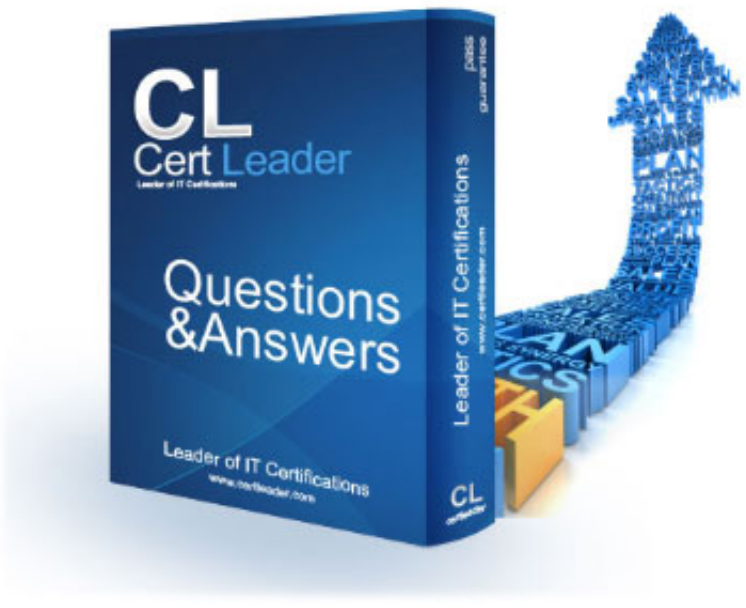
PCNSE Dumps

Palo Alto Networks Certified Security Engineer (PCNSE)PAN-OS 8.0

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

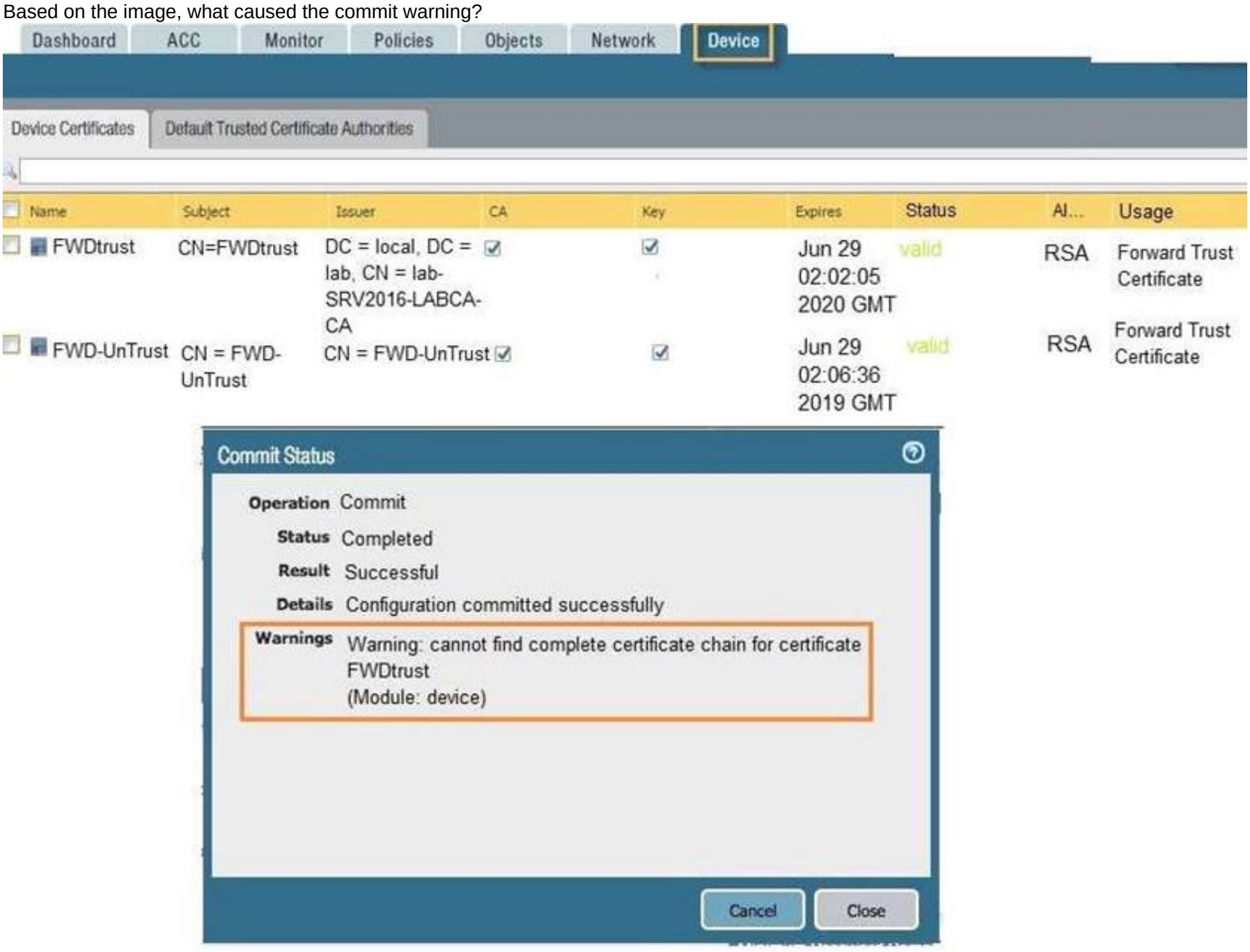


NEW QUESTION 1
SAML SLO is supported for which two firewall features? (Choose two.)

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

Answer: AB

NEW QUESTION 2
Based on the image, what caused the commit warning?



A. The CA certificate for FWDtrust has not been imported into the firewall.
B. The FWDtrust certificate has not been flagged as Trusted Root CA.
C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
D. The FWDtrust certificate does not have a certificate chain.

