Palo-Alto-Networks.Premium.PCNSE.by.VCEplus.155q

Number: PCNSE VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 6.3

Exam Code: PCNSE
Exam Name: Palo Alto Networks Certified Network Security Engineer
Certification Provider: Palo Alto Networks
Corresponding Certification: PCNSE
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-pcnse/

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in PCNSE exam products and you get latest questions. We strive to deliver the best PCNSE exam product for top grades in your first attempt.

Exam A

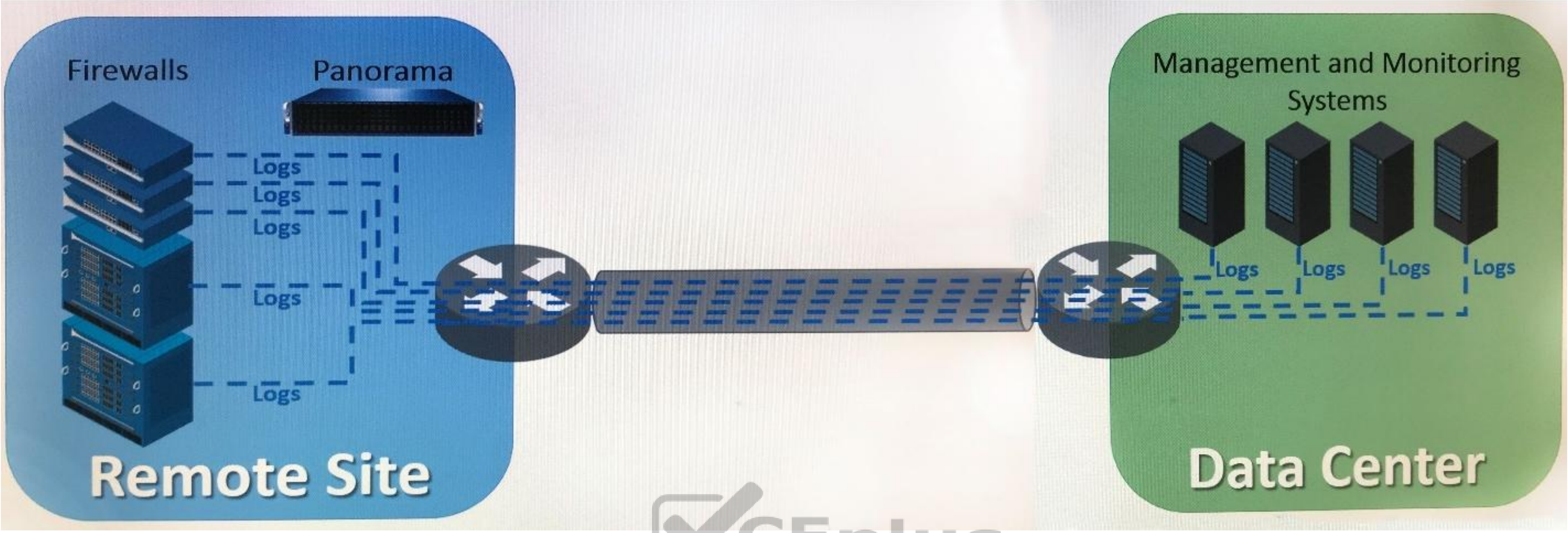
QUESTION 1
Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

A. check
B. find
C. test
D. sim

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html

QUESTION 2
Refer to 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 existing monitoring/security platforms?

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/network/network-interfaces/pa-7000-series-layer-2-interface

QUESTION 4
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/71/pan-os/pan-os/policy/antivirus-profiles

QUESTION 5
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of reconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.
Which VPN configuration would adapt to changes when deployed to the future site?

A. Preconfigured GlobalProtect satellite

B. Preconfigured GlobalProtect client

C. Preconfigured IPsec tunnels

D. Preconfigured PPTP Tunnels

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5.pdf (page 9)

QUESTION 7
An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair.
Which NGFW receives the configuration from Panorama?

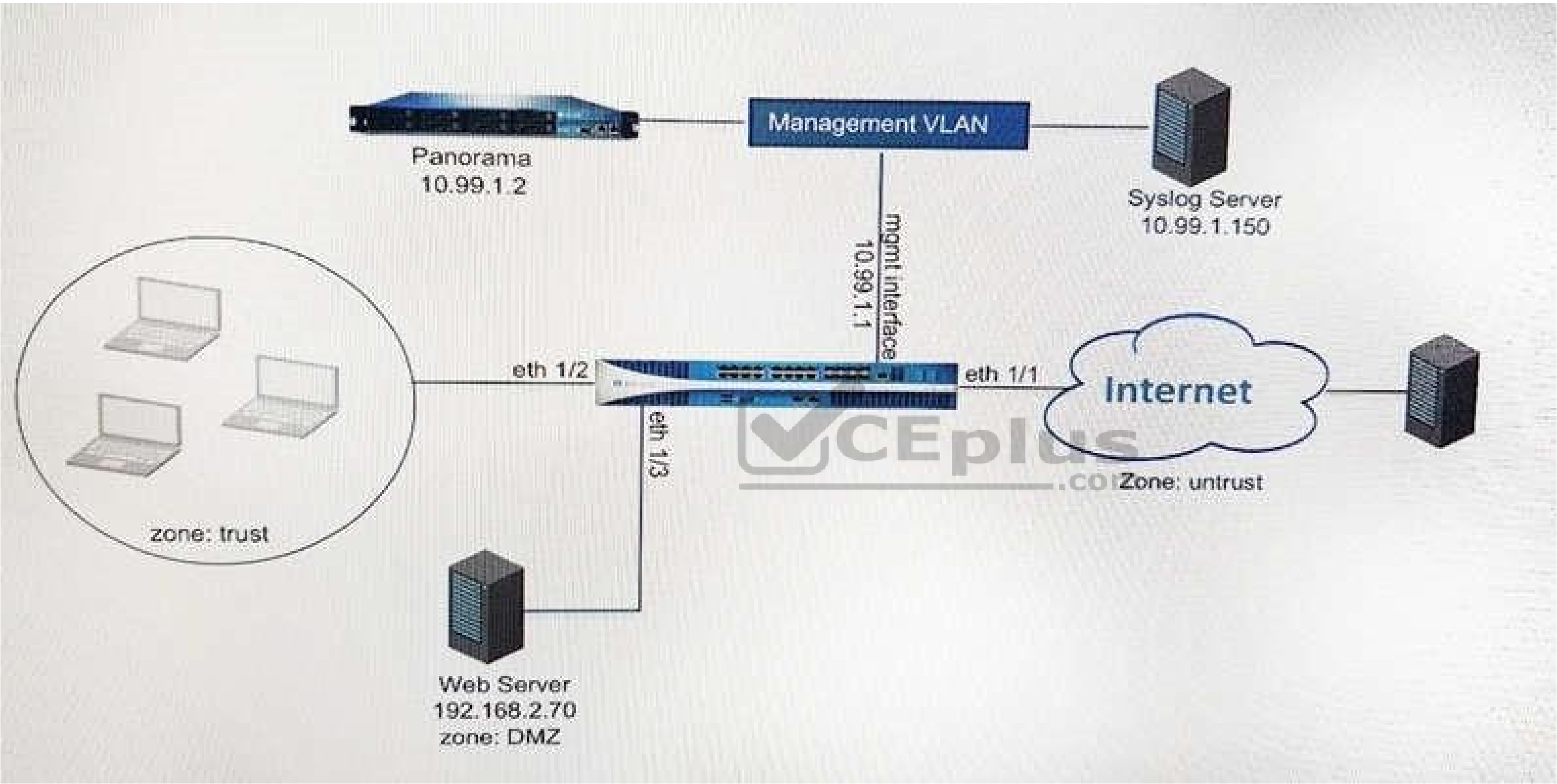
A. The Passive firewall, which then synchronizes to the active firewall
B. The active firewall, which then synchronizes to the passive firewall
C. Both the active and passive firewalls, which then synchronize with each other
D. Both the active and passive firewalls independently, with no synchronization afterward

