# Paloalto-Networks

## Exam Questions PCNSE

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

**NEW QUESTION 1**
SAML SLO is supported for which two firewall features? (Choose two.)

A. GlobalProtect Portal
B. CaptivePortal
C. WebUI
D. CLI

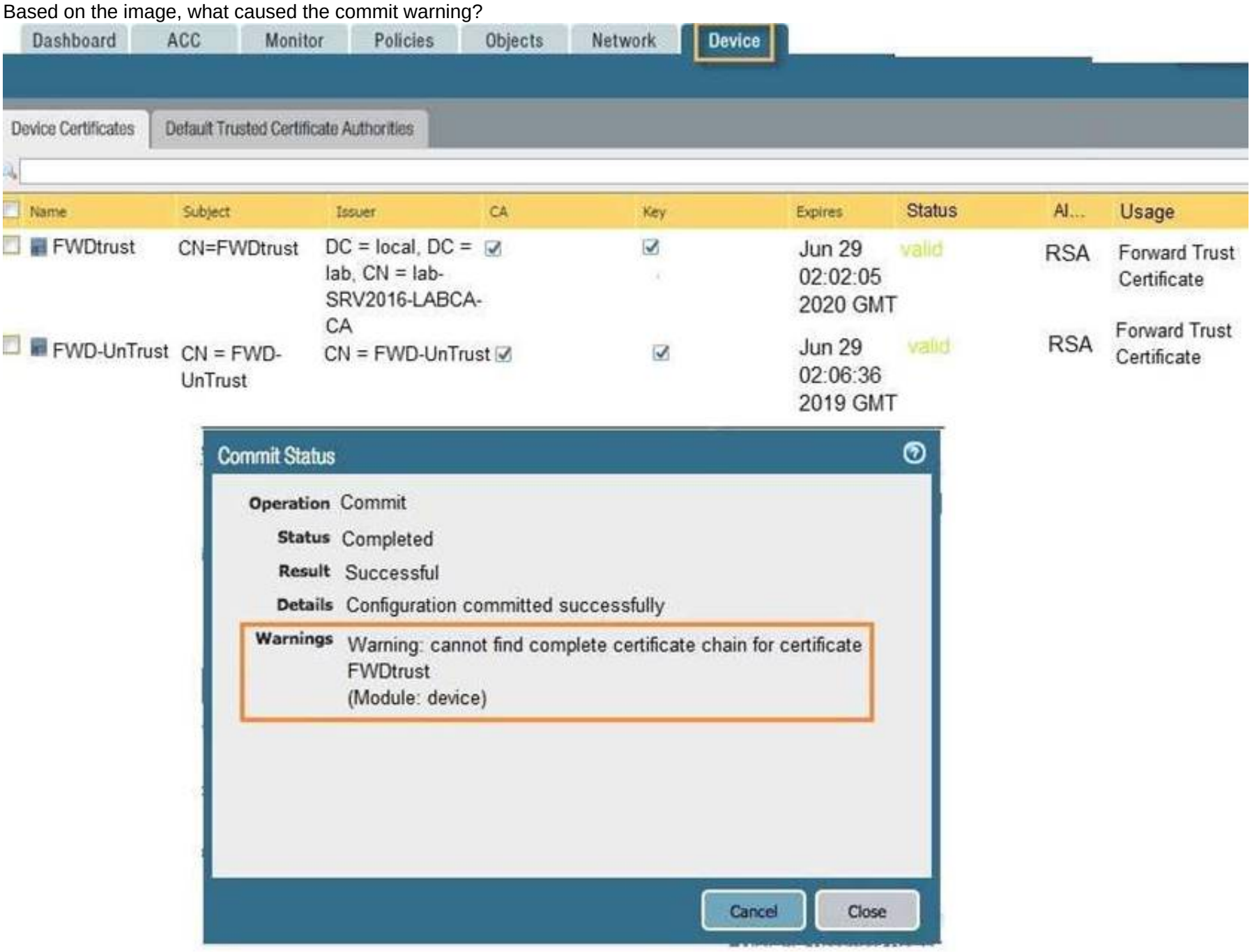
**Answer:** AB

**NEW QUESTION 2**
Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

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

**Answer:** ABC

**NEW QUESTION 3**
Based on 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.

**Answer:** D

**NEW QUESTION 4**
What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

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

D. Rule Usage Hit counter will reset.

**Answer:** AB

**NEW QUESTION 5**
Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 6**
Which administrative authentication method supports authorization by an external service?

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

**Answer:** C

**NEW QUESTION 7**
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.

**Answer:** A

**NEW QUESTION 8**
Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

A. GlobalProtect version 4.0 with PAN-OS 8.1
B. GlobalProtect version 4.1 with PAN-OS 8.1
C. GlobalProtect version 4.1 with PAN-OS 8.0
D. GlobalProtect version 4.0 with PAN-OS 8.0

**Answer:** B

**NEW QUESTION 9**
How does Panorama prompt VMWare NSX to quarantine an infected VM?

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

**Answer:** A

**NEW QUESTION 10**
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. 99
B. 1
C. 255

**Answer:** D

**Explanation:**
Reference:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5.pdf (page 9)

**NEW QUESTION 10**
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

**Answer:** C

**NEW QUESTION 12**
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

**Answer:** C

**Explanation:**
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

**NEW QUESTION 16**
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

**Answer:** D

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

**NEW QUESTION 21**
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

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

**Answer:** A

**NEW QUESTION 24**
To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

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

**Answer:** B

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

**NEW QUESTION 28**
An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

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

**Answer:** A

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

**NEW QUESTION 29**

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

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

**Answer:** BD

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

**NEW QUESTION 32**
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 invali
B. The Profile Settings section will be grayed out when the Action is set to "Deny".
C. The configuration will allow the matched session unless a vulnerability signature is detecte
D. The "Deny" action will supersede theper-severity defined actions defined in the associated Vulnerability Protection Profile.
E. The configuration is invali
F. It will cause the firewall to skip this Security policy rul
G. A warning will be displayed during a commit.
H. The configuration is vali
I. It will cause the firewall to deny the matched session
J. Any configured Security Profiles have no effect ifthe Security policy rule action is set to "Deny."

**Answer:** B

**NEW QUESTION 33**
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.

**Answer:** C

**NEW QUESTION 35**
Which Captive Portal mode must be configured to support MFA authentication?

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

**Answer:** B

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

**NEW QUESTION 40**
A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

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

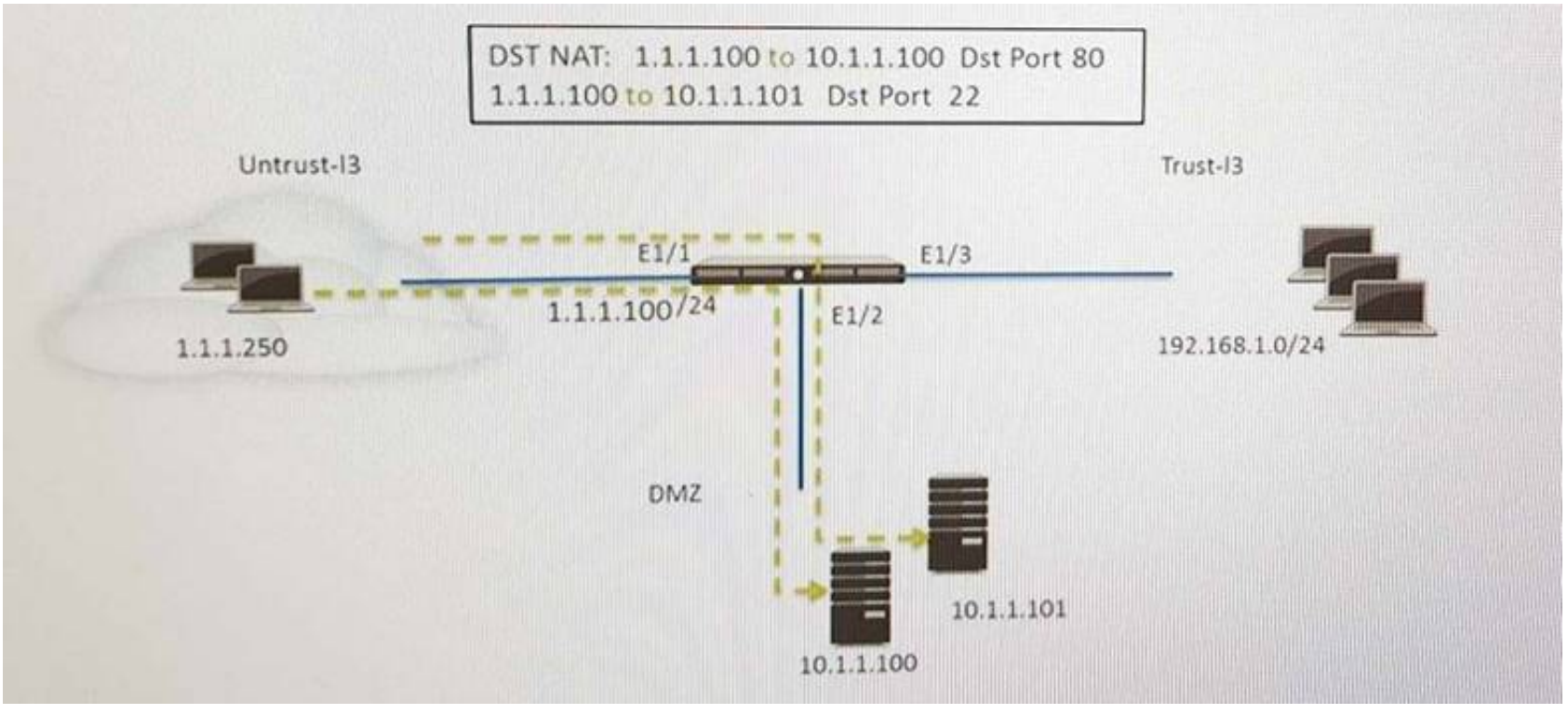
**Answer:** B

**NEW QUESTION 44**
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

**Answer:** C

**NEW QUESTION 45**
Refer to the exhibit.

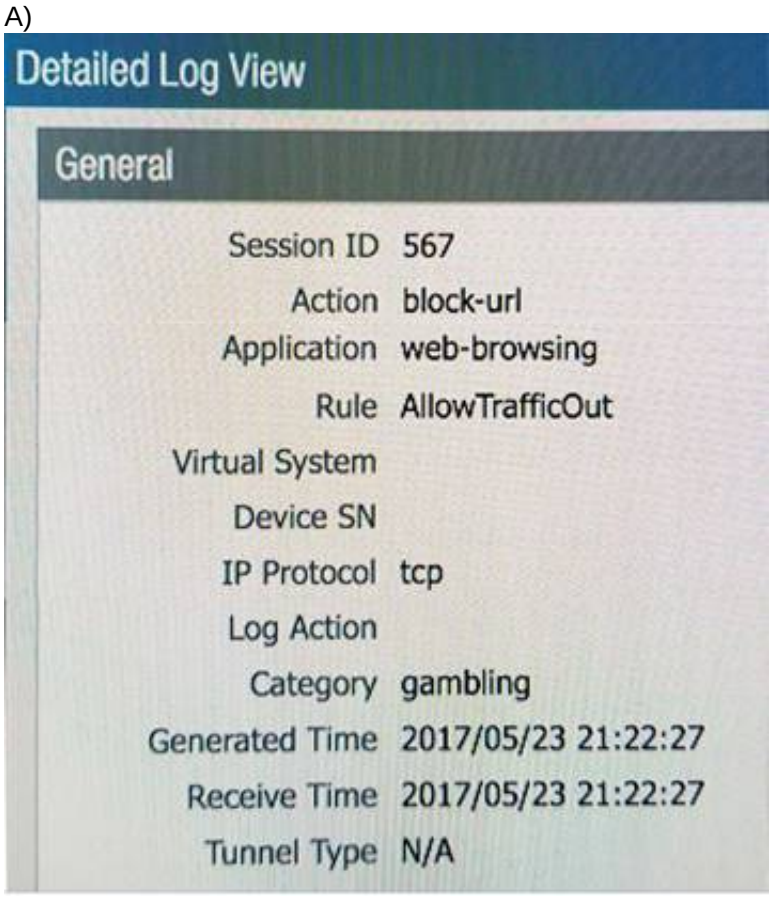



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.)
Which two security policy rules will accomplish this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

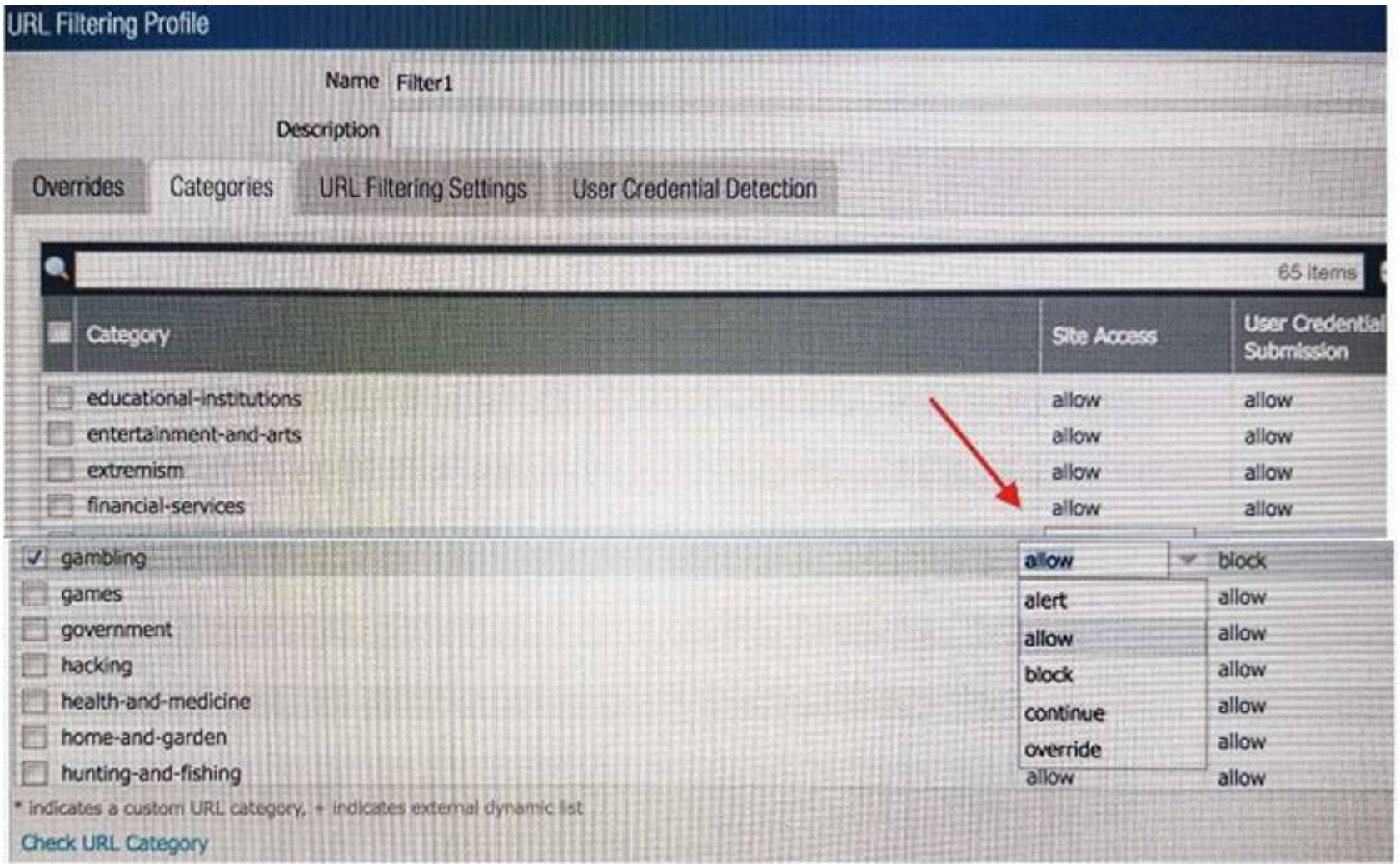
A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
D. Untrust (Any) to DMZ (10.1.1.1), ssh –Allow
E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