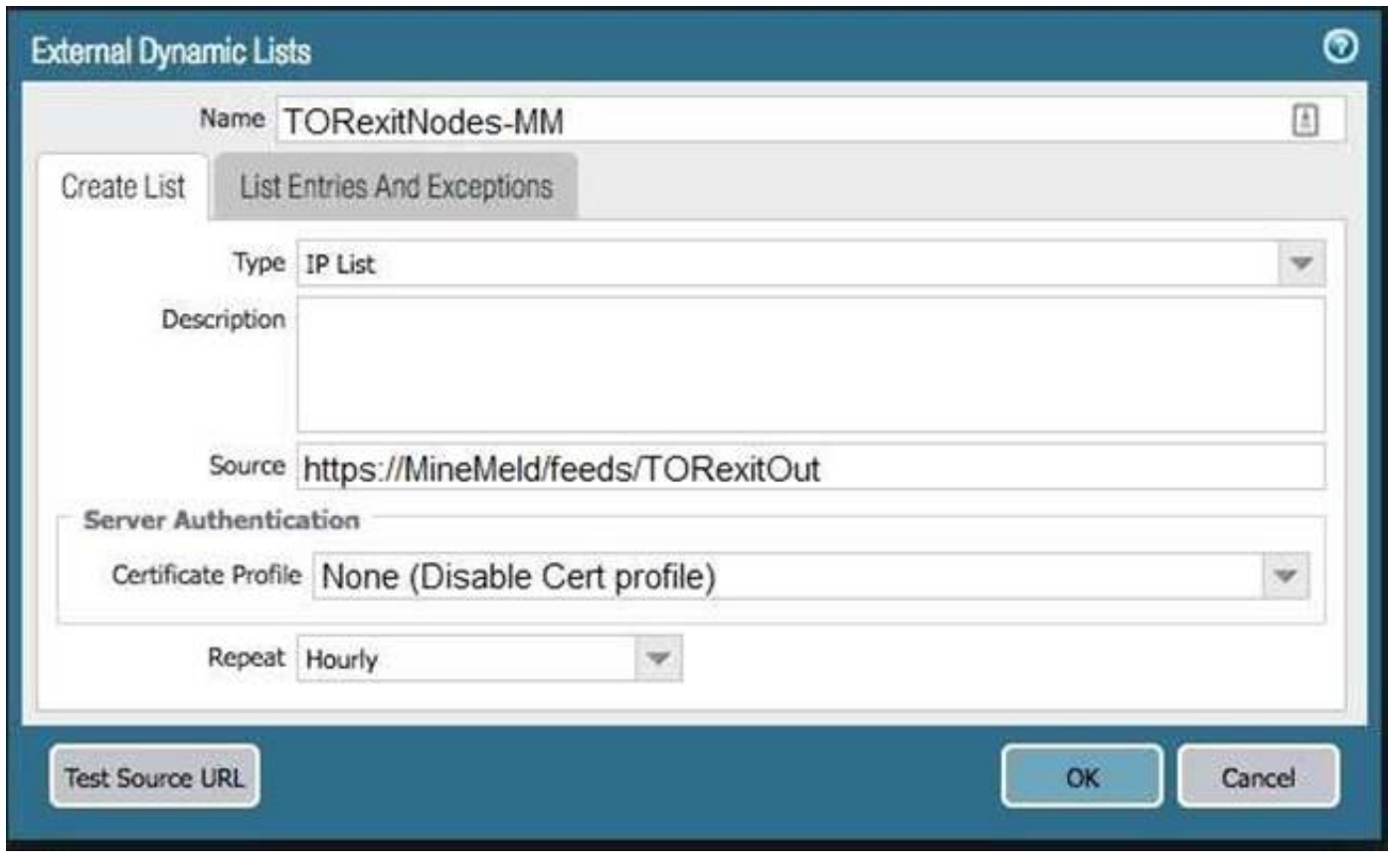
Answer: D

NEW QUESTION 3
An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

A. Enable and configure the Packet Buffer protection thresholds.Enable Packet Buffer Protection per ingress zone.
B. Enable and then configure Packet Buffer thresholdsEnable Interface Buffer protection.
C. Create and Apply Zone Protection Profiles in all ingress zones.Enable Packet Buffer Protection per ingress zone.
D. Configure and apply Zone Protection Profiles for all egress zones.Enable Packet Buffer Protection pre egress zone.
E. Enable per-vsys Session Threshold alerts and triggers for Packet Buffer Limits.Enable Zone Buffer Protection per zone.

Answer: A

NEW QUESTION 4
The firewall is not downloading IP addresses from MineMeld. Based, on the image, what most likely is wrong?



A. A Certificate Profile that contains the client certificate needs to be selected.
B. The source address supports only files hosted with an ftp://<address/file>.
C. External Dynamic Lists do not support SSL connections.
D. A Certificate Profile that contains the CA certificate needs to be selected.

Answer: D

NEW QUESTION 5
Which administrative authentication method supports authorization by an external service?

A. Certificates
B. LDAP
C. RADIUS
D. SSH keys

Answer: C

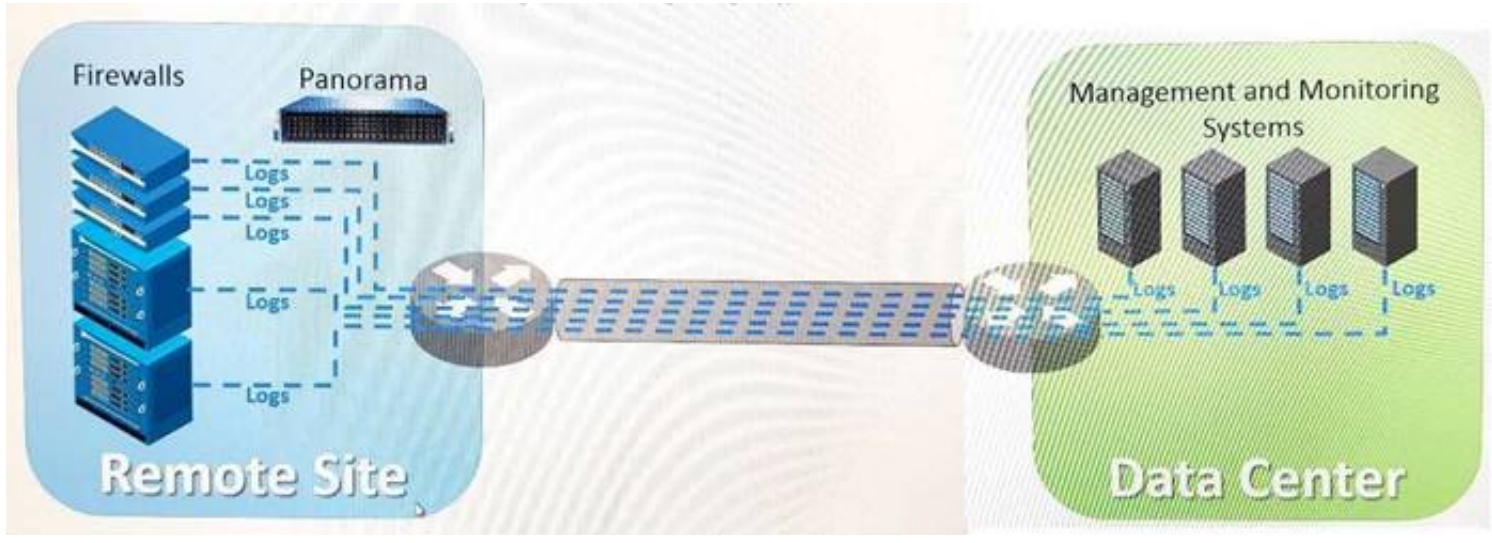
NEW QUESTION 6
Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

A. check
B. find
C. test
D. sim

Answer: C

Explanation:
Reference: http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html

NEW QUESTION 7
Refer to exhibit.



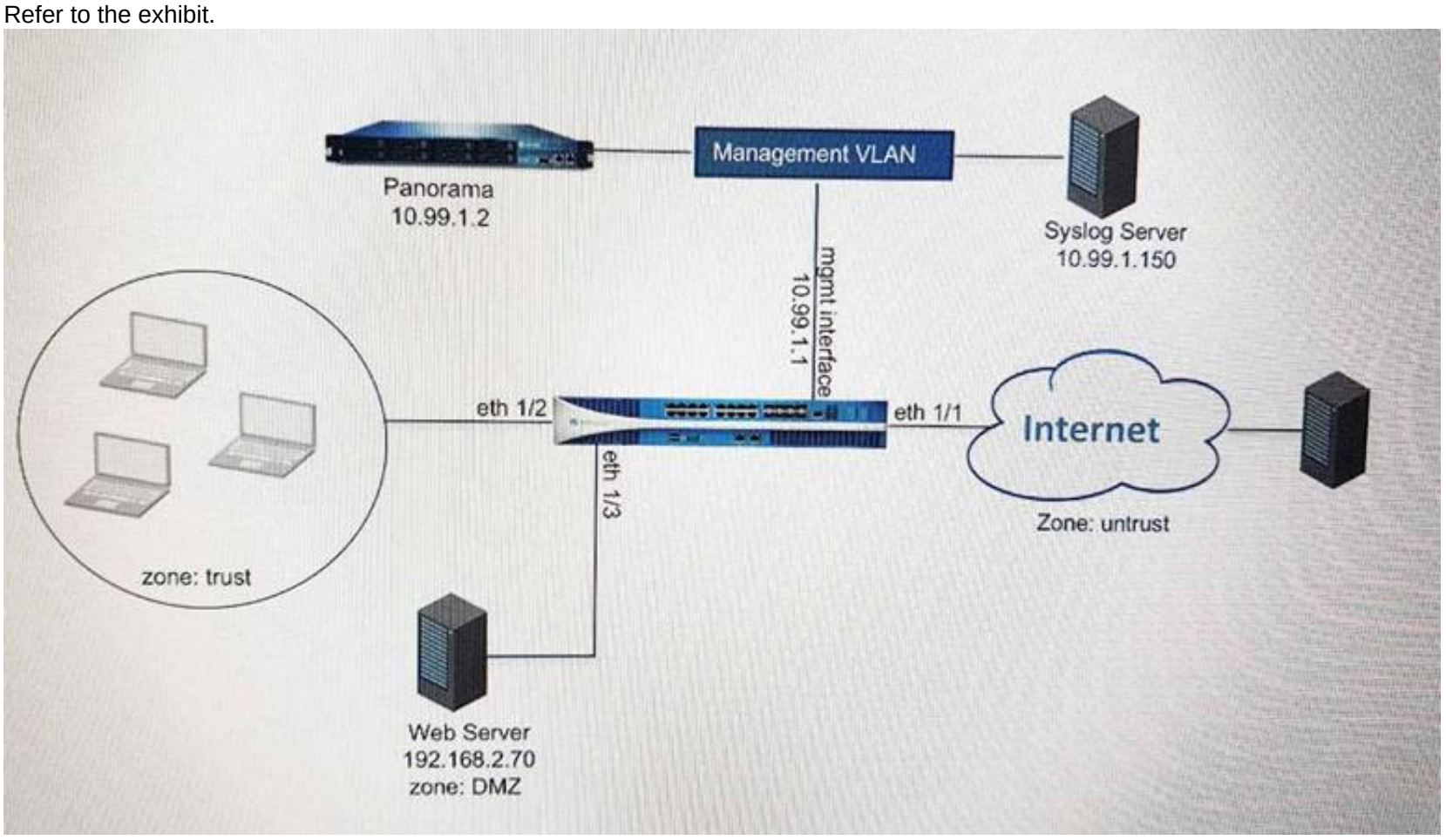
An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.
How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring/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

A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.

