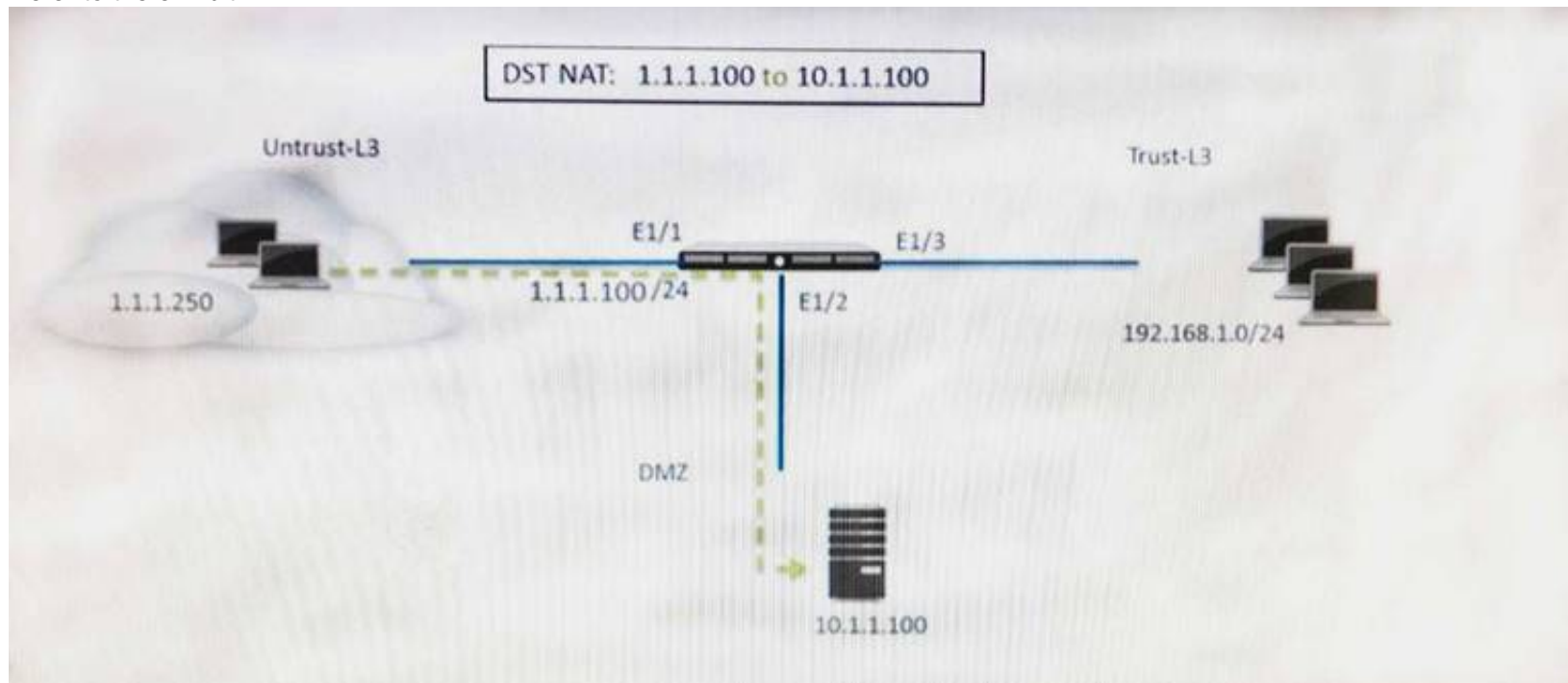# Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1
- (Exam Topic 2)
Refer to the exhibit.

A web server in the DMZ is being mapped to a public address through DNAT. Which Security policy rule will allow traffic to flow to the web server?

A. Untrust (any) to Untrust (10. 1.1. 100), web browsing – Allow
B. Untrust (any) to Untrust (1. 1. 1. 100), web browsing – Allow
C. Untrust (any) to DMZ (1. 1. 1. 100), web browsing – Allow
D. Untrust (any) to DMZ (10. 1. 1. 100), web browsing – Allow

Answer: C

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

NEW QUESTION 2
- (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. Redistribution of user mappings
C. Virtual Wire mode
D. Content inspection

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network.ht

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)
During the packet flow process, which two processes are performed in application identification? (Choose two.)

A. Pattern based application identification
B. Application override policy match
C. Application changed from content inspection
D. Session application identified.

Answer: AB

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0 http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

NEW QUESTION 5
- (Exam Topic 2)
Which method will dynamically register tags on the Palo Alto Networks NGFW?

A. Restful API or the VMWare API on the firewall or on the User-ID agent or the read-only domain controller (RODC)
B. Restful API or the VMware API on the firewall or on the User-ID agent
C. XML-API or the VMware API on the firewall or on the User-ID agent or the CLI
D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

Answer: D

Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/monitor-changes-in-the-virtual-environmen

NEW QUESTION 6
- (Exam Topic 2)
Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

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

Answer: C

NEW QUESTION 7
- (Exam Topic 2)
Which DoS protection mechanism detects and prevents session exhaustion attacks?

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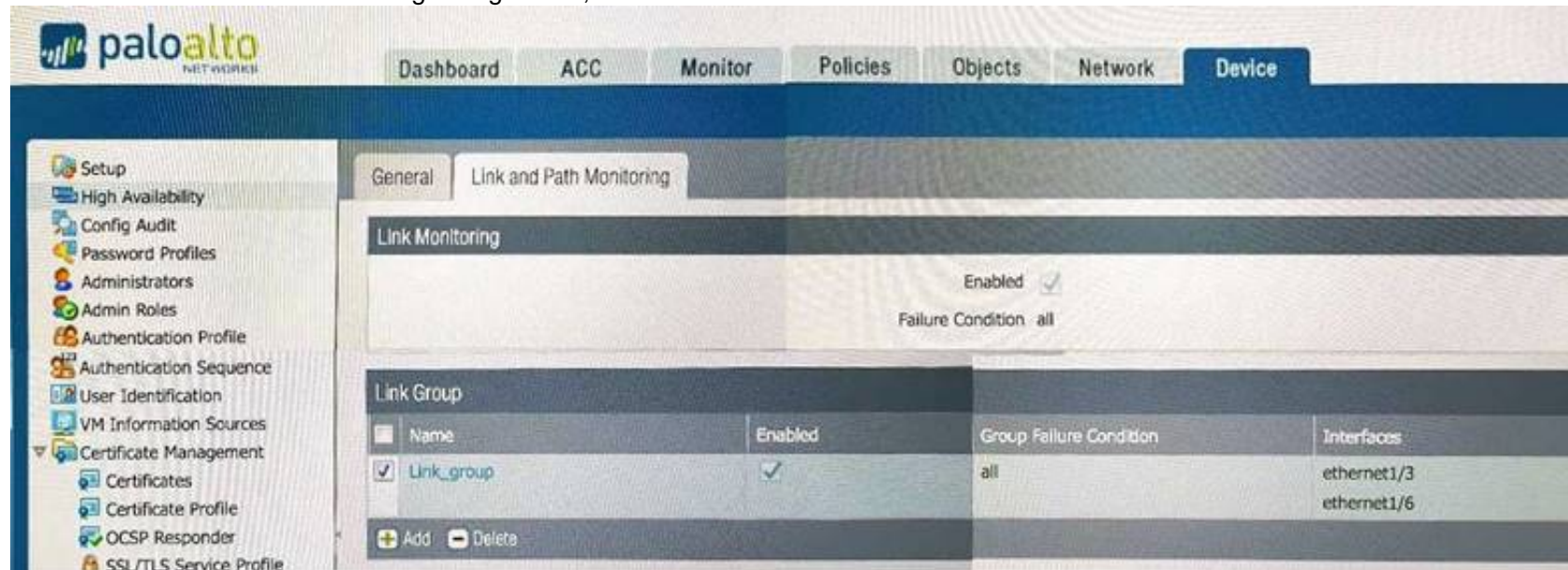D. TCP Port Scan Protection

Answer: C

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

NEW QUESTION 8
- (Exam Topic 2)
If the firewall has the link monitoring configuration, what will cause a failover?

A. ethernet1/3 and ethernet1/6 going down
B. ethernet1/3 going down
C. ethernet1/3 or Ethernet1/6 going down
D. ethernet1/6 going down

Answer: A

NEW QUESTION 9
- (Exam Topic 2)
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 10
- (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 10
- (Exam Topic 2)
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.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-inte

NEW QUESTION 11
- (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. Replay
C. Web Application
D. DoS Protection

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/vpns/set-up-site-to-site-vpn/set-up-an-ipsec-tunnel#

NEW QUESTION 15
- (Exam Topic 2)
Which is not a valid reason for receiving a decrypt-cert-validation error?