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

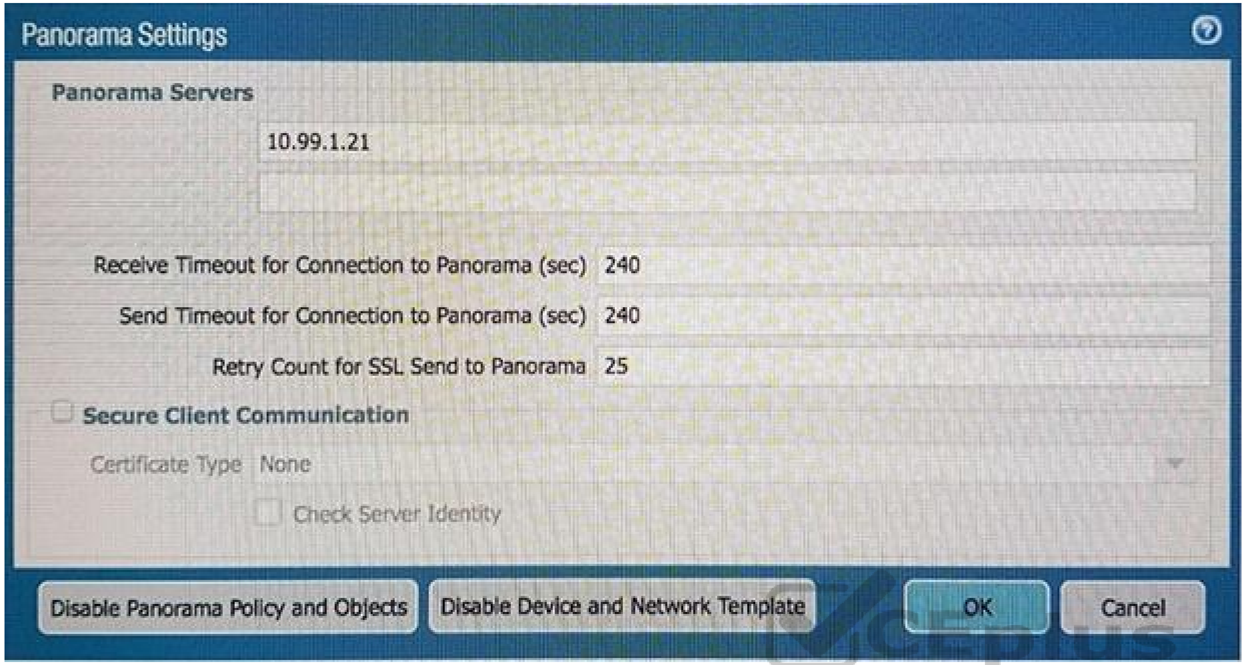
Refer to the exhibit.



An administrator cannot see any if the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side.

Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?

A.



Panorama Settings

Panorama Servers

10.99.1.21

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

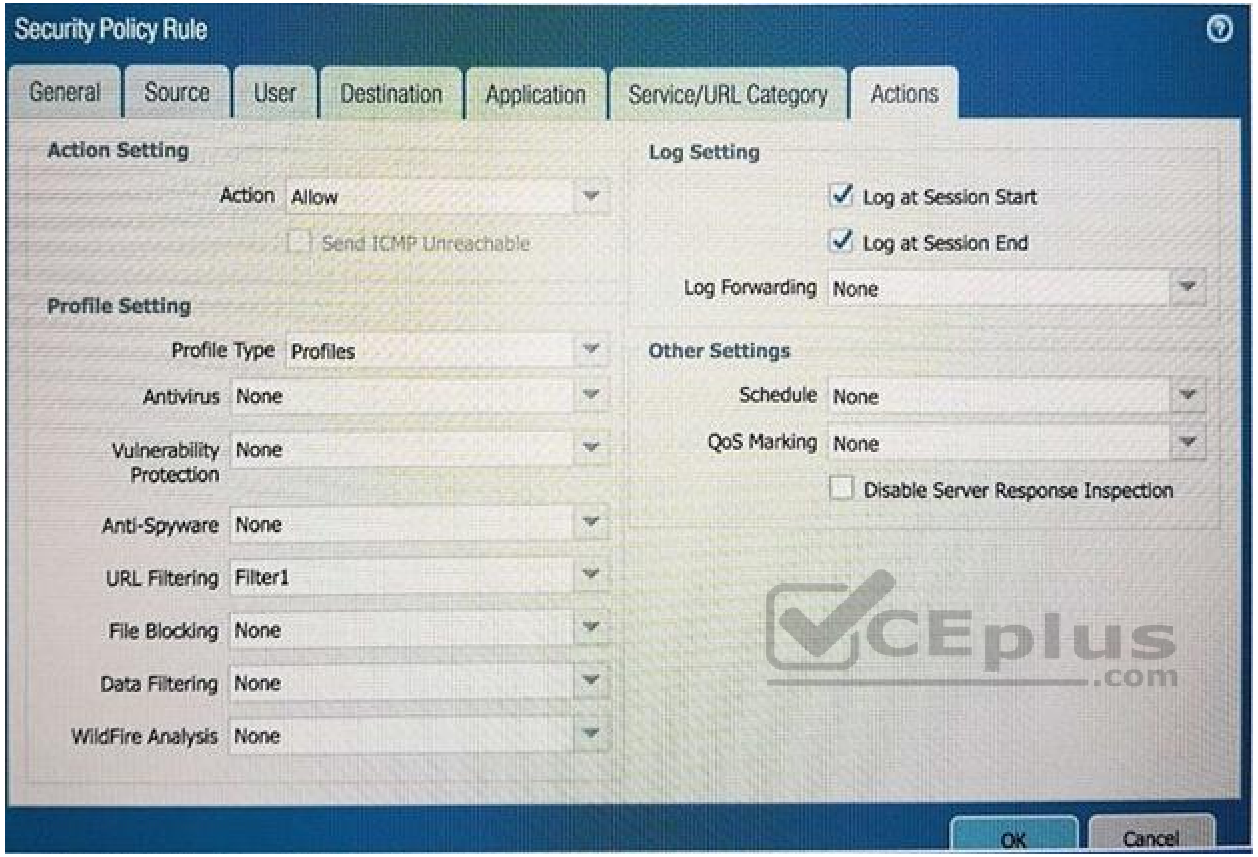
□ Secure Client Communication

Certificate Type None

□ Check Server Identity

Disable Panorama Policy and Objects
Disable Device and Network Template
OK
Cancel

B.



