Features Of Web-based Palo Alto Networks NetSec-Analyst Practice Exam

If you opting for this NetSec-Analyst study engine, it will be a shear investment. We never boost our achievements, and all we have been doing is trying to become more effective and perfect as your first choice, and determine to help you pass the NetSec-Analyst preparation questions as efficient as possible. And our high-efficiency of the NetSec-Analyst Exam Braindumps is well known among our loyal customers. If you study with our NetSec-Analyst learning materials for 20 to 30 hours, then you will pass the exam easily.

If you really intend to pass the NetSec-Analyst exam, our software will provide you the fast and convenient learning and you will get the best study materials and get a very good preparation for the exam. The content of the NetSec-Analyst guide torrent is easy to be mastered and has simplified the important information. What's more, our NetSec-Analyst prep torrent conveys more important information with less questions and answers. The learning is relaxed and highly efficiently.

>> NetSec-Analyst Braindumps <<

Testing NetSec-Analyst Center, Valid NetSec-Analyst Exam Simulator

The certificate is of significance in our daily life. At present we will provide all candidates who want to pass the NetSec-Analyst exam with three different versions for your choice. Any of the three versions can work in an offline state, and the version makes it possible that the websites is available offline. If you use the quiz prep, you can use our latest NetSec-Analyst Exam Torrent in anywhere and anytime. How can you have the chance to enjoy the study in an offline state? You just need to download the version that can work in an offline state, and the first time you need to use the version of our NetSec-Analyst quiz torrent online.

Palo Alto Networks Network Security Analyst Sample Questions (Q121-Q126):

NEW QUESTION # 121
A large enterprise uses a critical, internally developed database replication service that communicates exclusively between two specific database clusters (Cluster-A and Cluster-B) over TCP/1433 and TCP/50000-50005. App-ID occasionally misidentifies traffic on TCP/1433 as 'ms-sql-smb' and TCP/50000-50005 as 'unknown-tcp'. The security team wants to enforce strict security profiles on this replication traffic, ensuring it's always classified as 'internal-db-replication', a custom application previously defined. Additionally, they need to apply a specific QOS profile. Which set of configurations will best achieve this, considering the need for both precise identification and performance?

- A. 1. Create an Application Filter that includes 'ms-sql-smb' and 'unknown-tcp'. 2. Create a security policy allowing this Application Filter between Cluster-A and Cluster-B, with the desired profiles.
- B. 1. Disable App-ID for all traffic between Cluster-A and Cluster-B. 2. Create a security policy based on IP addresses and ports, applying the security and QOS profiles.
- C. 1. Create a Service Group including TCP/1433 and TCP/50000-50005. 2. Create a security policy allowing 'any' application with this Service Group between Cluster-A and Cluster-B, applying the security and QOS profiles.
- D. 1. Create two custom application signatures, one for TCP/1433 and another for TCP/50000-50005, both named 'internal-db-replication'. 2. Create a security policy allowing 'internal-db-replication' between Cluster-A and Cluster-B,

applying the desired security and QOS profiles.

- E. 1. Create two Application Override policies:

```
set application-override rule 'db-repl-1433' application 'internal-db-replication' protocol tcp port 1433 source 'Cluster-A-IPs'
destination 'Cluster-B-IPs'
```

Answer: E

Explanation:
This scenario highlights the precise application of Application Overrides for critical services. While Option A (custom signatures) is possible, it's more complex if the underlying protocol hasn't fundamentally changed, just its identification. Option B uses Application Overrides to force the correct classification ('internal-db-replication') for the specific source/destination/port combinations. Once the traffic is correctly identified by the override, the security policy can then precisely apply the necessary security and QOS profiles based on this accurate application ID. Options C, D, and E either bypass App-ID entirely, leading to less granular control and visibility, or don't properly reclassify the traffic for specific policy application.

