Paloalto-Networks

Exam Questions PCNSE

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

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 2)
An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.
Which configuration will enable this HA scenario?

A. The two firewalls will share a single floating IP and will use gratuitous ARP to share the floating IP.
B. Each firewall will have a separate floating IP, and priority will determine which firewall has the primary IP.
C. The firewalls do not use floating IPs in active/active HA.
D. The firewalls will share the same interface IP address, and device 1 will use the floating IP if device 0 fails.

Answer: A

NEW QUESTION 2
- (Exam Topic 2)
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: BDE

NEW QUESTION 3
- (Exam Topic 2)
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 4
- (Exam Topic 2)
An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

A. Client Probing
B. Terminal Services agent
C. GlobalProtect
D. Syslog Monitoring

Answer: C

NEW QUESTION 5
- (Exam Topic 2)
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

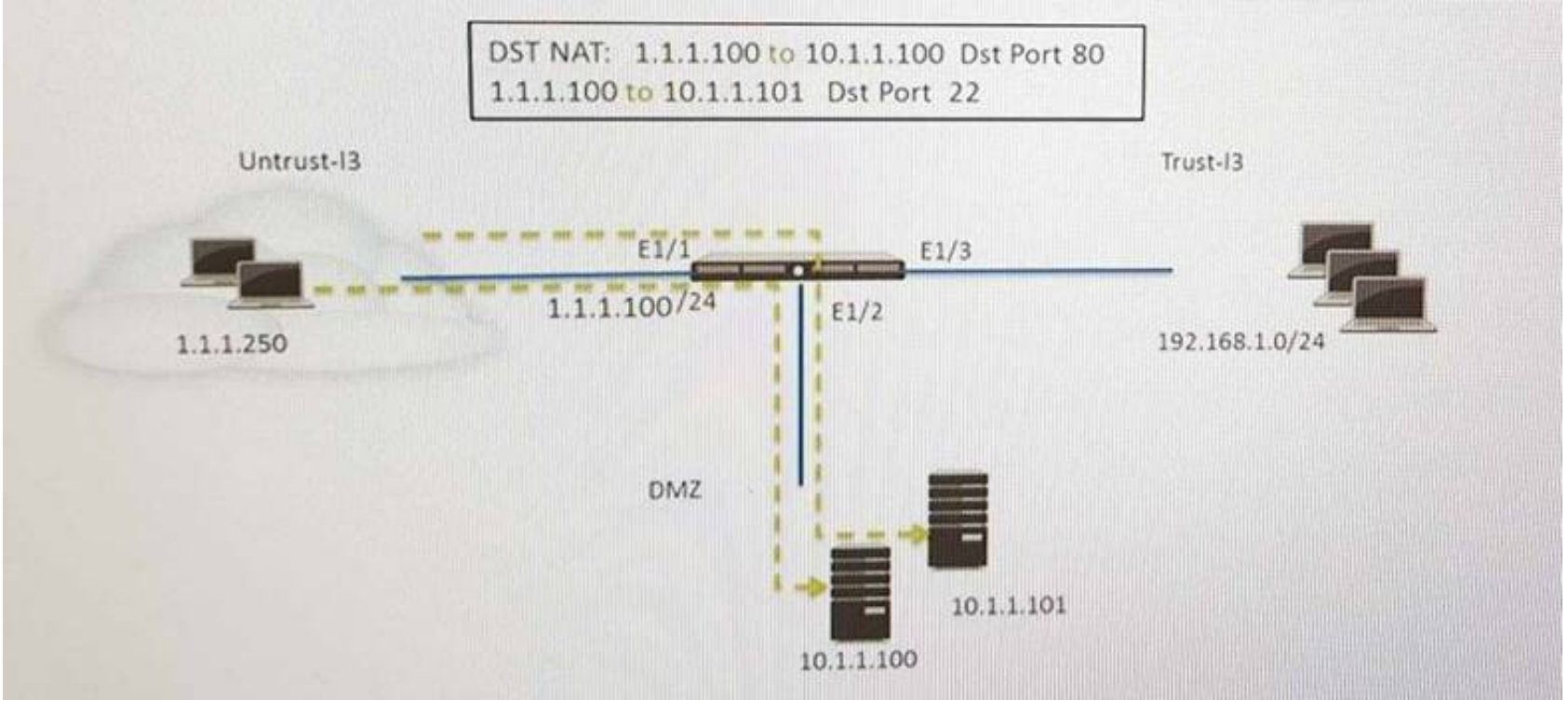
NEW QUESTION 6
- (Exam Topic 2)
A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server.
Which solution in PAN-OS® software would help in this case?

A. application override
B. Virtual Wire mode
C. content inspection
D. redistribution of user mappings

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-net

NEW QUESTION 7
- (Exam Topic 2)
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) received 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) Ssh-Allow
B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
D. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

Answer: CD

NEW QUESTION 8
- (Exam Topic 2)
An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router. Which two options enable the administrator to troubleshoot this issue? (Choose two.)

A. View Runtime Stats in the virtual router.
B. View System logs.
C. Add a redistribution profile to forward as BGP updates.
D. Perform a traffic pcap at the routing stage.

Answer: AB

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC

NEW QUESTION 9
- (Exam Topic 2)
Which item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

A. ACC
B. System Logs
C. App Scope
D. Session Browser

Answer: D

NEW QUESTION 10
- (Exam Topic 2)
An administrator sees several inbound sessions identified as unknown-tcp in the traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this as their accounting application and to scan this traffic for threats. Which option would achieve this result?

A. Create an Application Override policy and a custom threat signature for the application
B. Create an Application Override policy
C. Create a custom App-ID and use the "ordered conditions" check box
D. Create a custom App ID and enable scanning on the advanced tab

Answer: D

NEW QUESTION 10
- (Exam Topic 2)
A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously

being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg txi in the USB flash drive are as follows:

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

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

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

Answer: C

NEW QUESTION 11
- (Exam Topic 2)
Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

A. Configure a Decryption Profile and select SSL/TLS services.
B. Set up SSL/TLS under Polices > Service/URL Category>Service.
C. Set up Security policy rule to allow SSL communication.
D. Configure an SSL/TLS Profile.

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-mana ssltls-service-profile

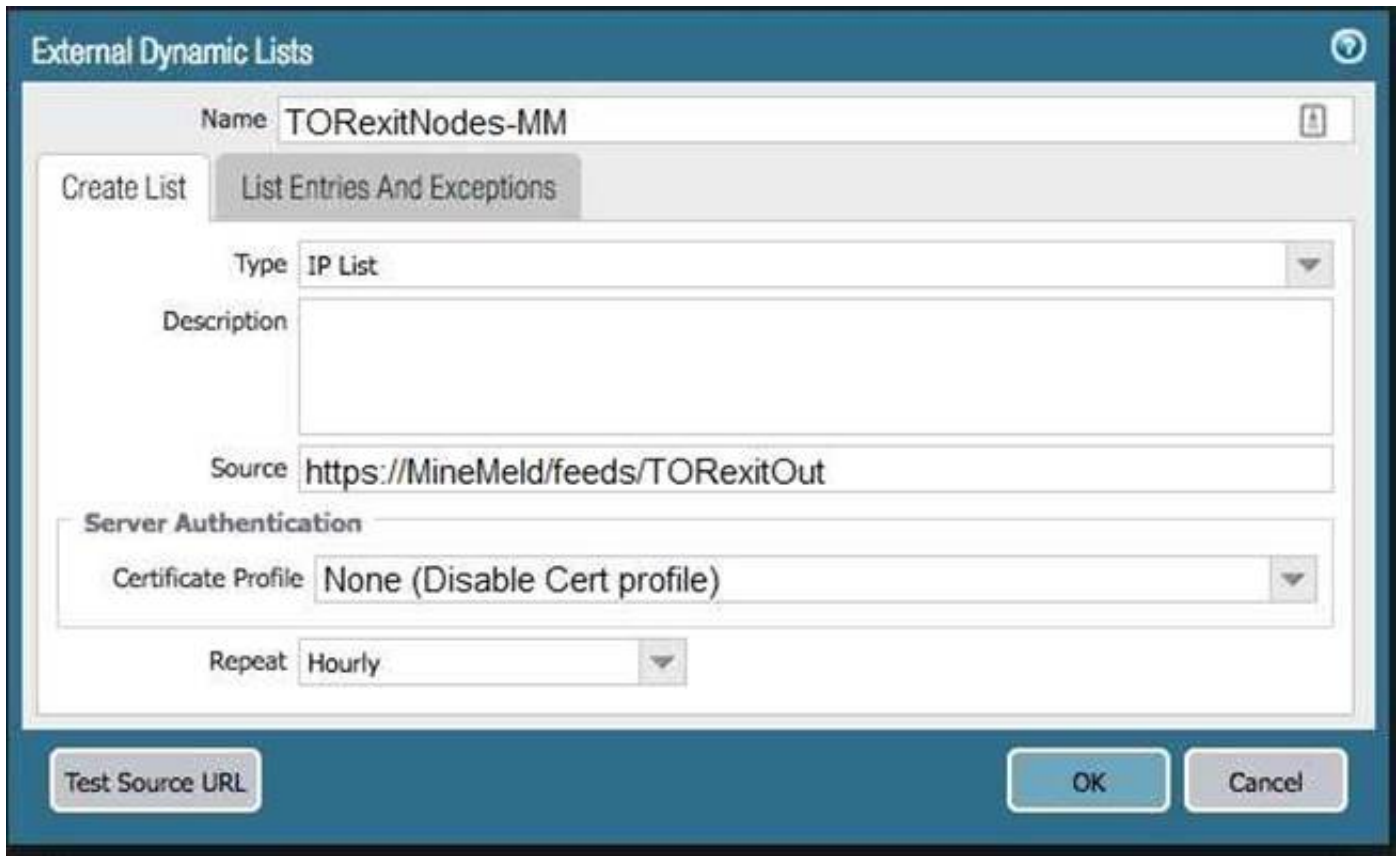
NEW QUESTION 12
- (Exam Topic 2)
Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

A. Red Hat Enterprise Virtualization (RHEV)
B. Kernel Virtualization Module (KVM)
C. Boot Strap Virtualization Module (BSVM)
D. Microsoft Hyper-V

Answer: BD

Explanation:
Reference:
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series
docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-deploy

NEW QUESTION 17
- (Exam Topic 2)
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 18
- (Exam Topic 2)
SD-WAN is designed to support which two network topology types? (Choose two.)

A. ring
B. point-to-point
C. hub-and-spoke
D. full-mesh

Answer: CD

NEW QUESTION 22
- (Exam Topic 2)
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?

A. Custom application
B. System logs show an application error and neither signature is used.
C. Downloaded application
D. Custom and downloaded application signature files are merged and both are used

Answer: C

NEW QUESTION 26
- (Exam Topic 2)
If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect when users browse to HTTP(S) websites?

A. SSL Forward Proxy
B. SSL Inbound Inspection
C. TLS Bidirectional proxy
D. SSL Outbound Inspection

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClV8CAK

NEW QUESTION 30
- (Exam Topic 2)
Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two)

A. Successful GlobalProtect Connection Activity
B. Successful GlobalProtect Deployed Activity

C. GlobalProtect Quarantine Activity
D. GlobalProtect Deployment Activity

Answer: AC

NEW QUESTION 35
- (Exam Topic 2)
An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications DNS, SSL, and web-browsing.
The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application SSL.
Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

A. Create a decryption rule matching the encrypted BitTorrent traffic with action “No-Decrypt,” and place the rule at the top of the Decryption policy.
B. Create a Security policy rule that matches application “encrypted BitTorrent” and place the rule at the top of the Security policy.
C. Disable the exclude cache option for the firewall.
D. Create a Decryption Profile to block traffic using unsupported cyphers, and attach the profile to the decryption rule.

Answer: D

NEW QUESTION 38
- (Exam Topic 2)
On the NGFW. how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?

A. * 1.Select Device > Certificate Management > Certificates >Devace > Certificates* 2. Import the certificate.* 3 Select Import Private Key* 4 Click Generate to generate the new certificate
B. * 1 Select Device > Certificates * 2 Select Certificate Profile* 3 Generate the certificate* 4 Select Block Private Key Export.
C. * 1 Select Device > Certificates * 2 Select Certificate Profile.* 3 Generate the certificate* 4 Select Block Private Key Export
D. * 1 Select Device > Certificate Management > Certificates > Device > Certificates * 2 Generate the certificate* 3 Select Block Private Key Export* 4 Click Genet ale to generate the new certificate.

Answer: D

NEW QUESTION 42
- (Exam Topic 2)
When is the content inspection performed in the packet flow process?

A. after the application has been identified
B. before session lookup
C. before the packet forwarding process
D. after the SSL Proxy re-encrypts the packet

Answer: A

Explanation:
Reference:
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

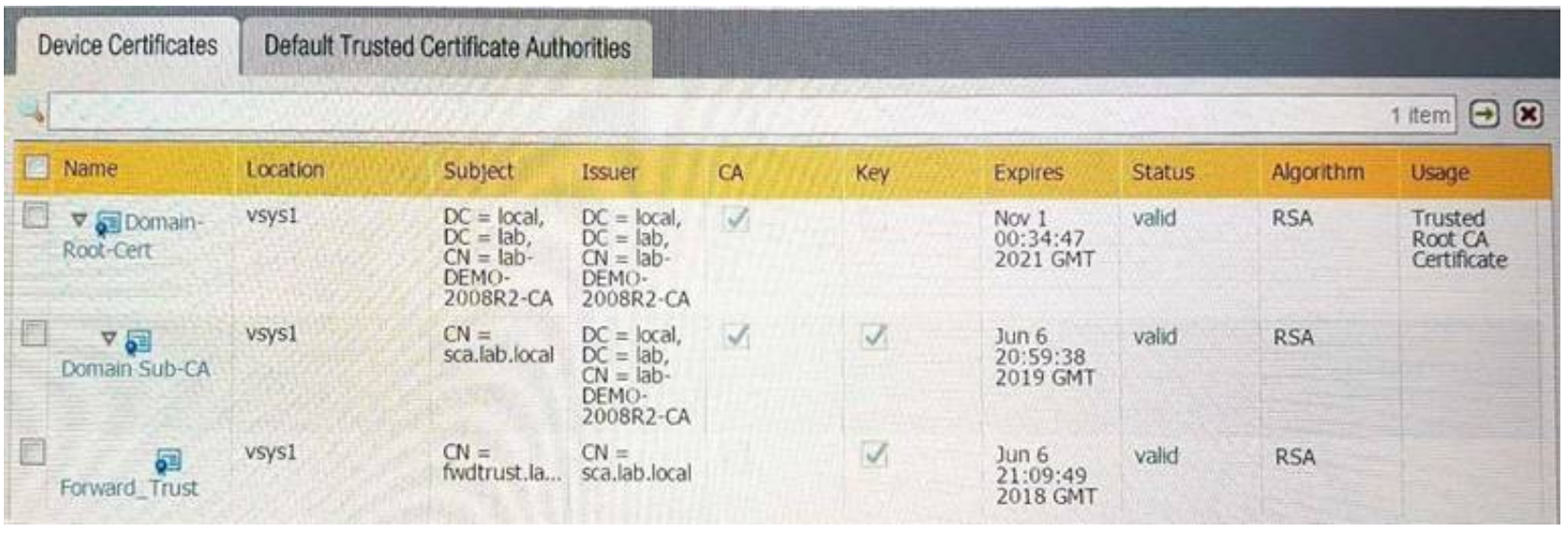
NEW QUESTION 44
- (Exam Topic 2)
Which CLI command enables an administrator to check the CPU utilization of the dataplane?