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: Filter1

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

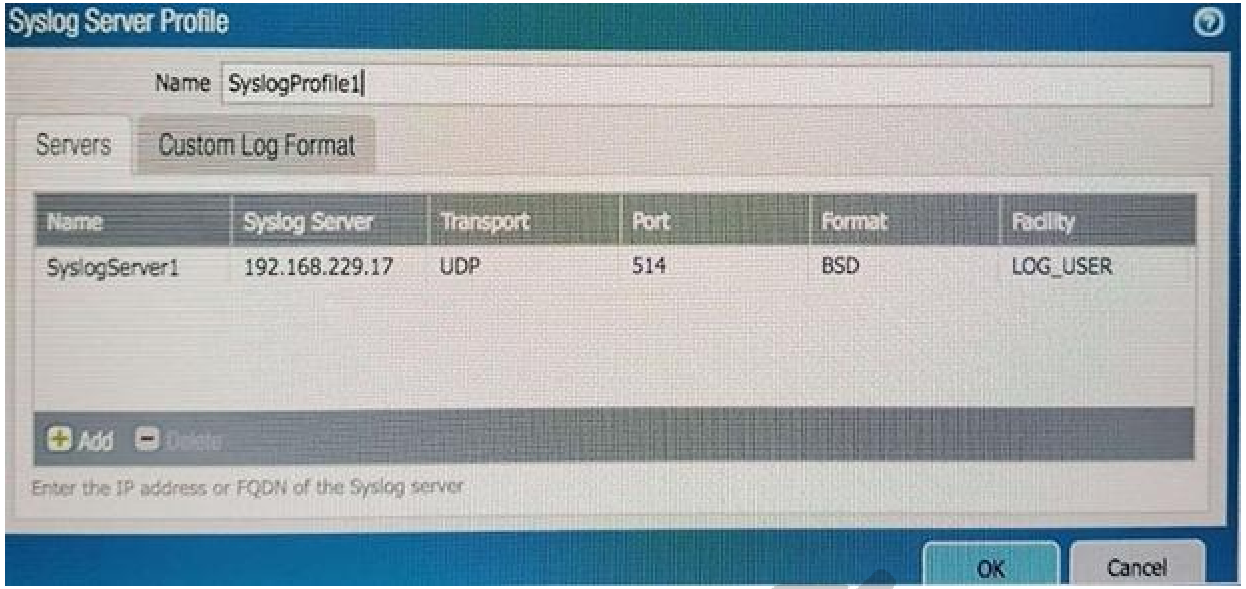
Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

C.

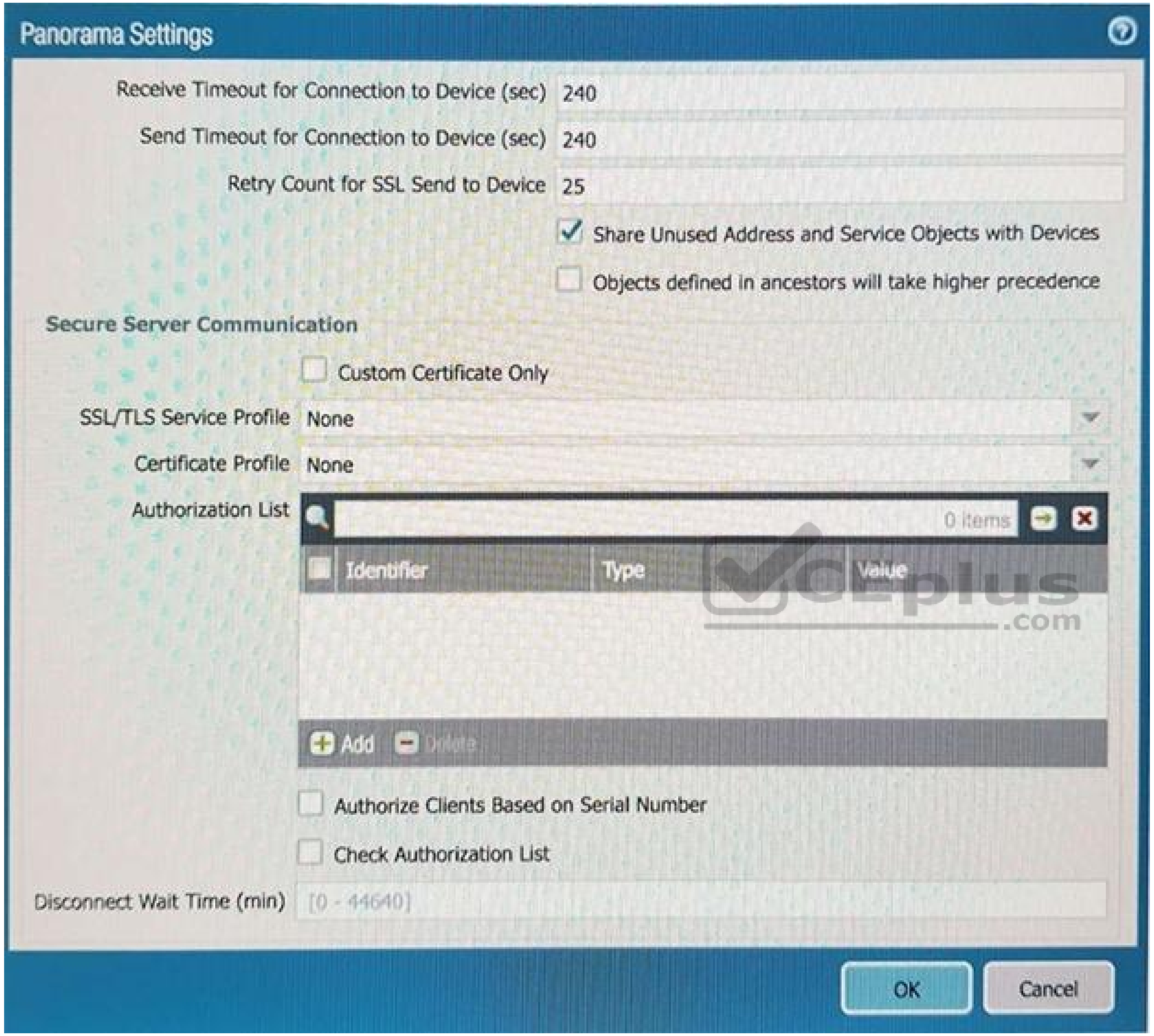


Name SyslogProfile1

Name	Syslog Server	Transport	Port	Format	Facility
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

D.



