Welcome to the wonderful world of Palo Alto Networks Certification! We are very excited you have decided to embark upon such a valuable and worthwhile journey. To aid and support you on your quest we’ve put together this PCNSE6 Study Guide.

The best way to prepare for this certification exam is to have extensive experience with our Next-Generation hardware firewalls, VM-Series firewalls, the Panorama management environment, and GlobalProtect and the MSM mobile security platform. That experience should be in a wide variety of situations, including both large and small deployments, and in edge and datacenter deployments.

If your experience is incomplete, you should strongly consider attending our Essentials I (201), Essentials II (205), and Panorama (221) classes. They can’t cover everything that a PCNSE6 needs to know, but they’re the most efficient way to start learning. When you have the basics mastered, you should spend time on our platform practicing using the information in the 6.1 versions of the Administrator’s Guides.
PCNSE6 Topics and Learning Objectives

There are six main topics covered on the PCNSE6 exam, with each main topic having its own set of learning objectives.

I. Architecture and Design
   • Identify how Palo Alto Networks products work together to detect and prevent threats.
   • Given a business scenario, design a solution that uses the Palo Alto Networks security platform to meet the business requirements.
   • Evaluate high availability (HA) designs and configurations in various deployments.
   • Identify the appropriate interface type and configuration for a specified network deployment.

II. Core Concepts
   • Identify the advantages of Palo Alto Networks next-generation firewalls over traditional firewalls.
• Identify the key features of a Palo Alto Networks next-generation firewall and its advantages over a legacy layer-4 firewall.
• Based on the Palo Alto Networks packet flow architecture, determine the results of a policy evaluation.
• Given an attack scenario, identify the appropriate Palo Alto Networks threat-prevention component.
• Identify methods to map users to IP addresses and troubleshoot related issues.
• Identify the fundamental functions residing on the management and data planes of a Palo Alto Networks next-generation firewall.

III. Logs and Reports

• Identify considerations when configuring external log forwarding.
• Interpret log files, reports, and graphs to determine traffic trends and threat trends.
• Identify system and traffic issues using the Palo Alto Networks platform’s Web UI and CLI tools.

IV. Management

• Identify the required settings and steps necessary to provision and deploy a next-generation firewall.
• Determine how to leverage Panorama to centrally manage device configurations and logs.
• Given a technical scenario, explain the process needed to update a Palo Alto Networks system to the latest version of its code or content.
• Identify how configuration management operations are used to ensure operational integrity.
• Identify methods of authorization, authentication, and device administration.
• Identify the proper use of public key infrastructure components.

V. Networking

• Given a technical scenario, determine how to configure and troubleshoot interface components.
Identify the configuration requirements and troubleshooting options for IPv6 implementations.

Given a networking scenario, configure and troubleshoot routing.

Identify the configuration settings for remote and site-to-site VPN.

Identify ways to mitigate the issues associated with denial of service attacks and reconnaissance scans.

VI. Policies

- Identify the deployment, configuration, and management features of the security rule-base.
- Identify the deployment, configuration and management features of security profiles and options.
- Identify the deployment, configuration, and management features of the NAT rule-base.
- Identify the SSL decryption deployment strategies.
- Given a business scenario, identify proper methods of application override configuration and their uses.

Recommended Study per Learning Objective for Each Topic

For each of the six major sections of the exam, this section lists reading and reference materials that can guide your practice and study. Most of the reference materials are Palo Alto Networks Administrator’s Guides.

Some references come from Palo Alto Networks Education Services course materials; those materials sometimes provide a different explanation of concepts covered in the Admin Guides. Course materials are provided ONLY to people who attend an authorized presentation of the course.