A. Unsupported HSM
B. Unknown certificate status
C. Client authentication
D. Untrusted issuer

Answer: A

NEW QUESTION 20
- (Exam Topic 2)
Starling with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

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

Answer: C

NEW QUESTION 24
- (Exam Topic 2)
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-ID identification
B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use of an "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the ports being used.
C. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use of a 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 of an "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 26
- (Exam Topic 2)
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/bootstrapp firewalls-for-rapid-deployment.html

NEW QUESTION 28
- (Exam Topic 2)
What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

A. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or template stacks.
B. An administrator must use the Expedition tool to adapt the configuration to the pre-PAN-OS 8.1 state.
C. When Panorama is reverted to an earlier PAN-OS release, variables used in templates or template stacks will be removed automatically.
D. Administrators need to manually update variable characters to those used in pre-PAN-OS 8.1.

Answer: A

NEW QUESTION 33
- (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 38
- (Exam Topic 2)
An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to PanoramA.
Pre-existing logs from the firewalls are not appearing in PanoramA.
Which action would enable the firewalls to send their pre-existing logs to Panorama?

A. Use the import option to pull logs into Panorama.
B. A CLI command will forward the pre-existing logs to Panorama.
C. Use the ACC to consolidate pre-existing logs.
D. The log database will need to exported form the firewalls and manually imported into Panorama.

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/management-features/pa-7000-series-firewal

NEW QUESTION 42
- (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 47
- (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 50
- (Exam Topic 2)
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 51
- (Exam Topic 2)
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.
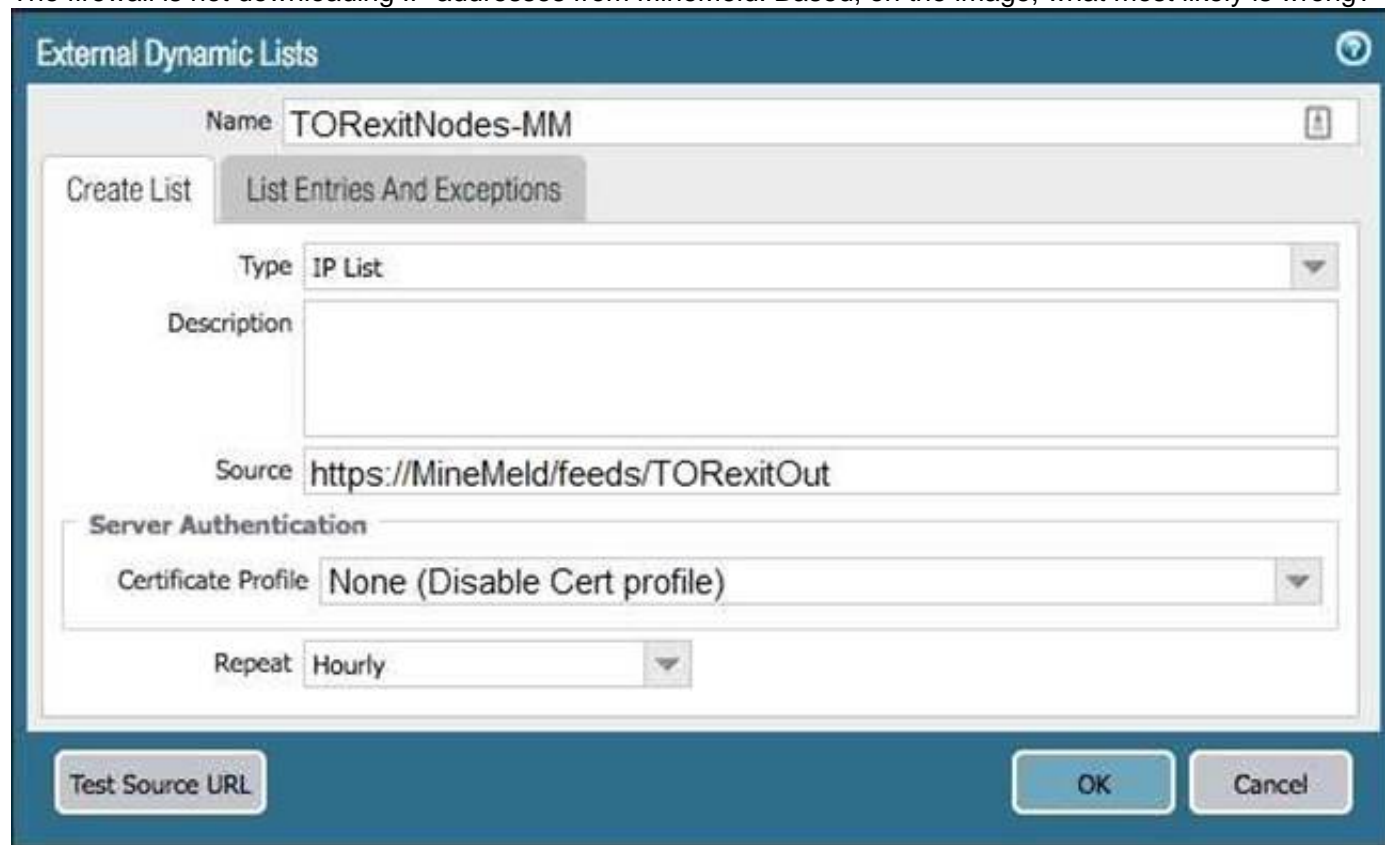
Answer: DE

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

NEW QUESTION 52
- (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 53
- (Exam Topic 2)
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-authe

NEW QUESTION 54
- (Exam Topic 2)
NO: 103
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
"In an SSH Proxy configuration, the firewall resides between a client and a server. SSH Proxy enables the firewall to decrypt inbound and outbound SSH connections and ensures that attackers don't use SSH to tunnel unwanted applications and content. SSH decryption does not require certificates and the firewall automatically generates the key used for SSH decryption when the firewall boots up."

NEW QUESTION 55
- (Exam Topic 2)
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A. Configuration Logs
B. System Logs
C. Task Manager
D. Traffic Logs

Answer: BC

NEW QUESTION 59
- (Exam Topic 2)
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?

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

Answer: B

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

NEW QUESTION 62
- (Exam Topic 2)
Which Palo Alto Networks VM-Series firewall is valid?

A. VM-25
B. VM-800
C. VM-50
D. VM-400

Answer: C

Explanation:
Reference:
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/about-the-vm-series-firewall/vm-series

NEW QUESTION 63
- (Exam Topic 2)
How does Panorama prompt VMWare NSX to quarantine an infected VM?

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

Answer: A

NEW QUESTION 64
- (Exam Topic 2)
What is the purpose of the firewall decryption broker?

A. Decrypt SSL traffic a then send it as cleartext to a security chain of inspection tools
B. Force decryption of previously unknown cipher suites
C. Inspection traffic within IPsec tunnel
D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

