

Paloalto-Networks

Exam Questions PCNSE

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



NEW QUESTION 1

An engineer must configure the Decryption Broker feature

Which Decryption Broker security chain supports bi-directional traffic flow?

- A. Layer 2 security chain
- B. Layer 3 security chain
- C. Transparent Bridge security chain
- D. Transparent Proxy security chain

Answer: B

Explanation:

Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

NEW QUESTION 2

Which log type will help the engineer verify whether packet buffer protection was activated?

- A. Data Filtering
- B. Configuration
- C. Threat
- D. Traffic

Answer: C

Explanation:

The log type that will help the engineer verify whether packet buffer protection was activated is Threat Logs. Threat Logs are logs generated by the Palo Alto Networks firewall when it detects a malicious activity on the network. These logs contain information about the source, destination, and type of threat detected. They also contain information about the packet buffer protection that was activated in response to the detected threat. This information can help the engineer verify that packet buffer protection was activated and determine which actions were taken in response to the detected threat.

NEW QUESTION 3

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 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 engineer is deploying multiple firewalls with common configuration in Panorama. What are two benefits of using nested device groups? (Choose two.)

- A. Inherit settings from the Shared group
- B. Inherit IPSec crypto profiles
- C. Inherit all Security policy rules and objects
- D. Inherit parent Security policy rules and objects

Answer: BD

Explanation:

* B. Inherit IPSec crypto profiles

This is correct because IPSec crypto profiles are one of the objects that can be inherited from a parent device group1. You can also create IPSec crypto profiles for use in shared or device group policy1.

* D. Inherit parent Security policy rules and objects

This is correct because Security policy rules and objects are also inheritable from a parent device group1. You can also create Security policy rules and objects for use in shared or device group policy1.

NEW QUESTION 6

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 MFA1?

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

Answer: C

NEW QUESTION 7

A company with already deployed Palo Alto firewalls has purchased their first Panorama server. The security team has already configured all firewalls with the Panorama IP address and added all the firewall serial numbers in Panorama. What are the next steps to migrate configuration from the firewalls to Panorama?

- A. Use API calls to retrieve the configuration directly from the managed devices
- B. Export Named Configuration Snapshot on each firewall followed by Import Named Configuration Snapshot in Panorama
- C. Import Device Configuration to Panorama followed by Export or Push Device Config Bundle
- D. Use the Firewall Migration plugin to retrieve the configuration directly from the managed devices

Answer: C

NEW QUESTION 8

Which benefit do policy rule UUIDs 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

A firewall administrator has been tasked with ensuring that all Panorama-managed firewalls forward traffic logs to Panorama. In which section is this configured?

- A. Panorama > Managed Devices
- B. Monitor > Logs > Traffic
- C. Device Groups > Objects > Log Forwarding
- D. Templates > Device > Log Settings

Answer: C

NEW QUESTION 10

An engineer is creating a template and wants to use variables to standardize the configuration across a large number of devices. Which two variable types can be defined? (Choose two.)

- A. Path group
- B. Zone
- C. IP netmask
- D. FQDN

Answer: CD

NEW QUESTION 10

An engineer needs to permit XML API access to a firewall for automation on a network segment that is routed through a Layer 3 subinterface on a Palo Alto Networks firewall. However, this network segment cannot access the dedicated management interface due to the Security policy. Without changing the existing access to the management interface, how can the engineer fulfill this request?

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

Answer: B

NEW QUESTION 12

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 faster failover timer settings.
- C. Use the Recommended timer for faster failover timer settings.
- D. Use the Aggressive timer for faster failover timer settings.

Answer:

C

NEW QUESTION 14

Place the steps in the WildFire process workflow in their correct order.

The firewall hashes the file and looks for a verdict in the WildFire database. However, the firewall does not find a match.

Wildfire uses static analysis based on machine learning to analyze the file in order to classify malicious features.

Regardless of the verdict, WildFire uses its heuristic engine to examine the file and determines that the file exhibits suspicious behavior.

WildFire generates a new DNS, URL categorization, and antivirus signature for the new threat.

