



Actual exam question from Palo Alto Networks's PCNSE

Question #: 1

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer



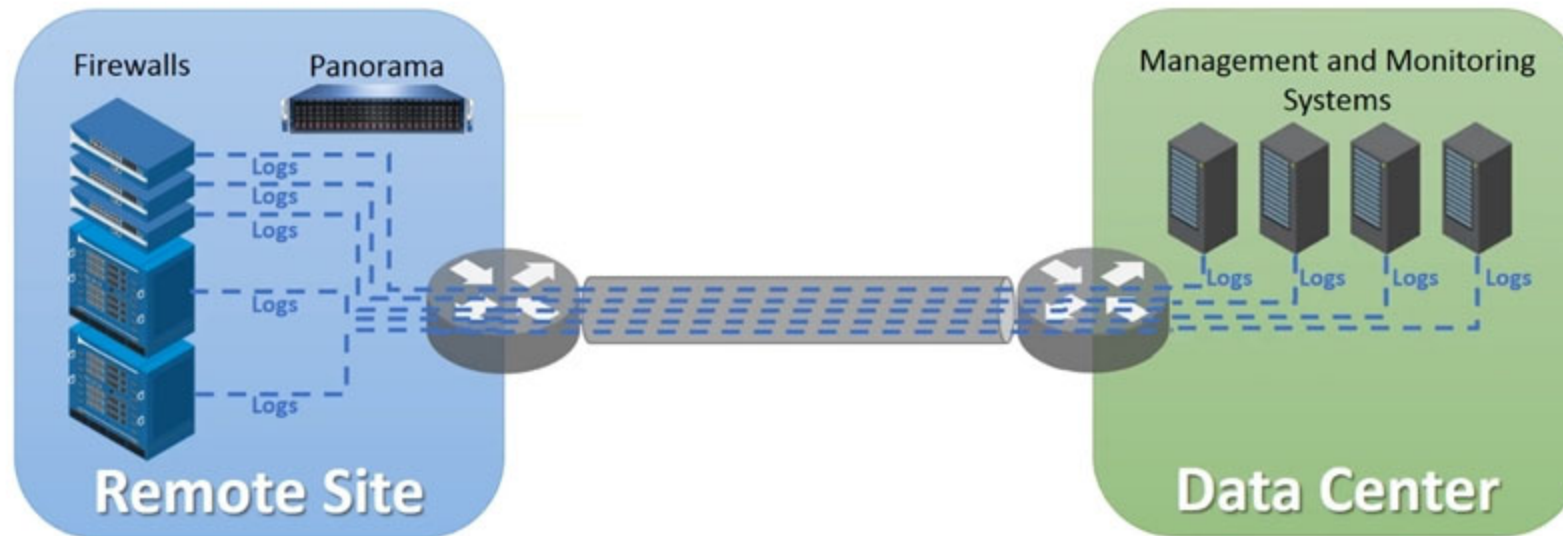
Actual exam question from Palo Alto Networks's PCNSE

Question #: 2

Topic #: 1

[\[All PCNSE Questions\]](#)

Refer to the exhibit.



An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.

How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 3

Topic #: 1

[\[All PCNSE Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 4

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans.
Which Security Profile type will protect against worms and trojans?

- A. Anti-Spyware
- B. Instruction Prevention
- C. File Blocking
- D. Antivirus

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 5

Topic #: 1

[\[All PCNSE Questions\]](#)

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 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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 6

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall. Which priority is correct for the passive firewall?

- A. 0
- B. 99
- C. 1
- D. 255

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 7

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 8

Topic #: 1

[\[All PCNSE Questions\]](#)

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 firewall to Panorama?

A.

Panorama Settings

Panorama Servers

10.99.1.21

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

Secure Client Communication

Certificate Type None

Check Server Identity

Disable Panorama Policy and Objects Disable Device and Network Template OK Cancel

B.

Security Policy Rule

General Source User Destination Application Service/URL Category **Actions**

Action Setting

Action Allow

Send ICMP Unreachable

Profile Setting

Profile Type Profiles

Antivirus None

Vulnerability Protection None

Anti-Spyware None

URL Filtering Filter1

File Blocking None

Data Filtering None

WildFire Analysis None

Log Setting

Log at Session Start

Log at Session End

Log Forwarding None

Other Settings

Schedule None

QoS Marking None

Disable Server Response Inspection

OK Cancel

C.

Syslog Server Profile

Name SyslogProfile1

Panorama

Servers Custom Log Format

Name	Syslog Server	Transport	Port	Format	Facility
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

+ Add - Delete

Enter the IP address or FQDN of the Syslog server

OK Cancel

D.

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



Actual exam question from Palo Alto Networks's PCNSE

Question #: 9

Topic #: 1

[\[All PCNSE Questions\]](#)

When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

- A. To enable Gateway authentication to the Portal
- B. To enable Portal authentication to the Gateway
- C. To enable user authentication to the Portal
- D. To enable client machine authentication to the Portal

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 10

Topic #: 1

[\[All PCNSE Questions\]](#)

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 prompted 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.

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 11

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 12

Topic #: 1

[\[All PCNSE Questions\]](#)

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 13

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 14

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 15

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 16

Topic #: 1

[\[All PCNSE Questions\]](#)

Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS® software?

- A. XML API
- B. Port Mapping
- C. Client Probing
- D. Server Monitoring

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 17

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 18

Topic #: 1

[\[All PCNSE Questions\]](#)

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. Security policy
- B. Decryption policy
- C. Authentication policy
- D. Application Override policy

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 19

Topic #: 1

[\[All PCNSE Questions\]](#)

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 invalid. The Profile Settings section will be grayed out when the 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 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`.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 20

Topic #: 1

[\[All PCNSE Questions\]](#)

A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach `http://www.company.com`. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to `http://www.company.com`.

How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 21

Topic #: 1

[\[All PCNSE Questions\]](#)

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 from the Shared group
- D. Overwrites local firewall configuration

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 22

Topic #: 1

[\[All PCNSE Questions\]](#)

Which Captive Portal mode must be configured to support MFA authentication?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 23

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required. Which interface type would support this business requirement?

- A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
- B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only
- C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRP protocols)
- D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 24

Topic #: 1

[\[All PCNSE Questions\]](#)

A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port to 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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 25

Topic #: 1

[\[All PCNSE Questions\]](#)

A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable we browsing access to the server.

Which application and service need to be configured to allow only cleartext web-browsing traffic to thins server on tcp/8080?

- A. application: web-browsing; service: application-default
- B. application: web-browsing; service: service-https
- C. application: ssl; service: any
- D. application: web-browsing; service: (custom with destination TCP port 8080)

Show Suggested Answer



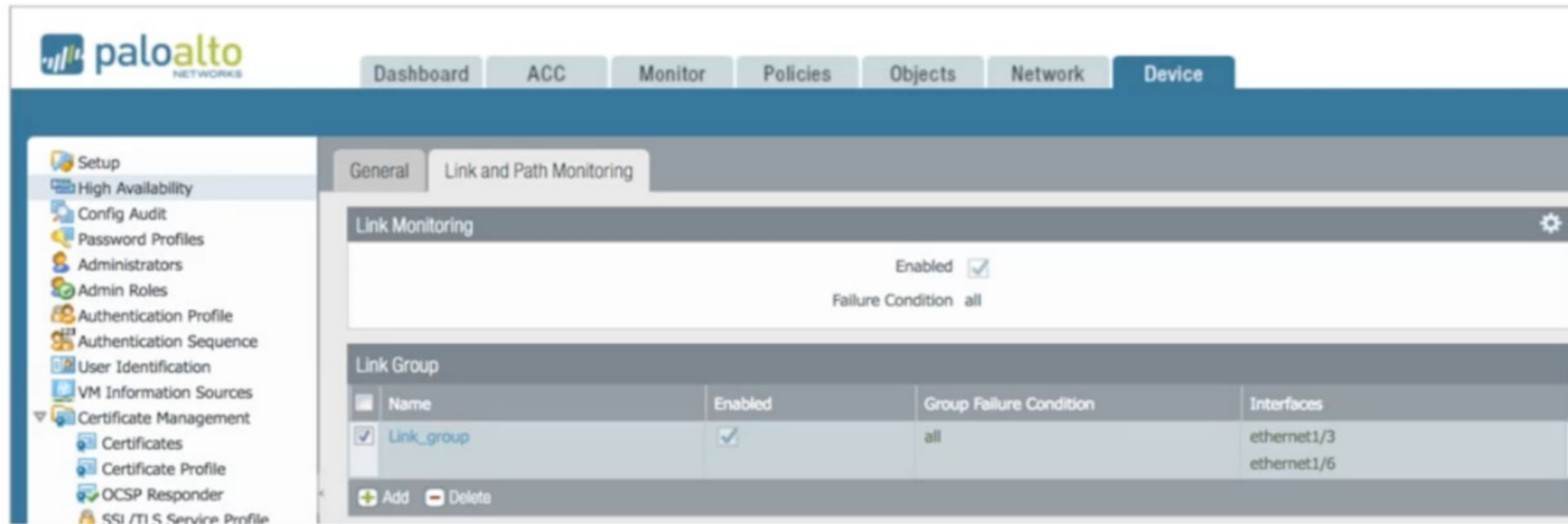
Actual exam question from Palo Alto Networks's PCNSE

Question #: 26

Topic #: 1

[\[All PCNSE Questions\]](#)

If the firewall has the following link monitoring configuration, what will cause a failover?



The screenshot shows the Palo Alto Networks management interface. The top navigation bar includes: Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The left sidebar lists various configuration categories, with 'High Availability' expanded. The main content area is titled 'Link and Path Monitoring' and contains the following configuration:

- Link Monitoring:** Enabled . Failure Condition: all.
- Link Group Table:**

	Name	Enabled	Group Failure Condition	Interfaces
<input checked="" type="checkbox"/>	Link_group	<input checked="" type="checkbox"/>	all	ethernet1/3 ethernet1/6

At the bottom of the table are 'Add' and 'Delete' buttons.

- 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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 27

Topic #: 1

[\[All PCNSE Questions\]](#)

In the image, what caused the commit warning?

The screenshot shows the Palo Alto Networks configuration interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The 'Device' tab is active, and the 'Commit' button is visible. Below the navigation bar, there are tabs for 'Device Certificates' and 'Default Trusted Certificate Authorities'. A table lists two certificates:

Name	Subject	Issuer	CA	K...	Expires	Sta...	Al...	Usage
FWDtrust	CN = FWDtrust	DC = local, DC = lab, CN = lab-SRV2016-LABCA-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:02:05 2020 GMT	valid	RSA	Forward Trust Certificate
FWD-UnTrust	CN = FWD-UnTrust	CN = FWD-UnTrust	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:06:36 2019 GMT	valid	RSA	Forward Untrust Certificate

Below the table, a 'Commit Status' dialog box is open, showing the following information:

- Operation:** Commit
- Status:** Completed
- Result:** Successful
- Details:** Configuration committed successfully
- Warnings:** Warning: cannot find complete certificate chain for certificate FWDtrust (Module: device)

The warning message is highlighted with an orange box.

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 28

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 29

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 30

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 31

Topic #: 1

[\[All PCNSE Questions\]](#)

A session in the Traffic log is reporting the application as `incomplete`.

What does `incomplete` mean?

- A. The three-way TCP handshake was observed, but the application could not be identified.
- B. The three-way TCP handshake did not complete.
- C. The traffic is coming across UDP, and the application could not be identified.
- D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

Show Suggested Answer



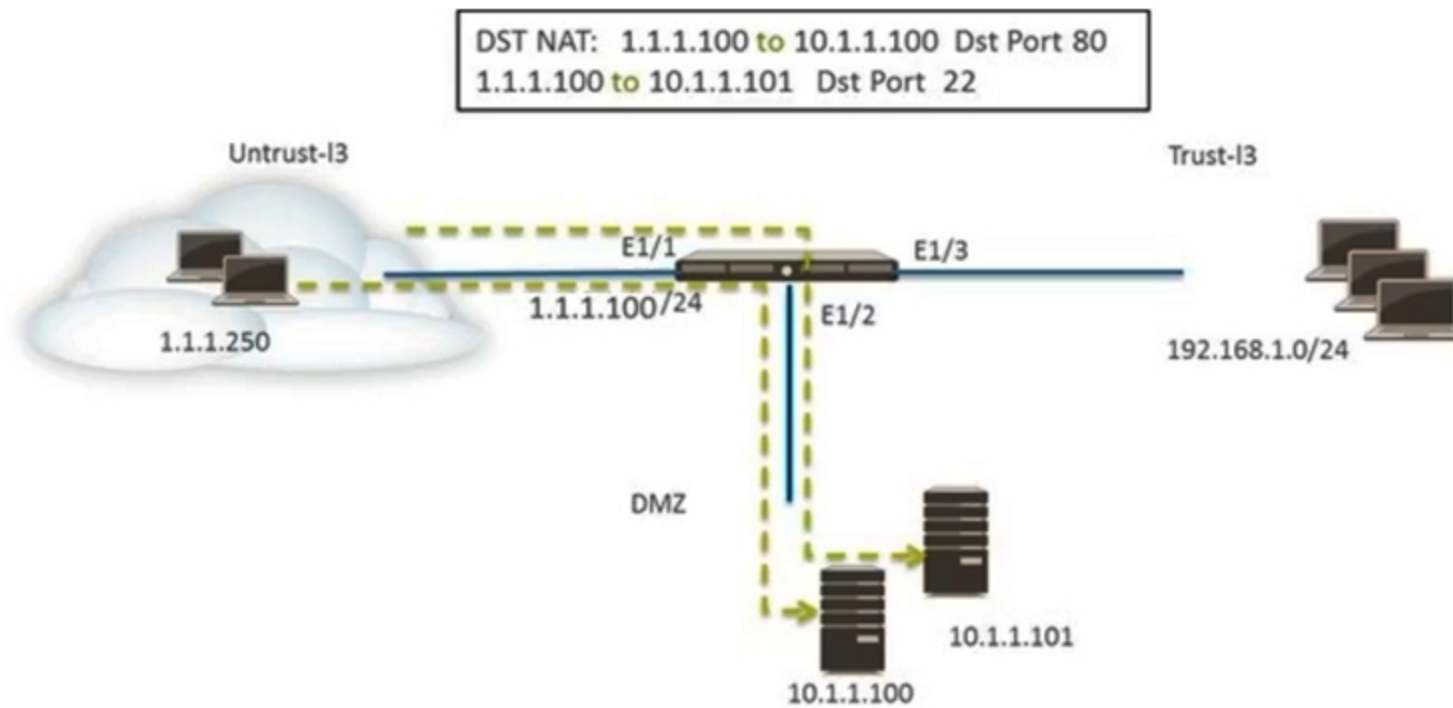
Actual exam question from Palo Alto Networks's PCNSE

Question #: 32

Topic #: 1

[\[All PCNSE Questions\]](#)

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 λ €" Allow
- B. Untrust (Any) to Untrust (10.1.1.1), ssh λ €" Allow
- C. Untrust (Any) to DMZ (1.1.1.100), web-browsing λ €" Allow
- D. Untrust (Any) to DMZ (1.1.1.100), ssh λ €" Allow
- E. Untrust (Any) to DMZ (10.1.1.100, 10.1.1.101), ssh, web-browsing λ €" Allow

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

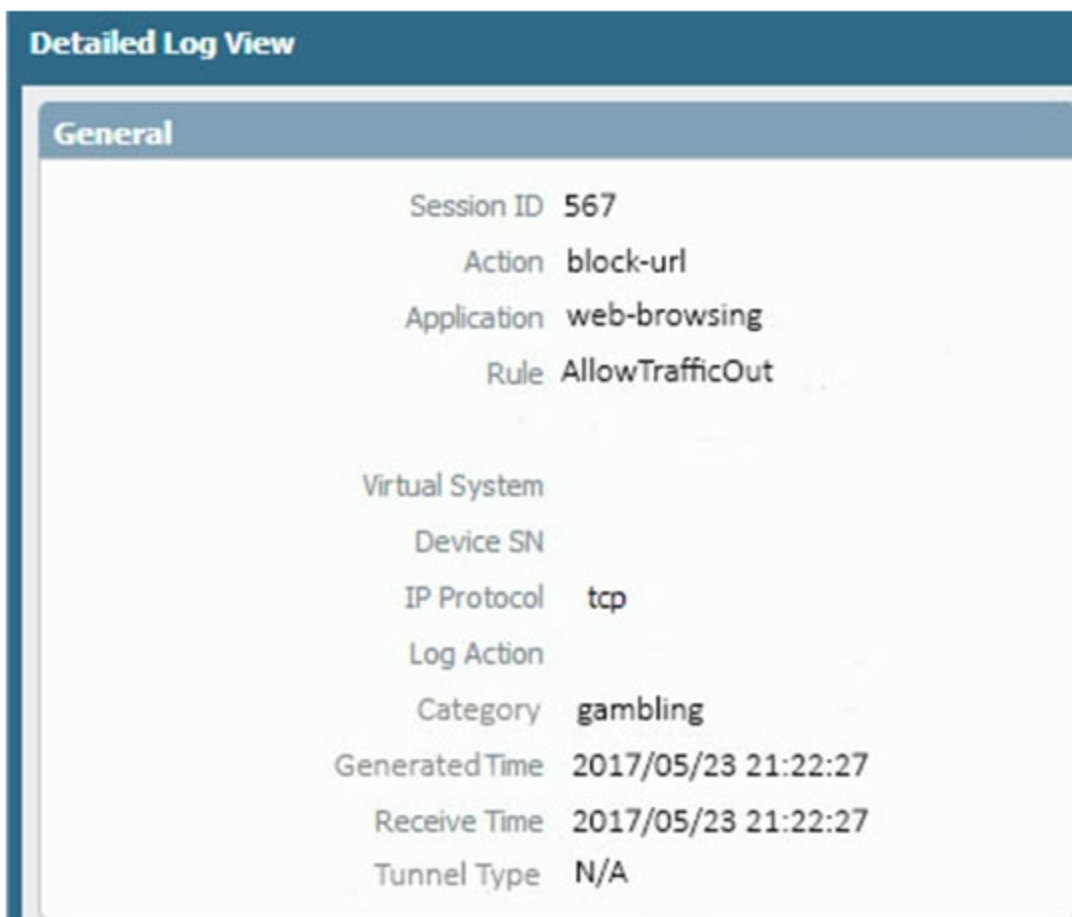
Question #: 33

Topic #: 1

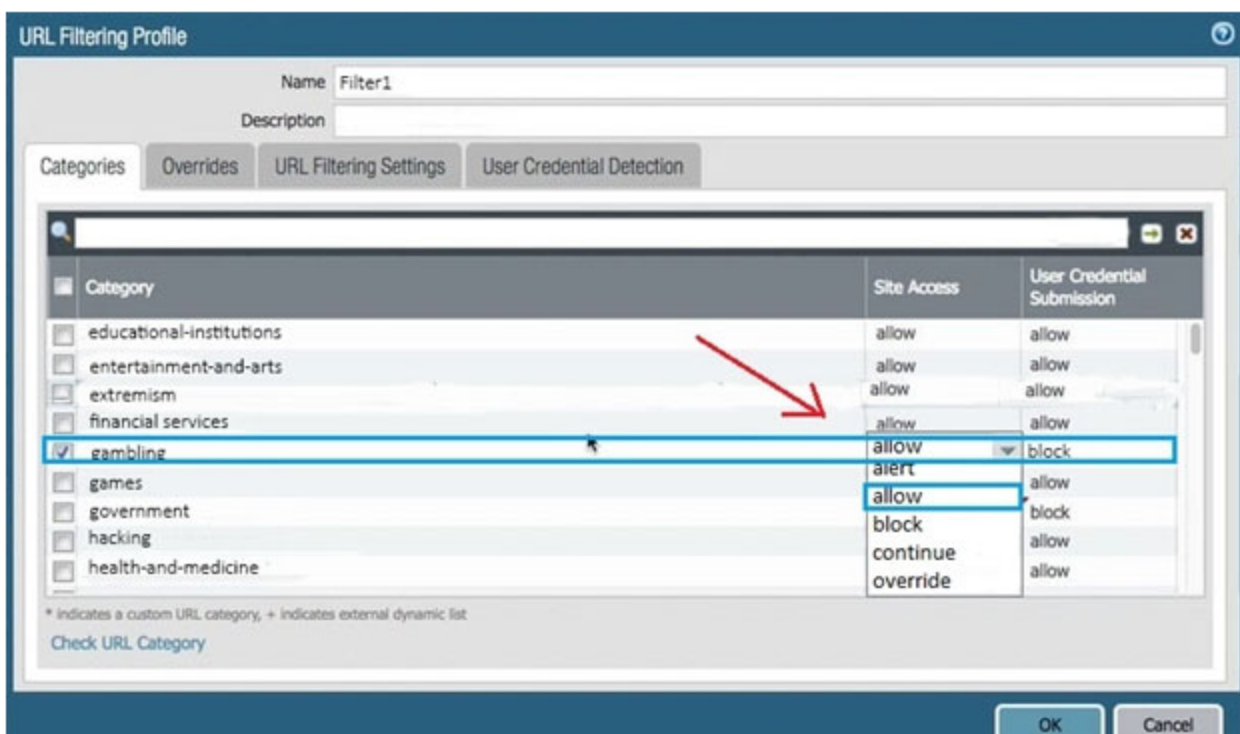
[\[All PCNSE Questions\]](#)

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?

