NSE7_SDW-6.4 Q&As

Fortinet NSE 7 - SD-WAN 6.4

Pass Fortinet NSE7_SDW-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

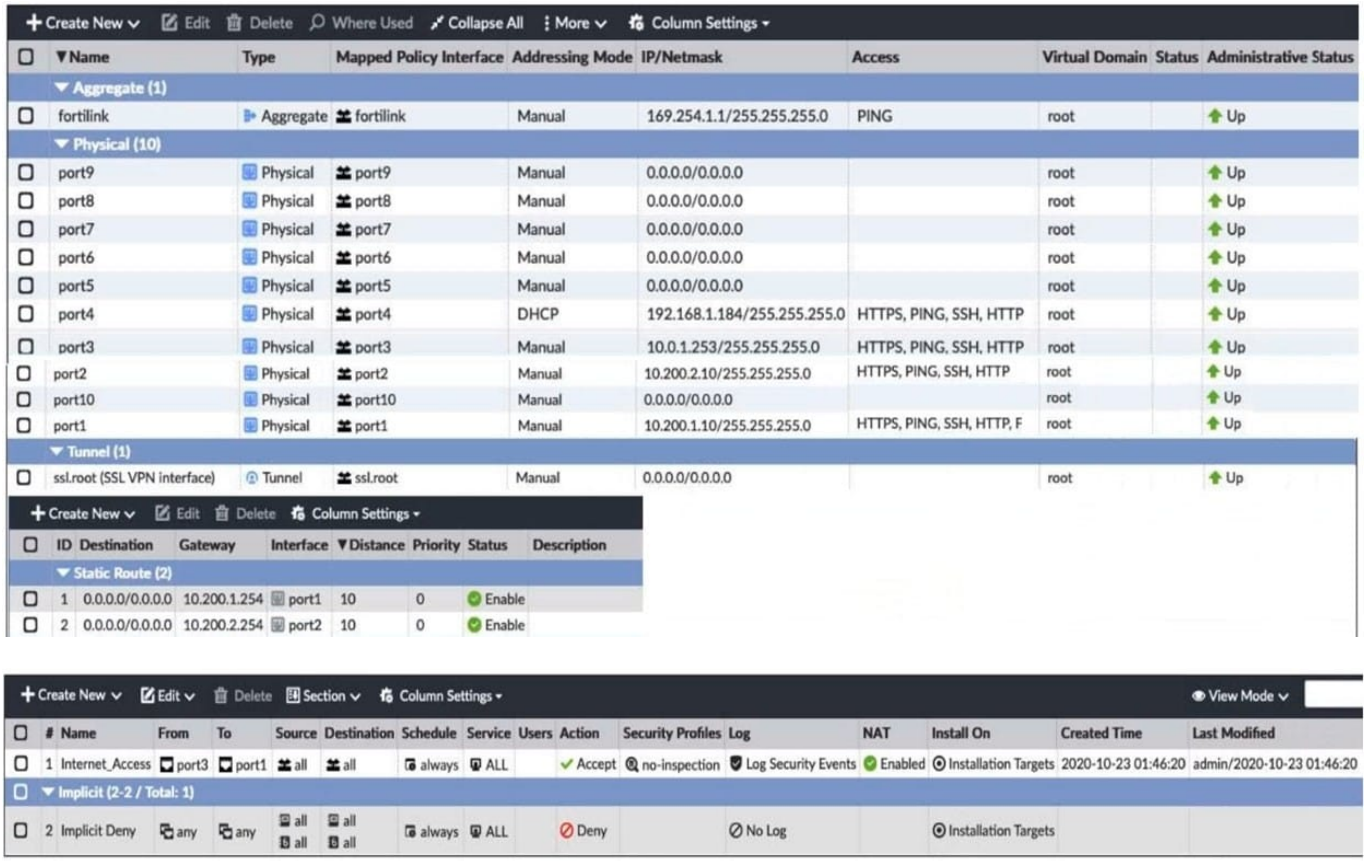
https://www.leads4pass.com/nse7_sdw-6-4.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibits.



