Test - Accredited Configuration Engineer (ACE) Exam - PAN-OS 6.0 Version

ACE Exam

Question 1 of 50.

Which of the following statements is NOT True about Palo Alto Networks firewalls?

- System defaults may be restored by performing a factory reset in Maintenance Mode.
- The Admin account may be disabled.
- The Admin account may not be disabled.
- Initial configuration may be accomplished thru the MGT interface or the Console port.

Mark for follow up

Question 2 of 50.

Users may be authenticated sequentially to multiple authentication servers by configuring:

- Multiple RADIUS servers sharing a VSA configuration.
- An Authentication Sequence.
- A custom Administrator Profile.
- An Authentication Profile.

Mark for follow up

Question 3 of 50.

Palo Alto Networks firewalls support the use of both Dynamic (built-in user roles) and Role-Based (customized user roles) for Administrator Accounts.

True False

Mark for follow up

Question 4 of 50.

When an interface is in Tap mode and a Policy's action is set to "block", the interface will send a TCP reset.

True False

Mark for follow up

Question 5 of 50.

Which of the following must be enabled in order for User-ID to function?

- Security Policies must have the User-ID option enabled.
- User-ID must be enabled for the source zone of the traffic that is to be identified.
- Captive Portal must be enabled.
- Captive Portal Policies must be enabled.

Mark for follow up

Question 6 of 50.

When troubleshooting Phase 1 of an IPsec VPN tunnel, which location and log will be most informative?

- Initiating side, System log
- Responding side, Traffic log
- Initiating side, Traffic log
- Responding side, System Log

Mark for follow up

Question 7 of 50.

Which of the following interface types can have an IP address assigned to it? (Select all correct answers.)

- Layer 3
- Layer 2
- Tap
- Virtual Wire

Mark for follow up

Question 8 of 50.

After the installation of a new version of PAN-OS, the firewall must be rebooted.

True False

Mark for follow up

Question 9 of 50.

Which statement about config locks is True?

- A config lock will expire after 24 hours, unless it was set by a superuser.
- A config lock can be removed only by the administrator who set it.
- A config lock can be removed only by a superuser.
- A config lock can only be removed by the administrator who set it or by a superuser.

Mark for follow up

Question 10 of 50.

Besides selecting the Heartbeat Backup option when creating an Active-Passive HA Pair, which of the following also prevents "Split-Brain"?

- Configuring a backup HA2 link that points to the MGT interface of the other device in the pair.
- Creating a custom interface under Service Route Configuration, and assigning this interface as the backup HA2 link.
- Under “Packet Forwarding”, selecting the VR Sync checkbox.
- Configuring an independent backup HA1 link.

Mark for follow up

Question 11 of 50.

A "Continue" action can be configured on which of the following Security Profiles?

- URL Filtering and File Blocking
- URL Filtering only
- URL Filtering, File Blocking, and Data Filtering
- URL Filtering and Anti-virus

Mark for follow up

Question 12 of 50.

What will be the user experience when the safe search option is NOT enabled for Google search but the firewall has "Safe Search Enforcement" Enabled?

- The user will be redirected to a different search site that is specified by the firewall administrator.
- A task bar pop-up message will be presented to enable Safe Search.
- The Firewall will enforce Safe Search if the URL filtering license is still valid.
- A block page will be presented with instructions on how to set the strict Safe Search option for the Google search.

Mark for follow up

Question 13 of 50.

When using remote authentication for users (LDAP, RADIUS, Active Directory, etc.), what must be done to allow a user to authenticate through multiple methods?

- This cannot be done. Although multiple authentication methods exist, a firewall must choose a single, global authentication type--and all users must use this method.
- This cannot be done. A single user can only use one authentication type.
- Create an Authentication Sequence, dictating the order of authentication profiles.
- Create multiple authentication profiles for the same user.

Mark for follow up

Question 14 of 50.

Taking into account only the information in the screenshot above, answer the following question. An administrator is using SSH on port 3333 and BitTorrent on port 7777. Which statements are True?

- [ ] The BitTorrent traffic will be denied.
- [ ] The SSH traffic will be denied.
- [ ] The BitTorrent traffic will be allowed.
- [ ] The SSH traffic will be allowed.

Mark for follow up

Question 15 of 50.