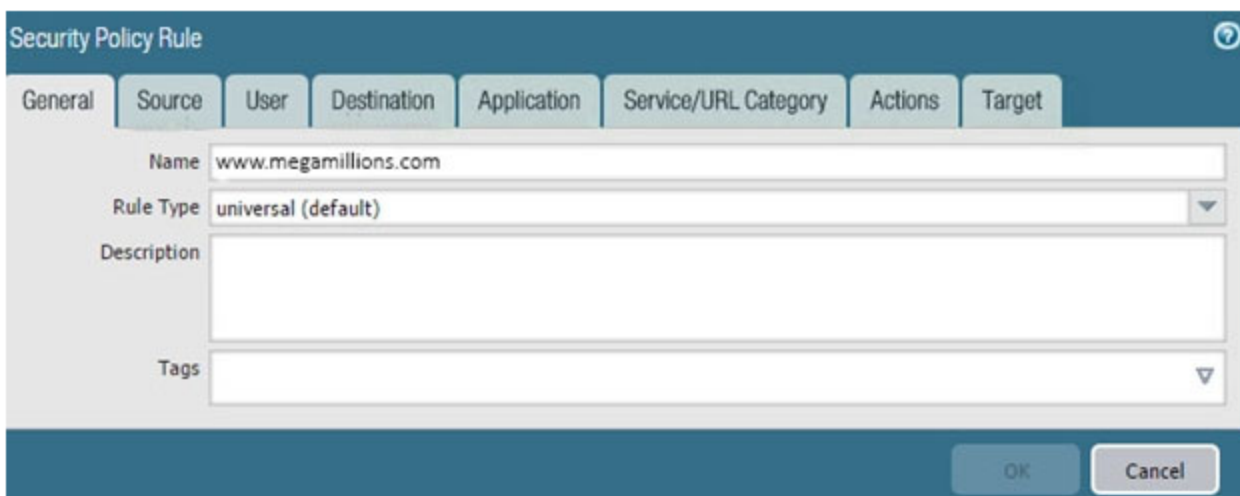
A.



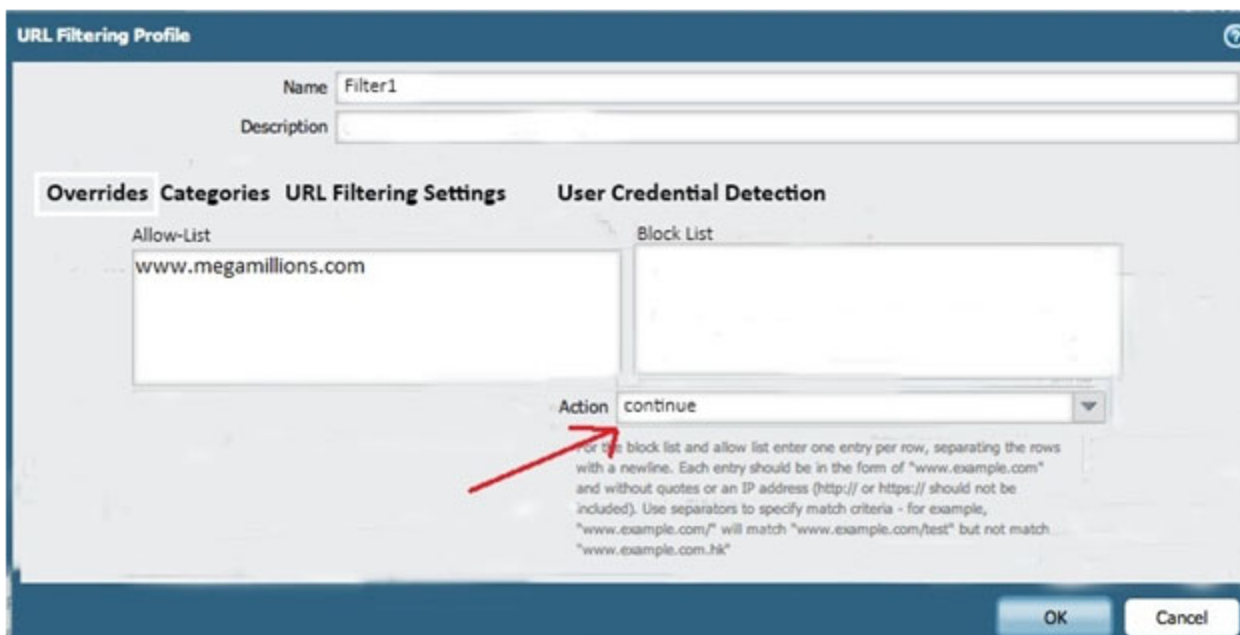
B.



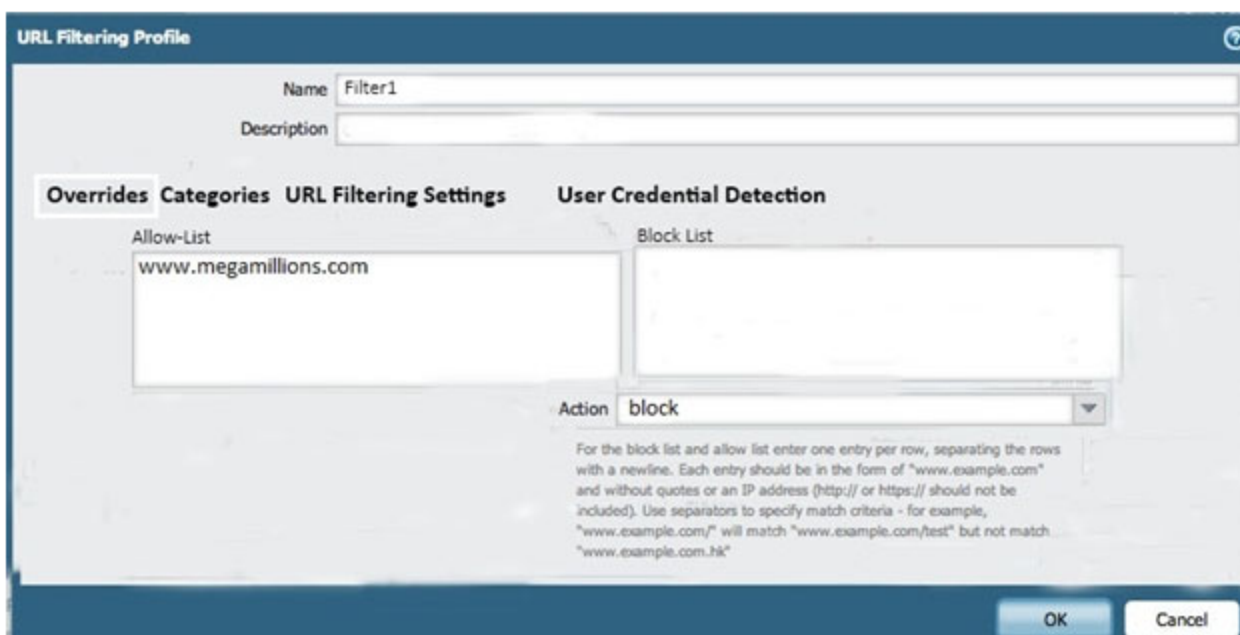
C.



D.



E.





Actual exam question from Palo Alto Networks's PCNSE

Question #: 34

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 35

Topic #: 1

[\[All PCNSE Questions\]](#)

A customer has an application that is being identified as unknown-tcp 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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 36

Topic #: 1

[\[All PCNSE Questions\]](#)

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. Admin Role
- B. WebUI
- C. Authentication
- D. Authorization

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 37

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has left a firewall to use the default port for all management services.

Which three functions are performed by the dataplane? (Choose three.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 38

Topic #: 1

[\[All PCNSE Questions\]](#)

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 be exported from the firewalls and manually imported into Panorama.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 39

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall just submitted a file to WildFire for analysis. Assume a 5-minute window for analysis. The firewall is configured to check for verdicts every 5 minutes. How quickly will the firewall receive back a verdict?

- A. More than 15 minutes
- B. 5 minutes
- C. 10 to 15 minutes
- D. 5 to 10 minutes

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 40

Topic #: 1

[\[All PCNSE Questions\]](#)

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 of an `application` allows the firewall to take immediate action if the port being used is a member of the application standard port list.
- B. 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.
- C. 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
- D. Use of a `service` enables the firewall to take action after enough packets allow for App-ID identification

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 41

Topic #: 1

[\[All PCNSE Questions\]](#)

Which Palo Alto Networks VM-Series firewall is valid?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

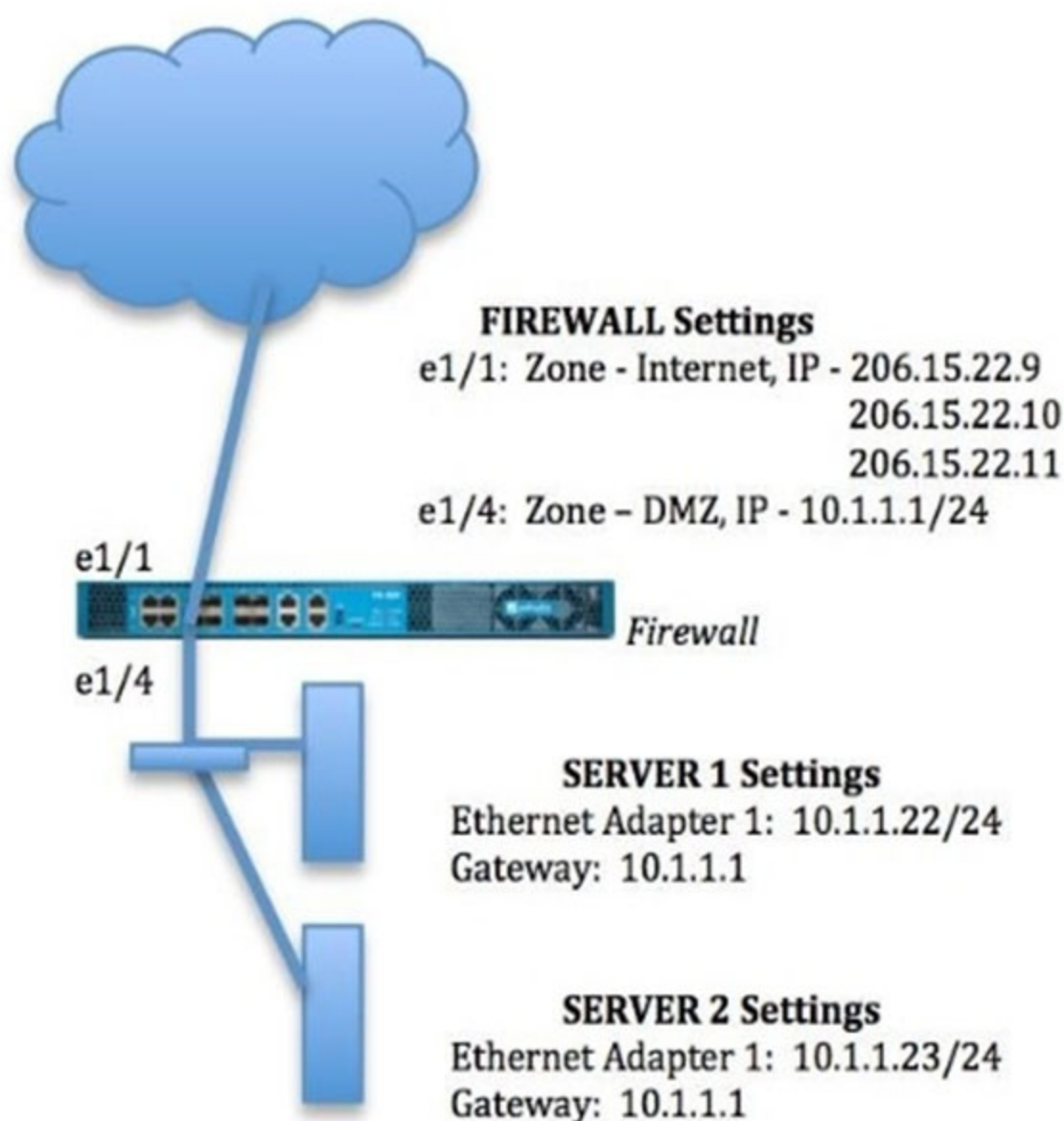
Question #: 42

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22

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



A.

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

B.

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

C.

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

D.

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 43

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 44

Topic #: 1

[\[All PCNSE Questions\]](#)

Starting with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 45

Topic #: 1

[\[All PCNSE Questions\]](#)

Refer to the exhibit.

```
#####
```

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

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

```
#####
```

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

```
total virtual-wire shown :          1
flags :   m - multicast firewalling
          p - link state pass-through
          s - vlan sub-interface
          i - ip+vlan sub-interface
          t - tenant sub-interface
```

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

```
#####
```

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

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 46

Topic #: 1

[\[All PCNSE Questions\]](#)

Which three authentication services can an 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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 47

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 48

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 49

Topic #: 1

[\[All PCNSE Questions\]](#)

A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers.

Which option will protect the individual servers?

- A. Enable packet buffer protection on the Zone Protection Profile.
- B. Apply an Anti-Spyware Profile with DNS sinkholing.
- C. Use the DNS App-ID with application-default.
- D. Apply a classified DoS Protection Profile.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 50

Topic #: 1

[\[All PCNSE Questions\]](#)

If the firewall is configured for credential phishing prevention using the `Domain Credential Filter` method, which login will be detected as credential theft?

- A. Mapping to the IP address of the logged-in user.
- B. First four letters of the username matching any valid corporate username.
- C. Using the same user's corporate username and password.
- D. Matching any valid corporate username.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 51

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has users accessing network resources through Citrix XenApp 7.x.

Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 52

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 53

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 54

Topic #: 1

[\[All PCNSE Questions\]](#)

Which option is part of the content inspection process?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 55

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 56

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications DNS, SSL, and web-browsing.

The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application SSL.

Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 57

Topic #: 1

[\[All PCNSE Questions\]](#)

Refer to the exhibit.

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
Domain-Root-Cert	CN = demo.local	CN = demo.local	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Nov 1 00:34:47 2021 GMT	valid	RSA	Trusted Root CA Certificate
Domain Sub-CA	CN = sub.demo.local	CN = demo.local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 20:59:38 2019 GMT	valid	RSA	
Forward_Trust	CN = fwdtrust.demo.local	CN = sub.demo.local	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 21:09:49 2018 GMT	valid	RSA	

Which certificates can be used as a Forward Trust certificate?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 58

Topic #: 1

[\[All PCNSE Questions\]](#)

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 Policies > Service/URL Category > Service.
- C. Set up Security policy rule to allow SSL communication.
- D. Configure an SSL/TLS Profile.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 59

Topic #: 1

[\[All PCNSE Questions\]](#)

Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 60

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 61

Topic #: 1

[\[All PCNSE Questions\]](#)

Which CLI command can be used to export the tcpdump capture?

- A. scp export tcpdump from mgmt.pcap to < username@host:path>
- B. scp extract mgmt-pcap from mgmt.pcap to < username@host:path>
- C. scp export mgmt-pcap from mgmt.pcap to < username@host:path>
- D. download mgmt-pcap

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 62

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 63

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 64

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 65

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 66

Topic #: 1

[\[All PCNSE Questions\]](#)

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. Session Browser
- B. Application Command Center
- C. TCP Dump
- D. Packet Capture

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 67

Topic #: 1

[\[All PCNSE Questions\]](#)

The certificate information displayed in the following image is for which type of certificate?

The screenshot shows a 'Certificate information' dialog box with the following details:

Name	demo-decrypt
Subject	/CN=sub.domain.local
Issuer	/CN=demo.local
Not Valid Before	Jul 23 16:52:26 2020 GMT
Not Valid After	Jul 23 16:52:26 2020 GMT
Algorithm	RSA

Below the fields are four checkboxes:

- Certificate Authority
- Forward Trust Certificate
- Forward Untrust Certificate
- Trusted Root CA

Buttons at the bottom: Revoke, OK, Cancel.

- A. Forward Trust certificate
- B. Self-Signed Root CA certificate
- C. Web Server certificate
- D. Public CA signed certificate

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 68

Topic #: 1

[\[All PCNSE Questions\]](#)

Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

- A. Disable SNMP on the management interface.
- B. Application override of SSL application.
- C. Disable logging at session start in Security policies.
- D. Disable predefined reports.
- E. Reduce the traffic being decrypted by the firewall.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 69

Topic #: 1

[\[All PCNSE Questions\]](#)

Which feature must you configure to prevent users from 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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 70

Topic #: 1

[\[All PCNSE Questions\]](#)

How can a candidate or running configuration be copied to a host external from Panorama?

- A. Commit a running configuration.
- B. Save a configuration snapshot.
- C. Save a candidate configuration.
- D. Export a named configuration snapshot.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 71

Topic #: 1

[\[All PCNSE Questions\]](#)

If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic when users browse to HTTP(S) websites?

- A. SSL Forward Proxy
- B. SSL Inbound Inspection
- C. SSL Reverse Proxy
- D. SSL Outbound Inspection

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 72

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this 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 a custom threat signature for the application.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 73

Topic #: 1

[\[All PCNSE Questions\]](#)

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router.

Which two options would help the administrator troubleshoot this issue? (Choose two.)