A. show running resource-monitor
B. debug data-plane dp-cpu
C. show system resources
D. debug running resources

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXwCAK

NEW QUESTION 45
- (Exam Topic 2)
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: B

NEW QUESTION 46
- (Exam Topic 2)
Updates to dynamic user group membership are automatic therefore using dynamic user groups instead of static group objects allows you to:

A. respond to changes in user behavior or potential threats using manual policy changes
B. respond to changes in user behavior or potential threats without automatic policy changes
C. respond to changes in user behavior and confirmed threats with manual policy changes
D. respond to changes in user behavior or potential threats without manual policy changes

Answer: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:tex

NEW QUESTION 49
- (Exam Topic 2)
An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:
•Firewall has Internet connectivity through e1/1.
•Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
•Service route is configured, sourcing update traffic from e1/1.
•A communication error appears in the System logs when updates are performed.
•Download does not complete.
What must be configured to enable the firewall to download the current version of PAN-OS software?

A. DNS settings for the firewall to use for resolution
B. scheduler for timed downloads of PAN-OS software
C. static route pointing application PaloAlto-updates to the update servers
D. Security policy rule allowing PaloAlto-updates as the application

Answer: D

NEW QUESTION 52
- (Exam Topic 2)
Which feature prevents the submission of corporate login information into website forms?

A. Data filtering
B. User-ID
C. File blocking
D. Credential phishing prevention

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-c
“Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose what websites you want to either allow, alert on, or block corporate credential submissions to based on the URL category of the website. Alternatively, you can present a page that warns users against submitting credentials to sites classified in certain URL categories. This gives you the opportunity to educate users against reusing corporate credentials, even on legitimate, non-phishing sites. In the event that corporate credentials are compromised, this feature allows you to identify the user who submitted credentials so that you can remediate.”

NEW QUESTION 54
- (Exam Topic 2)
A user’s traffic traversing a Palo Alto Networks NGFW sometimes can reach http://www.company.com. At other times the session times out. The NGFW has been

configured with a PBF rule that the user's traffic matches when it goes to http://www.company.com.
How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question:.
B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question.
C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFiCAK

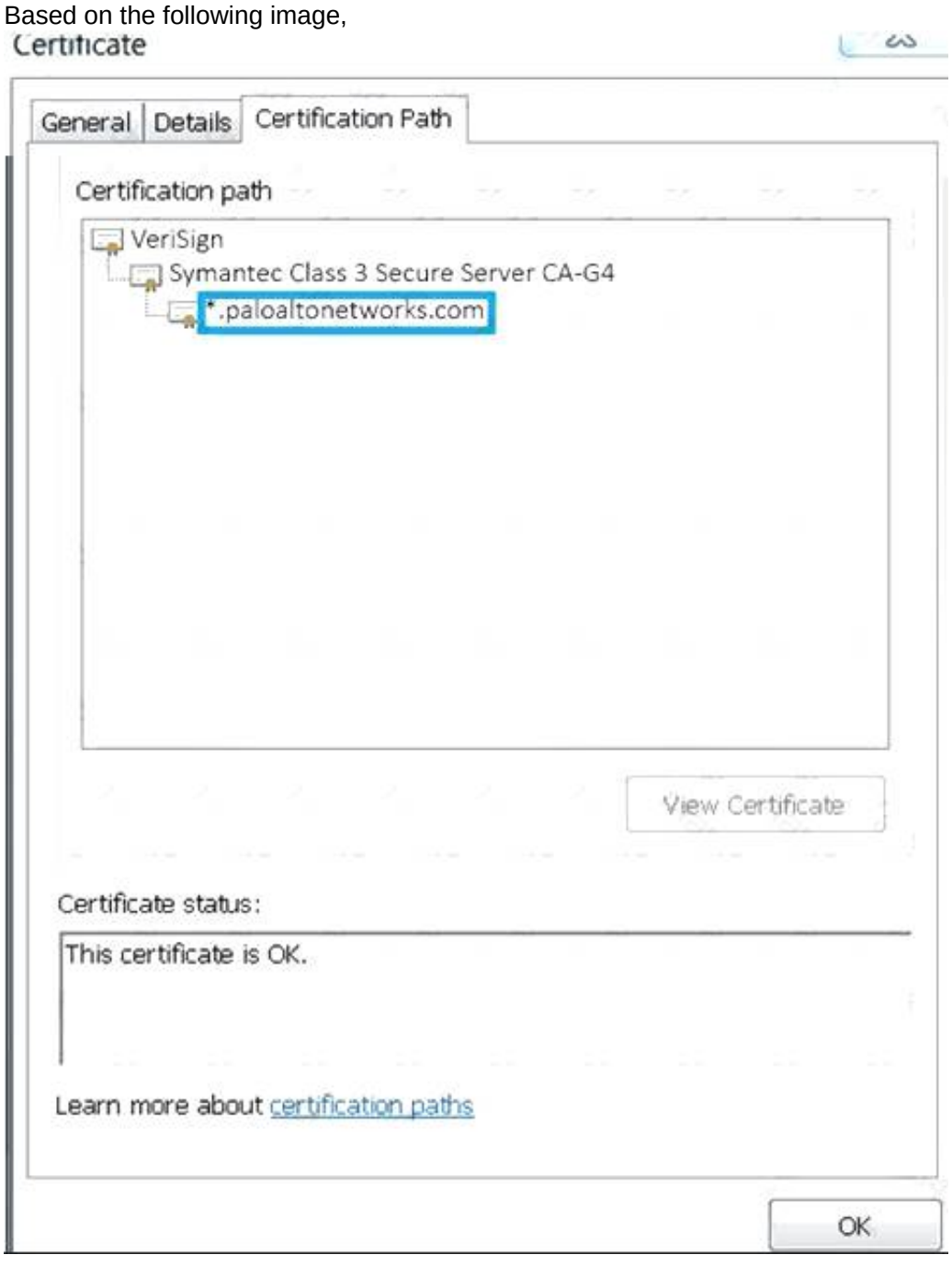
NEW QUESTION 57
- (Exam Topic 2)
Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

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

Answer: C

Explanation:
Reference: http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClQSCA0

NEW QUESTION 61
- (Exam Topic 2)
Based on the following image,



what is the correct path of root, intermediate, and end-user certificate?

A. Palo Alto Networks > Symantec > VeriSign
B. Symantec > VeriSign > Palo Alto Networks
C. VeriSign > Palo Alto Networks > Symantec
D. VeriSign > Symantec > Palo Alto Networks

Answer: B

NEW QUESTION 65
- (Exam Topic 2)
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: D

Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/set-up-site-to-site-vpn/set-up-an-ipsec

NEW QUESTION 69
- (Exam Topic 2)
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of reconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.
Which VPN configuration would adapt to changes when deployed to the future site?

A. Preconfigured GlobalProtect satellite
B. Preconfigured GlobalProtect client
C. Preconfigured IPsec tunnels
D. Preconfigured PPTP Tunnels

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect

NEW QUESTION 71
- (Exam Topic 2)
Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

A. User-logon (Always on)
B. At-boot
C. On-demand
D. Pre-logon

Answer: D

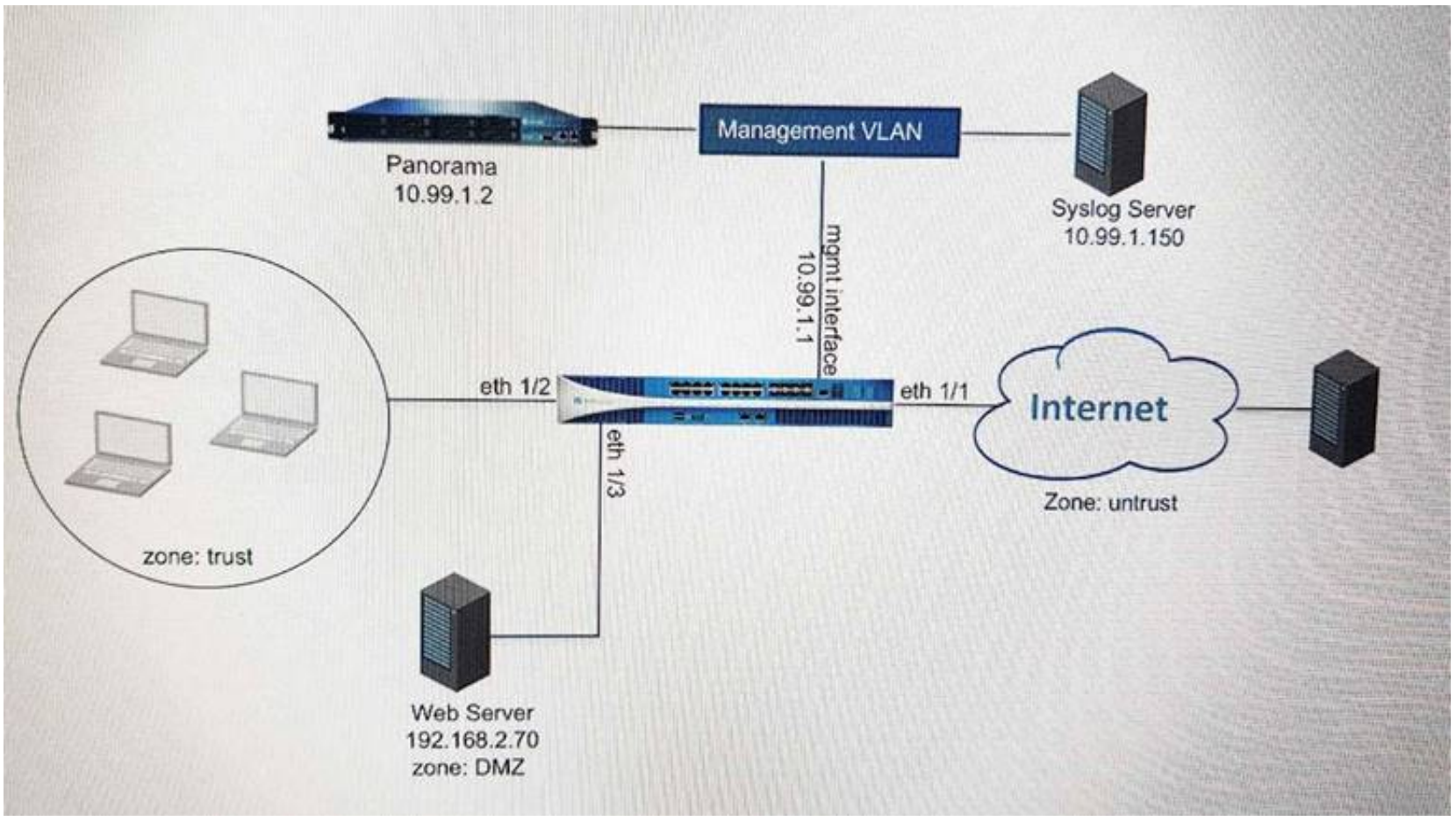
NEW QUESTION 75
- (Exam Topic 2)
Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a "No Decrypt" action? (Choose two.)

A. Block sessions with expired certificates
B. Block sessions with client authentication
C. Block sessions with unsupported cipher suites
D. Block sessions with untrusted issuers
E. Block credential phishing

Answer: AD

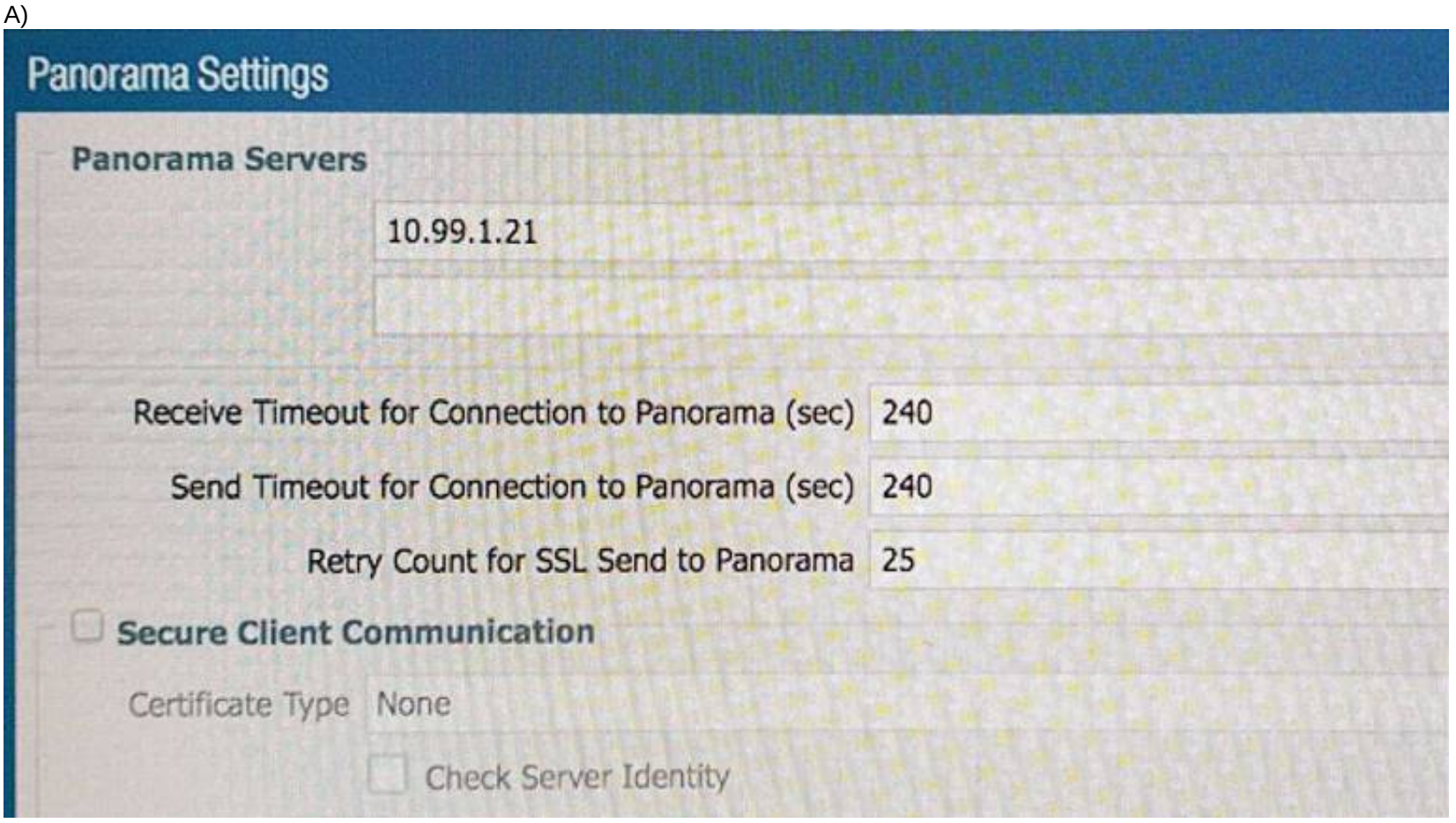
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-decryption-exception

NEW QUESTION 80
- (Exam Topic 2)
Refer to the exhibit.