Create New | Edit | Delete | Where Used | Collapse All | More | Column Settings

Name	Type	Mapped Policy Interface	Addressing Mode	IP/Netmask	Access	Virtual Domain	Status	Administrative Status
Aggregate (1)								
fortilink	Aggregate	fortilink	Manual	169.254.1.1/255.255.255.0	PING	root		Up
Physical (10)								
port9	Physical	port9	Manual	0.0.0.0/0.0.0.0		root		Up
port8	Physical	port8	Manual	0.0.0.0/0.0.0.0		root		Up
port7	Physical	port7	Manual	0.0.0.0/0.0.0.0		root		Up
port6	Physical	port6	Manual	0.0.0.0/0.0.0.0		root		Up
port5	Physical	port5	Manual	0.0.0.0/0.0.0.0		root		Up
port4	Physical	port4	DHCP	192.168.1.184/255.255.255.0	HTTPS, PING, SSH, HTTP	root		Up
port3	Physical	port3	Manual	10.0.1.253/255.255.255.0	HTTPS, PING, SSH, HTTP	root		Up
port2	Physical	port2	Manual	10.200.2.10/255.255.255.0	HTTPS, PING, SSH, HTTP	root		Up
port10	Physical	port10	Manual	0.0.0.0/0.0.0.0		root		Up
port1	Physical	port1	Manual	10.200.1.10/255.255.255.0	HTTPS, PING, SSH, HTTP, F	root		Up
Tunnel (1)								
ssl.root (SSL VPN interface)	Tunnel	ssl.root	Manual	0.0.0.0/0.0.0.0		root		Up

Create New | Edit | Delete | Column Settings

ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
Static Route (2)							
1	0.0.0.0/0.0.0.0	10.200.1.254	port1	10	0	Enable	
2	0.0.0.0/0.0.0.0	10.200.2.254	port2	10	0	Enable	

Create New | Edit | Delete | Section | Column Settings | View Mode

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log	NAT	Install On	Created Time	Last Modified
1	Internet_Access	port3	port1	all	all	always	ALL		Accept	no-inspection	Log Security Events	Enabled	Installation Targets	2020-10-23 01:46:20	admin/2020-10-23 01:46:20
Implicit (2-2 / Total: 1)															
2	Implicit Deny	any	any	all all	all all	always	ALL		Deny		No Log		Installation Targets		

ExhibitA 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. port2 is referenced in a static route.

B. port1 is assigned a manual IP address.

C. port1 and port2 are not administratively down.

D. port1 is referenced in a firewall policy.

Correct Answer: D

QUESTION 2

Which statement reflects how BGP tags work with SD-WAN rules?

A. BGP tags match the SD-WAN rule based on the order that these rules were installed.

B. BGP tags require that the adding of static routes be enabled on all ADVPN interfaces

C. Route tags are used for a BGP community and the SD-WAN rules are assigned the same tag

D. VPN topologies are formed using only BGP dynamic routing with SD-WAN

Correct Answer: C

QUESTION 3

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.