Answer Area

FIRST

SECOND

THIRD

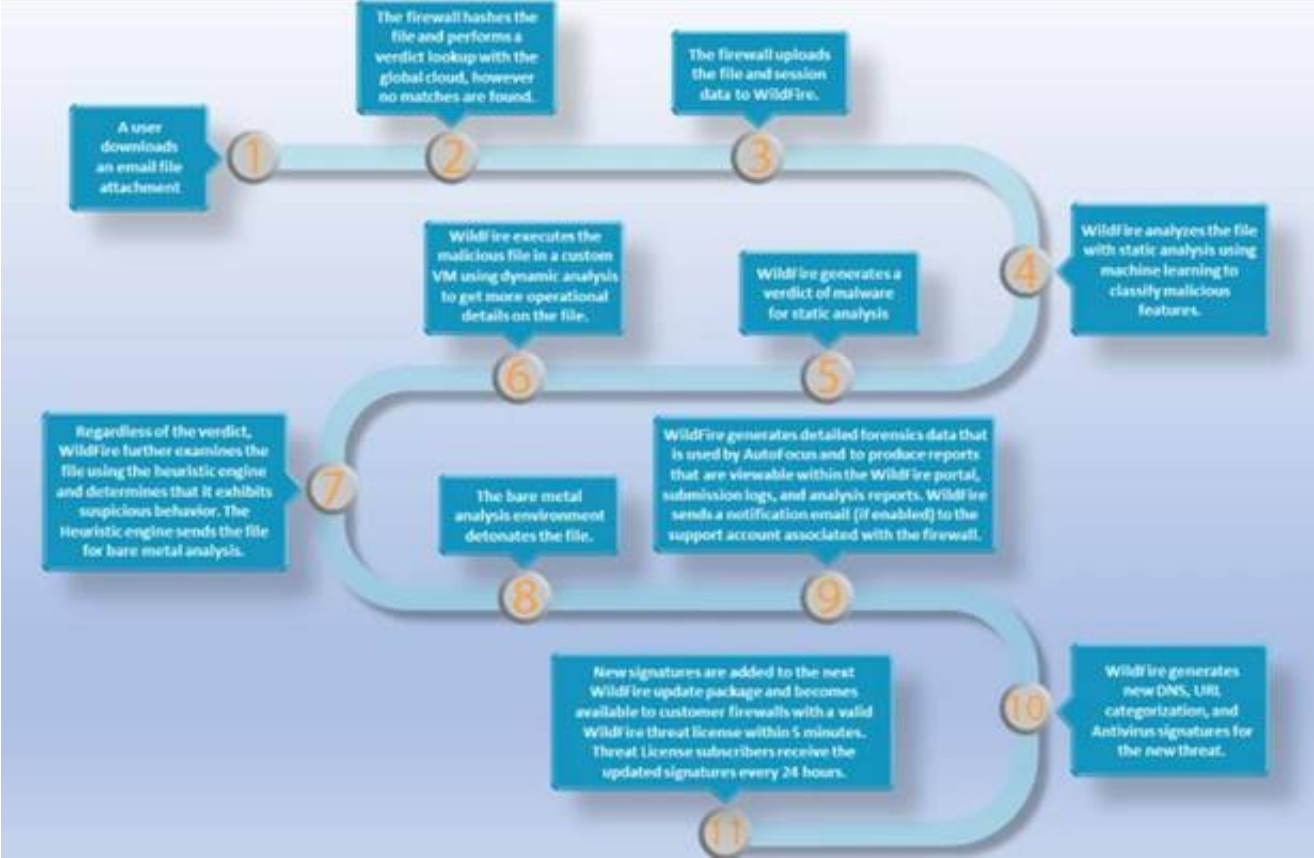
FOURTH

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Timeline Description automatically generated



<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html>

NEW QUESTION 16

A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.

Which two steps are likely to mitigate the issue? (Choose TWO)

- A. Exclude video traffic
- B. Enable decryption
- C. Block traffic that is not work-related
- D. Create a Tunnel Inspection policy

Answer: AC

Explanation:

This is because excluding video traffic from being sent over the VPN will reduce the amount of bandwidth being used during peak hours, allowing more bandwidth to be available for other types of traffic. Blocking non-work related traffic will also reduce the amount of bandwidth being used, further freeing up bandwidth for work-related traffic.

Enabling decryption and creating a Tunnel Inspection policy are not likely to mitigate the issue of decreased performance during peak-use hours, as they do not directly address the issue of limited bandwidth availability during these times.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP3ICAW>

NEW QUESTION 18

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 22

An internal system is not functioning. The firewall administrator has determined that the incorrect egress interface is being used. After looking at the configuration, the administrator believes that the firewall is not using a static route.

What are two reasons why the firewall might not use a static route? (Choose two.)

- A. no install on the route
- B. duplicate static route
- C. path monitoring on the static route
- D. disabling of the static route

Answer: AC

NEW QUESTION 27

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 30

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-Intermediate-CAi
- D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits [https //www example-website com/](https://www.example-website.com/) with a server certificate Common Name (CN) [www example-website com](https://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-Intermediate-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 32

A network security engineer must implement Quality of Service policies to ensure specific levels of delivery guarantees for various applications in the environment They want to ensure that they know as much as they can about QoS before deploying.

Which statement about the QoS feature is correct?

- A. QoS is only supported on firewalls that have a single virtual system configured
- B. QoS can be used in conjunction with SSL decryption
- C. QoS is only supported on hardware firewalls
- D. QoS can be used on firewalls with multiple virtual systems configured

Answer: D

NEW QUESTION 33

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 34

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 35

An organization wishes to roll out decryption but gets some resistance from engineering leadership regarding the guest network. What is a common obstacle for decrypting traffic from guest devices?

- A. Guest devices may not trust the CA certificate used for the forward untrust certificate.
- B. Guests may use operating systems that can't be decrypted.
- C. The organization has no legal authority to decrypt their traffic.
- D. Guest devices may not trust the CA certificate used for the forward trust certificate.

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices/decryption-best-practices/plan-s> <https://live.paloaltonetworks.com/t5/general-topics/decrypt-guest-network-traffic/td-p/119388>

NEW QUESTION 40

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 41

A firewall administrator has been tasked with ensuring that all Panorama configuration is committed and pushed to the devices at the end of the day at a certain time. How can they achieve this?

- A. Use the Scheduled Config Export to schedule Commit to Panorama and also Push to Devices.
- B. Use the Scheduled Config Push to schedule Push to Devices and separately schedule an API call to commit all Panorama changes.
- C. Use the Scheduled Config Export to schedule Push to Devices and separately schedule an API call to commit all Panorama changes.
- D. Use the Scheduled Config Push to schedule Commit to Panorama and also Push to Devices.

Answer: D

NEW QUESTION 46

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 47

In the screenshot above which two pieces of information can be determined from the ACC configuration shown? (Choose two)



- A. The Network Activity tab will display all applications, including FTP.
- B. Threats with a severity of "high" are always listed at the top of the Threat Name list
- C. Insecure-credentials, brute-force and protocol-anomaly are all a part of the vulnerability Threat Type
- D. The ACC has been filtered to only show the FTP application

Answer: AC

NEW QUESTION 52

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 54

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 59

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: C

NEW QUESTION 61

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.

