Palo-Alto-Networks.PCNSE.vJun-2024.by.Gary.238q

Number: PCNSE
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: PCNSE
Exam Name: Palo Alto Networks Certified Network Security Engineer

Exam A

QUESTION 1
Which log type would provide information about traffic blocked by a Zone Protection profile?

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

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clm9CACZone 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 profileis Threat4. This log type records events such as packet-based attacks, spyware, viruses, vulnerability exploits, and URL filtering.

QUESTION 2
An engineer is creating a template and wants to use variables to standardize the configuration across a large number of devices Which Mo variable types can be defined? (Choose two.)

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

Correct Answer: C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web- interface/panorama-templates/panorama-templates-template-variable

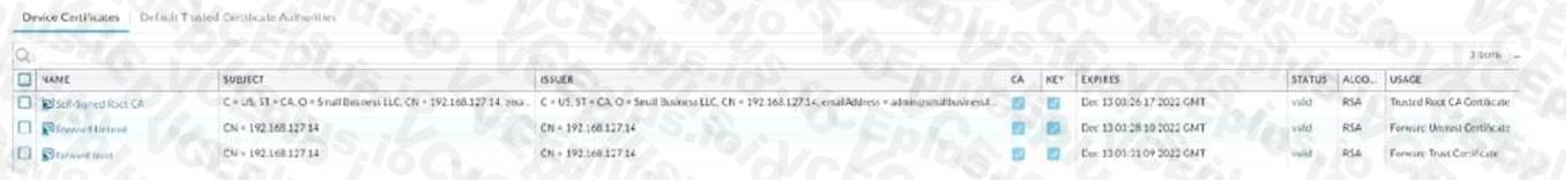
QUESTION 3
An engineer is bootstrapping a VM-Series Firewall Other than the 'config folder, which three directories are mandatory as part of the bootstrap package directory structure? (Choose three.)

A. /software
B. /opt
C. /license
D. /content
E. /plugins

Correct Answer: A, C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series- firewall/prepare-the-bootstrap-package

QUESTION 4

Review the screenshot of the Certificates page.



Device Certificates | Default Trusted Certificate Authorities

3 items

☐	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...	USAGE
☐	Self-Signed Root CA	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, ema...	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.14, emailAddress = admin@smallbusinessll...	☑	☑	Dec 13 03:26:17 2022 GMT	valid	RSA	Trusted Root CA Certificate
☐	Forward-Untrust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	Dec 13 03:28:10 2022 GMT	valid	RSA	Forward Untrust Certificate
☐	Forward-trust	CN = 192.168.127.14	CN = 192.168.127.14	☑	☑	Dec 13 03:31:09 2022 GMT	valid	RSA	Forward Trust Certificate

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

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

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/configure-ssl-forward- proxy

QUESTION 5
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 for faster failover timer settings.
D. Use the Aggressive timer for taster failover timer settings

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha- timers

QUESTION 6
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

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-upgrade/upgrade-panorama- plugins/panorama-plugins-upgrade-downgrade-considerations Before you upgrade to PAN-OS 11.0, you must download the Panorama plugin

version supported on PAN-OS 11.0 for all plugins installed on Panorama. This is required to successfully upgrade to PAN-OS 11.0. See the Compatibility Matrixfor more information.

QUESTION 7
An engineer needs to collect User-ID mappings from the company's existing proxies.
What two methods can be used to pull this data from third party proxies? (Choose two.)

A. Syslog
B. XFF Headers
C. Client probing
D. Server Monitoring

Correct Answer: A, B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/user-id-concepts/user- mapping/xff-headers#idf60a278d-2285-4b19-9cc3-95a4b88d5c51 https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/user-id-concepts/user- mapping/syslog#idee459093-72c1-4ca5-9e44-2c4f359090bb

QUESTION 8
An engineer is in the planning stages of deploying User-ID in a diverse directory services environment.
Which server OS platforms can be used for server monitoring with User-ID?

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

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/user-id-agent/which-servers-can-the-user-id-agent-monitor

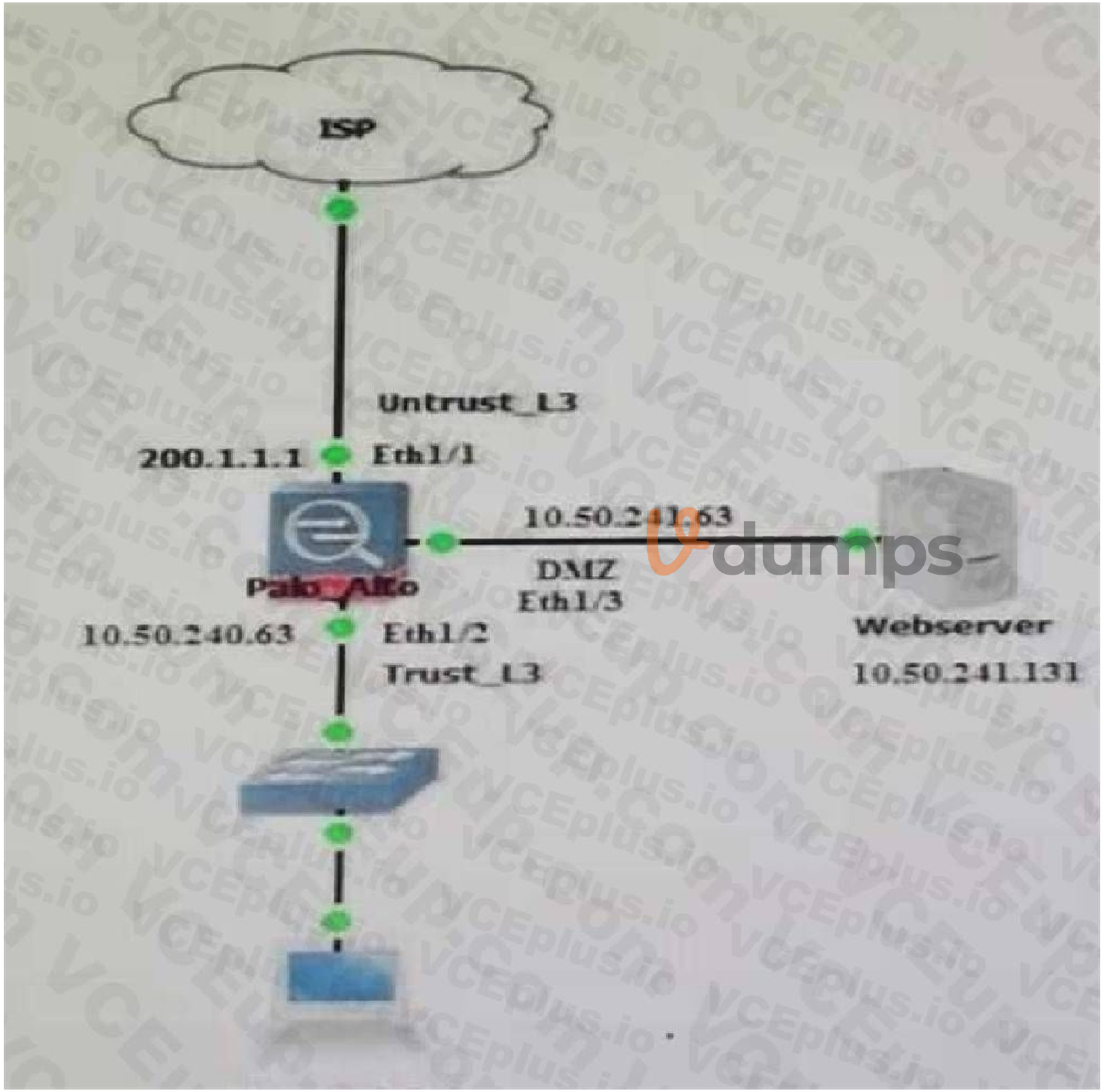
QUESTION 9
What are three reasons for excluding a site from SSL decryption? (Choose three.)

A. the website is not present in English
B. unsupported ciphers
C. certificate pinning
D. unsupported browser version
E. mutual authentication

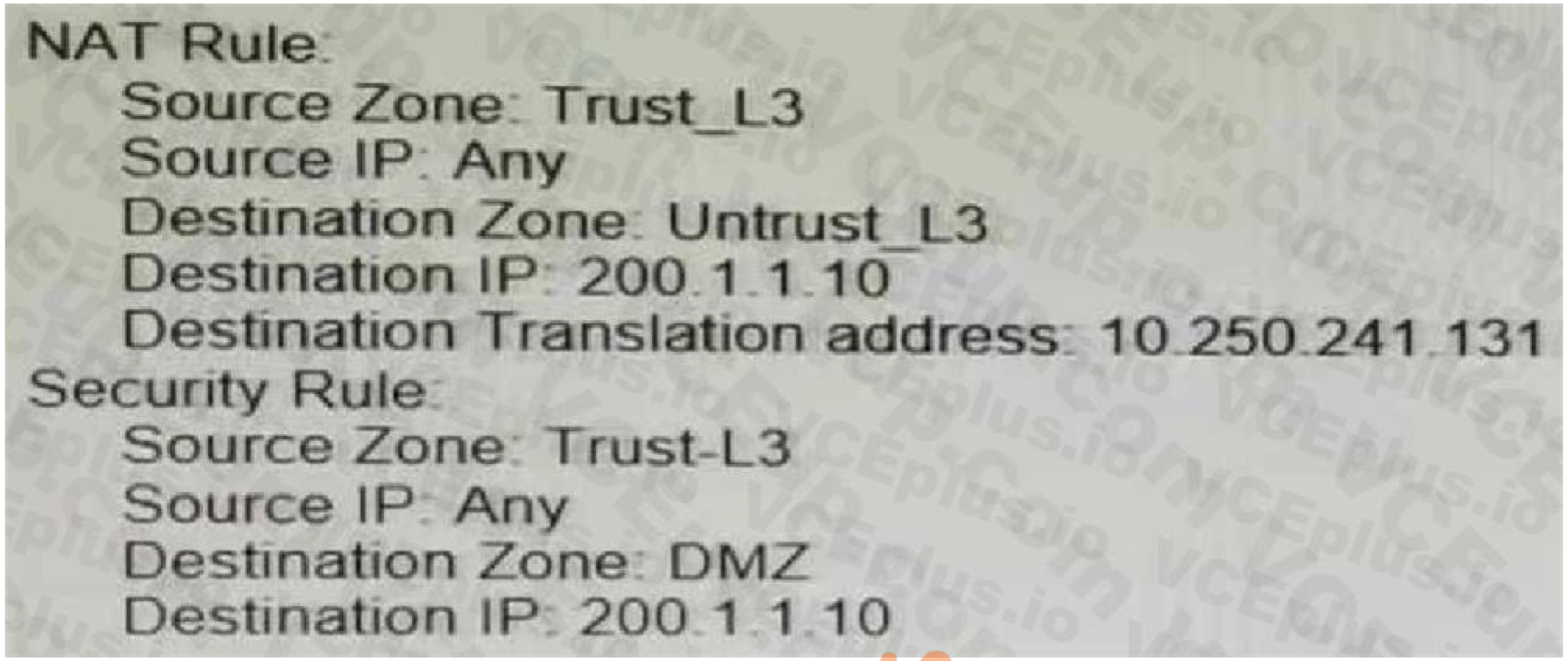
Correct Answer: B, C, E
Section:
Explanation:
Reasons that sites break decryption technically include pinned certificates, client authentication, incomplete certificate chains, and unsupported ciphers. https://docs.paloaltonetworks.com/panos/ 10-1/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption.html

QUESTION 10
A user at an internal system queries the DNS server for their web server with a private IP of 10 250 241 131 in the. The DNS server returns an address of the web server's public address, 200.1.1.10.

In order to reach the web server, which security rule and U-Turn NAT rule must be configured on the firewall?


ISP
Untrust_L3
200.1.1.1
Eth1/1
10.50.241.63
DMZ
Eth1/3
Palo_Alto
10.50.240.63
Eth1/2
Trust_L3
Webserver
10.50.241.131

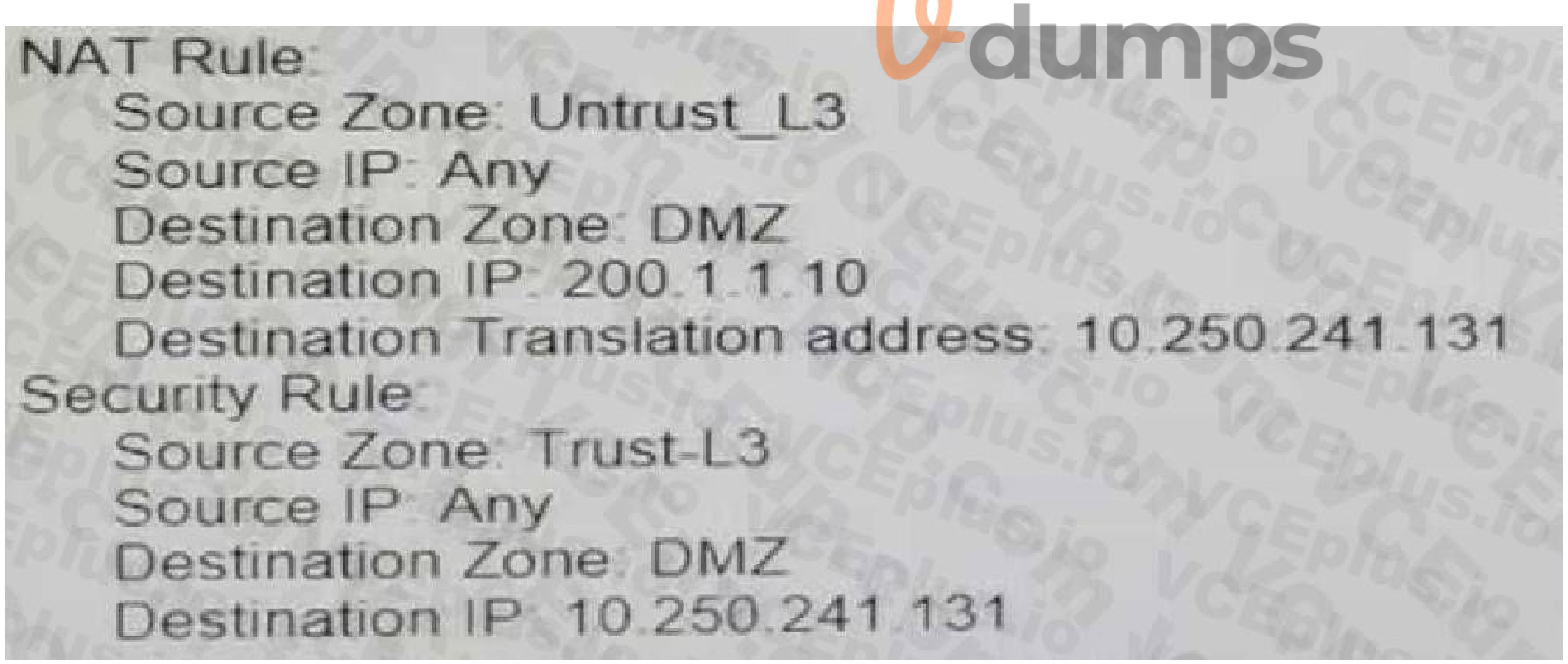
A.



NAT Rule:
Source Zone: Trust_L3
Source IP: Any
Destination Zone: Untrust_L3
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131

Security Rule:
Source Zone: Trust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10

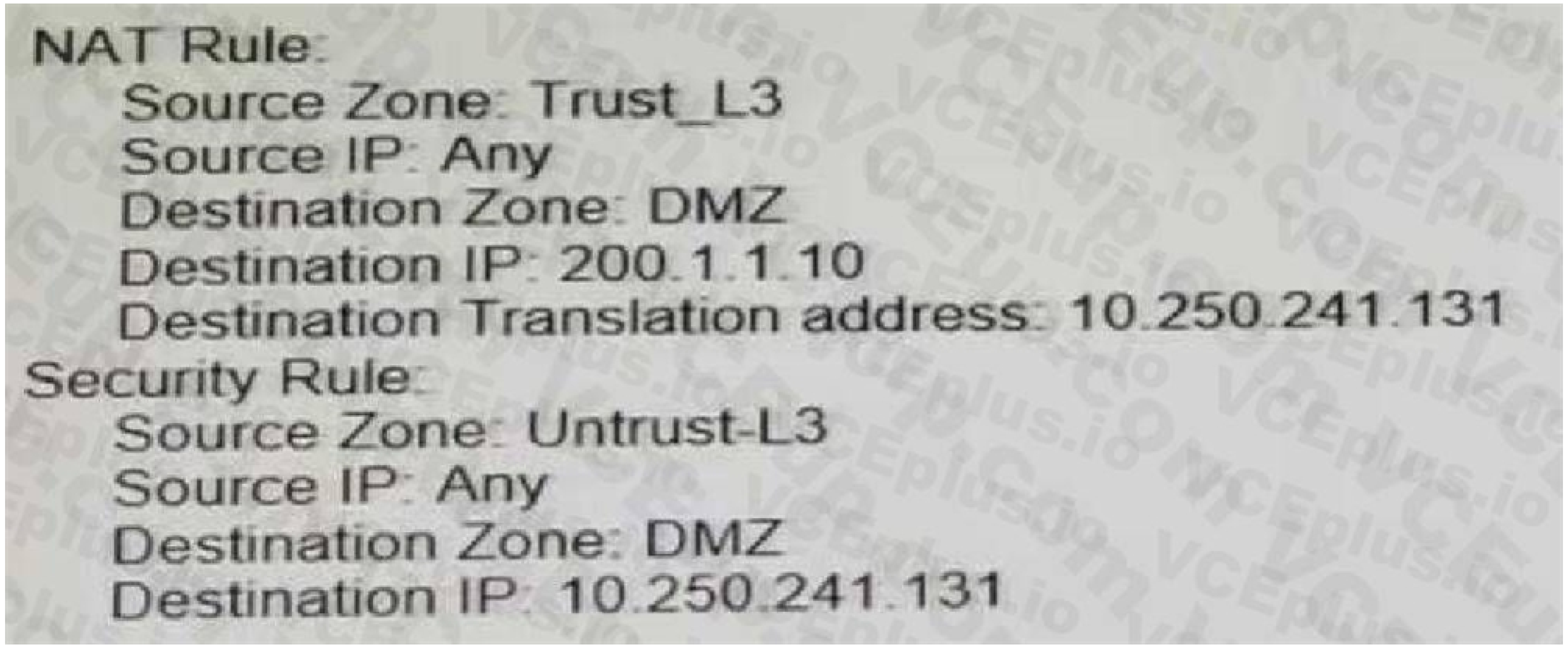
B.



NAT Rule:
Source Zone: Untrust_L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131

Security Rule:
Source Zone: Trust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 10.250.241.131

C.



NAT Rule:

Source Zone: Trust_L3

Source IP: Any

Destination Zone: DMZ

Destination IP: 200.1.1.10

Destination Translation address: 10.250.241.131

Security Rule:

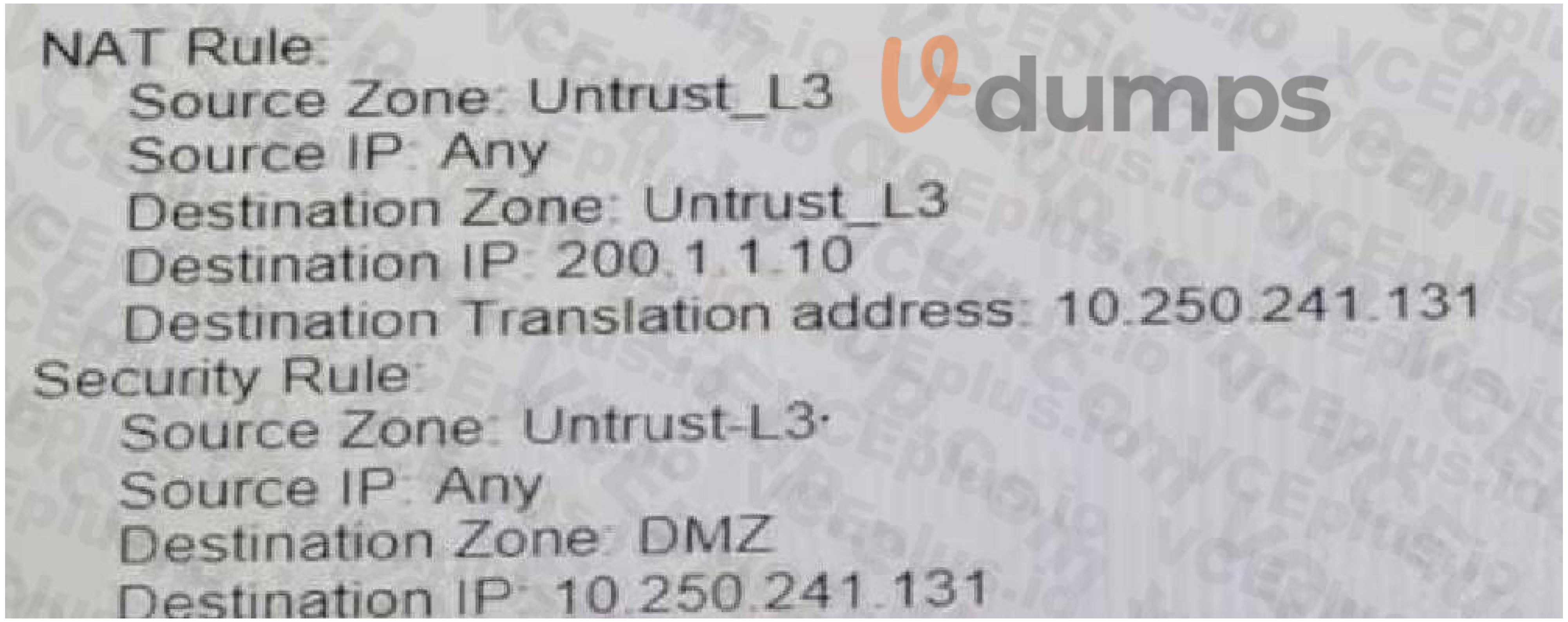
Source Zone: Untrust-L3

Source IP: Any

Destination Zone: DMZ

Destination IP: 10.250.241.131

D.



NAT Rule:

Source Zone: Untrust_L3

Source IP: Any

Destination Zone: Untrust_L3

Destination IP: 200.1.1.10

Destination Translation address: 10.250.241.131

Security Rule:

Source Zone: Untrust-L3

Source IP: Any

Destination Zone: DMZ

Destination IP: 10.250.241.131

Correct Answer: A
Section:

QUESTION 11

An administrator device-group commit push is tailing due to a new URL category How should the administrator correct this issue?

A. verify that the URL seed Tile has been downloaded and activated on the firewall

B. change the new category action to alert" and push the configuration again
C. update the Firewall Apps and Threat version to match the version of Panorama
D. ensure that the firewall can communicate with the URL cloud

Correct Answer: C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw

QUESTION 12
SAML SLO is supported for which two firewall features? (Choose two.)

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

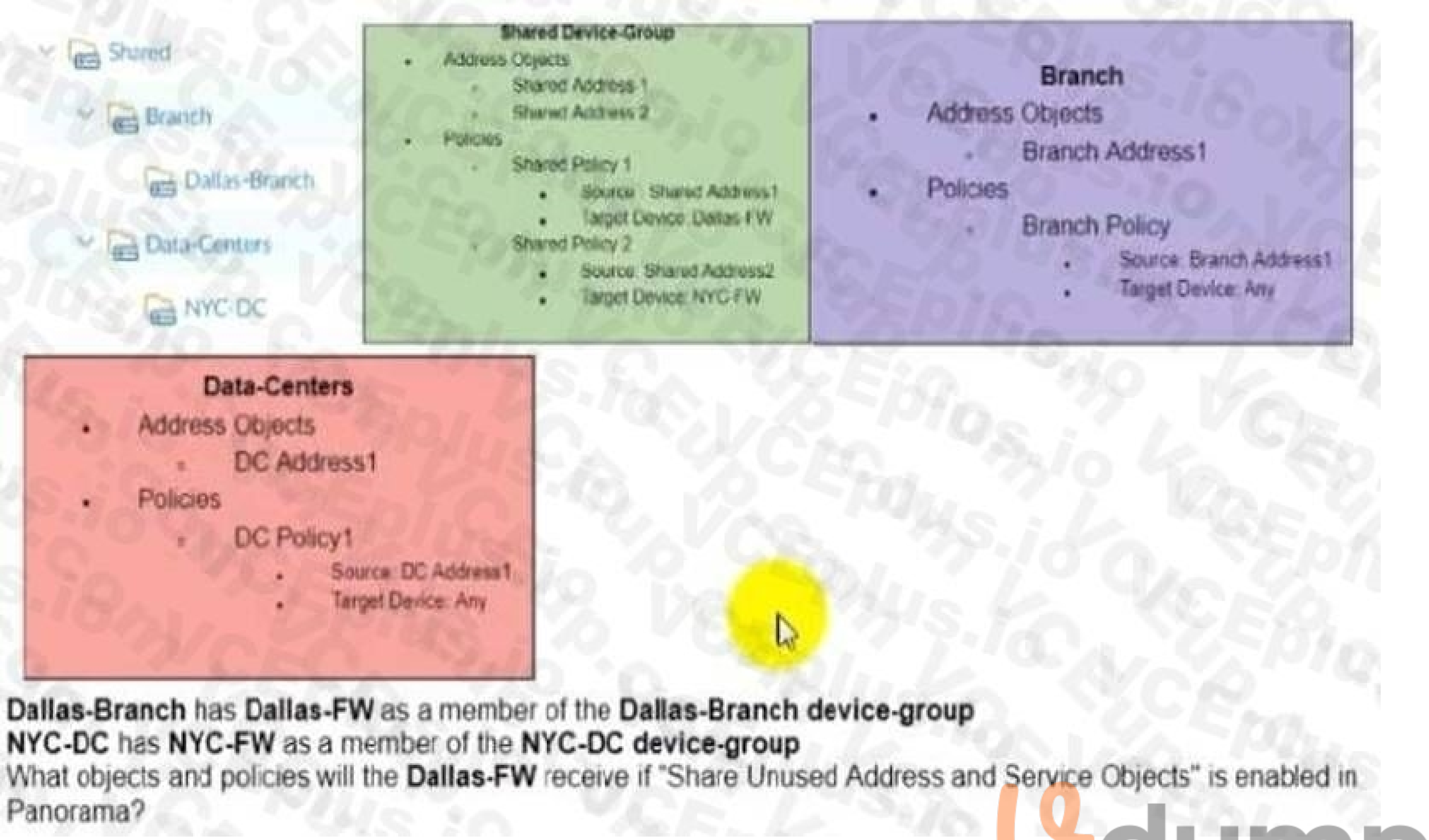
Correct Answer: A, B
Section:
Explanation:
SSO is available to administrators who access the web interface and to end users who access applications through GlobalProtect or Captive Portal. SLO is available to administrators and GlobalProtect end users, but not to Captive Portal end users.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/saml
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/device/device-server-profiles-saml-identity-provider

QUESTION 13
The manager of the network security team has asked you to help configure the company's Security Profiles according to Palo Alto Networks best practice As part of that effort, the manager has assigned you the Vulnerability Protection profile for the internet gateway firewall.
Which action and packet-capture setting for items of high severity and critical severity best matches Palo Alto Networks best practice?

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

Correct Answer: C
Section:

QUESTION 14
The following objects and policies are defined in a device group hierarchy



Shared Device-Group

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

Branch

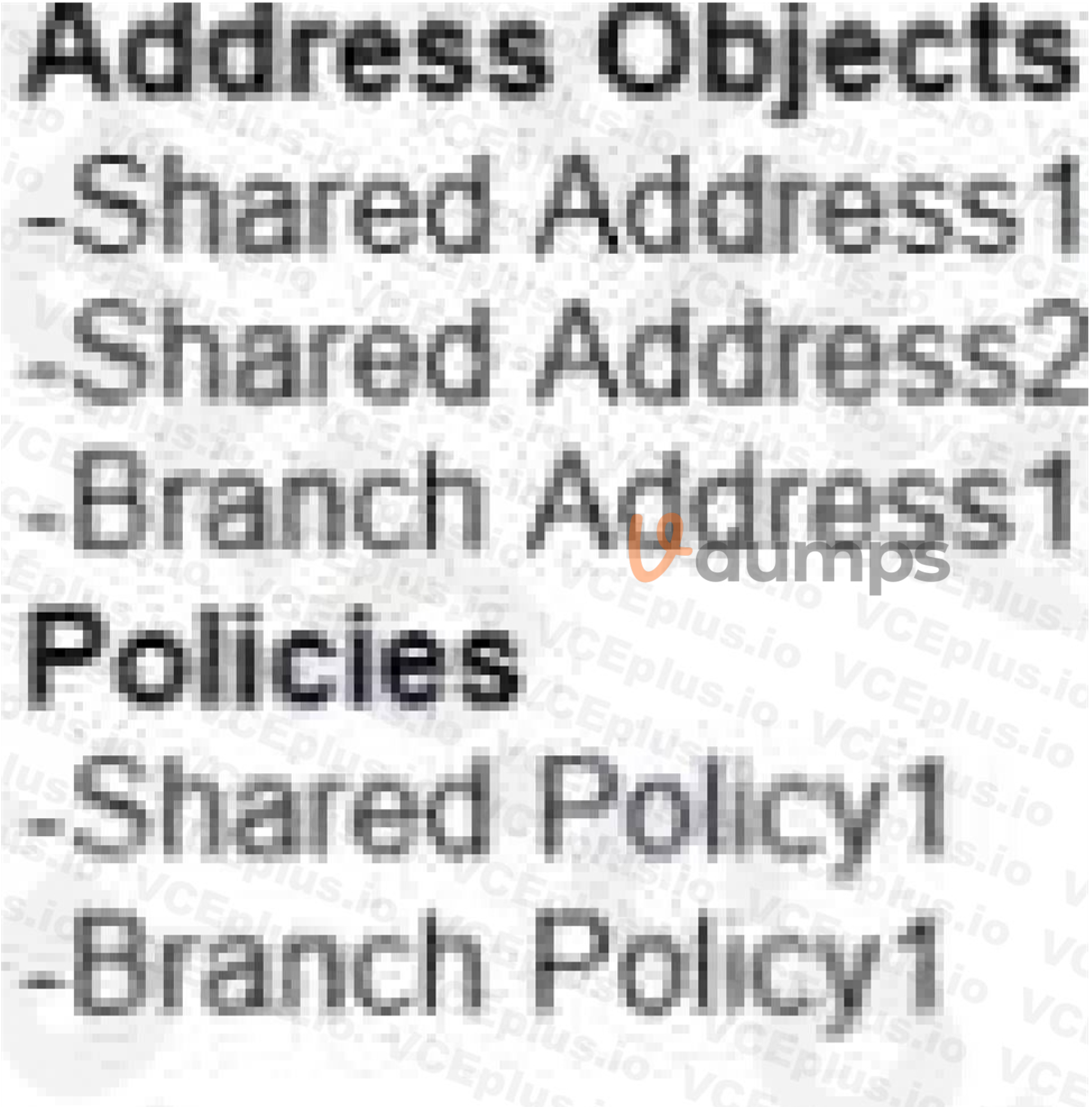
- Address Objects
  - Branch Address1
- Policies
  - Branch Policy
    - Source: Branch Address1
    - Target Device: Any

Data-Centers

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

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

A.



Address Objects

-Shared Address1

-Shared Address2

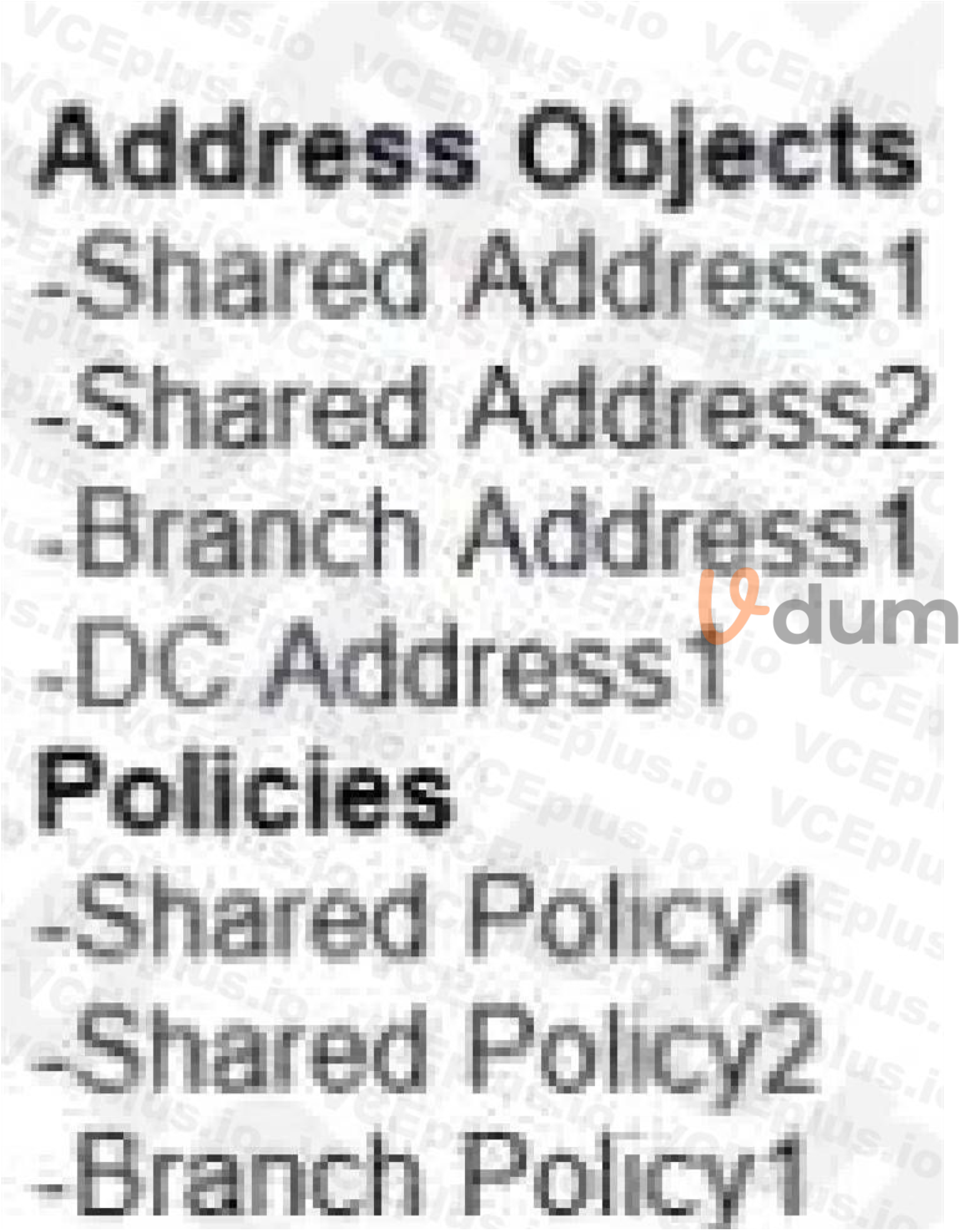
-Branch Address1

Policies

-Shared Policy1

-Branch Policy1

B.



Address Objects

-Shared Address1

-Shared Address2

-Branch Address1

-DC Address1

Policies

-Shared Policy1

-Shared Policy2

-Branch Policy1

C. Address Objects
-Shared Address 1
-Branch Address2 Policies
-Shared Polic1 l
-Branch Policy1

D. Address Objects -Shared Addressl -Shared Address2 -Branch Addressl Policies -Shared Policyl -Shared Policy2 -Branch Policy1

Correct Answer: A
Section:

QUESTION 15
An administrator is attempting to create policies tor deployment of a device group and template stack. When creating the policies, the zone drop down list does not include the required zone.
What must the administrator do to correct this issue?

A. Specify the target device as the master device in the device group

B. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings

C. Add the template as a reference template in the device group

D. Add a firewall to both the device group and the template

Correct Answer: C
Section:
Explanation:
Short According to the Palo Alto Networks documentation, "To use a template stack for a device group, you must add the template stack as a reference template in the device group. This enables you to use zones and interfaces defined in the template stack when creating policies for the device group." Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks

QUESTION 16
An existing NGFW customer requires direct interne! access offload locally at each site and iPSec connectivity to all branches over public internet. One requirement is mat no new SD-WAN hardware be introduced to the environment.
What is the best solution for the customer?

A. Configure a remote network on PAN-OS

B. Upgrade to a PAN-OS SD-WAN subscription

C. Deploy Prisma SD-WAN with Prisma Access

D. Configure policy-based forwarding

Correct Answer: B
Section:
Explanation:
According to the Palo Alto Networks documentation, "The PAN-OS software now includes a native SD-WAN subscription to provide intelligent and dynamic path selection on top of the industry- leading security that PAN-OS software already delivers. Key features of the SD-WAN implementation include centralized configuration management, automatic VPN topology creation, traffic distribution, monitoring, and troubleshooting." Reference: https:// docs.paloaltonetworks.com/sd-wan

QUESTION 17
Which GlobalProtect component must be configured to enable Clientless VPN?

