Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

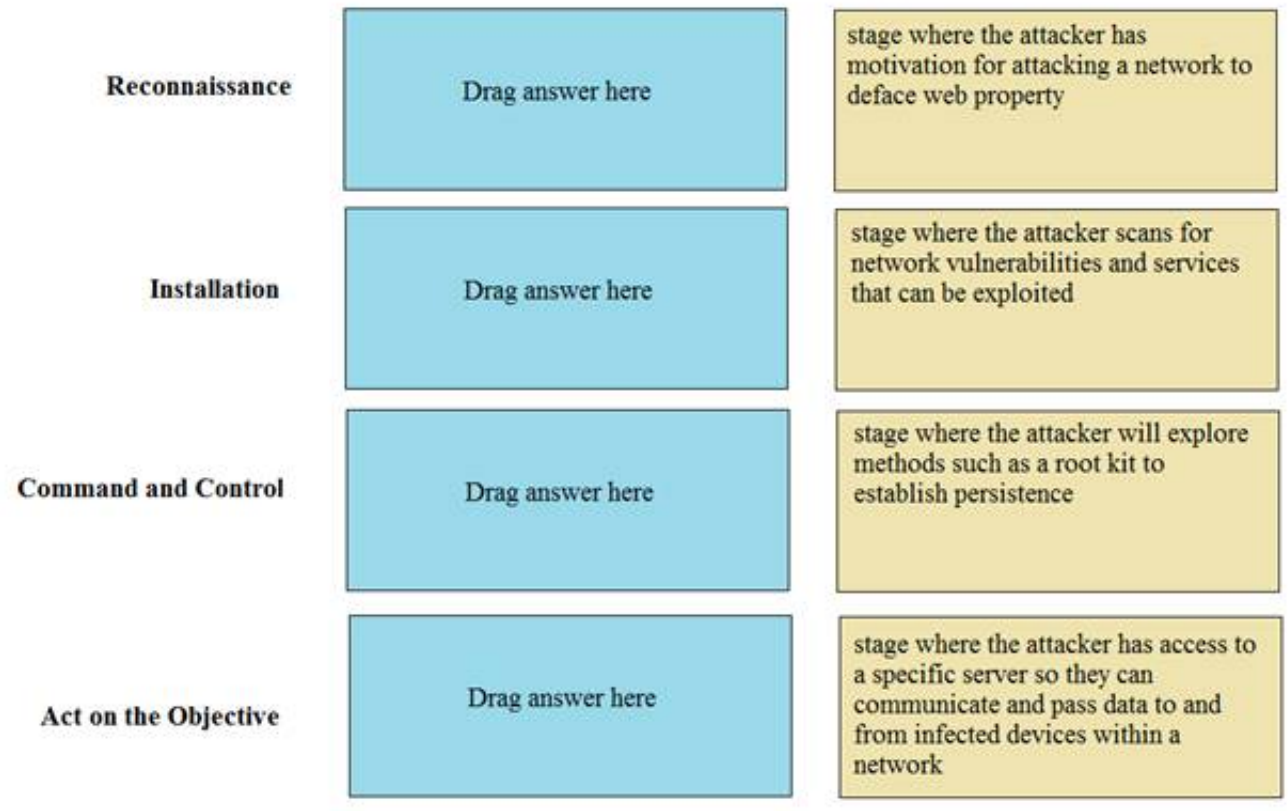
NEW QUESTION 1
Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

A. URL traffic
B. vulnerability protection
C. anti-spyware
D. antivirus

Answer: C

Explanation:

NEW QUESTION 2
DRAG DROP
Match the Cyber-Attack Lifecycle stage to its correct description.



A. Mastered
B. Not Mastered

Answer: A

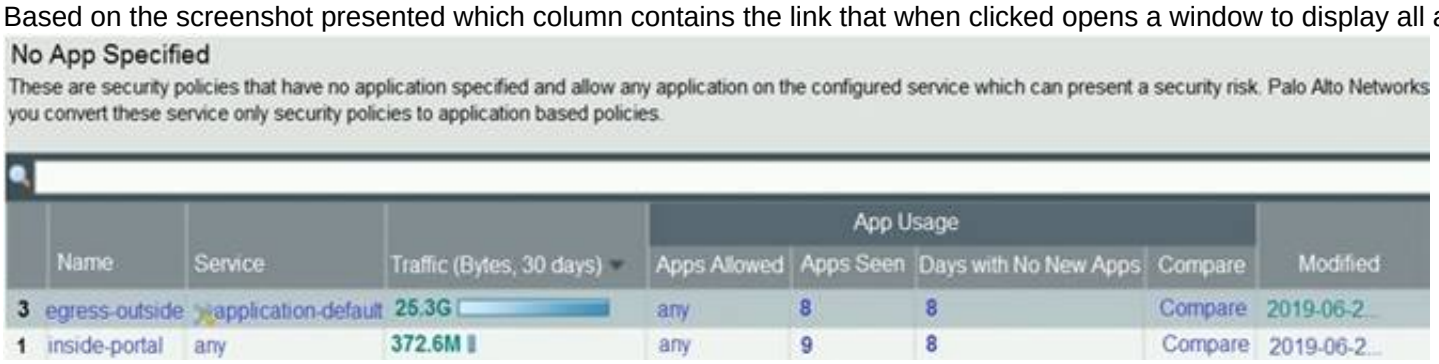
Explanation:
Reconnaissance – stage where the attacker scans for network vulnerabilities and services that can be exploited.
Installation – stage where the attacker will explore methods such as a root kit to establish persistence
Command and Control – stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.
Act on the Objective – stage where an attacker has motivation for attacking a network to deface web property

NEW QUESTION 3
What is a prerequisite before enabling an administrative account which relies on a local firewall user database?

A. Configure an authentication policy
B. Configure an authentication sequence
C. Configure an authentication profile
D. Isolate the management interface on a dedicated management VLAN

Answer: C

NEW QUESTION 4
Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?



A. Apps Allowed
B. Name
C. Apps Seen
D. Service

Answer: C

NEW QUESTION 5
Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet`s source and destination IP address?

A. DoS protection
B. URL filtering
C. packet buffering
D. anti-spyware

Answer: A

NEW QUESTION 6
Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?

