Vendor: Palo Alto Networks

Exam Code: PCNSA

Exam Name: Palo Alto Networks Certified Network Security Administrator

Version: DEMO

QUESTION 1
How is an address object of type IP range correctly defined?

A. 192.168.40.1-192.168.40.255
B. 192.168.40.1-255
C. 192.168.40.1, 192.168.40.255
D. 192.168.40.1/24

Answer: A
Explanation:
Enter an IP address range (Ex. 10.0.0.1-10.0.0.4). Each of the IP addresses in the range can also be in an IPv6 form (Ex. 2001:db8:123:1::1-2001:db8:123:1::11).

QUESTION 2
What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

A. firewall logs
B. custom API scripts
C. Security Information and Event Management Systems (SIEMS), such as Splunk
D. biometric scanning results from iOS devices
E. DNS Security service

Answer: ABC
Explanation:
https://docs.paloaltonetworks.com/best-practices/10-1/user-id-best-practices/user-id-best-practices/user-id-best-practices-for-dynamic-user-groups
Identity the user information sources for the tags:
Firewall logs
For Authentication, Data, Threat, Traffic, Tunnel Inspection, URL, and WildFire logs, create a log forwarding profile and use the Built-In Actions.
For User-ID, HIP Match, GlobalProtect, and IP-Tag logs, configure the log settings.
Cortex XSOAR
Security Information and Event Management Systems (SIEMS), such as Splunk
Custom API scripts

QUESTION 3
According to best practices, how frequently should WildFire updates he made to perimeter firewalls?

A. every 10 minutes
B. every minute
C. every 5 minutes
D. in real time

Answer: D
Explanation:
https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices
If you are running PAN-OS 10.0 or later, configure your firewall to retrieve WildFire signatures in real-time. This provides access to newly-discovered malware signatures as soon as the WildFire public cloud can generate them, thereby preventing successful attacks by minimizing your

exposure time to malicious activity.

QUESTION 4
What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)

A. It uses techniques such as DGA/DNS tunneling detection and machine learning
B. It requires a valid Threat Prevention license.
C. It enables users to access real-time protections using advanced predictive analytics.
D. It requires a valid URL Filtering license.
E. It requires an active subscription to a third-party DNS Security service.

Answer: ABC
Explanation:
DNS Security subscription enables users to access real-time protections using advanced predictive analytics. When techniques such as DGA/DNS tunneling detection and machine learning are used, threats hidden within DNS traffic can be proactively identified and shared through an infinitely scalable cloud service. Because the DNS signatures and protections are stored in a cloud-based architecture, you can access the full database of ever-expanding signatures that have been generated using a multitude of data sources. This list of signatures allows you to defend against an array of threats using DNS in real-time against newly generated malicious domains. To combat future threats, updates to the analysis, detection, and prevention capabilities of the DNS Security service will be available through content releases. To access the DNS Security service, you must have a Threat Prevention license and DNS Security license.

QUESTION 5
Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?

A. save named configuration snapshot
B. export device state
C. export named configuration snapshot
D. save candidate config

Answer: C
Explanation:
Export Named Configuration Snapshot
This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

QUESTION 6
An administrator is investigating a log entry for a session that is allowed and has the end reason of aged-out. Which two fields could help in determining if this is normal? (Choose two.)

A. Packets sent/received
B. IP Protocol
C. Action
D. Decrypted

Answer: AB
Explanation:
When monitoring the traffic logs using Monitor > logs > Traffic, some traffic is seen with the Session End Reason as aged-out. Any traffic that uses UDP or ICMP is seen will have session end reason as aged-out in the traffic log. This is because unlike TCP, there is there is no way for a graceful termination of UDP session and so aged-out is a legitimate session-end reason for UDP (and ICMP) sessions.
Link: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMjLCAW

QUESTION 7
Which action can be set in a URL Filtering Security profile to provide users temporary access to all websites in a given category using a provided password?

A. exclude
B. continue
C. hold
D. override

Answer: D
Explanation:
The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security administrator or help-desk person would provide a password granting temporary access to all websites in the given category. A log entry is generated in the URL Filtering log. The Override webpage doesn't display properly on client systems configured to use a proxy server.

QUESTION 8
An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

A. Security policy = drop, Gambling category in URL profile = allow
B. Security policy = deny. Gambling category in URL profile = block
C. Security policy = allow, Gambling category in URL profile = alert
D. Security policy = allow. Gambling category in URL profile = allow

Answer: C
Explanation:
A log entry is generated in the URL filtering log.
https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-filtering-profiles

QUESTION 9
Which statement is true regarding NAT rules?

A. Static NAT rules have precedence over other forms of NAT.
B. Translation of the IP address and port occurs before security processing.
C. NAT rules are processed in order from top to bottom.
D. Firewall supports NAT on Layer 3 interfaces only.

Answer: C

Explanation:
1. the NAT rules are processed first before the security rules (https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0)
2. the NAT rules are processed from top down (https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overview)

QUESTION 10
Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?

A. Palo Alto Networks C&C IP Addresses
B. Palo Alto Networks Bulletproof IP Addresses
C. Palo Alto Networks High-Risk IP Addresses
D. Palo Alto Networks Known Malicious IP Addresses

Answer: D
Explanation:
Palo Alto Networks Known Malicious IP Addresses
--Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share Threat Intelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edls

QUESTION 11
You receive notification about a new malware that infects hosts. An infection results in the infected host attempting to contact a command-and-control server. Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?

A. Antivirus Profile
B. Data Filtering Profile
C. Vulnerability Protection Profile
D. Anti-Spyware Profile

Answer: D
Explanation:
Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.

QUESTION 12
If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?

A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL
B. Configure a frequency schedule to clear group mapping cache

C. Configure a Primary Employee ID number for user-based Security policies
D. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 or

Answer: A
Explanation:
If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups

QUESTION 13
Which administrative management services can be configured to access a management interface?

A. HTTP, CLI, SNMP, HTTPS
B. HTTPS, SSH, telnet, SNMP
C. SSH, telnet, HTTP, HTTPS
D. HTTPS, HTTP, CLI, API

Answer: C
Explanation:
The administrative management services are http, https, telnet and ssh.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/management-interfaces

QUESTION 14
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

A. Palo Alto Networks Bulletproof IP Addresses
B. Palo Alto Networks C&C IP Addresses
C. Palo Alto Networks Known Malicious IP Addresses
D. Palo Alto Networks High-Risk IP Addresses

Answer: A
Explanation:
To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PM0pCAG

QUESTION 15
Which attribute can a dynamic address group use as a filtering condition to determine its membership?

A. tag
B. wildcard mask
C. IP address
D. subnet mask

Answer: A
Explanation:
Dynamic Address Groups: A dynamic address group populates its members dynamically using looks ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-address-groups

QUESTION 16
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

A. SAML
B. TACACS+
C. LDAP
D. Kerberos

Answer: AB
Explanation:
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html

QUESTION 17
Which type of profile must be applied to the Security policy rule to protect against buffer overflows, illegal code execution, and other attempts to exploit system flaws?

A. URL filtering
B. vulnerability protection
C. file blocking
D. anti-spyware

Answer: B
Explanation:
Vulnerability Protection Security Profiles protect against threats entering the network. For example, Vulnerability Protection Security Profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection Security Profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**