PaloAltoNetworks.PCNSE.v2021-11-16.q121

Exam Code:	PCNSE
Exam Name:	Palo Alto Networks Certified Network Security Engineer Exam
Certification Provider:	Palo Alto Networks
Free Question Number:	121
Version:	v2021-11-16
# of views:	6315
# of Questions views:	1210
https://www.freepdfdumps.com/PaloAltoNetworks.PCNSE.v2021-11-16.q121.html	

NEW QUESTION: 1
In a virtual router, which object contains all potential routes?
A. MIB
B. RIB
C. SIP
D. FIB
Answer: (SHOW ANSWER)
Reference: https://www.google.com/url?
sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0ahUKEwiOkbfYzPzXAhVnEJoKHcwVCg4QFghiMAk
& url=https%3A%2F%
2Flive.paloaltonetworks.com%2Ftwzvq79624%2Fattachments%2Ftwzvq79624%2Fdocumentation_tk
b%2F487%2F1%2FRoute% 2520Redistribution%2520and%2520Filtering%2520TechNote%2520-
% 2520Rev% 2520B. pdf&usg=AOvVaw0H9qgaJK0oI2xjIJBNo1Km

NEW QUESTION: 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 (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-authentication

NEW QUESTION: 3
What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

A. Clean
B. Bengin
C. Adware
D. Suspicious
E. Grayware
F. Malware
Answer: B,E,F (LEAVE A REPLY)
Explanation
https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayw

NEW QUESTION: 4
The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?
A. 7-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Source User, URL Category, and Source Security Zone
B. 9-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application, and URL Category
C. 5-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Protocol
D. 6-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Protocol, and Source Security Zone
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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: (SHOW ANSWER)
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy- user-id-in-a-large-scale-network

NEW QUESTION: 6

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 (LEAVE A REPLY)
Panorama evaluates the templates listed in a stack configuration from top to bottom, with higher templates having priority.
https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/panorama- overview/templates-and-template-stacks

NEW QUESTION: 7
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device- dynamic-updates

NEW QUESTION: 8
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 7.0.4 across the enterprise? (Choose three)
A. Push the PAN-OS 7.0.4 updates from the support site to install on each firewall.
B. Download and push PAN-OS 7.0.4 from Panorama to each firewall.
C. Download and install PAN-OS 7.0.4 directly on each firewall.
D. Download PAN-OS 7.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.
E. Download PAN-OS 7.0.4 files from the support site and install them on each firewall after manually uploading.

F. Push the PAN-OS 7.0.4 update from one firewall to all of the other remaining after updating one firewall.

Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 9

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

A. port mapping

B. server monitoring

C. client probing

D. XFF headers

Answer: (SHOW ANSWER)

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

NEW QUESTION: 10

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

A. Clean Up Rules

B. Stealth Rules

C. Post Rules

D. Pre Rules

E. Default Rules

Answer: (SHOW ANSWER)

https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manage-firewalls/manage-the-rule-hierarchy

NEW QUESTION: 11

Refer to the exhibit.

Which certificates can be used as a Forwarded Trust certificate?

A. Domain Sub-CA

B. Domain-Root-Cert

C. Forward_Trust

D. Certificate from Default Trust Certificate Authorities

Answer: (SHOW ANSWER)

NEW QUESTION: 12

Refer to the exhibit.

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

A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
D. Untrust (Any) to DMZ (10.1.1.1), ssh -Allow
E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow
Answer: C,D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-many-mapping#

NEW QUESTION: 13
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 (LEAVE A REPLY)
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/5

NEW QUESTION: 14
Which two interface types can be used when configuring GlobalProtect Portal?(Choose two)
A. Tunnel
B. Loopback
C. Virtual Wire
D. Layer 3
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)
A. DoS Protection Profile
B. Data Filtering Profile
C. Zone Protection Profile
D. Vulnerability Object
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 16
Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?