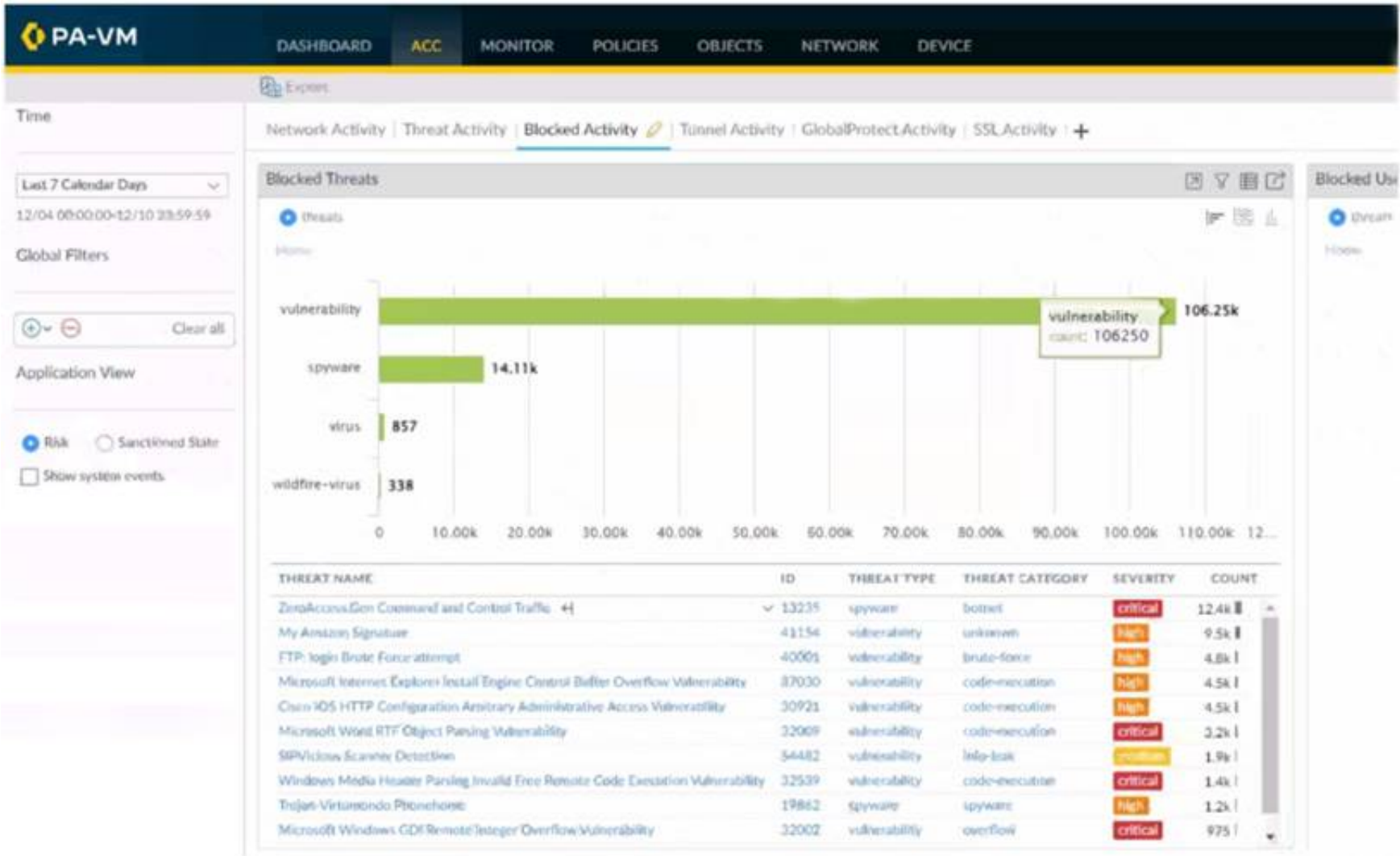
When performing an upgrade on Panorama to PAN-OS 10.2, what is the potential cause of a failed install?

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

Answer: A

NEW QUESTION 66

Refer to the exhibit.



Using the above screenshot of the ACC, what is the best method to set a global filter, narrow down Blocked User Activity, and locate the user(s) that could be compromised by a botnet?

- A. Click the hyperlink for the Zero Access.Gen threat.
- B. Click the left arrow beside the Zero Access.Gen threat.
- C. Click the source user with the highest threat count.
- D. Click the hyperlink for the hotport threat Category.

Answer: B

NEW QUESTION 69

Which log type would provide information about traffic blocked by a Zone Protection profile?

- A. Data Filtering
- B. IP-Tag
- C. Traffic
- D. Threat

Answer: D

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIm9CAC>

Zone Protection profile is a set of security policies that you can apply to an interface or zone to protect it from reconnaissance, flooding, brute force, and other types of attacks.

The log type that would provide information about traffic blocked by a Zone Protection profile is Thre4at. This log type records events such as packet-based attacks, spyware, viruses, vulnerability exploits, and URL filtering.

NEW QUESTION 74

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



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

Answer: B

NEW QUESTION 75

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-ssl-tls-service>

NEW QUESTION 80

An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls. The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls.

If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the configuration does not appear, what is the root cause?

- A. Panorama does not have valid licenses to push the dynamic updates.
- B. Panorama has no connection to Palo Alto Networks update servers.
- C. No service route is configured on the firewalls to Palo Alto Networks update servers.
- D. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed.

