PaloAltoNetworks.NetSec-Analyst.v2026-08-11.q121

Exam Code:	NetSec-Analyst
Exam Name:	Palo Alto Networks Network Security Analyst
Certification Provider:	Palo Alto Networks
Free Question Number:	121
Version:	v2026-08-11
# of views:	717
# of Questions views:	1444
https://www.dumpsfiles.com/files/Palo-Alto-Networks/NetSec-Analyst/PaloAltoNetworks.NetSec-Analyst.v2026-08-11.q121	

NEW QUESTION: 1
How would a Security policy need to be written to allow outbound traffic using Secure Shell (SSH) to destination ports tcp/22 and tcp/4422?
A. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin then creates a Security policy allowing application "ssh", service "tcp-4422". and service "application-default".
B. The admin creates a Security policy allowing application "ssh" and service "application-default".
C. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin then creates a Security policy allowing application "ssh" and service "tcp-4422".
D. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin also creates a custom service object named "tcp-22" with port tcp/22.The admin then creates a Security policy allowing application "ssh", service "tcp-4422". and service "tcp-22".
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
An analyst is creating a "Data Pattern" for DLP that needs to match a specific 10-digit customer account number that always starts with the letters "ACC". Which pattern type should be used?
A. File Properties
B. Regular Expression (Regex)
C. Predefined Pattern
D. Custom Dictionary
Answer: B (LEAVE A REPLY)
To identify specific, structured text patterns within a data stream, the analyst must use a Regular Expression (Regex). Regex allows for the definition of precise strings and numerical sequences.
In this scenario, the analyst would define a Regex such as ^ACC[0-9]{7}$ to capture exactly what is needed. This objective is fundamental to effective Data Loss Prevention (DLP), as it allows the organization to protect its unique, proprietary data formats that are not covered by standard predefined patterns like credit card numbers. By creating granular custom patterns, the analyst can prevent the exfiltration of sensitive internal documents while minimizing the false positives that occur with overly broad search terms.

NEW QUESTION: 3
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 (LEAVE A REPLY)

The Revert, Save, and Load operations all work with firewall co nfigurations local to the firewall. The Export operations transfer configurations as XML-formatted files from the firewall to the host running the web interface browser. From your local machine, you can save the files as configuration backups. The Import operations transfer XML configuration files from the host running the web interface browser to the firewall.
The XML file can be loaded as the candidate configuration or even be committed to becoming the running configuration. [Palo Alto Networks]

NEW QUESTION: 4

An organization relies heavily on Microsoft Remote Desktop Protocol (RDP) for administrative access, but they've implemented a custom RDP gateway on a non-standard port TCP/3390. While App-ID correctly identifies 'ms-rdp' on standard port 3389, it identifies TCP/3390 traffic as 'unknown-tcp'. The security team wants to ensure:
1 . All TCP/3390 traffic to the RDP gateway is explicitly identified as 'ms-rdp'.
2. Specific threat prevention profiles and a custom QOS profile are applied to this 'ms-rdp' traffic.
3. No other application override rule or App-ID signature should inadvertently reclassify this critical traffic.
Which of the following CLI command sequences for an Application Override policy would best meet these requirements?

A.
```
set application-override rule 'custom-rdp-override' application 'ms-rdp' protocol tcp port 3390
source-zone 'internal' destination-zone 'dmz' description 'Force RDP identification'
position-after 'web-browsing-override'
```

B.
```
set application-override rule 'custom-rdp-override' application 'ms-rdp' protocol tcp port 3390
source-zone 'internal' destination-zone 'dmz' description 'Force RDP identification'
position-before 'any'
```

C.
```
set application-override rule 'custom-rdp-override' application 'ms-rdp' protocol tcp port 3390
source 'any' destination 'any' description 'Force RDP identification'
position-top
```

D.
```
set application-override rule 'custom-rdp-override' application 'ms-rdp' protocol tcp port 3390
source-zone 'internal' destination-zone 'dmz' description 'Force RDP identification'
match-criteria 'all'
```

E.
```
set application-override rule 'custom-rdp-override' application 'ms-rdp' protocol tcp port 3390
source-zone 'internal' destination-zone 'dmz' description 'Force RDP identification'
order 'first'
```

Answer: B (LEAVE A REPLY)

The crucial part of the requirement is to ensure 'no other application override rule or App-ID signature should inadvertently reclassify this critical traffic'. Application Override rules are processed in order. By using 'position-before 'any", you ensure this specific override rule is placed at the very top of the override policy list, meaning it's evaluated before any other override or App-ID. This guarantees its precedence. 'position-top' (Option C) achieves a similar effect but might be less explicit in its positioning relative to other rules, depending on the specific CLI version and context. 'position-after' (Option A) would mean other rules might match first. 'match-criteria 'all" (Option D) is not a valid or relevant option for positioning. Option E 'order 'first" is not a standard CLI command for positioning. The specific source and destination zones also ensure the override is precise and doesn't broadly impact other traffic on TCP/3390 if it were to exist.

NEW QUESTION: 5

An administrator wants to create a No-NAT rule to exempt a flow from the default NAT rule. What is the best way to do this?

A. Create a Security policy rule to allow the traffic.

B. Create a static NAT rule with an application override.

C. Create a new NAT rule with the correct parameters and leave the translation type as None

D. Create a static NAT rule translating to the destination interface.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
A company is experiencing performance issues with their cloud-based CRM application (e.g., Salesforce), which uses App-ID: salesforce-base. Users in remote branches report slow response times, even though their internet links appear healthy. Investigation reveals occasional transient packet loss spikes and latency jitter affecting the application's performance. The network team wants to implement an SD-WAN policy that proactively steers Salesforce traffic away from paths experiencing degradation, even if the degradation is intermittent and temporary. Which of the following is the most appropriate configuration?
A. Create an SLA profile for Salesforce with strict thresholds for latency and packet loss. Configure a PBF rule for Salesforce traffic, and within the PBF, specify a primary path and a secondary path. The PBF will automatically failover if the primary path violates the SL
B. Define an SD-WAN policy for Salesforce. Use 'Dynamic Path Selection' with an SLA profile that monitors latency, jitter, and packet loss. Set the 'Path Selection Type' to 'Best Path' and configure multiple preferred paths. The system will continuously evaluate paths and select the one currently meeting the SLA.
C. Implement QOS policies on the WAN interfaces to prioritize Salesforce traffic. Configure a separate security policy for Salesforce to always use the most direct internet link, bypassing SD-WAN intelligence.
D. Configure health checks on all internet-facing interfaces. If any interface experiences degradation, manually disable that interface in the network configuration to force traffic to other links.
E. Utilize a standard static route for Salesforce traffic to a primary internet link. Implement BFD (Bidirectional Forwarding Detection) on the link to rapidly detect failures and switch to a pre-configured backup static route.
Answer: B (LEAVE A REPLY)
Option B is the correct approach. Palo Alto Networks SD-WAN's 'Dynamic Path Selection' (DPS) with 'Best Path' selection, coupled with a properly defined SLA profile monitoring latency, jitter, and packet loss, is designed precisely for scenarios where applications need to proactively steer away from degrading paths. The system constantly monitors path quality against the SLA and dynamically selects the best available path, ensuring optimal application performance even with intermittent network issues.

NEW QUESTION: 7
Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone.
Complete the security policy to ensure only Telnet is allowed.
Security Policy: Source Zone: Internal to DMZ Zone _____services "Application defaults", and action = Allow
A. Application = 'Telnet'
B. Log Forwarding
C. USER-ID = 'Allow users in Trusted'
D. Destination IP: 192.168.1.123/24
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
Which order of steps is the correct way to create a static route?
A. 1) Enter the route and netmask
2) Enter the IP address for the specific next hop
3) Specify the outgoing interface for packets to use to go to the next hop
4) Add an IPv4 or IPv6 route by name
B. 1) Enter the route and netmask
2) Specify the outgoing interface for packets to use to go to the next hop
3) Enter the IP address for the specific next hop
4) Add an IPv4 or IPv6 route by name
C. 1) Enter the IP address for the specific next hop
2) Enter the route and netmask

3) Add an IPv4 or IPv6 route by name
4) Specify the outgoing interface for packets to use to go to the next hop
D. 1) Enter the IP address for the specific next hop
2) Add an IPv4 or IPv6 route by name
3) Enter the route and netmask
4) Specify the outgoing interface for packets to use to go to the next hop
Answer: A (LEAVE A REPLY)
* Enter the route and netmask
* Enter the IP address for the specific next hop
* Specify the outgoing interface for packets to use to go to the next hop
* Add an IPv4 or IPv6 route by name Comprehensive Explanation: This is the correct order of steps to create a static route in a virtual router on the firewall. The first step is to enter the route and netmask for the destination network, such as 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address. The second step is to enter the IP address for the specific next hop, such as 192.168.56.1 or 2001:db8:49e:1::1. The third step is to specify the outgoing interface for packets to use to go to the next hop, such as ethernet1/1. The fourth step is to add an IPv4 or IPv6 route by name, such as route11. References:
* Configure a Static Route - Palo Alto Networks

NEW QUESTION: 9
A Palo Alto Networks firewall is configured with Decryption profiles for inbound SSL/TLS traffic inspection. Users are reporting certificate errors and browser warnings when accessing specific internal applications, while external HTTPS sites decrypt and load without issue. The firewall's trust store contains the CA certificate that signed the internal application servers' certificates. You've confirmed the decryption policy is enabled and applies to the internal traffic. What is the most likely, yet non-obvious, reason for these certificate errors, particularly when 'SSL Inbound Inspection' is in use?
A. The internal application servers are using unsupported cipher suites or TLS versions that the firewall cannot decrypt.
B. The decryption profile is configured to 'Block sessions with untrusted CA issuer', and the root CA certificate of the internal applications' signing CA is missing from the firewall's 'Trusted Root CA' store.
C. The firewall is re-signing the internal application server certificates with its own forward trust certificate, but this certificate is not trusted by the client browsers.
D. The internal application servers are presenting a certificate chain that the firewall cannot properly validate, perhaps due to missing intermediate CAS or revocation issues, causing it to block or present an invalid certificate.
E. The 'Forward Trust Certificate' configured in the Decryption Profile for inbound inspection is incorrect or not properly generated, leading to certificate path validation failures on the client side.
Answer: D (LEAVE A REPLY)
This scenario describes certificate errors on clients for internal applications when inbound SSL/TLS inspection is active, while external sites work. This immediately rules out the typical 'forward trust certificate' issues (C) which would affect outbound decryption. The firewall trusts the internal CA (stated in the question 'trust store contains the CA certificate'). The problem is likely with the server's certificate itself or its chain, as seen by the firewall. Option D, a faulty or incomplete certificate chain presented by the internal application server, is a very common and non-obvious issue. If the application server fails to present its full certificate chain (e.g., missing an intermediate CA certificate), even if the firewall has the root CA, it cannot build a complete trust path and thus considers the server's certificate invalid or untrusted. When the firewall then re-encrypts and presents its own certificate to the client, the client might still see an issue because the firewall's internal processing of the server's certificate was flawed. This is different from the firewall not trusting the root CA (B), as the question states it's in the trust store. Option A might lead to connection failures, but typically not 'certificate errors' specifically. Option E is for outbound decryption.

NEW QUESTION: 10
What is a primary benefit of using "Templates" within Panorama or Strata Cloud Manager?
A. To group firewalls based on their physical location.
B. To manage Layer 2 and Layer 3 network configurations across multiple devices.
C. To synchronize Security policy rules between firewalls.
D. To automate the backup of firewall configurations.
Answer: B (LEAVE A REPLY)
In the Palo Alto Networks centralized management model, Templates and Template Stacks are used specifically to manage the Network and Device tabs of the firewall configuration. This includes settings such as interfaces, zones, virtual routers, and server profiles (like LDAP or Syslog).

The benefit of using templates is that they allow an analyst to define a standard network baseline and push it to multiple firewalls simultaneously. For example, if an organization has 50 branch offices, the analyst can create a template that defines the standard NTP and DNS servers for all of them. This ensures consistency and significantly reduces the time required to deploy new hardware. It is important to distinguish templates from Device Groups, which are used to manage the Policies and Objects tabs. Understanding this separation is a key objective for an analyst to ensure that configurations are applied to the correct part of the management hierarchy.

NEW QUESTION: 11
Given the image, which two options are true about the Security policy rules. (Choose two.)

				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

A. The Allow Office Programs rule is using an Application Filter
B. In the Allow FTP to web server rule, FTP is allowed using App-ID
C. The Allow Office Programs rule is using an Application Group
D. In the Allow Social Networking rule, allows all of Facebook's functions
Answer: A,D (LEAVE A REPLY)
In the Allow FTP to web server rule, FTP is allowed using port based rule and not APP-ID.

NEW QUESTION: 12
A large enterprise utilizes a Palo Alto Networks firewall for its perimeter security. They have stringent compliance requirements, necessitating that all 'traffic', 'threat', and 'URL' logs be sent to a centralized logging platform (10.0.0.10) over UDP, while 'system' and 'configuration' logs must be sent to an internal audit server (10.0.0.20) over TCP, specifically in a custom format called 'AuditLogFormat'. All other log types should not be forwarded externally. The solution must be highly efficient and avoid sending unnecessary data.
A. Create two Log Forwarding Profiles. Profile 'Pl' for 10.0.0.10, include 'traffic', 'threat', 'URL'. Profile 'P2' for 10.0.0.20, include 'system', 'configuration', set 'AuditLogFormat'. Apply 'Pl' to security policies and 'P2' to global settings.
B. Create a single Log Forwarding Profile. Add 10.0.0.10 (UDP) with filters for 'traffic', 'threat', 'URL'. Add 10.0.0.20 (TCP, 'AuditLogFormat') with filters for 'system', 'configuration'. Apply this profile to all relevant security rules, as well as the 'Device -> Log Settings -Y System' and 'Device Log Settings Configuration' sections.
C. It's not possible to apply specific log types to different destinations using a single Log Forwarding Profile with distinct formats and transport protocols for each. Multiple profiles are mandatory, and applying them globally or to specific policies can be complex.
D. Implement two Log Forwarding Profiles. Profile 'LFP_Main' for 10.0.0.10 (UDP, default format) selecting 'traffic', 'threat', 'URL' in its 'Included Log Types'. Profile 'LFP_Audit' for 10.0.0.20 (TCP, 'AuditLogFormat') selecting 'system', 'configuration'. 'LFP_Main' will be attached to Security Policies. 'LFP_Audit' will be selected under 'Device Log Settings' for System and Configuration logs.
E. Configure a single Log Forwarding Profile. For 10.0.0.10 (UDP, default), set a filter:
```
(log.type eq 'traffic' or log.type eq 'threat' or log.type eq 'url')
```
Answer: (SHOW ANSWER)
Option D is the most robust and standard approach. While Option B/E tries to use a single profile, System and Configuration logs are generated by the device itself, not by security policies. They have separate forwarding settings under 'Device -> Log Settings'. Traffic, Threat, and URL logs are generated by security policies. Therefore, two profiles are necessary. Profile 1 (LFP_Main) for policy-generated logs (traffic, threat, URL) to the compliance platform. Profile 2 (LFP_Audit) for device-generated logs (system, configuration) to the audit server. Each profile can be configured with specific log types and destinations. Using custom filters as in E is possible within a profile, but the application mechanism (policy vs. device log settings) dictates separate profiles here for clean separation.

NEW QUESTION: 13

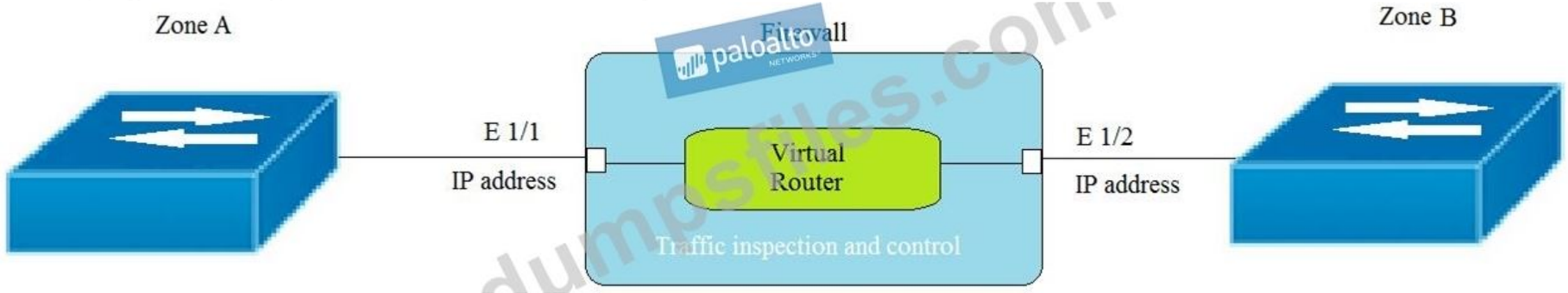
Which Security profile can you apply to protect against malware such as worms and Trojans?
A. data filtering
B. antivirus
C. vulnerability protection
D. anti-spyware
Answer: B (LEAVE A REPLY)
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security- profiles#:~:text=Antivirus%
20profiles%20protect%20against%20viruses,as
%20well%20as%20spyware%20downloads

NEW QUESTION: 14
A Palo Alto Networks Network Security Analyst notices a pattern of 'DNS sinkhole' logs in the Log Viewer. These logs indicate internal hosts attempting to resolve known malicious domains, and the firewall is successfully redirecting these requests to the configured sinkhole IP. However, no corresponding 'critical' or 'high' severity alerts are appearing on the Incidents and Alerts page, despite the potential severity of internal compromise. What configuration element is MOST likely missing or misconfigured that would prevent these sinkhole events from generating an incident?
A. The DNS Proxy setting on the firewall is not enabled, preventing proper sinkholing.
B. The Anti-Spyware profile applied to the relevant security policy does not have the 'DNS Sinkhole' action set to 'alert' or 'block' for the respective threat category.
C. The Log Fomarding profile is not configured to send 'threat' logs with 'severity: high' to the Cortex Data Lake for incident correlation.
D. The WildFire Analysis profile is not enabled for DNS traffic, so no verdict is generated.
E. The Security Policy rule allowing DNS traffic has its 'Action' set to 'allow' instead of 'allow-log'.
Answer: B (LEAVE A REPLY)
DNS Sinkholing is a feature of the Anti-Spyware profile. For DNS sinkhole events to generate alerts and incidents, the Anti-Spyware profile applied to the security policy allowing the DNS traffic must be configured to take an 'alert' or 'block' action when a DNS sinkhole event occurs. If the action is set to 'default' and the default does not include alerting, or if it's set to 'allow' without logging an alert, then no incident will be generated, even if the sinkholing itself is successful and logged. Option A is incorrect because sinkholing is occurring and logs are generated. Option C is plausible if no threat logs were generated at all, but here logs exist, just not alerts. Option D is irrelevant to basic DNS sinkhole alerting. Option E affects logging, but not the generation of an alert from a security profile's action.