A. GlobalProtect satellite

B. GlobalProtect app

C. GlobalProtect portal
D. GlobalProtect gateway

Correct Answer: C
Section:
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

QUESTION 18
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

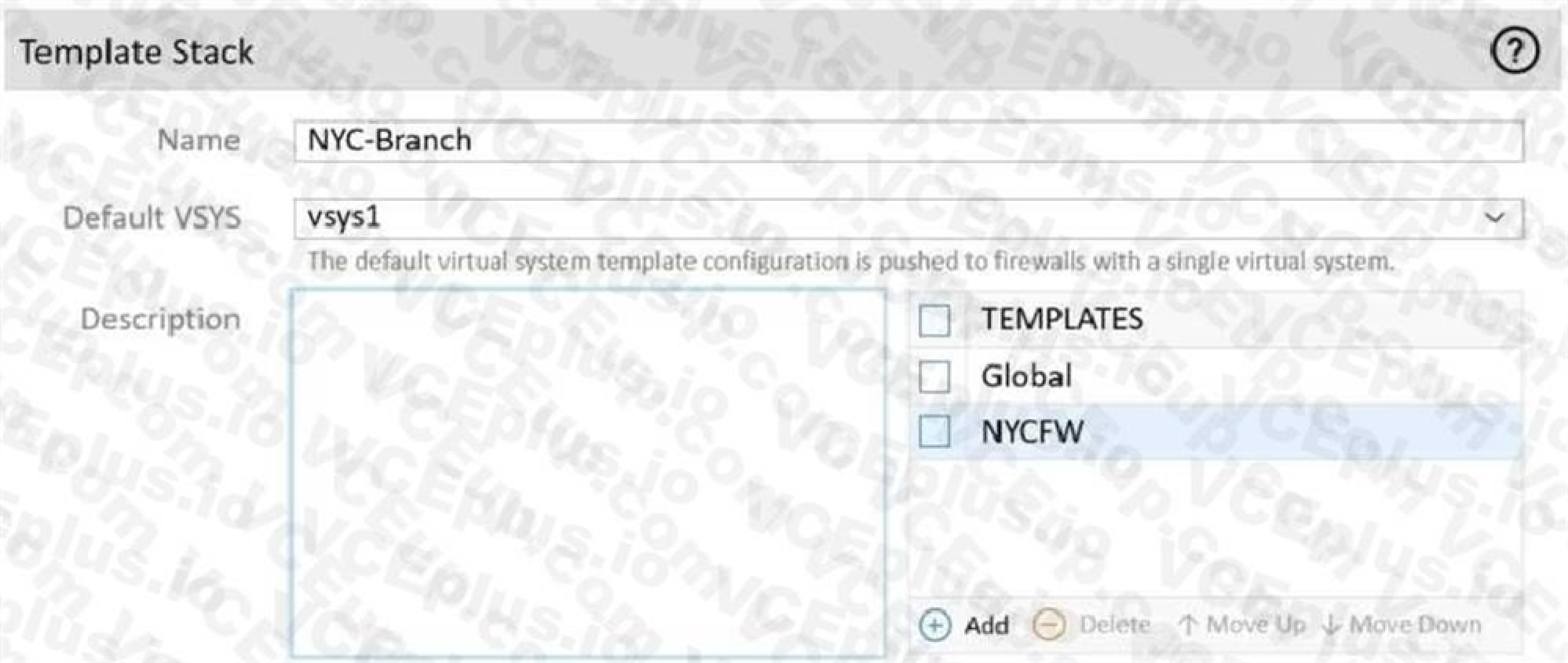
Correct Answer: C
Section:
Explanation:
According to the Palo Alto Networks documentation, "A successful phase 2 negotiation requires not only that the security proposals match, but also the proxy-ids on either peer, be a mirror image of each other. So it is mandatory to configure the proxy-IDs whenever you establish a tunnel between the Palo Alto Network firewall and the firewalls configured for policy-based VPNs." The log message indicates that the local and remote IDs are identical, which means they are not mirrored.Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClW8CAK

QUESTION 19
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

Correct Answer: D
Section:
Explanation:
According to the Palo Alto Networks documentation, "To configure a service route, you must specify a source interface and a source address. The source interface can be any data port (Ethernet interface) or a loopback interface. The source address must be a static IP address that is configured on the source interface." Reference: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/service- routes/service-routes-overview

QUESTION 20
Refer to the image.


Template Stack

Name NYC-Branch

Default VSYS vsys1

The default virtual system template configuration is pushed to firewalls with a single virtual system.

Description

□ TEMPLATES

□ Global

□ NYCFW

An administrator is tasked with correcting an NTP service configuration for firewalls that cannot use the Global template NTP servers. The administrator needs to change the IP address to a preferable server for this template stack but cannot impact other template stacks.
How can the issue be corrected?

A. Override the value on the NYCFW template.
B. Override a template value using a template stack variable.
C. Override the value on the Global template.
D. Enable "objects defined in ancestors will take higher precedence" under Panorama settings.

Correct Answer: B
Section:
Explanation:
Both templates and template stacks support variables. Variables allow you to create placeholder objects with their value specified in the template or template stack based on your configuration needs. Create a template or template stack variable to replace IP addresses, Group IDs, and interfaces in your configurations. https://docs.paloaltonetworks.com/panorama/10-0/panorama- admin/manage-firewalls/manage-templates-and-template-stacks/override-a-template-setting.html

QUESTION 21
You need to allow users to access the office-suite applications of their choice. How should you configure the firewall to allow access to any office-suite application?

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

Correct Answer: C
Section:
Explanation:

According to the Palo Alto Networks documentation, "Application filters enable you to create groups of applications based on specific characteristics such as subcategory, technology, risk factor, and so on. You can then use these groups in Security policy rules to allow or block access to the applications.For example, you can create an application filter that includes all applications in the office-programs subcategory and use it in a Security policy rule to allow access to any office-suite application." Reference: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage- applications-in-a-policy/use-application-filters-in-policy

QUESTION 22

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 SYN. ICMP ICMPv6, UDP. and other IP flood attacks

C. Add a WildFire subscription to activate DoS and zone protection features

D. Replace the hardware firewall because DoS and zone protection are not available with VM-Series systems

Correct Answer: A
Section:
Explanation:
1 - https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-bestpractices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-bestpractices.html#:~:text=DoS%20and%20Zone%20Protection%20help,device%20at%20the%20internet%20perimeter.
2 - https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dosprotection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds/how-tomeasure-cps.html
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dosprotection.html

QUESTION 23

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

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/bootstrap-the-vm- series-firewall/bootstrap-the-vm-series-firewall-in-azure The bootstrap process failed for the VM-Series firewall in Azure because the /content folder is missing from the bootstrap package 1. Reference: 1: Bootstrap the VM-Series Firewall on Azure - Palo Alto Networks

QUESTION 24

A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas) i. 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) ii. Enterprise-Untrusted-CA, which is verified as Forward Untrust Certificate iii. Enterprise-Intermediate-CA iv. Enterprise-Root-CA which is verified only as Trusted Root CA An end-user visits https // www example-website com/ with a server certificate Common Name (CN) www example-website com The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewall The end-user's browser will show that the certificate for www.example-website.com was issued by which of the following?

A. Enterprise-Untrusted-CA which is a self-signed CA

B. Enterprise-Trusted-CA which is a self-signed CA

C. Enterprise-Intermediate-CA which was. in turn, issued by Enterprise-Root-CA

D. Enterprise-Root-CA which is a self-signed CA

Correct Answer: A
Section:

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward- proxyEnterprise-Trusted-CA is installed in the trusted store of the end-user browser and system. So it should not lead to any certificate issue.
The most possible that www.example-website.com is signed by not trusted certificate authority which leads to use Enterprise-Untrusted-CA, which is not trusted as well

QUESTION 25
An administrator allocates bandwidth to a Prisma Access Remote Networks compute location with three remote networks.
What is the minimum amount of bandwidth the administrator could configure at the compute location?

A. 90Mbps
B. 300 Mbps
C. 75Mbps
D. 50Mbps

Correct Answer: D
Section:
Explanation:
The number you specify for the bandwidth applies to both the egress and ingress traffic for the remote network connection. If you specify a bandwidth of 50 Mbps, Prisma Access provides you with a remote network connection with 50 Mbps of bandwidth on ingress and 50 Mbps on egress. Your bandwidth speeds can go up to 10% over the specified amount without traffic being dropped; for a 50 Mbps connection, the maximum bandwidth allocation is 55 Mbps on ingress and 55
Mbps on egress (50 Mbps plus 10% overage allocation).
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prismaaccess-for-networks/how-to-calculate-network-bandwidth

QUESTION 26
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

Correct Answer: C
Section:
Explanation:
HA Promotion Hold Time is the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost 2. Reference: 2: PAN-OS Æ New Features Guide

QUESTION 27
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

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

Correct Answer: D
Section:
Explanation:
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capture-on-the-management-interface.html

QUESTION 28
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.

Correct Answer: C
Section:

QUESTION 29
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

Correct Answer: A, C
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/static-routes/static-route-removal-based-on-path-monitoring.html
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/static-routes/configure-a-static-route.html

QUESTION 30
An administrator has configured PAN-OS SD-WAN and has received a request to find out the reason for a session failover for a session that has already ended Where would you find this in Panorama or firewall logs?

A. Traffic Logs
B. System Logs
C. Session Browser
D. You cannot find failover details on closed sessions

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/configure-sd-wan/sd-wan-traffic- distribution-profiles

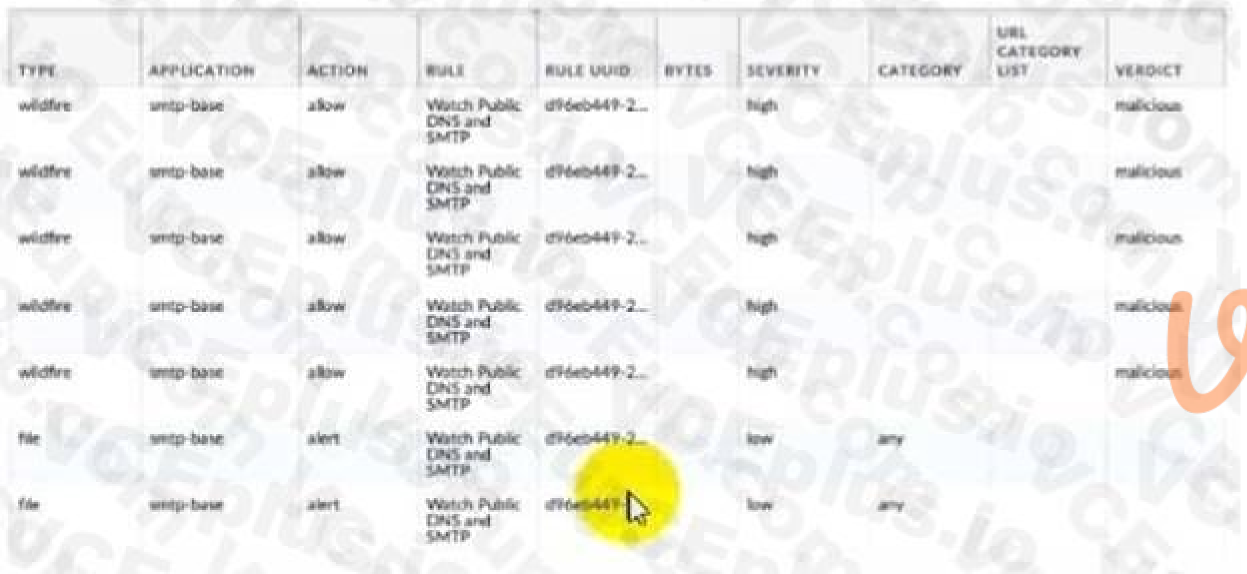
QUESTION 31
SSL Forward Proxy decryption is configured but the firewall uses Untrusted-CA to sign the website https //www important-website com certificate End-users are receiving me "security certificate isnot trusted is warning Without SSL decryption the web browser shows that the website certificate istrusted 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 import Well- Known-lntermediate-CA and Well-Known-Root-CA select the Trusted Root CA checkbox and commit the configuration
B. Install the Well-Known-lntermediate-CA and Well-Known-Root-CA certificates on all end-user systems m the user and local computer stores
C. Navigate to Device > Certificate Management - Certificates s Default Trusted Certificate Authorities import Well-Known-intermediate-CA and Well-Known-Root-CA select the Trusted Root CA check box and commit the configuration
D. Clear the Forward Untrust Certificate check box on the Untrusted-CA certificate and commit the configuration

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/device/device- certificate-management-certificates/manage-default-trusted-certificate-authorities

QUESTION 32
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		low	any		

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

Correct Answer: A
Section:
Explanation:
Threats that have the ability to become critical but have mitigating factors; for example, they may be difficult to exploit, do not result in elevated privileges, or do not have a large victim pool. WildFire Submissions log entries with a malicious verdict and an action set to allow are logged as High.https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage- logs/log-types-and-severity-levels/threat-logs#id5cea1511-a153-4005-9d5f-ab2482e838ae

QUESTION 33
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

Correct Answer: C
Section:
Explanation:
Report generation can also consume considerable resources, while some pre-defined reports may not be useful to the organization, or they've been replaced by a custom report. These pre-defined reports can be disabled from Device >
Setup > Logging and Reporting Settingshttps://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSvCAK

QUESTION 34
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

Correct Answer: A
Section:
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-usage/ports-used-for-globalprotect.html

QUESTION 35
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?

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

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

QUESTION 36
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

Correct Answer: A, C, E
Section:

QUESTION 37
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.

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama- overview/centralized-firewall-configuration-and-update-management/templates-and-template- stacks

QUESTION 38
WildFire will submit for analysis blocked files that match which profile settings?

A. files matching Anti-Spyware signatures
B. files that are blocked by URL filtering
C. files that are blocked by a File Blocking profile
D. files matching Anti-Virus signatures

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud- features/wildfire-analysis-of-blocked-files

QUESTION 39
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

Correct Answer: B
Section:

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

QUESTION 40
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

Correct Answer: C
Section:
Explanation:
If you have a Simple Certificate Enrollment Protocol (SCEP) server in your enterprise PKI, you can configure a SCEP profile to automate the generation and distribution of unique client certificates.https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/obtain- certificates/deploy-certificates-using-scep

QUESTION 41
During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons. In this case, the technical reason is unsupported ciphers. Traffic to these sites will therefore be blocked if decrypted How should the engineer proceed?

A. Allow the firewall to block the sites to improve the security posture
B. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption
C. Install the unsupported cipher into the firewall to allow the sites to be decrypted
D. Create a Security policy to allow access to those sites

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions Traffic that breaks decryption for technical reasons, such as using a pinned certificate, an incomplete certificate chain, unsupported ciphers, or mutual authentication (attempting to decrypt the traffic results in blocking the traffic). Palo Alto Networks provides a predefined SSL Decryption Exclusion list (DeviceCertificate ManagementSSL Decryption Exclusion) that excludes hosts with applications and services that are known to break decryption technically from SSL Decryption by default. If you encounter sites that break decryption technically and are not on the SSL Decryption Exclusion list, you can add them to list manually by server hostname. The firewall blocks sites whose applications and services break decryption technically unless you add them to the SSL Decryption Exclusion list.

QUESTION 42
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.

Correct Answer: A
Section:
Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates

QUESTION 43
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 SYN. ICMP ICMPv6, UDP. and other IP flood attacks
C. Add a WildFire subscription to activate DoS and zone protection features
D. Replace the hardware firewall because DoS and zone protection are not available with VM-Series systems

Correct Answer: A
Section:
Explanation:
1 - https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-bestpractices.html#:~:text=DoS%20and%20Zone%20Protection%20help,device%20at%20the%20internet%20perimeter.
2 - https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dosprotection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds/how-to-measure-cps.html
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dosprotection.html

QUESTION 44
An engineer wants to implement the Palo Alto Networks firewall in VWire mode on the internet gateway and wants to be sure of the functions that are supported on the vwire interface What are three supported functions on the VWire interface? (Choose three)

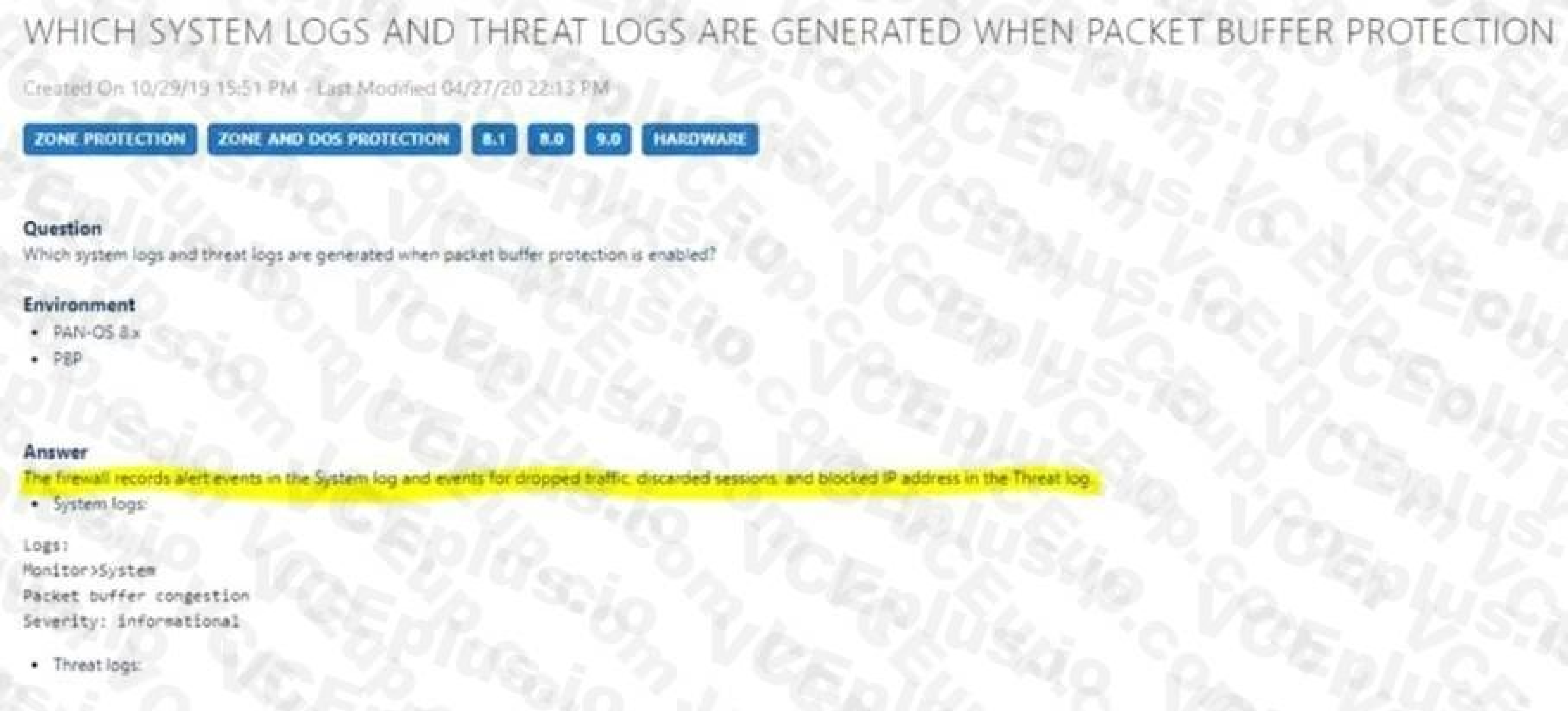
A. NAT
B. QoS
C. IPSec
D. OSPF
E. SSL Decryption

Correct Answer: A, B, E
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces"The virtual wire supports blocking or allowing traffic based on virtual LAN (VLAN) tags, in addition to supporting security policy rules, App-ID, Content-ID, User-ID, decryption, LLDP, active/passive and active/active HA, QoS, zone protection (with some exceptions), non-IP protocol protection, DoS protection, packet buffer protection, tunnel content inspection, and NAT."

QUESTION 45
Where is information about packet buffer protection logged?

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

Correct Answer: D
Section:
Explanation:



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

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:

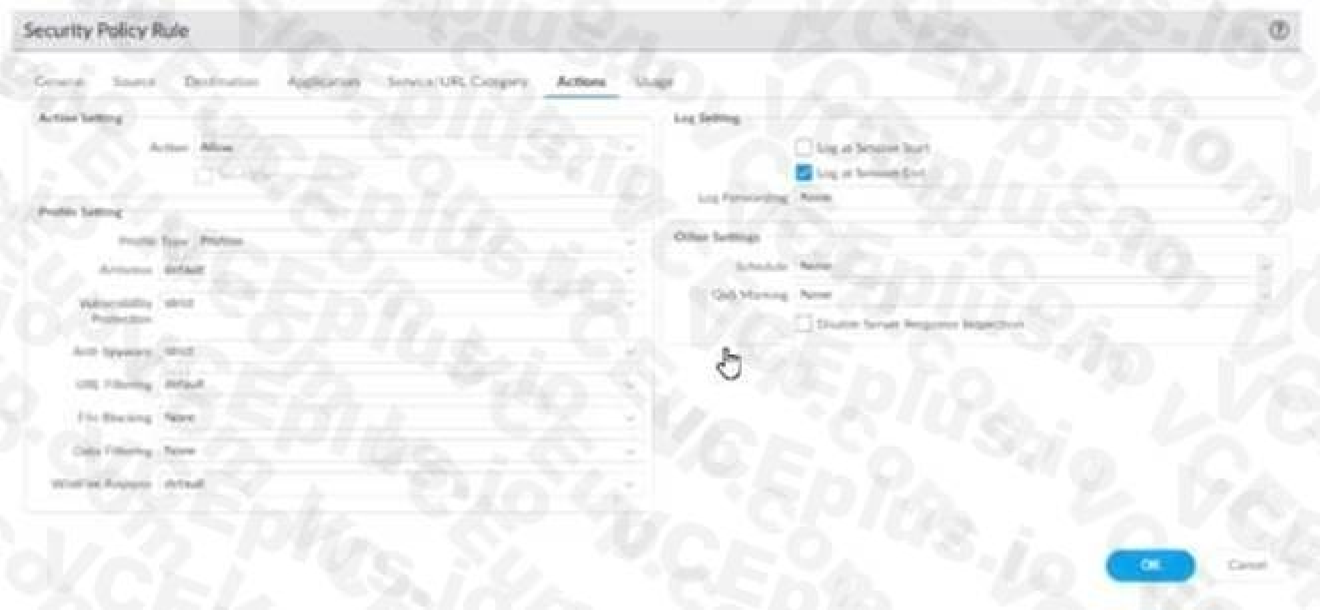
```
Logs:
Monitor>System
Packet buffer congestion
Severity: informational
```

- Threat logs:

QUESTION 46

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

Action Setting

Action: Allow

Profile Setting

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: strict

Anti-Spyware: strict

URL Filtering: default

File Blocking: None

Data Filtering: None

WildFire Analysis: default

Log Setting

☐ Log at Session Start

☑ Log at Session End

Log Forwarding: None

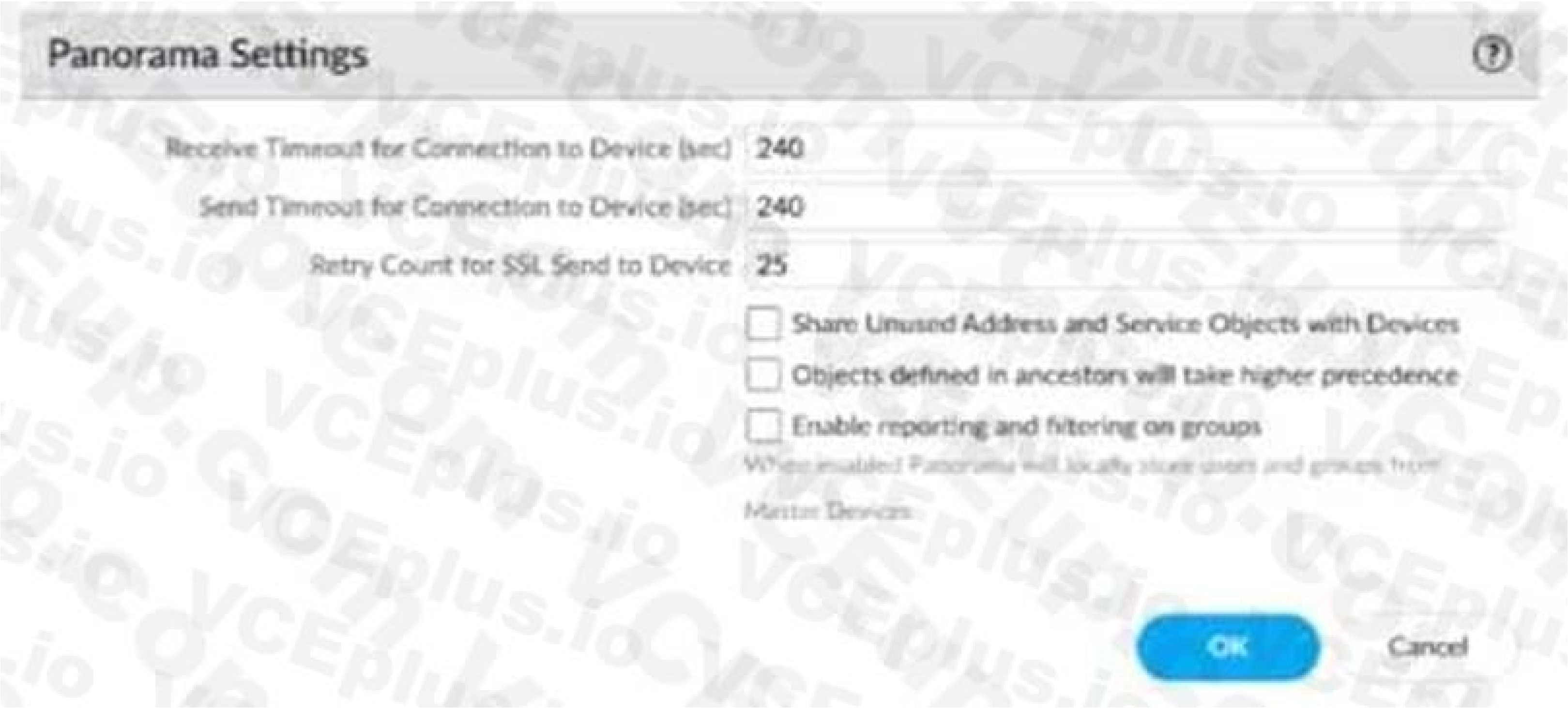
Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

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

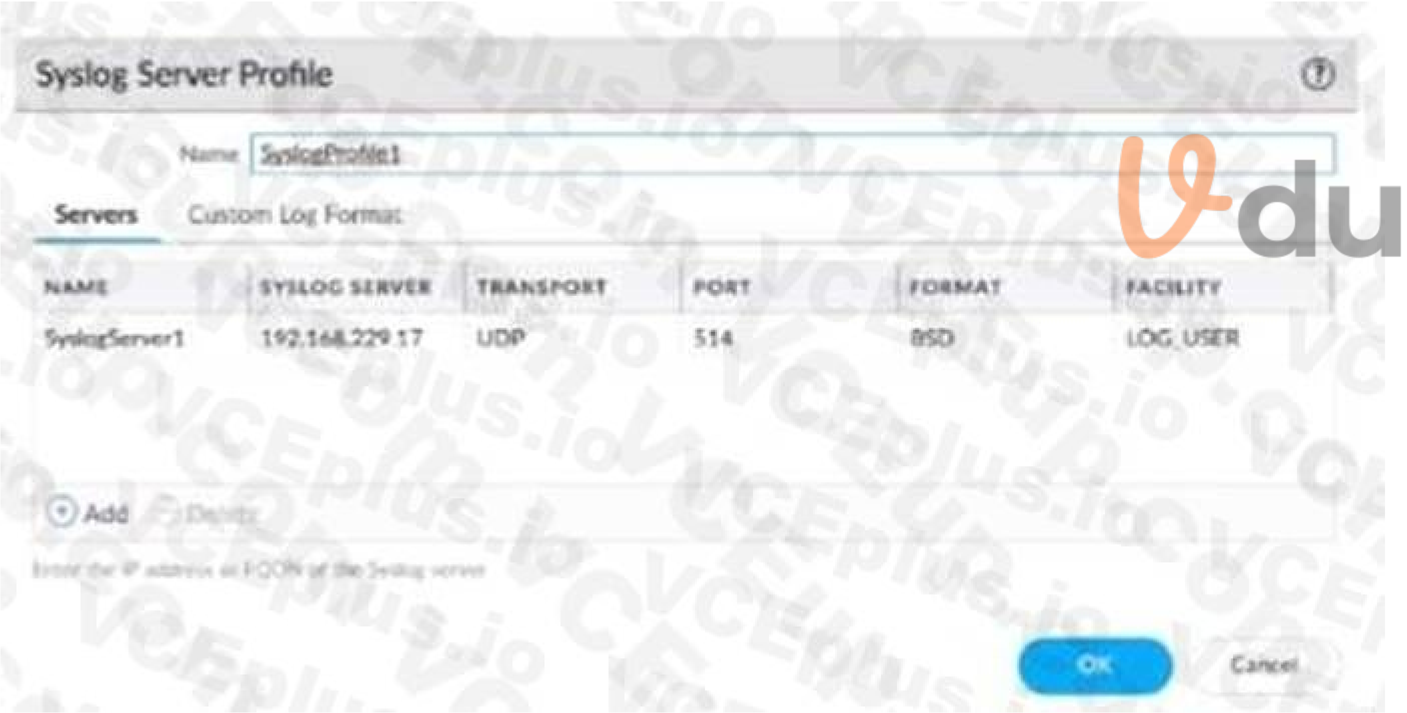
□ Share Unused Address and Service Objects with Devices

□ 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 Devices

C.



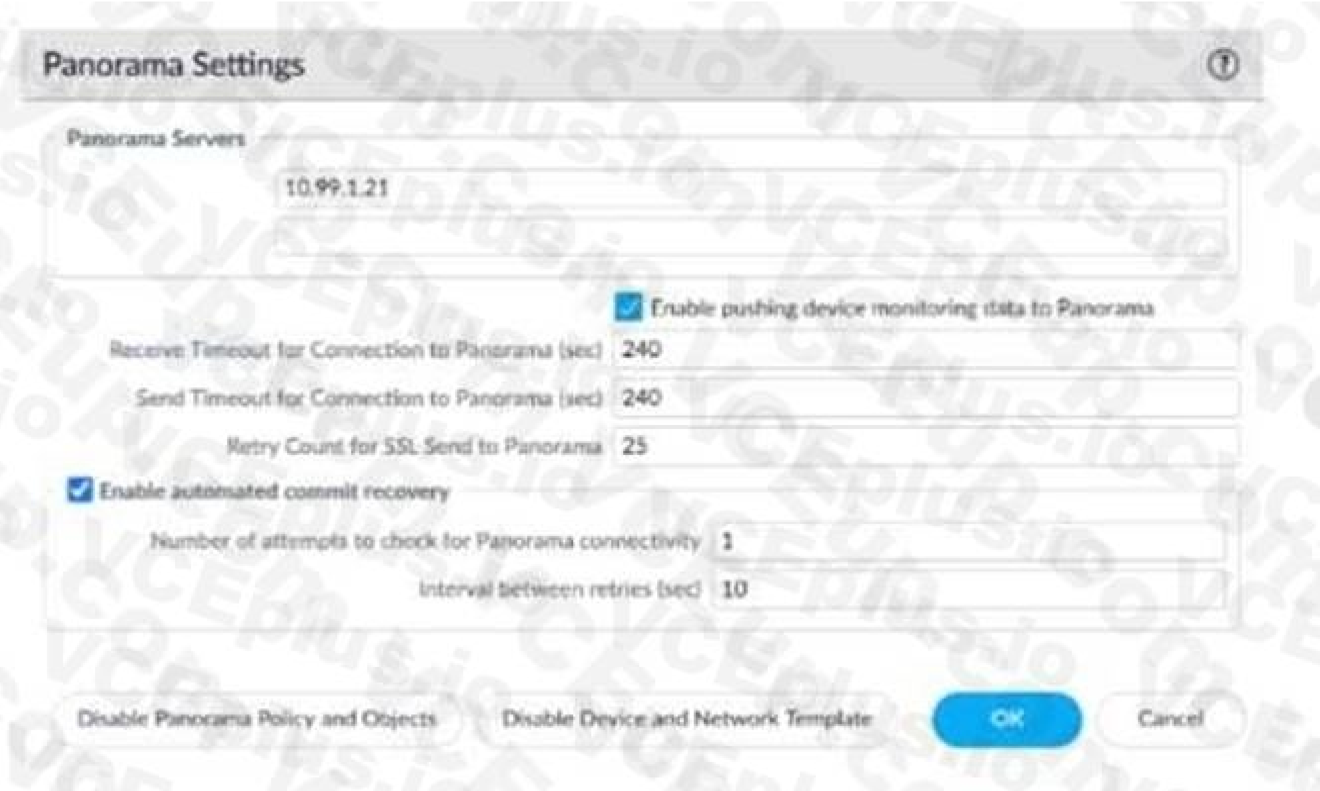
Syslog Server Profile

Name SyslogProfile1

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

Enter the IP address or FQDN of the Syslog server

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

E. Option A
F. Option B
G. Option C
H. Option D

Correct Answer: C
Section:

QUESTION 47
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

Correct Answer: A
Section:
Explanation:
The Best Practice Assessment (BPA) tool compares the configuration of firewalls and Panorama to the Palo Alto Networks best practice recommendations. Run the BPA periodically to identify security weaknesses, see the best practice settings, and implement them to improve your security posture.https://docs.paloaltonetworks.com/best-practices/10-2/bpa-getting-started

QUESTION 48
A network administrator plans a Prisma Access deployment with three service connections, each with a BGP peering to a CPE. The administrator needs to minimize the BGP configuration and management overhead on on-prem network devices.
What should the administrator implement?

A. target service connection for traffic steering

B. summarized BGP routes before advertising
C. hot potato routing
D. default routing

Correct Answer: B
Section:
Explanation:
The best way to minimize the BGP configuration and management overhead on on-prem network devices is to summarize BGP routes before advertising them. Route summarization is a technique that reduces the number of routes in a routing table by aggregating multiple routes into a single route with a less specific prefix. This reduces the size of routing updates and the memory and CPUusage of routers. Prisma Access supports route summarization for service connections and remotenetwork connections that use BGP routing1. You should not implement target service connection for traffic steering, as this is a feature that allows you to select a specific service connection for traffic from a remote network connection or a mobile user based on destination IP address orapplication. This does not affect the BGP configuration or management on on-prem networkdevices2. You should not implement hot potato routing, as this is a routing technique that selects the closest exit point to the destination network based on the number of hops or the lowest IGPmetric. This does not affect the BGP configuration or management on on-prem network devices3.You should not implement default routing, as this is a routing technique that uses a default route to forward packets to an unknown destination. This does not affect the BGP configuration ormanagement on on-prem network devices, and it may not provide optimal routing for Prisma Access traffic4. Reference: 1: https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access- panorama-admin/prepare-the-prisma-access-infrastructure/service-connection-overview/configure- route-summarization-for-service-connections 2: https://docs.paloaltonetworks.com/prisma/prisma- access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/service- connection-overview/target-service-connection-for-traffic-steering 3: https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed- admin/prisma-access-service-connections/service-connection-routing 4:https://docs.paloaltonetworks.com/prisma/prisma-access/ prisma-access-cloud-managed- admin/prisma-access-service-connections/service-connection-routing/routing-for-service-connection-traffic-cloud-management.html

QUESTION 49
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

Correct Answer: D
Section:
Explanation:
Logging is a function that is handled by the management plane (control plane) of a Palo Alto Networks firewall. The management plane is responsible for managing and configuring the firewall, as well as generating and storing logs and reports. The management plane communicates with the data plane (also known as the packet forwarding plane) through an internal backplane interface.Signature matching for content inspection, IPSec tunnel standup, and Quality of Service are functions that are handled by the data plane of a Palo Alto Networks firewall. The data plane is responsible for processing and forwarding packets, as well as applying security policies and features to the traffic.The data plane consists of multiple dedicated hardware components, such as the Single-Pass Parallel Processing (SP3) engine, the Security Processing Unit (SPU), and the Network Processing Unit (NPU).Reference: : https://docs.paloaltonetworks.com/ pan-os/10-2/pan-os-admin/firewall- administration/manage-firewall-administrators/firewall-management-interfaces :https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/firewall- concepts/firewall-overview

QUESTION 50
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

Correct Answer: B, E
Section:

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

QUESTION 51
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.

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices/decryption-best- practices/plan-ssl-decryption-best-practice-deployment https://live.paloaltonetworks.com/t5/general-topics/decrypt-guest-network-traffic/td-p/119388

QUESTION 52
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

Correct Answer: A, C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration

QUESTION 53
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

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/deploy-user-id-in-a-large- scale-network/redistribute-user-mappings-and-authentication-timestamps/firewall-deployment-for- user-id-redistribution#ide3661b46-4722-4936-bb9b-181679306809

QUESTION 54
An engineer is configuring Packet Buffer Protection on ingress zones to protect from single-session DoS attacks Which sessions does Packet Buffer Protection apply to?

A. It applies to existing sessions and is not global

B. It applies to new sessions and is global

C. It applies to new sessions and is not global

D. It applies to existing sessions and is global

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos- protection/zone-defense/packet-buffer-protection

QUESTION 55
The administrator for a small company has recently enabled decryption on their Palo Alto Networks firewall using a self-signed root certificate. They have also created a Forward Trust and Forward Untrust certificate and set them as such
The admin has not yet installed the root certificate onto client systems What effect would this have on decryption functionality?

A. Decryption will function and there will be no effect to end users

B. Decryption will not function because self-signed root certificates are not supported

C. Decryption will not function until the certificate is installed on client systems

D. Decryption will function but users will see certificate warnings for each SSL site they visit

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEZCA0

QUESTION 56
A firewall has Security policies from three sources

A. locally created policies

B. shared device group policies as pre-rules

C. the firewall's device group as post-rules
How will the rule order populate once pushed to the firewall?

D. shared device group policies, firewall device group policies. local policies.

E. firewall device group policies, local policies. shared device group policies

F. shared device group policies. local policies, firewall device group policies

G. local policies, firewall device group policies, shared device group policies

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage- device-groups/manage-the-rule-hierarchy

QUESTION 57
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

Correct Answer: A, C, E
Section:
Explanation:
Active/Active high availability is a deployment mode that allows both firewalls in an HA pair to actively process traffic and share the load. Active/Active HA is suitable for environments that require real, full-time redundancy from both firewalls at all times, as there is no failover time or session loss in case of a firewall failure. Active/Active HA is also suitable for environments that require that both firewalls maintain their own routing tables for faster dynamic routing protocol convergence, as each firewall can run its own routing protocols and exchange routes with other routers independently.Active/Active HA is also suitable for environments that require that traffic be load-balanced across both firewalls to handle peak traffic spikes, as each firewall can process a portion of the traffic and increase the overall throughput and performance. Active/Active HA is not suitable for environments that require Layer 2 interfaces in the deployment, as Layer 2 interfaces are not supported in Active/Active HA mode. Active/Active HA is also not suitable for environments that require that all configuration must be fully synchronized between both members of the HA pair, as some configuration settings are not synchronized in Active/Active HA mode, such as virtual router configuration, virtual wire configuration, and QoS configuration.
Reference: : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up- activeactive-ha/determine-your-activeactive-use-case

QUESTION 58
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

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web- interface/defining-policies-on-panorama

QUESTION 59
A company requires that a specific set of ciphers be used when remotely managing their Palo Alto Networks appliances. Which profile should be configured in order to achieve this?

