Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide

April 2022

Table of Contents

Table of Contents 2

How to Use This Study Guide 6

About the PCNSA Exam 6

Exam Format 6

How to Take This Exam 7

Disclaimer 7

Audience and Qualifications 7

Skills Required 7

Recommended Training 7

Domain 1: Device Management and Services 8

1.1 Demonstrate knowledge of firewall management interfaces 8

1.1.1 Management interfaces 8

1.1.2 Methods of access 8

1.1.3 Access restrictions 11

1.1.4 Identify management traffic flow 13

1.1.5 Management services 15

1.1.6 Service routes 16

1.2 Provision local administrators 18

1.2.1 Authentication profile 18

1.2.2 Authentication sequence 19

1.2.3 Reference 20

1.3 Assign role-based authentication 20

1.3.1 Reference 20

1.4 Maintain firewall configurations 20

1.4.1 Running configuration 21

1.4.2 Candidate configuration 22

1.4.3 Discern when to use load, save, import, and export 22

1.4.4 Differentiate between configuration states 24

1.4.5 Backup Panorama configurations and firewalls from Panorama 28

1.5 Push policy updates to Panorama-managed firewalls 29

1.5.1 Device groups and hierarchy 29

1.5.2 Where to place policies 31

1.5.3 Implications of Panorama management 32

1.5.4 Impact of templates, template stacks, and hierarchy 33

1.5.5 References 35

1.6 Schedule and install dynamic updates 36

1.6.1 Updates from Panorama 36

`

1.6.2 Updates from the firewall 36
1.6.3 Scheduling and staggering updates on HA pair 38
1.6.4 References 39
1.7 Create and apply security zones to policies 40
1.7.1 Identify zone types 40
1.7.2 External types 40
1.7.3 Layer 2 42
1.7.4 Layer 3 42
1.7.5 Tap 43
1.7.6 VWire 45
1.7.7 Tunnel 49
1.8 Identify and configure firewall interfaces 50
1.8.1 Different types of interfaces 50
1.8.2 How interface types affect Security policies 50
1.9 Maintain and enhance the configuration of a virtual or logical router 62
1.9.1 Steps to create a static route 62
1.9.2 How to use the routing table 63
1.9.3 What interface types can be added to a virtual or logical router 63
1.9.4 How to configure route monitoring 65
1.10 Sample Questions 70

Domain 2: Managing Objects 75
2.1 Create and maintain address and address group objects 75
2.1.1 How to tag objects 75
2.1.2 Differentiate between address objects 76
2.1.3 Static groups versus dynamic groups 78
2.1.4 References 81
2.2 Create and maintain services and service groups 82
2.3 Create and maintain external dynamic lists 88
2.3.1 References 89
2.4 Configure and maintain application filters and groups 89
2.4.1 When to use filters versus groups 89
2.4.2 The purpose of application characteristics as defined in the App-ID database 92
2.5 Sample Questions 93

Domain 3: Policy Evaluation and Management 95
3.1 Develop the appropriate application-based Security policy 95
3.1.1 Create an appropriate App-ID rule 95
3.1.2 Rule shadowing 99
3.1.3 Group rules by tag 100
3.1.4 The potential impact of App-ID updates to existing security policy rules 102
3.1.5 Policy usage statistics 102

3.1.6 Reference 106
3.2 Differentiate specific security rule types 106
3.2.1 Interzone rules 106
3.2.2 Intrazone rules 107
3.2.3 Universal rules 107
3.3 Configure Security policy match conditions, actions, and logging options 107
3.3.1 Use Application Filters and Groups 112
3.3.2 Use logging options 114
3.3.3 App-ID 115
3.3.4 User-ID 116
3.3.5 Device-ID 117
3.3.6 Include an application filter in policy 118
3.3.7 Include an application group in policy 119
3.3.8 EDLs 121
3.3.9 References 121
3.4 Identify and implement proper NAT policies 121
3.4.1 Destination NAT 121
3.4.2 Source NAT 124
3.5 Optimize Security policies using appropriate tools 127
3.5.1 Policy text match tool 127
3.5.2 Policy Optimizer 128
3.6 Sample Questions 129

Domain 4: Securing Traffic 133
4.1 Compare and contrast different types of Security profiles 133
4.1.1 Antivirus 133
4.1.2 Anti-Spyware 133
4.1.3 Vulnerability Protection 133
4.1.4 URL Filtering 134
4.1.5 WildFire analysis 134
4.2 Create, modify, add, and apply the appropriate Security profiles and groups 135
4.2.1 Antivirus 135
4.2.2 Anti-Spyware 136
4.2.3 Vulnerability protection 137
4.2.4 URL filtering 138
4.2.5 WildFire analysis 138
4.2.6 Configure Threat Prevention policy 139
4.3 Differentiate between Security profile actions 139
4.4 Use information available in logs 146
4.4.1 Traffic 146
4.4.2 Threat 146
4.4.3 Data 148

`

4.4.4 System logs 148
4.5 Enable DNS Security to control traffic based on domains 148
4.5.1 Where to configure DNS Security 148
4.5.2 How to apply DNS Security in policy 149
4.6 Create and deploy URL Filtering-based controls 150
4.6.1 Apply a URL profile in a Security policy 150
4.6.2 Create a URL Filtering profile 150
4.6.3 Create a custom URL category 153
4.6.4 Control traffic based on a URL category 155
4.6.5 Why a URL was blocked 155
4.6.6 How to allow a blocked URL 156
4.6.7 How to request a URL recategorization 156
4.7 Differentiate between group mapping and IP-to-user mapping within policies and logs 160
4.7.1 How to control access to specific locations 160
4.7.2 How to apply the specific policies 160
4.7.3 Identify users within the ACC and the monitor tab 161
4.8 Sample Questions 162

Appendix A: Sample Questions with Answers 164

Continuing Your Learning Journey with Palo Alto Networks 173

`

How to Use This Study Guide

Welcome to the Palo Alto Networks Certified Security Administrator Study Guide. The purpose of this guide is to help you prepare for your PCNSA: Palo Alto Networks Certified Security Administrator exam and achieve your PCNSA certification.

You can read through this study guide from start to finish, or you may jump straight to topics you would like to study. Hyperlinked cross-references will help you locate important definitions and background information from earlier sections.

About the PCNSA Exam

The PCNSA certification validates the knowledge and skills required for network security administrators responsible for deploying and operating Palo Alto Networks Next-Generation Firewalls (NGFWs). PCNSA certified individuals have demonstrated knowledge of the Palo Alto Networks NGFW feature set and in the Palo Alto Networks product portfolio core components.

More information is available from the Palo Alto Networks public page at: https://www.paloaltonetworks.com/services/education/palo-alto-networks-certified-network-security-administrator

PCNSA technical documentation is located at: https://beacon.paloaltonetworks.com/student/collection/668330-palo-alto-networks-certified-network-security-administrator-pcnsa?sid=997e3b6e-0839-4c30-a393-e134fbad744a&sid_i=0

Exam Format

The test format is 50-60 items. Candidates will have five minutes to review the NDA, 80 minutes to complete the exam questions, and five minutes to complete a survey at the end of the exam.

The approximate distribution of items by topic (Exam Domain) and topic weightings are shown in the following table.

This exam is based on Product version 10.2.

Exam Domain	Weight (%)
Device Management and Services	22%
Managing Objects	20%
Policy Evaluation and Management	28%
Securing Traffic	30%
TOTAL	**100%**

`

How to Take This Exam

The exam is available through the third-party Pearson VUE testing platform.
To register for the exam, visit: https://home.pearsonvue.com/paloaltonetworks

Disclaimer

This study guide is intended to provide information about the objectives covered by this exam, related resources, and recommended courses. The material contained within this study guide is not intended to guarantee that a passing score will be achieved on the exam. Palo Alto Networks recommends that candidates thoroughly understand the objectives indicated in this guide and use the resources and courses recommended in this guide where needed to gain that understanding.

Audience and Qualifications

Intended Audience

Security administrators responsible for deploying, operating, and managing Palo Alto Networks network security suite.

Skills Required

- You understand Palo Alto Networks firewall and centralized management components and, with minimum assistance, can configure, operate, and identify problems with configuring and operating the firewall as well as configure firewall policies, specifically App-ID and User-ID (those capabilities not tied to a subscription) as well as profiles and objects.
- You have 2 to 3 years' experience working in the Networking or Security industries, the equivalent of 6 months' experience working full-time with the Palo Alto Networks product portfolio and/or at least 6 months' experience in Palo Alto Networks NGFW administration and configuration.

Competencies Required

- Able to configure and operate Palo Alto Networks product portfolio components.
- An understanding of the unique aspects of the Palo Alto Networks product portfolio and how to administer one appropriately.
- An understanding of the networking and security policies used by PAN-OS software.

Recommended Training

Palo Alto Networks strongly recommends that you attend the following instructor-led training courses or equivalent digital-learning courses:

- Firewall Essentials: Configuration and Management (EDU-210) course

Domain 1: Device Management and Services

1.1 Demonstrate knowledge of firewall management interfaces

1.1.1 Management interfaces

Four methods are used to manage the Palo Alto Networks Next-Generation Firewalls:

- Web interface
- CLI
- Panorama
- XML API

All Palo Alto Networks firewalls provide an out-of-band management (MGT) port that you can use to perform firewall administration functions. The MGT port uses the control plane, thus separating the management functions of the firewall from the network-traffic processing functions (data plane). This separation between the control plane and data plane safeguards access to the firewall and enhances performance. When you use the web interface, you must perform all initial configuration tasks from the MGT port even if you plan to use an in-band data port for managing your firewall. A serial/console port also is available to accomplish initial configuration of the firewall using SSH or Telnet.

Some management tasks, such as retrieving licenses and updating the threat and application signatures on the firewall, require access to the internet, typically via the MGT port. If you do not want to enable external access via your MGT port, you can set up an in-band data port on the data plane to provide access to required external services (using service routes). Service routes are explained in more detail in a later section.

1.1.2 Methods of access

The initial step to gaining access to the firewall for the first time is to gather the following information for the MGT port. Note that if the firewall is set up as a DHCP client, this information will be included automatically via DHCP:

`

- IP address
- Netmask
- Default gateway
- At least one DNS server address

The second step is to connect a computer to the firewall using either an RJ-45 Ethernet cable or a serial cable.

An RJ-45 Ethernet cable is connected from your computer to the firewall MGT port. From a browser, navigate to https://192.168.1.1. Note that you might need to change the IP address on your computer to an address in the 192.168.1.0/24 subnet, such as 192.168.1.2, to access this URL.

If you want to perform your initial configuration via the CLI or don't know the address served to the management port via DHCP to access the web interface, connect the serial cable from your computer to the firewall console port using terminal emulation software such as SSH or Telnet. The default connection parameters are 9600-8-N-1.

`

The third step is to log in to the firewall. The default username is “admin,” and the default password is “admin”. Starting with PAN-OS 9.1, you are forced to change the admin account password the first time you log in to the web interface.

Four Firewall Management Methods

Web interface: The web interface is used for configuration and monitoring over HTTP or HTTPS using a web browser. HTTPS is the default method; HTTP is available as a less secure method than HTTPS.