A. global
B. intrazone
C. interzone
D. universal

Answer: C

Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content- updates/dynamic-contentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within% 20a%20minute%20of %20availability

NEW QUESTION 7
You receive notification about a new malware that infects hosts An infection results in the infected host attempting to contact a command-and-control server Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?

A. Antivirus Profile
B. Data Filtering Profile
C. Vulnerability Protection Profile
D. Anti-Spyware Profile

Answer: D

Explanation:
Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.

NEW QUESTION 8
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

A. SAML
B. TACACS+
C. LDAP
D. Kerberos

Answer: AB

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

NEW QUESTION 9
Which action results in the firewall blocking network traffic with out notifying the sender?

A. Drop
B. Deny
C. Reset Server
D. Reset Client

Answer: B

NEW QUESTION 10
Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choices to block the sameURL then which choice would be the last to block access to the URL?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The precedence is from the top down; First Match Wins: 1) Block list: Manually entered blocked URLs Objects - 2) Allow list: Manually entered allowed URLs Objects - 3) Custom URL Categories - 4) Cached Cached: URLs learned from External Dynamic Lists (EDLs) - 5) Pre-Defined Categories: PAN-DB or Brightcloud categories.

NEW QUESTION 10
How do you reset the hit count on a security policy rule?

A. First disable and then re-enable the rule.
B. Reboot the data-plane.
C. Select a Security policy rule, and then select Hit Count > Reset.
D. Type the CLI command reset hitcount <POLICY-NAME>.

Answer: C

NEW QUESTION 11
Which rule type is appropriate for matching traffic both within and between the source and destination zones?

A. interzone
B. shadowed
C. intrazone
D. universal

Answer: A

NEW QUESTION 12

Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)

A. Layer 2
B. Virtual Wire
C. Tap
D. Layer 3
E. HA

Answer: BDE

NEW QUESTION 16
Which option is part of the content inspection process?

A. IPsec tunnel encryption
B.

Packet egress process

C. SSL Proxy re-encrypt
D. Packet forwarding process

Answer: C

NEW QUESTION 20
In a security policy what is the quickest way to rest all policy rule hit counters to zero?

A. Use the CLI enter the command reset rules all
B. Highlight each rule and use the Reset Rule Hit Counter > Selected Rules.
C. use the Reset Rule Hit Counter > All Rules option.
D. Reboot the firewall.

Answer: C

NEW QUESTION 21
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

A. GlobalProtect agent
B. XML API
C.

User-ID Windows-based agent
D. log forwarding auto-tagging

Answer: BC

NEW QUESTION 26
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. Mastered
B. Not Mastered

Answer: A

Explanation:
Export Named Configuration Snapshot This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

NEW QUESTION 27
Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	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. any port
B. same port as ssl and snmpv3
C. the default port
D. only ephemeral ports

Answer: C

NEW QUESTION 31
Which option lists the attributes that are selectable when setting up an Application filters?

A. Category, Subcategory, Technology, and Characteristic
B. Category, Subcategory, Technology, Risk, and Characteristic
C. Name, Category, Technology, Risk, and Characteristic
D. Category, Subcategory, Risk, Standard Ports, and Technology

Answer: B

Explanation:
Explanation/Reference: Reference:
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects- application- filters

NEW QUESTION 33
What is the main function of the Test Policy Match function?

A. verify that policy rules from Expedition are valid
B. confirm that rules meet or exceed the Best Practice Assessment recommendations
C. confirm that policy rules in the configuration are allowing/denying the correct traffic
D. ensure that policy rules are not shadowing other policy rules

