Paloalto-Networks

Exam Questions PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE)PAN-OS 9.0

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Your company occupies one floor in a single building. You have two Active Directory domain controllers on a single network. The firewall's management-plane resources are lightly utilized.
Given the size of this environment, which User-ID collection method is sufficient?

A. Citrix terminal server agent deployed on the network
B. Windows-based agent deployed on each domain controller
C. PAN-OS integrated agent deployed on the firewall
D. a syslog listener

Answer: C

NEW QUESTION 2
An administrator wants to configure the Palo Alto Networks Windows User-ID agent to map IP addresses to usernames. The company uses four Microsoft Active Directory servers and two Microsoft Exchange servers, which can provide logs for login events.
All six servers have IP addresses assigned from the following subnet: 192.168 28.32/27. The Microsoft Active Directory servers reside in 192.168.28.32/28. and the Microsoft Exchange servers resideL in 192.168.28 48/28
What information does the administrator need to provide in the User Identification > Discovery section?

A. The IP-address and corresponding server type (Microsoft Active Directory or Microsoft Exchange) for each of the six servers
B. Network 192 168.28.32/28 with server type Microsoft Active Directory and network 192.168.28.48/28 with server type Microsoft Exchange
C. Network 192 168 28.32/27 with server type Microsoft
D. One IP address of a Microsoft Active Directory server and "Auto Discover" enabled to automatically obtain all five of the other servers

Answer: A

Explanation:
The administrator needs to provide the IP address and corresponding server type (Microsoft Active Directory or Microsoft Exchange) for each of the six servers in the User Identification > Discovery section. The administrator should enter the network address of 192.168.28.32/28 and select “Microsoft Active Directory” as the server type for the four Active Directory servers and enter the network address of 192.168.28.48/28 and select “Microsoft Exchange” as the server type for the two Exchange servers. This will allow the User-ID agent to discover and map the IP address of each server to the corresponding username.

NEW QUESTION 3
Using multiple templates in a stack to manage many firewalls provides which two advantages? (Choose two.)

A. inherit address-objects from templates
B. define a common standard template configuration for firewalls
C. standardize server profiles and authentication configuration across all stacks
D. standardize log-forwarding profiles for security polices across all stacks

Answer: BD

NEW QUESTION 4
What steps should a user take to increase the NAT oversubscription rate from the default platform setting?

A. Navigate to Device > Setup > TCP Settings > NAT Oversubscription Rate
B. Navigate to Policies > NAT > Destination Address Translation > Dynamic IP (with session distribution)
C. Navigate to Policies > NAT > Source Address Translation > Dynamic IP (with session distribution)
D. Navigate to Device > Setup > Session Settings > NAT Oversubscription Rate

Answer: D

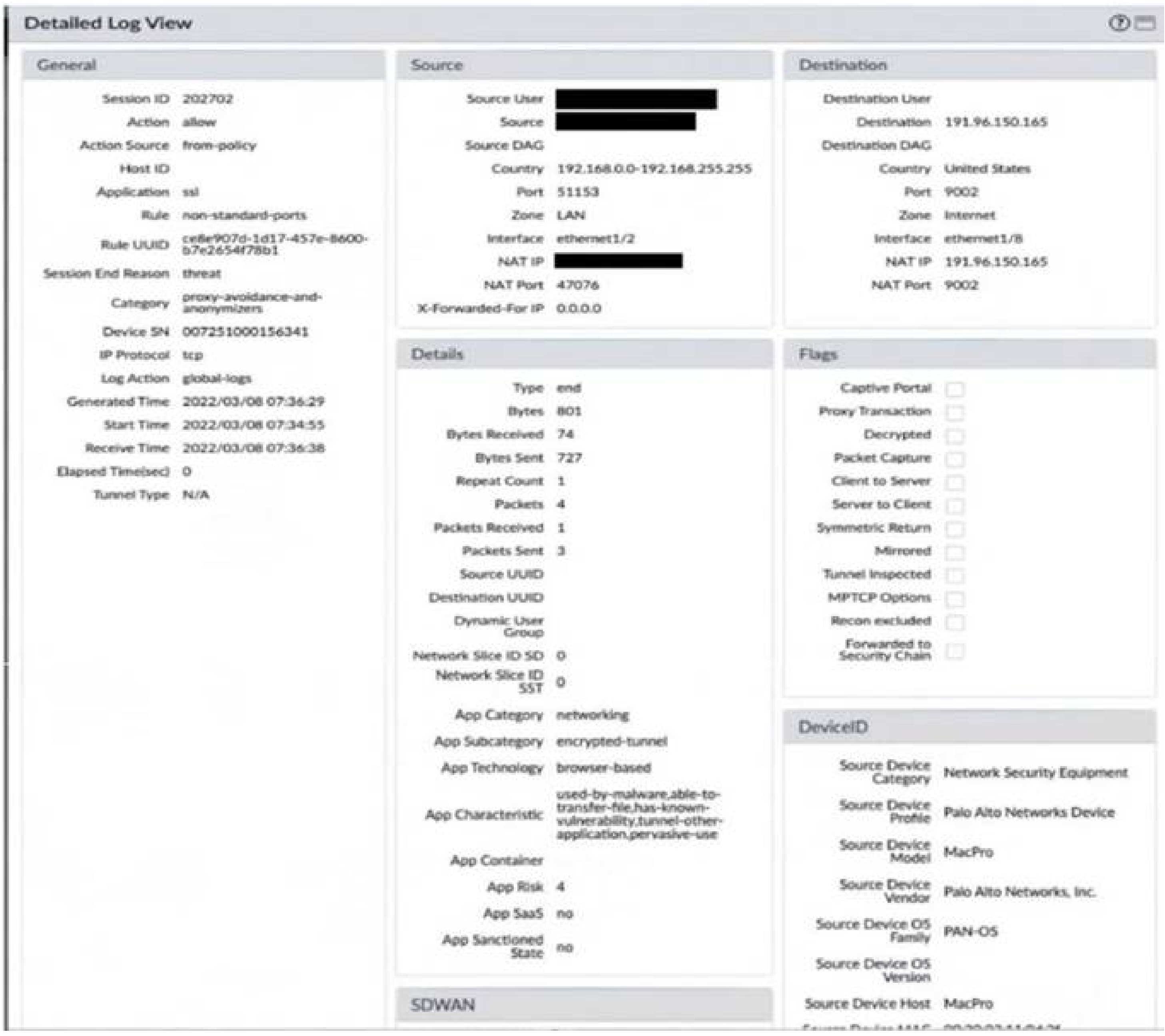
Explanation:
NAT oversubscription is a feature that allows you to reuse a translated IP address and port for multiple source devices. This can help you conserve public IP addresses and increase the number of sessions that can be translated by a NAT rule.

NEW QUESTION 5
An administrator is building Security rules within a device group to block traffic to and from malicious locations
How should those rules be configured to ensure that they are evaluated with a high priority?

A. Create the appropriate rules with a Block action and apply them at the top of the Default Rules
B. Create the appropriate rules with a Block action and apply them at the top of the Security Post-Rules.
C. Create the appropriate rules with a Block action and apply them at the top of the local firewall Security rules.
D. Create the appropriate rules with a Block action and apply them at the top of the Security Pre-Rules

Answer: D

NEW QUESTION 6
Given the screenshot, how did the firewall handle the traffic?



Detailed Log View

General

Session ID 202702
Action allow
Action Source from-policy
Host ID
Application ssl
Rule non-standard-ports
Rule UUID ce8e907d-1d17-457e-8600-b7e2654f78b1
Session End Reason threat
Category proxy-avoidance-and-anonymizers
Device SN 007251000156341
IP Protocol tcp
Log Action global-logs
Generated Time 2022/03/08 07:36:29
Start Time 2022/03/08 07:34:55
Receive Time 2022/03/08 07:36:38
Elapsed Time(sec) 0
Tunnel Type N/A

Source

Source User [redacted]
Source [redacted]
Source DAG
Country 192.168.0.0-192.168.255.255
Port 51153
Zone LAN
Interface ethernet1/2
NAT IP [redacted]
NAT Port 47076
X-Forwarded-For IP 0.0.0.0

Details

Type end
Bytes 801
Bytes Received 74
Bytes Sent 727
Repeat Count 1
Packets 4
Packets Received 1
Packets Sent 3
Source UUID
Destination UUID
Dynamic User Group
Network Slice ID SD 0
Network Slice ID SST 0
App Category networking
App Subcategory encrypted-tunnel
App Technology browser-based
App Characteristic used-by-malware,able-to-transfer-file,has-known-vulnerability,tunnel-other-application,pervasive-use
App Container
App Risk 4
App SaaS no
App Sanctioned State no

SDWAN

Destination

Destination User
Destination 191.96.150.165
Destination DAG
Country United States
Port 9002
Zone Internet
Interface ethernet1/8
NAT IP 191.96.150.165
NAT Port 9002

Flags

Captive Portal □
Proxy Transaction □
Decrypted □
Packet Capture □
Client to Server □
Server to Client □
Symmetric Return □
Mirrored □
Tunnel Inspected □
MPTCP Options □
Recon excluded □
Forwarded to Security Chain □

DeviceID

Source Device Category Network Security Equipment
Source Device Profile Palo Alto Networks Device
Source Device Model MacPro
Source Device Vendor Palo Alto Networks, Inc.
Source Device OS Family PAN-OS
Source Device OS Version
Source Device Host MacPro

A. Traffic was allowed by profile but denied by policy as a threat
B. Traffic was allowed by policy but denied by profile as..
C. Traffic was allowed by policy but denied by profile as ..
D. Traffic was allowed by policy but denied by profile as a..

Answer: D

NEW QUESTION 7
SSL Forward Proxy decryption is configured but the firewall uses Untrusted-CA to sign the website https://www important-website com certificate End-users are receiving me "security certificate is not trusted is warning Without SSL decryption the web browser shows that the website certificate is trusted and signed by a well-known certificate chain Well-Known-lntermediate and Well-Known-Root- CA.
The network security administrator who represents the customer requires the following two behaviors when SSL Forward Proxy is enabled:
1 End-users must not get the warning for the https://www.very-important-website.com website. 2 End-users should get the warning for any other untrusted website Which approach meets the two customer requirements?

A. Navigate to Device > Certificate Management > Certificates > Device Certificates importWell-Known-lntermediate-CA and Well-Known-Root-CA select the Trusted Root CA checkbox and commit the configuration
B. Install the Well-Known-lntermediate-CA and Well-Known-Root-CA certificates on all end-user systems m the user and local computer stores
C. Navigate to Device > Certificate Management - Certificates s Default Trusted Certificate Authorities import Well-Known-intermediate-CA and Well-Known-Root-CA select the Trusted Root CA check box and commit the configuration
D. Clear the Forward Untrust Certificate check box on the Untrusted-CA certificate and commit the configuration

Answer: C

NEW QUESTION 8
Which benefit do policy rule UUlDs provide?

A. An audit trail across a policy's lifespan
B. Functionality for scheduling policy actions
C. The use of user IP mapping and groups in policies
D. Cloning of policies between device-groups

Answer: A

NEW QUESTION 9
Which configuration is backed up using the Scheduled Config Export feature in Panorama?

A. Panorama running configuration
B. Panorama candidate configuration
C. Panorama candidate configuration and candidate configuration of all managed devices
D. Panorama running configuration and running configuration of all managed devices

Answer: D

NEW QUESTION 10
Which statement about High Availability timer settings is true?

A. Use the Moderate timer for typical failover timer settings.
B. Use the Critical timer for taster failover timer settings.
C. Use the Recommended timer tor faster failover timer settings.
D. Use the Aggressive timer for taster failover timer settings

Answer: C

NEW QUESTION 10
An engineer wants to configure aggregate interfaces to increase bandwidth and redundancy between the firewall and switch. Which statement is correct about the configuration of the interfaces assigned to an aggregate interface group?

A. They can have a different bandwidth.
B. They can have a different interface type such as Layer 3 or Layer 2.
C. They can have a different interface type from an aggregate interface group.
D. They can have different hardware media such as the ability to mix fiber optic and copper.

Answer: C

NEW QUESTION 12
Which statement is true regarding a Best Practice Assessment?

