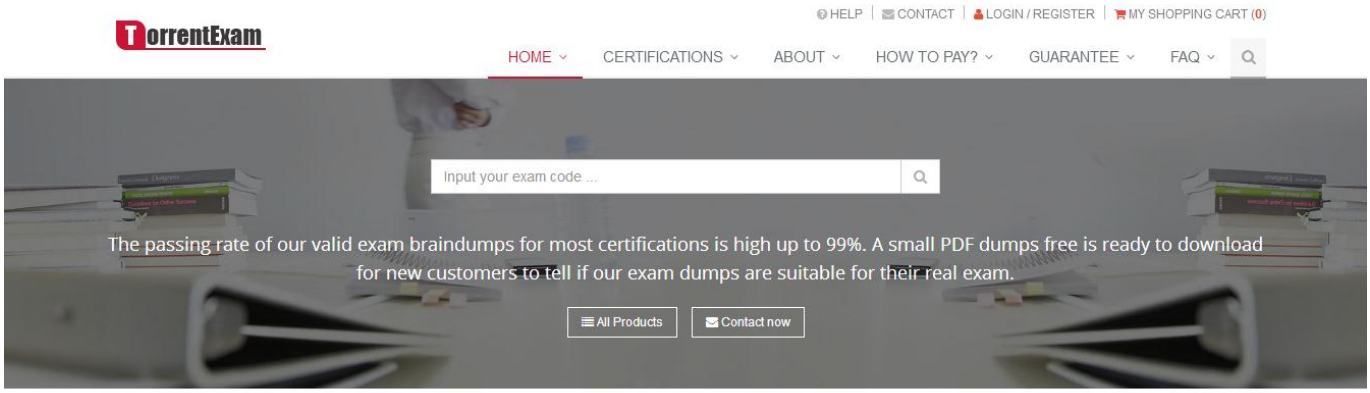
TorrentExam



Why Choose Us

QUALITY AND VALUE

RealExamFree Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our RealExamFree testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

RealExamFree offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

Customer Reviews

I wasted a lot of money and failed twice. Thanks to HPE0-J78 exam collection I pass now.

Noel

realexamfree is a reliable company. I pass exam at first shot. Many thanks

Julie

Pass BIMF.EN successfully. Really good dumps. It saves me a lot of time. Wonderful!

Ahern

online test engine is very useful for me,because i could practice the C-TERP10-67 question dumps in my phone when i was waititng or on the bus even without internet,i could make the most of my time.Last week,i passed the C-TERP10-67. so i want to share the realexamfree with you guys,hope you will get a good result in test.

Carl

http://www.torrentexam.com

Best Exam Bootcamp & Excellent VCE Torrent & Satisfying Dumps Torrent

Exam : **NGFW-Engineer**

Title : Palo Alto Networks Next-Generation Firewall Engineer

Vendor : Palo Alto Networks

Version : DEMO

NO.1 A firewall administrator needs to configure a new Palo Alto Networks firewall so that its management interface automatically obtains an IP address, netmask, and default gateway from the network.
Which command should be executed in the CLI to accomplish this goal?
A. set deviceconfig system interface mgt mode dhcp
B. set network interface management dhcp enable
C. set deviceconfig system type dhcp-client
D. configure system management-interface ip dynamic
Answer: C
Explanation:
Basic Concept: The CLI command to configure management as a DHCP client is made under deviceconfig system rather than under data-plane interface configuration.
Why C is Correct: set deviceconfig system type dhcp-client is the correct command syntax for enabling DHCP on the management interface.
Why A is Wrong: set deviceconfig system interface mgt mode dhcp is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.
Why B is Wrong: set network interface management dhcp enable is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.
Why D is Wrong: configure system management-interface ip dynamic is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