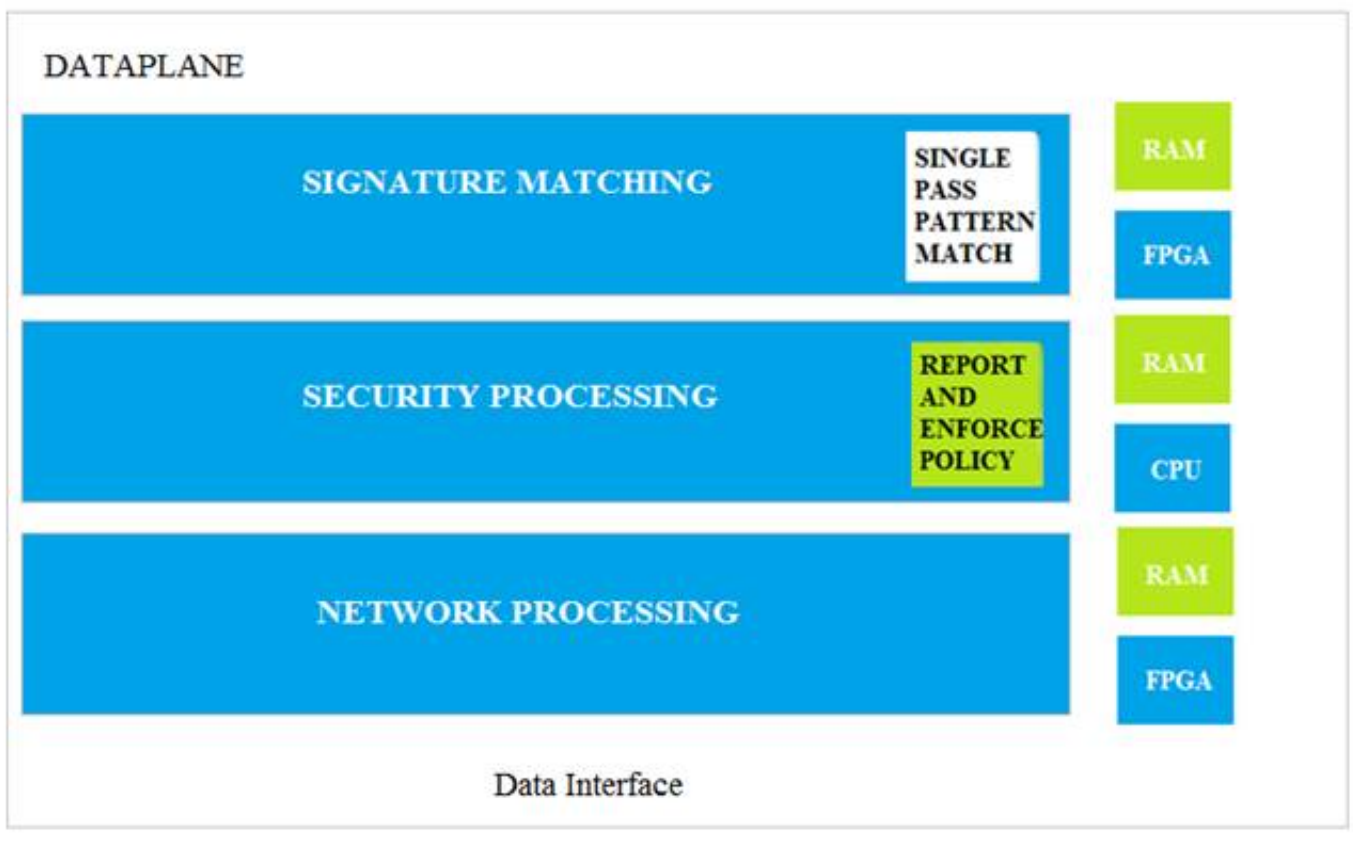
Answer: D

NEW QUESTION 36
What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

A. every 30 minutes
B. every 5 minutes
C. once every 24 hours
D. every 1 minute

Answer: D

NEW QUESTION 37
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



A. Signature Matching
B. Network Processing
C. Security Processing
D. Security Matching

Answer: A

NEW QUESTION 39
All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone.
Complete the empty field in the Security policy using an application object to permit only this type of access.
Source Zone: Internal - Destination Zone: DMZ Zone -
Application:
Service: application-default -
Action: allow

A. Application = "any"
B. Application = "web-browsing"
C. Application = "ssl"
D. Application = "http"

Answer: B

NEW QUESTION 40
You receive notification about new malware that infects hosts through malicious files transferred by FTP.
Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?

A. URL Filtering profile applied to inbound Security policy rules.

B. Data Filtering profile applied to outbound Security policy rules.
C. Antivirus profile applied to inbound Security policy rules.
D. Vulnerability Protection profile applied to outbound Security policy rules.

Answer: C

Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION 41
A server-admin in the USERS-zone requires SSH-access to all possible servers in all current and future Public Cloud environments. All other required connections have already been enabled between the USERS- and the OUTSIDE-zone. What configuration-changes should the Firewall-admin make?

A. Create a custom-service-object called SERVICE-SSH for destination-port-TCP-22. Create a security-rule between zone USERS and OUTSIDE to allow traffic from any source IP-address to any destination IP-address for SERVICE-SSH
B. Create a security-rule that allows traffic from zone USERS to OUTSIDE to allow traffic from any source IP-address to any destination IP-address for application SSH
C. In addition to option a, a custom-service-object called SERVICE-SSH-RETURN that contains source-port-TCP-22 should be create
D. A second security-rule is required that allows traffic from zone OUTSIDE to USERS for SERVICE-SSH-RETURN for any source- IP-address to any destination-Ip-address

SSH from any source-IP-address to any
E. In addition to option c, an additional rule from zone OUTSIDE to USERS for application
destination-IP-address is required to allow the return-traffic from the SSH-servers to reach the server-admin

Answer: B

NEW QUESTION 45
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

A. Management
B. High Availability
C. Aggregate
D. Aggregation

Answer: C

NEW QUESTION 49
Which profile should be used to obtain a verdict regarding analyzed files?

A. WildFire analysis
B. Vulnerability profile
Content-ID
C
D: Advanced threat prevention

Answer: A

Explanation:
? A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic1.
? There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis1.
? The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination2. WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware3. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats34.
? The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities. It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational5.
? Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.
? Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus.
Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.
References:
1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto
Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks : [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

NEW QUESTION 53
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

Explanation:
? 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 58
Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?