**Answer:** CD

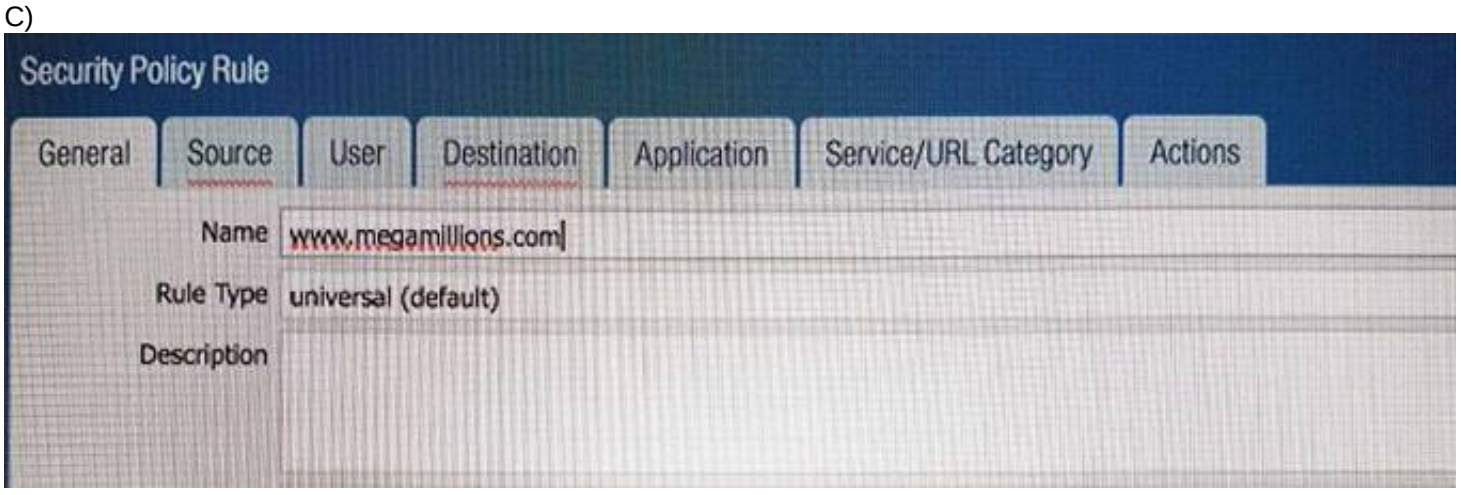
**NEW QUESTION 49**
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.
Which configuration change should the administrator make?
A)



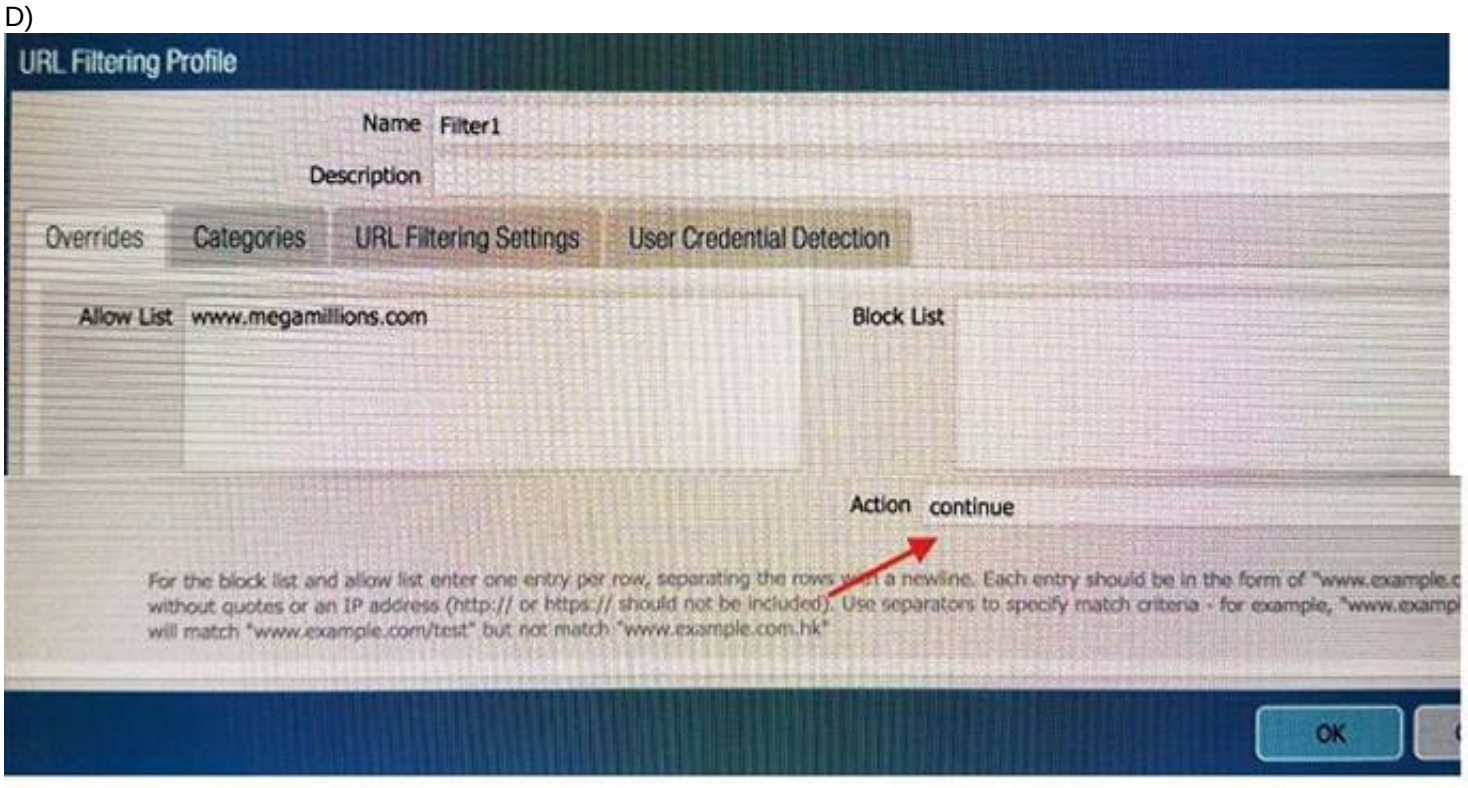

B)


URL Filtering Profile
Name Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
65 items
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial-services
gambling
games
government
hacking
health-and-medicine
home-and-garden
hunting-and-fishing
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category

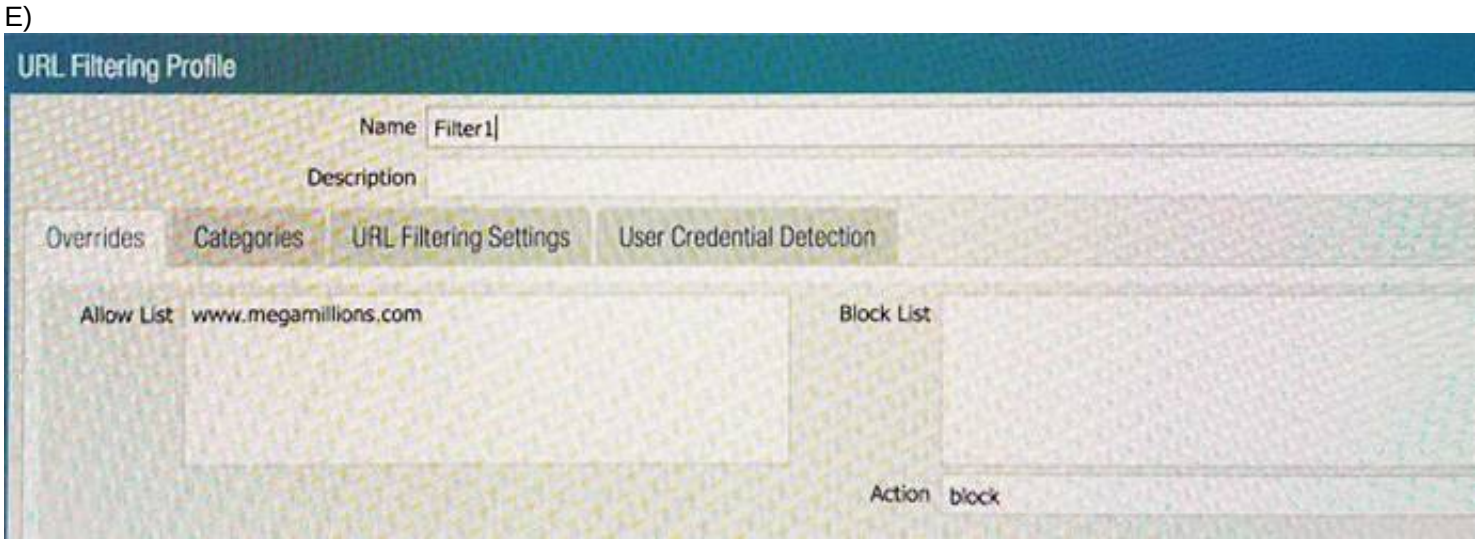
C)


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Name www.megamillions.com
Rule Type universal (default)
Description

D)


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.c
without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.exampl
will match "www.example.com/test" but not match "www.example.com.hk"
OK

E)


URL Filtering Profile
Name Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
Allow List www.megamillions.com
Block List
Action block

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

**Answer:** B

**NEW QUESTION 52**
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

**Answer:** A

**NEW QUESTION 53**
Which Palo Alto Networks VM-Series firewall is valid?

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

**Answer:** C

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

**NEW QUESTION 54**
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?

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

**Answer:** A

**NEW QUESTION 57**
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

**Answer:** DEF

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

**NEW QUESTION 59**
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

**Answer:** DEF

**NEW QUESTION 62**
Which event will happen if an administrator uses an Application Override Policy?

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override/ta-p/65513

**NEW QUESTION 66**
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

**Answer:** A

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

**NEW QUESTION 71**
If the firewall is configured for credential phishing prevention using the “Domain Credential Filter” method, which login will be detected as credential theft?

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 72**
An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

**Answer:** B

**NEW QUESTION 77**
Which protection feature is available only in a Zone Protection Profile?

A. SYN Flood Protection using SYN Flood Cookies
B. ICMP Flood Protection
C. Port Scan Protection
D. UDP Flood Protections

**Answer:** A

**NEW QUESTION 81**
Which CLI command can be used to export the tcpdump capture?

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 86**
During the packet flow process, which two processes are performed in application identification? (Choose two.)

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

**Answer:** BD

**NEW QUESTION 90**
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?

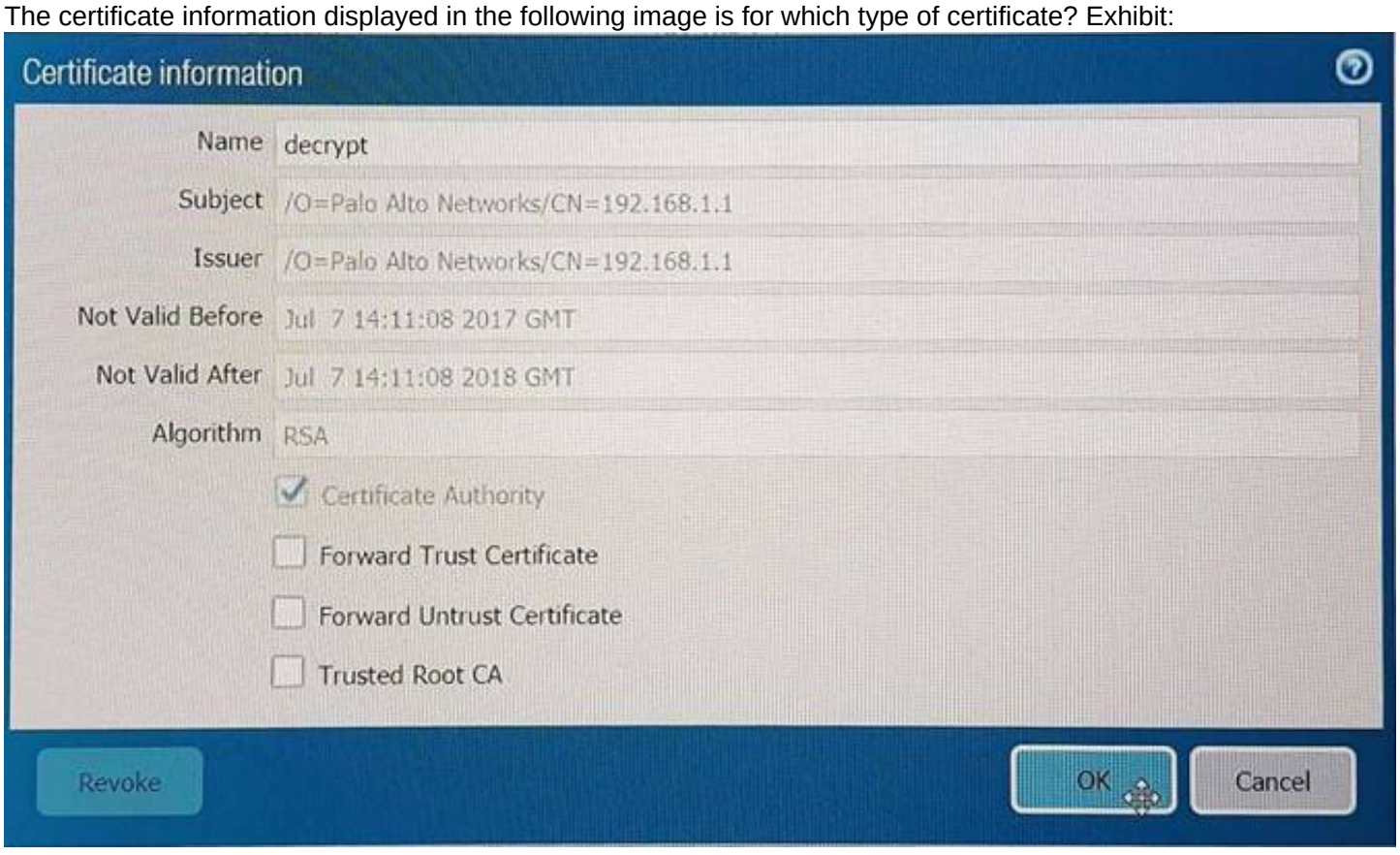
A. Session Browser

B. Application Command Center
C. TCP Dump
D. Packet Capture

**Answer:** B

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

**NEW QUESTION 94**
The certificate information displayed in the following image is for which type of certificate? Exhibit:




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

**Answer:** D

**NEW QUESTION 96**
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

**Answer:** A

**NEW QUESTION 101**
The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router. Which two options would help the administrator troubleshoot this issue? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 102**
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.

**Answer:** AB

**NEW QUESTION 103**

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

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

**Answer:** C

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf

**NEW QUESTION 105**
An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.
Which interface type and license feature are necessary to meet the requirement?

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

**Answer:** D

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring

**NEW QUESTION 106**
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

**Answer:** A

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

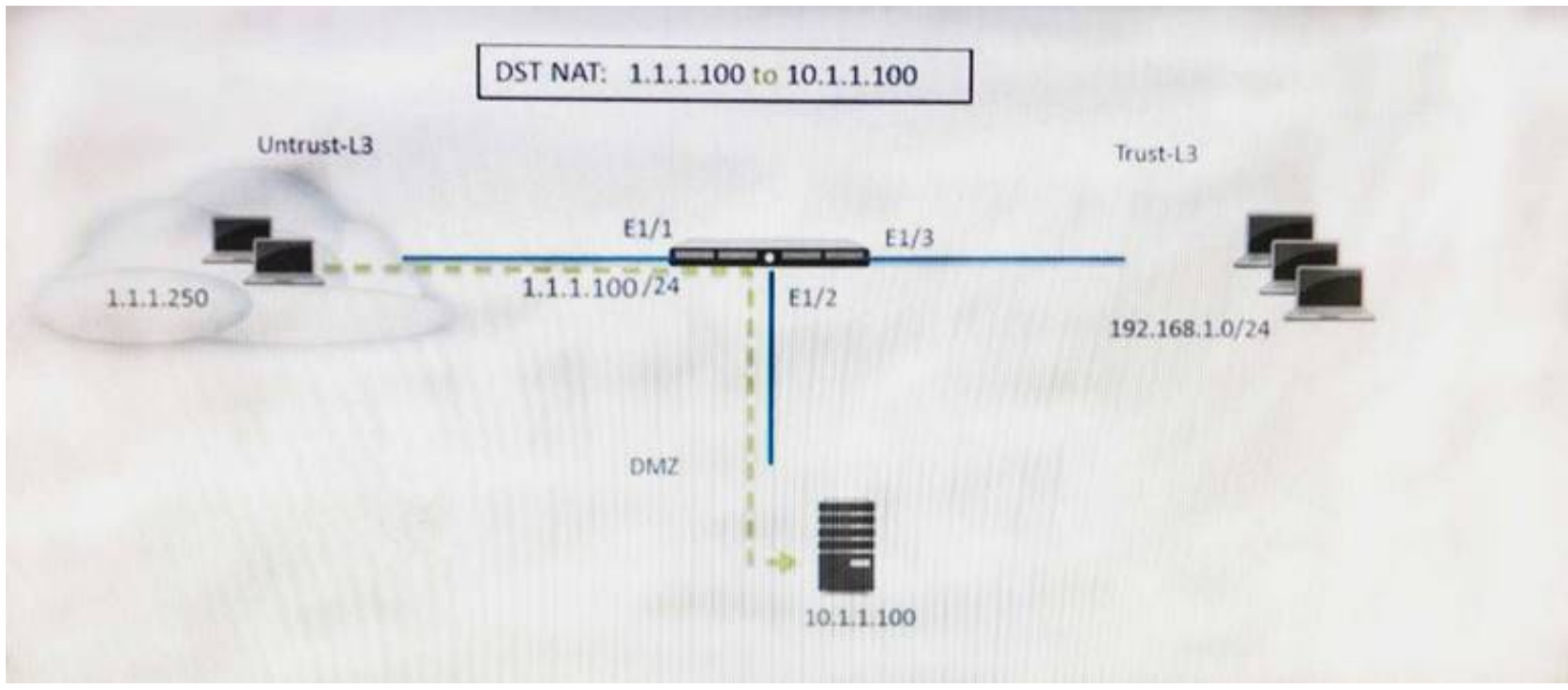
**NEW QUESTION 108**
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system. Which Security Profile type will prevent this attack?

