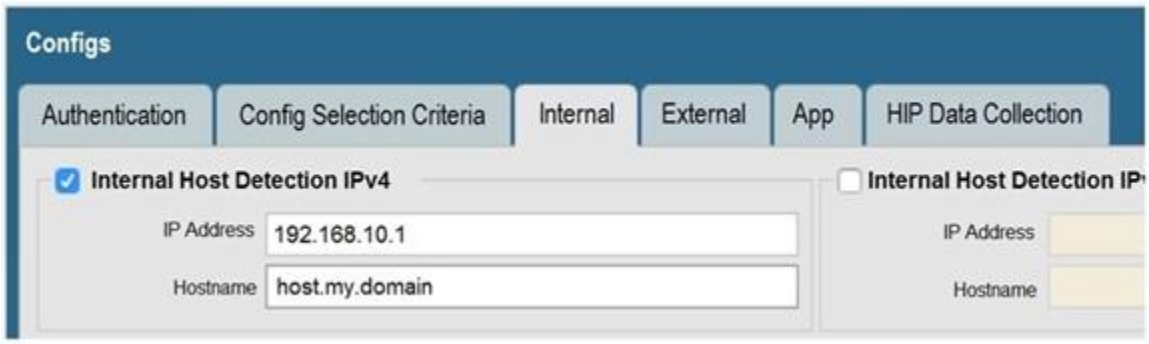
Vendor: Palo Alto Networks

Exam Code: PCNSC

Exam Name: Palo Alto Networks Certified Network Security Consultant

Version: DEMO

QUESTION 1
View the GlobalProtect configuration screen capture.
What is the purpose of this configuration?



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

Answer: D
Explanation:
https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-app-configurations

QUESTION 2
Which feature prevents the submission of corporate login information into website forms?

A. credential phishing prevention
B. file blocking
C. User-ID
D. data filtering

Answer: A
Explanation:
Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials.

QUESTION 3
A firewall engineer creates a new App-ID report under Monitor > Reports > Application Reports > New Applications to monitor new applications on the network and better assess any Security policy updates the engineer might want to make.

How does the firewall identify the New App-ID characteristic?

A. It matches to the New App-IDs downloaded in the last 90 days.
B. It matches to the New App-IDs in the most recently installed content releases.

C. It matches to the New App-IDs downloaded in the last 30 days.
D. It matches to the New App-IDs installed since the last time the firewall was rebooted.

Answer: B
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/monitor-new-app-ids

QUESTION 4
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. certification revocation
C. Content-ID
D. App-ID

Answer: D
Explanation:
The Palo Alto Networks firewall provides this capability by integrating the features App-ID and User-ID with the QoS configuration.

QUESTION 5
A Palo Alto Networks NGFW 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. 10 to 15 minutes
B. 5 to 10 minutes
C. More than 15 minutes
D. 5 minutes

Answer: B

QUESTION 6
Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

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

Answer: ACE
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleLCAS

QUESTION 7
If an administrator wants to decrypt SMTP traffic and possesses the saver'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 now proxy
D. SMTP inbound Decryption

Answer: B
Explanation:
Use SSL Inbound Inspection to decrypt and inspect inbound SSL/TLS traffic from a client to a targeted network server (any server you have the certificate for and can import it onto the firewall) and block suspicious sessions.
For example, if an employee is remotely connected to a web server hosted on the company network and is attempting to add restricted internal documents to his Dropbox folder (which uses SSL for data transmission), SSL Inbound Inspection can ensure that the sensitive data does not move outside the secure company network by blocking or restricting the session.
On the firewall, you must install the certificate and private key for each server for which you want to perform SSL inbound inspection. You must also install the public key certificate as well as the private key on each firewall that performs SSL inbound inspection. The way the firewall performs SSL inbound inspection depends on the type of key negotiated, Rivest, Shamir, Adleman (RSA) or Perfect Forward Secrecy (PFS).
For RSA keys, the firewall performs SSL inbound inspection without terminating the connection. As the encrypted session flows through the firewall, the firewall transparently makes a copy of it and decrypts it so that the firewall can apply the appropriate policy to the traffic.
Reference:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-inbound-inspection

QUESTION 8
An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

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

Answer: D
Explanation:
Inbound decryption is where you are decrypting traffic to your internal server. You don't use a Root CA, you load that server's cert and private key. The Root cert is 'Optional'.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-inbound-inspection

QUESTION 9
Which feature can be configured on VM-Series firewalls?

A. aggregate interlaces
B. multiple virtual systems

C. Globallprotect
D. machine learning

Answer: C

QUESTION 10
Which two benefits come from assigning a Decrypting Profile to a Decryption rule with a" NO Decrypt" action? (Choose two.)

A. Block sessions with unsuspected cipher suites
B. Block sessions with untrusted issuers
C. Block credential phishing.
D. Block sessions with client authentication
E. Block sessions with expired certificates

Answer: BE

QUESTION 11
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. Authentication policy
B. Decryption policy
C. Security policy
D. Application Override policy

Answer: A
Explanation:
Authentication policy enables you to authenticate end users before they can access services and applications. Whenever a user requests a service or application (such as by visiting a web page), the firewall evaluates Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors), such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication.

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**