A. data
B. network processing
C. management
D. security processing

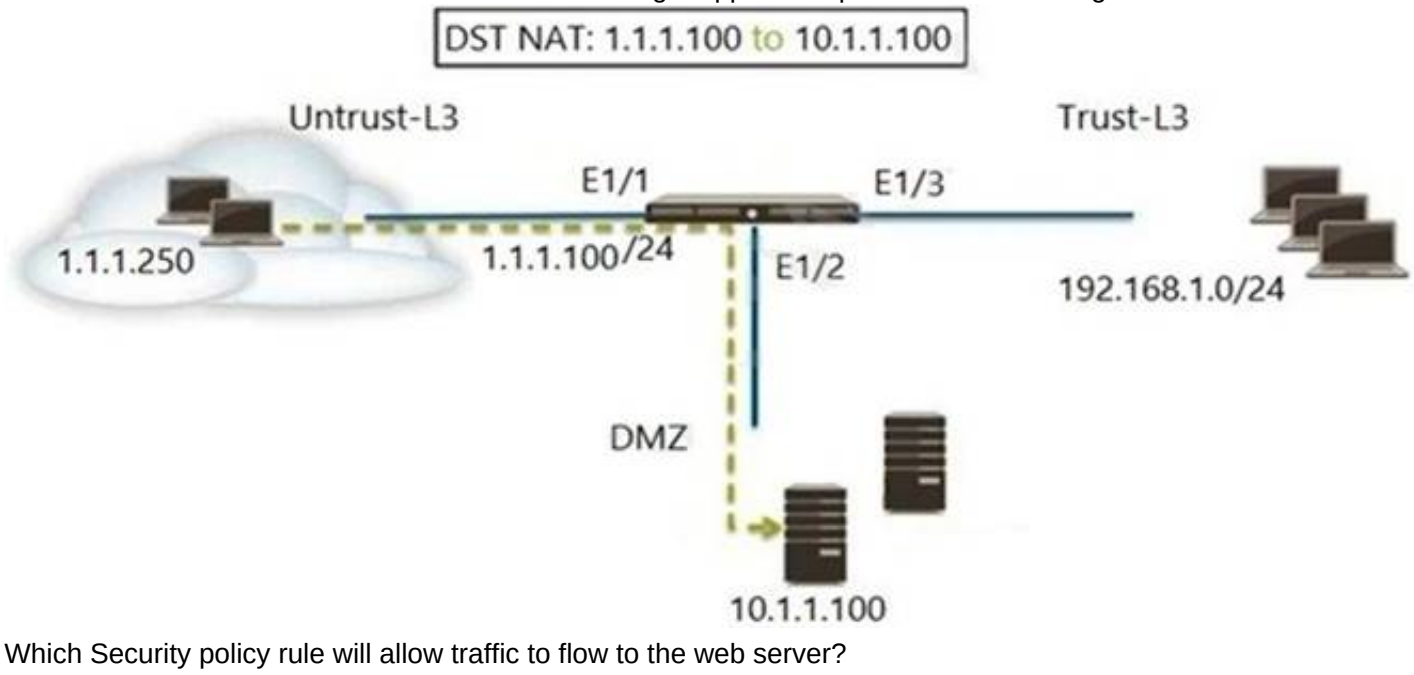
Answer: C

NEW QUESTION 59
The CFO found a malware infected USB drive in the parking lot, which when inserted infected their corporate laptop the malware contacted a known command-and-control server which exfiltrating corporate data.
Which Security profile feature could have been used to prevent the communications with the command-and-control server?

A. Create a Data Filtering Profile and enable its DNS sinkhole feature.
B. Create an Antivirus Profile and enable its DNS sinkhole feature.
C. Create an Anti-Spyware Profile and enable its DNS sinkhole feature.
D. Create a URL Filtering Profile and block the DNS sinkhole URL category.

Answer: C

NEW QUESTION 64
Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



Which Security policy rule will allow traffic to flow to the web server?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping

NEW QUESTION 69
An internal host wants to connect to servers of the internet through using source NAT. Which policy is required to enable source NAT on the firewall?

A. NAT policy with source zone and destination zone specified
B. post-NAT policy with external source and any destination address
C. NAT policy with no source of destination zone selected
D. pre-NAT policy with external source and any destination address

Answer: A

NEW QUESTION 72
Based on the screenshot what is the purpose of the included groups?

			Source			Destination				
	Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

A. They are only groups visible based on the firewall's credentials.

B. They are used to map usernames to group names.
C. They contain only the users you allow to manage the firewall.
D. They are groups that are imported from RADIUS authentication servers.

Answer: B

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to- groups.html

NEW QUESTION 76
Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	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. 80
B. 53
C. 22
D. 23

Answer: C

Explanation:

NEW QUESTION 78
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

Explanation:
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 82
What do dynamic user groups you to do?

A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
D. create a dynamic list of firewall administrators

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id- features/dynamic-user-
groups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintai ning%20user%20visibility.

NEW QUESTION 85
The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.
Which security profile feature could have been used to prevent the communication with the CnC server?

A. Create an anti-spyware profile and enable DNS Sinkhole
B. Create an antivirus profile and enable DNS Sinkhole
C. Create a URL filtering profile and block the DNS Sinkhole category
D. Create a security policy and enable DNS Sinkhole

Answer: A

Explanation:

NEW QUESTION 90
What must be configured before setting up Credential Phishing Prevention?

A. Anti Phishing Block Page
B. Threat Prevention
C. Anti Phishing profiles
D. User-ID

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat- prevention/prevent-credential-phishing/set-up-credential-phishing-prevention

NEW QUESTION 95
The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

A. Add zones attached to interfaces to the virtual router
B. Add interfaces to the virtual router
C. Enable the redistribution profile to redistribute connected routes
D. Add a static routes to route between the two interfaces

Answer: D

Explanation:

NEW QUESTION 99
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

A. Threat Prevention License
B. Threat Implementation License
C. Threat Environment License
D. Threat Protection License

Answer: A

NEW QUESTION 104
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. intrazone
C. interzone
D. universal

Answer: D

Explanation:

00ClomCAC
References:https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000

NEW QUESTION 108
Which path in PAN-OS 10.0 displays the list of port-based security policy rules?

A. Policies> Security> Rule Usage> No App Specified
B. Policies> Security> Rule Usage> Port only specified
C. Policies> Security> Rule Usage> Port-based Rules
D. Policies> Security> Rule Usage> Unused Apps

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules.html

NEW QUESTION 110
What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

A. Blometric scanning results from iOS devices
B. Firewall logs
C. Custom API scripts
D. Security Information and Event Management Systems (SIEMS), such as Splun
E. DNS Security service

Answer: BCE

NEW QUESTION 113
Complete the statement. A security profile can block or allow traffic

A. on unknown-tcp or unknown-udp traffic
B. after it is matched by a security policy that allows traffic
C. before it is matched by a security policy
D. after it is matched by a security policy that allows or blocks traffic

Answer: B

Explanation:
Security profiles are objects added to policy rules that are configured with an action of allow.

NEW QUESTION 118
Which tab would an administrator click to create an address object?

A. Device
B. Policies
C. Monitor
D. Objects

Answer: D

NEW QUESTION 123
Which type of administrator account cannot be used to authenticate user traffic flowing through the firewall's data plane?

A. Kerberos user
B. SAML user
C. local database user
D. local user

Answer: B

NEW QUESTION 125
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?

A. Review Apps
B. Review App Matches
C. Pre-analyze
D. Review Policies

Answer: D

Explanation:

NEW QUESTION 127
By default, what is the maximum number of templates that can be added to a template stack?

