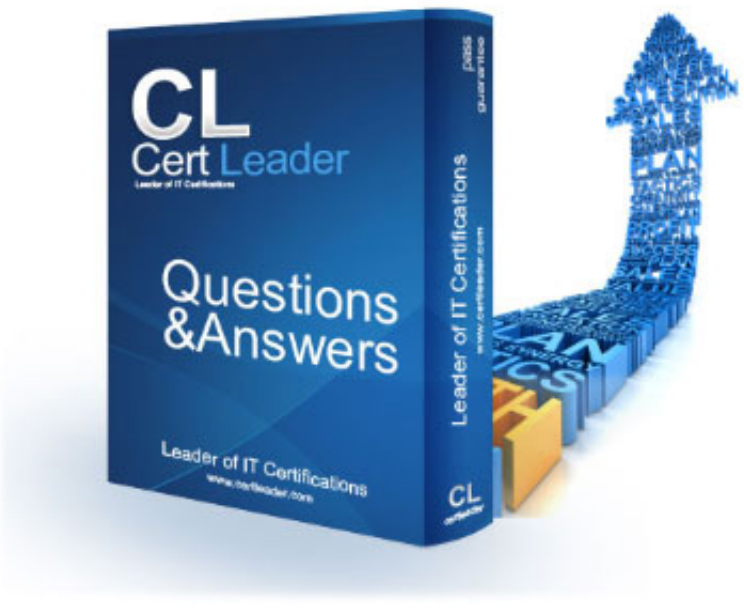
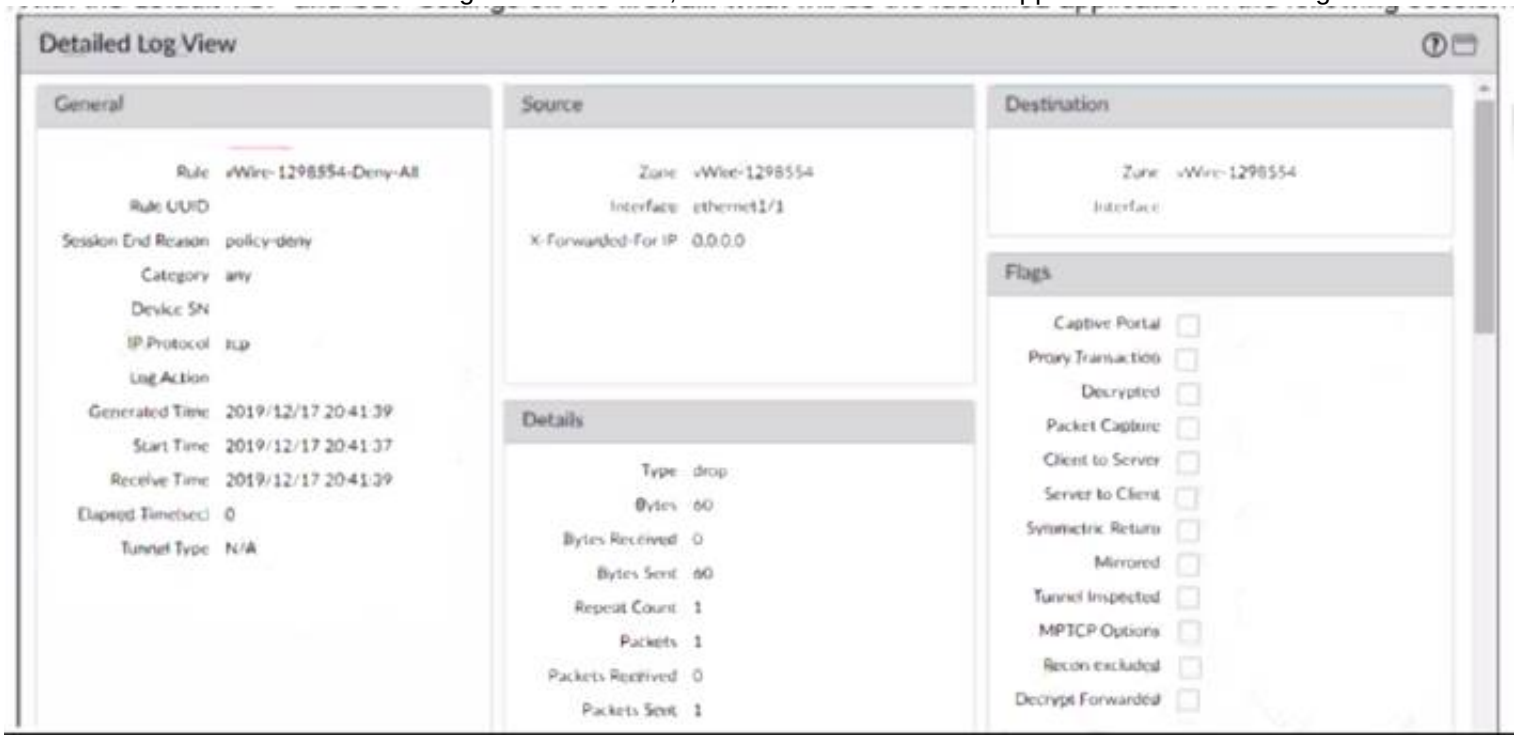
PCNSE Dumps

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

https://www.certleader.com/PCNSE-dumps.html



NEW QUESTION 1
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?