NO.2 An administrator configures a GlobalProtect gateway with split tunneling for network traffic based on an access route. Users report that public web browsing works, but they cannot resolve the names of internal servers. The administrator determines that all DNS queries are being sent to the public DNS servers configured on the users' endpoints.
Which GlobalProtect portal setting should be configured to resolve this issue?
A. Split tunneling for DNS and specify the internal corporate domains in the "Domain" list
B. DNS Proxy feature on the firewall to point clients to the gateway IP for DNS
C. "DNS Forwarding" option on the gateway's tunnel interface
D. NAT rule to allow DNS traffic from the GlobalProtect clients to the internal DNS servers
Answer: A
Explanation:
Basic Concept: Split tunnel access routes do not automatically control DNS resolution. Split DNS must specify which domains use VPN-assigned DNS servers.
Why A is Correct: Configuring split DNS with internal corporate domains sends those queries to corporate DNS while leaving public browsing DNS local.
Why B is Wrong: DNS Proxy feature on the firewall to point clients to the gateway IP for DNS relates to VPN configuration, but it does not address the specific PAN-OS requirement for selectors, tunnel interface functions, routing, or Security policy in this scenario.
Why C is Wrong: "DNS Forwarding" option on the gateway's tunnel interface relates to VPN configuration, but it does not address the specific PAN-OS requirement for selectors, tunnel interface functions, routing, or Security policy in this scenario.

Why D is Wrong: NAT rule to allow DNS traffic from the GlobalProtect clients to the internal DNS servers relates to VPN configuration, but it does not address the specific PAN-OS requirement for selectors, tunnel interface functions, routing, or Security policy in this scenario.

NO.3 What are two valid zone types that can be selected from the zone configuration menu, per Palo Alto Networks best practices? (Choose two.)

A. Layer 3

B. Layer 2

C. Management

D. DMZ

Answer: A B

Explanation:

Basic Concept: Zone type is the PAN-OS category that matches interface mode. Valid selectable zone types include Layer 2 and Layer 3, among others.

Why A and B are Correct: Layer 3 and Layer 2 are valid zone types; Management and DMZ are not PAN-OS zone types, although DMZ is often used as a zone name.

Why C is Wrong: Management is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

Why D is Wrong: DMZ is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

NO.4 Which two statements apply to configuring required security rules when setting up an IPSec tunnel between a Palo Alto Networks firewall and a third- party gateway? (Choose two.)

A. For incoming and outgoing traffic through the tunnel, creating separate rules for each direction is optional.

B. The IKE negotiation and IPSec/ESP packets are allowed by default via the intrazone default allow policy.

C. For incoming and outgoing traffic through the tunnel, separate rules must be created for each direction.

D. The IKE negotiation and IPSec/ESP packets are denied by default via the interzone default deny policy.

Answer: C D

Explanation:

Basic Concept: An IPSec VPN on PAN-OS involves two distinct flows: control-plane tunnel negotiation to the firewall and data-plane traffic entering or leaving the tunnel security zone. Both are enforced by Security policy.

Why C and D are Correct: The corrected answer reflects that data traffic initiated in either direction must be permitted by matching zone-based rules, and IKE/IPSec negotiation to the firewall/local zone is not simply allowed by intrazone-default.

Why A is Wrong: PAN-OS is stateful for return traffic, but if both sides must initiate new sessions through the VPN, directional policies are required for each relevant source and destination zone.

Why B is Wrong: IKE and IPSec/ESP negotiation traffic to the firewall is not simply covered by intrazone- default allow. It must match a Security policy between the peer-facing zone and the firewall local endpoint.

NO.5 A network architect is planning the deployment of a new IPSec VPN tunnel to connect a local data center to a cloud environment. The plan must include all necessary Security policy configurations for both tunnel negotiation and data transit.
Which two Security policy requirements must be included in the implementation plan? (Choose two answers)

A. The default interzone-default security policy is sufficient to allow the tunnel negotiation traffic between the firewall and the remote peer.

B. A pair of policies is required to control the flow of data traffic into and out of the security zone assigned to the tunnel interface.

C. A policy must explicitly permit only the IKE application between the external-facing zone and local zone.

D. A policy must explicitly permit the IPSec container application between the external-facing zone and local zone.

Answer: B D

Explanation:
Basic Concept: IPSec implementation planning must include Security policy for tunnel establishment and for decrypted data traffic through the tunnel zone.
Why B and D are Correct: A data-policy pair is required for flows through the tunnel zone, and a policy must permit the IPSec container application to the firewall/local endpoint.
Why A is Wrong: The default interzone-default security policy is sufficient to allow the tunnel negotiation traffic between the firewall and the remote peer. relates to VPN configuration, but it does not address the specific PAN-OS requirement for selectors, tunnel interface functions, routing, or Security policy in this scenario.
Why C is Wrong: A policy must explicitly permit only the IKE application between the external-facing zone and local zone. relates to VPN configuration, but it does not address the specific PAN-OS requirement for selectors, tunnel interface functions, routing, or Security policy in this scenario.