- A. View the System logs and look for the error messages about BGP.
- B. Perform a traffic pcap on the NGFW to see any BGP problems.
- C. View the Runtime Stats and look for problems with BGP configuration.
- D. View the ACC tab to isolate routing issues.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 74

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 75

Topic #: 1

[\[All PCNSE Questions\]](#)

Which three firewall states are valid? (Choose three.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 76

Topic #: 1

[\[All PCNSE Questions\]](#)

Which virtual router feature determines if a specific destination IP address is reachable?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 77

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 78

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 79

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 80

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 81

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 82

Topic #: 1

[\[All PCNSE Questions\]](#)

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

How would the administrator establish the chain of trust?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 83

Topic #: 1

[\[All PCNSE Questions\]](#)

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?

```
admin@Lab33-111-PA-3060(active)> show clock
```

```
Thu Jun  8 12:49:55 PDT 2017
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
```

```
test-pbf {
  action {
    forward {
      egress-interface ethernet1/5;
    }
  }
  from {
    zone L3-Trust;
  }
  enforce-symmetric-return {
    enabled no;
  }
  source 192.168.111.3;
  destination 10.46.41.113;
  source-user any;
  application any;
  service any;
  schedule schedule-pbf;
}
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
```

```
schedule-pbf {
  schedule-type {
    recurring {
      daily 16:00-21:00;
    }
  }
}
```

```
#####
```

```
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
67	10.10.20.0/24	0.0.0.0	u	ethernet1/7	1500
66	10.10.20.111/32	0.0.0.0	uh	ethernet1/7	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
49	10.46.44.0/23	0.0.0.0	u	ethernet1/5	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
48	10.46.45.111/32	0.0.0.0	uh	ethernet1/5	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

A. ethernet1/7

B. ethernet1/5

C. ethernet1/6

D. ethernet1/3

Show Suggested Answer

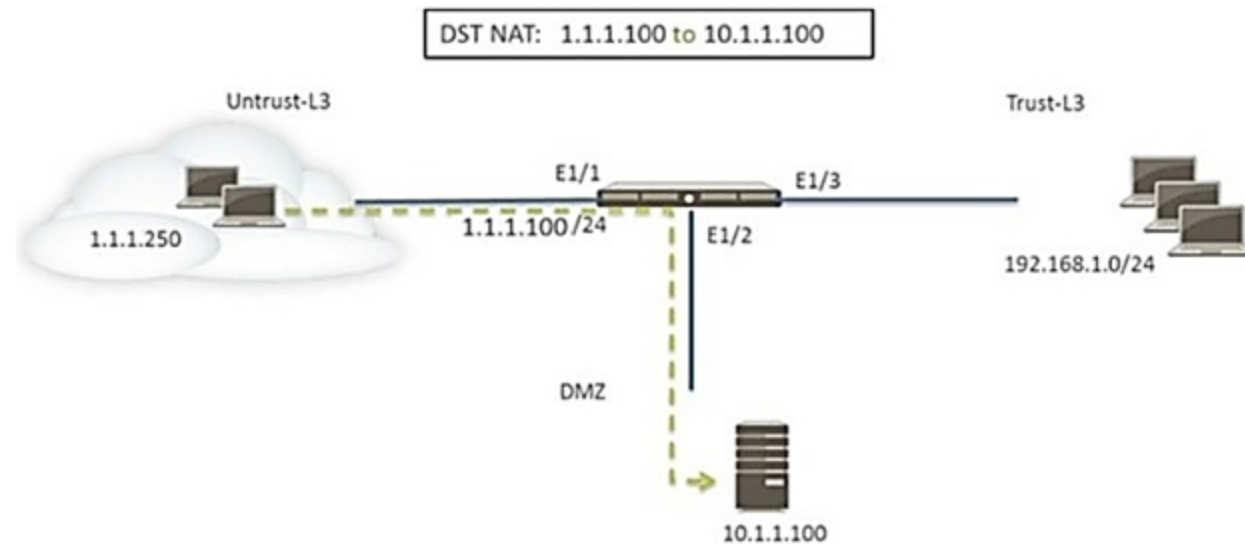
Actual exam question from Palo Alto Networks's PCNSE

Question #: 84

Topic #: 1

[\[All PCNSE Questions\]](#)

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 λ €" Allow
- B. Untrust (any) to Untrust (1.1.1.100), web browsing λ €" Allow
- C. Untrust (any) to DMZ (1.1.1.100), web browsing λ €" Allow
- D. Untrust (any) to DMZ (10.1.1.100), web browsing λ €" Allow

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 85

Topic #: 1

[\[All PCNSE Questions\]](#)

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web-browsing traffic to this server on tcp/443?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 86

Topic #: 1

[\[All PCNSE Questions\]](#)

Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

- A. The firewall is in multi-vsyst 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%.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 87

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 88

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 89

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 90

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 91

Topic #: 1

[\[All PCNSE Questions\]](#)

Which feature can be configured on VM-Series firewalls?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 92

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 93

Topic #: 1

[\[All PCNSE Questions\]](#)

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 App-ID request to Palo Alto Networks.
- D. Create a Security policy to identify the custom application.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 94

Topic #: 1

[\[All PCNSE Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 95

Topic #: 1

[\[All PCNSE Questions\]](#)

A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

- A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server.
- B. Add a Vulnerability Protection Profile to block the attack.
- C. Add QoS Profiles to throttle incoming requests.
- D. Add a DoS Protection Profile with defined session count.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 96

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 97

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 98

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 99

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 100

Topic #: 1

[\[All PCNSE Questions\]](#)

View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?

The screenshot shows the 'Configs' section of the Palo Alto Networks GlobalProtect configuration interface. The 'Internal' tab is selected. Under the 'Internal Host Detection IPv4' section, the checkbox is checked. The 'IP Address' field is set to '192.168.10.1' and the 'Hostname' field is set to 'host.my.domain'. The 'Internal Host Detection IPv6' section is disabled, with its checkbox unchecked and its fields empty.

- A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
- B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
- C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
- D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 101

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 102

Topic #: 1

[\[All PCNSE Questions\]](#)

What is exchanged through the HA2 link?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 103

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 104

Topic #: 1

[\[All PCNSE Questions\]](#)

A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation.

Which two formats are correct for naming aggregate interfaces? (Choose two.)

- A. ae.8
- B. aggregate.1
- C. ae.1
- D. aggregate.8

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 105

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 106

Topic #: 1

[\[All PCNSE Questions\]](#)

VPN traffic intended for an administrator's firewall 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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 107

Topic #: 1

[\[All PCNSE Questions\]](#)

Which Zone Pair and Rule Type will allow a successful connection for a user on the Internet zone to a web server hosted on the DMZ zone? The web server is reachable using a Destination NAT policy in the Palo Alto Networks firewall.

A.

Zone Pair:

Source Zone: Internet

Destination Zone: Internet

Rule Type:

'intrazone'

B.

Zone Pair:

Source Zone: Internet

Destination Zone: DMZ

Rule Type:

'interzone' or 'universal'

C.

Zone Pair:

Source Zone: Internet

Destination Zone: Internet

Rule Type:

'intrazone' or 'universal'

D.

Zone Pair:

Source Zone: Internet

Destination Zone: DMZ

Rule Type:

'intrazone'

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 108

Topic #: 1

[\[All PCNSE Questions\]](#)

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 interface
- B. Enable QoS in the Interface Management Profile
- C. Enable QoS Data Filtering Profile
- D. Enable QoS monitor

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 109

Topic #: 1

[\[All PCNSE Questions\]](#)

Which log file can be used to identify SSL decryption failures?

- A. Traffic
- B. ACC
- C. Configuration
- D. Threats

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 110

Topic #: 1

[\[All PCNSE Questions\]](#)

A customer wants to set up a site-to-site VPN using tunnel interfaces.

Which two formats are correct for naming tunnel interfaces? (Choose two.)

A. tunnel.1

B. vpn-tunnel.1

C. tunnel.1025

D. vpn-tunnel.1024

[Show Suggested Answer](#)



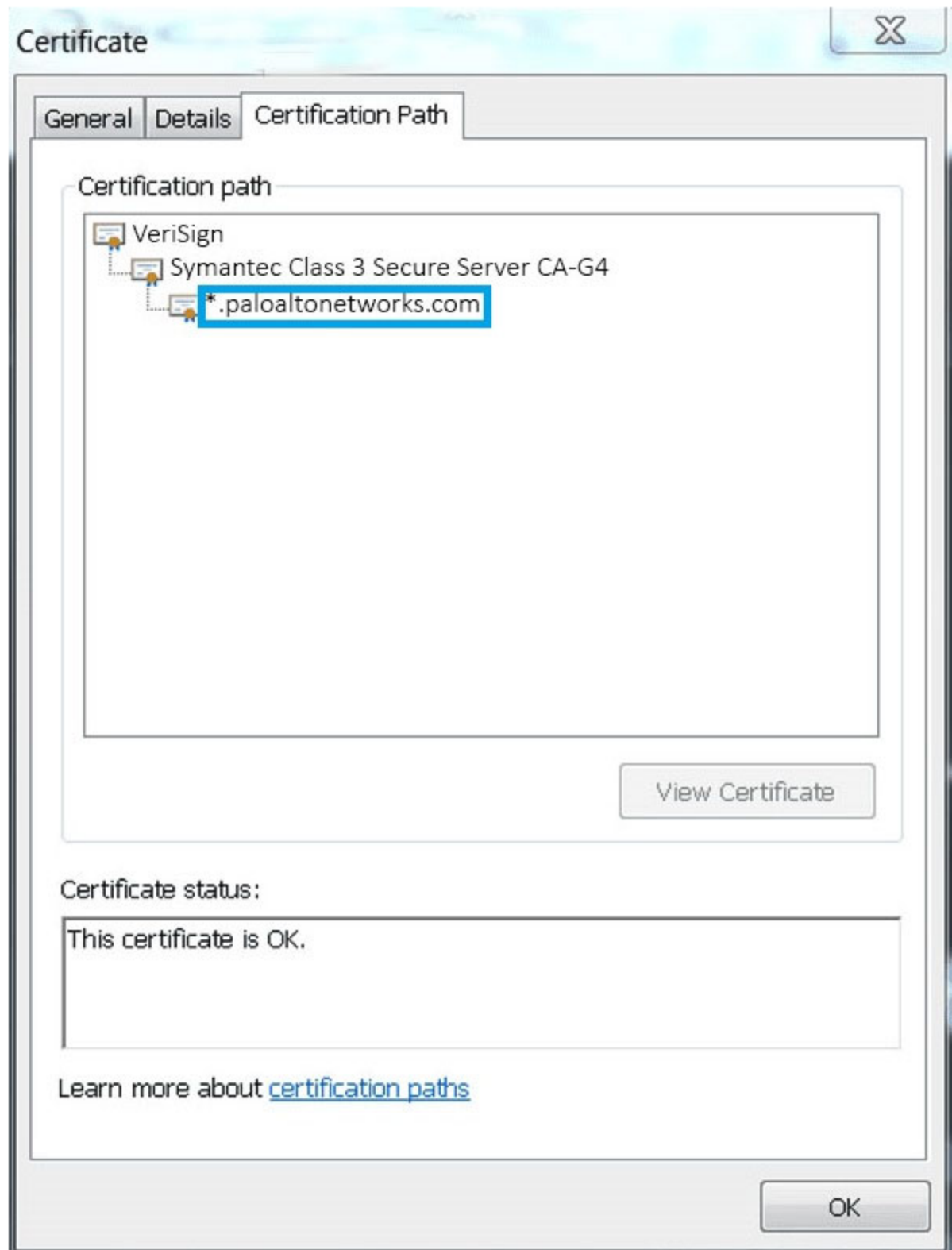
Actual exam question from Palo Alto Networks's PCNSE

Question #: 111

Topic #: 1

[\[All PCNSE Questions\]](#)

Based on the following image, what is the correct path of root, intermediate, and end-user certificate?



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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 112

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the Internet. Which configuration will enable the firewall to download and install application updates automatically?

- A. Download and install application updates cannot be done automatically if the MGT port cannot reach the Internet.
- B. Configure a service route for Palo Alto Networks Services that uses a dataplane interface that can route traffic to the Internet, and create a Security policy rule to allow the traffic from that interface to the update servers if necessary.
- C. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interfaced destined for the update servers goes out of the interface acting as your Internet connection.
- D. Configure a Security policy rule to allow all traffic to and from the update servers.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 113

Topic #: 1

[\[All PCNSE Questions\]](#)

A company wants to install a NGFW 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 option differentiates multiple VLANs into separate zones?

- A. Create V-Wire objects with two V-Wire interfaces and define a range of 10-4096 in the Tag Allowed field of the V-Wire object.
- B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.
- C. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface to a unique zone. Do not assign any interface an IP address.
- D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 114

Topic #: 1

[\[All PCNSE Questions\]](#)

Which data flow describes redistribution of user mappings?

- A. User-ID agent to firewall
- B. Domain Controller to User-ID agent
- C. User-ID agent to Panorama
- D. firewall to firewall

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 115

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 116

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 117

Topic #: 1

[\[All PCNSE Questions\]](#)

Which two features does PAN-OS® software use to identify applications? (Choose two.)

- A. transaction characteristics
- B. session number
- C. port number
- D. application layer payload

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 118

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator wants to upgrade a firewall from PAN-OS® 9.1 to PAN-OS® 10.0. The firewall is not a part of an HA pair.

What needs to be updated first?

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 119

Topic #: 1

[\[All PCNSE Questions\]](#)

When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 120

Topic #: 1

[\[All PCNSE Questions\]](#)

Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 121

Topic #: 1

[\[All PCNSE Questions\]](#)

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. Malware
- B. Grayware
- C. Phishing
- D. Spyware

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 122

Topic #: 1

[\[All PCNSE Questions\]](#)

When configuring the firewall for packet capture, what are the valid stage types?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 123

Topic #: 1

[\[All PCNSE Questions\]](#)

Which operation will impact the performance of the management plane?

- A. DoS protection
- B. WildFire submissions
- C. generating a SaaS Application report
- D. decrypting SSL sessions

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 124

Topic #: 1

[\[All PCNSE Questions\]](#)

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

- A. syslog listening
- B. server monitoring
- C. client probing
- D. port mapping

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 125

Topic #: 1

[\[All PCNSE Questions\]](#)

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. 6-tuple match: Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol, and Source Security Zone
- B. 5-tuple match: Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol
- C. 7-tuple match: Source IP Address, Destination IP Address, Source Port, Destination Port, Source User, URL Category, and Source Security Zone
- D. 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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 126

Topic #: 1

[\[All PCNSE Questions\]](#)

Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 127

Topic #: 1

[\[All PCNSE Questions\]](#)

Which feature can provide NGFWs with User-ID mapping information?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 128

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 129

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 130

Topic #: 1

[\[All PCNSE Questions\]](#)

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

- A. 10,000
- B. 15,000
- C. 7,500
- D. 5,000

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 131

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 132

Topic #: 1

[\[All PCNSE Questions\]](#)

For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 133

Topic #: 1

[\[All PCNSE Questions\]](#)

Which logs enable a firewall administrator to determine whether a session was decrypted?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 134

Topic #: 1

[\[All PCNSE Questions\]](#)

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 e 1/1.
- ⇒ 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. Static route pointing application PaloAlto-updates to the update servers
- B. Security policy rule allowing PaloAlto-updates as the application
- C. Scheduler for timed downloads of PAN-OS software
- D. DNS settings for the firewall to use for resolution

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 135

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 136

Topic #: 1

[\[All PCNSE Questions\]](#)

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. Antivirus update package.
- B. Applications and Threats update package.
- C. User-ID agent.
- D. WildFire update package.

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 137

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 138

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 139

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 140

Topic #: 1

[\[All PCNSE Questions\]](#)

Which administrative authentication method supports authorization by an external service?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 141

Topic #: 1

[\[All PCNSE Questions\]](#)

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. .fon

D. .apk

E. .pdf

F. .jar

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 142

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has been asked to configure active/active HA for a pair of firewalls. The firewalls use Layer 3 interfaces to send traffic to a single gateway IP for the pair. Which configuration will enable this HA scenario?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 143

Topic #: 1

[\[All PCNSE Questions\]](#)

Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

- A. GlobalProtect version 4.0 with PAN-OS 8.1
- B. GlobalProtect version 4.1 with PAN-OS 8.1
- C. GlobalProtect version 4.1 with PAN-OS 8.0
- D. GlobalProtect version 4.0 with PAN-OS 8.0

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 144

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 145

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

The screenshot shows the Palo Alto Networks Monitor tab with the following log entries:

Receive Time	Type	Severity	Event	Object	Description
06/16 08:41:43	general	informational	general		User admin accessed Monitor tab.
06/16 08:40:40	general	informational	general		User admin logged in via Web from 192.168.55.1 using https.
06/16 08:40:40	auth	informational	auth-success		authenticated for user 'admin'. From: 192.168.55.1.
06/16 08:40:06	general	informational	general		LOGIN ON tty1 BY admin.
06/16 08:39:43	general	informational	general		User admin logged in via CLI from Console.
06/16 08:39:42	auth	informational	auth-success		authenticated for user 'admin'. From: (null).
06/16 08:39:16	url-filtering	informational	upgrade-url-database-success		PAN-DB was upgraded to version 20170615.40151.
06/16 08:34:15	url-filtering	informational	upgrade-url-database-success		PAN-DB was upgraded to version 20170615.40150.
06/16 08:31:44	general	informational	general		Failed to connect to Panorama Server: 192.168.55.5 Port: 3978 Retry: 0
06/16 08:31:40	ntpd	informational	restart		NTP restart synchronization performed
06/16 08:31:33	general	informational	general		Commit job succeeded. Completion time=2017/06/16 05:31:33. JobId=29. User:admin

B.

The screenshot shows the Palo Alto Networks Monitor tab with the following traffic log entries:

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:03:45	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:59:36	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:59:06	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:40:27	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:39:57	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:56	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:55	drop	outside	outside	192.168.55.1		192.168.55.255

C.

05/23 20:49:30	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:49:29	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex
05/23 20:47:24	port	informational	link-change	ethernet1/1	Port ethernet1/1: Up 10Gb/s-full duplex
05/23 20:47:22	port	informational	link-change	MGT	Port MGT: Up Unknown
05/23 20:47:18	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:47:17	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex

D.

The screenshot shows the Task Manager - All Tasks window with the following task entries:

Type	Status	Start Time	Messages	Action
Config logs	Completed	06/16/17 08:40:53		
System logs	Completed	06/16/17 08:40:53		
Data logs	Completed	06/16/17 08:40:53		
Commit	Completed	06/16/17 08:31:19	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:31:19 <ul style="list-style-type: none"> Configuration committed successfully 	
Commit	Completed	06/16/17 08:30:15	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:30:15 <ul style="list-style-type: none"> Configuration committed successfully 	



Actual exam question from Palo Alto Networks's PCNSE

Question #: 146

Topic #: 1

[\[All PCNSE Questions\]](#)

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 a Dynamic Address Group for untrusted sites.
- C. Create a Security Policy rule with a vulnerability Security Profile attached.
- D. Enable the "Block sessions with untrusted issuers" setting.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 147

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 148

Topic #: 1

[\[All PCNSE Questions\]](#)

What is the purpose of the firewall decryption broker?

- A. decrypt SSL traffic and then send it as cleartext to a security chain of inspection tools.
- B. force decryption of previously unknown cipher suites
- C. reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools.
- D. inspect traffic within IPsec tunnels

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 149

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 150

Topic #: 1

[\[All PCNSE Questions\]](#)

What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

- A. Rule Usage Hit counter will not be reset.
- B. Highlight Unused Rules will highlight all rules.
- C. Highlight Unused Rules will highlight zero rules.
- D. Rule Usage Hit counter will reset.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 151

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 152

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 153

Topic #: 1

[\[All PCNSE Questions\]](#)

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

The screenshot shows the 'External Dynamic Lists' configuration window. The 'Name' field is 'TORexitNodes-MM'. The 'Type' is 'IP List'. The 'Source' is 'https://MineMeld/feeds/TORexitOut'. The 'Certificate Profile' is 'None (Disable Cert profile)'. The 'Repeat' is 'Hourly'. There are buttons for 'Test Source URL', 'OK', and 'Cancel'.

- 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.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 154

Topic #: 1

[\[All PCNSE Questions\]](#)

Which three split tunnel methods are supported by a GlobalProtect Gateway? (Choose three.)

- A. video streaming application
- B. Client Application Process
- C. Destination Domain
- D. Source Domain
- E. Destination user/group
- F. URL Category

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 155

Topic #: 1

[\[All PCNSE Questions\]](#)

Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two.)

- A. Successful GlobalProtect Deployed Activity
- B. GlobalProtect Deployment Activity
- C. Successful GlobalProtect Connection Activity
- D. GlobalProtect Quarantine Activity

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 156

Topic #: 1

[\[All PCNSE Questions\]](#)

Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 157

Topic #: 1

[\[All PCNSE Questions\]](#)

SD-WAN is designed to support which two network topology types? (Choose two.)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 158

Topic #: 1

[\[All PCNSE Questions\]](#)

Which option describes the operation of the automatic commit recovery feature?

- A. It enables a firewall to revert to the previous configuration if rule shadowing is detected.
- B. It enables a firewall to revert to the previous configuration if application dependency errors are found.
- C. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure.
- D. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 159

Topic #: 1

[\[All PCNSE Questions\]](#)

Which three items are important considerations during SD-WAN configuration planning? (Choose three.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 160

Topic #: 1

[\[All PCNSE Questions\]](#)

Starting with PAN-OS version 9.1, application dependency information is now reported in which two locations? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 161

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 162

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 163

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 164

Topic #: 1

[\[All PCNSE Questions\]](#)

How can an administrator configure the firewall 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 from connecting to the GlobalProtect gateway from a quarantined device
- B. 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 appropriate XSOAR playbook
- C. by using security policies, log forwarding profiles, and log settings
- D. there is no native auto-quarantine feature so a custom script would need to be leveraged

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 165

Topic #: 1

[\[All PCNSE Questions\]](#)

To protect your firewall and network from single source denial of service (DoS) attacks that can overwhelm its packet buffer and cause legitimate traffic to drop, you can configure:

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

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 166

Topic #: 1

[\[All PCNSE Questions\]](#)

A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg.txt. The firewall is currently running PAN-OS 10.0 and using a lab config. The contents of init-cfg.txt in the USB flash drive are as follows:

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

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

- A. The bootstrap.xml file is a required file, but it is missing
- B. Firewall must be in factory default state or have all private data deleted for bootstrapping
- C. The hostname is a required parameter, but it is missing in init-cfg.txt
- D. The USB must be formatted using the ext3 file system. FAT32 is not supported

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 167

Topic #: 1

[\[All PCNSE Questions\]](#)

An Administrator is configuring Authentication Enforcement and they would like to create an exemption rule to exempt a specific group from authentication. Which authentication enforcement object should they select?

- A. default-no-captive-portal
- B. default-authentication-bypass
- C. default-browser-challenge
- D. default-web-form

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 168

Topic #: 1

[\[All PCNSE Questions\]](#)

A bootstrap USB flash drive has been prepared using a Linux workstation to load the initial configuration of a Palo Alto Networks firewall. The USB flash drive was formatted using file system ntfs and the initial configuration is stored in a file named init-cfg.txt.

The contents of init-cfg.txt in the USB flash drive are as follows:

```
type=static
ip-address=10.5.107.19
default-gateway=10.5.107.1
netmask=255.255.255.0
ipv6-address=2001:400:f00::1/64
ipv6-default-gateway=2001:400:f00::2
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns_primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsyes, jumbo-frame
dhcp-send-hostname=no
dhcp-send-client-id=no
dhcp-accept-server-hostname=no
dhcp-accept-server-domain=no
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been powered on. Upon boot, the firewall fails to begin the bootstrapping process.