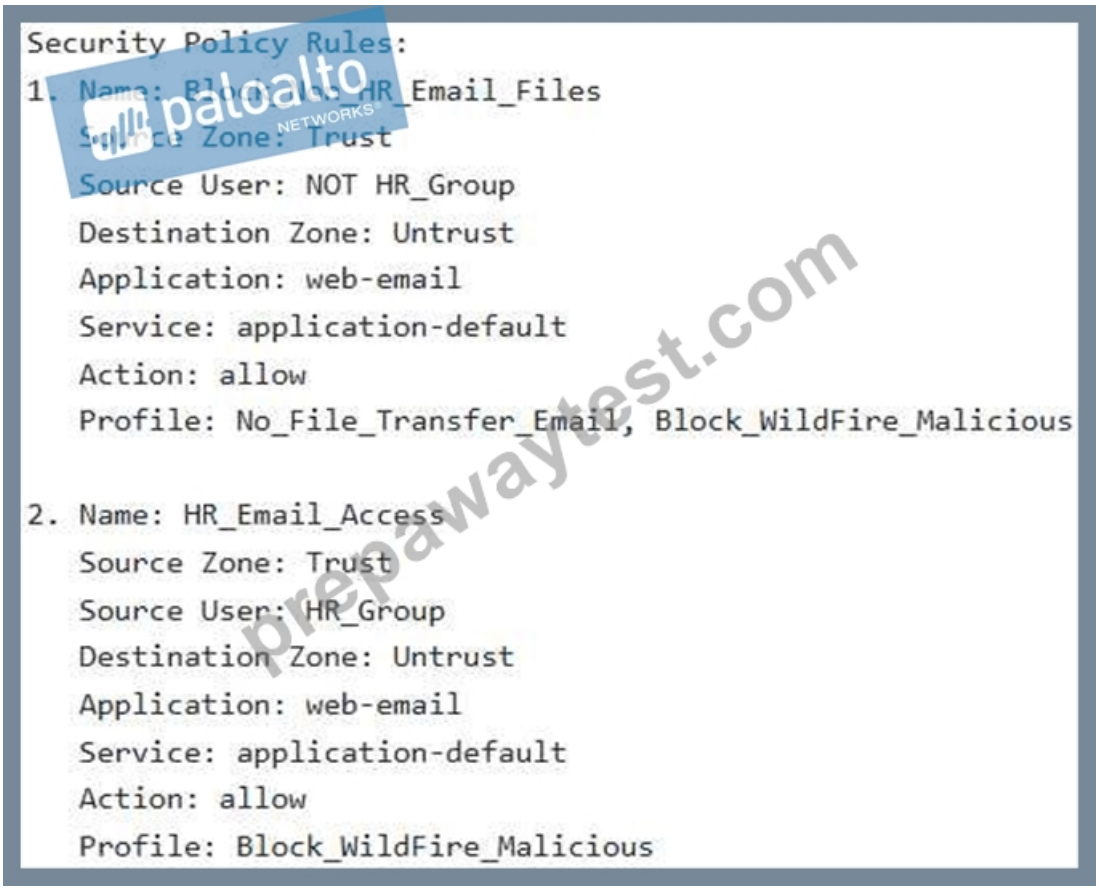
NEW QUESTION # 122
A Security Administrator wants to implement a policy to block all file transfers (upload and download) on web-based email applications (e.g., Gmail, Outlook Web Access) for non-HR users, while HR users should have unrestricted file transfer access. Additionally, for all web-based email traffic, regardless of user or application, all malicious files detected by WildFire should be blocked. Which set of configurations and policy rules best achieves this?

- A. Rule 1: Source User: HR_Group, Destination: Untrust, Application: web-email, Action: allow, Profiles: WildFire Analysis (block all). Rule 2: Source User: NOT HR_Group, Destination: Untrust, Application: web-email, Action: allow, Profiles: File Blocking (block all files), WildFire Analysis (block all).
- B. Define a custom File Blocking Profile 'No_File_Transfer_Email' to block all file types for 'upload' and 'download'. Define a WildFire Analysis Profile 'Block WildFire Malicious' to block all WildFire verdicts.

```
Security Policy Rules:
1. Name: HR_Email_Access
   Source Zone: Trust
   Source User: HR_Group
   Destination Zone: Untrust
   Application: web-email
   Service: application-default
   Action: allow
   Profile: Block_WildFire_Malicious

2. Name: Non_HR_Email_Access
   Source Zone: Trust
   Source User: NOT HR_Group
   Destination Zone: Untrust
   Application: web-email
   Service: application-default
   Action: allow
   Profile: No_File_Transfer_Email, Block_WildFire_Malicious
```

- C. Rule 1: Source User: HR_Group, Destination: Untrust, Application: gmail, outlook-web-access, Action: allow, Profiles: WildFire Analysis (block all). Rule 2: Source User: any, Destination: Untrust, Application: gmail, outlook-web-access, Action: allow, Profiles: File Blocking (block all files), WildFire Analysis (block all).
- D. Create a single policy rule that allows 'web-email' for all users. Apply a File Blocking Profile to block all files, and a WildFire Analysis Profile to block all. Then create a separate application override for HR users for web-email to bypass file blocking.
- E. Define a custom File Blocking Profile 'No_File_Transfer_Email' to block all file types for 'upload' and 'download'. Define a WildFire Analysis Profile 'Block WildFire Malicious' to block all WildFire verdicts.