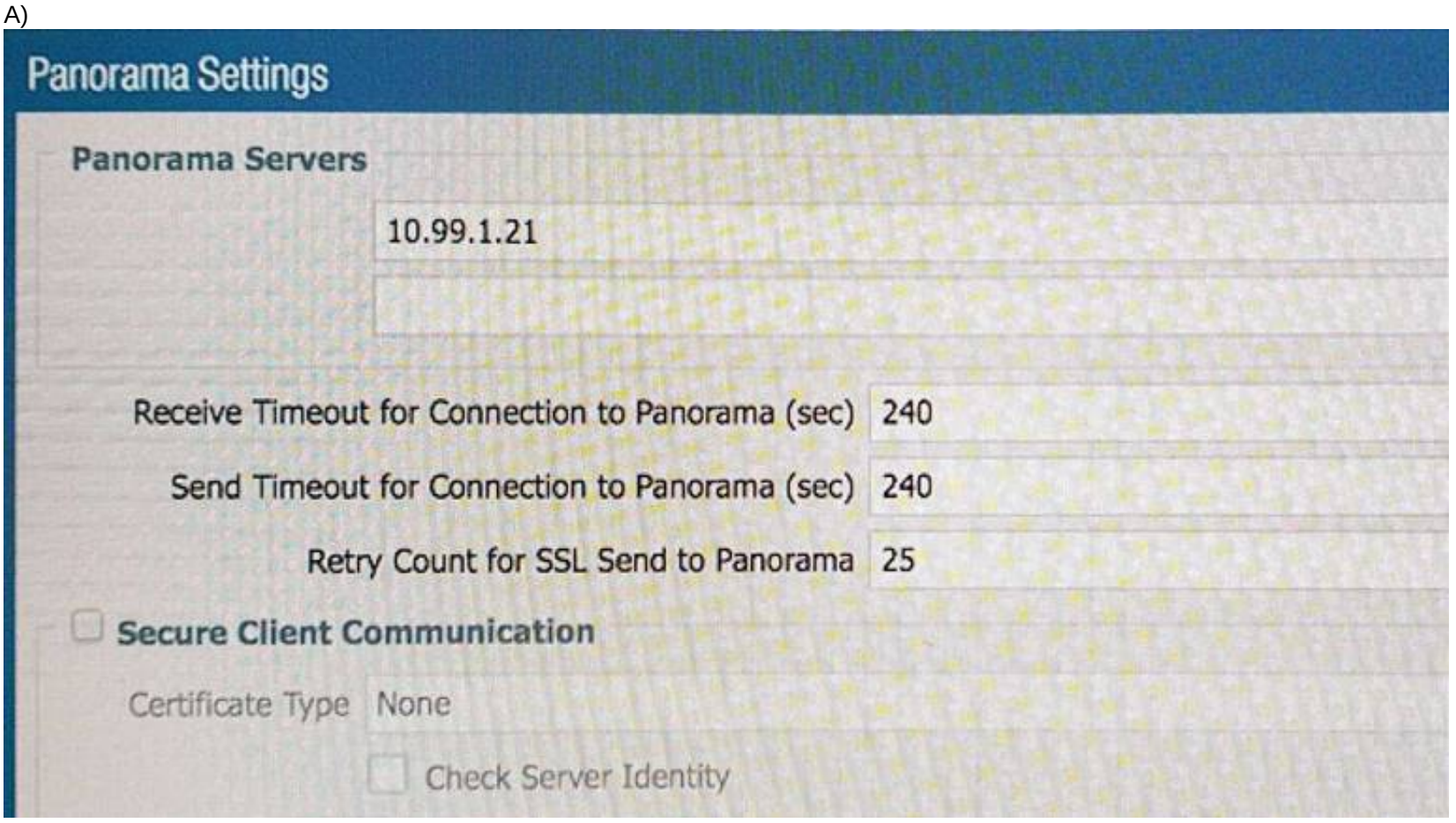
B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
C. Configure log compression and optimization features on all remote firewalls.
D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

Answer: A

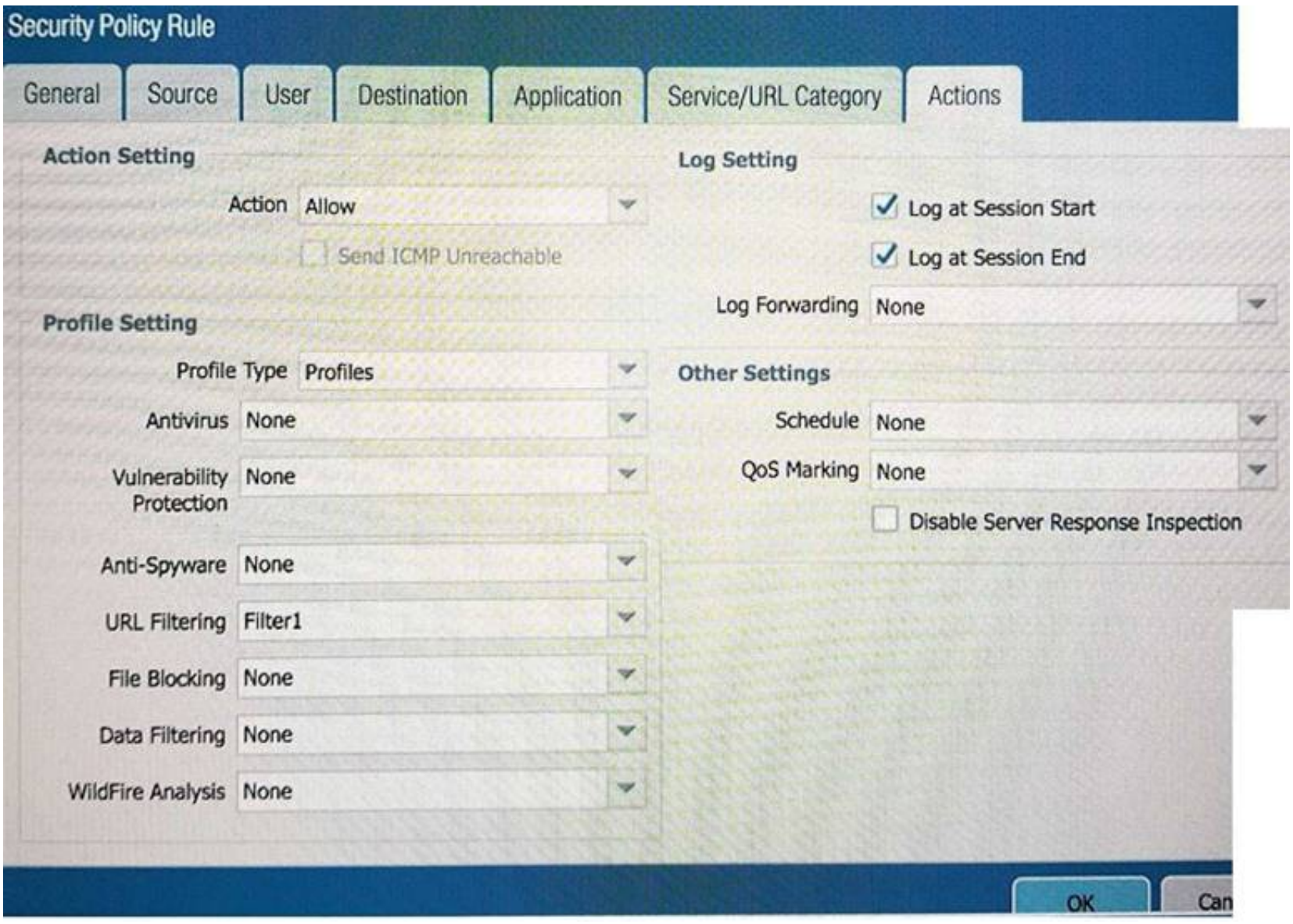
NEW QUESTION 8
Refer to the exhibit.



