

Latest Version: 27.0

Question: 1

An administrator is building Security rules within a device group to block traffic to and from malicious locations

How should those rules be configured to ensure that they are evaluated with a high priority?

- A. Create the appropriate rules with a Block action and apply them at the top of the Default Rules
- B. Create the appropriate rules with a Block action and apply them at the top of the Security Post-Rules.
- C. Create the appropriate rules with a Block action and apply them at the top of the local firewall Security rules.
- D. Create the appropriate rules with a Block action and apply them at the top of the Security Pre-Rules

Answer: A

Question: 2

An engineer is in the planning stages of deploying User-ID in a diverse directory services environment. Which server OS platforms can be used for server monitoring with User-ID?

- A. Microsoft Terminal Server, Red Hat Linux, and Microsoft Active Directory
- B. Microsoft Active Directory, Red Hat Linux, and Microsoft Exchange
- C. Microsoft Exchange, Microsoft Active Directory, and Novell eDirectory
- D. Novell eDirectory, Microsoft Terminal Server, and Microsoft Active Directory

Answer: B

Question: 3

Your company has two Active Directory domain controllers spread across multiple WAN links. All users authenticate to Active Directory. Each link has substantial network bandwidth to support all mission-critical applications. The firewalls management plane is highly utilized.

Given this scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

- A. PAN-OS integrated agent
- B. Captive Portal
- C. Citrix terminal server agent with adequate data-plane resources
- D. Windows-based User-ID agent on a standalone server

Answer: A

Question: 4

A customer is replacing their legacy remote access VPN solution. The current solution is in place to secure only internet egress for the connected clients. Prisma Access has been selected to replace the current remote access VPN solution. During onboarding, the following options and licenses were selected and enabled:

- Prisma Access for Remote Networks 300Mbps
- Prisma Access for Mobile Users 1500 Users
- Cortex Data Lake 2TB
- Trusted Zones trust
- Untrusted Zones untrust
- Parent Device Group shared

How can you configure Prisma Access to provide the same level of access as the current VPN solution?

- A. Configure mobile users with trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
- B. Configure mobile users with a service connection and trust-to-trust Security policy rules to allow the desired traffic outbound to the internet
- C. Configure remote networks with a service connection and trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
- D. Configure remote networks with trust-to-trust Security policy rules to allow the desired traffic outbound to the internet

Answer: D

Question: 5

Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?

- A. Measure and monitor the CPU consumption of the firewall data plane to ensure that each firewall is properly sized to support DoS and zone protection
- B. Create a zone protection profile with flood protection configured to defend an entire egress zone against SYN, ICMP, ICMPv6, UDP, and other IP flood attacks
- C. Add a WildFire subscription to activate DoS and zone protection features
- D. Replace the hardware firewall because DoS and zone protection are not available with VM-Series systems

Answer: A

Explanation:

1 - <https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/dosand->

zone-protection-best-practices/deploy-dos-and-zone-protection-using-bestpractices.
html#:~:text=DoS%20and%20Zone%20Protection%20help,device%20at%20the%20internet%20
Perimeter.

2 - [https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dosprotection/
zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds/how-to-measure-
cps.html](https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dosprotection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds/how-to-measure-cps.html)

[https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dosprotection.
html](https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dosprotection.html)