Answer: D

NEW QUESTION 82

An administrator needs to evaluate a recent policy change that was committed and pushed to a firewall device group. How should the administrator identify the configuration changes?

- A. review the configuration logs on the Monitor tab
- B. click Preview Changes under Push Scope
- C. use Test Policy Match to review the policies in Panorama
- D. context-switch to the affected firewall and use the configuration audit tool

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-co>

NEW QUESTION 86

An existing NGFW customer requires direct internet access offload locally at each site and IPSec connectivity to all branches over public internet. One requirement is that 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 91

Cortex XDR notifies an administrator about grayware on the endpoints. There are no entries about grayware in any of the logs of the corresponding firewall. Which setting can the administrator configure on the firewall to log grayware verdicts?

- A. within the log forwarding profile attached to the Security policy rule
- B. within the log settings option in the Device tab
- C. in WildFire General Settings, select "Report Grayware Files"
- D. in Threat General Settings, select "Report Grayware Files"

Answer: C

NEW QUESTION 92

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 96

A network security engineer is attempting to peer a virtual router on a PAN-OS firewall with an external router using the BGP protocol. The peer relationship is not establishing.

What command could the engineer run to see the current state of the BGP state between the two devices?

- A. show routing protocol bgp state
- B. show routing protocol bgp peer
- C. show routing protocol bgp summary
- D. show routing protocol bgp rib-out

Answer: B

NEW QUESTION 97

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 98

An administrator analyzes the following portion of a VPN system log and notices the following issue "Received local id 10 10 1 4/24 type IPv4 address protocol 0 port 0, received remote id 10.1.10.4/24 type IPv4 address protocol 0 port 0."

What is the cause of the issue?

- A. IPSec crypto profile mismatch
- B. IPSec protocol mismatch
- C. mismatched Proxy-IDs
- D. bad local and peer identification IP addresses in the IKE gateway

Answer: C

NEW QUESTION 99

Which Panorama mode should be used so that all logs are sent to, and only stored in. Cortex Data Lake?

- A. Legacy
- B. Log Collector
- C. Panorama
- D. Management Only

Answer: D

NEW QUESTION 102

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 104

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 105

A firewall administrator requires an A/P HA pair to fail over more quickly due to critical business application uptime requirements. What is the correct setting?

- A. Change the HA timer profile to "aggressive" or customize the settings in advanced profile.
- B. Change the HA timer profile to "fast".
- C. Change the HA timer profile to "user-defined" and manually set the timers.
- D. Change the HA timer profile to "quick" and customize in advanced profile.

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activepassive-ha/configure> In an A/P HA pair, HA (High Availability) timers are used to determine how quickly the firewall should fail over in case of a failure. Typically, the firewall administrator can choose between several predefined timer profiles such as "normal", "aggressive", and "fast".

Changing the HA timer profile to "user-defined" and manually setting the timers would allow the administrator to fine-tune the failover timing and make sure it meets the uptime requirements for the critical business applications. This approach allows the administrator to set the timers to the lowest possible value without compromising the stability and security of the firewall.

NEW QUESTION 109

An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

- A. certificate revocation
- B. Content-ID
- C. App-ID
- D. port inspection

Answer: C

NEW QUESTION 113

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.

	Answer Area
Static	20
OSPF External	120
EBGP	10
RIP	110

- 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 114

An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group. What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?

- A. A service route to the LDAP server
- B. A Master Device
- C. Authentication Portal
- D. A User-ID agent on the LDAP server

Answer: A

Explanation:

To configure LDAP authentication on Panorama, you need to23:

- Define an LDAP server profile that specifies the connection details and credentials for accessing the LDAP server.
- Define an authentication profile that references the LDAP server profile and defines how users authenticate to Panorama (such as username format and password expiration).
- Define an authentication sequence (optional) that allows users to authenticate using multiple methods (such as local database, LDAP, RADIUS, etc.).
- Assign the authentication profile or sequence to a Panorama administrator role or a device group role

NEW QUESTION 118

Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

- A. Create a no-decrypt Decryption Policy rule.
- B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
- C. Create a Dynamic Address Group for untrusted sites
- D. Create a Security Policy rule with vulnerability Security Profile attached.
- E. Enable the “Block sessions with untrusted issuers” setting.

Answer: AD

Explanation:

You can use the No Decryption tab to enable settings to block traffic that is matched to a decryption policy configured with the No Decrypt action (Policies > Decryption > Action). Use these options to control server certificates for the session, though the firewall does not decrypt and inspect the session traffic.

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-decryption-profile>

NEW QUESTION 120

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 123

An administrator would like to determine which action the firewall will take for a specific CVE. Given the screenshot below, where should the administrator navigate to view this information?

Vulnerability Protection Profile (Read Only)

Name

default

Description

Rules

Exceptions

	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	simple-client-critical	any	any	client	critical	default	disable
<input type="checkbox"/>	simple-client-high	any	any	client	high	default	disable
<input type="checkbox"/>	simple-client-medium	any	any	client	medium	default	disable
<input type="checkbox"/>	simple-server-critical	any	any	server	critical	default	disable
<input type="checkbox"/>	simple-server-high	any	any	server	high	default	disable
<input type="checkbox"/>	simple-server-medium	any	any	server	medium	default	disable

+

Add

-

Delete

↑

Move Up

↓

Move Down

⌙

Clone

🔍

Find Matching Signatures

OK

Cancel

- A. The profile rule action
- B. CVE column
- C. Exceptions lab
- D. The profile rule threat name