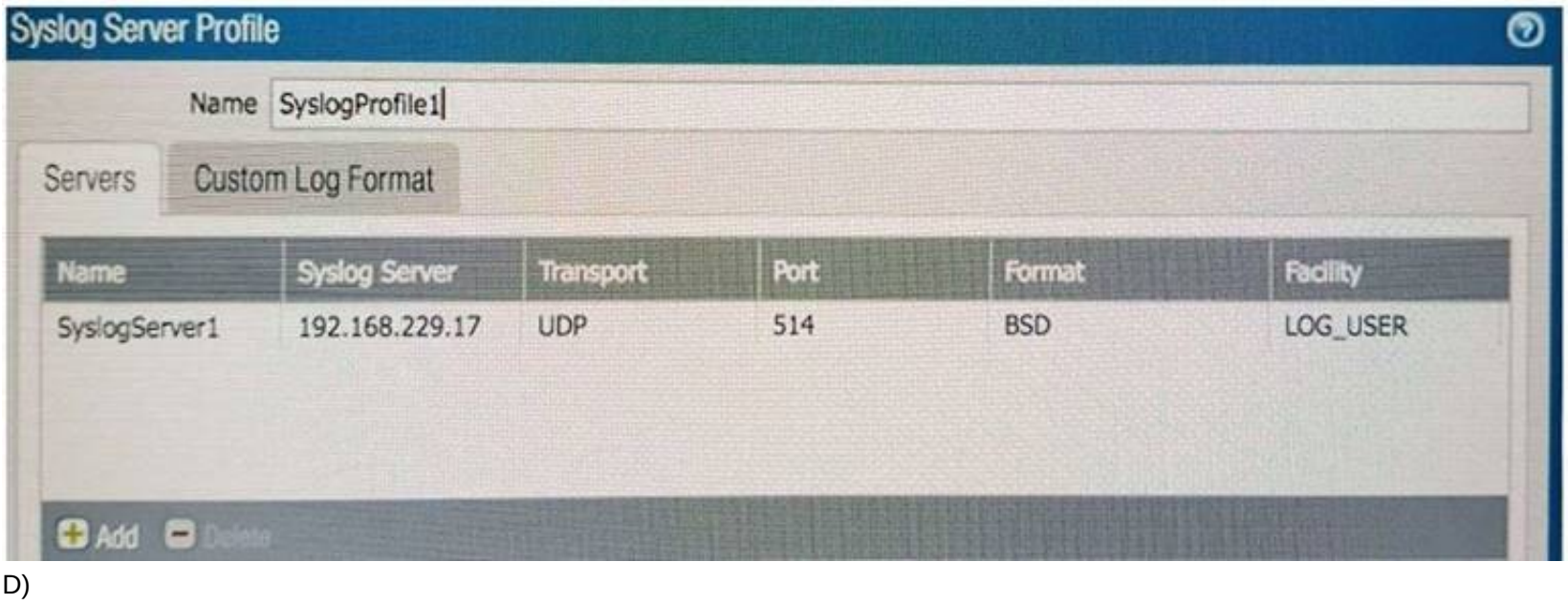
An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side.
Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?
A)



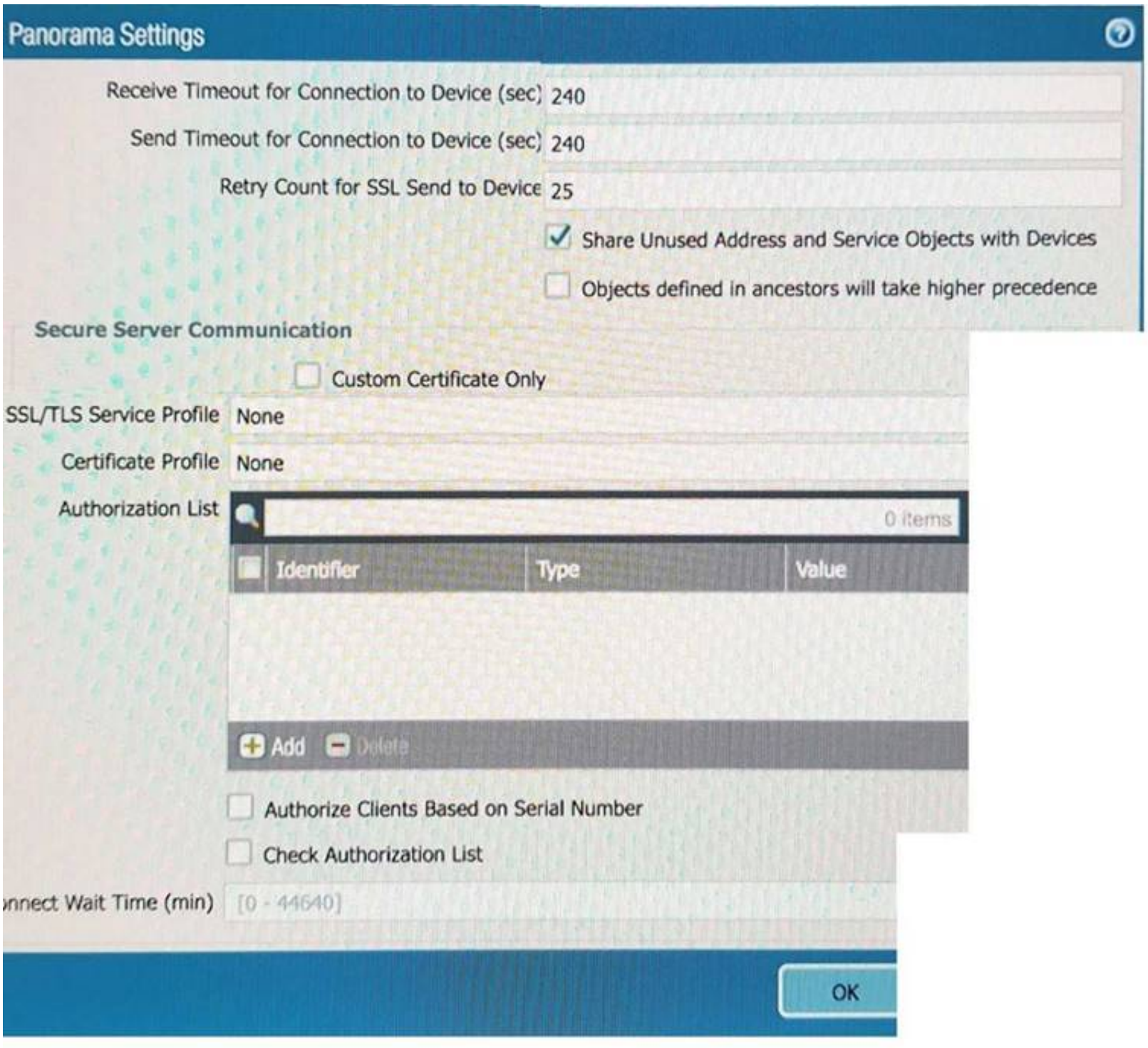
B)


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Action Setting
Action
Allow
Send ICMP Unreachable
Profile Setting
Profile Type
Profiles
Antivirus
None
Vulnerability Protection
None
Anti-Spyware
None
URL Filtering
Filter1
File Blocking
None
Data Filtering
None
WildFire Analysis
None
Log Setting
Log at Session Start
Log at Session End
Log Forwarding
None
Other Settings
Schedule
None
QoS Marking
None
Disable Server Response Inspection
OK
Can

C)


Syslog Server Profile
Name
SyslogProfile1
Servers
Custom Log Format
Name
Syslog Server
Transport
Port
Format
Facility
SyslogServer1
192.168.229.17
UDP
514
BSD
LOG_USER
Add
Delete

D)



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

Answer: D

NEW QUESTION 9
To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

A. Device>Setup>Services>AutoFocus
B. Device> Setup>Management >AutoFocus
C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
D. Device>Setup>WildFire>AutoFocus
E. Device>Setup> Management> Logging and Reporting Settings

Answer: B

Explanation:
Reference: https://www.paloaHYPERLINK "https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence"ltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence

NEW QUESTION 10
An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

A. Security policy rule allowing SSL to the target server
B. Firewall connectivity to a CRL
C. Root certificate imported into the firewall with “Trust” enabled
D. Importation of a certificate from an HSM

Answer: A

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection

NEW QUESTION 10
Decrypted packets from the website https://www.microsoft.com will appear as which application and service within the Traffic log?

