Free Questions for PCNSE by braindumpscollection

Shared by Finch on 06-06-2022

For More Free Questions and Preparation Resources

Question 1

An administrator has left a firewall to use the data of port for all management service which there functions are performed by the data face? (Choose three.)

Options:

A- NTP

B- Antivirus

C- Wildfire updates

D- NAT

E- File tracking

Answer:

A, C, D

Question 2

A users traffic traversing a Palo Alto networks NGFW sometimes can reach http //www company com At other times the session times out. At other times the session times out The NGFW has been configured with a PBF rule that the user traffic matches when it goes to http://www.company.com

How can the firewall be configured to automatically disable the PBF rule if the next hop goes down?
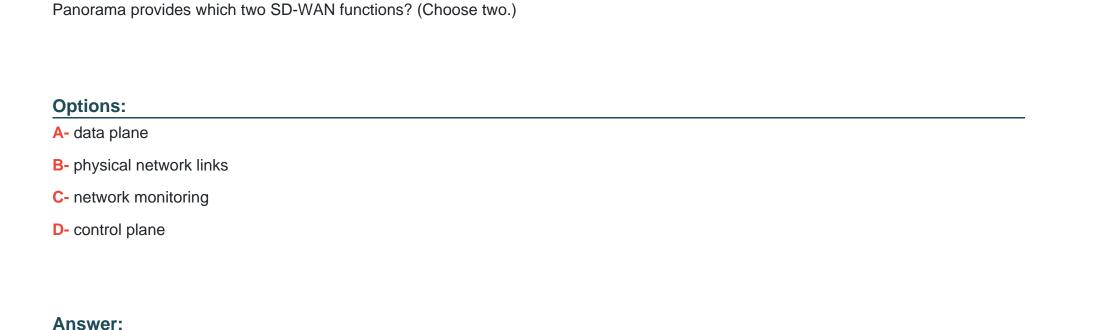
Options:

A- Create and add a monitor profile with an action of fail over in the PBF rule in question

B- Create and add a monitor profile with an action of wait recover in the PBF rule in question

C- Configure path monitoring for the next hop gateway on the default route in the virtual router

D- Enable and configure a link monitoring profile for the external interface of the firewall

Answer:

A

Question 3

Panorama provides which two SD-WAN functions? (Choose two.)

Options:

A- data plane

B- physical network links

C- network monitoring

D- control plane

Answer:

C, D

Explanation:

https://www.paloaltonetworks.com/resources/guides/sd-wan-architecture-guide

https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/about-sd-wan.html

(Network Monitoring & Control Plane). Data plane & Physical Interfaces are directly taken care through Firewalls where SD WAN is enabled.

Question 4

Which two events trigger the operation of automatic commit recovery? (Choose two.)

Options:

A- when an aggregate Ethernet interface component fails

B- when Panorama pushes a configuration

C- when a firewall HA pair fails over

D- when a firewall performs a local commit

Answer:

B, D

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html

Automatic commit recovery allows you to configure the firewall to attempt a specified number of connectivity tests after:

1- you push a configuration from Panorama or

2- commit a configuration change locally on the firewall.

Additionally, the firewall checks connectivity to Panorama every hour to ensure consistent communication in the event unrelated network configuration changes have disrupted connectivity between the firewall and Panorama or if implications to a pushed committed configuration may have affected connectivity.

Question 5

During the packet flow process, which two processes are performed in application identification? (Choose two.)

Options:

A- pattern based application identification

B- application changed from content inspection

C- session application identified

D- application override policy match

Answer:

A, D

Question 6

Question Type: **MultipleChoice**

Starting with PAN-OS version 9.1, Global logging information is now recoded in which firewall log?

Options:

A- Authentication

B- Globalprotect

C- Configuration

D- System

Answer:

D

Question 7

Which operation will impact performance of the management plane?