A. port mapping
B. server monitoring
C. client probing
D. XFF headers
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user- mapping-for-terminal-server-users

NEW QUESTION: 17
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: B (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manag templates-and-template-stacks/configure-a-template-stack

NEW QUESTION: 18
Which operation will impact performance of the management plane?
A. DoS protection
B. WildFire submissions
C. generating a SaaS Application report
D. decrypting SSL sessions
Answer: (SHOW ANSWER)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSvCAK

NEW QUESTION: 19
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:
B:
C:
D:
A. Option B
B. Option D
C. Option A
D. Option C
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
Decrypted packets from the website https://www.microsoft.com will appear as which application and service within the Traffic log?
A. SSL and 80
B. web-browsing and 80
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.
C. web-browsing and 443
D. SSL and 443
Answer: (SHOW ANSWER)

NEW QUESTION: 21
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 (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence

NEW QUESTION: 22
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: A,E,F (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrat

NEW QUESTION: 23
An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab. Which profile is the cause of the missing Policies tab?
A. Authentication
B. WebUI
C. Authorization
D. Admin Role
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
Starting with PAN-OS version 9.1, Global logging information is now recoded in which firewall log?
A. Globalprotect
B. Authentication
C. Configuration
D. System
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which event will happen if an administrator uses an Application Override Policy?
A. App-ID processing time is increased.
B. Threat-ID processing time is decreased.
C. The application name assigned to the traffic by the security rule is written to the Traffic log.
D. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
When performing the "ping" test shown in this CLI output:
What will be the source address in the ICMP packet?
A. 10.46.72.93
B. 192.168.93.1
C. 10.30.0.93
D. 10.46.64.94

Answer: (SHOW ANSWER)

NEW QUESTION: 27
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:
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 deed peer detection settings do not match between the Palo Alto Networks Firewall and the ASA
C. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.
D. The shared secerts do not match between the Palo Alto firewall and the ASA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is
allowed to access an internal application that contains highly-sensitive business data?
A. Application Override policy
B. Authentication policy
C. Security policy
D. Decryption policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
Which processing order will be enabled when a Panorama administrator selects the setting "Objects defined in ancestors will take higher precedence?"
A. Descendant objects will take precedence over other descendant objects.
B. Descendant objects will take precedence over ancestor objects.
C. Ancestor objects will have precedence over descendant objects.
D. Ancestor objects will have precedence over other ancestor objects.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device- setup-management

NEW QUESTION: 30
Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?
A. VM-200
B. VM-1000-HV
C. VM-100

D. VM-300
Answer: (SHOW ANSWER)

NEW QUESTION: 31
After Migrating from an ASA firewall to a Palo Alto Networks Firewall, the VPN connection between a remote network and the Palo Alto Networks Firewall is not establishing correctly.
The following entry is appearing in the logs:
Pfs group mismatched: my:0 peer:2
Which setting should be changed on the Palo Alto Networks Firewall to resolve this error message?
A. Update the IPSec Crypto profile for the Vendor IPSec Tunnel from no-pfs to group2.
B. Update the IKE Crypto profile for the Vendor IKE gateway from no pfs to group2.
C. Update the IKE Crypto profile for the Vendor IKE gateway from group2 to no pfs
D. Update- the IPSec Crypto profile for the Vendor IPSec Tunnel from group2 to no-pfs.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?
A. Port mapping
B. Syslog listening
C. Client Probing
D. Server monitoring
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
Which field is optional when creating a new Security Policy rule?
A. Name
B. Description
C. Destination Zone
D. Action
E. Source Zone
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?
A. Packet Capture
B. Session Browser
C. Application Command Center
D. TCP Dump
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
Based on the following image, what is the correct path of root, intermediate, and end-user certificate?
A. VeriSign > Palo Alto Networks > Symantec
B. Palo Alto Networks > Symantec > VeriSign
C. Symantec > VeriSign > Palo Alto Networks
D. VeriSign > Symantec > Palo Alto Networks
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
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. Enable User-ID on the zone object for the source zone
D. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
E. Configure a RADIUS server profile to point to a domain controller
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 37
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 (LEAVE A REPLY)
The GlobalProtect pre-logon connect method is a feature that enables GlobalProtect to authenticate the agent and establish the VPN tunnel to the GlobalProtect gateway using a pre- installed machine certificate before the user has logged in.