Panorama Settings

Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

☑ Share Unused Address and Service Objects with Devices

□ Objects defined in ancestors will take higher precedence

Secure Server Communication

□ Custom Certificate Only

SSL/TLS Service Profile None

Certificate Profile None

Authorization List 0 items

□	Identifier	Type	Value

□ Authorize Clients Based on Serial Number

□ Check Authorization List

Disconnect Wait Time (min) [0 - 44640]

A. Option A
B. Option B

C. Option C
D. Option D

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

A. To enable Gateway authentication to the Portal
B. To enable Portal authentication to the Gateway
C. To enable user authentication to the Portal
D. To enable client machine authentication to the Portal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
:
The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.
Reference https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/network-globalprotect-portals

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 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 11
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 read-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 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 14
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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 15
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 16
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
:
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 17
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 18
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 19
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 20

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 21
What are two benefits of nested device groups in Panorama? (Choose two.)

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 form the Shared group
D. Overwrites local firewall configuration

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
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 23
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 24
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

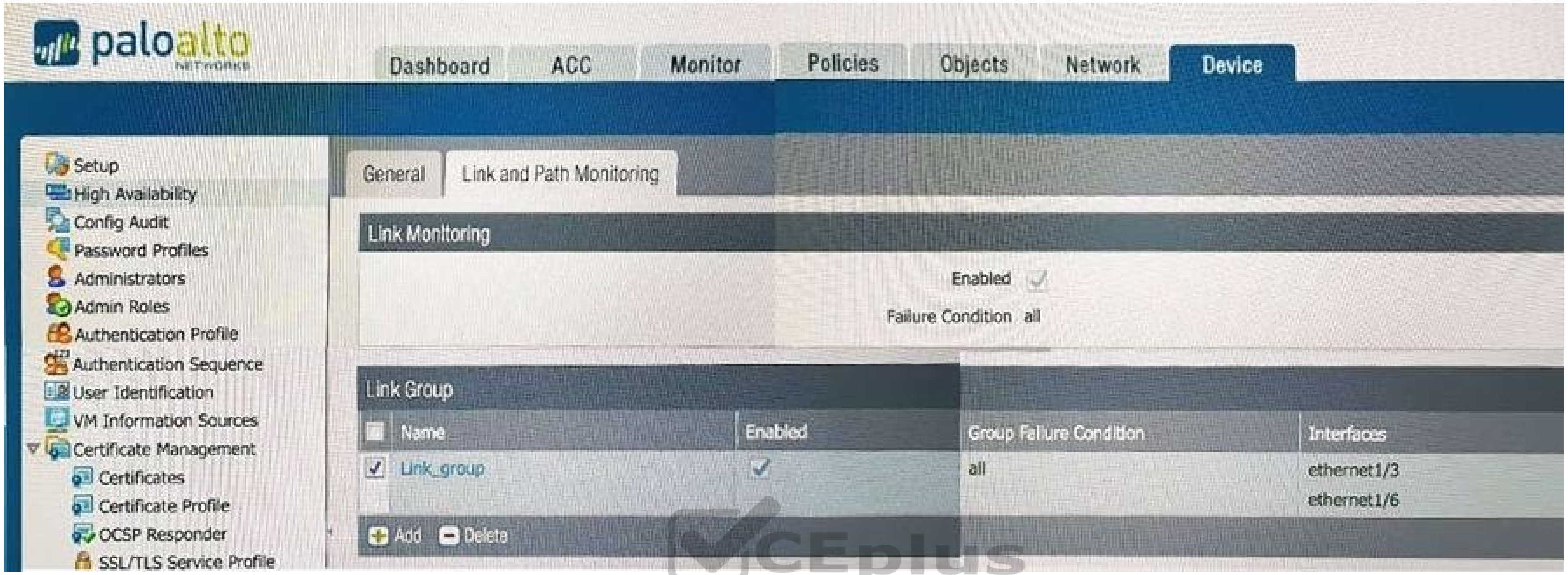
QUESTION 25
A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable we browsing access to the server.
Which application and service 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 26
If the firewall has the link monitoring configuration, what will cause a failover?



Link Monitoring

Enabled ✓

Failure Condition all

Link Group

☐	Name	Enabled	Group Failure Condition	Interfaces
☑	Link_group	✓	all	ethernet1/3 ethernet1/6

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 27
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?

A. Application override

B. Redistribution of user mappings
C. Virtual Wire mode
D. Content inspection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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 29
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 30
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

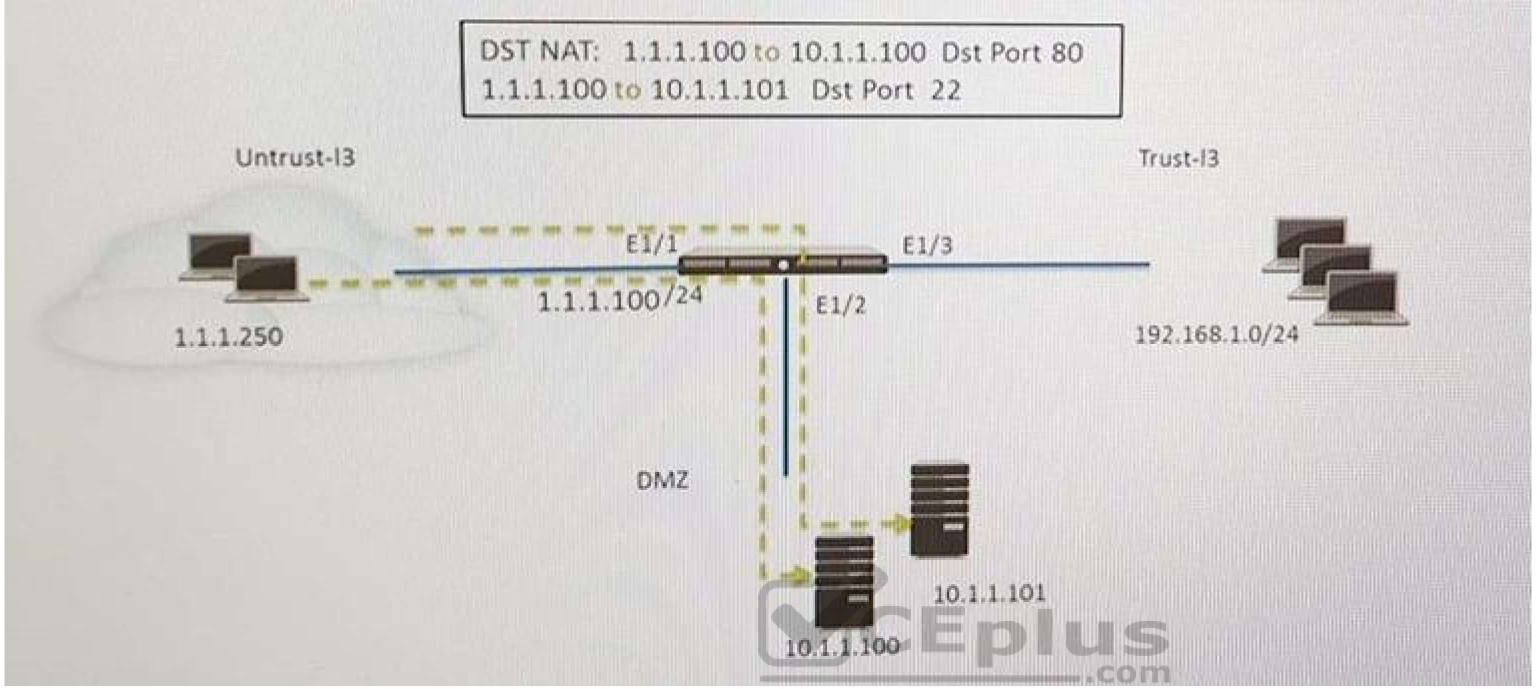
QUESTION 31
A session in the Traffic log is reporting the application as “incomplete.”
What does “incomplete” mean?