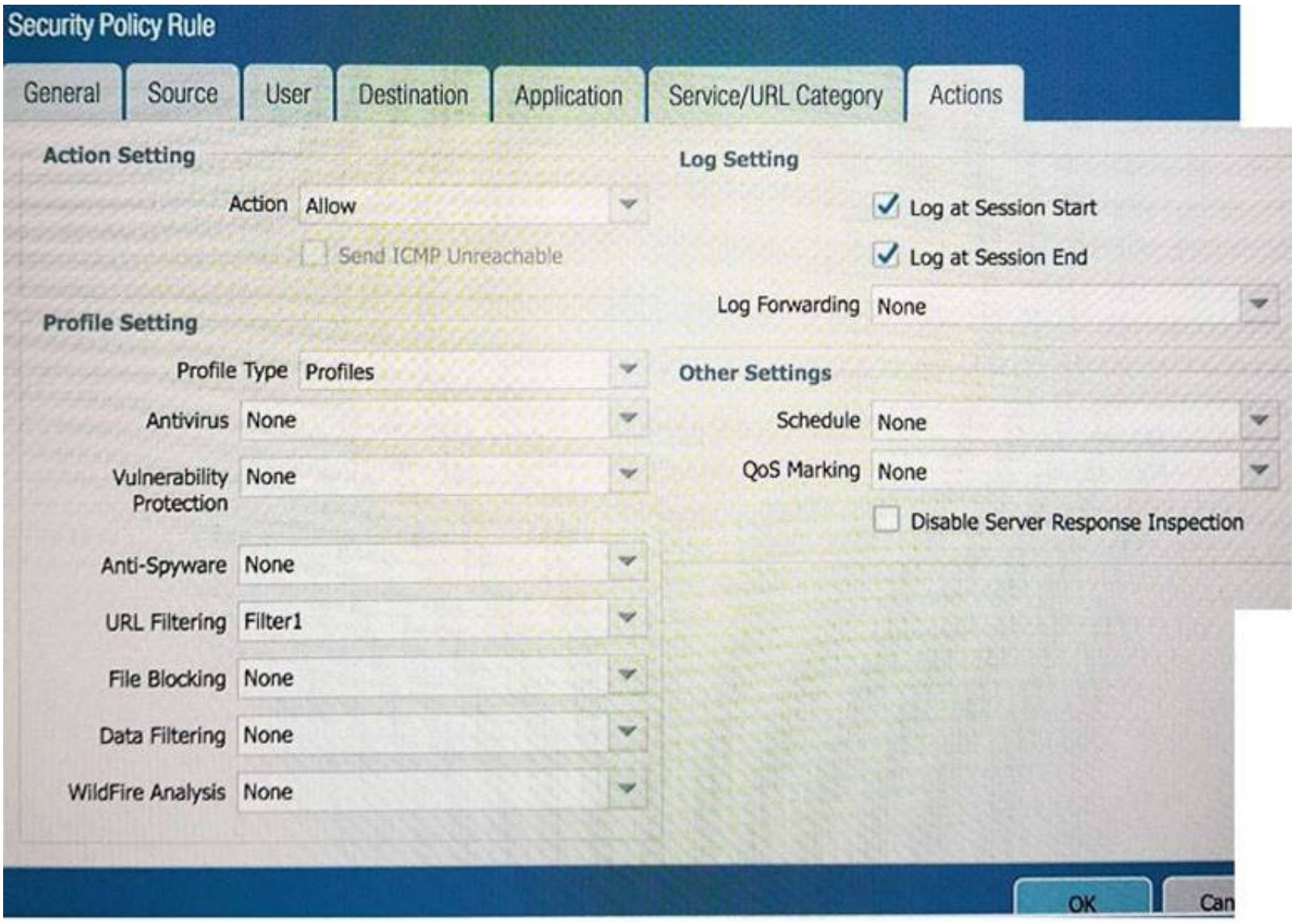


An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side. Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?

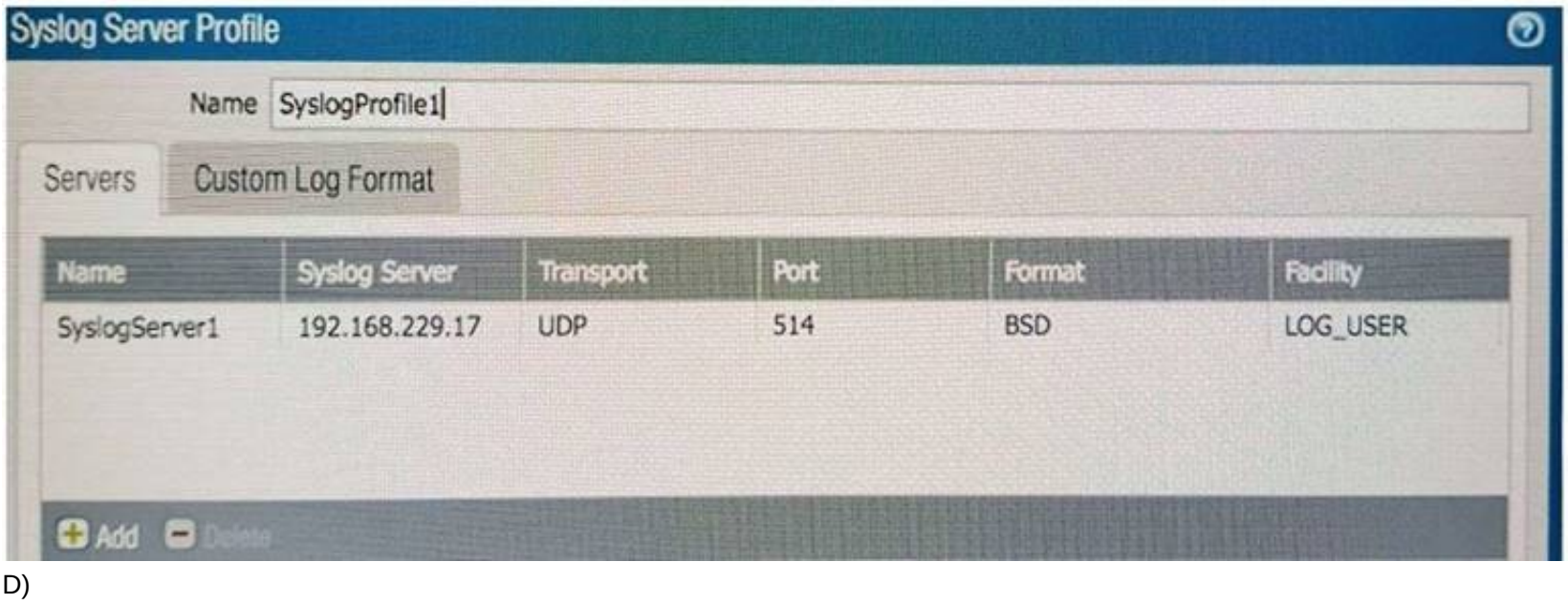
A)



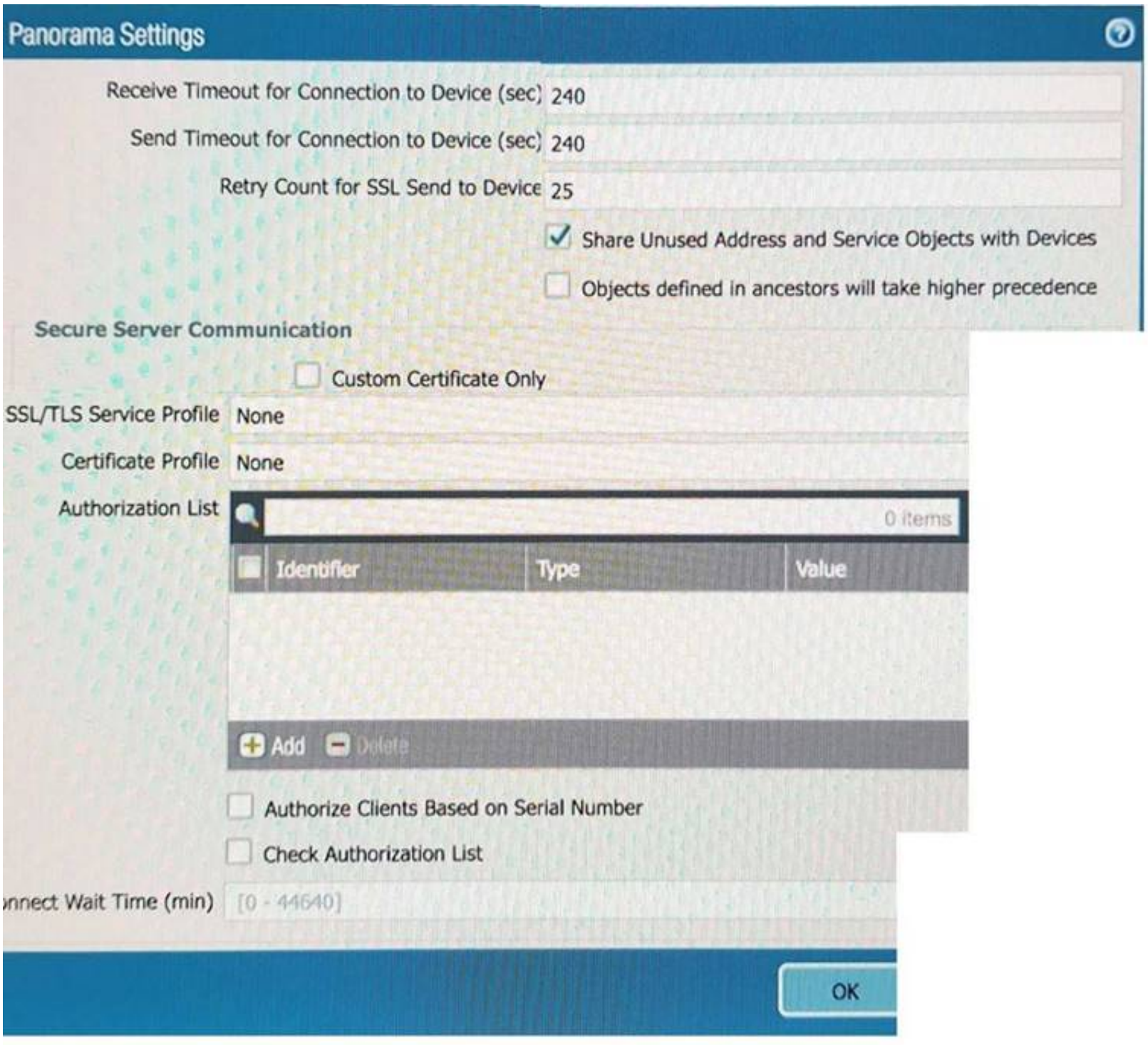
B)


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: A

Explanation:
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-log-collection/configure-log-forward

NEW QUESTION 85
- (Exam Topic 2)
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.
Which option would achieve this result?

A. Create a custom App-ID and enable scanning on the advanced tab.
B. Create an Application Override policy.
C. Create a custom App-ID and use the "ordered conditions" check box.
D. Create an Application Override policy and custom threat signature for the application.

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRoCAK

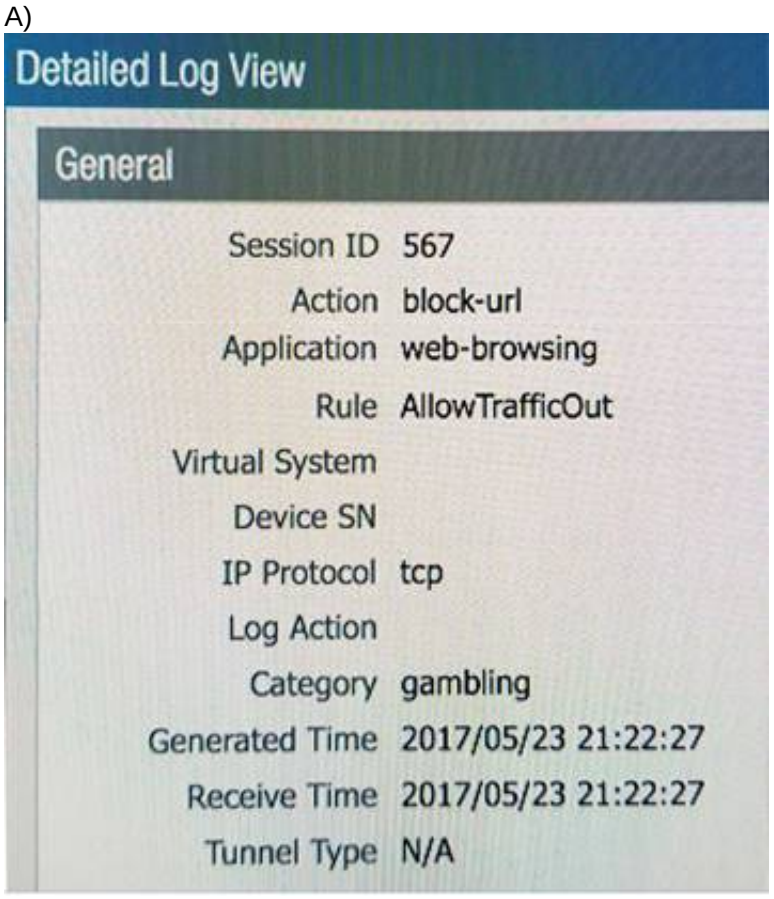
NEW QUESTION 89
- (Exam Topic 2)
Which Captive Portal mode must be configured to support MFA authentication?

