

PCNSE

Number: PCNSE
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



<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

Google+ : <https://plus.google.com/+Vcepluscom>

LinkedIn : <https://www.linkedin.com/company/vceplus>

PCNSE

Palo Alto Networks Certified Network Security Engineer

Exam A**QUESTION 1**

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 2

Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS® software?



<https://vceplus.com/>

- A. XML API
- B. Port Mapping
- C. Client Probing
- D. Server Monitoring

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/user-id-concepts>

QUESTION 3

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 4**

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 5

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 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 6

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 7

What are two benefits of nested device groups in Panorama? (Choose two.)



<https://vceplus.com/>

- A. Reuse of the existing Security policy rules and objects
- B. Requires configuring both function and location for every device
- C. All device groups inherit settings from the Shared group
- D. Overwrites local firewall configuration

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 8

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 9

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: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

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: B

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 11

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 web browsing access to the server.

Which application and service need to be configured to allow only cleartext web-browsing traffic to this 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

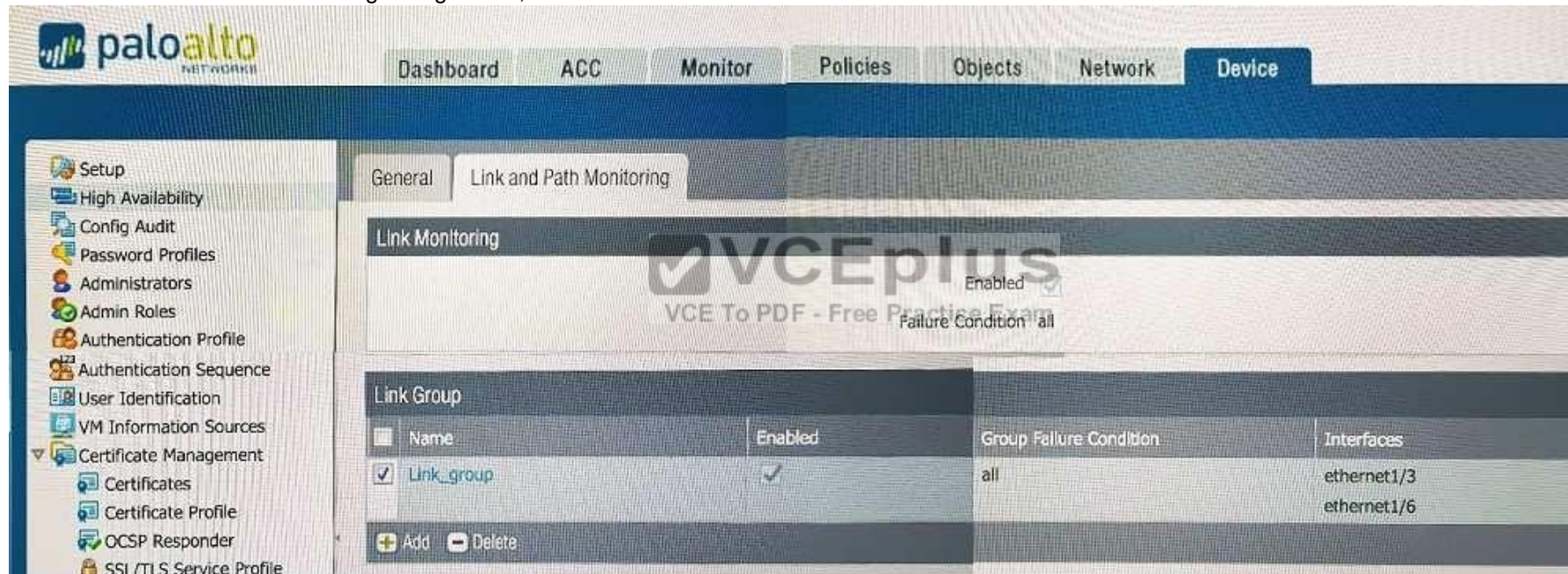
Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

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 PANOS® software would help in this case?