Correct Answer: C

QUESTION 4

Refer to exhibits

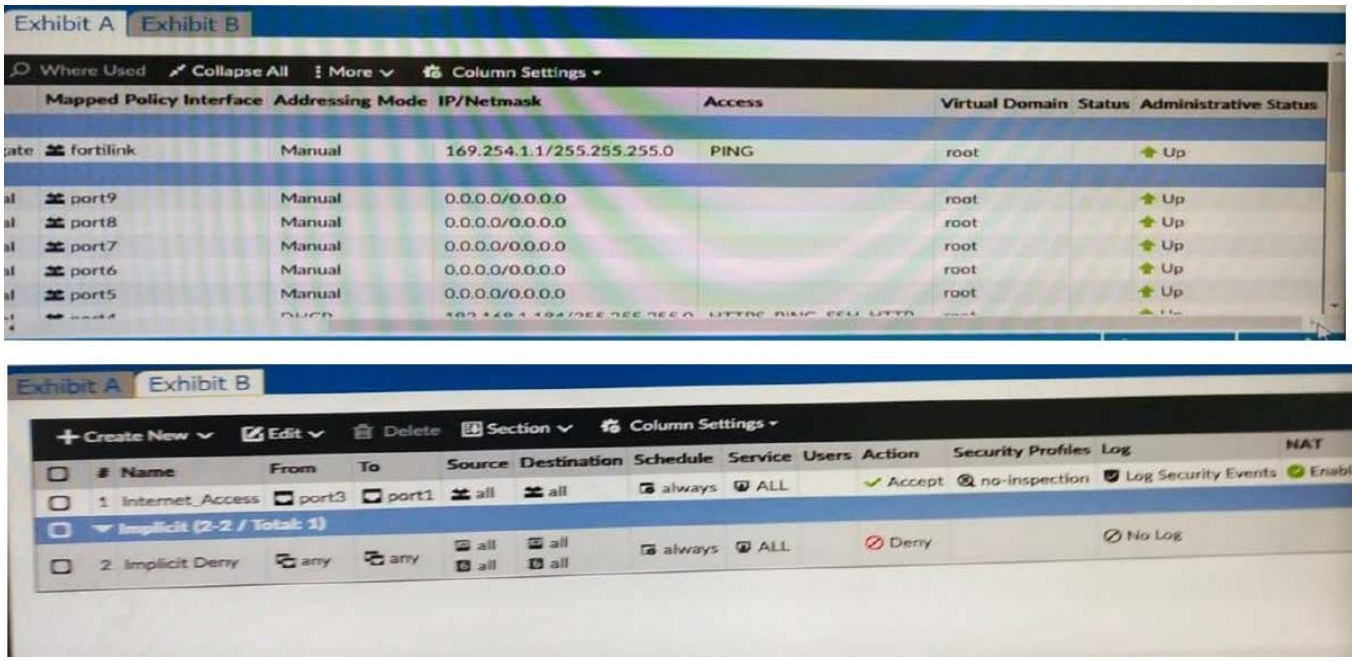


Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate

Based on the FortiGate configuration shown in the exhibits, what are two issues you might encounter when creating an SD-WAN interface on port1 and port2? {Choose two)

A. Member interfaces that are administratively down

B. Member interface that have IP address of 0.0.0.0/0.0.0.0

C. Member interfaces that are physical interfaces as well as VLAN aggregate, and iPsec interfaces

D. Member interfaces that are referenced by any other configuration element

Correct Answer: AD

QUESTION 5

FortiGate is connected to the internet and is obtaining the IP address on its egress interlace from the DHCP server

Which statement is due when FortiGate restarts and receives preconfigured settings to install as part of a zero-touch provisioning process?

A. FortiDeploy connects with FortiGate and provides the initial configuration to contact FortiManager

B. The zero-touch provisioning process completes internally, behind FortiGate

C. FortiManager registers FortiGate after the restart and retrieves the existing configuration

D. The FortiGate cloud key added to the FortiGate cloud portal and FortiGate performs a factory reset before the restart

Correct Answer: A

QUESTION 6

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

A. diagnose sys virtual-wan-link service

B. get router info routing-table

C. diagnose debug application ike

D. get ipsec tunnel list

Correct Answer: C

QUESTION 7

Which two configuration tasks are required to use SD-WAN? (Choose two.)

A. Add one or more members to an SD-WAN zone.

B. Configure at least one firewall policy for SD-WAN traffic.

C. Specify the outgoing interface routing cost.

D. Specify the incoming interfaces in SD-WAN rules.

Correct Answer: AB

QUESTION 8

Refer to the exhibits.

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member and the static routes configuration. If port2 is detected dead by FortiGate, which expected behavior is correct?

A. Port2 becomes alive after one successful probe is detected.

B. The SD-WAN interface becomes disabled and port1 becomes the WAN interface.

C. Dead members require manual administrator access to bring them back alive.

D. Subnets 10.0.20.0/23 and 172.20.0.0/16 are reachable only through port1.

Correct Answer: D

QUESTION 9

Refer to the exhibits. Exhibit A:

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Google.ICMP	all	Google-ICMP	Latency	port1, port2
2	Vimeo	all	Vimeo		port2
3	All_Access_Rules	all	all		port1
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any

Exhibit B:

Add Filter | Details

Date/Time	Source	Destination	Application Name	Result	Policy	Destination Interface
2020/10/15 11:12:27	10.0.1.10	151.101.250.109 (i.vimeocdn.com)	Vimeo	UTM Allowed	Internet Access (1)	port2
2020/10/15 11:12:22	10.0.1.10	34.120.15.67 (fresnel-events.vimeocdn.com)	Vimeo	2.00 kB / 4.33 kB	Internet Access (1)	port1
2020/10/15 11:12:20	10.0.1.10	172.217.13.227 (ocsp.pki.goog)	OCSP	1.28 kB / 1.49 kB	Internet Access (1)	port1
2020/10/15 11:12:07	10.0.1.10	23.47.205.151 (detectportal.firefox.com)	HTTP.BROWSER_Firefox	1.44 kB / 1.55 kB	Internet Access (1)	port1
2020/10/15 11:12:07	10.0.1.10	23.47.205.151 (detectportal.firefox.com)	HTTP.BROWSER_Firefox	1.43 kB / 1.60 kB	Internet Access (1)	port1
2020/10/15 11:12:04	10.0.1.10	99.84.221.62 (snippets.cdn.mozilla.net)	HTTPS.BROWSER	2.08 kB / 13.44 kB	Internet Access (1)	port1

Exhibit A shows the SD-WAN rules and exhibit B shows the traffic logs. The SD-WAN traffic logs reflect how FortiGate distributes traffic. Based on the exhibits, what are two expected behaviors when FortiGate processes SD-WAN traffic? (Choose two.)

A. The first Vimeo session may not match the Vimeo SD-WAN rule because the session is used for the application learning phase.

B. The implicit rule overrides all other rules because parameters widely cover sources and destinations.

C. The Vimeo SD-WAN rule steers Vimeo application traffic among all SD-WAN member interfaces.

D. SD-WAN rules are evaluated in the same way as firewall policies: from top to bottom.

Correct Answer: AD

QUESTION 10

Which two statements about SD-WAN central management are true? (Choose two.)

A. It does not allow you to monitor the status of SD-WAN members.

B. It is enabled or disabled on a per-ADOM basis.

C. It is enabled by default.

D. It uses templates to configure SD-WAN on managed devices.

Correct Answer: BD

QUESTION 11

Which three parameters are available to configure SD-WAN rules? (Choose three.)

A. Application signatures

B. Type of physical link connection

C. URL categories

D. Source and destination IP address

E. Internet service database (ISDB) address object

Correct Answer: ADE

QUESTION 12

Which statement is correct about the SD-WAN and ADVPN?

A. ADVPN interface can be a member of SD-WAN interface.

B. Dynamic VPN is not supported as an SD-Wan interface.

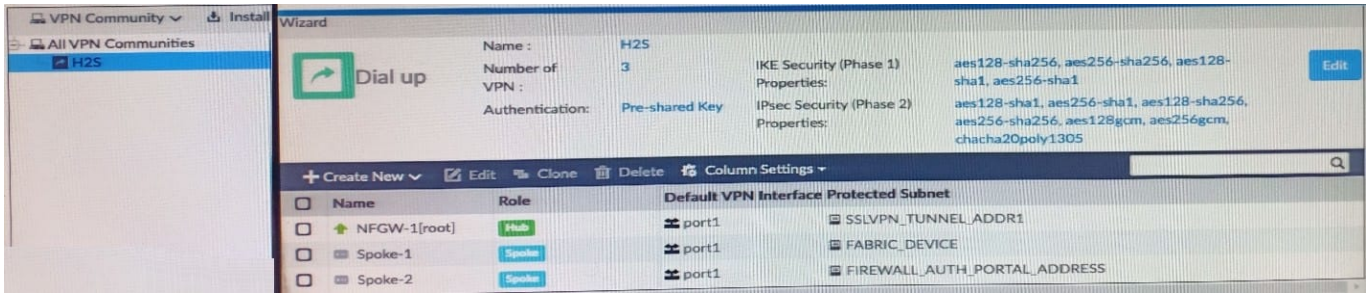
C. Spoke support dynamic VPN as a static interface.

D. Hub FortiGate is limited to use ADVPN as SD-WAN member interface.

Correct Answer: A

QUESTION 13

Refer to the exhibit.