A. NTLM
B. Redirect
C. Single Sign-On
D. Transparent

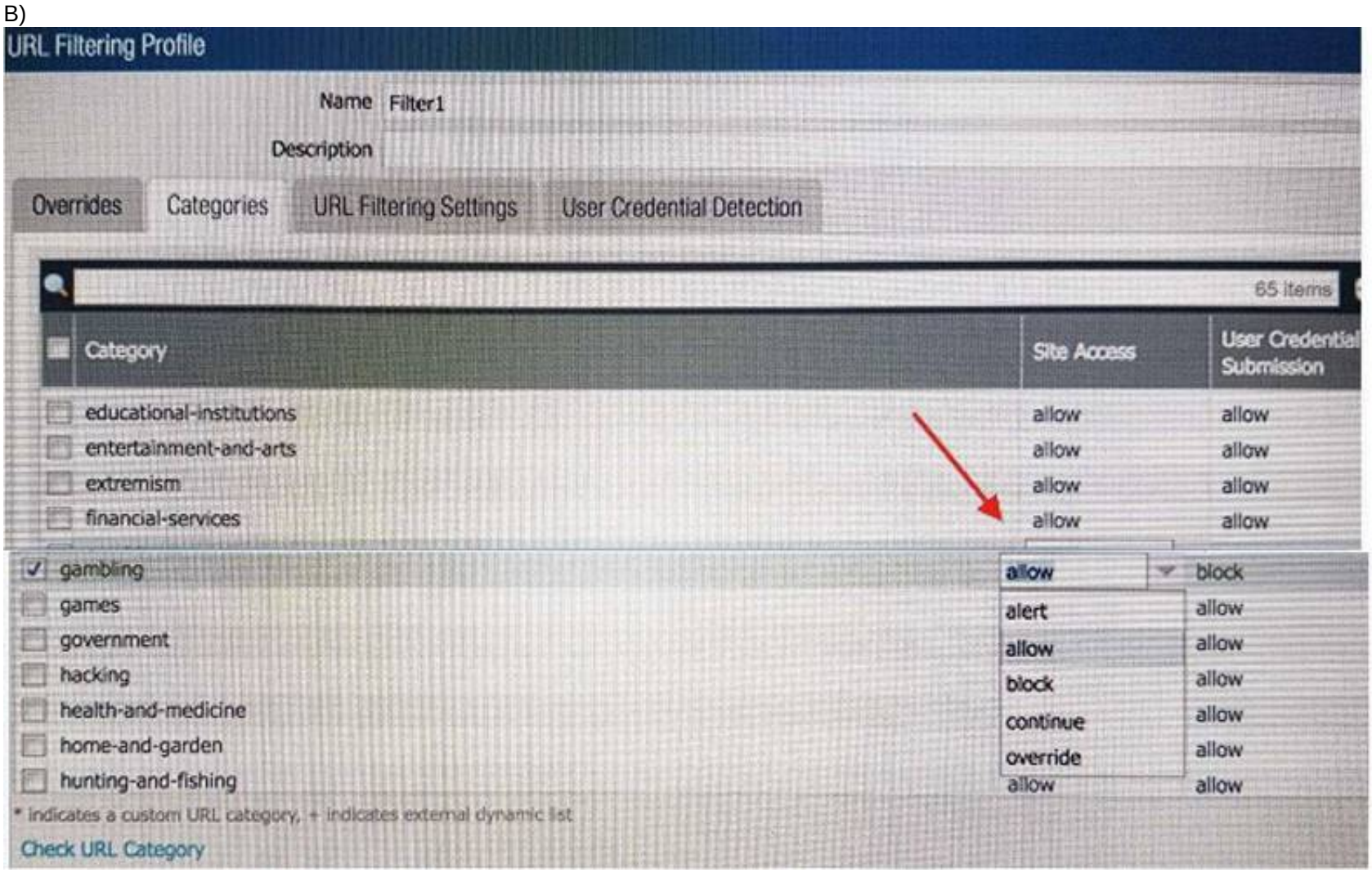
Answer: B

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

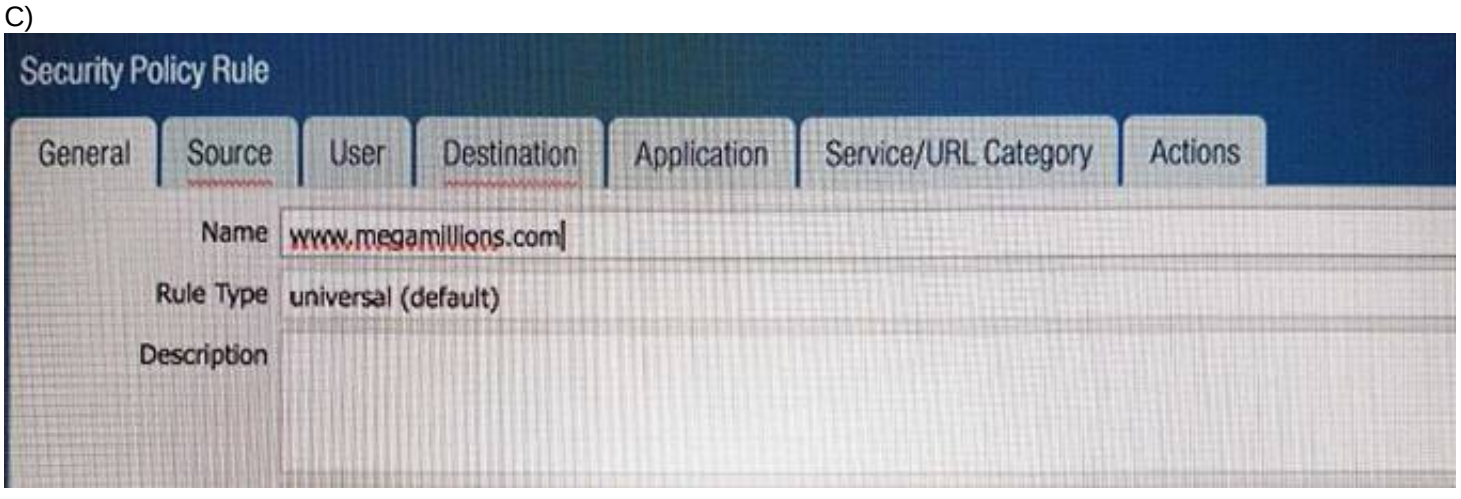
NEW QUESTION 94
- (Exam Topic 2)
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.
Which configuration change should the administrator make?
A)



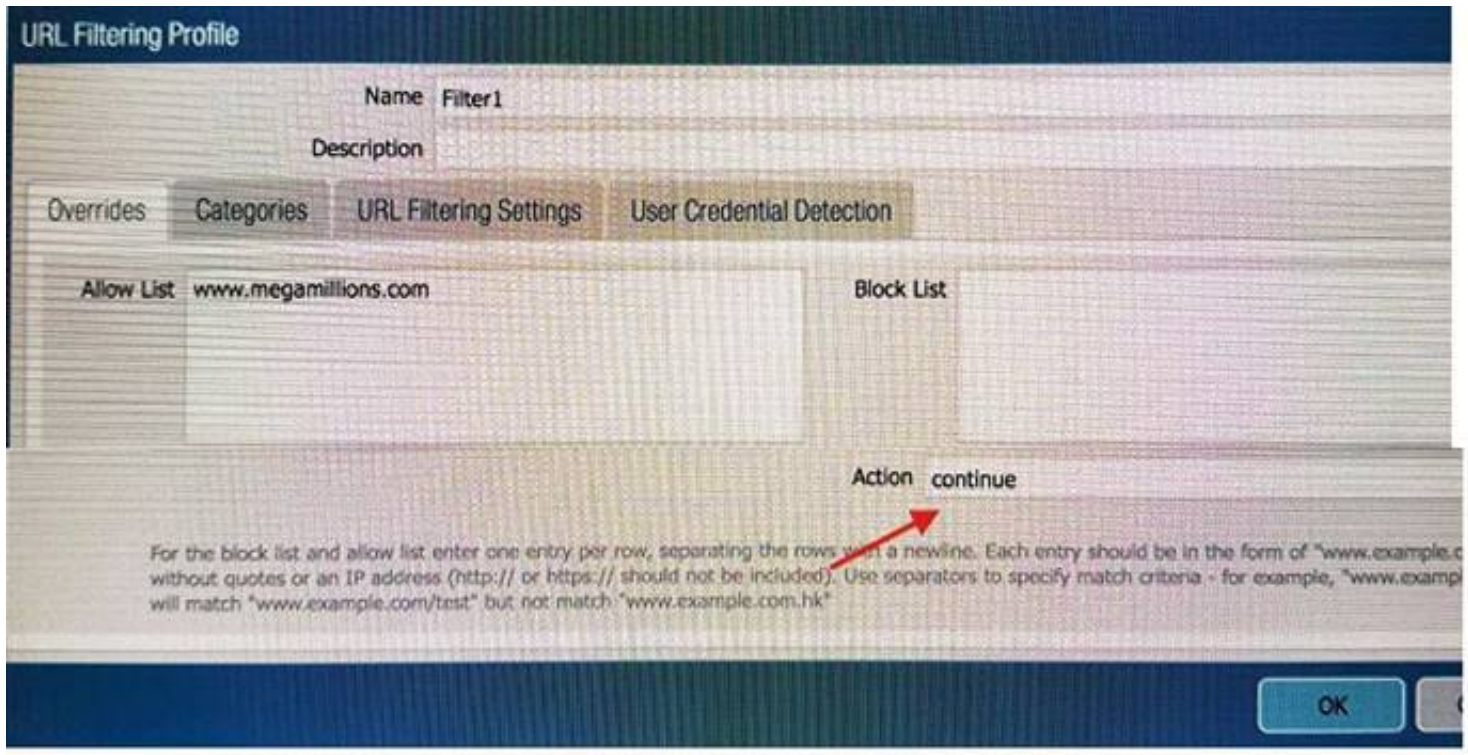
B)



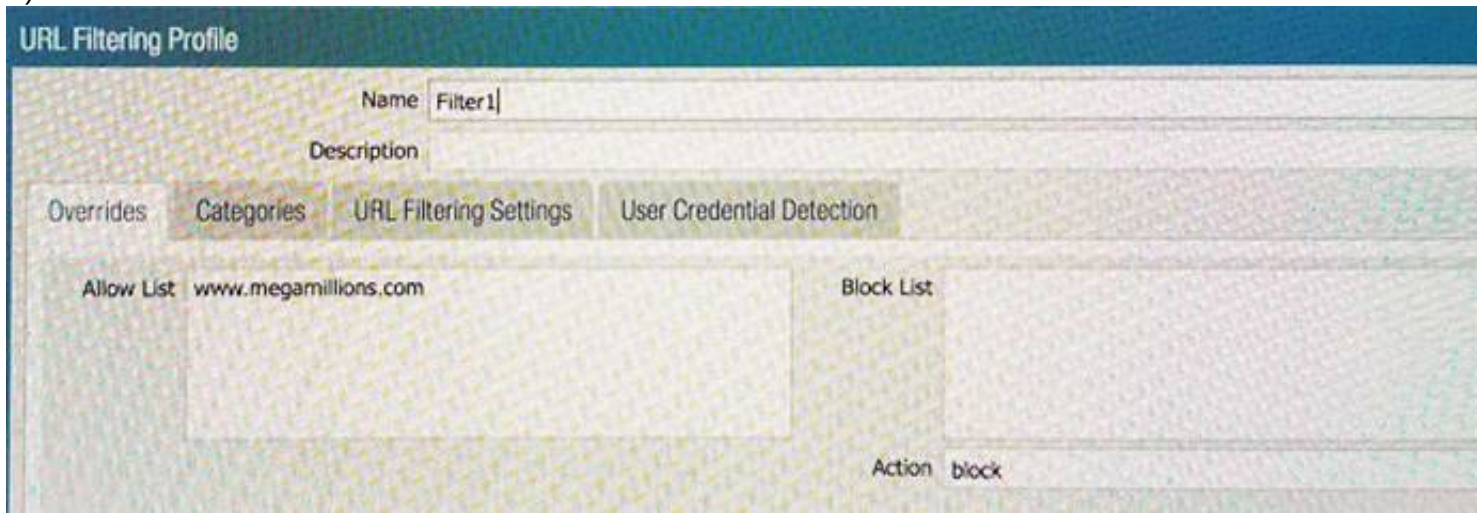
C)



D)



E)



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

Answer: B

NEW QUESTION 97
- (Exam Topic 2)
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

Explanation:
We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted. Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS

NEW QUESTION 102
- (Exam Topic 2)
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

Explanation:
To obtain user mappings from existing network services that authenticate users—such as wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms—Configure User-ID to Monitor Syslog Senders for User Mapping.While you can configure either the Windows agent or the PAN-OS integrated User-ID agent on the firewall to listen for authentication syslog messages from the network services, because only the PAN-OS integrated agent supports syslog listening over TLS, it is the preferred configuration.

NEW QUESTION 104
- (Exam Topic 2)
In the following image from Panorama, why are some values shown in red?

Device Name	Logging Rate (Log/sec)	Device	Session
		Throughput (KB/sec)	Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

A. sg2 session count is the lowest compared to the other managed devices.
B. us3 has a logging rate that deviates from the administrator-configured thresholds.
C. uk3 has a logging rate that deviates from the seven-day calculated baseline.
D. sg2 has misconfigured session thresholds.