A. 6
B. 8
C. 10
D. 12

Answer: B

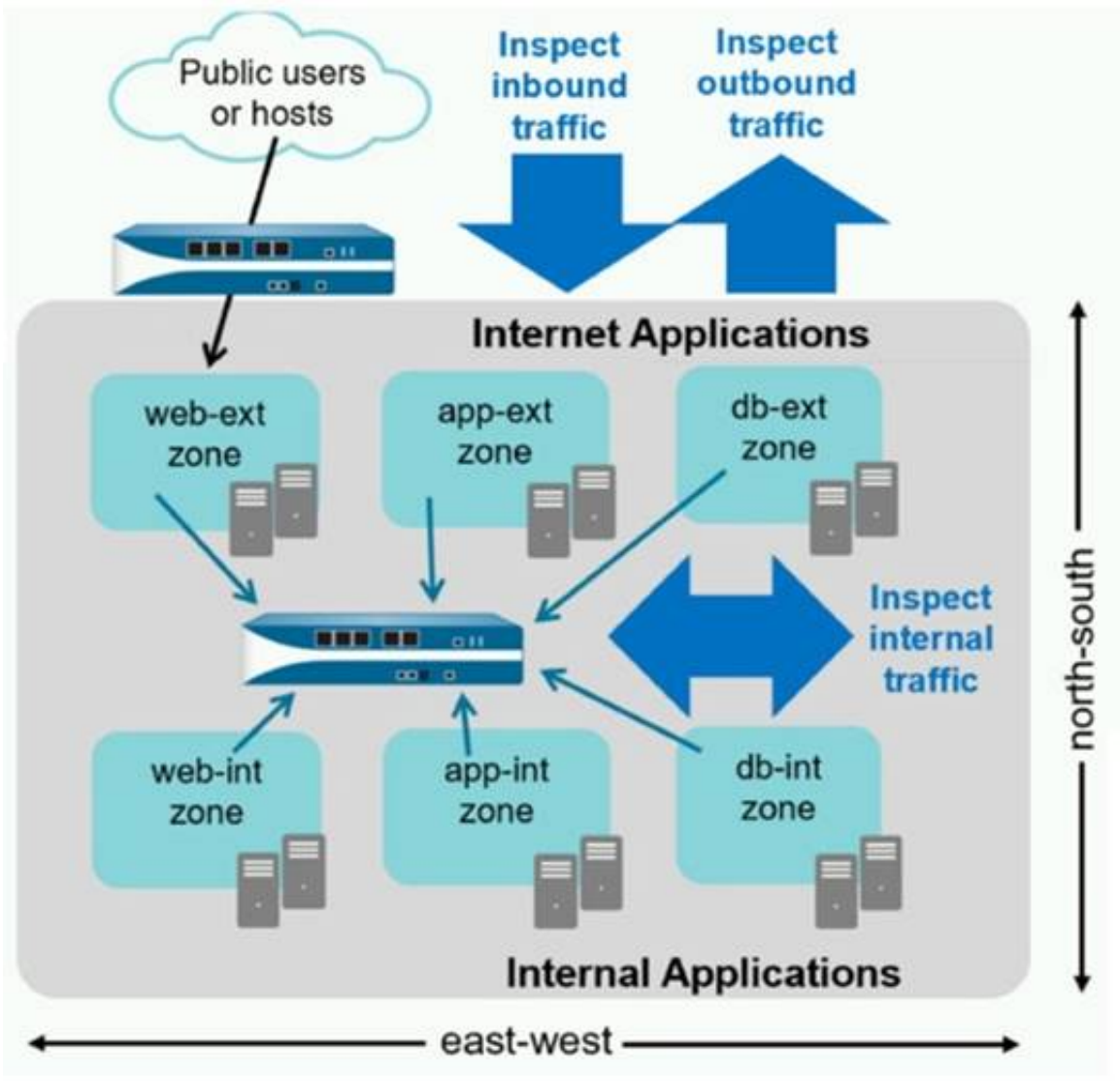
Explanation:
By default, the maximum number of templates that can be added to a template stack is 8. This is the recommended limit for performance reasons, as adding more templates may result in sluggish responses on the user interface. However, starting from PAN-OS 8.1.10 and 9.0.4, you can use a debug command to increase the maximum number of templates per stack to 16. This command requires a commit operation to take effect.
A template stack is a collection of templates that you can use to push common settings to multiple firewalls or Panorama managed collectors. A template contains the network and device settings that you want to share across devices, such as interfaces, zones, virtual routers, DNS, NTP, and login banners. You can create multiple templates for different device groups or locations and add them to a template stack in a hierarchical order. The settings in the lower templates override the settings in the higher templates if there are any conflicts. You can then assign a template stack to one or more devices and push the configuration changes.

NEW QUESTION 128
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see the traffic?

A. Traffic is being denied on the interzone-default policy.
B. The Log Forwarding profile is not configured on the policy.
C. The interzone-default policy is disabled by default
D. Logging on the interzone-default policy is disabled

Answer: D

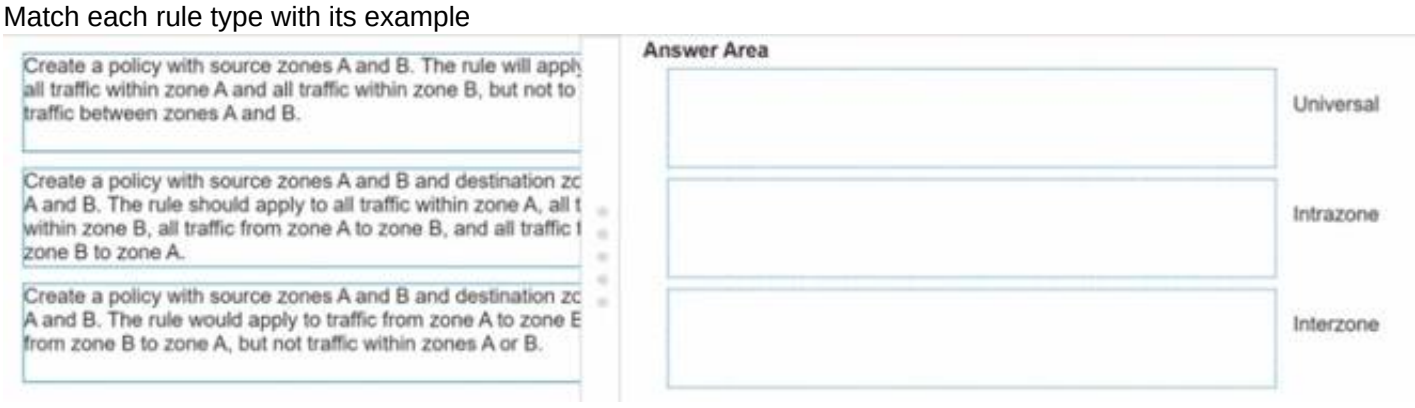
NEW QUESTION 131
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