CLI: The CLI is text-based configuration and monitoring over the serial console port, or over the MGT port using SSH or Telnet. The Palo Alto Networks firewall CLI offers access to debugging information; experienced administrators often use it for troubleshooting. The account used for authenticating into the CLI must have CLI access enabled.

The CLI will be in *operational mode* by default. The commands available within the context of operational mode include basic networking commands such as **`ping`** and **`traceroute`**, basic system commands such as **`show`**, and more advanced system commands such as **`debug`**. Commands to shutdown and restart the system also are available from within operational mode.

Access configuration mode by typing the command **`configure`** while in operational mode.

Configuration mode enables you to display and modify the configuration parameters of the firewall, verify candidate configuration, and commit the config.

The following figure shows an example CLI screen with the first lines of **`show system state`** while in operational mode:

`

Panorama: Panorama is a Palo Alto Networks product that provides centralized web-based management, reporting, and logging for multiple firewalls. Use Panorama for centralized policy and firewall management to increase operational efficiency in managing and maintaining a distributed network of firewalls. If six or more firewalls are deployed in your network, you should use Panorama to reduce the complexity and administrative overhead needed to manage configuration, policies, software, and dynamic content updates. The Panorama web interface is similar to the firewall web interface, but with additional management functions.

XML API: The XML API provides an interface based on representational state transfer (REST) to access firewall configurations, operational status, reports, and packet captures from the firewall. An API browser is available on the firewall at https://<firewall>/api, where <firewall> is the hostname or IP address of the firewall. You can use this API to access and manage your firewall through a third-party service, application, or script.

The PAN-OS XML API can be used to automate tasks such as:

- Create, update, and modify firewall and Panorama configurations
- Execute operational mode commands, such as restarting the system or validating configurations
- Retrieve reports
- Manage users through User-ID
- Update dynamic objects without having to modify or commit new configurations

1.1.3 Access restrictions

Management of Palo Alto Networks firewalls is not limited to using a dedicated MGT interface or console port. Data interfaces on the data plane also can be used as management interfaces. If the MGT interface goes down, you can continue to manage the firewall by allowing management access over another data interface. Each data interface includes configurations for binding various services to them:

- HTTPS (default)
- SSH (default)
- Ping (default)
- Telnet
- HTTP
- SNMP
- Response Pages
- User-ID

An Interface Management profile protects the firewall from unauthorized access by defining the protocols, services, and IP addresses that a firewall interface permits for management. For example, you might want to prevent users from accessing the firewall web interface over the ethernet1/1 interface but allow that interface to receive SNMP queries from your network monitoring system. In this case, you would enable SNMP and disable HTTP/HTTPS in an Interface Management profile and assign the profile to ethernet1/1.

`

HTTPS includes the web interface service and should be included on at least one data interface. The Permitted IP Addresses field allows an access control list to be included, thus restricting access to only specified IP addresses for any interface with this profile assigned. If no IP addresses are added to the list of permitted IP addresses, then any IP address is allowed. After at least one IP address is added to the list, only those IP addresses are allowed access.

You can assign an Interface Management profile to Layer 3 Ethernet interfaces (including subinterfaces) and to logical interfaces (aggregate group, VLAN, loopback, and tunnel interfaces). If you do not assign an Interface Management profile to an interface, the firewall denies management access for all IP addresses, protocols, and services by default.

1.1.4 Identify management traffic flow

Firewall Dashboard

The firewall **Dashboard** provides information in a condensed format. It is the main screen for web interface management.

The **Dashboard** is customizable and allows you to determine which widgets to display:

- Application widgets:
  - ACC Risk Factor
  - Top Applications
  - Top High Risk Applications
- Logs widgets:
  - Config Logs
  - Data Filtering Logs
  - System Logs
  - Threat Logs
  - URL Filtering Logs
- System widgets:
  - General Information
  - High Availability
  - Interfaces
  - Locks
  - Logged In Admins
  - System Resources

Functional Category Tabs

Management of the firewall is conducted using seven category tabs:

- **Dashboard**: Provides general information such as device name, MGT IP address, and licensing information. This page can be augmented by adding widgets.
- **ACC**: Uses the firewall logs to graphically depict traffic trends on your network.
- **Monitor**: Provides logging visibility and the ability to run packet captures.
- **Policies**: Allows the creation of policies such as Security policy and NAT policy.
- **Objects**: Allows the creation of objects such as address objects.
- **Network**: Allows the configuration of network parameters such as interfaces and zones.
- **Device**: Allows the configuration of system information such as the hostname or certificates.

Tasks Icon

The **Tasks** icon appears in the bottom right. Select it to display the tasks that you, other administrators, or the PAN-OS software has initiated since the last firewall reboot (for example, manual commits or automatic FQDN refreshes):

Service Routes

By default, the firewall uses the management interface to communicate with various servers including those for external dynamic lists (EDLs), DNS, email, and Palo Alto Networks update servers. It also uses the management interface to communicate with Panorama. Service routes are used so that the communication between the firewall and servers goes through the data ports on the data plane. These data ports require appropriate Security policy rules before external servers can be accessed.

`

1.1.5 Management services

Palo Alto Networks firewalls integrate with three important services: DNS, DHCP, and NTP. DNS and NTP must be set during the initial firewall configuration.

DNS
Domain Name System (DNS) is a protocol that translates (resolves) a user-friendly domain name such as www.paloaltonetworks.com to an IP address so that users can access computers, websites, services, or other resources on the internet or private networks. You must configure your firewall with at least one DNS server so it can resolve hostnames.

Configuring DNS
To configure DNS, select **Device > Setup > Services > Services_gear_icon**. On the **Services** tab, for DNS, click **Servers** and enter the **Primary DNS Server** address and **Secondary DNS Server** address. Click **OK** and **Commit**:

DHCP
A Palo Alto Networks firewall acting as a DHCP client (host) can request an IP address and other configuration settings from a DHCP server. The use of DHCP saves time and effort because users need not know the network's addressing plan or other options, such as default gateway, that they are inheriting from the DHCP server.

Configuration parameters that DHCP can learn dynamically include:

- IP address for MGT port
- Netmask

- Default gateway
- At least one DNS server address

NTP

NTP client information is optional but recommended. The NTP information can be obtained via DHCP if the firewall is configured as a DHCP client.

Configuring NTP

Select **Device > Setup > Services > Services_gear_icon**:

1.1.6 Service routes

By default, the firewall uses the management interface to communicate with various servers including those for external dynamic lists (EDLs), DNS, email, and Palo Alto Networks update servers. It also uses the management interface to communicate with Panorama. Service routes are used so that the communication between the firewall and servers goes through the data ports on the data plane. These data ports require appropriate Security policy rules before external servers can be accessed.

Configuring Service Routes

Go to **Device > Setup > Services > Service Route Configuration > Customize** and configure the appropriate service routes. See the following figure:

`

To configure service routes for non-predefined services, you can manually enter the destination addresses on the **Destination** tab:

`

In the example shown, the service route for 192.168.27.33 is configured to source from the data plane's ethernet1/2 interface, which has a source IP address of 192.168.27.254.

1.2 Provision local administrators

1.2.1 Authentication profile

Authentication profiles provide authentication settings that you can apply to administrator accounts, SSL-VPN access, and Captive Portal. An Authentication profile configuration screenshot follows:

Authentication Profiles

An Authentication profile references a Server profile:

`

A Server profile includes the server name, its IP address, the service port that it is listening to, and other values. An example of an LDAP Server profile follows:

1.2.2 Authentication sequence

Admin roles for external administrator accounts can be assigned to an authentication sequence, which includes a sequence of one or more authentication profiles that are processed in a specific order. The firewall checks against each authentication profile within the authentication sequence until one Authentication profile successfully authenticates the user. If an external administrator account does not reference an authentication sequence, it directly references an Authentication profile instead. A user is denied access only if authentication fails for all the profiles in the authentication sequence. A depiction of an authentication sequence follows:

Authentication Sequence

1.2.3 Reference

- Administrative Role Types, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types

1.3 Assign role-based authentication

There are times when you may want to configure the firewall and Panorama to provide local authentication for administrators and end users. For example, you may require special user accounts that you don't manage through the directory servers that your organization reserves for regular accounts. Another example is when you define a superuser account that is local to the firewall so that you can access the firewall even if the directory server is down. In these cases, you can use the following authentication methods:

- **Local database authentication**: Below are the high-level process steps to configure local database authentication:
    1. To add a user account to the local database, select **Device > Local User Database > Users** and click **Add**.
    2. Enter a user **Name** for the administrator.
    3. Enter a **Password** and **Confirm Password** or enter a **Password Hash**. **Enable** the account.

- **Local authentication without a database**: Below are the high-level process steps to configure firewall administrative accounts or Panorama administrative accounts without creating a database of users and user groups:
    1. To add an administrative account on the firewall, select **Device > Administrators** and **Add** an account.
    2. Enter a user **Name** for the administrator.
    3. Select an Authentication profile. If the firewall uses local authentication without a local user database, select **None** and enter a **Password**.
    4. Select the **Administrative Type**.
    5. Select a **Password Profile**.
    6. Click **OK** and **Commit**.

1.3.1 Reference

- Administrative Role Types, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types

1.4 Maintain firewall configurations

All configuration changes in a Palo Alto Networks firewall are done to a *candidate configuration*, which resides in memory on the control plane. A commit activates the changes since the last commit and installs the running configuration on the data plane, where it will become the *running configuration*.

`

1.4.1 Running configuration

The running configuration is a configuration that is saved within a file named running-config.xml. The running configuration exists in data-plane memory, where it is used to control firewall traffic and operate the firewall. A commit operation is necessary to write the candidate configuration to the running configuration.

After you commit changes, the firewall automatically saves a new version of the running configuration that is timestamped. You can load a previous version of the running configuration using the Load configuration version option. The firewall queues commit requests so that you can initiate a new commit while a previous commit is in progress. The firewall performs the commits in the order they are initiated but prioritizes commits that the firewall initiates automatically, such as FQDN refreshes.

If a system event or administrator action causes a firewall to reboot, the firewall automatically reverts to the current version of the running configuration.

`

1.4.2 Candidate configuration

The act of saving your changes to the candidate configuration does not activate those changes. A commit must be performed on the firewall to activate the changes and to cause the candidate configuration to become the running configuration. The commit can be done either via the web interface or the CLI.

You can save the candidate configuration as either a default snapshot file (snapshot.xml) or a custom-named snapshot file (<custom_name>.xml). However, a firewall does not automatically save the candidate configuration to persistent storage; you must manually save the candidate configuration. If the firewall reboots before you commit your changes, you can revert the candidate configuration to the current snapshot to restore changes you made between the last commit and the last snapshot using the Revert to last saved configuration option.

1.4.3 Discern when to use load, save, import, and export

Save Named Configuration Snapshot
This option creates a candidate configuration snapshot that does not overwrite the default snapshot (snapshot.xml). Enter a custom name for the snapshot or select an existing snapshot to overwrite. This function is useful when you create a backup file or a test configuration file that could be downloaded for a further modification or testing in the lab environment.

Save Candidate Configuration
This option creates or overwrites the default snapshot (snapshot.xml) of the candidate configuration (the snapshot that you create or overwrite when you click **Device > Setup > Operations > Save candidate configuration** or **Save** at the top right of the web interface).

