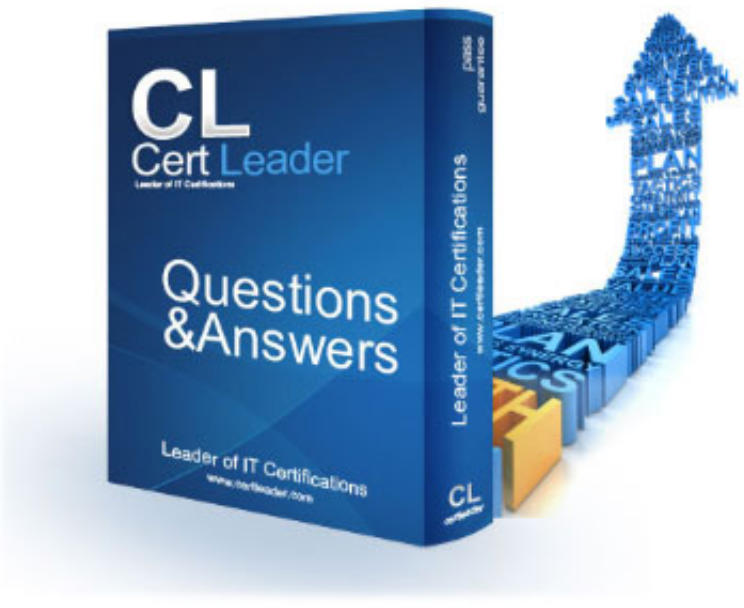
PCNSE Dumps

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

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



NEW QUESTION 1
A network-security engineer attempted to configure a bootstrap package on Microsoft Azure, but the virtual machine provisioning process failed. In reviewing the bootstrap package, the engineer only had the following directories: /config, /license and /software
Why did the bootstrap process fail for the VM-Series firewall in Azure?

A. All public cloud deployments require the /plugins folder to support proper firewall native integrations
B. The /content folder is missing from the bootstrap package
C. The VM-Series firewall was not pre-registered in Panorama and prevented the bootstrap process from successfully completing
D. The /config or /software folders were missing mandatory files to successfully bootstrap

Answer: B

NEW QUESTION 2
A Security policy rule is configured with a Vulnerability Protection Profile and an action of "Deny." Which action will this configuration cause on the matched traffic?

A. The Profile Settings section will be grayed out when the Action is set to "Deny"
B. It will cause the firewall to skip this Security policy rul
C. A warning will be displayed during a commit
D. The configuration will allow the matched session unless a vulnerability signature is detected.
E. The "Deny" action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile It will cause the firewall to deny the matched sessions.Any configured Security Profiles have no effect if the Security policy rule action is set to "Deny"

Answer: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/security-profiles.html First note in above link states:
"Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy."
The first thing the firewall checks per it's flow is the security policy match and action. The Security Profile never gets checked if a match happens on a policy set to deny that match.

NEW QUESTION 3
An administrator is building Security rules within a device group to block traffic to and from malicious locations
How should those rules be configured to ensure that they are evaluated with a high priority?