The failure is caused because:

- A. the bootstrap.xml file is a required file, but it is missing
- B. nit-cfg.txt is an incorrect filename, the correct filename should be init-cfg.xml
- C. The USB must be formatted using the ext4 file system
- D. There must be commas between the parameter names and their values instead of the equal symbols
- E. The USB drive has been formatted with an unsupported file system

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 169

Topic #: 1

[\[All PCNSE Questions\]](#)

To more easily reuse templates and template stacks, you can create template variables in place of firewall-specific and appliance-specific IP literals in your configurations.

Which one is the correct configuration?

- A. &Panorama
- B. @Panorama
- C. \$Panorama
- D. #Panorama

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 170

Topic #: 1

[\[All PCNSE Questions\]](#)

On the NGFW, how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 171

Topic #: 1

[\[All PCNSE Questions\]](#)

What is the maximum number of samples that can be submitted to WildFire manually per day?

- A. 1,000
- B. 2,000
- C. 5,000
- D. 15,000

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 172

Topic #: 1

[\[All PCNSE Questions\]](#)

What file type upload is supported as part of the basic WildFire service?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 173

Topic #: 1

[\[All PCNSE Questions\]](#)

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

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 174

Topic #: 1

[\[All PCNSE Questions\]](#)

Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?

- A. Create a zone protection profile with flood protection configured to defend an entire egress zone against SYN, ICMP, ICMPv6, UDP, and other IP flood attacks.
- B. Add a WildFire subscription to activate DoS and zone protection features.
- C. Replace the hardware firewall, because DoS and zone protection are not available with VM-Series systems.
- D. Measure and monitor the CPU consumption of the firewall data plane to ensure that each firewall is properly sized to support DoS and zone protection.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 175

Topic #: 1

[\[All PCNSE Questions\]](#)

DRAG DROP -

Please match the terms to their corresponding definitions.

Select and Place:

Answer Area

management plane

signature matching

security processing

network processing



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

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

high-density parallel processing for flexible standardized complex functions

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 176

Topic #: 1

[\[All PCNSE Questions\]](#)

An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices. The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed.

Which Panorama tool can help this organization?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 177

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 178

Topic #: 1

[\[All PCNSE Questions\]](#)

Which Panorama objects restrict administrative access to specific device-groups?

- A. admin roles
- B. authentication profiles
- C. templates
- D. access domains

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 179

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer is planning an SSL decryption implementation.

Which of the following statements is a best practice for SSL decryption?

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 180

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator receives the following error message:

"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192.168.33.33/24 type IPv4 address protocol 0 port 0, received remote id 172.16.33.33/24 type IPv4 address protocol 0 port 0."

How should the administrator identify the root cause of this error message?

- A. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure.
- B. Check whether the VPN peer on one end is set up correctly using policy-based VPN.
- C. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate.
- D. In the IPSec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers.

Show Suggested Answer



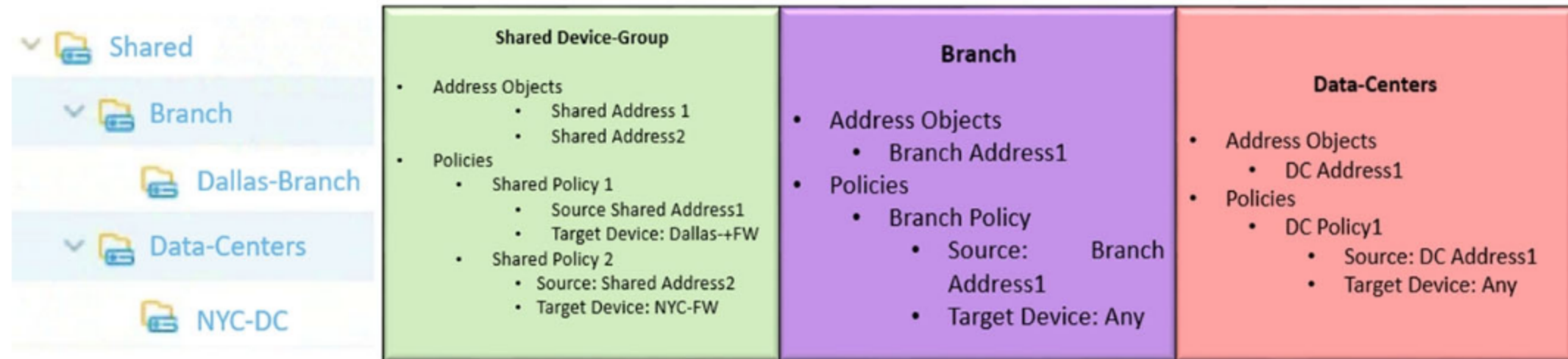
Actual exam question from Palo Alto Networks's PCNSE

Question #: 181

Topic #: 1

[\[All PCNSE Questions\]](#)

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



Dallas-Branch has Dallas-FW as a member of the Dallas-Branch device-group

NYC-DC has NYC-FW as a member of the NYC-DC device-group

What objects and policies will the Dallas-FW receive if "Share Unused Address and Service Objects" is enabled in Panorama?

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 182

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has purchased WildFire subscriptions for 90 firewalls globally.

What should the administrator consider with regards to the WildFire infrastructure?

- A. To comply with data privacy regulations, WildFire signatures and verdicts are not shared globally.
- B. Palo Alto Networks owns and maintains one global cloud and four WildFire regional clouds.
- C. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds.
- D. The WildFire Global Cloud only provides bare metal analysis.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 183

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (CAs): i. Enterprise-Trusted-CA, which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system.) ii. Enterprise-Untrusted-CA, which is verified as Forward Untrust Certificate iii. Enterprise-Intermediate-CA iv. Enterprise-Root-CA, which is verified only as Trusted Root CA

An end-user visits <https://www.example-website.com/> with a server certificate Common Name (CN): www.example-website.com. The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewall.

The end-user's browser will show that the certificate for www.example-website.com was issued by which of the following?

- A. Enterprise-Trusted-CA which is a self-signed CA
- B. Enterprise-Root-CA which is a self-signed CA
- C. Enterprise-Intermediate-CA which was, in turn, issued by Enterprise-Root-CA
- D. Enterprise-Untrusted-CA which is a self-signed CA

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 184

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 185

Topic #: 1

[\[All PCNSE Questions\]](#)

DRAG DROP -

Match each SD-WAN configuration element to the description of that element.

Select and Place:

Answer Area

SD-WAN interface profile

Path Quality profile

Traffic Distribution profile



This profile or rule matches traffic to applications and services, sources, destinations, and users. The profile or rule indicates when and how the firewall performs application-based SD-WAN path selection

This profile or rule specifies how the firewall selects a new best path if the current preferred path exceeds a path quality threshold.

This profile or rule specifies the maximum latency, jitter, and packet loss thresholds.

This profile or rule specifies the tag that is applied to the physical interface. The profile or rule also specifies which type of Link that interface is.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 186

Topic #: 1

[\[All PCNSE Questions\]](#)

When overriding a template configuration locally on a firewall, what should you consider?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 187

Topic #: 1

[\[All PCNSE Questions\]](#)

When setting up a security profile, which three items can you use? (Choose three.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 188

Topic #: 1

[\[All PCNSE Questions\]](#)

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 the HA pair to a base image.
- C. Upgrade one major version at a time.
- D. Upgrade two major versions at a time.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 189

Topic #: 1

[\[All PCNSE Questions\]](#)

What are three types of Decryption Policy rules? (Choose three.)

- A. SSL Inbound Inspection
- B. SSH Proxy
- C. SSL Forward Proxy
- D. Decryption Broker
- E. Decryption Mirror

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 190

Topic #: 1

[\[All PCNSE Questions\]](#)

During SSL decryption, which three factors affect resource consumption? (Choose three.)

- A. key exchange algorithm
- B. transaction size
- C. TLS protocol version
- D. applications ta non-standard ports
- E. certificate issuer

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 191

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer must configure a new SSL decryption deployment.

Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

- A. A Decryption profile must be attached to the Decryption policy that the traffic matches.
- B. There must be a certificate with both the Forward Trust option and Forward Untrust option selected.
- C. A Decryption profile must be attached to the Security policy that the traffic matches.
- D. There must be a certificate with only the Forward Trust option selected.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 192

Topic #: 1

[\[All PCNSE Questions\]](#)

Which two features require another license on the NGFW? (Choose two.)

- A. SSL Inbound Inspection
- B. SSL Forward Proxy
- C. Decryption Mirror
- D. Decryption Broker

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 193

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has a PA-820 firewall with an active Threat Prevention subscription. The administrator is considering adding a WildFire subscription. How does adding the WildFire subscription improve the security posture of the organization?

- A. WildFire and Threat Prevention combine to minimize the attack surface.
- B. After 24 hours, WildFire signatures are included in the antivirus update.
- C. Protection against unknown malware can be provided in near real-time.
- D. WildFire and Threat Prevention combine to provide the utmost security posture for the firewall.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 194

Topic #: 1

[\[All PCNSE Questions\]](#)

What are two characteristic types that can be defined for a variable? (Choose two.)

- A. zone
- B. FQDN
- C. IP netmask
- D. path group

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 195

Topic #: 1

[\[All PCNSE Questions\]](#)

A remote administrator needs access to the firewall on an untrust interface. Which three options would you configure on an Interface Management profile to secure management access? (Choose three.)

- A. Permitted IP Addresses
- B. SSH
- C. https
- D. User-ID
- E. HTTP

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 196

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator needs to troubleshoot a User-ID deployment. The administrator believes that there is an issue related to LDAP authentication. The administrator wants to create a packet capture on the management plane.

Which CLI command should the administrator use to obtain the packet capture for validating the configuration?

- A. > scp export mgmt-pcap from mgmt.pcap to (username@host:path)
- B. > scp export poap-mgmt from poap.mgmt to (username@host:path)
- C. > ftp export mgmt-pcap from mgmt.pcap to <FTF host>
- D. > scp export pcap from pcap to (username@host:path)

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 197

Topic #: 1

[\[All PCNSE Questions\]](#)

When you configure an active/active high availability pair, which two links can you use? (Choose two.)

- A. 311
- B. Console Backup
- C. HSCI-C
- D. HA2 backup

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 198

Topic #: 1

[\[All PCNSE Questions\]](#)

What are two common reasons to use a "No Decrypt" action to exclude traffic from SSL decryption? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 199

Topic #: 1

[\[All PCNSE Questions\]](#)

PBF can address which two scenarios? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 200

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall should be advertising the static route 10.2.0.0/24 into OSPF. The configuration on the neighbour is correct, but the route is not in the neighbour's routing table.

Which two configurations should you check on the firewall? (Choose two.)

- A. Ensure that the OSPF neighbour state is "2-Way"
- B. In the OSPF configuration, ensure that the correct redistribution profile is selected in the OSPF Export Rules section.
- C. Within the redistribution profile ensure that Redist is selected.
- D. In the redistribution profile check that the source type is set to "ospf."

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 201

Topic #: 1

[\[All PCNSE Questions\]](#)

Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 202

Topic #: 1

[\[All PCNSE Questions\]](#)

What are three valid qualifiers for a Decryption Policy Rule match? (Choose three.)

- A. App-ID
- B. Custom URL Category
- C. User-ID
- D. Destination Zone
- E. Source Interface

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 203

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator needs to gather information about the CPU utilization on both the management plane and the data plane.

Where does the administrator view the desired data?

- A. Resources Widget on the Dashboard
- B. Monitor > Utilization
- C. Support > Resources
- D. Application Command and Control Center

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 204

Topic #: 1

[\[All PCNSE Questions\]](#)

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

- A. > show system state filter-pretty sys.s1.p8.stats
- B. > show system state filter-pretty sys.s1.p8.med
- C. > show interface ethernet1/8
- D. > show system state filter-pretty sys.s1.p8.phy

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 205

Topic #: 1

[\[All PCNSE Questions\]](#)

A variable name must start with which symbol?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 206

Topic #: 1

[\[All PCNSE Questions\]](#)

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" re 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 1
- B. Route 3
- C. Route 2
- D. Route 4

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 207

Topic #: 1

[\[All PCNSE Questions\]](#)

In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 208

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator plans to deploy 15 firewalls to act as GlobalProtect gateways around the world. Panorama will manage the firewalls.

The firewalls will provide access to mobile users and act as edge locations to on-premises infrastructure. The administrator wants to scale the configuration out quickly and wants all of the firewalls to use the same template configuration.

Which two solutions can the administrator use to scale this configuration? (Choose two.)

- A. virtual systems
- B. template stacks
- C. variables
- D. collector groups

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 209

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 210

Topic #: 1

[\[All PCNSE Questions\]](#)

As a best practice, which URL category should you target first for SSL decryption?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 211

Topic #: 1

[\[All PCNSE Questions\]](#)

Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

- A. LDAP Server Profile configuration
- B. GlobalProtect
- C. Windows-based User-ID agent
- D. PAN-OS integrated User-ID agent

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 212

Topic #: 1

[\[All PCNSE Questions\]](#)

DRAG DROP -

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration. Place the steps in order.

Select and Place:

Answer Area

In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Upload or drag and drop the technical support file.

Map the zone type and area of the architecture to each zone.

Follow the steps to download the BPA report bundle.

Step 1

Step 2

Step 3

Step 4

Step 5

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 213

Topic #: 1

[\[All PCNSE Questions\]](#)

DRAG DROP -

Place the steps in the WildFire process workflow in their correct order.

Select and Place:

Answer Area

The firewall hashes the file and looks up a verdict in the WildFire database. However, the firewall does not find a match.

WildFire uses static analysis based on machine learning to analyze the file, in order to classify malicious features.

Regardless of the verdict, WildFire uses a heuristic engine to examine the file and determines that the file exhibits suspicious behavior.

WildFire generates a new DNS, URL categorization, and antivirus signatures for the new threat.

FIRST

SECOND

THIRD

FOURTH

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 214

Topic #: 1

[\[All PCNSE Questions\]](#)

In a Panorama template, which three types of objects are configurable? (Choose three.)

- A. certificate profiles
- B. HIP objects
- C. QoS profiles
- D. security profiles
- E. interface management profiles

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 215

Topic #: 1

[\[All PCNSE Questions\]](#)

An internal system is not functioning. The firewall administrator has determined that the incorrect egress interface is being used. After looking at the configuration, the administrator believes that the firewall is not using a static route.

What are two reasons why the firewall might not use a static route? (Choose two.)

- A. duplicate static route
- B. no install on the route
- C. disabling of the static route
- D. path monitoring on the static route

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 216

Topic #: 1

[\[All PCNSE Questions\]](#)

A customer is replacing its legacy remote-access VPN solution. Prisma Access has been selected as the replacement. During onboarding, the following options and licenses were selected and enabled:

- Prisma Access for Remote Networks: 300Mbps
- Prisma Access for Mobile Users: 1500 Users
- Cortex Data Lake: 2TB
- Trusted Zones: trust
- Untrusted Zones: untrust
- Parent Device Group: shared

The customer wants to forward to a Splunk SIEM the logs that are generated by users that are connected to Prisma Access for Mobile Users. Which two settings must the customer configure? (Choose two.)

- A. Configure Panorama Collector group device log forwarding to send logs to the Splunk syslog server.
- B. Configure Cortex Data Lake log forwarding and add the Splunk syslog server.
- C. Configure a log forwarding profile and select the Panorama/Cortex Data Lake checkbox. Apply the Log Forwarding profile to all of the security policy rules in Mobile_User_Device_Group.
- D. Configure a Log Forwarding profile, select the syslog checkbox, and add the Splunk syslog server. Apply the Log Forwarding profile to all of the security policy rules in the Mobile_User_Device_Group.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 217

Topic #: 1

[\[All PCNSE Questions\]](#)

A network administrator wants to use a certificate for the SSL/TLS Service Profile. Which type of certificate should the administrator use?

- A. machine certificate
- B. server certificate
- C. certificate authority (CA) certificate
- D. client certificate

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 218

Topic #: 1

[\[All PCNSE Questions\]](#)

In a security-first network, what is the recommended threshold value for content updates to be dynamically updated?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 219

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 220

Topic #: 1

[\[All PCNSE Questions\]](#)

In a firewall, which three decryption methods are valid? (Choose three.)

- A. SSL Outbound Proxyless Inspection
- B. SSL Inbound Inspection
- C. SSH Proxy
- D. SSL Inbound Proxy
- E. Decryption Mirror

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 221

Topic #: 1

[\[All PCNSE Questions\]](#)

DRAG DROP -

Match each type of DoS attack to an example of that type of attack.

Select and Place:

Answer Area

application-based attack

protocol-based attack

volumetric attack

Slowloris attack

SYN flood attack

UDP flood attack

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 222

Topic #: 1

[\[All PCNSE Questions\]](#)

Using multiple templates in a stack to manage many firewalls provides which two advantages? (Choose two.)

- A. inherit address-objects from templates
- B. define a common standard template configuration for firewalls
- C. standardize server profiles and authentication configuration across all stacks
- D. standardize log-forwarding profiles for security polices across all stacks

Show Suggested Answer







Actual exam question from Palo Alto Networks's PCNSE

Question #: 223

Topic #: 1

[\[All PCNSE Questions\]](#)

The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.

<input type="checkbox"/>	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...	USAGE
<input type="checkbox"/>	 Forward-Trust-Certificate	CN = Forward-Trust-Certificate	CN = Forward-Trust-Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:48:4...	valid	RSA	Forward Trust Certificate
<input type="checkbox"/>	 Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:49:0...	valid	RSA	
<input type="checkbox"/>	 Firewall-CA	CN = Firewall-CA	CN = Firewall-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:55:2...	valid	RSA	
<input type="checkbox"/>	 Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:56:4...	valid	RSA	

An end-user visits the untrusted website <https://www.firewall-do-not-trust-website.com>.

Which certificate authority (CA) certificate will be used to sign the untrusted webserver certificate?