NEW QUESTION: 15
Which action ensures that sensitive information such as medical records, financial transactions, and legal communications are not decrypted and that they maintain strong security?
A. Create a log forwarding filter to exclude sensitive information.
B. Disable decryption globally to avoid exposing sensitive data.
C. Create an SSL Inbound Inspection policy to identify users sending sensitive information.
D. Create a no-decrypt policy for traffic matching specific URL categories.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
In a Palo Alto Networks environment, decryption is essential for visibility, but legal and compliance requirements often dictate that certain types of traffic-specifically those involving sensitive personal data- must remain encrypted. To comply with these regulations while still inspecting other high-risk traffic, a Network Security Analyst should create a "no-decrypt" policy for traffic matching specific URL categories (D).
Palo Alto Networks provides predefined URL categories such as financial-services, health-and-medicine, and government. When these categories are used as matching criteria in a Decryption Policy rule with the action set to "No Decrypt," the firewall will bypass the SSL/TLS decryption process for that specific traffic.
This ensures that the privacy of sensitive transactions, like medical records or banking, is maintained and that the raw data is never exposed in the firewall's memory or logs.
Furthermore, to maintain "strong security" as requested, the analyst should attach a Decryption Profile to this no-decrypt rule. This profile can be configured to block sessions that use weak protocols (like SSLv3 or TLS 1.0) or expired certificates, ensuring that even if the traffic is not decrypted, it is still forced to meet modern security standards before entering or leaving the network.

NEW QUESTION: 16
Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?
A. override
B. authorization
C. authentication
D. continue
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url- filteringprofile-actions.html

NEW QUESTION: 17
Given the topology, which zone type should zone A and zone B to be configured with?



A. Layer2
B. Tap
C. Layer3
D. Virtual Wire
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
In the context of Palo Alto Networks SD-WAN configuration, what is the primary purpose of a Link Tag within an SD-WAN Interface Profile??
A. To assign a unique identifier to each physical interface
B. To group multiple physical links for traffic distribution and path selection
C. To define the security policies applied to SD-WAN interfaces

D. To specify the IP addressing scheme for SD-WAN interfaces?
Answer: (SHOW ANSWER)
In the context of Palo Alto Networks SD-WAN, a Link Tag within an SD-WAN Interface Profile is primarily used to group multiple physical links that are part of the same logical connection. This grouping allows for traffic distribution across these links and enables intelligent path selection for routing traffic based on performance, link health, and other criteria.
Link tags help in managing multiple WAN links, allowing the firewall to evaluate which path to use for traffic flow based on the defined SD-WAN policies.

NEW QUESTION: 19
A network administrator creates an intrazone security policy rule on a NGFW. The source zones are set to IT. Finance, and HR.
To which two types of traffic will the rule apply? (Choose two.)
A. Within zone HR
B. Within zone IT
C. Between zone IT and zone HR
D. Between zone IT and zone Finance
Answer: (SHOW ANSWER)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTHCA0

NEW QUESTION: 20
There are intermittent connectivity issues between two internal zones on a PA-Series firewall.
Although the Security policies appear correctly configured, traffic between the zones is experiencing unexpected drops. Which troubleshooting step will isolate the root cause of this behavior?
A. Use the PAN-OS GUI Troubleshooting tool to review interface status, verify zone assignments, and confirm that all links are operational.
B. Use the CLI command show system state filter sys.s1.* | match Error to find interface errors across all the interfaces.
C. Use the CLI command tcpdump filter and set the source and destination zones in the filter to capture and analyze traffic flows between zones, checking for packet loss on the data plane.
D. Use the CLI command show system info to monitor CPU and memory usage, ensuring that resource constraints are not causing interfaces to drop packets between zones.
Answer: (SHOW ANSWER)
A packet capture targeted to the source and destination zones lets you directly observe whether packets enter and leave the firewall as expected and where they are being lost. This isolates whether the drops are occurring on the data plane during forwarding/inspection versus being caused by link state or management-plane visibility.

NEW QUESTION: 21
Assume a custom URL Category Object of "NO-FILES" has been created to identify a specific website How can file uploading/downloading be restricted for the website while permitting general browsing access to that website?
A. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate File Blocking profile
B. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate Data Filtering profile
C. Create a Security policy with a URL Filtering profile that references the site access setting of block to NO-FILES
D. Create a Security policy with a URL Filtering profile that references the site access setting of continue to NO-FILES
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
Where within the URL Filtering security profile must a user configure the action to prevent credential submissions?
A. URL Filtering > Inline Categorization
B. URL Filtering > Categories
C. URL Filtering > URL Filtering Settings
D. URL Filtering > HTTP Header Insertion

Answer: B (LEAVE A REPLY)
URL filtering technology protects users from web-based threats by providing granular control over user access and interaction with content on the Internet. You can develop a URL filtering policy that limits access to sites based on URL categories, users, and groups. For example, you can block access to sites known to host malware and prevent end users from entering corporate credentials to sites in certain categories.

NEW QUESTION: 23
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

			Source		Destination				
	Name	Type	Zone	Address	Zone	Address	Application	Service	Action
1	inside-portal	universal	inside	any	outside	203.0.113.20	any	any	Allow
2	internal-inside-dmz	universal	inside	any	dmz	any	ftp ssh ssl web-browsing	application-default	Allow
3	egress-outside	universal	inside	any	outside	any	any	application-default	Allow
4	egress-outside-content-id	universal	inside	any	outside	any	any	application-default	Allow
5	danger-simulated-traffic	universal	danger	any	danger	any	any	application-default	Allow
6	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	Allow
7	intrazone-default	intrazone	any	any	any	any	any	any	Deny

A. internal-inside-dmz
B. engress outside
C. intercone-default
D. inside-portal
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
In Strata Cloud Manager (SCM), which logical container is used to group firewalls that share the same configuration requirements, such as those at a specific regional office?
A. Template Stacks
B. Snippets
C. Folders
D. Device Groups
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
In the SCM management architecture, Folders are the primary organizational units used to manage both policies and network settings for groups of firewalls. Folders replace the separate "Device Group" and "Template" hierarchy found in traditional Panorama deployments, providing a more streamlined "Unified Policy" approach.
Folders support inheritance, meaning an analyst can define a "Global" folder with company-wide policies and then create sub-folders (e.g., "Region-North") that inherit those global rules while adding region-specific configurations. This structure allows the analyst to manage hundreds of devices as a single entity, ensuring consistency across the fleet. Understanding the SCM folder structure is a core objective for analysts migrating to cloud-based management, as it is the foundation for scaling security operations without increasing complexity.

NEW QUESTION: 25

With Strata Cloud Manager (SCM) or Panorama, customers can monitor and manage which three solutions?
(Choose three.)
A. Prisma Access
B. Prisma Cloud
C. Cortex XSIAM
D. NGFW
E. Prisma SD-WAN
Answer: A,D,E (LEAVE A REPLY)
* Prisma Access (Answer A):
* Strata Cloud Manager (SCM) and Panorama provide centralized visibility and management for Prisma Access, Palo Alto Networks' cloud-delivered security platform for remote users and branch offices.
* NGFW (Answer D):
* Both SCM and Panorama are used to manage and monitor Palo Alto Networks Next- Generation Firewalls (NGFWs) deployed in on-premise, hybrid, or multi-cloud environments.
* Prisma SD-WAN (Answer E):
* SCM and Panorama integrate with Prisma SD-WAN to manage branch connectivity and security, ensuring seamless operation in an SD-WAN environment.
* Why Not B:
* Prisma Cloud is a distinct platform designed for cloud-native security and is not directly managed through Strata Cloud Manager or Panorama.
* Why Not C:
* Cortex XSIAM (Extended Security Intelligence and Automation Management) is part of the Cortex platform and is not managed by SCM or Panorama.
References from Palo Alto Networks Documentation:
* Strata Cloud Manager Overview
* Panorama Features and Benefits

NEW QUESTION: 26
An analyst is configuring a security policy to allow an application that uses a dynamic range of ports. Instead of opening a wide range of ports, which Palo Alto Networks feature should be leveraged to identify the application based on its unique payload?
A. Service Objects
B. App-ID
C. Custom URL Categories
D. Dynamic Address Groups
Answer: (SHOW ANSWER)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
The core objective of a Palo Alto Networks analyst is to move away from legacy port-based rules toward an application-aware security posture. App-ID is the proprietary traffic classification technology that identifies applications traversing the network regardless of the port, protocol, or encryption used.
When an application uses dynamic ports (such as various peer-to-peer or modern web applications), relying on Service Objects (Option A) would require opening a vast range of ports, which increases the attack surface. By using App-ID, the analyst can specify the exact application in the security policy. The firewall's data plane performs multiple layers of analysis-including application signatures, protocol decoding, and heuristics-to identify the traffic. Once identified, the firewall allows only that specific application, even if it shifts to a different port during the session. This ensures a "Positive Enforcement Model" where only sanctioned applications are permitted, effectively neutralizing attackers who try to hide malicious traffic on non-standard ports.

NEW QUESTION: 27
Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

TYPE	FROM ZONE	TO ZONE	INGRESS I/F	SOURCE	NAT APPLIED	EGRESS I/F	DESTINATION	TO PORT	APPLICATION	ACTION	SESSION END REASON	BYTES	ACTION SOURCE	LOG ACTION	BYTES SENT	BYTES RECEIVED	LOG TYPE
end	LAN	internet	ethernet1/2	192.168.200.100	yes	ethernet1/5	198.54.12.97	443	web-browsing	allow	threat	3.3k	from-policy	default	2.7k	541	traffic

A. The web session was unsuccessfully decrypted.
B. The traffic was denied by URL filtering.
C. The traffic was denied by security profile.
D. The web session was decrypted.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 28
Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?
A. Data redistribution
B. Dynamic updates
C. Service route
D. SNMP setup
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
The firewall sends employees an application block page when they try to access Youtube.
Which Security policy rule is blocking the youtube application?

	Name	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. intrazone-default
B. interzone-default
C. Deny Google
D. allowed-security services
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
A Palo Alto Networks firewall is performing SSL Forward Proxy decryption. An analyst observes that certain legitimate SaaS applications (e.g., specific Microsoft 365 services) are experiencing intermittent connectivity issues when decryption is enabled, despite having valid certificates. After reviewing the traffic logs, the analyst sees 'Application not recognized' or 'Unknown' for these connections. Which advanced decryption profile setting is most likely to resolve this issue without disabling decryption entirely for these critical applications?
A. Disabling 'Block Session on Certificate Status' to ignore certificate errors for these applications.
B. Enabling 'Forward Untrusted Certificates' in the SSL Forward Proxy profile and adding the SaaS application domains to a custom URL category that is exempted from decryption.
C. Configuring the Decryption Profile to 'No Decryption' for the specific SaaS application URLs/IPs.

D. Leveraging the 'SSL Decryption Exclusion' list within the Decryption Profile by adding the FQDNs of the problematic SaaS applications.
E. Adjusting the 'Minimum Protocol Version' to TLS 1.0 to increase compatibility.
Answer: D (LEAVE A REPLY)
Certain applications, particularly those that employ certificate pinning or have complex TLS implementations (like some Microsoft 365 services), can break when subjected to SSL Fomard Proxy decryption. The 'SSL Decryption Exclusion' list within the Decryption Profile (under 'SSL Forward Proxy') is specifically designed for this purpose. By adding the FQDNs of these sensitive applications to this list, the firewall will automatically bypass decryption for traffic destined to those domains, allowing the original TLS session to proceed directly to the destination without interruption. This is more granular and preferred over broad 'No Decryption' rules.

NEW QUESTION: 31
When creating a custom URL category object, which is a valid type?
A. category match
B. host names
C. wildcard
D. domain match
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?
A. SAML
B. Multi-Factor Authentication
C. Role-based
D. Dynamic
Answer: (SHOW ANSWER)
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage- firewall-administrators/administrative-role-types.html

NEW QUESTION: 33
At which point in the app-ID update process can you determine if an existing policy rule is affected by an app- ID update?
A. after clicking Check New in the Dynamic Update window
B. after connecting the firewall configuration
C. after downloading the update
D. after installing the update
Answer: A (LEAVE A REPLY)
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device- dynamicupdates

NEW QUESTION: 34
Which prevention technique will prevent attacks based on packet count?

A. antivirus profile
B. vulnerability profile
C. URL filtering profile
D. zone protection profile
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
An analyst notices latency on the firewall and wants to improve performance. Which steps can be taken to reduce management plane CPU while working to determine the underlying problem?
A. Disable log at session start and only log at session end.
B. Enable logging for intrazone-default and interzone-default security rules.
C. Disable log at session end and only log at session start.
D. Enable log forwarding from the firewall to an external destination.
Answer: (SHOW ANSWER)
Logging at session start increases log generation frequency and management plane processing overhead. Disabling session-start logging and keeping only session-end logging reduces the number of logs created during active sessions, lowering management plane CPU utilization while you investigate the root cause.

NEW QUESTION: 36
Which log type is the most useful for identifying if a user is repeatedly attempting to visit an "Unauthorized" website category that is being blocked by a security profile?
A. Traffic Log
B. URL Filtering Log
C. System Log
D. Authentication Log
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
While Traffic Logs show that a connection was denied, the URL Filtering Log provides the specific context required to understand why it was denied. It explicitly lists the URL being visited, the specific URL category (e.g., adult or gambling), and the action taken by the profile.
For a Network Security Analyst, monitoring this log is a core objective for identifying potential "insider threats" or users who require additional security training. If a host is generating hundreds of "block" entries for high-risk categories in a short period, it could indicate that the device is infected with malware that is attempting to "call home" to a malicious site or that a user is actively trying to bypass security controls.

NEW QUESTION: 37
Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?
A. Virtual Wire
B. Tap
C. Layer 3
D. Layer 2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 38
A Security Administrator is tasked with preventing the exfiltration of sensitive HR data (e.g., employee salaries, national ID numbers) from the internal network through unencrypted channels. They have identified that this data often appears within PDF and Microsoft Office documents. Which combination of Palo Alto Networks security profiles and policy configurations would be most effective in addressing this specific data exfiltration risk, while minimizing false positives?

A. Enable 'WildFire Analysis' on the outbound security policy for unknown file types and configure a custom URL Filtering profile to block access to cloud storage sites.
B. Create a 'Data Filtering' profile with a 'File Blocking' rule for PDF and Office documents, and apply it to a 'Security Policy' rule allowing outbound traffic.
C. Configure a 'Data Filtering' profile utilizing 'Predefined Data Patterns' for PII and 'Custom Data Patterns' for specific HR document keywords, then apply this profile to a 'Security Policy' rule with 'Action: Block' and 'Log at Session End'.
D. Implement an 'Antivirus' profile with strict heuristics and an 'Anti-Spyware' profile on all outbound security policies, and enable 'SSL Decryption' for all outbound traffic.
E. Utilize a 'Vulnerability Protection' profile with a 'Strict' setting and an 'Anti-Spyware' profile for outbound traffic, focusing on signature-based detection.
Answer: (SHOW ANSWER)
Option C is the most effective. 'Data Filtering' is specifically designed for preventing sensitive data exfiltration. Using 'Predefined Data Patterns' covers common PII, and 'Custom Data Patterns' allows for highly specific detection of HR-related keywords within documents. Applying this profile with a 'Block' action on outbound security policies directly addresses the exfiltration risk. Logging helps with auditing. Other options are less targeted: WildFire is for malware, File Blocking might be too broad, Antivirus/Anti-Spyware/Vulnerability Protection are for threats, not data content.

NEW QUESTION: 39
A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?
A. PAN-OS integrated agent
B. Windows-based agent on a domain controller
C. Captive Portal
D. Citrix terminal server with adequate data-plane resources
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which object would an administrator create to block access to all high-risk applications?
A. HIP profile
B. application filter
C. application group
D. Vulnerability Protection profile
Answer: B (LEAVE A REPLY)
Explanation/Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKECA0

NEW QUESTION: 41
A security analyst is reviewing an SD-WAN profile implemented via Panorama'. They notice an SD-WAN policy rule structured as follows:

```
<name>Critical_Traffic_SLA</name>
<application>SAP_DB</application>
<source>any</source>
<destination>any</destination>
<path-selection>
  <performance-based>
    <profile>High_Availability_SLA</profile
    <active-backup>
      <path>ethernet1/1.100</path>
      <path>ethernet1/1.200</path>
    </active-backup>
  </performance-based>
</path-selection>
<qos-profile>High_Priority_QoS</qos-profile
<priority>1</priority>
```

Given this configuration, what potential issues or limitations should the analyst be aware of regarding how 'SAP DB' traffic will behave under varying network conditions, and what key components are implicitly assumed or missing for this rule to function optimally?

A. The 'active-backup' configuration directly specifies interfaces (ethernet1/1. 100, ethernet1/1 .200) instead of SD-WAN links, which might lead to incorrect path selection if these interfaces are part of multiple SD-WAN links.

B. The 'High_Availability_SLA' performance profile must explicitly define 'Good' and 'Bad' thresholds for latency, jitter, and packet loss. If the 'active' path

C. This configuration assumes that 'Path Monitoring' profiles are correctly configured for both 'ethernet1/1. 100' and 'ethernet1/1 .200' to continuously assess their real-time quality metrics against the 'High_Availability_SLA' profile.

D. The 'qos-profile' specified ('High_Priority_QoS') will only apply if bandwidth management policies are also configured on the egress interfaces of the firewall, otherwise it primarily marks traffic but doesn't guarantee bandwidth.

E. The 'active-backup' selection with 'performance-based' ensures that traffic will only use 'ethernet1/1. 100' until its performance degrades past the SLA. It will not dynamically switch back to 'ethernet1/1. 100' even if it recovers, unless a 'failback' mechanism is configured (which is not explicit here).

Answer: B,C,D (LEAVE A REPLY)

Option B is correct. 'Performance-based' path selection relies on the 'Good' threshold of the associated 'Path Quality' (SLA) profile. If the active path's metrics fall below 'Good', it triggers a failover. Option C is correct. Path Monitoring is fundamental for SD-WAN; without it, the firewall cannot gather the real-time metrics needed to evaluate against the SLA. Option D is correct. A QOS profile alone primarily marks traffic; actual bandwidth enforcement requires bandwidth management policies on the egress interfaces. Option A is incorrect. In Palo Alto Networks SD-WAN, 'path' in 'active-backup' or 'preferred-path' contexts within SD-WAN policy rules refers to configured SD-WAN links, which are associated with interfaces. So, specifying the interface name is correct for identifying the link. Option E is incorrect. 'Performance-based' path selection does support failback by default (it will revert to the preferred path once its quality returns to 'Good'), unless a specific 'sticky' or 'no-failback' option is configured (which is not shown here).