<https://vceplus.com/>

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

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 15

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 topdump command.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 16

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/71/pan-os/pan-os/quality-of-service/qos-for-applications-and-users>

QUESTION 17

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 USP, 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: C

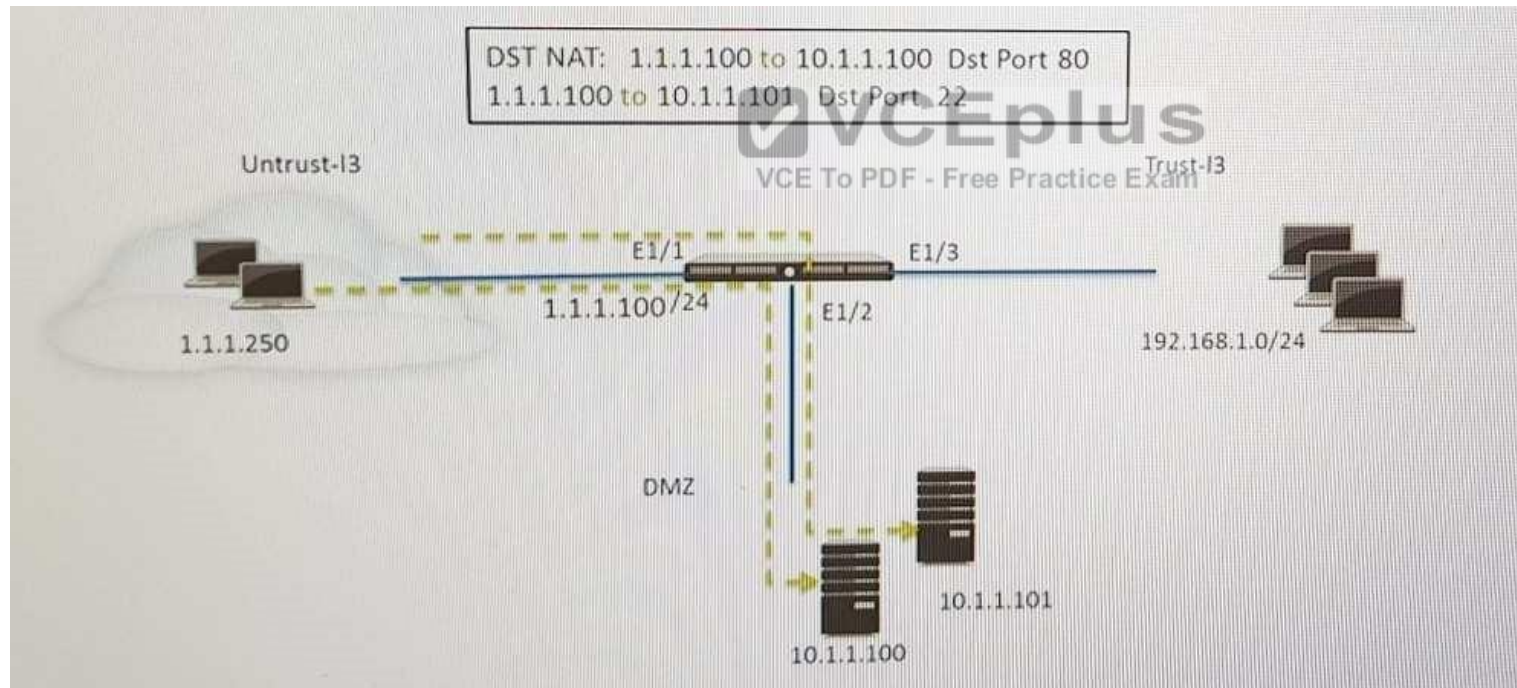
Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

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

Correct Answer: CD

Section: (none)