Answer: A

NEW QUESTION 127

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 131

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 133

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 134

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 #1 application: ssl; service: application-default; action: allow Rule #2 application; web-browsing; service application-default; action: allow

Answer: B

NEW QUESTION 138

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 142

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:

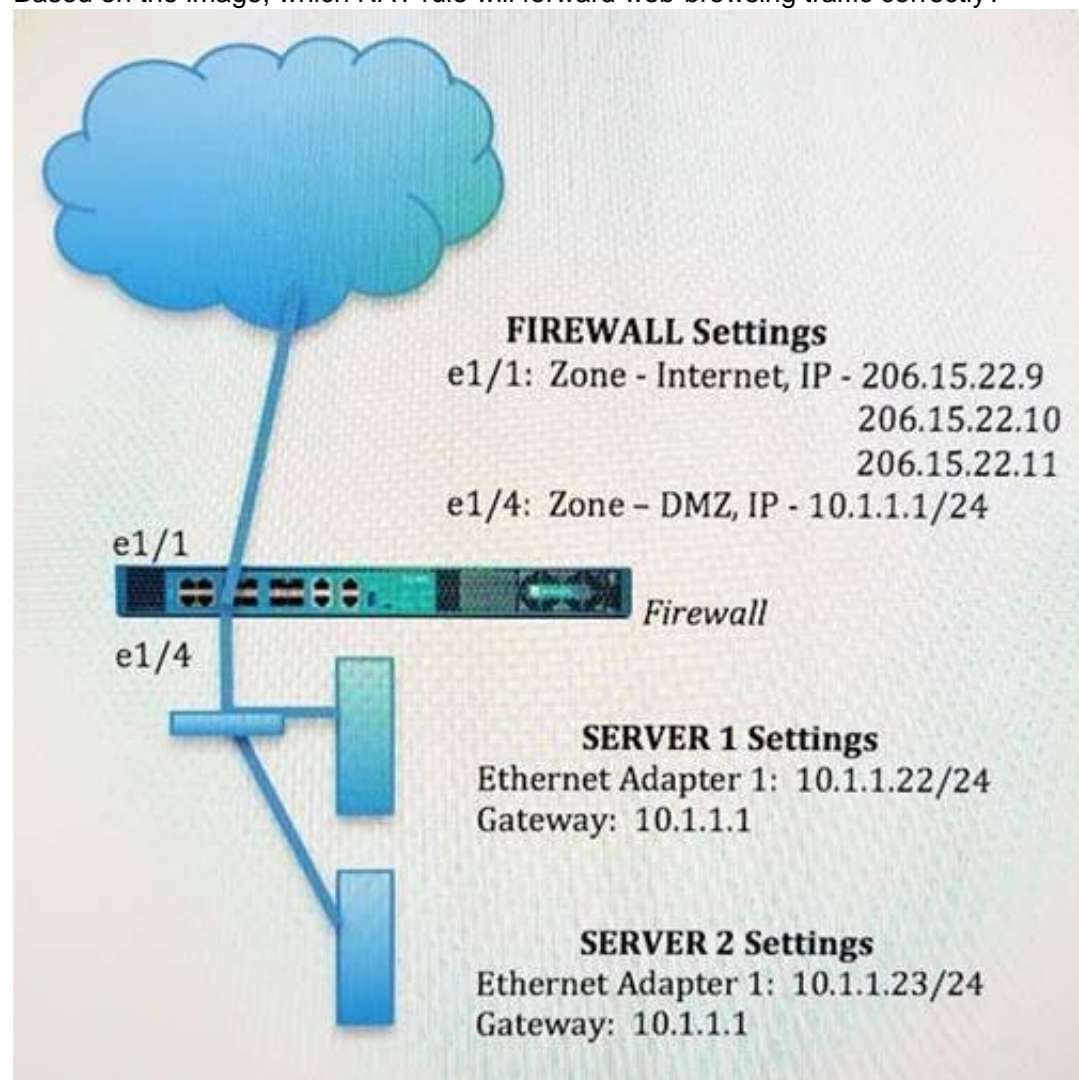
Support for multiple instances per link—With OSPFv3, you can run multiple instances of the OSPF protocol over a single link. This is accomplished by assigning an OSPFv3 instance ID number. An interface that is assigned to an instance ID drops packets that contain a different ID.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/ospf/ospf-concepts/ospfv3>

NEW QUESTION 144

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?



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 147

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 in 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 152

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 157

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 158

Where is information about packet buffer protection logged?

- A. Alert entries are in the Alarms log
- 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 log
- 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 160

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 161

SAML SLO is supported for which two firewall features? (Choose two.)

- A. GlobalProtect Portal
- B. CaptivePortal
- C. WebUI
- D. CLI

Answer: AB

Explanation:

SSO is available to administrators who access the web interface and to end users who access applications through GlobalProtect or Captive Portal. SLO is available to administrators and GlobalProtect end users, but not to Captive Portal end users.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/saml>

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/device/device-server-profiles-saml-id>

NEW QUESTION 164

Refer to the exhibit.

Device Group: DATACENTER_DG				
	NAME	LOCATION	TAGS	TYPE
1	intrazone-default	DATACENTER_DG	none	Intrazone
2	interzone-default	Predefined	none	Interzone

Device Group: Shared				
	NAME	LOCATION	TAGS	TYPE
1	intrazone-default	Shared	none	Intrazone
2	interzone-default	Predefined	none	Interzone

Based on the screenshots above what is the correct order in which the various rules are deployed to firewalls inside the DATACENTER_DG device group?