Answer: E

Explanation:
Option D is the most precise and correctly ordered approach. The key here is the order of policies and applying the correct profiles.
1. The first rule for 'NOT HR_Group' explicitly applies the 'No_File_Transfer_Email' (blocking all files for both upload/download) and the 'Block_WildFire_Malicious' profiles.
2. The second rule, for 'HR_Group', being evaluated AFTER the non-HR rule, will apply only the 'Block_WildFire_Malicious' profile, ensuring HR can transfer files but malicious files are still blocked for them. Option C has the correct profiles but the rule order is crucial. If the HR rule is first, and a non-HR user falls into it (e.g., due to a previous misconfiguration), they might get unrestricted access. The 'NOT HR_Group' rule must come first to enforce the stricter policy. Option A and B are less granular with application groups and profile application. Option E is not a standard or efficient way to manage this with Security Policies.

NEW QUESTION # 123
A company is deploying a new Palo Alto Networks firewall and requires comprehensive visibility into encrypted traffic. They plan to implement SSL Forward Proxy decryption. During testing, users report issues accessing various websites, including some financial institutions and healthcare portals. Upon investigation, the firewall logs show 'Untrusted Certificate' errors. Which of the following is the most likely cause and the immediate corrective action?

- A. The 'SSL Inbound Inspection' profile is misconfigured.
- B. The decryption policy rule is set to 'No Decryption' for these specific URL categories.
- C. The firewall's clock is out of sync with NTP, leading to certificate validity issues.
- D. The firewall's root CA certificate used for signing intercepted traffic has not been distributed to client trust stores.
- E. The 'Block Sessions with Unknown Status' setting is enabled in the SSL Protocol Settings of the decryption profile.

Answer: D

Explanation:
When SSL Forward Proxy decryption is enabled, the firewall acts as a man-in-the-middle, generating new certificates for intercepted connections, signed by its own Root CA. If this Root CA is not trusted by the client devices (i.e., not distributed to their trust stores), clients will receive an 'Untrusted Certificate' error. This is a very common initial hurdle in forward proxy deployments. Options B and D are unlikely to cause 'Untrusted Certificate' errors. Option C might cause blocks, but the primary error message

points to trust. Option E is a possibility for certificate validity, but 'Untrusted Certificate' directly implies a missing trust anchor for the firewall's self-signed certificates.

NEW QUESTION # 124
A critical industrial control system (ICS) network, isolated from the internet, requires extremely low latency and high availability. While internal DoS attacks are rare, a misconfigured or rogue device could potentially flood the network. The security team wants to implement a DoS protection profile that proactively identifies and drops unusually high rates of UDP traffic targeting specific ICS application ports, without introducing any significant processing overhead or latency. Which configuration approach in Palo Alto Networks firewall DoS protection would best achieve this goal?

- A. Create a 'DoS Protection Policy' rule with 'Packet Based Attack Protection' for 'UDP Flood' and specify the target application ports, setting 'Action: Syn-Cookie' to mitigate.
- B. Apply an 'IP Address Block' profile to the ICS interface, monitoring for any source IP exceeding a 'Session Rate' of 100 sessions/second and blocking for 300 seconds.
- C. Configure a 'Zone Protection' profile for the ICS zone with 'Flood Protection' enabled for 'UDP Flood', setting a 'Per-Packet Rate' threshold and 'Action: Drop'.
- D. Utilize 'Packet Based Attack Protection' within a 'DoS Protection Policy' rule, targeting 'UDP Flood' on specific destination ports, and configure a 'Per-Packet Rate' threshold with 'Action: Drop'.
- E. Implement a 'Data Filtering' profile to identify specific UDP payload patterns associated with ICS applications and block traffic not conforming to these patterns.