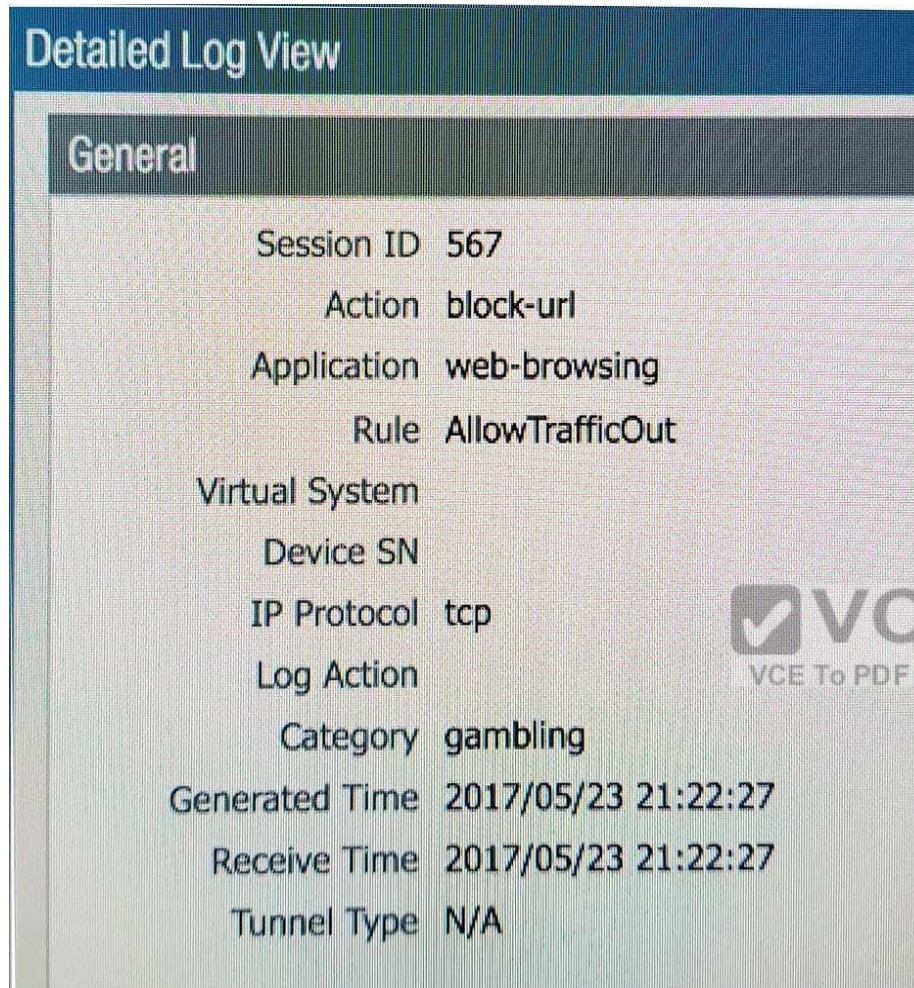
Explanation

Explanation/Reference:

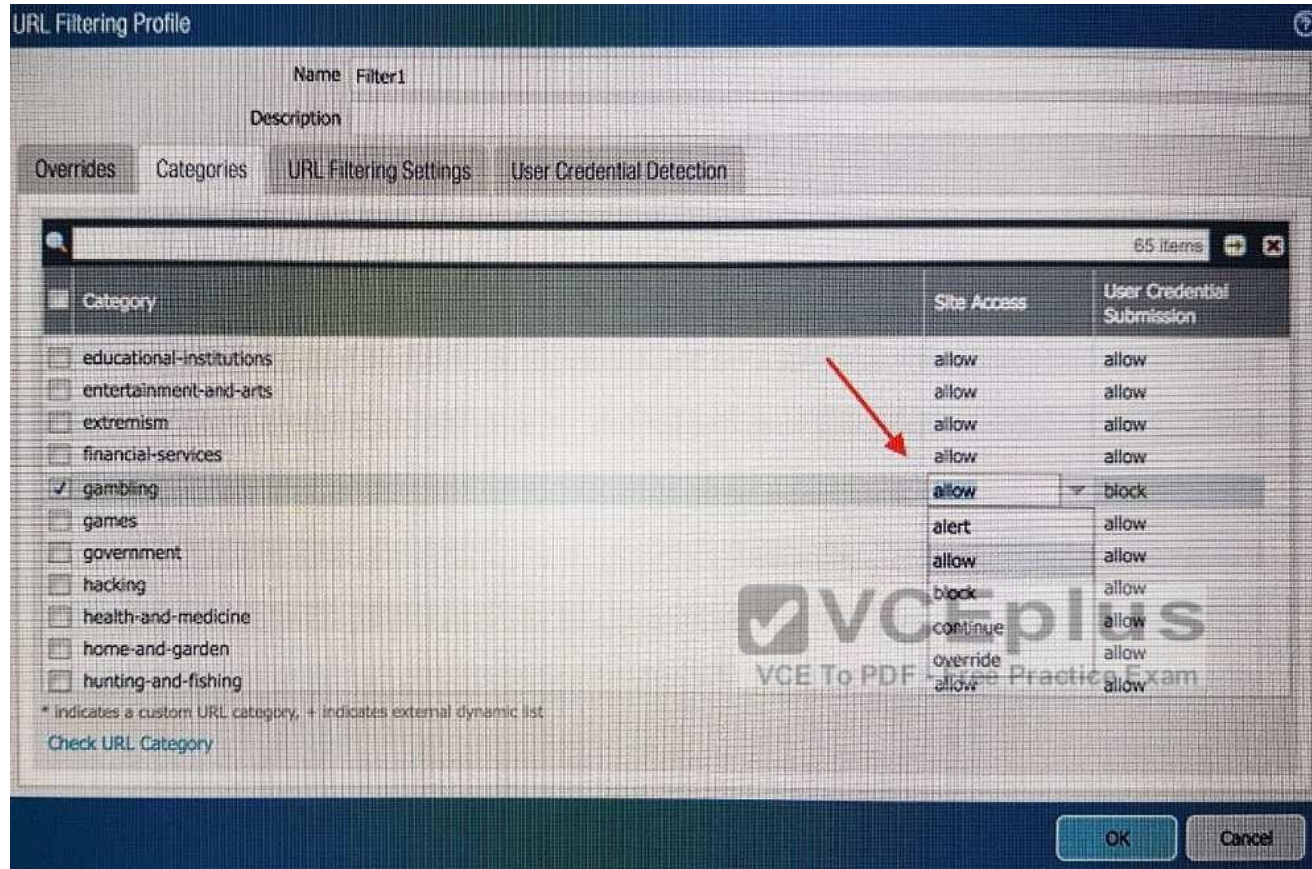
QUESTION 19

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.



B.



C.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name www.megamillions.com

Rule Type universal (default)

Description

Tags

OK Cancel

D.