A. SSH Service profile

B. SSL/TLS Service profile

C. Decryption profile

D. Certificate profile

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure- an-ssh-service-profile

QUESTION 60
A company is using wireless controllers to authenticate users. Which source should be used for User- ID mappings?

A. Syslog

B. XFF headers

C. server monitoring
D. client probing

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-overview

QUESTION 61
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

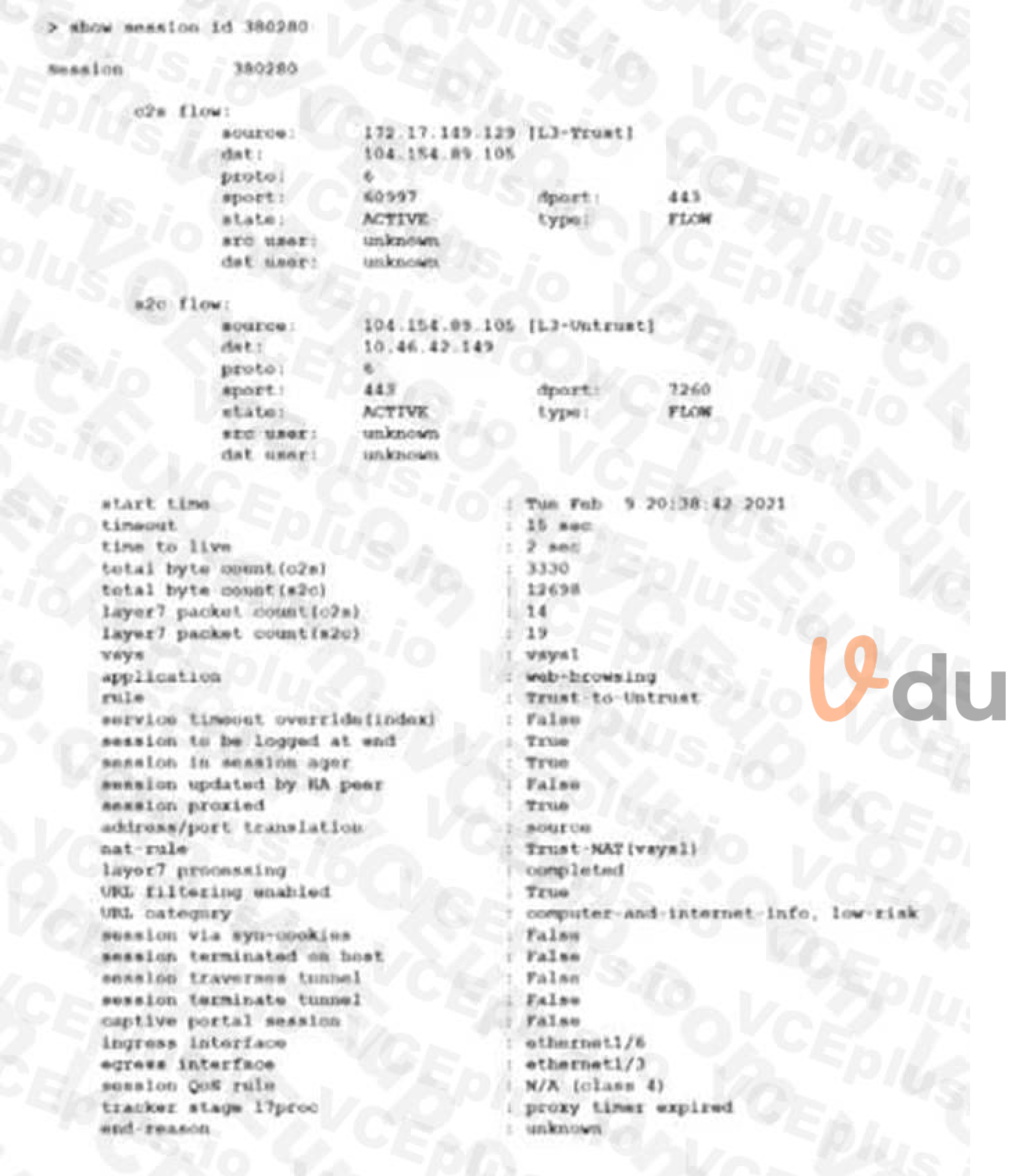
Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-inbound- inspection We recommend uploading a certificate chain (a single file) to the firewall if your end- entity (leaf) certificate is signed by one or more intermediate certificates and your web server supports TLS 1.2 and Rivest, Shamir, Adleman (RSA) or Perfect Forward Secrecy (PFS) key exchange algorithms. Uploading the chain avoids client-side server certificate authentication issues. You should arrange the certificates in the file as follows: End-entity (leaf) certificate Intermediate certificates (in issuing order) (Optional) Root certificate

QUESTION 62
A firewall administrator needs to be able to inspect inbound HTTPS traffic on servers hosted in theirDMZ to prevent the hosted service from being exploited. Which combination of features can allowPAN-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

Correct Answer: C
Section:
Explanation:
A vulnerability protection profile enables the firewall to detect and prevent exploit attempts against known vulnerabilities in network protocols and applications. A decryption policy allows the firewall to decrypt and inspect inbound HTTPS traffic for potential threats. A data filtering profile is used for detecting and controlling the transfer of sensitive data such as credit card numbers or social security numbers. A WildFire profile is used for submitting unknown files or email links to the WildFire cloud for analysis and verdict. A file blocking profile is used for blocking or allowing the transfer of files based on their type, direction, or application. A QoS policy is used for managing the bandwidth allocation and priority of network traffic based on various criteria. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-concepts/ssl- inbound-inspection https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/set-up- vulnerability-protection.html

QUESTION 63
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.

Correct Answer: A, C
Section:
Explanation:
The session went through SSL decryption processing because the Decryption column shows a green check mark, indicating that the firewall decrypted the traffic and applied security policies. The application has been identified as web-browsing because the Application column shows web- browsing as the application name. The session has not ended yet because the Session End Reason column shows N/A, indicating that the session is still active. The session did go through SSL decryption processing, so option D is incorrect. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/monitor/monitor- network/monitor-sessions

QUESTION 64
While analyzing the Traffic log, you see that some entries show "unknown-tcp" in the Application column What best explains these occurrences?

A. A handshake took place, but no data packets were sent prior to the timeout.
B. A handshake took place; however, there were not enough packets to identify the application.
C. A handshake did take place, but the application could not be identified.
D. A handshake did not take place, and the application could not be identified.

Correct Answer: C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC#:~:text=un known%2Dtcp%3A,firewall%20does%20not%20have%20signatures.Unknown-tcp means the firewall captured the three-way TCP handshake, but the application was not identified. This may be due to the use of a custom application for which the firewall does not have signatures

QUESTION 65
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."

Correct Answer: A, B
Section:
Explanation:
A redistribution profile defines which routes from one routing protocol are redistributed into another routing protocol. In the OSPF configuration, the OSPF Export Rules section allows you to select which redistribution profiles to apply for exporting routes into OSPF. Within the redistribution profile, you need to select Redist as the option to redistribute the routes that match the profile filter. If you select No Redist, the routes that match the profile filter will not be redistributed.
Ensuring that the OSPF neighbor state is "2-Way" is not relevant for advertising a static route into OSPF, as this state indicates that the neighbor relationship is established but not synchronized. In the redistribution profile, the source type should be set to "static" if you want to redistribute a static route into OSPF, not "ospf". Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/route- redistribution/configure-route-redistribution https:// knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClfnCAC

QUESTION 66
Which statement best describes the Automated Commit Recovery feature?

A. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. It reverts the configuration changes on the firewall if the check fails.
B. It restores the running configuration on a firewall and Panorama if the last configuration commit fails.
C. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. It reverts the configuration changes on the firewall and on Panorama if the check fails.
D. It restores the running configuration on a firewall if the last configuration commit fails.

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer- panorama/enable-automated-commit-recoveryThe Automated Commit Recovery feature enables the firewall to automatically revert to a previous configuration if a commit operation causes connectivity loss between the firewall and Panorama. The feature performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. If the check fails, the firewall reverts to the last known good configuration and restores connectivity with Panorama. The feature does not restore the running configuration on a firewall or Panorama if the last commit fails, as this would require manual intervention. The feature does not revert the configuration changes on Panorama, as Panorama is not affected by the commit operation on the firewall. Reference: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/panorama- features/ automatic-panorama-connection-recovery https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/administer- panorama/enable-automated-commit-recovery

QUESTION 67
A firewall administrator wants to avoid overflowing the company syslog server with traffic logs.
What should the administrator do to prevent the forwarding of DNS traffic logs to syslog?

A. Disable logging on security rules allowing DNS.

B. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application not equal to DNS.

C. Create a security rule to deny DNS traffic with the syslog server in the destination

D. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application equal to DNS.

Correct Answer: B
Section:
Explanation:
A log forwarding profile defines which logs are forwarded to which destinations, such as syslog servers. By creating a filter with application not equal to DNS, the log forwarding profile will exclude DNS traffic logs from being forwarded to syslog. Disabling logging on security rules allowing DNS will prevent the firewall from generating any logs for DNS traffic, which may not be desirable. Creating a security rule to deny DNS traffic with the syslog server in the destination will block the communication between the firewall and the syslog server, which may affect other logs. Creating a filter with application equal to DNS will forward only DNS traffic logs to syslog, which is the opposite of what is required.
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-forwarding https://docs.paloaltonetworks.com/network-security/security-policy/objects/log-forwarding

QUESTION 68
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.

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward- proxy(Best Practice) Enterprise CA-signed CertificatesóAn enterprise CA can issue a signing certificate that the firewall can use to sign the certificates for sites which require SSL decryption. When the firewall trusts the CA that signed the certificate of the destination server, the firewall can send a copy of the destination server certificate to the client, signed by the enterprise CA. This is a best practice because usually all network devices already trust the Enterprise CA (it is usually already installed in the devices' CA Trust storage), so you don't need to deploy the certificate on the endpoints, so therollout process is smoother. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os- admin/decryption/configure-ssl-forward-proxy.html

QUESTION 69
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

Correct Answer: C
Section:
Explanation:
QoS natively integrates with App-ID, which is a feature that identifies applications based on their unique characteristics and behaviors, regardless of port, protocol, encryption, or evasive tactics. By using App-ID, QoS can prioritize or limit traffic based on the application name, category, subcategory, technology, or risk level. Certificate revocation is a process of invalidating digital certificates that are no longer trusted or secure. Content-ID is a feature that scans content and data within allowed applications for threats and sensitive data. Port inspection is a method of identifying applications based on the TCP or UDP port numbers they use, which is not reliable or granular enough for QoS purposes. Reference:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/configure-qos https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id

QUESTION 70
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

Correct Answer: D
Section:
Explanation:
If you have a Simple Certificate Enrollment Protocol (SCEP) server in your enterprise PKI, you can configure a SCEP profile to automate the generation and distribution of unique client certificates.https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/obtain- certificates/deploy-certificates-using-scep

QUESTION 71
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

Correct Answer: A, B, D
Section:
Explanation:
Panorama can perform three actions when deploying PAN-OS images to its managed devices: upload-only, upload and install, and upload and install and reboot. Upload-only transfers the PAN-OS image from Panorama to the managed device without installing it. Upload and install transfers the PAN-OS image from Panorama to the managed device and installs it, but does not reboot the device.Upload and install and reboot transfers the PAN-OS image from Panorama to the managed device, installs it, and reboots the device. Verify and install is not a valid action for deploying PAN-OS images from Panorama. Install and reboot is not a valid action for deploying PAN-OS images from Panorama, as the image needs to be uploaded first. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/panorama/panorama-device- deployment/manage-software-and-content-updates
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cles

QUESTION 72
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.

Correct Answer: B
Section:
Explanation:
Generate a CA certificate for Forward Trust (step 2) a self-signed CA for Forward Untrust (step 4)https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward- proxy

QUESTION 73
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

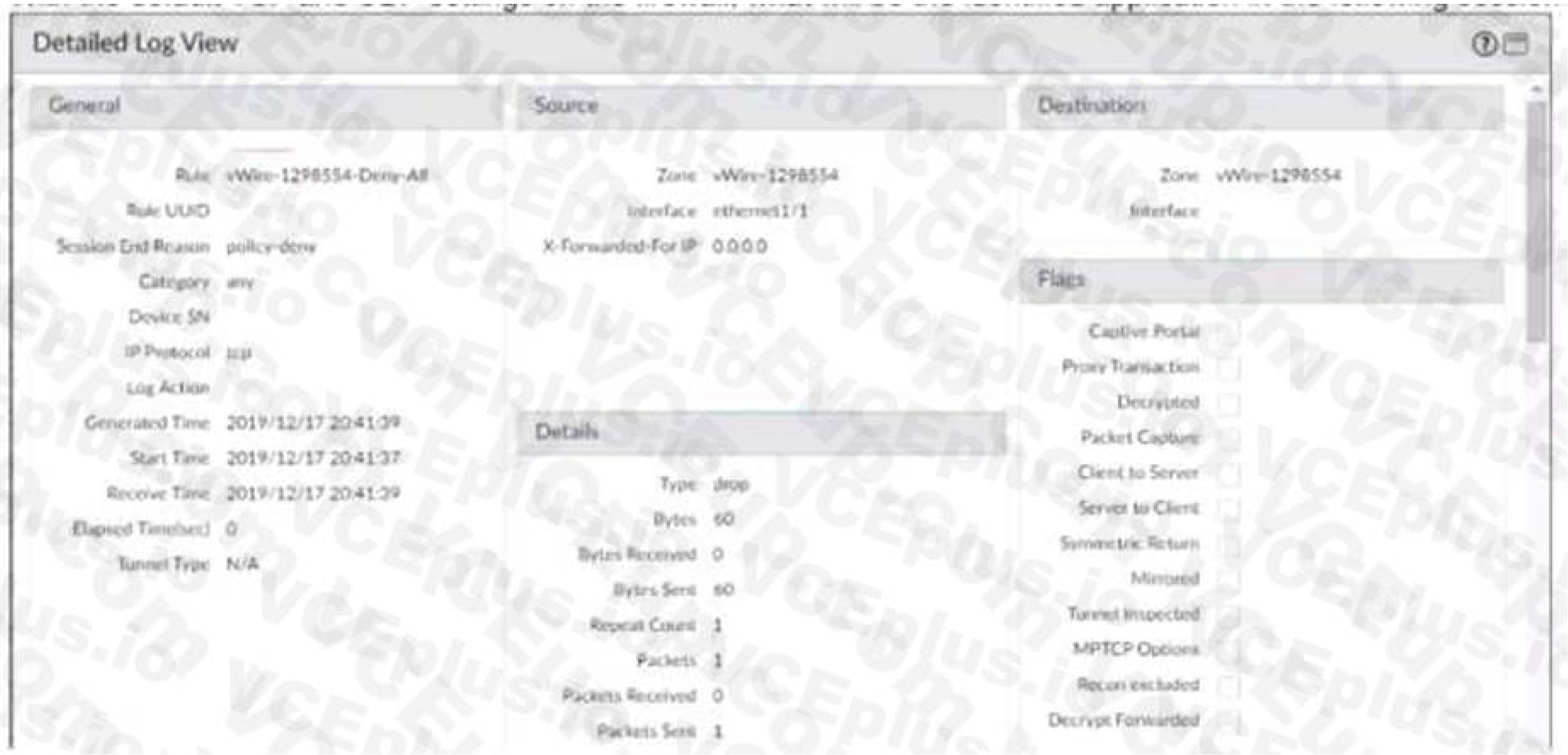
Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClivCAC
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/advanced- routing/create-bfd-profiles#idf2ccda44-0678-4df3-ad1d-2ec8f47cec7b then https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/advanced- routing/configure-bgp-on-an-advanced-routing-engine

QUESTION 74
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.

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-high- availability/ha-link-and-path-monitoring

QUESTION 75
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?



Detailed Log View

General

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

Source

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

Details

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

Destination

Zone vWire-1298554
Interface

Flags

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

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

Correct Answer: B
Section:
Explanation:
UDP connection on port 443. This would trigger unknown-udp. Incomplete is used in TCP connections only.https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

QUESTION 76
Which profile generates a packet threat type found in threat logs?

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

Correct Answer: A
Section:
Explanation:
"Threat/Content Type (subtype) Subtype of threat log." "packetóPacket-based attack protectiontriggered by a Zone Protection profile." https://docs.paloaltonetworks.com/pan-os/10-2/pan-os- admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/threat-log-fieldshttps://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-syslog-for- monitoring/syslog-field-descriptions/threat-log-fields packetóPacket-based attack protection triggered by a Zone Protection profile.

QUESTION 77

A client wants to detect the use of weak and manufacturer-default passwords for IoT devices. Which option will help the customer?

A. Configure a Data Filtering profile with alert mode.
B. Configure an Antivirus profile with alert mode.
C. Configure a Vulnerability Protection profile with alert mode
D. Configure an Anti-Spyware profile with alert mode.

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles

QUESTION 78

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.

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos- protection/configure-zone-protection-to-increase-network-security/configure-reconnaissance- protection

QUESTION 79

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

Correct Answer: B
Section:
Explanation:
An interface management profile defines which services are available on an interface, such as HTTPS, SSH, ping, or SNMP. By enabling HTTPS in an interface management profile on the subinterface, the engineer can allow XML API access to the firewall for automation on the network segment that is routed through the subinterface. Specifying the subinterface as a management interface in Setup > Device > Interfaces is not possible, as only physical interfaces can be designated as management interfaces. Adding the network segment's IP range to the Permitted IP Addresses list will not help, as this list only applies to the dedicated management interface. Configuring a service route for HTTP to use the subinterface will not help, as this will only affect the outbound traffic from the firewall to external services, not the inbound traffic to the firewall for XML API access. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/ networking/configure- interfaces/configure-interface-management-profiles https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/enable-api-access

QUESTION 80

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

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

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhdCAC

QUESTION 81
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.

Correct Answer: C
Section:
Explanation:
An email profile defines the email server and sender address for sending email notifications from the firewall or Panorama. To forward system logs to email, the engineer needs to create a new email profile under Device > Server Profiles > Email and configure the required settings, such as SMTP server, sender email address, and recipient email address. Then, the engineer needs to navigate to Device > Log Settings > System and select the email profile under Email for each severity level of system logs that need to be forwarded. Enabling log forwarding under the email profile in the Objects tab or in the Device tab is not possible, as log forwarding profiles are configured under Objects > Log Forwarding. Log forwarding profiles are used for forwarding threat, traffic, URL filtering, data filtering, HIP match, configuration, and correlation logs, not system logs. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-email-alerts https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-forwarding

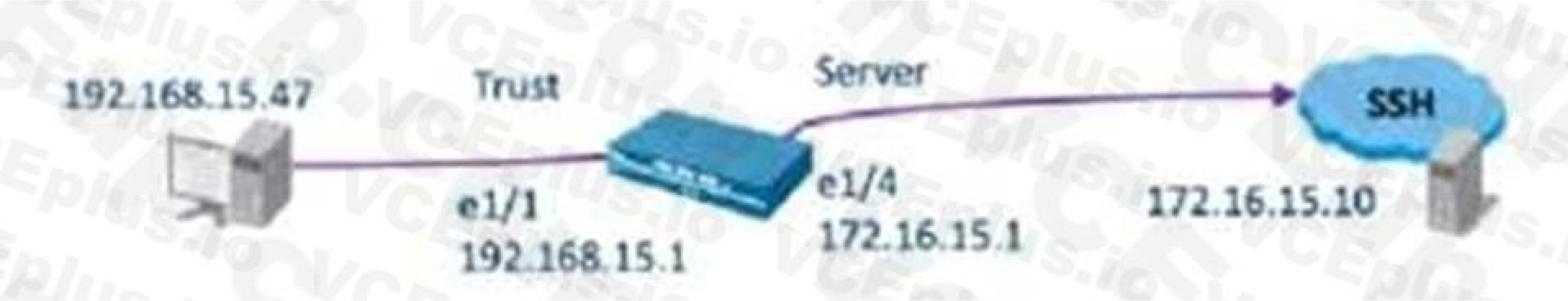
QUESTION 82
A network security administrator has an environment with multiple forms of authentication. There is a network access control system in place that authenticates and restricts access for wireless users, multiple Windows domain controllers, and an MDM solution for company-provided smartphones. 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

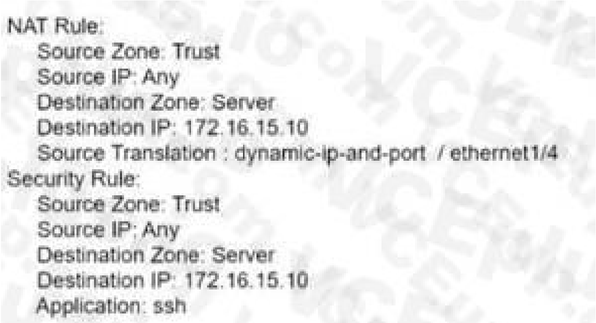
Correct Answer: C
Section:
Explanation:
A syslog listener is a User-ID agent that listens for syslog messages from network devices that contain user mapping information, such as network access control systems, domain controllers, or MDM solutions. By configuring a syslog listener on the firewall or Panorama and specifying the syslog format and filters, User-ID can parse the syslog messages and extract user mapping information from multiple sources. Agentless User-ID with redistribution is a method of using an existing firewall as a User-ID agent that redistributes user mappings to other firewalls or Panorama. This method does not involve syslog messages. A standalone User-ID agent is a software application that runs on a Windows server and collects user mappings from Active Directory servers or other sources. This method requires installing and managing a separate agent software. A captive portal is a web page that prompts users to authenticate before accessing certain network resources. This method does not involve syslog messages. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to- users/syslog-monitoring.html https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to- users/user-id-agents.html

QUESTION 83

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?

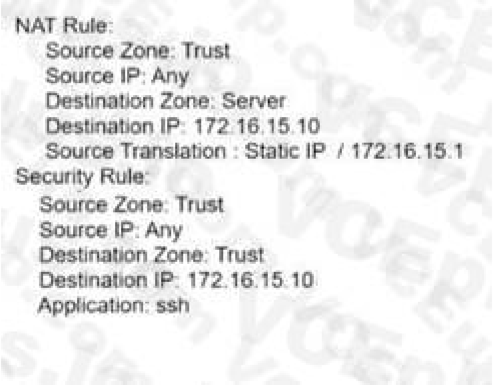


A.



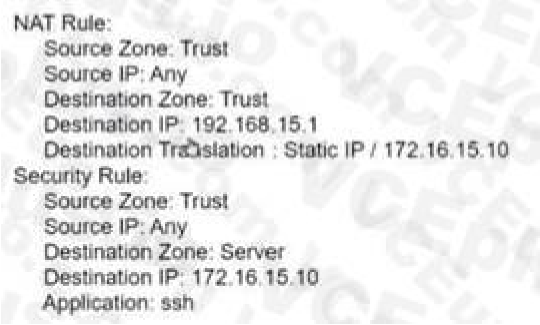
```
NAT Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Server
    Destination IP: 172.16.15.10
    Source Translation : dynamic-ip-and-port  / ethernet1/4
Security Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Server
    Destination IP: 172.16.15.10
   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

B.



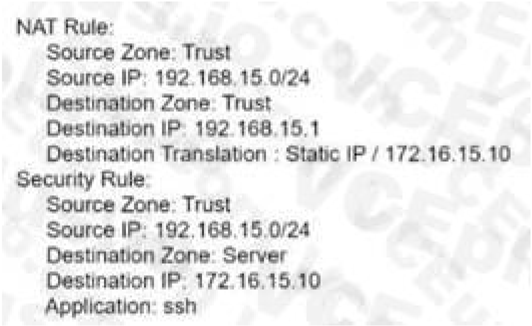
```
NAT Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Server
    Destination IP: 172.16.15.10
    Source Translation : Static IP  / 172.16.15.1
Security Rule:
    Source Zone: Trust
    Source IP: Any
    Destination Zone: Trust
    Destination IP: 172.16.15.10
    Application: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

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/source-nat-and- destination-nat/source-nat

QUESTION 84
Which Panorama feature protects logs against data loss if a Panorama server fails?

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

Correct Answer: B
Section:
Explanation:
A Panorama Collector Group is a group of dedicated log collectors that receive logs from firewalls and Panorama management servers. By enabling log redundancy in a collector group, Panorama can ensure that each log is written to two log collectors in the group, providing backup in case one log collector fails. Panorama HA does not automatically ensure that no logs are lost if a server fails inside the HA cluster, as HA only provides redundancy for configuration and device management, not for logging. Panorama HA with log redundancy is not a valid option, as log redundancy is configured at the collector group level, not at the HA level. Panorama Collector Group does not automatically ensure that no logs are lost if a server fails inside the Collector Group, as log redundancy needs to be enabled explicitly in the collector group settings. Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-collection- and-forwarding/configure-log-collection-on-panorama https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-collection- and-forwarding/configure-log-redundancy

QUESTION 85
An administrator is seeing one of the firewalls in a HA active/passive pair moved to 'suspended" state due to Non-functional loop. Which three actions will help the administrator troubleshool this issue? (Choose three.)

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

Correct Answer: A, B, C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhJCAS&lang=ja&r efURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail

QUESTION 86
Which User-ID mapping method should be used in a high-security environment where all IP addressto- 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

Correct Answer: B
Section:
Explanation:
Because GlobalProtect users must authenticate to gain access to the network, the IP address-to- username mapping is explicitly known. This is the best solution in sensitive environments where you must be certain of who a user is in order to allow access to an application or service.https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user- mapping/globalprotect.html

QUESTION 87
What can be used to create dynamic address groups?

A. dynamic address
B. region objects
C. tags
D. FODN addresses

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/monitor-changes-in-the- virtual-environment/use-dynamic-address-groups-in-policy

QUESTION 88
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 lo 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.

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/schedule-a- configuration-push-to-managed-firewalls Log in to the Panorama Web Interface. Create a scheduled configuration push. Select PanoramaScheduled Config Push and Add a new scheduled configuration push. You can also schedule a configuration push to managed firewalls when you push to devices (CommitPush to Devices).

QUESTION 89
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.

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems/customize-service- routes-for-a-virtual-system "When a firewall is enabled for multiple virtual systems, the virtual systems inherit the global service and service route settings. For example, the firewall can use a shared email server to originate email alerts to all virtual systems. In some scenarios, you'd want to create different service routes for each virtual system."

QUESTION 90
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.

Correct Answer: D
Section:
Explanation:
You must upgrade all Log Collectors in a collector group at the same time to avoid losing log data https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-panorama/deploy- updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/deploy-an-update-to- log-collectors-when-panorama-is-internet-connected

QUESTION 91
Which configuration is backed up using the Scheduled Config Export feature in Panorama?

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

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer- panorama/manage-panorama-and-firewall-configuration-backups

QUESTION 92
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"

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/monitor-wildfire-activity/use-the- firewall-to-monitor-malware/configure-wildfire-submissions-log-settings/enable-logging-for-benign- and-grayware-samples

QUESTION 93

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

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the- firewall-pan-os/upgrade-firewalls-using-panorama

QUESTION 94
A network security engineer has applied a File Blocking profile to a rule with the action of Block. The user of a Linux CLI operating system has opened a ticket. The ticket states that the user is being blocked by the firewall when trying to download a TAR file. The user is getting no error response on the system.
Where is the best place to validate if the firewall is blocking the user's TAR file?

A. URL Filtering log
B. Data Filtering log
C. Threat log
D. WildFire Submissions log

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClZ1CAK

QUESTION 95
A network engineer has discovered that asymmetric routing is causing a Palo Alto Networks firewall to drop traffic. The network architecture cannot be changed to correct this.
Which two actions can be taken on the firewall to allow the dropped traffic permanently? (Choose two.)

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

Correct Answer: A, D
Section:
Explanation:
Option A is correct because setting "Reject Non-syn-TCP" to No and "Asymmetric Path" to Bypass in the Zone Protection profile disables the TCP checks that can cause the firewall to drop packets due to asymmetric routing. This allows the firewall to accept non-SYN TCP packets without a session match and packets that are out of sequence or out of window.Option D is correct because setting session tcp-reject-non-syn to no in the CLI also disables the TCP checks that can cause the firewall to drop packets due to asymmetric routing. This allows the firewall to accept non-SYN TCP packets without a session match and packets that are out of sequence or out of window.Option B is incorrect because setting session tcp-reject-non-syn to no in the CLI has the same effect as setting "Reject Non-syn-TCP" to No in the Zone Protection profile, so there is no need to do both.Also, setting "Asymmetric Path" to Global in the Zone Protection profile does not disable the TCP checks that can cause the firewall to drop packets due to asymmetric routing. It only allows the firewall to use a global timer for asymmetric path detection instead of a per-session timer.Option C is incorrect because setting "Reject Non-syn-TCP" to Global and "Asymmetric Path" to Global in the Zone Protection profile does not disable the TCP checks that can cause the firewall to drop packets due to asymmetric routing. It only allows the firewall to use a global timer for both non- SYN TCP rejection and asymmetric path detection instead of a per-session timer.Reference: 1

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClReCAK 2 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSHCA0

QUESTION 96
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

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClgZCAS

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.

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC Incomplete in the application field: Incomplete means that either the three-way TCP handshake did not complete OR the three-way TCP handshake did complete but there was no enough data after the handshake to identify the application. In other words that traffic being seen is not really an application. One example is, if a client sends a server a SYN and the Palo Alto Networks device creates a session for that SYN , but the server never sends a SYN ACK back to the client, then that session is incomplete.

QUESTION 98
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

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama- overview/panorama-modelsManagement Only mode is the only Panorama mode that allows all logs to be sent to and only stored in Cortex Data Lake. In this mode, Panorama does not store any logs locally and only acts as a management interface for the firewalls and Cortex Data Lake. The other modes either store somelogs locally (Legacy and Log Collector) or do not support Cortex Data Lake (Panorama).

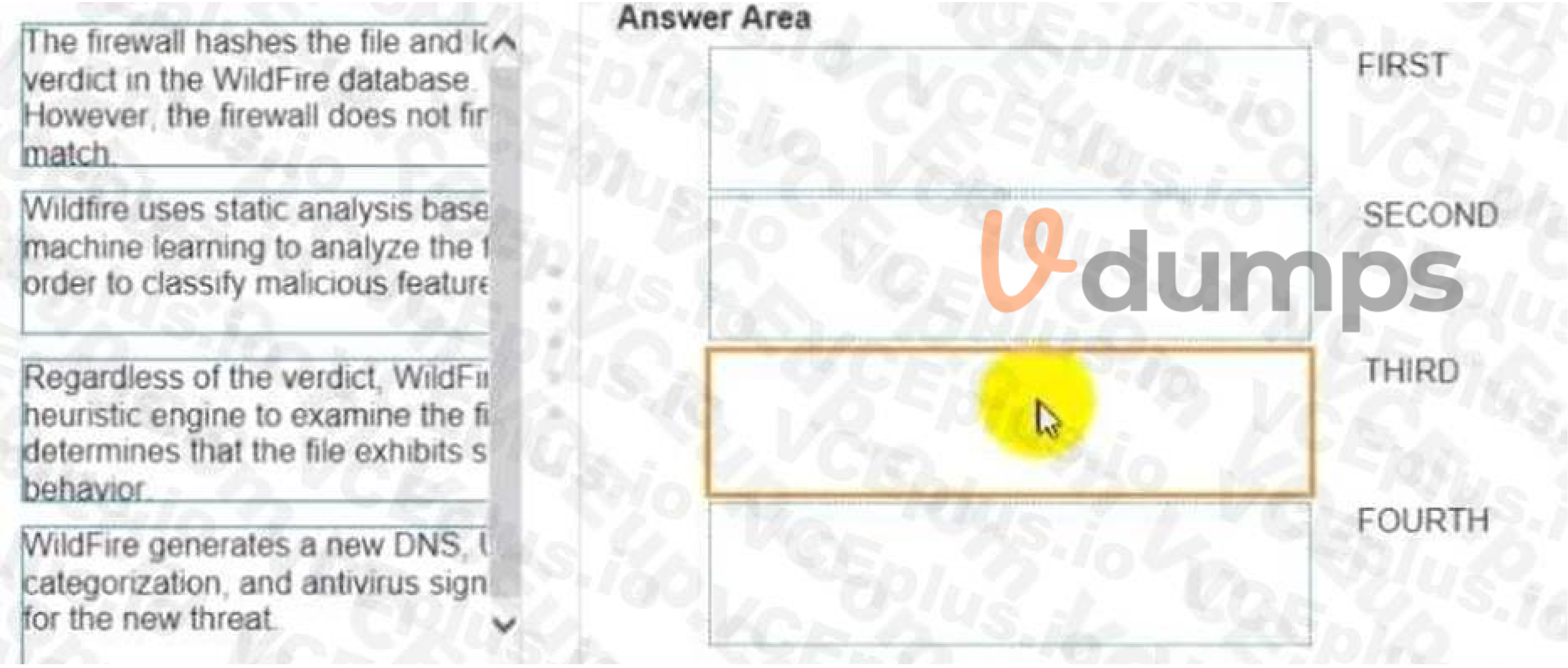
QUESTION 99
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Link and Path Monitoring Is enabled with the Failure Condition set to "any." There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure 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

Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClG7CAK

QUESTION 100
DRAG DROP
Place the steps in the WildFire process workflow in their correct order.

Select and Place:



The firewall hashes the file and lo verdict in the WildFire database. However, the firewall does not fir match.

Wildfire uses static analysis base machine learning to analyze the f order to classify malicious feature

Regardless of the verdict, WildFi heuristic engine to examine the fi determines that the file exhibits s behavior.

WildFire generates a new DNS, U categorization, and antivirus sign for the new threat.

Answer Area

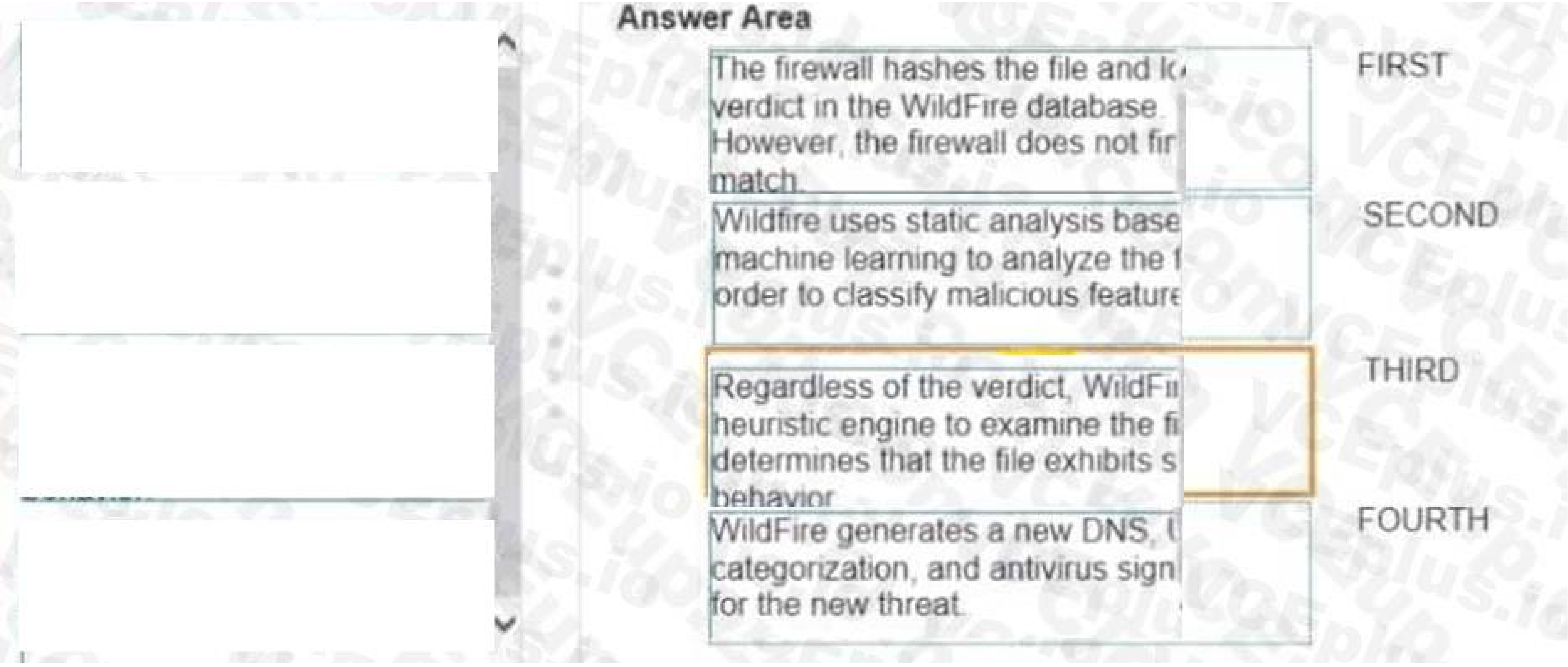
FIRST

SECOND

THIRD

FOURTH

Correct Answer:



Answer Area

The firewall hashes the file and lo verdict in the WildFire database. However, the firewall does not fir match.

