

Exam Questions PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 8.0

<https://www.2passeasy.com/dumps/PCNSE/>



NEW QUESTION 1

What is the purpose of the firewall decryption broker?

- A. Decrypt SSL traffic a then send it as cleartext to a security chain of inspection tools
- B. Force decryption of previously unknown cipher suites
- C. Inspection traffic within IPsec tunnel
- D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

Answer: A

NEW QUESTION 2

Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

- A. video streaming application
- B. Client Application Process
- C. Destination Domain
- D. Source Domain
- E. Destination user/group
- F. URL Category

Answer: ABC

NEW QUESTION 3

What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

- A. Rule Usage Hit counter will not be reset
- B. Highlight Unused Rules will highlight all rules.
- C. Highlight Unused Rules will highlight zero rules.
- D. Rule Usage Hit counter will reset.

Answer: AB

NEW QUESTION 4

The firewall is not downloading IP addresses from MineMeld. Based, on the image, what most likely is wrong?

The screenshot shows the configuration for an External Dynamic List named 'TORexitNodes-MM'. The list type is 'IP List' and the source is 'https://MineMeld/feeds/TORexitOut'. The server authentication is set to 'None (Disable Cert profile)'. The list is updated hourly. The 'Test Source URL' button is present, but the list is not downloading IP addresses from MineMeld.

- A. A Certificate Profile that contains the client certificate needs to be selected.
- B. The source address supports only files hosted with an ftp://<address/file>.
- C. External Dynamic Lists do not support SSL connections.
- D. A Certificate Profile that contains the CA certificate needs to be selected.

Answer: D

NEW QUESTION 5

Which is not a valid reason for receiving a decrypt-cert-validation error?

- A. Unsupported HSM
- B. Unknown certificate status
- C. Client authentication
- D. Untrusted issuer

Answer: A

NEW QUESTION 6

Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

- A. CRL
- B. CRT
- C. OCSP
- D. Cert-Validation-Profile
- E. SSL/TLS Service Profile

Answer: AC

NEW QUESTION 7

How does Panorama prompt VMWare NSX to quarantine an infected VM?

- A. HTTP Server Profile
- B. Syslog Server Profile
- C. Email Server Profile
- D. SNMP Server Profile

Answer: A

NEW QUESTION 8

An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A

Receive Time	Type	Severity	Event	Object	Description
06/16 08:41:43	general	Informational	general		User admin accessed Monitor tab
06/16 08:40:40	general	Informational	general		User admin logged in via Web from 192.168.55.1 using https
06/16 08:40:40	auth	Informational	auth-success		authenticated for user 'admin'. From: 192.168.55.1.
06/16 08:40:06	general	Informational	general		LOGIN ON tty1 BY admin
06/16 08:39:43	general	Informational	general		User admin logged in via CLI from Console
06/16 08:39:42	auth	Informational	auth-success		authenticated for user 'admin'. From: (null).
06/16 08:39:16	url-filtering	Informational	upgrade-uri-database-success		PAN-DB was upgraded to version 20170615.40151.
06/16 08:34:15	url-filtering	Informational	upgrade-uri-database-success		PAN-DB was upgraded to version 20170615.40150.
06/16 08:31:44	general	Informational	general		Failed to connect to Panorama Server: 192.168.55.5 Port: 3978 Retry: 0
06/16 08:31:40	ntp	Informational	restart		NTP restart synchronization performed
06/16 08:31:33	general	Informational	general		Commit job succeeded. Completion time=2017/06/16 05:31:33. JobId=29. User=admin

B

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:03:45	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:59:38	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:59:06	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:40:27	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:39:57	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:56	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:55	drop	outside	outside	192.168.55.1		192.168.55.255

C

05/23 20:49:30	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:49:29	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex
05/23 20:47:24	port	informational	link-change	ethernet1/1	Port ethernet1/1: Up 10Gb/s-full duplex
05/23 20:47:22	port	informational	link-change	MGT	Port MGT: Up Unknown
05/23 20:47:18	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:47:17	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex

D

Type	Status	Start Time	Messages	Action
Config Logs	Completed	06/16/17 08:40:53		
System Logs	Completed	06/16/17 08:40:53		
Data Logs	Completed	06/16/17 08:40:53		
Commit	Completed	06/16/17 08:31:19	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:31:19 <ul style="list-style-type: none"> Configuration committed successfully 	
Commit	Completed	06/16/17 08:30:15	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:30:15 <ul style="list-style-type: none"> Configuration committed successfully 	

- A. Exhibit A
- B. Exhibit B
- C. Exhibit C
- D. Exhibit D

Answer: AD

NEW QUESTION 9

A customer wants to set up a VLAN interface for a Layer 2 Ethernet port. Which two mandatory options are used to configure a VLAN interface? (Choose two.)

- A. Virtual router
- B. Security zone
- C. ARP entries
- D. Netflow Profile

Answer: AB

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa-7000-series-layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd-8064499f5b9d>

NEW QUESTION 10

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans. Which Security Profile type will protect against worms and trojans?

- A. Anti-Spyware
- B. WildFire
- C. Vulnerability Protection
- D. Antivirus

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/antivirus- profiles>

NEW QUESTION 10

If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

- A. The settings assigned to the template that is on top of the stack.
- B. The administrator will be prompted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.
- D. Depending on the firewall location, Panorama decides which settings to send.

Answer: B

Explanation:

Reference:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manage-templates-and-template-stacks/configure-a-template-stack

NEW QUESTION 12

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

- A. Configure the option for "Threshold".
- B. Disable automatic updates during weekdays.
- C. Automatically "download only" and then install Applications and Threats later, after the administrator approves the update.
- D. Automatically "download and install" but with the "disable new applications" option used.

Answer: A

NEW QUESTION 15

To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

- A. Device>Setup>Services>AutoFocus
- B. Device> Setup>Management >AutoFocus
- C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
- D. Device>Setup>WildFire>AutoFocus
- E. Device>Setup> Management> Logging and Reporting Settings

Answer: B

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence>

"<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence>"

NEW QUESTION 17

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

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

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection>

NEW QUESTION 20

Which two virtualization platforms officially support the deployment of Palo Alto Networks VM- Series firewalls? (Choose two.)

- A. Red Hat Enterprise Virtualization (RHEV)
- B. Kernel Virtualization Module (KVM)
- C. Boot Strap Virtualization Module (BSVM)
- D. Microsoft Hyper-V

Answer: BD

Explanation:

Reference: <https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series>

NEW QUESTION 25

Decrypted packets from the website <https://www.microsoft.com> will appear as which application and service within the Traffic log?

- A. web-browsing and 443
- B. SSL and 80
- C. SSL and 443
- D. web-browsing and 80

Answer: A

NEW QUESTION 26

Which Captive Portal mode must be configured to support MFA authentication?

- A. NTLM
- B. Redirect
- C. Single Sign-On
- D. Transparent

Answer: B

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

NEW QUESTION 29

A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects. How would an administrator configure the interface to 1Gbps?