Answer: A

NEW QUESTION 67
- (Exam Topic 2)
The certificate information displayed in the following image is for which type of certificate? Exhibit:
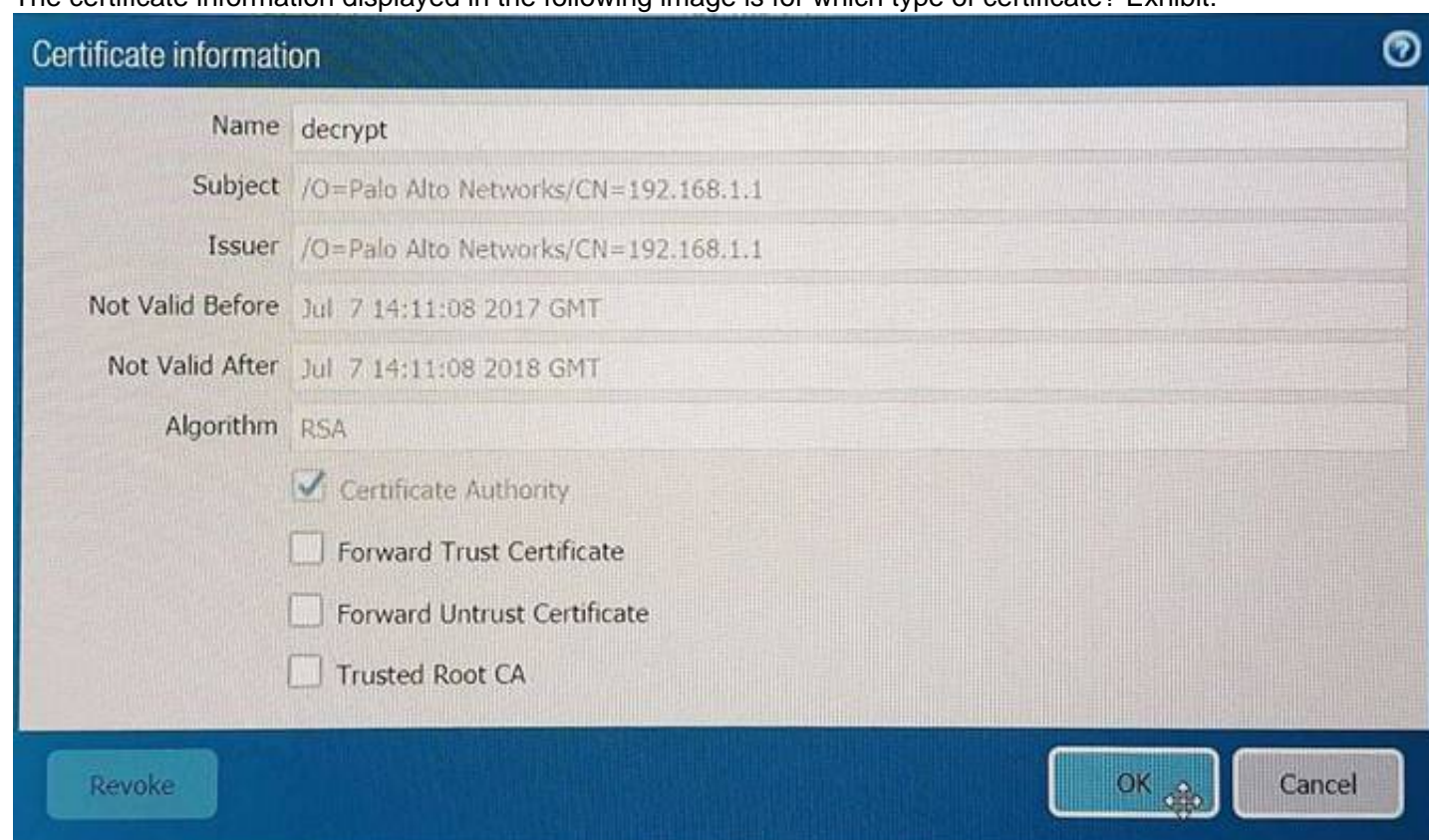
A. Forward Trust certificate
B. Self-Signed Root CA certificate
C. Web Server certificate
D. Public CA signed certificate

Answer: B

NEW QUESTION 71
- (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 75
- (Exam Topic 2)
Which three options are supported in HA Lite? (Choose three.)

A. Virtual link
B. Active/passive deployment
C. Synchronization of IPsec security associations
D. Configuration synchronization
E. Session synchronization

Answer: BCD

Explanation:
"The PA-200 firewall supports HA Lite only. HA Lite is an active/passive deployment that provides configuration synchronization and some runtime data synchronization such as IPSec security associations. It does not support any session synchronization (HA2), and therefore does not offer stateful failover."
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability

NEW QUESTION 77
- (Exam Topic 2)
A Security policy rule is configured with a Vulnerability Protection Profile and an action of 'Deny'. Which action will this cause configuration on the matched traffic?

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

Answer: D

Explanation:
"Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy."
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/security-profiles.html#

NEW QUESTION 82
- (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 85
- (Exam Topic 2)
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: BDE

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administra

NEW QUESTION 86
- (Exam Topic 2)
The firewall identifies a popular application as an unknown-tcp.
Which two options are available to identify the application? (Choose two.)

A. Create a custom application.
B. Create a custom object for the custom application server to identify the custom application.
C. Submit an Apple-ID request to Palo Alto Networks.
D. Create a Security policy to identify the custom application.

Answer: AD

Explanation:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/manage-custom-or-unknown-applic

NEW QUESTION 90
- (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 94
- (Exam Topic 2)
Which virtual router feature determines if a specific destination IP address is reachable?

A. Heartbeat Monitoring
B. Failover
C. Path Monitoring
D. Ping-Path

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf

NEW QUESTION 98
- (Exam Topic 2)
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
"Before you can enable Decryption Mirroring, you must obtain and install a Decryption Port Mirror license. The license is free of charge and can be activated through the support portal as described in the following procedure. After you install the Decryption Port Mirror license and reboot the firewall, you can enable decryption port mirroring. "

NEW QUESTION 102
- (Exam Topic 2)
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

A. Virtual router
B. Security zone
C. ARP entries
D. Netflow Profile

Answer: AB

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa
layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd-8064499f5b9d

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRqCAK
VLAN interface is not necessary but in this scenarion we assume it is. Create VLAN object, VLAN interface and VLAN Zone. Attach VLAN interface to VLAN object together with two L2 interfaces then attach VLAN interface to virtual router. Without VLAN interface you can pass traffic between interfaces on the same network and with VLAN interface you can route traffic to other networks.

NEW QUESTION 103
- (Exam Topic 2)
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects. How would an administrator configure the interface to 1Gbps?

A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
B. set deviceconfig system speed-duplex 1Gbps-duplex
C. set deviceconfig system speed-duplex 1Gbps-full-duplex
D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex

Answer: C

Explanation:
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Man Port/ta-p/59034
user@PA# set deviceconfig system speed-duplex100Mbps-full-duplex
100Mbps-full-duplex100Mbps-half-duplex 100Mbps-half-duplex10Mbps-full-duplex 10Mbps-full-duplex10Mbps-half-duplex 10Mbps-half-duplex1Gbps-full-duplex 1Gbps-full-duplex1Gbps-half-duplex 1Gbps-half-duplexauto-negotiate auto-negotiate

NEW QUESTION 107
- (Exam Topic 2)
In a virtual router, which object contains all potential routes?

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

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/virtual-routers

NEW QUESTION 111
- (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 113
- (Exam Topic 2)
Refer to exhibit.
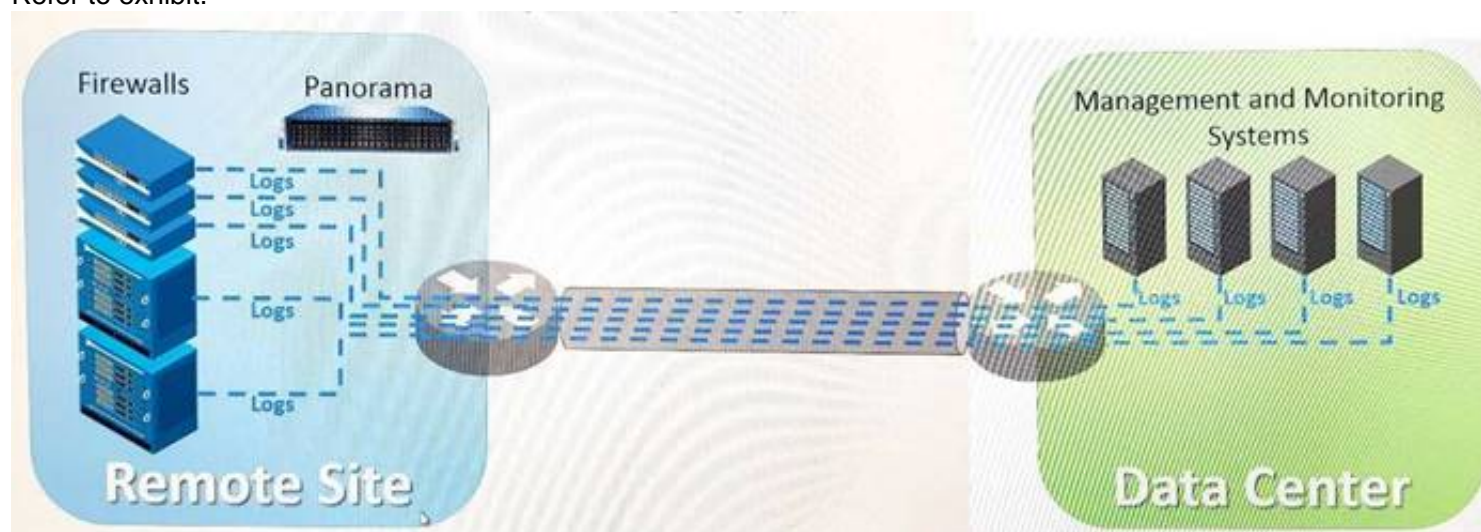
An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.
How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring/ 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

Explanation:
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKFCA0
"When this has to be done over a WAN link with bandwidth limitation, it is necessary to consider reducing the number of log streams that are sent over the link"
"With this configuration, firewalls will forward logs to Panorama, assuming that log forwarding was configured correctly on the firewall. The logs are forwarded to the syslog server, thus reducing the number of log streams significantly."