A. web-browsing and 443
B. SSL and 80
C. SSL and 443
D. web-browsing and 80

Answer: A

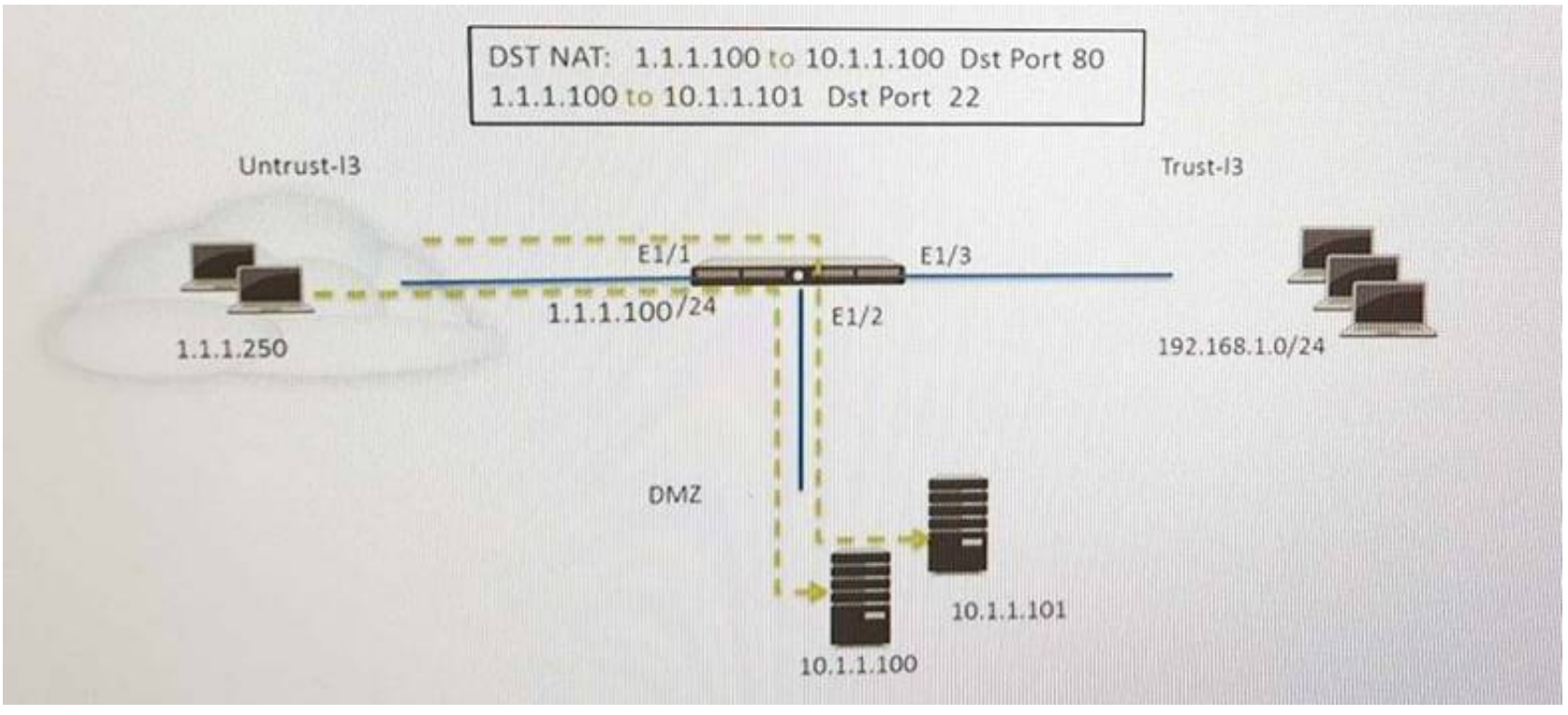
NEW QUESTION 14
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

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

Answer: D

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

NEW QUESTION 15
Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.)
Which two security policy rules will accomplish this configuration? (Choose two.)

A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
D. Untrust (Any) to DMZ (10.1.1.1), ssh –Allow
E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

Answer: CD

NEW QUESTION 16
An administrator has left a firewall to use the default port for all management services. Which three functions are performed by the dataplane? (Choose three.)

A. WildFire updates
B. NAT
C. NTP
D. antivirus E.File blocking

Answer: ABC

NEW QUESTION 17
VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A. Zone Protection
B. DoS Protection
C. Web Application
D. Replay

Answer: A

NEW QUESTION 21
An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN- OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web-browsing traffic from any to any zone. What must the administrator configure so that the PAN-OS® software can be upgraded?

A. Security policy rule
B. CRL
C. Service route
D. Scheduler

Answer: A

NEW QUESTION 23
Which option is part of the content inspection process?

A. Packet forwarding process
B. SSL Proxy re-encrypt
C. IPsec tunnel encryption
D. Packet egress process

Answer: A

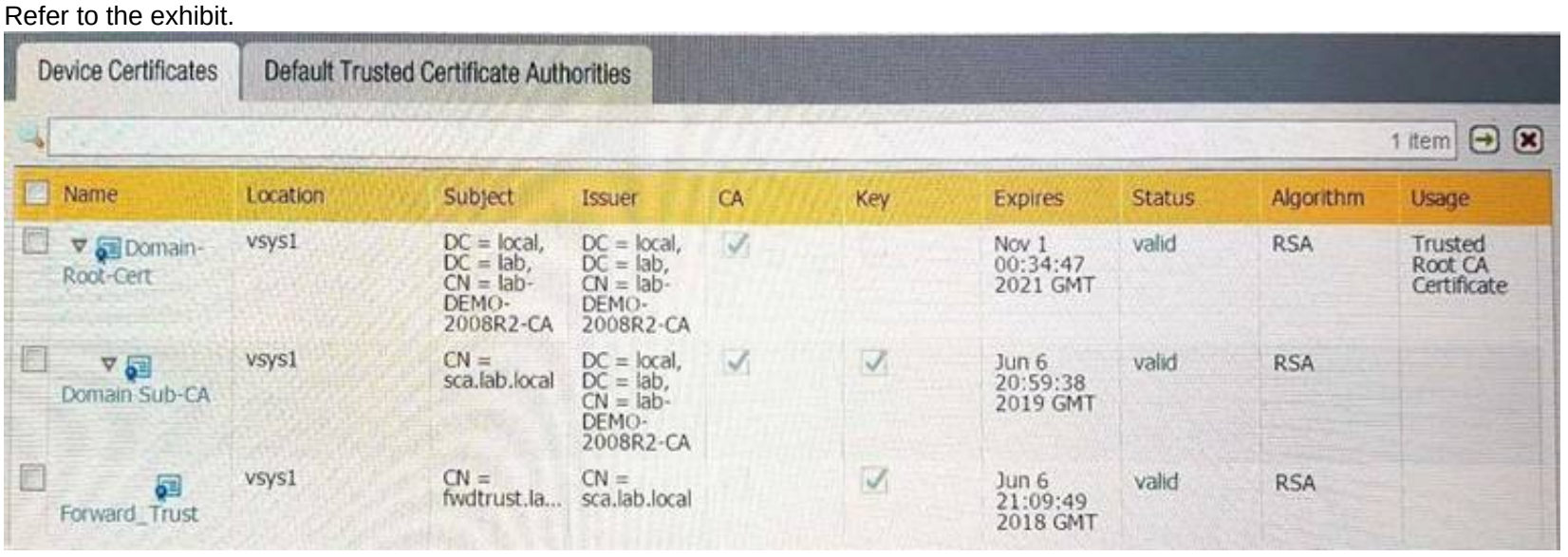
NEW QUESTION 27
In a virtual router, which object contains all potential routes?