- A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
- B. set deviceconfig system speed-duplex 1Gbps-duplex
- C. set deviceconfig system speed-duplex 1Gbps-full-duplex
- D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex

Answer: B

Explanation:

Reference: <https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management-Port/ta-p/59034>

NEW QUESTION 34

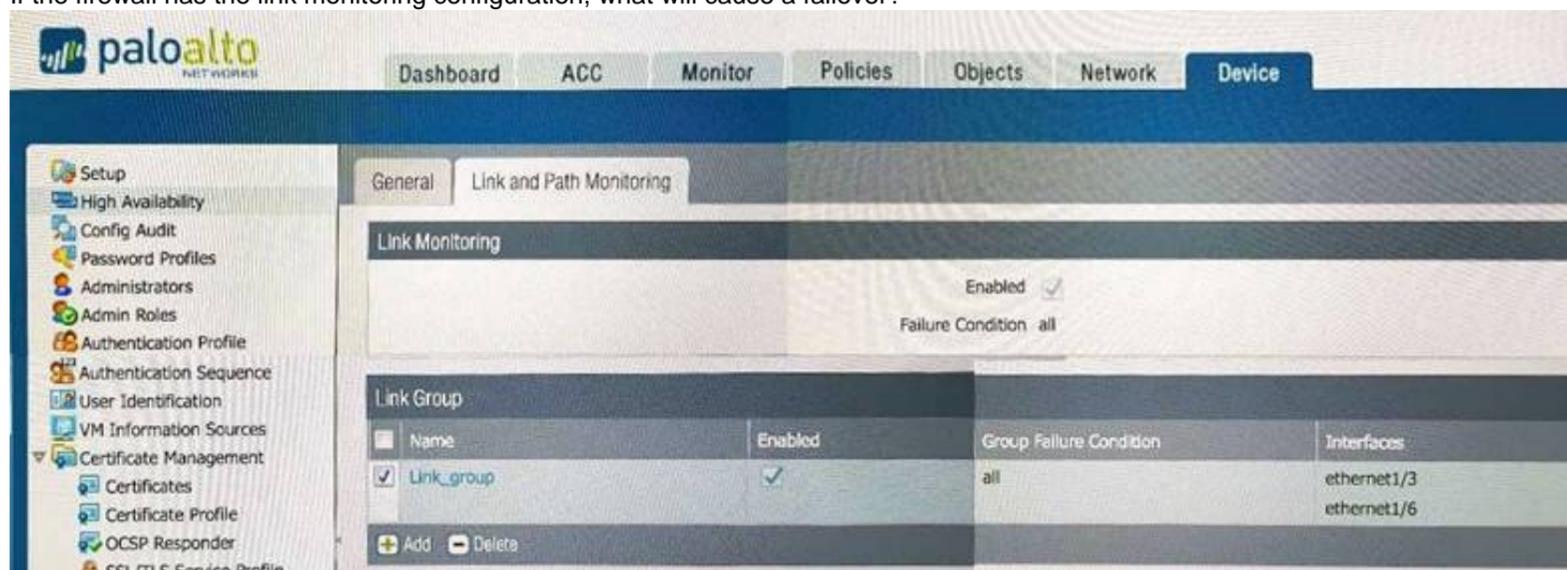
A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable we browsing access to the server. Which application and service need to be configured to allow only cleartext web-browsing traffic to thins server on tcp/8080.

- A. application: web-browsing; service: application-default
- B. application: web-browsing; service: service-https
- C. application: ssl; service: any
- D. application: web-browsing; service: (custom with destination TCP port 8080)

Answer: A

NEW QUESTION 37

If the firewall has the link monitoring configuration, what will cause a failover?



- A. ethernet1/3 and ethernet1/6 going down
- B. ethernet1/3 going down
- C. ethernet1/3 or Ethernet1/6 going down
- D. ethernet1/6 going down

Answer: A

NEW QUESTION 40

A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

- A. Application override
- B. Redistribution of user mappings
- C. Virtual Wire mode
- D. Content inspection

Answer: B

NEW QUESTION 43

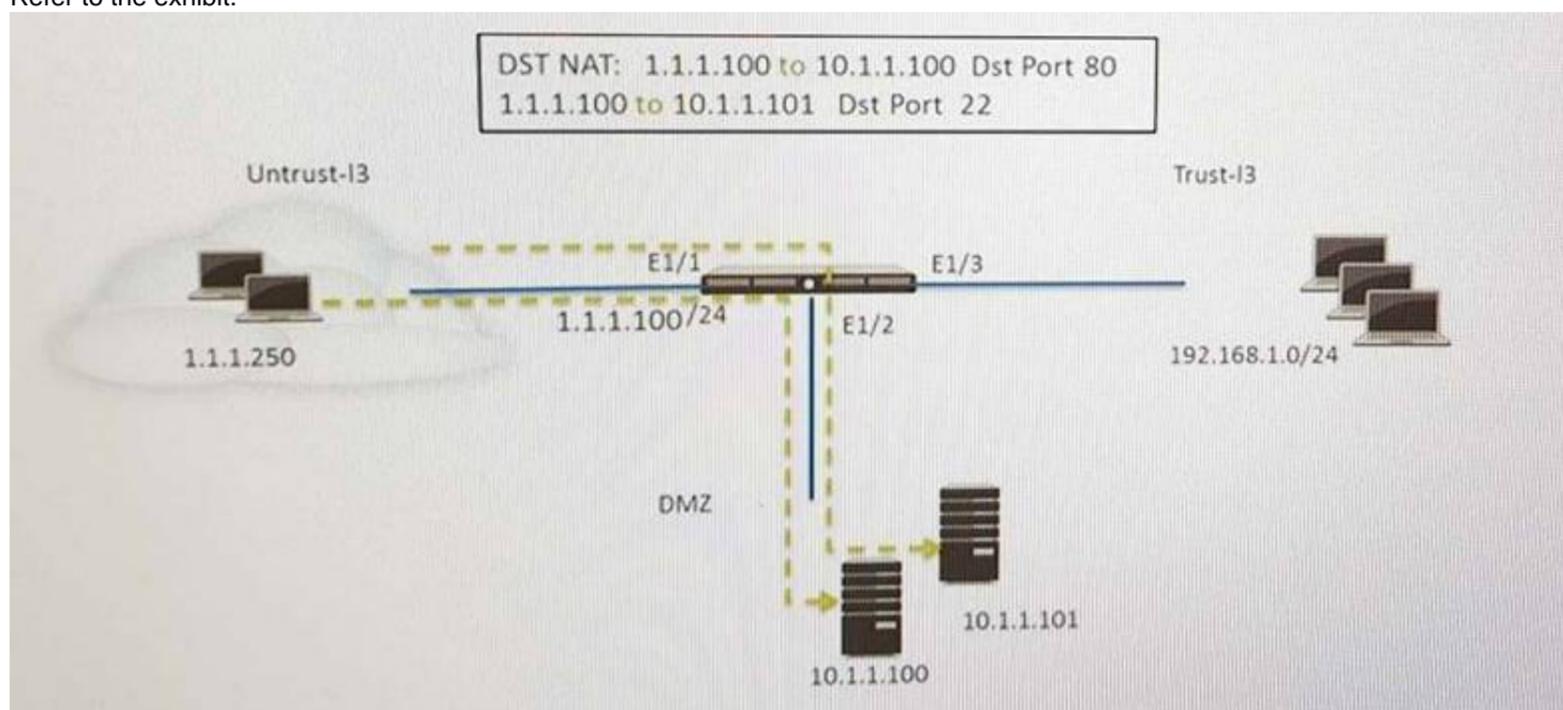
A session in the Traffic log is reporting the application as “incomplete.” What does “incomplete” mean?

- A. The three-way TCP handshake was observed, but the application could not be identified.
- B. The three-way TCP handshake did not complete.
- C. The traffic is coming across UDP, and the application could not be identified.
- D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

Answer: B

NEW QUESTION 47

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 Untrust (10.1.1.1), web-browsing -Allow
- B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
- C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
- D. Untrust (Any) to DMZ (10.1.1.1), ssh -Allow
- E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

Answer: CD

NEW QUESTION 50

An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?

