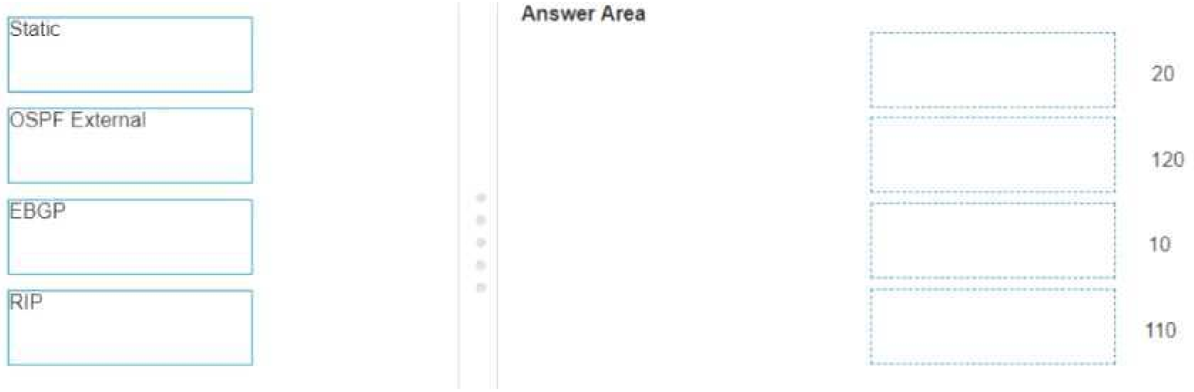
Latest Version: 29.0

Question: 1

DRAG DROP
An engineer is troubleshooting traffic routing through the virtual router. The firewall uses multiple routing protocols, and the engineer is trying to determine routing priority Match the default Administrative Distances for each routing protocol.



Static

OSPF External

EBGP

RIP

Answer Area

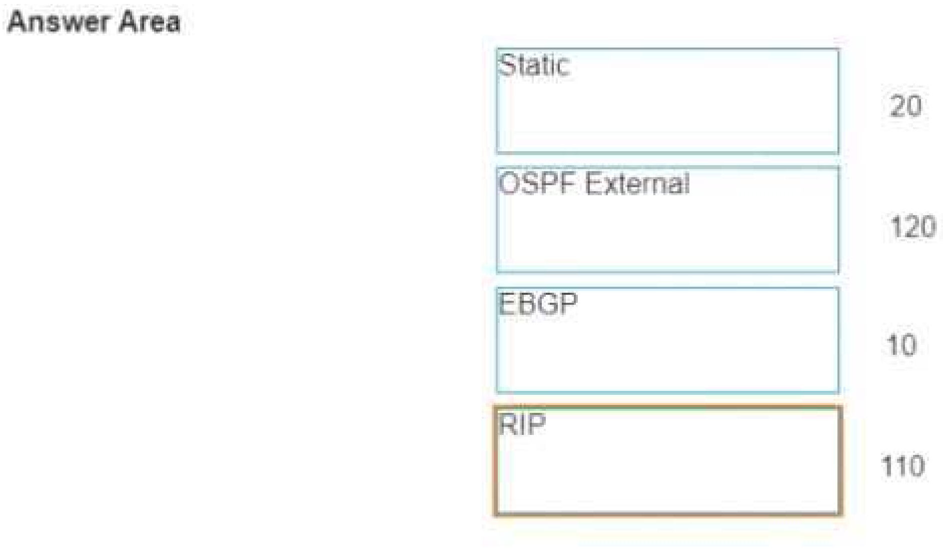
20

120

10

110

Answer:



Answer Area

Static 20

OSPF External 120

EBGP 10

RIP 110

Question: 2

An engineer needs to permit XML API access to a firewall for automation on a network segment that is routed through a Layer 3 subinterface on a Palo Alto Networks firewall. However this network segment cannot access the dedicated management interface due to the Security policy

Without changing the existing access to the management interface how can the engineer fulfill this request?

