Palo Alto Networks Certified Network Security Administrator (PCNSA) Exam Blueprint

Domain	Weight (%)
Device Management and Services	**22%**
Managing Objects	**20%**
Policy Evaluation and Management	**28%**
Securing Traffic	**30%**

Domain 1 Device Management and Services 22%

Task 1.1 Demonstrate knowledge of firewall management interfaces

- 1.1.1 Management interfaces
- 1.1.2 Methods of access
- 1.1.3 Access restrictions
- 1.1.4 Identity-management traffic flow
- 1.1.5 Management services
- 1.1.6 Service routes

Task 1.2 Provision local administrators

- 1.2.1 Authentication profile
- 1.2.2 Authentication sequence

Task 1.3 Assign role-based authentication

Task 1.4 Maintain firewall configurations

- 1.4.1 Running configuration
- 1.4.2 Candidate configuration
- 1.4.3 Discern when to use load, save, import, and export

1.4.4 Differentiate between configuration states

1.4.5 Back up Panorama configurations and firewalls from Panorama

Task 1.5 Push policy updates to Panorama-managed firewalls

1.5.1 Device groups and hierarchy

1.5.2 Where to place policies

1.5.3 Implications of Panorama management

1.5.4 Impact of templates, template stacks, and hierarchy

Task 1.6 Schedule and install dynamic updates

1.6.1 From Panorama

1.6.2 From the firewall

1.6.3 Scheduling and staggering updates on an HA pair

Task 1.7 Create and apply security zones to policies

1.7.1 Identify zone types

1.7.2 External types

1.7.3 Layer 2

1.7.4 Layer 3

1.7.5 TAP

1.7.6 VWire

1.7.7 Tunnel

Task 1.8 Identify and configure firewall interfaces

1.8.1 Different types of interfaces

1.8.2 How interface types affect Security policies

Task 1.9 Maintain and enhance the configuration of a virtual or logical router

1.9.1 Steps to create a static route

1.9.2 How to use the routing table

1.9.3 What interface types can be added to a virtual or logical router

1.9.4 How to configure route monitoring

Domain 2 Managing Objects 20%

Task 2.1 Create and maintain address and address group objects

2.1.1 How to tag objects

2.1.2 Differentiate between address objects

2.1.3 Static groups versus dynamic groups

Task 2.2 Create and maintain services and service groups

Task 2.3 Create and maintain external dynamic lists

Task 2.4 Configure and maintain application filters and application groups

2.4.1 When to use filters versus groups

2.4.2 The purpose of application characteristics as defined in the App-ID database

Domain 3 Policy Evaluation and Management 28%

Task 3.1 Develop the appropriate application-based Security policy

3.1.1 Create an appropriate App-ID rule

3.1.2 Rule shadowing

3.1.3 Group rules by tag

3.1.4 The potential impact of App-ID updates to existing Security policy rules

3.1.5 Policy usage statistics

Task 3.2 Differentiate specific security rule types

3.2.1 Interzone

3.2.2 Intrazone

3.2.3 Universal

Task 3.3 Configure Security policy match conditions, actions, and logging options

3.3.1 Application filters and groups

3.3.2 Logging options

3.3.3 App-ID

3.3.4 User-ID

3.3.5 Device-ID

3.3.6 Application filter in policy

3.3.7 Application group in policy

3.3.8 EDLs

Task 3.4 Identify and implement proper NAT policies

3.4.1 Destination

3.4.2 Source

Task 3.5 Optimize Security policies using appropriate tools

3.5.1 Policy test match tool

3.5.2 Policy Optimizer

Domain 4 Securing Traffic 30%

Task 4.1 Compare and contrast different types of Security profiles

4.1.1 Antivirus

4.1.2 Anti-Spyware

4.1.3 Vulnerability Protection

4.1.4 URL Filtering

4.1.5 WildFire Analysis

Task 4.2 Create, modify, add, and apply the appropriate Security profiles and groups

- 4.2.1 Antivirus
- 4.2.2 Anti-Spyware
- 4.2.3 Vulnerability Protection
- 4.2.4 URL Filtering
- 4.2.5 WildFire Analysis
- 4.2.6 Configure threat prevention policy

Task 4.3 Differentiate between Security profile actions

Task 4.4 Use information available in logs

- 4.4.1 Traffic
- 4.4.2 Threat
- 4.4.3 Data
- 4.4.4 System logs

Task 4.5 Enable DNS Security to control traffic based on domains

- 4.5.1 Configure DNS Security
- 4.5.2 Apply DNS Security in policy

Task 4.6 Create and deploy URL-filtering-based controls

- 4.6.1 Apply a URL profile in a Security policy
- 4.6.2 Create a URL Filtering profile
- 4.6.3 Create a custom URL category
- 4.6.4 Control traffic based on a URL category
- 4.6.5 Why a URL was blocked
- 4.6.6 How to allow a blocked URL
- 4.6.7 How to request a URL recategorization

Task 4.7 Differentiate between group mapping and IP-to-user mapping within policies and logs

4.7.1 How to control access to specific locations

4.7.2 How to apply to specific policies

4.7.3 Identify users within the ACC and the monitor tab