A. It shows how your current configuration compares to Palo Alto Networks recommendations
B. It runs only on firewalls
C. When guided by an authorized sales engineer, it helps determine the areas of greatest risk where you should focus prevention activities.
D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Answer: A

NEW QUESTION 13
A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas)

A. Enterprise-Trusted-CA; which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system)i
B. Enterprise-Untrusted-CA, which is verified as Forward Untrust Certificateii
C. Enterprise-lntermediate-CAi
D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits https //www example-website com/ with a server certificate Common Name (CN) www example-website com The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewallThe end-user's browser will show that the certificate for www.example-website.com was issued by which of the following?
E. Enterprise-Untrusted-CA which is a self-signed CA
F. Enterprise-Trusted-CA which is a self-signed CA
G. Enterprise-lntermediate-CA which wa
H. in turn, issued by Enterprise-Root-CA
I. Enterprise-Root-CA which is a self-signed CA

Answer: B

NEW QUESTION 14
An engineer is tasked with configuring a Zone Protection profile on the untrust zone. Which three settings can be configured on a Zone Protection profile? (Choose three.)

A. Ethernet SGT Protection
B. Protocol Protection
C. DoS Protection
D. Reconnaissance Protection
E. Resource Protection

Answer: BCD

Explanation:
* B. Protocol Protection: Protocol protection is used to limit or block traffic that uses certain protocols or application functions. For example, a Zone Protection profile can be configured to block traffic that uses non-standard protocols, such as IP-in-IP, or to limit the number of concurrent sessions for certain protocols, such as SIP.
* C. DoS Protection: DoS protection is used to protect against various types of denial-of-service (DoS) attacks, such as SYN floods, UDP floods, ICMP floods, and others. A Zone Protection profile can be configured to limit the rate of traffic for certain protocols or to drop traffic that matches specific patterns, such as malformed packets or packets with invalid headers.
* D. Reconnaissance Protection: Reconnaissance protection is used to prevent attackers from gathering information about the network, such as by using port scans or other techniques. A Zone Protection profile can be configured to limit the rate of traffic for certain types of reconnaissance, such as port scans or OS fingerprinting, or to drop traffic that matches specific patterns, such as packets with invalid flags or payloads.

NEW QUESTION 18
A company has configured a URL Filtering profile with override action on their firewall. Which two profiles are needed to complete the configuration? (Choose two)

A. SSUTLS Service

B. HTTP Server
C. Decryption
D. Interface Management

Answer: AD

NEW QUESTION 23
An engineer is planning an SSL decryption implementation
Which of the following statements is a best practice for SSL decryption?

A. Use the same Forward Trust certificate on all firewalls in the network.
B. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate.
C. Obtain an enterprise CA-signed certificate for the Forward Trust certificate.
D. Use an enterprise CA-signed certificate for the Forward Untrust certificate.

Answer: C

NEW QUESTION 27
Which three firewall multi-factor authentication factors are supported by PAN-OS? (Choose three)

A. SSH key
B. User logon
C. Short message service
D. One-Time Password
E. Push

Answer: BDE

Explanation:
According to Palo Alto Networks documentation123, multi-factor authentication (MFA) is a method of verifying a user's identity using two or more factors, such as something they know, something they have, or something they are.
The firewall supports MFA for administrative access, GlobalProtect VPN access, and Captive Portal access. The firewall can integrate with external MFA providers such as RSA SecurID, Duo Security, or Okta Verify.
The three firewall MFA factors that are supported by PAN-OS are:

- User logon: This is something the user knows, such as a username and password.
- One-Time Password: This is something the user has, such as a code generated by an app or sent by email or SMS.
- Push: This is something the user is, such as a biometric verification or a device approval.

NEW QUESTION 29
An engineer needs to see how many existing SSL decryption sessions are traversing a firewall What command should be used?

A. show dataplane pool statistics I match proxy
B. debug dataplane pool statistics I match proxy
C. debug sessions I match proxy
D. show sessions all

Answer: B

NEW QUESTION 32
A firewall administrator is trying to identify active routes learned via BGP in the virtual router runtime stats within the GUI. Where can they find this information?

A. routes listed in the routing table with flags
B. routes listed in the routing table with flags A?
C. under the BGP Summary tab
D. routes listed in the forwarding table with BGP in the Protocol column

Answer: C

NEW QUESTION 34
Which three methods are supported for split tunneling in the GlobalProtect Gateway? (Choose three.)

A. Video Streaming Application
B. Destination Domain
C. Client Application Process
D. Source Domain
E. URL Category

Answer: BCE

Explanation:
The GlobalProtect Gateway supports three methods for split tunneling23:

- Access Route — You can define a list of IP addresses or subnets that are accessible through the VPN tunnel. All other traffic goes directly to the internet.
- Domain and Application — You can define a list of domains or applications that are accessible through the VPN tunnel. All other traffic goes directly to the internet. You can also use this method to exclude specific domains or applications from the VPN tunnel.
- Video Traffic — You can exclude video streaming traffic from the VPN tunnel based on predefined categories or custom URLs. This method reduces latency and jitter for video streaming applications.

NEW QUESTION 36
An organization is interested in migrating from their existing web proxy architecture to the Web Proxy feature of their PAN-OS 11.0 firewalls. Currently. HTTP and SSL requests contain the c IP address of the web server and the client browser is redirected to the proxy
Which PAN-OS proxy method should be configured to maintain this type of traffic flow?

A. DNS proxy
B. Explicit proxy
C. SSL forward proxy
D. Transparent proxy

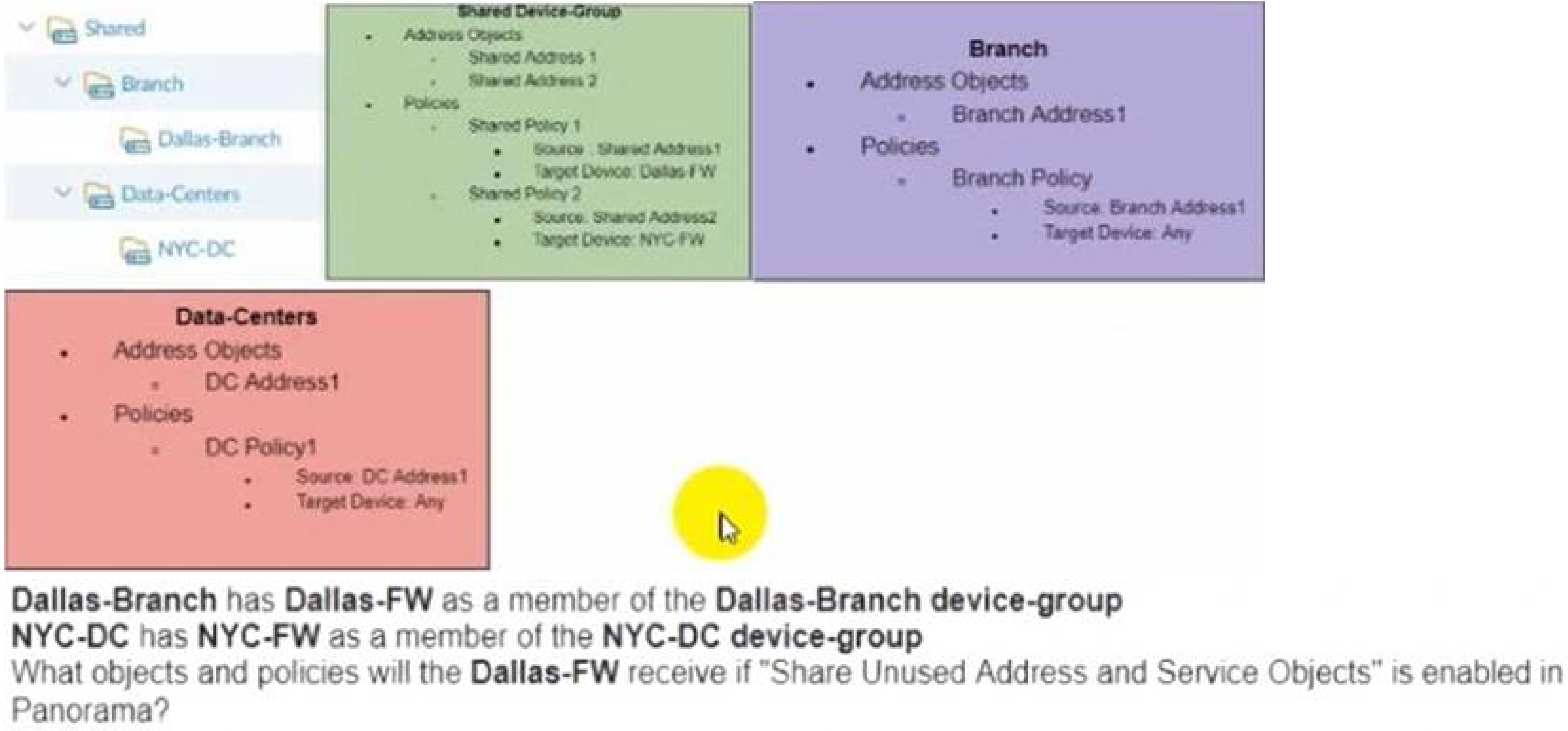
Answer: D

Explanation:
A transparent proxy is a type of web proxy that intercepts and redirects HTTP and HTTPS requests without requiring any configuration on the client browser1. The firewall acts as a gateway between the client and the web server, and performs security checks on the traffic.
A transparent proxy can be configured on PAN-OS 11.0 firewalls by performing the following steps1:

- Enable Web Proxy under Device > Setup > Services
- Select Transparent Proxy as the Proxy Type
- Configure a Service Route for Web Proxy
- Configure SSL/TLS Service Profile for Web Proxy
- Configure Security Policy Rules for Web Proxy Traffic

By configuring a transparent proxy on PAN-OS 11.0 firewalls, an organization can migrate from their existing web proxy architecture without changing their network topology or client settings2. The firewall will maintain the same type of traffic flow as before, where HTTP and HTTPS requests contain the IP address of the web server and the client browser is redirected to the proxy1.
Answer A is not correct because DNS proxy is a type of web proxy that intercepts DNS queries from clients and resolves them using an external DNS server3. This type of proxy does not redirect HTTP or HTTPS requests to the firewall.

NEW QUESTION 40
The following objects and policies are defined in a device group hierarchy



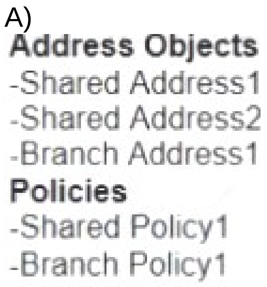
Shared Device-Group
- Address Objects
  - Shared Address 1
  - Shared Address 2
- Policies
  - Shared Policy 1
    - Source : Shared Address1
    - Target Device: Dallas-FW
  - Shared Policy 2
    - Source: Shared Address2
    - Target Device: NYC-FW

Branch
- Address Objects
  - Branch Address1
- Policies
  - Branch Policy
    - Source: Branch Address1
    - Target Device: Any

Data-Centers
- Address Objects
  - DC Address1
- Policies
  - DC Policy1
    - Source: DC Address1
    - Target Device: Any

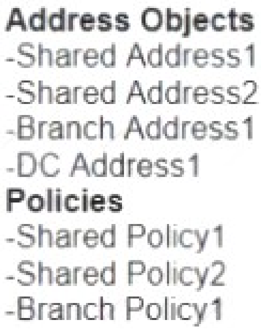
Dallas-Branch has **Dallas-FW** as a member of the **Dallas-Branch device-group**
NYC-DC has **NYC-FW** as a member of the **NYC-DC device-group**
What objects and policies will the **Dallas-FW** receive if "Share Unused Address and Service Objects" is enabled in Panorama?

A)



Address Objects
-Shared Address1
-Shared Address2
-Branch Address1
Policies
-Shared Policy1
-Branch Policy1

B)



Address Objects
-Shared Address1
-Shared Address2
-Branch Address1
-DC Address1
Policies
-Shared Policy1
-Shared Policy2
-Branch Policy1

C)
Address Objects
-Shared Address 1
-Branch Address2 Policies -Shared Polic1 l -Branch Policyl
D)
Address Objects -Shared Addressl -Shared Address2 -Branch Addressl Policies -Shared Policyl -Shared Policy2 -Branch Policyl

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

Answer: A

NEW QUESTION 41
An administrator is seeing one of the firewalls in a HA active/passive pair moved to 'suspended" state due to Non-functional loop. Which three actions will help the administrator troubleshool this issue? (Choose three.)

A. Use the CLI command show high-availability flap-statistics
B. Check the HA Link Monitoring interface cables.
C. Check the High Availability > Link and Path Monitoring settings.
D. Check High Availability > Active/Passive Settings > Passive Link State
E. Check the High Availability > HA Communications > Packet Forwarding settings.

Answer: ABC

NEW QUESTION 46
A network administrator troubleshoots a VPN issue and suspects an IKE Crypto mismatch between peers. Where can the administrator find the corresponding logs after running a test command to initiate the VPN?

