Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://tw.fast2test.com

高效的考試材料是最高通過率的考試題庫

Exam : **PCNSE**

Title : Palo Alto Networks Certified Network Security Engineer Exam

Vendor : Palo Alto Networks

Version : DEMO

NO.1 A company.com wants to enable Application Override. Given the following screenshot:

Which two statements are true if Source and Destination traffic match the Application Override policy? (Choose two)

A. Traffic that matches "rtp-base" will bypass the App-ID and Content-ID engines.

B. Traffic will be forced to operate over UDP Port 16384.

C. Traffic utilizing UDP Port 16384 will now be identified as "rtp-base".

D. Traffic utilizing UDP Port 16384 will bypass the App-ID and Content-ID engines.

Answer: CD

Explanation:

An application override policy is changes how the Palo Alto Networks firewall classifies network traffic into applications. An application override with a custom application prevents the session from being processed by the App-ID engine, which is a Layer-7 inspection.

NO.2 Which three fields can be included in a pcap filter? (Choose three)

A. Egress interface

B. Source IP

C. Rule number

D. Destination IP

E. Ingress interface

Answer: BDE

Explanation:

https://knowledgebase.paloaltonetworks.com/servlet/rtaImage?eid=ka10g000000U0KT&feoid=00N0g000003VPSv&refid=0EM0g000001Ja97

NO.3 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:

The WildFire verdicts are: Benign, Grayware, Malware.

https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/wildfire-submissions-logs

NO.4 A logging infrastructure may need to handle more than 10,000 logs per second.

Which two options support a dedicated log collector function? (Choose two)

A. Panorama virtual appliance on ESX(i) only

B. M-500

C. M-100 with Panorama installed

D. M-100

Answer: BD

NO.5 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

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/map-ip-addresses-to-users.html#id61f141da-8b89-49c9-b34a-ed11b434d1db

NO.6 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

Explanation:

In a Layer 2 deployment, the firewall provides switching between two or more interfaces. Each group of interfaces must be assigned to a VLAN object in order for the firewall to switch between them.

In a Layer 3 deployment, the firewall routes traffic between ports. An IP address must be assigned to each interface and a virtual router must be defined to route the traffic. Choose this option when routing is required.

NO.7 The IT department has received complaints abou VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter.

Which feature can be used to identify, in real time, the applications taking up the most bandwidth?

A. QoS Statistics

B. Applications Report

C. Application Command Center (ACC)

D. QoS Log

Answer: C

Explanation:

Network Activity

Displays an overview of traffic and user activity on your network including:

Top applications in use

Top users who generate traffic (with a drill down into the bytes, content, threats or URLs accessed by the user) Most used security rules against which traffic matches occur In addition, you can also view network activity by source or destination zone, region, or IP address, ingress or egress interfaces, and GlobalProtect host information such as the operating systems of the devices most commonly used on the network.

NO.8 A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?

A. Blocked Activity

B. Bandwidth Activity

C. Threat Activity

D. Network Activity

Answer: D

Explanation:

The Network Activity tab of the Application Command Center (ACC) displays an overview of traffic and user activity on your network including:
Top applications in use
Top users who generate traffic (with a drill down into the bytes, content, threats or URLs accessed by the user) Most used security rules against which traffic matches occur In addition, you can also view network activity by source or destination zone, region, or IP address, ingress or egress interfaces, and GlobalProtect host information such as the operating systems of the devices most commonly used on the network.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/acc/acc-tabs

NO.9 Which three options does the WF-500 appliance support for local analysis? (Choose three)
A. E-mail links
B. APK files
C. jar files
D. PNG files
E. Portable Executable (PE) files
Answer: ACE
Explanation:

File Types Supported for Analysis	WildFire Global Cloud	WildFire Europe Cloud	WildFire Japan Cloud	WildFire Singapore Cloud	WildFire Private Cloud (WF-500 appliance)
Links contained in emails	✓	✓	✓	✓	✓
Android application package (APK) files	✓	✓	✓	✓	–
Adobe Flash files	✓	✓	✓	✓	✓
Java Archive (JAR) files	✓	✓	✓	✓	✓
Microsoft Office files	✓	✓	✓	✓	✓
Portable executable (PE) files	✓	✓	✓	✓	✓
Portable document format (PDF) files	✓	✓	✓	✓	✓
Mac OS X files	✓	✓	✓	✓	–
Archive (RAR and 7z) files	✓	✓	✓	✓	–