A. MIB
B. RIB
C. SIP
D. FIB

Answer: B

Explanation:
Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0ahUKEwiOkbfYzPzXAhVnEJoKHcwVCg4QFghiMAk&url=https%3A%2F%2Flive.paloaltonetworks.com%2Ftwzvq79624%2Fattachments%2Ftwzvq79624%2Fdocumentation_tkb%2F487%2F1%2FRoute%2520Redistribution%2520and%2520Filtering%2520TechNote%2520-%2520Rev% 2520B. pdf&usg=AOvVaw0H9qgaJK0oI2xjIJBNo1Km

NEW QUESTION 28
Refer to the exhibit.



Which certificates can be used as a Forwarded Trust certificate?

A. Certificate from Default Trust Certificate Authorities
B. Domain Sub-CA
C. Forward_Trust
D. Domain-Root-Cert

Answer: A

NEW QUESTION 33
An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.
Which configuration setting or step will allow the firewall to get automatic application signature updates?

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

Answer: D

Explanation:
The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates

NEW QUESTION 36
An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.
Which interface type and license feature are necessary to meet the requirement?

A. Decryption Mirror interface with the Threat Analysis license
B. Virtual Wire interface with the Decryption Port Export license
C. Tap interface with the Decryption Port Mirror license
D. Decryption Mirror interface with the associated Decryption Port Mirror license

Answer: D

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring

NEW QUESTION 38
An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port. Which log entry can the administrator use to verify that sessions are being decrypted?

A. In the details of the Traffic log entries
B. Decryption log
C. Data Filtering log
D. In the details of the Threat log entries

Answer: A

Explanation:
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719

NEW QUESTION 40
Which processing order will be enabled when a Panorama administrator selects the setting “Objects defined in ancestors will take higher precedence?”

A. Descendant objects will take precedence over other descendant objects.
B. Descendant objects will take precedence over ancestor objects.
C. Ancestor objects will have precedence over descendant objects.
D. Ancestor objects will have precedence over other ancestor objects.

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management

NEW QUESTION 44
An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.
How would the administrator establish the chain of trust?

A. Use custom certificates
B. Enable LDAP or RADIUS integration
C. Set up multi-factor authentication
D. Configure strong password authentication

Answer: A

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/plan-your-panorama-deployment

NEW QUESTION 48
An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in “the cloud”). Bootstrapping is the most expedient way to perform this task. Which option describes deployment of a bootstrap package in an on-premise virtual environment?

A. Use config-drive on a USB stick.
B. Use an S3 bucket with an ISO.
C. Create and attach a virtual hard disk (VHD).
D. Use a virtual CD-ROM with an ISO.

Answer: D

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapping-firewalls-for-rapid-deployment.html

NEW QUESTION 53
Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?

A. port mapping
B. server monitoring
C. client probing
D. XFF headers

Answer: A

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-terminal-server-users

NEW QUESTION 57
Which feature can be configured on VM-Series firewalls?

A. aggregate interfaces
B. machine learning
C. multiple virtual systems
D. GlobalProtect

Answer: D

NEW QUESTION 58
A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.
How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

NEW QUESTION 59
Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)

A. Verify AutoFocus status using CLI.
B. Check the WebUI Dashboard AutoFocus widget.
C. Check for WildFire forwarding logs.
D. Check the license
E. Verify AutoFocus is enabled below Device Management tab.

Answer: BD

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence

NEW QUESTION 62
Which DoS protection mechanism detects and prevents session exhaustion attacks?

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

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

NEW QUESTION 67
Which two subscriptions are available when configuring panorama to push dynamic updates to connected devices? (Choose two.)

A. Content-ID
B. User-ID
C. Applications and Threats
D. Antivirus

Answer: CD

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-dynamic-updates

NEW QUESTION 70
Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)

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

Answer: ADF

NEW QUESTION 74
What is exchanged through the HA2 link?

A. hello heartbeats
B. User-ID information
C. session synchronization
D. HA state information

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links

NEW QUESTION 77
Which prerequisite must be satisfied before creating an SSH proxy Decryption policy?

A. Both SSH keys and SSL certificates must be generated.
B. No prerequisites are required.
C. SSH keys must be manually generated.
D. SSL certificates must be generated.

Answer: B

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssh-proxy

NEW QUESTION 80
Which three authentication factors does PAN-OS® software support for MFA (Choose three.)

A. Push
B. Pull
C. Okta Adaptive
D. Voice E.SMS

Answer: ADE

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication

NEW QUESTION 81
VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A. Zone Protection
B. Replay
C. Web Application
D. DoS Protection

Answer: A

NEW QUESTION 86
An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.
What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Dependencies : Before upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS Upgrade. Reference: https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS- Upgrade/ta-p/111045

NEW QUESTION 88
Which four NGFW multi-factor authentication factors are supported by PAN-OSS? (Choose four.)

A. User logon
B. Short message service
C. Push
D. SSH keyE.One-Time Password F.Voice

Answer: BCEF

NEW QUESTION 89
Which is the maximum number of samples that can be submitted to WildFire per day, based on wildfire subscription?

A. 15,000
B. 10,000
C. 75,00
D. 5,000

Answer: B

NEW QUESTION 91
An administrator has configured a QoS policy rule and a QoS profile that limits the maximum allowable bandwidth for the YouTube application. However , YouTube is consuming more than the maximum bandwidth allotment configured.
Which configuration step needs to be configured to enable QoS?

A. Enable QoS Data Filtering Profile
B. Enable QoS monitor
C. Enable Qos interface
D. Enable Qos in the interface Management Profile.

Answer: C

NEW QUESTION 93
Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?

A. Client Probing
B. Port mapping
C. Server monitoring
D. Syslog listening

Answer: D

NEW QUESTION 94
What are the differences between using a service versus using an application for Security Policy match?

A. Use of a "service" enables the firewall to take action after enough packets allow for App-IDidentification
B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use ofan "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the portsbeing used.
C. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use ofa friendly application name instead of port numbers.
D. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port number
E. Use ofan "application" allows the firewall to take immediate action it the port being used is a member of the application standardport list

Answer: B

NEW QUESTION 95
In which two types of deployment is active/active HA configuration supported? (Choose two.)

A. TAP mode
B. Layer 2 mode
C. Virtual Wire mode
D. Layer 3 mode

Answer: CD

NEW QUESTION 96
A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial of-service attacks.
How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
B. Add QoS Profiles to throttle incoming requests
C. Add a tuned DoS Protection Profile
D. Add an Anti-Spyware Profile to block attacking IP address

Answer: C

NEW QUESTION 99
Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

A. System log
B. CPU Utilization widget
C. Resources widget
D. System Utilization log

Answer: C

NEW QUESTION 104
Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

A. Dynamic
B. Custom Panorama Admin
C. Role Based
D. Device Group E.Template Admin

Answer: DE

NEW QUESTION 105
Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.

A. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:“intrazone”
B. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:“intrazone” or “universal”
C. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:“intrazone” or “universal”
D. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:“intrazone”

Answer: B

NEW QUESTION 110
Which three fields can be included in a pcap filter? (Choose three)