Load Named Configuration Snapshot
This option overwrites the current candidate configuration with one of the following:

- Custom-named candidate configuration snapshot (instead of the default snapshot)

`

- Custom-named running configuration that you imported
- Current running configuration (running-config.xml)

Load Configuration Version

This option overwrites the current candidate configuration with a previous version of the running configuration that is stored on the firewall. The firewall creates a timestamped version of the running configuration whenever a commit is made.

Save Candidate Configuration

This option creates or overwrites the default snapshot (snapshot.xml) of the candidate configuration (the snapshot that you create or overwrite when you click **Device > Setup > Operations > Save candidate configuration** or **Save** at the top right of the web interface).

`

Import Named Configuration Snapshot
This option imports a running or candidate configuration as an XML file from any network location, such as a host computer. Click **Browse** and select the configuration file to be imported. You can then load the XML file as a candidate configuration and even ultimately as the running configuration if required.

Import Device State
This option imports the state information file that you exported from a firewall using the Export device state option. The state information includes the running configuration, device group, and template settings pushed from Panorama, if applicable. If the firewall is a GlobalProtect portal, the bundle also includes certificate information, a list of satellites, and satellite authentication information. If you replace a firewall or portal, you can restore the information on the replacement by importing the state bundle.

Export Named Configuration Snapshot
This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. You can also use these XML files as templates for building other firewall configurations.

1.4.4 Differentiate between configuration states

Palo Alto Networks firewall configurations are managed using five categories, which are found under **Device > Setup > Operations** and are described in the next sections:

- Revert
- Save
- Load
- Export
- Import

As a best practice, periodically save candidate configurations.

Revert to Last Saved Configuration
This option restores the default snapshot (snapshot.xml) of the candidate configuration (the snapshot that you create or overwrite when you click **Device > Setup > Operations > Save candidate configuration** or **Save** at the top right of the web interface). This option restores the last saved candidate configuration from the local drive. The current candidate configuration is overwritten. This quick restore is useful when you work on "hot" boxes.

The first message asks whether you want to continue with the revert:

`

The second message informs you which file has been reverted:

Save Named Configuration Snapshot

This option creates a candidate configuration snapshot that does not overwrite the default snapshot (snapshot.xml). Enter a custom name for the snapshot or select an existing snapshot to overwrite. This function is useful when you create a backup file or a test configuration file that could be downloaded for a further modification or testing in the lab environment.

Load Named Configuration Snapshot

This option overwrites the current candidate configuration with one of the following:

- Custom-named candidate configuration snapshot (instead of the default snapshot)
- Custom-named running configuration that you imported
- Current running configuration (running-config.xml)

Export Named Configuration Snapshot

This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

Export Device State

This option exports the firewall state information as a file. In addition to the running configuration, the state information includes device group and template settings pushed from Panorama, if applicable. If the firewall is a GlobalProtect portal, the bundle also includes certificate information, a list of satellites that the portal manages, and satellite authentication information. If you replace a firewall or portal, you can restore the exported information on the replacement by importing the state bundle.

Import Named Configuration Snapshot

This option imports a running or candidate configuration as an XML file from any network location such as a host computer. Click **Browse** and select the configuration file to be imported. The XML file then can be loaded as a candidate configuration and even ultimately loaded as the running configuration if required.

`

Import Device State
This option imports the state information file that you exported from a firewall using the **Export device state** option. The state information includes the running configuration and device group and template settings pushed from Panorama, if applicable. If the firewall is a GlobalProtect portal, the bundle also includes certificate information, a list of satellites, and satellite authentication information. If you replace a firewall or portal, you can restore the information on the replacement by importing the state bundle.

1.4.5 Backup Panorama configurations and firewalls from Panorama

The running configuration on Panorama comprises all the settings that you have committed and that are therefore active. The candidate configuration is a copy of the running configuration plus any inactive changes that you made since the last commit. Saving backup versions of the running or candidate configuration enables you to restore those versions later. For example, if a commit validation shows that the current candidate configuration has more errors than you want to fix, you can restore a previous candidate configuration. You can also revert to the current running configuration without saving a backup first.

After a commit on a local firewall that runs PAN-OS 5.0 or later, a backup of the firewall's running configuration is sent to Panorama. Any commits performed on the local firewall will trigger the backup, including commits that an administrator performs locally on the firewall or automatic commits that PAN-OS initiates (such as an FQDN refresh). By default, Panorama stores up to 100 backups for each firewall, though this is configurable. To store Panorama and firewall configuration backups on an external host, you can schedule exports from Panorama or export on demand. You can also import configurations from firewalls into Panorama device groups and templates to Transition a Firewall to Panorama Management.

(VMware ESXi and vCloud Air only) VMware snapshot functionality is not supported for a Panorama virtual appliance deployed on VMware ESXi and vCloud Air. Taking snapshots of a Panorama virtual appliance can impact performance, result in intermittent and inconsistent packet loss, and cause Panorama to become unresponsive. Additionally, you may lose access to the Panorama CLI and

web interface, and switching to Panorama mode is not supported. Instead, save and export your named configuration snapshot to any network location.

1.5 Push policy updates to Panorama-managed firewalls

1.5.1 Device groups and hierarchy

You can Create a Device Group Hierarchy to nest device groups in a tree hierarchy of up to four levels, with lower-level groups inheriting the settings (policy rules and objects) of higher-level groups. At the bottom level, a device group can have parent, grandparent, and great-grandparent device groups (ancestors). At the top level, a device group can have child, grandchild, and great-grandchild device groups (descendants). All device groups inherit settings from the Shared location—a container at the top of the hierarchy for configurations that are common to all device groups.

Creating a device-group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. For example, you could configure shared settings that are global to all firewalls, configure device groups with function-specific settings at the first level, and configure device groups with location-specific settings at lower levels. Without a hierarchy, you would have to configure both function- and location-specific settings for every device group in a single level under Shared.

Device Group Policies:
Device groups provide a way to implement a layered approach for managing policies across a network of managed firewalls. A firewall evaluates policy rules by layer (shared, device group, and local) and by type (pre-rules, post-rules, and default rules) in the following order from top to bottom. When the firewall receives traffic, it performs the action defined in the first evaluated rule that matches the traffic and disregards all subsequent rules. To change the evaluation order for rules within a particular layer, type, and rulebase (for example, shared Security pre-rules), see Manage the Rule Hierarchy.

Whether you view rules on a firewall or in Panorama, the web interface displays them in evaluation order. All the shared, device-group, and default rules that the firewall inherits from Panorama are shaded orange. Local firewall rules display between the pre-rules and post-rules.

EVALUATION ORDER	RULE SCOPE AND DESCRIPTION	ADMINISTRATION DEVICE
Shared pre-rules	Panorama pushes shared pre-rules to all the firewalls in all device groups. Panorama pushes device-group-specific pre-rules to all the firewalls in a particular device group and its descendant device groups. If a firewall inherits rules from device groups at multiple levels in the device group hierarchy, it evaluates pre-rules in the order of highest to lowest level. This means the firewall first evaluates shared rules and last evaluates the rules of device groups with no descendants. You can use pre-rules to enforce the acceptable use policy of an organization. For example, a pre-rule might block access to specific URL categories or allow Domain Name System (DNS) traffic for all users.	These rules are visible on firewalls, but you can only manage them in Panorama.
Device group pre-rules		
Local firewall rules	Local rules are specific to a single firewall or virtual system (vsys).	A local firewall administrator, or a Panorama administrator who switches to a local firewall context, can edit local firewall rules.

Device group post-rules	Panorama pushes shared post-rules to all the firewalls in all device groups. Panorama pushes device-group-specific post-rules to all the firewalls in a particular device group and its descendant device groups. If a firewall inherits rules from device groups at multiple levels in the device-group hierarchy, it evaluates post-rules in the order of lowest to highest level. This means that the firewall first evaluates the rules of device groups with no descendants and last evaluates shared rules. Post-rules typically include rules to deny access to traffic based on the App-ID™ signatures, User-ID™ information (users or user groups), or service.	These rules are visible on firewalls, but you can only manage them in Panorama.
Shared post-rules		
Intrazone-default	The default rules apply only to the Security rulebase and are predefined on Panorama (at the Shared level) and the firewall (in each vsys). These rules specify how PAN-OS handles traffic that doesn't match any other rule. The intrazone-default rule allows all traffic within a zone. The interzone-default rule denies all traffic between zones. If you override default rules, their order of precedence runs from the lowest context to the highest overridden settings at the firewall level take precedence over settings at the device-group level, which take precedence over settings at the Shared level.	Default rules are initially read-only, either because they are part of the predefined configuration or because Panorama pushed them to firewalls. However, you can override the rule settings for tags, action, logging, and Security profiles. The context determines the level at which you can override the rules: • Panorama—At the Shared or device-group level, you can override default rules that are part of the predefined configuration. • Firewall—You can override default rules that are part of the predefined configuration on the firewall or vsys, or that Panorama pushed from the Shared location or a device group.
Interzone-default		

1.5.2 Where to place policies

You can use Panorama to manage your firewalls. You'll need to enable the connection from the firewall to Panorama; to enable this connection, add a firewall as a managed device.

To add a firewall as a managed device, perform the following high-level process tasks:

1. Configure the firewall so it's accessible with Panorama over the network.

`

2. Configure each data interface on the firewall you plan to use and attach it to a **security zone**. This will allow you to push configuration and policy updates.
3. Add the **Panorama IP address** to the firewall.
4. Add one or more firewalls to Panorama (**Panorama > Managed Devices > Summary**).
5. Enter the firewall **Serial** number. Select the **Associate Devices** check box.
6. Assign the **Device Group**, **Template Stack**, **Collector Group**, and **Log Collector**.
7. Enable **Auto Push on 1st connect**.
8. Add a **tag**.
9. Select **Commit > Commit to Panorama** and **Commit**.

These are the high-level steps to start receiving push policy updates. If you've configured this correctly, you now have the option to automatically push the configuration to your newly added firewall when the firewall first connects to Panorama. This ensures that firewalls are immediately configured and ready to secure your networks.

1.5.3 Implications of Panorama management

Panorama enables you to effectively configure, manage, and monitor your Palo Alto Networks firewalls with central oversight. The three main areas in which Panorama adds value are:

- Centralized configuration and deployment—To simplify central management and rapid deployment of the firewalls and WildFire appliances on your network, use Panorama to pre-stage the firewalls and WildFire appliances for deployment. You can then assemble the firewalls into groups, create templates to apply a base network and device configuration, and use device groups to administer globally shared and local policy rules. See Centralized Firewall Configuration and Update Management.

- Aggregated logging with central oversight for analysis and reporting—Collect information on activity across all the managed firewalls on the network and centrally analyze, investigate, and report on the data. This comprehensive view of network traffic, user activity, and the associated risks empowers you to respond to potential threats using the rich set of policies to securely enable applications on your network. See Centralized Logging and Reporting.

- Distributed administration—Enables you to delegate or restrict access to global and local firewall configurations and policies. See Role-Based Access Control for delegating appropriate levels of access for distributed administration.