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

Answer: D

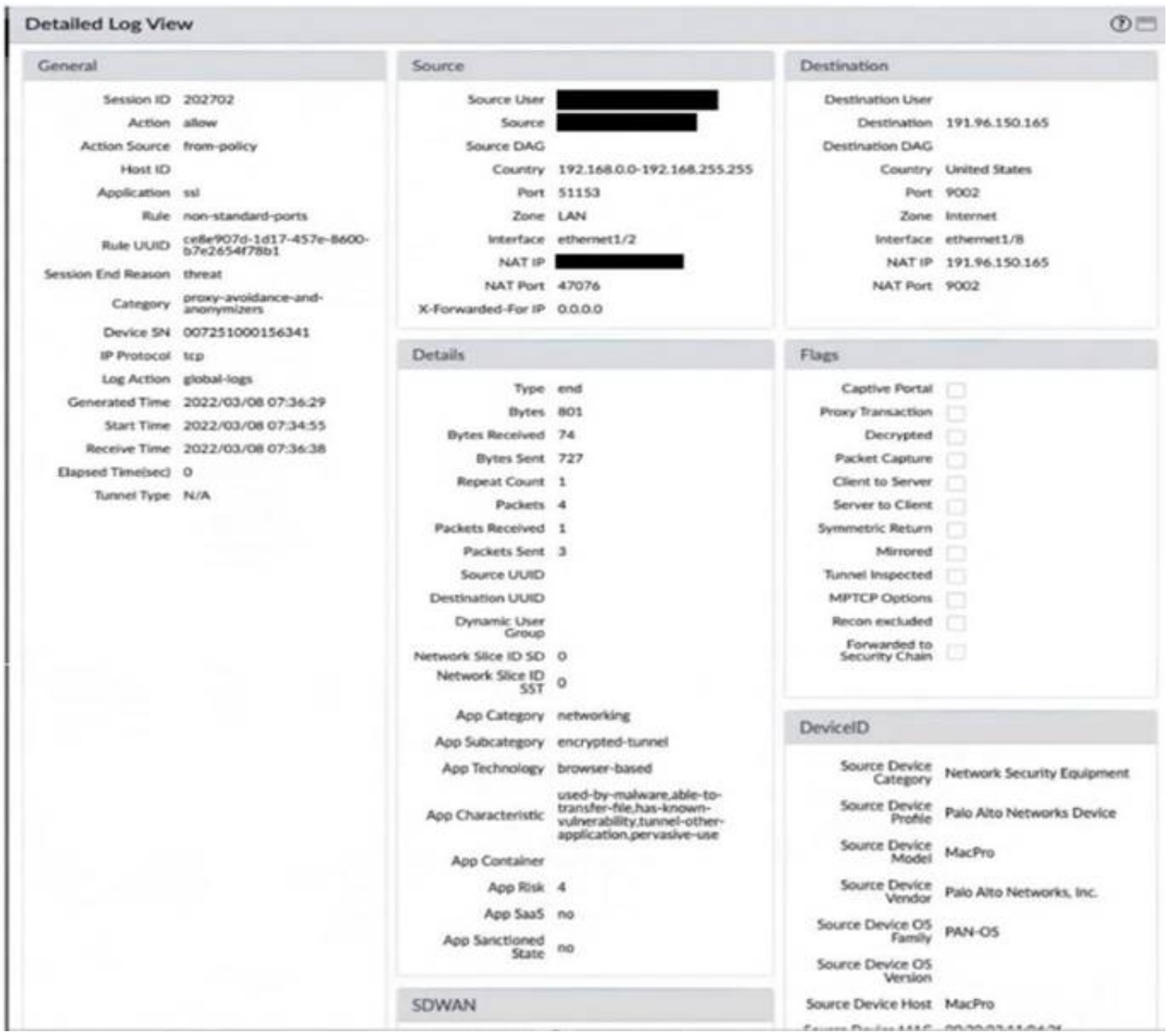
NEW QUESTION 4
A standalone firewall with local objects and policies needs to be migrated into Panorama. What procedure should you use so Panorama is fully managing the firewall?

A. Use the "import Panorama configuration snapshot" operation, then perform a device-group commit push with "include device and network templates"
B. Use the "import device configuration to Panorama" operation, then "export or push device config bundle" to push the configuration
C. Use the "import Panorama configuration snapshot" operation, then "export or push device config bundle" to push the configuration
D. Use the "import device configuration to Panorama" operation, then perform a device-group commit push with "include device and network templates"

Answer: B

Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-a-firewall-to-pan

NEW QUESTION 5
Given the screenshot, how did the firewall handle the traffic?



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

Answer: D

NEW QUESTION 6
SSL Forward Proxy decryption is configured but the firewall uses Untrusted-CA to sign the website https://www important-website com certificate End-users are receiving me "security certificate is not trusted is warning Without SSL decryption the web browser shows that the website certificate is trusted and signed by a well-known certificate chain Well-Known-Intermediate and Well-Known-Root- CA.
The network security administrator who represents the customer requires the following two behaviors when SSL Forward Proxy is enabled:
1 End-users must not get the warning for the https://www.very-important-website.com website. 2 End-users should get the warning for any other untrusted website
Which approach meets the two customer requirements?