A. Configuration logs
B. System logs
C. Traffic logs
D. Tunnel Inspection logs

Answer: B

NEW QUESTION 47
What are two valid deployment options for Decryption Broker? (Choose two)

A. Transparent Bridge Security Chain
B. Layer 3 Security Chain
C. Layer 2 Security Chain
D. Transparent Mirror Security Chain

Answer: AB

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker

NEW QUESTION 50
The decision to upgrade to PAN-OS 10.2 has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when trying to install.
When performing an upgrade on Panorama to PAN-OS 10.2, what is the potential cause of a failed install?

A. Management only mode
B. Expired certificates
C. Outdated plugins
D. GlobalProtect agent version

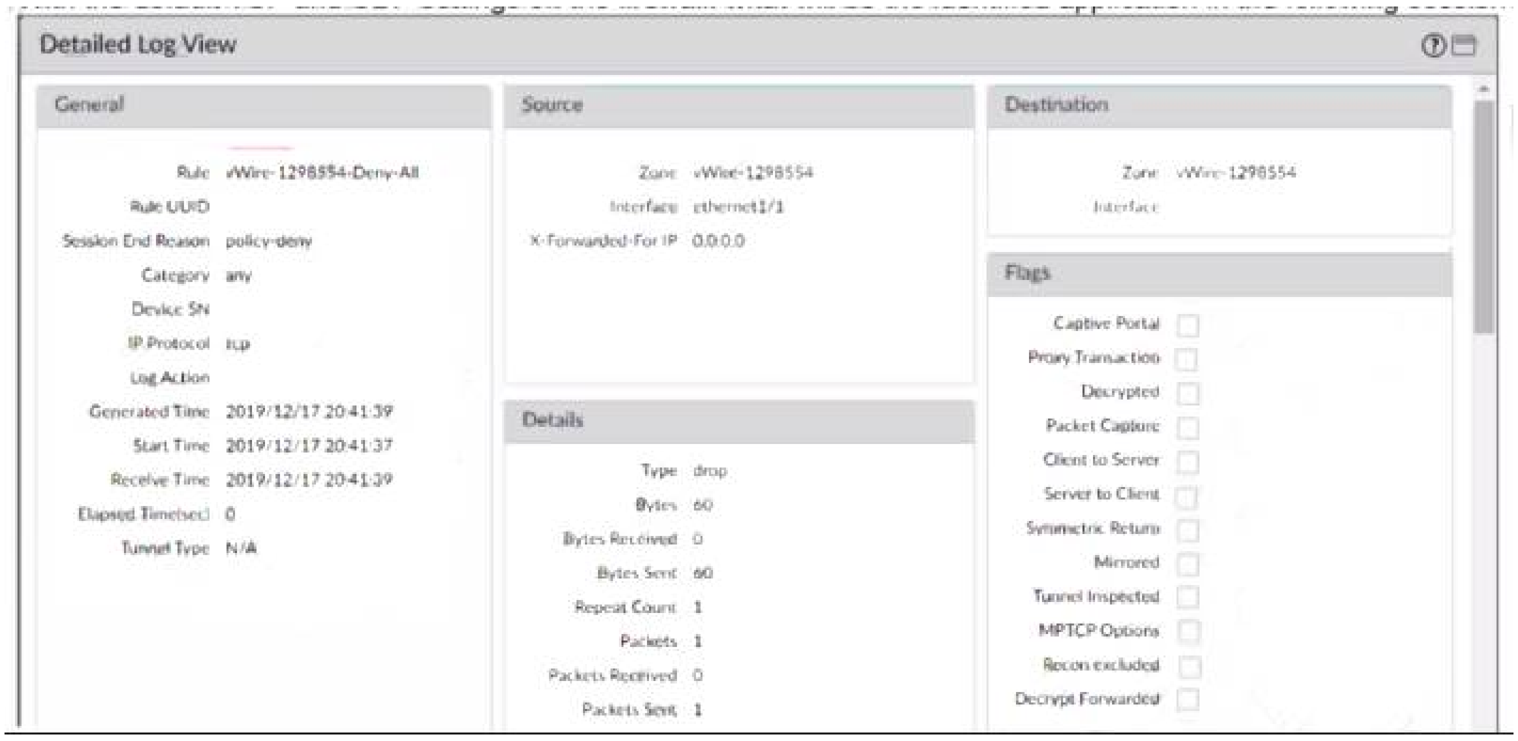
Answer: A

NEW QUESTION 54
What is a key step in implementing WildFire best practices?

A. In a mission-critical network, increase the WildFire size limits to the maximum value.
B. Configure the firewall to retrieve content updates every minute.
C. In a security-first network, set the WildFire size limits to the minimum value.
D. Ensure that a Threat Prevention subscription is active.

Answer: D

NEW QUESTION 55
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?



Detailed Log View

General

Rule vWire-1298554-Deny-All
Rule UUID
Session End Reason policy-deny
Category any
Device SN
IP Protocol tcp
Log Action
Generated Time 2019/12/17 20:41:39
Start Time 2019/12/17 20:41:37
Receive Time 2019/12/17 20:41:39
Elapsed Time(sec) 0
Tunnel Type N/A

Source

Zone vWire-1298554
Interface ethernet1/1
X-Forwarded-For IP 0.0.0.0

Details

Type drop
Bytes 60
Bytes Received 0
Bytes Sent 60
Repeat Count 1
Packets 1
Packets Received 0
Packets Sent 1

Destination

Zone vWire-1298554
Interface

Flags

Captive Portal □
Proxy Transaction □
Decrypted □
Packet Capture □
Client to Server □
Server to Client □
Symmetric Return □
Mirrored □
Tunnel Inspected □
MPTCP Options □
Recon excluded □
Decrypt Forwarded □

A. Incomplete
B. unknown-udp
C. Insufficient-data
D. not-applicable

Answer: B

NEW QUESTION 56
A network administrator wants to use a certificate for the SSL/TLS Service Profile. Which type of certificate should the administrator use?

A. certificate authority (CA) certificate
B. client certificate
C. machine certificate
D. server certificate

Answer: D

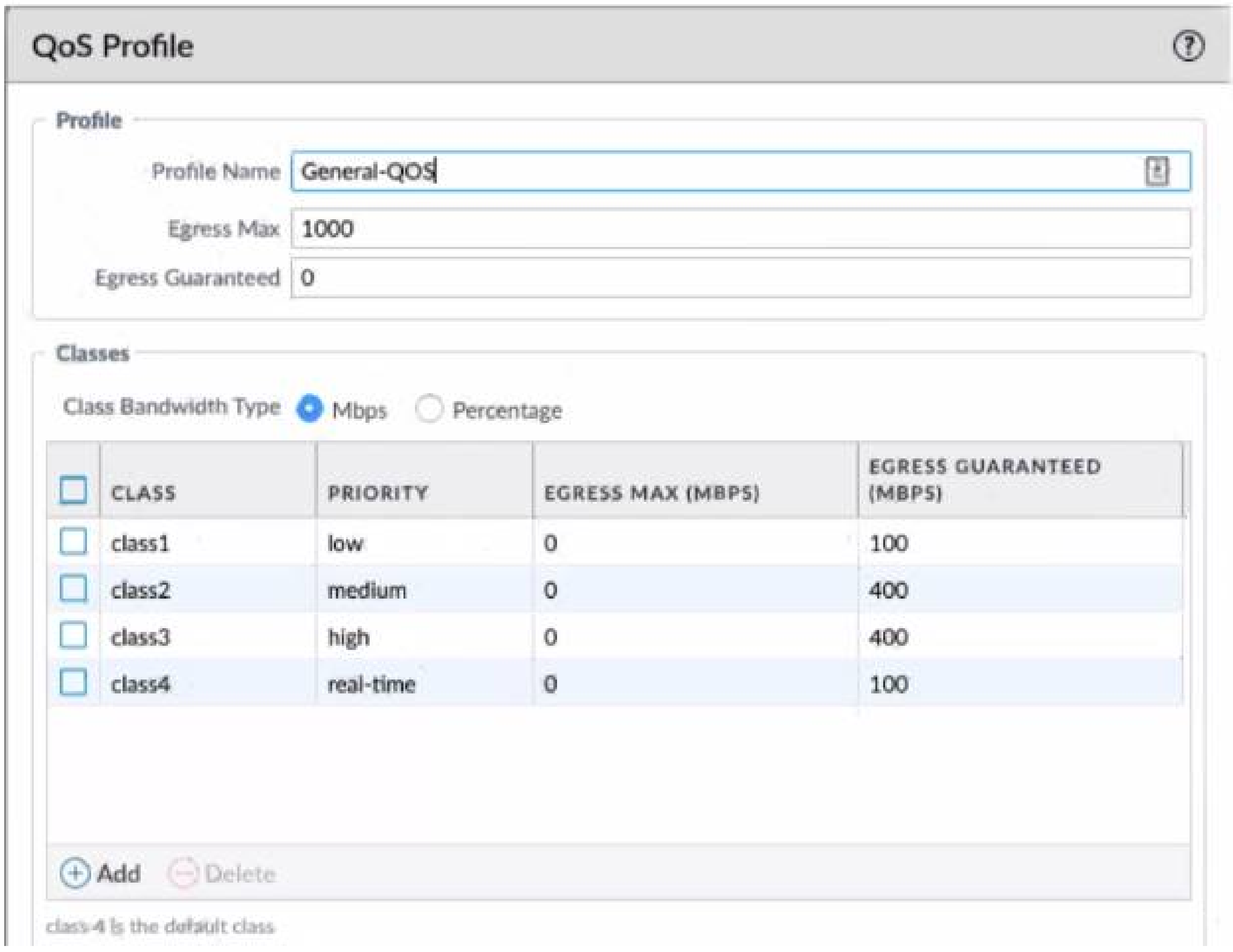
Explanation:
Use only signed certificates, not CA certificates, in SSL/TLS service profiles. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssltls-service

NEW QUESTION 60
A firewall administrator needs to be able to inspect inbound HTTPS traffic on servers hosted in their DMZ to prevent the hosted service from being exploited. Which combination of features can allow PAN-OS to detect exploit traffic in a session with TLS encapsulation?

A. Decryption policy and a Data Filtering profile
B. a WildFire profile and a File Blocking profile
C. Vulnerability Protection profile and a Decryption policy
D. a Vulnerability Protection profile and a QoS policy

Answer: C

NEW QUESTION 61
View the screenshots.



QoS Profile

Profile

Profile Name: General-QOS

Egress Max: 1000

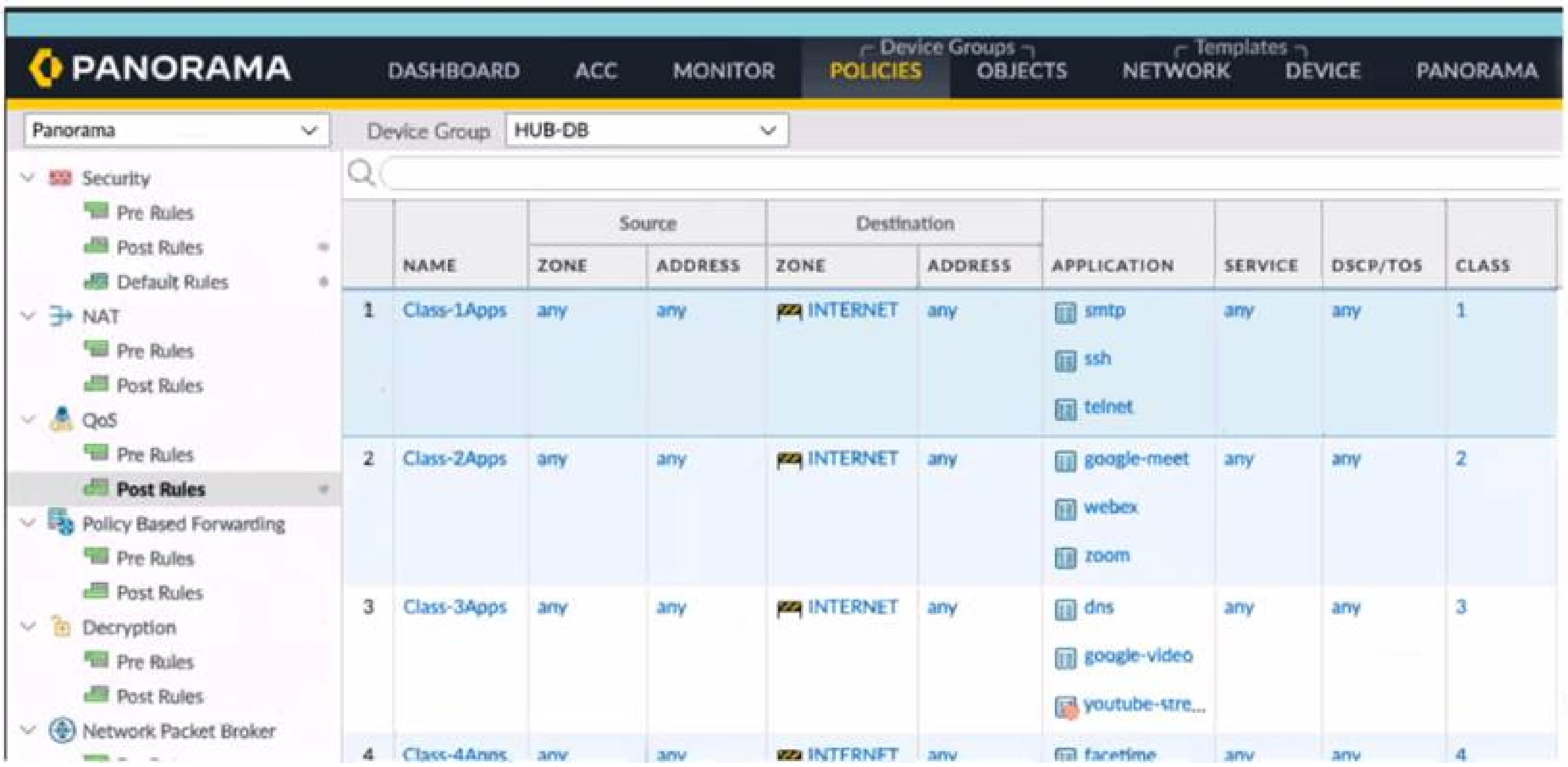
Egress Guaranteed: 0

Classes

Class Bandwidth Type: ● Mbps ○ Percentage

□	CLASS	PRIORITY	EGRESS MAX (MBPS)	EGRESS GUARANTEED (MBPS)
□	class1	low	0	100
□	class2	medium	0	400
□	class3	high	0	400
□	class4	real-time	0	100