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

Answer: D

Explanation:
Traffic didnt match any other policies and so landed at the implicit "deny all" policy. If it's deny all, the traffic was dropped before the application could be determined. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

NEW QUESTION 2
An engineer is troubleshooting a traffic-routing issue. What is the correct packet-flow sequence?

A. PBF > Zone Protection Profiles > Packet Buffer Protection
B. BGP > PBF > NAT
C. PBF > Static route > Security policy enforcement
D. NAT > Security policy enforcement > OSPF

Answer: C

Explanation:
The correct packet-flow sequence is C. PBF > Static route > Security policy enforcement. This sequence describes the order of operations that the firewall performs when processing a packet. PBF stands for
Policy-Based Forwarding, which is a feature that allows the firewall to override the routing table and forward
traffic based on the source and destination addresses, application, user, or service. PBF is evaluated before the static route lookup, which is the default method of forwarding traffic based on the destination address and the longest prefix match. Security policy enforcement is the stage where the firewall applies the security policy rules to allow or block traffic based on various criteria, such as zone, address, port, user, application, etc12. References: Policy-Based Forwarding, Packet Flow Sequence in PAN-OS

NEW QUESTION 3
After implementing a new NGFW, a firewall engineer sees a VoIP traffic issue going through the firewall After troubleshooting the engineer finds that the firewall performs NAT on the voice packets payload and opens dynamic pinholes for media ports
What can the engineer do to solve the VoIP traffic issue?

A. Disable ALG under H.323 application
B. Increase the TCP timeout under H.323 application
C. Increase the TCP timeout under SIP application
D. Disable ALG under SIP application

Answer: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/disable-the-sip-application-level-gateway-a

NEW QUESTION 4
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: C

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. The following link has a video that demonstrates that B is the correct answer.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNfeCAG

NEW QUESTION 5
Which statement about High Availability timer settings is true?

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

Answer: D

Explanation:
Recommended: Use for typical failover timer settings. Unless you're sure that you need different settings, the best practice is to use the Recommended settings.
Aggressive: Use for faster failover timer settings.
Advanced: Allows you to customize the values to suit your network requirement for each of the following timers:

NEW QUESTION 6
A security engineer needs firewall management access on a trusted interface.
Which three settings are required on an SSL/TLS Service Profile to provide secure Web UI authentication? (Choose three.)

A. Minimum TLS version
B. Certificate
C. Encryption Algorithm
D. Maximum TLS version
E. Authentication Algorithm

Answer: ABD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssltls-service

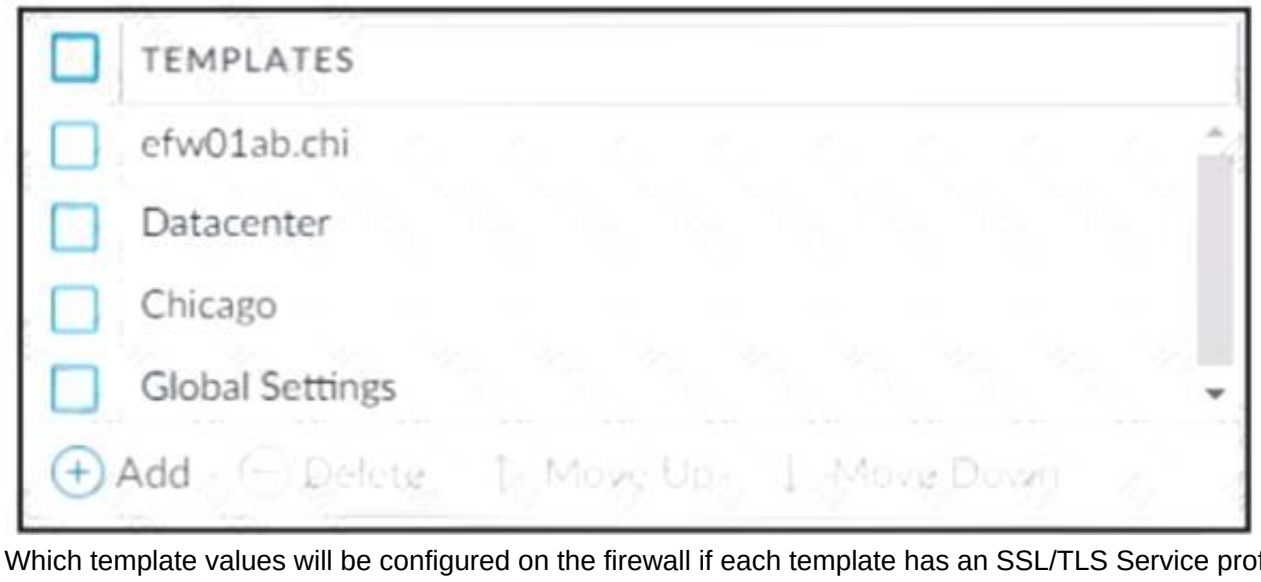
NEW QUESTION 7
In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

A. 1 to 4 hours
B. 6 to 12 hours
C. 24 hours
D. 36 hours

Answer: B

Explanation:
Schedule content updates so that they download-and-install automatically. Then, set a Threshold that determines the amount of time the firewall waits before installing the latest content. In a security-first network, schedule a six to twelve hour threshold.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-thr
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/best-practices-for

NEW QUESTION 8
Which template values will be configured on the firewall if each template has an SSL to be deployed. The template stack should consist of four templates arranged according to the diagram.



Which template values will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management?