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

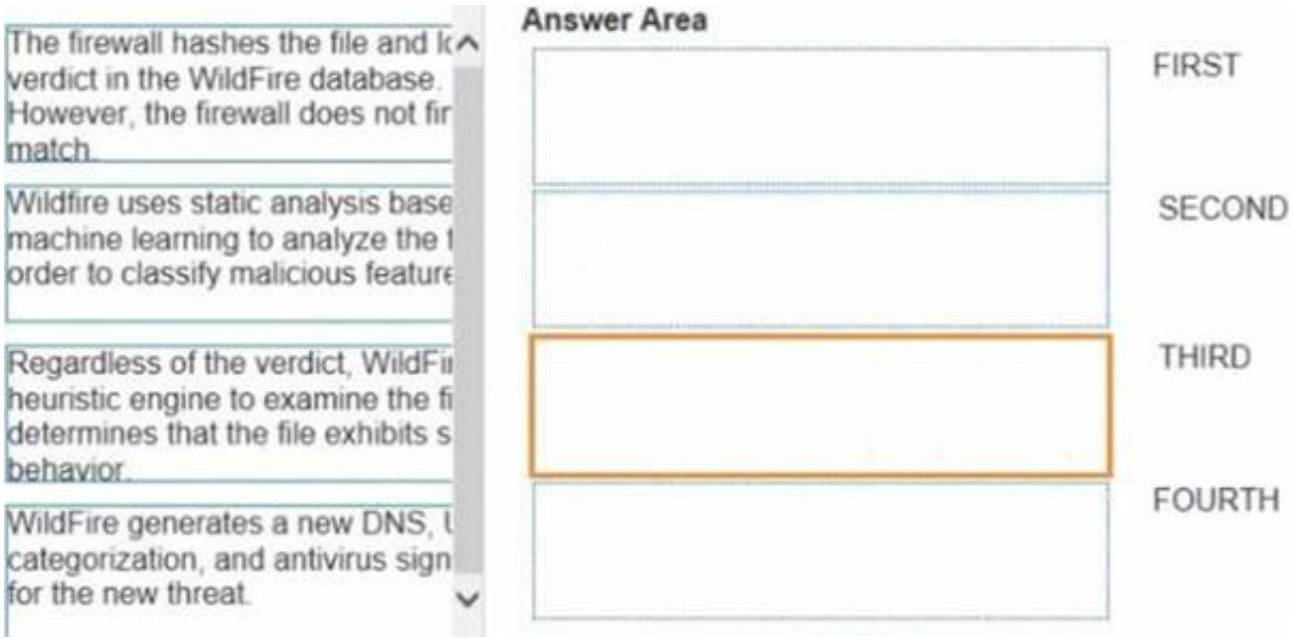
Answer: C

NEW QUESTION 7
Which statement about High Availability timer settings is true?