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

**Answer:** A

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection

**NEW QUESTION 111**
Refer to the exhibit.




A web server in the DMZ is being mapped to a public address through DNAT. Which Security policy rule will allow traffic to flow to the web server?

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

**Answer:** B

**NEW QUESTION 113**
Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

A. The firewall is in multi-vsys mode.
B. The traffic is offloaded.
C. The traffic does not match the packet capture filter.
D. The firewall's DP CPU is higher than 50%.

**Answer:** BC

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload

**NEW QUESTION 116**
Which feature can be configured on VM-Series firewalls?

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

**Answer:** D

**NEW QUESTION 118**
If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 122**
View the GlobalProtect configuration screen capture.


What is the purpose of this configuration?

A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

**Answer:** C

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations

**NEW QUESTION 126**
What is exchanged through the HA2 link?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 127**
Which three authentication factors does PAN-OS® software support for MFA (Choose three.)

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

**Answer:** ADE

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

**NEW QUESTION 130**
An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.
What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 131**
A company wants to install a PA-3060 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 options differentiates multiple VLAN into separate zones?

A. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN I
B. Repeat forevery additional VLANand use a VLAN ID of 0 for untagged traffi
C. Assign each interface/subinterface to a unique zone.
D. Create V-Wire objects with two V-Wire sub interface and assign only a single VLAN ID to the "Tag Allowed field one of the V-Wire object Repeat for every additional VLAN and use a VIAN ID of 0 for untagged traffi
E. Assign each interface/subinterfaceto a unique zone.
F. Create V-Wire objects with two V-Wire interfaces and define a range “0- 4096" in the 'Tag Allowed filed of the V-Wire object.
G. Create Layer 3 sub interfaces that are each assigned to a single VLAN ID and a common virtual route
H. The physical Layer 3interface would handle untagged traffi
I. Assign each interface /subinterface to a unique zon
J. Do not assign any interface anIP address

**Answer:** C

**NEW QUESTION 132**
Which logs enable a firewall administrator to determine whether a session was decrypted?

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

**Answer:** B

**NEW QUESTION 135**
Which data flow describes redistribution of user mappings?

A. User-ID agent to firewall
B. firewall to firewall
C. Domain Controller to User-ID agent
D. User-ID agent to Panorama

**Answer:** B

**NEW QUESTION 137**
Which two features does PAN-OS® software use to identify applications? (Choose two)

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

**Answer:**

CD

**NEW QUESTION 140**
Which log file can be used to identify SSL decryption failures?

A. Configuration
B. Threats
C. ACC
D. Traffic

**Answer:** C

**NEW QUESTION 143**
Which three firewall states are valid? (Choose three)

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

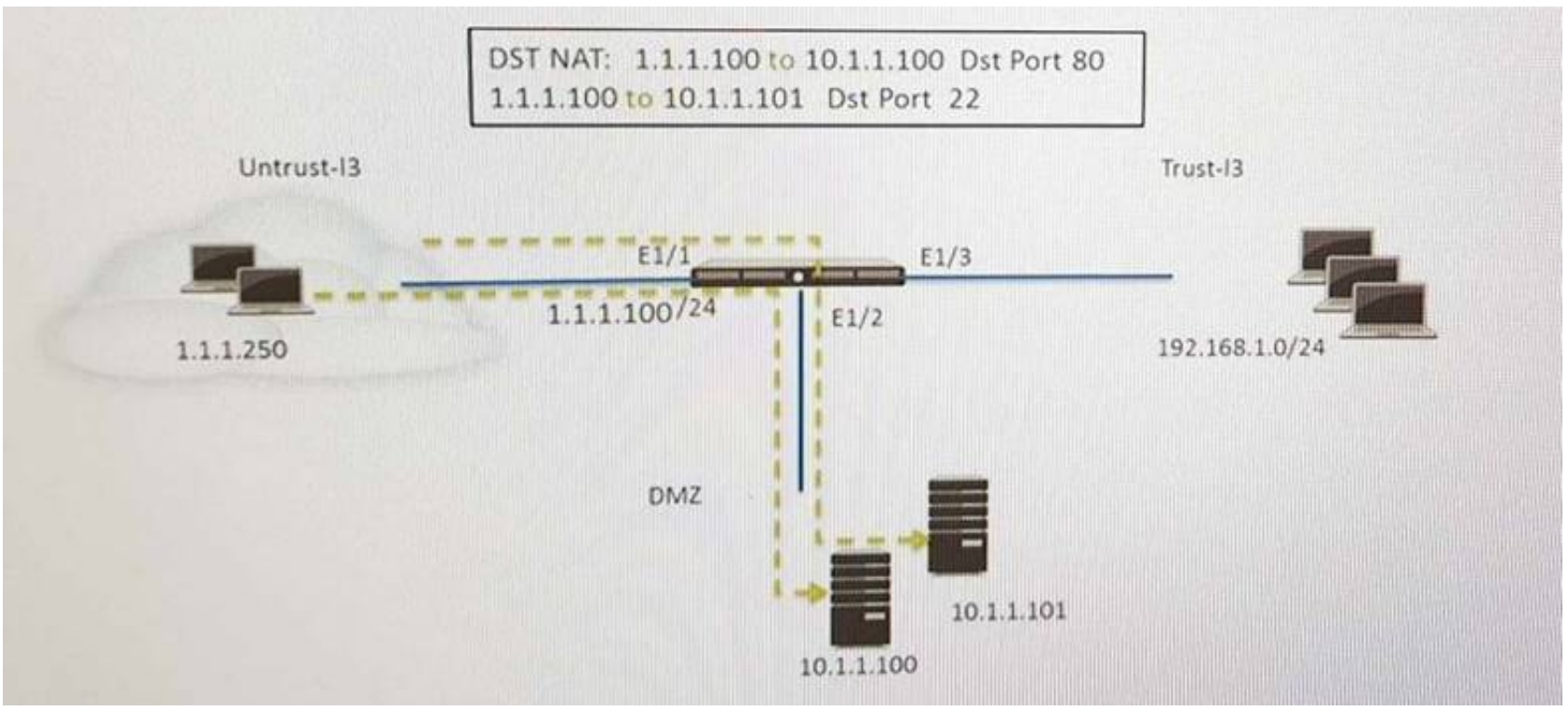
**Answer:** ABC

**NEW QUESTION 144**
An administrator wants to upgrade an NGFW from PAN-OS® 7 .1. 2 to PAN-OS® 8 .0.2 The firewall is not a part of an HA pair. What needs to be updated first?

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

**Answer:** B

**NEW QUESTION 149**
Refer to the exhibit.




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

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

**Answer:** CD

**NEW QUESTION 154**
Which is the maximum number of samples that can be submitted to WildFire per day, based on wildfire subscription?

A. 15,000
B. 10,000
C. 75,00
D. 5,000

**Answer:** B

**NEW QUESTION 156**
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 Data Filtering Profile
B. Enable QoS monitor
C. Enable Qos interface
D. Enable Qos in the interface Management Profile.

**Answer:** C

**NEW QUESTION 161**
When configuring the firewall for packet capture, what are the valid stage types?

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

**Answer:** D

**NEW QUESTION 163**
What are the differences between using a service versus using an application for Security Policy match?

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

**Answer:** B

**NEW QUESTION 168**
In which two types of deployment is active/active HA configuration supported? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 173**
A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial of-service attacks.
How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

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

**Answer:** C

**NEW QUESTION 178**
Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

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

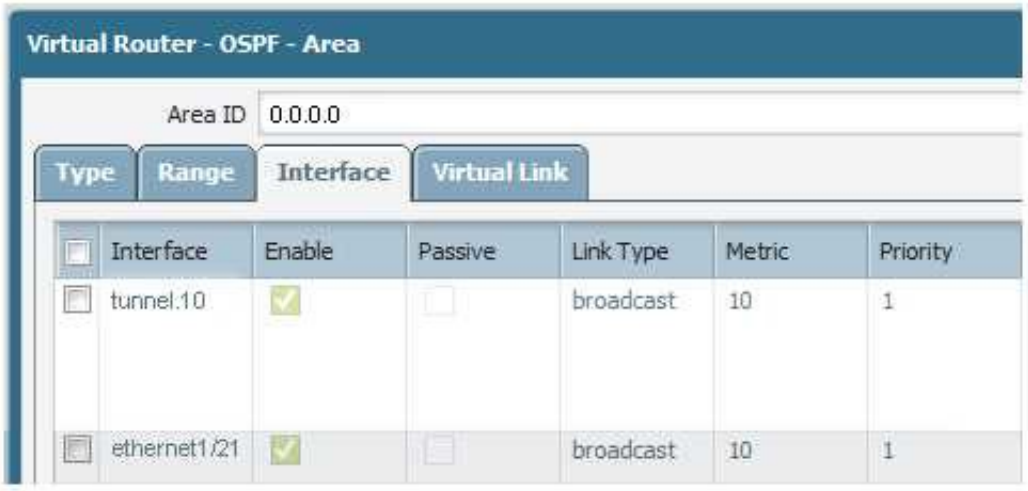
**Answer:** DE

**NEW QUESTION 181**
Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.

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

**Answer:** B

**NEW QUESTION 186**
Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunner is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.

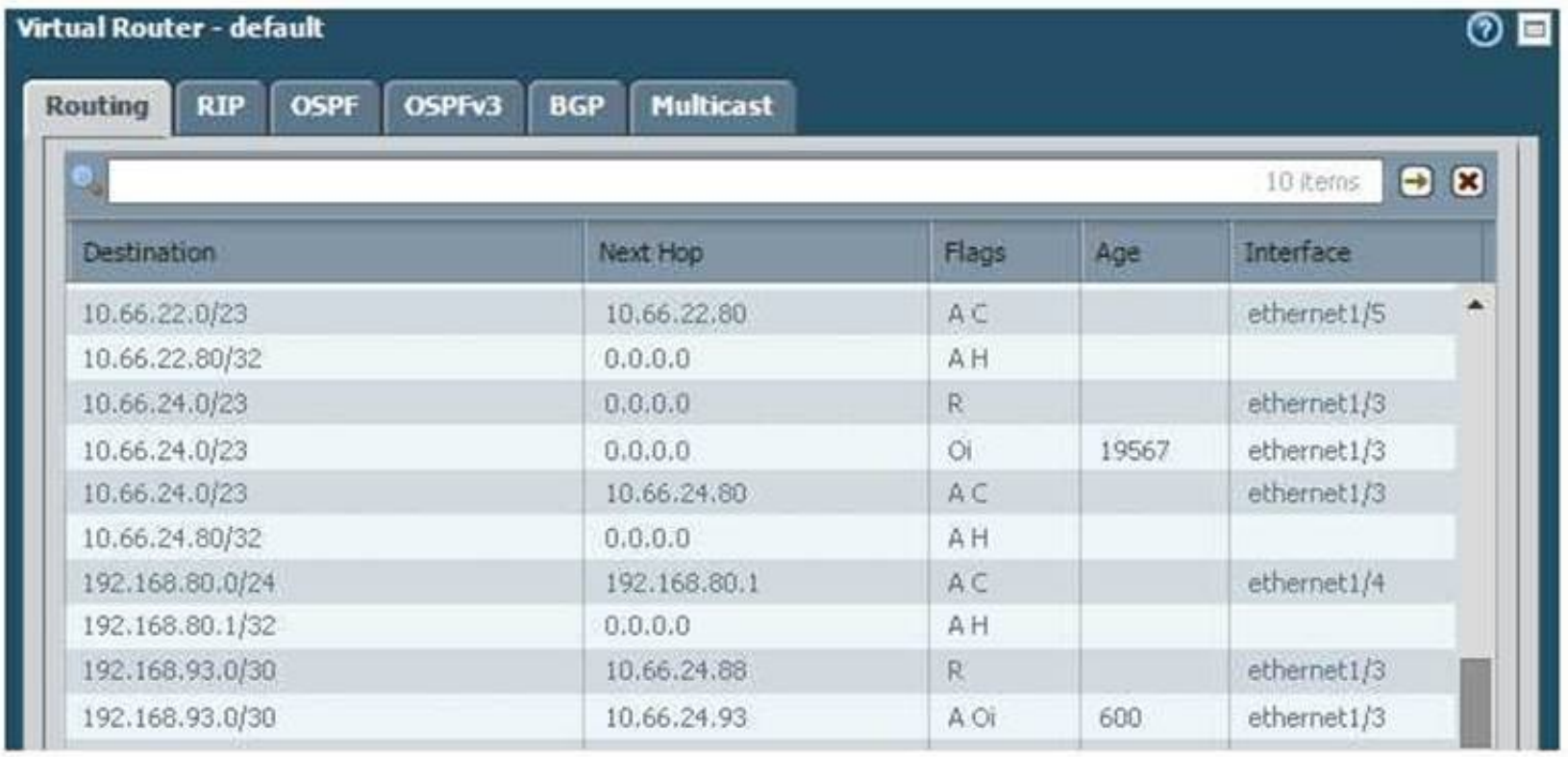



Which Link Type setting will correct the error?

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

**Answer:** A

**NEW QUESTION 187**
Given the following table.




Which configuration change on the firewall would cause it to use 10.66.24.88 as the next hop for the 192.168.93.0/30 network?

A. Configuring the administrative Distance for RIP to be lower than that of OSPF Int.
B. Configuring the metric for RIP to be higher than that of OSPF Int.
C. Configuring the administrative Distance for RIP to be higher than that of OSPF Ext.
D. Configuring the metric for RIP to be lower than that OSPF Ext.

**Answer:** A

**NEW QUESTION 189**
A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk.
What action will bring the VPN up and allow traffic to start passing between the sites?

A. Change the Site-B IKE Gateway profile version to match Site-A,
B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.
C. Enable NAT Traversal on the Site-A IKE Gateway profile.
D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A

**Answer:** D

**NEW QUESTION 194**
A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.
Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?( Choose three)

A. Download PAN-OS 8.0.4 files from the support site and install them on each firewall after manually uploading.
B. Download PAN-OS 8.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.
C. Push the PAN-OS 8.0.4 updates from the support site to install on each firewall.
D. Push the PAN-OS 8.0.4 update from one firewall to all of the other remaining after updating one firewall.
E. Download and install PAN-OS 8.0.4 directly on each firewall.
F. Download and push PAN-OS 8.0.4 from Panorama to each firewall.

**Answer:** ACF

**NEW QUESTION 198**
A network engineer has revived a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.
Which CLI command will help identify the issue?

A. test routing fib virtual-router vr1
B. show routing route type static destination 98.139.183.24
C. test routing fib-lookup ip 98.139.183.24 virtual-router vr1
D. show routing interface

**Answer:** C

**NEW QUESTION 200**
A network Administrator needs to view the default action for a specific spyware signature. The administrator follows the tabs and menus through Objects> Security Profiles> Anti-Spyware and select default profile.
What should be done next?

A. Click the simple-critical rule and then click the Action drop-down list.
B. Click the Exceptions tab and then click show all signatures.
C. View the default actions displayed in the Action column.
D. Click the Rules tab and then look for rules with "default" in the Action column.

**Answer:** B

**NEW QUESTION 203**
Which two mechanisms help prevent a spilt brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

A. Configure the management interface as HA3 Backup
B. Configure Ethernet 1/1 as HA1 Backup
C. Configure Ethernet 1/1 as HA2 Backup
D. Configure the management interface as HA2 Backup
E. Configure the management interface as HA1 Backup
F. Configure ethernet1/1 as HA3 Backup

**Answer:** BE

**NEW QUESTION 204**
How is the Forward Untrust Certificate used?

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

**Answer:** C

**NEW QUESTION 205**
Which command can be used to validate a Captive Portal policy?

A. eval captive-portal policy <criteria>
B. request cp-policy-eval <criteria>
C. test cp-policy-match <criteria>
D. debug cp-policy <criteria>

**Answer:** C

**NEW QUESTION 206**
Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

A. Set the type to Aggregate, clear the session’s box and set the Maximum concurrent Sessions to 4000.
B. Set the type to Classified, clear the session’s box and set the Maximum concurrent Sessions to 4000.
C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.
D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000.