A. Egress interface
B. Source IP
C. Rule number
D. Destination IP
E. Ingress interface

Answer: BCD

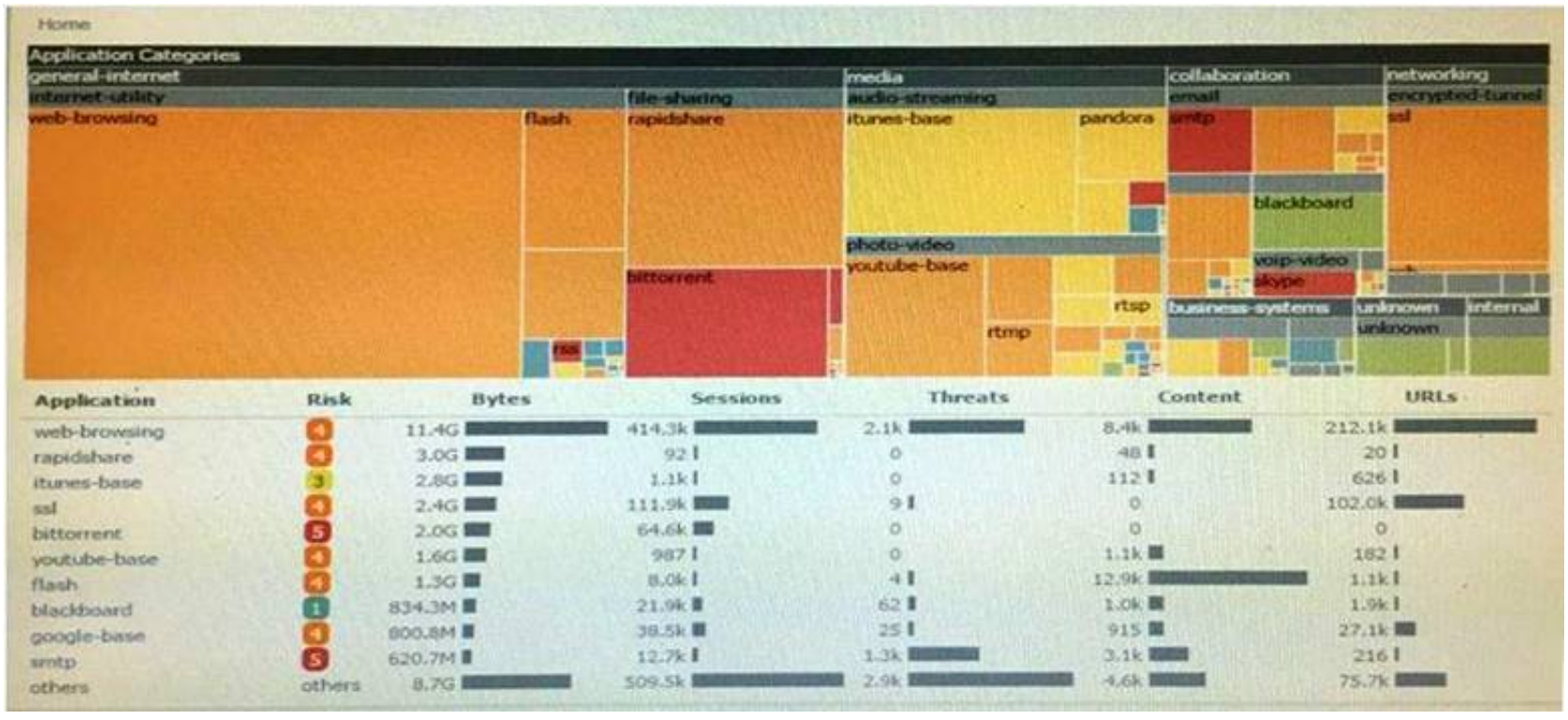
Explanation:
(https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta- p/72069)

NEW QUESTION 113
A company hosts a publically accessible web server behind a Palo Alto Networks next generation firewall with the following configuration information.
Users outside the company are in the "Untrust-L3" zone The web server physically resides in the "Trust-L3" zone. Web server public IP address: 23.54.6.10
Web server private IP address: 192.168.1.10
Which two items must be NAT policy contain to allow users in the untrust-L3 zone to access the web server? (Choose two)

A. Untrust-L3 for both Source and Destination zone
B. Destination IP of 192.168.1.10
C. Untrust-L3 for Source Zone and Trust-L3 for Destination Zone
D. Destination IP of 23.54.6.10

Answer: CD

NEW QUESTION 117
Click the Exhibit button



An administrator has noticed a large increase in bittorrent activity. The administrator wants to determine where the traffic is going on the company.
What would be the administrator's next step?

A. Right-Click on the bittorrent link and select Value from the context menu
B. Create a global filter for bittorrent traffic and then view Traffic logs.
C. Create local filter for bittorrent traffic and then view Traffic logs.
D. Click on the bittorrent application link to view network activity

Answer: D

NEW QUESTION 118
Which client software can be used to connect remote Linux client into a Palo Alto Networks Infrastructure without sacrificing the ability to scan traffic and protect against threats?

A. X-Auth IPsec VPN
B. GlobalProtect Apple IOS
C. GlobalProtect SSL
D. GlobalProtect Linux

Answer: A

Explanation:
(http://blog.webernetz.net/2014/03/31/palo-alto-globalprotect-for-linux-with-vpnc/)

NEW QUESTION 120
A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and post.
Which option when enabled with the correction threshold would mitigate this attack without dropping legitirnate traffic to other hosts insides the network?

A. Zone Protection Policy with UDP Flood Protection
B. QoS Policy to throttle traffic below maximum limit
C. Security Policy rule to deny trafic to the IP address and port that is under attack
D. Classified DoS Protection Policy using destination IP only with a Protect action

Answer: D

NEW QUESTION 123
Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.
D. Enter the command logger-mode enable the enter Y to confirm the change to Log Collector mode.
E. Log in the Panorama CLI of the dedicated Log Collector

Answer: BE

Explanation:
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance)

NEW QUESTION 127
Palo Alto Networks maintains a dynamic database of malicious domains.
Which two Security Platform components use this database to prevent threats? (Choose two)

A. Brute-force signatures
B. BrightCloud Url Filtering
C. PAN-DB URL Filtering

D. DNS-based command-and-control signatures

Answer: CD

NEW QUESTION 132
A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?

A. Blocked Activity
B. Bandwidth Activity
C. Threat Activity
D. Network Activity

Answer: D

NEW QUESTION 135
A network administrator uses Panorama to push security polices to managed firewalls at branch offices. Which policy type should be configured on Panorama if the administrators at the branch office sites to override these products?

A. Pre Rules
B. Post Rules
C. Explicit Rules
D. Implicit Rules

Answer: A

NEW QUESTION 136
Which three function are found on the dataplane of a PA-5050? (Choose three)

A. Protocol Decoder
B. Dynamic routing
C. Management
D. Network Processing
E. Signature Match

Answer: BDE

NEW QUESTION 139
Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?

A. Disable Server Response Inspection
B. Apply an Application Override
C. Disable HIP Profile
D. Add server IP Security Policy exception

Answer: A

NEW QUESTION 144
A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

A. DHCP has been set to Auto.
B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.
C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.
D. DNS has not been properly configured on the firewall

Answer: B

NEW QUESTION 146
Which interface configuration will accept specific VLAN IDs?

A. Tab Mode
B. Subinterface
C. Access Interface
D. Trunk Interface

Answer: B

NEW QUESTION 147
A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

A. The two devices must share a routable floating IP address
B. The two devices may be different models within the PA-5000 series
C. The HA1 IP address from each peer must be on a different subnet
D. The management port may be used for a backup control connection

Answer: D

NEW QUESTION 151
Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?

A. VM-100
B. VM-200
C. VM-1000-HV
D. VM-300

Answer: C

NEW QUESTION 153
A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations.
How should this be accomplished?

A. Create a Template with the appropriate IKE Gateway settings
B. Create a Template with the appropriate IPSec tunnel settings
C. Create a Device Group with the appropriate IKE Gateway settings
D. Create a Device Group with the appropriate IPSec tunnel settings

Answer: B

NEW QUESTION 158
Firewall administrators cannot authenticate to a firewall GUI.
Which two logs on that firewall will contain authentication-related information useful in troubleshooting this issue? (Choose two.)

A. ms log
B. authd log
C. System log
D. Traffic log
E. dp-monitor .log

Answer: BC

NEW QUESTION 160
What are two prerequisites for configuring a pair of Palo Alto Networks firewalls in an active/passive High Availability (HA) pair? (Choose two.)

A. The firewalls must have the same set of licenses.
B. The management interfaces must to be on the same network.
C. The peer HA1 IP address must be the same on both firewalls.
D. HA1 should be connected to HA1. Either directly or with an intermediate Layer 2 device.

Answer: AD

NEW QUESTION 161
People are having intermittent quality issues during a live meeting via web application.

A. Use QoS profile to define QoS Classes
B. Use QoS Classes to define QoS Profile
C. Use QoS Profile to define QoS Classes and a QoS Policy
D. Use QoS Classes to define QoS Profile and a QoS Policy

Answer: C

NEW QUESTION 164
Several offices are connected with VPNs using static IPV4 routes. An administrator has been tasked with implementing OSPF to replace static routing.
Which step is required to accoumplish this goal?