- A. Forward-Untrust-Certificate
- B. Forward-Trust-Certificate
- C. Firewall-CA
- D. Firewall-Trusted-Root-CA

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 224

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 225

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 226

Topic #: 1

[\[All PCNSE Questions\]](#)

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 SSL/TLS connection?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 227

Topic #: 1

[\[All PCNSE Questions\]](#)

When you configure a Layer 3 interface, what is one mandatory step?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 228

Topic #: 1

[\[All PCNSE Questions\]](#)

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. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall.
- C. Virtual systems cannot have dedicated service routes configured; and virtual systems always use the global service and service route settings for the firewall.
- D. The interface must be used for traffic to the required external services.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 229

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version.

What is considered best practice for this scenario?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 230

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls. The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls.

If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the configuration does not appear, what is the root cause?

- A. Panorama does not have valid licenses to push the dynamic updates.
- B. Panorama has no connection to Palo Alto Networks update servers.
- C. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed.
- D. No service route is configured on the firewalls to Palo Alto Networks update servers.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 231

Topic #: 1

[\[All PCNSE Questions\]](#)

An enterprise Information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems. However, a recent phishing campaign against the organization has prompted information Security to look for more controls that can secure access to critical assets. For users that need to access these systems, Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA.

What should the enterprise do to use PAN-OS MFA?

- A. Use a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns.
- B. Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy.
- C. Configure a Captive Portal authentication policy that uses an authentication sequence.
- D. Configure a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 232

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator wants to enable zone protection.

Before doing so, what must the administrator consider?

- A. Activate a zone protection subscription.
- B. Security policy rules do not prevent lateral movement of traffic between zones.
- C. The zone protection profile will apply to all interfaces within that zone.
- D. To increase bandwidth, no more than one firewall interface should be connected to a zone.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 233

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 234

Topic #: 1

[\[All PCNSE Questions\]](#)

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 supported version of the app + threat update.
- D. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 235

Topic #: 1

[\[All PCNSE Questions\]](#)

The UDP-4501 protocol-port is used between which two GlobalProtect components?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 236

Topic #: 1

[\[All PCNSE Questions\]](#)

An enterprise has a large Palo Alto Networks footprint that includes onsite firewalls and Prisma Access for mobile users, which is managed by Panorama. The enterprise already uses GlobalProtect with SAML authentication to obtain IP-to-user mapping information.

However, Information Security wants to use this information in Prisma Access for policy enforcement based on group mapping. Information Security uses on-premises Active Directory (AD) but is uncertain about what is needed for Prisma Access to learn groups from AD.

How can policies based on group mapping be learned and enforced in Prisma Access?

- A. Configure Prisma Access to learn group mapping via SAML assertion.
- B. Set up group mapping redistribution between an onsite Palo Alto Networks firewall and Prisma Access.
- C. Assign a master device in Panorama through which Prisma Access learns groups.
- D. Create a group mapping configuration that references an LDAP profile that points to on-premises domain controllers.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 237

Topic #: 1

[\[All PCNSE Questions\]](#)

What happens to traffic traversing SD-WAN fabric that doesn't match any SD-WAN policies?

- A. Traffic is dropped because there is no matching SD-WAN policy to direct traffic.
- B. Traffic matches a catch-all policy that is created through the SD-WAN plugin.
- C. Traffic matches implied policy rules and is redistributed round robin across SD-WAN links.
- D. Traffic is forwarded to the first physical interface participating in SD-WAN based on lowest interface number (i.e., Eth1/1 over Eth1/3).

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 238

Topic #: 1

[\[All PCNSE Questions\]](#)

A remote administrator needs firewall access on an untrusted interface. Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two.)

- A. certificate authority (CA) certificate
- B. server certificate
- C. client certificate
- D. certificate profile

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 239

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator with 84 firewalls and Panorama does not see any WildFire logs in Panorama.

All 84 firewalls have an active WildFire subscription. On each firewall, WildFire logs are available.

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

- A. WildFire logs
- B. System logs
- C. Threat logs
- D. Traffic logs

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 240

Topic #: 1

[\[All PCNSE Questions\]](#)

A company wants to use their Active Directory groups to simplify their Security policy creation from Panorama.
Which configuration is necessary to retrieve groups from Panorama?

- A. Configure an LDAP Server profile and enable the User-ID service on the management interface.
- B. Configure a group mapping profile to retrieve the groups in the target template.
- C. Configure a Data Redistribution Agent to receive IP User Mappings from User-ID agents.
- D. Configure a master device within the device groups.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 241

Topic #: 1

[\[All PCNSE Questions\]](#)

How can packet buffer protection be configured?

- A. at zone level to protect firewall resources and ingress zones, but not at the device level
- B. at the interface level to protect firewall resources
- C. at the device level (globally) to protect firewall resources and ingress zones, but not at the zone level
- D. at the device level (globally) and, if enabled globally, at the zone level

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 242

Topic #: 1

[\[All PCNSE Questions\]](#)

An existing NGFW customer requires direct internet access offload locally at each site, and IPSec connectivity to all branches over public internet. One requirement is that no new SD-WAN hardware be introduced to the environment.

What is the best solution for the customer?

- A. Configure a remote network on PAN-OS
- B. Upgrade to a PAN-OS SD-WAN subscription
- C. Configure policy-based forwarding
- D. Deploy Prisma SD-WAN with Prisma Access

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 243

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator requires an A/P HA pair to fail over more quickly due to critical business application uptime requirements.

What is the correct setting?

- A. Change the HA timer profile to "user-defined" and manually set the timers.
- B. Change the HA timer profile to "fast".
- C. Change the HA timer profile to "aggressive" or customize the settings in advanced profile.
- D. Change the HA timer profile to "quick" and customize in advanced profile.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 244

Topic #: 1

[\[All PCNSE Questions\]](#)

What is the function of a service route?

- A. The service packets exit the firewall on the port assigned for the external service. The server sends its response to the configured source interface and source IP address.
- B. The service packets enter the firewall on the port assigned from the external service. The server sends its response to the configured destination interface and destination IP address.
- C. The service route is the method required to use the firewall's management plane to provide services to applications.
- D. Service routes provide access to external services, such as DNS servers, external authentication servers or Palo Alto Networks services like the Customer Support Portal.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 245

Topic #: 1

[\[All PCNSE Questions\]](#)

DRAG DROP -

Place the steps to onboard a ZTP firewall into Panorama/CSP/ZTP-Service in the correct order.

Select and Place:

Installer or IT administrator registers ZTP firewalls by adding them to Panorama using firewall serial number and claim key.

After connecting to the internet, the ZTP firewall requests a device certificate from the CSP in order to connect to the ZTP service.

The ZTP firewalls connect to Panorama and the device group and template configurations are pushed from Panorama to the ZTP firewalls.

The ZTP service pushes the Panorama IP or FQDN to the ZTP firewalls.

Panorama registers the firewalls with the CSP. After the firewalls are successfully registered, the firewall is associated with the same ZTP tenant as the Panorama in the ZTP service.

Answer Area

FIRST

SECOND

THIRD

FOURTH

FIFTH

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 246

Topic #: 1

[\[All PCNSE Questions\]](#)

Which of the following commands would you use to check the total number of the sessions that are currently going through SSL Decryption processing?

- A. show session all filter ssl-decryption yes total-count yes
- B. show session all ssl-decrypt yes count yes
- C. show session all filter ssl-decrypt yes count yes
- D. show session filter ssl-decryption yes total-count yes

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 247

Topic #: 1

[\[All PCNSE Questions\]](#)

Template Stack



Name

NYC-Branch

Default VSYS

vsys1



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

Description



TEMPLATES



Global



NYCFW



Add



Delete



Move Up



Move Down

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

How can the issue be corrected?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 248

Topic #: 1

[\[All PCNSE Questions\]](#)

While troubleshooting an SSL Forward Proxy decryption issue, which PAN-OS CLI command would you use to check the details of the end entity certificate that is signed by the Forward Trust Certificate or Forward Untrust Certificate?

- A. show system setting ssl-decrypt certs
- B. show system setting ssl-decrypt certificate
- C. debug dataplane show ssl-decrypt ssl-stats
- D. show system setting ssl-decrypt certificate-cache

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 249

Topic #: 1

[\[All PCNSE Questions\]](#)

Which action disables Zero Touch Provisioning (ZTP) functionality on a ZTP firewall during the onboarding process?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 250

Topic #: 1

[\[All PCNSE Questions\]](#)

In URL filtering, which component matches URL patterns?

- A. live URL feeds on the management plane
- B. security processing on the data plane
- C. single-pass pattern matching on the data plane
- D. signature matching on the data plane

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 251

Topic #: 1

[\[All PCNSE Questions\]](#)

In a template, you can configure which two objects? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 252

Topic #: 1

[\[All PCNSE Questions\]](#)

An organization's administrator has the funds available to purchase more firewalls to increase the organization's security posture.

The partner SE recommends placing the firewalls as close as possible to the resources that they protect.

Is the SE's advice correct, and why or why not?

- A. No. Firewalls provide new defense and resilience to prevent attackers at every stage of the cyberattack lifecycle, independent of placement.
- B. Yes. Firewalls are session-based, so they do not scale to millions of CPS.
- C. No. Placing firewalls in front of perimeter DDoS devices provides greater protection for sensitive devices inside the network.
- D. Yes. Zone Protection profiles can be tailored to the resources that they protect via the configuration of specific device types and operating systems.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 253

Topic #: 1

[\[All PCNSE Questions\]](#)

DRAG DROP -

Match each GlobalProtect component to the purpose of that component.

Select and Place:

Answer Area

GlobalProtect Gateway

GlobalProtect clientless

GlobalProtect Portal

GlobalProtect app



management functions for
GlobalProtect infrastructure

security enforcement for
traffic from GlobalProtect apps

software on endpoints that
enables access to network
resources

secure remote access to
common enterprise web
applications

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 254

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator needs to validate that policies that will be deployed will match the appropriate rules in the device-group hierarchy. Which tool can the administrator use to review the policy creation logic and verify that unwanted traffic is not allowed?

- A. Preview Changes
- B. Policy Optimizer
- C. Managed Devices Health
- D. Test Policy Match

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 255

Topic #: 1

[\[All PCNSE Questions\]](#)

What is a key step in implementing WildFire best practices?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 256

Topic #: 1

[\[All PCNSE Questions\]](#)

What happens when an A/P firewall cluster synchronizes IPsec tunnel security associations (SAs)?

- A. Phase 2 SAs are synchronized over HA2 links.
- B. Phase 1 and Phase 2 SAs are synchronized over HA2 links.
- C. Phase 1 SAs are synchronized over HA1 links.
- D. Phase 1 and Phase 2 SAs are synchronized over HA3 links.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 257

Topic #: 1

[\[All PCNSE Questions\]](#)

A security engineer needs to mitigate packet floods that occur on a set of servers behind the internet facing interface of the firewall.

Which Security Profile should be applied to a policy to prevent these packet floods?

- A. Vulnerability Protection profile
- B. DoS Protection profile
- C. Data Filtering profile
- D. URL Filtering profile

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 258

Topic #: 1

[\[All PCNSE Questions\]](#)

What are three reasons why an installed session can be identified with the "application incomplete" tag? (Choose three.)

- A. There was no application data after the TCP connection was established.
- B. The client sent a TCP segment with the PUSH flag set.
- C. The TCP connection was terminated without identifying any application data.
- D. There is not enough application data after the TCP connection was established.
- E. The TCP connection did not fully establish.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 259

Topic #: 1

[\[All PCNSE Questions\]](#)

Which three statements correctly describe Session 380280? (Choose three.)

```
> show session id 380280
Session                               380280
c2s flow:
  source:                             172.17.149.129 [L3-Trust]
  dst:                                  104.154.09.105
  proto:                                6
  sport:                               60997          dport:         443
  state:                               ACTIVE         type:          FLOW
  src user:                            unknown
  dst user:                            unknown

s2c flow:
  source:                             104.154.89.105 [L3-Untrust]
  dst:                                  10.46.42.149
  proto:                                6
  sport:                               443          dport:         7260
  state:                               ACTIVE         type:          FLOW
  src user:                            unknown
  dst user:                            unknown

start time                            : Tue Feb 9 20:38:42 2021
timeout                                : 15 sec
time to live                            : 2 sec
total byte count (c2s)                  : 3330
total byte count (s2c)                  : 12698
layer7 packet count (c2s)               : 14
layer7 packet count (s2c)               : 19
vsys                                    : vsys1
application                             : web-browsing
rule                                     : Trust-to-Untrust
service timeout override (index)        : False
session to be logged at end              : True
session in session ager                  : True
session updated by HA peer               : False
session proxied                          : True
address/port translation                 : source
nat-rule                                 : Trust-NAT (vsys1)
Layer7 processing                        : Completed
URL filtering enabled                    : True
URL category                             : computer-and-internet-info, low-risk
session via syn-cookies                  : False
session terminated on host                : False
session traverses tunnel                  : False
session terminate tunnel                 : False
captive portal session                   : False
ingress interface                        : etheriet1/6
egress interface                         : ethernet1/3
session GOS rule                          : N/A (class 4)
tracker stage 17proc                     : proxy timer expired
end-reason                               : unknown
```

- A. The application was initially identified as "ssl."
- B. The session has ended with the end-reason "unknown."
- C. The session did not go through SSL decryption processing.
- D. The application shifted to "web-browsing."
- E. The session went through SSL decryption processing.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 260

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator's device-group commit push is failing due to a new URL category.

How should the administrator correct this issue?

- A. update the Firewall Apps and Threat version to match the version of Panorama
- B. change the new category action to "alert" and push the configuration again
- C. ensure that the firewall can communicate with the URL cloud
- D. verify that the URL seed tile has been downloaded and activated on the firewall

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 261

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 262

Topic #: 1

[\[All PCNSE Questions\]](#)

Which type of interface does a firewall use to forward decrypted traffic to a security chain for inspection?

- A. Layer 3
- B. Layer 2
- C. Tap
- D. Decryption Mirror

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 263

Topic #: 1

[\[All PCNSE Questions\]](#)

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.

Security Policy Rule ?

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Action Setting

Actions Allow v

Send ICMP unreachable

Log Setting

Log at Session Start

Log at Session End

Log Forwarding None v

Profile Setting

Profile Type Profiles v

Antivirus default v

Vulnerability Protections strict v

Anti-Spyware strict v

URL Filtering default v

File Blocking None v

Data Filtering None v

WildFire Analysis default v

Other Settings

Schedule None v

QoS Marking None v

Disable Server Responsive Inspection

OK
Cancel

B.

Syslog Server Profile ?

Name SyslogProfile1

Servers | Custom Log Format

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

+ Add
 - Delete

Enter the IP address or FQDN of the Syslog server

OK
Cancel

C.

Panorama Settings ?

Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

Share Unused Address and Service Objects with Devices

Objects defined in ancestors will take higher precedence

Enable reporting and filtering on groups

When enabled Panorama will locally store users and groups from Master Devices

OK
Cancel

D.

Panorama Settings

Panorama Servers

10.99.1.21

Enable pushing device monitoring data to Panorama

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

Enable automated commit recovery

Number of attempts to check for Panorama connectivity 1

Interval between retries (sec) 10

Disable Panorama Policy and Objects
Disable Device and Network Template
OK
Cancel



Actual exam question from Palo Alto Networks's PCNSE

Question #: 264

Topic #: 1

[\[All PCNSE Questions\]](#)

Which configuration task is best for reducing load on the management plane?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 265

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 266

Topic #: 1

[\[All PCNSE Questions\]](#)

Cortex XDR notifies an administrator about grayware on the endpoints. There are no entries about grayware in any of the logs of the corresponding firewall. Which setting can the administrator configure on the firewall to log grayware verdicts?

- A. in Threat General Settings, select "Report Grayware Files"
- B. within the log settings option in the Device tab
- C. in WildFire General Settings, select "Report Grayware Files"
- D. within the log forwarding profile attached to the Security policy rule

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 267

Topic #: 1

[\[All PCNSE Questions\]](#)

Your company has 10 Active Directory domain controllers spread across multiple WAN links. All users authenticate to Active Directory. Each link has substantial network bandwidth to support all mission-critical applications. The firewall's management plane is highly utilized. Given this scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

- A. PAN-OS integrated agent
- B. Citrix terminal server agent with adequate data-plane resources
- C. Captive Portal
- D. Windows-based User-ID agent on a standalone server

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 268

Topic #: 1

[\[All PCNSE Questions\]](#)

Which component enables you to configure firewall resource protection settings?

- A. DoS Protection Profile
- B. QoS Profile
- C. Zone Protection Profile
- D. DoS Protection policy

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 269

Topic #: 1

[\[All PCNSE Questions\]](#)

How can an administrator use the Panorama device-deployment option to update the apps and threat version of an HA pair of managed firewalls?

- A. Choose the download and install action for both members of the HA pair in the Schedule object
- B. Switch context to the firewalls to start the download and install process
- C. Download the apps to the primary no further action is required
- D. Configure the firewall's assigned template to download the content updates

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 270

Topic #: 1

[\[All PCNSE Questions\]](#)

A Panorama administrator configures a new zone and uses the zone in a new Security policy. After the administrator commits the configuration to Panorama, which device-group commit push operation should the administrator use to ensure that the push is successful?

- A. merge with candidate config
- B. include device and network templates
- C. specify the template as a reference template
- D. force template values

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 271

Topic #: 1

[\[All PCNSE Questions\]](#)

What would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain?

- A. a Security policy with 'known-user' selected in the Source User field
- B. a Security policy with 'unknown' selected in the Source User field
- C. an Authentication policy with 'known-user' selected in the Source User field
- D. an Authentication policy with 'unknown' selected in the Source User field

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 272

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator needs firewall access on a trusted interface. Which two components are required to configure certificate-based, secure authentication to the web UI? (Choose two.)

- A. server certificate
- B. SSL/TLS Service Profile
- C. certificate profile
- D. SSH Service Profile

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 273

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator is building Security rules within a device group to block traffic to and from malicious locations. How should those rules be configured to ensure that they are evaluated with a high priority?

- A. Create the appropriate rules with a Block action and apply them at the top of the local firewall Security rules
- B. Create the appropriate rules with a Block action and apply them at the top of the Security Pre-Rules
- C. Create the appropriate rules with a Block action and apply them at the top of the Security Post-Rules
- D. Create the appropriate rules with a Block action and apply them at the top of the Default Rules

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 274

Topic #: 1

[\[All PCNSE Questions\]](#)

When planning to configure SSL Forward Proxy on a PA-5260, a user asks how SSL decryption can be implemented using a phased approach in alignment with Palo Alto Networks best practices. What should you recommend?

- A. Enable SSL decryption for known malicious source IP addresses
- B. Enable SSL decryption for malicious source users
- C. Enable SSL decryption for source users and known malicious URL categories
- D. Enable SSL decryption for known malicious destination IP addresses

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 275

Topic #: 1

[\[All PCNSE Questions\]](#)

What are two valid deployment options for Decryption Broker? (Choose two.)

- A. Transparent Bridge Security Chain
- B. Transparent Mirror Security Chain
- C. Layer 2 Security Chain
- D. Layer 3 Security Chain

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 276

Topic #: 1

[\[All PCNSE Questions\]](#)

A network security engineer is attempting to peer a virtual router on a PAN-OS firewall with an external router using the BGP protocol. The peer relationship is not establishing. What command could the engineer run to see the current state of the BGP state between the two devices?

- A. show routing protocol bgp rib-out
- B. show routing protocol bgp peer
- C. show routing protocol bgp summary
- D. show routing protocol bgp state

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 277

Topic #: 1

[\[All PCNSE Questions\]](#)

What is the best description of the HA4 Keep-alive Threshold (ms)?

- A. the timeframe that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing
- B. the timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional
- C. the maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational
- D. the time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 278

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer is tasked with enabling SSL decryption across the environment. What are three valid parameters of an SSL Decryption policy? (Choose three.)

- A. GlobalProtect HIP
- B. source users
- C. App-ID
- D. URL categories
- E. source and destination IP addresses

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 279

Topic #: 1

[\[All PCNSE Questions\]](#)

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

- A. It applies to existing sessions and is not global
- B. It applies to existing sessions and is global
- C. It applies to new sessions and is global
- D. It applies to new sessions and is not global

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 280

Topic #: 1

[\[All PCNSE Questions\]](#)

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

- A. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs
- B. Study the release notes and install new App-IDs if they are determined to have low impact
- C. Configure a security policy rule to allow new App-IDs that might have network-wide impact
- D. Perform a Best Practice Assessment to evaluate the impact of the new or modified App-IDs

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 281

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 282

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer needs to redistribute User-ID mappings from multiple data centers. Which data flow best describes redistribution of user mappings?