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 32
Refer to the exhibit.



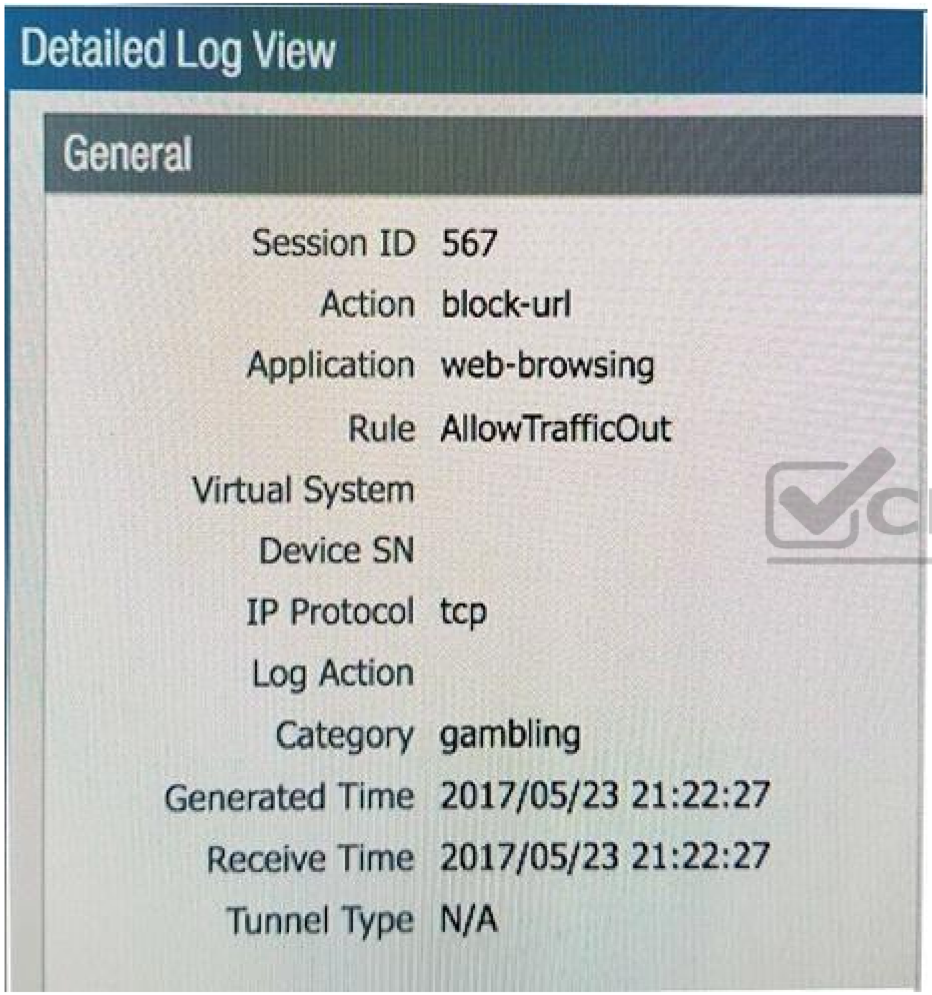
An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.)
Which two security policy rules will accomplish this 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 33
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.

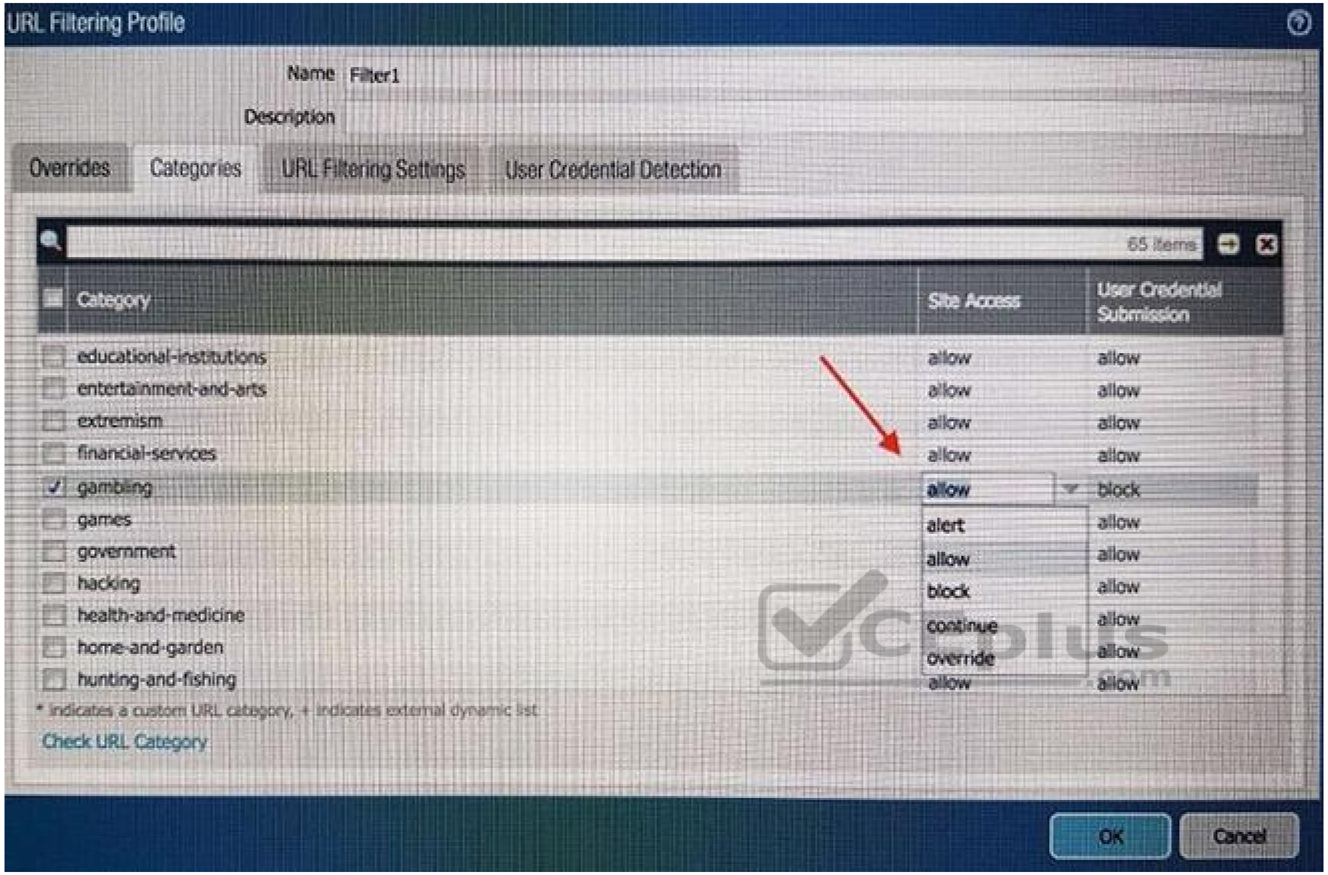


Detailed Log View

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.