NO.6 What is the requirement for interface link speeds when configuring a virtual wire on a Palo Alto Networks firewall?

A. They must be configured with auto-negotiate settings regardless of the port type.

B. They must all be either copper or fiber optic, however they can be different.

C. They must have the same link speed and transmission mode.

D. They must be the same media type.

Answer: C

Explanation:
Basic Concept: Virtual wire binds two physical interfaces into an inline transparent pair. The two interfaces must have compatible Layer 1 characteristics.
Why C is Correct: Same link speed and transmission mode are required so the virtual wire can bridge traffic correctly between the paired interfaces.
Why A is Wrong: They must be configured with auto-negotiate settings regardless of the port type. is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.
Why B is Wrong: They must all be either copper or fiber optic, however they can be different. is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

Why D is Wrong: They must be the same media type. is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

NO.7 Which two services are configured by applying an SSL/TLS service profile? (Choose two.)

A. Global Protect portal

B. Log forwarding to Strata Logging Service

C. Forward-Trust certificate

D. Syslog server monitoring

Answer: A C

Explanation:

Basic Concept: SSL/TLS service profiles apply certificates and TLS parameters to firewall services. GlobalProtect portal is a clear service-profile use case; this item uses imprecise wording for the second option.

Why A and C are Correct: GlobalProtect portal is valid, and the keyed Forward-Trust certificate relates to SSL Forward Proxy trust material, although strictly it is a certificate role rather than a service profile consumer.

Why B is Wrong: Log forwarding to Strata Logging Service uses onboarding, certificates, and logging settings, not a standard SSL/TLS service profile attached to a firewall-hosted service.

Why D is Wrong: Syslog over TLS uses syslog/certificate configuration, not the SSL/TLS service profile used by services such as GlobalProtect or Authentication Portal.

NO.8 Which configuration step is required when implementing a new self-signed root certificate authority (CA) certificate for SSL decryption on a Palo Alto Networks firewall?

A. Import the new subordinate CA certificate into the trust stores of all client devices.

B. Set the subordinate CA certificate as the default routing certificate for all network traffic.

C. Configure the subordinate CA to issue certificates with indefinite validity periods.

D. Disable all existing SSL decryption rules until the new certificate is fully propagated.

Answer: A

Explanation:

Basic Concept: SSL Forward Proxy requires endpoints to trust the firewall's issuing CA certificate; otherwise browsers reject dynamically generated substitute certificates.

Why A is Correct: Importing the CA certificate into client trust stores is required so clients trust certificates generated by the firewall during decryption.

Why B is Wrong: Set the subordinate CA certificate as the default routing certificate for all network traffic. is associated with authentication, PKI, or TLS configuration, but it is not the object or step that enforces the certificate validation or service identity requirement being tested.

Why C is Wrong: Configure the subordinate CA to issue certificates with indefinite validity periods. is associated with authentication, PKI, or TLS configuration, but it is not the object or step that enforces the certificate validation or service identity requirement being tested.

Why D is Wrong: Disable all existing SSL decryption rules until the new certificate is fully propagated. is associated with authentication, PKI, or TLS configuration, but it is not the object or step that enforces the certificate validation or service identity requirement being tested.

NO.9 A network security engineer needs to permit traffic between two distinct VSYS that reside on

one Palo Alto Networks firewall. This traffic will not egress the firewall to an external device.
Which zone type must be configured to act as the logical source and destination for this traffic flow?

A. External

B. TAP

C. Layer 3

D. Layer 2

Answer: A

Explanation:
Basic Concept: Inter-VSYS traffic that remains within the firewall uses external zones as logical source /destination zones for Security policy.
Why A is Correct: External is the correct zone type because the traffic crosses VSYS boundaries without using a physical interface.
Why B is Wrong: TAP is related to management or logging, but it does not provide the required Panorama operation, rule hierarchy behavior, or dual-log forwarding outcome.
Why C is Wrong: Layer 3 is related to management or logging, but it does not provide the required Panorama operation, rule hierarchy behavior, or dual-log forwarding outcome.
Why D is Wrong: Layer 2 is related to management or logging, but it does not provide the required Panorama operation, rule hierarchy behavior, or dual-log forwarding outcome.