I. Architecture and Design

1. Identify how Palo Alto Networks products work together to detect and prevent threats.
2. Given a business scenario, design a solution that uses the Palo Alto Networks security platform to meet the business requirements.
3. Evaluate high availability (HA) designs and configurations in various deployments.
4. Identify the appropriate interface type and configuration for a specified network deployment.
Recommended Study Materials for Architecture and Design:

- PAN-OS Admin Guide v.6.1
  - Enable Basic Threat Prevention Features
  - URL Filtering
  - BGP
  - User Mapping
  - HA Concepts – HA Links and Backup Links
  - HA Concepts – Device Priority and Preemption
  - Configure Active/Passive HA

- Panorama Administrator’s Guide v6.1
  - Manage Log Collection

- GlobalProtect Admin Guide
  - What Client OS Versions are supported with GlobalProtect?
  - Configure GlobalProtect Gateways
  - Setup the GlobalProtect Infrastructure

- VM-Series Deployment Guide PAN-OS 6.1
  - Setup a VM-Series NSX Edition Firewall
  - High Availability

- WildFire Admin Guide
  - WildFire Overview
  - About WildFire and Detailed Decision Flow
  - WildFire Report Contents
  - WildFire Concepts – Supported File Types
  - WildFire Report Contents

- Palo Alto Networks Website, Online Documentation and Knowledgebase
  - What is HA-Lite on PA-200 and VM-Series Firewalls? (DOC-3091)
  - Understanding and Configuring NAT Tech Note (DOC-1517)

- PAN-EDU-201 Essentials I Course
  - Basic Interface Configuration Module 3
  - Basic Content-ID - Module 6
  - Active/Passive High Availability Module 11

- PAN-EDU-205 Essentials II Course
  - Active/Active High Availability Module 9

II. Core Concepts

1. Identify the advantages of Palo Alto Networks next-generation firewalls over traditional firewalls.
2. Identify the key features of a Palo Alto Networks next-generation firewall and its advantages over a legacy layer-4 firewall.
3. Based on the Palo Alto Networks packet flow architecture, determine the results of a policy evaluation.
4. Given an attack scenario, identify the appropriate Palo Alto Networks threat-prevention component.
5. Identify methods to map users to IP addresses and troubleshoot related issues.
6. Identify the fundamental functions residing on the management and data planes of a Palo Alto Networks next-generation firewall.

**Recommended Study Materials for Core Concepts:**

- **PAN-OS 6.1 Admin Guide**
  - App-ID Overview
  - Decryption Overview
  - Security Policy
  - Security Profiles
    - Anti-Spyware Profiles
    - File Blocking Profiles
    - DoS Protection Profiles
    - Vulnerability Protection Profiles
    - Zone Protection Profiles
  - NAT Rules and Security Policies
  - Reports and Logging
    - Forward Logs to External Services
  - User-ID Overview
  - Map IP Addresses to Users
  - Quality of Service Overview
    - QoS Concepts
    - Configure QoS

- **Panorama Admin Guide version 6.1**
  - Manage Log Collection
  - Manage Device Groups

- **PAN-EDU-201 Essentials I Course**
  - Platforms and Architecture Module 1
  - Basic Interface Configuration Module 3
  - Security and NAT Policies Module 4
  - Basic App-ID Module 5
  - Basic Content-ID Module 6
  - Decryption Module 7
  - Basic User-ID Module 8

- **PAN-EDU-205 Essentials II Course**
  - App-ID: Custom Applications Module 2
  - Advanced Content-ID Module 3
  - Advanced User-ID Module 4
  - Quality of Service (QoS) Module 5
III. Logs and Reports
1. Identify considerations when configuring external log forwarding.
2. Interpret log files, reports, and graphs to determine traffic trends and threat trends.
3. Identify system and traffic issues using the Palo Alto Networks platform’s Web UI and CLI tools.

