Team-9a

Inject: NETW10a

Denial of Service

1) Identify device and the configuration changes to implement this requirement.

– Palo Alto Firewall,

A) We can configure the Palo Alto Firewall to Monitor traffic and use tools such as intrusion detection systems.

B) We can also set up rate limiting which limits the number of requests that a single IP address can make to prevent overwhelming the network.

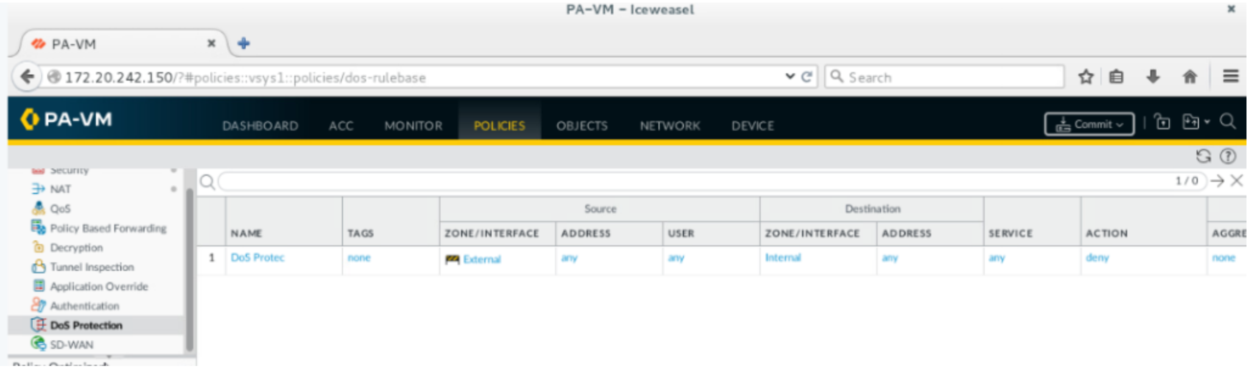
C) We can also Block IP address that have a history of attacking, or use IP reputation services to identify and block malicious IP addresses.

2) Explain the different types of DoS attacks that the configuration changes were designed to address.

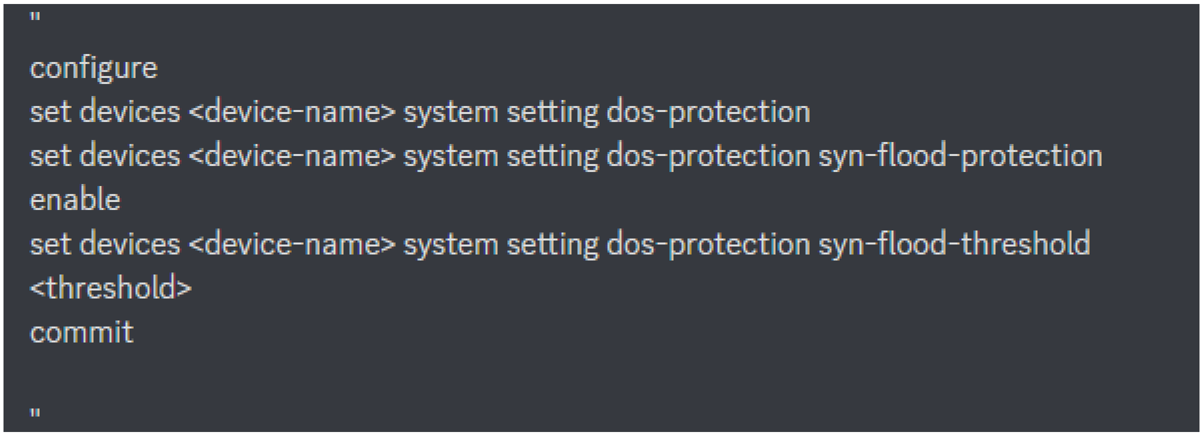
A) These configuration changes can stop Volume based DDoS Attacks that use a large amount of network traffic to overwhelm our network.

B) We can also stop Protocol Attacks that use specific protocols of our network that would be used to exploit specific vulnerabilities or misconfigurations.

3) Provide screenshots of the configuration commands or GUI Display.



			Source			Destination				
	NAME	TAGS	ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS	SERVICE	ACTION	AGGRE
1	DoS Protec	none	External	any	any	Internal	any	any	deny	none



```
"
configure
set devices <device-name> system setting dos-protection
set devices <device-name> system setting dos-protection syn-flood-protection
enable
set devices <device-name> system setting dos-protection syn-flood-threshold
<threshold>
commit

"
```