- A. shared pre-rules DATACENTER DG pre rulesrules configured locally on the firewall shared post-rules DATACENTER_DG post-rules DATACENTER.DG default rules
- B. shared pre-rulesDATACENTER_DG pre-rulesrules configured locally on the firewall shared post-rulesDATACENTER.DG post-rules shared default rules
- C. shared pre-rules DATACENTER_DG pre-rulesrules configured locally on the firewall DATACENTER_DG post-rules shared post-rulesshared default rules
- D. shared pre-rules DATACENTER_DG pre-rulesrules configured locally on the firewall DATACENTER_DG post-rules shared post-rules DATACENTER_DG default rules

Answer: A

NEW QUESTION 168

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 allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.
- C. Explicit proxy supports interception of traffic using non-standard HTTPS ports.
- D. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request

Answer: BC

Explanation:

- > B. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy¹². This means that the client can see the proxy's IP address and port number, and can use tools like ping or traceroute to check connectivity and latency issues. Transparent proxies are invisible to the client browser, which makes it harder to diagnose problems.
- > C. Explicit proxy supports interception of traffic using non-standard HTTPS ports³. This means that the proxy can handle HTTPS requests that use ports other than 443, which may be required by some applications or websites. Transparent proxies can only intercept HTTPS traffic on port 443, which limits their functionality.

NEW QUESTION 170

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 174

When you navigate to Network: > GlobalProtect > Portals > Method section, which three options are available? (Choose three)

- A. user-logon (always on)
- B. pre-logon then on-demand
- C. on-demand (manual user initiated connection)
- D. post-logon (always on)
- E. certificate-logon

Answer: ABC

NEW QUESTION 176

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 reboot). 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 177

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 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 181

A firewall should be advertising the static route 10.2.0.0/24 Into OSPF. The configuration on the neighbor is correct, but the route is not in the neighbor's routing table.

Which two configurations should you check on the firewall? (Choose two.)

- A. In the OSFP configuration, ensure that the correct redistribution profile is selected in the OSPF Export Rules section.
- B. Within the redistribution profile ensure that Redist is selected.
- C. Ensure that the OSPF neighbor state Is "2-Way."
- D. In the redistribution profile check that the source type is set to "ospf."

Answer: AB

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 186

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 191

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 192

What can an engineer use with GlobalProtect to distribute user-specific client certificates to each GlobalProtect user?

- A. Certificate profile
- B. SSL/TLS Service profile
- C. OCSP Responder
- D. SCEP

Answer: D

NEW QUESTION 194

Given the following snippet of a WildFire submission log. did the end-user get access to the requested information and why or why not?

TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-2...		low	any		
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-2...		low	any		

- A. Ye
- B. because the action is set to "allow "
- C. No because WildFire categorized a file with the verdict "malicious"
- D. Yes because the action is set to "alert"
- E. No because WildFire classified the severity as "high."

Answer: A

NEW QUESTION 197

Which profile generates a packet threat type found in threat logs?

- A. Zone Protection
- B. WildFire
- C. Anti-Spyware
- D. Antivirus

Answer: A

NEW QUESTION 198

Which statement accurately describes service routes and virtual systems?

- A. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall.
- B. Virtual systems can only use one interface for all global service and service routes of the firewall.
- C. Virtual systems cannot have dedicated service routes configured; and virtual systems always use the global service and service route settings for the firewall.
- D. The interface must be used for traffic to the required external services.

Answer: A

NEW QUESTION 202

Which function is handled by the management plane (control plane) of a Palo Alto Networks firewall?

- A. signature matching for content inspection
- B. IPSec tunnel standup
- C. Quality of Service
- D. logging

Answer: D

NEW QUESTION 204

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

Security Policy Rule

General Source Destination Application Service/URL Category **Actions** Usage

Action Setting:

Action: **Allow**

☐ Auto NAT Calculation

Profile Setting:

Profile Type: **Profiles**

Antivirus: **default**

Vulnerability Protection: **strict**

Anti-Spyware: **strict**

URL Filtering: **default**

File Blocking: **None**

Data Filtering: **None**

Workflow Profiles: **default**

Log Setting:

☐ Log at Session Start

☒ Log at Session End

Log Retention: **None**

Other Settings:

Schedule: **None**

QoS Marking: **None**

☐ Disable Scheduler Response Inspection

OK **Cancel**

B)

Panorama Settings

Receive Timeout for Connection to Device (sec): **240**

Send Timeout for Connection to Device (sec): **240**

Retry Count for SSL Send to Device: **25**

☐ Share Unused Address and Service Objects with Devices

☐ Objects defined in ancestors will take higher precedence

☐ Enable reporting and filtering on groups

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

OK **Cancel**

C)

Syslog Server Profile

Name: **initat(profile1)**

Servers Custom Log Format

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

Add **Remove**

Enter any IP address or FQDN of the Syslog server

OK **Cancel**

D)

Panorama Settings

Panorama Servers

10.99.1.21

☒ Enable pushing device monitoring data to Panorama

Receive Timeout for Connection to Panorama (sec): **240**

Send Timeout for Connection to Panorama (sec): **240**

Retry Count for SSL Send to Panorama: **25**

☒ Enable automated commit recovery

Number of attempts to check for Panorama connectivity: **1**

Interval between retries (sec): **10**

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

- A. Option A
 B. Option B
 C. Option C

D. Option D

Answer: C

NEW QUESTION 205

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 209

Which data flow describes redistribution of user mappings?

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

Answer: B

Explanation:

[https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redistribute-](https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redistribute) <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/red>

NEW QUESTION 213

You have upgraded Panorama to 10.2 and need to upgrade six Log Collectors. When upgrading Log Collectors to 10.2, you must do what?