https://www.paloaltonetworks.com/documentation/60/globalprotect/global_protect_6-0/globalprotect-quick-configs/remote-access-vpn-with-pre-logon

NEW QUESTION: 38
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: A,B,D,F (LEAVE A REPLY)
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure- multi-factor-authentication

NEW QUESTION: 39
DRAG DROP
When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.
Answer options may be used more than once or not at all.
Answer:
Explanation:
IMAP , POP3 , SMTP - > Alert
HTTP,FTP,SMB -> Reset-both

NEW QUESTION: 40
Which event will happen if an administrator uses an Application Override Policy?
A. Threat-ID processing time is decreased.
B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
C. The application name assigned to the traffic by the security rule is written to the Traffic log.
D. App-ID processing time is increased.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override/ta-p/65513

NEW QUESTION: 41
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: (SHOW ANSWER)
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 A 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-O

NEW QUESTION: 42
In High Availability, which information is transferred via the HA data link?
A. session information
B. User-ID information
C. HA state information
D. heartbeats
Answer: (SHOW ANSWER)

NEW QUESTION: 43

A. A CLI command will forward the pre-existing logs to PanoramA.
B. 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?
C. The log database will need to exported form the firewalls and manually imported into PanoramA.
D. Use the ACC to consolidate pre-existing logs.
E. Use the import option to pull logs into PanoramA.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
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: C,D (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device- dynamic-updates

NEW QUESTION: 45
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 assign untagged (native) traffic to its own zone.
Which option differentiates multiple VLANs 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 Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router.
The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface to a unique zone. Do not assign any interface an IP address.
C. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the "Tag Allowed" field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.
D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?
A. Firewall connectivity to a CRL
B. Root certificate imported into the firewall with "Trust" enabled
C. Importation of a certificate from an HSM
D. Security policy rule allowing SSL to the target server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content-IDs to traffic?
A. Select download-and-install
B. Select download-only
C. Select download-and-install, with "Disable new apps in content update" selected
D. Select disable application updates and select "Install only Threat updates"
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 48
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 Maximum Ingress
B. Inbound profile with Guaranteed Egress
C. Outbound profile with Guaranteed Ingress
D. Inbound profile with Maximum Egress
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
An administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. the following is the output from the command:
What could be the cause of this problem?
A. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.
B. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
C. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.
D. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.
Answer: (SHOW ANSWER)

NEW QUESTION: 50
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. DMZ-L3
B. Untrust-L3
C. Guest-L3
D. Trust-L3
Answer: (SHOW ANSWER)

NEW QUESTION: 51
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: B (LEAVE A REPLY)
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Mana Port/ta-p/59034 user@PA# set deviceconfig system speed-duplex100Mbps-full-duplex 100Mbps-full-duplex
100Mbps-half-duplex 100Mbps-half-duplex10Mbps-full-duplex 10Mbps-full-duplex10Mbps-half-duplex 10Mbps-half-duplex1Gbps-full-duplex 1Gbps-full-duplex1Gbps-half-duplex 1Gbps-half-duplex auto-negotiate auto-negotiate

NEW QUESTION: 52
When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinhole enabled, generating a traffic log.
What will be the destination IP Address in that log entry?
A. The IP Address of sinkhole.paloaltonetworks.com
B. The IP Address of the command-and-control server

C. The IP Address specified in the sinkhole configuration
D. The IP Address of one of the external DNS servers identified in the anti-spyware database
Answer: C (LEAVE A REPLY)
https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864