class-4 is the default class



Device Group: HUB-DB

		Source		Destination					
	NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	DSCP/TOS	CLASS
1	Class-1Apps	any	any	INTERNET	any	smtp ssh telnet	any	any	1
2	Class-2Apps	any	any	INTERNET	any	google-meet webex zoom	any	any	2
3	Class-3Apps	any	any	INTERNET	any	dns google-video youtube-stre...	any	any	3
4	Class-4Apps	any	any	INTERNET	any	facetime	any	any	4

A QoS profile and policy rules are configured as shown. Based on this information, which two statements are correct? (Choose two.)

A. DNS has a higher priority and more bandwidth than SSH.
B. Google-video has a higher priority and more bandwidth than WebEx.
C. SMTP has a higher priority but lower bandwidth than Zoom.
D. Facetime has a higher priority but lower bandwidth than Zoom.

Answer: CD

NEW QUESTION 62
An existing NGFW customer requires direct interne! access offload locally at each site and iPSec connectivity to all branches over public internet. One requirement is mat no new SD-WAN hardware be introduced to the environment.
What is the best solution for the customer?

A. Configure a remote network on PAN-OS
B. Upgrade to a PAN-OS SD-WAN subscription
C. Deploy Prisma SD-WAN with Prisma Access
D. Configure policy-based forwarding

Answer: B

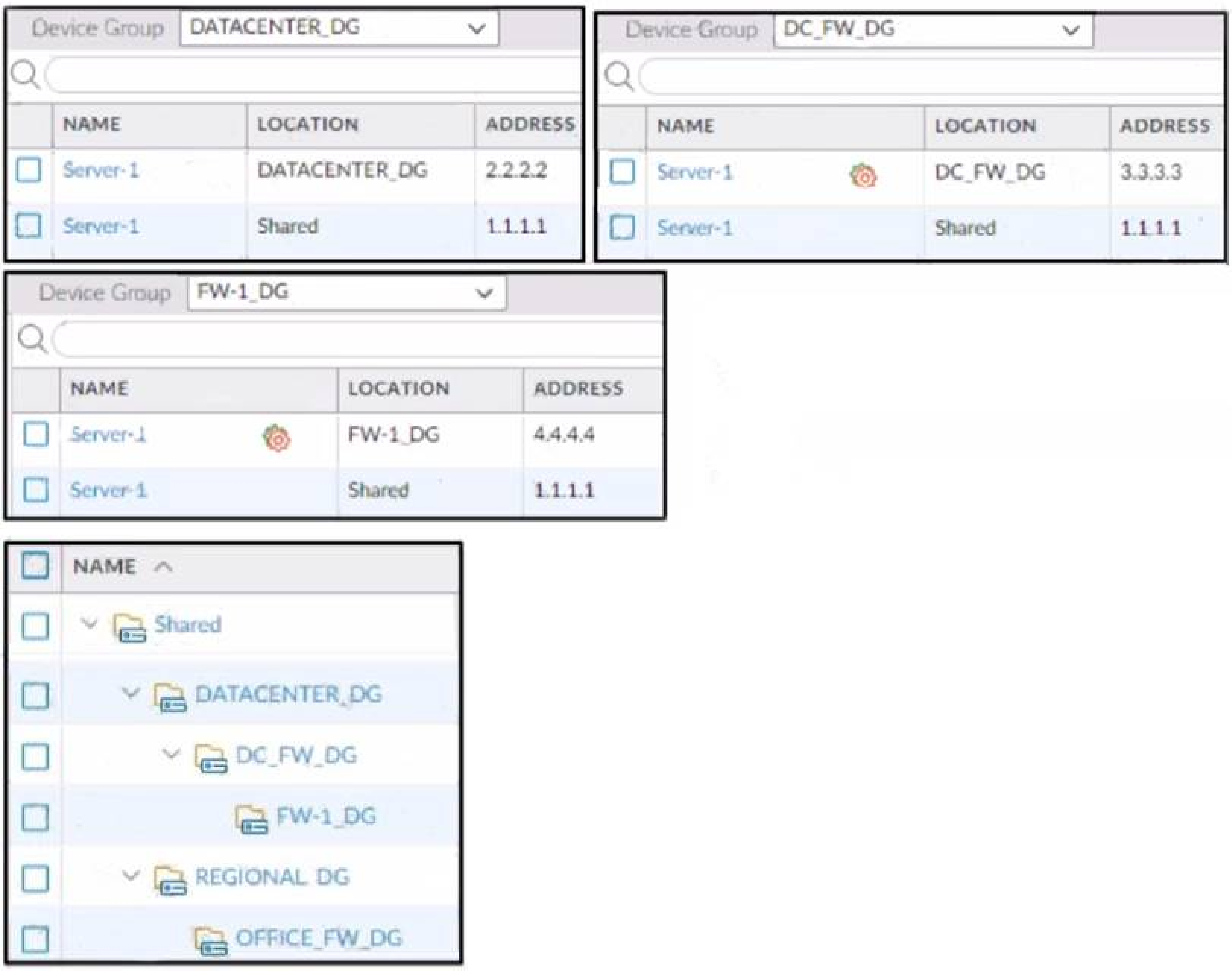
NEW QUESTION 67
An engineer is bootstrapping a VM-Series Firewall Other than the 'config folder, which three directories are mandatory as part of the bootstrap package directory structure? (Choose three.)

A. /software
B. /opt

C. /license
D. /content
E. /plugins

Answer: AD

NEW QUESTION 70
Refer to the exhibit.



Device Group: DATACENTER_DG

	NAME	LOCATION	ADDRESS
□	Server-1	DATACENTER_DG	2.2.2.2
□	Server-1	Shared	1.1.1.1

Device Group: DC_FW_DG

	NAME	LOCATION	ADDRESS
□	Server-1	DC_FW_DG	3.3.3.3
□	Server-1	Shared	1.1.1.1

Device Group: FW-1_DG

	NAME	LOCATION	ADDRESS
□	Server-1	FW-1_DG	4.4.4.4
□	Server-1	Shared	1.1.1.1

□ NAME
- □ Shared
  - □ DATACENTER_DG
    - □ DC_FW_DG
      - □ FW-1_DG
  - □ REGIONAL_DG
    - □ OFFICE_FW_DG

Review the screenshots and consider the following information:
• FW-1 is assigned to the FW-1_DG device group, and FW-2 is assigned to OFFICE_FW_DG.
• There are no objects configured in REGIONAL_DG and OFFICE_FW_DG device groups.
Which IP address will be pushed to the firewalls inside Address Object Server-1?

A. Server-1 on FW-1 will have IP 1.1.1.1. Server-1 will not be pushed to FW-2.
B. Server-1 on FW-1 will have IP 3.3.3.3. Server-1 will not be pushed to FW-2.
C. Server-1 on FW-1 will have IP 2.2.2.2. Server-1 will not be pushed to FW-2.
D. Server-1 on FW-1 will have IP 4.4.4.4. Server-1 on FW-2 will have IP 1.1.1.1.

Answer: C

NEW QUESTION 71
An engineer has been tasked with reviewing traffic logs to find applications the firewall is unable to identify with App-ID. Why would the application field display as incomplete?

A. The client sent a TCP segment with the PUSH flag set.
B. The TCP connection was terminated without identifying any application data.
C. There is insufficient application data after the TCP connection was established.
D. The TCP connection did not fully establish.

Answer: C

NEW QUESTION 76
A network administrator wants to deploy SSL Forward Proxy decryption. What two attributes should a forward trust certificate have? (Choose two.)

A. A subject alternative name
B. A private key
C. A server certificate
D. A certificate authority (CA) certificate

Answer: AC

Explanation:
When deploying SSL Forward Proxy decryption, a forward trust certificate must have a subject alternative name (SAN) and be a server certificate. SAN is an extension to the X.509 standard that allows multiple domain names to be protected by a single SSL/TLS certificate. It is used to identify the domain names or IP addresses that the certificate should be valid for. A private key is also required but it is not mentioned in the options. A certificate authority (CA) certificate is not required as the forward trust certificate itself is a CA certificate.

NEW QUESTION 78
An engineer decides to use Panorama to upgrade devices to PAN-OS 10.2. Which three platforms support PAN-OS 10 2? (Choose three.)

A. PA-5000 Series
B. PA-500
C. PA-800 Series
D. PA-220
E. PA-3400 Series

Answer: CDE

Explanation:
According to the Palo Alto Networks Compatibility Matrix1, the three platforms that support PAN-OS 10.2 are:

- PA-800 Series2
- PA-2202
- PA-3400 Series2

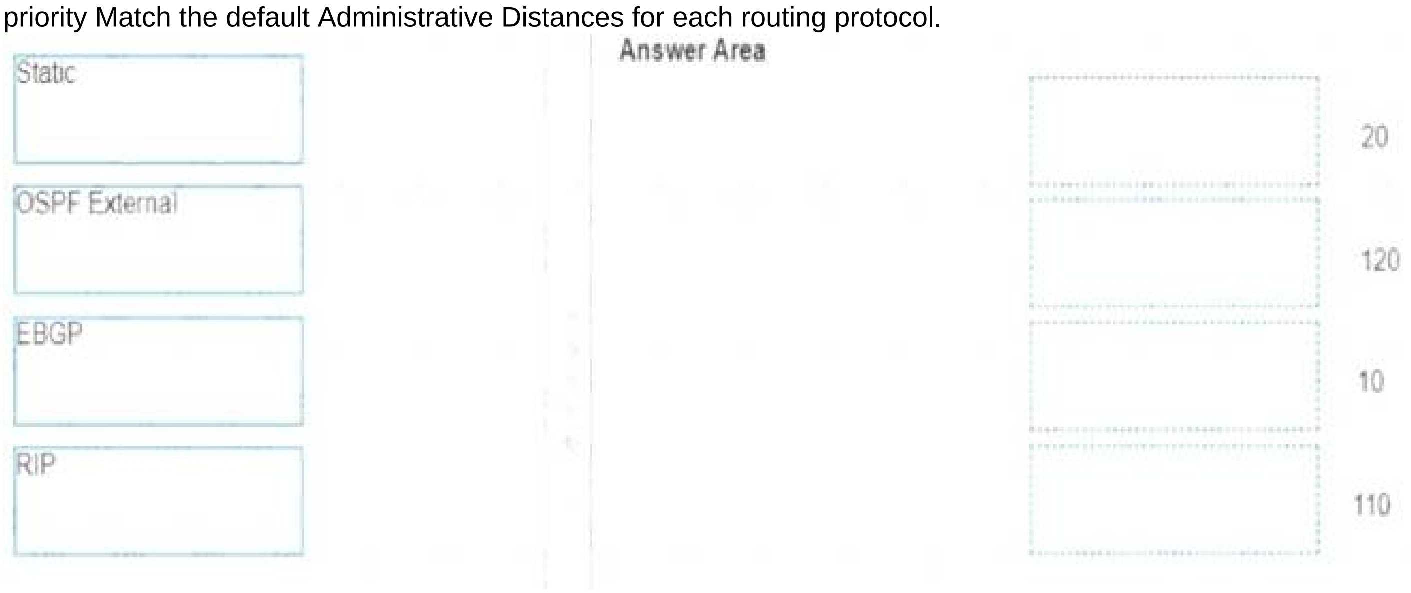
The PA-5000 Series and PA-500 do not support PAN-OS 10.22.
To upgrade devices to PAN-OS 10.2 using Panorama, you need to determine the upgrade path3, upgrade Panorama itself4, and then upgrade the firewalls using Panorama5.