Answer: D

Explanation:
The requirement is to proactively identify and drop high rates of UDP traffic on specific application ports with low latency. 'Packet Based Attack Protection' within a 'DoS Protection Policy' is the most granular and efficient way to achieve this. By targeting 'UDP Flood' and specifying destination ports, the firewall can quickly identify and drop excessive UDP packets without the overhead of session tracking or SYN- cookie mechanisms (which are for TCP). Option A (Zone Protection) provides less granularity on specific ports. Option B incorrectly suggests 'Syn- Cookie' for UDP. Option C (IP Address Block) is reactive and might block legitimate devices due to misconfiguration. Option D (Data Filtering) is for content inspection, not volume-based DoS. Option E precisely matches the requirements for efficient, targeted UDP flood protection.

NEW QUESTION # 125
You are debugging a connectivity issue where an internal application server, running a custom SSH service on port 2222, cannot establish connections to an external cloud logging service. The firewall logs show 'deny' actions with application 'ssh' and service 'application-default', even though a specific policy rule allows 'custom_ssh_app' (a custom App-ID for port 2222) to the logging service. What is the most likely cause and solution?

- A. The firewall is correctly identifying the traffic as standard SSH (App-ID: ssh) despite the custom port. The solution is to modify the allowing rule to explicitly allow 'ssh' application and 'tcp/2222' as the service.
- B. The custom App-ID 'custom_ssh_app' is incorrectly defined and is not identifying the traffic as SSH. The solution is to redefine the custom App-ID to accurately match the SSH handshake on port 2222.
- C. The security policy rule for 'custom_ssh_app' has a lower priority than a generic 'deny all SSH' rule. The solution is to move the 'custom_ssh_app' rule to a higher priority.
- D. The issue is with Application Override. The firewall is incorrectly overriding the custom App-ID with the default 'ssh' App-I The solution is to remove any Application Override rules that might conflict with this custom application.
- E. The traffic is being identified as 'application-incomplete' before the custom App-ID can classify it. The solution is to allow 'application-incomplete' for the destination IP, then refine the rule.

Answer: A

Explanation:
This is a classic App-ID behavior scenario. Palo Alto Networks firewalls perform deep packet inspection. Even if you define a custom App-ID for a non-standard port, if the traffic itself inherently resembles a known application (like SSH), the firewall will identify it as that known application's App-ID. The log showing 'application: ssh' confirms this. Therefore, the allowing rule needs to specify the 'ssh' App-ID and the custom port 'tcp/2222' as the service. Option A is unlikely if the custom App-ID was meant for a custom protocol, but here it's still SSH. Option B is possible but the log showing 'ssh' indicates App-ID identification, not just a generic deny. Option D is incorrect; Application Override forces a specific application, it wouldn't cause it to be seen as 'ssh' if a custom App-ID was intended. Option E is incorrect as the application IS identified as 'ssh'.

NEW QUESTION # 126
.....

Our customer service is available 24 hours a day. You can contact us by email or online at any time. In addition, all customer information for purchasing Palo Alto Networks Network Security Analyst test torrent will be kept strictly confidential. We will not disclose your privacy to any third party, nor will it be used for profit. Then, we will introduce our products in detail. On the one hand, Palo Alto Networks Network Security Analyst test torrent is revised and updated according to the changes in the syllabus and the latest developments in theory and practice. On the other hand, a simple, easy-to-understand language of NetSec-Analyst Test Answers frees any learner from any learning difficulties - whether you are a student or a staff member. These two characteristics determine that almost all of the candidates who use NetSec-Analyst guide torrent can pass the test at one time. This is not self-determination.

Testing NetSec-Analyst Center: https://www.prepawaytest.com/Palo-Alto-Networks/NetSec-Analyst-practice-exam-dumps.html

Besides, the concise layout of NetSec-Analyst test quiz can make you find what you want to read and remember, If you are still not sure you can pass exams certainly you had better look for valid NetSec-Analyst latest dumps, Just buy our NetSec-Analyst learning quiz, and you will get all you want, Therefore, we have created these formats so that every applicant can prepare successfully for the Palo Alto Networks Network Security Analyst (NetSec-Analyst) exam on the first attempt, Just come to our official website and click on the corresponding website link of the NetSec-Analyst exam materials, then seek the information you need, the test samples are easy to obtain.