NEW QUESTION 116
- (Exam Topic 2)
An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.
Which configuration setting or step will allow the firewall to get automatic application signature updates?

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

Answer: A

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-update

NEW QUESTION 119
- (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 122
- (Exam Topic 2)
If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

A. The settings assigned to the template that is on top of the stack.
B. The administrator will be promoted to choose the settings for that chosen firewall.
C. All the settings configured in all templates.
D. Depending on the firewall location, Panorama decides with settings to send.

Answer: A

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/mana templates-and-template-stacks/configure-a-template-stack

NEW QUESTION 127
- (Exam Topic 2)
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

A. .dll
B. .exe
C. .src
D. .apk
E. .pdf
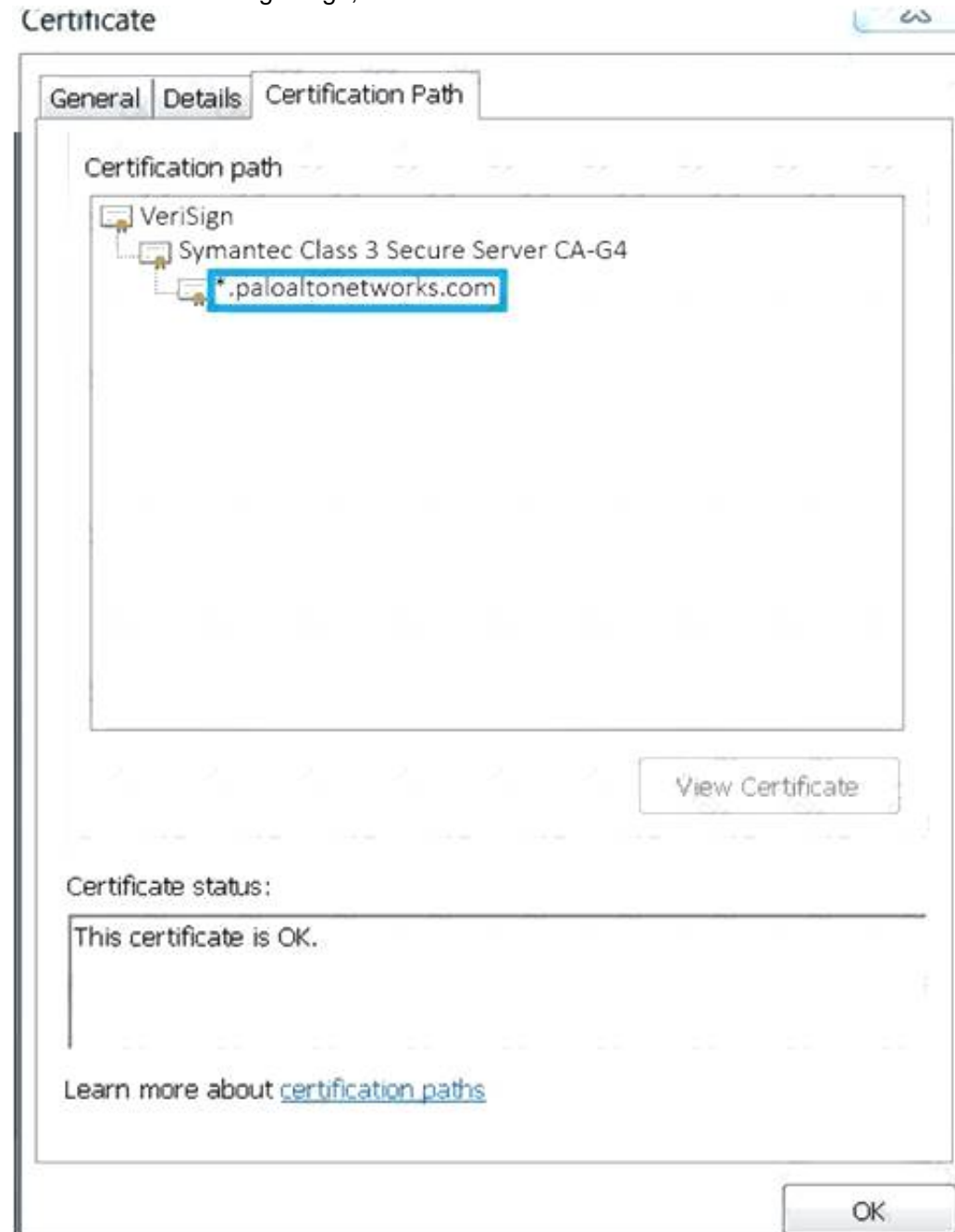F. .jar

Answer: DEF

Explanation:
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

NEW QUESTION 129
- (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 133
- (Exam Topic 2)
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/5

NEW QUESTION 138
- (Exam Topic 2)
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

Explanation:
System Resources (widget)Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or
Panorama).https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/dashboard/dashboard-widg

NEW QUESTION 142
- (Exam Topic 2)
Which administrative authentication method supports authorization by an external service?

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

Answer: C

NEW QUESTION 146
- (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 148
- (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 150
- (Exam Topic 2)
Which three settings are defined within the Templates object of Panorama? (Choose three.)

A. Setup
B. Virtual Routers
C. Interfaces
D. Security
E. Application Override

Answer: ABC

NEW QUESTION 152
- (Exam Topic 2)
A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

A. Application Override policy.
B. Security policy to identify the custom application.
C. Custom application.
D. Custom Service object.

Answer: AC

Explanation:
Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy's matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the Application entry box.Choices are limited to applications currently in the App-ID database.Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer-4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy and QoS.Use CasesThree primary uses cases for Application Override Policy are:

To identify "Unknown" App-IDs with a different or custom application signature To re-identify an existing application signature
To bypass the Signature Match Engine (within the SP3 architecture) to improve processing timesA discussion of typical uses of application override and specific implementation examples is here:https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application

NEW QUESTION 154
- (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 159
- (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 162
- (Exam Topic 2)
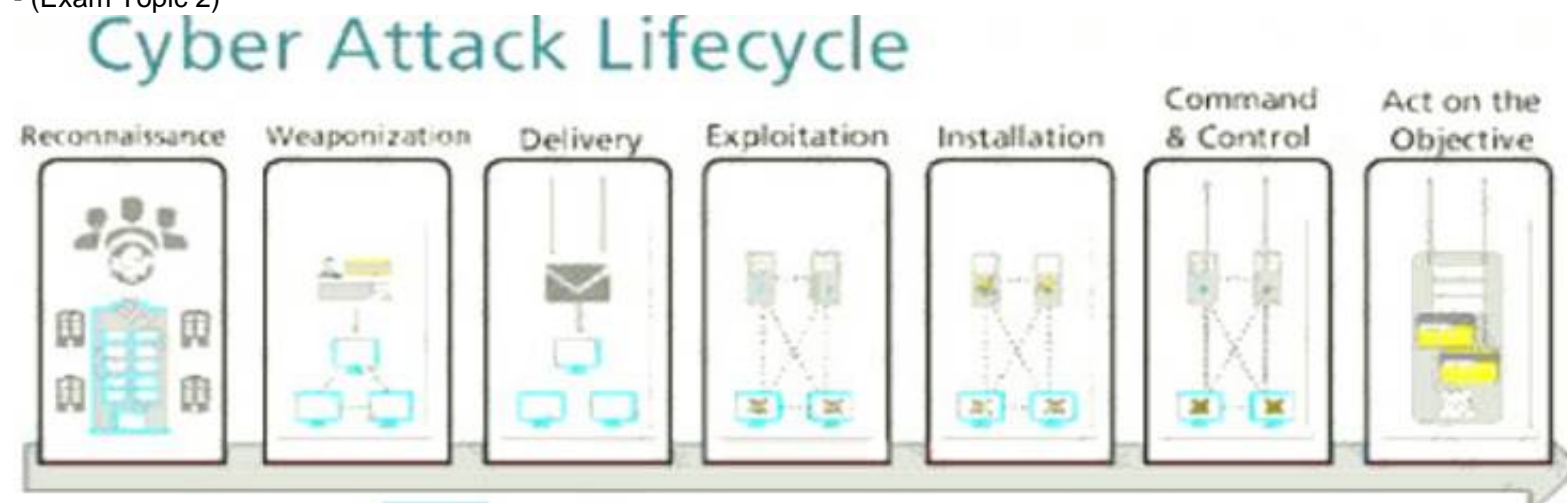
At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?