FIRST

Wildfire uses static analysis base machine learning to analyze the f order to classify malicious feature

SECOND

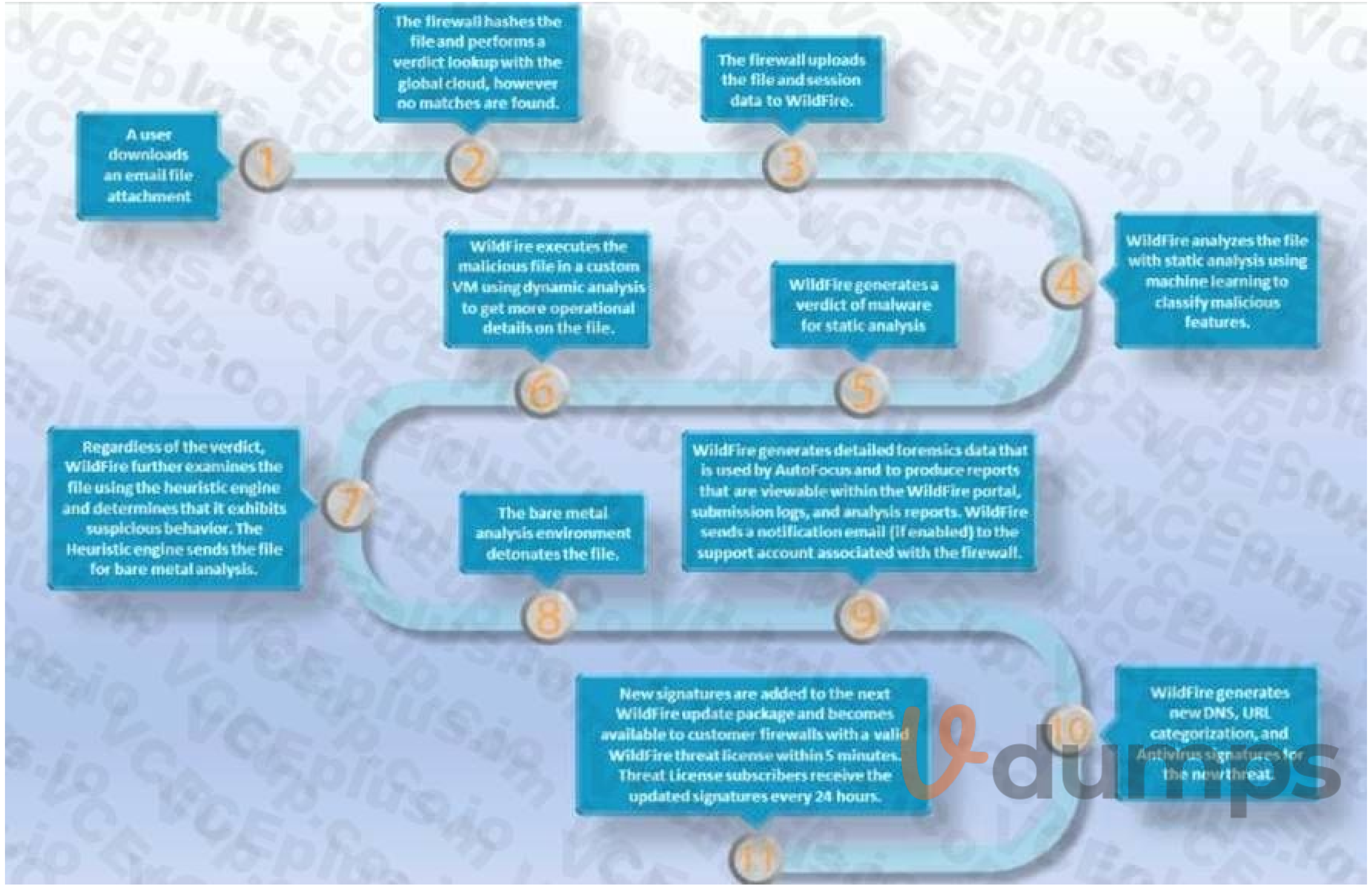
Regardless of the verdict, WildFi heuristic engine to examine the fi determines that the file exhibits s behavior

THIRD

WildFire generates a new DNS, U categorization, and antivirus sign for the new threat.

FOURTH

Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html



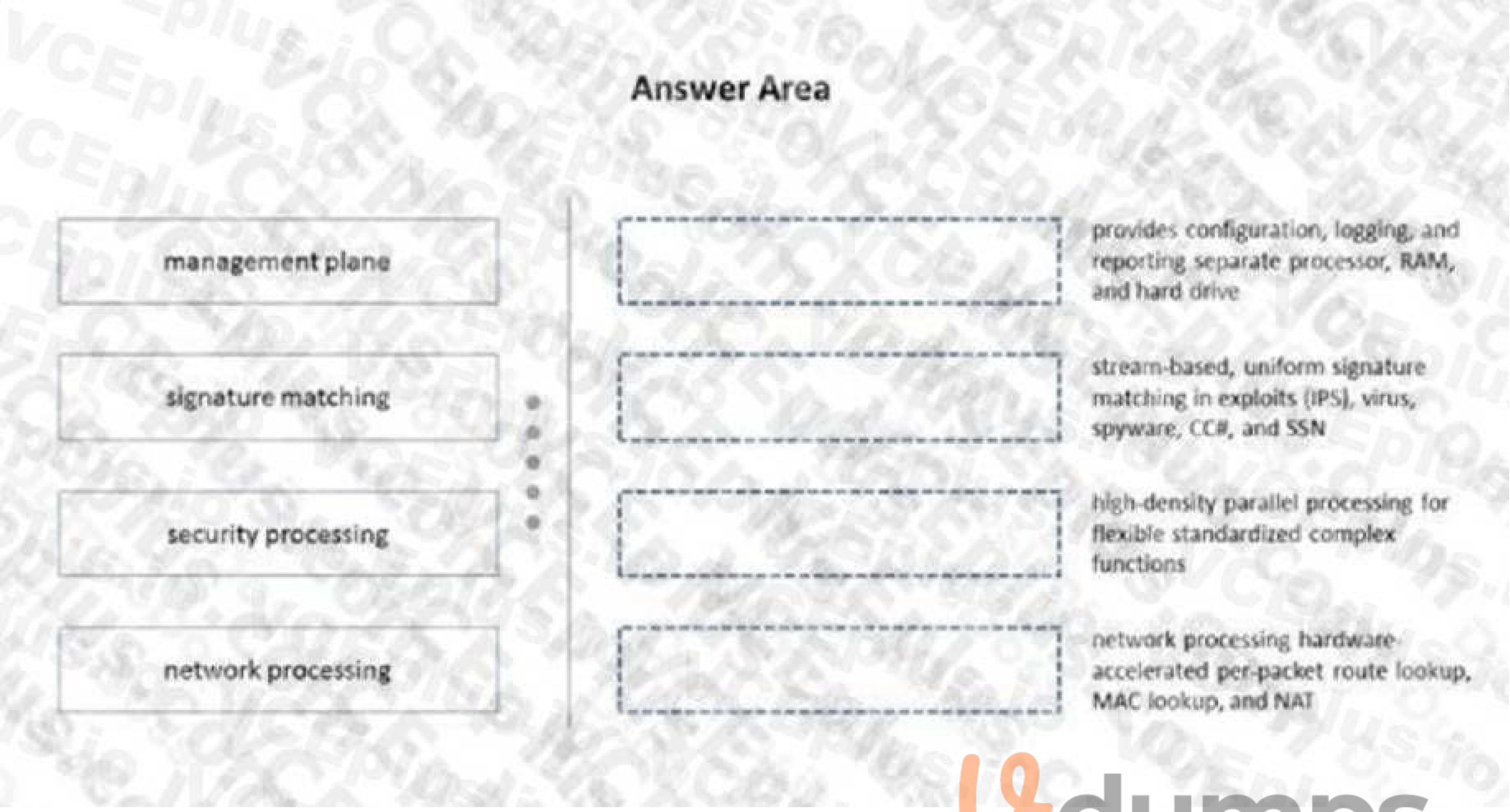
1. A user downloads an email file attachment
2. The firewall hashes the file and performs a verdict lookup with the global cloud, however no matches are found.
3. The firewall uploads the file and session data to WildFire.
4. WildFire analyzes the file with static analysis using machine learning to classify malicious features.
5. WildFire generates a verdict of malware for static analysis
6. WildFire executes the malicious file in a custom VM using dynamic analysis to get more operational details on the file.
7. Regardless of the verdict, WildFire further examines the file using the heuristic engine and determines that it exhibits suspicious behavior. The Heuristic engine sends the file for bare metal analysis.
8. The bare metal analysis environment detonates the file.
9. WildFire generates detailed forensics data that is used by AutoFocus and to produce reports that are viewable within the WildFire portal, submission logs, and analysis reports. WildFire sends a notification email (if enabled) to the support account associated with the firewall.
10. WildFire generates new DNS, URL categorization, and Antivirus signatures for the new threat.
11. New signatures are added to the next WildFire update package and becomes available to customer firewalls with a valid WildFire threat license within 5 minutes. Threat License subscribers receive the updated signatures every 24 hours.

QUESTION 101

DRAG DROP

Please match the terms to their corresponding definitions.

Select and Place:



Answer Area

management plane

signature matching

security processing

network processing

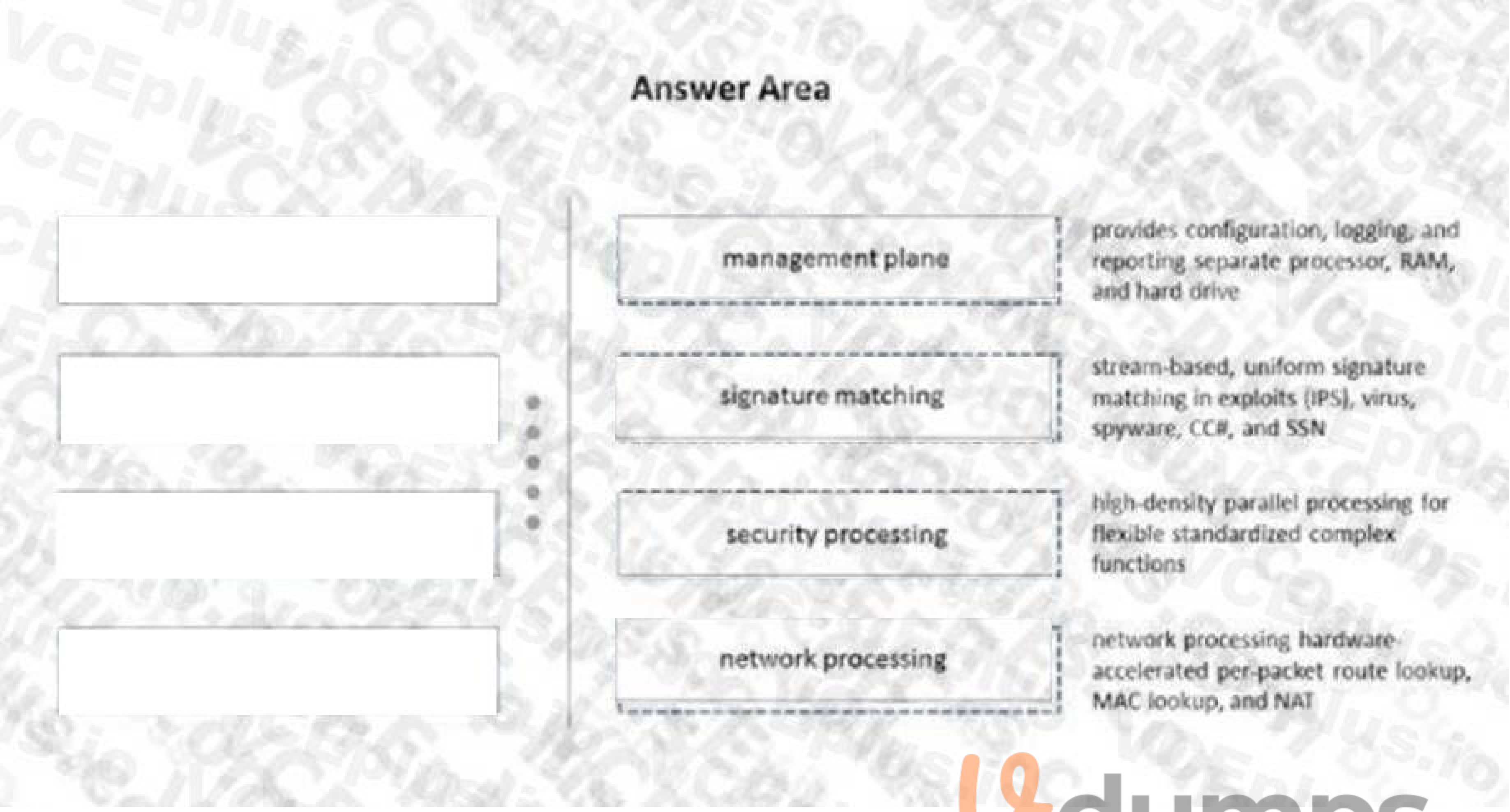
provides configuration, logging, and reporting separate processor, RAM, and hard drive

stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN

high-density parallel processing for flexible standardized complex functions

network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Correct Answer:



Answer Area

management plane — provides configuration, logging, and reporting separate processor, RAM, and hard drive

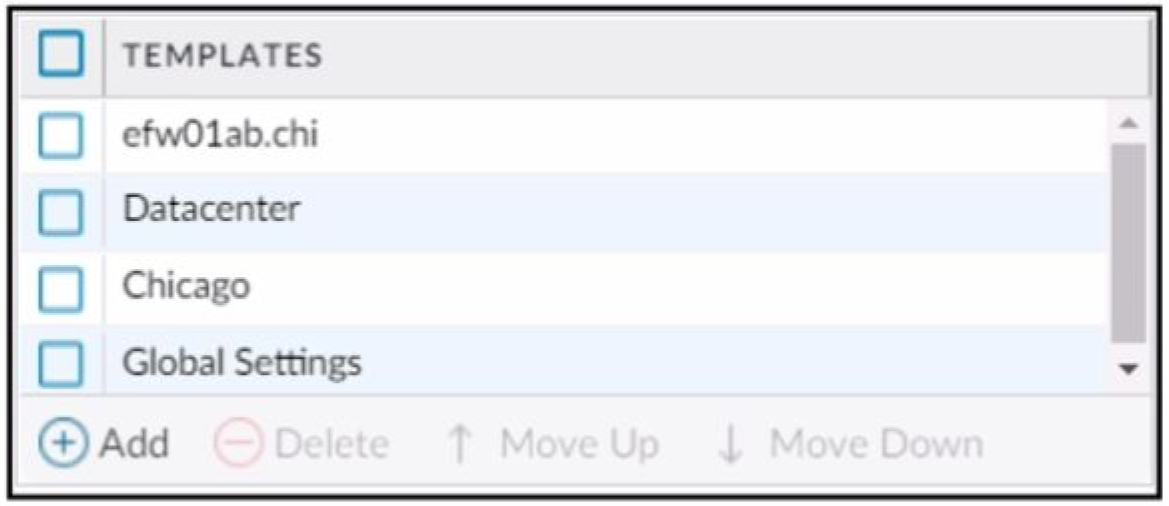
signature matching — stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN

security processing — high-density parallel processing for flexible standardized complex functions

network processing — network processing hardware accelerated per-packet route lookup, MAC lookup, and NAT

Section:
Explanation:

QUESTION 102
Which template values will be configured on the firewall if each template has an SSL to be deployed. The template stack should consist of four templates arranged according to the diagram.



□	TEMPLATES
□	efw01ab.chi
□	Datacenter
□	Chicago
□	Global Settings

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

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

D. Values in Chicago

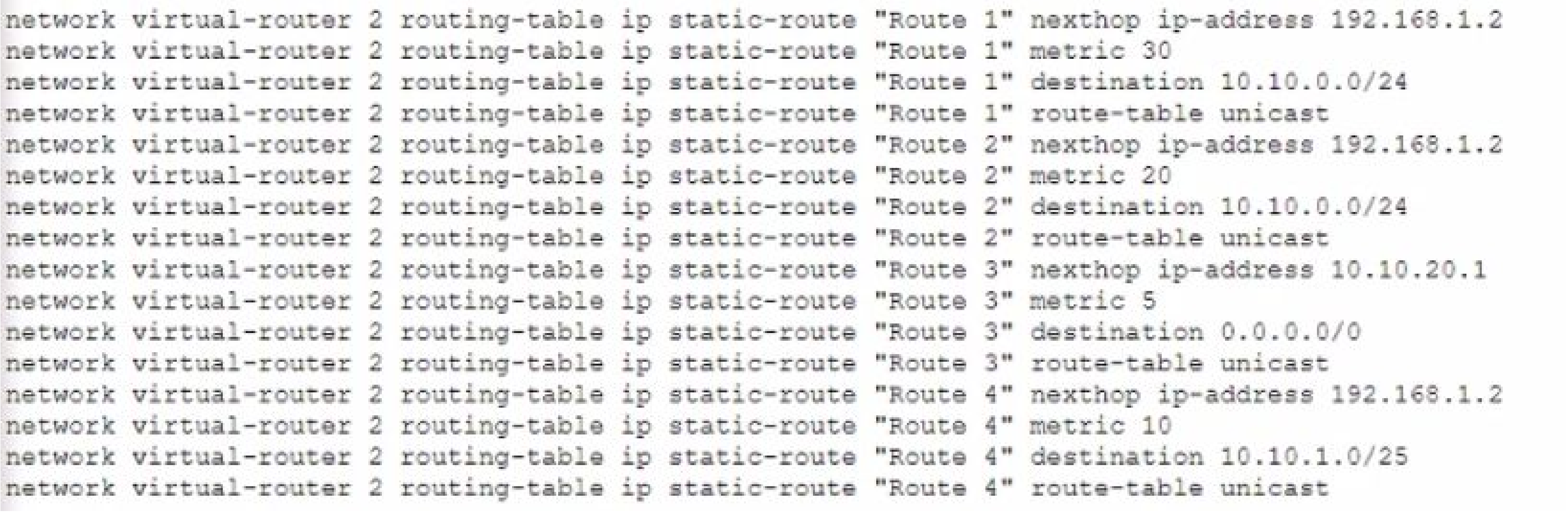
Correct Answer: D
Section:
Explanation:
The template stack should consist of four templates arranged according to the diagram. The template values that will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management will be the values in Chicago. This is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

QUESTION 103
An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.
What should an administrator configure to route interesting traffic through the VPN tunnel?

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

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

QUESTION 104
Given the following configuration, which route is used for destination 10 10 0 4?

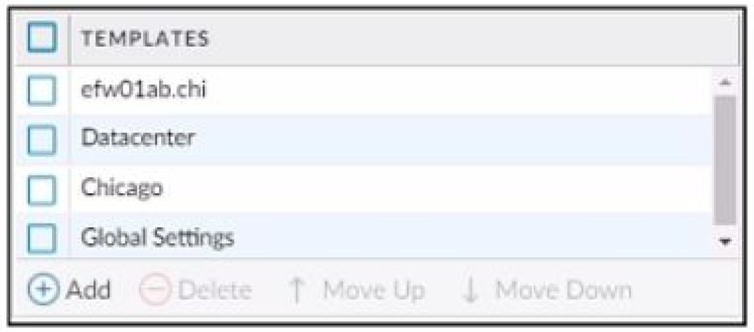


```
network virtual-router 2 routing-table ip static-route "Route 1" nexthop ip-address 192.168.1.2
network virtual-router 2 routing-table ip static-route "Route 1" metric 30
network virtual-router 2 routing-table ip static-route "Route 1" destination 10.10.0.0/24
network virtual-router 2 routing-table ip static-route "Route 1" route-table unicast
network virtual-router 2 routing-table ip static-route "Route 2" nexthop ip-address 192.168.1.2
network virtual-router 2 routing-table ip static-route "Route 2" metric 20
network virtual-router 2 routing-table ip static-route "Route 2" destination 10.10.0.0/24
network virtual-router 2 routing-table ip static-route "Route 2" route-table unicast
network virtual-router 2 routing-table ip static-route "Route 3" nexthop ip-address 10.10.20.1
network virtual-router 2 routing-table ip static-route "Route 3" metric 5
network virtual-router 2 routing-table ip static-route "Route 3" destination 0.0.0.0/0
network virtual-router 2 routing-table ip static-route "Route 3" route-table unicast
network virtual-router 2 routing-table ip static-route "Route 4" nexthop ip-address 192.168.1.2
network virtual-router 2 routing-table ip static-route "Route 4" metric 10
network virtual-router 2 routing-table ip static-route "Route 4" destination 10.10.1.0/25
network virtual-router 2 routing-table ip static-route "Route 4" route-table unicast
```

A. Route 2
B. Route 3
C. Route 1
D. Route 4

Correct Answer: A
Section:

QUESTION 105
An engineer configures a new template stack for a firewall that needs to be deployed. The template stack should consist of four templates arranged according to the diagram



□ TEMPLATES
□ efw01ab.chi
□ Datacenter
□ Chicago
□ Global Settings

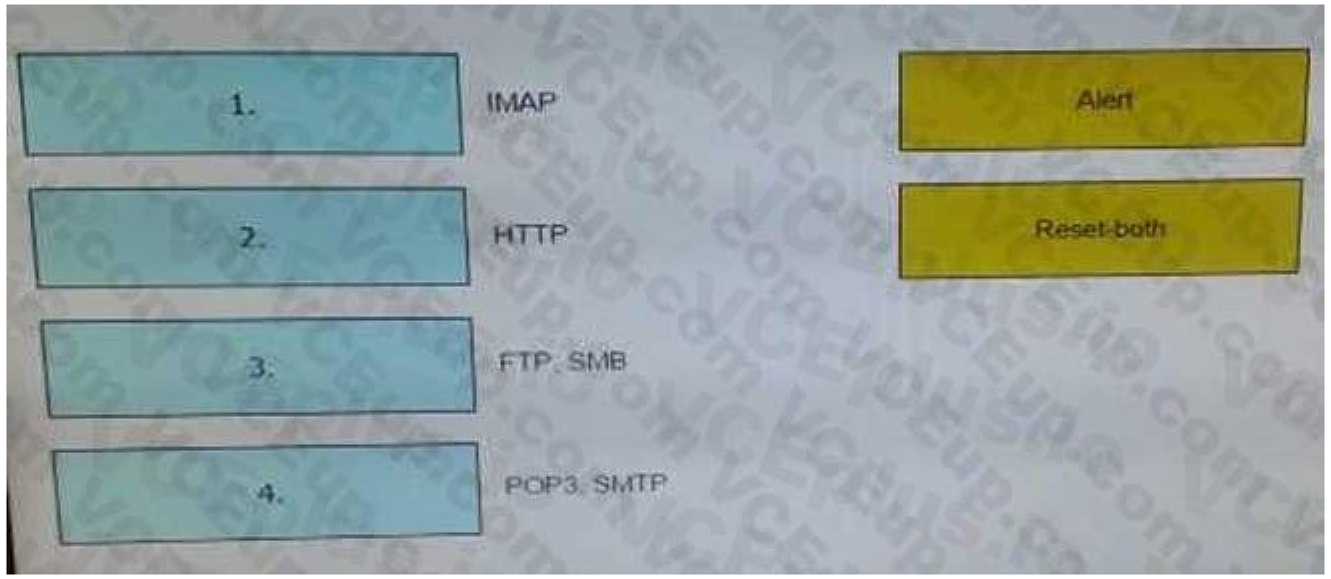
Which template values will be configured on the firewall If each template has an SSL/TLS Service profile configured named Management?

A. Values in Chicago
B. Values in efw01lab.chi
C. Values in Datacenter
D. Values in Global Settings

Correct Answer: B
Section:

QUESTION 106
DRAG DROP
When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.
Answer options may be used more than once or not at all.

Select and Place:



1. IMAP

2. HTTP

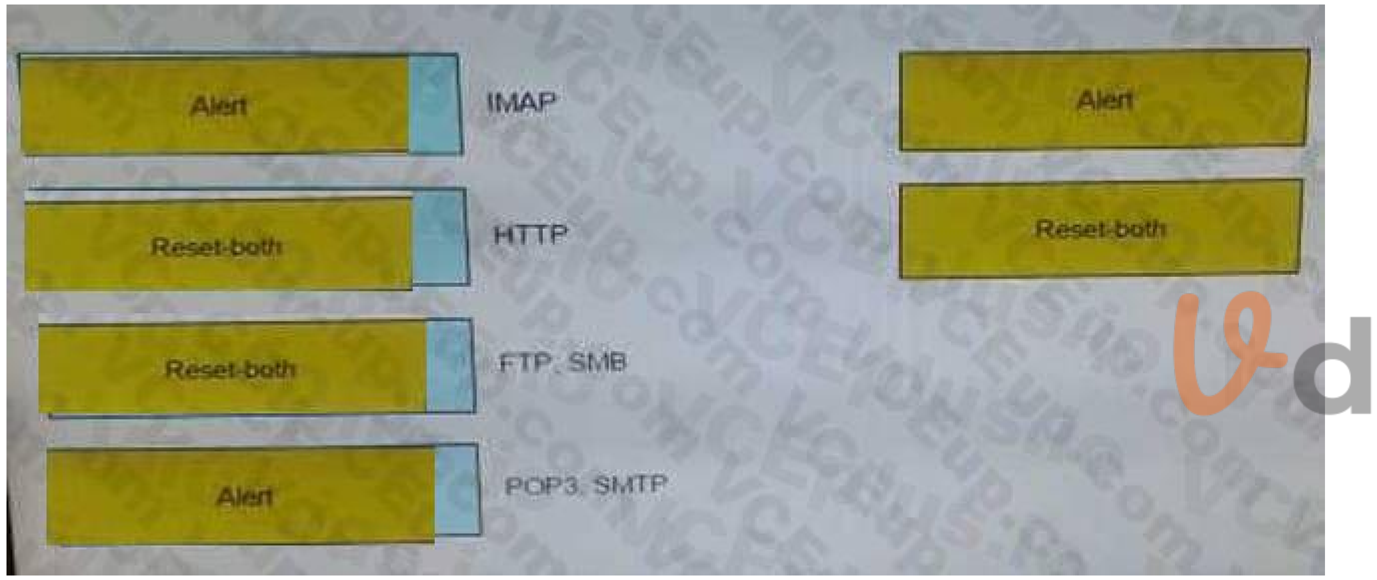
3. FTP, SMB

4. POP3, SMTP

Alert

Reset-both

Correct Answer:



Alert IMAP

Reset-both HTTP

Reset-both FTP, SMB

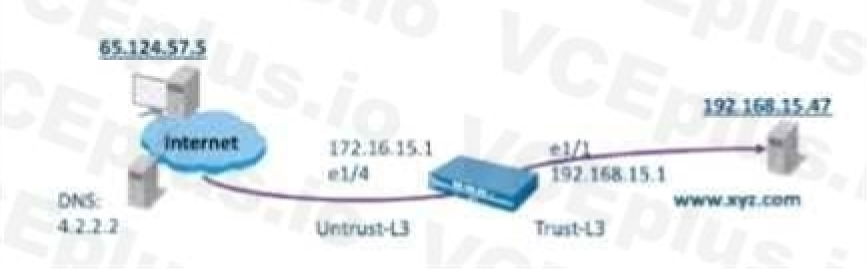
Alert POP3, SMTP

Alert

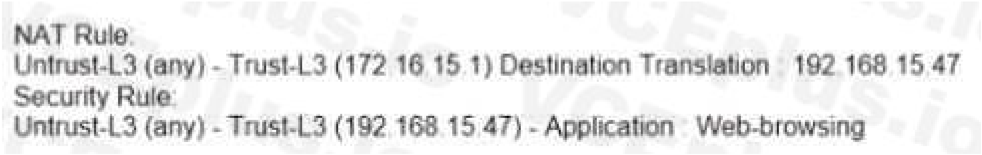
Reset-both

Section:
Explanation:

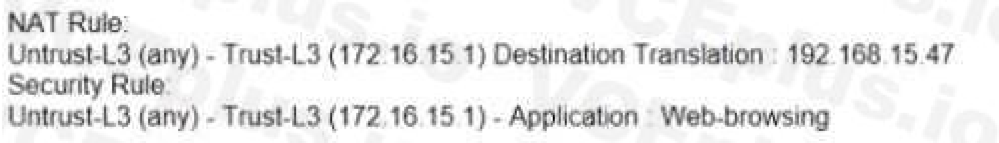
QUESTION 107
A user at an external system with the IP address 65.124 57 5 quenes the DNS server at 4 2 2 2 for the IP address of the web server www xyz com The DNS server returns an address of 172 16 151 In order to reach the web server, which
Security rule and NAT rule must be configured on the firewall?



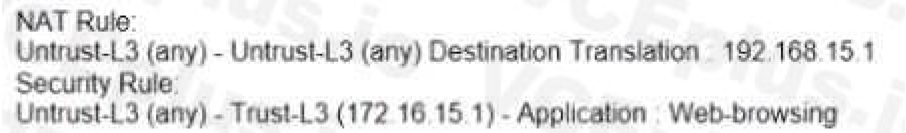
A.


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

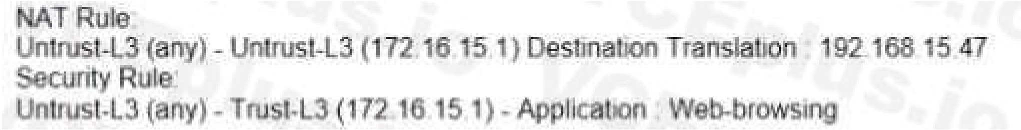
B.


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 (any) Destination Translation : 192.168.15.1
Security Rule:
Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application : Web-browsing

D.


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

Correct Answer: D
Section:

QUESTION 108
An administrator has left a firewall to use the default port for all management services. Which three functions are performed by the dataplane?

A. NTP
B. Antivirus
C. Wildfire updates
D. NAT
E. File tracking

Correct Answer: A, C, D
Section:

QUESTION 109
Which two events trigger the operation of automatic commit recovery? (Choose two.)

A. when an aggregate Ethernet interface component fails
B. when Panorama pushes a configuration
C. when a firewall HA pair fails over
D. when a firewall performs a local commit

Correct Answer: B, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panoramafeatures/automatic-panorama-connection-recovery.htmlAutomatic commit recovery allows you to configure the firewall to attempt a specified number ofconnectivity tests after:
1- you push a configuration from Panorama or
2- commit a configuration change locally on the firewall.

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

QUESTION 110
Panorama provides which two SD-WAN functions? (Choose two.)

A. data plane
B. physical network links
C. network monitoring
D. control plane

Correct Answer: C, D
Section:
Explanation:
https://www.paloaltonetworks.com/resources/guides/sd-wan-architecture-guide
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/about-sdwan.html
(Network Monitoring & Control Plane). Data plane & Physical Interfaces are directly taken care through Firewalls where SD WAN is enabled.

QUESTION 111
A users traffic traversing a Palo Alto networks NGFW sometimes can reach http //www company comAt other times the session times out. At other times the session times out The NGFW has beenconfigured with a PBF rule that the user traffic matches when it goes to http://www.company.comgoes to http://www company comHow can the firewall be configured to automatically disable the PBF rule if the next hop goes down?

A. Create and add a monitor profile with an action of fail over in the PBF rule in question
B. Create and add a monitor profile with an action of wait recover in the PBF rule in question
C. Configure path monitoring for the next hop gateway on the default route in the virtual router
D. Enable and configure a link monitoring profile for the external interface of the firewall

Correct Answer: A
Section:

QUESTION 112
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.

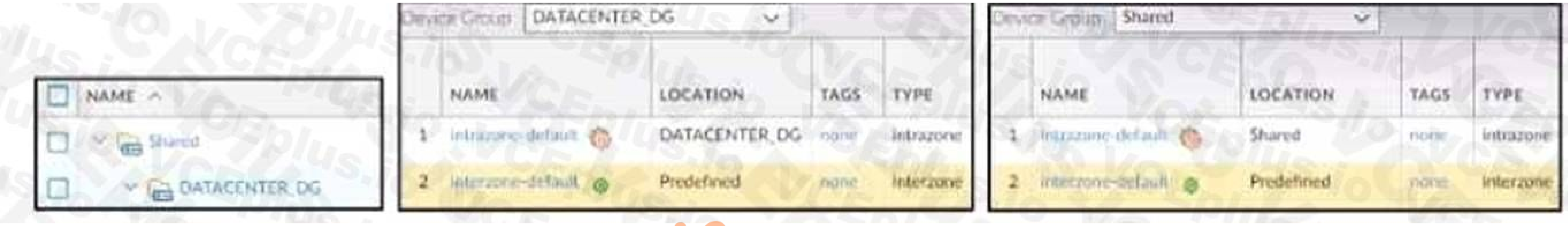
Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up- activepassive-ha/configure-activepassive-ha

QUESTION 113
An engineer needs to configure SSL Forward Proxy to decrypt traffic on a PA-5260. The engineer uses a forward trust certificate from the enterprise PKI that expires December 31, 2025. The validity date on the PA-generated certificate is taken from what?

A. The trusted certificate
B. The server certificate
C. The untrusted certificate
D. The root CA

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm8wCA"The validity date on the Palo Alto Networks firewall generated certificate is taken from the validity date on the real server certificate."

QUESTION 114
Refer to the exhibit.



□	NAME ^
□	Shared
□	DATACENTER_DG

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 rules
rules configured locally on the firewall
shared post-rules
DATACENTER_DG post-rules
DATACENTER.DG default rules

B. shared pre-rules
DATACENTER_DG pre-rules
rules configured locally on the firewall
shared post-rules
DATACENTER.DG post-rules
shared default rules

C. shared pre-rules
DATACENTER_DG pre-rules
rules configured locally on the firewall
DATACENTER_DG post-rules
shared post-rules
shared default rules

D. shared pre-rules
DATACENTER_DG pre-rules
rules configured locally on the firewall
DATACENTER_DG post-rules
shared post-rules
DATACENTER_DG default rules

Correct Answer: A
Section:

QUESTION 115
How can Panorama help with troubleshooting problems such as high CPU or resource exhaustion on a managed firewall?

A. Firewalls send SNMP traps to Panorama when resource exhaustion is detected Panorama generates a system log and can send email alerts
B. Panorama provides visibility into all the system and traffic logs received from firewalls it does not offer any ability to see or monitor resource utilization on managed firewalls
C. Panorama monitors all firewalls using SNMP It generates a system log and can send email alerts when resource exhaustion is detected on a managed firewall
D. Panorama provides information about system resources of the managed devices in the Managed Devices > Health menu

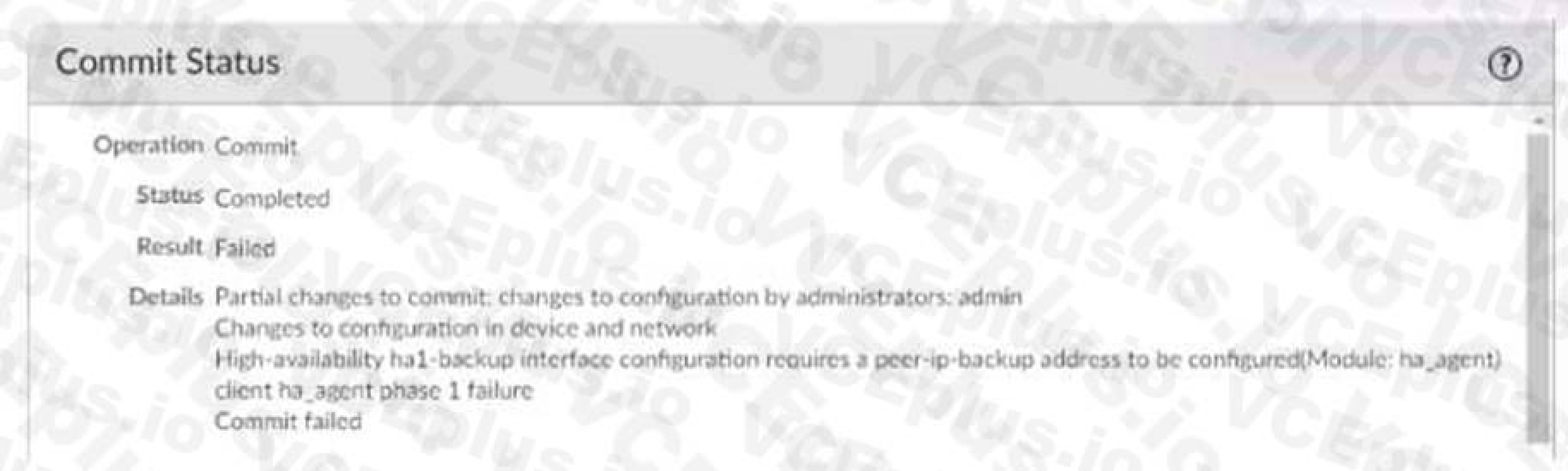
Correct Answer: D
Section:
Explanation:
Panorama can help with troubleshooting problems such as high CPU or resource exhaustion on a managed firewall by providing information about system resources of the managed devices in the Managed Devices > Health menu. This is explained in the Palo Alto Networks PCNSE Study Guide in Chapter 13: Panorama, under the section "Monitoring Managed Firewalls with Panorama": "The Panorama web interface provides information about the system resources of the managed devices. In the Managed Devices > Health menu, you can view the CPU, memory, and disk usage of each managed device. This information can help you troubleshoot problems such as high CPU or resource exhaustion on a managed firewall."

QUESTION 116
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

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClyTCAS The order in which the device checks for URL categories is as follows:Block list Allow list Custom categories Device cache BrightCloud downloaded database Cloud lookup (if enabled

QUESTION 117
After configuring HA in Active/Passive mode on a pair of firewalls the administrator gets a failed commit with the following details.