Four Panorama Models are available. The Panorama virtual appliance, M-600 appliance, M-500 appliance, and M-200 appliance are supported in PAN-OS 10.1. Panorama Centralized Management illustrates how you can deploy Panorama in a high availability (HA) configuration to manage firewalls.

1.5.4 Impact of templates, template stacks, and hierarchy

Use templates and template stacks to configure the settings that enable firewalls to operate on the network. Templates are the basic building blocks you use to configure the Network and Device tabs on Panorama. You can use templates to define interface and zone configurations, to manage the server profiles for logging and syslog access, or to define VPN configurations. Template stacks give you the ability to layer multiple templates and create a combined configuration. Template stacks simplify management because they allow you to define a common base configuration for all devices attached to the template stack and they give you the ability to layer templates to create a combined configuration. This enables you to define templates with location- or function-specific settings and then stack the templates in descending order of priority so that firewalls inherit the settings based on the order of the templates in the stack.

`

Both templates and template stacks support variables. Variables allow you to create placeholder objects with their value specified in the template or template stack based on your configuration needs. Create a template or template stack variable to replace IP addresses, Group IDs, and interfaces in your configurations. Template variables are inherited by the template stack and you can override them to create a template stack variable. However, templates do not inherit variables defined in the template stack. When a variable is defined in the template or template stack and pushed to the firewall, the value defined for the variable is displayed on the firewall.

Use templates to accommodate firewalls that have unique settings. Alternatively, you can push a broader, common base configuration and then override certain pushed settings with firewall-specific values on individual firewalls. When you override a setting on the firewall, the firewall saves that setting to its local configuration and Panorama no longer manages the setting. To restore template values after you override them, use Panorama to force the template or template-stack configuration onto the firewall. For example, after you define a common NTP server in a template and override the NTP server configuration on a firewall to accommodate a local time zone, you can later revert to the NTP server defined in the template.

When defining a template stack, consider assigning firewalls that are the same hardware model and require access to similar network resources, such as gateways and syslog servers. This enables you to avoid the redundancy of adding every setting to every template stack. The following figure illustrates an example configuration in which you assign data-center firewalls in the Asia-Pacific (APAC) region to a stack with global settings, one template with APAC-specific settings, and one template with data-center-specific settings. To manage firewalls in an APAC branch office, you can then reuse the global and APAC-specific templates by adding them to another stack that includes a template with branch-specific settings. Templates in a stack have a configurable priority order that ensures that Panorama pushes only one value for any duplicate setting. Panorama evaluates the templates listed in a stack configuration from top to bottom with higher templates having priority. The following figure illustrates a data-center stack in which the data-center template has a higher priority than the global template; Panorama pushes the idle timeout value from the data-center template and ignores the value from the global template.

`

You cannot use templates or template stacks to set firewall modes, such as virtual private network (VPN) mode, multiple virtual systems (multi-vsys) mode, or operational modes (normal or FIPS-CC mode). For details, see Template Capabilities and Exceptions. However, you can assign firewalls that have nonmatching modes to the same template or stack. In such cases, Panorama pushes mode-specific settings only to firewalls that support those modes. As an exception, you can configure Panorama to push the settings of the default vsys in a template to firewalls that don't support virtual systems or that don't have any virtual systems configured.

1.5.5 References

- Set Up Zero Touch Provisioning, https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning
- Transition a Firewall to Panorama Management, https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management

1.6 Schedule and install dynamic updates

1.6.1 Updates from Panorama

Dynamic Updates
To ensure that you always are protected from the latest threats (including those that have not yet been discovered), you must keep your firewalls up to date with the latest content and software updates published by Palo Alto Networks. Palo Alto Networks regularly posts updates for application detection, threat protection, and GlobalProtect data files through dynamic updates.

1.6.2 Updates from the firewall

The following diagram illustrates how often updated information is made available to the firewall:

The following content updates are available, depending on which subscriptions you have:

- **Antivirus**: Includes new and updated antivirus signatures, including WildFire signatures and automatically generated command-and-control (C2) signatures. WildFire signatures detect malware seen first by firewalls from around the world. You must have a Threat Prevention subscription to get these updates. New antivirus signatures are published daily.
- **Applications**: Includes new and updated application signatures. This update does not require any additional subscriptions, but it does require a valid maintenance support contract. New applications are published monthly, and modified applications are published

`

weekly. To best deploy application updates to ensure application availability, be sure to follow the best practices for Applications and Threats content updates.

- **Applications and Threats**: Includes new and updated application and threat signatures, including those that detect spyware and vulnerabilities. This update is available if you have a Threat Prevention subscription (and you get it instead of the Applications update). New and modified threat signatures and modified applications signatures are published weekly; new application signatures are published monthly. The firewall can retrieve the latest update within 30 minutes of availability. To best deploy application and threat updates based on your security and application availability needs, be sure to follow the best practices for Applications and Threats content updates.
- **GlobalProtect Data File**: Contains vendor-specific information for defining and evaluating host information profile (HIP) data returned by GlobalProtect clients. You must have a GlobalProtect license (subscription) and create an update schedule to receive these updates.
- **GlobalProtect Clientless VPN**: Contains new and updated application signatures to enable clientless VPN access to common web applications from the GlobalProtect portal. You must have a GlobalProtect license (subscription) and create an update schedule to receive these updates and enable clientless VPN to function.
- **Palo Alto Networks (PAN-DB) URL Filtering**: Complements App-ID by enabling you to configure the firewall to identify and control access to web (HTTP and HTTPS) traffic and to protect your network from attack. If URL filtering is enabled, all web traffic is compared against the URL filtering database, which contains a listing of millions of websites that have been categorized into different categories.

Although the Palo Alto Networks URL filtering solution supports both BrightCloud and PAN-DB, only the PAN-DB URL filtering solution allows you to choose between the PAN-DB public cloud and the PAN-DB private cloud. Use the public cloud solution if the Palo Alto Networks Next-Generation Firewalls on your network can directly access the internet. If the network security requirements in your enterprise prohibit the firewalls from directly accessing the internet, you can deploy a PAN-DB private cloud on one or more M-500 appliances that function as PAN-DB servers within your network. PAN-DB URL filtering requires a PAN-DB URL Filtering license.

Every five to ten minutes, a new version is published that contains updated categorization data and an incremented version number. Each time the Palo Alto Networks firewall sends a request to the cloud, it checks the current version number. If the number is different, the firewall upgrades the device's version to the current cloud version. The primary purpose of the frequency of updates is to leverage native integration with WildFire, which creates new signatures and records malicious URLs every five minutes.

- **BrightCloud URL Filtering**: Provides updates to the BrightCloud URL filtering database only. You must have a BrightCloud subscription to get these updates. New BrightCloud URL database updates are published daily. End of sale was January 1, 2018, and end of support was July 21, 2021.

`

- **WildFire**: This update is available with a WildFire subscription and provides real-time malware and antivirus signatures created as a result of the analysis done by the WildFire cloud service. As a best practice, schedule the firewall to retrieve WildFire updates every minute. If you have a Threat Prevention subscription and not a WildFire subscription, you must wait 24 to 48 hours for the WildFire signatures to be added into the antivirus update.
- **WF-Private**: Provides malware signatures generated by an on-premises WildFire appliance.

1.6.3 Scheduling and staggering updates on HA pair

You can view the latest updates, read the release notes for each update, and then select the update you want to download and install. You also can revert to a previously installed version of an update.

Always review content Release Notes for the list of the newly identified and modified applications and threat signatures that the content release introduces:

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION	DOCUMENTATION
Antivirus	Last checked: 2020/06/01 17:37:31 UTC	Schedule: None								
3252-3763	panup-all-antivirus-3252-3763		Full	111 MB	1624f9fcfc3...	2020/02/10 13:34:15 UTC	✓ previously		Revert	Release Notes
3312-3823	panup-all-antivirus-3312-3823		Full	99 MB	091ba98d7a...	2020/04/09 11:01:30 UTC				Release Notes
3362-3873	panup-all-antivirus-3362-3873		Full	102 MB		2020/05/28 11:01:06 UTC			Download	Release Notes
3363-3874	panup-all-antivirus-3363-3874		Full	101 MB		2020/05/29 11:01:09 UTC			Download	Release Notes
3364-3875	panup-all-antivirus-3364-3875		Full	100 MB		2020/05/30 11:00:29 UTC			Download	Release Notes
3365-3876	panup-all-antivirus-3365-3876		Full	100 MB		2020/05/31 14:23:23 UTC			Download	Release Notes
3366-3877	panup-all-antivirus-3366-3877		Full	98 MB		2020/06/01 16:06:52 UTC	✓		Install	Release Notes
Applications and Threats	Last checked: 2020/06/01 17:36:59 UTC	Schedule: Every Wednesday at 01:02 (Download only)								
8266-6066	panupv2-all-contents-8266-6066	Apps, Threats	Full	50 MB		2020/05/01 23:17:14 UTC			Download	Release Notes
8267-6070	panupv2-all-contents-8267-6070	Apps, Threats	Full	50 MB		2020/05/06 02:12:12 UTC			Download	Release Notes
8268-6073	panupv2-all-contents-8268-6073	Apps, Threats	Full	50 MB		2020/05/07 23:00:08 UTC			Download	Release Notes
8269-6074	panupv2-all-contents-8269-6074	Apps, Threats	Full	50 MB		2020/05/08 21:48:30 UTC			Download	Release Notes
8270-6076	panupv2-all-contents-8270-6076	Apps, Threats	Full	50 MB		2020/05/12 15:04:19 UTC			Download	Release Notes
8271-6079	panupv2-all-contents-8271-6079	Apps, Threats	Full	50 MB		2020/05/13 02:33:59 UTC			Download	Release Notes
8272-6086	panupv2-all-contents-8272-6086	Apps, Threats	Full	50 MB		2020/05/15 03:12:06 UTC	✓ previously		Revert	Release Notes
8273-6091	panupv2-all-contents-8273-6091	Apps, Threats	Full	50 MB		2020/05/16 06:56:18 UTC			Download	Release Notes
8274-6098	panupv2-all-contents-8274-6098	Apps, Threats	Full	50 MB		2020/05/18 01:08:13 UTC			Download	Release Notes
8275-6101	panupv2-all-contents-8275-6101	Apps, Threats	Full	50 MB		2020/05/19 23:25:38 UTC		✓	Review Policies Review Apps	Release Notes
8276-6104	panupv2-all-contents-8276-6104	Apps, Threats	Full	50 MB		2020/05/22 02:59:18 UTC			Download	Release Notes
8277-6107	panupv2-all-contents-8277-6107	Apps, Threats	Full	50 MB		2020/05/23 01:11:27 UTC			Install	Release Notes

You can download updates directly from the Palo Alto Networks update server. You also can download the updates to another system such as a user desktop or a Panorama management appliance and then upload them to the firewall. Whether you download an update through the web or upload an update from Panorama, the update will appear in the list of available updates at **Device > Dynamic Updates**. Click **Install** to install the updates.