NO.10 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

Explanation:
Create a Custom Application with a signature and attach it to a security policy, or create a custom application and define an application override policy--A custom application allows you to customize

the definition of the internal application--its characteristics, category and sub-category, risk, port, timeout--and exercise granular policy control in order to minimize the range of unidentified traffic on your network. Creating a custom application also allows you to correctly identify the application in the ACC and traffic logs and is useful in auditing/reporting on the applications on your network. For a custom application you can specify a signature and a pattern that uniquely identifies the application and attach it to a security policy that allows or denies the application.
Alternatively, if you would like the firewall to process the custom application using fast path (Layer-4 inspection instead of using App-ID for Layer-7 inspection), you can reference the custom application in an application override policy rule. An application override with a custom application will prevent the session from being processed by the App-ID engine, which is a Layer-7 inspection. Instead it forces the firewall to handle the session as a regular stateful inspection firewall at Layer-4, and thereby saves application processing time.
For example, if you build a custom application that triggers on a host header www.mywebsite.com, the packets are first identified as web-browsing and then are matched as your custom application (whose parent application is web-browsing). Because the parent application is web-browsing, the custom application is inspected at Layer-7 and scanned for content and vulnerabilities.
If you define an application override, the firewall stops processing at Layer-4. The custom application name is assigned to the session to help identify it in the logs, and the traffic is not scanned for threats.
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/manage-custom-or- unknown-applications.html#id74b58a78-164f-4dc5-aa4e-31ce62f2af0d

NO.11 After pushing a security policy from Panorama to a PA-3020 firewall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

A. A Server Profile has not been configured for logging to this Panorama device.

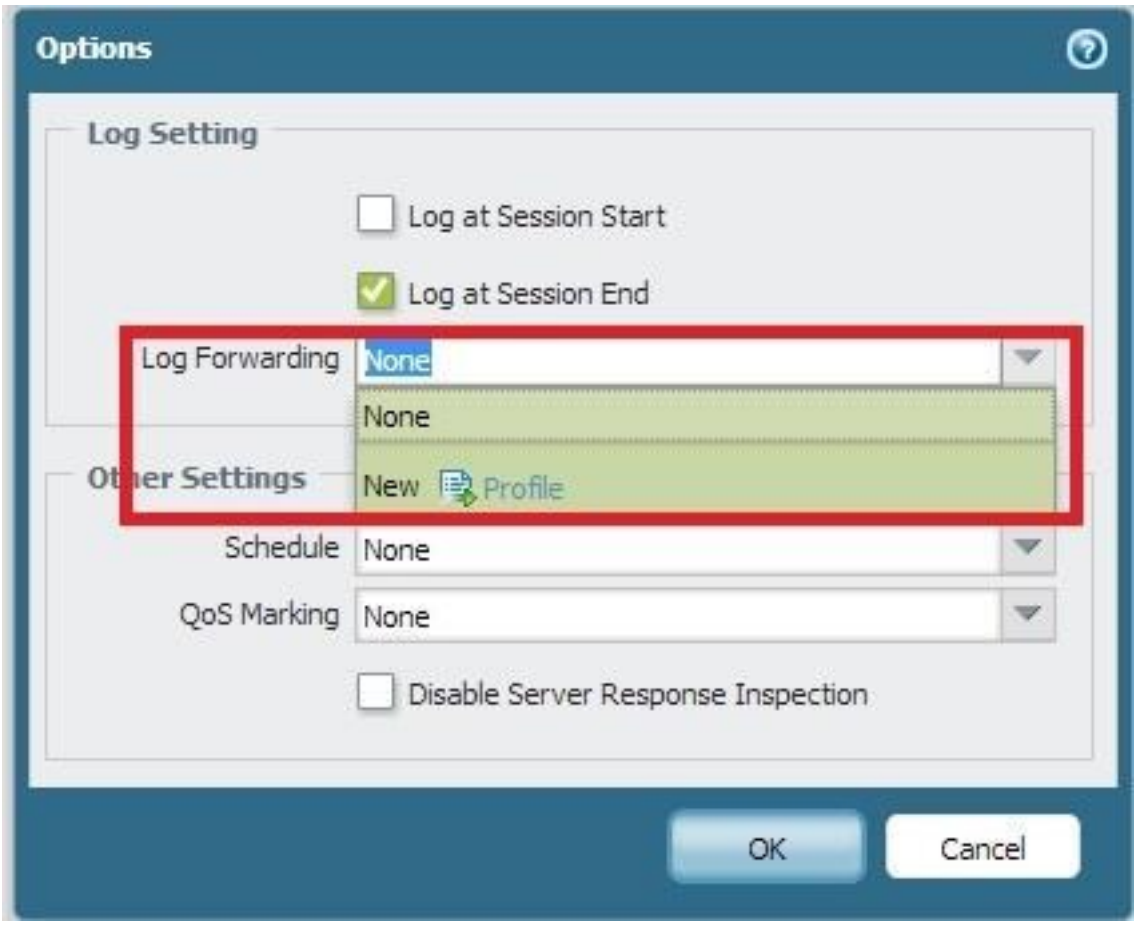
B. Panorama is not licensed to receive logs from this particular firewall.