- A. User-ID agent to firewall
- B. firewall to firewall
- C. Domain Controller to User-ID agent
- D. User-ID agent to Panorama

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 283

Topic #: 1

[\[All PCNSE Questions\]](#)

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

- A. Add a firewall to both the device group and the template
- B. Add the template as a reference template in the device group
- C. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings
- D. Specify the target device as the master device in the device group

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 284

Topic #: 1

[\[All PCNSE Questions\]](#)

What best describes the HA Promotion Hold Time?

- A. the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost
- B. the time that is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously
- C. the time that is recommended to avoid an HA failover due to the occasional flapping of neighboring devices
- D. the time that a passive firewall with a low device priority will wait before taking over as the active firewall if the firewall is operational again

Show Suggested Answer



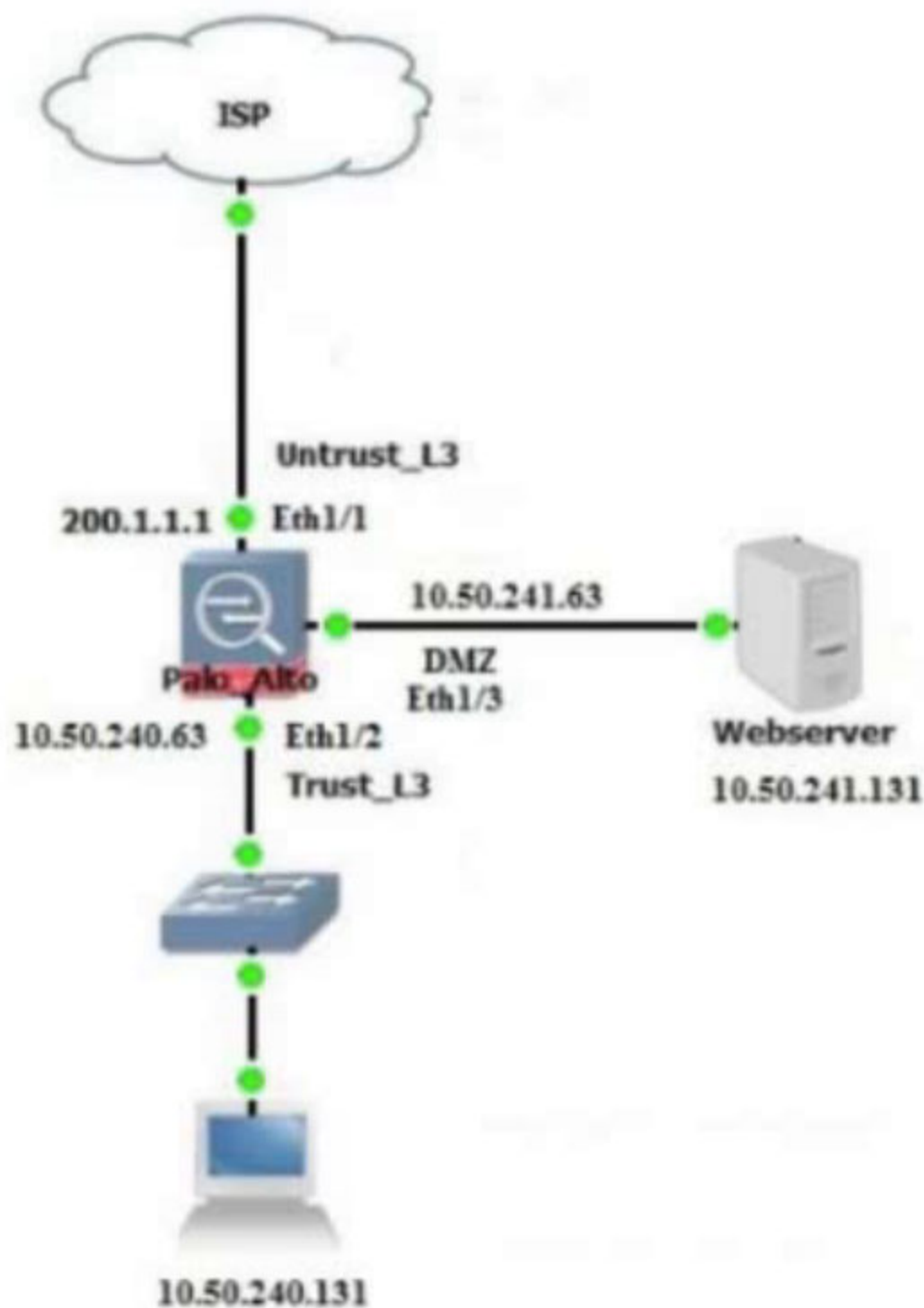
Actual exam question from Palo Alto Networks's PCNSE

Question #: 285

Topic #: 1

[\[All PCNSE Questions\]](#)

A user at an internal system queries the DNS server for their web server with a private IP of 10.250.241.131 in the DMZ. The DNS server returns an address of the web servers public address, 200.1.1.10. In order to reach the web server, which security rule and U-Turn NAT rule must be configured on the firewall?



- A. NAT Rule: Source Zone: Untrust_L3 Source IP: Any Destination Zone: DMZ Destination IP: 200.1.1.10 Destination Translation address: 10.250.241.131 Security Rule: Source IP: Any Destination Zone: DMZ Destination IP: 10.250.241.131
- B. NAT Rule: Source Zone: Trust_L3 Source IP: Any Destination Zone: DMZ Destination IP: 200.1.1.10 Destination Translation address: 10.250.241.131 Security Rule: Source Zone: Untrust-L3 Source IP: Any Destination Zone: DMZ Destination IP: 10.250.241.131
- C. NAT Rule: Source Zone: Untrust_L3 Source IP: Any Destination Zone: Untrust_L3 Destination IP: 200.1.1.10 Destination Translation address: 10.250.241.131 Security Rule: Source Zone: Untrust-L3 Source IP: Any Destination Zone: DMZ Destination IP: 10.250.241.131
- D. NAT Rule: Source Zone: Trust_L3 Source IP: Any Destination Zone: Untrust_L3 Destination IP: 200.1.1.10 Destination Translation address: 10.250.241.131 Security Rule: Source Zone: Trust-L3 Source IP: Any Destination Zone: DMZ Destination IP: 200.1.1.10

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 286

Topic #: 1

[\[All PCNSE Questions\]](#)

What is considered the best practice with regards to zone protection?

- A. Use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs
- B. Review DoS threat activity (ACC > Block Activity) and look for patterns of abuse
- C. Set the Alarm Rate threshold for event-log messages to high severity or critical severity
- D. If the levels of zone and DoS protection consume too many firewall resources, disable zone protection

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 287

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 288

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer must configure the Decryption Broker feature. Which Decryption Broker security chain supports bi-directional traffic flow?

- A. Layer 2 security chain
- B. Layer 3 security chain
- C. Transparent Bridge security chain
- D. Transparent Proxy security chain

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 289

Topic #: 1

[\[All PCNSE Questions\]](#)

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

- A. Use the import option to pull logs.
- B. Use the scp logdb export command.
- C. Export the log database.
- D. Use the ACC to consolidate the logs.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 290

Topic #: 1

[\[All PCNSE Questions\]](#)

A prospect is eager to conduct a Security Lifecycle Review (SLR) with the aid of the Palo Alto Networks NGFW. Which interface type is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive?

- A. Layer 2
- B. Virtual Wire
- C. Tap
- D. Layer 3

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 291

Topic #: 1

[\[All PCNSE Questions\]](#)

A network-security engineer attempted to configure a bootstrap package on Microsoft Azure, but the virtual machine provisioning process failed. In reviewing the bootstrap package, the engineer only had the following directories: /config, /license and /software. Why did the bootstrap process fail for the VM-Series firewall in Azure?

- A. All public cloud deployments require the /plugins folder to support proper firewall native integrations
- B. The VM-Series firewall was not pre-registered in Panorama and prevented the bootstrap process from successfully completing
- C. The /config or /software folders were missing mandatory files to successfully bootstrap
- D. The /content folder is missing from the bootstrap package

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 292

Topic #: 1

[\[All PCNSE Questions\]](#)

Which GlobalProtect component must be configured to enable Clientless VPN?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 293

Topic #: 1

[\[All PCNSE Questions\]](#)

Which statement regarding HA timer settings is true?

- A. Use the Moderate profile for typical failover timer settings
- B. Use the Critical profile for faster failover timer settings
- C. Use the Aggressive profile for slower failover timer settings
- D. Use the Recommended profile for typical failover timer settings

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 294

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 295

Topic #: 1

[\[All PCNSE Questions\]](#)

Which statement is correct given the following message from the PanGPA.log on the GlobalProtect app?

Failed to connect to server at port:4767

- A. The GlobalProtect app failed to connect to the GlobalProtect Gateway on port 4767
- B. The GlobalProtect app failed to connect to the GlobalProtect Portal on port 4767
- C. The PanGPS process failed to connect to the PanGPA process on port 4767
- D. The PanGPA process failed to connect to the PanGPS process on port 4767

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 296

Topic #: 1

[\[All PCNSE Questions\]](#)

A customer is replacing their legacy remote access VPN solution. The current solution is in place to secure only Internet egress for the connected clients. Prisma Access has been selected to replace the current remote access VPN solution. During onboarding the following options and licenses were selected and enabled:

- Prisma Access for Remote Networks: 300Mbps
- Prisma Access for Mobile Users: 1500 Users
- Cortex Data Lake: 2TB
- Trusted Zones: trust
- Untrusted Zones: untrust
- Parent Device Group: shared

How can you configure Prisma Access to provide the same level of access as the current VPN solution?

- A. Configure mobile users with trust-to-untrust Security policy rules to allow the desired traffic outbound to the Internet
- B. Configure remote networks with a service connection and trust-to-untrust Security policy rules to allow the desired traffic outbound to the Internet
- C. Configure remote networks with trust-to-trust Security policy rules to allow the desired traffic outbound to the Internet
- D. Configure mobile users with a service connection and trust-to-trust Security policy rules to allow the desired traffic outbound to the Internet

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 297

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator analyzes the following portion of a VPN system log and notices the following issue:

`Received local id 10.10.1.4/24 type IPv4 address protocol 0 port 0, received remote id 10.1.10.4/24 type IPv4 address protocol 0 port 0.`

What is the cause of the issue?

- A. bad local and peer identification IP addresses in the IKE gateway
- B. IPSec crypto profile mismatch
- C. mismatched Proxy-IDs
- D. IPSec protocol mismatch

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 298

Topic #: 1

[\[All PCNSE Questions\]](#)

A network security engineer must implement Quality of Service policies to ensure specific levels of delivery guarantees for various applications in the environment. They want to ensure that they know as much as they can about QoS before deploying. Which statement about the QoS feature is correct?

- A. QoS can be used in conjunction with SSL decryption
- B. QoS is only supported on hardware firewalls
- C. QoS is only supported on firewalls that have a single virtual system configured
- D. QoS can be used on firewalls with multiple virtual systems configured

[Show Suggested Answer](#)



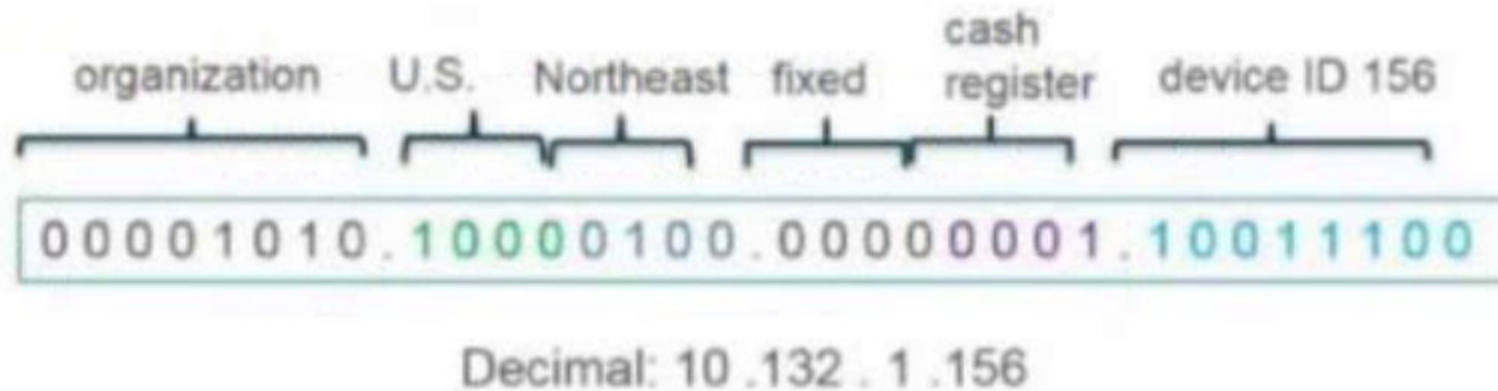
Actual exam question from Palo Alto Networks's PCNSE

Question #: 299

Topic #: 1

[\[All PCNSE Questions\]](#)

What type of address object would be useful for internal devices where the addressing structure assigns meaning to certain bits in the address, as illustrated in the diagram?



- A. IP Netmask
- B. IP Range
- C. IP Address
- D. IP Wildcard Mask

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 300

Topic #: 1

[\[All PCNSE Questions\]](#)

Given the following snippet of a WildFire submission log, did the end-user get access to the requested information and why or why not?

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

- A. No, because WildFire classified the severity as `high`
- B. Yes, 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`

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 301

Topic #: 1

[\[All PCNSE Questions\]](#)

Which statement is true regarding a Best Practice Assessment?

- A. It runs only on firewalls
- B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
- C. It shows how your current configuration compares to Palo Alto Networks recommendations
- D. When guided by an authorized sales engineer, it helps determine the areas of greatest risk where you should focus prevention activities

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 302

Topic #: 1

[\[All PCNSE Questions\]](#)

What are three important considerations during SD-WAN configuration planning? (Choose three.)

- A. link requirements
- B. IP Addresses
- C. connection throughput
- D. dynamic routing
- E. branch and hub locations

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 303

Topic #: 1

[\[All PCNSE Questions\]](#)

A standalone firewall with local objects and policies needs to be migrated into Panorama. What procedure should you use so Panorama is fully managing the firewall?

- A. Use the "import device configuration to Panorama" operation, then "export or push device config bundle" to push the configuration
- B. Use the "import Panorama configuration snapshot" operation, then perform a device-group commit push with "include device and network templates"
- C. Use the "import Panorama configuration snapshot" operation, then "export or push device config bundle" to push the configuration
- D. Use the "import device configuration to Panorama" operation, then perform a device-group commit push with "include device and network templates"

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 304

Topic #: 1

[\[All PCNSE Questions\]](#)

When you navigate to Network > GlobalProtect > Portals > Agent > (config) > App and look in the Connect Method section, which three options are available? (Choose three.)

- A. user-logon (always on)
- B. certificate-logon
- C. pre-logon then on-demand
- D. on-demand (manual user initiated connection)
- E. post-logon (always on)

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 305

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 306

Topic #: 1

[\[All PCNSE Questions\]](#)

Where is information about packet buffer protection logged?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 307

Topic #: 1

[\[All PCNSE Questions\]](#)

SSL Forward Proxy decryption is configured, but the firewall uses Untrusted-CA to sign the website <https://www.important-website.com> certificate. End-users are receiving the "security certificate is not trusted" warning. Without SSL decryption, the web browser shows that the website certificate is trusted and signed by a well-known certificate chain: Well-Known-Intermediate and Well-Known-Root-CA.

The network security administrator who represents the customer requires the following two behaviors when SSL Forward Proxy is enabled:

1. End-users must not get the warning for the <https://www.very-important-website.com/> website
2. End-users should get the warning for any other untrusted website

Which approach meets the two customer requirements?

- A. Clear the Forward Untrust Certificate check box on the Untrusted-CA certificate and commit the configuration
- B. Install the Well-Known-Intermediate-CA and Well-Known-Root-CA certificates on all end-user systems in the user and local computer stores
- C. Navigate to Device > Certificate Management > Certificates > Device Certificates, import Well-Known-Intermediate-CA and Well-Known-Root-CA, select the Trusted Root CA check box, and commit the configuration
- D. Navigate to Device > Certificate Management > Certificates > Default Trusted Certificate Authorities, import Well-Known-Intermediate-CA and Well-Known-Root-CA, select the Trusted Root CA check box, and commit the configuration

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 308

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator needs to evaluate a recent policy change that was committed and pushed to a firewall device group. How should the administrator identify the configuration changes?

- A. review the configuration logs on the Monitor tab
- B. use Test Policy Match to review the policies in Panorama
- C. context-switch to the affected firewall and use the configuration audit tool
- D. click Preview Changes under Push Scope

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 309

Topic #: 1

[\[All PCNSE Questions\]](#)

The administrator for a small company has recently enabled decryption on their Palo Alto Networks firewall using a self-signed root certificate. They have also created a Forward Trust and Forward Untrust certificate and set them as such.

The admin has not yet installed the root certificate onto client systems.

What effect would this have on decryption functionality?

- A. Decryption will not function because self-signed root certificates are not supported
- B. Decryption will function, but users will see certificate warnings for each SSL site they visit
- C. Decryption will not function until the certificate is installed on client systems
- D. Decryption will function, and there will be no effect to end users

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 310

Topic #: 1

[\[All PCNSE Questions\]](#)

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

What should the administrator implement?

- A. hot potato routing
- B. summarized BGP routes before advertising
- C. default routing
- D. target service connection for traffic steering

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 311

Topic #: 1

[\[All PCNSE Questions\]](#)

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

How should the engineer proceed?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 312

Topic #: 1

[\[All PCNSE Questions\]](#)

A network security engineer wants to prevent resource-consumption issues on the firewall.

Which strategy is consistent with decryption best practices to ensure consistent performance?

- A. Use Decryption profiles to downgrade processor-intensive ciphers to ciphers that are less processor-intensive
- B. Use Decryption profiles to drop traffic that uses processor-intensive ciphers
- C. Use PFS in a Decryption profile for higher-priority and higher-risk traffic, and use less processor-intensive decryption methods for lower-risk traffic
- D. Use RSA in a Decryption profile for higher-priority and higher-risk traffic, and use less processor-intensive decryption methods for lower-risk traffic

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 313

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Detailed Log View

General	Source	Destination
Session ID: 224641	Source User: test	Destination User:
Action: allow	Source: 172.254.254.253	Destination: 172.217.5.106
Action Source: from-policy	Source DAG:	Destination DAG:
Host ID:	Country: United States	Country: United States
Application: XXXXXXXXXX	Port: 64345	Port: 443
Rule: Trust-to-Untrust	Zone: L3-Trust	Zone: L3-Untrust
Rule UUID: 0b39bd48-bafd-4b4c-9b08-6e96c8eca701	Interface: tunnel.2	Interface: ethernet1/3
Session End Reason: aged-out	NAT IP: 10.46.42.149	NAT IP: 172.217.5.106
Category: any	NAT Port: 41854	NAT Port: 443
Device SN:	X-Forwarded-For IP: 0.0.0.0	
IP Protocol: udp		
Log Action:		
Generated Time: 2020/12/22 13:06:02		
Start Time: 2020/12/22 13:05:32		
Receive Time: 2020/12/22 13:06:02		
Elapsed Time(sec): 0		
Tunnel Type: N/A		

Details
Type: end
Bytes: 10147
Bytes Received: 6113
Bytes Sent: 4034
Repeat Count: 1
Packets: 22
Packets Received: 11
Packets Sent: 11

Flags
Captive Portal <input type="checkbox"/>
Proxy Transaction <input type="checkbox"/>
Decrypted <input type="checkbox"/>
Packet Capture <input checked="" type="checkbox"/>
Client to Server <input type="checkbox"/>
Server to Client <input type="checkbox"/>
Symmetric Return <input type="checkbox"/>
Mirrored <input type="checkbox"/>
Tunnel Inspected <input type="checkbox"/>
MPTCP Options <input type="checkbox"/>
Recon excluded <input type="checkbox"/>
Decrypt Forwarded <input type="checkbox"/>

- A. unknown-udp
- B. not-applicable
- C. insufficient-data
- D. incomplete

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 314

Topic #: 1

[\[All PCNSE Questions\]](#)

A remote administrator needs firewall access on an untrusted interface. Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two.)