**Answer:** C

**NEW QUESTION 211**

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

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

**Answer:** ABF

**NEW QUESTION 215**
A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled.
Which component once enabled on a perirneter firewall will allow the identification of existing infected hosts in an environment?

A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
B. File Blocking profiles applied to outbound security policies with action set to alert
C. Vulnerability Protection profiles applied to outbound security policies with action set to block
D. Antivirus profiles applied to outbound security policies with action set to alert

**Answer:** A

**NEW QUESTION 220**
Which three options are available when creating a security profile? (Choose three)

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

**Answer:** ABF

**NEW QUESTION 224**
Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

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

**Answer:** BD

**NEW QUESTION 229**
A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and post.
Which option when enabled with the correction threshold would mitigate this attack without dropping legitirnate traffic to other hosts insides the network?

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

**Answer:** D

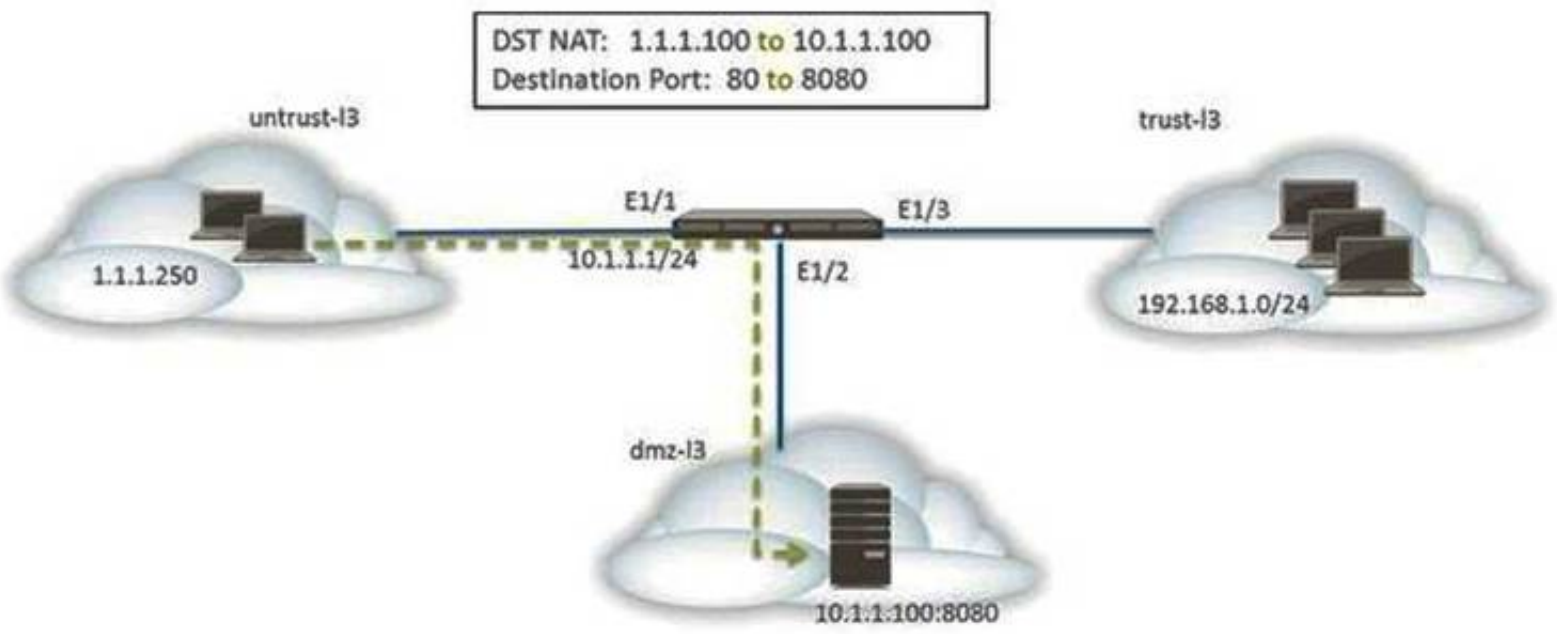
**NEW QUESTION 232**
Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

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

**Answer:** BE

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

**NEW QUESTION 237**
The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and report to 10.1.1.100 on TCP Port 8080.




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

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

**Answer:** BD

**NEW QUESTION 238**
Palo Alto Networks maintains a dynamic database of malicious domains.
Which two Security Platform components use this database to prevent threats? (Choose two)

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

**Answer:** CD

**NEW QUESTION 241**
A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall
Which part of files needs to be imported back into the replacement firewall that is using Panorama?

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

**Answer:** A

**NEW QUESTION 245**
A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.
Given the following zone information:
• DMZ zone: DMZ-L3
• Public zone: Untrust-L3
• Guest zone: Guest-L3
• Web server zone: Trust-L3
• Public IP address (Untrust-L3): 1.1.1.1
• Private IP address (Trust-L3): 192.168.1.50
What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

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

**Answer:** A

**NEW QUESTION 247**
Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.
Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

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

D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

**Answer:** D

**NEW QUESTION 252**
A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.
What could cause this condition?

A. The firewall does not have an active WildFire subscription.
B. The engineer's account does not have permission to view WildFire Submissions.
C. A policy is blocking WildFire Submission traffic.
D. Though WildFire is working, there are currently no WildFire Submissions log entries.

**Answer:** B

**NEW QUESTION 255**
A network administrator uses Panorama to push security polices to managed firewalls at branch offices. Which policy type should be configured on Panorama if the administrators at the branch office sites to override these products?

A. Pre Rules
B. Post Rules
C. Explicit Rules
D. Implicit Rules

**Answer:** A

**NEW QUESTION 256**
What are three valid method of user mapping? (Choose three)

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

**Answer:** ABE

**NEW QUESTION 261**
What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

A. Clean
B. Bengin
C. Adware
D. Suspicious
E. Grayware
F. Malware

**Answer:** BEF

**Explanation:**
https://www.paloaltonetworks.com/documentation/70/pan-HYPERLINK "https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict"os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict

**NEW QUESTION 262**
How are IPV6 DNS queries configured to user interface ethernet1/3?

A. Network > Virtual Router > DNS Interface
B. Objects > CustomerObjects > DNS
C. Network > Interface Mgrnt
D. Device > Setup > Services > Service Route Configuration

**Answer:** D

**NEW QUESTION 264**
A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

A. From the CLI, issue the show counter global filter pcap yes command.
B. From the CLI, issue the show counter global filter packet-filter yes command.
C. From the GUI, select show global counters under the monitor tab.
D. From the CLI, issue the show counter interface command for the ingress interface.

**Answer:** B

**NEW QUESTION 265**

A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

A. DHCP has been set to Auto.
B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.
C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.
D. DNS has not been properly configured on the firewall

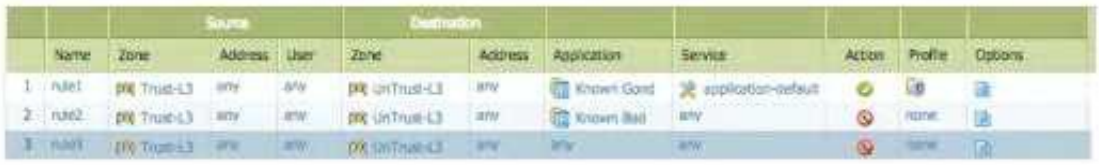
**Answer:** B

**NEW QUESTION 267**
Which interface configuration will accept specific VLAN IDs?

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

**Answer:** B

**NEW QUESTION 271**
A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's
firewall.




Which interface configuration will accept specific VLAN IDs?
Which two benefits are gained from having both rule 2 and rule 3 presents? (choose two)

A. A report can be created that identifies unclassified traffic on the network.
B. Different security profiles can be applied to traffic matching rules 2 and 3.
C. Rule 2 and 3 apply to traffic on different ports.
D. Separate Log Forwarding profiles can be applied to rules 2 and 3.

**Answer:** BD

**NEW QUESTION 276**
Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?

A. VM-100
B. VM-200
C. VM-1000-HV
D. VM-300

**Answer:** C

**NEW QUESTION 279**
After pushing a security policy from Panorama to a PA-3020 firwall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

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

**Answer:** D

**NEW QUESTION 281**
A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations.
How should this be accomplished?

A. Create a Template with the appropriate IKE Gateway settings
B. Create a Template with the appropriate IPSec tunnel settings
C. Create a Device Group with the appropriate IKE Gateway settings
D. Create a Device Group with the appropriate IPSec tunnel settings

**Answer:** B

**NEW QUESTION 284**
What are two prerequisites for configuring a pair of Palo Alto Networks firewalls in an active/passive High Availability (HA) pair? (Choose two.)

A. The firewalls must have the same set of licenses.

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

**Answer:** AD

**NEW QUESTION 285**
A network design change requires an existing firewall to start accessing Palo Alto Updates from a data plane interface address instead of the management interface.
Which configuration setting needs to be modified?

A. Service route
B. Default route
C. Management profile
D. Authentication profile

**Answer:** A

**NEW QUESTION 286**
Which URL Filtering Security Profile action togs the URL Filtering category to the URL Filtering log?

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

**Answer:** B

**NEW QUESTION 287**
Which Panorama feature allows for logs generated by Panorama to be forwarded to an external Security Information and Event Management(SIEM) system?

A. Panorama Log Settings
B. Panorama Log Templates
C. Panorama Device Group Log Forwarding
D. Collector Log Forwarding for Collector Groups

**Answer:** A

**Explanation:**
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_admiHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"nguidHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"e/manage-log- collection/enable-log-forwarding-from-panorama-to-external-destinaHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"tions

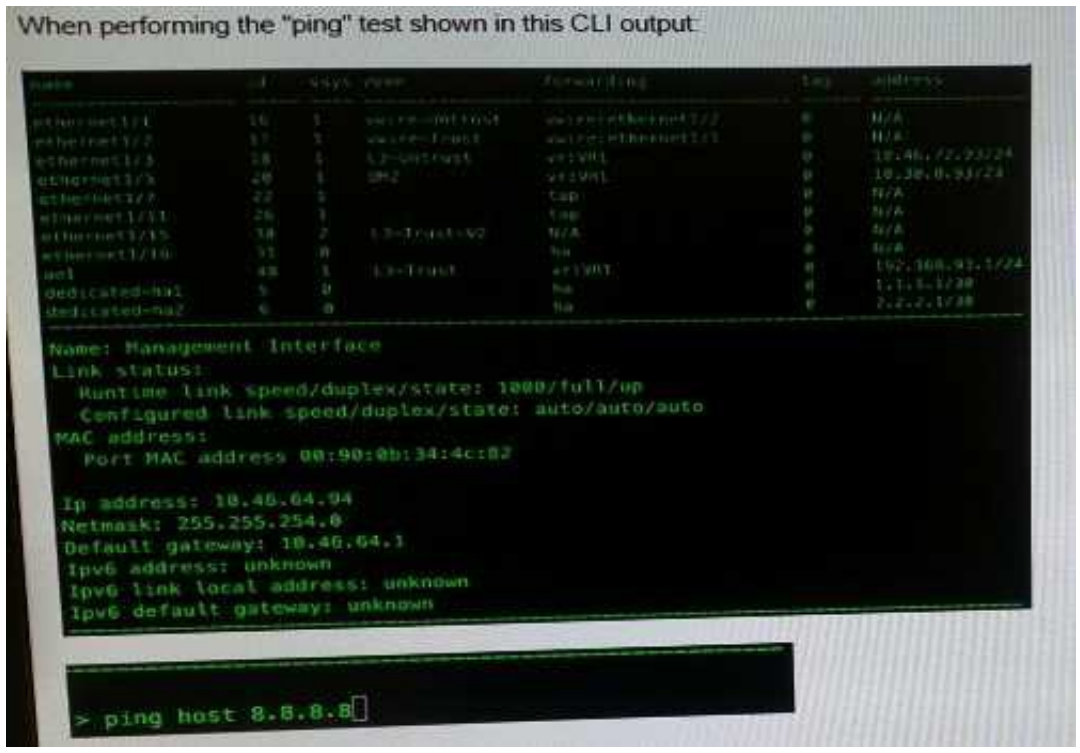
**NEW QUESTION 288**
Which CLI command displays the current management plan memory utilization?

A. > show system info
B. > show system resources
C. > debug management-server show
D. > show running resource-monitor

**Answer:** B

**Explanation:**
https://live.paloaltonetworks.comHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of-9999/ta-p/58149"/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of- 9999/ta-p/58149

**NEW QUESTION 290**
What will be the source address in the ICMP packet?




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

**Answer:** C

**NEW QUESTION 291**
A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?

A. Block all unauthorized applications using a security policy
B. Block all known internal custom applications
C. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
D. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks

**Answer:** D

**NEW QUESTION 294**
A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

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

**Answer:** BD

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

**NEW QUESTION 296**
Which CLI command displays the current management plane memory utilization?

A. > debug management-server show
B. > show running resource-monitor
C. > show system info
D. > show system resources

**Answer:** D

**Explanation:**
https://HYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364"live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret- show-system-resources/ta-p/59364
"The command show system resources gives a snapshot of Management Plane (MP) resource utilization including memory and CPU. This is similar to the 'top' command in Linux." https://live.HYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret- show-system-resources/ta-p/59364"paloHYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system- resources/ta-p/59364"altonetworHYPERLINK "https://live.paloaltonetworks.com/t5/Learning- Articles/How-to-Interpret-show-system-resources/ta-p/59364"ks.com/t5/Learning-Articles/How-to- Interpret-show-system-resources/ta-p/59364

**NEW QUESTION 297**
When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinhole enabled, generating a traffic log.
What will be the destination IP Address in that log entry?

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

**Answer:** C

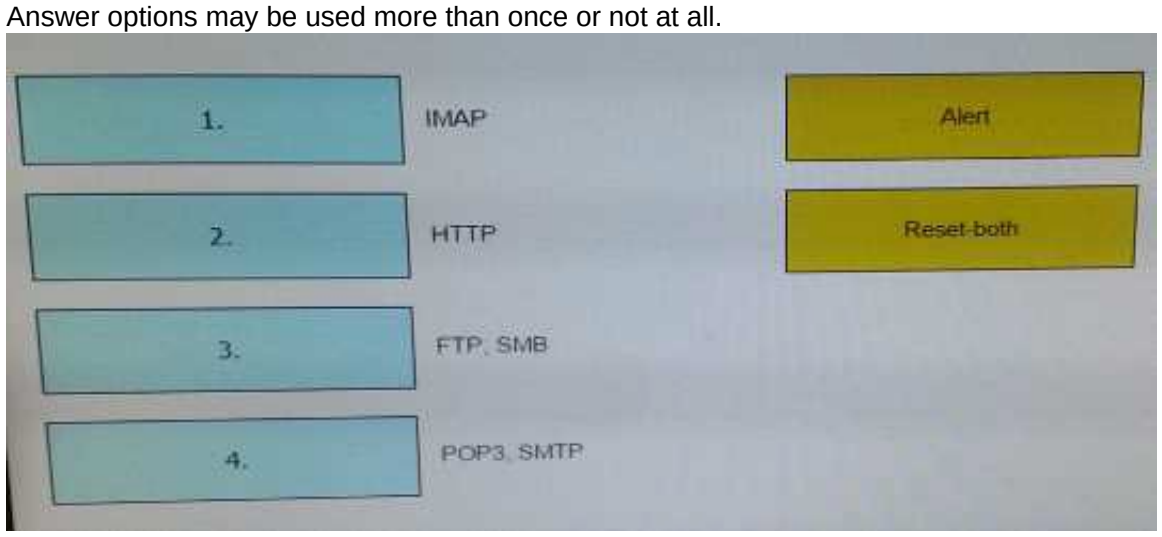
**Explanation:**
https://live.paloaltonetworks.com/t5/MaHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function- is-Working/ta-p/65864"naHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864"gement-Articles/How-to-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

**NEW QUESTION 302**
A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:
* Users outside the company are in the "Untrust-L3" zone.
* The web server physically resides in the "Trust-L3" zone.
* Web server public IP address: 23.54.6.10
* Web server private IP address: 192.168.1.10
Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

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

**Answer:** AB

**NEW QUESTION 305**
DRAG DROP
When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.
Answer options may be used more than once or not at all.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
**IMAP , POP3 , SMTP - > Alert**
**HTTP,FTP,SMB -> Reset-both**