C. The firewall is not licensed for logging to this Panorama device.

D. None of the firewall's policies have been assigned a Log Forwarding profile

Answer: D

Explanation:
In order to see entries in the Panorama Monitor > Traffic or Monitor > Log screens, a profile must be created on the Palo Alto Networks device (or pushed from Panorama) to forward log traffic to Panorama.
Steps:
1. Go to Policies > Security and open the Options for a rule.
2. Under Log Setting, select New for Log Forwarding to create a new forwarding profile:



Etc.
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Create-a-Profile-to-Forward-Logs-to-Panorama/ta-p/54038

NO.12 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 perimeter 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
Explanation:
Starting with PAN-OS 6.0, DNS sinkhole is an action that can be enabled in Anti-Spyware profiles. A DNS sinkhole can be used to identify infected hosts on a protected network using DNS traffic in environments where the firewall can see the DNS query to a malicious URL.
The DNS sinkhole enables the Palo Alto Networks device to forge a response to a DNS query for a known malicious domain/URL and causes the malicious domain name to resolve to a definable IP address (fake IP) that is given to the client. If the client attempts to access the fake IP address and there is a security rule in place that blocks traffic to this IP, the information is recorded in the logs.

https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/ta-p/58891

NO.13 Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

A. The devices are pre-configured with a virtual wire pair out the first two interfaces.

B. The devices are licensed and ready for deployment.

C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.

D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.

E. The interfaces are pingable.

Answer: AC

Explanation:

https://popravak.wordpress.com/2014/07/31/initial-setup-of-palo-alto-networks-next-generation-firewall/

NO.14 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

NO.15 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

Explanation:

This document explains how to perform a fib lookup for a particular destination within a particular virtual router on a Palo Alto Networks firewall.

1. Select the desired virtual router from the list of virtual routers configured with the command:

> test routing fib-lookup virtual-router <value>

2. Specify a destination IP address:

> test routing fib-lookup virtual-router default ip <ip address>

https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Perform-FIB-Lookup-for-a- Particular -Destination/ta-p/52188

NO.16 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

Explanation:

E: For firewalls without dedicated HA ports, select two data interfaces for the HA2 link and the backup HA1 link. Then, use an Ethernet cable to connect these in-band HA interfaces across both firewalls.

Use the management port for the HA1 link and ensure that the management ports can connect to each other across your network.

B:

1. In Device > High Availability > General, edit the Control Link (HA1) section.
2. Select the interface that you have cabled for use as the HA1 link in the Port drop down menu.