NEW QUESTION: 53
When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.
Answer options may be used more than once or not at all.
Answer:
Explanation
IMAP , POP3 , SMTP - > Alert
HTTP,FTP,SMB -> Reset-both

NEW QUESTION: 54
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 ACC to consolidate pre-existing logs.
B. The log database will need to exported form the firewalls and manually imported into Panorama.
C. A CLI command will forward the pre-existing logs to Panorama.
D. Use the import option to pull logs into Panorama.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
Refer to the exhibit.
An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panoram a. 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. Option
B. Option
C. Option
D. Option
Answer: B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html#

NEW QUESTION: 56
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)
A. link requirements
B. IP Addresses
C. branch and hub locations
D. the name of the ISP
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 57
Which event will happen if an administrator uses an Application Override Policy?
A. Threat-ID processing time is decreased.
B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
C. The application name assigned to the traffic by the security rule is written to the Traffic log.
D. App-ID processing time is increased.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#

NEW QUESTION: 58
During the packet flow process, which two processes are performed in application identification? (Choose two.)
A. Session application identified.
B. Pattern based application identification
C. Application override policy match
D. Application changed from content inspection
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 59
A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:
* Users outside the company are in the "Untrust-L3" zone.
* The web server physically resides in the "Trust-L3" zone.
* Web server public IP address: 23.54.6.10
* Web server private IP address: 192.168.1.10
Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server?
(Choose two.)
A. Destination IP of 192.168.1.10
B. UntrustL3 for both Source and Destination Zone
C. Destination IPof 23.54.6.10

D. UntrustL3 for Source Zone and Trust-L3 for Destination Zone
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 60
An administrator just submitted a newly found piece of spyware for WildFire analysis. The spyware passively monitors behavior without the user's knowledge.
What is the expected verdict from WildFire?
A. Grayware
B. Malware
C. Spyware
D. Phishing
Answer: A (LEAVE A REPLY)
Explanation
Wildfire verdictions are as follow1-Begnin2-Greyware3-Mallicious4-Phishing
https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-concepts/ve

NEW QUESTION: 61
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 (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-auth

NEW QUESTION: 62
Panorama provides which two SD-WAN functions? (Choose two.)
A. network monitoring

B. control plane
C. data plane
D. physical network links
Answer: B,C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 63
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 (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text

NEW QUESTION: 64
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: A,D (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC

NEW QUESTION: 65
Which three authentication services can administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)
A. Kerberos
B. PAP
C. SAML
D. TACACS+
E. RADIUS
F. LDAP
Answer: A,C,F (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication The administrative accounts are defined on an external

SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall. For details, see:
Configure SAML Authentication Configure TACACS+ Authentication Configure RADIUS Authentication

NEW QUESTION: 66
A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.
Which Security Profile type will prevent these behaviors?
A. Anti-Spyware
B. WildFire
C. Vulnerability Protection
D. Antivirus
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/anti-spyware-profiles

NEW QUESTION: 67
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 (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/quality-of-service/qos-concepts/qos-for-applications-and-users#idaed4e749-80b4-4641-a37c-c741aba562e9

NEW QUESTION: 68
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:
B:
C:

D:

A. Option C

B. Option A

C. Option D

D. Option B

Answer: A (LEAVE A REPLY)

NEW QUESTION: 69

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: D,E,F (LEAVE A REPLY)

Reference: https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-support

NEW QUESTION: 70

When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinkhole enabled, generating a traffic log.

What will be the destination IP address in that log entry?

A. The IP address specified in the sinkhole configuration.

B. The IP address of the command-and-control server.

C. The IP address of sinkhole.paloaltonetworks.com

D. The IP address of one of the external DNS servers identified in the anti-spyware database.

Answer: A (LEAVE A REPLY)

Change the "Action on DNS queries" to 'sinkhole'.