Name Filter1

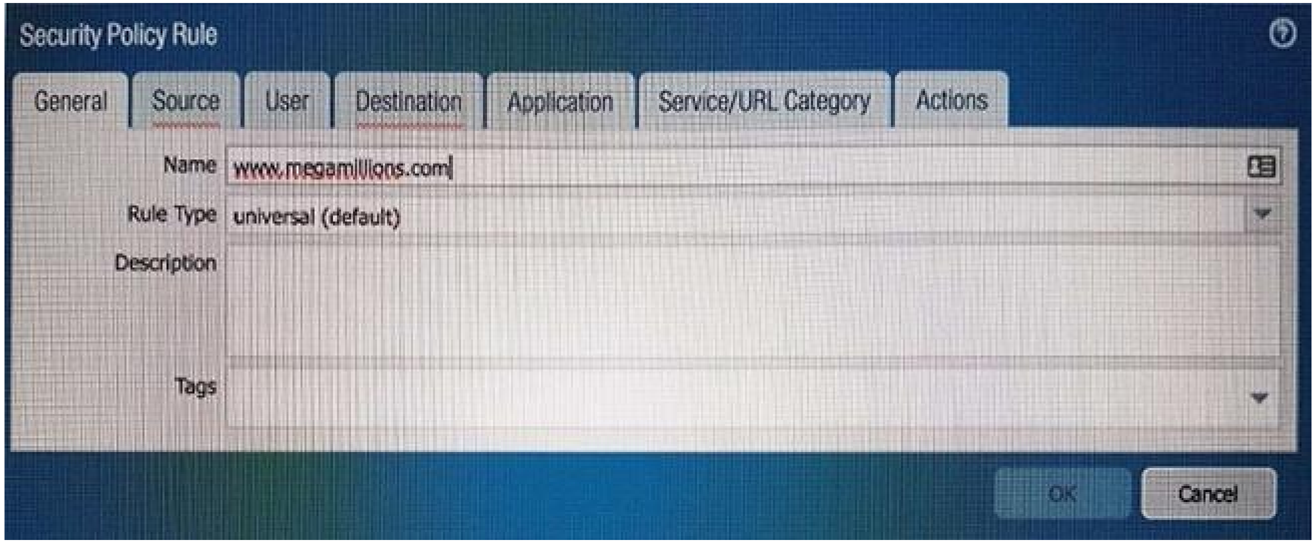
Description

	Category	Site Access	User Credential Submission
□	educational-institutions	allow	allow
□	entertainment-and-arts	allow	allow
□	extremism	allow	allow
□	financial-services	allow	allow
✓	gambling	allow	block
□	games		allow
□	government		allow
□	hacking		allow
□	health-and-medicine		allow
□	home-and-garden		allow
□	hunting-and-fishing	allow	allow

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

Check URL Category

C.



Security Policy Rule

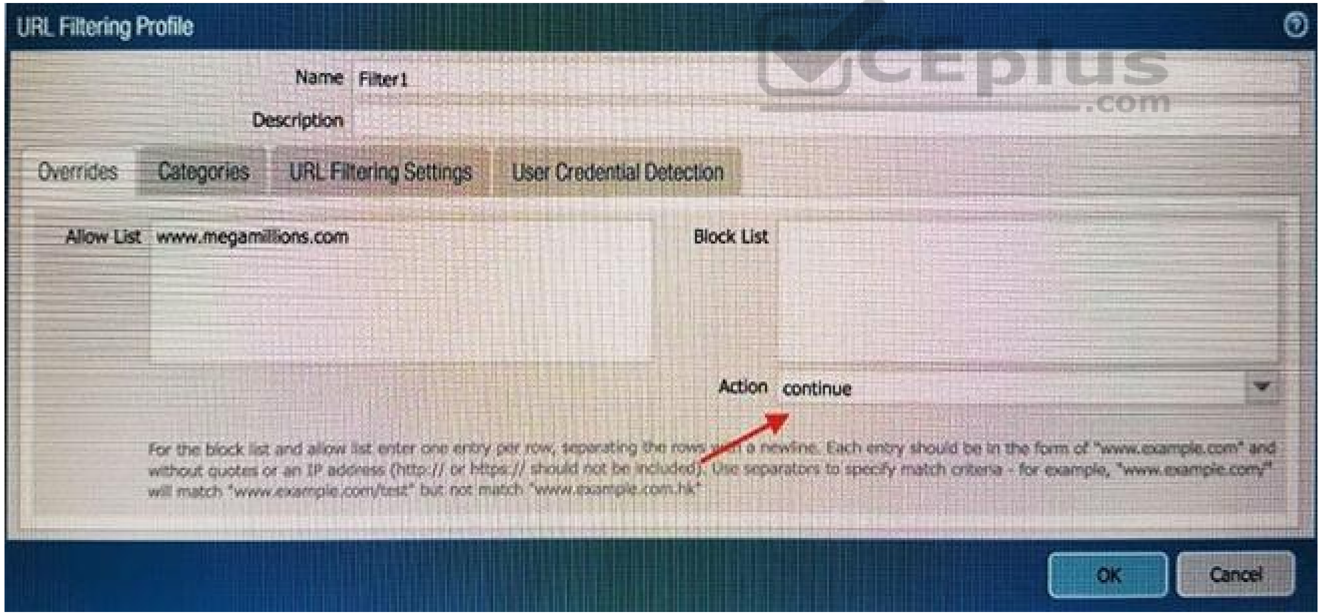
Name www.megamillions.com

Rule Type universal (default)

Description

Tags

D.