A. exploitation
B. IP command and control
C. delivery
D. reconnaissance

Answer: D

NEW QUESTION 163
- (Exam Topic 2)
Which feature can provide NGFWs with User-ID mapping information?

A. GlobalProtect
B. Web Captcha
C. Native 802.1q authentication
D. Native 802.1x authentication

Answer: A

NEW QUESTION 165
- (Exam Topic 2)
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

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-qos/qos-interface-set

NEW QUESTION 167
- (Exam Topic 2)
When configuring the firewall for packet capture, what are the valid stage types?

A. Receive, management , transmit , and drop
B. Receive , firewall, send , and non-syn
C. Receive management , transmit, and non-syn
D. Receive , firewall, transmit, and drop

Answer: D

NEW QUESTION 172
- (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 177
- (Exam Topic 2)
Exhibit:

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

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


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

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

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

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


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

What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

A. ethernet1/7
B. ethernet1/5
C. ethernet1/6
D. ethernet1/3

Answer: D

NEW QUESTION 178
- (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 182
- (Exam Topic 2)
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. Wildfire update package
B. User-ID agent
C. Anti virus update package
D. Application and Threats update package

Answer: D

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.
: https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045

NEW QUESTION 186

- (Exam Topic 2)
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-update

NEW QUESTION 188
- (Exam Topic 2)
Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

A. CRL
B. CRT
C. OCSP
D. Cert-Validation-Profile
E. SSL/TLS Service Profile

Answer: AC

NEW QUESTION 189
- (Exam Topic 1)
Which CLI command displays the physical media that are connected to ethernetl/8?
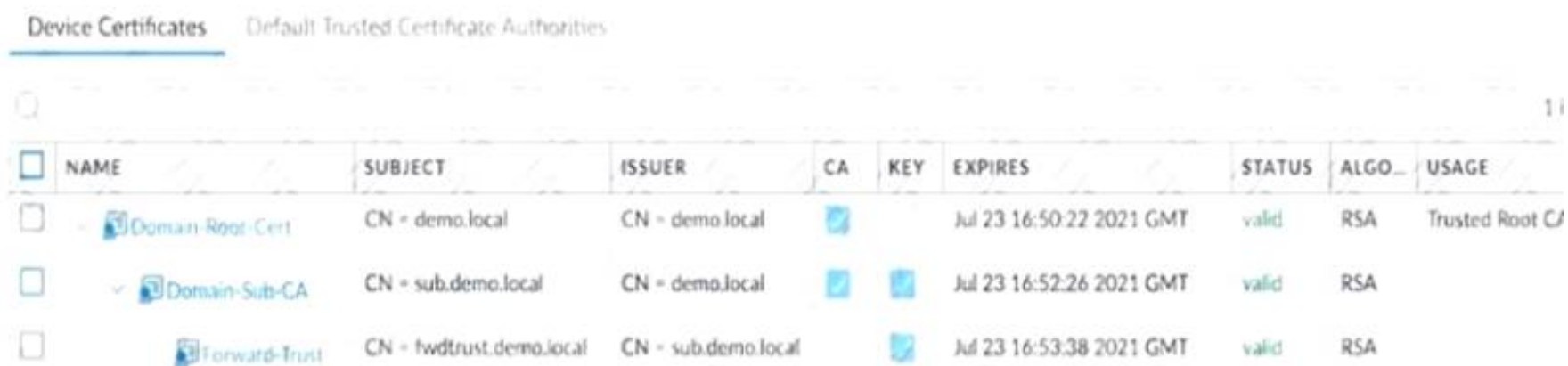
A. > show system state filter-pretty sys.si.p8.stats
B. > show interface ethernetl/8
C. > show system state filter-pretty sys.sl.p8.phy
D. > show system state filter-pretty sys.si.p8.med

Answer: D

NEW QUESTION 190
- (Exam Topic 1)
Refer to the exhibit.

Which certificate can be used as the Forward Trust certificate?

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

Answer: D

NEW QUESTION 194
- (Exam Topic 1)
When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

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

Answer: A

NEW QUESTION 197
- (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 201
- (Exam Topic 1)
In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

A. wildcard server certificate
B. enterprise CA certificate
C. client certificate
D. server certificate
E. self-signed CA certificate

Answer: BE

NEW QUESTION 206
- (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 207
- (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 211
- (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?

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 214
- (Exam Topic 1)
Match each type of DoS attack to an example of that type of attack

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Plan to defend your network against different types of DoS attacks:

≫ Application-Based Attacks
—Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it. An example of this is the Slowloris attack.

≫ Protocol-Based Attacks
—Also known as state-exhaustion attacks, these attacks target protocol weaknesses. A common example is a SYN flood attack.

≫ Volumetric Attacks
—High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing those resources. An example of this is a UDP flood attack.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense.ht

NEW QUESTION 216
- (Exam Topic 1)
When you configure a Layer 3 interface what is one mandatory step?

A. Configure Security profiles, which need to be attached to each Layer 3 interface
B. Configure Interface Management profiles which need to be attached to each Layer 3 interface
C. Configure virtual routers to route the traffic for each Layer 3 interface
D. Configure service routes to route the traffic for each Layer 3 interface

Answer: A

NEW QUESTION 219
- (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 220
- (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 223
- (Exam Topic 1)
During SSL decryption which three factors affect resource consumption1? (Choose three)

A. TLS protocol version
B. transaction size
C. key exchange algorithm
D. applications that use non-standard ports

E. certificate issuer

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ss

NEW QUESTION 226
- (Exam Topic 1)
A traffic log might list an application as "not-applicable" for which two reasons'? (Choose two)

A. 0The firewall did not install the session
B. The TCP connection terminated without identifying any application data
C. The firewall dropped a TCP SYN packet
D. There was not enough application data after the TCP connection was established

Answer: AD

NEW QUESTION 230
- (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 233
- (Exam Topic 1)
The UDP-4501 protocol-port is used between which two GlobalProtect components?

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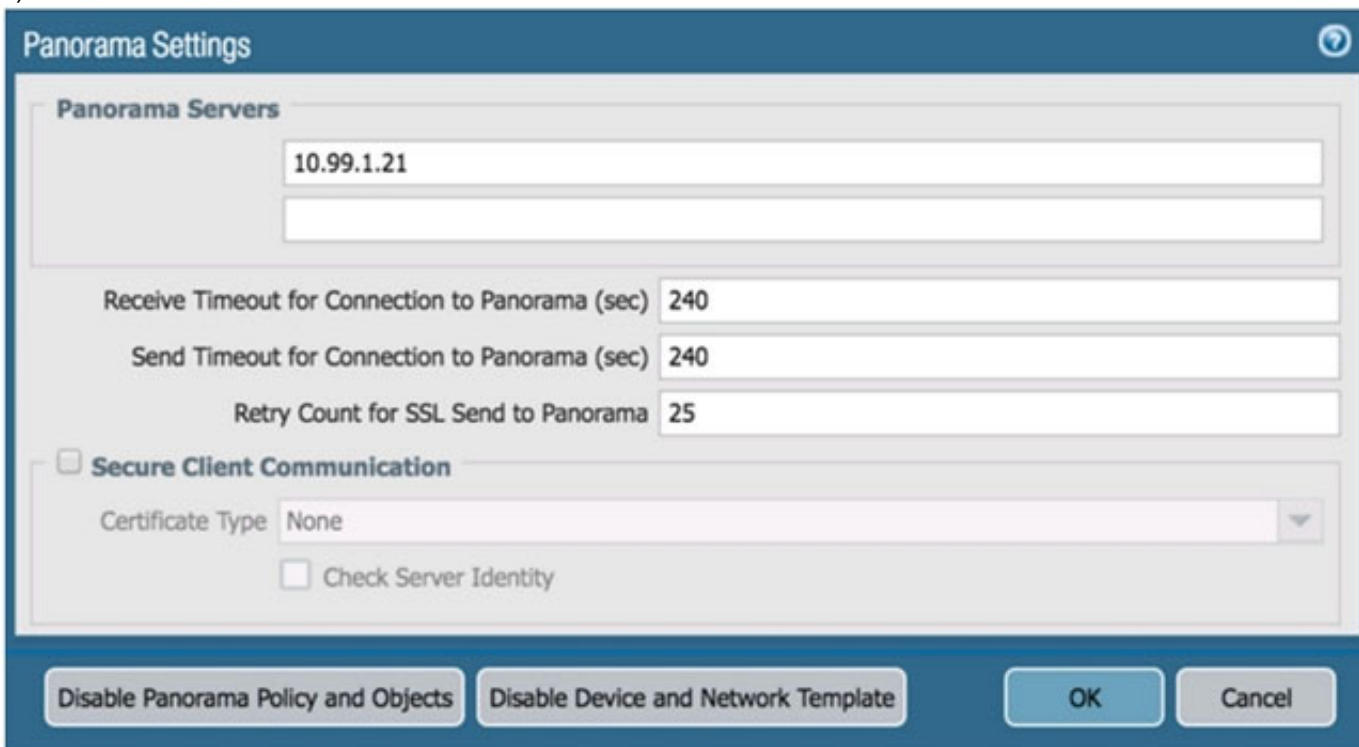D. GlobalProtect app and GlobalProtect portal