A. Assign an IP address on each tunnel interface at each site
B. Enable OSPFv3 on each tunnel interface and use Area ID 0.0.0.0
C. Assign OSPF Area ID 0.0.0.0 to all Ethernet and tunnel interfaces
D. Create new VPN zones at each site to terminate each VPN connection

Answer: C

NEW QUESTION 166
A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.
What can be done to simplify the NAT policy?

A. Configure ECMP to handle matching NAT traffic
B. Configure a NAT Policy rule with Dynamic IP and Port
C. Create a new Source NAT Policy rule that matches the existing traffic and enable the Bi-directional option

D. Create a new Destination NAT Policy rule that matches the existing traffic and enable the Bi- directional option

Answer: C

Explanation:
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-configuration-examples

NEW QUESTION 171
Which CLI command displays the current management plan memory utilization?

A. > show system info
B. > show system resources
C. > debug management-server show
D. > show running resource-monitor

Answer: B

Explanation:
https://live.paloaltonetworks.comHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of-9999/ta-p/58149"/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of- 9999/ta-p/58149

NEW QUESTION 176
When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinhole enabled, generating a traffic log.
What will be the destination IP Address in that log entry?

A. The IP Address of sinkhole.paloaltonetworks.com
B. The IP Address of the command-and-control server
C. The IP Address specified in the sinkhole configuration
D. The IP Address of one of the external DNS servers identified in the anti-spyware database

Answer: C

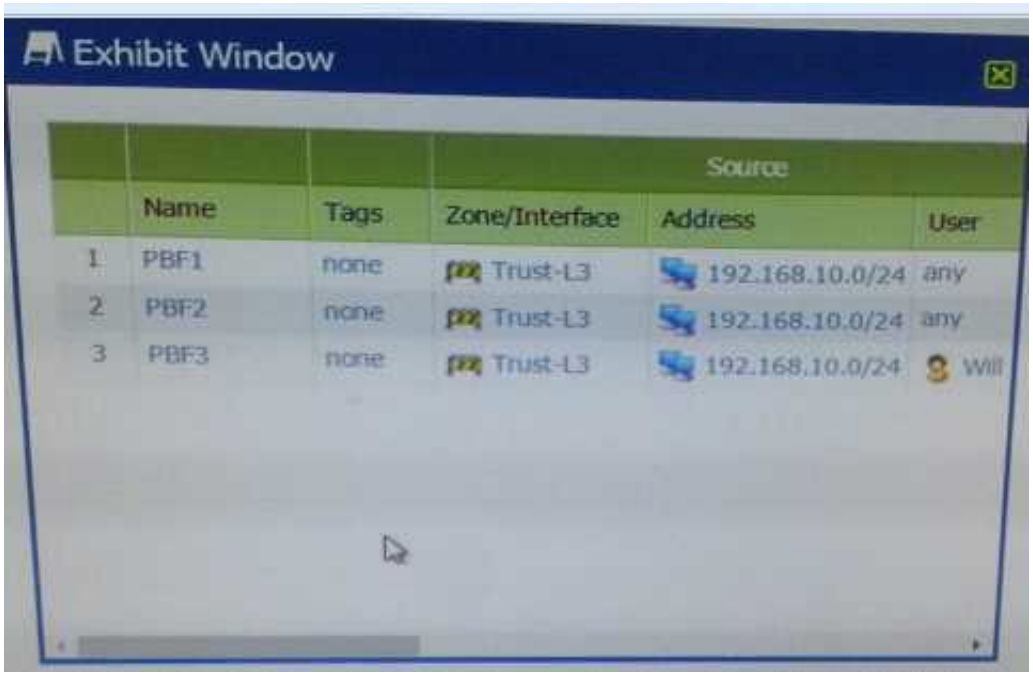
Explanation:
https://live.paloaltonetworks.com/t5/MaHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function- is-Working/ta-p/65864"naHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864"gement-Articles/How-to- Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864

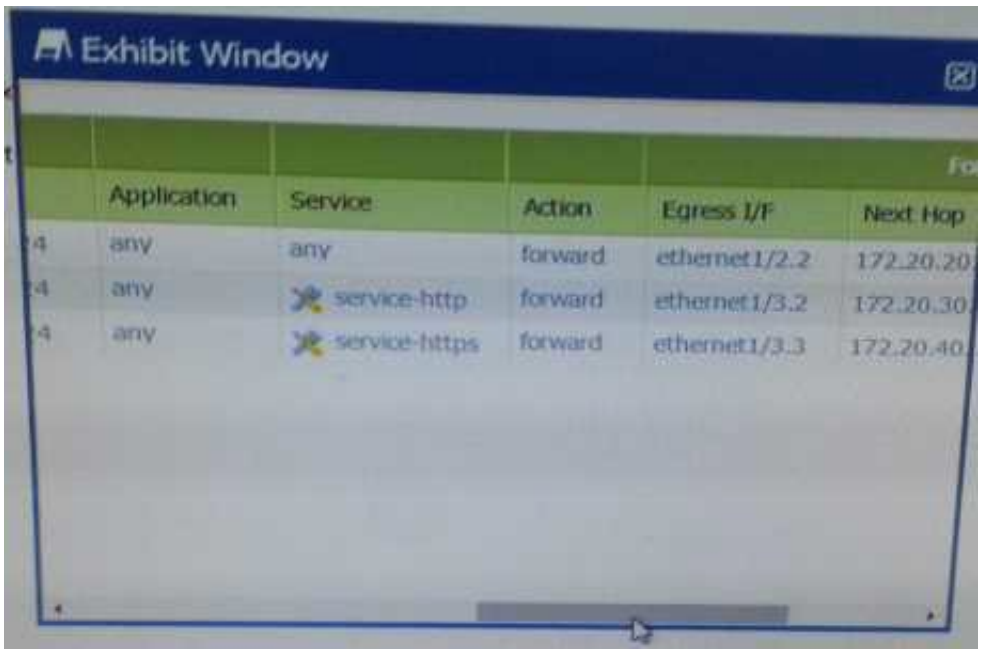
NEW QUESTION 179
A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:
* Users outside the company are in the "Untrust-L3" zone.
* The web server physically resides in the "Trust-L3" zone.
* Web server public IP address: 23.54.6.10
* Web server private IP address: 192.168.1.10
Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

A. Destination IPof 23.54.6.10
B. UntrustL3 for both Source and Destination Zone
C. Destination IP of 192.168.1.10
D. UntrustL3 for Source Zone and Trust-L3 for Destination Zone

Answer: AB

NEW QUESTION 182
Refer to Exhibit:





A firewall has three PDF rules and a default route with a next hop of 172.29.19.1 that is configured in the default VR. A user named XX-bes a PC with a 192.168.101.10 IP address.
He makes an HTTPS connection to 172.16.10.29.
What is the next hop IP address for the HTTPS traffic from Wills PC.

A. 172.20.30.1
B. 172.20.20.1
C. 172.20.10.1
D. 172.20.40.1

Answer: B

NEW QUESTION 183
Which two actions are required to make Microsoft Active Directory users appear in a firewall traffic log? (Choose two.)

A. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions
B. Enable User-ID on the zone object for the destination zone
C. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
D. Enable User-ID on the zone object for the source zone
E. Configure a RADIUS server profile to point to a domain controller

Answer: AD

NEW QUESTION 187
Site-A and Site-B need to use IKEv2 to establish a VPN connection. Site A connects directly to the internet using a public IP address. Site-B uses a private IP address behind an ISP router to connect to the internet.
How should NAT Traversal be implemented for the VPN connection to be established between Site-A and Site-B?

A. Enable on Site-A only
B. Enable on Site-B only
C. Enable on Site-B only with passive mode
D. Enable on Site-A and Site-B

Answer: D

NEW QUESTION 188
YouTube videos are consuming too much bandwidth on the network, causing delays in mission- critical traffic. The administrator wants to throttle YouTube traffic.
The following interfaces and zones are in use on the firewall:
* ethernet1/1, Zone: Untrust (Internet-facing)
* ethernet1/2, Zone: Trust (client-facing)
A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS profile called Inbound.
Which setting for class 6 with throttle YouTube traffic?

A. Outbound profile with Guaranteed Ingress
B. Outbound profile with Maximum Ingress
C. Inbound profile with Guaranteed Egress
D. Inbound profile with Maximum Egress

Answer: D

NEW QUESTION 190
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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