- A)

Detailed Log View

General

Session ID 567
Action block-url
Application web-browsing
Rule AllowTrafficOut
Virtual System
Device SN
IP Protocol tcp
Log Action
Category gambling
Generated Time 2017/05/23 21:22:27
Receive Time 2017/05/23 21:22:27
Tunnel Type N/A

B)

URL Filtering Profile

Name Filter1
Description

Overrides Categories URL Filtering Settings User Credential Detection

65 items

Category	Site Access	User Credential Submission
<input type="checkbox"/> educational-institutions	allow	allow
<input type="checkbox"/> entertainment-and-arts	allow	allow
<input type="checkbox"/> extremism	allow	allow
<input type="checkbox"/> financial-services	allow	allow
<input checked="" type="checkbox"/> gambling	allow	block
<input type="checkbox"/> games	allow	allow
<input type="checkbox"/> government	allow	allow
<input type="checkbox"/> hacking	allow	allow
<input type="checkbox"/> health-and-medicine	allow	allow
<input type="checkbox"/> home-and-garden	allow	allow
<input type="checkbox"/> hunting-and-fishing	allow	allow

* indicates a custom URL category, + indicates external dynamic list
[Check URL Category](#)

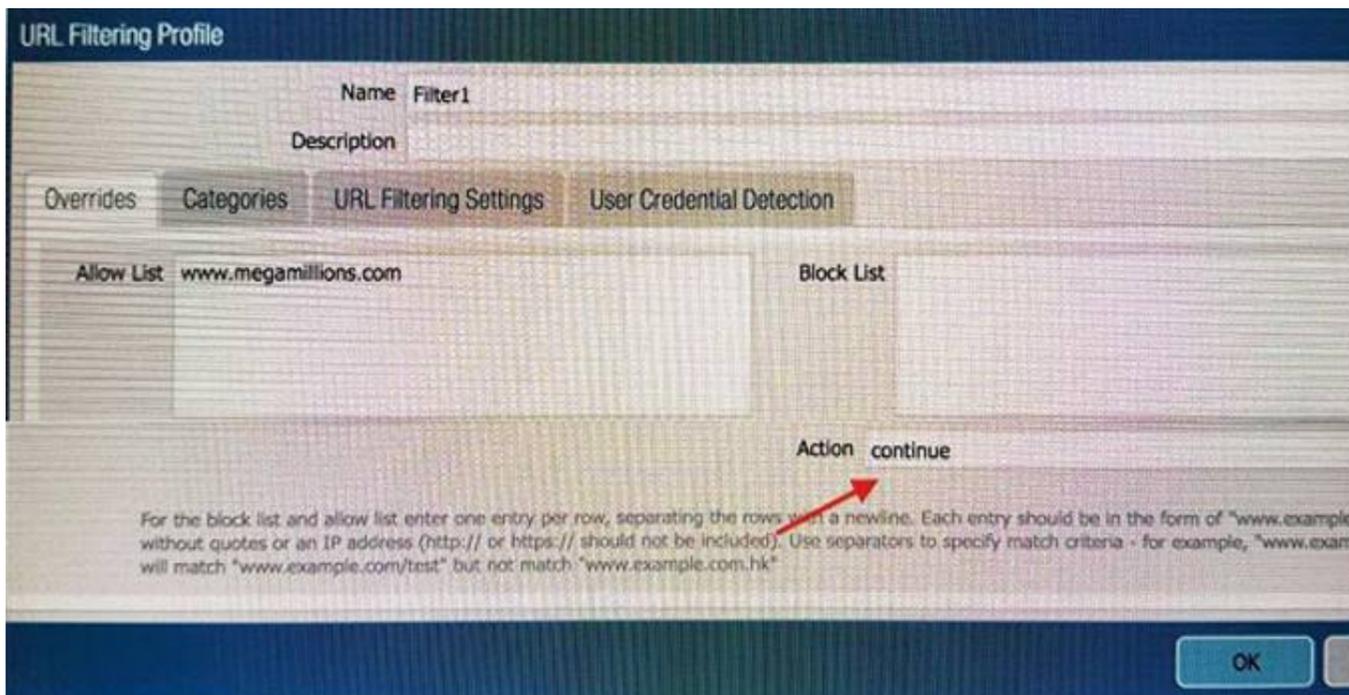
C)

Security Policy Rule

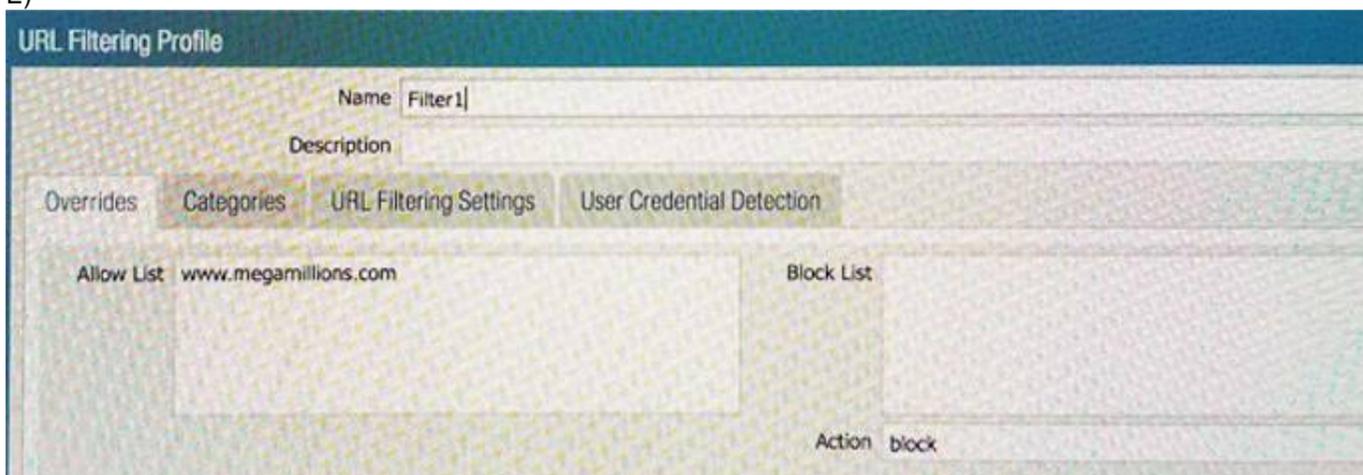
General Source User Destination Application Service/URL Category Actions

Name www.megamillions.com
Rule Type universal (default)
Description

D)



E)



- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: B

NEW QUESTION 52

Which three settings are defined within the Templates object of Panorama? (Choose three.)

- A. Setup
- B. Virtual Routers
- C. Interfaces
- D. Security
- E. Application Override

Answer: ADE

NEW QUESTION 55

A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

- A. Application Override policy.
- B. Security policy to identify the custom application.
- C. Custom application.
- D. Custom Service object.

Answer: BD

NEW QUESTION 58

An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in Panorama.

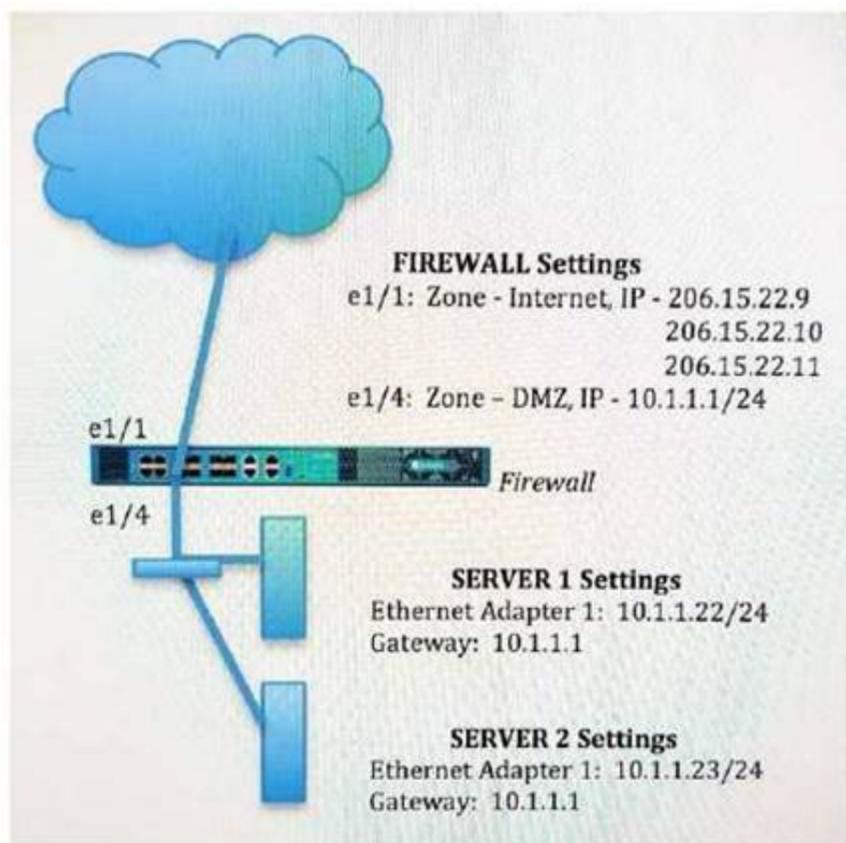
Which action would enable the firewalls to send their pre-existing logs to Panorama?