Recommended Study Materials for Logs and Reports:
- PAN-OS 6.1 Admin Guide
  - Device Management
    - Web Interface Access Privileges
    - Web Interface Administrator Access
  - Manage Log Collection
  - Reports and Logging
    - Monitor the Firewall
    - Syslog Field Descriptions
    - Forward Logs to External Services
    - Manage Reporting
  - Threat Prevention
    - Use DNS Queries to Identify Infected Hosts on the Network
  - Use the Application Command Center
- Palo Alto Networks Knowledgebase and Online Documentation
  - https://live.paloaltonetworks.com/docs/DOC-7088
  - https://live.paloaltonetworks.com/docs/DOC-1549
  - Common Event Format Configuration Guide PAN-OS 6.0
- Panorama Admin Guide version 6.1
  - Manage Log Collection
    - Enable Log Forwarding from Panorama to External Destinations
- PAN-OS Command Line Reference Guide v6.1
  - Operational Mode Commands
    - Show Session
- PAN-EDU-201 Essentials I Course
  - Monitoring and Reporting Module 6
- PAN-EDU 311 Advanced Troubleshooting Course
  - Tools Module 3

IV. Management
1. Identify the required settings and steps necessary to provision and deploy a next-generation firewall.
2. Determine how to leverage Panorama to centrally manage device configurations and logs.
3. Given a technical scenario, explain the process needed to update a Palo Alto Networks system to the latest version of its code or content.
4. Identify how configuration management operations are used to ensure operational integrity.
5. Identify methods of authorization, authentication, and device administration.
6. Identify the proper use of public key infrastructure components.

Recommended Study Materials for Management:

- PAN-OS Administrators Guide 6.1
  o Getting Started
    - Integrate the Firewall into your Management Network
    - Enable Basic Threat Prevention Features
  o Device Management
    - Manage Firewall Administrators
    - Management Interfaces
  o Certificate Management
    - Key Certificates
    - Certificate Revocation
  o Virtual Systems
    - Overview and Benefits of Virtual Systems
    - Platform Support and Licensing for Virtual Systems
    - Configure Virtual Systems
- Palo Alto Networks WildFire Admin Guide 6.1
  o WildFire Concepts
  o High Availability
  o Getting Started
- PAN-OS Firewall Inline Help Resource
  o Defining Virtual Systems
- PAN-OS Getting Started Guide 6.0
  o Prerequisites for Active/Passive HA
- PAN-OS Web Interface Reference Guide version 6.1
  o Appendix C
- Panorama Admin Guide version 6.1
  o Setup Panorama
  o Centralized Logging and Reporting
    - Managed Collectors and Collector Groups
  o Manage Firewalls
    - Manage Device Groups
  o Panorama Overview
    - Device Groups
  o Administer Panorama
Manage Configuration Backups

- PAN-EDU 201 Essentials I Course
  - Initial Configuration Module 2
  - Basic Content-ID Module 6
  - Decryption Module 7
- PAN-EDU 205 Essentials II Course
  - GlobalProtect Module 7
- PAN-EDU 221 Panorama Essentials Course
  - Log Collection Module 6

V. Networking
1. Given a technical scenario, determine how to configure and troubleshoot interface components.
2. Identify the configuration requirements and troubleshooting options for IPv6 implementations.
3. Given a networking scenario, configure and troubleshoot routing.
4. Identify the configuration settings for remote and site-to-site VPN.
5. Identify ways to mitigate the issues associated with denial of service attacks and reconnaissance scans.

Recommended Study Materials for Networking:
- PAN-OS Admin Guide version 6.1
  - Plan the Deployment
  - Create the Security Perimeter
  - Interface Deployments
  - About Security Policy
  - Configure Interfaces and Zones
  - Virtual Routes
  - NAT
  - Configure OSPF
  - Static Routes
  - Site-to-Site VPN with Static and Dynamic Routing
  - Networking
  - Virtual Routers
  - RIP
- Palo Alto Networks Online Technical Document, Online Knowledgebase and Resources
  - Designing Networks with Palo Alto Networks Firewalls – Tech Note: DOC-2561
  - Online Technical Documentation – DOC-6791
  - Application DDoS Mitigation – Tech Doc-7158
- GlobalProtect Administration Guide version 6.1
  - Configure GlobalProtect Gateways
VI. Policies

1. Identify the deployment, configuration, and management features of the security rule-base.
2. Identify the deployment, configuration and management features of security profiles and options.
3. Identify the deployment, configuration, and management features of the NAT rule-base.
4. Identify the SSL decryption deployment strategies.
5. Given a business scenario, identify proper methods of application override configuration and their uses.