Downloading Updates

WildFire	Last checked: 2016/01/12 14:10:06 PST	Schedule: None						
28675-29396	panupv2-all-wildfire-28675-29396.candidate	PAN-OS 7.1 and later	Full	4 MB	2016/01/12 14:08:33 PST			Download

Installing Updates

28676-29397	panupv2-all-wildfire-28676-29397.candidate	PAN-OS 7.1 and later	Full	4 MB	2016/01/12 14:13:34 PST	✔		Install

Software Updates

PAN-OS updates are managed in the **Device > Software** section of the web interface. You must perform a final system reboot to put the new PAN-OS software into production. This reboot is disruptive and should be done during a change control window.

The software downloads are done over the MGT interface by default. A data interface can be used to download the software using a service route. The latest version of applications and threats must be installed to complete the software installation. If your firewall does not have internet access from the management port, you can download the software image from the Palo Alto Networks Support Portal and then manually **Upload** it to your firewall.

Before you upgrade to a newer version of software:

- Always review the release notes to determine any impact of upgrading to a newer version of software.
- Ensure that the firewall is connected to a reliable power source. A loss of power during an upgrade can make the firewall unusable.
- Although the firewall automatically creates a configuration backup, follow best practice and create and externally store a backup before you upgrade.

To upgrade to a newer version of software, complete the following steps:

1. Ensure that you follow the correct upgrade path. When you upgrade, typically you must download the x.0 base release before you install the maintenance or feature release. For example, to upgrade from 7.x.y to 8.x.y, download both 8.0 and 8.x.y. 8.0 automatically is installed when you install 8.x.y.
2. Select **Device Software** and click **Check Now** to display the latest PAN-OS updates.
3. Locate and **Download** the applicable PAN-OS software.
4. After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image:

VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION	
9.2.0-b30	788 MB	2020/04/06 15:29:53	Downloaded		Install	Release Notes
9.2.0-b36	796 MB	2020/05/06 04:18:05	Downloaded	✓	Reinstall	Release Notes

5. After the installation completes successfully, reboot the firewall.

1.6.4 References

- Deploy Applications and Threats Content Updates, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/app-and-threat-content-updates/configure-app-threat-updates

`

- Manage New App-IDs Introduced in Content Releases, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases
- Managing dynamic updates from Panorama, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/manage-software-and-content-updates

1.7 Create and apply security zones to policies

1.7.1 Identify zone types

Security Zones
Palo Alto Networks firewalls use security zones to analyze, control, and log network traffic as it traverses from one zone interface to another zone interface. Zones logically group networks that contain particular types of traffic that are contained within defined security classifications. Examples of such classifications are Internet, Data Center Applications, Users, IT Infrastructure, and Customer Data.

Security zones are divided into two broad categories: Intrazone and Interzone. Security zones contain one or more physical or virtual interfaces. An interface can belong to only one zone. Intrazone traffic, by default, allows traffic to flow between interfaces that exist in the same zone. Interzone traffic, by default, denies traffic from flowing between interfaces that exist in different zones.

Security policy rules are applied to zones (not interfaces) to allow or deny traffic, apply QoS, perform NAT, apply Security profiles, or set logging parameters. Security policy rules are described in another section of this study guide.

1.7.2 External types

The following diagram is an example of network segments partitioned into multiple zones based on their security classification. You should make the zones and the corresponding Security policy rules as definitive as possible to reduce your network's attack surface. All zone names are custom names that the firewall administrator defines. There are five primary zone types (Layer 2, Layer 3, Tap, Virtual Wire, and Tunnel) that support only specific interface types; they are depicted in the following diagram. Different zone and interface types can be used simultaneously on different physical firewall interfaces. Tunnel zones became available in PAN-OS 8.0 and are used for a feature named tunnel content inspection.

A sixth zone type named External is a special zone that is available only on some firewall models. The External zone allows traffic to pass between virtual systems when multiple virtual systems are configured on the same firewall. Virtual systems are supported only on the PA-2000, PA-3000, PA-4000, PA-5000, and PA-7000 Series firewalls. The External zone type is visible in the drop-down list only when it is supported by a firewall with the virtual systems feature enabled.

Note that MGT and HA interfaces are not assigned to a zone.

`

Tap Interface
Layer 2 Interface
Loopback Interface
Layer 3 Interface
VLAN Interface
Tunnel Interface
Virtual Wire Interface
No interfaces on Tunnel Zones
Tap Zone
Layer 2 Zone
Layer 3 Zone
Virtual Wire Zone
Tunnel Zone
Layer 2 Zone
Layer 3 Zone
Virtual Wire Zone
Tunnel Zone
No Interfaces on Tunnel Zones
Layer 2 Interface
Loopback Interface
Layer 3 Interface
VLAN Interface
Tunnel Interface
Virtual Wire Interface

`

1.7.3 Layer 2

Layer 2 interfaces are used to switch traffic between other Layer 2 interfaces. Before switching can take place, each Layer 2 interface must be assigned to a VLAN object. Assignment of interfaces that belong to the same VLAN but exist in different Layer 2 zones enables you to analyze, shape, manage, and decrypt the traffic. Layer 2 traffic can route to other Layer 3 interfaces using a Layer 3 VLAN interface. Note that Layer 2 interfaces do not participate in spanning tree other than forward BPDUs.

1.7.4 Layer 3

The following figure shows that the Layer 3 zone allows five interface types: Layer 3 (Ethernet1/4 and 1/5), loopback, sdwan, tunnel, and vlan:

`

1.7.5 Tap

Tap: A Tap interface monitors traffic that is connected to a network switch's MIRROR/SPAN port. This mirrored traffic is forwarded by a switch port to a firewall's Tap interface and is analyzed for App-ID, User-ID, Content-ID, and other traffic, just like any other normal data traffic that would pass through the firewall. Before traffic can be logged, you must configure a Security policy that includes the Tap zone. Tap interfaces are easy to deploy and can be implemented without disruption to your existing network. Tap mode offers visibility in the Traffic log and the ACC tab. You can use the information to help configure Security policy rules and to make other firewall configuration changes. Tap traffic is not managed (blocked, allowed, or shaped). Tap interfaces must be assigned to a Tap zone.

To configure a Tap interface, go to **Network > Interfaces > Ethernet > <select_interface>**.

1.7.6 VWire

A Virtual Wire interface is used to pass traffic through a firewall by binding two Ethernet interfaces and allowing traffic to pass between them. Virtual Wire interfaces often are placed between an existing firewall and a secured network to enable analysis of the traffic before actually migrating from a legacy firewall to a Palo Alto Networks firewall.

- No IP or MAC addresses are assigned to Virtual Wire interfaces. No routing or switching is done on a Virtual Wire interface. A Virtual Wire interface that receives a frame or packet ignores any Layer 2 or Layer 3 addresses for switching or routing purposes. However, it applies your Security or NAT policy rules before passing an allowed frame or packet over the virtual wire to the second Virtual Wire interface and on to the network device connected to it. A virtual wire requires no changes to adjacent network devices. A virtual wire can bind two Ethernet interfaces of the same medium (both either copper or fiber) or bind a copper interface to a fiber interface.
- Two Virtual Wire interfaces, each in a virtual wire zone (the zone can be the same or different), and a virtual wire object are required to complete a virtual wire configuration. The following figure shows one interface in one zone (Internet) and the other interface in another zone (Inside). If both interfaces are in different zones (interzone traffic), all traffic will be inspected by Security policy rules until sessions can be established, and then you can check for User-ID, App-ID, and Content-ID and perform logging, QoS, decryption, LLDP, zone protection, DoS protection, and NAT.
- If both interfaces are in the same zone (intrazone traffic), all the traffic would be allowed by default, and sessions can be easily established. However, you also can check for User-ID, App-ID, and Content-ID and perform logging, QoS, decryption, LLDP, zone protection, DoS protection, and NAT.
- Virtual Wire interfaces can be subdivided into Virtual Wire subinterfaces that can be used to classify traffic according to VLAN tags, IP addresses, IP ranges, or subnets. Use of subinterfaces enables you to separate traffic into different zones for more granular control than regular (non-subinterface) Virtual Wire interfaces.

`

To configure a virtual wire object, go to **Network > Virtual Wires > Add**:

To configure a Virtual Wire interface, go to **Network > Interfaces > Ethernet > <select_interface>**:

Virtual Wire Subinterfaces

Virtual wire deployments can use Virtual Wire subinterfaces to separate traffic into different zones. Virtual Wire subinterfaces provide flexibility in enforcing distinct policies when you need to manage traffic from multiple customer networks. Virtual Wire subinterfaces enable you to control and separate traffic by specifying criteria such as VLAN tags and IP classifiers. IP classifiers consist of host IP addresses, IP subnets, and IP ranges. Assign each subinterface to a different zone, and then enforce Security policy rules for the traffic that matches the defined criteria. Note that zones can belong to separate virtual systems.

To configure a Virtual Wire subinterface, go to **Network > Interfaces > Ethernet** and select, but do not open, a Virtual Wire interface. Then click **Add Subinterfaces** at the bottom of the web interface window:

`

Virtual Wire Subinterface

1.7.7 Tunnel

Tunnel: A Tunnel interface is a logical (virtual) interface used with VPN tunnels to deliver encrypted traffic between two endpoints. The Tunnel interface must belong to a security zone before policy can be applied, and it must be assigned to a virtual router to use the existing routing infrastructure. A Tunnel interface does not require an IP address to route traffic between the sites. An IP address is required only if you want to enable tunnel monitoring or if you are using a dynamic routing protocol to route traffic across the tunnel.

`

1.8 Identify and configure firewall interfaces

1.8.1 Different types of interfaces

The interface configurations of firewall data ports enable traffic to enter and exit the firewall. A Palo Alto Networks firewall can operate in multiple deployments simultaneously because you can Configure Interfaces to support different deployments. For example, you can configure the Ethernet interfaces on a firewall for virtual wire, Layer 2, Layer 3, and Tap mode deployments. The interfaces that the firewall supports are:

- **Physical Interfaces**—The firewall supports two kinds of media—copper and fiber-optic—that can send and receive traffic at different transmission rates. You can configure Ethernet interfaces as the following types: Tap, High Availability (HA), Log Card (interface and subinterface), Decrypt Mirror, Virtual Wire (interface and subinterface), Layer 2 (interface and subinterface), Layer 3 (interface and subinterface), and aggregate Ethernet. The available interface types and transmission speeds vary by hardware model.
- **Logical Interfaces**—These include virtual local area network (VLAN) interfaces, loopback interfaces, and tunnel interfaces. You must set up the physical interface before defining a VLAN or a tunnel interface.

1.8.2 How interface types affect Security policies

PAN-OS software has the following Ethernet interface types: Tap, Virtual Wire, Layer 2, Layer 3, and High Availability (HA). (HA interfaces are not discussed in this section). A firewall can be configured with multiple instances of each interface type to accommodate its functional requirements within a network. The following figure shows how a firewall can be used in Tap, Virtual Wire, Layer 2, or Layer 3 mode.

Ethernet Interface Types

`

• App-ID, Content-ID, and User-ID visibility without inline deployment • Traffic logged to provide visibility	• SSL decryption (no encryption) • Allows NAT	• All the Virtual Wire mode capabilities, including Layer 2 or Layer 3 services: virtual routers, VPN, and routing protocols

Other available interface types include the following:

- **Decrypt Mirror**: This feature enables decrypted traffic from a firewall to be copied and sent to a traffic-collection tool that can receive raw packet captures, such as NetWitness or Solera, for archiving and analysis. Decrypt Mirror often is used to route decrypted traffic through an external interface to a data loss prevention (DLP) service. DLP is a product category for products that scan internet-bound traffic for keywords and patterns that identify sensitive information. Note that a free license is required to use this feature. This feature is not available on the VM-Series firewalls.