Answer: A

NEW QUESTION 236
- (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)

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)

Panorama Settings

Receive Timeout for Connection to Device (sec)	240
Send Timeout for Connection to Device (sec)	240
Retry Count for SSL Send to Device	25

☑ Share Unused Address and Service Objects with Devices

☐ Objects defined in ancestors will take higher precedence

Secure Server Communication

☐ Custom Certificate Only

SSL/TLS Service Profile	None
Certificate Profile	None
Authorization List	🔍 _____ 0 items ➡ ❌

☐ Identifier	Type	Value

⊕ Add ⊖ Delete

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

Disconnect Wait Time (min): [0 - 44640]

OK   Cancel

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

D. Option D

Answer: B

NEW QUESTION 240
- (Exam Topic 1)
What are two common reasons to use a "No Decrypt" action to exclude traffic from SSL decryption? (Choose two.)

A. the website matches a category that is not allowed for most users
B. the website matches a high-risk category
C. the web server requires mutual authentication
D. the website matches a sensitive category

Answer: AD

NEW QUESTION 245
- (Exam Topic 1)
As a best practice, which URL category should you target first for SSL decryption*?

A. Online Storage and Backup
B. High Risk
C. Health and Medicine
D. Financial Services

Answer: A

NEW QUESTION 246
- (Exam Topic 1)
An administrator wants to upgrade a firewall HA pair to PAN-OS 10.1 The firewalls are currently running PAN-OS 8.1.17.
Which upgrade path maintains synchronization of the HA session (and prevents network outage)?

A. Upgrade directly to the target major version
B. Upgrade one major version at a time
C. Upgrade the HA pair to a base image
D. Upgrade two major versions at a time

Answer: D

NEW QUESTION 251
- (Exam Topic 1)
Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

A. not-applicable
B. incomplete
C. unknown-ip
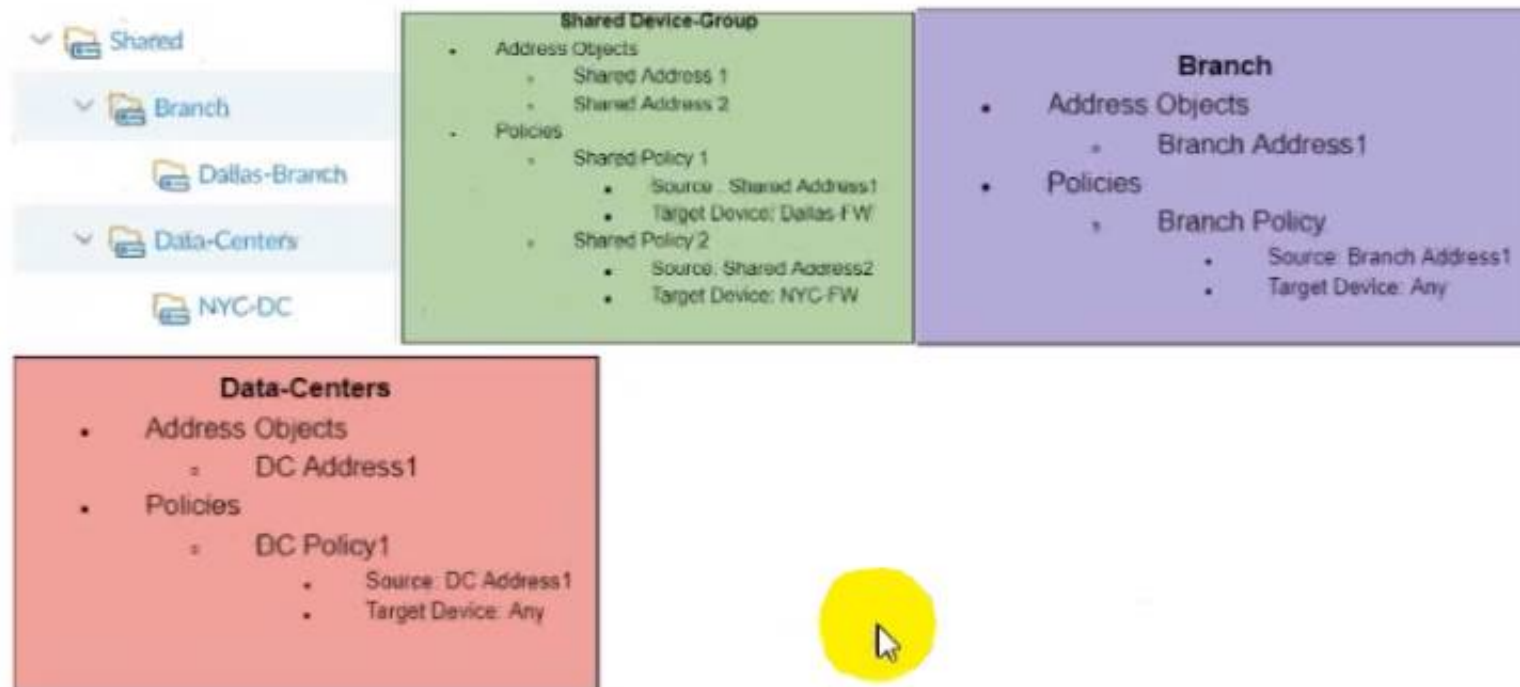D. unknown-udp

Answer: D

Explanation:
To safely enable applications you must classify all traffic, across all ports, all the time. With App-ID, the only applications that are typically classified as unknown traffic—tcp, udp or non-syn-tcp—in the ACC and the Traffic logs are commercially available applications that have not yet been added to App-ID, internal or custom applications on your network, or potential threats.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-cu

NEW QUESTION 254
- (Exam Topic 1)
The following objects and policies are defined in a device group hierarchy

Shared
- **Branch**
  - Dallas-Branch
- **Data-Centers**
  - NYC-DC

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

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

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

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

A)
Address Objects
-Shared Address1
-Shared Address2
-Branch Address1
Policies
-Shared Policy1
-Branch Policy1

B)
Address Objects
-Shared Address1
-Shared Address2
-Branch Address1
-DC Address1
Policies
-Shared Policy1
-Shared Policy2
-Branch Policy1

C)
Address Objects
-Shared Address 1
-Branch Address2 Policies -Shared Polic1 l -Branch 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 259
- (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 263
- (Exam Topic 1)
Please match the terms to their corresponding definitions.

management plane

signature matching

security processing

network processing

Answer Area

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

management plane

signature matching

security processing

network processing

Answer Area

provides configurat network processing inctions on a separate processor

stream-based, unifo security processing ing vulnerability exploits (IPS), virus,

high-density paralle management plane vare acceleration for standardized compl

hardware-accelerat signature matching MAC lookup, and NAT

NEW QUESTION 264
- (Exam Topic 1)
Given the following configuration, which route is used for destination 10.10.0.4?

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

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

Answer: A

NEW QUESTION 265

- (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 268
- (Exam Topic 2)
Which four NGFW multi-factor authentication factors are supported by PAN-OS? (Choose four.)

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

Answer: ABDF

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/authentication/authentication-types/multi-factor-aut

---

NEW QUESTION 271
- (Exam Topic 2)
For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two)

A. equal-cost multipath
B. ingress processing errors
C. rule match with action "allow"
D. rule match with action "deny"

Answer: BD

NEW QUESTION 274
- (Exam Topic 2)
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

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

Answer: DE

NEW QUESTION 278
- (Exam Topic 2)
An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

A. Port Inspection
B. Certificate revocation
C. Content-ID
D. App-ID

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/quality-of-service/qos-for-applications-and


NEW QUESTION 281
- (Exam Topic 2)
When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

A. Load named configuration snapshot
B. Load configuration version
C. Save candidate config
D. Export device state

Answer: D

NEW QUESTION 283

- (Exam Topic 2)
Refer to the exhibit.

