

PCNSE

Number: PCNSE
Passing Score: 800
Time Limit: 120 min
File Version: 1

PCNSE



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

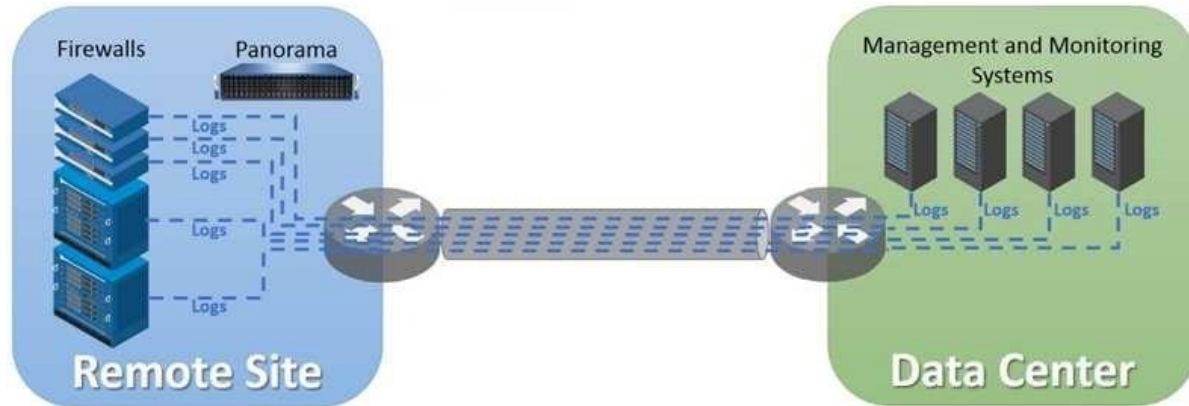
<https://vceplus.com/>

<https://vceplus.com/>

Exam A

QUESTION 1

Refer to the exhibit.



An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.

How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?



<https://vceplus.com/>

- A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
- B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
- C. Configure log compression and optimization features on all remote firewalls.
- D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

<https://vceplus.com/>

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

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. Instruction Prevention
- C. File Blocking
- D. Antivirus

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/security-profiles>

QUESTION 3

An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall.

Which priority is correct for the passive firewall?

- A. 0
- B. 99
- C. 1
- D. 255

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/high-availability/device-priority-and-preemption>

QUESTION 4

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 promoted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.
- D. Depending on the firewall location, Panorama decides with settings to send.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 5**

Which method will dynamically register tags on the Palo Alto Networks NGFW?

- A. Restful API or the VMware API on the firewall or on the User-ID agent or the *ready-only domain controller* (RODC)
- B. Restful API or the VMware API on the firewall or on the User-ID agent
- C. XML API or the VMware API on the firewall or on the User-ID agent or the CLI
- D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/register-ip-addresses-and-tags-dynamically>

QUESTION 6

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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 8

Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

- A. Security policy
- B. Decryption policy
- C. Authentication policy
- D. Application Override policy

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

A Security policy rule is configured with a Vulnerability Protection Profile and an action of “Deny”.

Which action will this cause configuration on the matched traffic?

- A. The configuration is invalid. The Profile Settings section will be grayed out when the Action is set to “Deny”.
- B. The configuration will allow the matched session unless a vulnerability signature is detected. The “Deny” action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile.
- C. The configuration is invalid. It will cause the firewall to skip this Security policy rule. A warning will be displayed during a commit.
- D. The configuration is valid. It will cause the firewall to deny the matched sessions. Any configured Security Profiles have no effect if the Security policy rule action is set to “Deny”.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 10

A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach <http://www.company.com>. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to <http://www.company.com>.

How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

- A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question.
- B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question.
- C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
- D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 12

An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required.

Which interface type would support this business requirement?