SD-WAN 6.4.5 Guide Page 76. https://docs.fortinet.com/document/fortigate/7.2.1/administration-guide/22371/sd-wan-rules-best-quality

What must you configure to enable ADVPN?

A. On the hub VPN, only the device needs additional phase one sett

B. ADVPN should only be enabled on unmanaged FortiGate devices.

C. Each VPN device has a unique pre-shared key configured separately on phase one

D. The protected subnets should be set to address object to all (0.0 .0. 0/0).

Correct Answer: D

SD-WAN 6.4.5 Study Guide. pg 210

QUESTION 14

Refer to the exhibit.

```
config system virtual-wan-link
     set status enable
     set load-balance-mode source-ip-based
     config members
          edit 1
                    set interface "port1"
                    set gateway 100.64.1.254
                    set source 100.64.1.1
                    set cost 15
          next
          edit 2
                    set interface "port2"
                    set gateway 100.64.2.254
                    set priority 10
          next
     end
end
```

Based on output shown in the exhibit, which two commands can be used by SD-WAN rules? (Choose two.)

A. set cost 15.

B. set source 100.64.1.1.

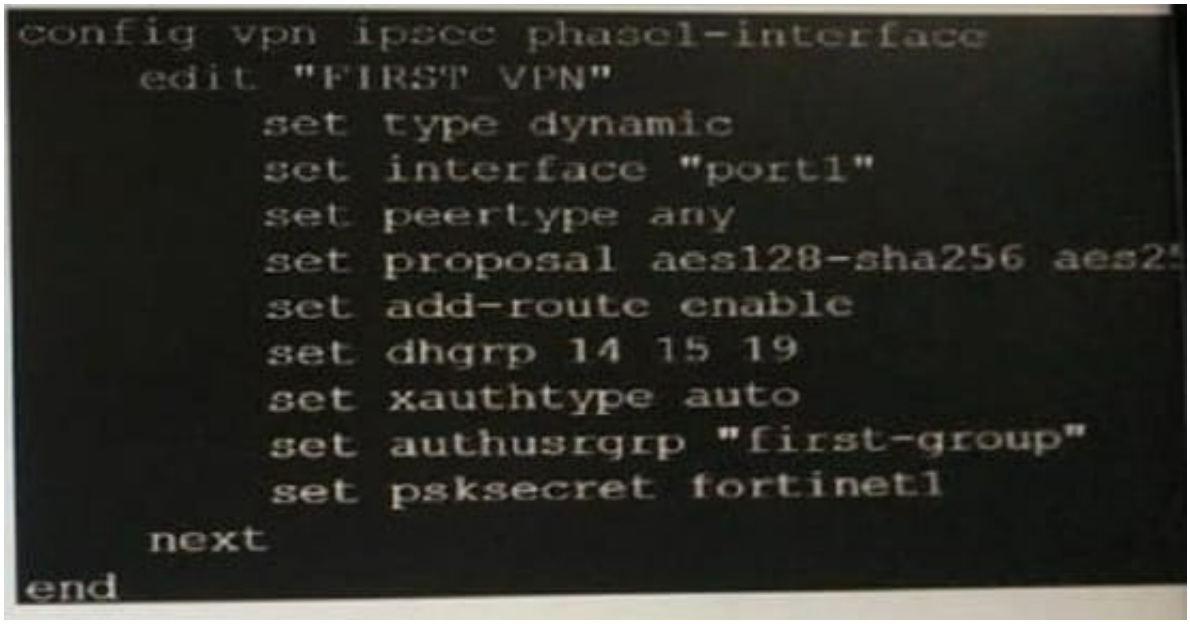
C. set priority 10.

D. set load-balance-mode source-ip-based.

Correct Answer: CD

QUESTION 15

Refer to Exhibit:



Which statement is correct it the responder FortiGate is using a dynamic routing protocol over the IPsec VPN interface?

A. The phase 1 type must be changed to static for dynamic routing.

B. Only dial-up connections without XAuth can be used for the dynamic routing

C. add-route must be disabled to prevent FortiGate from installing VPN static routes

D. peertype must be set to accept only one peer ID for a unique VPN interface

Correct Answer: C