Considering the information in the screenshot above, what is the order of evaluation for this URL Filtering Profile?

- URL Categories (BrightCloud or PAN-DB), Custom Categories, Block List, Allow List.
- Allow List, Block List, Custom Categories, URL Categories (BrightCloud or PAN-DB).
- Block List, Allow List, Custom Categories, URL Categories (BrightCloud or PAN-DB).
- Block List, Allow List, URL Categories (BrightCloud or PAN-DB), Custom Categories.

Mark for follow up

Question 16 of 50.

Which type of license is required to perform Decryption Port Mirroring?

- A subscription-based SSL Port license
- A Client Decryption license
- A free PAN-PA-Decrypt license
- A subscription-based PAN-PA-Decrypt license

Mark for follow up

Question 17 of 50.

In a Palo Alto Networks firewall, every interface in use must be assigned to a zone in order to process traffic.

True False

Mark for follow up

Question 18 of 50.

When configuring a Decryption Policy rule, which option allows a firewall administrator to control SSHv2 tunneling in policies by specifying the SSH-tunnel App-ID?

- SSH Proxy
- SSL Forward Proxy
- SSL Inbound Inspection
- SSL Reverse Proxy

Mark for follow up

Question 19 of 50.

An interface in tap mode can transmit packets on the wire.

True False

Mark for follow up

Question 20 of 50.

What are two sources of information for determining whether the firewall has been successful in communicating with an external User-ID Agent?

- System Logs and an indicator light on the chassis.
- System Logs and Authentication Logs.

- System Logs and the indicator light under the User-ID Agent settings in the firewall.
- Traffic Logs and Authentication Logs.

Mark for follow up

Question 21 of 50.

WildFire may be used for identifying which of the following types of traffic?

- OSPF
- DHCP
- Malware
- RIPv2

Mark for follow up

Question 22 of 50.

When using Config Audit, the color yellow indicates which of the following?

- A setting has been changed between the two config files
- A setting has been deleted from a config file.
- A setting has been added to a config file
- An invalid value has been used in a config file.

Mark for follow up

Question 23 of 50.

You can assign an IP address to an interface in Virtual Wire mode.

True False

Mark for follow up

Question 24 of 50.

In PAN-OS, the WildFire Subscription Service allows updates for malware signatures to be distributed as often as…

- Once a week
- Once an hour
- Once a day
- Once every 15 minutes

Mark for follow up

Question 25 of 50.

Which of the following most accurately describes Dynamic IP in a Source NAT configuration?

- A single IP address is used, and the source port number is changed.
- A single IP address is used, and the source port number is unchanged.
- The next available address in the configured pool is used, and the source port number is changed.
- The next available IP address in the configured pool is used, but the source port number is unchanged.

Mark for follow up

Question 26 of 50.

“What is the result of an Administrator submitting a WildFire report’s verdict back to Palo Alto Networks as “Incorrect”?

- You will receive an update within 15 minutes.
- You will receive an email to disable the signature manually.
- The signature will be updated for False positive and False negative files in the next Application signature update.
- The signature will be updated for False positive and False negative files in the next AV signature update.

Mark for follow up

Question 27 of 50.

A user complains that she is no longer able to access a needed work application after the administrator implemented vulnerability and anti-spyware profiles. How best can the administrator resolve this issue so the user will once again have access to the needed application?

- Create and enable an Application Override Policy, specifying the port used by this application.
- Check the Threat Log and locate an event showing the user's application being blocked. Using the source IP address displayed in that event, create an IP address-based exemption for the group that the user is a member of.
- In the vulnerability and anti-spyware Profiles, create an application exemption for the group's application.
- Create a custom Security Policy for this user so that she will be able to access the required application. Be sure not to apply the vulnerability and anti-spyware profiles to this policy.

Mark for follow up

Question 28 of 50.

Which of the following are methods that HA clusters use to identify network outages?

- Link and Session Monitors
- VR and VSYS Monitors
- Heartbeat and Session Monitors
- Path and Link Monitoring

Mark for follow up

Question 29 of 50.

Which routing protocol is supported on the Palo Alto Networks platform?

- BGP
- RIPv1
- ISIS
- RSTP

Mark for follow up

Question 30 of 50.

When configuring the firewall for User-ID, what is the maximum number of Domain Controllers that can be

configured?