- A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
- B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only
- C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRP protocols)
- D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 14

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)



Correct Answer: A

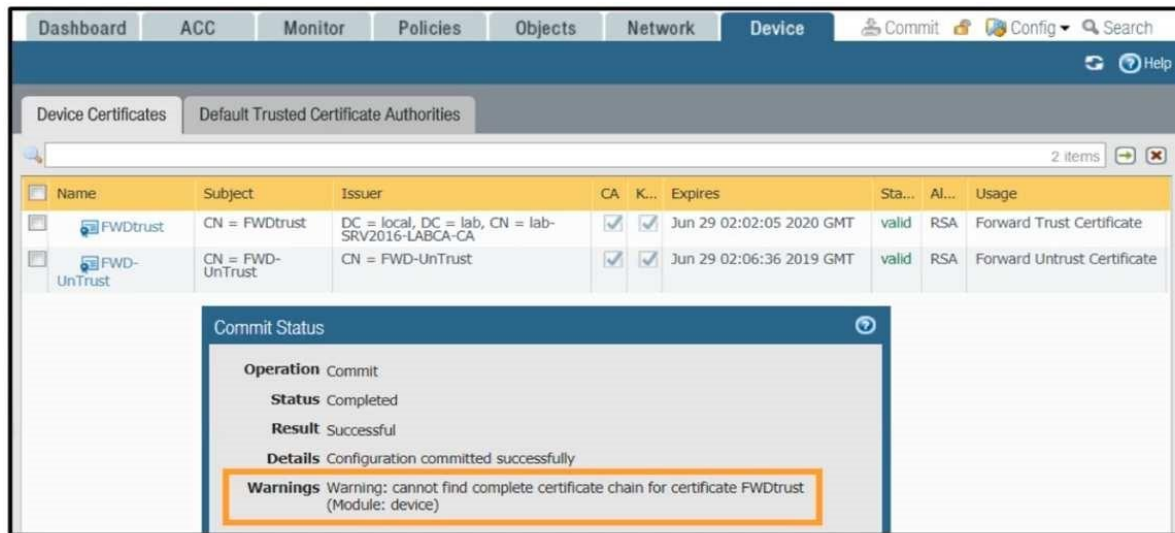
Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

In the image, what caused the commit warning?



- A. The CA certificate for FWDtrust has not been imported into the firewall.
- B. The FWDtrust certificate has not been flagged as Trusted Root CA.
- C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
- D. The FWDtrust certificate does not have a certificate chain.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

- A. Okta
- B. DUO
- C. RADIUS
- D. PingID

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

- A. Use the debug dataplane packet-diag set capture stage firewall file command.
- B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
- C. Use the debug dataplane packet-diag set capture stage management file command.
- D. Use the tcpdump command.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390>

QUESTION 18

An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

- A. Port Inspection
- B. Certificate revocation
- C. Content-ID
- D. App-ID

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/quality-of-service/qos-concepts/qos-for-applications-and-users#daed4e749-80b44641-a37c-c741aba562e9>

QUESTION 19

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.

Correct Answer: B

Section: (none)

Explanation

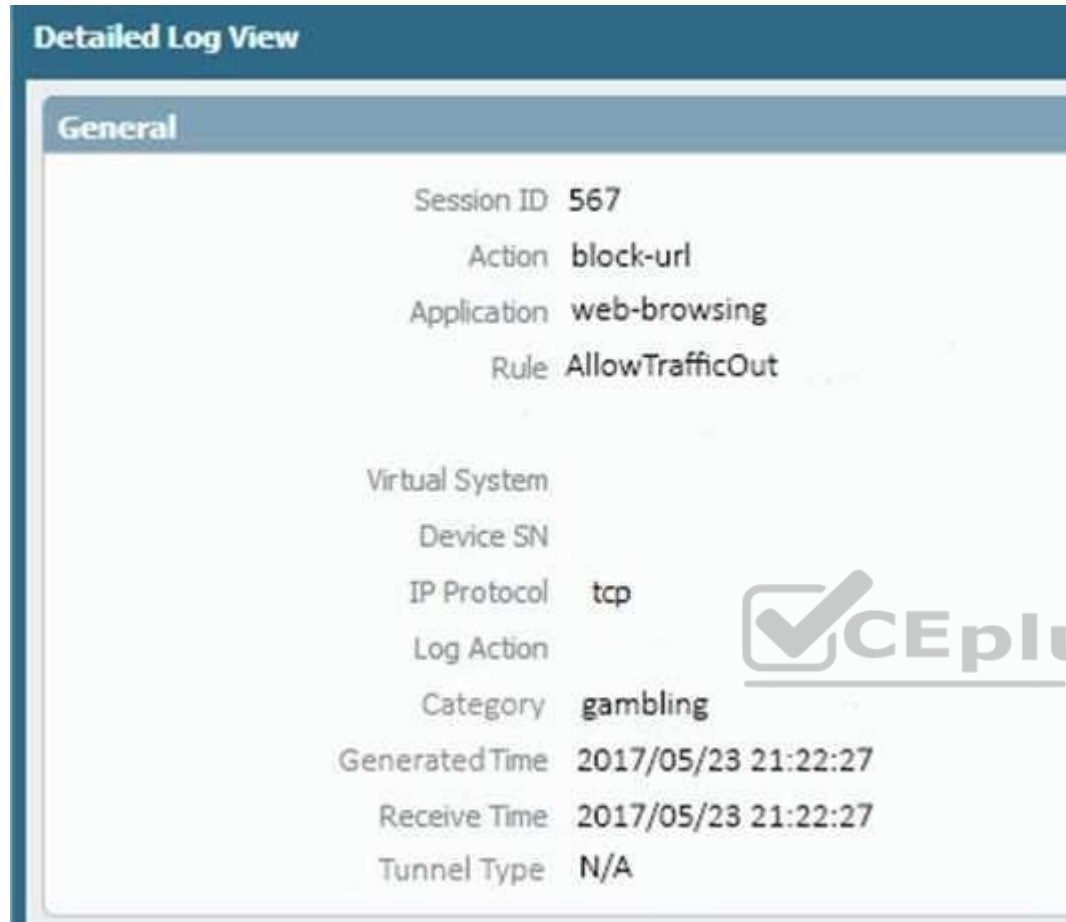
Explanation/Reference:

QUESTION 20

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.

URL Filtering Profile

Name: Filter1

Description:

Categories | Overrides | URL Filtering Settings | User Credential Detection

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	block	block
<input type="checkbox"/> health-and-medicine	continue	allow
	override	allow

* indicates a custom URL category; + indicates external dynamic list

Check URL Category

OK Cancel

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions | Target

Name: www.megamillions.com

Rule Type: universal (default)

Description:

Tags:

OK Cancel

B. C.

<https://vceplus.com/>

URL Filtering Profile

Name:

Description:

Overrides Categories URL Filtering Settings User Credential Detection

Allow-List:

Block List:

Action:

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

D.

URL Filtering Profile

Name:

Description:

Overrides Categories URL Filtering Settings User Credential Detection

Allow-List:

Block List:

Action:

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

E.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

A customer has an application that is being identified as unknown-tcp 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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

An administrator has left a firewall to use the default port for all management services.

Which three functions are performed by the dataplane? (Choose three.)

- A. WildFire updates
- B. NAT



<https://vceplus.com/>

- C. NTP
- D. antivirus
- E. file blocking

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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.

<https://vceplus.com/>

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Starting with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

- A. GlobalProtect
- B. System
- C. Authentication

D. Configuration

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/enhanced-logging-for-globalprotect.html>

QUESTION 26

Which three authentication services can an administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)

- A. Kerberos
- B. PAP
- C. SAML
- D. TACACS+
- E. RADIUS
- F. LDAP

Correct Answer: ACF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

- A. Deny application facebook-chat before allowing application facebook
- B. Deny application facebook on top
- C. Allow application facebook on top
- D. Allow application facebook before denying application facebook-chat

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/115673>

QUESTION 28

A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers.

Which option will protect the individual servers?

- A. Enable packet buffer protection on the Zone Protection Profile.
- B. Apply an Anti-Spyware Profile with DNS sinkholing.
- C. Use the DNS App-ID with application-default.
- D. Apply a classified DoS Protection Profile.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

Refer to the exhibit.

Device Certificates										
Default Trusted Certificate Authorities										
1 item										
Name	Location	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage	
Domain-Root-Cert	vsys1	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Nov 1 00:34:47 2021 GMT	valid	RSA	Trusted Root CA Certificate	
Domain Sub-CA	vsys1	CN = sca.lab.local	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 20:59:38 2019 GMT	valid	RSA		
Forward_Trust	vsys1	CN = fwdtrust.la...	CN = sca.lab.local	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 21:09:49 2018 GMT	valid	RSA		

Which certificates can be used as a Forward Trust certificate?