**NEW QUESTION 306**
.....

# About Exambible

***Your Partner of IT Exam***

# Found in 1998

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

# Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

**NEW QUESTION 1**
SAML SLO is supported for which two firewall features? (Choose two.)

A. GlobalProtect Portal
B. CaptivePortal
C. WebUI
D. CLI

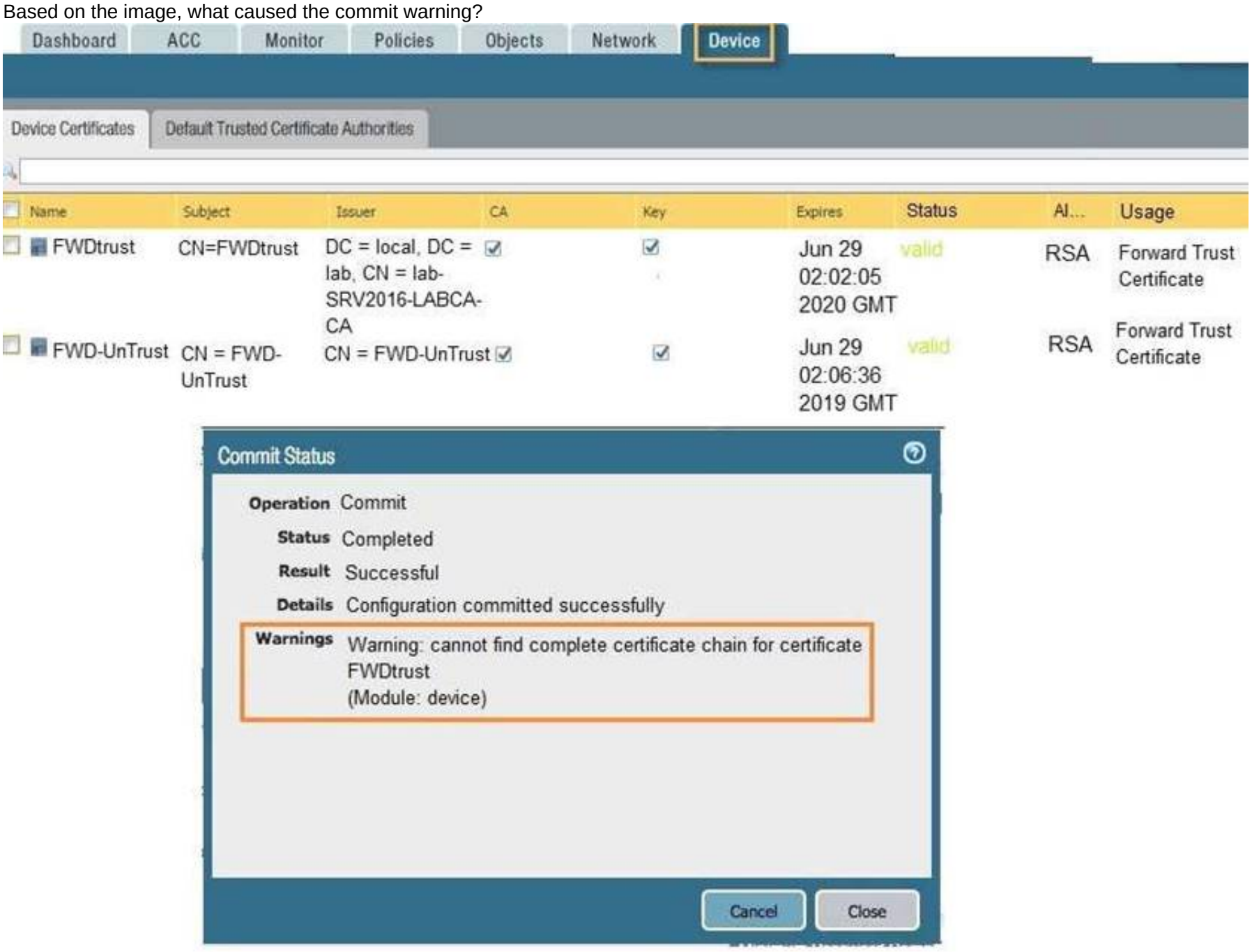
**Answer:** AB

**NEW QUESTION 2**
Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

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

**Answer:** ABC

**NEW QUESTION 3**
Based on 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.

**Answer:** D

**NEW QUESTION 4**
What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

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

D. Rule Usage Hit counter will reset.

**Answer:** AB

**NEW QUESTION 5**
Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 6**
Which administrative authentication method supports authorization by an external service?

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

**Answer:** C

**NEW QUESTION 7**
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.

**Answer:** A

**NEW QUESTION 8**
Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

A. GlobalProtect version 4.0 with PAN-OS 8.1
B. GlobalProtect version 4.1 with PAN-OS 8.1
C. GlobalProtect version 4.1 with PAN-OS 8.0
D. GlobalProtect version 4.0 with PAN-OS 8.0

**Answer:** B

**NEW QUESTION 9**
How does Panorama prompt VMWare NSX to quarantine an infected VM?

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

**Answer:** A

**NEW QUESTION 10**
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. 99
B. 1
C. 255

**Answer:** D

**Explanation:**
Reference:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5.pdf (page 9)

**NEW QUESTION 10**
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

**Answer:** C

**NEW QUESTION 12**
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

**Answer:** C

**Explanation:**
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

**NEW QUESTION 16**
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

**Answer:** D

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

**NEW QUESTION 21**
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

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

**Answer:** A

**NEW QUESTION 24**
To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

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

**Answer:** B

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

**NEW QUESTION 28**
An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

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

**Answer:** A

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

**NEW QUESTION 29**

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

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

**Answer:** BD

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

**NEW QUESTION 32**
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 invali
B. The Profile Settings section will be grayed out when the Action is set to "Deny".
C. The configuration will allow the matched session unless a vulnerability signature is detecte
D. The "Deny" action will supersede theper-severity defined actions defined in the associated Vulnerability Protection Profile.
E. The configuration is invali
F. It will cause the firewall to skip this Security policy rul
G. A warning will be displayed during a commit.
H. The configuration is vali
I. It will cause the firewall to deny the matched session
J. Any configured Security Profiles have no effect ifthe Security policy rule action is set to "Deny."

**Answer:** B

**NEW QUESTION 33**
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.

**Answer:** C

**NEW QUESTION 35**
Which Captive Portal mode must be configured to support MFA authentication?

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

**Answer:** B

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

**NEW QUESTION 40**
A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

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

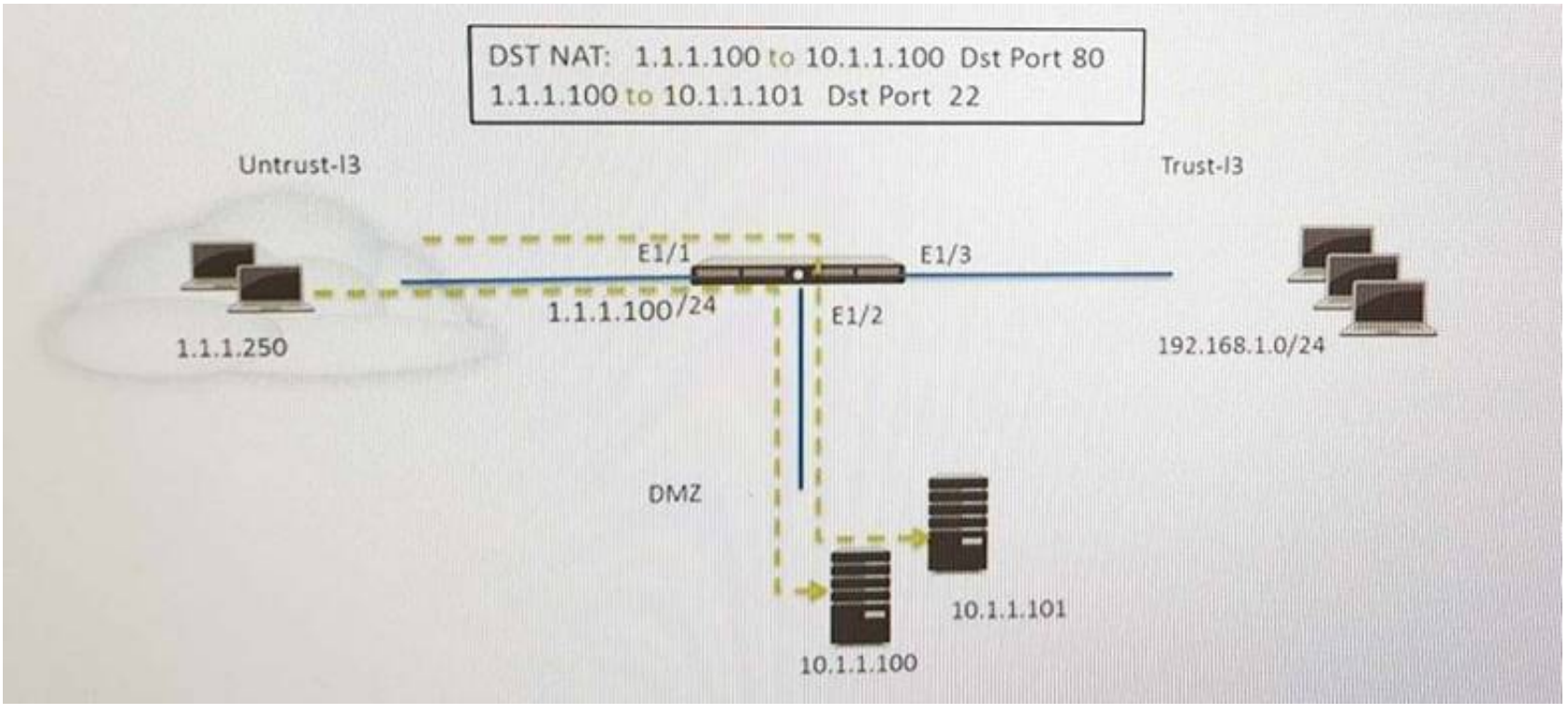
**Answer:** B

**NEW QUESTION 44**
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

**Answer:** C

**NEW QUESTION 45**
Refer to the exhibit.

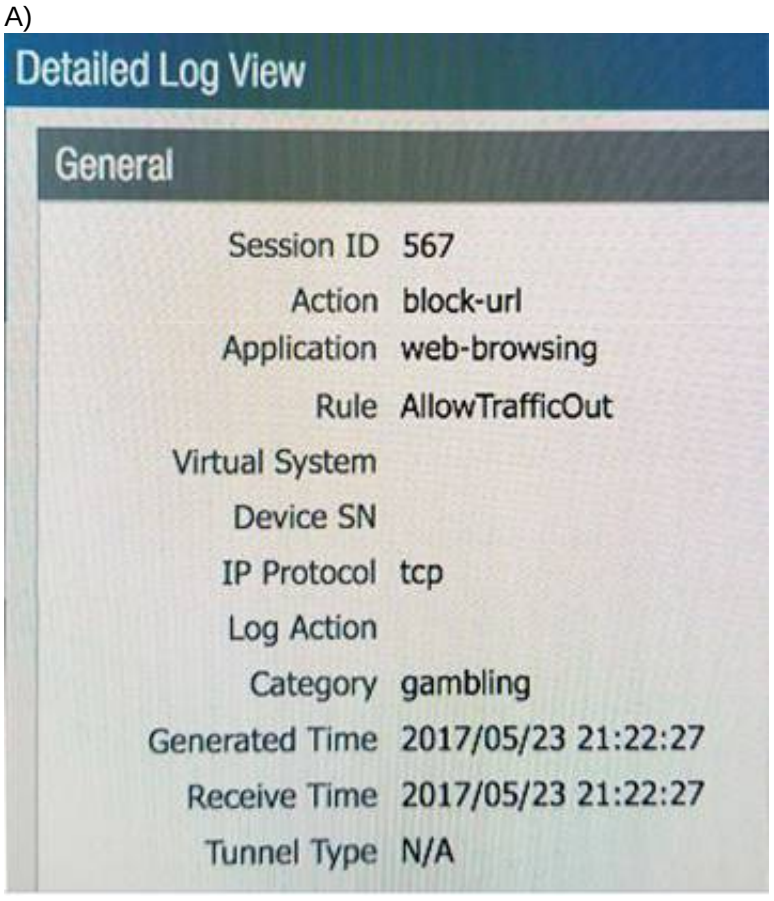



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.)
Which two security policy rules will accomplish this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

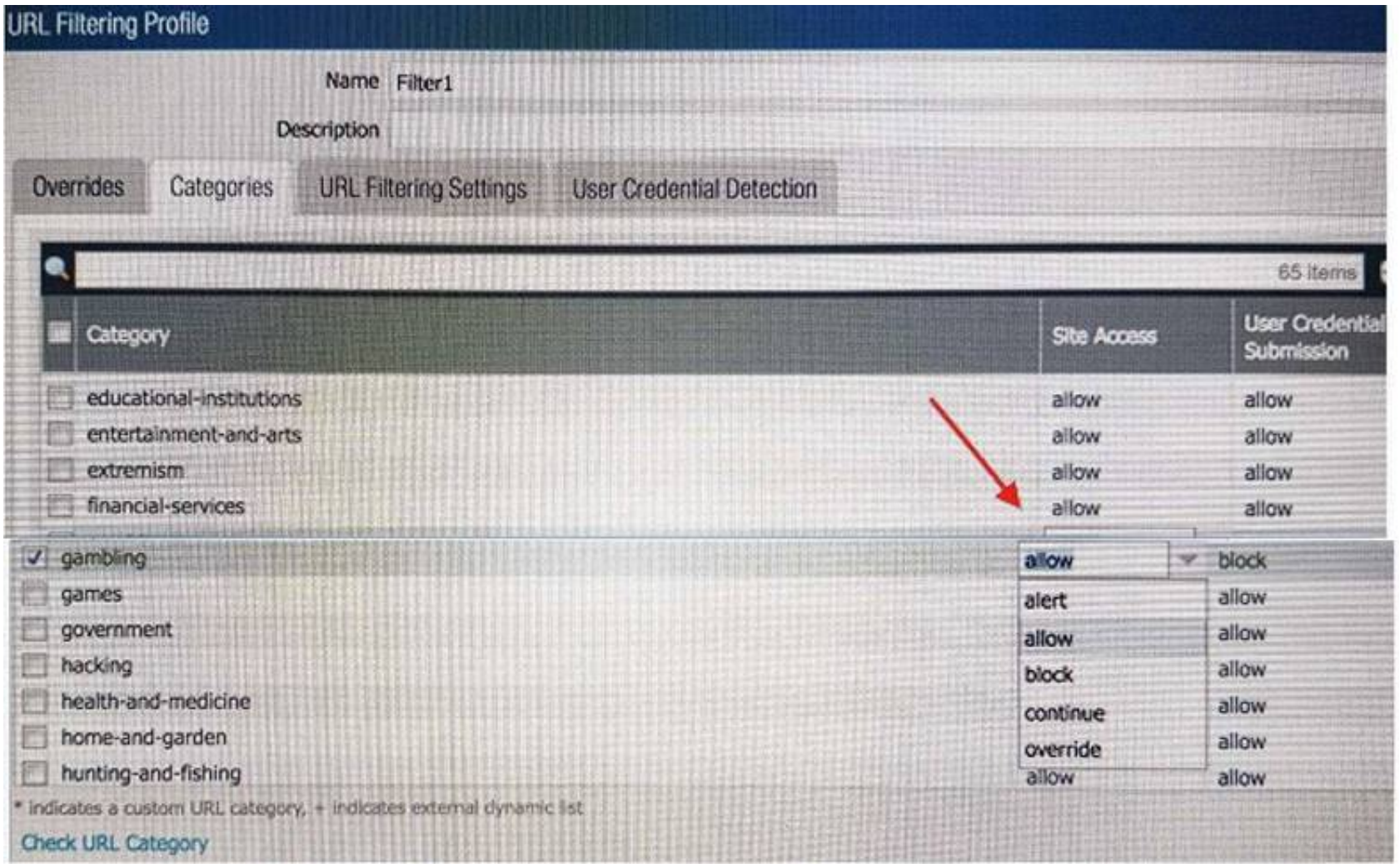
A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
D. Untrust (Any) to DMZ (10.1.1.1), ssh –Allow
E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

