Free Questions for PCNSE

Shared by Marshall on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization wants to begin decrypting guest and BYOD traffic.

Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

Options:

A- Authentication Portal

B- SSL Decryption profile

C- SSL decryption policy

D- comfort pages

Answer:

A

Explanation:

An authentication portal is a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An authentication portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The authentication portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button.The authentication portal can also be configured to use different authentication methods, such as local database, RADIUS, LDAP, Kerberos, or SAML1.By using an authentication portal, the firewall can redirect BYOD users to a web page where they can learn about the decryption policy, download and install the CA certificate, and agree to the terms of use before accessing the network or the internet2.

An SSL decryption profile is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption profile is a set of options that define how the firewall handles SSL/TLS traffic that it decrypts.An SSL decryption profile can include settings such as certificate verification, unsupported protocol handling, session caching, session resumption, algorithm selection, etc3. An SSL decryption profile does not provide any user identification or notification functions.

An SSL decryption policy is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption policy is a set of rules that determine which traffic the firewall decrypts based on various criteria, such as source and destination zones, addresses, users, applications, services, etc.An SSL decryption policy can also specify which type of decryption to apply to the traffic, such as SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy4. An SSL decryption policy does not provide any user identification or notification functions.

Comfort pages are not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. Comfort pages are web pages that the firewall displays to users when it blocks or fails to decrypt certain traffic due to security policy or technical reasons.Comfort pages can include information such as the reason for blocking or failing to decrypt the traffic, the URL of the original site, the firewall serial number, etc5. Comfort pages do not provide any user identification or notification functions before decrypting the traffic.

Question 2

Question Type: MultipleChoice

An administrator is informed that the engineer who previously managed all the VPNs has left the company. According to company policies the administrator must update all the IPSec VPNs with new pre-shared keys Where are the pre-shared keys located on the firewall?

Options:

A- Network/IPSec Tunnels

B- Network/Network Profiles/IKE Gateways

C- Network/Network ProfilesTIPSec Crypto

D- Network/Network Profiles/IKE Crypto

Answer:

B

Question 3

Question Type: MultipleChoice

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?

Options:

A- A Decryption profile must be attached to the Decryption policy that the traffic matches.

B- A Decryption profile must be attached to the Security policy that the traffic matches.

C- There must be a certificate with only the Forward Trust option selected.

D- There must be a certificate with both the Forward Trust option and Forward Untrust option selected.

Answer:

C

Question 4

Question Type: MultipleChoice

In the New App Viewer under Policy Optimizer, what does the compare option for a specific rule allow an administrator to compare?

Options:

A- The running configuration with the candidate configuration of the firewall

B- Applications configured in the rule with applications seen from traffic matching the same rule

C- Applications configured in the rule with their dependencies

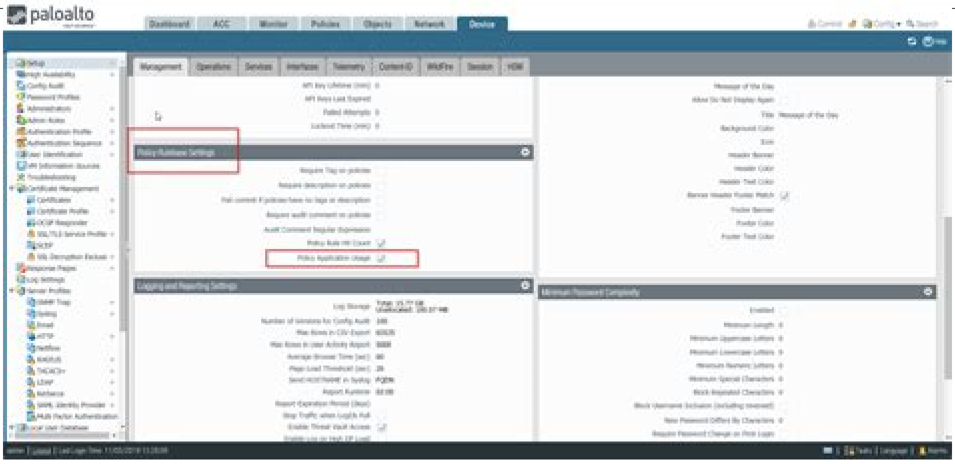
D- The security rule with any other security rule selected

Answer:

B

Explanation:

The compare option for a specific rule in the New App Viewer under Policy Optimizer allows an administrator to compare the applications configured in the rule with the applications seen from traffic matching the same rule. This helps the administrator to identify any new applications that are not explicitly defined in the rule, but are implicitly allowed by the firewall based on the dependencies of the configured applications.The compare option also shows the usage statistics and risk levels of the applications, and provides suggestions for optimizing the rule by adding, removing, or replacing applications12.Reference:New App Viewer (Policy Optimizer), PCNSE Study Guide (page 47)



API Key Lifetime (min) 0
API Keys Last Expired
Failed Attempts 0
Lockout Time (min) 0

Policy Rulebase Settings

Require Tag on policies
Require description on policies
Fail commit if policies have no tags or description
Require audit comment on policies
Audit Comment Regular Expression
Policy Rule Hit Count ✓
Policy Application Usage ✓

Logging and Reporting Settings

Log Storage Total: 15.77 GB
Unallocated: 150.37 MB
Number of Versions for Config Audit 100
Max Rows in CSV Export 65535
Max Rows in User Activity Report 5000
Average Browse Time (sec) 60
Page Load Threshold (sec) 20
Send HOSTNAME in Syslog FQDN
Report Runtime 02:00
Report Expiration Period (days)
Stop Traffic when LogDb Full
Enable Threat Vault Access ✓
Enable Log on High DP Load

Message of the Day
Allow Do Not Display Again
Title Message of the Day
Background Color
Icon
Header Banner
Header Color
Header Text Color
Banner Header Footer Match ✓
Footer Banner
Footer Color
Footer Text Color

Minimum Password Complexity

Enabled
Minimum Length 0
Minimum Uppercase Letters 0
Minimum Lowercase Letters 0
Minimum Numeric Letters 0
Minimum Special Characters 0
Block Repeated Characters 0
Block Username Inclusion (including reversed)
New Password Differs By Characters 0
Require Password Change on First Login

admin | Logout | Last Login Time: 11/05/2018 11:28:08

Tasks | Language | Alarms