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

Answer: C

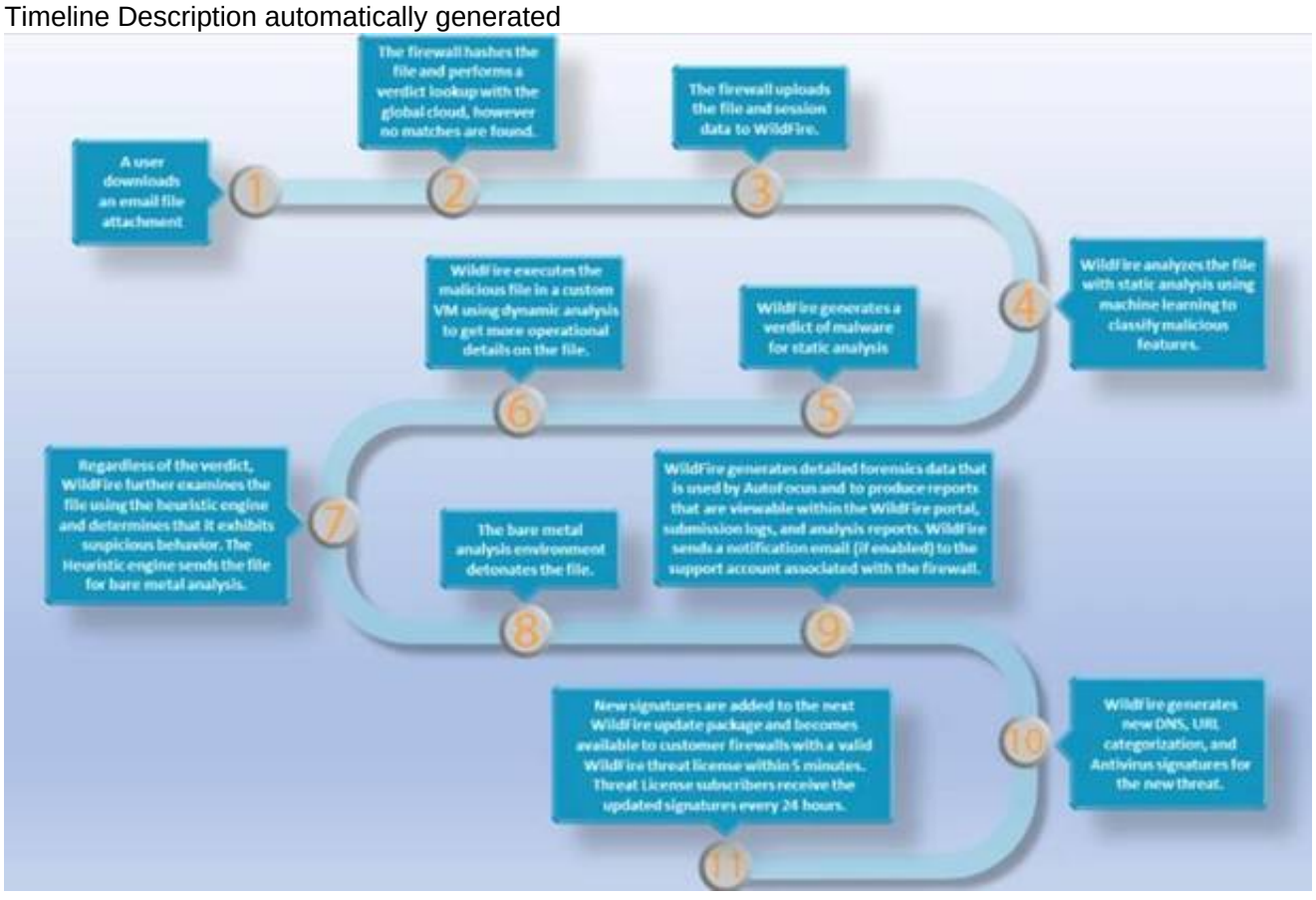
NEW QUESTION 8
Place the steps in the WildFire process workflow in their correct order.



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 9
Which statement regarding HA timer settings is true?

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

Answer: A

NEW QUESTION 10
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 10
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 13
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 14
Which three methods are supported for split tunneling in the GlobalProtect Gateway? (Choose three.)