URL Filtering Profile

Name Filter1

Description

Overrides Categories URL Filtering Settings User Credential Detection

Allow List www.megamillions.com

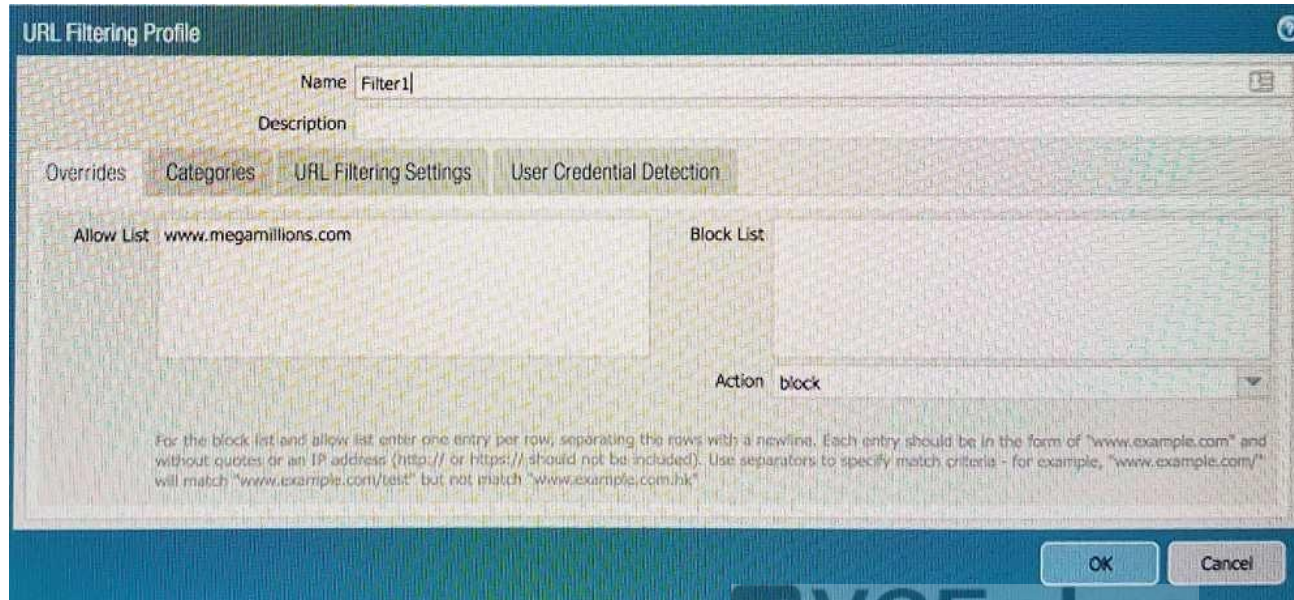
Block List

Action continue

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"

OK Cancel

E.



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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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

- A. Setup



<https://vceplus.com/>

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

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:



QUESTION 21

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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab. Which profile is the cause of the missing Policies tab?

- A. Admin Role
- B. WebUI
- C. Authentication
- D. Authorization

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

A Palo Alto Networks NGFW just submitted a file to WildFire for analysis. Assume a 5-minute window for analysis. The firewall is configured to check for verdicts every 5 minutes.

How quickly will the firewall receive back a verdict?

- A. More than 15 minutes
- B. 5 minutes
- C. 10 to 15 minutes
- D. 5 to 10 minutes



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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. DoS Protection
- C. Web Application
- D. Replay

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

Which Palo Alto Networks VM-Series firewall is valid?

- A. VM-25
- B. VM-800 C. VM-50
- D. VM-400

Correct Answer: C

Section: (none)