Set the IP address and netmask. Enter a Gateway IP address only if the HA1 interfaces are on separate subnets. Do not add a gateway if the devices are directly connected.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/set-up- activepassive -ha/configure-activepassive-ha

NO.17 What are three valid actions in a File Blocking Profile? (Choose three)

A. Forward

B. Block

C. Alret

D. Upload

E. Reset-both

F. Continue

Answer: BCF

Explanation:

You can configure a file blocking profile with the following actions:

* Forward - When the specified file type is detected, the file is sent to WildFire for analysis. A log is also generated in the data filtering log.
* Block - When the specified file type is detected, the file is blocked and a customizable block page is presented to the user. A log is also generated in the data filtering log.
* Alert - When the specified file type is detected, a log is generated in the data filtering log.
* Continue - When the specified file type is detected, a customizable response page is presented to the user. The user can click through the page to download the file. A log is also generated in the data filtering log. Because this type of forwarding action requires user interaction, it is only applicable for web traffic.
* Continue-and-forward - When the specified file type is detected, a customizable continuation page is presented to the user. The user can click through the page to download the file. If the user clicks through the continue page to download the file, the file is sent to WildFire for analysis.

A log is also generated in the data filtering log.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/set-up-file-blocking

NO.18 An Administrator is configuring an IPSec VPN toa Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is th output from the command:

```
less mp-log ikemgr.log:

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

What could be the cause of this problem?

A. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.

B. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.

C. The shared secrets do not match between the Palo Alto firewall and the ASA

D. The deed peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

Answer: A

Explanation:

IF ERROR IS THIS:	TRY THIS:
IKE phase-1 negotiation is failed as initiator, main mode. Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout. or IKE phase 1 negotiation is failed. Couldn't find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]	• Verify that the public IP address for each VPN peer is accurate in the IKE Gateway configuration. • Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure.

https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/troubleshooting/test- vpn-connectivity

NO.19 Which interface configuration will accept specific VLAN IDs?

A. Tab Mode

B. Subinterface

C. Access Interface

D. Trunk Interface

Answer: B

Explanation:

You can only assign a single VLAN to a subinterface, and not to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic.

http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/intrface.html

NO.20 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
Explanation:
C: PAN-DB categorizes URLs based on their content at the domain, file and page level, and receives updates from WildFire cloud-based malware analysis environment every 30 minutes to make sure that, when web content changes, so do categorizations. This continuous feedback loop enables you to keep pace with the rapidly changing nature of the web, automatically.
D: DNS is a very necessary and ubiquitous application, as such, it is a very commonly abused protocol for command-and-control and data exfiltration. This tech brief summarizes the DNS classification, inspection and protection capabilities supported by our next-generation security platform, which includes:
1. Malformed DNS messages (symptomatic of vulnerability exploitation attack).
2. DNS responses with suspicious composition (abused query types, DNS-based denial of service attacks).
3. DNS queries for known malicious domains. Our ability to prevent threats from hiding within DNS
The passive DNS network feature allows you to opt-in to share anonymized DNS query and response data with our global passive DNS network. The data is continuously mined to discover malicious domains that are then added to the PAN-OS DNS signature set that is delivered daily, enabling timely detection of compromised hosts within the network and the disruption of command-and-control channels that rely on name resolution.

NO.21 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
Explanation:
B: There are two DoS protection mechanisms that the Palo Alto Networks firewalls support.
* Flood Protection - Detects and prevents attacks where the network is flooded with packets resulting in too many half-open sessions and/or services being unable to respond to each request. In this case the source address of the attack is usually spoofed.
* Resource Protection - Detects and prevent session exhaustion attacks. In this type of attack, a large number of hosts (bots) are used to establish as many fully established sessions as possible to consume all of a system's resources.
You can enable both types of protection mechanisms in a single DoS protection profile.
D: Provides additional protection between specific network zones in order to protect the zones against attack. The profile must be applied to the entire zone, so it is important to carefully test the

profiles in order to prevent issues that may arise with the normal traffic traversing the zones.
When defining packets per second (pps) thresholds limits for zone protection profiles, the threshold is based on the packets per second that do not match a previously established session.
Incorrect Answers:
A: Vulnerability protection stops attempts to exploit system flaws or gain unauthorized access to systems. For example, this feature will protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.
C: Data Filtering helps to prevent sensitive information such as credit card or social security numbers from leaving a protected network.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/security-profiles

NO.22 A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured.
What can be the cause of this problem?
A. No Zone has been configured on Ethernet 1/4.
B. Interface Ethernet 1/1 is in Virtual Wire Mode.
C. DNS has not been properly configured on the firewall.
D. DNS has not been properly configured on the host.
Answer: A

NO.23 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

NO.24 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
Explanation:
You can check global counters for a specific source and destination IP addresses by setting a packet filter. We recommend that you use the global counter command with a packet filter to get specific traffic outputs. These outputs will help isolate the issue between two peers.
Use the following CLI command to show when traffic is passing through the Palo Alto Networks

firewall from that source to destination.
> show counter global filter packet-filter yes delta yes
Global counters:
Elapsed time since last sampling: 20.220 seconds
name value rate severity category aspect description
---------- pkt_recv 6387398 4 info packet pktproc Packets received pkt_recv_zero 370391 0 info packet pktproc Packets received from QoS 0 Etc.
https://live.paloaltonetworks.com/t5/Management-Articles/How-to-check-global-counters-for-a-specific-source-and/ta-p/65794