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

Answer: BCE

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

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

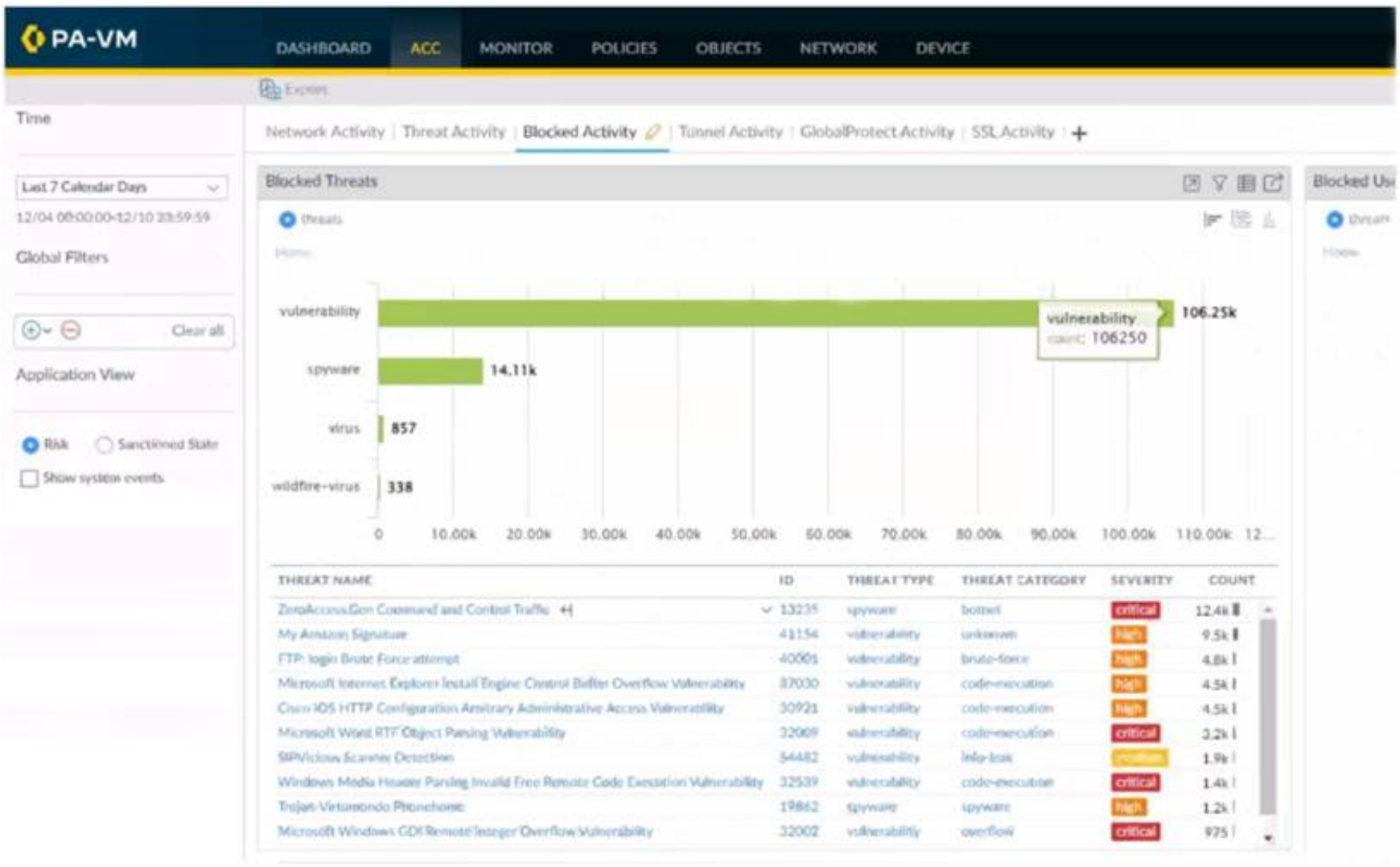
NEW QUESTION 15
What are two valid deployment options for Decryption Broker? (Choose two)

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

Answer: AB

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

NEW QUESTION 18
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 23
A firewall has been assigned to a new template stack that contains both "Global" and "Local" templates in Panorama, and a successful commit and push has been performed. While validating the configuration on the local firewall, the engineer discovers that some settings are not being applied as intended.
The setting values from the "Global" template are applied to the firewall instead of the "Local" template that has different values for the same settings.
What should be done to ensure that the settings in the "Local" template are applied while maintaining settings from both templates?

A. Move the "Global" template above the "Local" template in the template stack.
B. Perform a commit and push with the "Force Template Values" option selected.
C. Move the "Local" template above the "Global" template in the template stack.
D. Override the values on the local firewall and apply the correct settings for each value.

Answer: C

NEW QUESTION 24
A network administrator wants to use a certificate for the SSL/TLS Service Profile. Which type of certificate should the administrator use?

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

Answer: D

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

NEW QUESTION 27
A firewall administrator needs to be able to inspect inbound HTTPS traffic on servers hosted in their DMZ to prevent the hosted service from being exploited.
Which combination of features can allow PAN-OS to detect exploit traffic in a session with TLS encapsulation?

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

Answer: C

NEW QUESTION 29
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.