Answer: A

NEW QUESTION 105
- (Exam Topic 2)
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 110
- (Exam Topic 2)
Which three firewall states are valid? (Choose three.)

A. Active
B. Functional
C. Pending
D. Passive
E. Suspended

Answer: ADE

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states

NEW QUESTION 115
- (Exam Topic 2)
Which logs enable a firewall administrator to determine whether a session was decrypted?

A. Correlated Event
B. Traffic
C. Decryption
D. Security Policy

Answer: B

NEW QUESTION 116
- (Exam Topic 1)
An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed
Which Panorama tool can help this organization?

A. Config Audit
B. Policy Optimizer
C. Application Groups
D. Test Policy Match

Answer: A

NEW QUESTION 120
- (Exam Topic 1)
A variable name must start with which symbol?

A. $
B. &
C. !
D. #

Answer: A

Explanation:
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-firewalls/manage-templates-and-tem

NEW QUESTION 125
- (Exam Topic 1)
Which statement accurately describes service routes and virtual systems?

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

Answer: A

NEW QUESTION 128
- (Exam Topic 1)
When setting up a security profile which three items can you use? (Choose three)

A. Wildfire analysis
B. anti-ransom ware
C. antivirus
D. URL filtering
E. decryption profile

Answer: ACD

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION 130
- (Exam Topic 1)
An organization is building a Bootstrap Package to deploy Palo Alto Networks VM-Series firewalls into their AWS tenant Which two statements are correct regarding the bootstrap package contents? (Choose two)

A. The /config /content and /software folders are mandatory while the /license and /plugin folders are optional
B. The bootstrap package is stored on an AFS share or a discrete container file bucket
C. The directory structure must include a /config /content, /software and /license folders
D. The init-cfg txt and bootstrap.xml files are both optional configuration items for the /config folder
E. The bootstrap xml file allows for automated deployment of VM-Senes firewalls with full network and policy configurations.

Answer: DE

NEW QUESTION 133
- (Exam Topic 1)
Given the following snippet of a WildFire submission log. did the end-user get access to the requested information and why or why not?

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

A. Ye
B. because the action is set to "allow "
C. No because WildFire categorized a file with the verdict "malicious"

D. Yes because the action is set to "alert"
E. No because WildFire classified the seventy as "high."

Answer: B

NEW QUESTION 137
- (Exam Topic 1)
PBF can address which two scenarios? (Select Two)

A. forwarding all traffic by using source port 78249 to a specific egress interface
B. providing application connectivity the primary circuit fails
C. enabling the firewall to bypass Layer 7 inspection
D. routing FTP to a backup ISP link to save bandwidth on the primary ISP link

Answer: AC

NEW QUESTION 139
- (Exam Topic 1)
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 Decryption policy that the traffic matches
C. A Decryption profile must be attached to the Security policy that the traffic matches
D. There must be a certificate with only the Forward Trust option selected

Answer: A

NEW QUESTION 144
- (Exam Topic 1)
Before you upgrade a Palo Alto Networks NGFW what must you do?

A. Make sure that the PAN-OS support contract is valid for at least another year
B. Export a device state of the firewall
C. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.
D. Make sure that the firewall is running a supported version of the app + threat update

Answer: B

NEW QUESTION 146
- (Exam Topic 1)
When overriding a template configuration locally on a firewall, what should you consider?

A. Only Panorama can revert the override
B. Panorama will lose visibility into the overridden configuration
C. Panorama will update the template with the overridden value
D. The firewall template will show that it is out of sync within Panorama

Answer: B

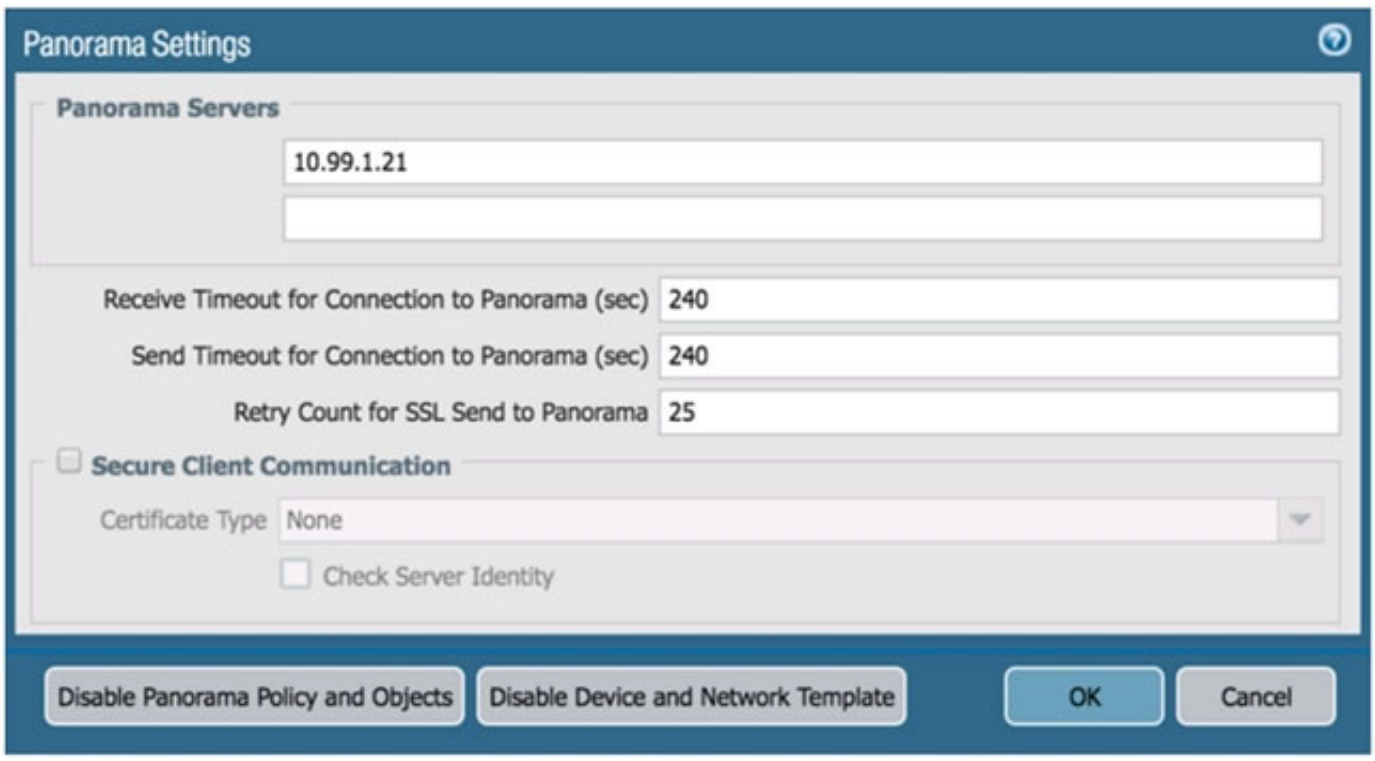
NEW QUESTION 150
- (Exam Topic 1)
What does SSL decryption require to establish a firewall as a trusted third party and to establish trust between a client and server to secure an SSL/TLS connection?

A. link state
B. stateful firewall connection
C. certificates
D. profiles

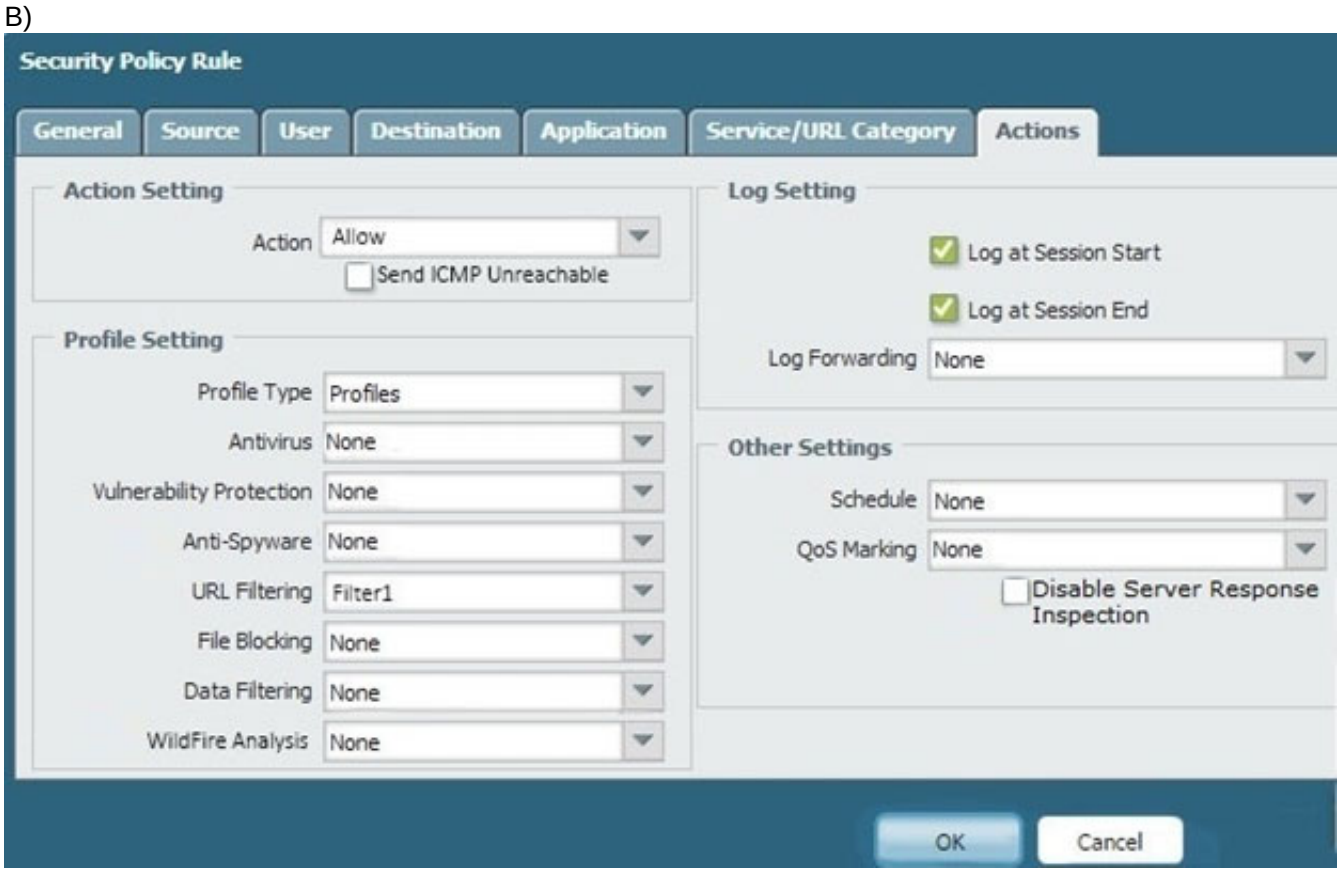
Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-overview.html#:~:text=SSL

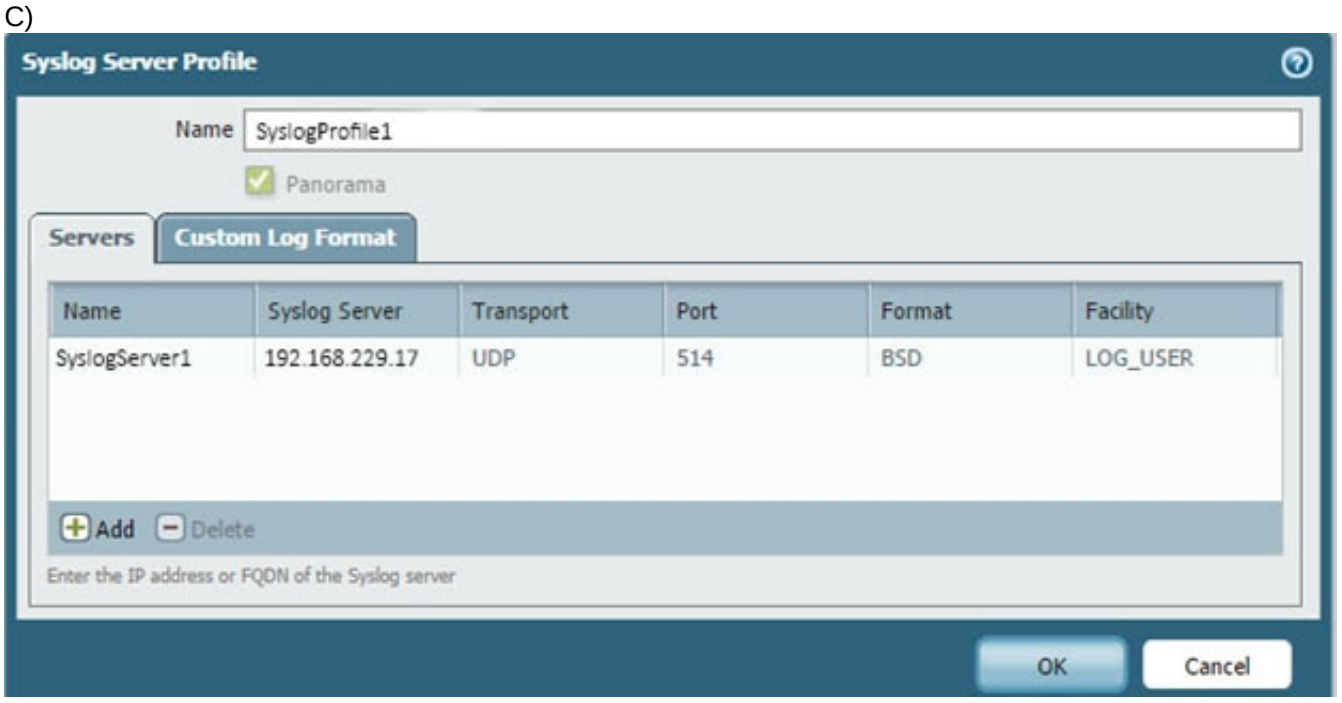
NEW QUESTION 152
- (Exam Topic 1)
An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)


