EndExam
QUESTION & ANSWER

Accurate study guides, High passing rate!

Exam :   **PCNSE**

Title :   Palo Alto Networks Certified Network Security Engineer Exam

Version :   DEMO

1.A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config.
The contents of init-cfg txt in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command:> request resort system Upon restart, the firewall fails to begin the bootstrapping process. The failure is caused because
A. Firewall must be in factory default state or have all private data deleted for bootstrapping
B. The hostname is a required parameter, but it is missing in init-cfg txt
C. The USB must be formatted using the ext3 file system, FAT32 is not supported
D. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x
E. The bootstrap.xml file is a required file but it is missing
Answer: C
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive.html#id8378007f-d6e5-4f2d-84a4-5d50b0b3ad7d

2.Where is information about packet buffer protection logged?
A. Alert entries are in the Alarms log. Entries for dropped traffic, discarded sessions, and blocked IP address are in the Threat log
B. All entries are in the System log
C. Alert entries are in the System log. Entries for dropped traffic, discarded sessions and blocked IP addresses are in the Threat log
D. All entries are in the Alarms log
Answer: D
Explanation:

WHICH SYSTEM LOGS AND THREAT LOGS ARE GENERATED WHEN PACKET BUFFER PROTECTION

Created On 10/29/19 15:51 PM - Last Modified 04/27/20 22:13 PM

ZONE PROTECTION **ZONE AND DOS PROTECTION** **8.1** **8.0** **9.0** **HARDWARE**

Question
Which system logs and threat logs are generated when packet buffer protection is enabled?

Environment
- PAN-OS 8.x
- PBP

Answer
The firewall records alert events in the System log and events for dropped traffic, discarded sessions, and blocked IP address in the Threat log.
- System logs:

Logs:
Monitor>System
Packet buffer congestion
Severity: informational

- Threat logs:

Graphical user interface, text, application
Description automatically generated

3.An engineer troubleshooting a VPN issue needs to manually initiate a VPN tunnel from the CLI.
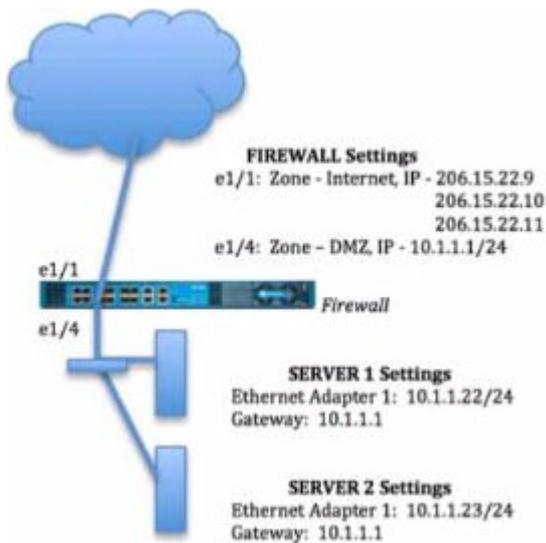Which CLI command can the engineer use?
A. test vpn flow
B. test vpn Ike—sa
C. test vpn tunnel
D. test vpn gateway
Answer: D
Explanation:
The engineer can use the test vpn gateway CLI command to manually initiate a VPN tunnel from the
CLI. This command allows the engineer to specify the name of the VPN gateway and the IP address of
the peer to initiate an IKE negotiation and establish a VPN tunnel. Option A is incorrect because test vpn
flow is not a valid CLI command. Option B is incorrect because test vpn ike-sa is a CLI command that
displays information about the IKE security associations, not initiates a VPN tunnel. Option C is incorrect
because test vpn tunnel is a CLI command that displays information about the IPSec security
associations, not initiates a VPN tunnel.

4.An administrator wants multiple web servers In the DMZ to receive connections initiated from the
internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22.

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

e1/1
Firewall
e1/4

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

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

Based on the image, which NAT rule will forward web-browsing traffic correctly?

A)
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP

B)
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

C)
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

D)
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP

A. Option

B. Option

C. Option

D. Option

Answer: B

Explanation:

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping.html

5.A company is using wireless controllers to authenticate users.

Which source should be used for User-ID mappings?

A. Syslog

B. XFF headers

C. server monitoring

D. client probing

Answer: A

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-overview