- Log Card: For PA-7000 Series firewalls only. A log card data port performs log forwarding for syslog, email, Simple Network Management Protocol (SNMP), and WildFire file forwarding.

`

One data port on a PA-7000 must be configured as a Log Card interface because the MGT interface cannot handle all the logged traffic.

- Aggregate: Used to bundle multiple physical HA3, Virtual Wire, Layer 2, or Layer 3 interfaces into a logical interface for better performance (via load balancing) and redundancy using IEEE 802.1AX (LACP) link aggregation. The interface types to be bundled must be the same. VM-Series models do not support Aggregate Ethernet (AE) interface groups.
- HA: Each HA interface has a specific function. One HA interface is for configuration synchronization and heartbeats; the other HA interface is for state synchronization. If active/active high availability is enabled, the firewall also can use a third HA interface to forward packets.
- Management: MGT interfaces are used to manage a firewall using a network cable.
- Loopback: Loopback interfaces are Layer 3 virtual interfaces that connect to virtual routers in the firewall. Loopback interfaces are used for multiple network engineering and implementation purposes. They can be destination configurations for DNS sinkholes, GlobalProtect service interfaces (portals and gateways), routing identification, and more.
- Tunnel: A Tunnel interface is a logical (virtual) interface used with VPN tunnels to deliver encrypted traffic between two endpoints. The tunnel interface must belong to a security zone before policy can be applied, and it must be assigned to a virtual router to use the existing routing infrastructure. A tunnel interface does not require an IP address to route traffic between the sites. An IP address is required only if you want to enable tunnel monitoring or if you are using a dynamic routing protocol to route traffic across the tunnel.
- SD-WAN: Create and configure a virtual SD-WAN interface to specify one or more physical, SD-WAN-capable Ethernet interfaces that go to the same destination, such as to a specific hub or to the internet. In fact, all links in a virtual SD-WAN interface must be the same type: all VPN tunnel links or all direct internet access (DIA) links. An SD-WAN interface works with an SD-WAN Interface profile that defines the characteristics of the ISP connections. Details about these interfaces and their configuration are beyond the scope of the PCNSA certification.

Tap Virtual Wire, Layer 2, and Layer 3 Interfaces

Tap: A Tap interface monitors traffic that is connected to a network switch's MIRROR/SPAN port. This mirrored traffic is forwarded by a switch port to a firewall's Tap interface and is analyzed for App-ID, User-ID, Content-ID, and other traffic, just like any other normal data traffic that would pass through the firewall. Before traffic can be logged, a Security policy must be configured that includes the Tap zone. Tap interfaces are easy to deploy and can be implemented without disruption to your existing network. Tap mode offers visibility in the Traffic log and also in the ACC tab. The information can be used to help configure Security policy rules, and to make other firewall configuration changes. Tap traffic is not managed (blocked, allowed, or shaped). TAP interfaces must be assigned to a Tap zone.

`

To configure a Tap interface, go to **Network > Interfaces > Ethernet > <select_interface>**.

Virtual Wire

A Virtual Wire interface is used to pass traffic through a firewall by binding two Ethernet interfaces and allowing traffic to pass between them. Virtual Wire interfaces often are placed between an existing firewall and a secured network to enable analysis of the traffic before actually migrating from a legacy firewall to a Palo Alto Networks firewall.

`

- No IP or MAC addresses are assigned to Virtual Wire interfaces. No routing or switching is done on a Virtual Wire interface. A Virtual Wire interface that receives a frame or packet ignores any Layer 2 or Layer 3 addresses for switching or routing purposes, but applies your security or NAT policy rules before passing an allowed frame or packet over the virtual wire to the second Virtual Wire interface and on to the network device connected to it. A virtual wire requires no changes to adjacent network devices. A virtual wire can bind two Ethernet interfaces of the same medium (both either copper or fiber) or bind a copper interface to a fiber interface.

- Two Virtual Wire interfaces, each in a virtual wire zone (the zone can be the same or different), and a Virtual Wire object are required to complete a virtual wire configuration. The following figure shows one interface in one zone (Internet) and the other interface in another zone (Inside). If both interfaces are in different zones (interzone traffic), all traffic will be inspected by Security policy rules until sessions can be established, and then you can check for User-ID, App-ID, and Content-ID, and perform logging, QoS, decryption, LLDP, zone protection, DoS protection, and NAT.

- If both interfaces are in the same zone (intrazone traffic), all the traffic would be allowed by default, and sessions can be easily established. However, you also can check for User-ID, App-ID, and Content-ID, and perform logging, QoS, decryption, LLDP, zone protection, DoS protection, and NAT.

- Virtual Wire interfaces can be subdivided into Virtual Wire subinterfaces that can be used to classify traffic according to VLAN tags, IP addresses, IP ranges, or subnets. Use of subinterfaces enables you to separate traffic into different zones for more granular control than regular (non-subinterface) Virtual Wire interfaces.

`

To configure a Virtual Wire object, go to **Network > Virtual Wires > Add**:

To configure a Virtual Wire interface, go to **Network > Interfaces > Ethernet > <select_interface>**:

Layer 2 Interfaces

Layer 2 interfaces are used to switch traffic between other Layer 2 interfaces. Before switching can take place, each Layer 2 interface must be assigned to a VLAN object. Assignment of interfaces that belong to the same VLAN but exist in different Layer 2 zones enables you to analyze, shape, manage, and decrypt the traffic. Layer 2 traffic can route to other Layer 3 interfaces using a Layer 3 VLAN interface. Note that Layer 2 interfaces do not participate in spanning tree other than forward BPDUs.

To configure a VLAN object, go to **Network > VLAN > Add**:

To configure a Layer 2 interface, go to **Network > Interfaces > Ethernet > <select_interface>**:

Layer 3 Interfaces

In a Layer 3 deployment, the firewall routes traffic between multiple interfaces. A virtual router object must exist for the firewall to route traffic between Layer 3 interfaces. Layer 3 interfaces are assigned IP addresses. PAN-OS software supports both IPv4 and IPv6 addressing. As is the case in most interface types, Layer 3 traffic can be monitored, analyzed, managed, shaped, translated, and encrypted or decrypted. If a tunnel is used for routing or if tunnel monitoring is turned on, the tunnel needs an IP address. The Advanced tab contains options that enable you to configure a variety of Layer 3 interface settings such as MTU, static ARP, LLDP, IPv6 NDP, link speed, and duplex settings. You can configure both IPv4 and IPv6 addresses on a single interface.

`

Loopback interfaces are Layer 3 virtual interfaces that connect to virtual routers in the firewall. Loopback interfaces are used for multiple network engineering and implementation purposes. They can be destination configurations for DNS sinkholes, GlobalProtect service interfaces (portals and gateways), routing identification, and more.

Unlike Tap, Virtual Wire, or Layer 2 interfaces, Layer 3 interfaces can be used to manage firewalls using an Interface Management profile. An Interface Management profile protects the firewall from unauthorized access by defining the protocols, services, and IP addresses that a firewall Layer 3 interface permits for management traffic. Interface Management profiles are discussed in more detail in a different section of this study guide.

You can configure a Layer 3 interface with one or more static IPv4 addresses or as a DHCP client. A single Layer 3 interface can be assigned multiple IPv4 addresses, although they should not be in the same subnet. You can configure a Layer 3 interface with one or more IPv6 addresses, either as a link-local address or a global address.

Layer 3 interfaces also can be configured as subinterfaces, where each subinterface is assigned a unique IP address.

To configure a virtual router object, go to **Network > Virtual Routers > Add**:

To configure a Layer 3 interface, go to **Network > Interfaces > Ethernet > <select_interface>**:

`

Aggregate Interfaces

An aggregate interface group uses IEEE 802.1AX link aggregation to combine multiple Ethernet interfaces into a single virtual interface that connects the firewall to another network device or another firewall. An aggregate group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy; when one interface fails, the remaining interfaces continue supporting traffic.

Before you configure an aggregate group, you must configure its interfaces. The hardware media can differ among the interfaces assigned to an aggregate group (for example, you can mix fiber optic and copper), but the bandwidth and interface type must be the same.

Before you can create an Aggregate interface, you must first create an aggregate interface group. Select **Network > Interfaces > Ethernet** and **Add Aggregate Group**:

Provide a group ID number and configure LACP protocol settings as required. You must choose the **Interface Type** of the aggregate interface group from the options shown. After you select the type, you might need to configure the interface. The following screenshot shows the Layer 3 configuration options:

After an aggregate interface group is created, it is added to the available Ethernet interfaces list:

To add physical Ethernet interfaces the group, set the physical **Interface Type** to **Aggregate Ethernet** and select the **Aggregate Group** to which they are assigned:

`

The following screenshot illustrates an aggregate interface group with three assigned physical Ethernet interfaces:

The PA-3200 Series, PA-5200 Series, and most PA-7000 Series firewalls support 16 aggregate Ethernet (AE) interface groups. All other physical firewall appliances support eight. The exception is the PA-7000 Series firewall with PA-7000-100G-NPC-A and SMC-B, which supports 32 AE interface groups. On this firewall, QoS is supported on only the first 16 AE interface groups. On the other supported firewall models, QoS is supported on only the first eight AE interface groups. VM-Series firewalls do not support aggregate interface groups.

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

1.9.1 Steps to create a static route

Static routes have the lowest administrative distances by default, other than locally connected routes. This default administrative distance value is 10, which can be changed.

Static routes have a default metric value of 10, which also can be changed. If you have multiple static routes to the same destination, you can make one preferable over the other by changing the metric. The default metric in the following example was changed from its default value of 10 to 5:

`

1.9.2 How to use the routing table

By viewing the routing table, you can see whether OSPF routes have been established. The routing table is accessible from either the web interface or the CLI. If you are using the CLI, use the following commands:

- show routing route
- show routing fib

If you are using the web interface to view the routing table, use the following workflow:

Step 1: Select **Network > Virtual Routers** and in the same row as the virtual router you are interested in, click the **More Runtime Stats** link.

Step 2: Select **Routing > Route Table** and examine the **Flags** column of the routing table for routes that were learned by OSPF.

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

Virtual Routers
PAN-OS software provides two virtual route engines of which one type can run at a given time: the BGP route engine that supports only BGP and static routing and the legacy route engine that supports multiple dynamic routing protocols. The following firewall models support the BGP route engine:

`

- PA-7000 Series
- PA-5200 Series
- PA-3200 Series
- VM-Series

Although a supported firewall can have a configuration that uses the legacy route engine and a configuration that uses the BGP route engine, only one route engine is in effect at a time. Each time you change the engine that the firewall will use (enable or disable Advanced Routing to access the BGP route engine or legacy route engine, respectively), you must commit the configuration and reboot the firewall for the change to take effect.

The BGP route engine supports only one logical router (known as a virtual router on the legacy route engine).

