

➤ **Vendor: Palo Alto Networks**

➤ **Exam Code: PCNSE**

➤ **Exam Name: Palo Alto Networks Certified Security Engineer (PCNSE)  
PAN-OS 10.0**

➤ **New Updated Questions from [Braindump2go](https://www.braindump2go.com) (Updated in [April / 2022](#))**

### **Visit Braindump2go and Download Full Version PCNSE Exam Dumps**

#### **QUESTION 460**

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 461**

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 462**

Your company has to 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 463**

**[PCNSE Exam Dumps](#) [PCNSE Exam Questions](#) [PCNSE PDF Dumps](#) [PCNSE VCE Dumps](#)**

**<https://www.braindump2go.com/pcnse.html>**

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 464**

What best describes the HA Promotion Hold Time?

- A. the time that is recommended to avoid an HA failover due to the occasional flapping of neighboring devices
- B. the time that is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously
- C. the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost
- D. the time that a passive firewall with a low device priority will wait before taking over as the active firewall if the firewall is operational again

**Answer: B**

#### **QUESTION 465**

During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons.

In this case, the technical reason is unsupported ciphers. Traffic to these sites will therefore be blocked if decrypted.

How should the engineer proceed?

- A. Allow the firewall to block the sites to improve the security posture
- B. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption
- C. Install the unsupported cipher into the firewall to allow the sites to be decrypted
- D. Create a Security policy to allow access to those sites

**Answer: A**

#### **QUESTION 466**

When using certificate authentication for firewall administration, which method is used for authorization?

- A. Radius
- B. LDAP
- C. Kerberos

D. Local

**Answer: C**

**QUESTION 467**

When you navigate to Network: > GlobalProtect > Portals > Method section, which three options are available? (Choose three )

- A. user-logon (always on)
- B. pre-logon then on-demand
- C. on-demand (manual user initiated connection)
- D. post-logon (always on)
- E. certificate-logon

**Answer: ACD**

**QUESTION 468**

An administrator analyzes the following portion of a VPN system log and notices the following issue "Received local id 10.10.1.4/24 type IPv4 address protocol 0 port 0, received remote id 10.1.10.4/24 type IPv4 address protocol 0 port 0." What is the cause of the issue?

- A. IPSec crypto profile mismatch
- B. IPSec protocol mismatch
- C. mismatched Proxy-IDs
- D. bad local and peer identification IP addresses in the IKE gateway

**Answer: C**

**QUESTION 469**

What is considered the best practice with regards to zone protection?

- A. Review DoS threat activity (ACC > Block Activity) and look for patterns of abuse
- B. Use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs
- C. If the levels of zone and DoS protection consume too many firewall resources, disable zone protection
- D. Set the Alarm Rate threshold for event-log messages to high severity or critical severity

**Answer: C**

**QUESTION 470**

An engineer wants to implement the Palo Alto Networks firewall in VWire mode on the internet gateway and wants to be sure of the functions that are supported on the vwire interface. What are three supported functions on the VWire interface? (Choose three )

- A. NAT
- B. QoS
- C. IPSec
- D. OSPF
- E. SSL Decryption

**Answer: ABC**

**QUESTION 471**

An administrator needs to build Security rules in a Device Group that allow traffic to specific users and groups defined

**[PCNSE Exam Dumps](#) [PCNSE Exam Questions](#) [PCNSE PDF Dumps](#) [PCNSE VCE Dumps](#)**

**<https://www.braindump2go.com/pcnse.html>**

in Active Directory.

What must be configured in order to select users and groups for those rules from Panorama?

- A. The Security rules must be targeted to a firewall in the device group and have Group Mapping configured
- B. A master device with Group Mapping configured must be set in the device group where the Security rules are configured
- C. User-ID Redistribution must be configured on Panorama to ensure that all firewalls have the same mappings
- D. A User-ID Certificate profile must be configured on Panorama

**Answer: D**

#### **QUESTION 472**

Which three use cases are valid reasons for requiring an Active/Active high availability deployment? (Choose three )

- A. The environment requires real, full-time redundancy from both firewalls at all times
- B. The environment requires Layer 2 interfaces in the deployment
- C. The environment requires that both firewalls maintain their own routing tables for faster dynamic routing protocol convergence
- D. The environment requires that all configuration must be fully synchronized between both members of the HA pair
- E. The environment requires that traffic be load-balanced across both firewalls to handle peak traffic spikes

**Answer: BCD**

#### **QUESTION 473**

Which protocol is supported by GlobalProtect Clientless VPN?

- A. HTTPS
- B. FTP
- C. RDP
- D. SSH

**Answer: C**

#### **QUESTION 474**

Cortex XDR notifies an administrator about grayware on the endpoints. There are no entries about grayware in any of the logs of the corresponding firewall.

Which setting can the administrator configure on the firewall to log grayware verdicts?

- A. within the log settings option in the Device tab
- B. within the log forwarding profile attached to the Security policy rule
- C. in WildFire General Settings, select "Report Grayware Files"
- D. in Threat General Settings, select "Report Grayware Files"

**Answer: D**

#### **QUESTION 475**

What would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain'?

- A. a Security policy with 'known-user' selected in the Source User field
- B. an Authentication policy with 'unknown' selected in the Source User field

- C. a Security policy with 'unknown' selected in the Source User field
- D. an Authentication policy with 'known-user' selected in the Source User field

**Answer:** A

**QUESTION 476**

Which statement is correct given the following message from the PanGPA log on the GlobalProtect app?

Failed to connect to server at port:4767

- A. The PanGPS process failed to connect to the PanGPA process on port 4767
- B. The GlobalProtect app failed to connect to the GlobalProtect Portal on port 4767
- C. The PanGPA process failed to connect to the PanGPS process on port 4767
- D. The GlobalProtect app failed to connect to the GlobalProtect Gateway on port 4767

**Answer:** D

**QUESTION 477**

Which GlobalProtect component must be configured to enable Clientless VPN?

- A. GlobalProtect satellite
- B. GlobalProtect app
- C. GlobalProtect portal
- D. GlobalProtect gateway

**Answer:** C

**Explanation:**

Creating the GlobalProtect portal is as simple as letting it know if you have accessed it already. A new gateway for accessing the GlobalProtect portal will appear. Client authentication can be used with an existing one.

<https://www.nstec.com/how-to-configure-clientless-vpn-in-palo-alto/#5>