NO.25 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

NO.26 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
Explanation:
Licenses for the VM-Series NSX Edition Firewall
In order to automate the provisioning and licensing of the VM-Series NSX Edition firewall in the VMware integrated NSX solution, two license bundles are available:
One bundle includes the VM-Series capacity license (VM-1000-HV only), Threat Prevention license and a premium support entitlement.
Another bundle includes the VM-Series capacity license (VM-1000-HV only) with the complete suite of licenses that include Threat Prevention, GlobalProtect, WildFire, PAN-DB URL Filtering, and a premium support entitlement.

NO.27 A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?
A. The two devices must share a routable floating IP address
B. The two devices may be different models within the PA-5000 series
C. The HA1 IP address from each peer must be on a different subnet
D. The management port may be used for a backup control connection
Answer: D
Explanation:
Set up the backup control link connection.
1. In Device > High Availability > General, edit the Control Link (HA1 Backup) section.

2. Select the HA1 backup interface and set the IPv4/IPv6 Address and Netmask.
Note: Use the management port for the HA1 link.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/set-up- activepassive -ha/configure-activepassive-ha

NO.28 What must be used in Security Policy Rule that contain addresses where NAT policy applies?
A. Pre-NAT addresse and Pre-NAT zones
B. Post-NAT addresse and Post-Nat zones
C. Pre-NAT addresse and Post-Nat zones
D. Post-Nat addresses and Pre-NAT zones
Answer: C
Explanation:
NAT Policy Rule Functionality
Upon ingress, the firewall inspects the packet and does a route lookup to determine the egress interface and zone. Then the firewall determines if the packet matches one of the NAT rules that have been defined, based on source and/or destination zone. It then evaluates and applies any security policies that match the packet based on the original (pre-NAT) source and destination addresses, but the post-NAT zones.
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/nat/nat-policy-rules/nat-policy-overview

NO.29 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.

		Source			Destination						
	Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	rule1	Trust-L3	any	any	UnTrust-L3	any	Known Good	application-default			
2	rule2	Trust-L3	any	any	UnTrust-L3	any	Known Bad	any		none	
3	rule3	Trust-L3	any	any	UnTrust-L3	any	any	any		none	

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: AD

NO.30 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
Explanation:

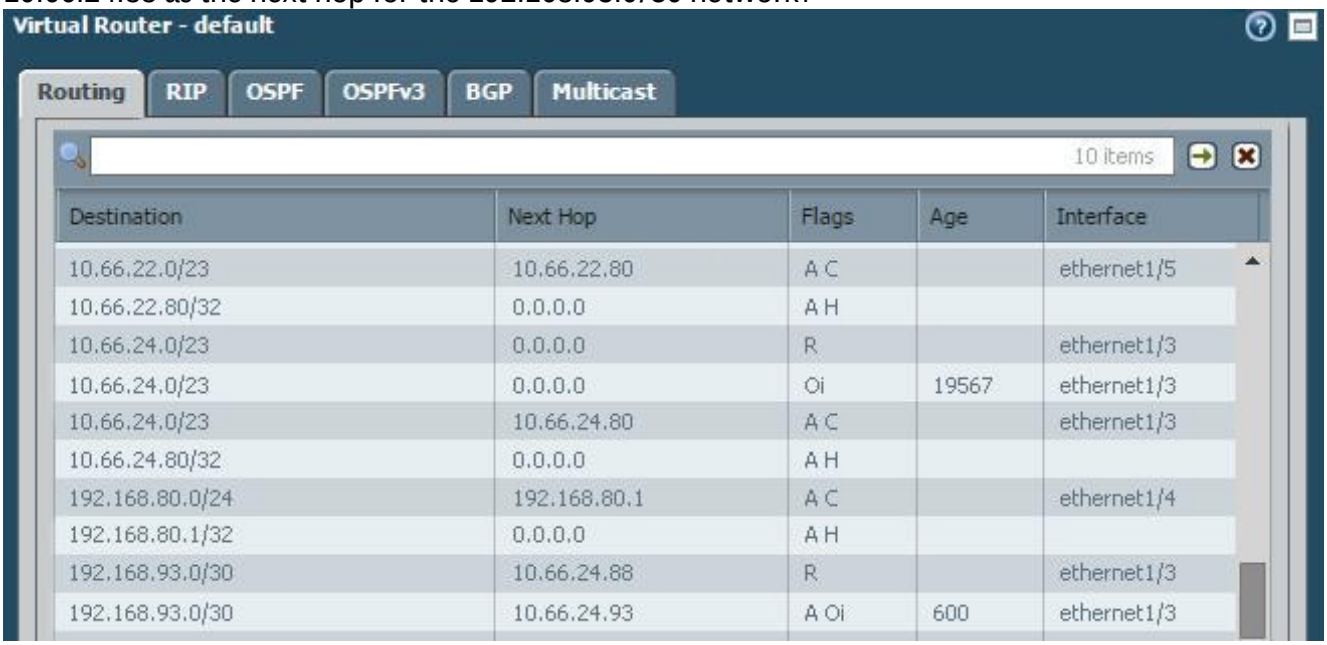
Configure the service routes.
1. Select Device > Setup > Services > Global and click Service Route Configuration.
Note: For the purposes of activating your licenses and getting the most recent content and software updates, you will want to change the service route for DNS, Palo Alto Updates, URL Updates, WildFire, and AutoFocus.
2. Click the Customize radio button, and select one of the following:
For a predefined service, select IPv4 or IPv6 and click the link for the service for which you want to modify the Source Interface and select the interface you just configured.

NO.31 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
Explanation:
Step 1: Configure a DoS Protection profile for flood protection.
1. Select Objects > Security Profiles > DoS Protection and Add a profile Name.
2. Select Classified as the Type.
3. For Flood Protection, select the check boxes for all of the following types of flood protection:
* SYN Flood
* UDP Flood
* ICMP Flood
* ICMPv6 Flood
* Other IP Flood