NEW QUESTION: 42

A security administrator wants to determine which action a URL Filtering profile will take on the URL "www.chatgpt.com." The firewall has a custom URL object with "www.chatgpt.com/" as a member called "Permitted-AI." The URL "www.chatgpt.com" is also categorized as "Artificial- Intelligence, " "Computer-and-Internet-Info," and "Low-Risk." The URL Filtering profile has the following in descending order:

- Artificial-Intelligence set to continue
- Computer-and-Internet-Info set to block
- Low-Risk set to alert
- Permitted-AI set to allow

Which action will the URL Filtering profile take when traffic matches the "www.chatgpt.com" URL on a rule with this profile attached?

A. Continue

B. Alert

C. Allow

D. Block

Answer: (SHOW ANSWER)

Custom URL categories take precedence over predefined URL category matches in the profile evaluation. Since the URL is explicitly included in the custom object mapped to an allow action, that rule is applied before the standard category actions, resulting in the traffic being permitted.

NEW QUESTION: 43
An organization relies heavily on Palo Alto Networks firewalls for perimeter security. They want to implement a custom Threat Signature to detect a highly evasive malware strain that attempts to communicate over HTTP/S using a specific pattern in its TLS Client Hello extension (e.g., a unique, non-standard extension value or an unusual ordering of standard extensions). The challenge is that the malware changes its C2 domain frequently, and traditional URL/DNS blacklisting is ineffective. Which type of custom signature and what specific 'Location' for the pattern match would be most appropriate for this detection, assuming the pattern is 'malware_tls_signature_bytes' and is located within the 'client_hello_extensions' field?
A. Signature Type: Vulnerability, Location: 'tcp-payload'
B. Signature Type: Spyware, Location: 'ssl-client-hello'
C. Signature Type: Custom Threat, Location: 'ssl-client-hello-extensions'
D. Signature Type: DoS, Location: 'tls-handshake'
E. Signature Type: Protocol Anomaly, Location: 'http-request-headers'
Answer: C (LEAVE A REPLY)
This question targets advanced custom signature creation, specifically focusing on TLS handshake details. The key is detecting a pattern within the 'TLS Client Hello extension'. Signature Type: Custom Threat - This is the general category for detecting specific malicious patterns not covered by pre-defined signatures. While 'Vulnerability' or 'Spyware' could potentially be used for broader malware, 'Custom Threat' is designed for specific, targeted threat detection. Location: 'ssl-client-hello-extensions' - This is the crucial part. Palo Alto Networks custom signatures offer specific 'Locations' to target different parts of network protocols. To inspect details within the TLS Client Hello extensions , the 'ssl-client-hello-extensions' location is the precise target. 'ssl-client-hello' would match the entire Client Hello, but 'ssl-client-hello-extensions' provides a more granular context for patterns specifically within the extensions field, which is what the problem describes. Let's review other options: A. Signature Type: Vulnerability, Location: 'tcp-payload' : 'tcp-payload' is too broad; it inspects the entire TCP payload, which would be inefficient and prone to false positives if the pattern is specific to TLS handshake elements. 'Vulnerability' is generally for exploits. B. Signature Type: Spyware, Location: 'ssl-client-hello' : While 'ssl-client-hello' is closer, it's less specific than 'ssl-client-hello-extensions' if the goal is to target patterns within the extensions. 'Spyware' is a valid threat category, but the location precision is important here. D. Signature Type: DoS, Location: 'tls-handshakes : DoS signatures are for denial-of-service attacks. 'tls-handshake' is a valid location but 'ssl-client-hello-extensions' is even more granular and accurate for the specific problem. E. Signature Type: Protocol Anomaly, Location: 'http-request-headers' : Protocol Anomaly signatures detect deviations from RFCs. 'http-request-headers' is for HTTP headers, not TLS handshake details.

NEW QUESTION: 44
Which the app-ID application will you need to allow in your security policy to use facebook-chat?
A. facebook
B. facebook-base
C. facebook-chat
D. facebook-email
Answer: (SHOW ANSWER)

NEW QUESTION: 45

An administrator is updating Security policy to align with best practices.

Which Policy Optimizer feature is shown in the screenshot below?

A. New App Viewer

B. Unused Unused Apps

C. Rule Usage

D. Rules without App Controls

Answer: C (LEAVE A REPLY)

NEW QUESTION: 46

You are deploying a new application on a Palo Alto Networks firewall and need to create a custom Application (App-ID) for it. The application communicates over TCP port 8443, uses TLS, and sends a specific HTTP header 'X-App-ID: MyWebApp' in all its requests. The application also uses a unique URI path structure, To ensure the most accurate and robust App-ID, which custom application signature configuration would be most appropriate?

A. Signature Type: `http`, Pattern Context: `http-request-headers`, Pattern: `X-App-ID: MyWebApp`, Port: `tcp/8443`

B. Signature Type: `ssl`, Pattern Context: `ssl-server-hello`, Pattern: `MyWebApp`, Port: `tcp/8443`

C. Signature Type: `http`, Pattern Context: `http-request-uri`, Pattern: `^/mywebapp/api/v2/secure/. $`, Port: `tcp/8443`

D. Signature Type: `ssl`, Pattern Context: `any`, Pattern: `MyWebApp`, Port: `tcp/8443`

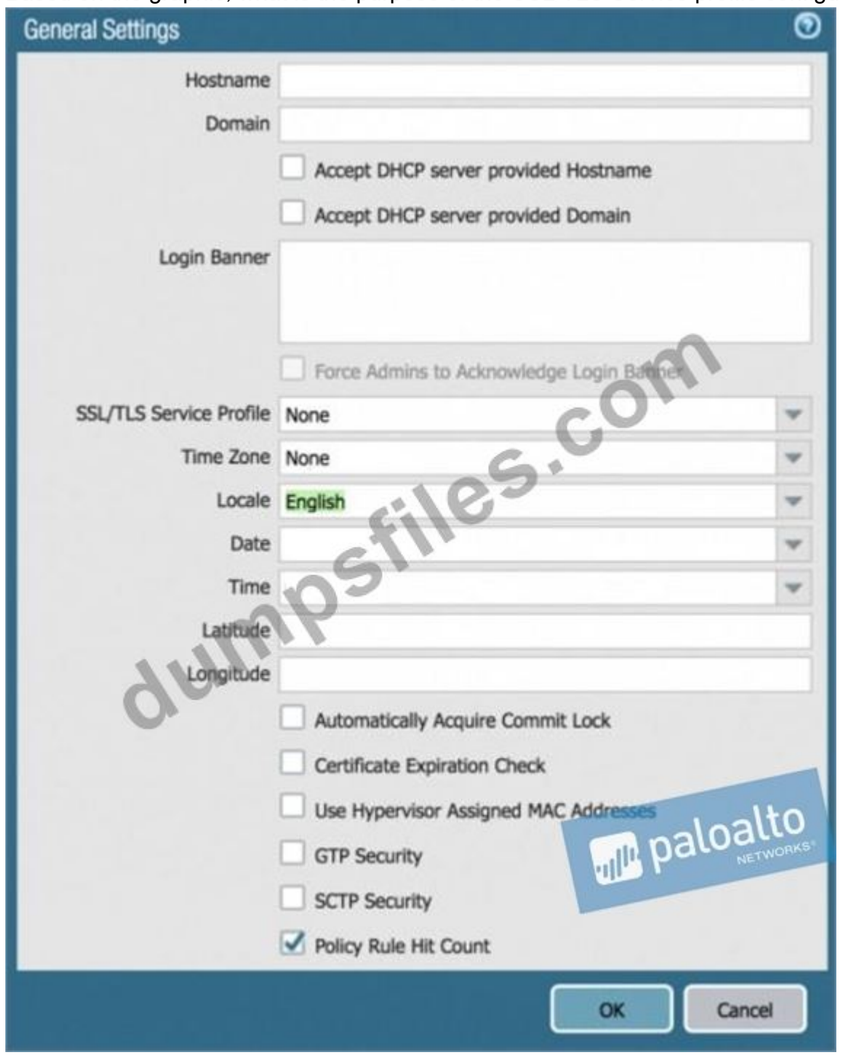
E. Signature Type: `http`, Pattern Context: `http-request-headers` (for `X-App-ID: MyWebApp`) OR Pattern Context: `http-request-uri` (for `^/mywebapp/api/v2/secure/. $`), Port: `tcp/8443`, with 'AND' condition between header and URI for higher confidence.

Answer: E (LEAVE A REPLY)

This question assesses the ability to create robust custom App-IDs by combining multiple matching criteria for higher confidence. Analysis of Requirements: TCP port 8443 Uses TLS Specific HTTP header: 'X-App-ID: MyWebApp' Unique URI path: Evaluation of Options: A: Detects the header, but only relies on one element. This is good but can be improved for robustness. B: 'ssl-server-hello' context is for inspecting the TLS handshake, not application-layer HTTP headers or URIs. Also, 'MyWebApp' might not appear directly in the server hello. C: Detects the URI path, but only relies on one element. Good, but can be improved. D: any' pattern context with 'ssr type and just 'MyWebApp' as pattern is too broad and likely to cause false positives. 'MyWebApp' could appear anywhere in the TLS payload. E (Correct): This option proposes combining the header and URI patterns using an 'AND' logic. Palo Alto Networks custom App-IDs support combining multiple patterns. This is the most robust approach because it requires both the unique header and the unique URI structure to be present. This significantly reduces the chance of false positives compared to relying on just one of these elements, while still correctly identifying the application. The App-ID will first identify the session as SSL/TLS (implicitly due to port 8443 and the nature of the application) and

then, after decryption (if configured), it will look for the HTTP-layer patterns. The type remains Shttps for matching HTTP-layer attributes, and the port is 'tcp/8443'. The ability to define multiple patterns with AND/OR logic within a single custom App-ID provides this precision.

NEW QUESTION: 47
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?



A. It defines the SSUTLS encryption strength used to protect the management interface.
B. It defines the CA certificate used to verify the client's browser.
C. It defines the certificate to send to the client's browser from the management interface.
D. It defines the firewall's global SSL/TLS timeout values.
Answer: C (LEAVE A REPLY)
Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFGCA0

NEW QUESTION: 48
When using Strata Cloud Manager (SCM), which tool allows an analyst to automatically migrate local firewall configurations to a centralized management folder?
A. Strata Cloud Manager Transition
B. Policy Optimizer
C. Config Audit
D. Template Variable
Answer: (SHOW ANSWER)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
The Strata Cloud Manager Transition tool is specifically designed to facilitate the migration of local, standalone firewall configurations into the SCM centralized management framework. This is a critical workflow for analysts moving toward a "unified management" model.
The tool analyzes the existing local configuration-including objects, policies, and network settings-and maps them to the appropriate Folders and Snippets within SCM. This ensures that the local "Source of Truth" is successfully shifted to the cloud management plane without losing granular security settings. During this process, the analyst can identify and resolve naming conflicts or redundant objects, cleaning up the configuration as it is centralized.
Transitioning firewalls into SCM is a key objective as it unlocks AI-powered monitoring, centralized auditing, and simplified lifecycle management across the entire global estate.

NEW QUESTION: 49
A company is implementing a zero-trust architecture. As part of this, they need to restrict SSH access to their critical production servers. Specifically, SSH access should only be permitted from a jump host and only if the SSH client is running a specific, approved version. All other SSH attempts, even from the jump host, should be denied if the client version does not match. Which combination of Palo Alto Networks features would enable this level of granular control?
A. Security Policy for Source IP of Jump Host, Destination IP of Production Servers, Application 'ssh', and a 'File Blocking' profile to block unapproved SSH versions.
B. User-ID for authenticated jump host users, a Security Policy with Source IP of Jump Host, Destination IP of Production Servers, Application 'ssh', and a 'URL Filtering' profile to inspect SSH client strings.
C. Security Policy with Source IP of Jump Host, Destination IP of Production Servers, Application 'ssh'. Additionally, create a 'Custom Application' signature (or leverage an existing application's capabilities if available) that matches the specific SSH client version string within the SSH protocol handshake, then apply this custom application in the policy with an 'Allow' action.
D. GlobalProtect with Host Information Profile (HIP) checks to verify the SSH client version on the jump host, combined with a Security Policy allowing traffic based on HIP match.
E. Deploy a 'Vulnerability Protection' profile with a custom signature to detect the unapproved SSH client versions and apply it to the outbound security policy from the jump host.
Answer: (SHOW ANSWER)
Option D is the most robust and accurate solution for this complex scenario. While Option C might seem plausible for creating a custom application signature, inspecting SSH client versions often falls under the purview of endpoint posture assessment. GlobalProtect's Host Information Profile (HIP) is specifically designed to collect detailed information about the connecting endpoint, including installed software versions (like SSH clients). This HIP data can then be used as a match criterion in security policies. This allows dynamic enforcement based on the endpoint's compliance rather than relying solely on network-level signatures which might be brittle or difficult to maintain for specific software versions across all vendors. Option C (Custom Application) would be the next best, but HIP is designed for this specific type of endpoint posture enforcement. Others are irrelevant: File Blocking, URL Filtering are not for SSH client versions, and Vulnerability Protection is for exploits, not client version enforcement.

NEW QUESTION: 50
Which definition describes the guiding principle of the zero-trust architecture?
A. never trust, never connect

B. always connect and verify
C. never trust, always verify
D. trust, but verity
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference:
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

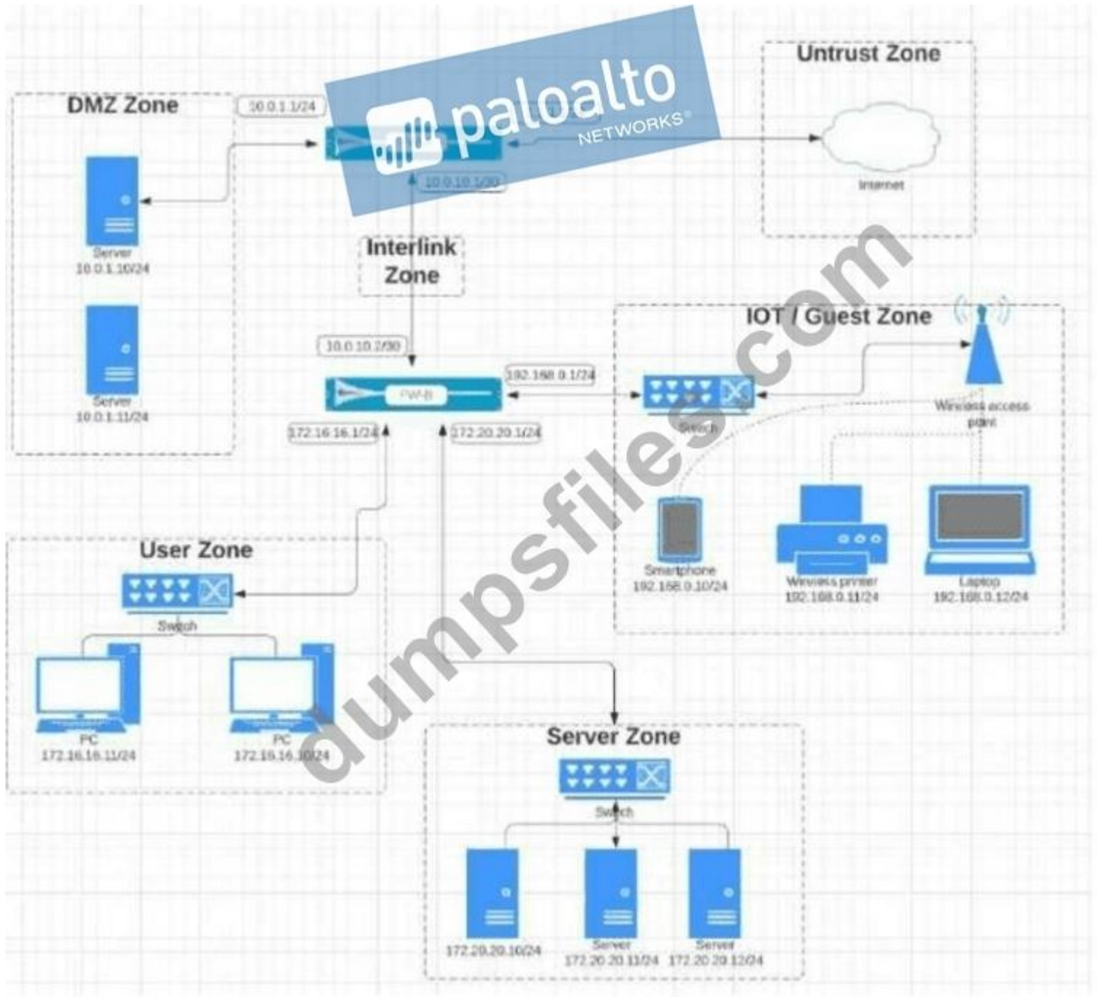
NEW QUESTION: 51
A Palo Alto Networks firewall is experiencing frequent 'URL Filtering: category-not-resolved' errors in the traffic logs, leading to inconsistent web access for users. The firewall has valid subscriptions for URL Filtering and DNS Proxy is configured. The external DNS servers are reachable. Which of the following is the MOST LIKELY cause of this issue, and what specific configuration element should be scrutinized?
A. The URL Filtering license has expired, preventing category lookups. Check 'Device > Licenses' for the URL Filtering license status.
B. The firewall is unable to reach the Palo Alto Networks URL Filtering cloud database. Verify connectivity to update servers (update.paloaltonetworks.com) and check 'Device > Dynamic Updates' for URL database status.
C. The DNS Proxy configuration is incorrectly routing DNS queries for URL lookups through an internal DNS server that cannot resolve external URLs. Review 'Network > DNS Proxy' and ensure 'DNS Proxy Rule' for Palo Alto Networks Services' is correctly configured.
D. The URL Filtering profile applied to the security policy has an action of 'alert' or 'allow' for 'unknown' categories, but the default action for 'category-not-resolved' is implicit deny. Review 'Objects > URL Filtering Profile > <Profile Name> > Categories'.
E. There is a routing issue preventing the firewall from sending DNS requests for URL resolution to its configured DNS servers. Check 'Network > Virtual Routers > <Router Name> > Static Routes' and 'Network > DNS' settings.
Answer: B (LEAVE A REPLY)
'category-not-resolved' specifically indicates that the firewall tried to look up a URL's category but failed to get a response from the URL filtering cloud service. While DNS is involved, the primary reason for this specific message, assuming licenses are valid (A) and basic DNS is working, is a connectivity issue between the firewall and the Palo Alto Networks URL filtering cloud. This could be due to routing, an intermediate firewall blocking the connection, or an issue on the cloud side itself. Option B points directly to verifying this critical connection and dynamic update status. Option C relates to DNS proxy but primarily for client DNS, not the firewall's internal URL lookup. Option D is about policy action, not the lookup failure itself. Option E is broader DNS routing, but B is more direct for the specific 'category-not-resolved' error.