Click in the Sinkhole IPv4 field and type in the fake IP. The example here shows using 1.1.1.1 for simplicity, but as long as this fake IP is not used inside of the network, then it should be Ok.

Alternatively, you can also use either a Loopback IP (127.0.0.1) or Palo Alto Networks Sinkhole IP (71.19.152.112).

https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/ta- p/58891

NEW QUESTION: 71

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

A. port mapping

B. server monitoring

C. client probing
D. XFF headers
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-m

NEW QUESTION: 72
The certificate information displayed in the following image is for which type of certificate?
Exhibit:
A. Web Server certificate
B. Public CA signed certificate
C. Self-Signed Root CA certificate
D. Forward Trust certificate
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
Which feature must you configure to prevent users form accidentally submitting their corporate credentials
to a phishing website?
A. URL Filtering profile
B. Zone Protection profile
C. Anti-Spyware profile
D. Vulnerability Protection profile
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-
credential-phishing

NEW QUESTION: 74
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 (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-many-mapping

NEW QUESTION: 75
A logging infrastructure may need to handle more than 10,000 logs per second.
Which two options support a dedicated log collector function? (Choose two)
A. Panorama virtual appliance on ESX(i) only
B. M-500
C. M-100 with Panorama installed
D. M-100
Answer: (SHOW ANSWER)
Explanation
(https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181)

NEW QUESTION: 76
Given these tables:
SVR1 is a webserver hosted in the DMZ zone. The FQDN of www.myserver.com is registered to an external DNS provider and resolves to 203.1.200.123 in the Untrust-L3 zone. Users in the Trust-L3 zone use the external FQDN to access SVR1.
Which NAT rule will process traffic sourced from the Trust-L3 zone destined for SVR1?
A. NAT2
B. NAT4
C. NAT1
D. NAT3
Answer: D (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEiCAK
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cln3CAC

NEW QUESTION: 77
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. The log database will need to exported form the firewalls and manually imported into Panorama.
B. A CLI command will forward the pre-existing logs to Panorama.
C. Use the import option to pull logs into Panorama.
D. Use the ACC to consolidate pre-existing logs.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 78
Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)
A. Verify AutoFocus status using the CLI "test" command.
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: (SHOW ANSWER)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/getting-started/enable- autofocus-threat-intelligence

NEW QUESTION: 79
Support for which authentication method was added in PAN-OS 8.0?
A. RADIUS
B. LDAP
C. Diameter
D. TACACS+
Answer: D (LEAVE A REPLY)
Explanation
https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1

NEW QUESTION: 80
An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?
A. Enable and configure the Packet Buffer Protection thresholds.
Enable Packet Buffer Protection per ingress zone.
B. Enable and then configure Packet Buffer thresholds.
Enable Interface Buffer protection.
C. Create and Apply Zone Protection Profiles in all ingress zones.
Enable Packet Buffer Protection per ingress zone.
D. Configure and apply Zone Protection Profiles for all egress zones.
Enable Packet Buffer Protection per egress zone.

E. Enable per-vsys Session Threshold alerts and triggers for Packet Buffer Limits.
Enable Zone Buffer Protection per zone.
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos- protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection

NEW QUESTION: 81
Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)
A. The firewall is in multi-vsys mode.
B. The traffic is offloaded.
C. The traffic does not match the packet capture filter.
D. The firewall's DP CPU is higher than 50%.
Answer: (SHOW ANSWER)
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-ha offload

NEW QUESTION: 82
An administrator wants to upgrade an NGFW from PAN-OS® 7.1.2 to PAN-OS® 8.0.2. The firewall is not a part of an HA pair.
What needs to be updated first?
A. PAN-OS® Upgrade Agent
B. Applications and Threats
C. XML Agent
D. WildFire
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
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 (LEAVE A REPLY)