NO.10 A security administrator is creating a new custom report to get a consolidated view of network events and needs to select a database to query for the report data.
Which valid set of databases is available for the task?

A. Threat, URL Filtering, WildFire Submissions, GlobalProtect

B. Traffic, User-ID, Application Statistics, HIP Match

C. Data Filtering, IP-Tag, User-ID, Endpoint Security

D. System, Config, Authentication, Session Flow

Answer: B

Explanation:
Basic Concept: Custom reports query selected log databases. Traffic, User-ID, Application Statistics, and HIP Match are valid data sources in PAN-OS reporting contexts.
Why B is Correct: The selected set contains valid databases for consolidated reporting from the choices provided.
Why A is Wrong: Threat, URL Filtering, WildFire Submissions, GlobalProtect is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.
Why C is Wrong: Data Filtering, IP-Tag, User-ID, Endpoint Security is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.
Why D is Wrong: System, Config, Authentication, Session Flow is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

NO.11 A network security engineer wants to create Security policy rules that allow or deny traffic based on a user's department, which corresponds to groups in the company's Active Directory. To achieve this, the firewall needs to retrieve group information from the directory server.

Which configuration object must be created first to establish the connection with the Active Directory server?

A. LDAP server profile

B. User-ID agent service account

C. Authentication sequence

D. Kerberos server profile

Answer: A

Explanation:

Basic Concept: Group-based policy requires group mapping, and group mapping requires a directory connection. LDAP Server profiles establish that directory connection.

Why A is Correct: Creating an LDAP server profile first lets PAN-OS query Active Directory for group membership used in Security policy.

Why B is Wrong: User-ID agent service account is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

Why C is Wrong: Authentication sequence is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

Why D is Wrong: Kerberos server profile is a valid Palo Alto Networks or networking concept in another context, but it does not implement the exact configuration outcome required by this question.

NO.12 How does a Palo Alto Networks firewall choose the best route when it receives routes for the same destination from different routing protocols?

A. The route that was received first will be entered into the forwarding table, and all subsequent routes will be rejected.

B. It will attempt to load balance the traffic across all routes.

C. It compares the administrative distance and chooses the one with the highest value.

D. It compares the administrative distance and chooses the one with the lowest value.

Answer: D

Explanation:

Basic Concept: When routes to the same destination are learned from different routing protocols, PAN-OS compares administrative distance before metrics from the same protocol.

Why D is Correct: The lowest administrative distance wins because it represents the most preferred route source; higher values are less trusted.

Why A is Wrong: The route that was received first will be entered into the forwarding table, and all subsequent routes will be rejected. is a routing-related concept, but it is not the PAN-OS routing attribute, prerequisite, or route-selection behavior required by this question.

Why B is Wrong: It will attempt to load balance the traffic across all routes. is a routing-related concept, but it is not the PAN-OS routing attribute, prerequisite, or route-selection behavior required by this question.

Why C is Wrong: It compares the administrative distance and chooses the one with the highest value. is a routing-related concept, but it is not the PAN-OS routing attribute, prerequisite, or route-selection behavior required by this question.

NO.13 Which two Palo Alto Networks firewall services are secured by attaching an SSL/TLS service profile to their configuration? (Choose two.)

A. Authentication portal

B. GlobalProtect portal

C. LDAP server profiles

D. Prisma Access service connections

Answer: A B

Explanation:

Basic Concept: SSL/TLS service profiles secure firewall-hosted TLS services by binding certificates and protocol settings.

Why A and B are Correct: Authentication Portal and GlobalProtect Portal are services that present TLS certificates and use SSL/TLS service profiles.

Why C is Wrong: LDAP server profiles is associated with authentication, PKI, or TLS configuration, but it is not the object or step that enforces the certificate validation or service identity requirement being tested.

Why D is Wrong: Prisma Access service connections is associated with authentication, PKI, or TLS configuration, but it is not the object or step that enforces the certificate validation or service identity requirement being tested.