A. Values in Datacenter
B. Values in efwOlab.chi
C. Values in Global Settings

D. Values in Chicago

Answer: D

Explanation:
The template stack should consist of four templates arranged according to the diagram. The template values that will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management will be the values in Chicago. This is because the SSL/TLS Service profile is configured in the Chicago template, which is the highest priority template in the stack. The firewall will inherit the settings from the highest priority template that has the setting configured, and ignore the settings from the lower priority templates that have the same setting configured. Therefore, the values in Datacenter, efwOlab.chi, and Global Settings will not be applied to the firewall. References:

- [Template Stack Configuration]
- [Template Stack Priority]

NEW QUESTION 9
Why would a traffic log list an application as "not-applicable”?

A. The firewall denied the traffic before the application match could be performed.
B. The TCP connection terminated without identifying any application data
C. There was not enough application data after the TCP connection was established
D. The application is not a known Palo Alto Networks App-ID.

Answer: A

Explanation:
traffic log would list an application as “not-applicable” if the firewall denied the traffic before the application match could be performed. This can happen if the traffic matches a security rule that is set to deny based on any parameter other than the application, such as source, destination, port, service, etc1. In this case, the firewall does not inspect the application data and discards the traffic, resulting in a “not-applicable” entry in the application field of the traffic log1.

NEW QUESTION 10
An engineer is configuring a firewall with three interfaces:
• MGT connects to a switch with internet access.
• Ethernet1/1 connects to an edge router.
• Ethernet1/2 connects to a visualization network.
The engineer needs to configure dynamic updates to use a dataplane interface for internet traffic. What should be configured in Setup > Services > Service Route Configuration to allow this traffic?

A. Set DNS and Palo Alto Networks Services to use the ethernet1/1 source interface.
B. Set DNS and Palo Alto Networks Services to use the ethernet1/2 source interface.
C. Set DNS and Palo Alto Networks Services to use the MGT source interface.
D. Set DDNS and Palo Alto Networks Services to use the MGT source interface.

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0

NEW QUESTION 10
An engineer troubleshoots a Panorama-managed firewall that is unable to reach the DNS servers configured via a global template. As a troubleshooting step, the engineer needs to configure a local DNS server in place of the template value.
Which two actions can be taken to ensure that only the specific firewall is affected during this process? (Choose two)

A. Configure the DNS server locally on the firewall.
B. Change the DNS server on the global template.
C. Override the DNS server on the template stack.
D. Configure a service route for DNS on a different interface.

Answer: AC

Explanation:
To override a device and network setting applied by a template, you can either configure the setting locally on the firewall or override the setting on the template stack. Configuring the setting locally on the firewall will
copy the setting to the local configuration of the device and will no longer be controlled by the template. Overriding the setting on the template stack will apply the setting to all the firewalls that are assigned to the template stack, unless the setting is also overridden locally on a firewall. Changing the setting on the global template will affect all the firewalls that inherit the setting from the template, which is not desirable in this scenario. Configuring a service route for DNS on a different interface will not change the DNS server address, but only the interface that the firewall uses to reach the DNS server. References:

- Override a Template Setting
- Overriding Panorama Template settings

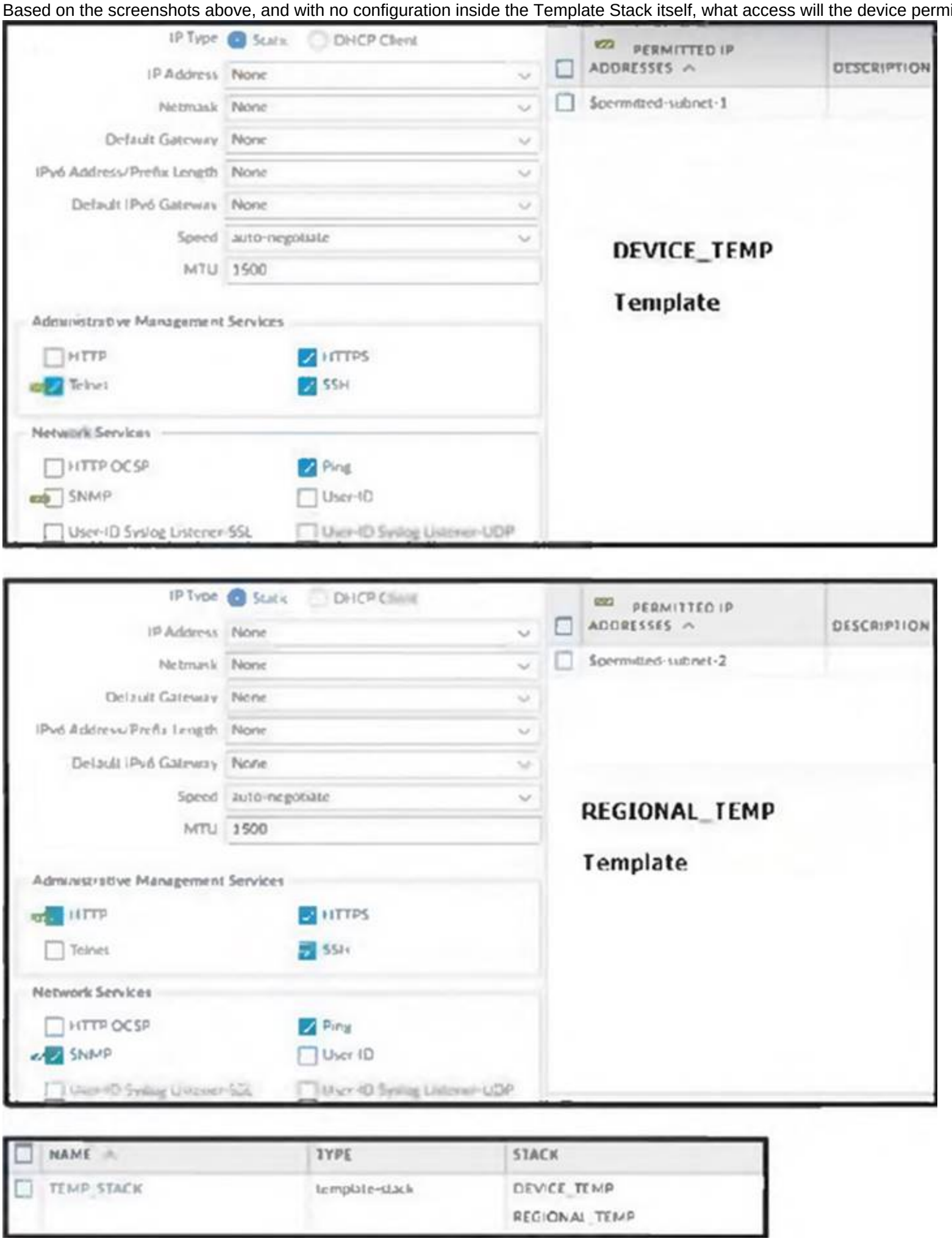
NEW QUESTION 14
What can be used as an Action when creating a Policy-Based Forwarding (PBF) policy?