Options:

A- DoS protection

B- WildFire submissions

C- generating a SaaS Application report

D- decrypting SSL sessions

Answer:

C

Question 8

An administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. the following is the output from the command:

```
less mp-log ikemgr.log:

2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: =====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
=====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <=====
2014-08-05 03:52:33 [PROTO_NOTIFY]: =====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
=====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <===== Due to
timeout.
2014-08-05 03:52:33 [INFO]: =====> PHASE-1 SA DELETED <====
=====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <=====
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: =====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
=====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <=====
2014-08-05 03:53:54 [PROTO_NOTIFY]: =====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
=====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <===== Due to
timeout.
2014-08-05 03:53:54 [INFO]: =====> PHASE-1 SA DELETED <====
```

What could be the cause of this problem?

Options:

A- The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.

B- The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.

C- The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.

D- The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

Answer:

C

Question 9

YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic. The following interfaces and zones are in use on the firewall:
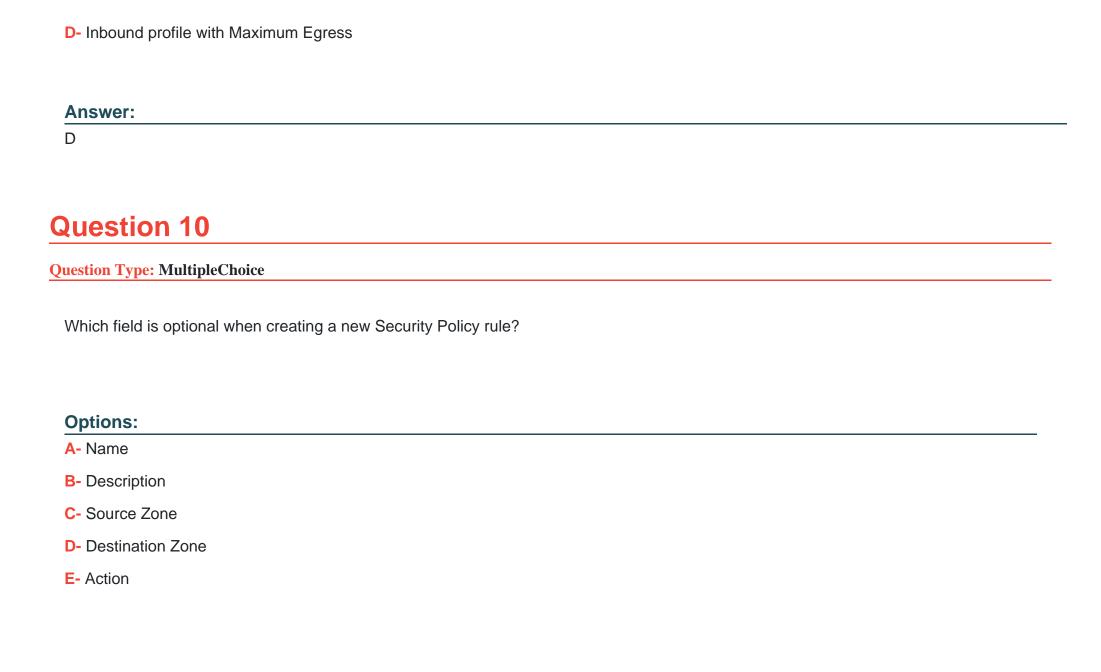
* ethernet1/1, Zone: Untrust (Internet-facing)

* ethernet1/2, Zone: Trust (client-facing)

A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS profile called Inbound.

Which setting for class 6 with throttle YouTube traffic?

Options:
A- Outbound profile with Guaranteed Ingress

B- Outbound profile with Maximum Ingress

C- Inbound profile with Guaranteed Egress

D- Inbound profile with Maximum Egress

Answer:

D

Question 10

Question Type: **MultipleChoice**

Which field is optional when creating a new Security Policy rule?

Options:

A- Name

B- Description

C- Source Zone

D- Destination Zone

E- Action

Answer:

B

Question 11

Question Type: MultipleChoice

Site-A and Site-B need to use IKEv2 to establish a VPN connection. Site A connects directly to the internet using a public IP address. Site-B uses a private IP address behind an ISP router to connect to the internet.

How should NAT Traversal be implemented for the VPN connection to be established between Site-A and Site-B?

Options:

A- Enable on Site-A only

B- Enable on Site-B only

C- Enable on Site-B only with passive mode

D- Enable on Site-A and Site-B

Answer:

D