- A. Certificate from Default Trust Certificate Authorities
- B. Domain Sub-CA
- C. Forward_Trust
- D. Domain-Root-Cert

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

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.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 33

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

- A. scp export tcpdump from mgmt.pcap to < username@host:path>
- B. scp extract mgmt-pcap from mgmt.pcap to < username@host:path>
- C. scp export mgmt-pcap from mgmt.pcap to < username@host:path>
- D. download mgmt-pcap

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 34

Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

- A. Session Browser
- B. Application Command Center

- C. TCP Dump
- D. Packet Capture

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Management-Articles/Tips-and-Tricks-How-to-Use-the-Application-Command-Center-ACC/ta-p/67342>

QUESTION 35

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

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

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

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

- A. URL Filtering profile
- B. Zone Protection profile
- C. Anti-Spyware profile
- D. Vulnerability Protection profile

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 37

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.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 38

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.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router.

Which two options enable the administrator to troubleshoot this issue? (Choose two.)

- A. View Runtime Stats in the virtual router.
- B. View System logs.
- C. Add a redistribution profile to forward as BGP updates.
- D. Perform a traffic pcap at the routing stage.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

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

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



Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 41

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

- A. Heartbeat Monitoring
- B. Failover

- C. Path Monitoring
- D. Ping-Path

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf> **QUESTION 42**

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

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/decryption-concepts/decryption-mirroring>

QUESTION 43

When is the content inspection performed in the packet flow process?

- A. after the application has been identified
- B. before session lookup
- C. before the packet forwarding process
- D. after the SSL Proxy re-encrypts the packet

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081>

QUESTION 44

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 45

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.

Which Security Profile type will prevent this attack?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