NEW QUESTION: 84
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 Untrust (10.1.1.1) Web-browsing -Allow
D. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 85
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 Device Group with the appropriate IPSec tunnel settings
C. Create a Template with the appropriate IPSec tunnel settings
D. Create a Device Group with the appropriate IKE Gateway settings
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
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 Security Policy rule with vulnerability Security Profile attached.
B. Create a Dynamic Address Group for untrusted sites
C. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
D. Enable the "Block sessions with untrusted issuers" setting.
E. Create a no-decrypt Decryption Policy rule.
Answer: (SHOW ANSWER)

NEW QUESTION: 87
ON NO: 80
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.
Which Security Profile type will prevent this attack?
A. Vulnerability Protection
B. Anti-Spyware
C. URL Filtering
D. Antivirus
Answer: A (LEAVE A REPLY)

Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profile vulnerability-protection

NEW QUESTION: 88
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 (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-netw

NEW QUESTION: 89
What happens when the traffic log shows an internal host attempting to open a session to a properly configured sinkhole address?
A. The internal host attempted to use DNS to resolve a known malicious domain into an IP address.
B. A malicious domain tried to contact an internal DNS server.
C. A rogue DNS server used the sinkhole address to direct traffic to a known malicious domain.
D. The internal host tried to resolve a DNS query by connecting to a rogue DNS server.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
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 immediate action with the first observed packet based on port numbers. Use ofan "application" allows the firewall to take immediate action it the port being used is a member of the application standardport list
B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use ofan "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the portsbeing used.
C. Use of a "service" enables the firewall to take action after enough packets allow for App-ID identification
D. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use ofa friendly application name instead of port numbers.
Answer: (SHOW ANSWER)

NEW QUESTION: 91
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. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question:.
C. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question:.
D. Configure path monitoring for the next hop gateway on the default route in the virtual router.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 92
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. System Utilization log
D. Resources widget
Answer: D (LEAVE A REPLY)

NEW QUESTION: 93
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 (LEAVE A REPLY)
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: 94
Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)
A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.
D. Enter the command logger-mode enable the enter Y to confirm the change to Log Collector mode.
E. Log in the Panorama CLI of the dedicated Log Collector
Answer: B,E (LEAVE A REPLY)
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance)

NEW QUESTION: 95
Which Palo Alto Networks VM-Series firewall is valid?
A. VM-25
B. VM-800
C. VM-50
D. VM-400
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation- firewall/vm-series

NEW QUESTION: 96
Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS version, and serial number?
A. debug system details
B. show session info
C. show system info
D. show system details
Answer: C (LEAVE A REPLY)
Reference: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN-OS-6.0- CLI-ref.pdf

NEW QUESTION: 97
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. Different security profiles can be applied to traffic matching rules 2 and 3.
B. A report can be created that identifies unclassified traffic on the network.
C. Separate Log Forwarding profiles can be applied to rules 2 and 3.
D. Rule 2 and 3 apply to traffic on different ports.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 98
Which protection feature is available only in a Zone Protection Profile?
A. SYN Flood Protection using SYN Flood Cookies
B. ICMP Flood Protection
C. Port Scan Protection
D. UDP Flood Protections
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/network/network-network-profiles-zone-protection

NEW QUESTION: 99
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) Web-browsing -Allow
B. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
C. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
D. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 100
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: C (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clp3CAC

NEW QUESTION: 101
A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?
A. Threat Activity
B. Blocked Activity
C. Network Activity
D. Bandwidth Activity
Answer: C (LEAVE A REPLY)

NEW QUESTION: 102
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 (LEAVE A REPLY)
Explanation
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-th

NEW QUESTION: 103
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 (LEAVE A REPLY)
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgradedowngrade-considerations

NEW QUESTION: 104
Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two)
A. GlobalProtect Quarantine Activity
B. Successful GlobalProtect Connection Activity