A. Deny
B. Discard
C. Allow
D. Next VR

Answer: B

Explanation:
Set the Action to take when matching a packet: Forward—Directs the packet to the specified Egress Interface.
Forward to VSYS (On a firewall enabled for multiple virtual systems)—Select the virtual system to which to forward the packet.
Discard—Drops the packet.
No PBF—Excludes packets that match the criteria for source, destination, application, or service defined in the rule. Matching packets use the route table instead of PBF; the firewall uses the route table to exclude the matched traffic from the redirected port.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/policy-based-forwarding/create-a-policy-ba

NEW QUESTION 19
Based on the screenshots above, and with no configuration inside the Template Stack itself, what access will the device permit on its Management port?



A. The firewall will allow HTTP Telnet, HTTPS, SSH, and Ping from IP addresses defined as$permitted-subnet-1.
B. The firewall will allow HTTP Telnet, HTTPS, SSH, and Ping from IP addresses defined as$permitted-subnet-2.
C. The firewall will allow HTTP, Telnet, SNMP, HTTPS, SSH and Ping from IP addresses defined as$permitted-subnet-1 and $permitted-subnet-2.
D. The firewall will allow HTTP, Telnet, HTTPS, SSH, and Ping from IP addresses defined as$permitted-subnet-1 and $permitted-subnet-2.

Answer: A

Explanation:
https://live.paloaltonetworks.com/t5/panorama-discussions/panorama-force-template-value-option/td-p/496620 "- Force Template Value will as the name suggest remove any local configuratio and apply the value define the panorama template. But this is valid only for overlapping configuration" "You need to be careful, what is actually defined in the template. For example - if you decide to enable HA in the template, but after that you decide to not push it with template and just disable it again (remove the check from the "Enable HA" checkbox). This still will be part of the template, because now your template is explicitely defining HA disabled. If you made a change in the template, and later decide that you don't want to control this setting with template, you need to revert the config by clicking the green bar

next to the changed value"

NEW QUESTION 20
Where can a service route be configured for a specific destination IP?

A. Use Netw ork > Virtual Routers, select the Virtual Router > Static Routes > IPv4
B. Use Device > Setup > Services > Services
C. Use Device > Setup > Services > Service Route Configuration > Customize > Destination
D. Use Device > Setup > Services > Service Route Configuration > Customize > IPv4

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0

NEW QUESTION 24
A firewall engineer creates a destination static NAT rule to allow traffic from the internet to a webserver hosted behind the edge firewall. The pre-NAT IP address of the server is 153.6 12.10, and the post-NAT IP address is 192.168.10.10. Refer to the routing and interfaces information below.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1				none	none	Untagged	none	none
ethernet1/2	Layer3	Inside		192.168.1.1/24	default	Untagged	none	Inside
ethernet1/3	Layer3			Dynamic-DHCP Client	default	Untagged	none	Outside

Virtual Router - default

Router Settings
Static Routes
Redistribution Profile
RIP
OSPF
OSPFv3
BGP
Multicast

IPv4 IPv6

3 items

NAME	DESTINATION	INTERFACE	Next Hop TYPE	Next Hop VALUE	ADMIN DISTANCE	M...	ROUTE TABLE
route1	153.6.12.0/27	ethernet1/2	ip-address	192.168.1.2	default	10	unicast
route2	192.168.10.0/24	ethernet1/2	ip-address	192.168.1.2	default	10	unicast
default	0.0.0.0/0	ethernet1/3	ip-address	207.212.10.1	default	10	unicast

Add Delete Clone

OK Cancel

What should the NAT rule destination zone be set to?