NEW QUESTION: 52
Which action would an administrator take to ensure that a service object will be available only to the selected device group?
A. create the service object in the specific template
B. uncheck the shared option
C. ensure that disable override is selected
D. ensure that disable override is cleared
Answer: D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-device-groups
/create-objects-for-use-in-shared-or-device-group-policy

NEW QUESTION: 53
An analyst wants to create a custom application for an internal tool that uses a specific proprietary protocol. Which information is required to ensure the firewall correctly identifies this application using App-ID?
A. Source and Destination IP addresses.
B. Signature patterns found in the packet payload.
C. The URL category of the server.
D. The MAC address of the server.
Answer: B (LEAVE A REPLY)

App-ID is the core technology that allows Palo Alto Networks firewalls to identify applications regardless of the port or protocol they use. For standard applications, these signatures are provided by Palo Alto Networks. However, for proprietary internal tools, an analyst must create a Custom Application.
The most critical component of a custom application is the Signature. This involves identifying a unique pattern in the packet payload--such as a specific hex string or text identifier--that only appears when this specific application is running. The analyst uses the "Signature" tab in the Application object to define these patterns and specify where in the packet the firewall should look for them (e.g., the HTTP header or the TCP payload). By defining a signature, the firewall can move beyond simple port-based blocking and apply full Layer 7 security inspection to the custom traffic, ensuring that the proprietary tool is not used as a cover for malicious activity.

NEW QUESTION: 54
Review the Screenshot:



Given the network diagram, traffic must be permitted for SSH and MYSQL from the DMZ to the SERVER zones, crossing two firewalls. In addition, traffic should be permitted from the SERVER zone to the DMZ on SSH only.
Which rule group enables the required traffic?

A.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
FW-A_RuleGroup-02-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	InterLink	172.20.20.0/24	any	mysql ssh	application-default	any	Allow
FW-B_RuleGroup-02-X	FW-B	universal	InterLink	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql ssh	application-default	any	Allow
FW-A_RuleGroup-02-Y	FW-A	universal	InterLink	172.20.20.0/24	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow
FW-B_RuleGroup-02-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLink	10.0.1.0/24	any	ssh	application-default	any	Allow

B.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
FW-A_RuleGroup-03-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql ssh	application-default	any	Allow
FW-B_RuleGroup-03-X	FW-B	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql ssh	application-default	any	Allow
FW-A_RuleGroup-03-Y	FW-A	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow
FW-B_RuleGroup-03-Z	FW-B	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow

C.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
FW-A_RuleGroup-04-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql ssh	application-default	any	Allow
FW-B_RuleGroup-04-X	FW-B	universal	InterLink	10.0.1.0/24	any	any	Server	172.20.20.0/24	any	mysql ssh	application-default	any	Allow
FW-A_RuleGroup-04-Y	FW-A	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow
FW-B_RuleGroup-04-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLink	10.0.1.0/24	any	ssh	application-default	any	Allow

D.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
FW-A_RuleGroup-01-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	InterLink	10.0.10.0/30	any	mysql ssh	application-default	any	Allow
FW-B_RuleGroup-01-X	FW-B	universal	InterLink	10.0.10.0/30	any	any	Server	172.20.20.0/24	any	mysql ssh	application-default	any	Allow
FW-A_RuleGroup-01-Y	FW-A	universal	InterLink	10.0.10.0/30	any	any	DMZ	10.0.1.0/24	any	ssh	application-default	any	Allow
FW-B_RuleGroup-01-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLink	10.0.10.0/30	any	ssh	application-default	any	Allow

Answer: B (LEAVE A REPLY)
Option B enables the required traffic by allowing SSL and web-browsing from UNTRUST to DMZ, denying SSH from UNTRUST to DMZ, allowing MYSQL from DMZ to SERVER, and allowing SSH from SERVER to DMZ. Option A allows SSH from UNTRUST to DMZ, which is not required. Option C denies all the required traffic. Option D denies all traffic from UNTRUST to TRUST, which is irrelevant to the question
https://www.paloaltonetworks.com/services/education/palo-alto-networks-certified-network-security- administrator

NEW QUESTION: 55
Your company is highly concerned with their Intellectual property being accessed by unauthorized resources.
There is a mature process to store and include metadata tags for all confidential documents.
Which Security profile can further ensure that these documents do not exit the corporate network?
A. File Blocking
B. Data Filtering
C. Anti-Spyware
D. URL Filtering
Answer: B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles- data-filtering

NEW QUESTION: 56
A critical server application relies on a set of custom web services running on non-standard ports. The security team needs to ensure that these specific web services are protected by comprehensive threat prevention, including WildFire analysis, but without impacting the performance of other high-volume, less critical HTTP/S traffic. The firewall must distinguish between these custom services and standard HTTP/S. Which approach offers the most efficient and secure configuration?
A. Create a custom application for each specific web service using a signature-based approach or by specifying the application name (e.g., 'web-browsing') with custom ports. Then, create a single security policy rule for all web traffic (HTTP/S and custom services), and apply a comprehensive Security Profile Group (including WildFire) to this rule.
B. Define a custom application for each non-standard web service, explicitly identifying its port and application type. Create a dedicated security policy rule for these custom applications, allowing traffic from relevant sources to the critical server. To this rule, attach a Security Profile Group containing Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering (tuned for web services), File Blocking, and a WildFire Analysis profile configured for all file types.
C. Configure the existing 'web-browsing' application to include the custom non-standard ports within the service object. Create a security policy rule for this modified 'web-browsing' application, allowing it to the critical server. Apply a comprehensive Security Profile Group (with WildFire) to this rule, and then create a separate, less restrictive policy for general HTTP/S traffic.
D. Utilize policy-based forwarding (PBF) to direct all traffic destined for the critical server through a dedicated Vwire interface. On this Vwire, apply a zone protection profile and a comprehensive Security Profile Group including WildFire. For other HTTP/S traffic, apply standard security policies.

E. Create a service object for each custom port. Define a security policy rule allowing these service objects to the critical server. Apply a Security Profile Group containing Antivirus, Anti-Spyware, Vulnerability Protection, and a WildFire Analysis profile. For standard HTTP/S traffic, apply a separate security policy with a less CPU-intensive Security Profile Group.
Answer: (SHOW ANSWER)
Option B is the most efficient and secure approach. By defining custom applications for the non-standard web services, the firewall can accurately identify and classify this specific traffic, even on non-standard ports. This allows for the creation of a dedicated security policy rule with granular source/destination/user matching. Applying a comprehensive Security Profile Group (including WildFire) to this specific rule ensures that only the critical web services receive intensive inspection, without impacting general HTTP/S traffic. This granular application of profiles is key to balancing security and performance. Option A is inefficient as it applies comprehensive inspection to all web traffic. Option C modifies a built-in app, which is generally not recommended for such specific requirements and can lead to unintended consequences. Option D involves network topology changes (PBF, Vwire) which are unnecessary for this security profile requirement. Option E uses service objects but doesn't leverage App-ID's ability to classify the application itself, leading to less accurate and potentially less secure identification.

NEW QUESTION: 57
An analyst needs to configure a NAT policy to allow internal users to access the internet. The company only has one public IP address available on the firewall's outside interface. Which NAT type should be used?
A. Static IP
B. Dynamic IP
C. Dynamic IP and Port (DIPP)
D. Bi-directional NAT
Answer: C (LEAVE A REPLY)
In environments with limited public IP addresses, Dynamic IP and Port (DIPP) NAT--also known as Port Address Translation (PAT)--is the standard solution for outbound internet access.
DIPP allows the firewall to translate multiple internal private IP addresses to a single public IP address by assigning a unique source port to each internal session. The firewall maintains a translation table to ensure that returning traffic from the internet is routed back to the correct internal host. This is the most efficient way to provide internet connectivity for a large number of users using a minimal amount of public IP space. For an analyst, configuring DIPP is a core task that involves defining a "Source NAT" rule where the "Original Packet" is the internal subnet and the "Translated Packet" uses the interface address of the firewall's public-facing port.

NEW QUESTION: 58
What are the two default behaviors for the intrazone-default policy? (Choose two.)
A. Deny
B. Logging disabled
C. Allow
D. Log at Session End
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 59
A malware incident involving compromised internal hosts communicating with a command-and- control (C2) server has been resolved. In response, the C2 IP address is blocked. Which two actions using the Log Viewer will ensure the incident has been fully mitigated? (Choose two.)
A. Build and save a custom filter based on the affected endpoints and continue to monitor for suspicious traffic from the endpoints.
B. Review the authentication alerts on the affected devices.
C. Review the audit alerts and check for integrity protection alerts on the affected devices.
D. Continue to monitor for traffic going to the C2 server's IP address.
Answer: (SHOW ANSWER)
Creating and saving a custom filter for the affected endpoints allows continuous monitoring of their activity to detect any remaining or recurring suspicious communications. Monitoring traffic to the blocked C2 IP verifies that no further connections are attempted, confirming that the malicious communication channel has been effectively contained.

NEW QUESTION: 60

Which Security policy match condition would an administrator use to block traffic from IP addresses on the Palo Alto Networks EDL of Known Malicious IP Addresses list?
A. destination address
B. source address
C. destination zone
D. source zone
Answer: (SHOW ANSWER)
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list- in-policy/external-dynamic-list.html

NEW QUESTION: 61
Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?
A. URL traffic
B. anti-spyware
C. antivirus
D. vulnerability protection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62
How often does WildFire release dynamic updates?
A. every 5 minutes
B. every 15 minutes
C. every 60 minutes
D. every 30 minutes
Answer: A (LEAVE A REPLY)
References:

NEW QUESTION: 63
A security analyst is investigating a complex NAT issue on a Palo Alto Networks firewall. An internal application server (172.16.10.10) in the 'DMZ' zone needs to establish a connection to an external third-party API (api.example.com, IP: 198.51.100.20) on port 443. The firewall's 'External' interface has multiple public IP addresses (203.0.113.1, 203.0.113.2). The requirement is that all traffic from 172.16.10.10 to 198.51.100.20 must source NAT to 203.0.113.2, while all other outbound traffic from 172.16.10.10 should source NAT to 203.0.113.1. Additionally, the firewall has the following NAT policies configured (listed in order of evaluation):

```
Rule 1 (Dynamic IP and Port):
  Original Packet:
    Source Zone: DMZ
    Destination Zone: External
    Source Address: 172.16.10.0/24
    Destination Address: Any
  Translated Packet:
    Source Address: Interface Address (External interface)
    Source Port: Dynamic

Rule 2 (Static IP - Specific):
  Original Packet:
    Source Zone: DMZ
    Destination Zone: External
    Source Address: 172.16.10.10
    Destination Address: 198.51.100.20
  Translated Packet:
    Source Address: 203.0.113.2

Rule 3 (Destination NAT - Inbound Web Server):
 Original Packet:
    Source Zone: External
    Destination Zone: DMZ
    Destination Address: 203.0.113.15
 Translated Packet:
    Destination Address: 172.16.10.50
```


When 172.16.10.10 attempts to connect to 198.51.100.20, what will be the effective source IP address for this connection, and why? Assume the External interface's primary IP is 203.0.113.1.

A. 203.0.113.2, because Rule 2 is more specific and therefore evaluated first.

B. 203.0.113.1, because Rule 1 is evaluated first and matches the traffic.

C. The connection will be dropped because of a NAT misconfiguration, preventing any translation.

D. The connection will use a randomly selected IP from the firewall's available public IPs.

E. It depends on the order of security policies, not NAT policies, as NAT is processed after security.

Answer: B (LEAVE A REPLY)

Palo Alto Networks firewalls process NAT rules in the order they appear in the policy list, from top to bottom, and the first match is applied. Rule 1 is a broader rule matching any traffic from 172.16.10.0/24 to 'Any' destination in the 'External' zone. Rule 2 is more specific for 172.16.10.10 to 198.51.100.20. However, since Rule 1 is listed BEFORE Rule 2, the traffic from 172.16.10.10 to 198.51.100.20 will match Rule 1 first, resulting in the source IP being translated to the 'External' interface's primary IP (203.0.113.1). To achieve the desired outcome, Rule 2 should be moved above Rule 1 in the NAT policy list.

NEW QUESTION: 64

Which path is used to save and load a configuration with a Palo Alto Networks firewall?

A. Device>Setup>Management

B. Device>Setup>Operations

C. Device>Setup>Services

D. Device>Setup>Interfaces

Answer: B (LEAVE A REPLY)

NEW QUESTION: 65
Which two options does the firewall use to dynamically populate address group members? (Choose two.)
A. IP Addresses
B. Tags
C. MAC Addresses
D. Tag-based filters
Answer: B,D (LEAVE A REPLY)
A dynamic address group populates its members dynamically using look ups for tags and tag-based filters. Tags are metadata elements or attribute-value pairs that are registered for each IP address. Tag-based filters use logical and and or operators to match the tags and determine the membership of the dynamic address group. For example, you can create a dynamic address group that includes all IP addresses that have the tags "web-server" and "linux". You can also use static tags as part of the filter criteria. Reference: Policy Object: Address Groups, Use Dynamic Address Groups in Policy, Statics vs. Dynamic Address Objects Groups

NEW QUESTION: 66
A security administrator needs to block access to a specific list of 500 malicious domains. These domains are updated daily by a third-party intelligence feed. What is the most efficient way to manage these domains as an object?
A. Create a Custom URL Category and manually paste the domains daily.
B. Create an External Dynamic List (EDL) of type "Domain."
C. Create a Domain-based FQDN Address Group.
D. Add the domains to the "Block List" of a URL Filtering profile.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
For high-volume, frequently changing indicators of compromise (IoCs), manual entry is not scalable. An External Dynamic List (EDL) allows the firewall to automatically import a list of domains from an external web server.
When configured as a "Domain" type EDL, the analyst simply provides the URL of the text file hosted by the intelligence provider. The firewall then periodically retrieves this file (e.g., every 5 minutes or hourly) and updates the security policy in real-time without requiring a configuration commit. This automation is a critical objective for maintaining a proactive security posture. Using an EDL ensures that the perimeter defense is always synchronized with the latest threat intelligence, whereas manual lists (Options A and D) introduce significant administrative overhead and a "security gap" between the time a threat is identified and the time the firewall is updated.

NEW QUESTION: 67
Where in Panorama Would Zone Protection profiles be configured?
A. Shared
B. Templates
C. Device Groups
D. Panorama tab
Answer: B (LEAVE A REPLY)
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/use-templates-to-administer-a-base-configuration

NEW QUESTION: 68
According to a customer's CIO, who is upgrading PAN-OS versions, "Finding issues and then engaging with your support people requires expertise that our operations team can better utilize elsewhere on more valuable tasks for the business." The upgrade project was initiated in a rush because the company did not have the appropriate tools to indicate that their current NGFWs were reaching capacity.
Which two actions by the Palo Alto Networks team offer a long-term solution for the customer? (Choose two.)
A. Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.
B. Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.

C. Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.
D. Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.
Answer: B,D (LEAVE A REPLY)
The customer's CIO highlights two key pain points: (1) the operations team lacks expertise to efficiently manage PAN-OS upgrades and support interactions, diverting focus from valuable tasks, and (2) the company lacked tools to monitor NGFW capacity, leading to a rushed upgrade. The goal is to recommend long-term solutions leveraging Palo Alto Networks' offerings for Strata Hardware Firewalls. Options B and D-training and AIOps Premium within Strata Cloud Manager (SCM)- address these issues by enhancing team capability and providing proactive management tools. Below is a detailed explanation, verified against official documentation.
Step 1: Analyzing the Customer's Challenges
* Expertise Gap: The CIO notes that identifying issues and engaging support requires expertise the operations team doesn't fully have or can't prioritize. Upgrading PAN-OS on Strata NGFWs involves tasks like version compatibility checks, pre-upgrade validation, and troubleshooting, which demand familiarity with PAN-OS tools and processes.
* Capacity Visibility: The rushed upgrade stemmed from not knowing the NGFWs were nearing capacity (e.g., CPU, memory, session limits), indicating a lack of monitoring or predictive analytics.
Long-term solutions must address both operational efficiency and proactive capacity management, aligning with Palo Alto Networks' ecosystem for Strata firewalls.
Reference: PAN-OS Administrator's Guide (11.1) - Upgrade Overview
"Successful upgrades require planning, validation, and monitoring to avoid disruptions and ensure capacity is sufficient." Step 2: Evaluating the Recommended Actions Option A: Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.
Analysis: AIOps for NGFW (free version) is a cloud-based tool that uses machine learning to monitor firewall health, detect anomalies, and provide upgrade recommendations. It offers basic telemetry (e.g., CPU usage, session counts) and alerts, which could have flagged capacity issues earlier. However, it lacks advanced features like automated remediation, detailed capacity planning, or integration with Strata Cloud Manager, limiting its long-term impact. Additionally, it doesn't address the expertise gap, as the team still needs knowledge to interpret and act on insights.
Conclusion: Helpful but not a comprehensive long-term solution.
Reference: AIOps for NGFW Documentation
"The free version provides basic health monitoring and ML-driven insights but lacks premium features for proactive management." Option B: Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.
Analysis: Palo Alto Networks offers training through the Palo Alto Networks Authorized Training Partners and Cybersecurity Academy, covering PAN-OS administration, upgrades, and troubleshooting. For Strata NGFWs, courses like "Firewall Essentials: Configuration and Management (EDU-210)" teach upgrade best practices, capacity monitoring (e.g., via Device > High Availability > Resources), and support engagement.
How It Solves the Issue:
Reduces reliance on external expertise by upskilling the team.
Enables efficient upgrade planning (e.g., using Best Practice Assessment (BPA) tool).
Frees the team for higher-value tasks by minimizing support escalations.
Long-Term Benefit: A trained team can proactively manage upgrades and capacity, addressing the CIO's concern about expertise allocation.
Conclusion: A strong long-term solution.
Reference: Palo Alto Networks Training Catalog
"Training empowers operations teams to confidently manage NGFWs, including upgrades and capacity planning." Option C: Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.
Analysis: New PAN-OS versions (e.g., 11.1) bring features like enhanced App-ID, decryption, or ML- based threat detection, improving security. However, these don't inherently solve upgrade complexity or capacity visibility. Capacity issues depend on hardware limits (e.g., PA-5200 Series max sessions), not software features, and upgrades still require expertise. This response oversells benefits without addressing root causes.
Conclusion: Not a valid long-term solution.
Reference: PAN-OS 11.1 Release Notes
"New features enhance security but do not automate upgrade processes or capacity monitoring." Option D: Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.
Analysis: AIOps Premium, integrated with Strata Cloud Manager (SCM), is a subscription-based service for managing Strata NGFWs. It provides:
Predictive Analytics: Forecasts capacity needs (e.g., CPU, memory, sessions) using ML.
Upgrade Planning: Recommends optimal upgrade paths and validates configurations.