Commit Status

Operation Commit

Status Completed

Result Failed

Details Partial changes to commit: changes to configuration by administrators: admin
Changes to configuration in device and network
High-availability ha1-backup interface configuration requires a peer-ip-backup address to be configured(Module: ha_agent)
client ha_agent phase 1 failure
Commit failed

What are two s for this type of issue? (Choose two)

A. The peer IP is not included in the permit list on Management Interface Settings
B. The Backup Peer HA1 IP Address was not configured when the commit was issued
C. Either management or a data-plane interface is used as HA1-backup
D. One of the firewalls has gone into the suspended state

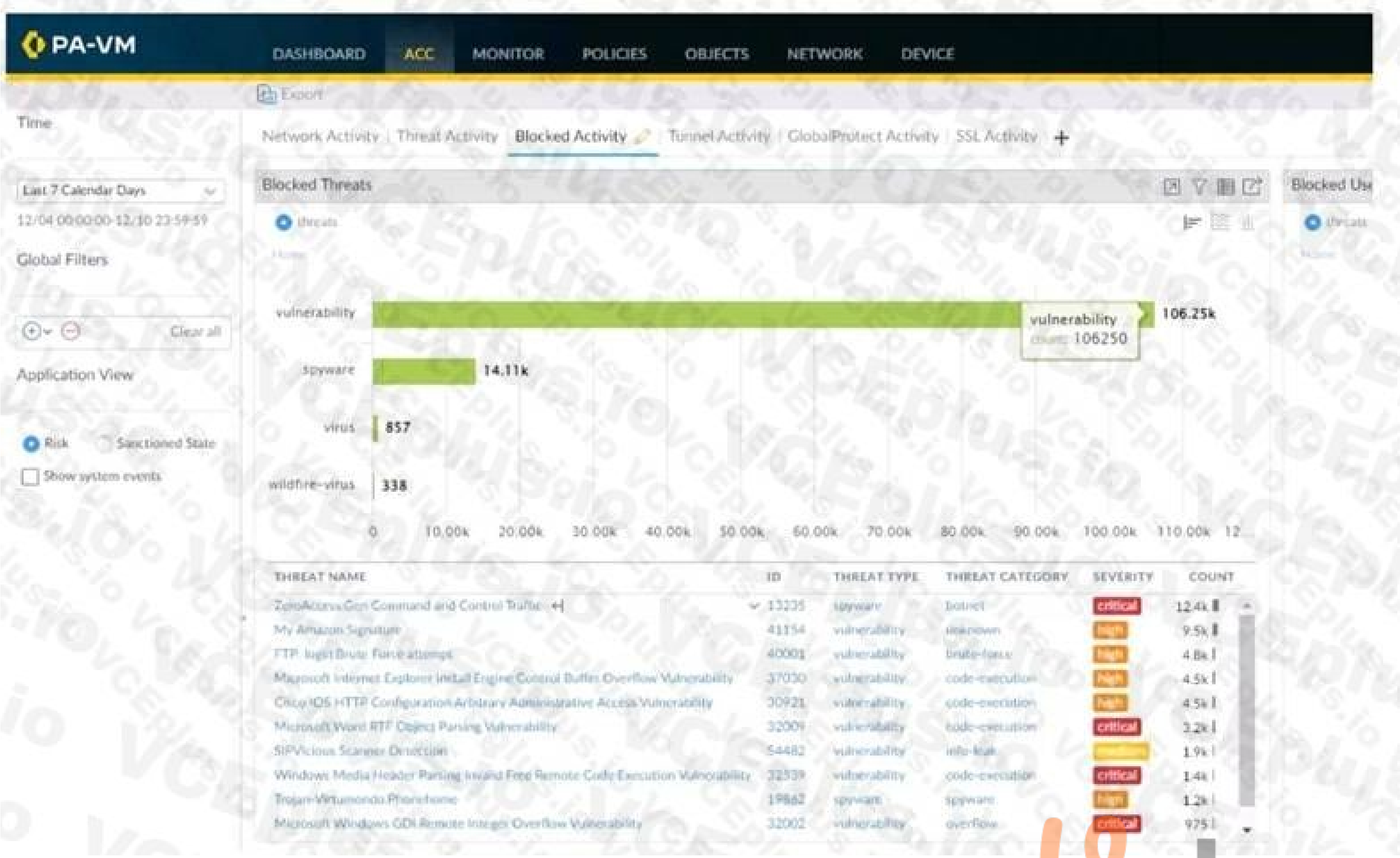
Correct Answer: B, C
Section:
Explanation:
Cause The issue is seen when the HA1-backup is configured with either management (MGT) or an in- band interface. The "Backup Peer HA1 IP Address" is not configured :
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?
id=kA14u0000008UmPCAU&lang=e n_US%E2%80%A9

QUESTION 118
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 Panoram a.
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

Correct Answer: C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CloRCAS

QUESTION 119
Refer to the exhibit.



THREAT NAME	ID	THREAT TYPE	THREAT CATEGORY	SEVERITY	COUNT
ZeroAccess.Gen Command and Control Traffic	13235	spyware	botnet	critical	12.4k
My Amazon Signature	41154	vulnerability	unknown	high	9.5k
FTP: login Brute Force attempt	40001	vulnerability	brute-force	high	4.8k
Microsoft Internet Explorer Install Engine Control Buffer Overflow Vulnerability	37030	vulnerability	code-execution	high	4.5k
Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	30921	vulnerability	code-execution	high	4.5k
Microsoft Word RTF Object Parsing Vulnerability	32009	vulnerability	code-execution	critical	3.2k
SIPVicious Scanner Detection	54482	vulnerability	info-leak	medium	1.9k
Windows Media Header Parsing Invalid Free Remote Code Execution Vulnerability	32539	vulnerability	code-execution	critical	1.4k
Trojan-Virtumonde Phonehome	19862	spyware	spyware	high	1.2k
Microsoft Windows GDI Remote Integer Overflow Vulnerability	32002	vulnerability	overflow	critical	975

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.

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-the-application- command-center/interact-with-the-acc#id5cc39dae-04cf-4936-9916-1a4b0f3179b9

QUESTION 120
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.

Correct Answer: B, C
Section:
Explanation:
These two methods allow the administrator to see the dependent applications for a security policy rule that uses application-based criteria. The App Dependency application list shows the applications that are required for

the rule to function properly1. The Depends On application list shows the applications that are implicitly added to the rule based on the predefined dependencies2.Reference: 1: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/app-id-features/simplified-application-dependency-workflow 2: https://docs.paloaltonetworks.com/pan- os/10-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies

QUESTION 121
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.

Correct Answer: C
Section:
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=e n_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetailhttps://help.aryaka.com/display/public/KNOW/Palo+Alto+Networks+NFV+Technical+Brief

QUESTION 122
An engineer is designing a deployment of multi-vsys firewalls.
What must be taken into consideration when designing the device group structure?

A. Multiple vsys and firewalls can be assigned to a device group, and a multi-vsys firewall must have all its vsys in a single device group.
B. Only one vsys or one firewall can be assigned to a device group, except for a multi-vsys firewall, which must have all its vsys in a single device group.
C. Multiple vsys and firewalls can be assigned to a device group, and a multi-vsys firewall can have each vsys in a different device group.
D. Only one vsys or one firewall can be assigned to a device group, and a multi-vsys firewall can have each vsys in a different device group.

Correct Answer: C
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClETCA0

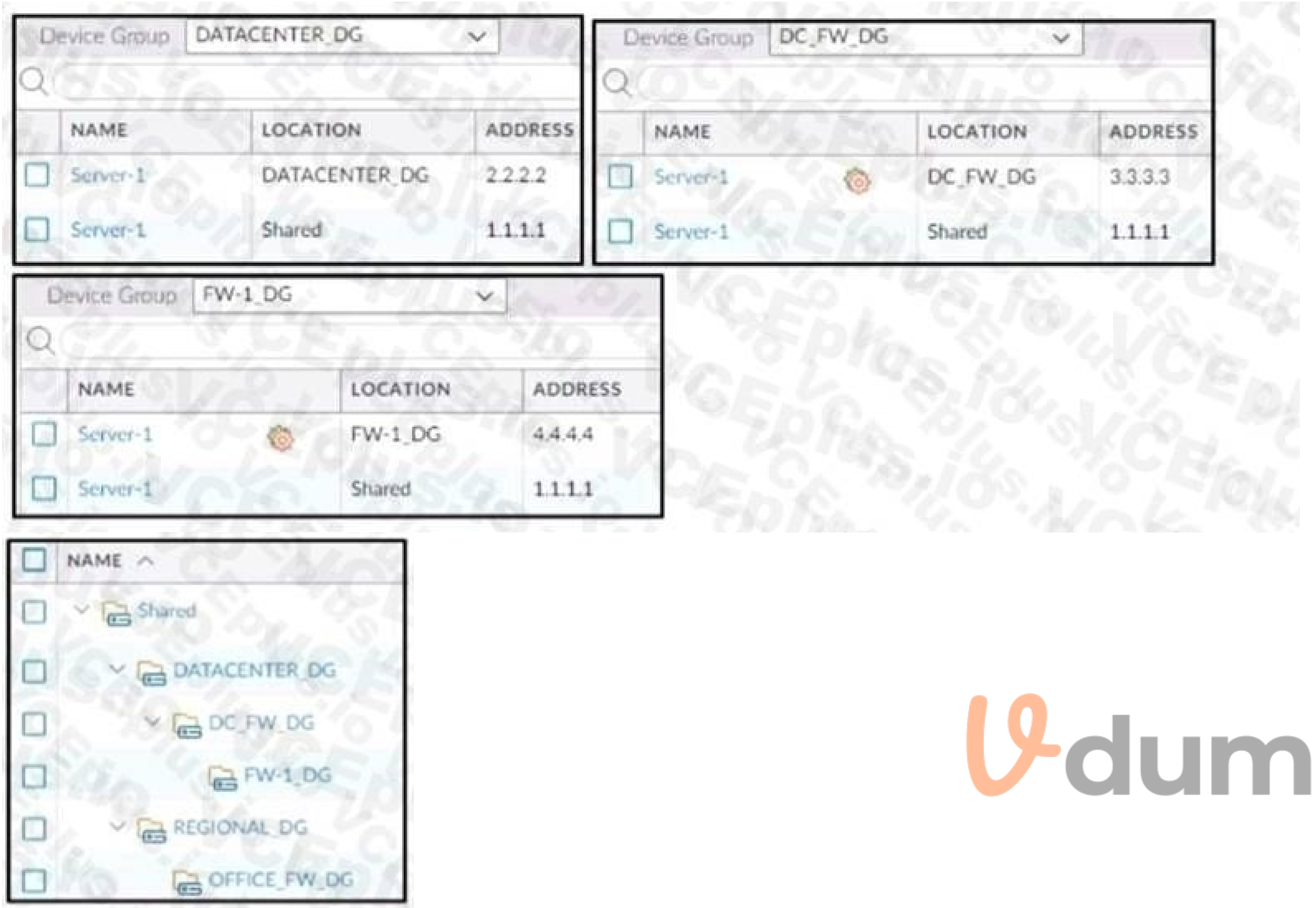
QUESTION 123
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same firewall. The update contains an application that matches the same traffic signatures as the custom application.
Which application will be used to identify traffic traversing the firewall?

A. Custom application
B. Unknown application
C. Incomplete application
D. Downloaded application

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom- application-and-threat-signatures/about-custom-application-signatures.html

QUESTION 124

Refer to the exhibit.



Device Group: DATACENTER_DG

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

Device Group: DC_FW_DG

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

Device Group: FW-1_DG

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

□ NAME

□ Shared

□ DATACENTER_DG

□ DC_FW_DG

□ FW-1_DG

□ REGIONAL_DG

□ OFFICE_FW_DG

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

A. Server-1 on FW-1 will have IP 1.1.1.1. Server-1 will not be pushed to FW-2.

B. Server-1 on FW-1 will have IP 3.3.3.3. Server-1 will not be pushed to FW-2.

C. Server-1 on FW-1 will have IP 2.2.2.2. Server-1 will not be pushed to FW-2.

D. Server-1 on FW-1 will have IP 4.4.4.4. Server-1 on FW-2 will have IP 1.1.1.1.

Correct Answer: D
Section:
Explanation:
FW-1 will get the value from FW-DG1 while FW-2 will get the value from the Shared DG since novalues are present in its parent DGs. https://docs.paloaltonetworks.com/panorama/9-1/panorama- admin/manage-firewalls/manage-device-groups/manage-precedence-of-inherited-objects

QUESTION 125

What happens, by default, when the GlobalProtect app fails to establish an IPSec tunnel to the GlobalProtect gateway?

A. It stops the tunnel-establishment processing to the GlobalProtect gateway immediately.
B. It tries to establish a tunnel to the GlobalProtect gateway using SSL/TLS.
C. It keeps trying to establish an IPSec tunnel to the GlobalProtect gateway.
D. It tries to establish a tunnel to the GlobalProtect portal using SSL/TLS.

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClfoCAC "Should the IPSec connection fail, VPN will fall back to SSL protocol."

QUESTION 126
An engineer wants to configure aggregate interfaces to increase bandwidth and redundancy between the firewall and switch. Which statement is correct about the configuration of the interfaces assigned to an aggregate interface group?

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

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure- interfaces/configure-an-aggregate-interface-group

QUESTION 127
What is a key step in implementing WildFire best practices?

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

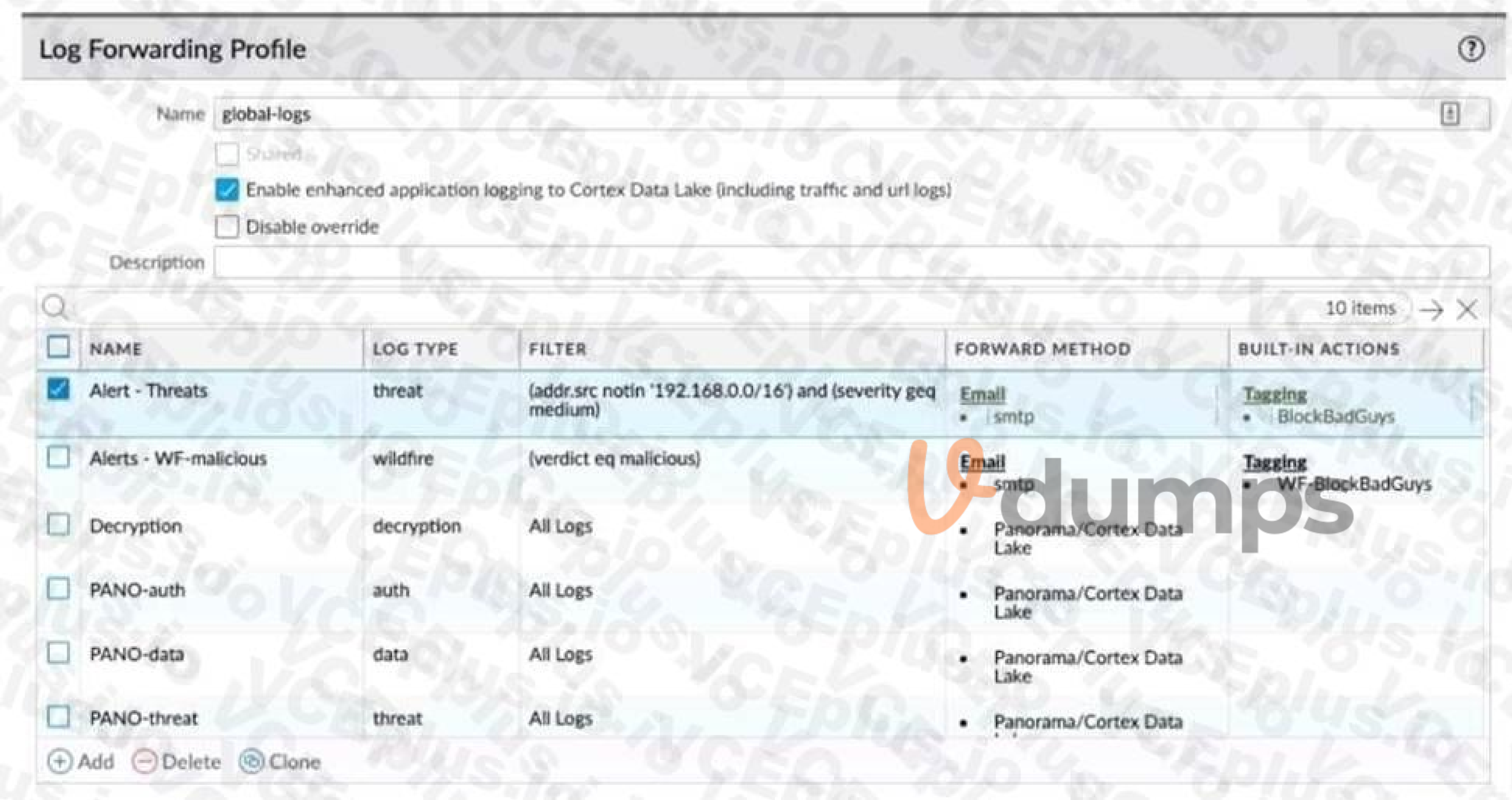
Correct Answer: D
Section:
Explanation:
In the WildFire best practices linked below, the first step is to "... make sure that you have an active Threat Prevention subscription. Together, WildFireÆ and Threat Prevention enable comprehensivethreat detection and prevention." https:// docs.paloaltonetworks.com/wildfire/10-1/wildfire- admin/wildfire-deployment-best-practices/wildfire-best-practices.html

QUESTION 128
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.

Correct Answer: D
Section:
Explanation:
Short According to the Palo Alto Networks documentation, "To use a template stack for a device group, you must add the template stack as a reference template in the device group. This enables you to use zones and interfaces defined in the template stack when creating policies for the device group." Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks

QUESTION 129
Review the images.



Log Forwarding Profile

Name global-logs

□ Shared

☑ Enable enhanced application logging to Cortex Data Lake (including traffic and url logs)

□ Disable override

Description

10 items

□	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
☑	Alert - Threats	threat	(addr.src notin '192.168.0.0/16') and (severity geq medium)	Email • smtp	Tagging • BlockBadGuys
□	Alerts - WF-malicious	wildfire	(verdict eq malicious)	Email • smtp • Panorama/Cortex Data Lake	Tagging • WF-BlockBadGuys
□	Decryption	decryption	All Logs	• Panorama/Cortex Data Lake	
□	PANO-auth	auth	All Logs	• Panorama/Cortex Data Lake	
□	PANO-data	data	All Logs	• Panorama/Cortex Data Lake	
□	PANO-threat	threat	All Logs	• Panorama/Cortex Data	

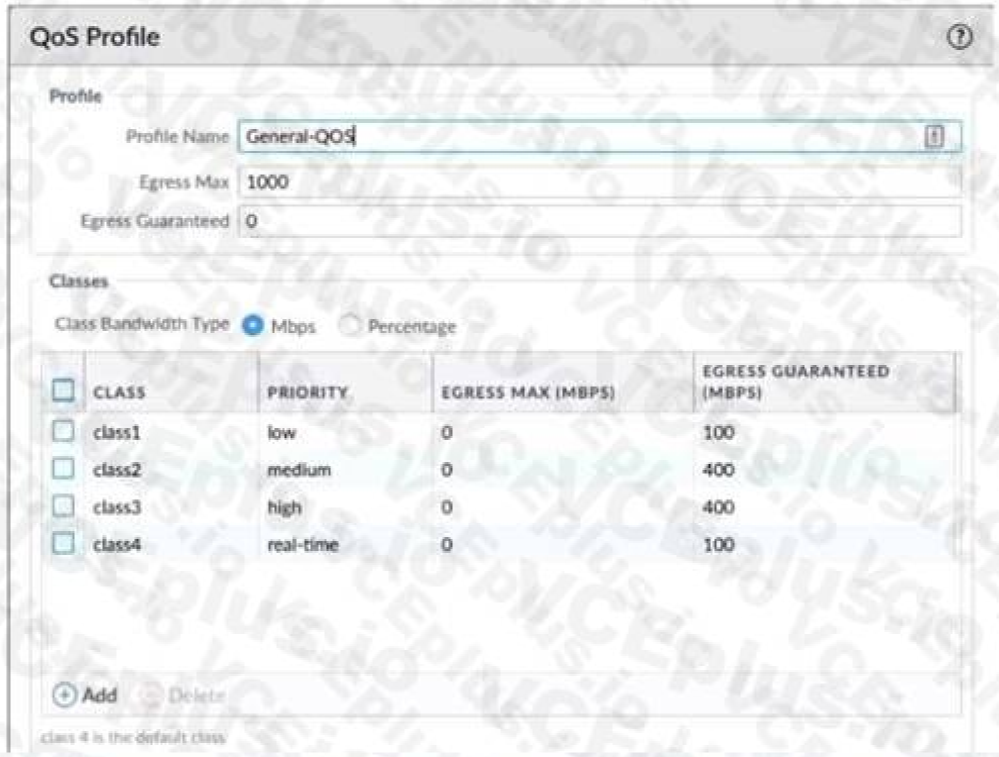
A firewall policy that permits web traffic includes the What is the result of traffic that matches the "Alert - Threats" Profile Match List?

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.

Correct Answer: C
Section:
Explanation:
The threat profile has the action set to "alert" which means that the traffic is allowed but logged. The profile also has the "Tag Source IP" option enabled with the tag name "BadGuys" and the timeout value of 180 minutes. This means that any source IP address that matches a threat signature will be tagged with "BadGuys" for 180 minutes. The tag can be used for dynamic address groups or external dynamic lists to enforce policy actions based on the tag. Reference: :https:// docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/set-up-antivirus- anti-spyware-and-vulnerability-protection/tag-source-ip-addresses-that-trigger-threat-signatures

QUESTION 130

View the screenshots.



QoS Profile

Profile

Profile Name: General-QOS

Egress Max: 1000

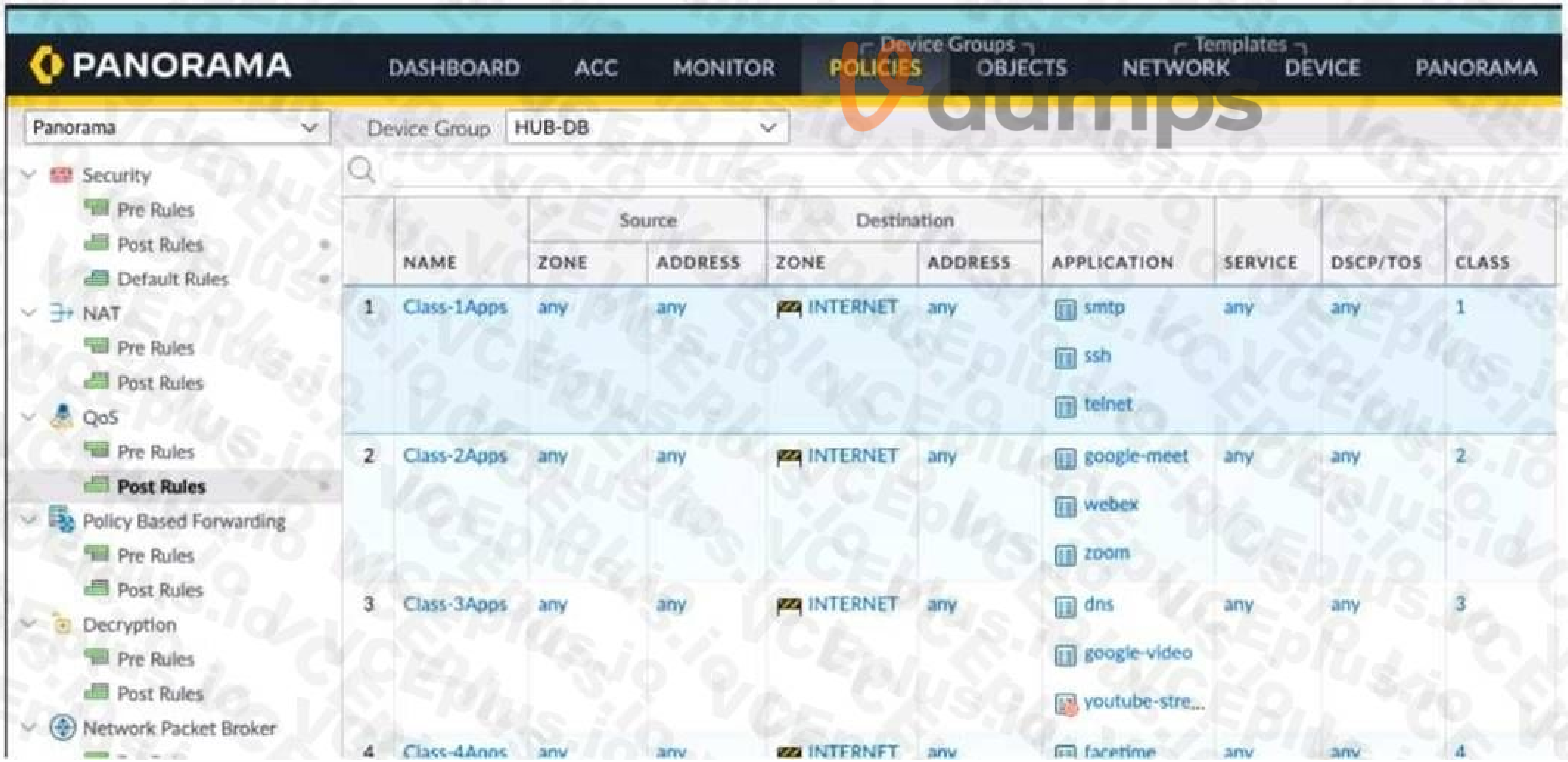
Egress Guaranteed: 0

Classes

Class Bandwidth Type: ● Mbps ○ Percentage

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

class 4 is the default class



Device Group: HUB-DB

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

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

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

Correct Answer: A, B
Section:
Explanation:
The QoS profile assigns different classes and guaranteed bandwidth percentages to different applications. The QoS policy rules apply the QoS profile to the traffic based on the source and destination zones. The priority of a class is determined by its number, with lower numbers having higher priority. The bandwidth of a class is determined by its guaranteed percentage, with higher percentages having more bandwidth. Based on this information, DNS belongs to class 1 which has the highest priority (1) and the most bandwidth (40%). SSH belongs to class 4 which has the lowest priority (4) and the least bandwidth (5%). Therefore, DNS has a higher priority and more bandwidth than SSH. Similarly, Google-video belongs to class 2 which has the second highest priority (2) and the second most bandwidth (30%). WebEx belongs to class 3 which has the third highest priority (3) and the third most bandwidth (25%). Therefore, Google-video has a higher priority and more bandwidththan WebEx. Reference: : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of- service/qos-concepts/qos-profiles

QUESTION 131
A system administrator runs a port scan using the company tool as part of vulnerability check. The administrator finds that the scan is identified as a threat and is dropped by the firewall. After further investigating the logs, the administrator finds that the scan is dropped in the Threat Logs.
What should the administrator do to allow the tool to scan through the firewall?

A. Remove the Zone Protection profile from the zone setting.
B. Add the tool IP address to the reconnaissance protection source address exclusion in the Zone Protection profile.
C. Add the tool IP address to the reconnaissance protection source address exclusion in the DoS Protection profile.
D. Change the TCP port scan action from Block to Alert in the Zone Protection profile.

Correct Answer: B
Section:
Explanation:
The administrator should add the tool IP address to the reconnaissance protection source address exclusion in the Zone Protection profile to allow the tool to scan through the firewall. Reconnaissance protection is a feature of Zone Protection profiles that allows the firewall to detect and block network reconnaissance attempts, such as port scans. The source address exclusion list allows theadministrator to whitelist up to 20 IP addresses or netmask address objects that are exempt fromreconnaissance protection1. Option A is incorrect because removing the Zone Protection profile from the zone setting would disable all the zone protection features, not just reconnaissance protection.This would reduce the security of the zone and expose it to other types of attacks. Option C is incorrect because adding the tool IP address to the reconnaissance protection source address exclusion in the DoS Protection profile would not have any effect. DoS Protection profiles are used to protect against excessive traffic volume, not network reconnaissance attempts. Option D is incorrect because changing the TCP port scan action from Block to Alert in the Zone Protection profile would only affect TCP port scans, not other types of scans. It would also affect all TCP port scans, not just those from the tool IP address.https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos- protection/configure-zone-protection-to-increase-network-security/configure-reconnaissance- protection

QUESTION 132
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.

Correct Answer: D
Section:

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKQCA0 "Locally defined dynamic updates setting on a managed Palo Alto Networks firewall take preference over the Panorama pushed setting."

QUESTION 133
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

Correct Answer: A, B, E
Section:

QUESTION 134
An administrator wants to grant read-only access to all firewall settings, except administrator accounts, to a new-hire colleague in the IT department.
Which dynamic role does the administrator assign to the new-hire colleague?

A. Device administrator (read-only)
B. System administrator (read-only)
C. Firewall administrator (read-only)
D. Superuser (read-only)

Correct Answer: A
Section:
Explanation:
Read-only access to all firewall settings except password profiles (no access) and administratoraccounts (only the logged in account is visible). https://docs.paloaltonetworks.com/pan-os/10- 1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types

QUESTION 135
Which feature checks Panorama connectivity status after a commit?

A. Automated commit recovery
B. Scheduled config export
C. Device monitoring data under Panorama settings
D. HTTP Server profiles

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama- features/automatic-panorama-connection-recovery

QUESTION 136
What is the dependency for users to access services that require authentication?

A. An Authentication profile that includes those services
B. Disabling the authentication timeout
C. An authentication sequence that includes those services
D. A Security policy allowing users to access those services

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication- policy/configure-authentication-policy

QUESTION 137
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>

Correct Answer: B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClivCAC

QUESTION 138
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

Correct Answer: B
Section:
Explanation:
The **IKE crypto profile** is used to set up the encryption and authentication algorithms used for the key exchange process in IKE Phase 1, and lifetime of the keys, which specifies how long the keys are valid. To invoke the profile, you must attach it to the IKE Gateway configuration. The **IPSec crypto profile** is invoked in IKE Phase 2. It specifies how the data is secured within the tunnel when Auto Key IKE is used to automatically generate keys for the IKE SAs.

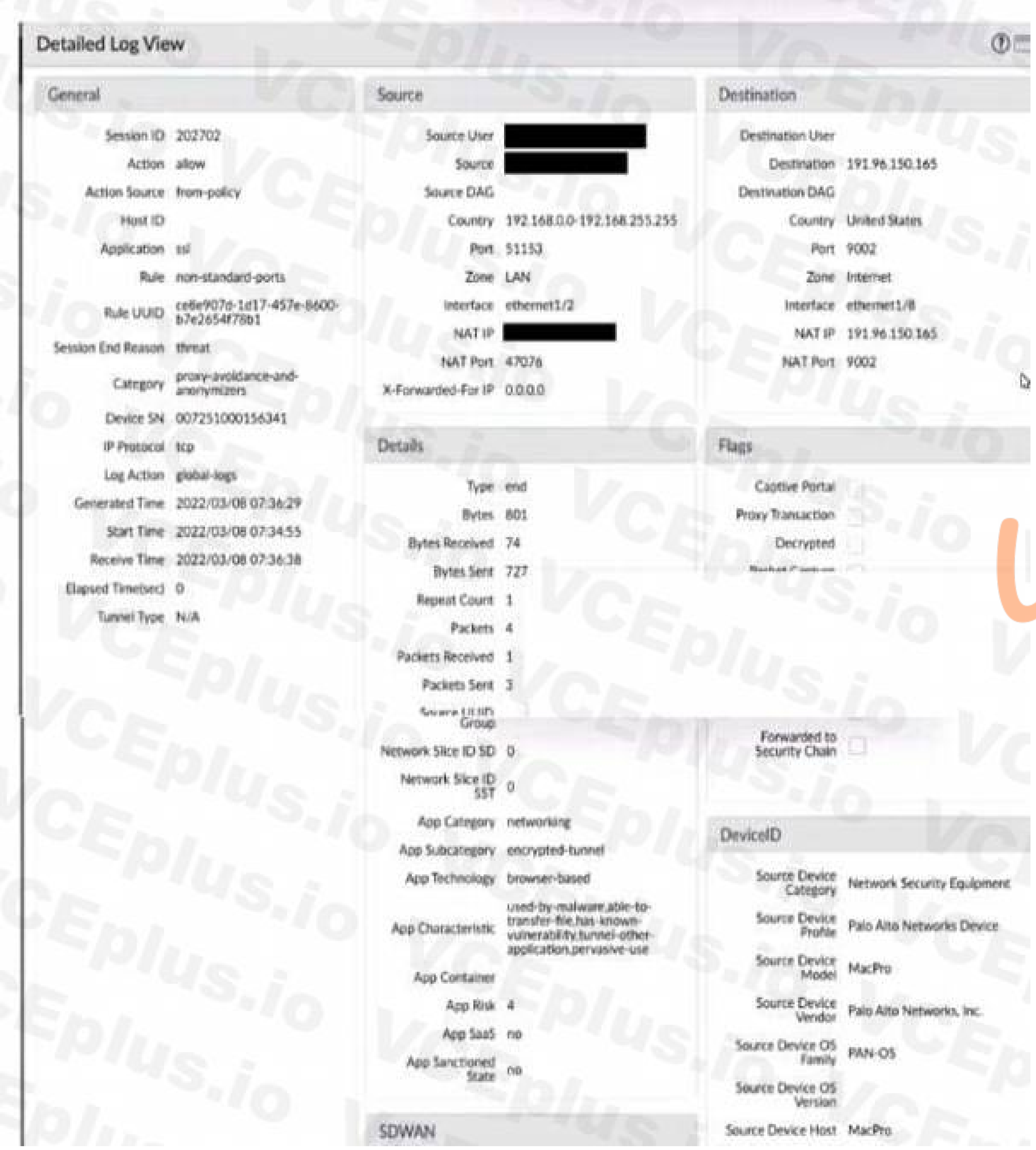
QUESTION 139
How does Panorama prompt VMWare NSX to quarantine an infected VM?

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

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/set-up-the-vm-series- firewall-on-nsx/set-up-the-vm-series-firewall-on-vmware-nsx/dynamically-quarantine-infected- guests.html#id8e9a242e-e038-4ba2-b0ea-eaaf53690be0

QUESTION 140

Given the screenshot, how did the firewall handle the traffic?



Detailed Log View

General

Session ID 202702
Action allow
Action Source from-policy
Host ID
Application ssl
Rule non-standard-ports
Rule UUID ce6e907d-1d17-457e-8600-b7e2654f78b1
Session End Reason threat
Category proxy-avoidance-and-anonymizers
Device SN 007251000156341
IP Protocol tcp
Log Action global-logs
Generated Time 2022/03/08 07:36:29
Start Time 2022/03/08 07:34:55
Receive Time 2022/03/08 07:36:38
Elapsed Time(sec) 0
Tunnel Type N/A

Source

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

Destination

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

Details

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

SDWAN

Flags

Captive Portal □
Proxy Transaction □
Decrypted □
Forwarded to Security Chain □

DeviceID

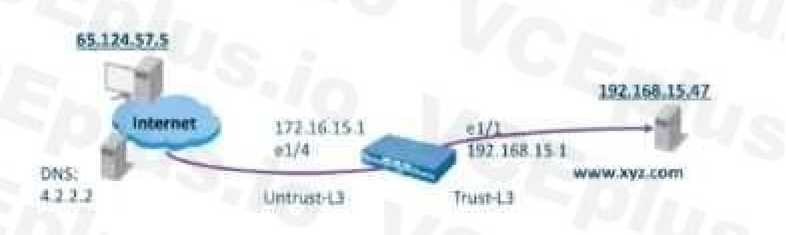
Source Device Category Network Security Equipment
Source Device Profile Palo Alto Networks Device
Source Device Model MacPro
Source Device Vendor Palo Alto Networks, Inc.
Source Device OS Family PAN-OS
Source Device OS Version
Source Device Host MacPro

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

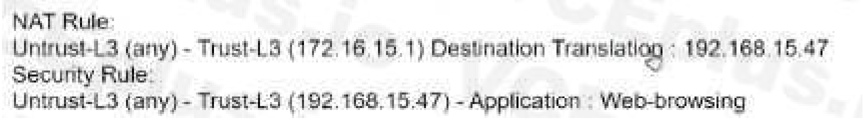
Correct Answer: B

Section:
Explanation:
The screenshot shows the threat log which records the traffic that matches a threat signature or is blocked by a security profile. The log entry indicates that the traffic was allowed by the security policy rule "Allow-All" but was denied by the vulnerability protection profile "strict" as a threat. The threat name is "Microsoft Windows SMBv1 Multiple Vulnerabilities (MS17-010: EternalBlue)" and the action is "reset-both" which means that the firewall reset both the client and server connections.Reference: : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog- for-monitoring/syslog-field-descriptions/threat-log-fields

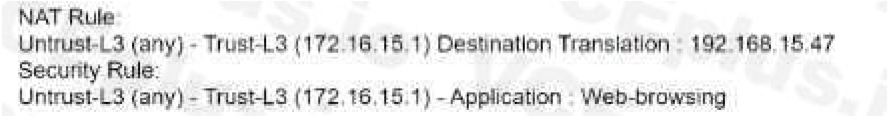
QUESTION 141
A user at an external system with the IP address 65.124.57.5 queries the DNS server at 4. 2.2.2 for the IP address of the web server, www,xyz.com. The DNS server returns an address of 172.16.15.1
In order to reach Ire web server, which Security rule and NAT rule must be configured on the firewall?



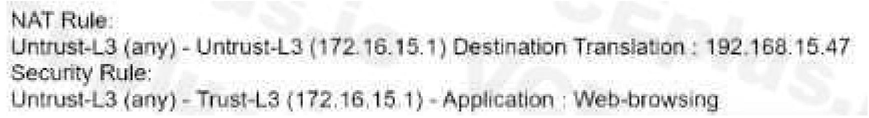
A.


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

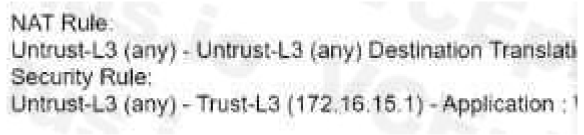
B.


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 Translati
Security Rule:
Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application : \

Correct Answer: C
Section:
Explanation:
The addresses used in destination NAT rules always refer to the original IP address in the packet (that is, the pre-translated address). The destination zone in the NAT rule is determined after the route lookup of the destination IP address in the original packet (that is, the pre-NAT destination IP address). The addresses in the security policy also refer to the IP address in the original packet (that is, the pre-NAT address). However, the destination zone is the zone where the end host is physically connected. In other words, the destination zone in the security rule is determined after the routelookup of the post-NAT destination IP address.
https://docs.paloaltonetworks.com/pan-os/9-1/pan- os-admin/networking/nat/ nat-configuration-examples/destination-nat-exampleone-to-one-mapping

QUESTION 142
An administrator is receiving complaints about application performance degradation. After checking the ACC. the administrator observes that there Is an excessive amount of SSL traffic
Which three elements should the administrator configure to address this issue? (Choose three.)

A. QoS on the ingress Interface for the traffic flows
B. An Application Override policy for the SSL traffic
C. A QoS policy for each application ID

D. A QoS profile defining traffic classes
E. QoS on the egress interface for the traffic flows

Correct Answer: A, D, E
Section:
Explanation:
To address the issue of excessive SSL traffic, the administrator should configure QoS on both the ingress and egress interfaces for the traffic flows. This will allow the administrator to control the bandwidth allocation and priority of different applications based on their QoS classes. The administrator should also define a QoS profile that specifies the traffic classes and their guaranteed bandwidth percentages. The QoS profile can then be applied to a QoS policy rule that matches the SSL traffic based on source and destination zones or other criteria. Reference: :https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/configure-qos

QUESTION 143
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

Correct Answer: B, C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-inboundinspection

QUESTION 144
A network security administrator has been tasked with deploying User-ID in their organization.
What are three valid methods of collecting User-ID information in a network? (Choose three.)