Panorama Settings
Panorama Servers
10.99.1.21
Receive Timeout for Connection to Panorama (sec) 240
Send Timeout for Connection to Panorama (sec) 240
Retry Count for SSL Send to Panorama 25
Secure Client Communication
Certificate Type None
Check Server Identity
Disable Panorama Policy and Objects
Disable Device and Network Template
OK
Cancel

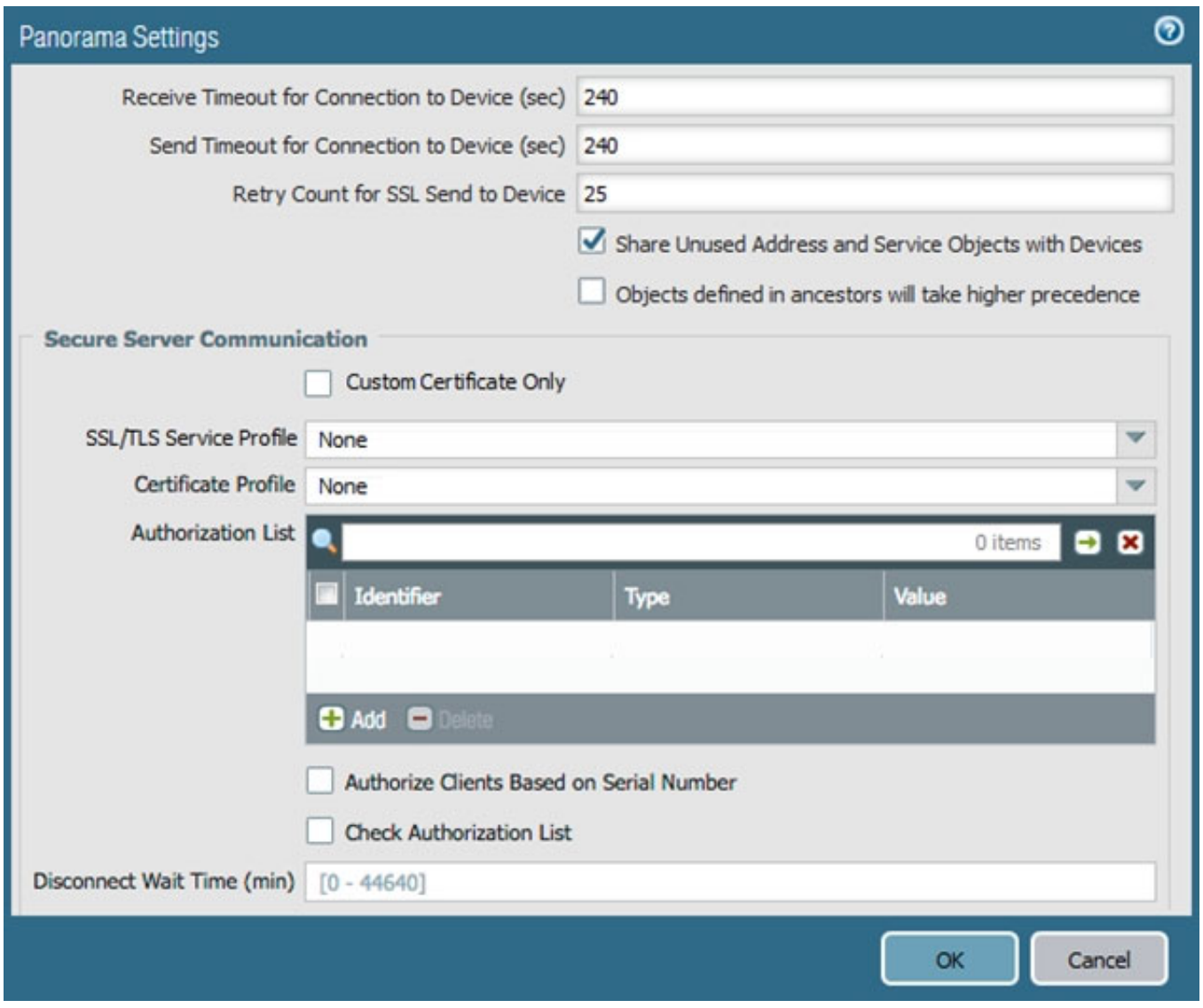
B)


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
Cancel

C)


Syslog Server Profile
Name SyslogProfile1
Panorama
Servers
Custom Log Format
Name
Syslog Server
Transport
Port
Format
Facility
SyslogServer1
192.168.229.17
UDP
514
BSD
LOG_USER
Add
Delete
Enter the IP address or FQDN of the Syslog server
OK
Cancel

D)



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

Answer: B

NEW QUESTION 157
- (Exam Topic 1)
In a security-first network what is the recommended threshold value for content updates to be dynamically updated?

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

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-thr

NEW QUESTION 161
- (Exam Topic 1)
An administrator needs to troubleshoot a User-ID deployment The administrator believes that there is an issue related to LDAP authentication The administrator wants to create a packet capture on the management plane
Which CLI command should the administrator use to obtain the packet capture for validating the configuration^

A. > ftp export mgmt-pcap from mgmt.pcap to <FTP host>
B. > scp export mgmt-pcap from mgmt.pcap to {usernameQhost:path>
C. > scp export pcap-mgmt from pcap.mgiat to (username@host:path)
D. > scp export pcap from pcap to (usernameQhost:path)

Answer: C

NEW QUESTION 165
- (Exam Topic 1)
An engineer is planning an SSL decryption implementation
Which of the following statements is a best practice for SSL decryption?

A. Obtain an enterprise CA-signed certificate for the Forward Trust certificate
B. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate
C. Use an enterprise CA-signed certificate for the Forward Untrust certificate
D. Use the same Forward Trust certificate on all firewalls in the network

Answer: D

NEW QUESTION 166
- (Exam Topic 1)
Which configuration task is best for reducing load on the management plane?

A. Disable logging on the default deny rule
B. Enable session logging at start
C. Disable pre-defined reports
D. Set the URL filtering action to send alerts

Answer: A

NEW QUESTION 168
- (Exam Topic 1)
Which rule type controls end user SSL traffic to external websites?

A. SSL Outbound Proxyless Inspection
B. SSL Forward Proxy
C. SSL Inbound Inspection
D. SSH Proxy

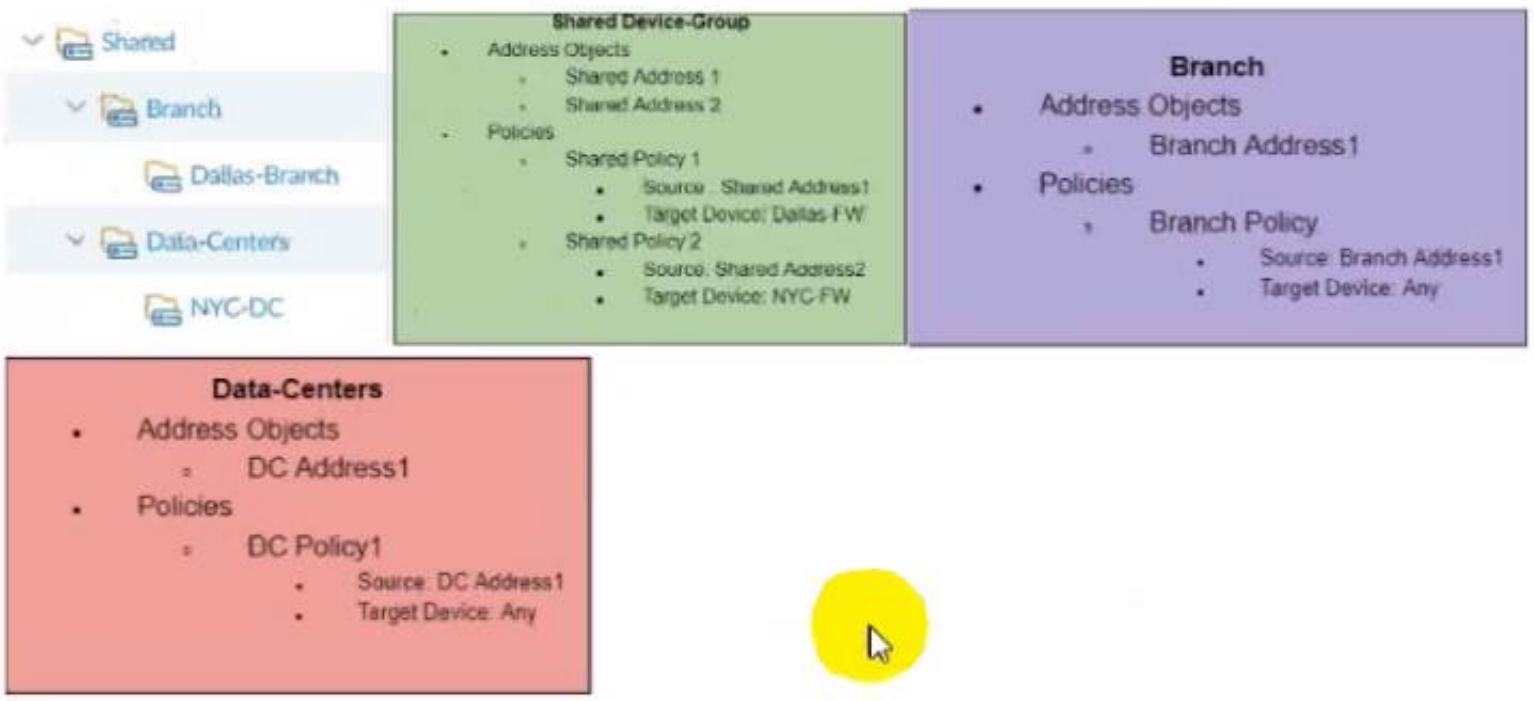
Answer: C

NEW QUESTION 172
- (Exam Topic 1)
An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version
What is considered best practice for this scenario?

A. Perform the Panorama and firewall upgrades simultaneously
B. Upgrade the firewall first wait at least 24 hours and then upgrade the Panorama version
C. Upgrade Panorama to a version at or above the target firewall version
D. Export the device state perform the update, and then import the device state

Answer: A

NEW QUESTION 175
- (Exam Topic 1)
The following objects and policies are defined in a device group hierarchy



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 Policyl
D)
Address Objects -Shared Addressl -Shared Address2 -Branch Addressl Policies -Shared Policyl -Shared Policy2 -Branch Policyl

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

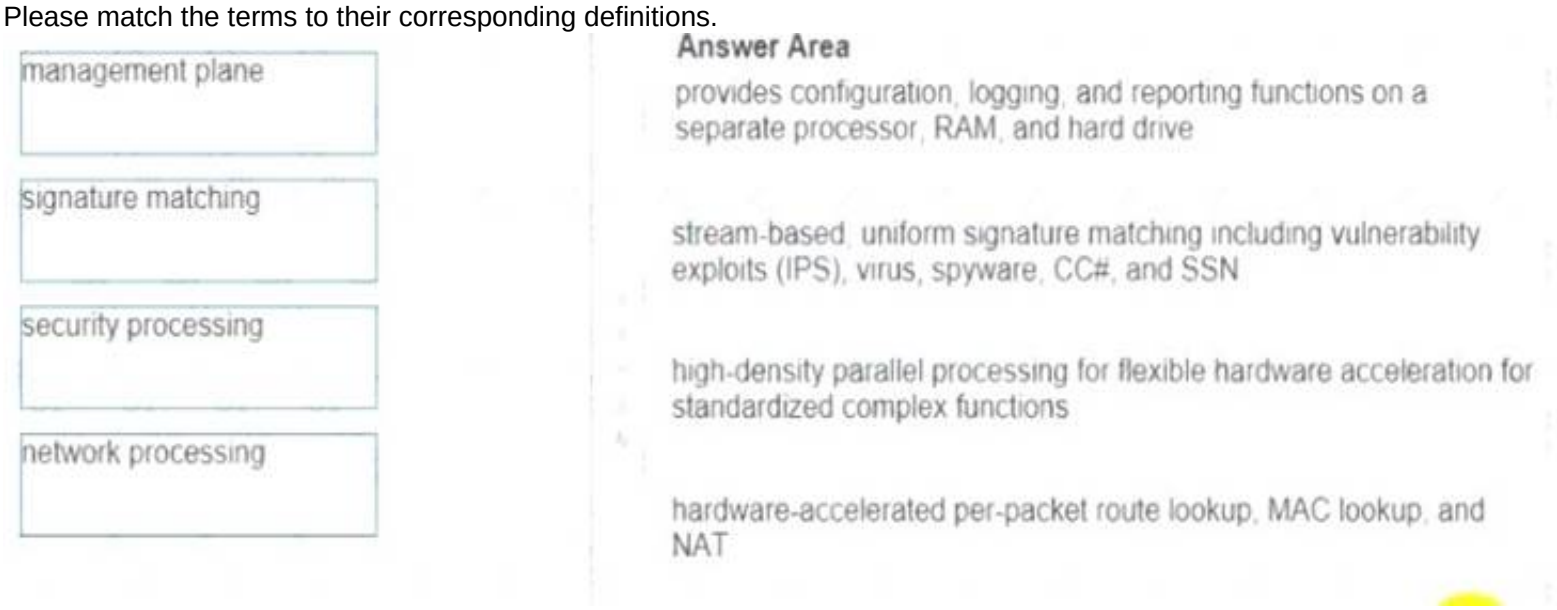
Answer: A

NEW QUESTION 177
- (Exam Topic 1)
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration Once deployed each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers
Which VPN preconfigured configuration would adapt to changes when deployed to the future site?