- A. Use the import option to pull logs into Panorama.
- B. A CLI command will forward the pre-existing logs to Panorama.
- C. Use the ACC to consolidate pre-existing logs.
- D. The log database will need to be exported from the firewalls and manually imported into Panorama.

Answer: B

NEW QUESTION 62

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22



Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly?

- A)
 - Source IP: Any
 - Destination IP: 206.15.22.9
 - Source Zone: Internet
 - Destination Zone: DMZ
 - Destination Service: 80/TCP
 - Action: Destination NAT
 - Translated IP: 10.2.2.23
 - Translated Port: 53/UDP
- B)
 - Source IP: Any
 - Destination IP: 206.15.22.9
 - Source Zone: Internet
 - Destination Zone: Internet
 - Destination Service: 80/TCP
 - Action: Destination NAT
 - Translated IP: 10.1.1.22
 - Translated Port: 53/UDP
- C)
 - Source IP: Any
 - Destination IP: 206.15.22.9
 - Source Zone: Internet
 - Destination Zone: Internet
 - Destination Service: 80/TCP
 - Action: Destination NAT
 - Translated IP: 10.1.1.22
 - Translated Port: None
- D)
 - Source IP: Any
 - Destination IP: 206.15.22.9
 - Source Zone: Internet
 - Destination Zone: DMZ
 - Destination Service: 80/TCP
 - Action: Destination NAT
 - Translated IP: 10.1.1.22
 - Translated Port: 80/TCP

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 66

An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?

- A. Custom application
- B. System logs show an application error and neither signature is used.
- C. Downloaded application
- D. Custom and downloaded application signature files are merged and both are used

Answer: A

NEW QUESTION 71

Which event will happen if an administrator uses an Application Override Policy?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-and-Tricks-How-to-Create-an-Application-Override/ta-p/65513>

NEW QUESTION 76

An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

- A. Client Probing
- B. Terminal Services agent
- C. GlobalProtect
- D. Syslog Monitoring

Answer: B

NEW QUESTION 81

Which option is part of the content inspection process?

- A. Packet forwarding process
- B. SSL Proxy re-encrypt
- C. IPsec tunnel encryption
- D. Packet egress process

Answer: A

NEW QUESTION 82

Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

- A. Configure a Decryption Profile and select SSL/TLS services.
- B. Set up SSL/TLS under Policies > Service/URL Category>Service.
- C. Set up Security policy rule to allow SSL communication.
- D. Configure an SSL/TLS Profile.

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-management-sslTls-service-profile>

NEW QUESTION 87

Which CLI command can be used to export the tcpdump capture?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference: <https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-Interface/ta-p/55415>

NEW QUESTION 88

During the packet flow process, which two processes are performed in application identification? (Choose two.)

- A. Pattern based application identification
- B. Application override policy match
- C. Application changed from content inspection
- D. Session application identified.

Answer: BD

NEW QUESTION 92

Which feature must you configure to prevent users from accidentally submitting their corporate credentials to a phishing website?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishing>

NEW QUESTION 94

How can a candidate or running configuration be copied to a host external from Panorama?

- A. Commit a running configuration.
- B. Save a configuration snapshot.
- C. Save a candidate configuration.
- D. Export a named configuration snapshot.

Answer: D

Explanation:

Reference:

https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/back-up-panorama-and-firewall-configurations

NEW QUESTION 98

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router. Which two options would help the administrator troubleshoot this issue? (Choose two.)

- A. View the System logs and look for the error messages about BGP.
- B. Perform a traffic pcap on the NGFW to see any BGP problems.
- C. View the Runtime Stats and look for problems with BGP configuration.
- D. View the ACC tab to isolate routing issues.

Answer: CD

NEW QUESTION 102

Which three firewall states are valid? (Choose three.)

- A. Active
- B. Functional
- C. Pending
- D. Passive
- E. Suspended

Answer: ADE

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states>

NEW QUESTION 104

Which virtual router feature determines if a specific destination IP address is reachable?

- A. Heartbeat Monitoring
- B. Failover
- C. Path Monitoring
- D. Ping-Path

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf>

NEW QUESTION 106

An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.

Which interface type and license feature are necessary to meet the requirement?

- A. Decryption Mirror interface with the Threat Analysis license
- B. Virtual Wire interface with the Decryption Port Export license
- C. Tap interface with the Decryption Port Mirror license
- D. Decryption Mirror interface with the associated Decryption Port Mirror license

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring>

NEW QUESTION 111

An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port. Which log entry can the administrator use to verify that sessions are being decrypted?

- A. In the details of the Traffic log entries
- B. Decryption log
- C. Data Filtering log
- D. In the details of the Threat log entries

Answer: A

Explanation:

Reference: <https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719>

NEW QUESTION 112

Which processing order will be enabled when a Panorama administrator selects the setting "Objects defined in ancestors will take higher precedence?"

- A. Descendant objects will take precedence over other descendant objects.
- B. Descendant objects will take precedence over ancestor objects.
- C. Ancestor objects will have precedence over descendant objects.
- D. Ancestor objects will have precedence over other ancestor objects.

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management>

NEW QUESTION 115

Exhibit:

```
#####
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination      nexthop      flags      interface      mtu
-----
47      0.0.0.0/0        10.46.40.1   ug         ethernet1/3    1500
46      10.46.40.0/23    0.0.0.0      u          ethernet1/3    1500
45      10.46.41.111/32  0.0.0.0      uh         ethernet1/3    1500
70      10.46.41.113/32  10.46.40.1   ug         ethernet1/3    1500
51      192.168.111.0/24 0.0.0.0      u          ethernet1/6    1500
50      192.168.111.2/32 0.0.0.0      uh         ethernet1/6    1500

#####
```

```
admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags: m-multicast firewalling
       p= link state pass-through
       s- vlan sub-interface
       i- ip+vlan sub-interface
       t-tenant sub-interface

name      interface1      interface2      flags      allowed-tags
-----
VW-1      ethernet1/7     ethernet1/5     p
```

#####

What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time

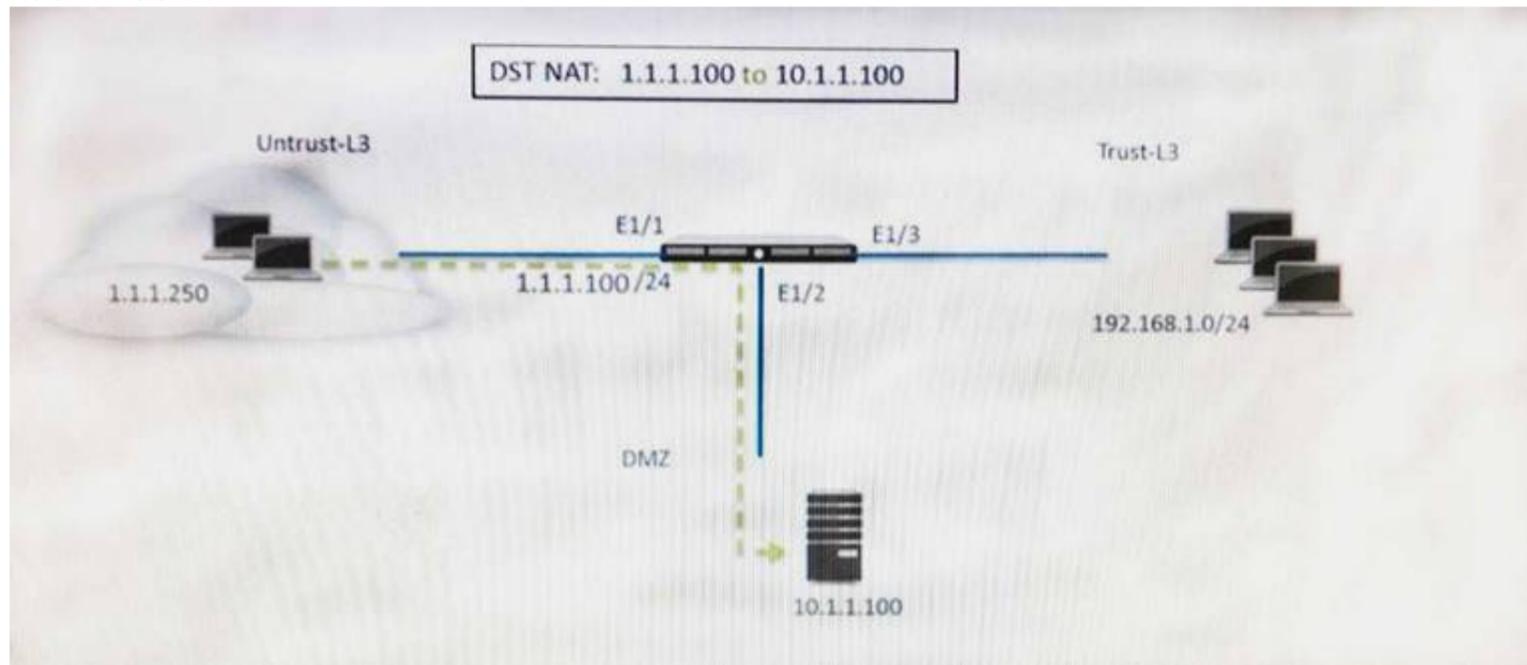
shown in the image?