Proactive Alerts: Identifies issues before they escalate, reducing support calls.
Centralized Management: Monitors all firewalls from SCM, integrating with existing PAN-OS deployments.
How It Solves the Issue:
Prevents rushed upgrades by predicting capacity limits (e.g., via Capacity Saturation Reports).
Simplifies upgrade preparation with automated insights, reducing expertise demands.
Aligns with existing Strata technology, enhancing ROI.
Long-Term Benefit: Offers a scalable, proactive toolset to manage NGFWs, addressing both capacity and operational efficiency.
Conclusion: A robust long-term solution.
Reference: Strata Cloud Manager AIOps Premium Documentation
"AIOps Premium provides advanced capacity planning and upgrade readiness, minimizing operational burden." Step 3: Why B and D Are the Best Choices B (Training): Directly tackles the expertise gap, empowering the team to handle upgrades and capacity monitoring independently. It's a foundational fix, ensuring long-term self-sufficiency.
D (AIOps Premium in SCM): Provides a technological solution to preempt capacity issues and streamline upgrades, reducing the need for deep expertise and support escalations. It complements training by automating complex tasks.
Synergy: Together, they address both human (expertise) and systemic (tools) challenges, aligning with the CIO's goals of operational efficiency and business value.
Step 4: How These Actions Integrate with Strata NGFWs
Training: Teaches use of PAN-OS tools like System Resources (CLI: show system resources) and Dynamic Updates for capacity and upgrade prep.
AIOps Premium: Enhances Strata NGFW management via SCM, pulling telemetry (e.g., from Device > Setup > Telemetry) to predict and resolve issues.
Reference: PAN-OS Administrator's Guide (11.1) - Monitoring
"Combine training and tools like AIOps to optimize NGFW performance and upgrades."

NEW QUESTION: 69
A large enterprise uses a Palo Alto Networks firewall to manage Internet access. They have multiple internal networks, each with its own egress NAT requirements. The network team has defined the following:
1. 'Internal _ Dev' (10.0.10.0/24) needs to Source NAT to a dedicated public IP 203.0.113.100.
2. 'Internal _ Prod' (10.0.20.0/24) needs to Source NAT to a pool of public IPs (203.0.113.101-203.0.113.105) for high concurrency.
3. 'Internal_Guest' (10.0.30.0/24) needs to Source NAT to the firewall's egress interface IP.
All three internal zones egress through the 'External' zone. You need to design the NAT policy order to ensure these requirements are met without conflicting. Which of the following ordered NAT policy sets (top to bottom) would achieve the desired outcome, assuming the External interface IP is 203.0.113.1?

A.

```
ule 1 (Dev Static):
 Original: Source Zone: Internal_Dev, Source IP: 10.0.10.0/24, Dest Zone: External, Dest IP: Any
 Translated: Source IP: 203.0.113.100 (Static IP)

ule 2 (Prod Dynamic Pool):
 Original: Source Zone: Internal_Prod, Source IP: 10.0.20.0/24, Dest Zone: External, Dest IP: Any
 Translated: Source IP: 203.0.113.101-203.0.113.105 (Dynamic IP and Port)

ule 3 (Guest Interface):
 Original: Source Zone: Internal_Guest, Source IP: 10.0.30.0/24, Dest Zone: External, Dest IP: An
 Translated: Source IP: Interface IP (External Interface) (Dynamic IP and Port)
```

B.

```
Rule 1 (Guest Interface):
  Original: Source Zone: Internal_Guest, Source IP: 10.0.30.0/24, Dest Zone: External, Dest IP: Any
  Translated: Source IP: Interface IP (External Interface) (Dynamic IP and Port)

Rule 2 (Prod Dynamic Pool):
  Original: Source Zone: Internal_Prod, Source IP: 10.0.20.0/24, Dest Zone: External, Dest IP: Any
  Translated: Source IP: 203.0.113.101-203.0.113.105 (Dynamic IP and Port)

Rule 3 (Dev Static):
  Original: Source Zone: Internal_Dev, Source IP: 10.0.10.0/24, Dest Zone: External, Dest IP: Any
  Translated: Source IP: 203.0.113.100 (Static IP)
```

C.

```
ule 1 (catch all interface NAT):
 Original: Source Zone: any, Source IP: any, Dest Zone: External, Dest IP: Any
 Translated: Source IP: Interface IP (External Interface) (Dynamic IP and Port)

ule 2 (Dev Static):
 Original: Source Zone: Internal_Dev, Source IP: 10.0.10.0/24, Dest Zone: External, Dest IP: Any
 Translated: Source IP: 203.0.113.100 (Static IP)

ule 3 (Prod Dynamic Pool):
 Original: Source Zone: Internal_Prod, Source IP: 10.0.20.0/24, Dest Zone: External, Dest IP: An
 Translated: Source IP: 203.0.113.101-203.0.113.105 (Dynamic IP and Port)
```

D.

```
Rule 1 (Prod Dynamic Pool):
  Original: Source Zone: Internal_Prod, Source IP: 10.0.20.0/24, Dest Zone: External, Dest IP: Any
  Translated: Source IP: 203.0.113.101-203.0.113.105 (Dynamic IP and Port)

Rule 2 (Guest Interface):
  Original: Source Zone: Internal_Guest, Source IP: 10.0.30.0/24, Dest Zone: External, Dest IP: Any
  Translated: Source IP: Interface IP (External Interface) (Dynamic IP and Port)

Rule 3 (Dev Static)
  Original: Source Zone: Internal_Dev, Source IP: 10.0.10.0/24, Dest Zone: External, Dest IP: Any
  Translated: Source IP: 203.0.113.100 (Static IP)
```

E. The order of Source NAT policies does not matter; only Destination NAT policy order is critical.

Answer: (SHOW ANSWER)

Palo Alto Networks firewalls process NAT rules from top to bottom, applying the first match. In this scenario, all three networks have specific NAT requirements. Since none of the networks overlap in IP address space or source zone, the order of these specific rules doesn't inherently cause a conflict among themselves IF they are placed before any broader 'catch-all' NAT rules. However, following a logical order of more specific to less specific (or just ensuring specific rules are above broad ones) is good practice.

All three options A, B, and D correctly define the individual NAT rules. The question asks for an order that achieves the desired outcome without conflicting . Since each rule targets a distinct source network (10.0.10.0/24, 10.0.20.0/24, 10.0.30.0/24), any order of these three specific rules (A, B, or D) will work, as long as there isn't a broader rule above them that would match their traffic prematurely. Option A presents a valid order. Option C is

incorrect because placing a 'Catch-all Interface NAT' at the top would match all traffic from the specific zones before their dedicated rules are hit, leading to incorrect translation for Dev and Prod. Option E is incorrect; the order of Source NAT policies absolutely matters, just as with any policy type on the firewall, due to the top-down matching logic.

NEW QUESTION: 70
Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?
A. data
B. management
C. network processing
D. security processing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
An organization relies heavily on cloud applications. Due to compliance requirements, they must log all successful and unsuccessful login attempts to sensitive cloud applications, including the user, application, and source IP. Additionally, they need to generate real- time alerts for any failed login attempts exceeding a threshold (e.g., 3 failed attempts within 5 minutes) from a single source IP to a sensitive application. How would you configure Palo Alto Networks firewall logs and profiles to meet these requirements?
A. Enable 'Log at Session End' on the security policy for the sensitive applications. Configure an 'Alert Log' setting in the 'Monitor' tab for 'authentication-failed' messages with a threshold.
B. Enable 'Log at Session Start' for the security policy. Create a custom 'Log Forwarding Profile' to send all traffic logs to an external SIEM. Configure the SIEM to generate alerts based on failed authentication events and thresholds.
C. For the security policy governing sensitive cloud applications, set 'Log at Session End'. Create a 'Log Forwarding Profile' to forward 'Authentication' logs to the Panorama management server. On Panorama, configure a 'Managed Log Forwarding Profile' with an 'Email' alert for 'authentication-failed' events, and enable 'Alerting on Repeated Failures' with the specified threshold and timeframe.
D. Enable 'SSL Decryption' for all cloud application traffic. Configure a 'Vulnerability Protection' profile with a custom signature to detect failed login attempts and set the action to 'alert'.
E. Set the security policy 'Action' to 'Deny' for sensitive applications, which will automatically log failed attempts. Use an 'External Dynamic List' for sensitive application URLs and link it to a 'URL Filtering' profile that generates alerts on block actions.
Answer: C (LEAVE A REPLY)
Option C is the most comprehensive and correct approach. 1. Logging All Login Attempts: 'Log at Session End' on the security policy ensures that the full session details, including application and user (if User-ID is enabled, which is crucial for this scenario), are logged. Successful and unsuccessful authentication attempts are part of these logs, especially if App-ID properly identifies the login process. 2. Real-time Alerts for Failed Attempts with Threshold: The key here is using the 'Authentication' logs, which are distinct from generic 'Traffic' logs and specifically contain authentication events. Forwarding these to Panorama (or a Syslog server, but Panorama provides built-in alerting). Panorama's 'Managed Log Forwarding Profile' allows for granular alerting on specific log types ('Authentication' logs in this case) and, critically, offers 'Alerting on Repeated Failures' with configurable thresholds for time and count from a source. This directly addresses the requirement for failed login attempt alerting with a threshold from a single source IP. Other options are less precise: A lacks the specific 'Authentication' log forwarding and thresholding mechanism. B offloads everything to the SIEM, which is valid but doesn't leverage the firewall's built-in advanced alerting. D (Vulnerability Protection) is for exploits, not authentication logging/alerting. E (Deny action and URL Filtering) is incorrect as it focuses on blocking and URL categorization rather than granular authentication logging and repeated failure alerting.

NEW QUESTION: 72
The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering "gambling" category.
Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the "gambling" URL category?
A. Add *.powerball.com to the URL Filtering allow list.
B. Manually remove powerball.com from the gambling URL category.
C. Add just the URL www.powerball.com to a Security policy allow rule.
D. Create a custom URL category, add *.powerball.com to it and allow it in the Security Profile.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 73
An organization is troubleshooting a complex PBF deployment. They have multiple PBF rules, some using 'Application' as a match criterion, and others using 'Service'. They observe that some traffic, which should be steered by a PBF rule with 'Application: custom- app-udp-port-5000' and 'Egress Interface: tunnel. 1', is instead following the default route. However, a security policy rule for 'custom-app- udp-port-5000' allows the traffic. A packet capture on the firewall shows the UDP traffic leaving via the default internet uplink. What is the most likely reason for this PBF misbehavior?
A. The PBF rule with 'Application: custom-app-udp-port-5000' is placed below a more general PBF rule (e.g., 'Application: any' or 'Service: any') that is matching the traffic first.
B. The custom application 'custom-app-udp-port-5000' has not been correctly identified by App-ID, and thus the PBF rule cannot match it. It's being identified as 'incomplete' or 'unknown-udp'.
C. The firewall is failing to resolve the destination FQDN for the 'custom-app-udp-port-5000' application, causing the PBF rule to be skipped.
D. The 'Service' field in the PBF rule should be explicitly set to 'udp/5000' instead of relying solely on the 'Application' field for UDP traffic.
E. The 'Egress Interface: tunnel.1' is down or its next-hop is unreachable, causing the PBF rule to implicitly fall back to the default route, even without explicit fallback configured.
Answer: (SHOW ANSWER)
This scenario points directly to an App-ID issue. PBF rules that match on 'Application' rely entirely on the firewall's ability to identify the application using App-ID. If 'custom-app-udp-port-5000' is not being correctly identified (e.g., if the traffic pattern doesn't match its signature, or if it's new traffic that hasn't been learned), App-ID might classify it as 'incomplete' or 'unknown-udp'. When an application cannot be identified, PBF rules that rely on that specific App-ID will not match, and the traffic will proceed to be evaluated by subsequent PBF rules or, ultimately, the VR's routing table (leading to the default route). The fact that a security policy rule allows it doesn't mean App-ID is working correctly for PBF; security policies can also use 'service' which is port-based and not App-ID dependent for basic allowance. Option A: While rule order is critical, if the traffic is consistently going to the default route, it suggests the specific rule is not matching at all, not just being preempted by another PBF rule. Option C: FQDN resolution issues would prevent the PBF rule from matching the destination, but the question implies the application itself is the issue, not necessarily the destination's FQDN. Option D: PBF rules can match on 'Application' alone. The 'Service' field is for matching on port/protocol if you don't want to rely on App-ID or for services that don't have a specific App-ID. If 'Application' is used, App-ID is paramount. Option E: If the egress interface or next hop is down, and no explicit fallback is configured, the PBF rule would typically result in a discard (traffic being dropped) or a fall-through to the next PBF rule if one exists, not an implicit fallback to the default route without specific configuration.

NEW QUESTION: 74
A cybersecurity firm manages numerous Palo Alto Networks firewalls for clients, leveraging Panoram a. They need to implement a security policy where certain applications (e.g., specific SaaS apps) are only accessible from specific source IP ranges, which are dynamically updated via an external asset management system. Furthermore, different client firewalls may have different source IP ranges for the same application. How can this be achieved in Panorama using variables and dynamic objects efficiently, without creating a unique policy for every client and every application?
A. Create a separate device group and template stack for each client, and within each stack, define unique address objects and security policies for every application based on the client's specific IP ranges.
B. Utilize Panorama's Variables' within a shared Security Policy Rule. The source IP ranges for the applications would be defined as 'Runtime Variables' that are dynamically populated per device group, or using 'Device Group Variables' that override a default value. Dynamic Address Groups (DAGs) would be used for the application FQDNs, updated by an external script.
C. Configure 'Policy Based Forwarding' rules on each firewall to direct traffic for specific applications to different egress interfaces based on the source IP, bypassing security policies for this specific requirement.
D. Use a single security policy rule applying to all firewalls. The source IP ranges are hardcoded into the rule, and administrators manually update them whenever the external asset management system changes.
E. Employ 'Application Filters' in security policies to match applications. The source IP enforcement is handled by network ACLs upstream of the firewalls.
Answer: B (LEAVE A REPLY)
Option B is the most elegant and efficient solution leveraging Panorama's advanced features: Shared Security Policy Rule: A single policy rule can be defined at a higher level in Panorama (e.g., a shared device group or template). Variables: For the dynamic source IP ranges, Panorama Variables' are crucial. 'Device Group Variables' allow defining a variable (e.g., with different values for different device groups (each client having its own device group). This variable can then be referenced in the shared security policy rule's source address field. Alternatively, 'Runtime Variables' could be updated via API for extreme dynamism per firewall. Dynamic Address Groups (DAGs): For the SaaS application FQDNs, DAGs are ideal. An external script or integration can populate these DAGs with the latest FQDNs or IP addresses of the SaaS applications. This allows the application destination to also be dynamic. This approach avoids policy duplication, simplifies management, and ensures that updates from the asset management system can automatically propagate without requiring manual policy edits for each client. Option A leads to significant configuration sprawl. Option C is not a security policy enforcement method. Option D is manual and not scalable. Option E delegates the security enforcement to another layer, which might not be desirable or feasible.

NEW QUESTION: 75
An analyst needs to create a security rule to allow access to a specific web application that identifies itself as

"web-browsing" but uses a custom, non-standard port of TCP 9000. Which configuration ensures the App-ID engine can still inspect this traffic?
A. Change the Service to "application-default."
B. Create a custom Service object for TCP 9000 and use it in the rule.
C. Use an Application Override rule for port 9000.
D. Change the application to "any" and the service to TCP 9000.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
In a Palo Alto Networks environment, the Service column in a security rule defines the destination port used for the initial session establishment. If an application like web-browsing (which typically uses TCP 80 or 443) is running on a non-standard port like TCP 9000, the analyst must create a custom Service object for that port.
Using this custom service object in the security rule allows the session to be established on port 9000 while maintaining full App-ID inspection. This is critical because it allows the firewall to verify that the traffic is actually web-browsing and not a threat masquerading as a web service. Option A is incorrect because
"application-default" would restrict the traffic to standard ports only. Option C (Application Override) is incorrect because it would disable Layer 7 inspection entirely, which is a significant security risk. By using a custom service with the correct App-ID, the analyst ensures that security remains granular and effective without disrupting non-standard business applications.

NEW QUESTION: 76
A firewall administrator implementing Palo Alto Networks best practices on the company firewall reviews NGFW alerts in Strata Cloud Manager (SCM) and determines that one alert does not apply to this environment. If the administrator has no intention to resolve the underlying issue, what is the appropriate next step?
A. Click "Copilot" in the top right, and ask the Copilot to make an exception for the NGFW alert.
B. Assign the NGFW alert to the "Dismiss" user.
C. Change the NGFW alert priority to "Not Set."
D. Open the NGFW alert and click "Suppress" under "Actions."
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
Within the Strata Cloud Manager (SCM) interface, managing the lifecycle of incidents and alerts is a core responsibility. When an administrator encounters an NGFW alert that is deemed irrelevant or inapplicable to their specific environment, SCM provides a mechanism to silence that alert to reduce "alert fatigue" and keep the dashboard focused on actionable items.
The appropriate action in this scenario is to Open the NGFW alert and click "Suppress" under "Actions".
Suppression allows the administrator to mute specific incidents or alerts that they do not intend to remediate, effectively acknowledging the risk but choosing to ignore it in the reporting and notification workflows. This is often used for non-critical alerts or during maintenance windows. Unlike dismissing or changing priorities, Suppression is a formal administrative action within the SCM incident framework that can be granularly controlled, allowing for custom raise and clear conditions to be overridden based on the organization's unique operational needs. This ensures that the "Health Score" or "Security Posture" metrics are not unfairly penalized by known, accepted environmental conditions.

NEW QUESTION: 77
An enterprise is deploying a new containerized application infrastructure, using Kubernetes, exposed via a dedicated load balancer that sits behind a Palo Alto Networks firewall. The security team anticipates a very high, burstable volume of legitimate traffic, but also expects sophisticated HTTP/2-based DoS attacks that exploit the protocol's multiplexing capabilities and header compression. The firewall needs to detect and mitigate these without impacting

legitimate, high-concurrency connections. Given that standard HTTP/I .1 flood protection might be insufficient, what advanced DoS profile configurations should be prioritized for the Palo Alto Networks firewall to protect this environment, assuming HTTP/2 inspection is enabled?

A. Enable 'HTTP Flood' protection with 'Per-Request Rate' and 'Per-Source IP Rate' thresholds, and configure 'Syn-Cookie' as the action. Also, set a low 'Client Read Timeout' in 'Slow HTTP Protection' to counter slow HTTP/2 attacks.

B. Focus on 'Session Based Attack Protection' with very high 'Max Concurrent Sessions' and 'Session Rate' thresholds, coupled with 'Packet Based Attack Protection' for TCP and UDP floods to handle general volumetric attacks.