<https://vceplus.com/>

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection>

QUESTION 46

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?



```
admin@Lab33-111-PA-3060(active)> show clock
```

```
Thu Jun  8 12:49:55 PDT 2017
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
```

```
test-pbf {
  action {
    forward {
      egress-interface ethernet1/5;
    }
  }
  from {
    zone L3-Trust;
  }
  enforce-symmetric-return {
    enabled no;
  }
  source 192.168.111.3;
  destination 10.46.41.113;
  source-user any;
  application any;
  service any;
  schedule schedule-pbf;
}
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
```

```
schedule-pbf {
  schedule-type {
    recurring {
      daily 16:00-21:00;
    }
  }
}
```

```
#####
```

```
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
67	10.10.20.0/24	0.0.0.0	u	ethernet1/7	1500
66	10.10.20.111/32	0.0.0.0	uh	ethernet1/7	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
49	10.46.44.0/23	0.0.0.0	u	ethernet1/5	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
48	10.46.45.111/32	0.0.0.0	uh	ethernet1/5	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

A. ethernet1/7

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

Correct Answer: D

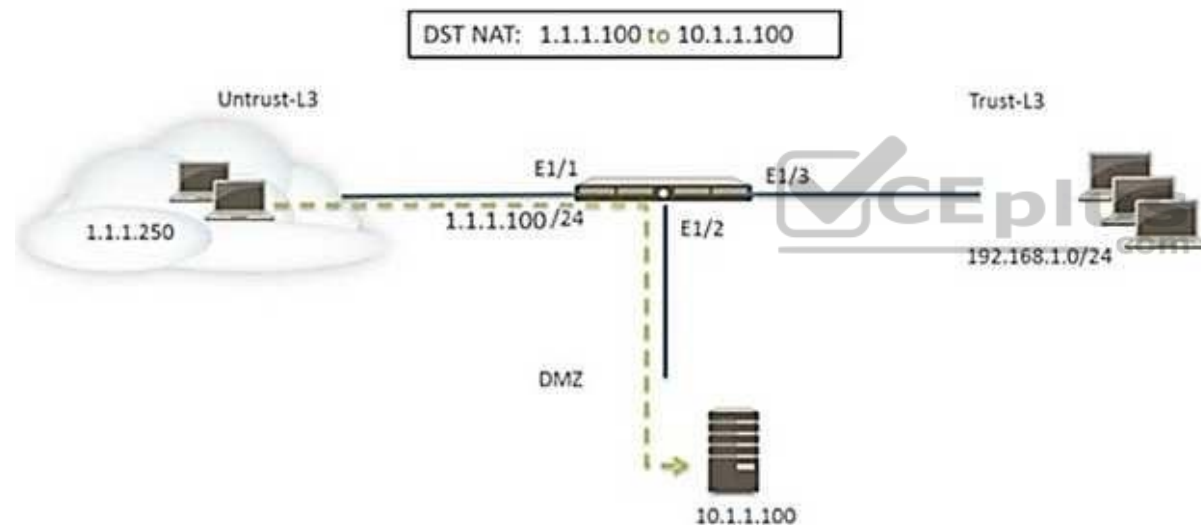
Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web-browsing traffic to this server on tcp/443?

- A. Rule #1: application: web-browsing; service: application-default; action: allow
Rule #2: application: ssl; service: application-default; action: allow
- B. Rule #1: application: web-browsing; service: service-http; action: allow Rule
#2: application: ssl; service: application-default; action: allow
- C. Rule # 1: application: ssl; service: application-default; action: allow
Rule #2: application: web-browsing; service: application-default; action: allow
- D. Rule #1: application: web-browsing; service: service-https; action: allow Rule
#2: application: ssl; service: application-default; action: allow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-network>

QUESTION 50

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/define-traffic-to-decrypt/create-a-decryption-profile>

QUESTION 51

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 52

Which feature can be configured on VM-Series firewalls?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links>

QUESTION 54

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. TLS Bidirectional Inspection
- B. SSL Inbound Inspection
- C. SSH Forward Proxy
- D. SMTP Inbound Decryption

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 55

Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)

- A. Verify AutoFocus status using the CLI "test" command.
- B. Check the WebUI Dashboard AutoFocus widget.
- C. Check for WildFire forwarding logs.
- D. Check the license.
- E. Verify AutoFocus is enabled below Device Management tab.



Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence>

QUESTION 56

Which two subscriptions are available when configuring Panorama to push dynamic updates to connected devices? (Choose two.)

- A. Content-ID
- B. User-ID
- C. Applications and Threats
- D. Antivirus

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates>

QUESTION 57

What is exchanged through the HA2 link?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links>

QUESTION 58

Which prerequisite must be satisfied before creating an SSH proxy Decryption policy?

- A. Both SSH keys and SSL certificates must be generated.
- B. No prerequisites are required.
- C. SSH keys must be manually generated.
- D. SSL certificates must be generated.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssh-proxy>

QUESTION 59

VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor.

When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

- A. Zone Protection
- B. Replay
- C. Web Application
- D. DoS Protection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

An administrator has configured a QoS policy rule and a QoS Profile that limits the maximum allowable bandwidth for the YouTube application. However, YouTube is consuming more than the maximum bandwidth allotment configured.

Which configuration step needs to be configured to enable QoS?

- A. Enable QoS interface
- B. Enable QoS in the Interface Management Profile
- C. Enable QoS Data Filtering Profile
- D. Enable QoS monitor

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

Which log file can be used to identify SSL decryption failures?

- A. Traffic

- B. ACC
- C. Configuration
- D. Threats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62

A customer wants to set up a site-to-site VPN using tunnel interfaces.

Which two formats are correct for naming tunnel interfaces? (Choose two.)

- A. tunnel.1
- B. vpn-tunnel.1
- C. tunnel.1025
- D. vpn-tunnel.1024



Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63

An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the Internet.