Explanation

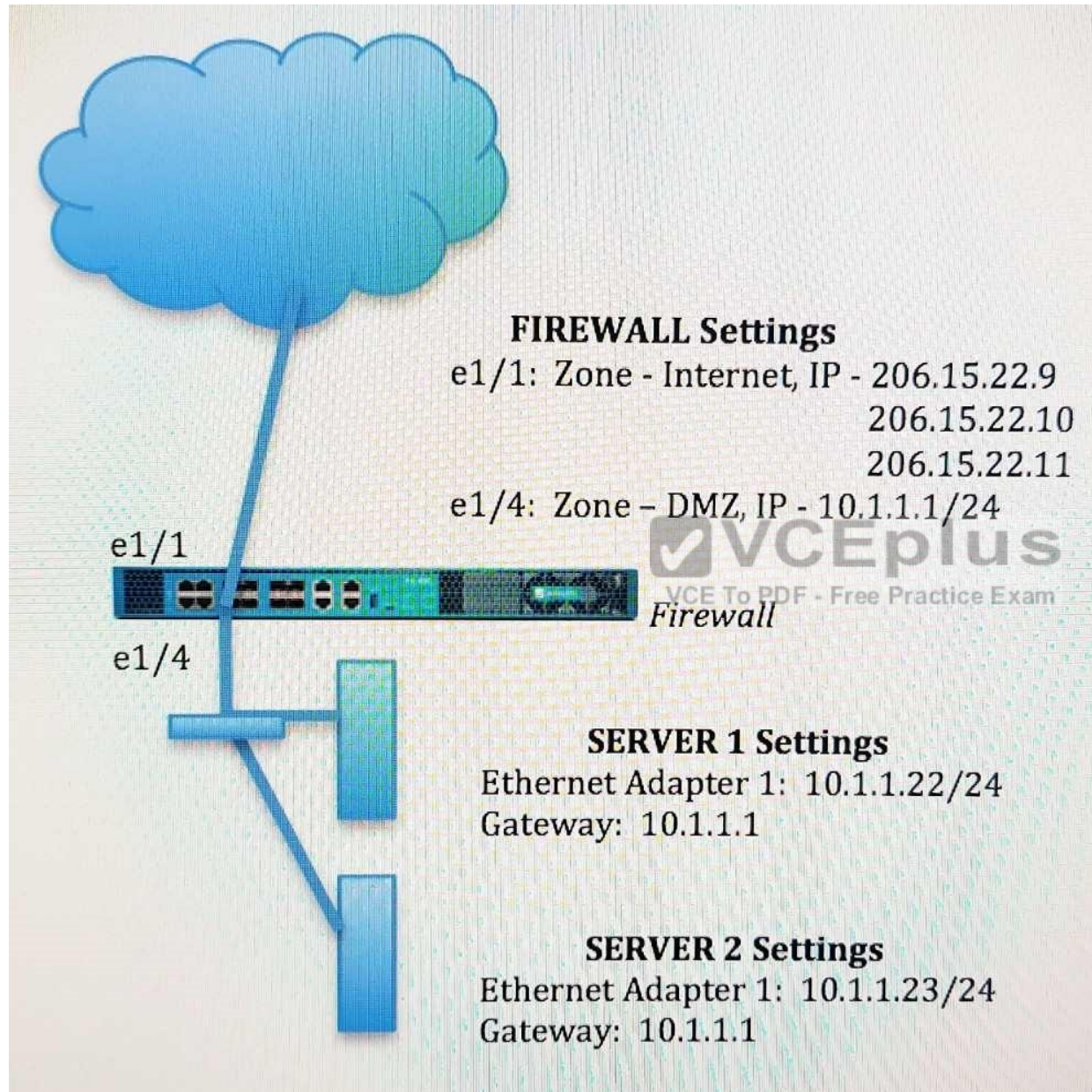
Explanation/Reference:

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

QUESTION 28

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: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

B.

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/UDP

C.

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

D.

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

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 30

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. .src
- D. .apk
- E. .pdf
- F. .jar



Correct Answer: DEF

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-support

QUESTION 31

Refer to the 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	

#####

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

Which three authentication services can 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 33

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

- A. Threat-ID processing time is decreased.
- B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.

- C. The application name assigned to the traffic by the security rule is written to the Traffic log.
- D. App-ID processing time is increased.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 34

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 35

Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?

- A. debug system details
- B. show session info
- C. show system info
- D. show system details

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN-OS-6.0-CLI-ref.pdf **QUESTION 36**

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



<https://vceplus.com/>

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 37

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)