A. branch office traffic
B. north-south traffic
C. perimeter traffic
D. east-west traffic

Answer: D

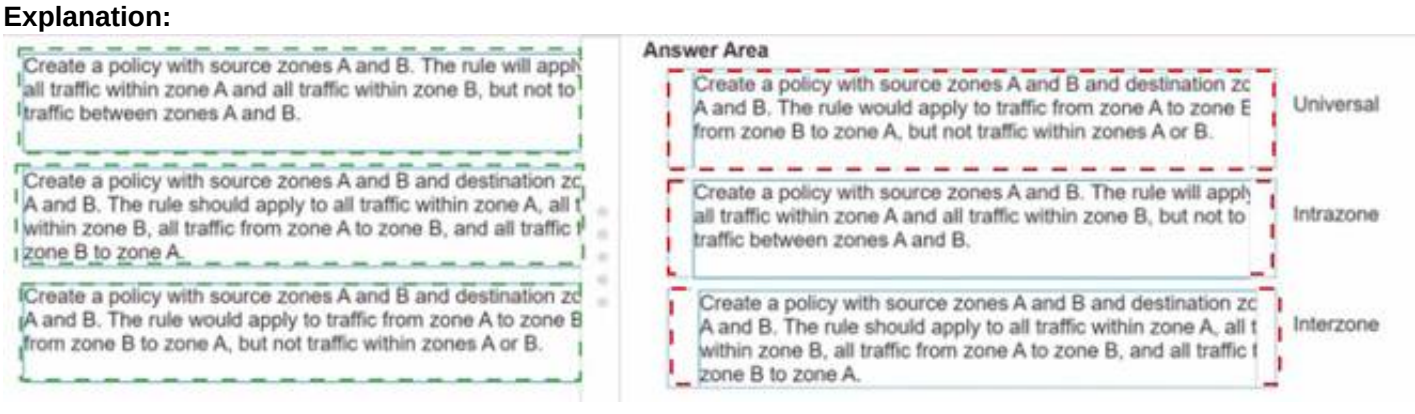
NEW QUESTION 133
DRAG DROP
Match each rule type with its example



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 136
What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?

A. Increase the backup capacity for configuration backups per firewall
B. Increase the per-firewall capacity for address and service objects
C. Reduce the configuration and session synchronization time between HA pairs
D. Reduce the number of objects pushed to a firewall

Answer: D

NEW QUESTION 140
Which path is used to save and load a configuration with a Palo Alto Networks firewall?

A. Device>Setup>Services
B. Device>Setup>Management
C. Device>Setup>Operations
D. Device>Setup>Interfaces

Answer: C

NEW QUESTION 143
What are three Palo Alto Networks best practices when implementing the DNS Security Service? (Choose three.)

A. Implement a threat intel program.
B. Configure a URL Filtering profile.
C. Train your staff to be security aware.
D. Rely on a DNS resolver.
E. Plan for mobile-employee risk

Answer: ABD

NEW QUESTION 146
An administrator is reviewing the Security policy rules shown in the screenshot below. Which statement is correct about the information displayed?

A. Eleven rules use the "Infrastructure* tag.
B. The view Rulebase as Groups is checked.
C. There are seven Security policy rules on this firewall.
D. Highlight Unused Rules is checked.

Answer: B

Explanation:

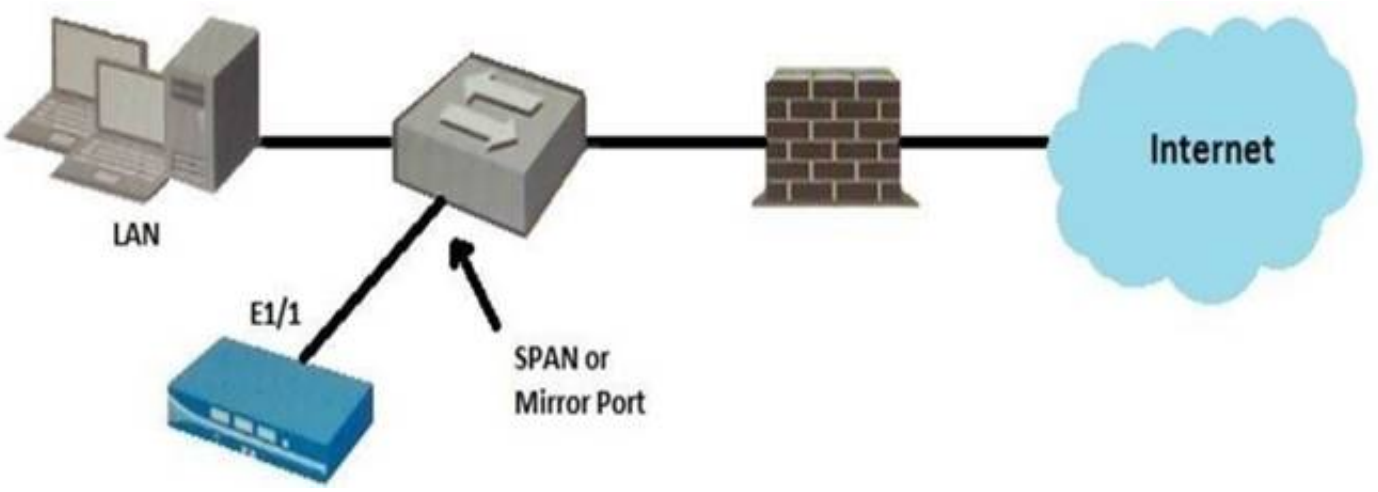
NEW QUESTION 147
According to the best practices for mission critical devices, what is the recommended interval for antivirus updates?

A. by minute
B. hourly
C. daily
D. weekly

Answer: C

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-mission- critical.html

NEW QUESTION 151
Given the topology, which zone type should you configure for firewall interface E1/1?



A. Tap
B. Tunnel
C. Virtual Wire
D. Layer3

Answer: A

NEW QUESTION 154
An administrator has an IP address range in the external dynamic list and wants to create an exception for one specific IP address in this address range.
Which steps should the administrator take?

A. Add the address range to the Manual Exceptions list and exclude the IP address by selecting the entry.
B. Add each IP address in the range as a list entry and then exclude the IP address by adding it to the Manual Exceptions list.
C. Select the address range in the List Entries list
D. A column will open with the IP addresse
E. Select the entry to exclude.
F. Add the specific IP address from the address range to the Manual Exceptions list by using regular expressions to define the entry.

Answer: D

NEW QUESTION 158
The firewall sends employees an application block page when they try to access Youtube. Which Security policy rule is blocking the youtube application?