NEW QUESTION 82
A firewall has Security policies from three sources
* 1. locally created policies
* 2. shared device group policies as pre-rules
* 3. the firewall's device group as post-rules
How will the rule order populate once pushed to the firewall?

A. shared device group policies, firewall device group policie
B. local policies.
C. firewall device group policies, local policie
D. shared device group policies
E. shared device group policie
F. local policies, firewall device group policies
G. local policies, firewall device group policies, shared device group policies

Answer: C

NEW QUESTION 84
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

- Static

—Range is 10-240; default is 10.

- OSPF Internal

—Range is 10-240; default is 30.

- OSPF External

—Range is 10-240; default is 110.

- IBGP

—Range is 10-240; default is 200.

- EBGP

—Range is 10-240; default is 20.

- RIP

—Range is 10-240; default is 120.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/virtual-routers

NEW QUESTION 85
A network security administrator has been tasked with deploying User-ID in their organization. What are three valid methods of collecting User-ID information in a network? (Choose three.)

A. Windows User-ID agent
B. GlobalProtect
C. XMLAPI
D. External dynamic list
E. Dynamic user groups

Answer: ABC

Explanation:
User-ID is a feature that enables the firewall to identify users and groups based on their IP addresses, usernames, or other attributes.
There are three valid methods of collecting User-ID information in a network:

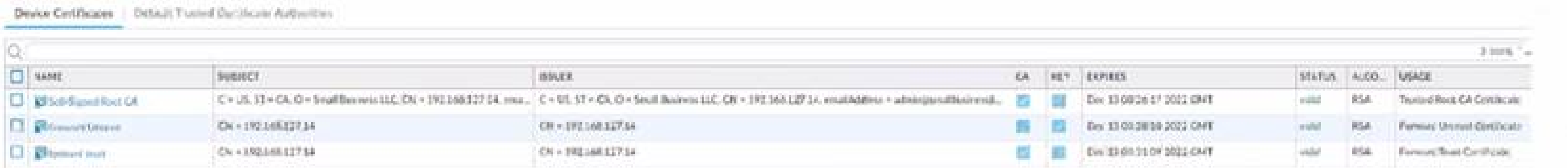
- Windows User-ID agent: This is a software agent that runs on a Windows server and collects user mapping information from Active Directory, Exchange servers, or other sources.
- GlobalProtect: This is a VPN solution that provides secure remote access for users and devices. It also collects user mapping information from endpoints that connect to the firewall using GlobalProtect.
- XMLAPI: This is an application programming interface that allows third-party applications or scripts to send user mapping information to the firewall using XML format.

NEW QUESTION 88
An engineer needs to redistribute User-ID mappings from multiple data centers. Which data flow best describes redistribution of user mappings?

A. Domain Controller to User-ID agent
B. User-ID agent to Panorama
C. User-ID agent to firewall
D. firewall to firewall

Answer: D

NEW QUESTION 92
Review the screenshot of the Certificates page.



□	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...	USAGE
□	Self-Signed Root CA	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, ema...	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, emailAddress = admin@smallbusinessll...	☑	☑	Dec 13 08:26:17 2022 GMT	valid	RSA	Trusted Root CA Certificate
□	Forward Untrust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	Dec 13 03:28:10 2022 GMT	valid	RSA	Forward Untrust Certificate
□	Forward trust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	Dec 13 03:11:09 2022 GMT	valid	RSA	Forward Trust Certificate

An administrator tor a small LLC has created a series of certificates as shown, to use tor a planned Decryption roll out The administrator has also installed the sell-signed root certificate <n all client systems When testing, they noticed that every time a user visited an SSL site they received unsecured website warnings What is the cause of the unsecured website warnings.

A. The forward trust certificate has not been signed by the set-singed root CA certificate
B. The self-signed CA certificate has the same CN as the forward trust and untrust certificates
C. The forward untrust certificate has not been signed by the self-singed root CA certificate
D. The forward trust certificate has not been installed in client systems

Answer: C

NEW QUESTION 95
An administrator is receiving complaints about application performance degradation. After checking the ACC. the administrator observes that there Is an excessive amount of SSL traffic
Which three elements should the administrator configure to address this issue? (Choose three.)

A. QoS on the ingress Interface for the traffic flows
B. An Application Override policy for the SSL traffic
C. A QoS policy for each application ID
D. A QoS profile defining traffic classes
E. QoS on the egress interface for the traffic flows

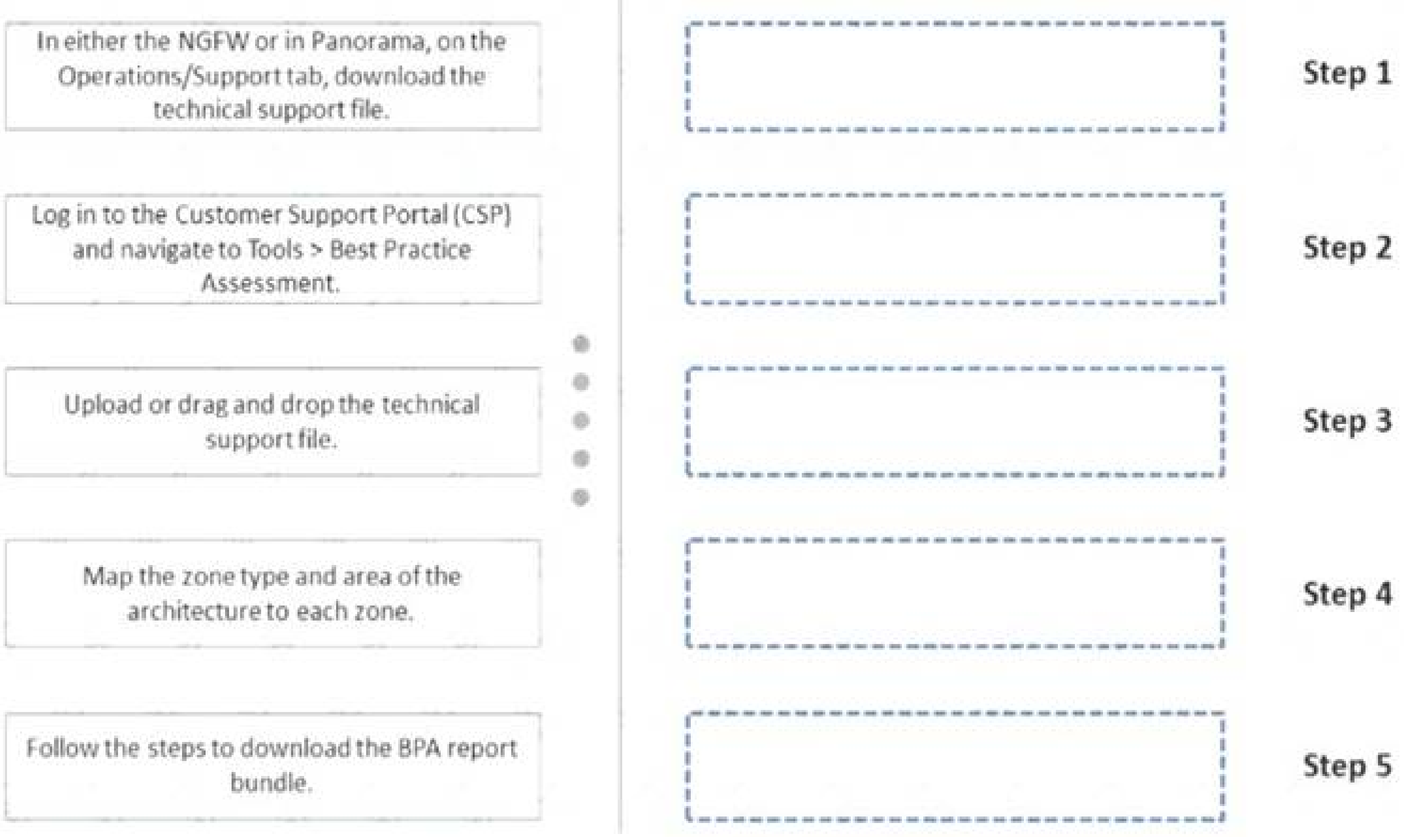
Answer: BCD

NEW QUESTION 99
When planning to configure SSL Froward Proxy on a PA 5260, a user asks how SSL decryption can be implemented using phased approach in alignment with Palo Alto Networks best practices
What should you recommend?

A. Enable SSL decryption for known malicious source IP addresses
B. Enable SSL decryption for source users and known malicious URL categories
C. Enable SSL decryption for malicious source users
D. Enable SSL decryption for known malicious destination IP addresses

Answer: B

NEW QUESTION 104
Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.



In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Upload or drag and drop the technical support file.

Map the zone type and area of the architecture to each zone.

Follow the steps to download the BPA report bundle.

Step 1

Step 2

Step 3

Step 4

Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1. In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.
Step 2. Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment. Step 3. Upload or drag and drop the technical support file.
Step 4. Map the zone type and area of the architecture to each zone. Step 5.Follow the steps to download the BPA report bundle.

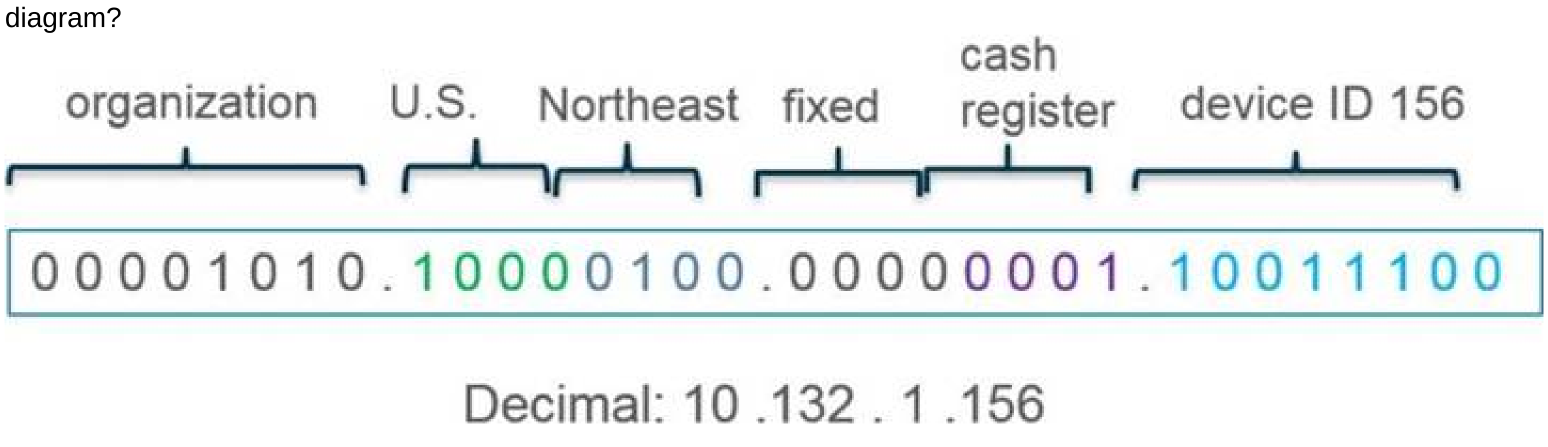
NEW QUESTION 107
The UDP-4501 protocol-port is used between which two GlobalProtect components?

A. GlobalProtect app and GlobalProtect gateway
B. GlobalProtect portal and GlobalProtect gateway
C. GlobalProtect app and GlobalProtect satellite
D. GlobalProtect app and GlobalProtect portal

Answer: A

Explanation:
UDP 4501 Used for IPSec tunnel connections between GlobalProtect apps and gateways. https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/reference-port-number-usag

NEW QUESTION 112
What type of address object would be useful for internal devices where the addressing structure assigns meaning to certain bits in the address, as illustrated in the diagram?



A. IP Netmask
B. IP Wildcard Mask
C. IP Address
D. IP Range

Answer: B

NEW QUESTION 117
A network engineer is troubleshooting a VPN and wants to verify whether the decapsulation/encapsulation counters are increasing. Which CLI command should the engineer run?