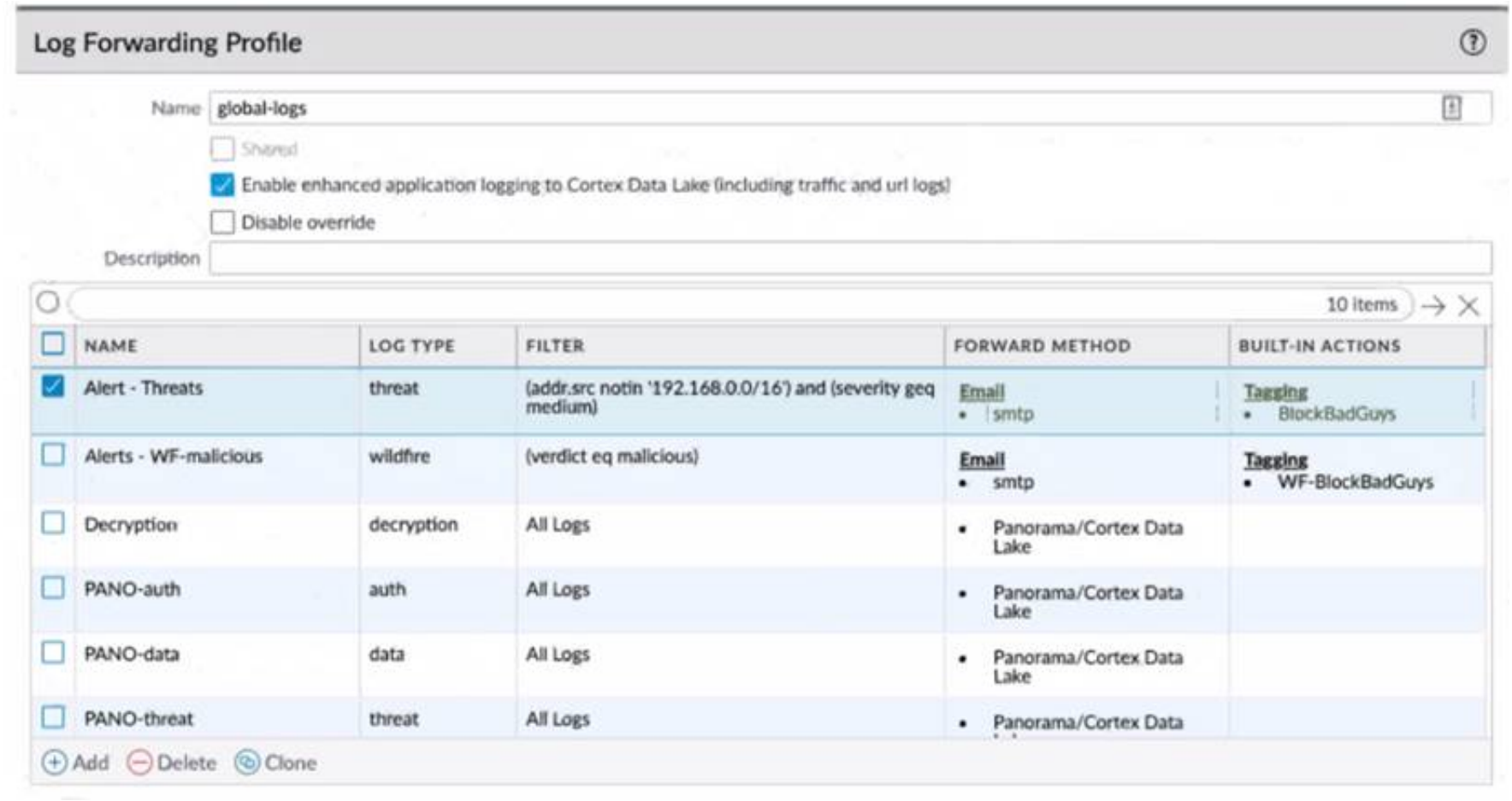
Answer: D

NEW QUESTION 32
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 33
Review the images.



A firewall policy that permits web traffic includes the
What is the result of traffic that matches the "Alert - Threats" Profile Match List?

A. The source address of SMTP traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.
B. The source address of traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.
C. The source address of traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.
D. The source address of SMTP traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

Answer: D

NEW QUESTION 37
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 39
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 43
An administrator needs to assign a specific DNS server to one firewall within a device group. Where would the administrator go to edit a template variable at the device level?

A. Variable CSV export under Panorama > templates
B. PDF Export under Panorama > templates
C. Manage variables under Panorama > templates
D. Managed Devices > Device Association

Answer: B

NEW QUESTION 46
A firewall has Security policies from three sources
* 1. locally created policies
* 2. shared device group policies as pre-rules
* 3. the firewall's device group as post-rules
How will the rule order populate once pushed to the firewall?