And teachers use it a lot in the classroom, and we have a free NetSec-Analyst course outline to suggest how you can incorporate the book into either a workshop format or semester-long classes.

This technique is referred to as tail recursion, Besides, the concise layout of NetSec-Analyst Test Quiz can make you find what you want to read and remember, If you are still not sure you can pass exams certainly you had better look for valid NetSec-Analyst latest dumps.

Free PDF NetSec-Analyst - Palo Alto Networks Network Security Analyst Perfect Braindumps

Just buy our NetSec-Analyst learning quiz, and you will get all you want, Therefore, we have created these formats so that every applicant can prepare successfully for the Palo Alto Networks Network Security Analyst (NetSec-Analyst) exam on the first attempt.

Just come to our official website and click on the corresponding website link of the NetSec-Analyst exam materials, then seek the information you need, the test samples are easy to obtain.

- NetSec-Analyst Certificate Exam □ Interactive NetSec-Analyst Questions □ NetSec-Analyst Free Sample □ Open website ➠ www.pass4leader.com □ and search for ⇛ NetSec-Analyst ⇚ for free download □NetSec-Analyst Certificate Exam
- Updated Palo Alto Networks Braindumps – High Pass Rate Testing NetSec-Analyst Center □ Search for 「 NetSec-Analyst 」 and download it for free on □ www.pdfvce.com □ website □NetSec-Analyst Relevant Questions
- NetSec-Analyst PDF VCE □ NetSec-Analyst PDF VCE □ NetSec-Analyst PDF VCE □ Immediately open □ www.lead1pass.com □ and search for { NetSec-Analyst } to obtain a free download □Valid NetSec-Analyst Exam Cost
- Top Three Types of Pdfvce Palo Alto Networks NetSec-Analyst Exam Dumps □ Download ✔ NetSec-Analyst □✔□ for free by simply entering ➤ www.pdfvce.com □ website □New NetSec-Analyst Test Forum
- NetSec-Analyst Actual Exam Dumps □ Questions NetSec-Analyst Pdf □ NetSec-Analyst PDF VCE □ Open （ www.passcollection.com ） enter ⇛ NetSec-Analyst ⇚ and obtain a free download □NetSec-Analyst Practice Engine
- New NetSec-Analyst Test Forum □ NetSec-Analyst PDF VCE □ Exam Sample NetSec-Analyst Questions □ Go to website { www.pdfvce.com } open and search for ➠ NetSec-Analyst □ to download for free □Reliable NetSec-Analyst Test Review
- Professional NetSec-Analyst Braindumps - Leader in Qualification Exams - First-Grade Palo Alto Networks Palo Alto Networks Network Security Analyst □ Open [www.passtestking.com] and search for ▹ NetSec-Analyst ◃ to download exam materials for free □Questions NetSec-Analyst Pdf
- NetSec-Analyst Practice Engine ▸ Valid NetSec-Analyst Exam Cost □ Exam Sample NetSec-Analyst Questions □ The page for free download of " NetSec-Analyst " on ▹ www.pdfvce.com ◃ will open immediately □NetSec-Analyst Practice Engine
- Interactive NetSec-Analyst Practice Exam □ NetSec-Analyst Interactive Course □ New NetSec-Analyst Test Forum □

□ Easily obtain 《 NetSec-Analyst 》 for free download through □ www.examcollectionpass.com □ □Questions NetSec-Analyst Pdf

- Professional NetSec-Analyst Braindumps - Leader in Qualification Exams - First-Grade Palo Alto Networks Palo Alto Networks Network Security Analyst □ Immediately open ➡ www.pdfvce.com □□□ and search for ✔ NetSec-Analyst □✔□ to obtain a free download □NetSec-Analyst Practice Engine
- Interactive NetSec-Analyst Practice Exam □ NetSec-Analyst Latest Test Prep □ NetSec-Analyst Pass4sure Study Materials □ Search on ➡ www.prep4away.com □□□ for ▹ NetSec-Analyst ◃ to obtain exam materials for free download □Interactive NetSec-Analyst Practice Exam
- bhushansc.in, www.stes.tyc.edu.tw, skill.prestasimuda.com, yonyou.club, techsafetycourses.com, edu.globalfinx.in, digitalrepublix.com, 51.cuntuyun.cn, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, elearning.eauqardho.edu.so, Disposable vapes