Step 2: Configure a DoS Protection policy rule that specifies the criteria for matching the incoming traffic.
This step include: (Optional) For Destination Address, select Any or enter the IP address of the device you want to protect.

NO.32 Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?
A. Disable Server Response Inspection
B. Apply an Application Override
C. Disable HIP Profile
D. Add server IP Security Policy exception
Answer: A
Explanation:
In the Other Settings section, select the option to Disable Server Response Inspection. This setting disables the antivirus and anti-spyware scanning on the server-side responses, and thus reduces the load on the firewall.

NO.33 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: BCF
Explanation:
Using the URL Category as match criteria allows you to customize security profiles (antivirus, anti-spyware, vulnerability, file-blocking, Data Filtering, and DoS) on a per-URL-category basis.

NO.34 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
Explanation:
The best route is then selected among them based on Administrative Distance (AD) value of routing protocols which routes came from and that route is marked with flag A, stating that it is the Active route.
Administrative distance (AD) is an arbitrary numerical value assigned to dynamic routes, static routes and directly-connected routes. The value is used by vendor-specific routers to rank routes from most preferred to least preferred. When multiple paths to the same destination are available, the router uses the route with the lowest administrative distance and inserts the preferred route into its routing table.

https://live.paloaltonetworks.com/t5/Management-Articles/Routing-Table-has-Multiple-Prefixes- for -the-Same-Route/ta-p/54781

NO.35 A company hosts a publically 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 be NAT policy contain to allow users in the untrust-L3 zone to access the web server? (Choose two)

A. Untrust-L3 for both Source and Destination zone

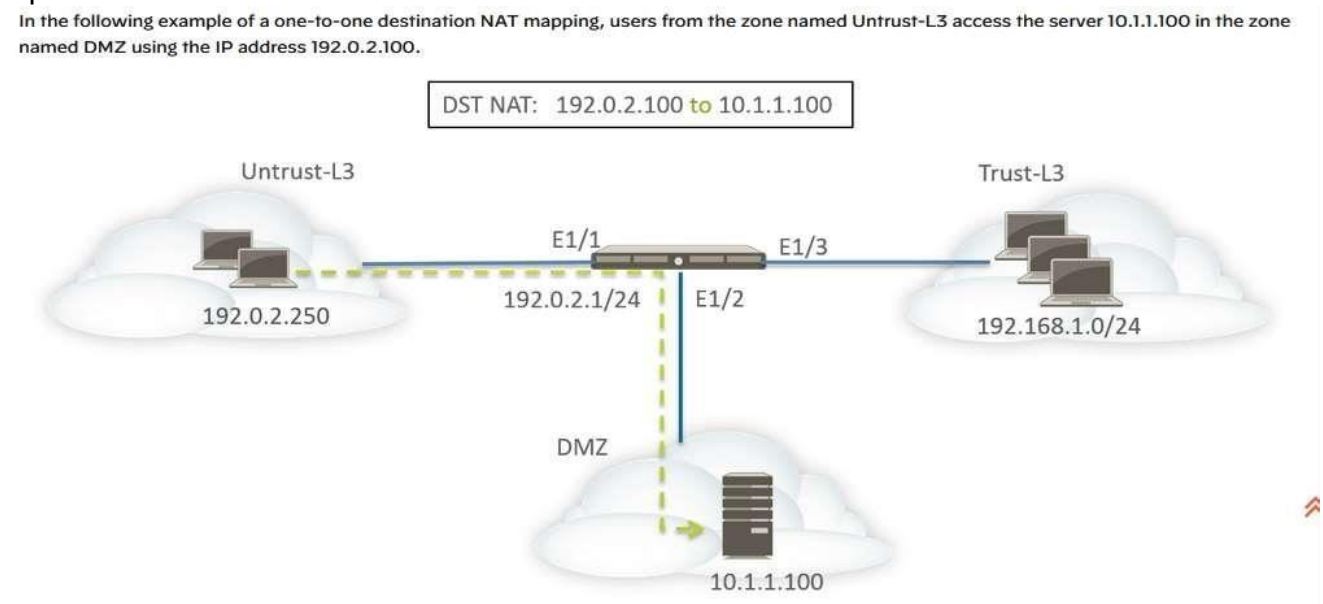
B. Destination IP of 192.168.1.10

C. Untrust-L3 for Source Zone and Trust-L3 for Destination Zone

D. Destination IP of 23.54.6.10

Answer: AD

Explanation:



Before configuring the NAT rules, consider the sequence of events for this scenario.
Host 192.0.2.250 sends an ARP request for the address 192.0.2.100 (the public address of the destination server).
The firewall receives the ARP request packet for destination 192.0.2.100 on the Ethernet1/1 interface and processes the request. The firewall responds to the ARP request with its own MAC address because of the destination NAT rule configured.
The NAT rules are evaluated for a match. For the destination IP address to be translated, a destination NAT rule from zone Untrust-L3 to zone Untrust-L3 must be created to translate the destination IP of 192.0.2.100 to 10.1.1.100.
After determining the translated address, the firewall performs a route lookup for destination 10.1.1.100 to determine the egress interface. In this example, the egress interface is Ethernet1/2 in zone DMZ.
The firewall performs a security policy lookup to see if the traffic is permitted from zone Untrust- L3 to DMZ.

The direction of the policy matches the ingress zone and the zone where the server is physically located.
The security policy refers to the IP address in the original packet, which has a destination address of 192.0.2.100.

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private

The direction of the NAT rules is based on the result of route lookup.

The configured security policy to provide access to the server from the Untrust-L3 zone would look like this:

	Source		Destination						
NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	