choose two.)

- A. LAG
- B. IPsec
- C. Physical
- D. GRE

Answer: BD

NEW QUESTION 52

Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. The administrator configured ADVPN on both hub-and-spoke groups.\



Which two outcomes are expected if a user in Toronto sends traffic to London? (Choose two.)

- A. London generates an IKE information message that contains the Toronto public IP address.
- B. Traffic from Toronto to London triggers the dynamic negotiation of a direct site-to-site VPN.
- C. Toronto needs to establish a site-to-site tunnel with Hub 2 to bypass Hub 1.
- D. The first packets from Toronto to London are routed through Hub 1 then to Hub 2.

Answer: BD

NEW QUESTION 53

Refer to the exhibit.

```
# diagnose firewall shaper per-ip-shaper list
name FTP_5M
maximum-bandwidth 625 KB/sec
maximum-concurrent-session 5
tos ff/ff
packets dropped 65
bytes dropped 81040
    addr=10.1.0.1 status: bps=0 ses=1
    addr=10.1.0.100 status: bps=0 ses=1
    addr=10.1.10.1 status: bps=1656 ses=3
```

Which are two expected behaviors of the traffic that matches the traffic shaper? (Choose two.)

- A. The number of simultaneous connections among all source IP addresses cannot exceed five connections.
- B. The traffic shaper limits the combined bandwidth of all connections to a maximum of 5 MB/sec.
- C. The number of simultaneous connections allowed for each source IP address cannot exceed five connections.
- D. The traffic shaper limits the bandwidth of each source IP address to a maximum of 625 KB/sec.

Answer: CD

NEW QUESTION 54

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_SDW-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_SDW-7.2 Product From:

https://www.2passeasy.com/dumps/NSE7_SDW-7.2/

Money Back Guarantee

NSE7_SDW-7.2 Practice Exam Features:

- * NSE7_SDW-7.2 Questions and Answers Updated Frequently
- * NSE7_SDW-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_SDW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year