A. IPsec tunnels using IKEv2
B. PPTP tunnels
C. GlobalProtect satellite
D. GlobalProtect client

Answer: C

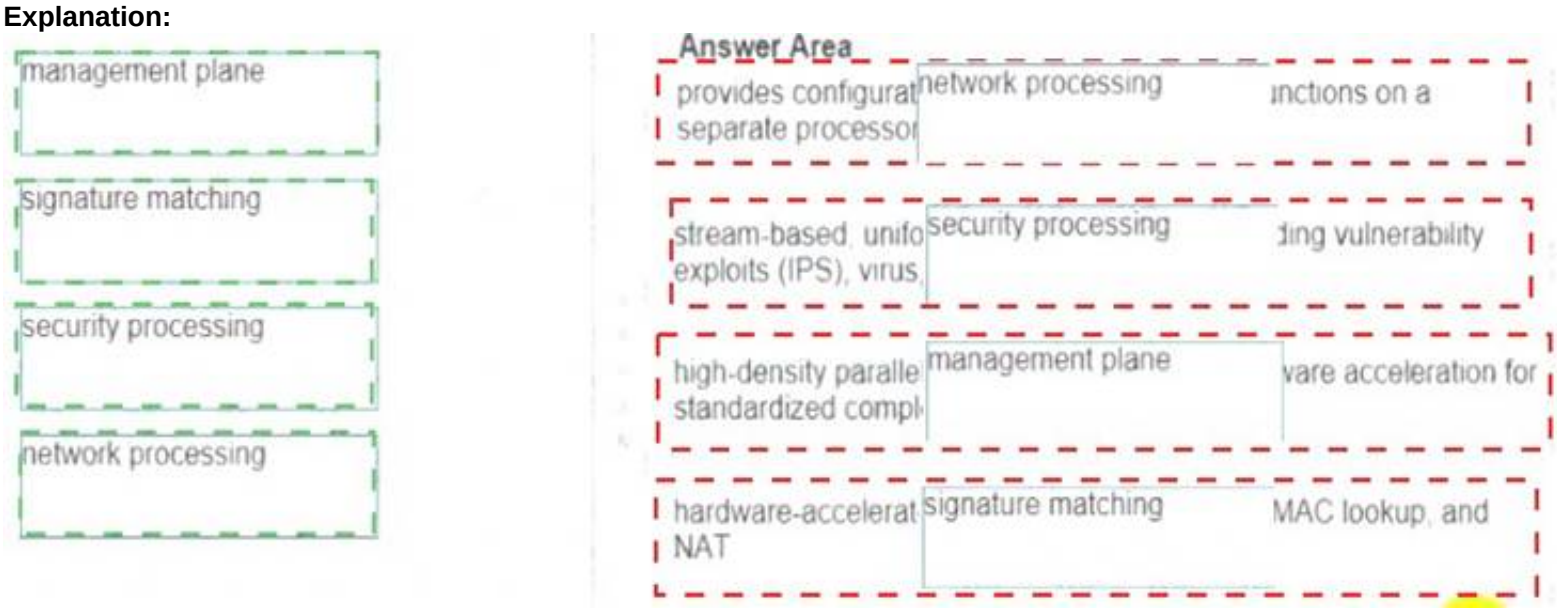
NEW QUESTION 180
- (Exam Topic 1)
Please match the terms to their corresponding definitions.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 183
- (Exam Topic 1)
Which action disables Zero Touch Provisioning (ZTP) functionality on a ZTP firewall during the onboarding process?

A. performing a local firewall commit
B. removing the firewall as a managed device in Panorama
C. performing a factory reset of the firewall
D. removing the Panorama serial number from the ZTP service

Answer: D

NEW QUESTION 187
- (Exam Topic 2)
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two)

A. log forwarding auto-tagging
B. GlobafProtect agent
C. User-ID Windows-based agent
D. XML API

Answer: BC

NEW QUESTION 191
- (Exam Topic 2)
What file type upload is supported as part of the basic WildFire service?

A. PE
B. BAT
C. VBS
D. ELF

Answer: A

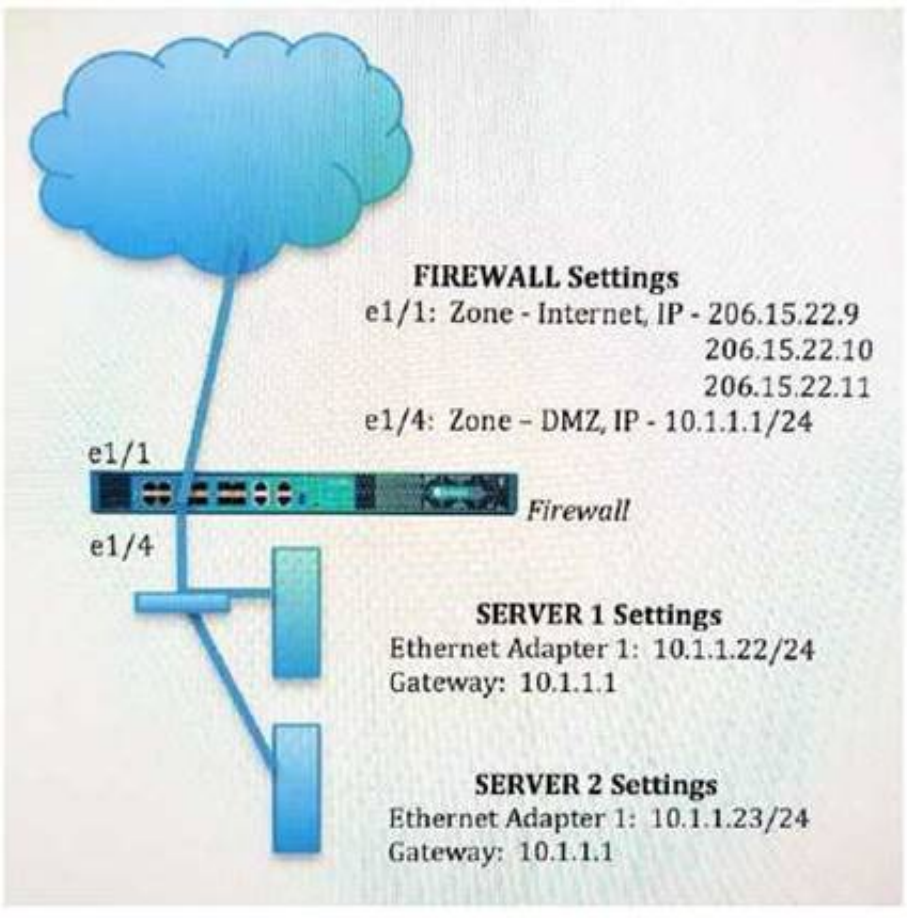
NEW QUESTION 195
- (Exam Topic 2)
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

A. HA1 IP Address
B. Network Interface Type
C. Master Key
D. Zone Protection Profile

Answer: AC

Explanation:
https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/manage-firewalls/template-capabilities-and-e

NEW QUESTION 198
- (Exam Topic 2)
An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22



Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly? A)

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B)

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

C)

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

D)

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP

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

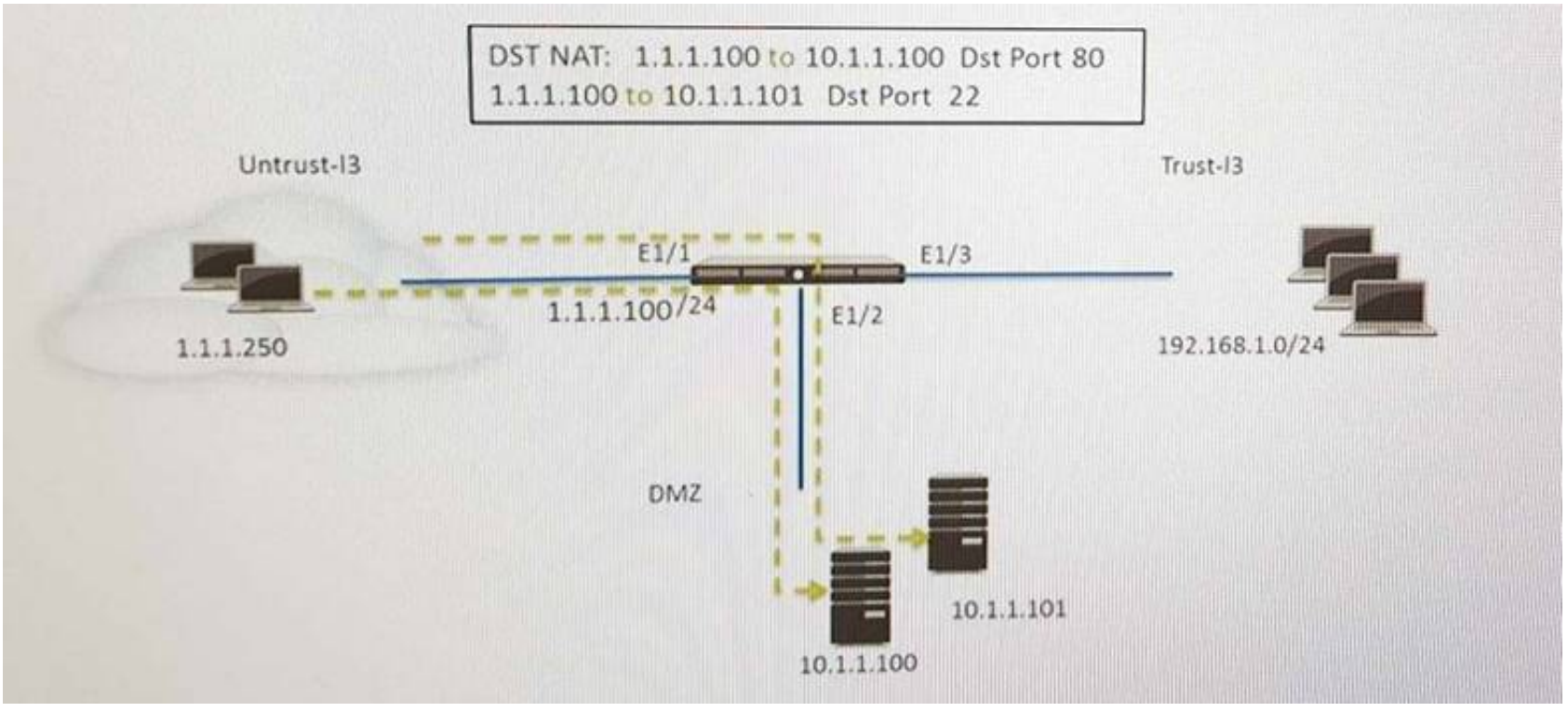
Answer: C

NEW QUESTION 202
- (Exam Topic 2)
To protect your firewall and network from single source denial of service (DoS) attacks that can overwhelm its packet buffer and cause legitimate traffic to drop, you can configure.

A. BGP (Border Gateway Protocol)
B. PBP (Packet Buffer Protection)
C. PGP (Packet Gateway Protocol)
D. PBP (Protocol Based Protection)

Answer: D

NEW QUESTION 207
- (Exam Topic 2)
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 DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing –Allow
B. Untrust (Any) to DMZ (1.1.1.100), web-browsing –Allow
C. Untrust (Any) to Untrust (10.1.1.1), web-browsing –Allow
D. Untrust (Any) to Untrust (10.1.1.1), SSH -Allow
E. Untrust (Any) to DMZ (1.1.1.100), SSH –Allow

Answer: BE

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION 210
- (Exam Topic 2)
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

A. Configure the option for “Threshold”.
B. Disable automatic updates during weekdays.
C. Automatically “download only” and then install Applications and Threats later, after the administratorapproves the update.
D. Automatically “download and install” but with the “disable new applications” option used.

Answer: A

Explanation:
For Antivirus and Applications and Threats updates, you have the option to set a minimum Threshold of time that a content update must be available before the firewall installs it. Very rarely, there can be an error in a content update and this threshold ensures that the firewall only downloads content releases that have been available and functioning in customer environments for the specified amount of time. https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamic-updates

NEW QUESTION 213
- (Exam Topic 2)
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP
port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.
Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web- browsing traffic to this server on tcp/443.

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

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEyCAK

NEW QUESTION 214
- (Exam Topic 2)
An administrator wants to upgrade an NGFW from PAN-OS® 9.0 to PAN-OS® 10.0. The firewall is not a part of an HA pair. What needs to be updated first?

A. XML Agent
B. Applications and Threats
C. WildFire
D. PAN-OS® Upgrade Agent

Answer: B

Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-t

NEW QUESTION 216
- (Exam Topic 2)
Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

A. Okta
B. DUO
C. RADIUS
D. PingID

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-aut

NEW QUESTION 219
- (Exam Topic 2)
An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

A. The Passive firewall, which then synchronizes to the active firewall
B. The active firewall, which then synchronizes to the passive firewall
C. Both the active and passive firewalls, which then synchronize with each other
D. Both the active and passive firewalls independently, with no synchronization afterward

Answer: D

Explanation:
Palo Alto NetworksPanorama 7.0 Administrator's Guide •77Manage FirewallsManage Device GroupsManage Device GroupsAdd a Device GroupCreate a Device Group HierarchyCreate Objects for Use in Shared or Device Group PolicyRevert to Inherited Object ValuesManage Unused Shared ObjectsManage Precedence of Inherited ObjectsMove or Clone a Policy Rule or Object to a Different Device GroupSelect a URL Filtering Vendor on PanoramaPush a Policy Rule to a Subset of FirewallsManage the Rule HierarchyAdd a Device GroupAfter adding firewalls (see Add a Firewall as a Managed Device), you can group them into Device Groups (up to 256), as follows. Be sure to assign both firewalls in an active-passive high availability (HA) configuration to the same device group so that Panorama will push the same policy rules and objects to those firewalls. ##############PAN-OS doesn't synchronize pushed rules across HA peers.########## To manage rules and objects at different administrative levels in your organization, Create a Device Group Hierarchy.
https://docs.paloaltonetworks.com/panorama/8-0/panorama-admin/manage-firewalls/transition-a-firewall-to-pan
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS

NEW QUESTION 221
- (Exam Topic 2)
Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

A. Deny application facebook-chat before allowing application facebook
B. Deny application facebook on top
C. Allow application facebook on top
D. Allow application facebook before denying application facebook-chat

Answer: A

Explanation:
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/1

NEW QUESTION 225
- (Exam Topic 3)
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