**Answer:** CD

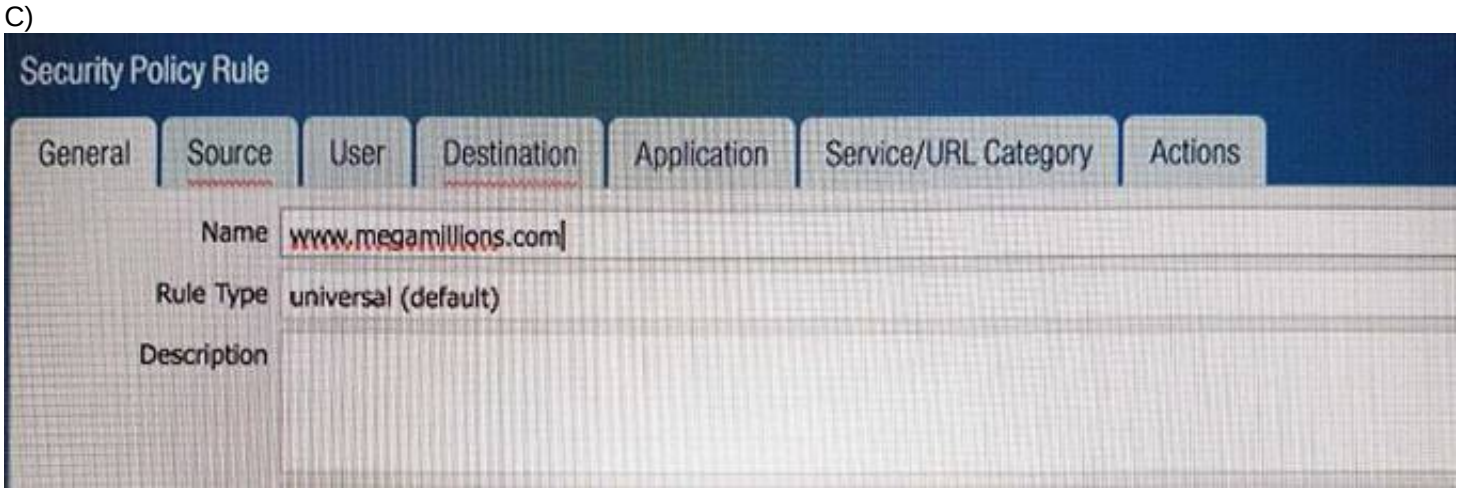
**NEW QUESTION 49**
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.
Which configuration change should the administrator make?
A)



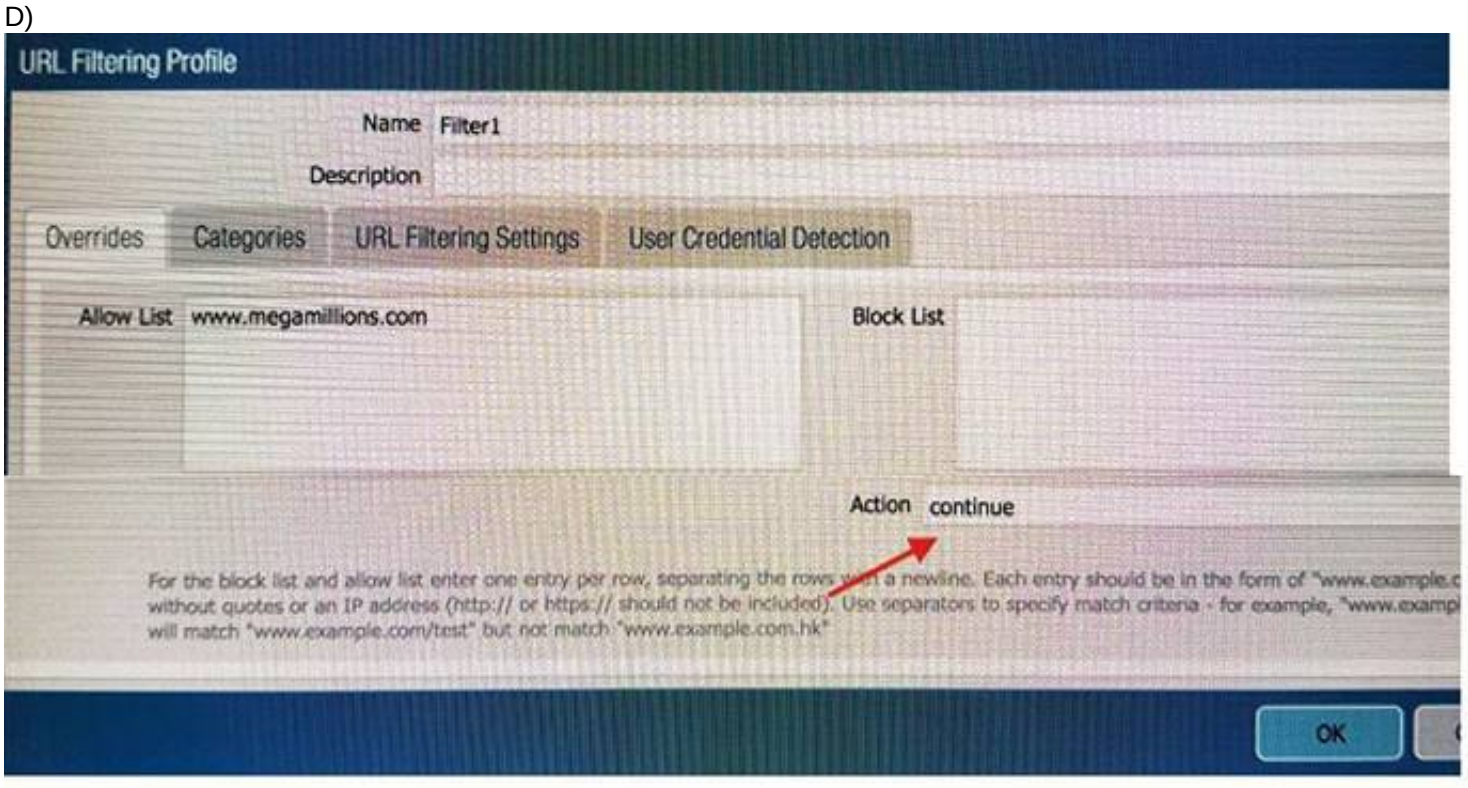

B)


URL Filtering Profile
Name Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
65 items
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial-services
gambling
games
government
hacking
health-and-medicine
home-and-garden
hunting-and-fishing
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category

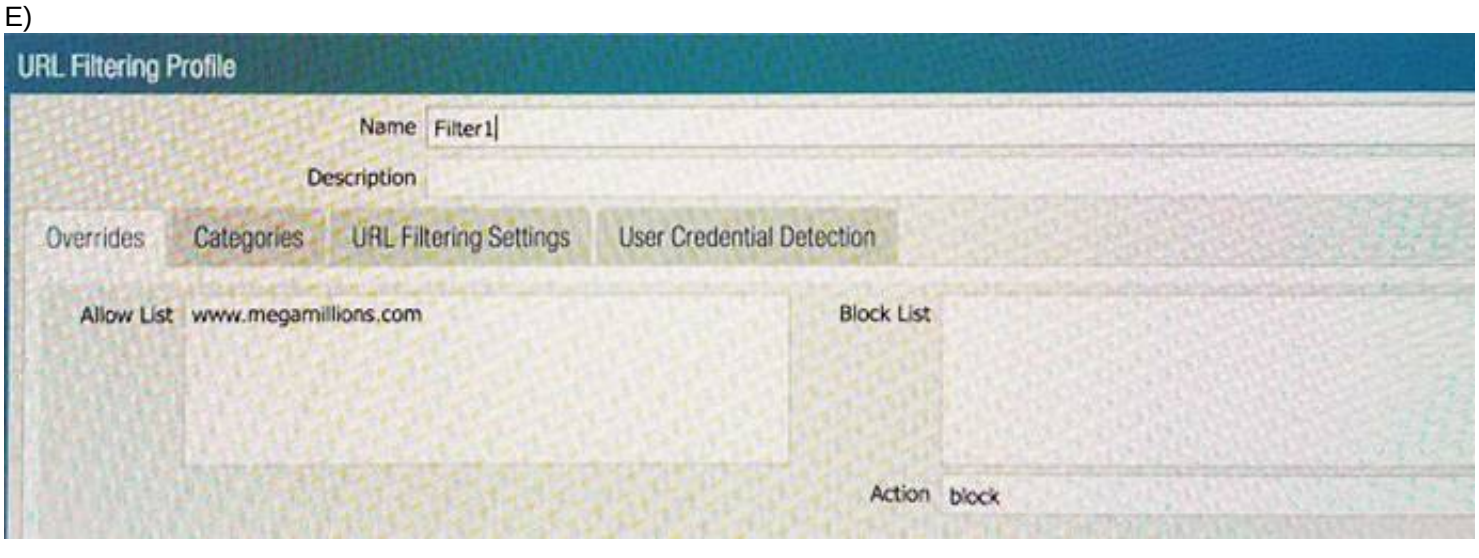
C)


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Name www.megamillions.com
Rule Type universal (default)
Description

D)


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.c
without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.exampl
will match "www.example.com/test" but not match "www.example.com.hk"
OK

E)


URL Filtering Profile
Name Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
Allow List www.megamillions.com
Block List
Action block

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

**Answer:** B

**NEW QUESTION 52**
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

**Answer:** A

**NEW QUESTION 53**
Which Palo Alto Networks VM-Series firewall is valid?

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

**Answer:** C

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

**NEW QUESTION 54**
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?

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

**Answer:** A

**NEW QUESTION 57**
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

**Answer:** DEF

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

**NEW QUESTION 59**
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

**Answer:** DEF

**NEW QUESTION 62**
Which event will happen if an administrator uses an Application Override Policy?

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override/ta-p/65513

**NEW QUESTION 66**
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

**Answer:** A

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

**NEW QUESTION 71**
If the firewall is configured for credential phishing prevention using the “Domain Credential Filter” method, which login will be detected as credential theft?

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 72**
An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

**Answer:** B

**NEW QUESTION 77**
Which protection feature is available only in a Zone Protection Profile?

A. SYN Flood Protection using SYN Flood Cookies
B. ICMP Flood Protection
C. Port Scan Protection
D. UDP Flood Protections

**Answer:** A

**NEW QUESTION 81**
Which CLI command can be used to export the tcpdump capture?

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 86**
During the packet flow process, which two processes are performed in application identification? (Choose two.)

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

**Answer:** BD

**NEW QUESTION 90**
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?

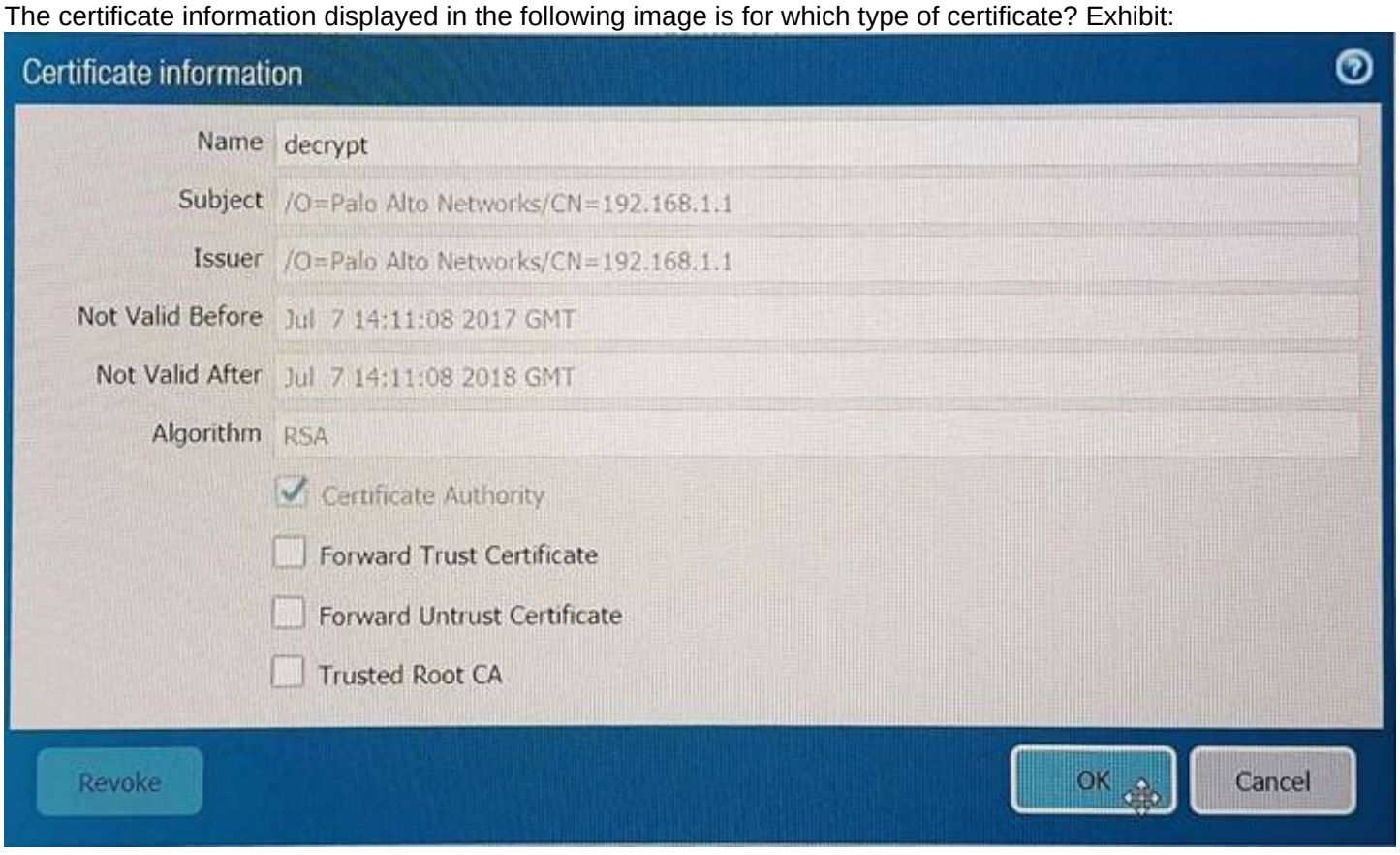
A. Session Browser

B. Application Command Center
C. TCP Dump
D. Packet Capture

**Answer:** B

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

**NEW QUESTION 94**
The certificate information displayed in the following image is for which type of certificate? Exhibit:




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

**Answer:** D

**NEW QUESTION 96**
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

**Answer:** A

**NEW QUESTION 101**
The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router. Which two options would help the administrator troubleshoot this issue? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 102**
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.

**Answer:** AB

**NEW QUESTION 103**

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

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

**Answer:** C

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf

**NEW QUESTION 105**
An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.
Which interface type and license feature are necessary to meet the requirement?

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

**Answer:** D

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring

**NEW QUESTION 106**
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

**Answer:** A

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

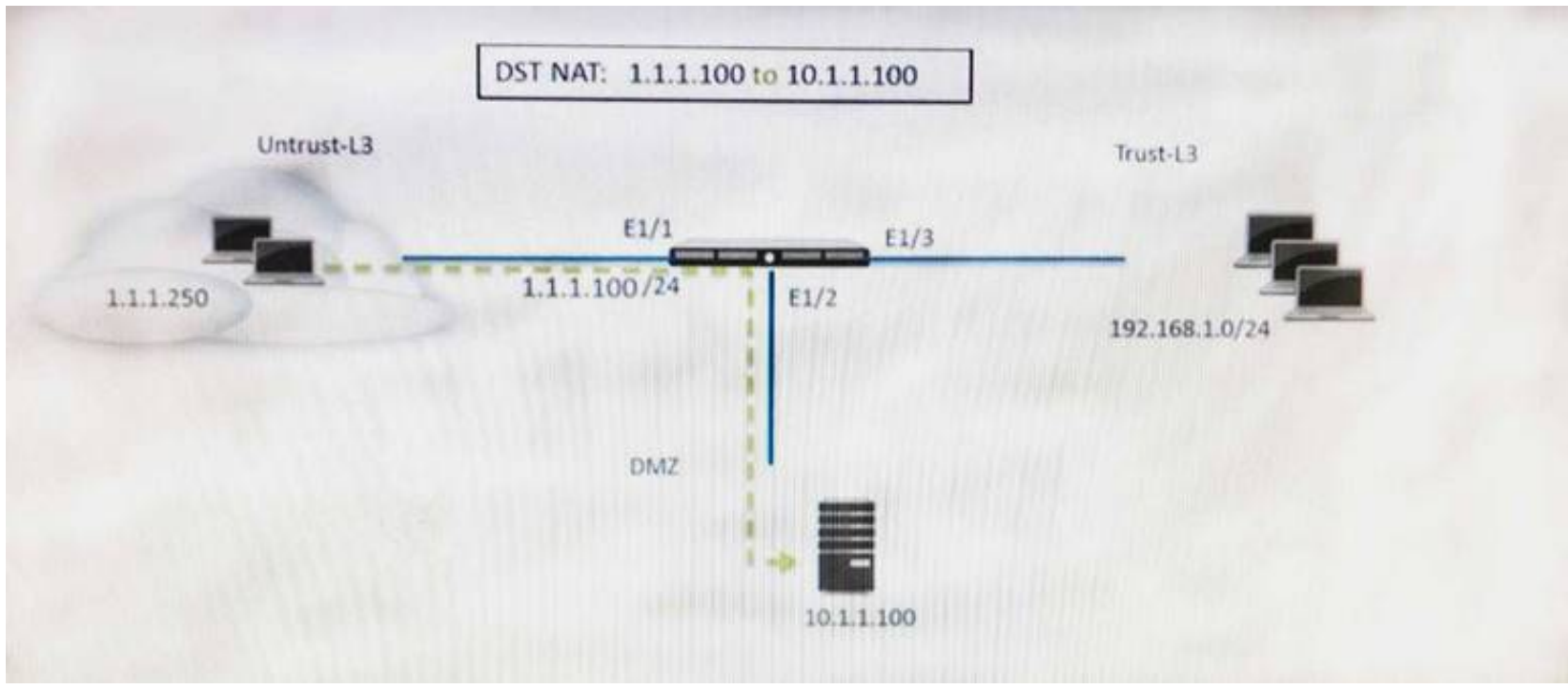
**NEW QUESTION 108**
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system. Which Security Profile type will prevent this attack?