			Source		Destination						
	Name	**Type**	**Zone**	**Address**	**Zone**	**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. Deny Google
C. allowed-security services
D. interzone-default

Answer: D

NEW QUESTION 161
For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?

A. TACACS+
B. RADIUS
C. LDAP
D. SAML

Answer: C

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-an-authenticationprofile-and-sequence

NEW QUESTION 164
An administrator is investigating a log entry for a session that is allowed and has the end reason of aged-out. Which two fields could help in determining if this is normal? (Choose

two.)

A. Packets sent/received
B. IP Protocol
C. Action
D. Decrypted

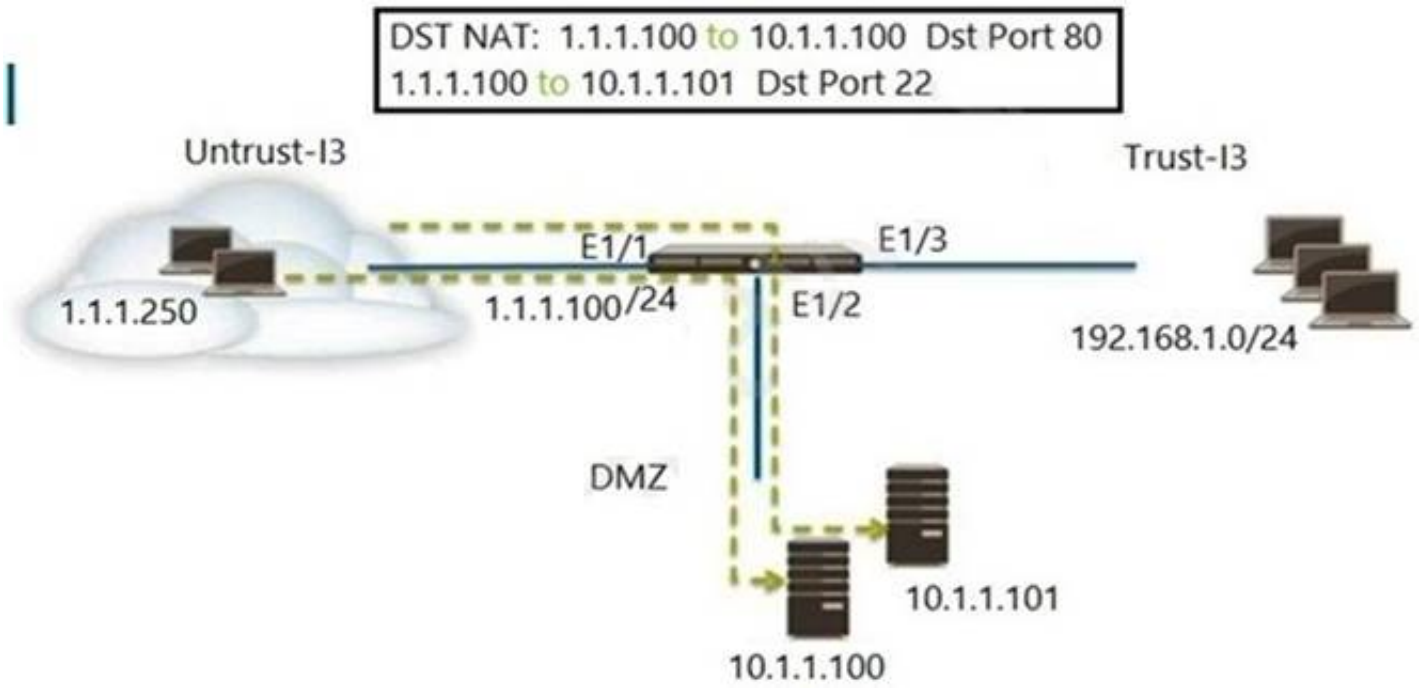
Answer: BD

NEW QUESTION 165
Palo Alto Networks firewall architecture accelerates content map minimizing latency using which two components'? (Choose two)

A. Network Processing Engine
B. Single Stream-based Engine
C. Policy Engine
D. Parallel Processing Hardware

Answer: B

NEW QUESTION 167
FILL IN THE BLANK
Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.



Which two Security policy rules will accomplish this configuration? (Choose two.) A- Untrust (Any) to DMZ (1.1.1.100), ssh - Allow

A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
C. Untrust (Any)to DMZ (10.1.1.100. 10.1.1.101), ssh, web-browsing-Allow
D. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow

Answer: AE

NEW QUESTION 172
Why should a company have a File Blocking profile that is attached to a Security policy?

A. To block uploading and downloading of specific types of files
B. To detonate files in a sandbox environment
C. To analyze file types
D. To block uploading and downloading of any type of files

Answer: A

NEW QUESTION 175
An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?

A. Disable all logging
B. Enable Log at Session End
C. Enable Log at Session Start
D. Enable Log at both Session Start and End

Answer: B

Explanation:

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clt5CAC

NEW QUESTION 176
Why does a company need an Antivirus profile?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 179
Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)

A. XML API
B. log forwarding auto-tagging
C. GlobalProtect agent
D. User-ID Windows-based agent

Answer: AD

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

NEW QUESTION 182
The PowerBall Lottery has reached a high payout amount and a company has decided to help employee morale by allowing employees to check the number, but doesn't want to unblock the gambling URL category.
Which two methods will allow the employees to get to the PowerBall Lottery site without the company unlocking the gambling URL category? (Choose two.)

A. Add all the URLs from the gambling category except powerball.com to the block list and then set the action for the gambling category to allow.
B. Manually remove powerball.com from the gambling URL category.
C. Add *.powerball.com to the allow list
D. Create a custom URL category called PowerBall and add *.powerball.com to the category and set the action to allow.

Answer: CD

Explanation:

NEW QUESTION 185
URL categories can be used as match criteria on which two policy types? (Choose two.)

A. authentication
B. decryptionC application override
C. NAT

Answer: AB

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-category-as-policy-match-criteria.html

NEW QUESTION 189
An administrator wants to prevent users from submitting corporate credentials in a phishing attack.
Which Security profile should be applied?

A. antivirus
B. anti-spyware
C. URL filtering
D. vulnerability protection

Answer: B

NEW QUESTION 194
Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized.
Which user-ID agent sufficient in your network?