Recommended Study Materials for Policies:

- PAN-OS Admin Guide version 6.1
  - Reports and Logging
    - Forward Logs to External Services
  - URL Filtering Overview
    - URL Filtering Profile Actions
  - Networking
    - NAT
  - Threat Prevention
    - Use DNS Queries to Identify Infected Hosts on the Network
    - Prevent Brute Force Attacks
  - App-ID
    - Disable the SIP Application-Level Gateway (ALG)
    - Manage Custom or Unknown Applications
  - Network Integration
  - Policy
    - Security Profiles
      - Antivirus Profiles
    - File Blocking Profiles
    - Certificate Management
      - Keys and Certificates
Sample Questions for Each Main Topic

Here are two sample questions from each of the six domains above to give you an idea as to what you’ll encounter on the exam. The answers to all of the sample questions can be found in the Answers to Sample Questions section of this document below.

I. Architecture and Design

Sample Question 1:
A client downloads a malicious file from the Internet. The Palo Alto firewall has a valid WildFire subscription. The following Security
Policy rule matches the client HTTP session:

Which three actions take place when the firewall's Content-ID engine detects a virus in the file and the decoder action is set to block?

A. A threat log entry is generated.
B. A file is received by the client.
C. The file download is terminated.
D. A Data Filtering log entry is generated.
E. The client receives a block page.
F. The file and session information is sent to WildFire.

Sample question 2:
Which Interface Type can be used to manage a firewall via SSH or HTTPS?

A. HA
B. Tap
C. Layer2
D. Layer3
E. Virtual Wire

II. Core Concepts

**Sample question 1:**
When would there be a benefit from the creation of a custom application signature?

A. When the application can be used to send and receive malware
B. When the ability of an application to port hop needs to be eliminated
C. When the risk level of a Palo Alto Networks-provided application signature needs to be changed
D. When a company wants to know, and perhaps restrict, who is watching World Cup soccer matches during work hours

**Sample question 2:**
Given the following Security Policy and information about traffic traversing the firewall:

```
Source Address: 192.168.64.10  
Source Zone: Trust-L3  
Destination Address: 199.167.55.50  
Destination Zone: Untrust-L3  
Destination port: 85  
Application: web-browsing
```

Which rule will match the specified traffic?

A. Rule number 2  
B. Rule number 3  
C. Rule number 4  
D. Rule number 6
III. Logs and Reports

**Sample question 1:**
Which CLI command would allow an administrator to assess CPU usage by process on the management plane?

A. show process list
B. show system resources
C. show system statistics
D. show running resource monitor

**Sample question 2:**
Which statement is true about how Palo Alto Networks firewalls monitor traffic on the network?

A. Palo Alto Networks firewalls use Content-ID to examine the content of traffic to identify applications in logs and reports.
B. Traffic logs are generated by policies that have "deny" defined as their action, and will not log any traffic that match policies configured to "allow".
C. Unlike traditional firewalls that use port or protocol to identify applications, the Palo Alto Networks firewalls use the Application Override Rules to identify and monitor applications.
D. Unlike traditional firewalls that use port or protocol to identify applications, the Palo Alto Networks firewalls use the application signature (the App-ID technology) to identify applications.

IV. Management

**Sample question 1:**
What can be used to push Network and Device configurations from Panorama to firewalls running PAN-OS?

A. Templates
B. Device Groups
C. Service Profiles
D. Management Groups

**Sample question 2:**
Put the activities in the order they are performed when provisioning a new Palo Alto Networks firewall.
1. 1st Activity  
2. 2nd Activity  
3. 3rd Activity  
4. 4th Activity

V. Networking

**Sample question 1:**
Which statement is true of an OSPFv3 configuration on the Palo Alto Networks firewall?

A. It requires MD5 authentication.  
B. It uses IPv4 addresses for the area ID.  
C. It is enabled per-subnet instead of per-link.  
D. It supports dynamic interfaces such as DHCP.