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

Correct Answer: A, B, C
Section:
Explanation:
User-ID is a feature that enables the firewall to identify users and groups based on their IP addresses, usernames, or other attributes.
There are three valid methods of collecting User-ID information in a network:
Windows User-ID agent: This is a software agent that runs on a Windows server and collects user mapping information from Active Directory, Exchange servers, or other sources.
GlobalProtect: This is a VPN solution that provides secure remote access for users and devices. It also collects user mapping information from endpoints that connect to the firewall using GlobalProtect.
XMLAPI: This is an application programming interface that allows third-party applications or scripts to send user mapping information to the firewall using XML format.

QUESTION 145
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

Correct Answer: D
Section:
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.

QUESTION 146
A network administrator is trying to prevent domain username and password submissions to phishing sites on some allowed URL categories Which set of steps does the administrator need to take in the URL Filtering profile to prevent credential phishing on the firewall?

A. Choose the URL categories on Site Access column and set action to block Click the User credential Detection tab and select IP User Mapping Commit
B. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select use IP User Mapping Commit
C. Choose the URL categories in the User Credential Submission column and set action to block Select the URL filtering settings and enable Domain Credential Filter Commit
D. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select Use Domain Credential Filter Commit

Correct Answer: D
Section:

QUESTION 147
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

Correct Answer: B, D
Section:
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.

QUESTION 148
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

Correct Answer: C
Section:
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.

QUESTION 149
How should an administrator enable the Advance Routing Engine on a Palo Alto Networks firewall?

A. Enable Advanced Routing Engine in Device > Setup > Session > Session Settings, then commit and reboot.

B. Enable Advanced Routing in Network > Virtual Routers > Redistribution Profiles and then commit.

C. Enable Advanced Routing in Network > Virtual Routers > Router Settings > General, then commit and reboot.

D. Enable Advanced Routing in General Settings of Device > Setup > Management, then commit and reboot

Correct Answer: C
Section:
Explanation:
Enable Advanced Routing in Network > Virtual Routers > Router Settings > General, then commit and reboot1. This means that the administrator can enable advanced routing features such as RIB filtering, BFD, multicast, and redistribution profiles for each virtual router on the firewall. The firewall requires a reboot after enabling advanced routing to apply the changes.

QUESTION 150
A firewall engineer creates a new App-ID report under Monitor > Reports > Application Reports > New Application to monitor new applications on the network and better assess any Security policy updates the engineer might want to make.
How does the firewall identify the New App-ID characteristic?

A. It matches to the New App-IDs downloaded in the last 30 days.

B. It matches to the New App-IDs downloaded in the last 90 days

C. It matches to the New App-IDs installed since the last time the firewall was rebooted

D. It matches to the New App-IDs in the most recently installed content releases.

Correct Answer: D
Section:
Explanation:
When creating a new App-ID report under Monitor > Reports > Application Reports > New Application, the firewall identifies new applications based on the New App-IDs in the most recently installed content releases. The New App-IDs are the application signatures that have been added in the latest content release, which can be found under Objects > Security Profiles > Application. This allows the engineer to monitor any new applications that have been added to the firewall's database and evaluate whether to allow or block them with a Security policy update.

QUESTION 151
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

Correct Answer: B, C
Section:
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 thatthe proxy can handle HTTPS requests that use ports other than 443, which may be required by someapplications or websites. Transparent proxies can only intercept HTTPS traffic on port 443, whichlimits their functionality.

QUESTION 152
What is the best definition of the Heartbeat Interval?

A. The interval in milliseconds between hello packets

B. The frequency at which the HA peers check link or path availability

C. The frequency at which the HA peers exchange ping

D. The interval during which the firewall will remain active following a link monitor failure

Correct Answer: A
Section:
Explanation:
According to the Palo Alto Networks Knowledge Base12, the best definition of the Heartbeat Interval is A. The interval in milliseconds between hello packets.
The Heartbeat Interval is a CLI command that configures how often an HA peer sends an ICMP ping to its partner through the HA control link. The ping verifies network connectivity and ensures that the peer kernel is responsive. The default value is 1000ms for all Palo Alto Networks platforms.

QUESTION 153
An administrator wants to configure the Palo Alto Networks Windows User-ID agent to map IP addresses to usernames. The company uses four Microsoft Active Directory servers and two Microsoft Exchange servers, which can provide logs for login events.
All six servers have IP addresses assigned from the following subnet: 192.168 28.32/27. The Microsoft Active Directory servers reside in 192.168.28.32/28. and the Microsoft Exchange servers resideL in 192.168.28 48/28
What information does the administrator need to provide in the User Identification > Discovery section?

A. The IP-address and corresponding server type (Microsoft Active Directory or Microsoft Exchange) for each of the six servers

B. Network 192 168.28.32/28 with server type Microsoft Active Directory and network 192.168.28.48/28 with server type Microsoft Exchange

C. Network 192 168 28.32/27 with server type Microsoft

D. One IP address of a Microsoft Active Directory server and "Auto Discover" enabled to automatically obtain all five of the other servers

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

QUESTION 154
A network engineer troubleshoots a VPN Phase 2 mismatch and decides that PFS (Perfect Forward Secrecy) needs to be enabled.
What action should the engineer take?

A. Add an authentication algorithm in the IPSec Crypto profile.
B. Enable PFS under the IPSec Tunnel advanced options.
C. Select the appropriate DH Group under the IPSec Crypto profile.
D. Enable PFS under the IKE gateway advanced options

Correct Answer: C
Section:
Explanation:
PFS (Perfect Forward Secrecy) is a feature that ensures that the encryption keys used for each IPSec session are not derived from previous keys. This provides more security in case one key is compromised. To enable PFS, the administrator needs to select the appropriate DH (Diffie-Hellman) Group under the IPSec Crypto profile that is applied to the IPSec tunnel. The DH Group determinesthe strength of the key exchange and should match on both ends of the tunnel1. The other optionsdo not enable PFS. The authentication algorithm in the IPSec Crypto profile is used to verify theintegrity of the IPSec packets. The PFS option under the IPSec Tunnel advanced options or the IKE gateway advanced options does not exist in the WebUI. Reference: 1: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpn/site-to-site-vpn/configure-the- ipsec-crypto-profile

QUESTION 155
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

Correct Answer: B
Section:
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 (PIMDM).
PIM-SM uses a rendezvous point (RP) as a central point for distributing multicast traffic, while PIM-DM uses flooding and pruning techniques2. 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.

QUESTION 156
A super user is tasked with creating administrator accounts for three contractors. For compliance purposes, all three contractors will be working with different device-groups m their hierarchy to deploy policies and objects.
Which type of role-based access is most appropriate for this project?

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

Correct Answer: B
Section:
Explanation:
A Device Group and Template Admin is a type of role-based access that allows the administrator to assign different privileges for different device groups and templates. This is useful for managing multiple firewalls with different configuration needs. For example, the administrator can create aDevice Group and Template Admin role that allows the contractors to deploy policies and objects only to their assigned device groups and templates1. The other options are not suitable for this project. A Dynamic Admin with the Panorama Administrator role has full access to all device groups and templates2. A Custom Panorama Admin can have limited access to device groups and templates, but cannot have different privileges for different device groups and templates3. A Dynamic Read onlysuperuser can only view the configuration and logs, but cannot deploy policies and objects.Reference: 1: https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama- overview/role-based-access-control/administrative-roles/device-group-and-template-admin 2:https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role- based-access-control/administrative-roles/dynamic-admin 3: https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role- based-access-control/administrative-roles/custom-panorama-admin : https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role- based-access-control/administrative-roles/dynamic-read-

only-superuser

QUESTION 157

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

Correct Answer: B

Section:

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)4. 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-rejectnon- 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.

QUESTION 158

In an existing deployment, an administrator with numerous firewalls and Panorama does not see any WildFire logs in Panoram a. Each firewall has an active WildFire subscription On each firewall. WildFire togs are available.

This issue is occurring because forwarding of which type of logs from the firewalls to Panorama is missing?

A. Threat logs

B. Traffic togs

C. System logs

D. WildFire logs

Correct Answer: A

Section:

Explanation:

Access to the WildFire logs from Panorama requires the following: a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama.https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/monitor-network- activity/use-case-respond-to-an-incident-using-panorama/review-wildfire-logs

QUESTION 159

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

A. GlobalProtect

B. Microsoft Active Directory

C. Microsoft Exchange

D. Syslog Listener

Correct Answer: B

Section:

Explanation:

For collecting User-ID user mapping information, the most reliable and commonly used source is directory services, with Microsoft Active Directory being the predominant choice in many organizational environments.

C) Microsoft Active Directory:

Microsoft Active Directory is a directory service used for user authentication and authorization. It provides a comprehensive database of user accounts, groups, and other objects within an organization's network. Palo Alto Networks firewalls can integrate with Active Directory to obtain real-time user mapping information, which is crucial for implementing security policies based on user identity.

The integration involves monitoring Active Directory domain controllers for security logs that contain user login events, IP address mappings, and other relevant information. This allows the firewall to accurately and dynamically map user identities to IP addresses, enhancing the granularity and effectiveness of security policies.

Compared to other sources like Syslog Listener, Microsoft Exchange, or GlobalProtect, Active Directory offers direct and comprehensive insights into user activities and is therefore considered the most reliable source for User-ID user mapping in Palo Alto Networks environments.

QUESTION 160
Where is Palo Alto Networks Device Telemetry data stored on a firewall with a device certificate installed?

A. Cortex Data Lake
B. Panorama
C. On Palo Alto Networks Update Servers
D. M600 Log Collectors

Correct Answer: C
Section:
Explanation:

Palo Alto Networks Device Telemetry data, collected from firewalls with a device certificate installed, is stored on Palo Alto Networks Update Servers. This telemetry data includes information about threats, device health, and other operational metrics that are crucial for the continuous improvement of security services and threat intelligence. The collected data is anonymized and securely transmitted to Palo Alto Networks, where it is used to enhance the overall effectiveness of threat identification and prevention capabilities across all deployed devices. This collaborative approach helps in keeping the security ecosystem updated and resilient against emerging threats.

QUESTION 161
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

Correct Answer: C, D, E
Section:
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.

QUESTION 162

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

Correct Answer: B, C, E
Section:
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.

QUESTION 163
An organization is interested in migrating from their existing web proxy architecture to the Web Proxy feature of their PAN-OS 11.0 firewalls. Currently. HTTP and SSL requests contain the c IP address of the web server and the client browser is redirected to the proxy Which PAN-OS proxy method should be configured to maintain this type of traffic flow?

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

Correct Answer: D
Section:
Explanation:
A transparent proxy is a type of web proxy that intercepts and redirects HTTP and HTTPS requestswithout requiring any configuration on the client browser1. The firewall acts as a gateway betweenthe client and the web server, and performs security checks on the traffic.
A transparent proxy can be configured on PAN-OS 11.0 firewalls by performing the following steps1:
Enable Web Proxy under Device > Setup > Services
Select Transparent Proxy as the Proxy Type
Configure a Service Route for Web Proxy
Configure SSL/TLS Service Profile for Web Proxy
Configure Security Policy Rules for Web Proxy Traffic
By configuring a transparent proxy on PAN-OS 11.0 firewalls, an organization can migrate from their existing web proxy architecture without changing their network topology or client settings2. The firewall will maintain the same type of traffic flow as before, where HTTP and HTTPS requests contain the IP address of the web server and the client browser is redirected to the proxy1.
Answer A is not correct because DNS proxy is a type of web proxy that intercepts DNS queries from clients and resolves them using an external DNS server3. This type of proxy does not redirect HTTP or
HTTPS requests to the firewall.

QUESTION 164
A company is deploying User-ID in their network. The firewall learn needs to have the ability to see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules How can this be achieved?

A. By configuring Data Redistribution Client in Panorama > Data Redistribution
B. By configuring User-ID source device in Panorama > Managed Devices

C. By configuring User-ID group mapping in Panorama > User Identification
D. By configuring Master Device in Panorama > Device Groups

Correct Answer: C
Section:
Explanation:
User-ID group mapping is a feature that allows Panorama to retrieve user and group information from directory services such as LDAP or Active Directory1. This information can be used to enforce security policies based on user identity and group membership.
To configure User-ID group mapping on Panorama, you need to perform the following steps1:
Select Panorama > User Identification > Group Mapping Settings
Click Add and enter a name for the server profile
Select a Server Type (LDAP or Active Directory)
Click Add and enter the server details (IP address, port number, etc.)
Click OK
Select Group Include List and click Add
Select the groups that you want to include in the group mapping
Click OK
Commit your changes
By configuring User-ID group mapping on Panorama, you can see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules2.

QUESTION 165
After importing a pre-configured firewall configuration to Panorama, what step is required to ensure a commit/push is successful without duplicating local configurations?

A. Ensure Force Template Values is checked when pushing configuration.
B. Push the Template first, then push Device Group to the newly managed firewal.
C. Perform the Export or push Device Config Bundle to the newly managed firewall.
D. Push the Device Group first, then push Template to the newly managed firewall

Correct Answer: C
Section:
Explanation:
When importing a pre-configured firewall configuration to Panorama, you need to perform the following steps12:
Add the serial number of the firewall under Panorama > Managed Devices In Panorama, import the firewall's configuration bundle under Panorama > Setup > Operations > Import device configuration to Panorama Make changes to the imported firewall configuration within Panorama Commit the changes you made to Panorama Perform an Export or push Device Config Bundle operation under Panorama > Setup > Operations The Export or push Device Config Bundle operation allows you to push a complete configuration bundle from Panorama to a managed firewall without duplicating local configurations3. This operation ensures that any local settings on the firewall are preserved and merged with the settings from Panorama.

QUESTION 166
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

Correct Answer: A
Section:

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.

QUESTION 167
An engineer is tasked with configuring SSL forward proxy for traffic going to external sites.
Which of the following statements is consistent with SSL decryption best practices?

A. The forward trust certificate should not be stored on an HSM.
B. The forward untrust certificate should be signed by a certificate authority that is trusted by the clients.
C. Check both the Forward Trust and Forward Untrust boxes when adding a certificate for use with SSL decryption
D. The forward untrust certificate should not be signed by a Trusted Root CA

Correct Answer: B
Section:
Explanation:
According to the PCNSE Study Guide1, SSL forward proxy is a feature that allows the firewall to decrypt and inspect SSL traffic going to external sites. The firewall acts as a proxy between the client and the server, generating a certificate on the fly for each site.
The best practices for configuring SSL forward proxy are23:
Use a forward trust certificate that is signed by a certificate authority (CA) that is trusted by the clients. This certificate is used to sign certificates for sites that have valid certificates from trusted CAs. The clients will not see any certificate errors if they trust the forward trust certificate.
Use a forward untrust certificate that is not signed by a trusted CA. This certificate is used to sign certificates for sites that have invalid or untrusted certificates. The clients will see certificate errors if they do not trust the forward untrust certificate. This helps alert users of potential risks and prevent man-in-the-middle attacks.
Do not store the forward trust or untrust certificates on an HSM (hardware security module). The HSM does not support on-the-fly signing of certificates, which is required for SSL forward proxy.

QUESTION 168
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

Correct Answer: B, C, E
Section:
Explanation:
The GlobalProtect Gateway supports three methods for split tunneling23:
Access Route ó 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 ó 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 ó 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.

QUESTION 169
An engineer discovers the management interface is not routable to the User-ID agent What configuration is needed to allow the firewall to communicate to the User-ID agent?

A. Create a NAT policy for the User-ID agent server
B. Add a Policy Based Forwarding (PBF) policy to the User-ID agent IP
C. Create a custom service route for the UID Agent
D. Add a static route to the virtual router

Correct Answer: C
Section:
Explanation:
To allow the firewall to communicate with the User-ID agent, you need to configure a custom service route for the UID Agent23. A custom service route allows you to specify which interface and source IP address the firewall uses to connect to a specific destination service. By default, the firewall uses its management interface for services such as User-ID, but you can override this behavior by creating a custom service route.
To configure a custom service route for the UID Agent, you need to do the following steps:
Go to Device > Setup > Services and click Service Route Configuration.
In the Service column, select User-ID Agent from the drop-down list.
In the Interface column, select an interface that can reach the User-ID agent server from the dropdown list.
In the Source Address column, select an IP address that belongs to that interface from the drop-down list.
Click OK and Commit your changes.
The correct answer is C. Create a custom service route for UID Agent

QUESTION 170
Which log type will help the engineer verify whether packet buffer protection was activated?

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

Correct Answer: C
Section:
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. Packet buffer protection is a feature that prevents packet buffer exhaustion by dropping packets, discarding sessions, or blocking source IP addresses when the packet buffer utilization exceeds a certain threshold. The firewall records these events in the threat log with different threat IDs andnames1. The system log also records an alert event when the packet buffer congestion reaches thealert threshold2. The other types of logs do not show packet buffer protection events. Reference: 1:https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection 2: https://docs.paloaltonetworks.com/pan-os/10- 2/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/system-log-fields

QUESTION 171
Which GlobalProtect gateway selling is required to enable split-tunneling by access route, destination domain, and application?

A. No Direct Access to local networks
B. Tunnel mode
C. iPSec mode
D. Satellite mode

Correct Answer: B
Section:

Explanation:
To enable split-tunneling by access route, destination domain, and application, you need to configure a split tunnel based on the domain and application on your GlobalProtect gateway2. This allows you to specify which domains and applications are included or excluded from the VPN tunnel.

QUESTION 172
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

Correct Answer: A, B, D
Section:
Explanation:
These three methods are examples of multi-factor authentication that can be used to authenticate access to the firewall. A one-time password is a code that is generated by an authentication app or sent by email or SMS and expires after a single use. A user certificate is a digital credential that is issued by a trusted authority and stored on the user's device. SMS is a text message that is sent tothe user's phone number with a code or a link to verify their identity1. The other methods are notsupported by the firewall for multi-factor authentication. Voice and fingerprint are biometric factorsthat require special hardware and software to capture and analyze. Reference: 1: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-multi- factor-authentication

QUESTION 173
A firewall administrator is investigating high packet buffer utilization in the company firewall. After looking at the threat logs and seeing many flood attacks coming from a single source that are dropped a by the firewall, the administrator decides to enable packet butter protection to protect against similar attacks.
The administrator enables packet buffer protection globally in the firewall but still sees a high packet buffer utilization rate.
What else should the administrator do to stop packet buffers from being overflowed?

A. Add the default Vulnerability Protection profile to all security rules that allow traffic from outside.

B. Enable packet buffer protection for the affected zones.

C. Add a Zone Protection profile to the affected zones.

D. Apply DOS profile to security rules allow traffic from outside.

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dosprotection/zone-defense/packet-buffer-protection

QUESTION 174
Which CLI command displays the physical media that are connected to ethernet1/8?

A. > show system state filter-pretty sys.si.p8.stats

B. > show system state filter-pretty sys.sl.p8.phy

C. > show interface ethernet1/8

D. > show system state filter-pretty sys.sl.p8.med

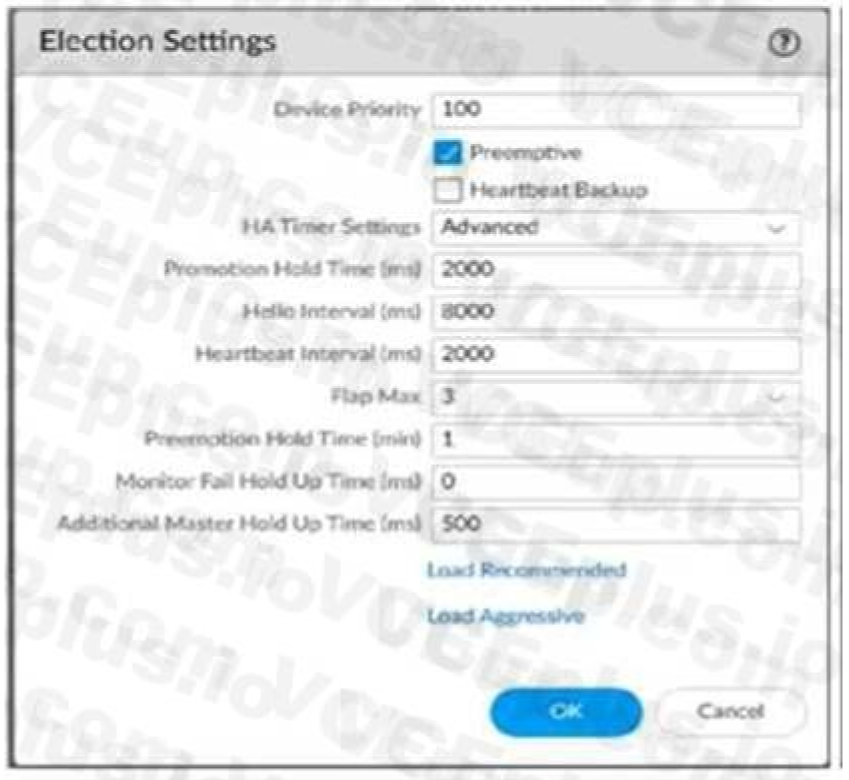
Correct Answer: B
Section:

Explanation:
Example output:

```
> show system state filter-pretty sys.s1.p1.phy
sys.s1.p1.phy: {
link-partner: { },
media: CAT5,
type: Ethernet,
}
```

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC

QUESTION 175



Election Settings

Device Priority 100
☑ Preemptive
□ Heartbeat Backup
HA Timer Settings Advanced
Promotion Hold Time (ms) 2000
Hello Interval (ms) 8000
Heartbeat Interval (ms) 2000
Flap Max 3
Preemption Hold Time (min) 1
Monitor Fail Hold Up Time (ms) 0
Additional Master Hold Up Time (ms) 500

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

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/ha- timers

QUESTION 176
An engineer must configure the Decryption Broker feature. To which router must the engineer assign the decryption forwarding interfaces that are used in Decryption Broker security chain?

A. A virtual router that has no additional interfaces for passing data-type traffic and no other configured routes than those used for the security chain.
B. The default virtual router. If there is no default virtual router , the engineer must create one during setup.
C. A virtual router that is configured with at least one dynamic routing protocol and has at least one entry in the RIB

D. The virtual router that routes the traffic that the Decryption Broker security chain inspects.

Correct Answer: D
Section:
Explanation:
Decryption Broker is a feature that allows you to use a Palo Alto Networks firewall as a decryption broker for other security devices in your network1. It works by decrypting traffic on one interface and forwarding it to another interface where it can be inspected by other devices before being reencrypted and sent to its destination2. The firewall acts as a transparent bridge between the two interfaces and does not change the source or destination IP addresses of the traffic2.
To configure Decryption Broker, you need to assign decryption forwarding interfaces (DFIs) to the virtual router that routes the traffic that you want to inspect. The DFIs are used to forward decrypted traffic from one interface to another in a security chain3. A security chain is a set of devices that perform different security functions on the same traffic flow3. You can have multiple security chains for different types of traffic or different segments of your network3.
The reason why you need to assign DFIs to the virtual router that routes the traffic is because Decryption Broker uses routing tables to determine which DFI belongs to which security chain and how to forward traffic between them2. If you assign DFIs to a different virtual router than the one that routes the traffic, Decryption Broker will not be able to find them or forward traffic correctly2.

QUESTION 177
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. Powershell scripts
D. VBscripts
E. APK

Correct Answer: A, B, C
Section:

QUESTION 178
A network security administrator wants to enable Packet-Based Attack Protection in a Zone Protection profile.
What are two valid ways to enable Packet-Based Attack Protection? (Choose two.)

A. ICMP Drop
B. TCP Drop
C. TCP Port Scan Block
D. SYN Random Early Drop

Correct Answer: B, D
Section:
Explanation:
Packet-Based Attack Protection is a feature of Zone Protection Profiles that allows the firewall to drop packets that are malformed, spoofed, or part of a port scan. TCP Drop and SYN Random Early Drop are two options under Packet-Based
Attack Protection that can be enabled to protect against TCPbased attacks. TCP Drop enables the firewall to check for spoofed IP addresses, mismatched overlapping TCP segments, and invalid IP options. SYN Random Early Drop enables the firewall to drop SYN packets randomly when the SYN queue is full, preventing SYN flood attacks. ICMP Drop and TCP Port Scan Block are not valid options under Packet-Based Attack Protection

QUESTION 179
Where can a service route be configured for a specific destination IP?

A. Use Network > Virtual Routers, select the Virtual Router > Static Routes > IPv4

B. Use Device > Setup > Services > Services
C. Use Device > Setup > Services > Service Route Configuration > Customize > Destination
D. Use Device > Setup > Services > Service Route Configuration > Customize > IPv4

Correct Answer: C
Section:
Explanation:
A service route is the path from the interface to the service on a server. By default, the firewall uses the management interface to communicate to various servers, including DNS, Email, Palo Alto
Updates, User-ID agent, Syslog, Panorama, dynamic updates, URL updates, licenses, and AutoFocus.
etc. Sometimes, it is necessary to use an alternative path other than Firewall management IP due to many restrictions. To configure service routes for non-predefined services, the destination addresses can be manually entered in the Destination section under Device > Setup > Services > Service Route Configuration > Customize1. Option A is incorrect because it is used to configure static routes for network traffic, not service routes for firewall services. Option B is incorrect because it is used to configure general service settings such as NTP server and proxy server, not service routes for specific destinations. Option D is incorrect because it is used to configure service routes for predefined services such as DNS and Syslog, not service routes for non-predefined services2.

QUESTION 180
Which feature of Panorama allows an administrator to create a single network configuration that can be reused repeatedly for large-scale deployments even if values of configured objects, such as routes and interface addresses, change?

A. Template stacks
B. Template variables
C. The Shared device group
D. A device group

Correct Answer: B
Section:
Explanation:
Template variables are placeholders that you can use in a template or a template stack to represent values that differ across firewalls, such as IP addresses, hostnames, or interface names. Template variables allow you to create a single network configuration that can be reused repeatedly for largescale deployments even if values of configured objects change1. Option A is incorrect because template stacks are used to group multiple templates together and apply them to firewalls or device groups. Template stacks do not allow you to use variables for different values2. Option C is incorrect because the Shared device group is used to push policies and objects that are common across all firewalls managed by Panoram a. The Shared device group does not allow you to use variables for different values3. Option D is incorrect because a device group is used to group firewalls that require similar policies and objects. A device group does not allow you to use variables for different values3.

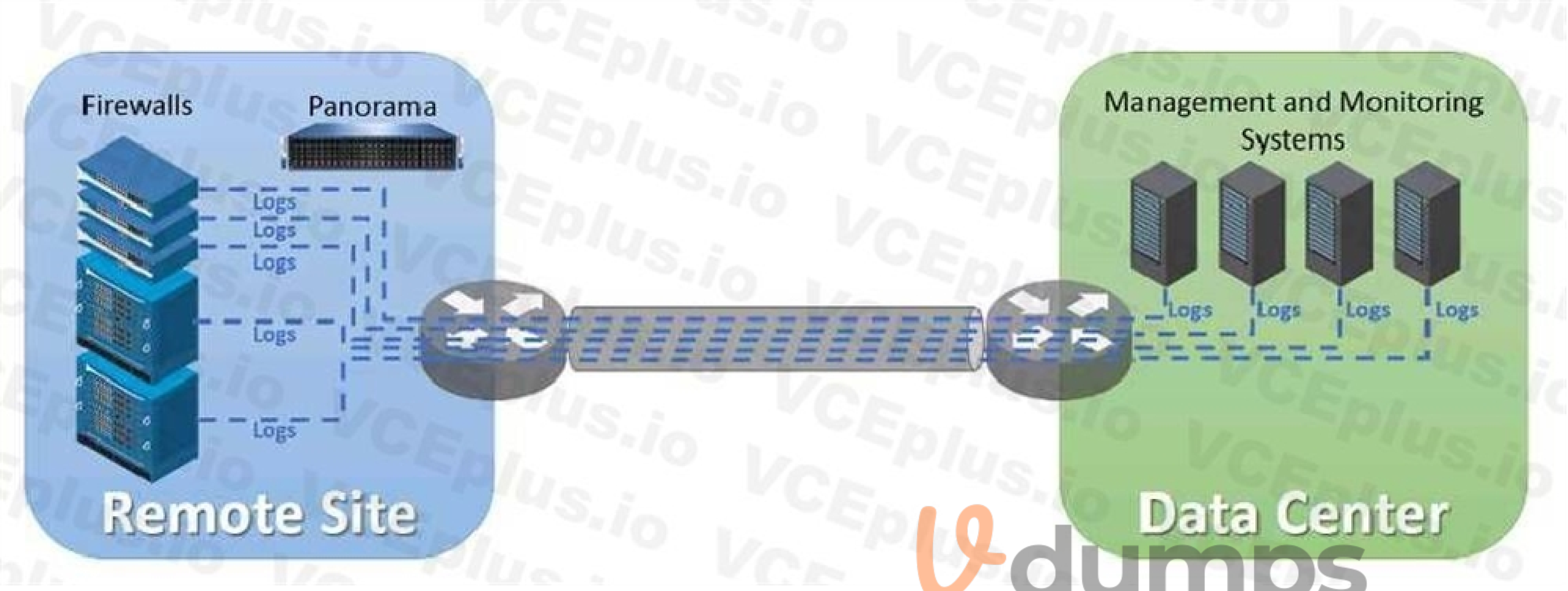
QUESTION 181
A firewall administrator wants to have visibility on one segment of the company network. The traffic on the segment is routed on the Backbone switch. The administrator is planning to apply Security rules on segment X after getting the visibility.
There is already a PAN-OS firewall used in L3 mode as an internet gateway, and there are enough system resources to get extra traffic on the firewall. The administrator needs to complete this operation with minimum service interruptions and without making any IP changes.
What is the best option for the administrator to take?

A. Configure the TAP interface for segment X on the firewall.
B. Configure vwire interfaces for segment X on the firewall.
C. Configure a Layer 3 interface for segment X on the firewall.
D. Configure a new vsys for segment X on the firewall.

Correct Answer: A
Section:
Explanation:
A TAP interface is a dedicated interface on the firewall that can be connected to a switch SPAN or mirror port to passively monitor traffic flows across a network. A TAP interface provides application visibility and threat

detection without being in the flow of network traffic. A TAP interface does not require any IP changes or service interruptions on the network segment1. Option B is incorrect because vwire interfaces are used to create virtual wires that transparently connect two network segments. Vwire interfaces require physical cabling changes and may cause service interruptions on the network segment2. Option C is incorrect because a Layer 3 interface is used to route traffic between different subnets. A Layer 3 interface requires IP changes and may cause service interruptions on the network segment2. Option D is incorrect because a new vsys is used to create a virtual system that can have its own set of policies and objects. A new vsys does not provide visibility or security for a specific network segment3.

QUESTION 182
Refer to the exhibit.



An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.
How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?

A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services
B. Configure log compression and optimization features on all remote firewalls
C. Any configuration on an M-500 would address the insufficient bandwidth concerns
D. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW

Correct Answer: A
Section:
Explanation:
Forwarding logs from firewalls only to Panorama and having Panorama forward logs to other external services is the best option for the administrator to reduce WAN traffic while maintaining support for all the existing monitoring/security platforms. This option minimizes the number of log forwarding destinations on each firewall and consolidates log forwarding on Panoram a. Panorama can forward logs to external destinations such as syslog servers, email servers, SNMP trap receivers, HTTP servers, or AutoFocus1. Option B is incorrect because configuring log compression and optimization features on all remote firewalls may reduce the size of log files but does not reduce the number of log forwarding destinations. Option C is incorrect because any configuration on an M-500 would not address the insufficient bandwidth concerns. An M-500 is a dedicated log collector that can store logs from multiple firewalls and Panorama appliances. However, it does not reduce the WAN traffic generated by log forwarding2. Option D is incorrect because forwarding logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW does not reduce WAN traffic while maintaining support for all the existing monitoring/security platforms. This option would increase the WAN traffic by sending logs back and forth between Panorama and the NGFW1.

QUESTION 183
An ISP manages a Palo Alto Networks firewall with multiple virtual systems for its tenants.
Where on this firewall can the ISP configure unique service routes for different tenants?

A. Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Inherit Global Service Route Configuration
B. Setup > Services > Global > Service Route Configuration > Customize
C. Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Customize
D. Setup > Services > Global > Service Route Configuration > Use Management Interface for all

Correct Answer: C
Section:
Explanation:
The best option for the ISP to configure unique service routes for different tenants is to use the Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Customize option on the firewall. This option allows the ISP to customize the service routes for each virtual system that represents a tenant. A service route is the path from the interface to the service on a server, such as DNS, email, or Panorama. By customizing the service routes for each virtual system, the ISP can ensure that each tenant uses a different interface or IP address to access these services1. Option A is incorrect because it is used to inherit the global service route configuration for a virtual system, not to customize it.
Option B is incorrect because it is used to customize the global service route configuration for all virtual systems, not for a specific one. Option D is incorrect because it is used to use the management interface for all service routes, not to customize them1.

QUESTION 184
In the New App Viewer under Policy Optimizer, what does the compare option for a specific rule allow an administrator to compare?

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

Correct Answer: C
Section:
Explanation:
The compare option for a specific rule in the New App Viewer under Policy Optimizer allows an administrator to compare the applications configured in the rule with the applications seen from traffic matching the same rule. This option helps the administrator to identify any discrepancies between the intended and actual applications allowed by the rule. The administrator can then optimize the rule by adding or removing applications as needed1. Option A is incorrect because the compare option does not compare the running configuration with the candidate configuration of the firewall. That is done by using the Commit > Commit and Push option2. Option B is incorrect because the compare option does not compare applications configured in the rule with their dependencies. That is done by using the App Dependencies tab under Policy Optimizer1. Option D is incorrect because the compare option does not compare the security rule with any other security rule selected. That is done by using the Compare Rules option under Policies > Security3.

QUESTION 185
A company has recently migrated their branch office's PA-220S to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices All device group and template configuration is managed solely within Panorama
They notice that commit times have drastically increased for the PA-220S after the migration
What can they do to reduce commit times?

A. Disable "Share Unused Address and Service Objects with Devices" in Panorama Settings.
B. Update the apps and threat version using device-deployment
C. Perform a device group push using the "merge with device candidate config" option
D. Use "export or push device config bundle" to ensure that the firewall is integrated with the Panorama config.

Correct Answer: A
Section:
Explanation:
According to the Palo Alto Networks documentation1, disabling "Share Unused Address and Service Objects with Devices" in Panorama Settings is a possible solution to reduce commit times for firewalls managed by

Panorama. This option prevents Panorama from pushing address and service objects that are not used in any policy rules to the firewalls, which can reduce the size of the configuration and improve the commit performance. Therefore, the correct answer is A.
The other options are not relevant or effective for reducing commit times:
Update the apps and threat version using device-deployment: This option would not help because it is not related to the commit process. Updating the apps and threat version using device-deployment is a feature that allows Panorama to distribute content updates to firewalls without requiring a commit2.
Perform a device group push using the "merge with device candidate config" option: This option would not help because it is not related to the commit performance. Performing a device group push using the "merge with device candidate config" option is a feature that allows Panorama to merge the local changes on a firewall with the Panorama configuration without overwriting them3.
Use "export or push device config bundle" to ensure that the firewall is integrated with the Panorama config: This option would not help because it is not related to the commit performance. Using "export or push device config bundle" is a feature that allows Panorama to export or push a complete configuration bundle to a firewall, which can be useful for troubleshooting or migrating configurations4.
Reference: 1:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleLCAS 2: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/managefirewalls/manage-content-updates-on-managed-firewalls/update-the-apps-and-threats-versionusing-device-deployment 3:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewalladministration/manage-firewalls/manage-firewall-configurations/perform-a-device-group-pushusing-the-merge-with-device-candidate-config-option 4:
https://docs.paloaltonetworks.com/panos/9-1/pan-os-admin/firewall-administration/manage-firewalls/manage-firewall-configurations/useexport-or-push-device-config-bundle-to-ensure-that-the-firewall-is-integrated-with-the-panoramaconfig

QUESTION 186
In a template, which two objects can be configured? (Choose two.)

A. SD-WAN path quality profile
B. Monitor profile
C. IPsec tunnel
D. Application group

Correct Answer: A
Section:
Explanation:

According to the Palo Alto Networks documentation1, a template is a set of configuration settings that you can apply to firewalls or Panorama managed collectors. A template can contain settings for network and device configuration, such as interfaces, zones, virtual routers, DNS, NTP, logging, and more. Therefore, the correct answer is A and B.
The other options are not objects that can be configured in a template:
IPsec tunnel: This option is not an object that can be configured in a template. IPsec tunnel is a feature that allows establishing secure VPN connections between firewalls or other devices. IPsec tunnel configuration is part of the policy configuration, not the network or device configuration2.
Application group: This option is not an object that can be configured in a template. Application group is an object that groups applications based on various criteria, such as category, subcategory, technology, or risk. Application group configuration is part of the object configuration, not the network or device configuration3.
Reference: 1: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/managefirewalls/manage-templates-and-template-stacks/manage-templates 2:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpn/site-to-site-vpn/set-up-a-site-tosite-vpn-between-two-firewalls 3:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-osadmin/app-id/manage-custom-or-unknown-applications/create-an-application-group

QUESTION 187
Phase two of a VPN will not establish a connection. The peer is using a policy-based VPN configuration. What part of the configuration should the engineer verify'?

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

Correct Answer: B
Section:
Explanation:
Proxy-ID is a parameter that identifies the traffic that needs to be encrypted and tunneled in an IPSec VPN. Proxy-ID consists of the local and remote IP addresses, protocols, and ports. Proxy-ID is used when the peer is using a

policy-based VPN configuration, which allows specifying the Proxy-ID settings manually. If the Proxy-ID settings do not match on both peers, the phase two of the VPN will not establish a connection. Therefore, the correct answer is B.

The other options are not parts of the configuration that the engineer should verify for phase two of a VPN:

PAN-OS versions: This option is not relevant for phase two of a VPN. PAN-OS versions are the software versions that run on Palo Alto Networks firewalls. They do not affect the VPN connection establishment, as long as they support the same VPN features and protocols2.

IKE Crypto Profile: This option is not relevant for phase two of a VPN. IKE Crypto Profile is a parameter that defines the encryption and authentication algorithms for IKE negotiation. IKE negotiation is part of phase one of the VPN, not phase two3.