- A. Upgrade the Log Collectors one at a time.
- B. Add Panorama Administrators to each Managed Collector.
- C. Add a Global Authentication Profile to each Managed Collector.
- D. Upgrade all the Log Collectors at the same time.

Answer: D

NEW QUESTION 214

Which CLI command is used to determine how much disk space is allocated to logs?

- A. show logging-status
- B. show system info
- C. debug log-receiver show
- D. show system logdfo-quota

Answer: D

NEW QUESTION 215

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 220

You have upgraded your Panorama and Log Collectors to 10.2 x. Before upgrading your firewalls using Panorama, what do you need do?

- A. Refresh your licenses with Palo Alto Network Support - Panorama/Licenses/Retrieve License Keys from License Server.
- B. Re-associate the firewalls in Panorama/Managed Devices/Summary.
- C. Commit and Push the configurations to the firewalls.
- D. Refresh the Master Key in Panorama/Master Key and Diagnostic

Answer: C

NEW QUESTION 224

Which three use cases are valid reasons for requiring an Active/Active high availability deployment? (Choose three.)

- A. The environment requires real, full-time redundancy from both firewalls at all times
- B. The environment requires Layer 2 interfaces in the deployment
- C. The environment requires that both firewalls maintain their own routing tables for faster dynamic routing protocol convergence

- D. The environment requires that all configuration must be fully synchronized between both members of the HA pair
- E. The environment requires that traffic be load-balanced across both firewalls to handle peak traffic spikes

Answer: BCD

NEW QUESTION 227

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 229

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 231

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 233

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 236

A network administrator is troubleshooting an issue with Phase 2 of an IPSec VPN tunnel. The administrator determines that the lifetime needs to be changed to match the peer.

Where should this change be made?

- A. IKE Gateway profile
- B. IPSec Crypto profile
- C. IPSec Tunnel settings
- D. IKE Crypto profile

Answer: C

NEW QUESTION 238

An engineer has been given approval to upgrade their environment 10 PAN-OS 10 2

The environment consists of both physical and virtual firewalls a virtual Panorama HA pair, and virtual log collectors

What is the recommended order when upgrading to PAN-OS 10.2?

- A. Upgrade Panorama, upgrade the log collectors, upgrade the firewalls
- B. Upgrade the firewalls upgrade log collectors, upgrade Panorama

- C. Upgrade the firewalls upgrade Panorama, upgrade the log collectors
 D. Upgrade the log collectors, upgrade the firewalls, upgrade Panorama

Answer: B

NEW QUESTION 239

A user at an external system with the IP address 65.124.57.5 queries the DNS server at 4. 2.2.2 for the IP address of the web server, www.xyz.com. The DNS server returns an address of 192.168.15.1

In order to reach the web server, which Security rule and NAT rule must be configured on the firewall?



A)

NAT Rule:
 Untrust-L3 (any) - Trust-L3 (172.16.15.1) Destination Translation : 192.168.15.47
 Security Rule:
 Untrust-L3 (any) - Trust-L3 (192.168.15.47) - Application : Web-browsing

B)

NAT Rule:
 Untrust-L3 (any) - Trust-L3 (172.16.15.1) Destination Translation : 192.168.15.47
 Security Rule:
 Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application : Web-browsing

C)

NAT Rule:
 Untrust-L3 (any) - Untrust-L3 (172.16.15.1) Destination Translation : 192.168.15.47
 Security Rule:
 Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application : Web-browsing

D)

NAT Rule:
 Untrust-L3 (any) - Untrust-L3 (any) Destination Translation : 192.168.15.47
 Security Rule:
 Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application : Web-browsing

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

Answer: C

NEW QUESTION 244

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 of 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 246

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
 C. Virtual Wire
 D. Tap
 E. Layer 3

Answer: BCE

Explanation:

SSL Forward Proxy is a feature that allows the firewall to decrypt and inspect outbound SSL traffic from internal users to external servers¹. The firewall acts as a proxy (MITM) generating a new certificate for the accessed URL and presenting it to the client during SSL handshake². SSL Forward Proxy can be configured on any interface type that supports security policies, which are Layer 2, Virtual Wire, and Layer 3 interfaces¹. These interface types allow the firewall to apply security profiles and URL filtering on the decrypted SSL traffic.

NEW QUESTION 251

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 254

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 256

An administrator needs to build Security rules in a Device Group that allow traffic to specific users and groups defined in Active Directory
What must be configured in order to select users and groups for those rules from Panorama?

- A. The Security rules must be targeted to a firewall in the device group and have Group Mapping configured
- B. A master device with Group Mapping configured must be set in the device group where the Security rules are configured
- C. User-ID Redistribution must be configured on Panorama to ensure that all firewalls have the same mappings
- D. A User-ID Certificate profile must be configured on Panorama

Answer: B

NEW QUESTION 257

Which source is the most reliable for collecting User-ID user mapping?

- A. GlobalProtect
- B. Microsoft Active Directory
- C. Microsoft Exchange
- D. Syslog Listener

Answer: A

Explanation:

User-ID is a feature that enables you to identify and control users on your network based on their usernames instead of their IP addresses¹. User mapping is the process of mapping IP addresses to usernames using various sources of information¹.

The most reliable source for collecting User-ID user mapping is GlobalProtect². GlobalProtect is a solution that provides secure access to your network and resources from anywhere. GlobalProtect agents on endpoints send user mapping information directly to the firewall or Panorama, which eliminates the need for probing other sources². GlobalProtect also supports dynamic IP address changes and roaming use²rs.