A. Show vpn tunnel name | match encap
B. Show vpn flow name <tunnel name>
C. Show running tunnel flow lookup
D. Show vpn ipsec-sa tunnel <tunnel name>

Answer: B

NEW QUESTION 120
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443 A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.
Which combination of service and application, and order of Security policy rules, needs to be configured to allow cJeartext web-browsing traffic to this server on tcp/443?

A. Rule #1 application: web-browsing; service application-default; action: allow Rule #2- application: ssl; service: application-default; action: allow
B. Rule #1: application; web-browsing; service: service-https; action: allow Rule #2 application: ssl; service: application-default, action: allow
C. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl; service: application-default; action: allow
D. Rule tf1 application: ssl; service: application-default; action: allow Rule #2 application; web-browsing; service application-default; action: allow

Answer: B

NEW QUESTION 122
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

A. link requirements
B. the name of the ISP
C. IP Addresses
D. branch and hub locations

Answer: ACD

Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration

NEW QUESTION 123
An engineer has been asked to limit which routes are shared by running two different areas within an OSPF implementation. However, the devices share a common link for communication. Which virtual router configuration supports running multiple instances of the OSPF protocol over a single link?

A. ASBR
B. ECMP
C. OSPFv3
D. OSPF

Answer: C

Explanation:
Support for multiple instances per link—With OSPFv3, you can run multiple instances of the OSPF protocol over a single link. This is accomplished by assigning an OSPFv3 instance ID number. An interface that is assigned to an instance ID drops packets that contain a different ID.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/ospf/ospf-concepts/ospfv3

NEW QUESTION 127
In an existing deployment, an administrator with numerous firewalls and Panorama does not see any WildFire logs in Panorama. Each firewall has an active WildFire subscription On each firewall. WildFire togs are available.
This issue is occurring because forwarding of which type of logs from the firewalls to Panorama is missing?

A. Threat logs
B. Traffic togs
C. System logs
D. WildFire logs

Answer: D

Explanation:
When an administrator has numerous firewalls and Panorama, WildFire logs need to be forwarded from the firewalls to Panorama in order for them to be visible in Panorama. WildFire logs contain information about malicious files that have been detected by WildFire and provide detailed information such as the file's hash value, severity, and other attributes. This information can then be used to help identify threats and take appropriate security measures. Proper configuration of forwarding WildFire logs is essential for monitoring malicious activity and ensuring the security of the network.

NEW QUESTION 129
An administrator is configuring SSL decryption and needs 10 ensure that all certificates for both SSL Inbound inspection and SSL Forward Proxy are installed

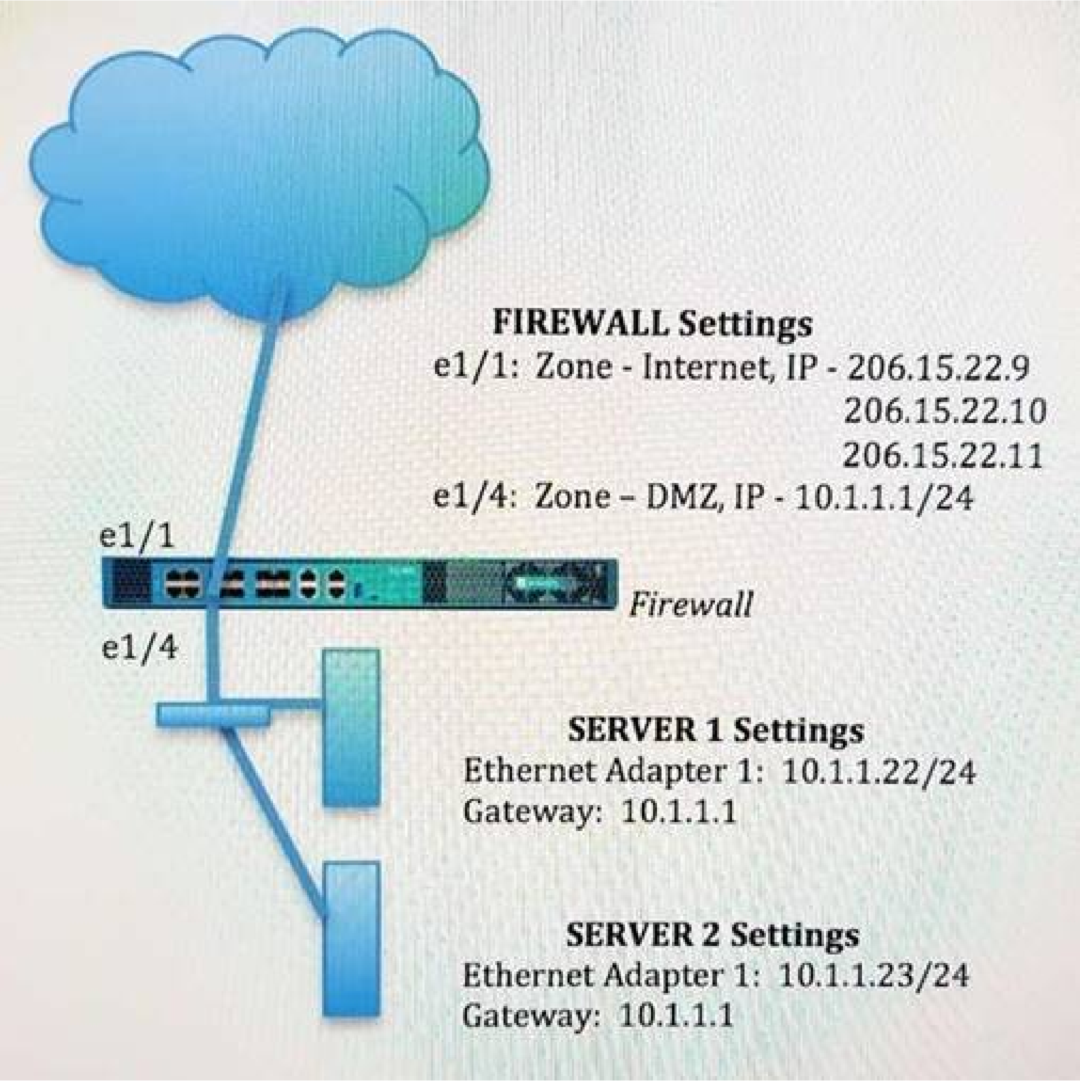
properly on the firewall. When certificates are being imported to the firewall for these purposes, which three certificates require a private key? (Choose three.)

A. Forward Untrust certificate
B. Forward Trust certificate
C. Enterprise Root CA certificate
D. End-entity (leaf) certificate
E. Intermediate certificate(s)

Answer: ABD

Explanation:
This is discussed in the Palo Alto Networks PCNSE Study Guide in Chapter 9: Decryption, under the section "SSL Forward Proxy and Inbound Inspection Certificates":
"When importing SSL decryption certificates, you need to provide private keys for the forward trust, forward untrust, and end-entity (leaf) certificates. You do not need to provide private keys for the root CA and intermediate certificates."

NEW QUESTION 131
An administrator wants multiple web servers In the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22.
Based on the image, which NAT rule will forward web-browsing traffic correctly?

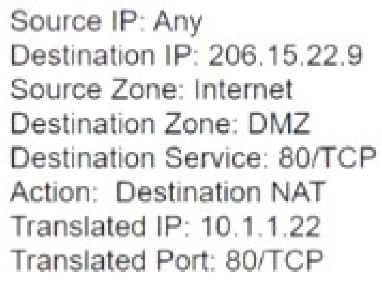


FIREWALL Settings
e1/1: Zone - Internet, IP - 206.15.22.9
206.15.22.10
206.15.22.11
e1/4: Zone – DMZ, IP - 10.1.1.1/24

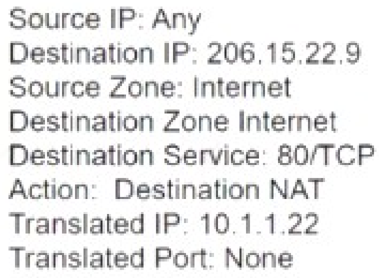
SERVER 1 Settings
Ethernet Adapter 1: 10.1.1.22/24
Gateway: 10.1.1.1

SERVER 2 Settings
Ethernet Adapter 1: 10.1.1.23/24
Gateway: 10.1.1.1

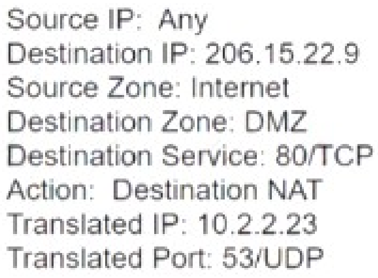
A)


Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP

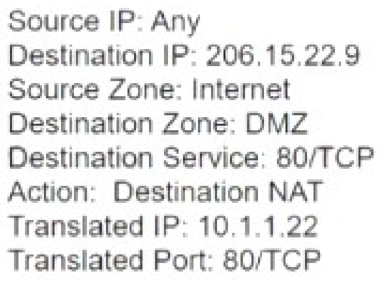
B)


Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

C)


Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

D)



Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP

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

Answer: B

NEW QUESTION 136
A super user is tasked with creating administrator accounts for three contractors. For compliance purposes, all three contractors will be working with different device-groups m their hierarchy to deploy policies and objects.
Which type of role-based access is most appropriate for this project?

A. Create a Dynamic Admin with the Panorama Administrator role.
B. Create a Device Group and Template Admin.
C. Create a Custom Panorama Admin.
D. Create a Dynamic Read only superuser

Answer: C

Explanation:
A Custom Panorama Admin is a type of role-based access that allows a super user to create separate Panorama administrator accounts for each of the three contractors. This will allow each contractor to work with different device-groups in their hierarchy and deploy policies and objects in accordance with the organization's compliance requirements. The Custom Panorama Admin role also allows the super user to assign separate permissions to each contractor's account, granting them access to only the resources they are authorized to use. This type of role-based access is the most appropriate for this project as it will ensure that each contractor is only able to access the resources they need in order to do their job.

NEW QUESTION 141
Where can an administrator see both the management-plane and data-plane CPU utilization in the WebUI?

A. System Resources widget
B. System Logs widget
C. Session Browser
D. General Information widget

Answer: A

Explanation:
The System Resources widget of the Exadata WebUI, displays a real-time overview of the various resources like CPU, Memory, and I/O usage across the entire Exadata Database Machine. It shows the usage of both management-plane and data-plane CPU utilization.
System Resources Widget Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or Panorama). https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/dashboard/dashboard-widgets.html

NEW QUESTION 146
A prospect is eager to conduct a Security Lifecycle Review (SLR) with the aid of the Palo Alto Networks NGFW.
Which interface type is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive?

A. Layer 3
B. Virtual Wire
C. Tap
D. Layer 2

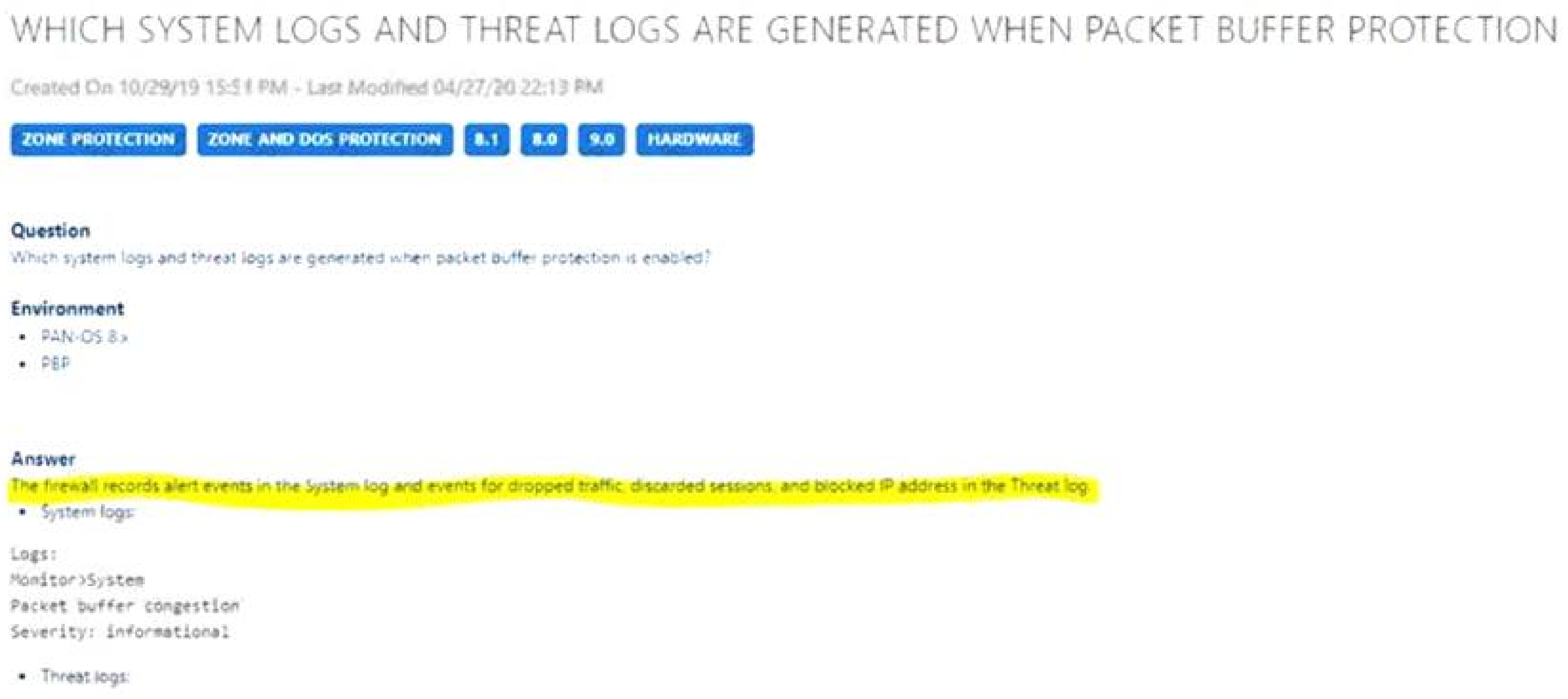
Answer: C

NEW QUESTION 149
Where is information about packet buffer protection logged?