- A. client certificate
- B. certificate profile
- C. certificate authority (CA) certificate
- D. server certificate

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 315

Topic #: 1

[\[All PCNSE Questions\]](#)

When configuring forward error correction (FEC) for PAN-OS SD-WAN, an administrator would turn on the feature inside which type of SD-WAN profile?

- A. Traffic Distribution profile
- B. Path Quality profile
- C. Certificate profile
- D. SD-WAN interface profile

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 316

Topic #: 1

[\[All PCNSE Questions\]](#)

DRAG DROP -

An engineer is troubleshooting traffic routing through the virtual router. The firewall uses multiple routing protocols, and the engineer is trying to determine routing priority. Match the default Administrative Distances for each routing protocol.

Select and Place:

Static

OSPF External

EBGP

RIP

Answer Area

20

120

10

110

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 317

Topic #: 1

[\[All PCNSE Questions\]](#)

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

- A. template variables
- B. the 'Shared' device group
- C. template stacks
- D. a device group

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 318

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer wants to implement the Palo Alto Networks firewall in VWire mode on the internet gateway and wants to be sure of the functions that are supported on the vwire interface.

What are three supported functions on the VWire interface? (Choose three.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 319

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall has been assigned to a new template stack that contains both "Global" and "Local" templates in Panorama, and a successful commit and push has been performed. While validating the configuration on the local firewall, the engineer discovers that some settings are not being applied as intended.

The setting values from the "Global" template are applied to the firewall instead of the "Local" template that has different values for the same settings.

What should be done to ensure that the settings in the "Local" template are applied while maintaining settings from both templates?

- A. Move the "Local" template above the "Global" template in the template stack.
- B. Perform a commit and push with the "Force Template Values" option selected.
- C. Override the values on the local firewall and apply the correct settings for each value.
- D. Move the "Global" template above the "Local" template in the template stack.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 320

Topic #: 1

[\[All PCNSE Questions\]](#)

A network administrator wants to deploy SSL Inbound Inspection. What two attributes should the required certificate have? (Choose two.)

- A. a client certificate
- B. a private key
- C. a server certificate
- D. a subject alternative name

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 321

Topic #: 1

[\[All PCNSE Questions\]](#)

When using certificate authentication for firewall administration, which method is used for authorization?

- A. LDAP
- B. Radius
- C. Local
- D. Kerberos

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 322

Topic #: 1

[\[All PCNSE Questions\]](#)

Which three use cases are valid reasons for requiring an Active/Active high availability deployment? (Choose three.)

- A. The environment requires real full-time redundancy from both firewalls at all times.
- B. The environment requires that traffic be load-balanced across both firewalls to handle peak traffic spikes.
- C. The environment requires Layer 2 interfaces in the deployment.
- D. The environment requires that all configuration must be fully synchronized between both members of the HA pair.
- E. The environment requires that both firewalls maintain their own routing tables for faster dynamic routing protocol convergence.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 323

Topic #: 1

[\[All PCNSE Questions\]](#)

An organization wishes to roll out decryption but gets some resistance from engineering leadership regarding the guest network.

What is a common obstacle for decrypting traffic from guest devices?

- A. Guest devices may not trust the CA certificate used for the forward trust certificate
- B. Guests may use operating systems that can't be decrypted
- C. The organization has no legal authority to decrypt their traffic
- D. Guest devices may not trust the CA certificate used for the forward untrust certificate

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 324

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator needs to build Security rules in a Device Group that allow traffic to specific users and groups defined in Active Directory. What must be configured in order to select users and groups for those rules from Panorama?

- A. The Security rules must be targeted to a firewall in the device group and have Group Mapping configured.
- B. User-ID Redistribution must be configured on Panorama to ensure that all firewalls have the same mappings.
- C. A master device with Group Mapping configured must be set in the device group where the Security rules are configured.
- D. A User-ID Certificate profile must be configured on Panorama.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 325

Topic #: 1

[\[All PCNSE Questions\]](#)

Which feature of PAN-OS SD-WAN allows you to configure a bandwidth-intensive application to go directly to the internet through the branch's ISP link instead of going back to the data-center hub through the VPN tunnel, thus saving WAN bandwidth costs?

- A. SD-WAN Full Mesh with branches only
- B. SD-WAN direct internet access (DIA) links
- C. SD-WAN Interface profile
- D. VPN Cluster

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 326

Topic #: 1

[\[All PCNSE Questions\]](#)

What can you use with GlobalProtect to assign user-specific client certificates to each GlobalProtect user?

- A. CSP Responder
- B. Certificate profile
- C. SCEP
- D. SSL/TLS Service profile

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 327

Topic #: 1

[\[All PCNSE Questions\]](#)

A user at an external system with the IP address 65.124.57.5 queries the DNS server at 4.2.2.2 for the IP address of the web server, www.xyz.com. The DNS server returns an address of 172.16.15.1.

In order to reach the web server, which Security rule and NAT rule must be configured on the firewall?



- A. NAT Rule: Untrust-L3 (any) - Untrust-L3 (172.16.15.1) Destination Translation: 192.168.15.47 Security Rule: Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application: Web-browsing
- B. NAT Rule: Untrust-L3 (any) - Trust-L3 (172.16.15.1) Destination Translation: 192.168.15.47 Security Rule: Untrust-L3 (any) - Trust-L3 (192.168.15.47) - Application: Web-browsing
- C. NAT Rule: Untrust-L3 (any) - Trust-L3 (172.16.15.1) Destination Translation: 192.168.15.47 Security Rule: Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application: Web-browsing
- D. NAT Rule: Untrust-L3 (any) - Untrust-L3 (any) Destination Translation: 192.168.15.1 Security Rule: Untrust-L3 (any) - Trust-L3 (172.16.15.1) - Application: Web-browsing

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 328

Topic #: 1

[\[All PCNSE Questions\]](#)

A network administrator is trying to prevent domain username and password submissions to phishing sites on some allowed URL categories.

Which set of steps does the administrator need to take in the URL Filtering profile to prevent credential phishing on the firewall?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 329

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 330

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall has Security policies from three sources:

1. locally created policies
2. shared device group policies as pre-rules
3. the firewall's device group as post-rules

How will the rule order populate once pushed to the firewall?

- A. shared device group policies, local policies, firewall device group policies
- B. firewall device group policies, local policies, shared device group policies
- C. local policies, firewall device group policies, shared device group policies
- D. shared device group policies, firewall device group policies, local policies

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 331

Topic #: 1

[\[All PCNSE Questions\]](#)

Which function is handled by the management plane (control plane) of a Palo Alto Networks firewall?

- A. logging
- B. signature matching for content inspection
- C. Quality of Service
- D. IPSec tunnel standup

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 332

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator wants to enable WildFire inline machine learning.

Which three file types does WildFire inline ML analyze? (Choose three.)

- A. APK
- B. VBscripts
- C. Powershell scripts
- D. ELF
- E. MS Office

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 333

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator needs to assign a specific DNS server to one firewall within a device group.

Where would the administrator go to edit a template variable at the device level?

- A. PDF Export under Panorama > templates
- B. Variable CSV export under Panorama > templates
- C. Managed Devices > Device Association
- D. Manage variables under Panorama > templates

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 334

Topic #: 1

[\[All PCNSE Questions\]](#)

What is a feature of the PA-440 hardware platform?

- A. It supports Zero Touch Provisioning to assist in automated deployments.
- B. It supports 10GbE SFP+ modules.
- C. It has twelve 1GbE Copper ports.
- D. It has dedicated interfaces for high availability.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 335

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 336

Topic #: 1

[\[All PCNSE Questions\]](#)

A Firewall Engineer is migrating a legacy firewall to a Palo Alto Networks firewall in order to use features like App-ID and SSL decryption.

Which order of steps is best to complete this migration?

- A. First migrate SSH rules to App-ID; then implement SSL decryption.
- B. Configure SSL decryption without migrating port-based security rules to App-ID rules.
- C. First implement SSL decryption; then migrate port-based rules to App-ID rules.
- D. First migrate port-based rules to App-ID rules; then implement SSL decryption.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 337

Topic #: 1

[\[All PCNSE Questions\]](#)

A security engineer received multiple reports of an IPSec VPN tunnel going down the night before. The engineer couldn't find any events related to VPN under system logs.

What is the likely cause?

- A. Tunnel Inspection settings are misconfigured.
- B. The log quota for GTP and Tunnel needs to be adjusted.
- C. The Tunnel Monitor is not configured.
- D. Dead Peer Detection is not enabled.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 338

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator notices that many Host Sweep scan attacks are being allowed through the firewall sourced from the outside zone. What should the firewall administrator do to mitigate this type of attack?

- A. Create a Zone Protection profile, enable reconnaissance protection, set action to Block, and apply it to the outside zone.
- B. Create a DOS Protection profile with SYN Flood protection enabled and apply it to all rules allowing traffic from the outside zone.
- C. Enable packet buffer protection in the outside zone.
- D. Create a Security rule to deny all ICMP traffic from the outside zone.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 339

Topic #: 1

[\[All PCNSE Questions\]](#)

The Aggregate Ethernet interface is showing down on a passive PA-7050 firewall of an active/passive HA pair. The HA Passive Link State is set to "Auto" under Device > High Availability > General > Active/Passive Settings. The AE interface is configured with LACP enabled and is up only on the active firewall.

Why is the AE interface showing down on the passive firewall?

- A. It does not participate in LACP negotiation unless Fast Failover is selected under the Enable LACP selection on the LACP tab of the AE Interface.
- B. It does not perform pre-negotiation LACP unless "Enable in HA Passive State" is selected under the High Availability Options on the LACP tab of the AE Interface.
- C. It performs pre-negotiation of LACP when the mode Passive is selected under the Enable LACP selection on the LACP tab of the AE Interface.
- D. It participates in LACP negotiation when Fast is selected for Transmission Rate under the Enable LACP selection on the LACP tab of the AE Interface.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 340

Topic #: 1

[\[All PCNSE Questions\]](#)

A company requires that a specific set of ciphers be used when remotely managing their Palo Alto Networks appliances.

Which profile should be configured in order to achieve this?

- A. Certificate profile
- B. SSL/TLS Service profile
- C. SSH Service profile
- D. Decryption profile

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 341

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer needs to permit XML API access to a firewall for automation on a network segment that is routed through a Layer 3 subinterface on a Palo Alto Networks firewall. However, this network segment cannot access the dedicated management interface due to the Security policy. Without changing the existing access to the management interface, how can the engineer fulfill this request?

- A. Specify the subinterface as a management interface in Setup > Device > Interfaces.
- B. Add the network segment's IP range to the Permitted IP Addresses list.
- C. Enable HTTPS in an Interface Management profile on the subinterface.
- D. Configure a service route for HTTP to use the subinterface.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 342

Topic #: 1

[\[All PCNSE Questions\]](#)

A client wants to detect the use of weak and manufacturer-default passwords for IoT devices.

Which option will help the customer?

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

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 343

Topic #: 1

[\[All PCNSE Questions\]](#)

When using SSH keys for CLI authentication for firewall administration, which method is used for authorization?

- A. Radius
- B. Kerberos
- C. LDAP
- D. Local

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 344

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer needs to see how many existing SSL decryption sessions are traversing a firewall.

What command should be used?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 345

Topic #: 1

[\[All PCNSE Questions\]](#)

A network engineer has discovered that asymmetric routing is causing a Palo Alto Networks firewall to drop traffic. The network architecture cannot be changed to correct this.

Which two actions can be taken on the firewall to allow the dropped traffic permanently? (Choose two.)

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 346

Topic #: 1

[\[All PCNSE Questions\]](#)

A company is using wireless controllers to authenticate users.

Which source should be used for User-ID mappings?

- A. server monitoring
- B. XFF headers
- C. Syslog
- D. client probing

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 347

Topic #: 1

[\[All PCNSE Questions\]](#)

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

Given the information, what is the best choice for deploying User-ID to ensure maximum coverage?

- A. agentless User-ID with redistribution
- B. Syslog listener
- C. captive portal
- D. standalone User-ID agent

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 348

Topic #: 1

[\[All PCNSE Questions\]](#)

You have upgraded your Panorama and Log Collectors to 10.2.x.

Before upgrading your firewalls using Panorama, what do you need do?

- A. Commit and Push the configurations to the firewalls.
- B. Refresh your licenses with Palo Alto Network Support \gg Panorama/Licenses/Retrieve License Keys from License Server.
- C. Refresh the Master Key in Panorama/Master Key and Diagnostic.
- D. Re-associate the firewalls in Panorama/Managed Devices/Summary.

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 349

Topic #: 1

[\[All PCNSE Questions\]](#)

Which steps should an engineer take to forward system logs to email?

- A. Create a new email profile under Device > server profiles; then navigate to Device > Log Settings > System and add the email profile under email.
- B. Enable log forwarding under the email profile in the Objects tab.
- C. Create a new email profile under Device > server profiles; then navigate to Objects > Log Forwarding profile > set log type to system and the add email profile.
- D. Enable log forwarding under the email profile in the Device tab.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 350

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator discovers that a file blocked by the WildFire inline ML feature on the firewall is a false-positive action. How can the administrator create an exception for this particular file?

- A. Add the related Threat ID in the Signature exceptions tab of the Antivirus profile.
- B. Disable the WildFire profile on the related Security policy.
- C. Set the WildFire inline ML action to allow for that protocol on the Antivirus profile.
- D. Add partial hash and filename in the file section of the WildFire inline ML tab of the Antivirus profile.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 351

Topic #: 1

[\[All PCNSE Questions\]](#)

What can be used to create dynamic address groups?

- A. tags
- B. FQDN addresses
- C. dynamic address
- D. region objects

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 352

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator wants to avoid overflowing the company syslog server with traffic logs.

What should the administrator do to prevent the forwarding of DNS traffic logs to syslog?

- A. Disable logging on security rules allowing DNS.
- B. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application not equal to DNS.
- C. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application equal to DNS.
- D. Create a security rule to deny DNS traffic with the syslog server in the destination.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 353

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has configured a pair of firewalls using high availability in Active/Passive mode.

Path Monitoring has been enabled with a Failure Condition of "any."

A path group is configured with Failure Condition of "all" and contains a destination IP of 8.8.8.8 and 4.2.2.2 with a Ping Interval of 500ms and a Ping count of 3.

Which scenario will cause the Active firewall to fail over?

- A. IP address 8.8.8.8 is unreachable for 1 second.
- B. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 2 seconds.
- C. IP address 4.2.2.2 is unreachable for 2 seconds.
- D. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 1 second.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 354

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator has been tasked with ensuring that all Panorama configuration is committed and pushed to the devices at the end of the day at a certain time.

How can they achieve this?

- A. Use the Scheduled Config Export to schedule Commit to Panorama and also Push to Devices.
- B. Use the Scheduled Config Push to schedule Commit to Panorama and also Push to Devices.
- C. Use the Scheduled Config Push to schedule Push to Devices and separately schedule an API call to commit all Panorama changes.
- D. Use the Scheduled Config Export to schedule Push to Devices and separately schedule an API call to commit all Panorama changes.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 355

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 356

Topic #: 1

[\[All PCNSE Questions\]](#)

While analyzing the Traffic log, you see that some entries show "unknown-tcp" in the Application column.

What best explains these occurrences?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 357

Topic #: 1

[\[All PCNSE Questions\]](#)

You have upgraded Panorama to 10.2 and need to upgrade six Log Collectors.

When upgrading Log Collectors to 10.2, you must do what?

- A. Upgrade the Log Collectors one at a time.
- B. Add Panorama Administrators to each Managed Collector.
- C. Upgrade all the Log Collectors at the same time.
- D. Add a Global Authentication Profile to each Managed Collector.

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 358

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator has been tasked with ensuring that all Panorama-managed firewalls forward traffic logs to Panorama. In which section is this configured?

- A. Templates > Device > Log Settings
- B. Device Groups > Objects > Log Forwarding
- C. Monitor > Logs > Traffic
- D. Panorama > Managed Devices

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 359

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer is pushing configuration from Panorama to a managed firewall.

What happens when the pushed Panorama configuration has Address Object names that duplicate the Address Objects already configured on the firewall?

- A. The firewall ignores only the pushed objects that have the same name as the locally configured objects, and it will commit the rest of the pushed configuration.
- B. The firewall rejects the pushed configuration, and the commit fails.
- C. The firewall fully commits all of the pushed configuration and overwrites its locally configured objects.
- D. The firewall renames the duplicate local objects with "-1" at the end signifying they are clones; it will update the references to the objects accordingly and fully commit the pushed configuration.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 360

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 361

Topic #: 1

[\[All PCNSE Questions\]](#)

A network administrator troubleshoots a VPN issue and suspects an IKE Crypto mismatch between peers. Where can the administrator find the corresponding logs after running a test command to initiate the VPN?

- A. Traffic logs
- B. System logs
- C. Tunnel Inspection logs
- D. Configuration logs

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 362

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator is required to create an application-based Security policy rule to allow Evernote. The Evernote application implicitly uses SSL and web browsing. What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?

- A. Create an Application Override using TCP ports 443 and 80.
- B. Add the HTTP, SSL, and Evernote applications to the same Security policy.
- C. Add the Evernote application to the Security policy rule, then add a second Security policy rule containing both HTTP and SSL.
- D. Add only the Evernote application to the Security policy rule.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 363

Topic #: 1

[\[All PCNSE Questions\]](#)

Which Panorama mode should be used so that all logs are sent to, and only stored in, Cortex Data Lake?

- A. Legacy
- B. Management Only
- C. Log Collector
- D. Panorama

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 364

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 365

Topic #: 1

[\[All PCNSE Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 366

Topic #: 1

[\[All PCNSE Questions\]](#)

Which CLI command is used to determine how much disk space is allocated to logs?

- A. debug log-receiver show
- B. show system info
- C. show system logdb-quota
- D. show logging-status

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 367

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator has configured a pair of firewalls using high availability in Active/Passive mode.

Link and Path Monitoring is enabled with the Failure Condition set to `any`.

There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure Condition set to `all`.

Which HA state will the Active firewall go into if ethernet1/1 link goes down due to a failure?

- A. Active
- B. Passive
- C. Active-Secondary
- D. Non-functional

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 368

Topic #: 1

[\[All PCNSE Questions\]](#)

Your company occupies one floor in a single building. You have two Active Directory domain controllers on a single network. The firewall's management-plane resources are lightly utilized.

Given the size of this environment, which User-ID collection method is sufficient?

- A. Windows-based agent deployed on each domain controller
- B. PAN-OS integrated agent deployed on the firewall
- C. a syslog listener
- D. Citrix terminal server agent deployed on the network

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 369

Topic #: 1

[\[All PCNSE Questions\]](#)

Which statement best describes the Automated Commit Recovery feature?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 370

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer has been tasked with reviewing traffic logs to find applications the firewall is unable to identify with App-ID.

Why would the application field display as incomplete?

- A. There is insufficient application data after the TCP connection was established.
- B. The TCP connection was terminated without identifying any application data.
- C. The TCP connection did not fully establish.
- D. The client sent a TCP segment with the PUSH flag set.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 371

Topic #: 1

[\[All PCNSE Questions\]](#)

Which Security profile generates a packet threat type found in threat logs?

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 372

Topic #: 1

[\[All PCNSE Questions\]](#)

What can an engineer use with GlobalProtect to assign user-specific client certificates to each GlobalProtect user?

- A. SCEP
- B. SSL/TLS Service profile
- C. OCSP Responder
- D. Certificate profile

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 373

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer was tasked to simplify configuration of multiple firewalls with a specific set of configurations shared across all devices.

Which two advantages would be gained by using multiple templates in a stack? (Choose two.)