A. PAN-OS integrated agent deployed on the firewall
B. Windows-based agent deployed on the internal network a domain member
C. Citrix terminal server agent deployed on the network
D. Windows-based agent deployed on each domain controller

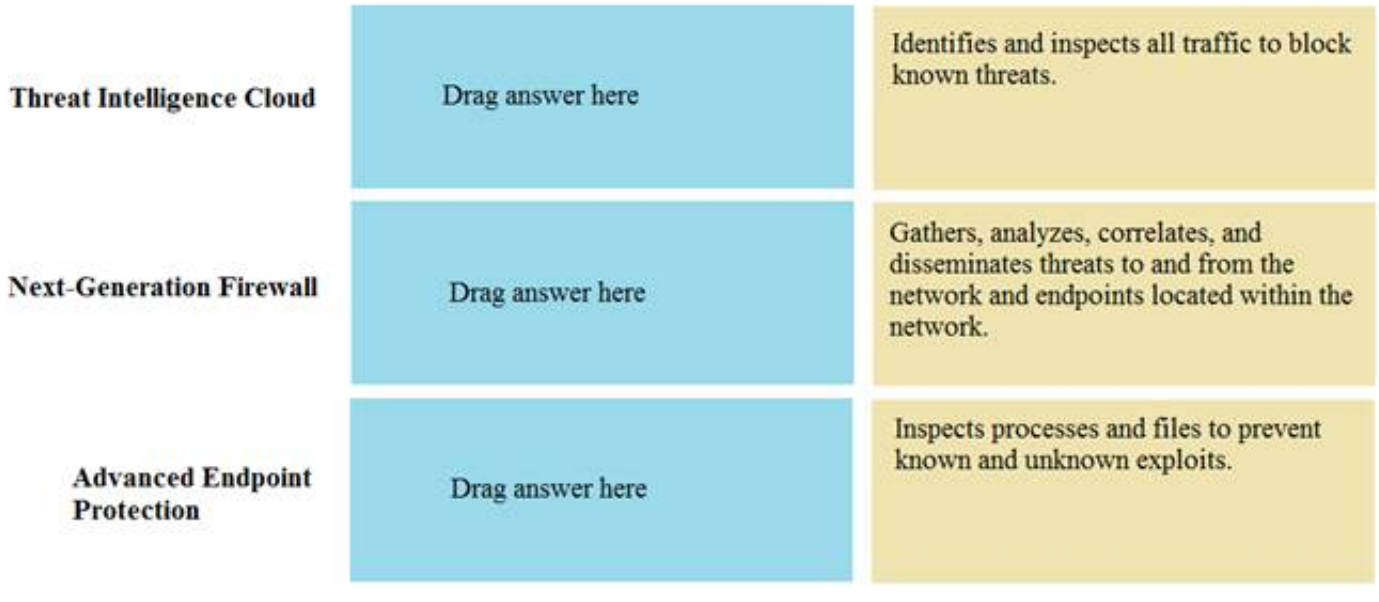
Answer: D

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser-mapping-using-the-

windows-user-id-agent/configure-the-windows-based-user-id-agent-for-usermapping.html

NEW QUESTION 196
DRAG DROP
Match the Palo Alto Networks Security Operating Platform architecture to its description.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Threat Intelligence Cloud – Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Next-Generation Firewall – Identifies and inspects all traffic to block known threats Advanced Endpoint Protection - Inspects processes and files to prevent known and unknown exploits

NEW QUESTION 200
Access to which feature requires PAN-OS Filtering licens?

A. PAN-DB database
B. URL external dynamic lists
C. Custom URL categories
D. DNS Security

Answer: A

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-and-subscriptions.html

NEW QUESTION 205
Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?

A. Layer 3
B. Virtual Wire
C. Tap
D. Layer 2

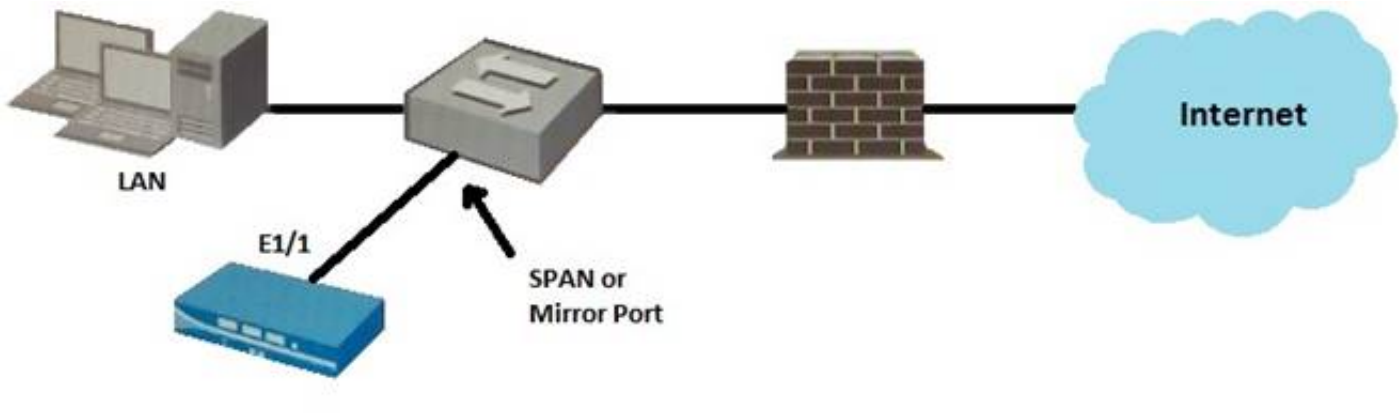
Answer: A

NEW QUESTION 207
Which URL profiling action does not generate a log entry when a user attempts to access that URL?

A. Override
B. Allow
C. Block
D. Continue

Answer: B

NEW QUESTION 209
Given the topology, which zone type should interface E1/1 be configured with?



A. Tap
B. Tunnel
C. Virtual Wire
D. Layer3

Answer: A

NEW QUESTION 213
.....

Relate Links

100% Pass Your PCNSA Exam with Exambible Prep Materials

https://www.exambible.com/PCNSA-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/