C. Utilize 'HTTP Flood' protection within a DoS Protection Profile, ensuring 'HTTP/2' is enabled for inspection on the relevant security policy. Set 'Per-Request Rate' and 'Per-Source IP Rate' aggressively, and importantly, tune 'Per-URL Rate' and 'URL Query String Length' thresholds to detect malformed or excessively long HTTP/2 requests/streams.

D. Implement 'Zone Protection' on the ingress zone, enabling 'Flood Protection' for 'HTTP Flood' and setting 'Action: Reset'. Complement this with 'IP Address Block' for sources exceeding a high connection rate.

E. Configure 'DoS Protection Policy' with 'Target' rules for the load balancer IPs. Within these rules, enable 'HTTP Flood' protection. Critically, utilize 'HTTP Header Length' and 'HTTP Header Count' thresholds to detect HTTP/2 'HPACK Bomb' or excessive header attacks. Also, set 'Client Read Timeout' for 'Slow HTTP Protection' and ensure 'Action: Protect' is chosen for relevant thresholds.

Answer: E (LEAVE A REPLY)

This is a very specific scenario targeting HTTP/2 vulnerabilities. Standard HTTP/I .1 rate limiting (A, B, C partially) might not be enough because HTTP/2 multiplexing means many logical streams (requests) can occur over a single TCP connection, potentially bypassing 'Per-session' limits. HTTP/2 also has vulnerabilities like 'HPACK Bomb' (excessive header size/count) and slow stream processing. Option E directly addresses these: 1. Target rules for load balancer IPs: Ensures protection is focused. 2. HTTP Flood protection: General HTTP volume. 3. HTTP Header Length and HTTP Header Count: These are CRITICAL for detecting HTTP/2-specific attacks like 'HPACK Bomb' which exploit header compression to consume resources with small packet sizes. This is an advanced feature not present in basic HTTP flood protection. 4. Client Read Timeout: Essential for slow HTTP/2 stream attacks. 5. Action: Protect: Provides a controlled response (e.g., reset stream) rather than outright blocking, minimizing impact on legitimate connections. Option C is close but misses the specific HTTP/2 header-based protections which are vital. Option A incorrectly suggests Syn-Cookie for HTTP and is too simplistic. Option B is too generic. Option D is less granular and reactive. Option E provides the most comprehensive and targeted defense for HTTP/2 DoS.

NEW QUESTION: 78

A security auditor requests a report detailing all network connections that leveraged a deprecated SSL/TLS version (e.g., TLSv1.0 or TLSv1.1) over the past 90 days. The organization uses Strata Logging Service for log aggregation. Provide the most effective Strata Logging Service Query Language (SLQL) query to retrieve this information, assuming relevant fields are captured.

A.
```
select time_generated, source_ip, destination_ip, app, ssl_version from traffic where ssl_version in ('TLSv1.0', 'TLSv1.1')
and time_generated between '90 days ago' and 'now'
```

B.
```
select   from threat where protocol eq 'ssl' and ssl_version like 'TLSv1.0%' or ssl_version like 'TLSv1.1%'
```

C.
```
select time, src, dst, application, ssl_proto from session where ssl_proto = 'TLSv1.0' or ssl_proto = 'TLSv1.1' and time > (now() - interval '90' day
```

D.
```
select time generated, source ip, destination_ip, app, ssl_version from traffic where ssl_version in ('TLSv1.0', 'TLSv1.1')
sort by time_generated desc limit 1000
```

E.
```
select time_generated, source_ip, destination_ip, app, ssl_version from url where ssl_version eq 'TLSv1.0' or ssl_version eq 'TLSv1.1'
```

Answer: (SHOW ANSWER)

Option A uses the correct log type ('traffic'), field names ('ssl_version'), and SLQL syntax for filtering by multiple values ('in') and a time range ('between'). Traffic logs capture details about network sessions, including SSL/TLS versions used. The time filter 'between '90 days ago' and 'now" accurately covers the requested period. Options B, C, and E use incorrect log types or field names. Option D lacks the time range specification, which is critical for the audit.

NEW QUESTION: 79

After configuring an EDL with a source URL, the firewall logs show "Unable to fetch external list.
Using old copy for refresh." What is the likely cause??

A. The EDL contains unsupported file types.

B. The firewall's antivirus license has expired.

C. The firewall cannot reach the EDL hosting server.

D. The EDL has been deleted from the firewall.

Answer: C (LEAVE A REPLY)
The error message "Unable to fetch external list. Using old copy for refresh" indicates that the firewall was unable to contact the server hosting the External Dynamic List (EDL), so it is using the last successfully fetched copy as a fallback.

NEW QUESTION: 80
Which protocol used to map username to user groups when user-ID is configured?
A. SAML
B. LDAP
C. RADIUS
D. TACACS+
Answer: (SHOW ANSWER)

NEW QUESTION: 81
An enterprise is facing a unique challenge with its SD-WAN deployment. They have a custom, latency-critical, stateful application (App-ID: proprietary-app) that requires all its traffic (initial connection and subsequent data) to be pinned to a single, consistent WAN path for the entire session duration to avoid session resets. This application must prefer a specific MPLS link (Link A) if its latency is below 30ms and packet loss is below 0.01 If Link A degrades, the application should failover to a dedicated Internet VPN tunnel (Tunnel B) if Tunnel B's latency is below 50ms and packet loss below 0.1%. If both links fail their respective SLAs, the traffic should be dropped. Furthermore, if a session is established on Tunnel B, it should not flap back to Link A even if Link A recovers, to maintain session consistency. Which configuration elements are crucial to implement this requirement?
A. 1. Create an SLA profile for 'proprietary-app' with latency (30ms) and packet loss (0.01 thresholds. Apply this SLA to Link 2. Configure a PBF rule for 'proprietary-app' with primary next-hop Link A and secondary next-hop Tunnel B. Enable 'Session Stickiness' on the PBF rule. 3. Configure a separate SLA profile for Tunnel B (latency 50ms, packet loss 0.1 %) and link it to the PBF secondary path.
B. 1. Define two SLA profiles: 'MPLS_SLA' (30ms lat, 0.01% loss) and 'Internet_SLX (50ms lat, 0.1% loss). 2. Create an SD-WAN policy for 'proprietary-app'. Configure 'Dynamic Path Selection' with 'Best Path' and the following order: LinkA (using 'MPLS SLA'), then Tunnel B (using 'Internet_SLA'). 3. Crucially, enable 'Session Stickiness' within the SD-WAN policy settings for this application to prevent flap-back.
C. 1. Configure Link A as the primary egress interface in a Zone. Configure Tunnel B as a backup interface in the same Zone. 2. Implement an SD-WAN policy for 'proprietary-app' that uses this Zone. 3. Use BFD on both Link A and Tunnel B to detect link failures. 4. Manually configure session persistence on the firewall for proprietary-app' to keep sessions on the initial path.
D. 1. Create a primary SD-WAN Path Group for Link A with a 30ms latency / 0.01% packet loss SLA. 2. Create a secondary SD-WAN Path Group for Tunnel B with a 50ms latency / 0.1% packet loss SLA. 3. Apply an SD-WAN policy for 'proprietary-app' that uses these path groups in order. 4. Enable 'Failover Only' mode for the secondary Path Group, which ensures once traffic moves to Tunnel B, it stays there until Tunnel B itself fails its SLA.
E. 1. Use a PBF rule for 'proprietary-app' to force it to LinkA as the primary interface. 2. Configure a monitor on Link A's health. If LinkA fails, automatically disable its interface. 3. Rely on routing to then pick Tunnel B as the next best path. 4. Implement a custom script to manually re-enable Link A only after a prolonged period of stability to prevent flapping.
Answer: (SHOW ANSWER)
Option D is the most precise and direct solution using Palo Alto Networks SD-WAN capabilities to address all requirements, especially the critical 'no flap-back' for session consistency. Primary/Secondary Path Groups with SLAs: This correctly handles the distinct SLA requirements for Link A and Tunnel B and their preference order. 'Failover Only' Mode: This is the key feature for the 'no flap-back' requirement. When 'Failover Only' is enabled on a secondary path group (Tunnel B in this case), once traffic for 'proprietary-app' switches from Link A to Tunnel B due to Link A's degradation, it will remain on Tunnel B even if Link A recovers, as long as Tunnel B itself continues to meet its configured SLA. This ensures session consistency. Traffic will only move off Tunnel B if Tunnel B itself fails its SLA, at which point the 'Fail Action' would dictate what happens (e.g., drop traffic). Session Stickiness (Context): While 'Session Stickiness' is a general concept to keep sessions on the same path, the 'Failover Only' mode for path groups is the more granular and explicit mechanism in Palo Alto Networks SD-WAN to prevent flapping back to a primary link after an SLA-triggered failover.

NEW QUESTION: 82
Which two features implement one-to-one translation of a source IP address while allowing the source port to change? (Choose two.)
A. Static IP
B. Dynamic IP / Port Fallback
C. Dynamic IP
D. Dynamic IP and Port (DIPP)

Answer: A,D (LEAVE A REPLY)
Static IP and Dynamic IP and Port (DIPP) are two features that implement one-to-one translation of a source IP address while allowing the source port to change. Static IP translates a single source address to a specific public address, and allows the source port to change dynamically1. Dynamic IP and Port (DIPP) translates the source IP address or range to a single IP address, and uses the source port to differentiate between multiple source IPs that share the same translated address2. Both of these features provide a one-to-one translation of IP addresses, but do not restrict the source port. Reference:
Static IP - Palo Alto Networks
Dynamic IP and Port - Palo Alto Networks

NEW QUESTION: 83
A security architect is designing an automated incident response playbook within their Security Orchestration, Automation, and Response (SOAR) platform. This playbook needs to interact with Strata Cloud Manager (SCM) to perform actions like blocking malicious IPs, quarantining compromised devices, and retrieving firewall logs. Which of the following Python code snippets demonstrates the correct initial step to authenticate and interact with SCM's API for such operations?

A.
```
import requests
url = 'https://api.strata.paloaltonetworks.com/auth/v1/oauth2/token'
headers = {'Content-Type': 'application/json'}
data = {'grant_type': 'client_credentials', 'client_id': 'YOUR_CLIENT_ID', 'client_secret': 'YOUR_CLIENT_SECRET'}
response = requests.post(url, headers=headers, json=data)
access_token = response.json()['access_token']
```

B.
```
import paramiko
ssh_client = paramiko.SSHClient()
ssh_client.connect('scm.paloaltonetworks.com', username='admin', password='password')
```

C.
```
import netmiko
connect_handler = netmiko.ConnectHandler(device_type='paloalto_panos', host='scm.paloaltonetworks.com', username='admin', password='password')
```

D.
```
import boto3
s3 = boto3.client('s3')
s3.list buckets()
```

E.
```
import xml.etree.ElementTree as ET
url = 'https://scm.paloaltonetworks.com/api/?type=op&cmd='
response = requests.get(url, auth=('admin', 'password'))
```

Answer: (SHOW ANSWER)
SCM primarily utilizes OAuth 2.0 for API authentication, typically with client credentials (client ID and client secret) for machine-to- machine interaction. Option A demonstrates the correct Python code to obtain an access token from SCM's OAuth 2.0 token endpoint. This access token is then used in subsequent API requests to authorize operations. Options B and C are for SSH/CLI interactions, Option D is for AWS S3, and Option E represents an older XML API authentication method which is not the primary or recommended method for SCM's modern REST API.

NEW QUESTION: 84
A security analyst needs to create a custom URL category for a new phishing campaign targeting the company. The phishing URLs frequently change their domain and path but always contain specific, unique query parameters used to track victims. Which combination of URL category types and regex patterns would be most effective and efficient for capturing these URLs while minimizing false positives, given the following example URL structures:
```
https://login.example.com/auth?token=abCdeF123&campaignID=Phish2024Q2&user=victim1
http://secure.malicious.net/login/confirm?id=xyz789&source=email&campaignID=Phish2024Q2
https://fraud.attack.org/verify?data=hashData&key=secret&campaignID=Phish2024Q2
```

A. Type: Regex. Pattern: `. campaignID=Phish2024Q2.`

B. Type: Domain. Entries: `example.com, malicious.net, attack.org`

C. Type: URL. Entries: `https://login.example.com/auth?token=abCdeF123&campaignID=Phish2024Q2&user=victim1, http://secure.malicious.net/login/confirm?id=xyz789&source=email&campaignID=Phish2024Q2`

D. Type: Wildcard. Entries: `campaignID=Phish2024Q2`

E. Type: Regex. Pattern: `(example|malicious|attack)\.(com|net|org)/. \?. campaignID=Phish2024Q2.`

Answer: A (LEAVE A REPLY)

The key information is that the URLs frequently change domain and path but consistently contain the 'campaignID=Phish2024Q2 query parameter. Option A, using a Regex type with the pattern' . campaignID=Phish2024Q2. & , is the most effective and efficient. It precisely targets the unique identifying query parameter regardless of the preceding domain or path, minimizing false positives and being resilient to URL changes. Option B (Domain) would miss URLs from new domains. Option C (URL) is too specific and won't match variations. Option D (Wildcard) in Palo Alto Networks URL categories typically applies to hostnames or path segments, not full query parameters with wildcards directly. Option E is overly complex and might be less efficient, as the crucial part is the query parameter, not necessarily the domain pattern.

NEW QUESTION: 85

Actions can be set for which two items in a URL filtering security profile? (Choose two.)

A. Block List

B. Custom URL Categories

C. PAN-DB URL Categories

D. Allow List

Answer: A,D (LEAVE A REPLY)

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

NEW QUESTION: 86

An organization is migrating its data to cloud storage platforms like AWS S3 and Azure Blob Storage. They need a security policy that allows upload and download of specific file types (e.g., .docx, .pdf, .xlsx) to and from these cloud storage services, but strictly blocks executable files (.exe, .zip, .rar) and prevents any sensitive data (e.g., credit card numbers, PII) from leaving the network. How would you configure Content-ID profiles to enforce this, considering both upload and download scenarios?

A. Create a File Blocking Profile to block .exe, .zip, .rar for 'upload' and 'download'. Create a Data Filtering Profile to block sensitive patterns for 'upload'. Apply these to the cloud access rule.

B. Create a File Blocking Profile with 'block' action for file types .exe, .zip, .rar. Create a Data Filtering Profile with 'block' action for sensitive data patterns. Apply both profiles to the security rule allowing cloud storage access, ensuring directionality (e.g., upload/download) is implicitly handled.

C. Create a File Blocking Profile: Rule 1: 'block' for .exe, .zip, .rar (both upload & download). Rule 2: 'allow' for .docx, .pdf, .xlsx (both upload & download). Create a Data Filtering Profile with sensitive data patterns, 'block' action for 'upload' and 'download'. Apply both to the cloud access rule.

D. Create a File Blocking Profile: Rule 1: 'block' for .exe, .zip, .rar (upload). Rule 2: 'block' for .exe, .zip, .rar (download). Create a Data Filtering Profile with sensitive data patterns, 'block' action for 'upload'. Apply these to the cloud access rule. Add a second Data Filtering Profile with 'block' for 'download' of sensitive data.

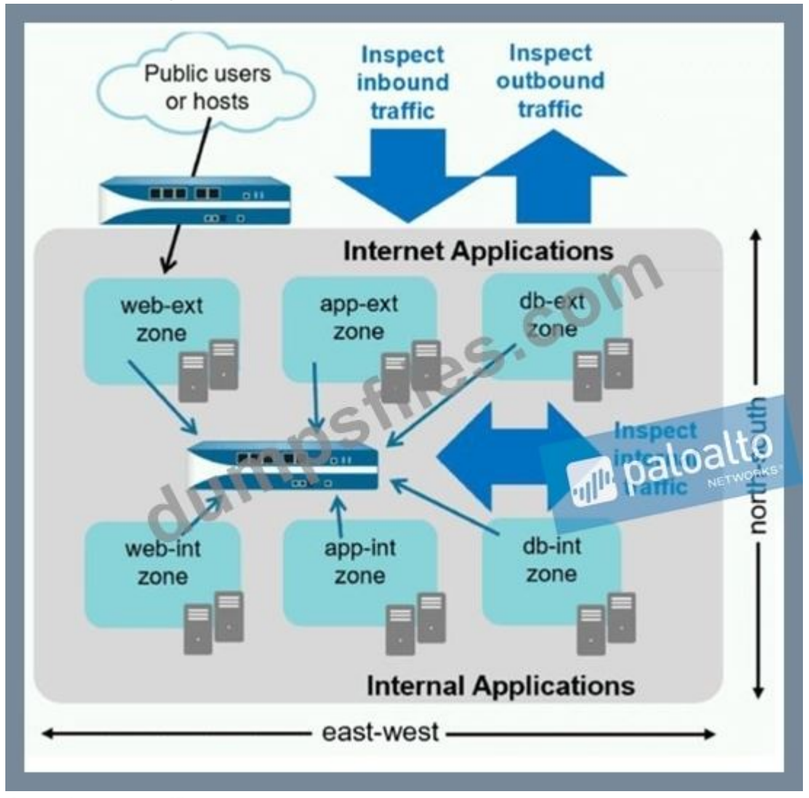
E. Create a File Blocking Profile: Rule for 'upload': block .exe, .zip, .rar. Rule for 'download': block .exe, .zip, .rar. Create a Data Filtering Profile: Rule for 'upload': block sensitive patterns. Rule for 'download': block sensitive patterns. Apply these combined profiles to the security policy rule allowing access to AWS S3 and Azure Blob. Also, ensure a WildFire Analysis Profile is applied.

Answer: (SHOW ANSWER)

Option E is the most comprehensive and correctly addresses both upload and download scenarios for both file blocking and data filtering, and importantly, adds WildFire for advanced threat detection. Palo Alto Networks File Blocking and Data Filtering profiles allow specifying direction (upload/download). By explicitly defining rules for both directions within each profile, you ensure precise control. A separate 'allow' rule for document types within file blocking isn't strictly necessary if the default action is deny and specific deny rules are in place. The WildFire profile adds an extra layer of security for unknown files. Option A and B don't explicitly specify direction for both profiles

and might not cover all aspects. Option C incorrectly suggests 'allow' rules within file blocking; usually, you define 'block' and let the application default handle others, or have a more granular list of allowed files with a final block. Option D misses the download data filtering and is more complex than necessary.