- A. standardizes log-forwarding profiles for security policies across all stacks
- B. defines a common standard template configuration for firewalls
- C. inherits address-objects from the templates
- D. standardizes server profiles and authentication configuration across all stacks

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 374

Topic #: 1

[\[All PCNSE Questions\]](#)

A network engineer is troubleshooting a VPN and wants to verify whether the decapsulation/encapsulation counters are increasing.

Which CLI command should the engineer run?

- A. Show running tunnel flow lookup
- B. Show vpn flow name <tunnel name>
- C. Show vpn ipsec-sa tunnel <tunnel name>
- D. Show vpn tunnel name | match encap

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 375

Topic #: 1

[\[All PCNSE Questions\]](#)

How would an administrator configure a Bidirectional Forwarding Detection profile for BGP after enabling the Advance Routing Engine run on PAN-OS 10.2?

- A. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Virtual Router > BGP > General > Global BFD Profile
- B. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Routing > Logical Routers > BGP > General > Global BFD Profile
- C. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Virtual Router > BGP > BFD
- D. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Routing > Logical Routers > BGP > BFD

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 376

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer is troubleshooting a traffic-routing issue.

What is the correct packet-flow sequence?

- A. PBF > Static route > Security policy enforcement
- B. BGP < PBF > NAT
- C. PBF > Zone Protection Profiles > Packet Buffer Protection
- D. NAT > Security policy enforcement > OSPF

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 377

Topic #: 1

[\[All PCNSE Questions\]](#)

While investigating a SYN flood attack, the firewall administrator discovers that legitimate traffic is also being dropped by the DoS profile. If the DoS profile action is set to Random Early Drop, what should the administrator do to limit the drop to only the attacking sessions?

- A. Enable resources protection under the DoS Protection profile.
- B. Change the SYN flood action from Random Early Drop to SYN cookies.
- C. Increase the activate rate for the SYN flood protection.
- D. Change the DoS Protection profile type from aggregate to classified.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 378

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator wants to have visibility on one segment of the company network. The traffic on the segment is routed on the Backbone switch. The administrator is planning to apply Security rules on segment X after getting the visibility.

There is already a PAN-OS firewall used in L3 mode as an internet gateway, and there are enough system resources to get extra traffic on the firewall. The administrator needs to complete this operation with minimum service interruptions and without making any IP changes.

What is the best option for the administrator to take?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 379

Topic #: 1

[\[All PCNSE Questions\]](#)

A company is deploying User-ID in their network. The firewall team needs to have the ability to see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules.

How can this be achieved?

- A. by configuring User-ID group mapping in Panorama > User Identification
- B. by configuring Master Device in Panorama > Device Groups
- C. by configuring User-ID source device in Panorama > Managed Devices
- D. by configuring Data Redistribution Client in Panorama > Data Redistribution

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 380

Topic #: 1

[\[All PCNSE Questions\]](#)

After some firewall configuration changes, an administrator discovers that application identification has started failing. The administrator investigates further and notices that a high number of sessions were going to a discard state with the application showing as unknown-tcp.

Which possible firewall change could have caused this issue?

- A. enabling Forward segments that exceed the TCP App-ID inspection queue in Device > Setup > Content-ID > Content-ID Settings
- B. enabling Forward segments that exceed the TCP content inspection queue in Device > Setup > Content-ID > Content-ID Settings
- C. Jumbo frames were enabled on the firewall, which reduced the App-ID queue size and the number of available packet buffers.
- D. Jumbo frames were disabled on the firewall, which reduced the queue sizes dedicated for out-of-order and application identification.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 381

Topic #: 1

[\[All PCNSE Questions\]](#)

Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

- A. upload-only
- B. install and reboot
- C. upload and install
- D. upload and install and reboot
- E. verify and install

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 382

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator is investigating high packet buffer utilization in the company firewall. After looking at the threat logs and seeing many flood attacks coming from a single source that are dropped by the firewall, the administrator decides to enable packet buffer protection to protect against similar attacks.

The administrator enables packet buffer protection globally in the firewall but still sees a high packet buffer utilization rate.

What else should the administrator do to stop packet buffers from being overflowed?

- A. Apply DOS profile to security rules allow traffic from outside.
- B. Enable packet buffer protection for the affected zones.
- C. Add the default Vulnerability Protection profile to all security rules that allow traffic from outside.
- D. Add a Zone Protection profile to the affected zones

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 383

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator is investigating high packet buffer utilization in the company firewall. After looking at the threat logs and seeing many flood attacks coming from a single source that are dropped by the firewall, the administrator decides to enable packet buffer protection to protect against similar attacks.

The administrator enables packet buffer protection globally in the firewall but still sees a high packet buffer utilization rate.

What else should the administrator do to stop packet buffers from being overflowed?

- A. Apply DOS profile to security rules allow traffic from outside.
- B. Enable packet buffer protection for the affected zones.
- C. Add the default Vulnerability Protection profile to all security rules that allow traffic from outside.
- D. Add a Zone Protection profile to the affected zones.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 384

Topic #: 1

[\[All PCNSE Questions\]](#)

What is a correct statement regarding administrative authentication using external services with a local authorization method?

- A. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall.
- B. Prior to PAN-OS 10.2, an administrator used the firewall to manage role assignments, but access domains have not been supported by this method.
- C. Starting with PAN-OS 10.2, an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.
- D. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 385

Topic #: 1

[\[All PCNSE Questions\]](#)

A network administrator notices there is a false-positive situation after enabling Security profiles. When the administrator checks the threat prevention logs, the related signature displays: threat type: spyware category: dns-c2 threat ID: 1000011111

Which set of steps should the administrator take to configure an exception for this signature?

- A. Navigate to Objects > Security Profiles > Anti-Spyware Select related profile Select the signature exceptions tab and then click show all signatures Search related threat ID and click enable Change the default action Commit
- B. Navigate to Objects > Security Profiles > Anti-Spyware Select related profile Select the Exceptions tab and then click show all signatures Search related threat ID and click enable Commit
- C. Navigate to Objects > Security Profiles > Vulnerability Protection Select related profile Select the Exceptions tab and then click show all signatures Search related threat ID and click enable Commit
- D. Navigate to Objects > Security Profiles > Anti-Spyware Select related profile Select DNS exceptions tabs Search related threat ID and click enable Commit

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 386

Topic #: 1

[\[All PCNSE Questions\]](#)

The screenshot displays the Palo Alto Networks PA-VM ACC interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. The 'Threat Activity' section is active, showing a bar chart with three categories: 'insecure-credentials' (count 50), 'brute-force' (count 47), and 'protocol-anomaly' (count 2). Below the chart is a table of threat names and IDs. The bottom part of the screenshot shows a severity bar chart with a value of 3.8 and a table of threat details including severity, threat type, threat category, and count.

THREAT NAME	ID
FTP: login Brute Force attempt	40001
Manufacturer default username and/or password found in FTP login	57354
Manufacturer default username and/or password found in FTP login	57355
Compromised username and/or password from previous data breach in inbound FTP login	58203
Compromised username and/or password from previous data breach in inbound FTP login	59567
Compromised username and/or password from previous data breach in inbound FTP login	59536
Compromised username and/or password from previous data breach in inbound FTP login	59540
Compromised username and/or password from previous data breach in inbound FTP login	59538
Compromised username and/or password from previous data breach in inbound FTP login	59549
Compromised username and/or password from previous data breach in inbound FTP login	59566

SEVERITY	THREAT TYPE	THREAT CATEGORY	COUNT
high	vulnerability	brute-force	47
informational	vulnerability	insecure-credentials	11
informational	vulnerability	insecure-credentials	10
low	vulnerability	insecure-credentials	10
low	vulnerability	insecure-credentials	6
low	vulnerability	insecure-credentials	5
low	vulnerability	insecure-credentials	4
low	vulnerability	insecure-credentials	3
low	vulnerability	insecure-credentials	3
low	vulnerability	insecure-credentials	3

In the screenshot above, which two pieces of information can be determined from the ACC configuration shown? (Choose two.)

- A. Insecure-credentials, brute-force, and protocol-anomaly are all a part of the vulnerability Threat Type.
- B. The Network Activity tab will display all applications, including FTP.
- C. Threats with a severity of 'high' are always listed at the top of the Threat Name list.
- D. The ACC has been filtered to only show the FTP application.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCNSE

Question #: 387

Topic #: 1

[\[All PCNSE Questions\]](#)

Detailed Log View ?

General	Source	Destination
Session ID 202702	Source User [REDACTED]	Destination User
Action allow	Source [REDACTED]	Destination 191.96.150.165
Action Source from-policy	Source DAG	Destination DAG
Host ID	Country 192.168.0.0-192.168.255.255	Country United States
Application ssl	Port 51153	Port 9002
Rule non-standard-ports	Zone LAN	Zone Internet
Rule UUID ce8e907d-1d17-457e-8600-b7e2654f78b1	Interface ethernet1/2	Interface ethernet1/8
Session End Reason threat	NAT IP [REDACTED]	NAT IP 191.96.150.165
Category proxy-avoidance-and-anonymizers	NAT Port 47076	NAT Port 9002
Device SN 007251000156341	X-Forwarded-For IP 0.0.0.0	
IP Protocol tcp		
Log Action global-logs		
Generated Time 2022/03/08 07:36:29		
Start Time 2022/03/08 07:34:55		
Receive Time 2022/03/08 07:36:38		
Elapsed Time(sec) 0		
Tunnel Type N/A		

Details	Flags
Type end	Captive Portal <input type="checkbox"/>
Bytes 801	Proxy Transaction <input type="checkbox"/>
Bytes Received 74	Decrypted <input type="checkbox"/>
Bytes Sent 727	Packet Capture <input type="checkbox"/>
Repeat Count 1	Client to Server <input type="checkbox"/>
Packets 4	Server to Client <input type="checkbox"/>
Packets Received 1	Symmetric Return <input type="checkbox"/>
Packets Sent 3	Mirrored <input type="checkbox"/>
Source UUID	Tunnel Inspected <input type="checkbox"/>
Destination UUID	MPTCP Options <input type="checkbox"/>
Dynamic User Group	Recon excluded <input type="checkbox"/>
Network Slice ID SD 0	Forwarded to Security Chain <input type="checkbox"/>
Network Slice ID SST 0	
App Category networking	
App Subcategory encrypted-tunnel	
App Technology browser-based	
App Characteristic used-by-malware,able-to-transfer-file,has-known-vulnerability,tunnel-other-application,pervasive-use	
App Container	
App Risk 4	
App SaaS no	
App Sanctioned State no	

DeviceID	
Source Device Category	Network Security Equipment
Source Device Profile	Palo Alto Networks Device
Source Device Model	MacPro
Source Device Vendor	Palo Alto Networks, Inc.
Source Device OS Family	PAN-OS
Source Device OS Version	
Source Device Host	MacPro
Source Device MAC	00:00:00:00:00:00

SDWAN

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

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

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 388

Topic #: 1

[\[All PCNSE Questions\]](#)

Your company wants greater visibility into their traffic and has asked you to start planning an SSL Decryption project. The company does not have a PKI infrastructure, and multiple certificates would be needed for this project. Which type of certificate can you use to generate other certificates?

- A. self-signed root CA
- B. external CA certificate
- C. server certificate
- D. device certificate

Show Suggested Answer

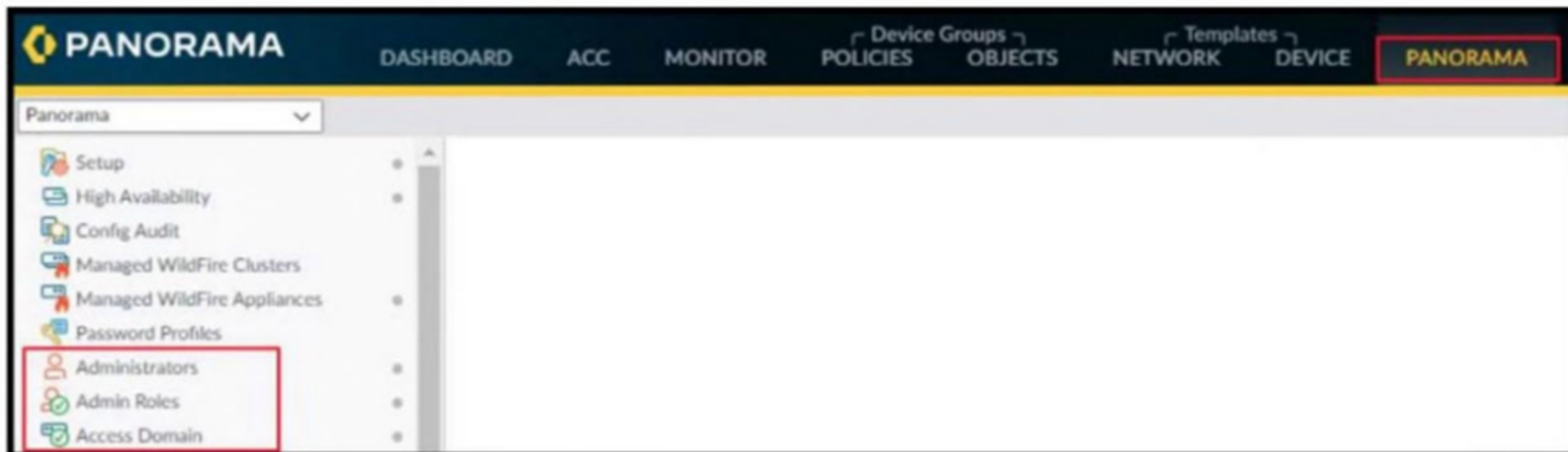


Actual exam question from Palo Alto Networks's PCNSE

Question #: 389

Topic #: 1

[\[All PCNSE Questions\]](#)



Refer to the screenshots. Without the ability to use Context Switch, where do admin accounts need to be configured in order to provide admin access to Panorama and to the managed devices?

- A. The Panorama section overrides the Device section. The accounts need to be configured only in the Panorama section.
- B. The sections are independent. The accounts need to be configured in both the Device and Panorama sections.
- C. The Device section overrides Panorama section. The accounts need to be configured only in the Device section.
- D. Configuration in the sections is merged together. The accounts need to be configured in either section.

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 390

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator needs to be able to inspect inbound HTTPS traffic on servers hosted in their DMZ to prevent the hosted service from being exploited. Which combination of features can allow PAN-OS to detect exploit traffic in a session with TLS encapsulation?

- A. a WildFire profile and a File Blocking profile
- B. a Vulnerability Protection profile and a Decryption policy
- C. a Vulnerability Protection profile and a QoS policy
- D. a Decryption policy and a Data Filtering profile

[Show Suggested Answer](#)





Actual exam question from Palo Alto Networks's PCNSE

Question #: 391

Topic #: 1

[\[All PCNSE Questions\]](#)

Engineer was tasked to simplify configuration of multiple firewalls with a specific set of configurations shared across all devices.

Which two advantages would be gained by using multiple templates in a stack? (Choose two.)

- A. inherits address-objects from the templates
- B. standardizes server profiles and authentication configuration across all stacks
- C. standardizes log-forwarding profiles for security policies across all stacks
- D. defines a common standard template configuration for firewalls

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 392

Topic #: 1

[\[All PCNSE Questions\]](#)

Which protocol is supported by GlobalProtect Clientless VPN?

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

Show Suggested Answer



Actual exam question from Palo Alto Networks's PCNSE

Question #: 393

Topic #: 1

[\[All PCNSE Questions\]](#)

During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. Additional device certificates and/or Subordinate certificates requiring an Enterprise CA chain of trust are signed by the company's Intermediate CA.

Which method should the administrator use when creating Forward Trust and Forward Untrust certificates on the firewall for use with decryption?

- A. Generate two subordinate CA certificates, one for Forward Trust and one for Forward Untrust.
- B. Generate a CA certificate for Forward Trust and a self-signed CA for Forward Untrust.
- C. Generate a single subordinate CA certificate for both Forward Trust and Forward Untrust.
- D. Generate a single self-signed CA certificate for Forward Trust and another for Forward Untrust.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 394

Topic #: 1

[\[All PCNSE Questions\]](#)

A firewall administrator needs to check which egress interface the firewall will use to route the IP 10.2.5.3.

Which command should they use?

- A. test routing fib-lookup ip 10.2.5.0/24 virtual-router default
- B. test routing route ip 10.2.5.3
- C. test routing route ip 10.2.5.3 virtual-router default
- D. test routing fib-lookup ip 10.2.5.3 virtual-router default

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 395

Topic #: 1

[\[All PCNSE Questions\]](#)

A client is concerned about web shell attacks against their servers.

Which profile will protect the individual servers?

- A. Anti-Spyware profile
- B. Zone Protection profile
- C. DoS Protection profile
- D. Antivirus profile

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 396

Topic #: 1

[\[All PCNSE Questions\]](#)

Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?

- A. service route
- B. data redistribution
- C. SNMP setup
- D. dynamic updates

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 397

Topic #: 1

[\[All PCNSE Questions\]](#)

How is an address object of type IP range correctly defined?

- A. 192 168 40 1-192 168 40 255
- B. 192.168 40 1/24
- C. 192.168 40 1, 192.168 40.255
- D. 192 168 40 1-255

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 398

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator wants to prevent users from unintentionally accessing malicious domains where data can be exfiltrated through established connections to remote systems. From the Pre-defined Categories tab within the URL Filtering profile what is the right configuration to prevent such connections?

- A. Set the malware category to block
- B. Set the Command and Control category to block
- C. Set the phishing category to override
- D. Set the hacking category to continue

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 399

Topic #: 1

[\[All PCNSE Questions\]](#)

In order to fulfill the corporate requirement to back up the configuration of Panorama and the Panorama-managed firewalls securely which protocol should you select when adding a new scheduled config export?

- A. HTTPS
- B. FTP
- C. SMB v3
- D. SCP

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 400

Topic #: 1

[\[All PCNSE Questions\]](#)

A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT, Finance, and HR. Which two types of traffic will the rule apply to? (Choose two.)

- A. traffic between zone Finance and zone HR
- B. traffic between zone IT and zone Finance
- C. traffic within zone HR
- D. traffic within zone IT

[Show Suggested Answer](#)



Actual exam question from Palo Alto Networks's PCNSE

Question #: 401

Topic #: 1

[\[All PCNSE Questions\]](#)

An administrator connected a new fiber cable and transceiver to interface Ethernet1/1 on a Palo Alto Networks firewall. However, the link does not seem to be coming up.

If an administrator were to troubleshoot, how would they confirm the transceiver type, tx-power, rx-power, vendor name, and part number via the CLI?

- A. `show system state filter sw.dev.interface.config`
- B. `show chassis status slot s1`
- C. `show system state filter-pretty sys.s1.*`
- D. `show system state filter ethernet1/1`

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 402

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer wants to forward all decrypted traffic on a PA-850 firewall to a forensic tool with a decrypt mirror interface.

Which statement is true regarding the configuration of the Decryption Port Mirroring feature?

- A. The engineer should install the Decryption Port Mirror license and reboot the firewall.
- B. The PA-850 firewall does not support decrypt mirror interface, so the engineer needs to upgrade the firewall to PA-3200 series.
- C. The engineer must assign an IP from the same subnet with the forensic tool to the decrypt mirror interface.
- D. The engineer must assign the related virtual-router to the decrypt mirror interface.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 403

Topic #: 1

[\[All PCNSE Questions\]](#)

Which statement is true regarding a heatmap in a BPA report?

- A. When guided by authorized sales engineer, it helps determine the areas of the greatest security risk.
- B. It runs only on firewalls.
- C. It provides a percentage of adoption for each assessment area.
- D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.

Show Suggested Answer





Actual exam question from Palo Alto Networks's PCNSE

Question #: 404

Topic #: 1

[\[All PCNSE Questions\]](#)

An engineer is configuring secure web access (HTTPS) to a Palo Alto Networks firewall for management.

Which profile should be configured to ensure that management access via web browsers is encrypted with a trusted certificate?

- A. A Certificate profile should be configured with a trusted root CA
- B. An SSL/TLS Service profile should be configured with a certificate assigned.
- C. An Interface Management profile with HTTP and HTTPS enabled should be configured.
- D. An Authentication profile with the allow list of users should be configured.

Show Suggested Answer