C. GlobalProtect Deployment Activity
D. Successful GlobalProtect Deployed Activity
Answer: (SHOW ANSWER)

NEW QUESTION: 105
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 and a QoS Policy
C. Use QoS Classes to define QoS Profile
D. Use QoS Profile to define QoS Classes and a QoS Policy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
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 an Application Override policy.
B. Create an Application Override policy and custom threat signature for the application.
C. Create a custom App-ID and enable scanning on the advanced tab.
D. Create a custom App-ID and use the "ordered conditions" check box.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
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 (LEAVE A REPLY)
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manag templates-and-template-stacks/configure-a-template-stack

NEW QUESTION: 108
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 management port may be used for a backup control connection
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 two devices must share a routable floating IP address
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon?
A. Online Certificate Status Protocol
B. Trusted root certificate
C. Certificate revocation list
D. Machine certificate
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?
A. Use the debug dataplane packet-diag set capture stage firewall file command.
B. Use the topdump command.
C. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
D. Use the debug dataplane packet-diag set capture stage management file command.
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Which Panorama administrator types require the configuration of at least one access domain? (Choose two.)
A. Device Group
B. Role Based
C. Dynamic
D. Custom Panorama Admin
E. Template Admin
Answer: (SHOW ANSWER)

NEW QUESTION: 112
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: (SHOW ANSWER)
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Mana 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: 113
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. Configuration and Large Scale VPN (LSVPN) setups file
B. Configuration and serial number files
C. Configuration and statistics files
D. Device state and license files
Answer: D (LEAVE A REPLY)

NEW QUESTION: 114
If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?
A. TLS Bidirectional Inspection
B. SSL Inbound Inspection
C. SSH Forward Proxy
D. SMTP Inbound Decryption
Answer: B (LEAVE A REPLY)
Explanation/Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl- inbound-inspection

NEW QUESTION: 115
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 (LEAVE A REPLY)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRoCAK

NEW QUESTION: 116
During the packet flow process, which two processes are performed in application identification? (Choose two.)
A. session application identified
B. application changed from content inspection
C. pattern based application identification
D. application override policy match
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 117
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 valid. It will cause the firewall to deny the matched sessions. Any configured Security Profiles have no effect if the Security policy rule action is set to "Deny."
B. The configuration will allow the matched session unless a vulnerability signature is detected. The "Deny" action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile.
C. The configuration is invalid. It will cause the firewall to skip this Security policy rule. A warning will be
displayed during a commit.
D. The configuration is invalid. The Profile Settings section will be grayed out when the Action is set to "Deny".
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
In High Availability, which information is transferred via the HA data link?
A. session information
B. heartbeats
C. HA state information
D. User-ID information
Answer: A (LEAVE A REPLY)

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links

NEW QUESTION: 119
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 E
B. Option B
C. Option C
D. Option D
E. Option A
Answer: B (LEAVE A REPLY)

NEW QUESTION: 120
Which Captive Portal mode must be configured to support MFA authentication?
A. NTLM
B. Redirect
C. Single Sign-On
D. Transparent
Answer: (SHOW ANSWER)
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication

NEW QUESTION: 121
To more easily reuse templates and template slacks , you can create term plate variables in place of firewall-specific and appliance-specific IP literals in your configurations Which one is the correct configuration?
A. &Panorama
B. #Pancrama
C. $Panorama
D. @Panorama
Answer: C (LEAVE A REPLY)

Valid PCNSE Dumps shared by Actual4test.com for Helping Passing PCNSE Exam! Actual4test.com now offer the **newest PCNSE exam dumps**, the Actual4test.com PCNSE exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com PCNSE dumps with Test Engine here: https://www.actual4test.com/PCNSE_examcollection.html (**375** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)

Valid PCNSE Dumps shared by Actual4test.com for Helping Passing PCNSE Exam! Actual4test.com now offer the **newest PCNSE exam dumps**, the Actual4test.com PCNSE exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com PCNSE dumps with Test Engine here: https://www.actual4test.com/PCNSE_examcollection.html (**375** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)