A. None
B. Outside
C. DMZ
D. Inside

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/nat-configuration-examples/destin

NEW QUESTION 28
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: BD

Explanation:
The two attributes that a forward trust certificate should have for SSL Forward Proxy decryption are:
B: A private key. This is the key that the firewall uses to sign the certificates that it generates for the decrypted sessions. The private key must be securely stored on the firewall and not shared with anyone1.
D: A certificate authority (CA) certificate. This is the certificate that the firewall uses to issue the certificates for the decrypted sessions. The CA certificate must be trusted by the client browsers and devices that receive the certificates from the firewall1.

NEW QUESTION 30
What is the best definition of the Heartbeat Interval?

A. The interval in milliseconds between hello packets

B. The frequency at which the HA peers check link or path availability
C. The frequency at which the HA peers exchange ping
D. The interval during which the firewall will remain active following a link monitor failure

Answer: C

Explanation:
The firewalls exchange hello messages and heartbeats at configurable intervals to verify that the peer firewall is responsive and operational. Hello messages are sent from one peer to the other to verify the state of the firewall. The heartbeat is an ICMP ping to the HA peer. A response from the peer indicates that the firewalls are connected and responsive.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClUcCAK
"A "heartbeat-interval" CLI command was added to the election settings for HA, this interval has a 1000ms minimum for all Palo Alto Networks platforms and is an ICMP ping to the other device through the HA control link." https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClMaCAK

NEW QUESTION 35
Which two profiles should be configured when sharing tags from threat logs with a remote User-ID agent? (Choose two.)

A. Log Ingestion
B. HTTP
C. Log Forwarding
D. LDAP

Answer: BC

Explanation:
>Threat logs, create a log forwarding profile to define how you want the firewall or Panorama to handle logs.
>Configure an HTTP server profile to forward logs to a remote User-ID agent. > Select the log forwarding profile you created then select this server profile as the HTTP server profile https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/use-auto-tagging-to-automate-security-actio

NEW QUESTION 40
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 allows the firewall to identify and classify users and groups on the network based on their usernames, IP addresses, and other attributes1. User-ID information can be collected from various sources, such as:

- A: Windows User-ID agent: A software agent that runs on a Windows server and collects user information from Active Directory domain controllers, Exchange servers, or eDirectory servers2. The agent then sends the user information to the firewall or Panorama for user mapping2.
- B: GlobalProtect: A software agent that runs on the endpoints and provides secure VPN access to the network3. GlobalProtect also collects user information from the endpoints and sends it to the firewall or Panorama for user mapping4.
- C: XMLAPI: An application programming interface that allows external systems or scripts to send user information to the firewall or Panorama in XML format. The XMLAPI can be used to integrate with third-party systems, such as identity providers, captive portals, or custom applications.

NEW QUESTION 42
An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.
What should an administrator configure to route interesting traffic through the VPN tunnel?

A. Proxy IDs
B. GRE Encapsulation
C. Tunnel Monitor
D. ToS Header

Answer: A

Explanation:
An administrator should configure proxy IDs to route interesting traffic through the VPN tunnel when the peer device is a policy-based VPN device. Proxy IDs are used to identify the traffic that belongs to a particular IPSec VPN and to direct it to the appropriate tunnel. Proxy IDs consist of a local IP address, a remote IP address, and an application (protocol and port numbers). Each proxy ID is considered to be a VPN tunnel and is counted towards the IPSec VPN tunnel capacity of the firewall. Proxy IDs are required for IKEv1 VPNs and optional for IKEv2 VPNs. If the proxy ID is not configured, the firewall uses the default values of source IP: 0.0.0.0/0, destination IP: 0.0.0.0/0, and application: any, which may not match the peer's policy and result in a failure to establish the VPN connection.
References:

- Proxy ID for IPSec VPN
- Set Up an IPSec Tunnel

NEW QUESTION 46
Which two key exchange algorithms consume the most resources when decrypting SSL traffic? (Choose two.)

A. ECDSA
B. ECDHE

C. RSA
D. DHE

Answer: BD

Explanation:
The two key exchange algorithms that consume the most resources when decrypting SSL traffic are ECDHE and DHE. These are both Diffie-Hellman based algorithms that enable perfect forward secrecy (PFS), which means that they generate a new and unique session key for each SSL/TLS session, and do not reuse any previous keys. This enhances the security of the encrypted communication, but also increases the computational cost and complexity of the key exchange process. ECDHE stands for Elliptic Curve Diffie-Hellman Ephemeral, which uses elliptic curve cryptography (ECC) to generate the session key. DHE stands for Diffie-Hellman Ephemeral, which uses modular arithmetic to generate the session key. Both ECDHE and DHE require more CPU and memory resources than RSA, which is a non-PFS algorithm that uses public and private keys to encrypt and decrypt the session key123. References: Key Exchange Algorithms, Best Practices for Enabling SSL Decryption, PCNSE Study Guide (page 60)

NEW QUESTION 51
An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0. What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

A. No client configuration is required for explicit proxy, which simplifies the deployment complexity.
B. Explicit proxy supports interception of traffic using non-standard HTTPS ports.
C. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request.
D. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.

Answer: CD

Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-us https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

NEW QUESTION 52
Which three options does Panorama offer for deploying dynamic updates to its managed devices? (Choose three.)

A. Check dependencies
B. Schedules
C. Verify
D. Revert content
E. Install

Answer: BDE

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de

NEW QUESTION 53
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 connection?