- 10
- 50
- 150
- 100

Mark for follow up

Question 31 of 50.

Which link is used by an Active/Passive cluster to synchronize session information?

- The Control Link
- The Uplink
- The Management Link
- The Data Link

Mark for follow up

Question 32 of 50.

A Config Lock may be removed by which of the following users? (Select all correct answers.)

- Superusers
- Device administrators
- Any administrator
- The administrator who set it

Mark for follow up

Question 33 of 50.

Which statement below is True?

- PAN-OS uses BrightCloud as its default URL Filtering database, but also supports PAN-DB.
- PAN-OS uses PAN-DB for URL Filtering, replacing BrightCloud.

- PAN-OS uses BrightCloud for URL Filtering, replacing PAN-DB.
- PAN-OS uses PAN-DB as the default URL Filtering database, but also supports BrightCloud.

Mark for follow up

Question 34 of 50.

The screenshot above shows part of a firewall's configuration. If ping traffic can traverse this device from e1/2 to e1/1, which of the following statements must be True about this firewall's configuration? (Select all correct answers.)

- There must be appropriate routes in the default virtual router.
- There must be a security policy from Internet zone to trust zone that allows ping.
- There must be a Management Profile that allows ping. (Then assign that Management Profile to e1/1 and e1/2.)
- There must be a security policy from trust zone to Internet zone that allows ping.

Mark for follow up

Question 35 of 50.

Taking into account only the information in the screenshot above, answer the following question: A span port or a switch is connected to e1/4, but there are no traffic logs. Which of the following conditions most likely explains this behavior?

- The interface is not assigned an IP address.
- The interface is not up.
- The interface is not assigned a virtual router.
- There is no zone assigned to the interface.

Mark for follow up

Question 36 of 50.

In Palo Alto Networks terms, an application is:

- A specific program detected within an identified stream that can be detected, monitored, and/or blocked.
- A combination of port and protocol that can be detected, monitored, and/or blocked.
- A file installed on a local machine that can be detected, monitored, and/or blocked.
- Web-based traffic from a specific IP address that can be detected, monitored, and/or blocked.

Mark for follow up

Question 37 of 50.

Both SSL decryption and SSH decryption are disabled by default.

True False

Mark for follow up

Question 38 of 50.

An enterprise PKI system is required to deploy SSL Forward Proxy decryption capabilities.

True False

Mark for follow up

Question 39 of 50.

Which of the following is NOT a valid option for built-in CLI Admin roles?

- devicereader
- read/write
- deviceadmin
- superuser

Mark for follow up

Question 40 of 50.

In PAN-OS 6.0, rule numbers are:

- Numbers that specify the order in which security policies are evaluated.
- Numbers created to be unique identifiers in each firewall's policy database.
- Numbers on a scale of 0 to 99 that specify priorities when two or more rules are in conflict.
- Numbers created to make it easier for users to discuss a complicated or difficult sequence of rules.

Mark for follow up

Question 41 of 50.

In PAN-OS 6.0 and later, which of these items may be used as match criterion in a Policy-Based Forwarding Rule? (Choose 3.)

- Destination Zone
- Application
- Source User
- Source Zone

Mark for follow up

Question 42 of 50.

Taking into account only the information in the screenshot above, answer the following question. Which applications will be allowed on their standard ports? (Select all correct answers.)

- Gnutella
- SSH
- BitTorrent
- Skype

Mark for follow up

Question 43 of 50.

All of the interfaces on a Palo Alto Networks device must be of the same interface type.

True False

Mark for follow up

Question 44 of 50.

Taking into account only the information in the screenshot above, answer the following question. An administrator is pinging 4.4.4.4 and fails to receive a response. What is the most likely reason for the lack of response?

- There is no route back to the machine originating the ping.
- The interface is down.
- There is no Management Profile.
- There is a Security Policy that prevents ping.

Mark for follow up

Question 45 of 50.

What is the function of the GlobalProtect Portal?

- To maintain the list of Global Protect Gateways and specify HIP data that the agent should report.
- To load-balance GlobalProtect client connections to GlobalProtect Gateways.
- To maintain the list of remote GlobalProtect Portals and the list of categories for checking the client machine.
- To provide redundancy for tunneled connections through the GlobalProtect Gateways.