Which configuration will enable the firewall to download and install application updates automatically?

- A. Download and install application updates cannot be done automatically if the MGT port cannot reach the Internet.
- B. Configure a service route for Palo Alto Networks Services that uses a dataplane interface that can route traffic to the Internet, and create a Security policy rule to allow the traffic from that interface to the update servers if necessary.
- C. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interfaced destined for the

update servers goes out of the interface acting as your Internet connection.

D. Configure a Security policy rule to allow all traffic to and from the update servers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

A company wants to install a NGFW firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone.

Which option differentiates multiple VLANs into separate zones?

- A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096" in the "Tag Allowed" field of the V-Wire object.
- B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the "Tag Allowed" field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.
- C. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface to a unique zone. Do not assign any interface an IP address.
- D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

- A. System Utilization log
- B. System log
- C. Resources widget



<https://vceplus.com/>

D. CPU Utilization widget

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

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

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

Correct Answer: ABDF

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 67

<https://vceplus.com/>

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

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

An administrator wants to upgrade an NGFW from PAN-OS® 7.1.2 to PAN-OS® 8.1.0. The firewall is not a part of an HA pair.

What needs to be updated first?

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



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

- A. Load configuration version
- B. Save candidate config
- C. Export device state
- D. Load named configuration snapshot

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

An administrator just submitted a newly found piece of spyware for WildFire analysis. The spyware passively monitors behavior without the user's knowledge.

What is the expected verdict from WildFire?

- A. Malware
- B. Grayware
- C. PhishingD. Spyware

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 71

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

Which User-ID method maps IP addresses to usernames for users connecting through a web proxy that has already authenticated the user?

- A. syslog listening
- B. server monitoring
- C. client probing
- D. port mapping

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

- A. At-boot
- B. Pre-logon
- C. User-logon (Always on)
- D. On-demand

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

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

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

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

QUESTION 75

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

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

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 76

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

Which is the maximum number of samples that can be submitted to WildFire per day, based on a WildFire subscription?

- A. 10,000
- B. 15,000
- C. 7,500

D. 5,000

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:

- Firewall has internet connectivity through e 1/1.
 - Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
 - Service route is configured, sourcing update traffic from e1/1.
 - A communication error appears in the System logs when updates are performed. ▪
- Download does not complete.

What must be configured to enable the firewall to download the current version of PAN-OS software?

- A. Static route pointing application PaloAlto-updates to the update servers
- B. Security policy rule allowing PaloAlto-updates as the application
- C. Scheduler for timed downloads of PAN-OS software
- D. DNS settings for the firewall to use for resolution

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

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. Add an Anti-Spyware Profile to block attacking IP address
- B. Define a custom App-ID to ensure that only legitimate application traffic reaches the server

- C. Add QoS Profiles to throttle incoming requests
- D. Add a tuned DoS Protection Profile

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

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. Antivirus update package.
- B. Applications and Threats update package.
- C. User-ID agent.
- D. WildFire update package.