A. Alert entries are in the Alarms lo
B. Entries for dropped traffic, discarded sessions, and blocked IP address are in the Threat log
C. All entries are in the System log
D. Alert entries are in the System lo
E. Entries for dropped traffic, discarded sessions and blocked IP addresses are in the Threat log
F. All entries are in the Alarms log

Answer: D

Explanation:
Graphical user interface, text, application Description automatically generated



WHICH SYSTEM LOGS AND THREAT LOGS ARE GENERATED WHEN PACKET BUFFER PROTECTION

Created On 10/29/19 15:51 PM - Last Modified 04/27/20 22:13 PM

ZONE PROTECTION | ZONE AND DOS PROTECTION | 8.1 | 8.0 | 9.0 | HARDWARE

Question

Which system logs and threat logs are generated when packet buffer protection is enabled?

Environment

- PAN-OS 8.x
- PBP

Answer

The firewall records alert events in the System log and events for dropped traffic, discarded sessions, and blocked IP address in the Threat log.

- System logs:

```
Logs:
Monitor>System
Packet buffer congestion
Severity: informational
```

- Threat logs:

NEW QUESTION 153

How would an administrator configure a Bidirectional Forwarding Detection profile for BGP after enabling the Advance Routing Engine run on PAN-OS 10.2?

A. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Virtual Router > BGP > BFD
B. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Virtual Router > BGP > General > Global BFD Profile
C. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Routing > Logical Routers > BGP > General > Global BFD Profile
D. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Routing > Logical Routers > BGP > BFD

Answer: B

NEW QUESTION 157

When configuring forward error correction (FEC) for PAN-OS SD-WAN, an administrator would turn on the feature inside which type of SD-WAN profile?

A. Certificate profile
B. Path Quality profile
C. SD-WAN Interface profile
D. Traffic Distribution profile

Answer: C

NEW QUESTION 159

Which GlobalProtect component must be configured to enable Clientless VPN?

A. GlobalProtect satellite
B. GlobalProtect app
C. GlobalProtect portal
D. GlobalProtect gateway

Answer: C

Explanation:

Creating the GlobalProtect portal is as simple as letting it know if you have accessed it already. A new gateway for accessing the GlobalProtect portal will appear. Client authentication can be used with an existing one.
https://www.nstec.com/how-to-configure-clientless-vpn-in-palo-alto/#5

NEW QUESTION 160

Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

A. PAN-OS integrated User-ID agent
B. GlobalProtect
C. Windows-based User-ID agent
D. LDAP Server Profile configuration

Answer: B

NEW QUESTION 164

An engineer receives reports from users that applications are not working and that websites are only partially loading in an asymmetric environment. After investigating, the engineer observes the flow_tcp_non_syn_drop counter increasing in the show counters global output.
Which troubleshooting command should the engineer use to work around this issue?

A. set deviceconfig setting tcp asymmetric-path drop

B. set deviceconfig setting session tcp-reject-non-syn no
C. set session tcp-reject-non-syn yes
D. set deviceconfig setting tcp asymmetric-path bypass

Answer: B

Explanation:
To work around this issue, one possible troubleshooting command is set deviceconfig setting session tcp-reject-non-syn no which disables TCP reject non-SYN temporarily (until reboo4t). This command allows non-SYN first packet through without dropping it.
The flow_tcp_non_syn_drop counter increases when the firewall receives packets with the ACK flag set, but not the SYN flag, which indicates asymmetric traffic flow. The tcp-reject-non-syn option enables or disables the firewall to drop non-SYN TCP packets. In this case, disabling the tcp-reject-non-syn option using the "set deviceconfig setting session tcp-reject-non-syn no" command can help work around the issue. This allows the firewall to accept non-SYN packets and create a session for the existing flow.

NEW QUESTION 169
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Link and Path Monitoring Is enabled with the Failure Condition set to "any." There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure Condition set to "all."
Which HA state will the Active firewall go into if ethernet1/1 link goes down due to a failure?

A. Non-functional
B. Passive
C. Active-Secondary
D. Active

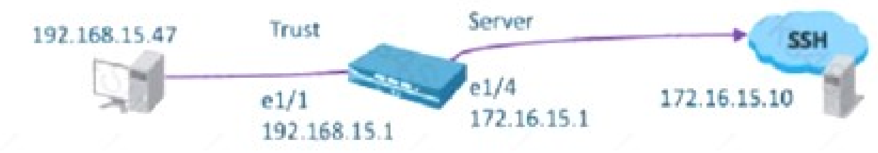
Answer: D

NEW QUESTION 171
When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

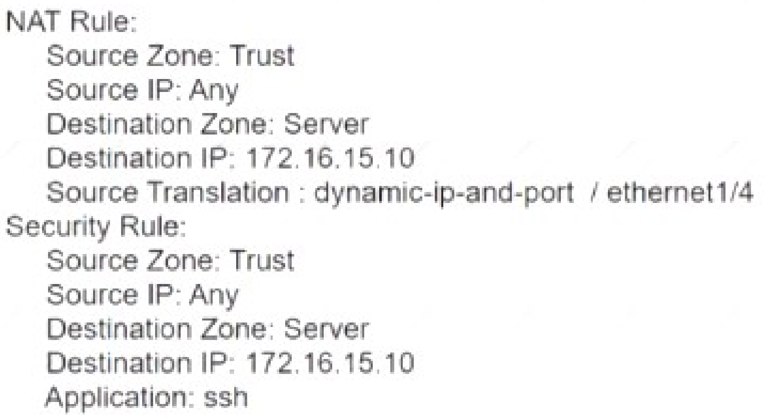
A. The interface must be used for traffic to the required services
B. You must enable DoS and zone protection
C. You must set the interface to Layer 2 Layer 3. or virtual wire
D. You must use a static IP address

Answer: D

NEW QUESTION 174
Refer to the diagram. Users at an internal system want to ssh to the SSH server The server is configured to respond only to the ssh requests coming from IP 172.16.16.1.
In order to reach the SSH server only from the Trust zone, which Security rule and NAT rule must be configured on the firewall?

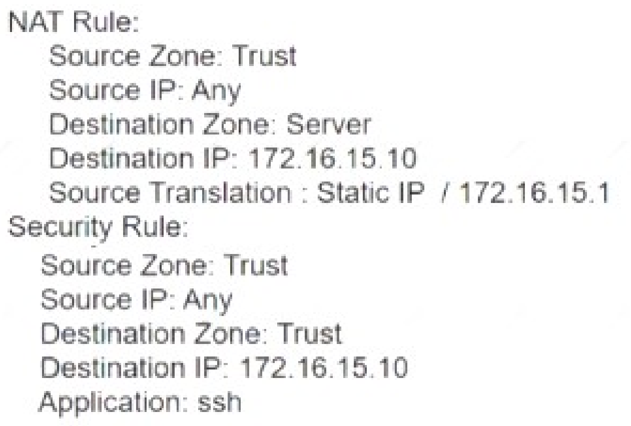


A)



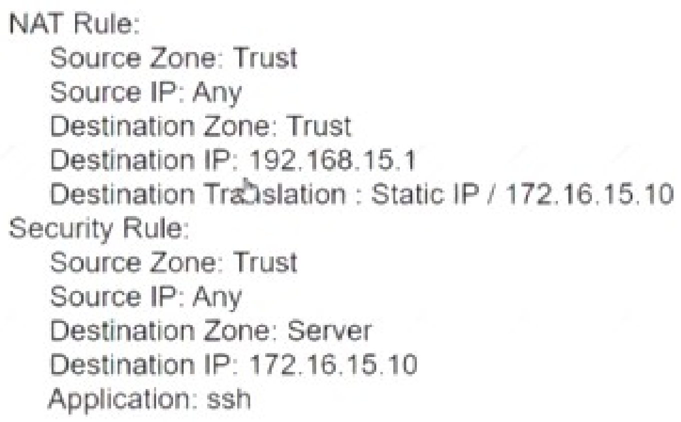
```
NAT Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Server
    Destination IP: 172.16.15.10
    Source Translation : dynamic-ip-and-port  / ethernet1/4
Security Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Server
    Destination IP: 172.16.15.10
    Application: ssh
```

B)



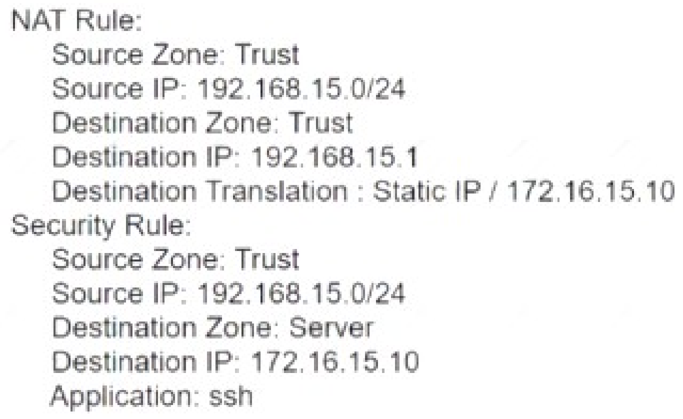
```
NAT Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Server
    Destination IP: 172.16.15.10
    Source Translation : Static IP  / 172.16.15.1
Security Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Trust
    Destination IP: 172.16.15.10
    Application: ssh
```

C)



```
NAT Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Trust
    Destination IP: 192.168.15.1
    Destination Translation : Static IP / 172.16.15.10
Security Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Server
    Destination IP: 172.16.15.10
    Application: ssh
```

D)



```
NAT Rule:
    Source Zone: Trust
    Source IP: 192.168.15.0/24
    Destination Zone: Trust
    Destination IP: 192.168.15.1
    Destination Translation : Static IP / 172.16.15.10
Security Rule:
    Source Zone: Trust
    Source IP: 192.168.15.0/24
    Destination Zone: Server
    Destination IP: 172.16.15.10
    Application: ssh
```

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

Answer: C

NEW QUESTION 179
Which steps should an engineer take to forward system logs to email?

A. Create a new email profile under Device > server profiles; then navigate to Objects > Log Forwarding profile > set log type to system and the add email profile.
B. Enable log forwarding under the email profile in the Objects tab.
C. Create a new email profile under Device > server profiles: then navigate to Device > Log Settings > System and add the email profile under email.
D. Enable log forwarding under the email profile in the Device tab.

Answer: C

NEW QUESTION 182
When using certificate authentication for firewall administration, which method is used for authorization?

A. Radius
B. LDAP
C. Kerberos
D. Local

Answer: A

NEW QUESTION 185
What is a correct statement regarding administrative authentication using external services with a local authorization method?

A. Prior to PAN-OS 10.2. an administrator used the firewall to manage role assignments, but access domains have not been supported by this method.
B. Starting with PAN-OS 10.2. an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.
C. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.
D. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall.

Answer: B

NEW QUESTION 187
A network administrator plans a Prisma Access deployment with three service connections, each with a BGP peering to a CPE. The administrator needs to minimize the BGP configuration and management overhead on on-prem network devices.
What should the administrator implement?

A. target service connection for traffic steering
B. summarized BGP routes before advertising
C. hot potato routing
D. default routing

Answer: C

NEW QUESTION 192
What is the best description of the HA4 Keep-Alive Threshold (ms)?

