PCSFE$^{Q\&As}$

Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

Pass Palo Alto Networks PCSFE Exam with 100% Guarantee

QUESTION 1

When implementing active-active high availability (HA), which feature must be configured to allow the HA pair to share a single IP address that may be used as the network\\'s gateway IP address?

A. ARP load sharing

B. Floating IP address

C. HSRP

D. VRRP

Correct Answer: B

QUESTION 2

Which component scans for threats in allowed traffic?

A. Intelligent Traffic Offload

B. TLS decryption

C. Security profiles

D. NAT

Correct Answer: C

Explanation: Security profiles are the components that scan for threats in allowed traffic. Security profiles are sets of rules or settings that define how the firewall will inspect and handle traffic based on various threat prevention technologies, such as antivirus, anti- spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis. Security profiles can be applied to Security policy rules to enforce granular protection against known and unknown threats in allowed traffic. Intelligent Traffic Offload, TLS decryption, and NAT are not components that scan for threats in allowed traffic, but they are related features that can enhance security and performance. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Security Profiles Overview], [Threat Prevention Datasheet]

QUESTION 3

Which two mechanisms could trigger a high availability (HA) failover event? (Choose two.)

A. Heartbeat polling

B. Ping monitoring

C. Session polling

D. Link monitoring

Correct Answer: AD

Explanation: Heartbeat polling and link monitoring are two mechanisms that can trigger an HA failover event. Heartbeat polling is a method of verifying the health of the peer firewall by sending periodic heartbeat messages. If the heartbeat messages are not received within a specified interval, the firewall assumes that the peer is down and initiates a failover. Link monitoring is a method of verifying the connectivity of the interfaces on the firewall by sending link state packets. If the link state packets are not received on a specified number of interfaces, the firewall assumes that the network is down and initiates a failover. Ping monitoring and session polling are not HA mechanisms, but they are used for path monitoring and session synchronization respectively. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [Configure HA Link Monitoring], [Configure HA Path Monitoring], [Configure Session Synchronization]

QUESTION 4

Which offering can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication?

A. OCSP

B. Secure Sockets Layer (SSL) Inbound Inspection

C. Advanced URL Filtering (AURLF)

D. WildFire

Correct Answer: B

Explanation: Secure Sockets Layer (SSL) Inbound Inspection is the offering that can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication. SSL Inbound Inspection is a feature that allows the firewall to decrypt and inspect inbound SSL/TLS traffic from external clients to internal servers. SSL Inbound Inspection can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication by applying threat prevention technologies, such as antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis, to the decrypted traffic and blocking any malicious content or activity. OCSP, Advanced URL Filtering (AURLF), and WildFire are not offerings that can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication, but they are related solutions that can enhance security and visibility. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [SSL Inbound Inspection], [Threat Prevention Datasheet]

QUESTION 5

Which two public cloud platforms does the VM-Series plugin support? (Choose two.)

A. Azure

B. lIBM Cloud

C. Amazon Web Services

D. lOCI

Correct Answer: AC

Explanation: The two public cloud platforms that the VM-Series plugin supports are: Azure Amazon Web Services (AWS) A public cloud platform is a cloud computing service that provides infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS) to customers over the internet. A public cloud platform requires network security that can protect the traffic between different cloud services or regions from cyberattacks and enforce granular security policies based on application, user, content, and threat information. VM-Series firewall is a virtualized version of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms. VM-Series plugin is a software component that extends the functionality of the VM-Series firewall and Panorama to support specific features and capabilities of different cloud platforms. Azure and AWS are two public cloud platforms that the VM-Series plugin supports. Azure is a public cloud platform that provides a range of cloud services, such as compute, storage, networking, databases, analytics, artificial intelligence, and more. AWS is a public cloud platform that provides a range of cloud services, such as EC2, S3, VPC, Lambda, and more. The VM- Series plugin supports Azure and AWS by enabling features such as bootstrapping, dynamic address groups, scaling, load balancing, high availability, monitoring, logging, and automation for VM-Series firewalls and Panorama on these platforms. IBM Cloud and OCI are not public cloud platforms that the VM-Series plugin supports, but they are related platforms that can be used for other purposes. References: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [VM-Series Plugin Overview], [VM-Series Plugin for Azure], [VM-Series Plugin for AWS], [What is Azure?], [What is AWS?]