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

Answer: C

NEW QUESTION 47
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 50
Which statement is correct given the following message from the PanGPA log on the GlobalProtect app? Failed to connect to server at port:47 67

A. The PanGPS process failed to connect to the PanGPA process on port 4767
B. The GlobalProtect app failed to connect to the GlobalProtect Portal on port 4767
C. The PanGPA process failed to connect to the PanGPS process on port 4767
D. The GlobalProtect app failed to connect to the GlobalProtect Gateway on port 4767

Answer: D

NEW QUESTION 51
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 55
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443 A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.
Which combination of service and application, and order of Security policy rules, needs to be configured to allow cJeartext web-browsing traffic to this server on tcp/443?

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

Answer: B

NEW QUESTION 56
What best describes the HA Promotion Hold Time?

A. the time that is recommended to avoid an HA failover due to the occasional flapping of neighboring devices
B. the time that is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously
C. the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost
D. the time that a passive firewall with a low device priority will wait before taking over as the active firewall if the firewall is operational again

Answer: C

NEW QUESTION 61
A network security administrator wants to configure SSL inbound inspection.
Which three components are necessary for inspecting the HTTPS traffic as it enters the firewall? (Choose three.)

A. An SSL/TLS Service profile
B. The web server's security certificate with the private key
C. A Decryption profile
D. A Decryption policy
E. The client's security certificate with the private key

Answer: BCD

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-inbound-inspection

NEW QUESTION 65
What is the function of a service route?

A. The service route is the method required to use the firewall's management plane to provide services to applications
B. The service packets enter the firewall on the port assigned from the external servic
C. The server sends its response to the configured destination interface and destination IP address
D. The service packets exit the firewall on the port assigned for the external servic
E. The server sends its response to the configured source interface and source IP address
F. Service routes provide access to external services such as DNS servers external authentication servers or Palo Alto Networks services like the Customer Support Portal

Answer: C

NEW QUESTION 70
A security engineer received multiple reports of an IPSec VPN tunnel going down the night before. The engineer couldn't find any events related to VPN under system togs.
What is the likely cause?

A. Dead Peer Detection is not enabled.
B. Tunnel Inspection settings are misconfigured.
C. The Tunnel Monitor is not configured.
D. The log quota for GTP and Tunnel needs to be adjusted

Answer: C

Explanation:
This means that the firewall does not have a mechanism to monitor the status of the IPSec VPN tunnel and generate logs when it goes down or up. The Tunnel Monitor is an optional feature that can be enabled on each IPSec tunnel interface and it uses ICMP probes to check the connectivity of the tunnel peer. If the firewall does not receive a response from the peer after a specified number of retries, it marks the tunnel as down and logs an event1.

NEW QUESTION 72
Which three multi-factor authentication methods can be used to authenticate access to the firewall? (Choose three.)

A. One-time password
B. User certificate
C. Voice
D. SMS
E. Fingerprint

Answer: ABE

Explanation:
The three multi-factor authentication methods that can be used to authenticate access to the firewall are One-time Password (OTP), User Certificate, and Fingerprint.
One-time Password (OTP) is a form of two-factor authentication in which a token or code is generated and sent to the user over a secure connection. The user then enters the code to authenticate their access.
User Certificate is a form of two-factor authentication in which the user is required to present a valid certificate in order to access the system. The certificate is usually stored on a physical device, such as a USB drive, and is usually issued by the authentication service provider.
Fingerprint is a form of two-factor authentication in which the user is required to present a valid fingerprint in order to access the system. The fingerprint is usually stored on a physical device, such as a fingerprint reader, and is usually issued by the authentication service provider.

NEW QUESTION 74
Which GlobalProtect component must be configured to enable Clientless VPN?

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

Answer: C

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

NEW QUESTION 79
Which time determines how long the passive firewall will wait before taking over as the active firewall alter losing communications with the HA peer?

A. Heartbeat Interval
B. Additional Master Hold Up Time
C. Promotion Hold Time
D. Monitor Fall Hold Up Time

Answer: A

NEW QUESTION 81
When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

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

Answer: D

NEW QUESTION 86
A network security administrator has an environment with multiple forms of authentication. There is a network access control system in place that authenticates and restricts access for wireless users, multiple Windows domain controllers, and an MDM solution for company-provided smartphones. All of these devices have their authentication events logged.
Given the information, what is the best choice for deploying User-ID to ensure maximum coverage?

