NSE7_SDW-7.0^{Q&As}

Fortinet NSE 7 - SD-WAN 7.0

Pass Fortinet NSE7_SDW-7.0 Exam with 100% Guarantee

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

https://www.passapply.com/nse7_sdw-7-0.html

100% Passing Guarantee
100% Money Back Assurance

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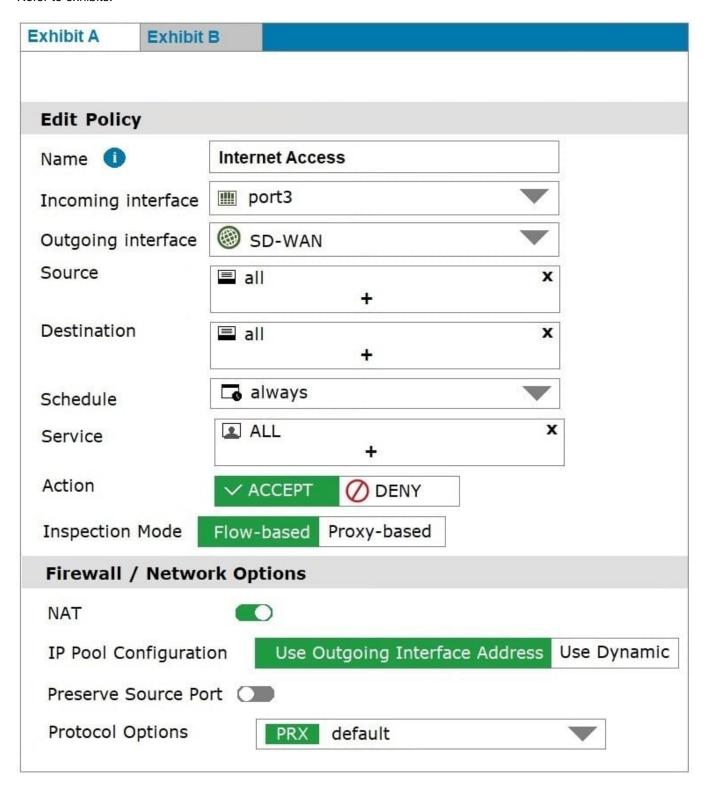Official Exam Center

QUESTION 1

Refer to exhibits.

Exhibit A	Exhibit B

Edit Policy

Name	Internet Access
Incoming interface	port3
Outgoing interface	SD-WAN
Source	all
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT / ⊘ DENY
Inspection Mode	Flow-based / Proxy-based

Firewall / Network Options

NAT	(on)
IP Pool Configuration	Use Outgoing Interface Address / Use Dynamic
Preserve Source Port	(off)
Protocol Options	PRX default

Exhibit A	**Exhibit B**	

Edit Traffic Shaping Policy

Name	inbound_outbound_shaper
Status	**⬆ Enabled** 🔴 Disabled
Comments	Write a comment... 0/255

If Traffic Matches:

Source	🖥 all **X**
	+

Destination	🖥 all **X**
	+

Schedule ⬭

Service	👤 ALL **X**
	+

Application ℹ	**+**

URL Category	**+**

Then:

Action	**Apply Shaper** Assign Shaping Class ID

Outgoing interface	🌐 SD-WAN **X**
	+

Shared shaper 🟢 | guarantee-10mbps ▼

Reverse shaper ⬭

Per-IP shaper ⬭

Exhibit A shows the firewall policy and exhibit B shows the traffic shaping policy.

The traffic shaping policy is being applied to all outbound traffic; however, inbound traffic is not being evaluated by the shaping policy.

Based on the exhibits, what configuration change must be made in which policy so that traffic shaping can be applied to inbound traffic?

A. The reverse shaper option must be enabled and a traffic shaper must be selected

B. The guaranteed-10mbps option must be selected as the reverse shaper option.

C. A new firewall policy must be created and SD-WAN must be selected as the incoming interface.

D. The guaranteed-10mbps option must be selected as the per-IP shaper option

Correct Answer: A

QUESTION 2

Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.

```
config vpn ipsec phase1-interface
    edit "T_INET_0_0"
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set comments "[created by FMG VPN Manager]"
        set idle-timeout enable
        set idle-timeoutinterval 5
        set auto-discovery-receiver enable
        set remote-gw 100.64.1.1
        set psksecret ENC
6D5rVsaK1MeAyVYt1z95BS24Psew761wY023hnFVviwb6deItSc51tCa+iNYhujT8gycfD4+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
LReOFShoH01SPFKz5IYCVA==
    next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD- WAN?

A. You must set ike-version to 1.

B. You must enable net-device.

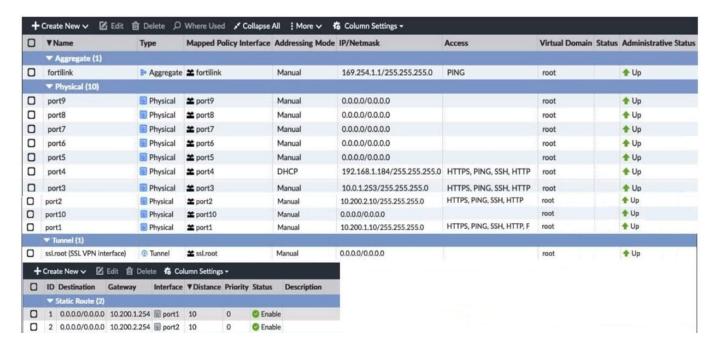C. You must enable auto-discovery-sender.
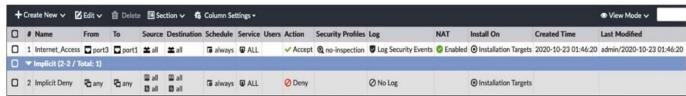
D. You must disable idle-timeout.

Correct Answer: B

QUESTION 3

Refer to the exhibits.

	▼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

	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	

	#	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 4

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.

Correct Answer: AC

SD-WAN 6.4.5 Study Guide. pg 182

QUESTION 5

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