- A. ethernet1/7
- B. ethernet1/5
- C. ethernet1/6
- D. ethernet1/3

Answer: D

NEW QUESTION 118

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. Untrust (any) to Untrust (10. 1.1. 100), web browsing – Allow
- B. Untrust (any) to Untrust (1. 1. 1. 100), web browsing – Allow
- C. Untrust (any) to DMZ (1. 1. 1. 100), web browsing – Allow
- D. Untrust (any) to DMZ (10. 1. 1. 100), web browsing – Allow

Answer: B

NEW QUESTION 122

A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

- A. application override
- B. Virtual Wire mode
- C. content inspection
- D. redistribution of user mappings

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-network>

NEW QUESTION 126

Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a “No Decrypt” action? (Choose two.)

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

Answer: ABC

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/create-a-decryption-profile>

NEW QUESTION 127

Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?

- A. port mapping
- B. server monitoring
- C. client probing
- D. XFF headers

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-terminal-server-users>

NEW QUESTION 129

Which feature can be configured on VM-Series firewalls?

- A. aggregate interfaces
- B. machine learning
- C. multiple virtual systems
- D. GlobalProtect

Answer: D

NEW QUESTION 134

In High Availability, which information is transferred via the HA data link?

- A. session information
- B. heartbeats
- C. HA state information
- D. User-ID information

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links>

NEW QUESTION 137

If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssl-inbound-inspection>

NEW QUESTION 139

A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles>

NEW QUESTION 140

Which CLI command enables an administrator to check the CPU utilization of the dataplane?

- A. show running resource-monitor
- B. debug data-plane dp-cpu
- C. show system resources
- D. debug running resources

Answer: A

NEW QUESTION 143

Which DoS protection mechanism detects and prevents session exhaustion attacks?

- A. Packet Based Attack Protection
- B. Flood Protection
- C. Resource Protection
- D. TCP Port Scan Protection

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles>

NEW QUESTION 148

What is exchanged through the HA2 link?

- A. hello heartbeats
- B. User-ID information
- C. session synchronization
- D. HA state information

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links>

NEW QUESTION 152

A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation. Which two formats are correct for naming aggregate interfaces? (Choose two.)

- A. ae.8
- B. aggregate.1
- C. ae.1
- D. aggregate.8

Answer: AC

NEW QUESTION 155

Which three authentication factors does PAN-OS® software support for MFA (Choose three.)

- A. Push
- B. Pull
- C. Okta Adaptive
- D. Voice E.SMS

Answer: ADE

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

NEW QUESTION 157

An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.

What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Dependencies : Before upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS Upgrade. Reference: <https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045>

NEW QUESTION 158

For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two)

- A. equal-cost multipath
- B. ingress processing errors
- C. rule match with action "allow"
- D. rule match with action "deny"

Answer: BD

NEW QUESTION 161

Which logs enable a firewall administrator to determine whether a session was decrypted?

- A. Correlated Event
- B. Traffic
- C. Decryption
- D. Security Policy

Answer: B

NEW QUESTION 163

Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

- A. App Scope

- B. ACC
- C. Session Browser
- D. System Logs

Answer: C

NEW QUESTION 167

Which two features does PAN-OS® software use to identify applications? (Choose two)

- A. port number
- B. session number
- C. transaction characteristics
- D. application layer payload

Answer: CD

NEW QUESTION 168

Which four NGFW multi-factor authentication factors are supported by PAN-OS®? (Choose four.)

- A. User logon
- B. Short message service
- C. Push
- D. SSH key
- E. One-Time Password
- F. Voice

Answer: BCEF

NEW QUESTION 171

Which three firewall states are valid? (Choose three)

- A. Suspended
- B. Passive
- C. Active
- D. Pending
- E. Functional

Answer: ABC

NEW QUESTION 172

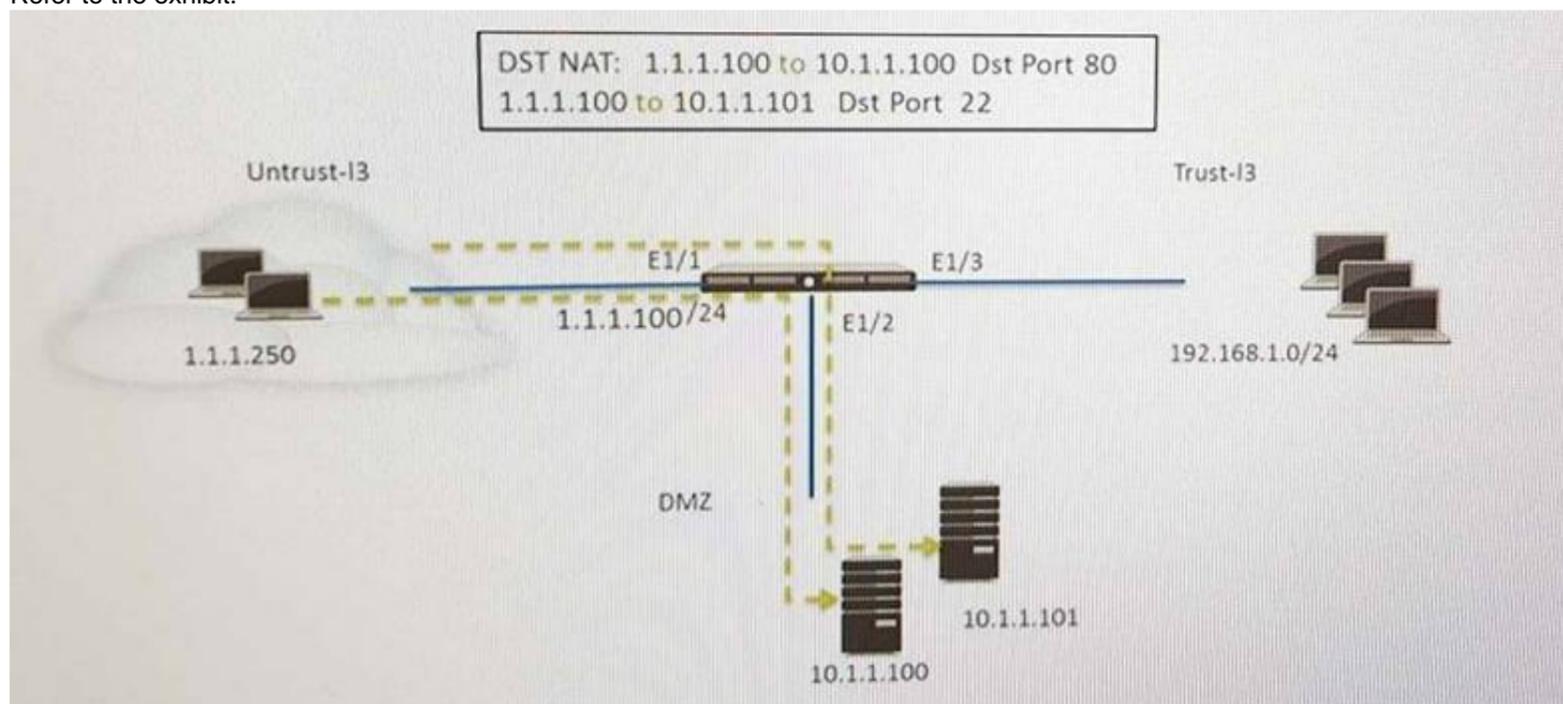
An administrator wants to upgrade an NGFW from PAN-OS® 7 .1. 2 to PAN-OS® 8 .0.2 The firewall is not a part of an HA pair. What needs to be updated first?