**Sample question 2:**
Given the following routing table:

Which nexthop(s) would be added to the Forwarding Information Base (FIB) for the 192.168.93.0/30 network?
VI. Policies

Sample question 1:
What is the order of precedence in which Panorama and Locally-configured rules will be evaluated?

A. Locally-configured Rules, Device Group Pre Rules, Device Group Post Rules, Shared Pre Rules, Shared Post Rules
B. Shared Pre Rules, Shared Post Rules, Device Group Pre Rules, Device Group Post Rules, Locally-configured Rules
C. Shared Pre Rules, Device Group Pre Rules, Locally-configured Rules, Device Group Post Rules, Shared Post Rules
D. Device Group Pre Rules, Shared Pre Rules, Locally-configured Rules, Shared Post Rules, Device Group Post Rules

Sample question 2:
A company has a Palo Alto Networks firewall configured with the following three zones:

Internet
DMZ
Inside

All users are located on the Inside zone and are using public DNS servers for name resolution. The company hosts a Publicly-accessible web application on a server in the DMZ zone.

Which NAT rule configuration will allow users on the Inside zone to access the web application using its public IP address?

A. Bi-directional NAT
B. Two zone U-turn NAT
C. Three zone U-turn NAT
D. Explicit No-NAT Policy Rule
More Exam Facts and Details You Should Know

The PCNSE6 certification indicates the holder is capable of designing, deploying, configuring, maintaining, and troubleshooting the vast majority of Palo Alto Networks-based network security implementations. PCNSE6 candidates can be anyone who uses Palo Alto Networks products, including customers, partners, system engineers, systems integrators, and support engineers.

This formal certification exam is hosted and proctored by the third-party testing company Kryterion and can be taken by anyone who is prepared to demonstrate a deep understanding of Palo Alto Networks technologies. This proctored exam is offered through Kryterion in over 100 countries worldwide. To find your nearest location, and to register for your PCNSE6 exam, login to our registration site here: Palo Alto Networks PCNSE6 Registration. The cost to take the proctored PCNSE6 exam is USD$160.

The PCNSE6 exam is comprised of 60 questions delivered in multiple-choice and multiple list & match format. The allotted time for the exam is 1.5 hours (90 minutes).

It should be noted that the PCNSE6 certification exam is scored only on a Pass or Fail basis. No number scoring or percentage rating is given. Upon completion of the exam you will receive either a “Pass” or “Fail” rating based upon how well you did on the exam. Should you receive a “Fail” rating we will provide you a list of areas in which you appeared to be weakest.

The PCNSE6 Certification does not expire. However, if you wish to keep current with each PAN-OS release, you will be required to pass the certification exam for that specific release. For instance, after the release of PAN-OS 7.0 you will need to pass the PCNSE7 Certification exam to stay current.

Answers to Sample Questions:

Architecture and Design:
Question 1 Answer: ACE
Question 2 Answer: D- Layer 3
Core Concepts:
Question 1 Answer: D
Question 2 Answer: Rule number 3

Logs and Reports:
Question 1 Answer: B-show system resources
Question 2 Answer: D

Management:
Question 1 Answer: A-Templates
Question 2 Answer: 1=D, 2=C, 3=B, 4=A

Networking:
Question 1 Answer: B-It uses IPv4 addresses for the area ID.
Question 2 Answer: C-10.66.24.93

Policies:
Question 1 Answer: C
Question 2 Answer: C-Three Zone U-turn NAT

Terms and Acronyms:
Below is a list of terms, acronyms, and concepts you are likely to encounter when working with the Palo Alto Networks platform. Each item includes either a definition of the term, or some key characteristic about it. Familiarity with these concepts and their use in Palo Alto Networks deployments will help you do what a PCNSE6 must be able to do.