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

Answer: B

Explanation:
When the peer device will act as the initiator and none of the peer addresses are known, the administrator can enable Passive Mode to establish the VPN connection. Passive Mode tells the firewall to wait for the peer device to initiate the VPN connection. The other options are incorrect. Option A, setting up certificate authentication, would require the administrator to know the peer device's certificate. Option C, using the Dynamic IP address type, would require the administrator to know the peer device's dynamic IP address.
Option D, configuring the peer address as an FQDN, would require the administrator to know the peer device's fully qualified domain name.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClIGCA0

NEW QUESTION 56
When an engineer configures an active/active high availability pair, which two links can they use? (Choose two)

A. HSCI-C
B. Console Backup
C. HA3
D. HA2 backup

Answer: CD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha/prerequisit
These are the two links that can be used to configure an active/active high availability pair. An active/active high availability pair consists of two firewalls that are both active and share the traffic load between them1. To configure an active/active high availability pair, the following links are required2:

- HA1: This is the control link that is used for exchanging heartbeat messages and configuration synchronization between the firewalls. It can be a dedicated

interface or a subinterface. It can also have a backup link for redundancy.

- HA2: This is the data link that is used for forwarding sessions from one firewall to another in case of failover or load balancing. It can be a dedicated interface or a subinterface. It can also have a backup link for redundancy.
- HA3: This is the session owner synchronization link that is used for synchronizing session information between the firewalls in different virtual systems. It can be a dedicated interface or a subinterface. It is only required for active/active high availability pairs, not for active/passive pairs.

NEW QUESTION 61
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. Active-Secondary
B. Non-functional
C. Passive
D. Active

Answer: D

NEW QUESTION 64
An enterprise Information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems. However, a recent phishing campaign against the organization has prompted Information Security to look for more controls that can secure access to critical assets. For users that need to access these systems. Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA.
What should the enterprise do to use PAN-OS MFA?

A. Configure a Captive Portal authentication policy that uses an authentication sequence.
B. Configure a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile.
C. Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy.
D. Use a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns.

Answer: A

Explanation:
To use PAN-OS multi-factor authentication (MFA) to secure access to critical assets, the enterprise should configure a Captive Portal authentication policy that uses an authentication sequence. An authentication sequence is a feature that allows the firewall to enforce multiple authentication methods (factors) for users who access sensitive services or applications. An authentication sequence can include up to four factors, such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication. The firewall can integrate with MFA vendors through RADIUS or vendor APIs to provide the additional factors12.
To configure an authentication sequence, the enterprise needs to create an authentication profile for each factor and then add them to the sequence in the desired order. The enterprise also needs to create a Captive Portal authentication policy that matches the traffic that requires MFA and applies the authentication sequence to it. The Captive Portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The Captive Portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button34.
When a user tries to access a service or application that matches the Captive Portal authentication policy, the firewall redirects the user to the Captive Portal web form for the first factor. After the user successfully authenticates for the first factor, the firewall prompts the user for the second factor through RADIUS or vendor API integration. The firewall repeats this process until all factors in the sequence are completed or until one factor fails. If all factors are completed successfully, the firewall allows the user to access the service or application. If one factor fails, the firewall denies access and logs an event56.
Configuring a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile is not sufficient to use PAN-OS MFA. This option only provides one factor of authentication through RADIUS integration with an MFA vendor. To use multiple factors of authentication, an authentication sequence is required.
Creating an authentication profile and assigning another authentication factor to be used by a Captive Portal authentication policy is not correct to use PAN-OS MFA. This option does not specify how to create or apply an authentication sequence, which is necessary for enforcing multiple factors of authentication.
Using a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns is not relevant to use PAN-OS MFA. This option is a feature of Palo Alto Networks Cortex XDR™ that helps protect endpoints from credential theft by malicious actors. It does not provide any MFA functionality for accessing critical assets.
References: Authentication Sequence, Configure Multi-Factor Authentication, Configure an Authenticatio Portal, Create an Authentication Profile, Create an Authentication Sequence, Create a Captive Portal Authentication Policy, [Credential Phishing Agent]

NEW QUESTION 68
If an administrator wants to apply QoS to traffic based on source, what must be specified in a QoS policy rule?

A. Post-NAT destination address
B. Pre-NAT destination address
C. Post-NAT source address
D. Pre-NAT source address

Answer: C

Explanation:
If an administrator wants to apply QoS to traffic based on source, they must specify the post-NAT source address in a QoS policy rule. This is because QoS is enforced on traffic as it egresses the firewall, and the firewall applies NAT rules before QoS rules. Therefore, the firewall will match the QoS policy rule based on the translated source address, not the original source address. If the administrator uses the pre-NAT source address in the QoS policy rule, the firewall will not be able to identify the traffic correctly and apply the desired QoS treatment. References:

- QoS Policy
- Configure QoS

NEW QUESTION 73
Which GlobalProtect gateway selling is required to enable split-tunneling by access route, destination domain, and application?

A. No Direct Access to local networks

B. Tunnel mode
C. iPSec mode
D. Satellite mode

Answer: B

NEW QUESTION 78
A company wants to add threat prevention to the network without redesigning the network routing. What are two best practice deployment modes for the firewall? (Choose two.)