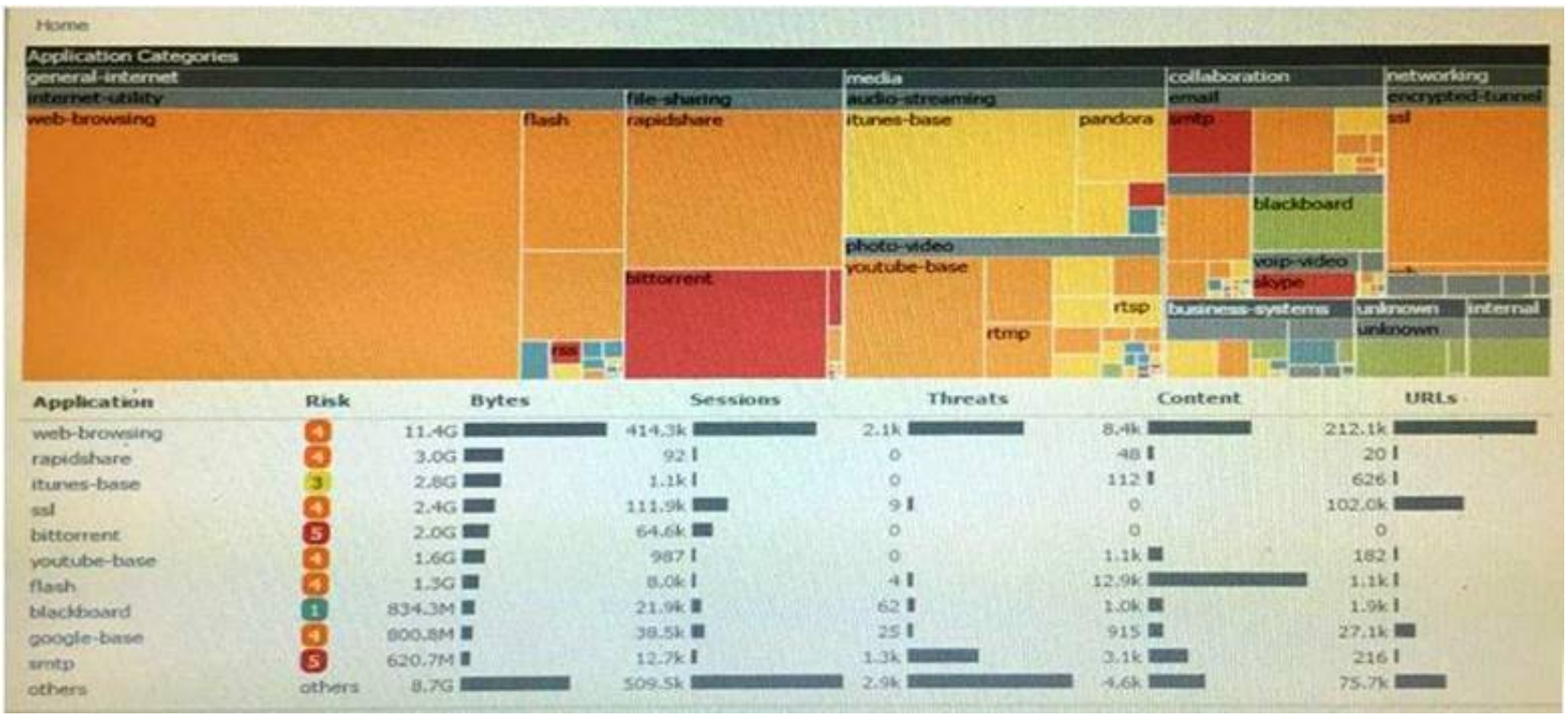
Answer: BDE

NEW QUESTION 230
- (Exam Topic 3)
Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

A. Vulnerability Object
B. DoS Protection Profile
C. Data Filtering Profile
D. Zone Protection Profile

Answer: BD

NEW QUESTION 233
- (Exam Topic 3)
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 238
- (Exam Topic 3)
Which Device Group option is assigned by default in Panorama whenever a new device group is created to manage a Firewall?

A. Master
B. Universal
C. Shared
D. Global

Answer: C

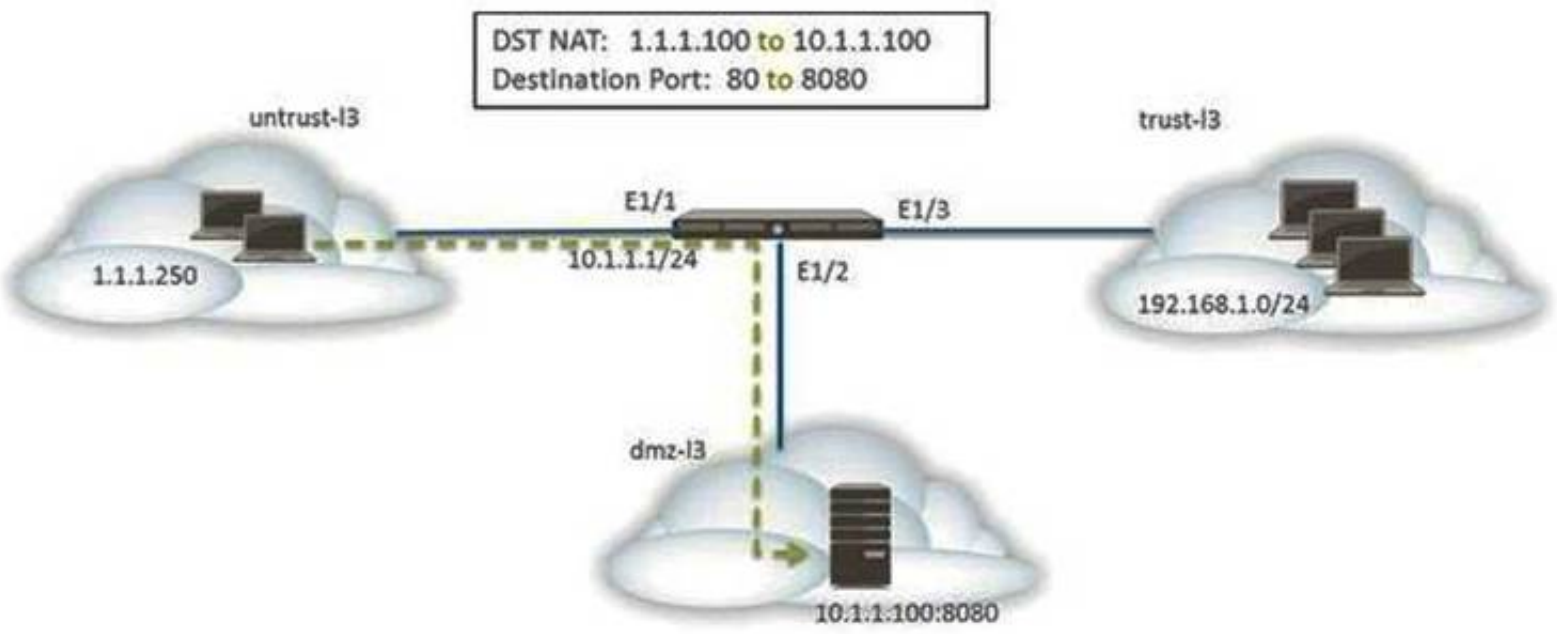
NEW QUESTION 241
- (Exam Topic 3)
What are three valid actions in a File Blocking Profile? (Choose three)

A. Forward
B. Block
C. Alret
D. Upload
E. Reset-both
F. Continue

Answer: ABC

Explanation:
https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p

NEW QUESTION 243
- (Exam Topic 3)
The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and report to 10.1.1.100 on TCP Port 8080.



Which NAT and security rules must be configured on the firewall? (Choose two)

A. A security policy with a source of any from untrust-I3 Zone to a destination of 10.1.1.100 in dmz-I3 zone using web-browsing application
B. A NAT rule with a source of any from untrust-I3 zone to a destination of 10.1.1.100 in dmz-zone using service-http service.
C. A NAT rule with a source of any from untrust-I3 zone to a destination of 1.1.1.100 in untrust-I3 zone using service-http service.
D. A security policy with a source of any from untrust-I3 zone to a destination of 1.1.100 in dmz-I3 zone using web-browsing application.

Answer: BD

NEW QUESTION 245
- (Exam Topic 3)
Which three options does the WF-500 appliance support for local analysis? (Choose three)

A. E-mail links
B. APK files
C. jar files
D. PNG files
E. Portable Executable (PE) files

Answer: ACE

NEW QUESTION 250
- (Exam Topic 3)
How are IPV6 DNS queries configured to user interface ethernet1/3?

A. Network > Virtual Router > DNS Interface
B. Objects > CustomerObjects > DNS
C. Network > Interface Mgrnt
D. Device > Setup > Services > Service Route Configuration

Answer: D

NEW QUESTION 253
- (Exam Topic 3)
A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?

A. Block all unauthorized applications using a security policy
B. Block all known internal custom applications
C. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
D. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks

Answer: D

NEW QUESTION 254
- (Exam Topic 3)
Which command can be used to validate a Captive Portal policy?

A. eval captive-portal policy <criteria>
B. request cp-policy-eval <criteria>
C. test cp-policy-match <criteria>
D. debug cp-policy <criteria>

Answer: C

NEW QUESTION 256
- (Exam Topic 3)
Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

A. Set the type to Aggregate, clear the session's box and set the Maximum concurrent Sessions to 4000.
B. Set the type to Classified, clear the session's box and set the Maximum concurrent Sessions to 4000.
C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.
D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000.

Answer: C

NEW QUESTION 257
- (Exam Topic 3)
A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

A. BGP not sure
B. OSPFv3
C. RIP
D. Static Route

Answer: BD

Explanation:
https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols

NEW QUESTION 259
- (Exam Topic 3)
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 261
- (Exam Topic 3)
Starting with PAN-OS version 9.1, Global logging information is now recoded in which firewall log?

A. Authentication
B. Globalprotect
C. Configuration
D. System

Answer: D

NEW QUESTION 264
- (Exam Topic 3)
Which Panorama feature allows for logs generated by Panorama to be forwarded to an external Security Information and Event Management(SIEM) system?

A. Panorama Log Settings
B. Panorama Log Templates
C. Panorama Device Group Log Forwarding
D. Collector Log Forwarding for Collector Groups

Answer: A

Explanation:
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manage-log-collection/e

NEW QUESTION 267
- (Exam Topic 3)
Which CLI command displays the current management plane memory utilization?

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

Answer: D

Explanation:
https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364 "The command show system resources gives a snapshot of Management Plane (MP) resource utilization
including memory and CPU. This is similar to the 'top' command in Linux."https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59

NEW QUESTION 270
- (Exam Topic 3)

Which three rule types are available when defining policies in Panorama? (Choose three.)

A. Pre Rules
B. Post Rules
C. Default Rules
D. Stealth Rules
E. Clean Up Rules

Answer: ABC

Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/defini

NEW QUESTION 275
- (Exam Topic 3)
Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

A. The devices are pre-configured with a virtual wire pair out the first two interfaces.
B. The devices are licensed and ready for deployment.
C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.
D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.
E. The interface are pingable.

Answer: BC

NEW QUESTION 276
- (Exam Topic 3)
A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall Which part of files needs to be imported back into the replacement firewall that is using Panorama?

A. Device state and license files
B. Configuration and serial number files
C. Configuration and statistics files
D. Configuration and Large Scale VPN (LSVPN) setups file

Answer: A

NEW QUESTION 280
- (Exam Topic 3)
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

A. link requirements
B. the name of the ISP
C. IP Addresses
D. branch and hub locations

Answer: ACD

NEW QUESTION 284
- (Exam Topic 3)
A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled.
Which component once enabled on a perirneter firewall will allow the identification of existing infected hosts in an environment?

A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
B. File Blocking profiles applied to outbound security policies with action set to alert
C. Vulnerability Protection profiles applied to outbound security policies with action set to block
D. Antivirus profiles applied to outbound security policies with action set to alert

Answer: A

NEW QUESTION 288
- (Exam Topic 3)
Which three log-forwarding destinations require a server profile to be configured? (Choose three)

A. SNMP Trap
B. Email
C. RADIUS
D. Kerberos
E. Panorama
F. Syslog

Answer: ABF

NEW QUESTION 291
- (Exam Topic 3)
After pushing a security policy from Panorama to a PA-3020 firwall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in

Panorama's traffic logs. What could be the problem?

A. A Server Profile has not been configured for logging to this Panorama device.
B. Panorama is not licensed to receive logs from this particular firewall.
C. The firewall is not licensed for logging to this Panorama device.
D. None of the firwwall's policies have been assigned a Log Forwarding profile

Answer: D

NEW QUESTION 296
- (Exam Topic 3)
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured. What can be the cause of this problem?

A. No Zone has been configured on Ethernet 1/4.
B. Interface Ethernet 1/1 is in Virtual Wire Mode.
C. DNS has not been properly configured on the firewall.
D. DNS has not been properly configured on the host.

Answer: A

NEW QUESTION 300
- (Exam Topic 3)
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 301
- (Exam Topic 3)
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.com/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-U

NEW QUESTION 302
- (Exam Topic 3)
How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

A. Enable support for non-standard syslog messages under device management
B. Check the custom-format check box in the syslog server profile
C. Select a non-standard syslog server profile
D. Create a custom log format under the syslog server profile

Answer: D

NEW QUESTION 304
- (Exam Topic 3)
A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.
Given the following zone information:
•DMZ zone: DMZ-L3
•Public zone: Untrust-L3
•Guest zone: Guest-L3
•Web server zone: Trust-L3
•Public IP address (Untrust-L3): 1.1.1.1
•Private IP address (Trust-L3): 192.168.1.50
What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

A. Untrust-L3

B. DMZ-L3
C. Guest-L3
D. Trust-L3

Answer: A

NEW QUESTION 306
- (Exam Topic 3)
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 311
- (Exam Topic 3)
Starting with PAN-OS version 9.1, application dependency information is now reported in which new locations? (Choose two.)

A. On the App Dependency tab in the Commit Status window
B. On the Application tab in the Security Policy Rule creation window
C. On the Objects > Applications browsers pages
D. On the Policy Optimizer's Rule Usage page

Answer: AB

NEW QUESTION 313
- (Exam Topic 3)
Which two mechanisms help prevent a spilt brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

A. Configure the management interface as HA3 Backup
B. Configure Ethernet 1/1 as HA1 Backup
C. Configure Ethernet 1/1 as HA2 Backup
D. Configure the management interface as HA2 Backup
E. Configure the management interface as HA1 Backup
F. Configure ethernet1/1 as HA3 Backup

Answer: BE

NEW QUESTION 316
- (Exam Topic 3)
Which URL Filtering Security Profile action logs the URL Filtering category to the URL Filtering log?

A. Log
B. Alert
C. Allow
D. Default

Answer: B

Explanation:
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering-profile-actions

NEW QUESTION 319
- (Exam Topic 3)
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 322
- (Exam Topic 3)
Which option is an IPv6 routing protocol?

A. RIPv3
B. OSPFv3
C. OSPv3
D. BGP NG

Answer: B

NEW QUESTION 326
- (Exam Topic 3)
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 329
.....

Relate Links

100% Pass Your PCNSE Exam with Exambible Prep Materials

https://www.exambible.com/PCNSE-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/