Security policy: This option is not relevant for phase two of a VPN. Security policy is a rule that allows or denies traffic based on various criteria, such as source, destination, application, user, and service. Security policy does not affect the VPN connection establishment, but only the traffic that passes through the VPN tunnel4.

Reference: 1: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpn/site-to-sitevpn/set-up-a-site-to-site-vpn-between-two-firewalls/policy-based-vpn 2:
https://docs.paloaltonetworks.com/pan-os.html 3:
https://docs.paloaltonetworks.com/pan-os/91/pan-os-admin/vpn/site-to-site-vpn-concepts/internet-key-exchange-ike-for-vpn/methods-ofsecuring-ipsec-vpn-tunnels-ike-phase-2 4:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-osadmin/policy/security-policy.html

QUESTION 188

Which three external authentication services can the firewall use to authenticate admins into the Palo Alto Networks NGFW without creating administrator account on the firewall? (Choose three.)

A. RADIUS
B. TACACS+
C. Kerberos
D. LDAP
E. SAML

Correct Answer: A, B, E
Section:
Explanation:

According to the Palo Alto Networks documentation1, the firewall can use three external authentication services to authenticate admins into the Palo Alto Networks NGFW without creating administrator accounts on the firewall: RADIUS, TACACS+, and SAML. These services allow the firewall to verify the credentials of admins against an external server and grant them access based on their assigned roles and permissions. Therefore, the correct answer is A, B, and E.

The other options are not external authentication services that the firewall can use to authenticate admins:

Kerberos: This option is not an external authentication service that the firewall can use to authenticate admins. Kerberos is a protocol that allows users to access network resources using a single sign-on mechanism. The firewall can use

Kerberos to authenticate users for GlobalProtect VPN or Captive Portal, but not for admin access2.

LDAP: This option is not an external authentication service that the firewall can use to authenticate admins. LDAP is a protocol that allows querying and modifying directory services over a network. The firewall can use LDAP to retrieve user and group information from an external server, but not to authenticate admins3.

Reference: 1: https://docs.paloaltonetworks.com/pan-os/9-1/pan-osadmin/authentication/authentication-types/external-authentication-services 2:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authenticationtypes/kerberos-authentication 3:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-osadmin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-users-using-an-ldap-server

QUESTION 189

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

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

Correct Answer: A
Section:

Explanation:
According to the best practices for content updates for security-first networks, the recommended threshold value for apps and threats to be dynamically updated is 1 to 4 hours. This ensures that the network is protected against the latest threats and exploits as soon as possible. Reference: 1 Best Practices for Content UpdatesóSecurity-First - Palo Alto Networks https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/software-and-content-updates/bestpractices-for-app-and-threat-content-updates/best-practices-security-first

QUESTION 190
Which DoS Protection Profile detects and prevents session exhaustion attacks against specific destinations?

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

Correct Answer: A
Section:
Explanation:
According to the documentation, resource protection detects and prevents session exhaustion attacks against specific destinations. This type of attack uses a large number of hosts to establish as many fully established sessions as possible to consume all of a system's resources. Resource protection defines the maximum number of concurrent connections for a destination IP address or zone. Reference: 1 Security Profile: DoS Protection Profile - Palo Alto Networks
https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/securityprofile-dos-protection-profile

QUESTION 191
Why would a traffic log list an application as "not-applicable"?

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

Correct Answer: A
Section:
Explanation:
According to the documentation, not-applicable means that the Palo Alto device has received data that will be discarded because the port or service that the traffic is coming in on is not allowed, or there is no rule or policy allowing that port or service. This occurs because the traffic was dropped or denied before the application match could be performed. Reference: 1 Not-applicable in Traffic Logs Palo Alto Networks 2 Not-Applicable, Incomplete, Insufficient Data in the Application Field - Palo Alto Networks
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClspCAC

QUESTION 192
A network administrator configured a site-to-site VPN tunnel where the peer device will act as initiator None of the peer addresses are known
What can the administrator configure to establish the VPN connection?

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

Correct Answer: B
Section:

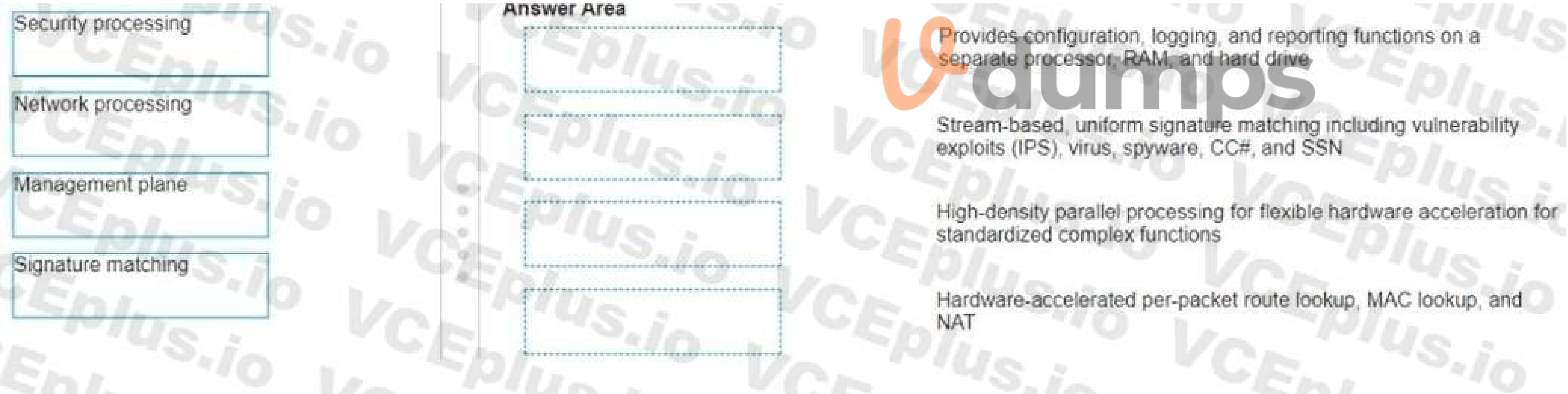
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClIGCA0

QUESTION 193
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

Correct Answer: A, B, E
Section:
Explanation:
"The WildFire inline ML option present in the Antivirus profile enables the firewall dataplane to apply machine learning on PE (portable executable), ELF (executable and linked format) and MS Office files, and PowerShell and shell scripts in real-time." from https://docs.paloaltonetworks.com/pan-os/102/pan-os-admin/threat-prevention/wildfire-inline-ml

QUESTION 194
DRAG DROP
Match the terms to their corresponding definitions
Select and Place:



Security processing

Network processing

Management plane

Signature matching

Answer Area

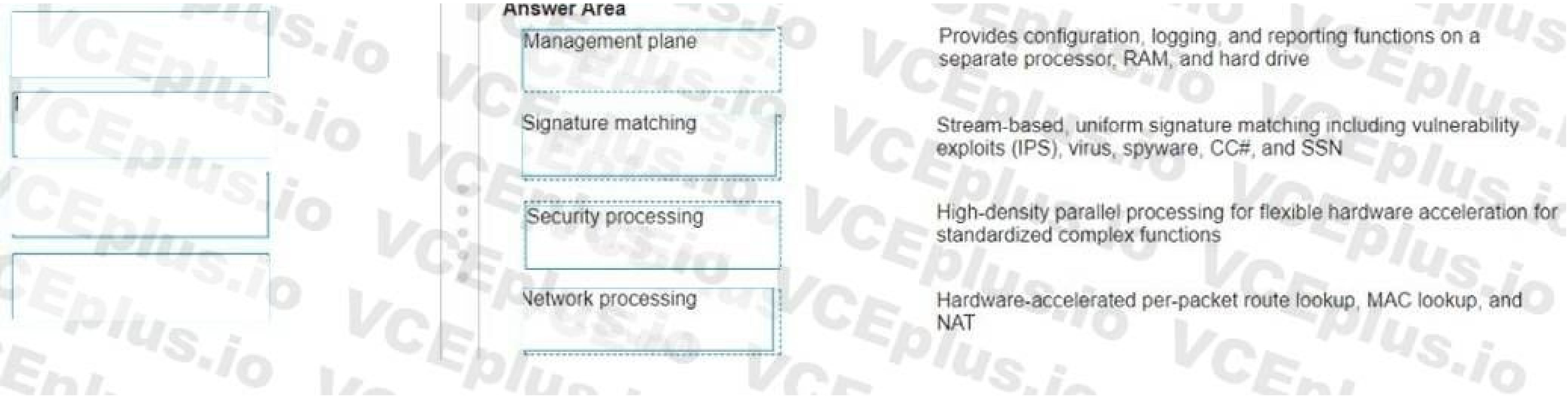
Provides configuration, logging, and reporting functions on a separate processor, RAM, and hard drive

Stream-based, uniform signature matching including vulnerability exploits (IPS), virus, spyware, CC#, and SSN

High-density parallel processing for flexible hardware acceleration for standardized complex functions

Hardware-accelerated per-packet route lookup, MAC lookup, and NAT

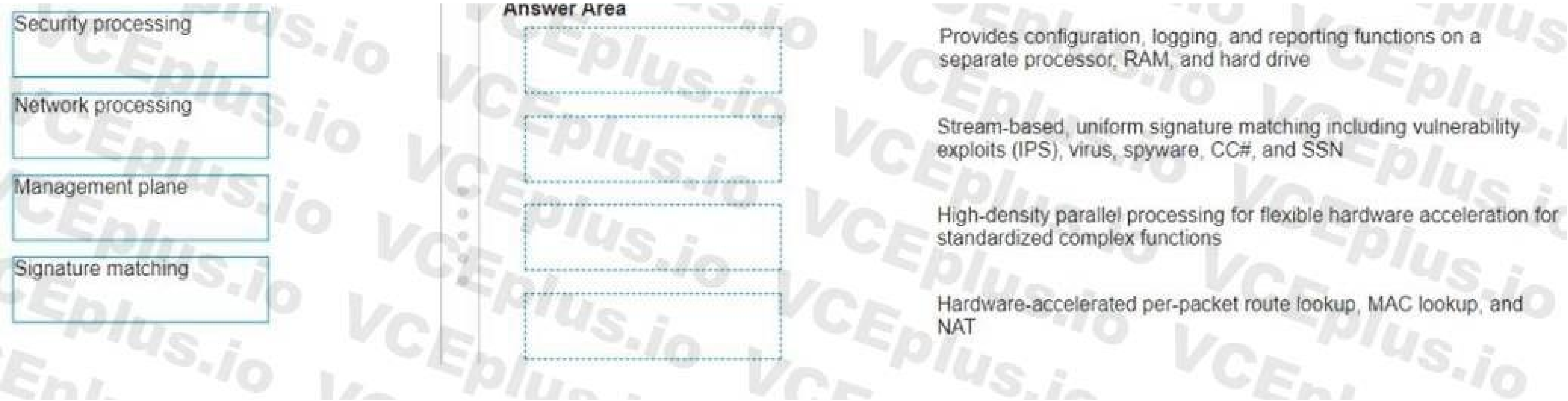
Answer:



Answer Area

Management plane	Provides configuration, logging, and reporting functions on a separate processor, RAM, and hard drive
Signature matching	Stream-based, uniform signature matching including vulnerability exploits (IPS), virus, spyware, CC#, and SSN
Security processing	High-density parallel processing for flexible hardware acceleration for standardized complex functions
Network processing	Hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Select and Place:



Security processing

Network processing

Management plane

Signature matching

Answer Area

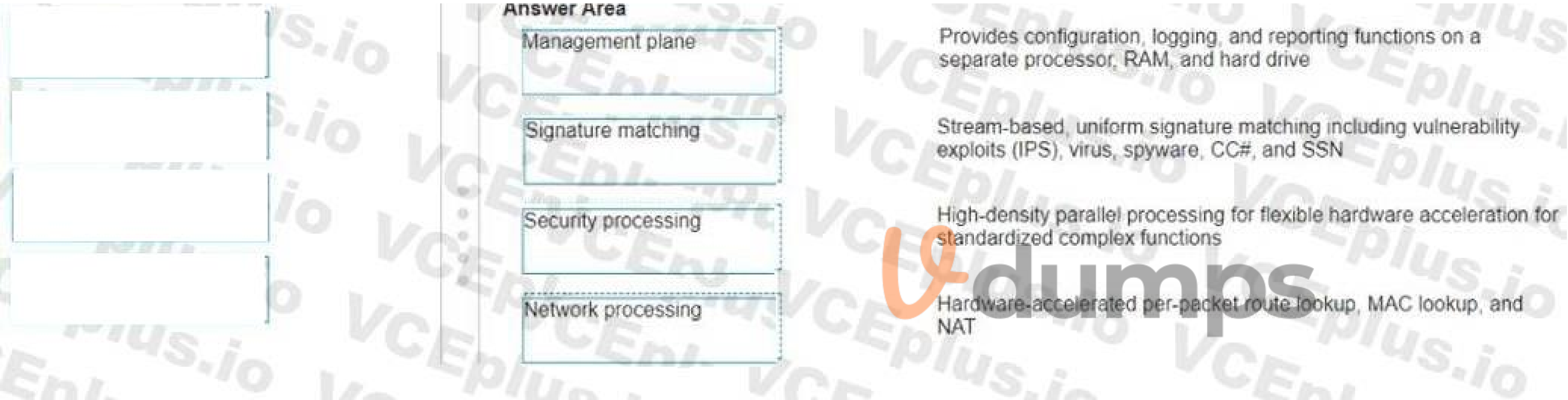
Provides configuration, logging, and reporting functions on a separate processor, RAM, and hard drive

Stream-based, uniform signature matching including vulnerability exploits (IPS), virus, spyware, CC#, and SSN

High-density parallel processing for flexible hardware acceleration for standardized complex functions

Hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Correct Answer:



Answer Area

Management plane	Provides configuration, logging, and reporting functions on a separate processor, RAM, and hard drive
Signature matching	Stream-based, uniform signature matching including vulnerability exploits (IPS), virus, spyware, CC#, and SSN
Security processing	High-density parallel processing for flexible hardware acceleration for standardized complex functions
Network processing	Hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Section:
Explanation:

QUESTION 195
Which protocol is supported by GlobalProtect Clientless VPN?

A. FTP
B. RDP
C. SSH
D. HTTPS

Correct Answer: D
Section:

QUESTION 196
What are three tasks that cannot be configured from Panorama by using a template stack? (Choose three.)

A. Change the firewall management IP address
B. Configure a device block list

C. Add administrator accounts

D. Rename a vsys on a multi-vsys firewall

E. Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode

Correct Answer: A, C, E
Section:
Explanation:
Change the firewall management IP address C. Add administrator accounts E.Enable operational modes such as normal mode, multi-vsys mode, or FIPS-CC mode Short Explanation of Correct Answer Only: These tasks cannot be configured from Panorama by using a template stack because they are device-specific settings that must be configured locally on each firewall1.A template stack can only configure settings that are common to multiple firewalls2.
Reference:1: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks2: https://docs.paloaltonetworks.com/best-practices/10-1/best-practices-for-managing-firewalls-with-panorama/configuration-management/template-and-template-stack-management

QUESTION 197
An engineer must configure a new SSL decryption deployment.
Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

A. There must be a certificate with both the Forward Trust option and Forward Untrust option selected.

B. A Decryption profile must be attached to the Security policy that the traffic matches.

C. A Decryption profile must be attached to the Decryption policy that the traffic matches.

D. There must be a certificate with only the Forward Trust option selected.

Correct Answer: C
Section:
Explanation:

QUESTION 198
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-3400Series

D. PA-220

E. PA-800 Series

Correct Answer: C, D, E
Section:

QUESTION 199
An engineer manages a high availability network and requires fast failover of the routing protocols. The engineer decides to implement BFD.
Which three dynamic routing protocols support BFD? (Choose three.)

A. OSPF

B. RIP

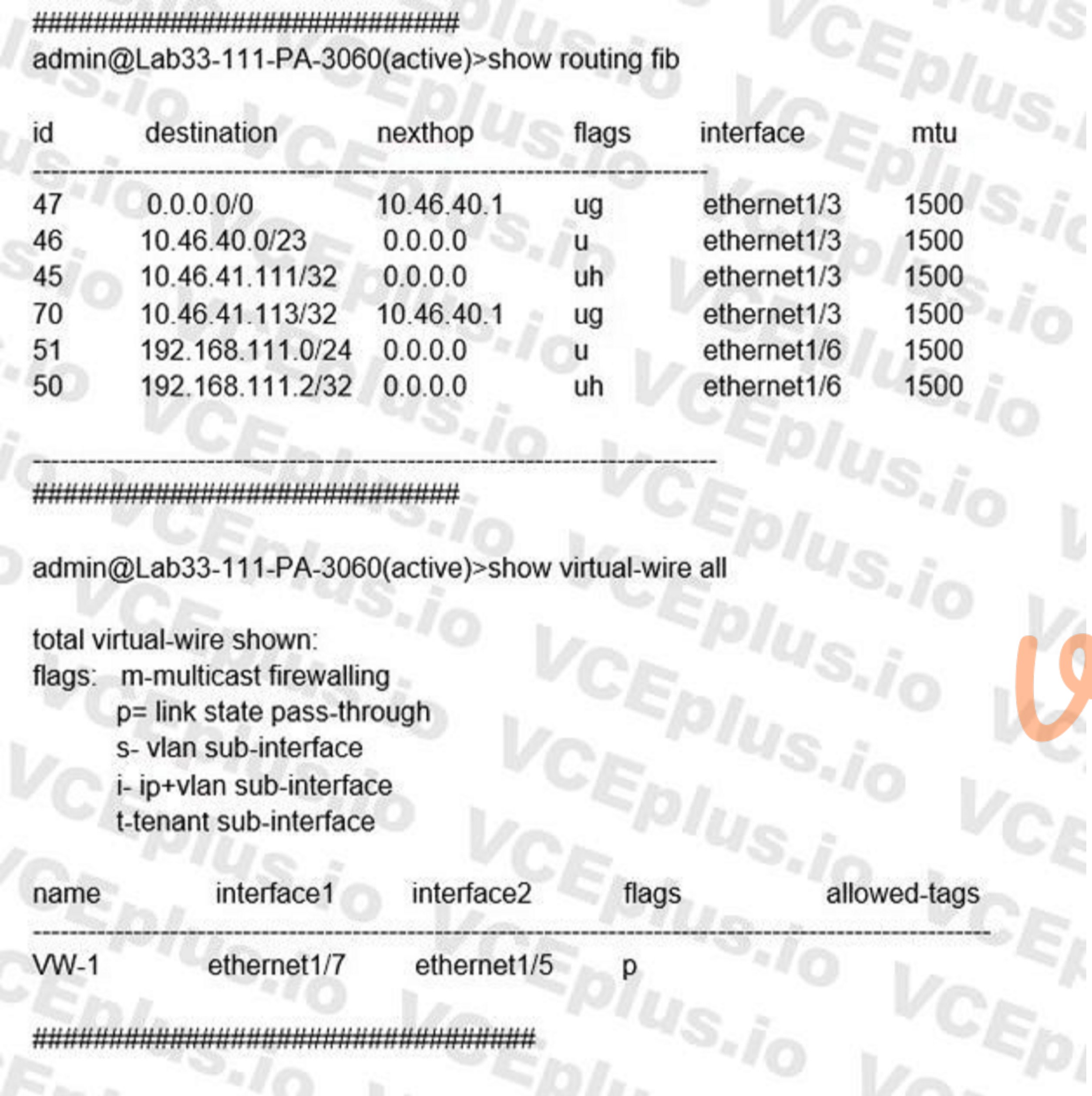
C. BGP

D. IGRP

E. OSPFv3 virtual link

Correct Answer: A, B, C
Section:

QUESTION 200
Refer to the exhibit.



```
################################
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination      nexthop     flags    interface     mtu
---------------------------------------------------------------
47      0.0.0.0/0        10.46.40.1  ug       ethernet1/3   1500
46      10.46.40.0/23    0.0.0.0     u        ethernet1/3   1500
45      10.46.41.111/32  0.0.0.0     uh       ethernet1/3   1500
70      10.46.41.113/32  10.46.40.1  ug       ethernet1/3   1500
51      192.168.111.0/24 0.0.0.0     u        ethernet1/6   1500
50      192.168.111.2/32 0.0.0.0     uh       ethernet1/6   1500

---------------------------------------------------------------
################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:  m-multicast firewalling
        p= link state pass-through
        s- vlan sub-interface
        i- ip+vlan sub-interface
        t-tenant sub-interface

name        interface1     interface2     flags          allowed-tags
-----------------------------------------------------------------------
VW-1        ethernet1/7    ethernet1/5    p

######################################
```

Which will be the egress interface if the traffic's ingress interface is ethernet1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

A. ethernet1/6

B. ethernet1/3

C. ethernet1/7

D. ethernet1/5

Correct Answer: D
Section:

QUESTION 201
An engineer is configuring a template in Panorama which will contain settings that need to be applied to all firewalls in production.
Which three parts of a template an engineer can configure? (Choose three.)

A. NTP Server Address
B. Antivirus Profile
C. Authentication Profile
D. Service Route Configuration
E. Dynamic Address Groups

Correct Answer: A, C, D
Section:
Explanation:
NTP Server Address D.Service Route Configuration Short Explanation of Correct Answer Only: These parts of a template can be configured on Panorama1.An antivirus profile and an authentication profile are not parts of a template, but parts of a device group2. Reference:1: https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/templates-and-template-stacks-overview2: https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-device-groups/device-group-overview

QUESTION 202
A security engineer needs firewall management access on a trusted interface.
Which three settings are required on an SSL/TLS Service Profile to provide secure Web UI authentication? (Choose three.)

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

Correct Answer: A, B, D
Section:

QUESTION 203
An administrator notices that an interface configuration has been overridden locally on a firewall. They require all configuration to be managed from Panorama and overrides are not allowed.
What is one way the administrator can meet this requirement?

A. Perform a commit force from the CLI of the firewall.
B. Perform a template commit push from Panorama using the 'Force Template Values' option.
C. Perform a device-group commit push from Panorama using the 'Include Device and Network Templates' option.
D. Reload the running configuration and perform a Firewall local commit

Correct Answer: B
Section:
Explanation:
This option will overwrite any local configuration on the firewall with the template configuration from Panorama1.Performing a commit force from the CLI of the firewall will not remove the local override2.Performing a device-group commit push from Panorama using the "Include Device and Network Templates" option will not remove the local override3.Reloading the running configuration and performing a Firewall local commit will not remove the local override. Reference:1: https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/force-template-values2: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/use-the-cli/commit-changes3: https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-device-groups/push-policy-and-configuration-to-firewalls : https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/manage-firewall-configurations/revert-to-a-previous-configuration

QUESTION 204
A firewall engineer reviews the PAN-OS GlobalProtect application and sees that it implicitly uses web-browsing and depends on SSL.
When creating a new rule, what is needed to allow the application to resolve dependencies?

A. Add SSL and web-browsing applications to the same rule.

B. Add web-browsing application to the same rule.

C. Add SSL application to the same rule.

D. SSL and web-browsing must both be explicitly allowed

Correct Answer: C
Section:

QUESTION 205

An administrator has configured OSPF with Advanced Routing enabled on a Palo Alto Networks firewall running PAN-OS 10.2. After OSPF was configured, the administrator noticed that OSPF routes were not being learned.
Which two actions could an administrator take to troubleshoot this issue? (Choose two.)

A. Run the CLI command show advanced-routing ospf neighbor

B. In the WebUI, view the Runtime Stats in the logical router.

C. In the WebUI, view the Runtime Stats in the virtual router.

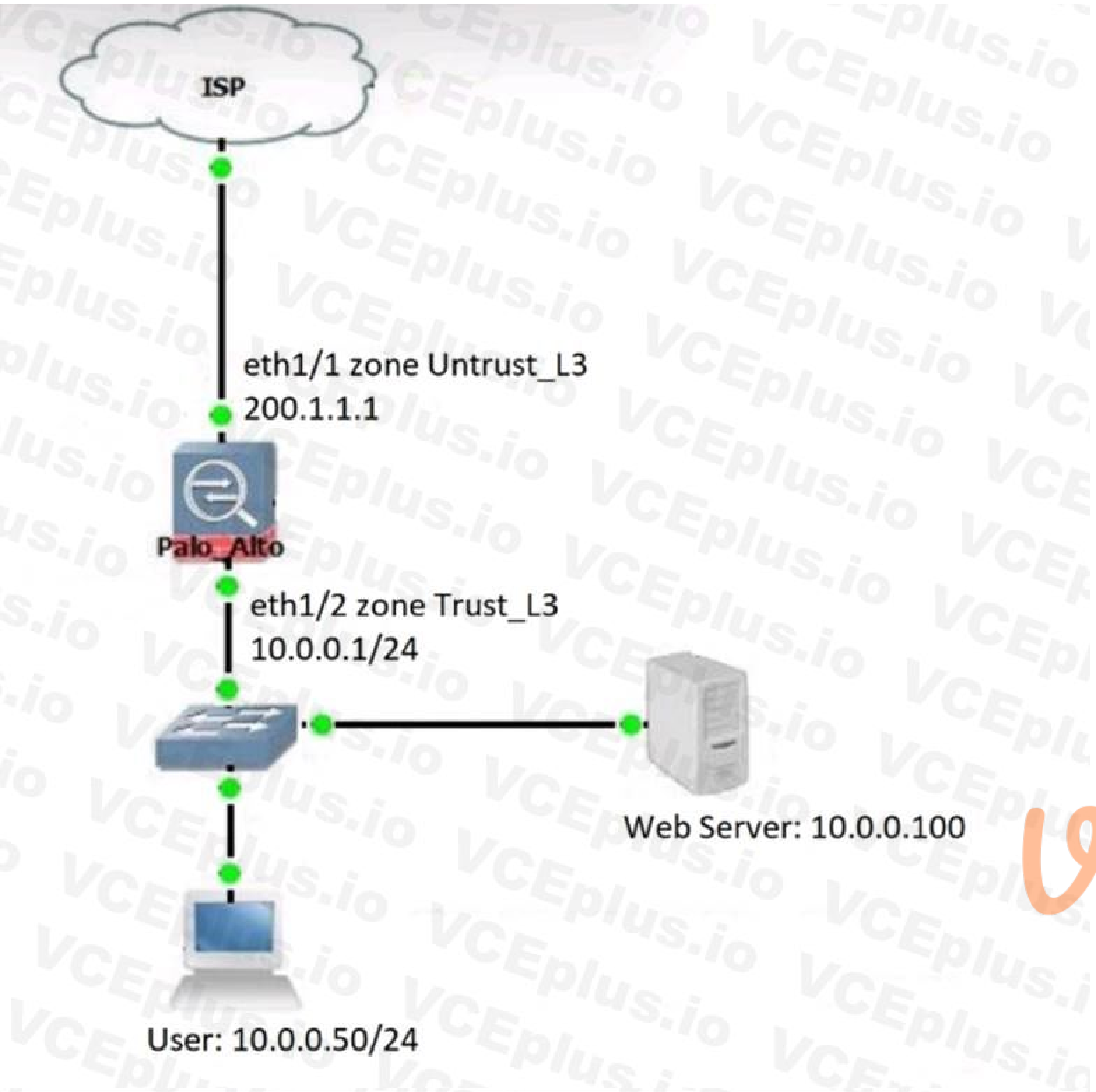
D. Look for configuration problems in Network > virtual router > OSPF

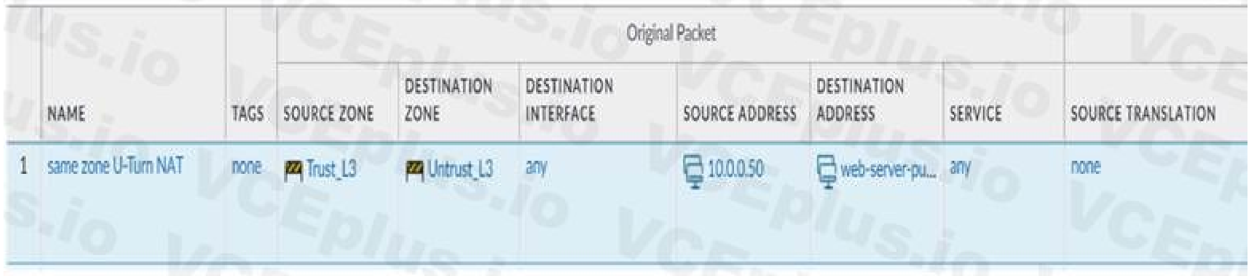
E.

Correct Answer: A, C
Section:

QUESTION 206

Review the information below. A firewall engineer creates a U-NAT rule to allow users in the trust zone access to a server in the same zone by using an external, public NAT IP for that server.
Given the rule below, what change should be made to make sure the NAT works as expected?





			Original Packet						
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION
1	same zone U-Turn NAT	none	Trust_L3	Untrust_L3	any	10.0.0.50	web-server-pu...	any	none

A. Change destination NAT zone to Trust_L3.

B. Change destination translation to Dynamic IP (with session distribution) using firewall ethl/2 address.

C. Change Source NAT zone to Untrust_L3.

D. Add source Translation to translate original source IP to the firewall eth1/2 interface translation.

Correct Answer: D
Section:

QUESTION 207

An administrator needs to identify which NAT policy is being used for internet traffic.
From the Monitor tab of the firewall GUI, how can the administrator identify which NAT policy is in use for a traffic flow?

A. Click Session Browser and review the session details.
B. Click Traffic view and review the information in the detailed log view.
C. Click Traffic view; ensure that the Source or Destination NAT columns are included and review the information in the detailed log view.
D. Click App Scope > Network Monitor and filter the report for NAT rules

Correct Answer: C
Section:

QUESTION 208
An administrator troubleshoots an issue that causes packet drops.
Which log type will help the engineer verify whether packet buffer protection was activated?

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

Correct Answer: B
Section:
Explanation:
The firewall records alert events in the System log and events for dropped traffic, discarded sessions, and blocked IP address in the Threat log when packet buffer protection is activated12.Packet buffer protection is a feature that helps prevent packet buffer exhaustion by identifying and dropping traffic from sources that consume excessive packet buffers3. Reference:3: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection1: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oNB7CAM&lang=en_US2: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

QUESTION 209
Which two policy components are required to block traffic in real time using a dynamic user group (DUG)? (Choose two.)

A. A Deny policy for the tagged traffic
B. An Allow policy for the initial traffic
C. A Decryption policy to decrypt the traffic and see the tag
D. A Deny policy with the 'tag' App-ID to block the tagged traffic

Correct Answer: A, B
Section:

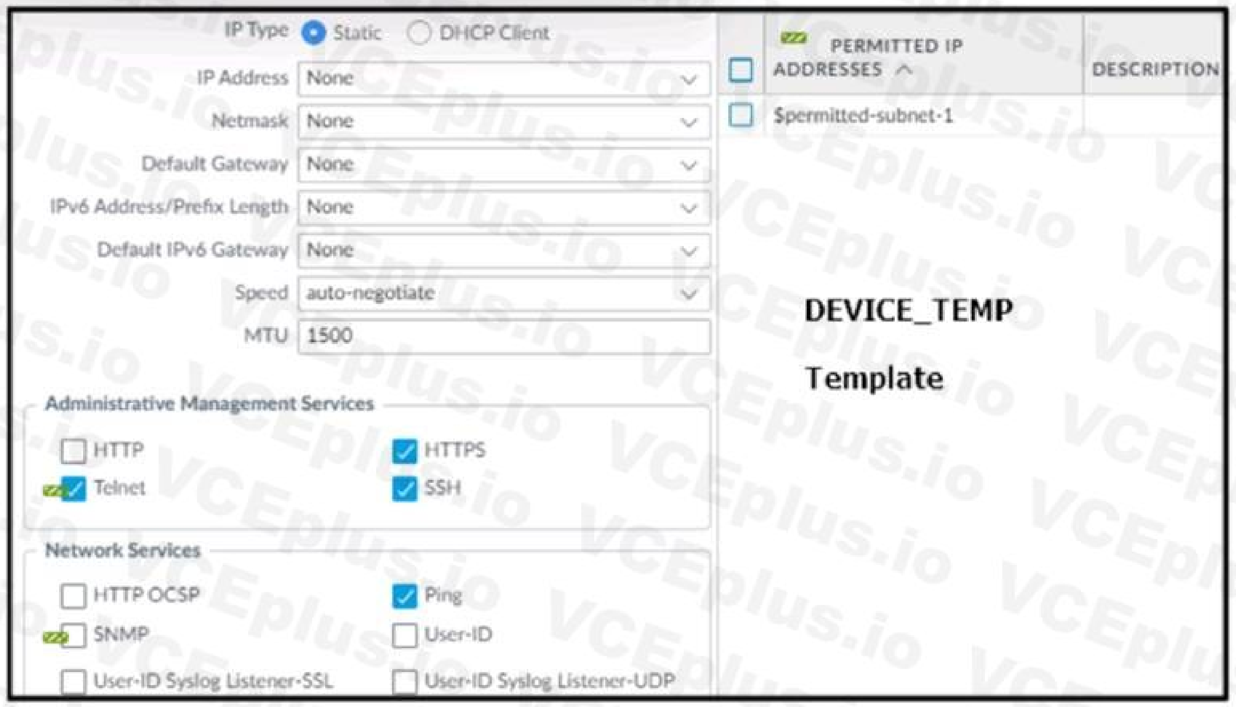
QUESTION 210
A network security administrator wants to inspect HTTPS traffic from users as it egresses through a firewall to the Internet/Untrust zone from trusted network zones.
The security admin wishes to ensure that if users are presented with invalid or untrusted security certificates, the user will see an untrusted certificate warning.
What is the best choice for an SSL Forward Untrust certificate?

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

Correct Answer: B
Section:

QUESTION 211

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



IP Type ● Static ○ DHCP Client

IP Address: None

Netmask: None

Default Gateway: None

IPv6 Address/Prefix Length: None

Default IPv6 Gateway: None

Speed: auto-negotiate

MTU: 1500

Administrative Management Services

□ HTTP ☑ HTTPS

☑ Telnet ☑ SSH

Network Services

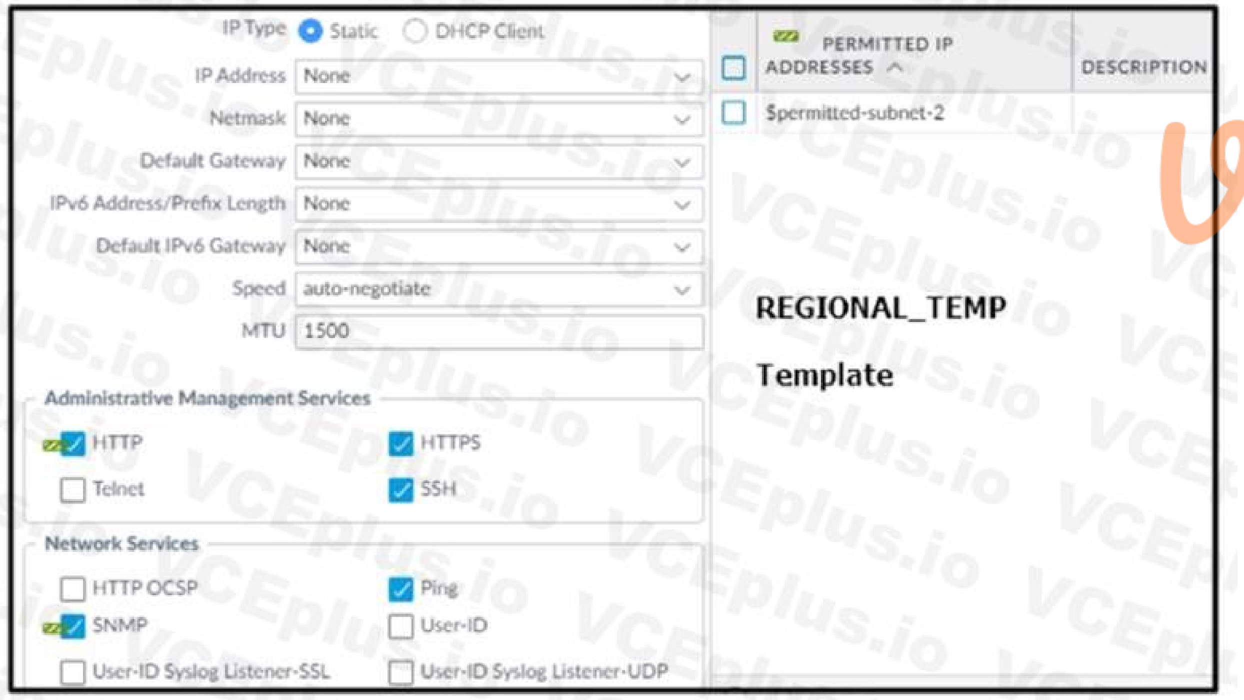
□ HTTP OCSP ☑ Ping

□ SNMP □ User-ID

□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	PERMITTED IP ADDRESSES	DESCRIPTION
□	$permitted-subnet-1	

DEVICE_TEMP Template



IP Type ● Static ○ DHCP Client

IP Address: None

Netmask: None

Default Gateway: None

IPv6 Address/Prefix Length: None

Default IPv6 Gateway: None

Speed: auto-negotiate

MTU: 1500

Administrative Management Services

☑ HTTP ☑ HTTPS

□ Telnet ☑ SSH

Network Services

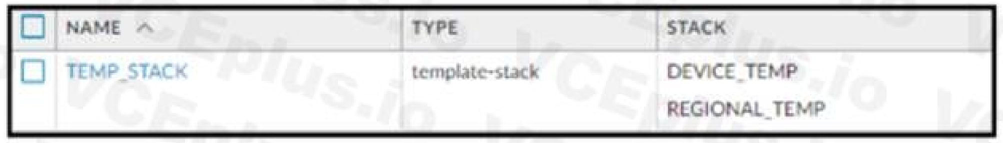
□ HTTP OCSP ☑ Ping

☑ SNMP □ User-ID

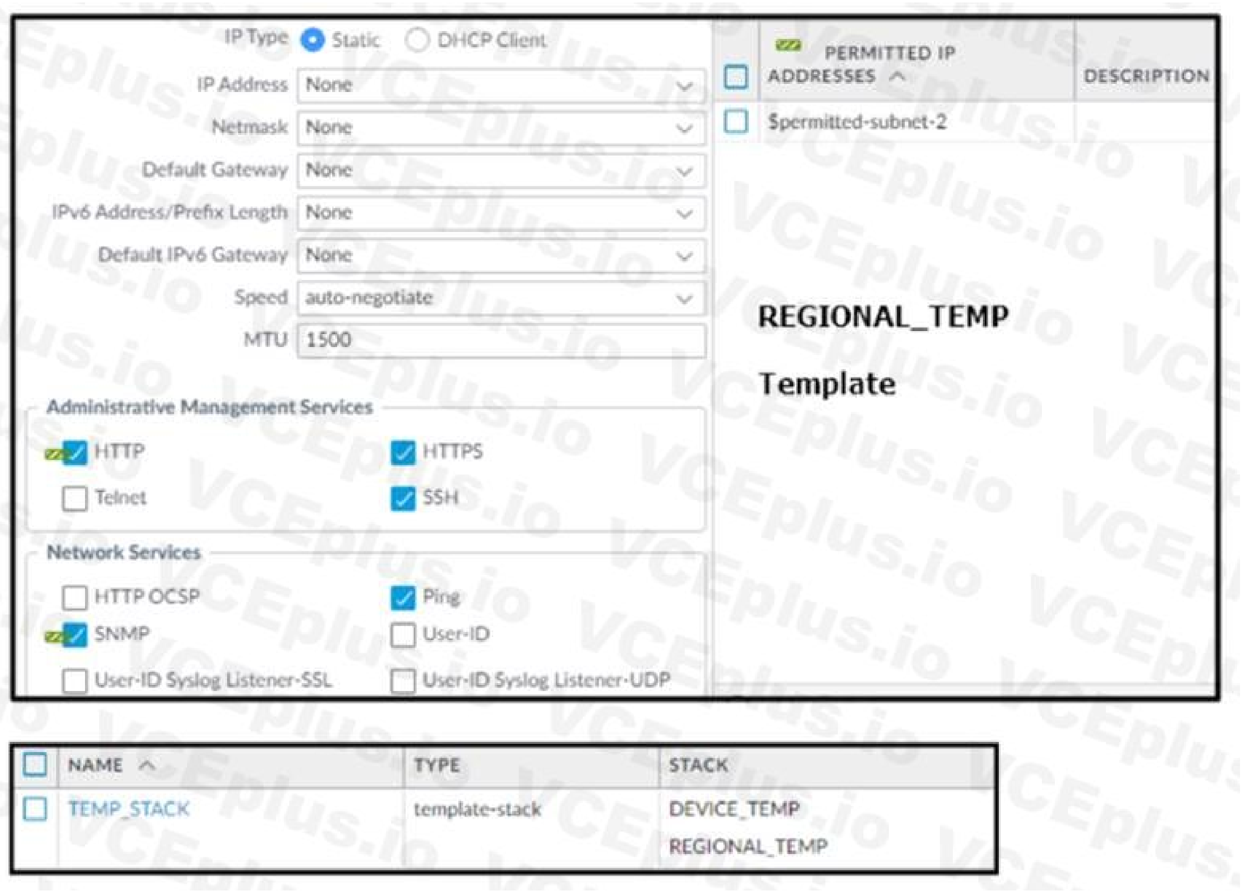
□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	PERMITTED IP ADDRESSES	DESCRIPTION
□	$permitted-subnet-2	

REGIONAL_TEMP Template



□	NAME	TYPE	STACK
□	TEMP_STACK	template-stack	DEVICE_TEMP REGIONAL_TEMP



IP Type ● Static ○ DHCP Client

IP Address None

Netmask None

Default Gateway None

IPv6 Address/Prefix Length None

Default IPv6 Gateway None

Speed auto-negotiate

MTU 1500

Administrative Management Services

☑ HTTP ☑ HTTPS

☐ Telnet ☑ SSH

Network Services

☐ HTTP OCSP ☑ Ping

☑ SNMP ☐ User-ID

☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

☐	PERMITTED IP ADDRESSES	DESCRIPTION
☐	$permitted-subnet-2	

REGIONAL_TEMP

Template

☐	NAME	TYPE	STACK
☐	TEMP_STACK	template-stack	DEVICE_TEMP REGIONAL_TEMP

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

B. The firewall will allow HTTP, Telnet, HTTPS, SSH, and Ping from IP addresses defined as $permitted-subnet-l and Spermitted-subnet-2.