A. VirtualWire
B. Layer3
C. TAP
D. Layer2

Answer: AD

Explanation:
A and D are the best practice deployment modes for the firewall if the company wants to add threat prevention to the network without redesigning the network routing. This is because these modes allow the firewall to act as a transparent device that does not affect the existing network topology or routing1.
A: VirtualWire mode allows the firewall to be inserted into any existing network segment without changing the IP addressing or routing of that segment2. The firewall inspects traffic between two interfaces that are configured as a pair, called a virtual wire. The firewall applies security policies to the traffic and forwards it to the same interface from which it was received2.
D: Layer 2 mode allows the firewall to act as a switch that forwards traffic based on MAC addresses3. The firewall inspects traffic between interfaces that are configured as Layer 2 interfaces and belong to the same VLAN. The firewall applies security policies to the traffic and forwards it to the appropriate interface based on the MAC address table3.
Verified References:
1: https://www.garlandtechnology.com/blog/whats-your-palo-alto-ngfw-deployment-plan
2: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/virtual-wire
3: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/layer-2.htm

NEW QUESTION 80
Which three items must be configured to implement application override? (Choose three)

A. Custom app
B. Security policy rule
C. Application override policy rule
D. Decryption policy rule
E. Application filter

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies-application-override
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PPDrCAO

NEW QUESTION 81
An administrator receives the following error message:
"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192.168 33 33/24 type IPv4 address protocol 0 port 0, received remote id 172.16 33.33/24 type IPv4 address protocol 0 port 0."
How should the administrator identify the root cause of this error message?

A. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate
B. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure
C. Check whether the VPN peer on one end is set up correctly using policy-based VPN
D. In the IPSec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers.

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-me The VPN peer on one end is using policy-based VPN. You must configure a Proxy ID on the Palo Alto
Networks firewall.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-me

NEW QUESTION 82
What must be configured to apply tags automatically based on User-ID logs?

A. Device ID
B. Log Forwarding profile
C. Group mapping
D. Log settings

Answer: B

Explanation:
To apply tags automatically based on User-ID logs, the engineer must configure a Log Forwarding profile that specifies the criteria for matching the logs and the tags to apply. The Log Forwarding profile can be attached to a security policy rule or a decryption policy rule to enable auto-tagging for the traffic that matches the rule. The tags can then be used for dynamic address groups, policy enforcement, or
reporting1. References: Use Auto-Tagging to Automate Security Actions, PCNSE Study Guide (page 49)

NEW QUESTION 85
An engineer configures SSL decryption in order to have more visibility to the internal users' traffic when it is regressing the firewall.
Which three types of interfaces support SSL Forward Proxy? (Choose three.)

A. High availability (HA)
B. Layer 3
C. Layer 2
D. Tap
E. Virtual Wire

Answer: BCE

Explanation:
PAN-OS can decrypt and inspect SSL inbound and outbound connections going through the firewall. SSL decryption can occur on interfaces in virtual wire, Layer 2 or Layer 3 mode https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClmyCAC

NEW QUESTION 87
Phase two of a VPN will not establish a connection. The peer is using a policy-based VPN configuration. What part of the configuration should the engineer verify?

A. IKE Crypto Profile
B. Security policy
C. Proxy-IDs
D. PAN-OS versions

Answer: C

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClbXCAS https://live.paloaltonetworks.com/t5/general-topics/phase-2-tunnel-is-not-up/td-p/424789

NEW QUESTION 89
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

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/globalprote GlobalProtect is a VPN solution that provides secure remote access to corporate networks. When a user connects to GlobalProtect, their identity is verified against an LDAP server. This ensures that all IP address-to-user mappings are explicitly known.

NEW QUESTION 90
An engineer manages a high availability network and requires fast failover of the routing protocols. The engineer decides to implement BFD.
Which three dynamic routing protocols support BFD? (Choose three.)

A. OSPF
B. RIP
C. BGP
D. IGRP
E. OSPFv3 virtual link

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/bfd/bfd-overview/bfd-for-dynamic-ro

NEW QUESTION 92
The decision to upgrade PAN-OS has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when attempting the install.
When performing an upgrade on Panorama to PAN-OS. what is the potential cause of a failed install?