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

**Answer:** A

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection

**NEW QUESTION 111**
Refer to the exhibit.




A web server in the DMZ is being mapped to a public address through DNAT. Which Security policy rule will allow traffic to flow to the web server?

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

**Answer:** B

**NEW QUESTION 113**
Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

A. The firewall is in multi-vsys mode.
B. The traffic is offloaded.
C. The traffic does not match the packet capture filter.
D. The firewall's DP CPU is higher than 50%.

**Answer:** BC

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload

**NEW QUESTION 116**
Which feature can be configured on VM-Series firewalls?

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

**Answer:** D

**NEW QUESTION 118**
If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 122**
View the GlobalProtect configuration screen capture.


What is the purpose of this configuration?

A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

**Answer:** C

**Explanation:**
Reference: https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations

**NEW QUESTION 126**
What is exchanged through the HA2 link?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 127**
Which three authentication factors does PAN-OS® software support for MFA (Choose three.)

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

**Answer:** ADE

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

**NEW QUESTION 130**
An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.
What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 131**
A company wants to install a PA-3060 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 options differentiates multiple VLAN into separate zones?

A. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN I
B. Repeat forevery additional VLANand use a VLAN ID of 0 for untagged traffi
C. Assign each interface/subinterface to a unique zone.
D. Create V-Wire objects with two V-Wire sub interface and assign only a single VLAN ID to the "Tag Allowed field one of the V-Wire object Repeat for every additional VLAN and use a VIAN ID of 0 for untagged traffi
E. Assign each interface/subinterfaceto a unique zone.
F. Create V-Wire objects with two V-Wire interfaces and define a range “0- 4096" in the 'Tag Allowed filed of the V-Wire object.
G. Create Layer 3 sub interfaces that are each assigned to a single VLAN ID and a common virtual route
H. The physical Layer 3interface would handle untagged traffi
I. Assign each interface /subinterface to a unique zon
J. Do not assign any interface anIP address

**Answer:** C

**NEW QUESTION 132**
Which logs enable a firewall administrator to determine whether a session was decrypted?

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

**Answer:** B

**NEW QUESTION 135**
Which data flow describes redistribution of user mappings?

A. User-ID agent to firewall
B. firewall to firewall
C. Domain Controller to User-ID agent
D. User-ID agent to Panorama

**Answer:** B

**NEW QUESTION 137**
Which two features does PAN-OS® software use to identify applications? (Choose two)

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

**Answer:**

CD

**NEW QUESTION 140**
Which log file can be used to identify SSL decryption failures?

A. Configuration
B. Threats
C. ACC
D. Traffic

**Answer:** C

**NEW QUESTION 143**
Which three firewall states are valid? (Choose three)

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

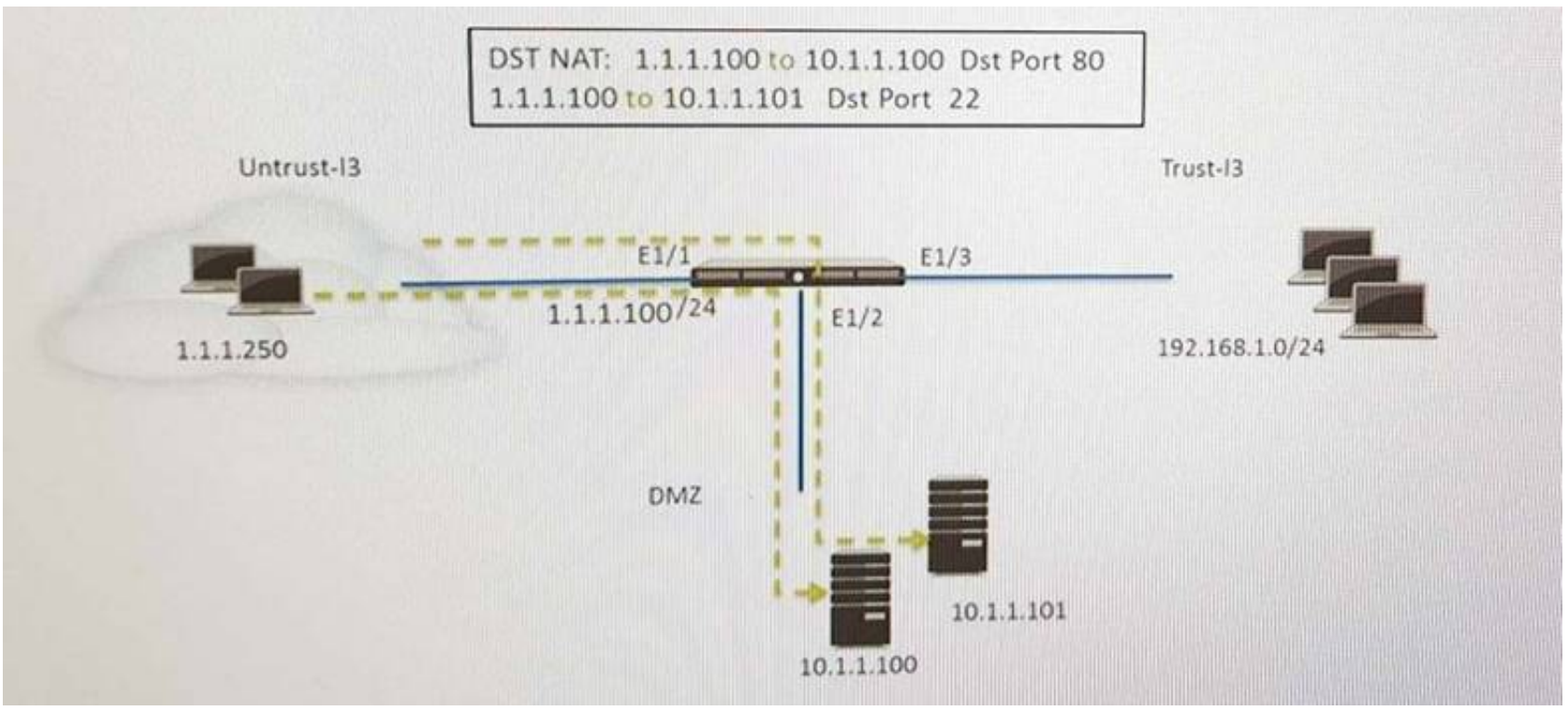
**Answer:** ABC

**NEW QUESTION 144**
An administrator wants to upgrade an NGFW from PAN-OS® 7 .1. 2 to PAN-OS® 8 .0.2 The firewall is not a part of an HA pair. What needs to be updated first?

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

**Answer:** B

**NEW QUESTION 149**
Refer to the exhibit.




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

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

**Answer:** CD

**NEW QUESTION 154**
Which is the maximum number of samples that can be submitted to WildFire per day, based on wildfire subscription?

A. 15,000
B. 10,000
C. 75,00
D. 5,000

**Answer:** B

**NEW QUESTION 156**
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 Data Filtering Profile
B. Enable QoS monitor
C. Enable Qos interface
D. Enable Qos in the interface Management Profile.

**Answer:** C

**NEW QUESTION 161**
When configuring the firewall for packet capture, what are the valid stage types?

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

**Answer:** D

**NEW QUESTION 163**
What are the differences between using a service versus using an application for Security Policy match?

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

**Answer:** B

**NEW QUESTION 168**
In which two types of deployment is active/active HA configuration supported? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 173**
A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial of-service attacks.
How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

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

**Answer:** C

**NEW QUESTION 178**
Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

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

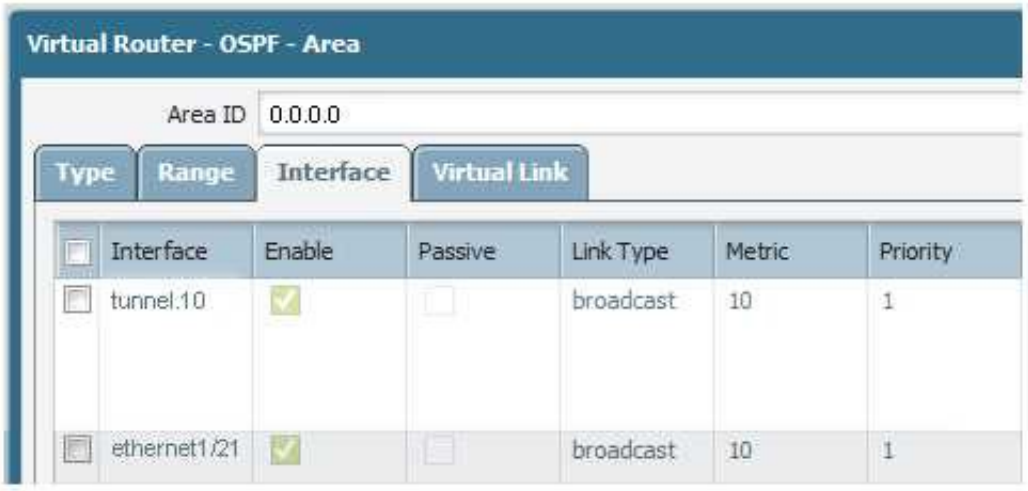
**Answer:** DE

**NEW QUESTION 181**
Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.

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

**Answer:** B

**NEW QUESTION 186**
Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunner is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.

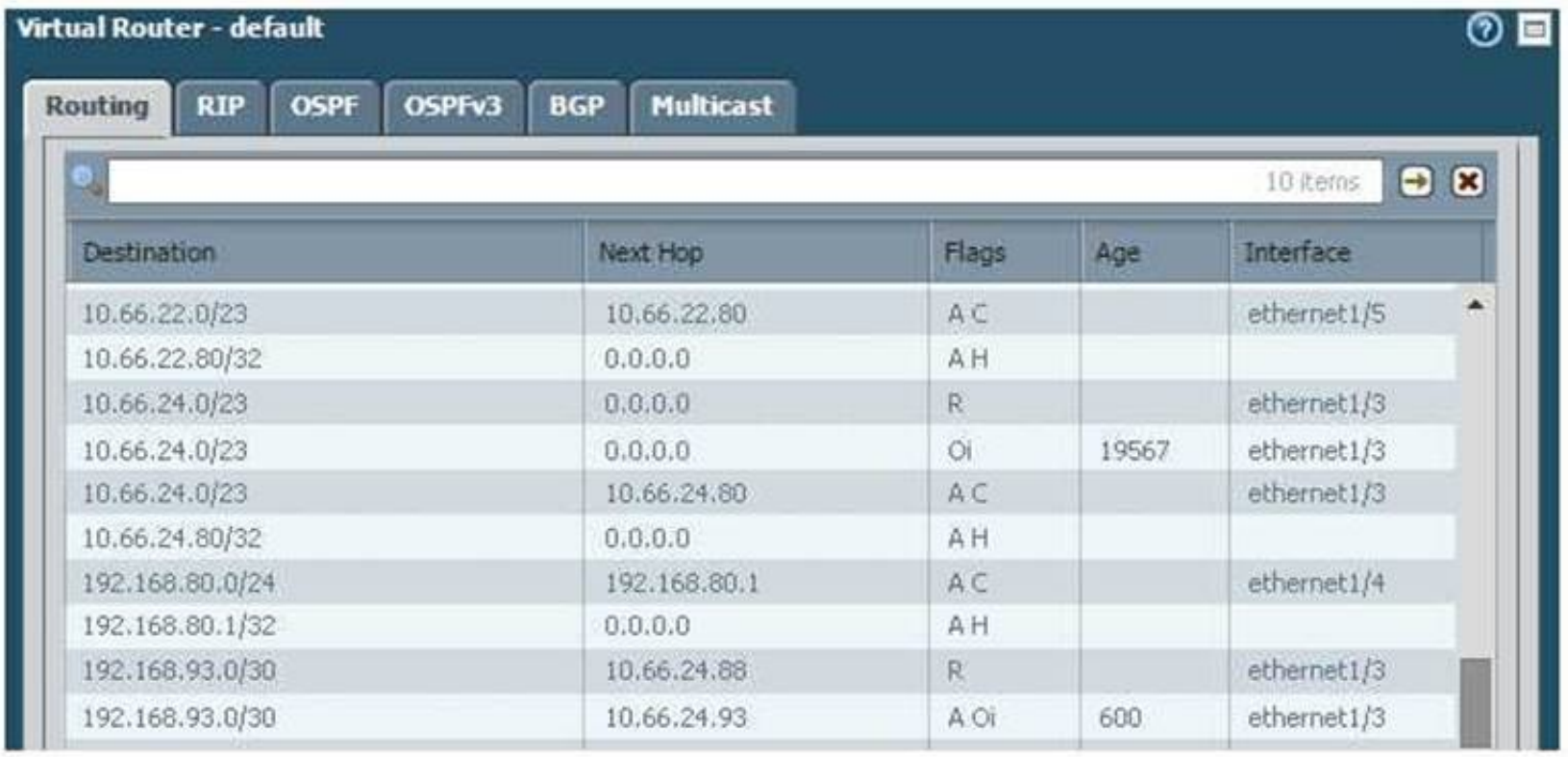



Which Link Type setting will correct the error?

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

**Answer:** A

**NEW QUESTION 187**
Given the following table.




Which configuration change on the firewall would cause it to use 10.66.24.88 as the next hop for the 192.168.93.0/30 network?

A. Configuring the administrative Distance for RIP to be lower than that of OSPF Int.
B. Configuring the metric for RIP to be higher than that of OSPF Int.
C. Configuring the administrative Distance for RIP to be higher than that of OSPF Ext.
D. Configuring the metric for RIP to be lower than that OSPF Ext.

**Answer:** A

**NEW QUESTION 189**
A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk.
What action will bring the VPN up and allow traffic to start passing between the sites?

A. Change the Site-B IKE Gateway profile version to match Site-A,
B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.
C. Enable NAT Traversal on the Site-A IKE Gateway profile.
D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A

**Answer:** D

**NEW QUESTION 194**
A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.
Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?( Choose three)

A. Download PAN-OS 8.0.4 files from the support site and install them on each firewall after manually uploading.
B. Download PAN-OS 8.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.
C. Push the PAN-OS 8.0.4 updates from the support site to install on each firewall.
D. Push the PAN-OS 8.0.4 update from one firewall to all of the other remaining after updating one firewall.
E. Download and install PAN-OS 8.0.4 directly on each firewall.
F. Download and push PAN-OS 8.0.4 from Panorama to each firewall.

**Answer:** ACF

**NEW QUESTION 198**
A network engineer has revived a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.
Which CLI command will help identify the issue?

A. test routing fib virtual-router vr1
B. show routing route type static destination 98.139.183.24
C. test routing fib-lookup ip 98.139.183.24 virtual-router vr1
D. show routing interface

**Answer:** C

**NEW QUESTION 200**
A network Administrator needs to view the default action for a specific spyware signature. The administrator follows the tabs and menus through Objects> Security Profiles> Anti-Spyware and select default profile.
What should be done next?

A. Click the simple-critical rule and then click the Action drop-down list.
B. Click the Exceptions tab and then click show all signatures.
C. View the default actions displayed in the Action column.
D. Click the Rules tab and then look for rules with "default" in the Action column.

**Answer:** B

**NEW QUESTION 203**
Which two mechanisms help prevent a spilt brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

A. Configure the management interface as HA3 Backup
B. Configure Ethernet 1/1 as HA1 Backup
C. Configure Ethernet 1/1 as HA2 Backup
D. Configure the management interface as HA2 Backup
E. Configure the management interface as HA1 Backup
F. Configure ethernet1/1 as HA3 Backup

**Answer:** BE

**NEW QUESTION 204**
How is the Forward Untrust Certificate used?

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

**Answer:** C

**NEW QUESTION 205**
Which command can be used to validate a Captive Portal policy?

A. eval captive-portal policy <criteria>
B. request cp-policy-eval <criteria>
C. test cp-policy-match <criteria>
D. debug cp-policy <criteria>

**Answer:** C

**NEW QUESTION 206**
Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

A. Set the type to Aggregate, clear the session’s box and set the Maximum concurrent Sessions to 4000.
B. Set the type to Classified, clear the session’s box and set the Maximum concurrent Sessions to 4000.
C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.
D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000.