Mark for follow up

Question 46 of 50.

Traffic going to a public IP address is being translated by a Palo Alto Networks firewall to an internal server's private IP address. Which IP address should the Security Policy use as the "Destination IP" in order to allow traffic to the server?

- The server's private IP
- The server's public IP

- The firewall's gateway IP
- The firewall's MGT IP

Mark for follow up

Question 47 of 50.

In an Anti-virus profile, setting the action to "Block" for IMAP and POP3 decoders will result in which of the following actions?

- The firewall with this Anti-virus profile will behave as if an "Alert" is the specified action, and the server sending the email will attempt to re-send it.
- The firewall will send an HTTP 404 error message back to the server that is attempting to send the email.
- All email messages sent using the IMAP or POP3 protocols will be dropped by the firewall, even if they are not infected with a virus.
- It's not possible to set an Anti-virus profile action to "Block" IMAP and POP3 traffic.

Mark for follow up

Question 48 of 50.

Which of the following platforms supports the Decryption Port Mirror function?

- PA-3000
- VM-Series 100
- PA-2000
- PA-4000

Mark for follow up

Question 49 of 50.

When you have created a Security Policy Rule that allows Facebook, what must you do to block all other web-browsing traffic?

- When creating the policy, ensure that web-browsing is included in the same rule.
- Nothing. You can depend on PAN-OS to block the web-browsing traffic that is not needed for Facebook use.
- Ensure that the Service column is defined as "application-default" for this Security policy. Doing this will automatically include the implicit web-browsing application dependency.

Create an additional rule that blocks all other traffic.

Mark for follow up

Question 50 of 50.

An interface in Virtual Wire mode must be assigned an IP address.

True False

Mark for follow up

Save / Return Later Summary

Incorrect Answers:

6781	**A "Continue" action can be configured on which of the following Security Profiles?**	Incorrect
7974	**A user complains that she is no longer able to access a needed work application after the administrator implemented vulnerability and anti-spyware profiles. How best can the administrator resolve this issue so the user will once again have access to the needed application?**	Incorrect
6791	**An enterprise PKI system is required to deploy SSL Forward Proxy decryption capabilities.**	Incorrect
7989	**Besides selecting the Heartbeat Backup option when creating an Active-Passive HA Pair, which of the following also prevents "Split-Brain"?**	Incorrect

8097	**Considering the information in the screenshot above, what is the order of evaluation for this URL Filtering Profile?**	Incorrect
8761	**In an Anti-virus profile, setting the action to "Block" for IMAP and POP3 decoders will result in which of the following actions?**	Incorrect
8751	**In Palo Alto Networks terms, an application is:**	Incorrect
8731	**In PAN-OS, the WildFire Subscription Service allows updates for malware signatures to be distributed as often as…**	Incorrect
8087	**Taking into account only the information in the screenshot above, answer the following question. An administrator is using SSH on port 3333 and BitTorrent on port 7777. Which statements are True?**	Incorrect
8072	**Taking into account only the information in the screenshot above, answer the following question: A span port or a switch is connected to e1/4, but there are no traffic logs. Which of the following conditions most likely explains this behavior?**	Incorrect
8082	**The screenshot above shows part of a firewall's configuration. If ping traffic can traverse this device from e1/2 to e1/1, which of the following statements must be True about this firewall's configuration? (Select all correct answers.)**	Incorrect
8696	**Users may be authenticated sequentially to multiple authentication servers by configuring:**	Incorrect
8636	**When configuring a Decryption Policy rule, which option allows a firewall administrator to control SSHv2 tunneling in policies by specifying the SSH-tunnel App-ID?**	Incorrect
7964	**When using Config Audit, the color yellow indicates which of the following?**	Incorrect
7969	**When using remote authentication for users (LDAP, RADIUS, Active Directory, etc.), what must be done to allow a user to authenticate through multiple methods?**	Incorrect
8606	**When you have created a Security Policy Rule that allows Facebook, what must you do to block all other web-browsing traffic?**	Incorrect

8531	**Which of the following interface types can have an IP address assigned to it? (Select all correct answers.)**	Incorrect
8516	**Which of the following must be enabled in order for User-ID to function?**	Incorrect
8485	**Which of the following statements is NOT True about Palo Alto Networks firewalls?**	Incorrect