A. Syslog listener
B. agentless User-ID with redistribution
C. standalone User-ID agent
D. captive portal

Answer: C

NEW QUESTION 90
Which two statements correctly describe Session 380280? (Choose two.)

```
> show session id 380280

Session              380280
    c2s flow:
            source:      172.17.149.129 [L3-Trust]
            dst:         104.154.89.105
            proto:       6
            sport:       60997          dport:       443
            state:       ACTIVE         type:        FLOW
            src user:    unknown
            dst user:    unknown

    s2c flow:
            source:      104.154.89.105 [L3-Untrust]
            dst:         10.46.42.149
            proto:       6
            sport:       443            dport:       7260
            state:       ACTIVE         type:        FLOW
            src user:    unknown
            dst user:    unknown

start time                          : Tue Feb  9 20:38:42 2021
timeout                             : 15 sec
time to live                        : 2 sec
total byte count(c2s)               : 3330
total byte count(s2c)               : 12698
layer7 packet count(c2s)            : 14
layer7 packet count(s2c)            : 19
vsys                                : vsys1
application                         : web-browsing
rule                                : Trust-to-Untrust
service timeout override(index)     : False
session to be logged at end         : True
session in session ager             : True
session updated by HA peer          : False
session proxied                     : True
address/port translation            : source
nat-rule                            : Trust-NAT(vsys1)
layer7 processing                   : completed
URL filtering enabled               : True
URL category                        : computer-and-internet-info, low-risk
session via syn-cookies             : False
session terminated on host          : False
session traverses tunnel            : False
session terminate tunnel            : False
captive portal session              : False
ingress interface                   : ethernet1/6
egress interface                    : ethernet1/3
session QoS rule                    : N/A (class 4)
tracker stage l7proc                : proxy timer expired
end-reason                          : unknown
```

A. The session went through SSL decryption processing.
B. The session has ended with the end-reason unknown.
C. The application has been identified as web-browsing.
D. The session did not go through SSL decryption processing.

Answer: AC

NEW QUESTION 95
Refer to the diagram. Users at an internal system want to ssh to the SSH server The server is configured to respond only to the ssh requests coming from IP 172.16.16.1.
In order to reach the SSH server only from the Trust zone, which Security rule and NAT rule must be configured on the firewall?

A)

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 99
When using certificate authentication for firewall administration, which method is used for authorization?

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

Answer: A

NEW QUESTION 102
What can you use with Global Protect to assign user-specific client certificates to each GlobalProtect user?

A. SSL/TLS Service profile
B. Certificate profile
C. SCEP

D. OCSP Responder

Answer: C

NEW QUESTION 107
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

A. upload-only
B. upload and install and reboot
C. verify and install
D. upload and install
E. install and reboot

Answer: CDE

NEW QUESTION 109
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 112
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 115
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 120
You have upgraded your Panorama and Log Collectors lo 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 Mastor Key in Panorama/Master Key and Diagnostic

Answer: C

NEW QUESTION 125
A network security engineer wants to prevent resource-consumption issues on the firewall. Which strategy is consistent with decryption best practices to ensure consistent performance?

A. Use RSA in a Decryption profile tor higher-priority and higher-risk traffic, and use less processor-intensive decryption methods for lower-risk traffic
B. Use PFS in a Decryption profile for higher-priority and higher-risk traffic, and use lessprocessor-intensive decryption methods for tower-risk traffic
C. Use Decryption profiles to downgrade processor-intensive ciphers to ciphers that are less processor-intensive
D. Use Decryption profiles to drop traffic that uses processor-intensive ciphers

Answer: B

NEW QUESTION 126
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 128
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 131
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 133
Four configuration choices are listed, and each could be used to block access to a specific URL
II you configured each choice to block the same URL, then which choice would be evaluated last in the processing order to block access to the URL1?

A. PAN-DB URL category in URL Filtering profile
B. Custom URL category in Security policy rule
C. Custom URL category in URL Filtering profile
D. EDL in URL Filtering profile

Answer: A

NEW QUESTION 137
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 141
What happens when an A/P firewall cluster synchronies IPsec tunnel security associations (SAs)?

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

Answer: A

Explanation:
From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all
IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls."
And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall."
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en_US%E

NEW QUESTION 146
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 150
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 154
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 156
.....

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