NEW QUESTION: 87
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



A. perimeter traffic
B. north-south traffic
C. east-west traffic
D. branch office traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 88
A network security analyst is attempting to push a new security policy configuration to a Palo Alto Networks firewall. The commit operation fails with the error message:

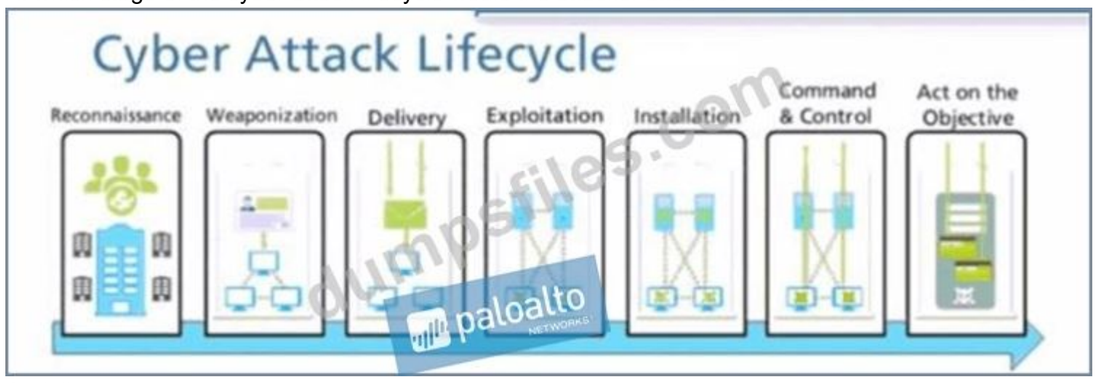
```
'Error: Rule 'Block Malware Sites' references an address object 'Malicious_IP_Feed' which does not exist in the configured
 zone 'Untrust'. Configuration validation failed.'
```

Which of the following is the MOST LIKELY root cause of this commit failure?
A. The security policy rule 'Block_Malware_Sites' has an incorrect service port configured.
B. The firewall is experiencing a high volume of traffic, leading to a timeout during the commit process.

C. The address object 'Malicious_IP_Feed' exists but is not associated with the 'Untrust' zone, or it has been deleted.
D. The administrator's role-based access control (RBAC) privileges are insufficient to modify security policies.
E. The device group hierarchy is misconfigured, preventing policy inheritance.
Answer: (SHOW ANSWER)
The error message explicitly states that the 'Malicious_IP_Feed' address object 'does not exist in the configured zone 'Untrust''. This indicates a configuration inconsistency where the security rule references an object that is either missing, misspelled, or not correctly defined within the scope of the 'Untrust' zone, or has been deleted. Options A, B, D, and E describe other potential issues but do not directly align with the specific error message provided.

NEW QUESTION: 89
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?
A. Review App Matches
B. Review Policies
C. Pre-analyze
D. Review Apps
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



A. delivery
B. command and control
C. explotation
D. installation
E. reinsurance
Answer: (SHOW ANSWER)

NEW QUESTION: 91
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. anti-spyware
B. URL filtering
C. vulnerability protection
D. file blocking

Answer: C (LEAVE A REPLY)
Reference:
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.

NEW QUESTION: 92
A systems engineer (SE) successfully demonstrates NGFW managed by Strata Cloud Manager (SCM) to a company. In the resulting planning phase of the proof of value (POV), the CISO requests a test that shows how the security policies are either meeting, or are progressing toward meeting, industry standards such as Critical Security Controls (CSC), and how the company can verify that it is effectively utilizing the functionality purchased.
During the POV testing timeline, how should the SE verify that the POV will meet the CISO's request?
A. Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.
B. At the beginning, work with the customer to create custom dashboards and reports for any information required, so reports can be pulled as needed by the customer.
C. Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.
D. At the beginning, use PANhandler golden images that are designed to align to compliance and to turning on the features for the CDSS subscription being tested.

Answer: B (LEAVE A REPLY)
The SE has demonstrated an NGFW managed by SCM, and the CISO now wants the POV to show progress toward industry standards (e.g., CSC) and verify effective use of purchased features (e.g., CDSS subscriptions like Advanced Threat Prevention). The SE must ensure the POV delivers measurable evidence during the testing timeline. Let's evaluate the options.
Step 1: Understand the CISO's Request
* Industry Standards (e.g., CSC): The Center for Internet Security's Critical Security Controls (e.g., CSC 1: Inventory of Devices, CSC 4: Secure Configuration) require visibility, threat prevention, and policy enforcement, which NGFW and SCM can address.
* Feature Utilization: Confirm that licensed functionalities (e.g., App-ID, Threat Prevention, URL Filtering) are active and effective.
* POV Goal: Provide verifiable progress and utilization metrics within the testing timeline.
Reference: Strata Cloud Manager Overview (docs.paloaltonetworks.com/strata-cloud-manager); CIS Critical Security Controls (www.cisecurity.org/controls).
Step 2: Define SCM Capabilities
Strata Cloud Manager (SCM): A cloud-based management platform for Palo Alto NGFWs, offering dashboards (e.g., Best Practices, Feature Adoption) and custom reporting to monitor security posture, policy compliance, and subscription usage.
Security Lifecycle Review (SLR): A report generated via the Customer Support Portal (not SCM) analyzing traffic logs for security gaps, not real-time POV progress.
Dashboards and Reports: SCM provides prebuilt and customizable views for real-time insights into policy effectiveness and feature adoption.
Reference: SCM Dashboards and Reports (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and- reports).
Step 3: Evaluate Each Option
A). Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.
Description: The SLR analyzes 7-30 days of traffic logs, providing a retrospective security posture assessment (e.g., threats blocked, policy gaps).
Process: Near POV end, upload logs to the Customer Support Portal (Support > Security Lifecycle Review), generate, and share the report.
Limitations:
SLR is a point-in-time analysis, not a real-time progress tracker during the POV timeline.

Requires post-POV log collection, delaying feedback.
Doesn't directly show feature utilization progress or CSC alignment in SCM.
Fit: Misses the "during the POV timeline" requirement; better for post-POV analysis.
Reference: Security Lifecycle Review Guide (support.paloaltonetworks.com, requires login).
B). At the beginning, work with the customer to create custom dashboards and reports for any information required, so reports can be pulled as needed by the customer.
Description: SCM allows custom dashboards and reports (Monitor > Dashboards or Reports) tailored to metrics like policy compliance (CSC alignment) and feature usage (e.g., Threat Prevention hits).
Process:
At POV start, collaborate with the CISO to define metrics (e.g., "Threats blocked by ATP" for CSC 6, "App- ID usage" for feature adoption).
Configure custom dashboards in SCM (Dashboards > Add Dashboard > Custom).
Set up scheduled or on-demand reports (Reports > Custom Reports).
Enable the customer to monitor progress throughout the POV.
Benefits:
Real-time visibility into policy effectiveness and feature use during the timeline.
Aligns with CSC (e.g., blocked malware events) and shows subscription ROI.
Empowers the customer to verify results independently.
Fit: Meets the CISO's request fully within the POV timeline.
Reference: SCM Custom Dashboards (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and- reports/custom-dashboards).
C). Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.
Description: SCM provides prebuilt dashboards:
Best Practices: Assesses policy alignment with security standards.
CDSS Adoption: Tracks subscription usage (e.g., ATP, URL Filtering).
NGFW Feature Adoption: Monitors features like App-ID or User-ID.
Limitations:
Waiting until "near the end" delays visibility, missing ongoing progress tracking.
Prebuilt dashboards may not fully align with CSC or specific customer needs without customization.
Fit: Useful but incomplete; lacks proactive setup and real-time monitoring throughout the POV.
Reference: SCM Prebuilt Dashboards (docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and- reports/prebuilt-dashboards).
D). At the beginning, use PANhandler golden images that are designed to align to compliance and to turning on the features for the CDSS subscription being tested.
Description: PANhandler is a tool for managing Skillets (configuration templates), including "golden images" for compliance (e.g., NIST, CIS benchmarks).
Process: Apply a Skillet at POV start to configure the NGFW with compliance settings and CDSS features.
Limitations:
Configures the NGFW but doesn't verify progress or utilization during the POV.
No reporting or dashboard integration for the CISO to track results.
Fit: Sets up the environment but doesn't meet the verification requirement.
Reference: PANhandler Skillets (github.com/PaloAltoNetworks/panhandler).
Step 4: Select the Best Approach
B is the strongest choice:
Proactive: Starts at the beginning, ensuring metrics are tracked throughout the POV.
Customizable: Tailors dashboards/reports to CSC (e.g., threat detection for CSC 6) and feature use (e.g., ATP events).
Verifiable: Enables the customer to pull reports as needed, meeting the CISO's request within the timeline.
Why not A, C, or D?

A: SLR is retrospective, not real-time, missing the "during" aspect.
C: Prebuilt dashboards are helpful but delayed and less flexible than custom options.
D: Golden images configure but don't verify progress or utilization.
Step 5: Verification with Palo Alto Documentation
SCM Custom Dashboards: Supports real-time, tailored monitoring (SCM Docs).
SLR: Post-analysis tool, not POV-progressive (Support Portal Docs).
Prebuilt Dashboards: Limited customization (SCM Docs).
PANhandler: Configuration-focused, not reporting-focused (PANhandler Docs).
Thus, the verified answer is B.

NEW QUESTION: 93
Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?
A. Prisma SaaS
B. GlobalProtect
C. Panorama
D. AutoFocus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.
Which type of NAT was configured?
A. Static IP
B. Dynamic IP
C. Destination NAT
D. Dynamic IP and Port
Answer: B (LEAVE A REPLY)
The size of the NAT pool should be equal to the number of internal hosts that require address translations. By default, if the source address pool is larger than the NAT address pool and eventually all of the NAT addresses are allocated, new connections that need address translation are dropped. To override this default behavior, use Advanced (Dynamic IP/Port Fallback) to enable the use of DIPP addresses when necessary

NEW QUESTION: 95
Which SCM feature allows an administrator to see a "Safety Score" for a proposed policy change before it is committed to the firewalls?
A. Policy Optimizer
B. Activity Insights
C. Best Practice Assessment (BPA)
D. Strata Cloud Manager (SCM) Copilot
Answer: (SHOW ANSWER)
The Best Practice Assessment (BPA) tool--which is integrated directly into Strata Cloud Manager as an inline check--allows analysts to evaluate their security configuration against Palo Alto Networks' recommended standards. It provides a "Security Adoption" or "Safety" score based on how well the policies implement features like App-ID, User-ID, and Security Profiles.

By reviewing these checks before a commit, the analyst can identify "overly permissive" rules or rules missing critical threat inspection profiles. This proactive approach ensures that new policy changes do not inadvertently weaken the organization's security posture. For a Network Security Analyst, using the inline BPA in SCM is a key objective for maintaining a high-quality rulebase and moving the organization toward a "best practice" implementation of the Next-Generation Firewall.

NEW QUESTION: 96
A Palo Alto Networks firewall is reporting consistently high data plane CPU utilization (around 80-90%), but the management plane CPU remains low. Users are experiencing intermittent packet loss and application latency. You suspect a large volume of specific traffic types or signatures are consuming resources. Which of the following steps would be most effective in identifying the specific traffic causing the high data plane utilization?
A. Run show session all filter application for known high-bandwidth applications.
B. Enable packet capture on the firewall for all interfaces and analyze the pcap file using Wireshark.
C. Utilize the ACC (Application Command Center) to filter for 'Top Applications' and 'Top Threats' over the last hour.
D. Execute debug flow basic on the CLI for a problematic source IP to trace packet flow.
E. Check the BFD (Bidirectional Forwarding Detection) status for all configured interfaces.
Answer: C (LEAVE A REPLY)
High data plane CPU with low management plane CPU points to traffic processing issues. The ACC (Application Command Center) is the primary graphical interface tool for gaining immediate visibility into 'Top Applications', 'Top Threats', 'Top Users', and 'Top URLs'. This allows for quick identification of what traffic is consuming the most resources and potentially causing the high data plane CPU. Option A requires knowing the application beforehand. Option B is resource-intensive and provides raw packet data, not immediate high-level insights into resource consumption. Option D is for specific packet flow debugging. Option E is for link health, not CPU utilization by traffic.

NEW QUESTION: 97
Which order of steps is the correct way to create a static route?
A. 1) Enter the route and netmask2) Enter the IP address for the specific next hop3) Specify the outgoing interface for packets to use to go to the next hop4) Add an IPv4 or IPv6 route by name
B. 1) Enter the route and netmask2) Specify the outgoing interface for packets to use to go to the next hop3) Enter the IP address for the specific next hop4) Add an IPv4 or IPv6 route by name
C. 1) Enter the IP address for the specific next hop2) Enter the route and netmask3) Add an IPv4 or IPv6 route by name4) Specify the outgoing interface for packets to use to go to the next hop
D. 1) Enter the IP address for the specific next hop2) Add an IPv4 or IPv6 route by name3) Enter the route and netmask4) Specify the outgoing interface for packets to use to go to the next hop
Answer: A (LEAVE A REPLY)
Enter the route and netmask
Enter the IP address for the specific next hop
Specify the outgoing interface for packets to use to go to the next hop Add an IPv4 or IPv6 route by name Comprehensive This is the correct order of steps to create a static route in a virtual router on the firewall. The first step is to enter the route and netmask for the destination network, such as 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address. The second step is to enter the IP address for the specific next hop, such as 192.168.56.1 or 2001:db8:49e:1::1. The third step is to specify the outgoing interface for packets to use to go to the next hop, such as ethernet1/1. The fourth step is to add an IPv4 or IPv6 route by name, such as route11.
Reference:
Configure a Static Route - Palo Alto Networks

NEW QUESTION: 98
Consider the following firewall policy configuration snippet from a Panorama managed firewall:

```
<rulebase>
  <entry name="Allow-Internal-HTTP">
    <from><member>Trust</member></from>
    <to><member>Trust</member></to>
    <source><member>any</member></source>
    <destination><member>any</member></destination>
    <application><member>web-browsing</member></application>
    <service><member>service-http</member></service>
    <action>allow</action>
  </entry>
  <entry name="Block-External-Browsing">
    <from><member>Trust</member></from>
    <to><member>Untrust</member></to>
    <source><member>any</member></source>
    <destination><member>any</member></destination>
    <application><member>web-browsing</member></application>
    <service><member>any</member></service>
    <action>deny</action>
  </entry>
</rulebase>
```


An analyst observes internal users are still able to browse external HTTP websites, contradicting the 'Block-External-Browsing' rule. Using Policy Optimizer, Command Center, and Activity Insights, what is the most likely reason for this behavior, and how would these tools help identify and rectify it? (Select all that apply)

A. Most Likely Reason: The 'Allow-Internal-HTTP' rule is shadowing 'Block-External-Browsing'. Tool Action: Policy Optimizer would highlight 'Allow-Internal-HTTP' as a shadowed rule or show its 'usage' affecting external traffic. Command Center would show sessions hitting 'Allow-Internal-HTTP' for external destinations.

B. Most Likely Reason: The firewall is not configured to perform App-ID on HTTP traffic. Tool Action: Activity Insights would show traffic categorized as 'unknown- tcp' instead of 'web-browsing' for HTTP. Command Center would display sessions with 'unknown-tcp' as the application.

C. Most Likely Reason: The 'service' in 'Block-External-Browsing' is 'any', making it less specific than 'Allow-Internal-HTTP' and thus being hit first for internal traffic. Tool Action: Policy Optimizer would recommend making the 'Block-External-Browsing' rule more specific, possibly by adding a source or destination zone.

D. Most Likely Reason: The 'Block-External-Browsing' rule is placed lower in the rulebase than 'Allow-Internal-HTTP'. Tool Action: Policy Optimizer's 'Rule Order' view would visually indicate the incorrect placement. Command Center session logs would confirm traffic hitting 'Allow-Internal-HTTP' instead of 'Block-External-Browsing'.

E. Most Likely Reason: Users are bypassing the firewall using a VPN. Tool Action: Activity Insights would show a drop in 'web-browsing' activity but an increase in VPN application usage. Command Center would show VPN tunnel traffic bypassing policy checks.

Answer: (SHOW ANSWER)

The core problem here is rule order and shadowing. Rule evaluation in Palo Alto Networks firewalls is top-down. The 'Allow- Internal-HTTP' rule is very broad (any-any source/destination, Trust zone to Trust zone). If a user initiates web-browsing traffic to an external site, the traffic originates from the 'Trust' zone. If the 'Allow-Internal-HTTP' rule is positioned above 'Block-External-Browsing', it will be evaluated first. Since its destination is 'any' and application is 'web-browsing', it will match and allow the traffic, even if the actual destination is external. This is classic rule shadowing. Option A: Correct. Policy Optimizer is specifically designed to identify shadowed rules. Command Center's detailed session logs would clearly show that external HTTP traffic is hitting the 'Allow-Internal-HTTP' rule, not the intended 'Block-External-Browsing' rule. Option B: Incorrect. App-ID typically works on HTTP. If it weren't, Activity Insights would show 'unknown-tcp', but the policy explicitly uses 'web-browsing', implying App-ID is functional. Option C: Incorrect. The 'service' being 'any' in 'Block-External-Browsing' makes it less specific, but for an external destination from Trust, the 'Block-External-Browsing' rule (Trust to Untrust) should be hit. The issue isn't the service specificity itself for this scenario, but the preceding 'Allow-Internal-HTTP' rule's broadness and placement. Option D: Correct. This directly addresses the rule order issue. Policy Optimizer has a 'Rule Order' view (or equivalent features in optimization dashboards) that would visually highlight if 'Allow-Internal-HTTP' is above

'Block-External-Browsing'. Command Center would provide the empirical evidence of which rule is actually being hit by the traffic. Option E: Incorrect. While VPN bypass is a possibility in general, given the policy snippet, the most direct and likely cause of this specific observed behavior (contradicting an explicit block rule) is a policy logic error (shadowing/ordering), not an external bypass method.

NEW QUESTION: 99
When performing a "Push to Devices" from Panorama, an analyst wants to ensure that the push only affects a specific firewall in a shared Device Group. Which option in the push window allows this granular selection?
A. Include Device and Network Templates
B. Force Template Values
C. Edit Selections
D. Merge with Device Candidate Config
Answer: C (LEAVE A REPLY)
In a large environment with hundreds of firewalls, an analyst rarely wants to push a configuration to the entire fleet at once. After selecting "Push to Devices," the analyst should use the "Edit Selections" button.
This opens a window where the analyst can uncheck the boxes for any firewalls that should not receive the update. This allows for a "staged" rollout, where the analyst can push a configuration to a single test firewall before deploying it to production units. Granular push control is a critical objective for maintaining high availability and minimizing the "blast radius" of potential configuration errors. It ensures that the analyst can carefully manage the deployment lifecycle of security policies across a complex enterprise network.

NEW QUESTION: 100
To what must an interface be assigned before it can process traffic?
A. Security policy
B. Security Zone
C. Security profile
D. Security Protection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
What is the purpose of the automated commit recovery feature?
A. It reverts the Panorama configuration.
B. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.
C. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.
D. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 102
Which file is used to save the running configuration with a Palo Alto Networks firewall?
A. running-config.xml
B. running-configuration.xml
C. run-configuratin.xml
D. run-config.xml
Answer: (SHOW ANSWER)

NEW QUESTION: 103
What do you configure if you want to set up a group of objects based on their ports alone?