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

Answer: A

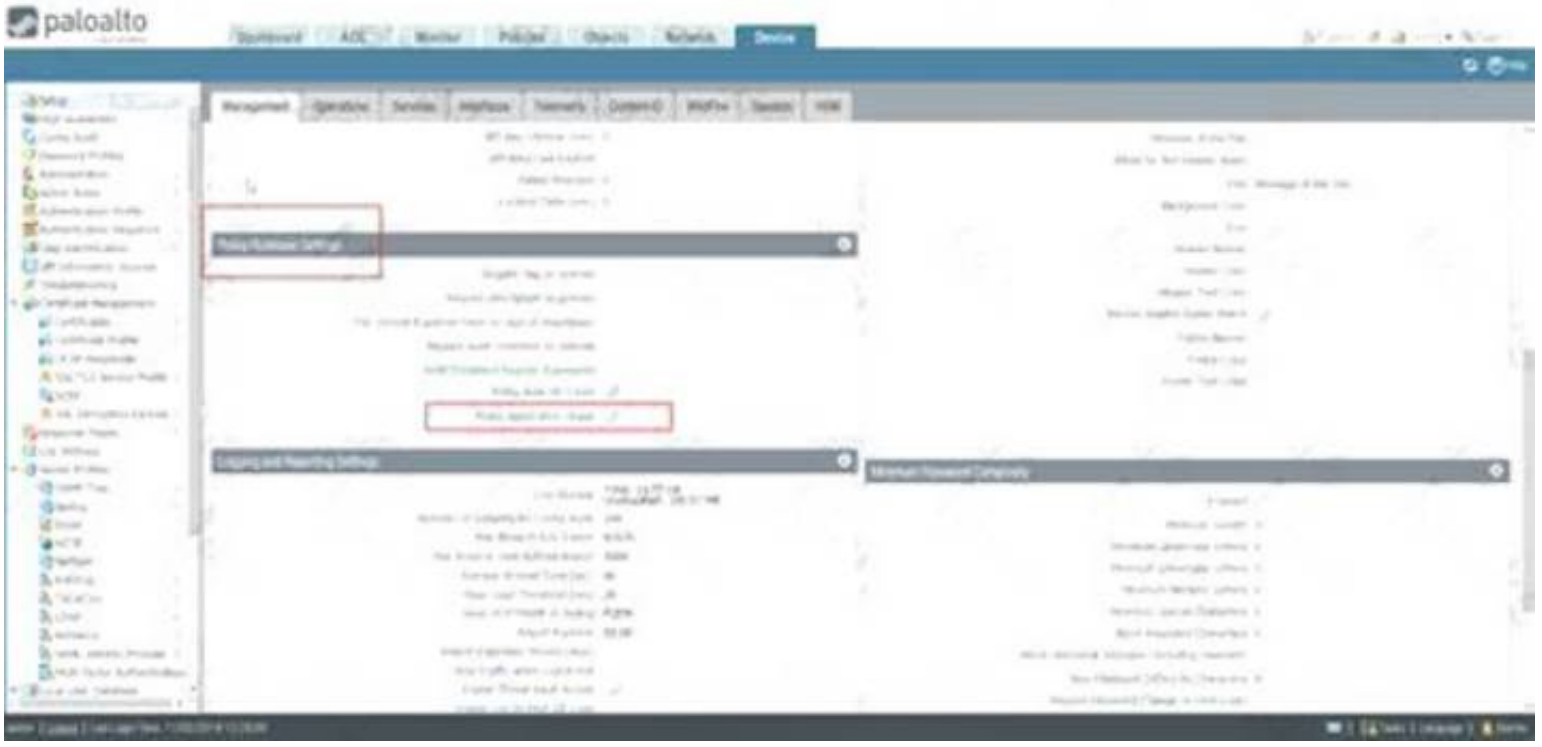
Explanation:
One of the potential causes of a failed install when upgrading Panorama to PAN-OS is having outdated plugins. Plugins are software extensions that enable Panorama to interact with Palo Alto Networks cloud services and third-party services. Plugins have dependencies on specific PAN-OS versions, so they must be updated before or after upgrading Panorama, depending on the plugin compatibility matrix2. If the plugins are not updated accordingly, the upgrade process may fail or cause issues with Panorama
functionality3. References: Panorama Plugins Upgrade/Downgrade Considerations, Troubleshoot Your Panorama Upgrade, PCNSE Study Guide (page 54)

NEW QUESTION 93
In the New App Viewer under Policy Optimizer, what does the compare option for a specific rule allow an administrator to compare?

A. The running configuration with the candidate configuration of the firewall
B. Applications configured in the rule with applications seen from traffic matching the same rule
C. Applications configured in the rule with their dependencies
D. The security rule with any other security rule selected

Answer: B

Explanation:
The compare option for a specific rule in the New App Viewer under Policy Optimizer allows an administrator to compare the applications configured in the rule with the applications seen from traffic matching the same rule. This helps the administrator to identify any new applications that are not explicitly defined in the rule, but are implicitly allowed by the firewall based on the dependencies of the configured applications. The compare option also shows the usage statistics and risk levels of the applications, and provides suggestions for optimizing the rule by adding, removing, or replacing applications12. References: New App Viewer (Policy Optimizer), PCNSE Study Guide (page 47)
Why use Security Policy Optimizer and what are the benefits?



NEW QUESTION 94
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. Create an Application Override using TCP ports 443 and 80.
C. Add the HTT
D. SS
E. and Evernote applications to the same Security policy.
F. Add only the Evernote application to the Security policy rule.

Answer: D

Explanation:
https://live.paloaltonetworks.com/t5/blogs/what-is-application-dependency/ba-p/344330
To create an application-based Security policy rule to allow Evernote, the administrator only needs to add the Evernote application to the Security policy rule. The Evernote application is a predefined App-ID that identifies the traffic generated by the Evernote client or web interface. The Evernote application implicitly uses SSL and web browsing as dependencies, which means that the firewall automatically allows these applications when the Evernote application is allowed. Therefore, there is no need to add HTTP, SSL, or web browsing applications to the same Security policy rule. Adding these applications would broaden the scope of the rule and potentially allow unwanted traffic12. References: App-ID Overview, Create a Security Policy Rule

NEW QUESTION 98
Which DoS Protection Profile detects and prevents session exhaustion attacks against specific destinations?

A. Resource Protection
B. TCP Port Scan Protection
C. Packet Based Attack Protection
D. Packet Buffer Protection

Answer: A

Explanation:

IP flood thresholds, you can also use DoS Protection profiles to detect and prevent session exhaustion attacks in which a large number of hosts (bots) establish as many sessions as possible to consume a target's resources. On the profile's Resources Protection tab, you can set the maximum number of concurrent sessions that the device(s) defined in the DoS Protection policy rule to which you apply the profile can receive. When the number of concurrent sessions reaches its maximum limit, new sessions are dropped.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/

NEW QUESTION 102
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PCNSE Exam with Our Prep Materials Via below:

https://www.certleader.com/PCNSE-dumps.html