URL Filtering Profile

Name Filter1

Description

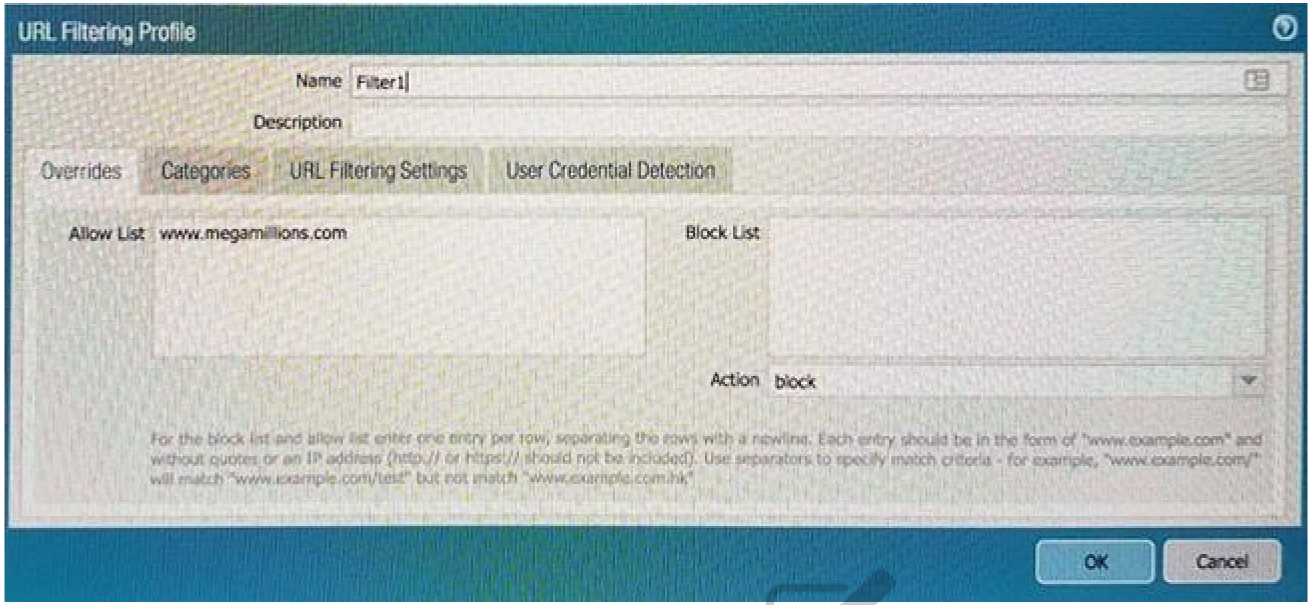
Allow List www.megamillions.com

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"

E.



URL Filtering Profile

Name Filter1

Description

Allow List www.megamillions.com

Block List

Action block

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"

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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 36
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 37
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 38
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 exported form the firewalls and manually imported into Panorama.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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 40
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 41
Which Palo Alto Networks VM-Series firewall is valid?

A. VM-25
B. VM-800

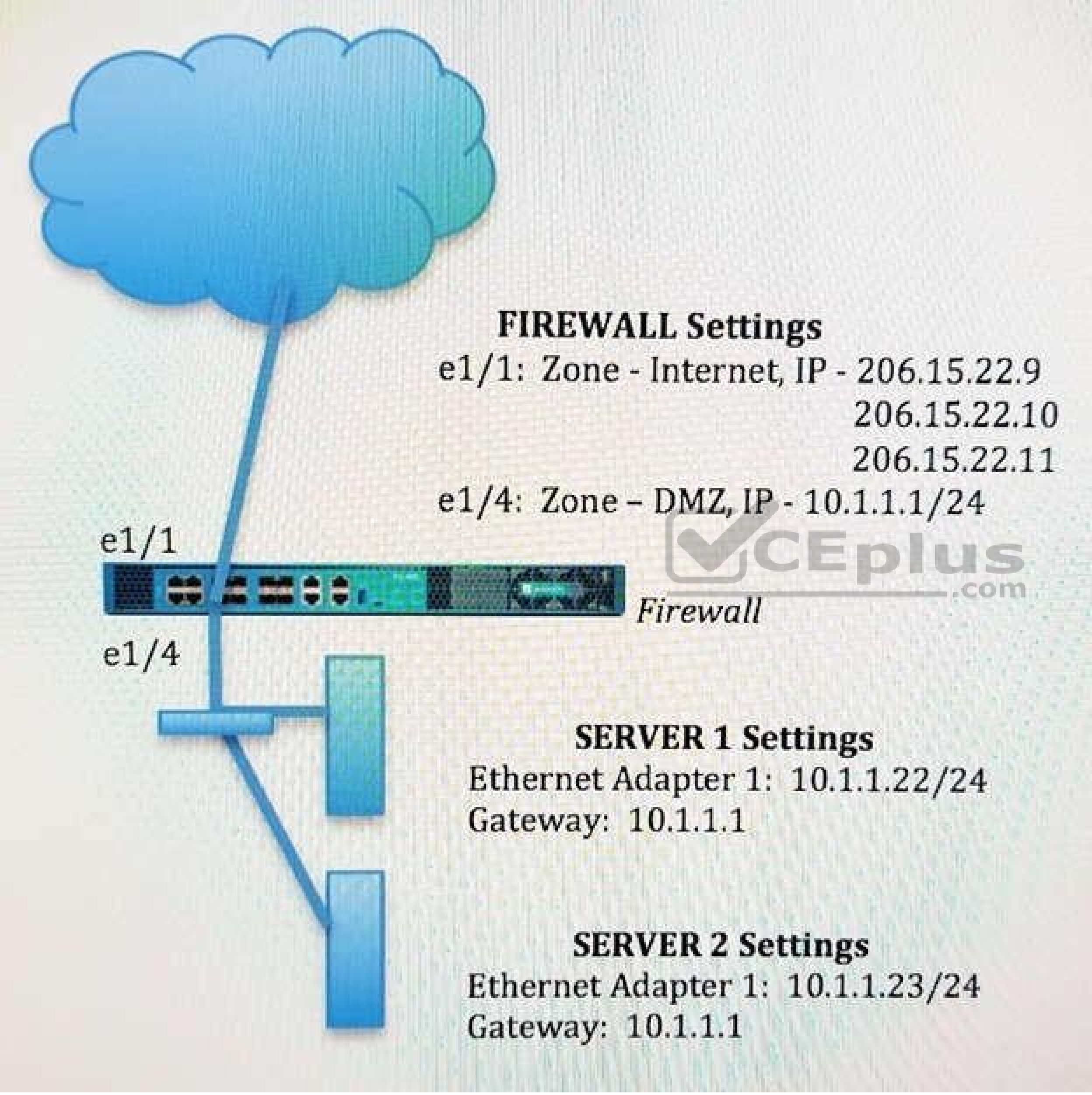
C. VM-50

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 42
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?

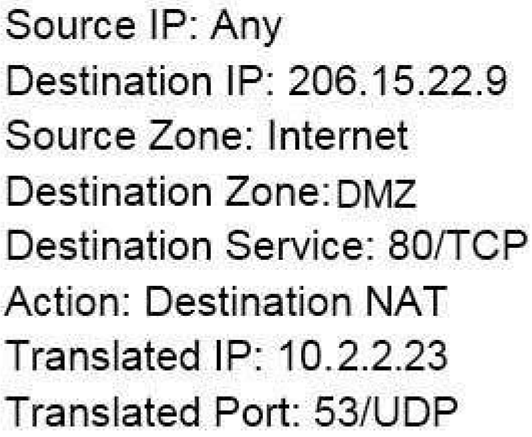


FIREWALL Settings
e1/1: Zone - Internet, IP - 206.15.22.9
206.15.22.10
206.15.22.11
e1/4: Zone – DMZ, IP - 10.1.1.1/24

SERVER 1 Settings
Ethernet Adapter 1: 10.1.1.22/24
Gateway: 10.1.1.1

SERVER 2 Settings
Ethernet Adapter 1: 10.1.1.23/24
Gateway: 10.1.1.1

A.