A/A HA – Active/Active High Availability. For redundancy, the firewall can be deployed in an active/active high availability (HA) configuration. When configured in HA, the HA peers mirror each other in configuration.

A/P HA – Active/Passive High Availability. For redundancy, the firewall can be deployed in an active/passive high availability (HA) configuration. When configured in HA, the HA peers mirror each other in configuration.

Address Object – An Address Object can include an IPv4 or IPv6 address (single IP, range, subnet) or a FQDN. It allows you to reuse the same object as a Source or Destination Address across all the policy rulebases without having to add it manually each time.
Antivirus Profiles – Protects against worms and viruses or to block spyware downloads.

Anti-spyware Profiles – To block attempts by spyware trying to access the protected network.

Application – In Palo Alto Network terms, an application is a specific program or feature that can be detected, monitored and blocked if necessary.

Application Command Center (ACC) – The ACC Page visually depicts the trends and historic view of traffic on your network.

Application Groups – Static, user-defined sets of applications, application filters and other application groups allowing the firewall administrator to create logical grouping of applications that can be applied to security policies.

App-ID – Provides the ability to identify application and application functions. App-ID is a core function of the Palo Alto Networks device using multiple identification mechanisms to determine the exact identity of applications traversing the network.

APT – Advanced Persistent Threat.

Captive Portal – Captive Portal is a feature of the Palo Alto Networks firewall that authenticates users via an alternate source, such as a RADIUS server.

CC/FIPS – Common Criteria/Federal Information Processing Standards Support

Content-ID – Content-ID provides fully integrated protection from vulnerability exploits, malware and malware generated command-and-control traffic by combining a real-time threat prevention engine with a comprehensive URL database.

CRL – Certificate Revocation List.

Data Filtering Profiles – Help to prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall.
DDoS – Distributed Denial-of-Service attack.

Decryption Port Mirror – A feature providing the ability to create a copy of decrypted traffic from a firewall and sending it to a traffic collection tool capable of receiving raw packet captures.

Destination NAT – Commonly used to provide external access to public servers on the private network.

Device Groups – Device groups can consist of firewalls and/or virtual systems that you want to manage as a group, such as the firewalls that manage a group of branch offices or individual departments in a company. Device Groups enable the bundling of Policy and Object configurations for application to groups of firewalls.

Dynamic Address Groups – A dynamic address group that populates its members dynamically using looks ups for tags and tag-based filters.

File Blocking Profiles – Blocks specified selected file types.

FIPS – Federal Information Processing Standards Support

FQDN – Fully Qualified Domain Name.

GlobalProtect Portal – Palo Alto Networks firewalls that provide centralized management for the GlobalProtect system. Portals authenticate users and provide connection information needed to access the GlobalProtect Gateways.

GlobalProtect Gateway – Palo Alto Networks firewalls that provide security enforcement for traffic from GlobalProtect clients. Gateways are the tunnel endpoints for the VPN connections. They authenticate the agent or satellite based on SSL certificates.

GlobalProtect Agent – A small client application that is installed on the client system and configured to connect to the portals and gateways to provide network access for the user’s system. The client also provides information about the user’s local configuration to the portal.

GP-100 for Global Protect Mobile Security Manager – Provides a unique, integrated mobile security solution to safely enable mobile devices for business use. It consists of three key components: GlobalProtect Gateway
(available on the Palo Alto Networks next-generation network security platform), GlobalProtect Mobile Security Manager (available on the Palo Alto Networks GP-100), and GlobalProtect App (available for iOS and Android devices).

**Group Mapping** – The ability to gather a list of available users and their corresponding groups from an LDAP server.

**HA** – High Availability.

**HA Lite** – The Active/Passive High Availability version for the PA-200 and VM-Series firewalls. Does not include any session synchronization.

**HSM** – Hardware Security Module: A physical device that securely generates, manages and stores digital keys.

**IKE** – Internet Key Exchange.

**Intrazone** – Traffic within the same zone (allowed by default).

**Interzone** – Traffic traversing from one zone to another (denied by default)

**Layer 2 Mode** – In Layer 2 Mode, all of the protection and decryption features of the firewall can be used for Trunk (VLAN) interfaces.