DST NAT: 1.1.1.100 to 10.1.1.100 Dst Port 80
1.1.1.100 to 10.1.1.101 Dst Port 22
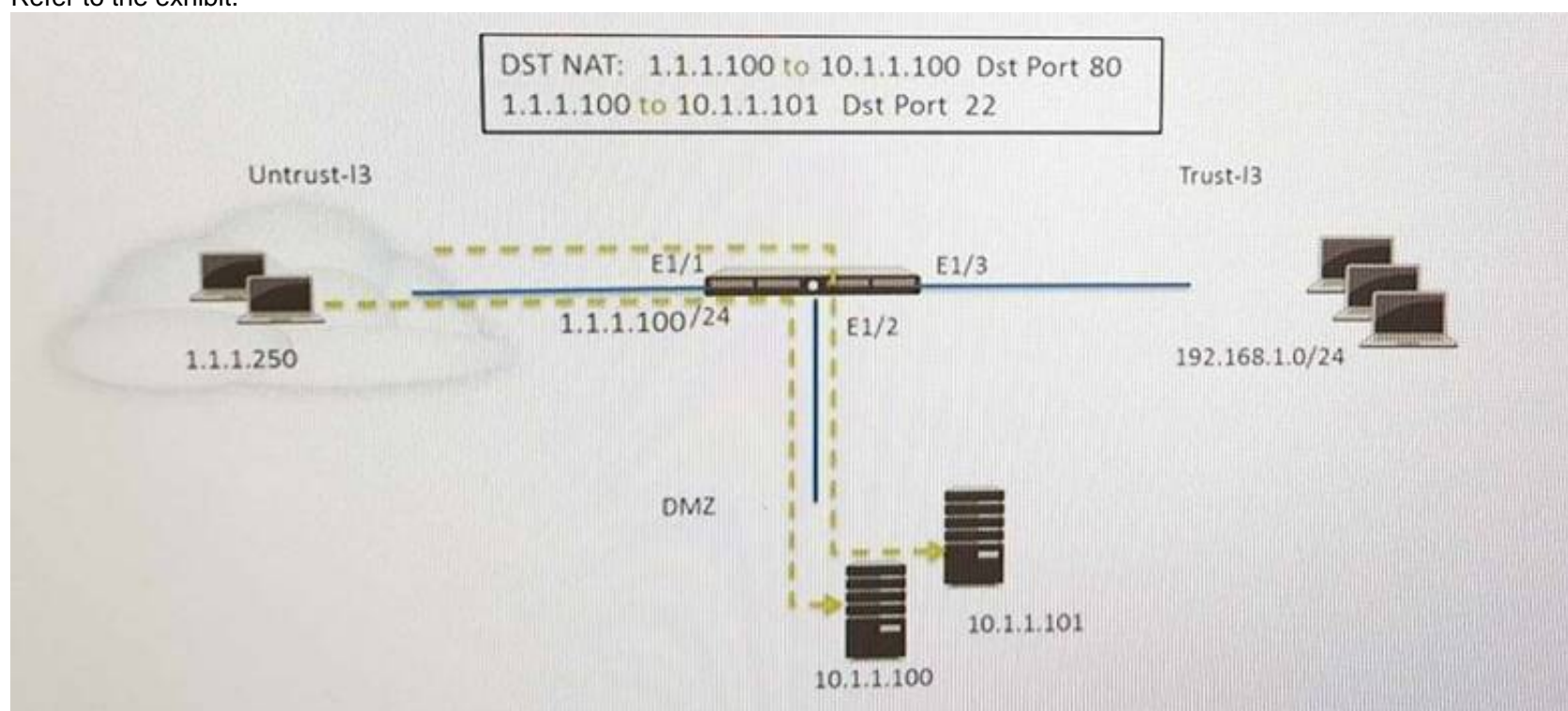
An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.)
Which two security policy rules will accomplish this 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 286
- (Exam Topic 2)
How can an administrator configure the NGFW to automatically quarantine a device using GlobalProtect?

A. by adding the device's Host ID to a quarantine list and configure GlobalProtect to prevent users fromconnecting to the GlobalProtect gateway from a quarantined device
B. by using secunty policies, log forwarding profiles, and log settings.
C. by exporting the list of quarantined devices to a pdf or csv file by selecting PDF/CSV at the bottom of the Device Quarantine page and leveraging the approbate XSOAR playbook
D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

Answer: A

NEW QUESTION 289
- (Exam Topic 2)
What are two benefits of nested device groups in Panorama? (Choose two.)

A. Reuse of the existing Security policy rules and objects
B. Requires configuring both function and location for every device
C. All device groups inherit settings form the Shared group
D. Overwrites local firewall configuration

Answer: AC

Explanation:
Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.

NEW QUESTION 293
- (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 297
- (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 299
- (Exam Topic 3)
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 300
- (Exam Topic 3)
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 302
- (Exam Topic 3)
The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.
Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

A. test panoramas-connect 10.10.10.5
B. show panoramas-status
C. show arp all I match 10.10.10.5
D. topdump filter "host 10.10.10.5
E. debug dataplane packet-diag set capture on

Answer: BD

NEW QUESTION 307
- (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 311
- (Exam Topic 3)
A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.
What could cause this condition?

A. The firewall does not have an active WildFire subscription.
B. The engineer's account does not have permission to view WildFire Submissions.
C. A policy is blocking WildFire Submission traffic.
D. Though WildFire is working, there are currently no WildFire Submissions log entries.

Answer: B

NEW QUESTION 316
- (Exam Topic 3)
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 321
- (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.
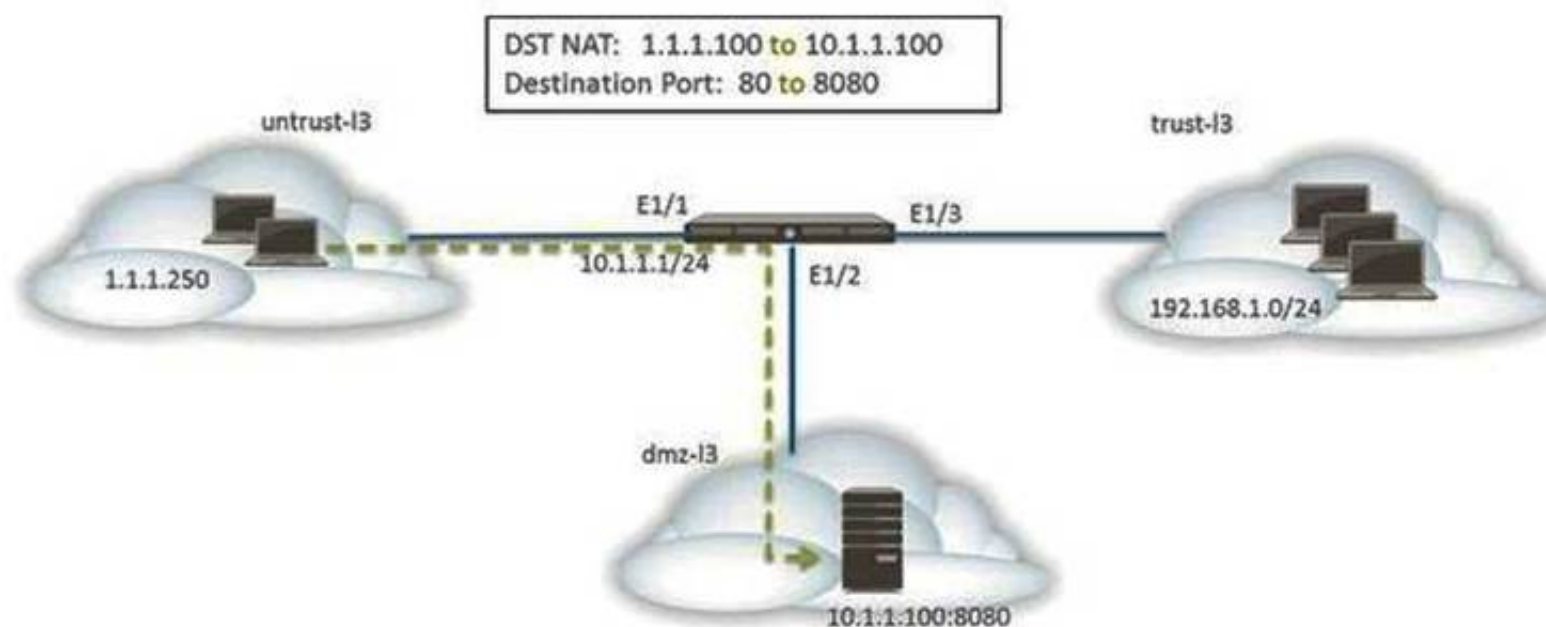
Which NAT and security rules must be configured on the firewall? (Choose two)

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 322
- (Exam Topic 3)
Support for which authentication method was added in PAN-OS 8.0?