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-the-firewall-to-pan-os-80/upgrade-an-ha-firewall-pair-to-pan-os-80>

QUESTION 81

A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.

Which Security Profile type will prevent these behaviors?

- A. Anti-Spyware
- B. WildFire

- C. Vulnerability Protection
- D. Antivirus

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 82

What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

- A. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or template stacks.
- B. An administrator must use the Expedition tool to adapt the configuration to the pre-PAN-OS 8.1 state.
- C. When Panorama is reverted to an earlier PAN-OS release, variables used in templates or template stacks will be removed automatically.
- D. Administrators need to manually update variable characters to those used in pre-PAN-OS 8.1.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgradedowngrade-considerations>

QUESTION 83

Which administrative authentication method supports authorization by an external service?

- A. Certificates
- B. LDAP
- C. RADIUS
- D. SSH keys

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/firewall-administration/manage-firewall-administrators/administrative-authentication>

QUESTION 84

Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

- A. .dll
- B. .exe
- C. .fon
- D. .apk
- E. .pdf
- F. .jar

Correct Answer: DEF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 85

An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.

Which configuration will enable this HA scenario?

- A. The two firewalls will share a single floating IP and will use gratuitous ARP to share the floating IP.
- B. Each firewall will have a separate floating IP, and priority will determine which firewall has the primary IP.
- C. The firewalls do not use floating IPs in active/active HA.
- D. The firewalls will share the same interface IP address, and device 1 will use the floating IP if device 0 fails.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/floating-ip-address-and-virtual-mac-address>

QUESTION 86

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-vmware-nsx/dynamically-quarantineinfected-guests>

QUESTION 87

Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

- A. Create a no-decrypt Decryption Policy rule.
- B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
- C. Configure a Dynamic Address Group for untrusted sites.
- D. Create a Security Policy rule with a vulnerability Security Profile attached.
- E. Enable the "Block sessions with untrusted issuers" setting.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-decryption-profile>

QUESTION 88

SAML SLO is supported for which two firewall features? (Choose two.)

- A. GlobalProtect Portal

- B. CaptivePortal
- C. WebUI
- D. CLI

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 89

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.



Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 90

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

Correct Answer: A

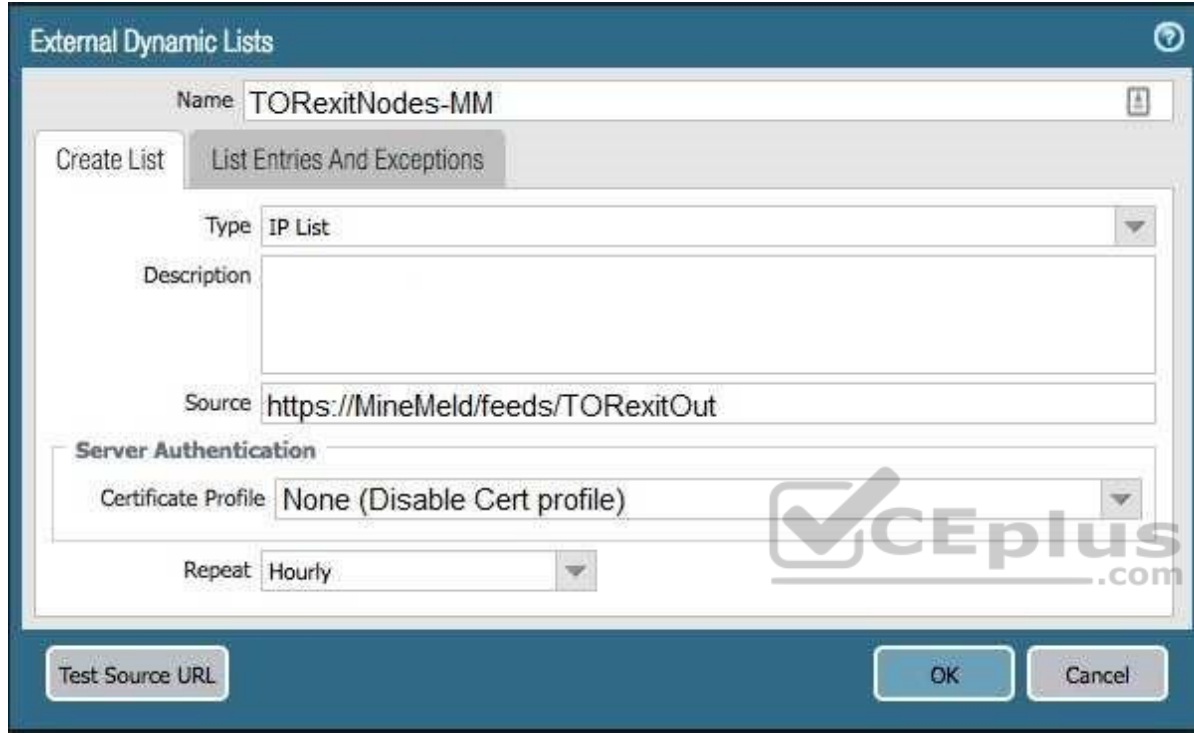
Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/networking-features/ssl-ssh-session-end-reasons> **QUESTION 91**

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



- 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.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/MineMeld-Articles/Connecting-PAN-OS-to-MineMeld-using-External-Dynamic-Lists/ta-p/190414>

QUESTION 92

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/globalprotect-features/split-tunnel-for-public-applications>

QUESTION 93

Which option describes the operation of the automatic commit recovery feature?

- A. It enables a firewall to revert to the previous configuration if rule shadowing is detected.
- B. It enables a firewall to revert to the previous configuration if application dependency errors are found.
- C. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure.
- D. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html>

QUESTION 94

Which three items are important considerations during SD-WAN configuration planning? (Choose three.)

- A. branch and hub locations
- B. link requirements

- C. the name of the ISP
- D. IP Addresses

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration>

QUESTION 95

Starting with PAN-OS version 9.1, application dependency information is now reported in which two new locations? (Choose two.)

- A. on the **App Dependency** tab in the **Commit Status** window
- B. on the Policy Optimizer's **Rule Usage** page
- C. on the **Application** tab in the **Security Policy Rule** creation window
- D. on the **Objects > Applications** browser pages

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies>

QUESTION 96

Panorama provides which two SD-WAN functions? (Choose two.)

- A. network monitoring
- B. control plane
- C. data plane
- D. physical network links

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:





<https://vceplus.com/>



<https://vceplus.com/>