**Layer 3 Mode** – In Layer 3 Mode the layer 3 interfaces of the firewall can take the place of any current enterprise firewall deployment.


**M-100** - The M-100 allows you to deploy Panorama management and logging functions on a dedicated appliance, or you can separate the functions in a distributed manner for improved performance and scalability.

**NTP Server** – A Network Time Protocol server.


**Panorama** – Panorama is a centralized security management system that provides global control over a network of Palo Alto Networks next-generation firewalls. Panorama is designed to provide three benefits: Centralized
configuration management, Centralized logging and reporting, and Centralized deployment management.

Panorama Templates - Templates enable the administrator to push device-level configurations, such as MGT interface setup and server profiles, to simply firewall setup.

PANW – Palo Alto Networks


PBF – Policy Based Forwarding.

PCAP – Packet Capture.

Policies – Policies allow you to control firewall operation by enforcing rules and automatically taking action. There are multiple types of policies such as NAT, PBF, QoS, Override, DoS, etc.

Policy objects – Elements that enable you to construct, schedule, and search for policies.

QoS – Quality of Service.

RADIUS – A Remote Authentication Dial-In User Service (RADIUS) used to authenticate users.

REST – Representational State Transfer.

Safe Search Enforcement – An option that can be enabled in a URL filtering profile to prevent users who are searching the Internet from viewing offensive, or inappropriate search results within specific browsers.

Security Policies – Policy rules that are compared against the incoming traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones. They are built using objects that hold values of addresses, applications, users and services.

Security Profiles – May be included within a Security Policy. Each Security Policy can include specification of one or more Security Profiles, which provide additional protection and control.
Security Profile Groups – Enable you to specify sets of Security Profiles that can be treated as a unit and then added to Security Policies.

Service Groups – Use Service Groups to simplify the creation of security policies by combining services that have the same security settings into service groups.

SLAAC – Stateless Address Auto-Configuration.

Source NAT – Translates internal private IP addresses to external public IP addresses. Commonly used to enable internal users to access the Internet.

SSL Inbound decryption – Use when you want to intercept and decrypt user traffic coming from the Internet to your DMZ servers.

SSL Outbound decryption – Use when you want to decrypt user traffic coming from the internal network and going to the external network.

Tap Mode – In Tap Mode the firewall can be connected to a core switch’s span port to identify applications running on the network. This option requires no changes to the existing network design. In this mode the firewall cannot block any traffic.


Universal Zone – Traffic applying to both zones Intrazone and Interzone.

URL Filtering Profiles – Restrict access to specific web sites and web site categories.

User Mapping – Maps an IP address of a packet to a Username using the User-ID agent.

Virtual Systems – An independent (virtual) firewall instance that can be managed separately within a physical firewall.

Virtual Wire Mode – In Virtual Wire Mode the firewall can be inserted into an existing topology, by using virtual wire interfaces, without requiring any reallocation of network addresses or redesign on the network topology. In this mode all of the protection and decryption features of the device can be used. NAT functionality is also provided in this mode.

VPN – Virtual Private Network.
Vulnerability Protection Profiles – To stop attempts to exploit system flaws or gain unauthorized access to systems.

WF-500 - Organizations that prefer not to use public cloud applications due to regulatory and privacy concerns can deploy WildFire as a private cloud using the WF-500.

WildFire – Identifies unknown malware and zero-day exploits using advanced static and dynamic analysis techniques while simplifying an organization’s response to the most dangerous threats—automatically detecting unknown malware and quickly preventing threats before organizations are compromised. Unlike legacy security solutions, WildFire quickly identifies and stops these advanced attacks without requiring manual human intervention or costly Incidence Response (IR) services after the fact.

XML API—Provides a Representational State Transfer (REST)-based interface to access device configuration, operational status, reports, and packet captures from the firewall.