- A. XML Agent
- B. Applications and Threats
- C. WildFire
- D. PAN-OS® Upgrade Agent

Answer: B

NEW QUESTION 175

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) received 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 Untrust (10.1.1.1) Ssh-Allow
- B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
- C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
- D. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

Answer: CD

NEW QUESTION 178

When configuring the firewall for packet capture, what are the valid stage types?

- A. Receive, management , transmit , and drop
- B. Receive , firewall, send , and non-syn
- C. Receive management , transmit, and non-syn
- D. Receive , firewall, transmit, and drop

Answer: D

NEW QUESTION 179

Which feature can provide NGFWs with User-ID mapping information?

- A. GlobalProtect
- B. Web Captcha
- C. Native 802.1q authentication
- D. Native 802.1x authentication

Answer: A

NEW QUESTION 184

What are the differences between using a service versus using an application for Security Policy match?

- A. Use of a "service" enables the firewall to take action after enough packets allow for App-ID identification
- B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use of an "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the ports being used.
- C. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use of a friendly application name instead of port numbers.
- D. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port number
- E. Use of an "application" allows the firewall to take immediate action if the port being used is a member of the application standard port list

Answer: B

NEW QUESTION 186

In which two types of deployment is active/active HA configuration supported? (Choose two.)

- A. TAP mode
- B. Layer 2 mode
- C. Virtual Wire mode
- D. Layer 3 mode

Answer: CD

NEW QUESTION 191

A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial-of-service attacks. How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

- A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
- B. Add QoS Profiles to throttle incoming requests
- C. Add a tuned DoS Protection Profile
- D. Add an Anti-Spyware Profile to block attacking IP address

Answer: C

NEW QUESTION 192

Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

- A. Dynamic
- B. Custom Panorama Admin
- C. Role Based
- D. Device Group E. Template Admin

Answer: DE

NEW QUESTION 193

Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content-IDs to traffic?

- A. Select download-and-install.
- B. Select download-and-install, with "Disable new apps in content update" selected.
- C. Select download-only.
- D. Select disable application updates and select "Install only Threat updates"

Answer: C

NEW QUESTION 196

Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

- A. HA1 IP Address
- B. Network Interface Type
- C. Master Key
- D. Zone Protection Profile

Answer: AB

NEW QUESTION 201

Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.

- A. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:"intrazone"
- B. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:"intrazone" or "universal"
- C. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:"intrazone" or "universal"
- D. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:"intrazone"

Answer: B

NEW QUESTION 205

Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunnel is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.

Virtual Router - OSPF - Area						
Area ID 0.0.0.0						
Type	Range	Interface	Virtual Link			
<input type="checkbox"/>	Interface	Enable	Passive	Link Type	Metric	Priority
<input type="checkbox"/>	tunnel.10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	broadcast	10	1
<input type="checkbox"/>	ethernet1/21	<input checked="" type="checkbox"/>	<input type="checkbox"/>	broadcast	10	1

Which Link Type setting will correct the error?

- A. Set tunne
- B. 1 to p2p
- C. Set tunne
- D. 1 to p2mp
- E. Set Ethernet 1/1 to p2mp
- F. Set Ethernet 1/1 to p2p

Answer: A

NEW QUESTION 208

Which three fields can be included in a pcap filter? (Choose three)

- A. Egress interface
- B. Source IP
- C. Rule number
- D. Destination IP
- E. Ingress interface

Answer: BCD

Explanation:

(<https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069>)

NEW QUESTION 209

Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

- A. The devices are pre-configured with a virtual wire pair out the first two interfaces.
- B. The devices are licensed and ready for deployment.
- C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.
- D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.
- E. The interface are pingable.

Answer: BC

NEW QUESTION 214

How is the Forward Untrust Certificate used?

- A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has been decrypted/
- B. It is used when web servers request a client certificate.
- C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by the firewall.
- D. It is used for Captive Portal to identify unknown users.

Answer: C

NEW QUESTION 217

What are three valid actions in a File Blocking Profile? (Choose three)

- A. Forward
- B. Block
- C. Alert
- D. Upload
- E. Reset-both
- F. Continue

Answer: ABC

Explanation:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623>
<https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623>
<https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623>

NEW QUESTION 221

The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.

Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

- A. test panoramas-connect 10.10.10.5
- B. show panoramas-status
- C. show arp all | match 10.10.10.5
- D. topdump filter "host 10.10.10.5
- E. debug dataplane packet-diag set capture on

Answer: BD

NEW QUESTION 225

Which Public Key Infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logout?

- A. Certificate revocation list
- B. Trusted root certificate
- C. Machine certificate
- D. Online Certificate Status Protocol

Answer: C

NEW QUESTION 227

Which three log-forwarding destinations require a server profile to be configured? (Choose three)

- A. SNMP Trap
- B. Email
- C. RADIUS
- D. Kerberos
- E. Panorama
- F. Syslog

Answer: ABF

NEW QUESTION 231

An Administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is the output from the command:

less mp-log ikemgr.log:

```
less mp-log ikemgr.log:
```

```
2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: ----> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <----
----> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <----
2014-08-05 03:52:33 [PROTO_NOTIFY]: ----> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <----
----> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <---- Due to
timeout.
2014-08-05 03:52:33 [INFO]: ----> PHASE-1 SA DELETED <----
----> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <----
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: ----> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <----
----> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <----
2014-08-05 03:53:54 [PROTO_NOTIFY]: ----> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <----
----> Failed.SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <---- Due to
timeout.
2014-08-05 03:53:54 [INFO]: ----> PHASE-1 SA DELETED <----
```

What could be the cause of this problem?

- A. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
- B. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.
- C. The shared secrets do not match between the Palo Alto firewall and the ASA
- D. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

Answer: B

NEW QUESTION 236

Which client software can be used to connect remote Linux client into a Palo Alto Networks Infrastructure without sacrificing the ability to scan traffic and protect against threats?

- A. X-Auth IPsec VPN
- B. GlobalProtect Apple IOS
- C. GlobalProtect SSL
- D. GlobalProtect Linux

Answer: A

Explanation:

(<http://blog.webernetz.net/2014/03/31/palo-alto-globalprotect-for-linux-with-vpnc/>)

NEW QUESTION 241

Which three options are available when creating a security profile? (Choose three)

- A. Anti-Malware
- B. File Blocking
- C. Url Filtering
- D. IDS/IPS
- E. Threat Prevention
- F. Antivirus

Answer: ABF

NEW QUESTION 243

Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

- A. Vulnerability Object
- B. DoS Protection Profile
- C. Data Filtering Profile
- D. Zone Protection Profile

Answer: BD

NEW QUESTION 248

The IT department has received complaints about VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter. Which feature can be used to identify, in real time, the applications taking up the most bandwidth?

- A. QoS Statistics
- B. Applications Report
- C. Application Command Center (ACC)
- D. QoS Log

Answer: A

NEW QUESTION 252

A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a

single destination IP address and port.

Which option when enabled with the correction threshold would mitigate this attack without dropping legitimate traffic to other hosts inside the network?