A. RADIUS
B. LDAP
C. Diameter
D. TACACS+

Answer: D

Explanation:
https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1

NEW QUESTION 325
- (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 329
- (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 330
- (Exam Topic 3)
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 334
- (Exam Topic 3)
Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon?

A. Certificate revocation list
B. Trusted root certificate
C. Machine certificate
D. Online Certificate Status Protocol

Answer: C

NEW QUESTION 339
- (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 343
- (Exam Topic 3)
Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.
Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

A. Create a custom Application without signatures, then create an Application Override policy that includes the source, Destination, Destination Port/Protocol and Custom Application of the traffic.
B. Wait until an official Application signature is provided from Palo Alto Networks.
C. Modify the session timer settings on the closest referanced application to meet the needs of the in-house application
D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

Answer: D

NEW QUESTION 344
- (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 346

- (Exam Topic 3)
A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.
Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?(Choose three)

A. Download PAN-OS 8.0.4 files from the support site and install them on each firewall after manually uploading.
B. Download PAN-OS 8.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.
C. Push the PAN-OS 8.0.4 updates from the support site to install on each firewall.
D. Push the PAN-OS 8.0.4 update from one firewall to all of the other remaining after updating one firewall.
E. Download and install PAN-OS 8.0.4 directly on each firewall.
F. Download and push PAN-OS 8.0.4 from Panorama to each firewall.

Answer: ACF

NEW QUESTION 351
- (Exam Topic 3)
A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

A. From the CLI, issue the show counter global filter pcap yes command.
B. From the CLI, issue the show counter global filter packet-filter yes command.
C. From the GUI, select show global counters under the monitor tab.
D. From the CLI, issue the show counter interface command for the ingress interface.

Answer: B

NEW QUESTION 356
- (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 360
- (Exam Topic 3)
A company.com wants to enable Application Override. Given the following screenshot:

Which two statements are true if Source and Destination traffic match the Application Override policy? (Choose two)

A. Traffic that matches "rtp-base" will bypass the App-ID and Content-ID engines.
B. Traffic will be forced to operate over UDP Port 16384.
C. Traffic utilizing UDP Port 16384 will now be identified as "rtp-base".
D. Traffic utilizing UDP Port 16384 will bypass the App-ID and Content-ID engines.

Answer: AC

NEW QUESTION 361
- (Exam Topic 3)
The GlobalProtect Portal interface and IP address have been configured. Which other value needs to be defined to complete the network settings configuration of GlobalPortect Portal?

A. Server Certificate
B. Client Certificate
C. Authentication Profile
D. Certificate Profile

Answer: A

Explanation:
(https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-GlobalProtect/ta-p/58351)

NEW QUESTION 364
- (Exam Topic 3)
Only two Trust to Untrust allow rules have been created in the Security policy Rule1 allows google-base
Rule2 allows youtube-base
The youtube-base App-ID depends on google-base to function. The google-base App-ID implicitly uses SSL and web-browsing. When user try to accesss https://www.youtube.com in a web browser, they get an error indecating that the server cannot be found.
Which action will allow youtube.com display in the browser correctly?

A. Add SSL App-ID to Rule1
B. Create an additional Trust to Untrust Rule, add the web-browsing, and SSL App-ID's to it
C. Add the DNS App-ID to Rule2
D. Add the Web-browsing App-ID to Rule2

Answer: C

NEW QUESTION 366
- (Exam Topic 3)
An Administrator is configuring an IPSec VPN toa Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is th output from the command:
less mp-log ikemgr.log:

```
less mp-log ikemgr.log:

2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:52:33 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <==== Due to
timeout.
2014-08-05 03:52:33 [INFO]: ====> PHASE-1 SA DELETED <====
====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <====
2014-08-05 03:53:54 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed.SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <==== Due to
timeout.
2014-08-05 03:53:54 [INFO]: ====> PHASE-1 SA DELETED <====
```

What could be the cause of this problem?

A. The public IP addresse do not match for both the Palo Alto Networks Firewall and the ASA.
B. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.
C. The shared secerts do not match between the Palo Alto firewall and the ASA
D. The deed peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

Answer: B

NEW QUESTION 370
- (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 373
- (Exam Topic 3)
A network design change requires an existing firewall to start accessing Palo Alto Updates from a data plane interface address instead of the management interface.
Which configuration setting needs to be modified?

A. Service route
B. Default route
C. Management profile
D. Authentication profile

Answer: A

NEW QUESTION 374
- (Exam Topic 3)
Which URL Filtering Security Profile action togs the URL Filtering category to the URL Filtering log?

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

Answer: B

NEW QUESTION 379
- (Exam Topic 3)
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 382
- (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 384
- (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 387
- (Exam Topic 3)
In an enterprise deployment, a network security engineer wants to assign to a group of administrators without creating local administrator accounts on the firewall.
Which authentication method must be used?

A. LDAP
B. Kerberos
C. Certification based authentication
D. RADIUS with Vendor-Specific Attributes

Answer: D

NEW QUESTION 391
- (Exam Topic 3)

When performing the "ping" test shown in this CLI output:

What will be the source address in the ICMP packet?

A. 10.30.0.93
B. 10.46.72.93
C. 10.46.64.94
D. 192.168.93.1

Answer: C

NEW QUESTION 396
- (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 401
- (Exam Topic 3)
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 402
- (Exam Topic 3)
What must be used in Security Policy Rule that contain addresses where NAT policy applies?

A. Pre-NAT addresse and Pre-NAT zones
B. Post-NAT addresse and Post-Nat zones
C. Pre-NAT addresse and Post-Nat zones
D. Post-Nat addresses and Pre-NAT zones

Answer: C

NEW QUESTION 403
- (Exam Topic 3)
A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's firewall.

Which interface configuration will accept specific VLAN IDs?
Which two benefits are gained from having both rule 2 and rule 3 presents? (choose two)

A. A report can be created that identifies unclassified traffic on the network.
B. Different security profiles can be applied to traffic matching rules 2 and 3.
C. Rule 2 and 3 apply to traffic on different ports.
D. Separate Log Forwarding profiles can be applied to rules 2 and 3.

Answer: BD

NEW QUESTION 407
- (Exam Topic 3) A
users traffic traversing a Palo Alto networks NGFW sometimes can reach http //www company com At other times the session times out. At other times the session times out The NGFW has been configured with a PBF rule that the user traffic matches when it goes to http://www.company.com goes to http://www company com
How can the firewall be configured to automatically disable the PBF rule if the next hop goes down?

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

Answer: C

NEW QUESTION 409
- (Exam Topic 3)
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 410
- (Exam Topic 3)
An administrator has left a firewall to use the data of port for all management service which there functions are performed by the data face? (Choose three.)

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

Answer: ACD

NEW QUESTION 412
- (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 413
- (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 414
- (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 418
- (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 423
- (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 426
- (Exam Topic 3)
Which interface configuration will accept specific VLAN IDs?

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

Answer: B

NEW QUESTION 427
- (Exam Topic 3)
How is the Forward Untrust Certificate used?

A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has be decrypted/
B. It is used when web servers request a client certificate.
C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by firewall.
D. It is used for Captive Portal to identify unknown users.

Answer: C

NEW QUESTION 430
- (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 431
- (Exam Topic 3)
A company has a pair of Palo Alto Networks firewalls configured as an Acitve/Passive High Availability (HA) pair.
What allows the firewall administrator to determine the last date a failover event occurred?

A. From the CLI issue use the show System log
B. Apply the filter subtype eq ha to the System log
C. Apply the filter subtype eq ha to the configuration log
D. Check the status of the High Availability widget on the Dashboard of the GUI

Answer: B

NEW QUESTION 433
- (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 436
- (Exam Topic 3)
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 440
- (Exam Topic 3)
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 444
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

PCNSE Practice Exam Features:

* PCNSE Questions and Answers Updated Frequently

* PCNSE Practice Questions Verified by Expert Senior Certified Staff

* PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PCNSE Practice Test Here](https://www.certshared.com/exam/PCNSE/)