A. the maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational.
B. The time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall
C. the timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional.
D. The timeframe that the local firewall wait before going to Active state when another cluster member is preventing the cluster from fully synchronizing.

Answer: D

NEW QUESTION 193
A customer is replacing their legacy remote access VPN solution The current solution is in place to secure only internet egress for the connected clients Prisma Access has been selected to replace the current remote access VPN solution During onboarding the following options and licenses were selected and enabled
- Prisma Access for Remote Networks 300Mbps
- Prisma Access for Mobile Users 1500 Users
- Cortex Data Lake 2TB
- Trusted Zones trust
- Untrusted Zones untrust
- Parent Device Group shared
How can you configure Prisma Access to provide the same level of access as the current VPN solution?

A. Configure mobile users with trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
B. Configure mobile users with a service connection and trust-to-trust Security policy rules to allow the desired traffic outbound to the internet
C. Configure remote networks with a service connection and trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
D. Configure remote networks with trust-to-trust Security policy rules to allow the desired traffic outbound to the internet

Answer: D

NEW QUESTION 195
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

A. Use the debug dataplane packet-diag set capture stage firewall file command.
B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
C. Use the debug dataplane packet-diag set capture stage management file command.
D. Use the tcpdump command.

Answer: D

NEW QUESTION 199
The manager of the network security team has asked you to help configure the company's Security Profiles according to Palo Alto Networks best practice As part of that effort, the manager has assigned you the Vulnerability Protection profile for the internet gateway firewall.
Which action and packet-capture setting for items of high severity and critical severity best matches Palo Alto Networks best practice?

A. action 'reset-both' and packet capture 'extended-capture'
B. action 'default' and packet capture 'single-packet'
C. action 'reset-both' and packet capture 'single-packet'
D. action 'reset-server' and packet capture 'disable'

Answer: C

Explanation:
https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices/best-practice-internet-gate "Enable extended-capture for critical, high, and medium severity events and single-packet capture for low severity events. "
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-vulner

NEW QUESTION 202
An administrator is using Panorama to manage me and suspects an IKE Crypto mismatch between peers, from the firewalls to Panorama. However, pre-existing logs from the firewalls are not appearing in Panorama.
Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

A. Export the log database.
B. Use the import option to pull logs.
C. Use the ACC to consolidate the logs.
D. Use the scp logdb export command.

Answer: D

NEW QUESTION 207
An administrator is attempting to create policies tor deployment of a device group and template stack. When creating the policies, the zone drop down list does not include the required zone.
What must the administrator do to correct this issue?

A. Specify the target device as the master device in the device group
B. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings
C. Add the template as a reference template in the device group
D. Add a firewall to both the device group and the template

Answer: D

NEW QUESTION 212
An engineer is in the planning stages of deploying User-ID in a diverse directory services environment. Which server OS platforms can be used for server monitoring with User-ID?

A. Microsoft Terminal Server, Red Hat Linux, and Microsoft Active Directory
B. Microsoft Active Directory, Red Hat Linux, and Microsoft Exchange
C. Microsoft Exchange, Microsoft Active Directory, and Novell eDirectory
D. Novell eDirectory, Microsoft Terminal Server, and Microsoft Active Directory

Answer: B

Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/user-id-agent/which-servers-can-the-user-id-agent-moni

NEW QUESTION 216
An administrator is required to create an application-based Security policy rule to allow Evernote. The Evernote application implicitly uses SSL and web browsing. What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

A. Add the Evernote application to the Security policy rule, then add a second Security policy rule containing both HTTP and SSL.
B. Add the HTTP, SSL, and Evernote applications to the same Security policy
C. Add only the Evernote application to the Security policy rule.
D. Create an Application Override using TCP ports 443 and 80.

Answer: C

NEW QUESTION 220
Which configuration task is best for reducing load on the management plane?

A. Disable logging on the default deny rule
B. Enable session logging at start
C. Disable pre-defined reports
D. Set the URL filtering action to send alerts

Answer: C

NEW QUESTION 222
What happens when an A/P firewall cluster synchronizes IPsec tunnel security associations (SAs)?

A. Phase 1 and Phase 2 SAs are synchronized over HA3 links.
B. Phase 1 SAs are synchronized over HA1 links.
C. Phase 2 SAs are synchronized over HA2 links.
D. Phase 1 and Phase 2 SAs are synchronized over HA2 links.

Answer: C

NEW QUESTION 224
A firewall administrator wants to avoid overflowing the company syslog server with traffic logs. What should the administrator do to prevent the forwarding of DNS traffic logs to syslog?

A. Disable logging on security rules allowing DNS.
B. Go to the Log Forwarding profile used to forward traffic logs to syslo
C. Then, under traffic logs match list, create a new filter with application not equal to DNS.
D. Create a security rule to deny DNS traffic with the syslog server in the destination
E. Go to the Log Forwarding profile used to forward traffic logs to syslo
F. Then, under traffic logs match list, create a new filter with application equal to DNS.

Answer: D

NEW QUESTION 227
Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?

A. Measure and monitor the CPU consumption of the firewall data plane to ensure that each firewall is properly sized to support DoS and zone protection
B. Create a zone protection profile with flood protection configured to defend an entire egress zone against SY
C. ICMP ICMPv6, UD
D. and other IP flood attacks
E. Add a WildFire subscription to activate DoS and zone protection features
F. Replace the hardware firewall because DoS and zone protection are not available with VM-Series systems

Answer: A

Explanation:
* 1 https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/dos-and-zone-prote
* 2 https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/ta
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection.html

NEW QUESTION 229
In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

A. wildcard server certificate
B. enterprise CA certificate
C. client certificate
D. server certificate
E. self-signed CA certificate

Answer: BE

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-forward-proxy.html

NEW QUESTION 234
A network security administrator wants to begin inspecting bulk user HTTPS traffic flows egressing out of the internet edge firewall. Which certificate is the best choice to configure as an SSL Forward Trust certificate?

A. A self-signed Certificate Authority certificate generated by the firewall
B. A Machine Certificate for the firewall signed by the organization's PKI
C. A web server certificate signed by the organization's PKI
D. A subordinate Certificate Authority certificate signed by the organization's PKI

Answer: A

NEW QUESTION 235
What are two best practices for incorporating new and modified App-IDs? (Choose two)

A. Configure a security policy rule to allow new App-IDs that might have network-wide impact
B. Study the release notes and install new App-IDs if they are determined to have low impact
C. Perform a Best Practice Assessment to evaluate the impact or the new or modified App-IDs
D. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs

Answer: AB

NEW QUESTION 236
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?

A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096 in the "Tag Allowed" field of the V-Wire object.
B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed" field of the V-Wire objec
C. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffi
D. Assign each interface/sub interface to a unique zone.
E. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router.The physical Layer 3 interface would handle untagged traffi
F. Assign each interface/subinterface t
G. unique zon
H. Do not assign any interface an IP address.
I. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN I
J. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffi
K. Assign each interface/sub interface to a unique zone.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags. VLAN tag 0 indicates untagged traffic.You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

NEW QUESTION 239
How does Panorama prompt VMWare NSX to quarantine an infected VM?

A. Email Server Profile
B. Syslog Sewer Profile
C. SNMP Server Profile
D. HTTP Server Profile

Answer: B

NEW QUESTION 243
A company requires that a specific set of ciphers be used when remotely managing their Palo Alto Networks appliances. Which profile should be configured in order to achieve this?

A. SSH Service profile
B. SSL/TLS Service profile
C. Decryption profile

D. Certificate profile

Answer: A

NEW QUESTION 247
A network engineer has discovered that asymmetric routing is causing a Palo Alto Networks firewall to drop traffic. The network architecture cannot be changed to correct this.
Which two actions can be taken on the firewall to allow the dropped traffic permanently? (Choose two.)

A. Navigate to Network > Zone Protection Click AddSelect Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to No Set "Asymmetric Path" to Bypass
B. > set session tcp-reject-non-syn no
C. Navigate to Network > Zone Protection Click AddSelect Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to Global Set "Asymmetric Path" to Global
D. # set deviceconfig setting session tcp-reject-non-syn no

Answer: CD

NEW QUESTION 252
What are three valid qualifiers for a Decryption Policy Rule match? (Choose three.)

A. Destination Zone
B. App-ID
C. Custom URL Category
D. User-ID
E. Source Interface

Answer: ACD

NEW QUESTION 257
An administrator is attempting to create policies for deployment of a device group and template stack. When creating the policies, the zone drop-down list does not include the required zone.
What can the administrator do to correct this issue?

A. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings.
B. Add a firewall to both the device group and the template.
C. Specify the target device as the master device in the device group.
D. Add the template as a reference template in the device group.

Answer: D

Explanation:
In order to see what is in a template, the device-group needs the template referenced. Even if you add the firewall to both the template and device-group, the device-group will not see what is in the template.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNfeCAG

NEW QUESTION 261
You need to allow users to access the office-suite applications of their choice. How should you configure the firewall to allow access to any office-suite application?

A. Create an Application Group and add Office 365, Evernote Google Docs and Libre Office
B. Create an Application Group and add business-systems to it.
C. Create an Application Filter and name it Office Programs, then filter it on the office programs subcategory.
D. Create an Application Filter and name it Office Programs then filter on the business-systems category.

Answer: C

NEW QUESTION 262
In a Panorama template which three types of objects are configurable? (Choose three)

A. certificate profiles
B. HIP objects
C. QoS profiles
D. security profiles
E. interface management profiles

Answer: ACE

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewall

NEW QUESTION 264
Which Panorama feature protects logs against data loss if a Panorama server fails?

A. Panorama HA automatically ensures that no logs are lost if a server fails inside the HA Cluster.
B. Panorama Collector Group with Log Redundancy ensures that no logs are lost if a server fails inside the Collector Group.
C. Panorama HA with Log Redundancy ensures that no logs are lost if a server fails inside the HA Cluster.

D. Panorama Collector Group automatically ensures that no logs are lost if a server fails inside the Collector Group

Answer: A

NEW QUESTION 268
A firewall administrator notices that many Host Sweep scan attacks are being allowed through the firewall sourced from the outside zone. What should the firewall administrator do to mitigate this type of attack?

A. Create a DOS Protection profile with SYN Flood protection enabled and apply it to all rules allowing traffic from the outside zone
B. Enable packet buffer protection in the outside zone.
C. Create a Security rule to deny all ICMP traffic from the outside zone.
D. Create a Zone Protection profile, enable reconnaissance protection, set action to Block, and apply it to the outside zone.

Answer: D

NEW QUESTION 273
An engineer is configuring SSL Inbound Inspection for public access to a company's application. Which certificate(s) need to be installed on the firewall to ensure that inspection is performed successfully?

A. Self-signed CA and End-entity certificate
B. Root CA and Intermediate CA(s)
C. Self-signed certificate with exportable private key
D. Intermediate CA (s) and End-entity certificate

Answer: D

NEW QUESTION 276
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Path Monitoring has been enabled with a Failure Condition of "any." A path group is configured with Failure Condition of "all" and contains a destination IP of 8.8.8.8 and 4.2.2.2 with a Ping Interval of 500ms and a Ping count of 3.
Which scenario will cause the Active firewall to fail over?

A. IP address 8.8.8.8 is unreachable for 1 second.
B. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 1 second.
C. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 2 seconds
D. IP address 4.2.2.2 is unreachable for 2 seconds.

Answer: C

NEW QUESTION 278
The same route appears in the routing table three times using three different protocols Which mechanism determines how the firewall chooses which route to use?

A. Administrative distance
B. Round Robin load balancing
C. Order in the routing table
D. Metric

Answer: A

Explanation:
Administrative distance is the measure of trustworthiness of a routing protocol. It is used to determine the best path when multiple routes to the same destination exist. The route with the lowest administrative distance is chosen as the best route.
When the same route appears in the routing table three times using three different protocols, the mechanism that determines which route the firewall chooses to use is the administrative distance. This is explained in the Palo Alto Networks PCNSE Study Guide in Chapter 6: Routing, under the section "Route Selection": "Administrative distance is a value assigned to each protocol that the firewall uses to determine which route to use if multiple protocols provide routes to the same destination. The route with the lowest administrative distance is preferred."

NEW QUESTION 279
The firewall identifies a popular application as an unKnown-tcp.
Which two options are available to identify the application? (Choose two.)

A. Create a custom application.
B. Submit an App-ID request to Palo Alto Networks.
C. Create a custom object for the application server.
D. Create a Security policy to identify the custom application.

Answer: AB

NEW QUESTION 283
......

Relate Links

100% Pass Your PCNSE Exam with Exambible Prep Materials

https://www.exambible.com/PCNSE-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/