- A. Zone Protection Policy with UDP Flood Protection
- B. QoS Policy to throttle traffic below maximum limit
- C. Security Policy rule to deny traffic to the IP address and port that is under attack
- D. Classified DoS Protection Policy using destination IP only with a Protect action

Answer: D

NEW QUESTION 254

Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

- A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
- B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
- C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.
- D. Enter the command logger-mode enable then enter Y to confirm the change to Log Collector mode.
- E. Log in the Panorama CLI of the dedicated Log Collector

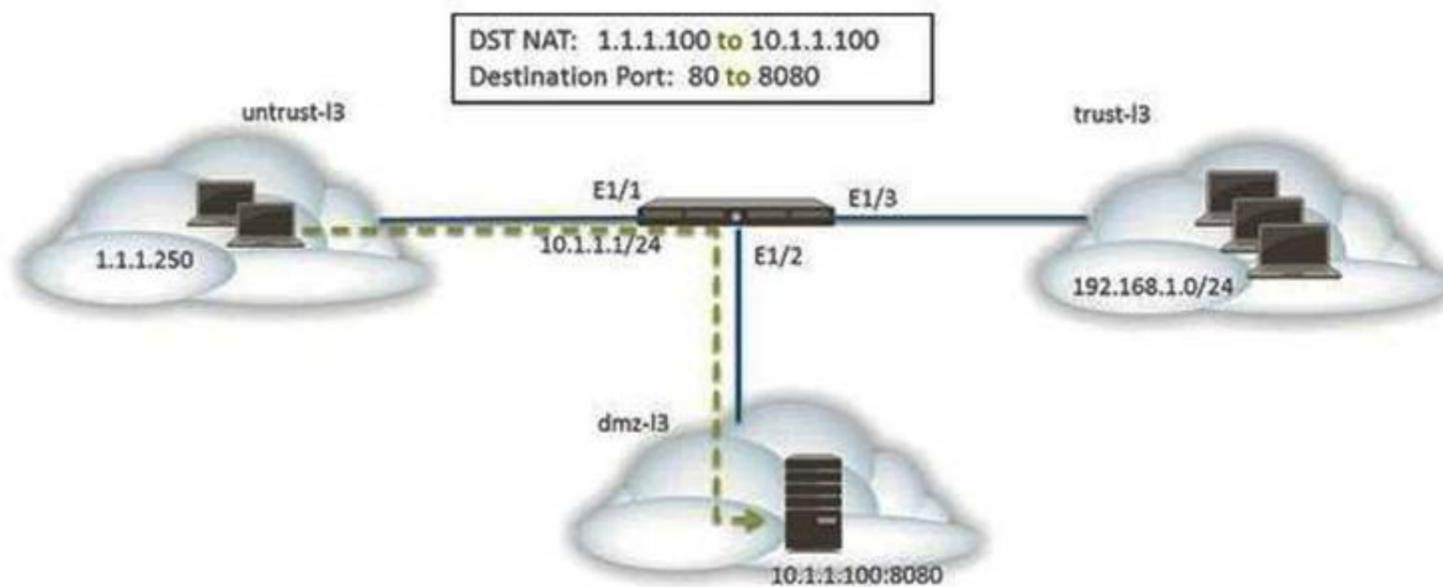
Answer: BE

Explanation:

(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance)

NEW QUESTION 255

The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and port to 10.1.1.100 on TCP Port 8080.



Which NAT and security rules must be configured on the firewall? (Choose two)

- A. A security policy with a source of any from untrust-I3 Zone to a destination of 10.1.1.100 in dmz-I3 zone using web-browsing application
- B. A NAT rule with a source of any from untrust-I3 zone to a destination of 10.1.1.100 in dmz-zone using service-http service.
- C. A NAT rule with a source of any from untrust-I3 zone to a destination of 1.1.1.100 in untrust-I3 zone using service-http service.
- D. A security policy with a source of any from untrust-I3 zone to a destination of 1.1.100 in dmz-I3 zone using web-browsing application.

Answer: BD

NEW QUESTION 256

Palo Alto Networks maintains a dynamic database of malicious domains.

Which two Security Platform components use this database to prevent threats? (Choose two)

- A. Brute-force signatures
- B. BrightCloud Url Filtering
- C. PAN-DB URL Filtering
- D. DNS-based command-and-control signatures

Answer: CD

NEW QUESTION 257

A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall

Which part of files needs to be imported back into the replacement firewall that is using Panorama?

- A. Device state and license files
- B. Configuration and serial number files
- C. Configuration and statistics files
- D. Configuration and Large Scale VPN (LSVPN) setups file

Answer: A

NEW QUESTION 262

A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.

Given the following zone information:

- DMZ zone: DMZ-L3
- Public zone: Untrust-L3
- Guest zone: Guest-L3
- Web server zone: Trust-L3
- Public IP address (Untrust-L3): 1.1.1.1
- Private IP address (Trust-L3): 192.168.1.50

What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

- A. Untrust-L3
- B. DMZ-L3
- C. Guest-L3
- D. Trust-L3

Answer: A

NEW QUESTION 266

Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.

Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

- A. Create a custom Application without signatures, then create an Application Override policy that includes the source, Destination, Destination Port/Protocol and Custom Application of the traffic.
- B. Wait until an official Application signature is provided from Palo Alto Networks.
- C. Modify the session timer settings on the closest referenced application to meet the needs of the in-house application
- D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

Answer: D

NEW QUESTION 269

What must be used in Security Policy Rule that contain addresses where NAT policy applies?

- A. Pre-NAT address and Pre-NAT zones
- B. Post-NAT address and Post-Nat zones
- C. Pre-NAT address and Post-Nat zones
- D. Post-Nat addresses and Pre-NAT zones

Answer: C

NEW QUESTION 274

What are three valid method of user mapping? (Choose three)

- A. Syslog
- B. XML API
- C. 802.1X
- D. WildFire
- E. Server Monitoring

Answer: ABE

NEW QUESTION 278

Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?

- A. Disable Server Response Inspection
- B. Apply an Application Override
- C. Disable HIP Profile
- D. Add server IP Security Policy exception

Answer: A

NEW QUESTION 283

The GlobalProtect Portal interface and IP address have been configured. Which other value needs to be defined to complete the network settings configuration of GlobalProtect Portal?

- A. Server Certificate
- B. Client Certificate
- C. Authentication Profile
- D. Certificate Profile

Answer: A

Explanation:

(<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-GlobalProtect/ta-p/58351>)

NEW QUESTION 284

Which interface configuration will accept specific VLAN IDs?

- A. Tab Mode
- B. Subinterface
- C. Access Interface
- D. Trunk Interface

Answer: B

NEW QUESTION 287

A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

- A. The two devices must share a routable floating IP address
- B. The two devices may be different models within the PA-5000 series
- C. The HA1 IP address from each peer must be on a different subnet
- D. The management port may be used for a backup control connection

Answer: D

NEW QUESTION 288

Which three options does the WF-500 appliance support for local analysis? (Choose three)

- A. E-mail links
- B. APK files
- C. jar files
- D. PNG files
- E. Portable Executable (PE) files

Answer: ACE

NEW QUESTION 290

After pushing a security policy from Panorama to a PA-3020 firewall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

- A. A Server Profile has not been configured for logging to this Panorama device.
- B. Panorama is not licensed to receive logs from this particular firewall.
- C. The firewall is not licensed for logging to this Panorama device.
- D. None of the firewall's policies have been assigned a Log Forwarding profile

Answer: D

NEW QUESTION 291

Support for which authentication method was added in PAN-OS 8.0?

- A. RADIUS
- B. LDAP
- C. Diameter
- D. TACACS+

Answer: D

Explanation:

<https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1>

NEW QUESTION 293

A network design calls for a "router on a stick" implementation with a PA-5060 performing inter-VLAN routing. All VLAN-tagged traffic will be forwarded to the PA-5060 through a single dot1q trunk interface.

Which interface type and configuration setting will support this design?

- A. Trunk interface type with specified tag
- B. Layer 3 interface type with specified tag
- C. Layer 2 interface type with a VLAN assigned
- D. Layer 3 subinterface type with specified tag

Answer: D

NEW QUESTION 298

Which option is an IPv6 routing protocol?