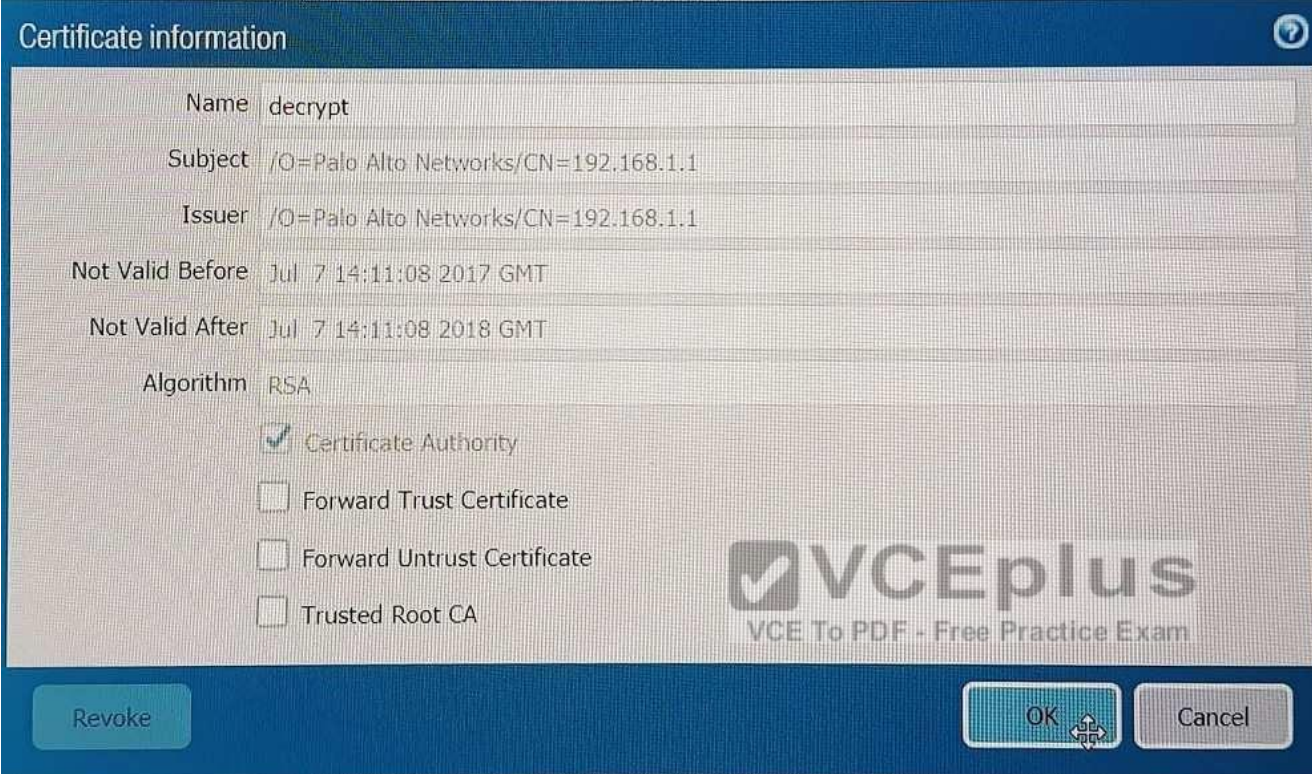
Explanation

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 38

The certificate information displayed in the following image is for which type of certificate?



The image shows a 'Certificate information' dialog box with the following details:

Name	decrypt
Subject	/O=Palo Alto Networks/CN=192.168.1.1
Issuer	/O=Palo Alto Networks/CN=192.168.1.1
Not Valid Before	Jul 7 14:11:08 2017 GMT
Not Valid After	Jul 7 14:11:08 2018 GMT
Algorithm	RSA

Below the table, there are four checkboxes:

- ☒ Certificate Authority
- ☐ Forward Trust Certificate
- ☐ Forward Untrust Certificate
- ☐ Trusted Root CA

At the bottom, there are three buttons: 'Revoke', 'OK', and 'Cancel'. A watermark for 'VCEplus VCE To PDF - Free Practice Exam' is visible in the background of the dialog box.

- A. Forward Trust certificate
- B. Self-Signed Root CA certificate
- C. Web Server certificate
- D. Public CA signed certificate

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

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 40

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 41

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 42

If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect when users browse to HTTP(S) websites?

- A. SSL Forward Proxy
- B. SSL Inbound Inspection
- C. TLS Bidirectional proxy
- D. SSL Outbound Inspection

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>