**Answer:** C

**NEW QUESTION 211**

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

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

**Answer:** ABF

**NEW QUESTION 215**
A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled.
Which component once enabled on a perirneter firewall will allow the identification of existing infected hosts in an environment?

A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
B. File Blocking profiles applied to outbound security policies with action set to alert
C. Vulnerability Protection profiles applied to outbound security policies with action set to block
D. Antivirus profiles applied to outbound security policies with action set to alert

**Answer:** A

**NEW QUESTION 220**
Which three options are available when creating a security profile? (Choose three)

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

**Answer:** ABF

**NEW QUESTION 224**
Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

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

**Answer:** BD

**NEW QUESTION 229**
A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and post.
Which option when enabled with the correction threshold would mitigate this attack without dropping legitirnate traffic to other hosts insides the network?

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

**Answer:** D

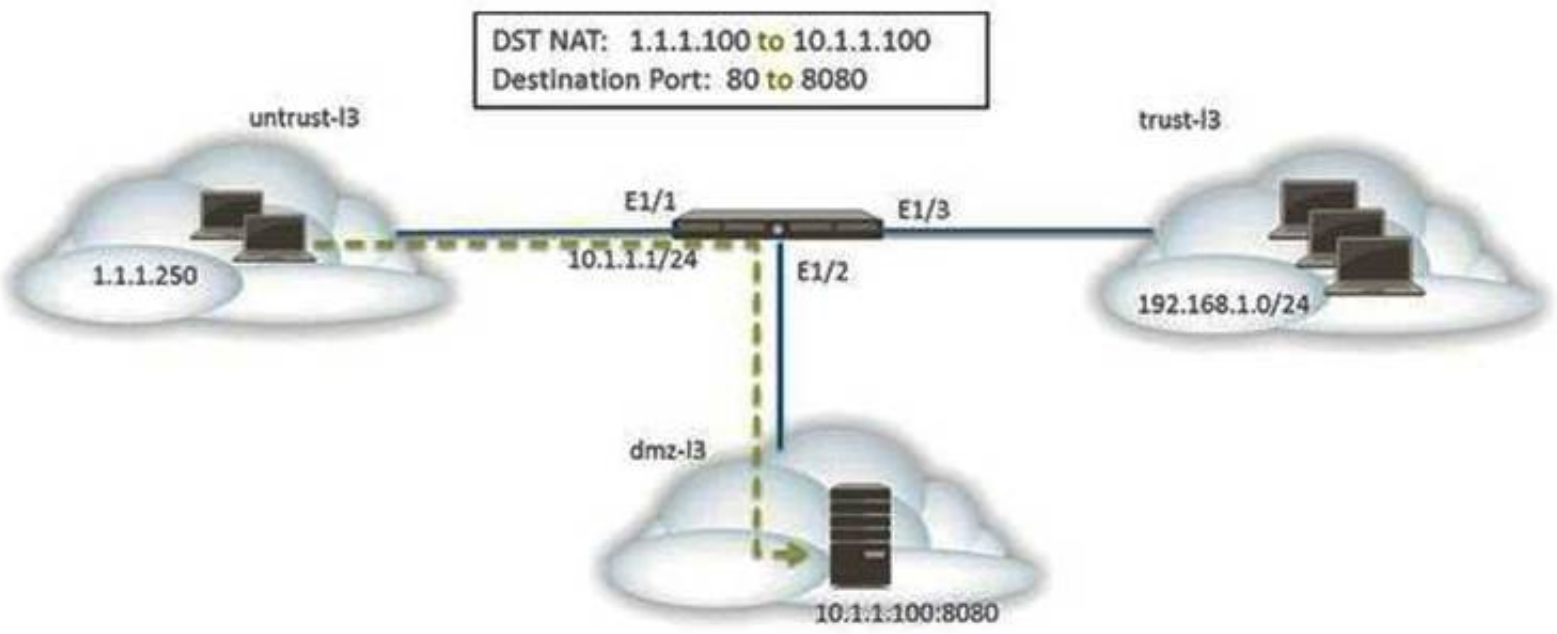
**NEW QUESTION 232**
Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

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

**Answer:** BE

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

**NEW QUESTION 237**
The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and report to 10.1.1.100 on TCP Port 8080.




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

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

**Answer:** BD

**NEW QUESTION 238**
Palo Alto Networks maintains a dynamic database of malicious domains.
Which two Security Platform components use this database to prevent threats? (Choose two)

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

**Answer:** CD

**NEW QUESTION 241**
A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall
Which part of files needs to be imported back into the replacement firewall that is using Panorama?

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

**Answer:** A

**NEW QUESTION 245**
A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.
Given the following zone information:
• DMZ zone: DMZ-L3
• Public zone: Untrust-L3
• Guest zone: Guest-L3
• Web server zone: Trust-L3
• Public IP address (Untrust-L3): 1.1.1.1
• Private IP address (Trust-L3): 192.168.1.50
What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

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

**Answer:** A

**NEW QUESTION 247**
Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.
Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

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

D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

**Answer:** D

**NEW QUESTION 252**
A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.
What could cause this condition?

A. The firewall does not have an active WildFire subscription.
B. The engineer's account does not have permission to view WildFire Submissions.
C. A policy is blocking WildFire Submission traffic.
D. Though WildFire is working, there are currently no WildFire Submissions log entries.

**Answer:** B

**NEW QUESTION 255**
A network administrator uses Panorama to push security polices to managed firewalls at branch offices. Which policy type should be configured on Panorama if the administrators at the branch office sites to override these products?

A. Pre Rules
B. Post Rules
C. Explicit Rules
D. Implicit Rules

**Answer:** A

**NEW QUESTION 256**
What are three valid method of user mapping? (Choose three)

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

**Answer:** ABE

**NEW QUESTION 261**
What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

A. Clean
B. Bengin
C. Adware
D. Suspicious
E. Grayware
F. Malware

**Answer:** BEF

**Explanation:**
https://www.paloaltonetworks.com/documentation/70/pan-HYPERLINK "https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict"os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict

**NEW QUESTION 262**
How are IPV6 DNS queries configured to user interface ethernet1/3?

A. Network > Virtual Router > DNS Interface
B. Objects > CustomerObjects > DNS
C. Network > Interface Mgrnt
D. Device > Setup > Services > Service Route Configuration

**Answer:** D

**NEW QUESTION 264**
A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

A. From the CLI, issue the show counter global filter pcap yes command.
B. From the CLI, issue the show counter global filter packet-filter yes command.
C. From the GUI, select show global counters under the monitor tab.
D. From the CLI, issue the show counter interface command for the ingress interface.

**Answer:** B

**NEW QUESTION 265**

A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

A. DHCP has been set to Auto.
B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.
C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.
D. DNS has not been properly configured on the firewall

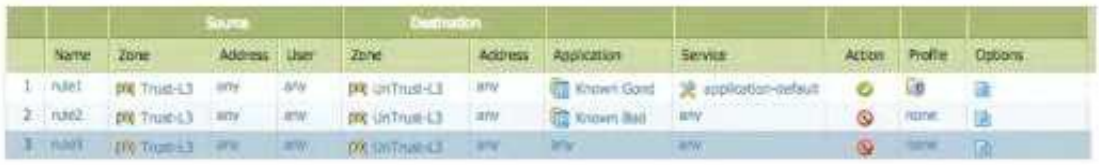
**Answer:** B

**NEW QUESTION 267**
Which interface configuration will accept specific VLAN IDs?

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

**Answer:** B

**NEW QUESTION 271**
A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's
firewall.




Which interface configuration will accept specific VLAN IDs?
Which two benefits are gained from having both rule 2 and rule 3 presents? (choose two)

A. A report can be created that identifies unclassified traffic on the network.
B. Different security profiles can be applied to traffic matching rules 2 and 3.
C. Rule 2 and 3 apply to traffic on different ports.
D. Separate Log Forwarding profiles can be applied to rules 2 and 3.

**Answer:** BD

**NEW QUESTION 276**
Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?

A. VM-100
B. VM-200
C. VM-1000-HV
D. VM-300

**Answer:** C

**NEW QUESTION 279**
After pushing a security policy from Panorama to a PA-3020 firwall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

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

**Answer:** D

**NEW QUESTION 281**
A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations.
How should this be accomplished?

A. Create a Template with the appropriate IKE Gateway settings
B. Create a Template with the appropriate IPSec tunnel settings
C. Create a Device Group with the appropriate IKE Gateway settings
D. Create a Device Group with the appropriate IPSec tunnel settings

**Answer:** B

**NEW QUESTION 284**
What are two prerequisites for configuring a pair of Palo Alto Networks firewalls in an active/passive High Availability (HA) pair? (Choose two.)

A. The firewalls must have the same set of licenses.

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

**Answer:** AD

**NEW QUESTION 285**
A network design change requires an existing firewall to start accessing Palo Alto Updates from a data plane interface address instead of the management interface.
Which configuration setting needs to be modified?

A. Service route
B. Default route
C. Management profile
D. Authentication profile

**Answer:** A

**NEW QUESTION 286**
Which URL Filtering Security Profile action togs the URL Filtering category to the URL Filtering log?

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

**Answer:** B

**NEW QUESTION 287**
Which Panorama feature allows for logs generated by Panorama to be forwarded to an external Security Information and Event Management(SIEM) system?

A. Panorama Log Settings
B. Panorama Log Templates
C. Panorama Device Group Log Forwarding
D. Collector Log Forwarding for Collector Groups

**Answer:** A

**Explanation:**
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_admiHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"nguidHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"e/manage-log- collection/enable-log-forwarding-from-panorama-to-external-destinaHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"tions

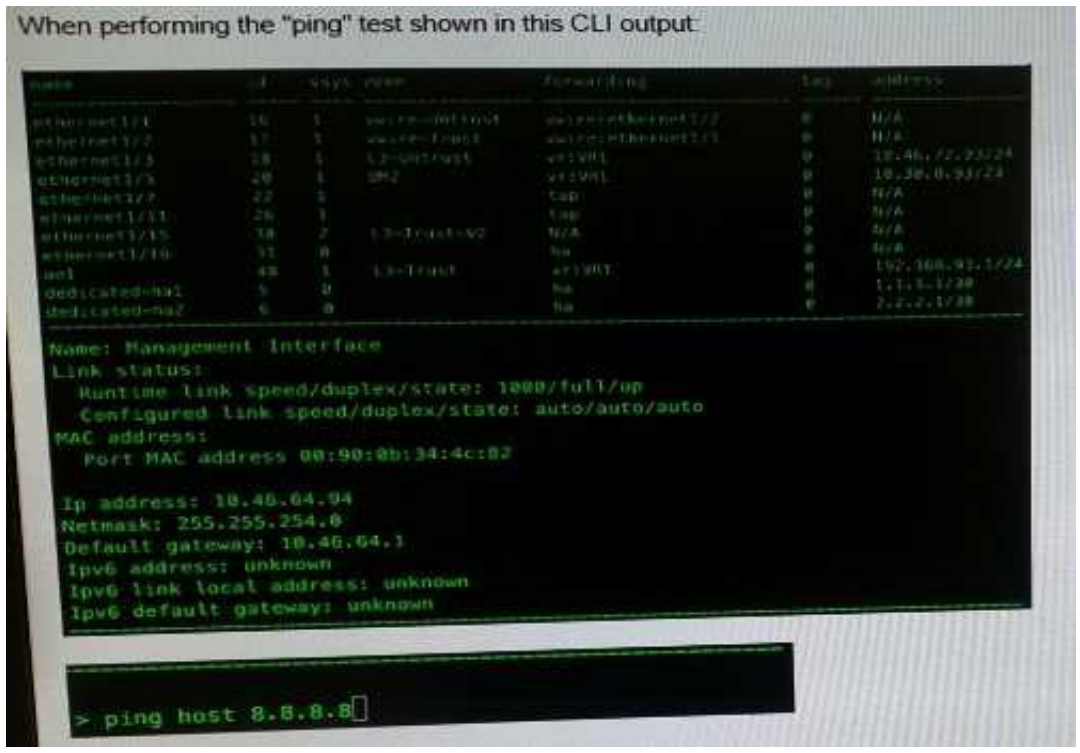
**NEW QUESTION 288**
Which CLI command displays the current management plan memory utilization?

A. > show system info
B. > show system resources
C. > debug management-server show
D. > show running resource-monitor

**Answer:** B

**Explanation:**
https://live.paloaltonetworks.comHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of-9999/ta-p/58149"/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of- 9999/ta-p/58149

**NEW QUESTION 290**
What will be the source address in the ICMP packet?




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

**Answer:** C

**NEW QUESTION 291**
A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?

A. Block all unauthorized applications using a security policy
B. Block all known internal custom applications
C. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
D. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks

**Answer:** D

**NEW QUESTION 294**
A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

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

**Answer:** BD

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

**NEW QUESTION 296**
Which CLI command displays the current management plane memory utilization?

A. > debug management-server show
B. > show running resource-monitor
C. > show system info
D. > show system resources

**Answer:** D

**Explanation:**
https://HYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364"live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret- show-system-resources/ta-p/59364
"The command show system resources gives a snapshot of Management Plane (MP) resource utilization including memory and CPU. This is similar to the 'top' command in Linux." https://live.HYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret- show-system-resources/ta-p/59364"paloHYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system- resources/ta-p/59364"altonetworHYPERLINK "https://live.paloaltonetworks.com/t5/Learning- Articles/How-to-Interpret-show-system-resources/ta-p/59364"ks.com/t5/Learning-Articles/How-to- Interpret-show-system-resources/ta-p/59364

**NEW QUESTION 297**
When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinhole enabled, generating a traffic log.
What will be the destination IP Address in that log entry?

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

**Answer:** C

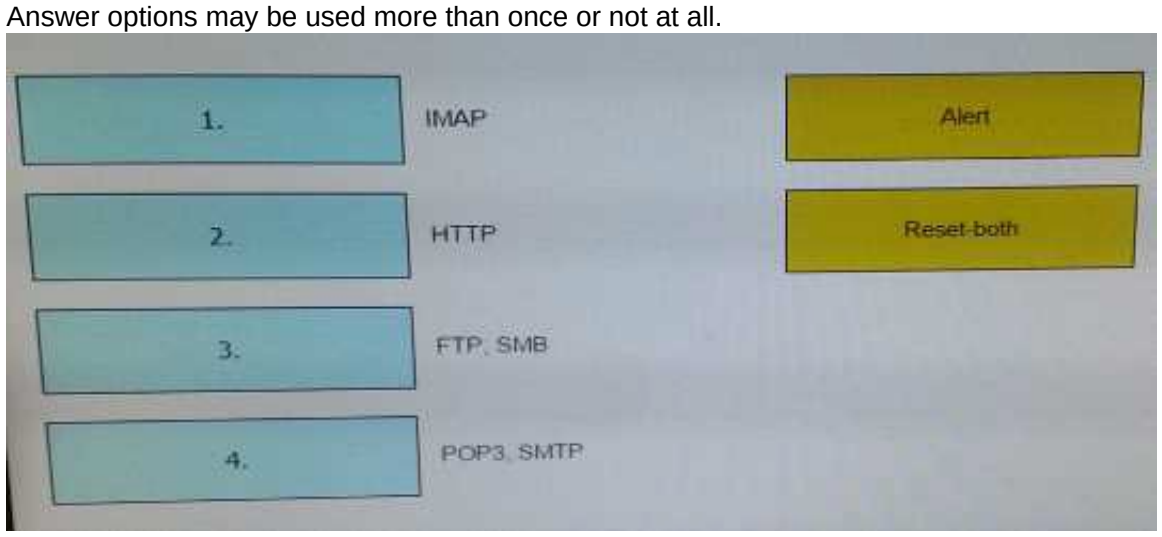
**Explanation:**
https://live.paloaltonetworks.com/t5/MaHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function- is-Working/ta-p/65864"naHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864"gement-Articles/How-to-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

**NEW QUESTION 302**
A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:
* Users outside the company are in the "Untrust-L3" zone.
* The web server physically resides in the "Trust-L3" zone.
* Web server public IP address: 23.54.6.10
* Web server private IP address: 192.168.1.10
Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

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

**Answer:** AB

**NEW QUESTION 305**
DRAG DROP
When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.
Answer options may be used more than once or not at all.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
**IMAP , POP3 , SMTP - > Alert**
**HTTP,FTP,SMB -> Reset-both**

**NEW QUESTION 306**
.....

# Relate Links

**100% Pass Your PCNSE Exam with Exambible Prep Materials**

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

# Contact us

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

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