C. The firewall will allow HTTP, Telnet, HTTPS, SSH, and Ping from IP addresses defined as $permitted-subnet-l.

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

Correct Answer: C
Section:

QUESTION 212

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

A. Set DNS and Palo Alto Networks Services to use the ethernet1/1 source interface.

B. Set DNS and Palo Alto Networks Services to use the ethernet1/2 source interface.

C. Set DNS and Palo Alto Networks Services to use the MGT source interface.

D. Set DDNS and Palo Alto Networks Services to use the MGT source interface

Correct Answer: A
Section:

QUESTION 213

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

Correct Answer: A
Section:
Explanation:
Make sure Panorama is running the same or a later PAN-OS version than you are upgrading to. You must upgrade Panorama and its Log Collectors to 10.2 before upgrading the managed firewalls to this version. In addition, when upgrading Log Collectors to 10.2, you must upgrade all Log Collectors at the same time due to changes in the logging infrastructure. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-firewalls-using- panorama

QUESTION 214
Which benefit do policy rule UUlDs provide?

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

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/enumeration-of-rules-within- a-rulebase To keep track of rules within a rulebase, you can refer to the rule number, which changes depending on the order of a rule in the rulebase. The rule number determines the order in which the firewall applies the rule. The universally unique identifier (UUID) for a rule never changes even if you modify the rule, such as when you change the rule name. The UUID allows you to track the rule across rule bases even after you deleted the rule.

QUESTION 215
A network security administrator wants to begin inspecting bulk user HTTPS traffic flows egressingout of the internet edge firewall. Which certificate is the best choice to configure as an SSL ForwardTrust 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

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward- proxy

QUESTION 216
During a laptop-replacement project, remote users must be able to establish a GlobalProtect VPN connection to the corporate network before logging in to their new Windows 10 endpoints.
The new laptops have the 5.2.10 GlobalProtect Agent installed, so the administrator chooses to use the Connect Before Logon feature to solve this issue.
What must be configured to enable the Connect Before Logon feature?

A. The GlobalProtect Portal Agent App Settings Connect Method to Pre-logon then On-demand.
B. Registry keys on the Windows system.
C. X-Auth Support in the GlobalProtect Gateway Tunnel Settings.
D. The Certificate profile in the GlobalProtect Portal Authentication Settings.

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/globalprotect/5-2/globalprotect-app-new-features/new- features-released-in-gp-app/connect-before-logon "To use Connect Before Logon, you must enable the settings in the Windows registry and choose the authentication method"

QUESTION 217
An engineer is monitoring an active/active high availability (HA) firewall pair.
Which HA firewall state describes the firewall that is currently processing traffic?

A. Initial
B. Passive
C. Active
D. Active-primary

Correct Answer: C
Section:
Explanation:
In an active/active high availability (HA) firewall pair, the firewall that is currently processing traffic is in the "Active" state. This state indicates that the firewall is fully functional and can own sessions and set up sessions. An active firewall can be either active-primary or active-secondary, depending on the Device ID and the HA configuration. An active-primary firewall connects to User-ID agents, runs DHCP server and DHCP relay, and matches NAT and PBF rules with the Device ID of the active-primary firewall. An active-secondary firewall connects to User-ID agents, runs DHCP server, and matches NAT and PBF rules with the Device ID of the active-secondary firewall.An active-secondary firewall does not support DHCP relay1.Reference:HA Firewall States, PCNSE Study Guide (page 53)

QUESTION 218
Which type of policy in Palo Alto Networks firewalls can use Device-ID as a match condition?

A. NAT
B. DOS protection
C. QoS
D. Tunnel inspection

Correct Answer: B
Section:

QUESTION 219
A company wants to add threat prevention to the network without redesigning the network routing.
What are two best practice deployment modes for the firewall? (Choose two.)

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

Correct Answer: A, D

Section:

Explanation:

VirtualWire and Layer2 deployment modes allow the firewall to act as a bump in the wire without changing the existing network routing. In VirtualWire mode, the firewall bridges two interfaces and passes traffic between them without any IP-layer processing. In Layer2 mode, the firewall acts as a transparent switch and processes traffic at Layer2 of the OSI model. Reference:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/configure-interfaces/virtual-wire-deployments.html

QUESTION 220

An administrator is using Panorama to manage multiple firewalls. After upgrading all devices to the latest PAN-OS software, the administrator enables log forwarding from the firewalls to Panorama.
However, pre-existing logs from the firewalls are not appearing in Panorama.
Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

A. Export the log database.

B. Use the import option to pull logs.

C. Use the scp logdb export command.

D. Use the ACC to consolidate the logs.

Correct Answer: B

Section:

Explanation:

The import option allows the administrator to pull logs from the firewalls to Panorama. This option is useful when the firewalls have pre-existing logs that were not forwarded to Panorama before. The import option can be configured on Panorama by selecting Device > Log Collection > Import Logs. Reference:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama/import-logs-from-firewallsto-panorama.html

QUESTION 221

An engineer configures a specific service route in an environment with multiple virtual systems instead of using the inherited global service route configuration.
What type of service route can be used for this configuration?

A. IPv6 Source or Destination Address

B. Destination-Based Service Route

C. IPv4 Source Interface

D. Inherit Global Setting

Correct Answer: C

Section:

Explanation:

The IPv4 Source Interface service route allows the administrator to specify a source interface for a service based on the virtual system. This option overrides the inherited global service route configuration and provides more granular control over the service routes for each virtual system. Reference:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/virtual-systems/customize-service-routes-for-a-virtual-system.html

QUESTION 222

A firewall engineer creates a NAT rule to translate IP address 1.1.1.10 to 192.168.1.10. The engineer also plans to enable DNS rewrite so that the firewall rewrites the IPv4 address in a DNS response based on the original destination IP address and translated destination IP address configured for the rule. The engineer wants the firewall to rewrite a DNS response of 1.1.1.10 to 192.168.1.10.
What should the engineer do to complete the configuration?

A. Create a U-Turn NAT to translate the destination IP address 192.168.1.10 to 1.1.1.10 with the destination port equal to UDP/53.

B. Enable DNS rewrite under the destination address translation in the Translated Packet section of the NAT rule with the direction Forward.

C. Enable DNS rewrite under the destination address translation in the Translated Packet section of the NAT rule with the direction Reverse.

D. Create a U-Turn NAT to translate the destination IP address 1.1.1.10 to 192.168.1.10 with the destination port equal to UDP/53.

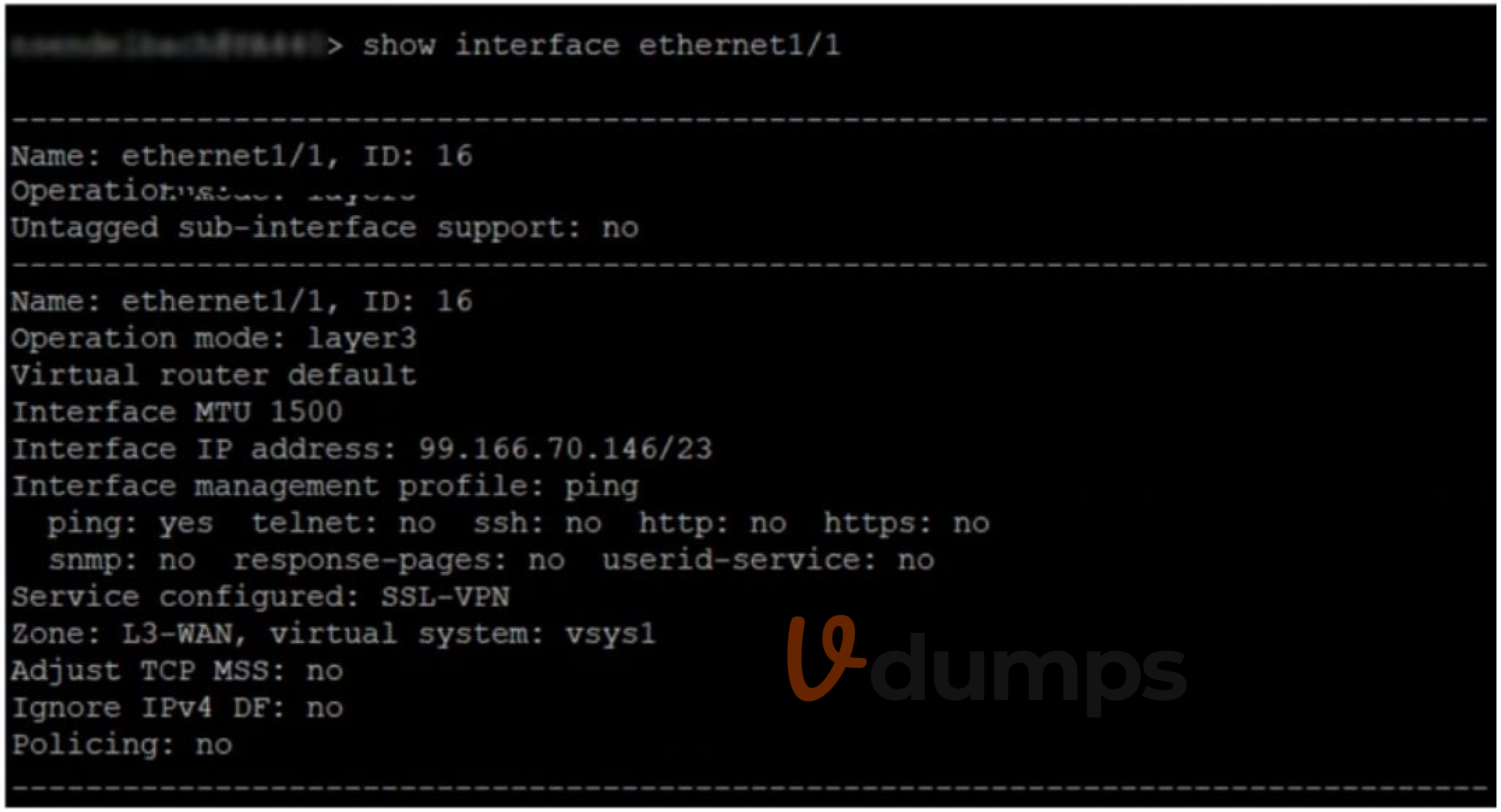
Correct Answer: B
Section:
Explanation:
If the DNS response matches the Original Destination Address in the rule, translate the DNS response using the same translation the rule uses. For example, if the rule translates IP address 1.1.1.10 to 192.168.1.10, the firewall rewrites a DNS response of 1.1.1.10 to 192.168.1.10. https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/source-nat-and-destination-nat/destination-nat-dns-rewrite-use-cases#id0d85db1b-05b9-4956-a467-f71d558263bb

QUESTION 223
An organization wants to begin decrypting guest and BYOD traffic.
Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

A. Authentication Portal
B. SSL Decryption profile
C. SSL decryption policy
D. comfort pages

Correct Answer: A
Section:
Explanation:
An authentication portal is a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An authentication portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The authentication portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button.The authentication portal can also be configured to use different authentication methods, such as local database, RADIUS, LDAP, Kerberos, or SAML1.By using an authentication portal, the firewall can redirect BYOD users to a web page where they can learn about the decryption policy, download and install the CA certificate, and agree to the terms of use before accessing the network or the internet2.
An SSL decryption profile is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption profile is a set of options that define how the firewall handles SSL/TLS traffic that it decrypts.An SSL decryption profile can include settings such as certificate verification, unsupported protocol handling, session caching, session resumption, algorithm selection, etc3. An SSL decryption profile does not provide any user identification or notification functions.
An SSL decryption policy is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption policy is a set of rules that determine which traffic the firewall decrypts based on various criteria, such as source and destination zones, addresses, users, applications, services, etc.An SSL decryption policy can also specify which type of decryption to apply to the traffic, such as SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy4. An SSL decryption policy does not provide any user identification or notification functions.
Comfort pages are not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. Comfort pages are web pages that the firewall displays to users when it blocks or fails to decrypt certain traffic due to security policy or technical reasons.Comfort pages can include information such as the reason for blocking or failing to decrypt the traffic, the URL of the original site, the firewall serial number, etc5. Comfort pages do not provide any user identification or notification functions before decrypting the traffic.

QUESTION 224
After switching to a different WAN connection, users have reported that various websites will not load, and timeouts are occurring. The web servers work fine from other locations.
The firewall engineer discovers that some return traffic from these web servers is not reaching the users behind the firewall. The engineer later concludes that the maximum transmission unit (MTU) on an upstream router interface is set to 1400 bytes.
The engineer reviews the following CLI output for ethernet1/1.



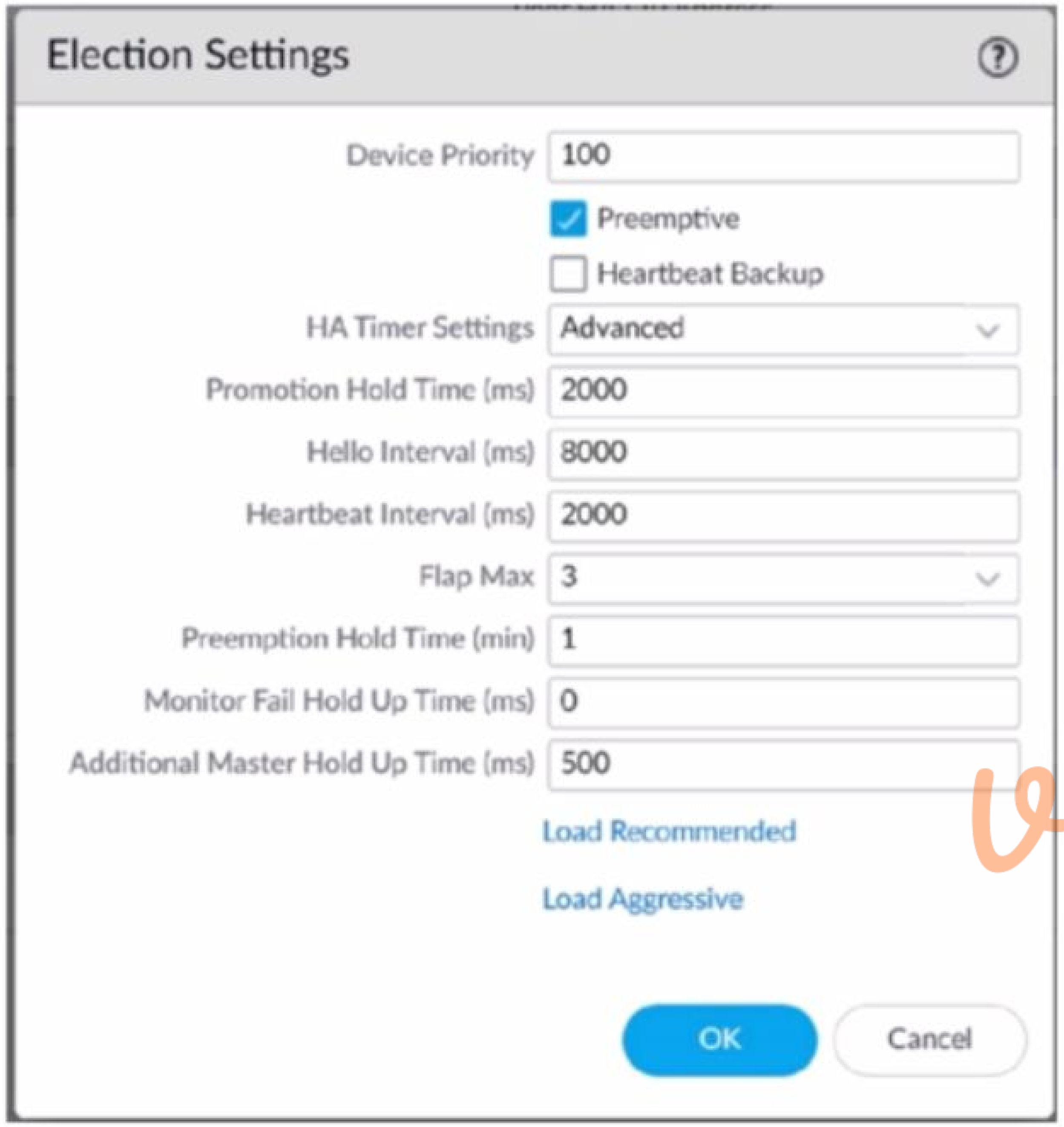
```
[redacted]> show interface ethernet1/1

--------------------------------------------------------------------------------
Name: ethernet1/1, ID: 16
Operation mode: layer3
Untagged sub-interface support: no
--------------------------------------------------------------------------------
Name: ethernet1/1, ID: 16
Operation mode: layer3
Virtual router default
Interface MTU 1500
Interface IP address: 99.166.70.146/23
Interface management profile: ping
  ping: yes  telnet: no  ssh: no  http: no  https: no
  snmp: no  response-pages: no  userid-service: no
Service configured: SSL-VPN
Zone: L3-WAN, virtual system: vsys1
Adjust TCP MSS: no
Ignore IPv4 DF: no
Policing: no
--------------------------------------------------------------------------------
```

Which setting should be modified on ethernet1/1 to remedy this problem?

A. Lower the interface MTU value below 1500.
B. Enable the Ignore IPv4 Don't Fragment (DF) setting.
C. Change the subnet mask from /23 to /24.
D. Adjust the TCP maximum segment size (MSS) value. *

Correct Answer: B
Section:
Explanation:

QUESTION 225
An engineer is reviewing the following high availability (HA) settings to understand a recent HAfailover event.



Election Settings

Device Priority: 100

☑ Preemptive

☐ Heartbeat Backup

HA Timer Settings: Advanced

Promotion Hold Time (ms): 2000

Hello Interval (ms): 8000

Heartbeat Interval (ms): 2000

Flap Max: 3

Preemption Hold Time (min): 1

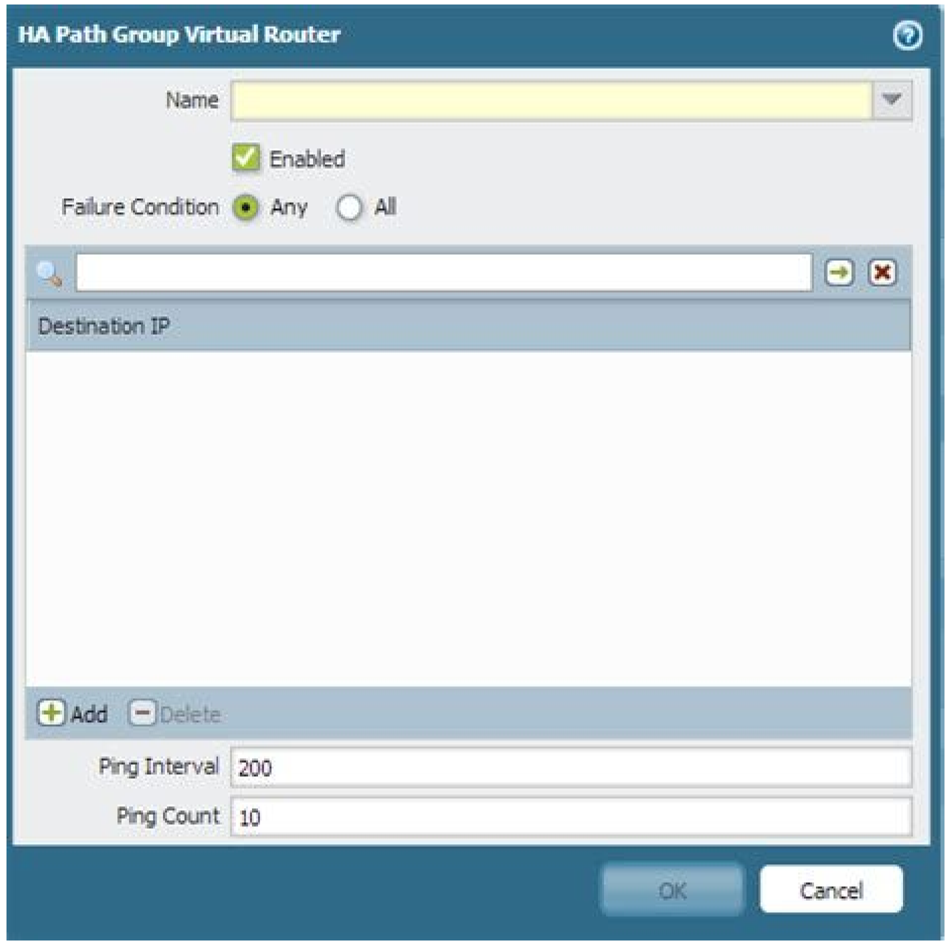
Monitor Fail Hold Up Time (ms): 0

Additional Master Hold Up Time (ms): 500

Which timer determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational?

A. Monitor Fail Hold Up Time
B. Promotion Hold Time
C. Heartbeat Interval
D. Hello Interval

Correct Answer: D
Section:
Explanation:
The timer that determines the frequency between packets sent to verify that the HA functionality on the other HA firewall is operational is the Hello Interval. The Hello Interval is the interval in milliseconds between hello packets that are sent to check the HA status of the peer firewall. The default value for the Hello Interval is 8000 ms for all platforms, and the range is 8000-60000 ms.If the firewall does not receive a hello packet from its peer within the specified interval, it will declare the peer as failed and initiate a failover12.Reference:HA Timers,Layer 3 High Availability with Optimal Failover Times Best Practices


HA Path Group Virtual Router

Name

☑ Enabled

Failure Condition ● Any ○ All

Destination IP

Ping Interval 200

Ping Count 10

QUESTION 226

What is the best description of the Cluster Synchronization Timeout (min)?

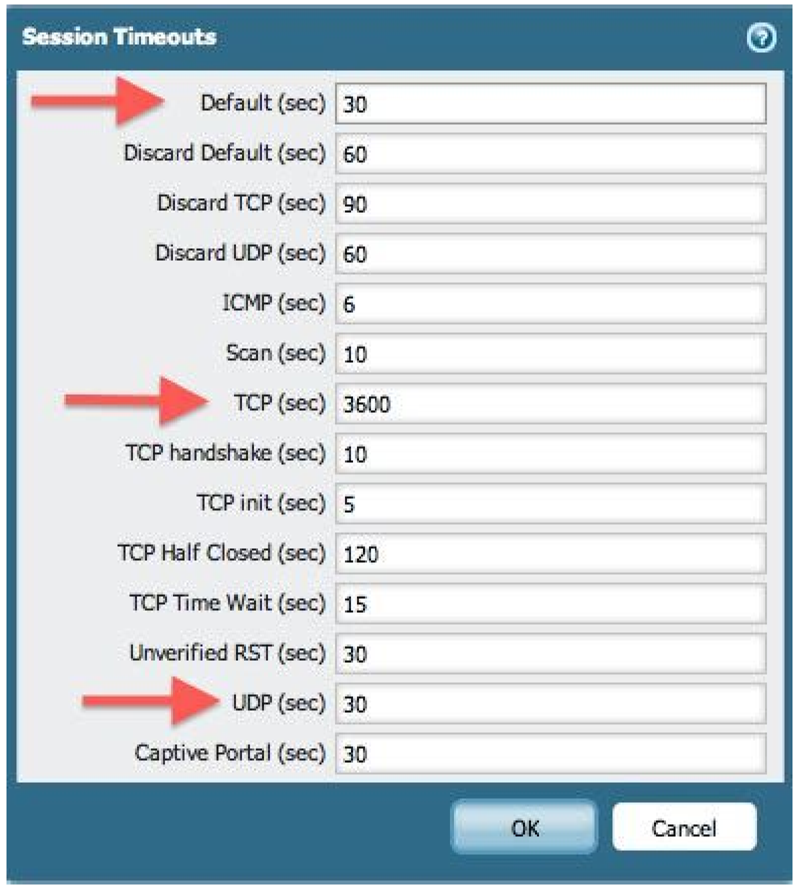
A. The maximum time that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing

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 maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational

Correct Answer: A
Section:
Explanation:
The best description of the Cluster Synchronization Timeout (min) is the maximum time that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing. This is a parameter that can be configured in an HA cluster, which is a group of firewalls that share session state and provide high availability and scalability. The Cluster Synchronization Timeout (min) determines how long the local firewall will wait for the cluster to reach a stable state before it decides to become Active and process traffic. A stable state means that all cluster members are either Active or Passive, and have synchronized their sessions with each other. If there is another cluster member that is in an unknown or unstable state, such as Initializing, Non-functional, or Suspended, then it may prevent the cluster from fully synchronizing and cause a delay in traffic processing. The Cluster Synchronization Timeout (min) can be set to a value between 0 and 30 minutes, with a default of 0. If it is set to 0, then the local firewall will not wait for any other cluster member and will immediately go to Active state.If it is set to a positive value, then the local firewall will wait for that amount of time before going to Active state, unless the cluster reaches a stable state earlier12.Reference:Configure HA Clustering, PCNSE Study Guide (page 53)



Default (sec) 30
Discard Default (sec) 60
Discard TCP (sec) 90
Discard UDP (sec) 60
ICMP (sec) 6
Scan (sec) 10
TCP (sec) 3600
TCP handshake (sec) 10
TCP init (sec) 5
TCP Half Closed (sec) 120
TCP Time Wait (sec) 15
Unverified RST (sec) 30
UDP (sec) 30
Captive Portal (sec) 30

QUESTION 227
What can the Log Forwarding built-in action with tagging be used to accomplish?

A. Block the source zones of selected unwanted traffic.
B. Block the destination IP addresses of selected unwanted traffic.
C. Forward selected logs to the Azure Security Center.
D. Block the destination zones of selected unwanted traffic.

Correct Answer: B
Section:
Explanation:
The Log Forwarding feature in Palo Alto Networks firewalls allows administrators to perform automated actions based on logs. One of the actions that can be configured is to tag an IP address, which can then be used in conjunction with Dynamic Address Groups (DAG) to enforce security policies. By tagging the destination IP addresses of unwanted traffic, an administrator can dynamically update policies to block traffic to those destinations. This method is particularly useful for responding quickly to detected threats by creating and enforcing a policy that blocks traffic to tagged destinations without the need for manual intervention or policy changes. For a detailed explanation, the Palo Alto Networks' 'PAN-OS Administrator's Guide' provides information on log forwarding and automated actions.

QUESTION 228
Which three statements accurately describe Decryption Mirror? (Choose three.)

A. Decryption Mirror requires a tap interface on the firewall
B. Use of Decryption Mirror might enable malicious users with administrative access to the firewall to harvest sensitive information that is submitted via an encrypted channel
C. Only management consent is required to use the Decryption Mirror feature.
D. Decryption, storage, inspection, and use of SSL traffic are regulated in certain countries.
E. You should consult with your corporate counsel before activating and using Decryption Mirror in a production environment.

Correct Answer: B, D, E
Section:
Explanation:
Decryption Mirror is a feature that allows a Palo Alto Networks firewall to send a copy of decrypted traffic to an external security device or tool for further analysis. The potential risk associated with Decryption Mirror is that if the firewall administrator's credentials are compromised, a malicious user could potentially access sensitive decrypted information. Hence, it's advised to be cautious and ensure proper handling of this feature.
Additionally, laws and regulations regarding the decryption, storage, inspection, and use of SSL/TLS encrypted traffic vary by country and industry. It is crucial to ensure compliance with relevant laws and best practices when using Decryption Mirror. This often requires consultation with corporate legal counsel to understand the implications and ensure that the use of such features does not violate privacy laws or regulatory requirements.
The need for administrative consent and the legal implications of using Decryption Mirror features are outlined in Palo Alto Networks' 'PAN-OS Administrator's Guide' and best practice documentation. It is not specifically required to have a tap interface to use Decryption Mirror, which eliminates option A. Option C is incorrect because it is not just management consent but legal compliance that needs to be considered.

QUESTION 229
A network security engineer needs to enable Zone Protection in an environment that makes use of Cisco TrustSec Layer 2 protections
What should the engineer configure within a Zone Protection profile to ensure that the TrustSec packets are identified and actions are taken upon them?

A. TCP Fast Open in the Strip TCP options
B. Ethernet SGT Protection
C. Stream ID in the IP Option Drop options
D. Record Route in IP Option Drop options

Correct Answer: B
Section:
Explanation:
Cisco TrustSec technology uses Security Group Tags (SGTs) to enforce access controls on Layer 2 traffic. When implementing Zone Protection on a Palo Alto Networks firewall in an environment with Cisco TrustSec, you should configure Ethernet SGT Protection. This setting ensures that the firewall can recognize SGTs in Ethernet frames and apply the appropriate actions based on the configured policies. The use of Ethernet SGT Protection in conjunction with TrustSec is covered in advanced firewall configuration documentation and in interoperability guides between Palo Alto Networks and Cisco systems.

QUESTION 230
When a new firewall joins a high availability (HA) cluster, the cluster members will synchronize all existing sessions over which HA port?

A. HA1
B. HA3
C. HA2
D. HA4

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/high-availability/ha-clustering-overview

QUESTION 231
Which three authentication types can be used to authenticate users? (Choose three.)

A. Local database authentication
B. PingID
C. Kerberos single sign-on
D. GlobalProtect client
E. Cloud authentication service

Correct Answer: A, C, E
Section:
Explanation:
The three authentication types that can be used to authenticate users are:
A: Local database authentication.This is the authentication type that uses the local user database on the firewall or Panorama to store and verify user credentials1.
C: Cloud authentication service.This is the authentication type that uses a cloud-based identity provider, such as Okta, PingOne, or PingFederate, to authenticate users and provide SAML assertions to the firewall or Panorama2.
E: Kerberos single sign-on.This is the authentication type that uses the Kerberos protocol to authenticate users who are logged in to a Windows domain and provide them with seamless access to resources on the firewall or Panorama3.

QUESTION 232
An administrator has been tasked with configuring decryption policies,
Which decryption best practice should they consider?

A. Consider the local, legal, and regulatory implications and how they affect which traffic can be decrypted.
B. Decrypt all traffic that traverses the firewall so that it can be scanned for threats.
C. Place firewalls where administrators can opt to bypass the firewall when needed.
D. Create forward proxy decryption rules without Decryption profiles for unsanctioned applications.

Correct Answer: A
Section:
Explanation:
The best decryption best practice that the administrator should consider isA: Consider the local, legal, and regulatory implications and how they affect which traffic can be decrypted.This is because decryption involves intercepting and inspecting encrypted traffic, which may raise privacy and compliance issues depending on the jurisdiction and the type of traffic1.Therefore, the administrator should be aware of the local, legal, and regulatory implications and how they affect which traffic can be decrypted, and follow the appropriate guidelines and policies to ensure that decryption is done in a lawful and ethical manner1.

QUESTION 233
An engineer needs to configure a standardized template for all Panorama-managed firewalls. These settings will be configured on a template named 'Global' and will be included in all template stacks.
Which three settings can be configured in this template? (Choose three.)

A. Log Forwarding profile
B. SSL decryption exclusion
C. Email scheduler
D. Login banner
E. Dynamic updates

Correct Answer: B, D, E
Section:
Explanation:
A template is a set of configuration options that can be applied to one or more firewalls or virtual systems managed by Panorama.A template can include settings from the Device and Network tabs on the firewall web interface, such as login banner, SSL decryption exclusion, and dynamic updates4. These settings can be configured in a template named ''Global'' and included in all template stacks.A template stack is a group of templates that Panorama pushes to managed firewalls in an ordered hierarchy4.Reference:Manage Templates and Template Stacks, PCNSE Study Guide (page 50)

QUESTION 234
What are two best practices for incorporating new and modified App-IDs? (Choose two)

A. Configure a security policy rule to allow new App-IDs that might have network-wide impact
B. Study the release notes and install new App-IDs if they are determined to have low impact

C. Perform a Best Practice Assessment to evaluate the impact or the new or modified App-IDs
D. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs

Correct Answer: A, B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content- updates/best-practices-for-app-and-threat-content-updates/best-practices-security- first#id184AH00F06E

QUESTION 235
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

Correct Answer: B, D, E
Section:
Explanation:
According to Palo Alto Networks documentation123, multi-factor authentication (MFA) is a methodof 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.

QUESTION 236
When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

A. Set the passive link state to shutdown'.
B. Disable config sync.
C. Disable the HA2 link.
D. Disable HA.

Correct Answer: B
Section:
Explanation:
To prevent the import from affecting ongoing traffic when you import the configuration of an HA pair into Panorama, you should disable config sync on both firewalls. Config sync is a feature that enables the firewalls in an HA pair to synchronize their configurations and maintain consistency. However, when you import the configuration of an HA pair into Panorama, you want to avoid any changes to the firewall configuration until you verify and commit the imported configuration on Panorama.Therefore, you should disable config sync before importing the configuration, and re-enable it after committing the changes on Panorama12.Reference:Migrate a Firewall HA Pair to Panorama Management, PCNSE Study Guide (page 50)

QUESTION 237
An engineer is troubleshooting a traffic-routing issue.
What is the correct packet-flow sequence?

A. PBF > Zone Protection Profiles > Packet Buffer Protection
B. BGP > PBF > NAT

C. PBF > Static route > Security policy enforcement

D. NAT > Security policy enforcement > OSPF

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

QUESTION 238
A consultant advises a client on designing an explicit Web Proxy deployment on PAN-OS 11 0 The client currently uses RADIUS authentication in their environment
Which two pieces of information should the consultant provide regarding Web Proxy authentication? (Choose two.)

A. Kerberos or SAML authentication need to be configured

B. LDAP or TACACS+ authentication need to be configured

C. RADIUS is only supported for a transparent Web Proxy.

D. RADIUS is not supported for explicit or transparent Web Proxy

Correct Answer: A, D
Section:
Explanation:
For explicit Web Proxy deployment on PAN-OS, Palo Alto Networks currently supports Kerberos and SAML as authentication methods. RADIUS is not supported for explicit or transparent Web Proxy authentication on Palo Alto Networks appliances, which means that if the client is currently using RADIUS, they will need to configure an alternate supported authentication method. LDAP or TACACS+ authentication is not directly supported for Web Proxy authentication in PAN-OS. For more information on supported Web Proxy authentication methods, please refer to the latest Palo Alto Networks 'PAN-OS Web Interface Reference Guide'.