NEW QUESTION 258

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 262

How can an administrator use the Panorama device-deployment option to update the apps and threat version of an HA pair of managed firewalls?

- A. Configure the firewall's assigned template to download the content updates.
- B. Choose the download and install action for both members of the HA pair in the Schedule object.
- C. Switch context to the firewalls to start the download and install process.
- D. Download the apps to the primary; no further action is required.

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/use-case-configure-firewa>

NEW QUESTION 263

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 265

A network security engineer configured IP multicast in the virtual router to support a new application. Users in different network segments are reporting that they are unable to access the application.

What must be enabled to allow an interface to forward multicast traffic?

- A. IGMP
- B. PIM
- C. BFD
- D. SSM

Answer: B

Explanation:

A protocol that enables routers to forward multicast traffic efficiently based on the source and destination addresses. PIM can operate in two modes: sparse mode (PIM-SM) or dense mode (PIM-DM). PIM-SM uses a rendezvous point (RP) as a central point for distributing multicast traffic, while PIM-DM uses flooding and pruning techniques.

to enable PIM on the interface which allows routers to forward multicast traffic using either sparse mode or dense mode depending on your network topology and requirements.

NEW QUESTION 267

What is considered the best practice with regards to zone protection?

- A. Review DoS threat activity (ACC > Block Activity) and look for patterns of abuse
- B. Use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs
- C. If the levels of zone and DoS protection consume too many firewall resources, disable zone protection
- D. Set the Alarm Rate threshold for event-log messages to high severity or critical severity

Answer: C

NEW QUESTION 270

An administrator creates an application-based security policy rule and commits the change to the firewall. Which two methods should be used to identify the dependent applications for the respective rule? (Choose two.)

- A. Use the show predefined xpath <value> command and review the output.
- B. Review the App Dependency application list from the Commit Status view.
- C. Open the security policy rule and review the Depends On application list.
- D. Reference another application group containing similar applications.

Answer: AB

NEW QUESTION 275

An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.

Which configuration setting or step will allow the firewall to get automatic application signature updates?

- A. A scheduler will need to be configured for application signatures.
- B. A Security policy rule will need to be configured to allow the update requests from the firewall to the update servers.
- C. A Threat Prevention license will need to be installed.
- D. A service route will need to be configured.

Answer: A

NEW QUESTION 280

An administrator needs firewall access on a trusted interface. Which two components are required to configure certificate based, secure authentication to the web UI? (Choose two)

- A. certificate profile
- B. server certificate
- C. SSH Service Profile
- D. SSL/TLS Service Profile

Answer: AD

NEW QUESTION 282

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 283

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 287

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 290

An administrator has a PA-820 firewall with an active Threat Prevention subscription The administrator is considering adding a WildFire subscription. How does adding the WildFire subscription improve the security posture of the organization1?

- A. Protection against unknown malware can be provided in near real-time
- B. WildFire and Threat Prevention combine to provide the utmost security posture for the firewall
- C. After 24 hours WildFire signatures are included in the antivirus update
- D. WildFire and Threat Prevention combine to minimize the attack surface

Answer: A

NEW QUESTION 294

A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg.txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg.txt in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsystjumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command:> request resort system Upon restart, the firewall fails to begin the bootstrapping process. The failure is caused because

- A. Firewall must be in factory default state or have all private data deleted for bootstrapping
- B. The hostname is a required parameter, but it is missing in init-cfg.txt
- C. The USB must be formatted using the ext3 file system, FAT32 is not supported
- D. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x
- E. The bootstrap.xml file is a required file but it is missing

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/boots>

NEW QUESTION 296

The Aggregate Ethernet interface is showing down on a passive PA-7050 firewall of an active/passive HA pair. The HA Passive Link State is set to "Auto" under Device > High Availability > General > Active/Passive Settings. The AE interface is configured with LACP enabled and is up only on the active firewall. Why is the AE interface showing down on the passive firewall?

- A. It does not perform pre-negotiation LACP unless "Enable in HA Passive State" is selected under the High Availability Options on the LACP tab of the AE Interface.
- B. It does not participate in LACP negotiation unless Fast Failover is selected under the Enable LACP selection on the LACP tab of the AE Interface.
- C. It participates in LACP negotiation when Fast is selected for Transmission Rate under the Enable LACP selection on the LACP tab of the AE Interface.
- D. It performs pre-negotiation of LACP when the mode Passive is selected under the Enable LACP selection on the LACP tab of the AE Interface.

Answer: A

NEW QUESTION 299

During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. Additional device certificates and/or Subordinate certificates requiring an Enterprise CA chain of trust are signed by the company's Intermediate CA.

Which method should the administrator use when creating Forward Trust and Forward Untrust certificates on the firewall for use with decryption?

- A. Generate a single subordinate CA certificate for both Forward Trust and Forward Untrust.
- B. Generate a CA certificate for Forward Trust and a self-signed CA for Forward Untrust.
- C. Generate a single self-signed CA certificate for Forward Trust and another for Forward Untrust
- D. Generate two subordinate CA certificates, one for Forward Trust and one for Forward Untrust.

Answer: B

NEW QUESTION 300

An administrator wants to enable WildFire inline machine learning. Which three file types does WildFire inline ML analyze? (Choose three.)

- A. MS Office
- B. ELF
- C. APK
- D. VBScripts
- E. Powershell scripts

Answer: CDE

NEW QUESTION 305

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

PCNSE Practice Exam Features:

- * PCNSE Questions and Answers Updated Frequently
- * PCNSE Practice Questions Verified by Expert Senior Certified Staff
- * PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PCNSE Practice Test Here](#)