- A. RIPv3
- B. OSPFv3
- C. OSPv3
- D. BGP NG

Answer: B

NEW QUESTION 302

When is it necessary to activate a license when provisioning a new Palo Alto Networks firewall?

- A. When configuring Certificate Profiles
- B. When configuring GlobalProtect portal
- C. When configuring User Activity Reports
- D. When configuring Antivirus Dynamic Updates

Answer: D

NEW QUESTION 305

What are two prerequisites for configuring a pair of Palo Alto Networks firewalls in an active/passive High Availability (HA) pair? (Choose two.)

- A. The firewalls must have the same set of licenses.
- B. The management interfaces must be on the same network.
- C. The peer HA1 IP address must be the same on both firewalls.
- D. HA1 should be connected to HA1. Either directly or with an intermediate Layer 2 device.

Answer: AD

NEW QUESTION 309

Which URL Filtering Security Profile action toggles the URL Filtering category to the URL Filtering log?

- A. Log
- B. Alert
- C. Allow
- D. Default

Answer: B

NEW QUESTION 312

Which URL Filtering Security Profile action logs the URL Filtering category to the URL Filtering log?

- A. Log
- B. Alert
- C. Allow
- D. Default

Answer: B

Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering-profile-actions>

NEW QUESTION 316

A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.

What can be done to simplify the NAT policy?

- A. Configure ECMP to handle matching NAT traffic
- B. Configure a NAT Policy rule with Dynamic IP and Port
- C. Create a new Source NAT Policy rule that matches the existing traffic and enable the Bi-directional option
- D. Create a new Destination NAT Policy rule that matches the existing traffic and enable the Bi-directional option

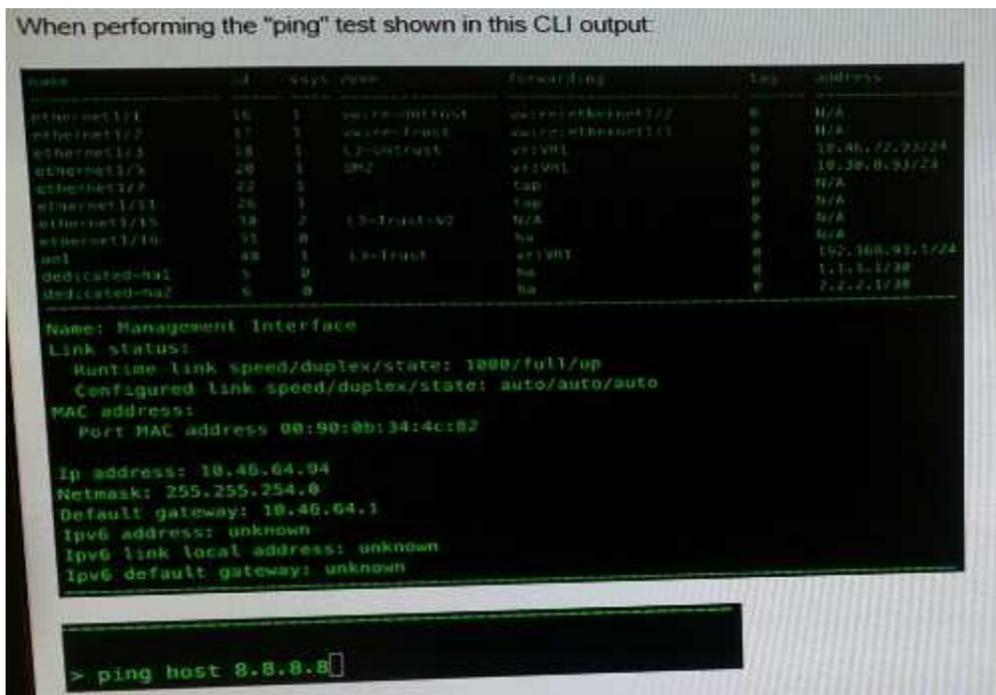
Answer: C

Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-configuration-examples>

NEW QUESTION 320

What will be the source address in the ICMP packet?



- A. 10.30.0.93
- B. 10.46.72.93
- C. 10.46.64.94
- D. 192.168.93.1

Answer: C

NEW QUESTION 321

A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

- A. BGP not sure
- B. OSPFv3
- C. RIP
- D. Static Route

Answer: BD

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols-OSPF-or-BGP-with/ta-p/62773>

NEW QUESTION 324

When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinkhole enabled, generating a traffic log. What will be the destination IP Address in that log entry?

- A. The IP Address of sinkhole.paloaltonetworks.com
- B. The IP Address of the command-and-control server
- C. The IP Address specified in the sinkhole configuration
- D. The IP Address of one of the external DNS servers identified in the anti-spyware database

Answer: C

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864> naHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864" gement-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864

NEW QUESTION 329

Which two logs on the firewall will contain authentication-related information useful for troubleshooting purpose (Choose two)

- A. ms.log
- B. traffic.log
- C. system.log
- D. dp-monitor.log
- E. authd.log

Answer: CE

NEW QUESTION 333

A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:

- * Users outside the company are in the "Untrust-L3" zone.
- * The web server physically resides in the "Trust-L3" zone.
- * Web server public IP address: 23.54.6.10
- * Web server private IP address: 192.168.1.10

Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

- A. Destination IP of 23.54.6.10
- B. UntrustL3 for both Source and Destination Zone
- C. Destination IP of 192.168.1.10
- D. UntrustL3 for Source Zone and Trust-L3 for Destination Zone

Answer: AB

NEW QUESTION 336

How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

- A. Enable support for non-standard syslog messages under device management
- B. Check the custom-format check box in the syslog server profile
- C. Select a non-standard syslog server profile
- D. Create a custom log format under the syslog server profile

Answer: D

NEW QUESTION 341

A distributed log collection deployment has dedicated log Collectors. A developer needs a device to send logs to Panorama instead of sending logs to the Collector Group.

What should be done first?

- A. Remove the cable from the management interface, reload the log Collector and then re-connect that cable
- B. Contact Palo Alto Networks Support team to enter kernel mode commands to allow adjustments
- C. remove the device from the Collector Group
- D. Revert to a previous configuration

Answer: C

NEW QUESTION 345

Which two actions are required to make Microsoft Active Directory users appear in a firewall traffic log? (Choose two.)

- A. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions
- B. Enable User-ID on the zone object for the destination zone
- C. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
- D. Enable User-ID on the zone object for the source zone
- E. Configure a RADIUS server profile to point to a domain controller

Answer: AD

NEW QUESTION 348

Which two virtualized environments support Active/Active High Availability (HA) in PAN-OS 8.0? (Choose two.)

- A. KVM
- B. VMware ESX
- C. VMware NSX
- D. AWS

Answer: AB

NEW QUESTION 352

Site-A and Site-B need to use IKEv2 to establish a VPN connection. Site A connects directly to the internet using a public IP address. Site-B uses a private IP address behind an ISP router to connect to the internet.

How should NAT Traversal be implemented for the VPN connection to be established between Site-A and Site-B?

- A. Enable on Site-A only
- B. Enable on Site-B only
- C. Enable on Site-B only with passive mode
- D. Enable on Site-A and Site-B

Answer: D

NEW QUESTION 356

Which field is optional when creating a new Security Policy rule?

- A. Name
- B. Description
- C. Source Zone
- D. Destination Zone
- E. Action

Answer: B

NEW QUESTION 357

YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic.

The following interfaces and zones are in use on the firewall:

* ethernet1/1, Zone: Untrust (Internet-facing)

* ethernet1/2, Zone: Trust (client-facing)

A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS profile called Inbound.

Which setting for class 6 with throttle YouTube traffic?

- A. Outbound profile with Guaranteed Ingress
- B. Outbound profile with Maximum Ingress
- C. Inbound profile with Guaranteed Egress
- D. Inbound profile with Maximum Egress

Answer: D

NEW QUESTION 359

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSE Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSE Product From:

<https://www.2passeasy.com/dumps/PCNSE/>

Money Back Guarantee

PCNSE Practice Exam Features:

- * PCNSE Questions and Answers Updated Frequently
- * PCNSE Practice Questions Verified by Expert Senior Certified Staff
- * PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year