Source IP: Any

Destination IP: 206.15.22.9

Source Zone: Internet

Destination Zone: DMZ

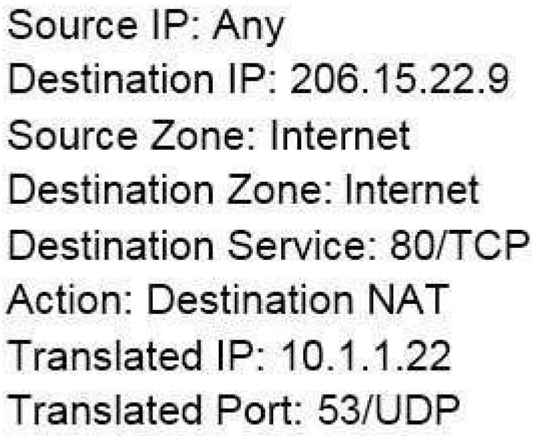
Destination Service: 80/TCP

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

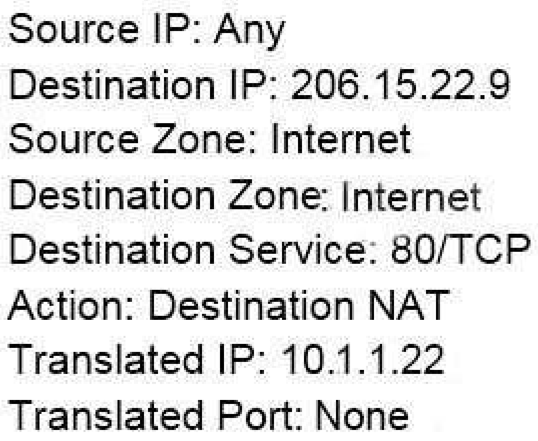
Destination Service: 80/TCP

Action: Destination NAT

Translated IP: 10.1.1.22

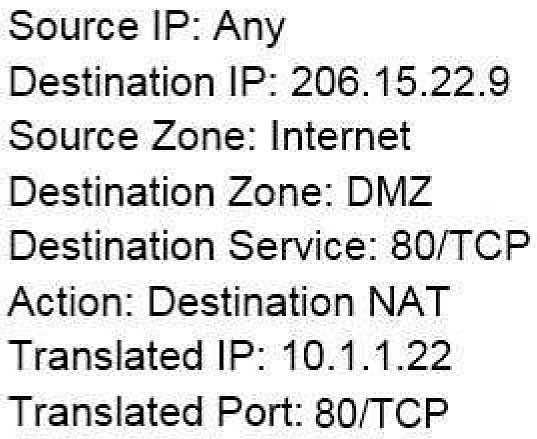
Translated Port: 53/UDP

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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:

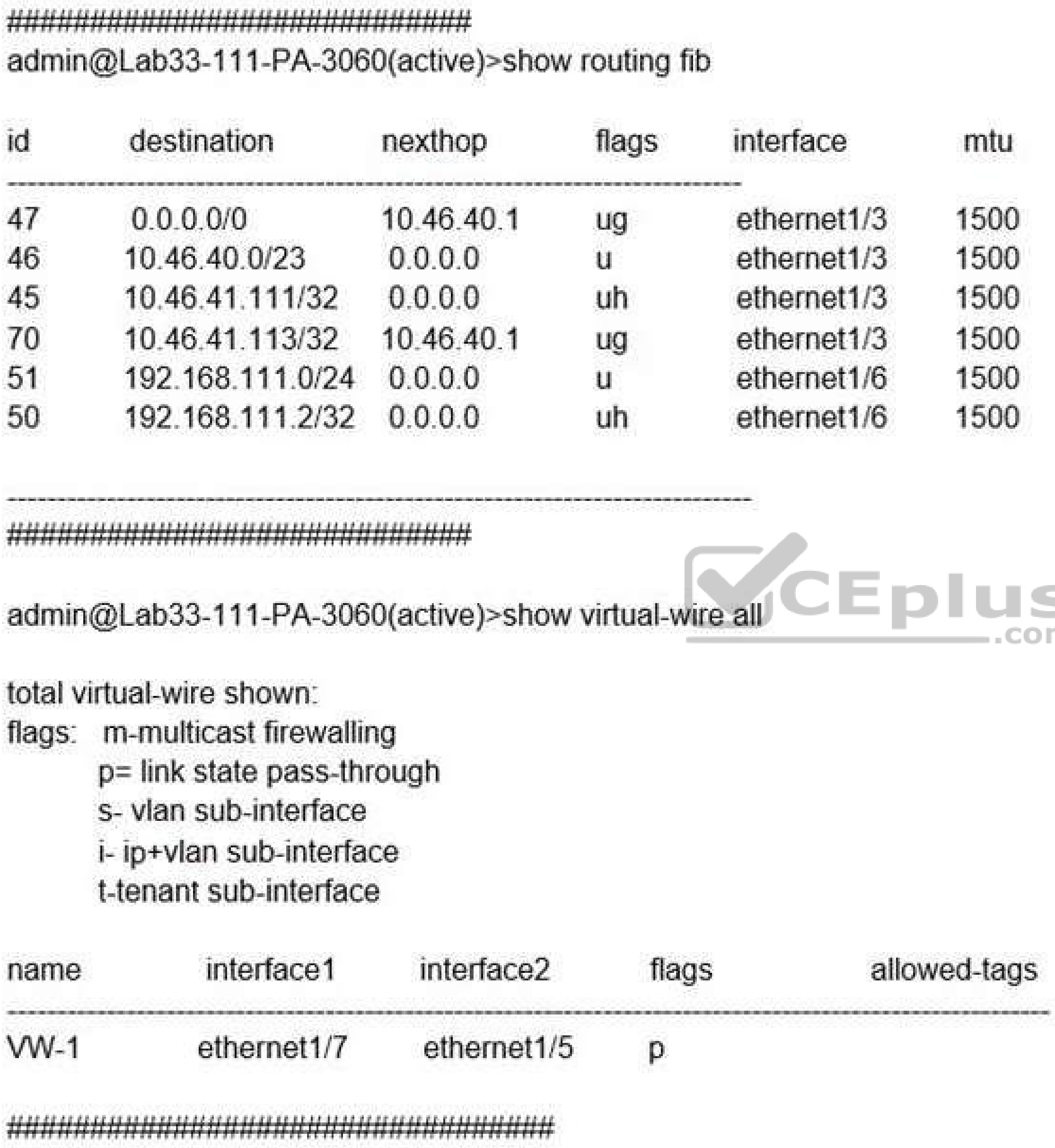
QUESTION 44
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

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 45
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 46
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 47
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-amp-Tricks-How-to-Create-an-Application-Override/ta-p/65513

QUESTION 48
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 49
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 50
If the firewall is configured for credential phishing prevention using the “Domain Credential Filter” method, which login will be detected as credential theft?

A. Mapping to the IP address of the logged-in user.
B. First four letters of the username matching any valid corporate username.
C. Using the same user’s corporate username and password.
D. Marching any valid corporate username.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/credential-phishing-prevention

QUESTION 51
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 52
An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all webbrowsing traffic from any to any zone.

What must the administrator configure so that the PAN-OS® software can be upgraded?

A. Security policy rule
B. CRL
C. Service route
D. Scheduler

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which feature prevents the submission of corporate login information into website forms?

A. Data filtering
B. User-ID
C. File blocking
D. Credential phishing prevention

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-compliance

QUESTION 54
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