Both route engines obtain routes to remote subnets either by the manual addition of static routes or the dynamic addition of routes using dynamic routing protocols. Each Layer 3 Ethernet, Loopback, VLAN, and Tunnel interface defined on the firewall must be associated with a virtual router. Although each interface can belong to only one virtual router, you can configure routing protocols and static routes using either routing engine.

Dynamic routing protocols available on a legacy virtual router are as follows:

- BGP4
- OSPFv2
- OSPVv3
- RIPv2

Multicast routing protocols available on a legacy virtual router are as follows:

- IGMPv1, IGMPv2, IGMPv3
- PIM-SM, PIM-ASM, PIM-SSM

Dynamic routing protocols have administrative distances applied to them that are used to determine the best route to a destination when multiple routes are available from two different routing protocols. The default administrative distances can be modified.

You can create multiple legacy virtual routers, each of which maintains a separate set of routes that aren't shared between these legacy virtual routers, thus enabling you to configure different routing behaviors for different interfaces. Legacy virtual routers can route to other legacy virtual routers within the same firewall if a next hop is specified to reach another legacy virtual router.

The firewall initially populates its learned routes into the firewall's IP routing information base (RIB). The virtual router obtains the best route from the RIB, and then places it in the forwarding information base (FIB). Packets then are forwarded to the next hop router defined in the FIB.

`

1.9.4 How to configure route monitoring

Legacy Virtual Router General Configuration Settings

The administrative distances are shown on the right side of the following screenshot. Most of these distances are consistent with the values in RFCs, but you can modify them to reflect the needs of your environment.

Legacy Static Route Configuration Settings

Static routes have the lowest administrative distances by default, other than locally connected routes. This default administrative distance value is 10, which can be changed.

Static routes have a default metric value of 10, which also can be changed. If you have multiple static routes to the same destination, you can make one preferable over the other by changing the metric. The default metric in the following example was changed from its default value of 10 to 5:

`

Path Monitoring for Static Routes Configuration Settings

Path monitoring monitors upstream interfaces on remote, reliable devices using ICMP pings. If the path monitoring fails, an associated static route is removed from the routing table. An alternative route then can be used to route traffic.

Path Monitoring	Select to enable path monitoring for the static route.
Failure Condition	Select the condition under which the firewall considers the monitored path down and thus the static route down: • **Any**—If any one of the monitored destinations for the static route is unreachable by ICMP, the firewall removes the static route from the RIB and FIB and adds the dynamic or static route that has the next lowest metric going to the same destination to the FIB. • **All**—If all of the monitored destinations for the static route are unreachable by ICMP, the firewall removes the static route from the RIB and FIB and adds the dynamic or static route that has the next lowest metric going to the same destination to the FIB. Select **All** to avoid the possibility of a single monitored destination signaling a static route failure when that monitored destination is simply offline for maintenance, for example.
Preemptive Hold Time (min)	Enter the number of minutes a downed path monitor must remain in Up state—the path monitor evaluates all of its member monitored destinations and must remain Up before the firewall reinstalls the static route into the RIB. If the timer expires without the link going down or flapping, the link is deemed stable, path monitor can remain Up, and the firewall can add the static route back into the RIB. If the link goes down or flaps during the hold time, path monitor fails and the timer restarts when the downed monitor returns to Up state. A **Preemptive Hold Time** of zero causes the firewall to reinstall the static route into the RIB immediately upon the path monitor coming up. Range is 0-1,440; default is 2.
Name	Enter a name for the monitored destination (up to 31 characters).
Enable	Select to enable path monitoring of this specific destination for the static route; the firewall sends ICMP pings to this destination.
Source IP	Select the IP address that the firewall will use as the source in the ICMP ping to the monitored destination: • If the interface has multiple IP addresses, select one. • If you select an interface, the firewall uses the first IP address assigned to the interface by default. • If you select **DHCP (Use DHCP Client address)**, the firewall uses the address that DHCP assigned to the interface. To see the DHCP address, select **Network** > **Interfaces** > **Ethernet** and in the row for the Ethernet interface, click on **Dynamic DHCP Client**. The IP Address appears in the Dynamic IP Interface Status window.
Destination IP	Enter a robust, stable IP address or address object for which the firewall will monitor the path. The monitored destination and the static route destination must use the same address family (IPv4 or IPv6)
Ping Interval (sec)	Specify the ICMP ping interval in seconds to determine how frequently the firewall monitors the path (pings the monitored destination; range is 1-60; default is 3).
Ping Count	Specify the number of consecutive ICMP ping packets that do not return from the monitored destination before the firewall considers the link down. Based on the **Any** or **All** failure condition, if path monitoring is in failed state, the firewall removes the static route from the RIB (range is 3-10; default is 5). For example, a Ping Interval of 3 seconds and Ping Count of 5 missed pings (the firewall receives no ping in the last 15 seconds) means path monitoring detects a link failure. If path monitoring is in failed state and the firewall receives a ping after 15 seconds, the link is deemed up; based on the **Any** or **All** failure condition, path monitoring to **Any** or **All** monitored destinations can be deemed up, and the Preemptive Hold Time starts.

This static route is removed from the routing table until reachability to the next hop is obtained.

Virtual Router Forwarding Information Base

The following screenshot shows the CLI output of the FIB. A GUI runtime display also is available.

```
admin@firewall-a> show routing fib

total virtual-router shown :              1


--------------------------------------------------------------------------------
virtual-router name: default
interfaces:
   ethernet1/1 ethernet1/2


route table:
flags: u - up, h - host, g - gateway, e - ecmp, * - preferred path

maximum of fib entries for device:                2500
maximum of IPv4 fib entries for device:           2500
maximum of IPv6 fib entries for device:           2500
number of fib entries for device:                 4
maximum of fib entries for this fib:              2500
number of fib entries for this fib:               4
number of fib entries shown:                      4

id      destination          nexthop            flags  interface          mtu
--------------------------------------------------------------------------------
9       10.0.0.0/24          0.0.0.0            u      ethernet1/1        1500
8       10.0.0.1/32          0.0.0.0            uh     ethernet1/1        1500
4       172.16.0.0/24        0.0.0.0            u      ethernet1/2        1500
3       172.16.0.1/32        0.0.0.0            uh     ethernet1/2        1500
--------------------------------------------------------------------------------
```

BGP Route Engine Configuration

To enable the BGP route engine on a firewall, select of **Advanced Routing** at **Device > Setup > Management** and edit the **General Settings**:

`

After you make the selection, the firewall must commit the configuration and reboot. After the reboot is complete the BGP routing engine requires the creation of a single **Logical Router** with appropriate settings:

BGP Routing Profiles can be created that specify specific BGP routing feature behavior.

1.10 Sample Questions

Q1. What are two firewall management methods? (Choose two.)

a. CLI
b. RDP
c. VPN
d. XML API

Q2. Which two devices are used to connect a computer to the firewall for management purposes? (Choose two.)

a. Rollover cable
b. Serial cable
c. RJ-45 Ethernet cable
d. USB cable

Q3. What is the default IP address assigned to the MGT interfaces of a Palo Alto Networks firewall?

a. 192.168.1.1
b. 192.168.1.254
c. 10.0.0.1
d. 10.0.0.254

Q4. What are the two default services that are available on the MGT interface? (Choose two.)

a. HTTPS
b. SSH
c. HTTP
d. Telnet

`

Q5. True or false? Service route traffic has Security policy rules applied against it.

a. true
b. false

Q6. Service routes may be used to forward which two traffic types out of a data port? (Choose two.)

a. External dynamic lists
b. MineMeld
c. Skype
d. Palo Alto Networks updates

Q7. Which command must be performed on the firewall to activate any changes?

a. Commit
b. Save
c. Load
d. Import

Q8 Which command backs up configuration files to a remote network device?

a. Import
b. Load
c. Copy
d. Export

Q9. The command load named configuration snapshot overwrites the current candidate configuration with which three items? (Choose three.)

a. Custom-named candidate configuration snapshot (instead of the default snapshot)
b. Custom-named running configuration that you imported
c. Snapshot.xml
d. Current running configuration (running-config.xml)
e. Palo Alto Networks updates

Q10. What are two firewall management methods? (Choose two.)

a. CLI
b. RDP
c. VPN
d. XML API

Q11. True or false? A Palo Alto Networks firewall automatically provides a backup of the configuration during a software upgrade.

a. true
b. false

Q12. If you have a Threat Prevention subscription but not a WildFire subscription, how long must you wait for the WildFire signatures to be added into the antivirus update?

a. 1 to 2 hours
b. 2 to 4 hours
c. 10 to 12 hours
d. 24 to 48 hours

`

Q13. Which three actions should you complete before you upgrade to a newer version of software? (Choose three.)

a. Review the release notes to determine any impact of upgrading to a newer version of software.
b. Ensure that the firewall is connected to a reliable power source.
c. Export the device state.
d. Create and externally store a backup before you upgrade.
e. Put the firewall in maintenance mode.

Q14. Which two default zones are included with the PAN-OS software? (Choose two.)

a. Interzone
b. Extrazone
c. Intrazone
d. Extranet

Q15. Which two zone types are valid options? (Choose two.)

a. Trusted
b. Tap
c. Virtual wire
d. Untrusted
e. DMZ

Q16. Which two statements about interfaces are correct? (Choose two.)

a. Interfaces must be configured before you can create a zone.
b. Interfaces do not have to be configured before you can create a zone.
c. An interface can belong to only one zone.
d. An interface can belong to multiple zones.

Q17. Which two interface types can belong in a Layer 3 zone? (Choose two.)

a. Loopback
b. Tap
c. Tunnel
d. Virtual Wire

Q18. What are used to control traffic through zones?

a. Access lists
b. Security policy lists
c. Security policy rules
d. Access policy rules

Q19. For inbound inspection, which two actions can be done with a Tap interface? (Choose two.)

a. Encrypt traffic
b. Decrypt traffic
c. Allow or block traffic
d. Log traffic

`

Q20. Which two actions can be done with a Virtual Wire interface? (Choose two.)

a. NAT
b. Route
c. Switch
d. Log traffic

Q21. Which two actions can be done with a Layer 3 interface? (Choose two.)

a. NAT
b. Route
c. Switch
d. Create a virtual wire object

Q22. Layer 3 interfaces support which two items? (Choose two.)

a. NAT
b. IPv6
c. Switching
d. Spanning tree

Q23. Layer 3 interfaces support which three advanced settings? (Choose three.)

a. IPv4 addressing
b. IPv6 addressing
c. NDP configuration
d. Link speed configuration
e. Link duplex configuration

Q24. Layer 2 interfaces support which three items? (Choose three.)

a. Spanning tree blocking
b. Traffic examination
c. Forwarding of spanning tree BPDUs
d. Traffic shaping via QoS
e. Firewall management
f. Routing

Q25. Which two interface types support subinterfaces? (Choose two.)

a. Virtual Wire
b. Layer 2
c. Loopback
d. Tunnel

Q26. Which two statements are true regarding Layer 3 interfaces? (Choose two.)

a. You can configure a Layer 3 interface with one or more IP addresses as a DHCP client.
b. A Layer 3 interface can only have one DHCP assigned address.
c. You can assign only one IPv4 address to the same interface.
d. You can enable an interface to send IPv4 router advertisements by selecting the Enable Router Advertisement check box on the Router Advertisement tab.
e. You can apply an Interface Management profile to the interface.