A. Enable HTTPS in an Interface Management profile on the subinterface
B. Add the network segment's IP range to the Permitted IP Addresses list
C. Specify the subinterface as a management interface in Setup > Device > Interfaces
D. Configure a service route for HTTP to use the subinterface

Answer: A

Question: 3

A Panorama administrator configures a new zone and uses the zone in a new Security policy.
After the administrator commits the configuration to Panorama, which device-group commit push operation should the administrator use to ensure that the push is successful?

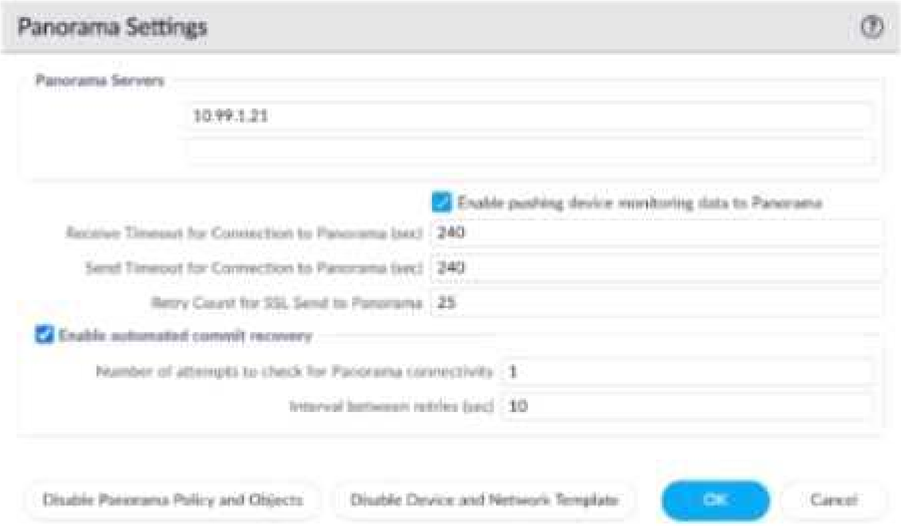
A. force template values
B. merge with candidate config
C. specify the template as a reference template
D. include device and network templates

Answer: D

Question: 4

An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall. Which settings if configured incorrectly most likely would stop only Traffic logs from being sent from the NGFW to Panorama?

A)



Panorama Settings

Panorama Servers

10.99.1.21

☑ Enable pushing device monitoring data to Panorama

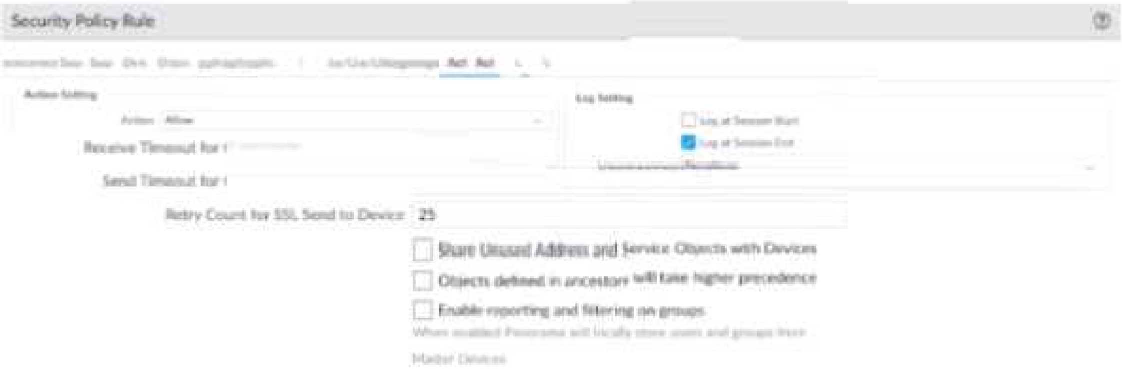
Receive Timeout for Connection to Panorama (sec)	240
Send Timeout for Connection to Panorama (sec)	240
Retry Count for SSL Send to Panorama	25