A. Address groups
B. Application groups
C. Custom objects
D. Service groups
Answer: D (LEAVE A REPLY)

NEW QUESTION: 104
In which two types of NAT can oversubscription be used? (Choose two.)
A. Static IP
B. Destination NAT
C. Dynamic IP and Port (DIPP)
D. Dynamic IP
Answer: C,D (LEAVE A REPLY)
Oversubscription is a feature that allows you to use more private IP addresses than public IP addresses for NAT. This means that multiple private IP addresses can share the same public IP address, as long as they use different ports. Oversubscription can be used in two types of NAT: Dynamic IP and Port (DIPP) and Dynamic IP. DIPP NAT translates both the source IP address and the source port number of the outgoing packets, and can have an oversubscription rate greater than 1. Dynamic IP NAT translates only the source IP address of the outgoing packets, and can have an oversubscription rate of 1 or less. Static IP and Destination NAT do not support oversubscription, as they require a one-to-one mapping between the private and public IP addresses. Reference: Source NAT, Configure NAT, NAT

NEW QUESTION: 105
An analyst needs to prevent users from downloading executable files from "High-Risk" URL categories while allowing them from "Business-and-Economy." Which profile should be configured to achieve this specific file-type restriction?
A. URL Filtering Profile
B. Data Filtering Profile
C. File Blocking Profile
D. Vulnerability Protection Profile
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
The File Blocking Profile is the primary tool used by Palo Alto Networks firewalls to control the movement of specific file types across the network. While a URL Filtering Profile (Option A) can block access to a website based on its category, it does not have the granular ability to distinguish between a PDF download and an EXE download on that site.
To meet the requirement, the analyst creates a File Blocking Profile with rules that target the .exe file extension. The profile allows the analyst to set actions like alert, block, or continue based on the direction of the traffic (upload or download) and the application being used. By attaching this profile to a Security policy rule, the firewall uses Content-ID to look deep into the payload-beyond just the file extension-to identify the true file type. This prevents users from bypassing security by simply renaming a malicious .exe file to .txt.
This is a core objective for ensuring that sanctioned web browsing does not become a vector for malware delivery.

NEW QUESTION: 106
An administrator has configured a Security policy where the matching condition includes a single application and the action is deny If the application s default deny action is reset-both what action does the firewall take*?
A. It silently drops the traffic
B. It sends a TCP reset to the server-side device
C. It sends a TCP reset to the client-side and server-side devices
D. It silently drops the traffic and sends an ICMP unreachable code
Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
A Network Security Analyst is tasked with investigating a persistent 'High Severity' alert on the Incidents and Alerts page, categorizing it as 'Malware Download'. Log Viewer analysis shows repeated 'threat' logs with 'file-type: PE', 'action: alert', and 'verdict: malicious' from WildFire. The logs consistently show the same internal source IP downloading the same malicious executable from various external, compromised web servers. Despite the alerts, the internal host remains infected. What is the MOST likely root cause of the persistent infection, and what advanced remediation steps should the analyst prioritize?
A. The firewall's WildFire profile is configured in 'monitor' mode instead of 'block'. The analyst should change the WildFire profile to 'block' or 'reset-both' for malicious verdicts and update the security policy.
B. The internal host is bypassing the firewall (e.g., using a VPN or direct internet access), so the malicious files are not traversing the firewall. The analyst should investigate network architecture and endpoint configurations.
C. The malicious file is polymorphic, and WildFire is only detecting some variants. The analyst should submit the observed malicious files manually to WildFire for deeper analysis and wait for new signatures.
D. The internal host is infected with persistent malware that re-downloads itself even after initial detection. The analyst must contain the host, initiate forensic analysis, and deploy endpoint detection and response (EDR) solutions.
E. The 'decryption profile' on the firewall is not enabled, preventing the firewall from inspecting encrypted traffic where the malware might be hidden. The analyst should enable SSL decryption.
Answer: D (LEAVE A REPLY)
The key phrase here is 'persistent infection' and 'repeated threat logs... from various external, compromised web servers' despite the firewall 'alerting' on the downloads. If the firewall is detecting the downloads and logging them, it implies traffic is traversing the firewall and WildFire is working. However, if the action is 'alert' only, the file is allowed to pass. Even with alerts, if the host remains infected and repeatedly downloads the same malware, the most likely root cause is a highly persistent malware on the internal host that automatically attempts to re- establish its presence or re-download components. Simply blocking future downloads (Option A) won't remediate the already infected host. Option B is less likely if the logs clearly show the firewall is seeing and alerting on the traffic. Option C suggests a detection gap, but the logs explicitly state 'verdict: malicious', implying detection is happening. Option E is plausible if no logs were being generated at all, but they are. Therefore, the priority shifts from network-level prevention to endpoint-level containment and remediation. Option D describes the correct and necessary advanced remediation steps for a persistent infection.

NEW QUESTION: 108
What is the most likely reason a primary data center firewall is no longer visible in the Strata Cloud Manager (SCM) dashboard?
A. Its environment is too complicated and cannot be onboarded in SCM.
B. Its firewall license has expired.
C. It does not have the appropriate device-level telemetry settings enabled.
D. User does not have the appropriate permissions.
Answer: (SHOW ANSWER)
Strata Cloud Manager relies on device-level telemetry to receive status, health, and visibility data from managed firewalls. If telemetry is not enabled or properly configured, the firewall cannot send information to SCM, causing it to be absent from the dashboard even though it may still be operational.

NEW QUESTION: 109
A Palo Alto Networks Network Security Analyst is tasked with optimizing security posture by decommissioning legacy, unused firewall rules. The challenge is identifying rules that genuinely have no active sessions or hit counts over an extended period (e.g., 6 months), distinguishing them from rules that might be critical but rarely triggered (e.g., a failover rule). Additionally, the analyst needs to propose a phased deprecation process to minimize risk. Which approach, integrating Command Center, Activity Insights, and Policy Optimizer, is most robust?
A. Use Policy Optimizer's 'Rule Usage' to identify rules with zero hit count over 6 months. 2. Delete these rules. 3. Monitor Command Center for any service disruptions.
B. 1. In Activity Insights, generate a report of all 'Application Usage' and 'User Activity' over 6 months to understand baseline traffic. 2. In Policy Optimizer, use the 'Security Policy Rule Optimization' dashboard to filter for rules with low hit counts over the last 6 months. 3. For these rules, change the action to 'Deny with Logging' and observe Command Center for new 'deny' logs. 4. If no legitimate denies, decommission the rule.

C. 1. In Policy Optimizer, specifically target 'any-any' rules with low hit counts. 2. For these rules, change action to 'Alert Only' and review Command Center daily for a week. 3. If no alerts, proceed with deletion.
D. 1. Utilize Command Center to view real-time session information for all active rules. 2. Identify rules with no active sessions. 3. Use Activity Insights to confirm these rules haven't had recent activity. 4. Delete the confirmed unused rules.
E. 1. In Policy Optimizer, use the 'Security Policy Rule Optimization' dashboard to identify rules with 'Low Usage'. 2. For rules identified as 'Low Usage' and having an 'any' source, destination, or service, change the rule's action to 'No Action' (or a similar audit mode if available) with logging enabled. 3. Monitor Command Center and Activity Insights over 3-6 months for any unintended traffic disruptions or legitimate session attempts hitting the 'No Action' rule. 4. If no issues, transition the rule to 'Deny' and then eventually delete after another grace period.
Answer: E (LEAVE A REPLY)
This is a comprehensive, risk-averse approach. Policy Optimizer's 'Security Policy Rule Optimization' is the core tool for identifying 'Low Usage' rules. The key differentiator here is the proposed phased deprecation: changing the rule to an 'audit mode' (like 'No Action' or setting an action that logs but doesn't block) first, and monitoring Command Center for real-time impact and Activity Insights for long-term trends. This allows for validation that the rule is truly unused without immediately causing an outage, especially for rarely-triggered but critical rules (like failover). Only after a prolonged monitoring period and confirmation of no impact should the rule be moved to 'Deny' and then finally deleted, minimizing risk.

NEW QUESTION: 110
Consider a scenario where a Palo Alto Networks firewall is configured with a Log Forwarding Profile named 'LFP Compliance SIEM'. This profile is attached to a Security Policy that permits outbound web access for internal users. The profile includes two syslog server destinations: 'Syslog_Archiver' (UDP, default format) and 'Syslog_SIEM' (TCP, CEF format). Due to a network change, the IP address of 'Syslog_SIEM' needs to be updated. Which of the following commands, executed in PAN-OS CLI operational mode, would allow verification of the currently configured Log Forwarding Profile details, specifically to confirm the change after it's applied?
A. `show log-forwarding profile LFP_Compliance_SIEM`
B. `show log forwarding profiles LFP_Compliance_SIEM`
C. `show running config | match LFP_Compliance_SIEM`
D. `show object log-forwarding profile LFP_Compliance_SIEM`
E. `show configuration full | grep 'log-forwarding-profile LFP_Compliance_SIEM'`
Answer: D (LEAVE A REPLY)
The correct command to display the details of an object, including Log Forwarding Profiles, is 'show object s. In this case, 'show object log-fomarding profile LFP_Compliance_SIEW will provide the detailed configuration of the profile, including syslog server definitions. Options A and B use incorrect syntax for showing objects. Options C and E are generic configuration searches that might show parts of the configuration but are not designed to present the structured object details efficiently for verification.

NEW QUESTION: 111
Which feature enables an administrator to review the Security policy rule base for unused rules?
A. Test Policy Match
B. Policy Optimizer
C. View Rulebase as Groups
D. Security policy tags eb
Answer: B (LEAVE A REPLY)
Policy Optimizer provides a simple workflow to migrate your legacy Security policy rulebase to an App-ID based rulebase, which improves your security by reducing the attack surface and gaining visibility into applications so you can safely enable them. Policy Optimizer can also identify unused rules, duplicate rules, and rules that can be merged or reordered to optimize your rulebase. You can use Policy Optimizer to review the usage statistics of your rules and take actions to clean up or modify your rulebase as needed1. Reference: Security Policy Rule Optimization, Updated Certifications for PAN-OS 10.1, Free PCNSE Questions for Palo Alto Networks PCNSE Exam

NEW QUESTION: 112
An administrator observes that an External Dynamic List (EDL) is not updating as expected. The last updated timestamp is several days old, but the source URL is confirmed to be accessible from another host on the network. What is the most likely cause of this issue on the Palo Alto Networks firewall?

A. The EDL's 'Repeat' interval is set to 'Never'.
B. The security policy allowing traffic from the firewall to the EDL source has been disabled or incorrectly configured.
C. The firewall's system clock is out of sync with the EDL source server.
D. The EDL source file exceeds the maximum supported size for the firewall model.
E. The EDL is configured with a 'Certificate Profile' that is no longer valid.
Answer: B (LEAVE A REPLY)
If the EDL source is accessible from another host but the firewall isn't updating, the most likely cause is that the firewall itself cannot reach the source. This typically points to a security policy issue preventing the firewall's management plane from establishing an outbound connection to the EDL source. While other options like 'Repeat' interval (A) or file size (D) could cause issues, a security policy blocking access is a very common troubleshooting point when connectivity fails. Clock sync (C) or certificate profile (E) are less common for basic connectivity issues, though a certificate issue would prevent HTTPS fetching.

NEW QUESTION: 113
Based on the image provided, which two statements apply to the Security policy rules? (Choose two.)

				Source			Destination						
	NAME	TAGS	TYPE	ZONE	ADDRESS	DEVICE	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
19	Allow-Office-Programs	none	universal	Internal	any	any	External	any	office-programs	application-defa...	Allow		
20	Allow-FTP	none	universal	Internal	any	any	External	FTP Server	any	FTP	Allow		
21	Allow-Social-Media	none	universal	Internal	any	any	External	any	facebook	application-defa...	Allow		
22	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	
23	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	

A. The Allow-Office-Programs rule is using an application group.
B. The Allow-Office-Programs rule is using an application filter.
C. In the Allow-FTP policy, FTP is allowed using App-ID.
D. The Allow-Social-Media rule allows all Facebook functions.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 114
Which two features implement one-to-one translation of a source IP address while allowing the source port to change? (Choose two.)
A. Static IP
B. Dynamic IP / Port Fallback
C. Dynamic IP
D. Dynamic IP and Port (DIPP)
Answer: A,D (LEAVE A REPLY)
Static IP and Dynamic IP and Port (DIPP) are two features that implement one-to-one translation of a source IP address while allowing the source port to change. Static IP translates a single source address to a specific public address, and allows the source port to change dynamically1. Dynamic IP and Port (DIPP) translates the source IP address or range to a single IP address, and uses the source port to differentiate between multiple source IPs that share the same translated address2. Both of these features provide a one-to-one translation of IP addresses, but do not restrict the source port. References:
* Static IP - Palo Alto Networks
* Dynamic IP and Port - Palo Alto Networks

NEW QUESTION: 115

Which policy set should be used to ensure that a policy is applied just before the default security rules?
A. Parent device-group post-rulebase
B. Child device-group post-rulebase
C. Local Firewall policy
D. Shared post-rulebase
Answer: D (LEAVE A REPLY)
The policy set that should be used to ensure that a policy is applied just before the default security rules is the shared post-rulebase. The shared post-rulebase is a set of Security policy rules that are defined on Panorama and apply to all firewalls or device groups. The shared post-rulebase is evaluated after the local firewall policy and the child device-group post-rulebase, but before the default security rules. The shared post-rulebase can be used to enforce common security policies across multiple firewalls or device groups, such as blocking high-risk applications or traffic1. Reference: Security Policy Rule Hierarchy, Security Policy Rulebase, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 116
A Security Operations Center (SOC) analyst is investigating a persistent outbound connection from an internal host to a known malicious IP address, despite an existing security policy attempting to block it. The analyst suspects policy shadowing or a misconfigured NAT rule. Which combination of Palo Alto Networks management tools would be most effective for rapidly identifying the root cause and verifying policy effectiveness?
A. Command Center for real-time traffic monitoring and Activity Insights for policy hit count analysis.
B. Policy Optimizer for identifying shadowed rules and Command Center for detailed session logs.
C. Activity Insights for application usage trends and Command Center for VPN tunnel status.
D. Policy Optimizer for rule cleanup and Panorama Device Groups for policy inheritance visualization.
E. Command Center for threat intelligence correlation and Policy Optimizer for security profile optimization.
Answer: (SHOW ANSWER)
Policy Optimizer is designed to identify shadowed rules, unused rules, and overly broad rules, which directly addresses the suspicion of policy shadowing. Command Center's ability to display detailed session logs, including matching policies and NAT rules, is crucial for verifying if the policy is indeed being hit or if NAT is altering the traffic in an unexpected way. Activity Insights provides broader trends, not granular session data for real-time troubleshooting.

NEW QUESTION: 117
Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)
A. Panorama
B. AutoFocus
C. GlobalProtect
D. Aperture
Answer: (SHOW ANSWER)

NEW QUESTION: 118
A Palo Alto Networks firewall, deployed as an internet edge device, experiences a sudden and severe performance degradation, with packet queues building up significantly and high latency for all outbound traffic. The firewall's system logs show repeated 'HA link flapping' messages, even though the physical HA links appear fine. No configuration changes were recently deployed. You suspect a 'split-brain' scenario or a misconfiguration impacting the HA state. Which of the following is the MOST PROBABLE cause, and what immediate action would you take to stabilize the environment (assuming a redundant setup)?
A. A network loop is detected on an interface participating in H Immediately disable HA preemption on both firewalls and then review network topology for loops.
B. The HA path monitoring or link monitoring thresholds are too aggressive, causing false positives. Increase the thresholds for path and link monitoring and commit.
C. The HA control link (heartbeat) is experiencing excessive latency or packet loss, leading to perceived link flapping. Check latency on the HA control link and consider relocating it or addressing congestion on the interconnect.
D. Acritical interface configured for HA path monitoring has failed on the active firewall, causing it to declare itself passive, but the passive firewall is also experiencing issues preventing it from becoming active. Manually force a failover to the healthy firewall using request high-availability state functional-hold if possible, or reboot the currently active firewall.

E. The HA configuration for the data plane is out of sync between the active and passive firewalls, causing traffic processing errors. Push a full configuration sync from the active device to the passive device using request high-availability synchronize configuration.

Answer: C,D (LEAVE A REPLY)

This is a multiple-response question. High latency/packet loss on the HA control link (heartbeat) (Option C) is a very common cause of 'HA link flapping' symptoms, as the firewalls cannot reliably communicate their health and state, leading to repeated role changes or split-brain. This directly impacts performance. Option D addresses a 'split-brain' or failed failover scenario where both units might be trying to be active or neither is fully active, leading to traffic disruption. Forcing a failover or rebooting a problematic active unit can restore service in such cases. Option A, while possible, is less directly indicated by 'HA link flapping' on the firewall itself unless it's impacting the HA links directly. Option B (increasing thresholds) is a long-term tuning, not an immediate fix for severe performance degradation. Option E addresses config sync, which can cause other issues, but not typically 'HA link flapping' in isolation if the config was already synchronized.

NEW QUESTION: 119

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 389

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 120

Which three Ethernet interface types are configurable on the Palo Alto Networks firewall? (Choose three.)

A. Virtual Wire

B. Tap

C. Dynamic

D. Layer 3

E. Static

Answer: A,B,D (LEAVE A REPLY)

Palo Alto Networks firewalls support three types of Ethernet interfaces that can be configured on the firewall:

virtual wire, tap, and layer 31. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:

Virtual Wire: A virtual wire interface allows the firewall to transparently pass traffic between two network segments without modifying the packets or affecting the routing. The firewall can still apply security policies and inspect the traffic based on the source and destination zones of the virtual wire2.

Tap: A tap interface allows the firewall to passively monitor traffic from a network switch or router without affecting the traffic flow. The firewall can only receive traffic from a tap interface and cannot send traffic out of it. The firewall can apply security policies and inspect the traffic based on the source and destination zones of the tap interface3.

Layer 3: A layer 3 interface allows the firewall to act as a router and participate in the network routing. The firewall can send and receive traffic from a layer 3 interface and apply security policies and inspect the traffic based on the source and destination IP addresses and zones of the interface4.

References: Ethernet Interface Types, Virtual Wire Interfaces, Tap Interfaces, Layer 3 Interfaces, Updated Certifications for PAN-OS 10.1, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 121

Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

A. global
B. universal
C. interzone
D. intrazone
Answer: B (LEAVE A REPLY)

Valid NetSec-Analyst Dumps shared by TrainingDump.com for Helping Passing NetSec-Analyst Exam! TrainingDump.com now offer the **newest NetSec-Analyst exam dumps**, the TrainingDump.com NetSec-Analyst exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com NetSec-Analyst dumps with Test Engine here: https://www.trainingdump.com/Palo-Alto-Networks/NetSec-Analyst-practice-exam-dumps.html (**120** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)