☑ Enable automated commit recovery

Number of attempts to check for Panorama connectivity	1
Interval between retries (sec)	10

Disable Panorama Policy and Objects
Disable Device and Network Template
OK
Cancel

B)



Security Policy Rule

Action Setting

Action: Allow

Log Setting

□ Log at Session Start

☑ Log at Session End

Receive Timeout for

Send Timeout for

Retry Count for SSL Send to Device: 25

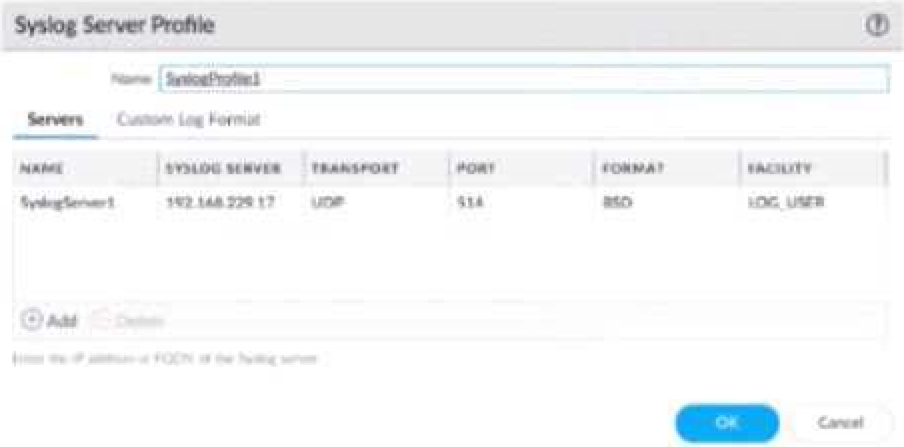
□ Share Unused Address and Service Objects with Devices

□ Objects defined in ancestors will take higher precedence

□ Enable reporting and filtering on groups

When enabled Panorama will locally store users and groups from Master Devices

C)



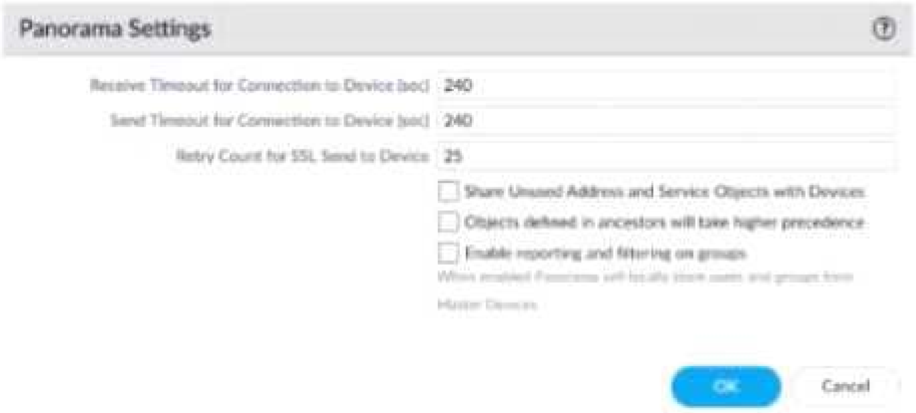
Syslog Server Profile

Name: SyslogProfile1

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

D)



Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

□ Share Unused Address and Service Objects with Devices

□ Objects defined in ancestors will take higher precedence

□ Enable reporting and filtering on groups

When enabled Panorama will locally store users and groups from Master Devices.

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

Question: 5

A network administrator configured a site-to-site VPN tunnel where the peer device will act as initiator None of the peer addresses are known What can the administrator configure to establish the VPN connection1?

A. Set up certificate authentication
B. Enable Passive Mode
C. Use the Dynamic IP address type
D. Configure the peer address as an FQDN

Answer: C