`

Q27. Which statement is true regarding aggregate Ethernet interfaces?

a. Members of an aggregate interface group can be of different media types.
b. An aggregate interface group can be set to a type of tap.
c. Ethernet interfaces that are members of an aggregate interface group must have the same transmission speeds.
d. A Layer 3 aggregate interface group can have more than one IP assigned to it.
e. Members of aggregate Ethernet interfaces can be assigned to different virtual routers.

Q28. What is the default administrative distance of a static route within the PAN-OS software?

a. 1
b. 5
c. 10
d. 100

Q29. Which two dynamic routing protocols are available in the PAN-OS software? (Choose two.)

a. RIP1
b. RIPv2
c. OSPFv3
d. EIGRP

Q30. Which value is used to distinguish the preference of routing protocols?

a. Metric
b. Weight
c. Distance
d. Cost
e. administrative distance

Q31. Which value is used to distinguish the best route within the same routing protocol?

a. Metric
b. Weight
c. Distance
d. Cost
e. Administrative distance

Q32. In path monitoring, what is used to monitor remote network devices?

a. ping
b. SSL
c. HTTP
d. HTTPS
e. link state

`

Domain 2: Managing Objects

2.1 Create and maintain address and address group objects

2.1.1 How to tag objects

You can tag objects to group related items and add color to the tag in order to visually distinguish them for easy scanning. You can create tags for the following objects: address objects, address groups, user groups, zones, service groups, and policy rules.

The firewall and Panorama support both static tags and dynamic tags. Dynamic tags are registered from a variety of sources and are not displayed with the static tags because dynamic tags are not part of the configuration on the firewall or Panorama. See Register IP Addresses and Tags Dynamically for information on registering tags dynamically. The tags discussed in this section are statically added and are part of the configuration.

You can apply one or more tags to objects and to policy rules, up to a maximum of 64 tags per object. Panorama supports a maximum of 10,000 tags, which you can apportion across Panorama (shared and device groups) and the managed firewalls (including firewalls with multiple virtual systems).

Use tags to identify the purpose of a rule or configuration object and to help you better organize your rulebase. To ensure that policy rules are properly tagged, see how to Enforce Policy Rule Description, Tag, and Audit Comment. Additionally, you can View Rules by Tag Group by first creating and then setting the tag as the Group tag.

Step 1: Create tags.

- Select **Objects > Tags**.
- On Panorama or a multiple virtual system firewall, select the **Device Group** or the **Virtual System** to make the tag available.
- **Add** a tag and enter a **Name** to identify the tag or select a zone **Name** to create a tag for a zone. The maximum length is 127 characters.
- (Optional) Select **Shared** to create the object in a shared location for access as a shared object in Panorama or for use across all virtual systems in a multiple virtual system firewall.
- (Optional) Assign a **Color** from the 17 predefined colors. By default, **Color** is **None**.

- Click **OK** and **Commit** to save your changes.

Step 2: Apply tags to policy.

- Select **Policies** and any rulebase under it.
- **Add** a policy rule and use the tagged objects you created in Step 1.
- Verify that the tags are in use.

				Source				Destination	
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	General Business Apps	Business Apps	universal	any	any	known-user	any	any	any

Step 3: Apply tags to an address object, address group, service, or service group.

- Create the object.

  For example, to create a service group, select **Objects > Service Groups > Add**.

- Select a tag (**Tags**) or enter a name in the field to create a new tag.

  To edit a tag or add color to the tag, see Modify Tags.

2.1.2 Differentiate between address objects

There are four types of address objects

- **IP Netmask**
- **IP Range**
- **IP Wildcard Mask**
- **FQDN**

Both IPv4 or IPv6 addresses are supported for the IP Netmask, IP Range, or FQDN address object types. However, IP Wildcard Mask can specify only IPv4 addresses.

To create an address object, perform the following steps:

`

1. Select **Objects > Addresses** and **Add** an address object by **Name**. The name is case-sensitive, and the name must be unique. There is a limit of 63 characters (letters, numbers, spaces, hyphens, and underscores).
2. Select the **Type** of address object.
3. Enter a **tag** to apply to the address object.
4. **Commit** changes.
5. View logs filtered by your address object.
6. View a custom report based on your address object.
7. Use a filter in the ACC to view network activity. Select **ACC > Network Activity**.

An address object of type IP Netmask, IP Range, or FQDN can specify IPv4 or IPv6 addresses. An address object of type IP Wildcard Mask can specify only IPv4 addresses.

An address object of type IP Netmask requires you to enter the IP address or network using slash notation to indicate the IPv4 network or the IPv6 prefix length—for example, 192.168.18.0/24 or 2001:db8:123:1::/64.

An address object of type IP Range requires you to enter the IPv4 or IPv6 range of addresses separated by a hyphen.

An address object of type FQDN (for example, paloaltonetworks.com) provides further ease of use because DNS provides the FQDN resolution to the IP addresses instead of you needing to know the IP addresses and manually updating them every time the FQDN resolves to new IP addresses.

An address object of type IP Wildcard Mask is useful if you define private IPv4 addresses to internal devices and your addressing structure assigns meaning to certain bits in the address. For example, the IP address of cash register 156 in the northeastern U.S. could be 10.132.1.156 based on these bit assignments:

An address object of type IP Wildcard Mask specifies which source or destination addresses are subject to a Security policy rule—or example, 10.132.1.1/0.0.2.255. A zero (0) bit in the mask indicates that the bit being compared must match the bit in the IP address that is covered by the zero. A one (1) bit in the mask (a wildcard bit) indicates that the bit being compared need not match the bit in the IP address. The following snippets of an IP address and wildcard mask illustrate how they yield four matches:

`

```
0 0 1 1     binary snippet
1 0 1 0     wildcard mask
---------
0 0 0 1     yields four matches
0 0 1 1
1 0 0 1
1 0 1 1
```

After you Create an Address Object, you can reference an address object of type IP Netmask, IP Range, or FQDN in a policy rule for Security, Authentication, NAT, NAT64, Decryption, DoS Protection, Policy-Based Forwarding (PBF), QoS, Application Override, or Tunnel Inspection; or in a NAT address pool, VPN tunnel, path monitoring, external dynamic list, Reconnaissance Protection, ACC global filter, log filter, or custom report log filter.

You can reference an address object of type IP Wildcard Mask only in a Security policy rule.

2.1.3 Static groups versus dynamic groups

In PAN-OS, you can create address objects, which can be further grouped into address groups. The most common method is to use a "static" type address group. However, the "dynamic" type address group allows for slight ease of management along with scalability.

Review the example below of a list of address objects:

Notice the tag on some objects. This will be relevant later.

Now, if you were to create a static address object, you would choose the ones you want to add.

`

This is perfectly fine for use in policies, but imagine having to manage hundreds (if not thousands) of address objects with constant additions, deletions, etc.

Note: For every address object you add/remove, you would have to include/exclude that object in each address group where that address object would be used. This can become cumbersome and makes the configuration prone to (manual) errors.

This is where dynamic address groups can shine.

With the use of tags when defining the address objects, you can use simple match criteria to create an address group. This is much more flexible because any addition/deletion only requires changing the address objects. The groups can remain untouched!

Let's look at an example.

Using the same address objects list as before, we'll create a dynamic address group.

Commit the changes and then click **more** to the entries in the group:

Only the objects with tags specified as Intranet were included in this group.

This is where the tags become useful. For this implementation of a dynamic address group, make sure to create an address object (or groups, if you wish to use the group within another group) with one or more tags.

`

You can enter a new tag or choose an already created one using the drop-down option.

You can create tags on the fly (see above image) or via **Objects > Tags**.

Moreover, we can have nested address groups with little to no additional overhead, other than adding/removing/editing the objects themselves.

2.1.4 References

- Use Tags to Group and Visually Distinguish Objects, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-tags-to-group-and-visually-distinguish-objects
- Register IP Addresses and Tags Dynamically, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/register-ip-addresses-and-tags-dynamically

`

- Create and Apply Tags, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-tags-to-group-and-visually-distinguish-objects/create-and-apply-tags

2.2 Create and maintain services and service groups

Administrator accounts control access to firewalls. By default, Palo Alto Networks firewalls have a predefined, default local admin account that has full access. Administrator accounts can be either local (internal) or non-local (external). Additional local or external administrator accounts can be created with customized administrative privileges by assigning them to Role Based admin role profiles, or you can assign administrator accounts to built-in account types using Dynamic admin roles.

Administrative Role Types
A *role* defines the type of access that an administrator has to the firewall. The two role types are **Role Based** profile roles and Dynamic roles:

- **Role Based** profile roles: These are custom roles you can configure for more granular access control over the functional areas of the web interface, CLI, and XML API. For example, you can create an Admin Role profile role for your operations staff that provides access to the firewall and network configuration areas of the web interface, and you can create a separate profile for your security administrators that provides access to Security policy definitions, logs, and reports. On a firewall with multiple virtual systems, you can select whether the role defines access for all virtual systems or specific virtual systems. After new features are added to the product, you must update the roles with corresponding access privileges; the firewall does not automatically add new features to custom role definitions.

Administrator Account Configuration

`

Role-Based Profile Types

- **Dynamic** roles: These are built-in or predefined roles that provide access to the firewall. When new features are added, the firewall automatically updates the definitions of **Dynamic** roles; you never need to manually update them. The following list identifies the access privileges associated with dynamic roles:
    - **Superuser**: Full access to the firewall, including defining new administrator accounts and virtual systems. You must have superuser privileges to create an administrative user with superuser privileges.
    - **Superuser** (read-only): Read-only access to the firewall.
    - **Virtual system administrator**: Full access to a selected virtual system (vsys) on the firewall, available only on firewalls that support virtual systems.
    - **Virtual system administrator** (read-only): Read-only access to a selected vsys on the firewall, available only on firewalls that support virtual systems.
    - **Device administrator**: Full access to all firewall settings except for defining new accounts or virtual systems.
    - **Device administrator** (read-only): Read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged-in account is visible).

`

Administrator Account Configuration

Local administrator accounts are authenticated using a local database:

External administrator accounts require an external authentication service that is specified using an authentication profile.

PAN-OS software supports the following authentication types:

- None
- Local Database
- RADIUS
- LDAP
- TACACS+
- SAML
- Kerberos

Authentication profiles provide authentication settings that you can apply to administrator accounts, SSL-VPN access, and Captive Portal. An authentication profile configuration screenshot follows:

Authentication Profiles

An authentication profile references a server profile:

A server profile includes the server name, its IP address, the service port that it is listening to, and other values. An example of a RADIUS server profile follows:

Authentication Sequence

Admin roles for external administrator accounts can be assigned to an Authentication Sequence, which includes a sequence of one or more Authentication Profiles that are processed in a specific order. The firewall checks against each Authentication Profile within the Authentication Sequence until one Authentication Profile successfully authenticates the user. If an external administrator account does not reference an Authentication Sequence, it directly references an Authentication Profile instead. A user is denied access only if authentication fails for all the profiles in the Authentication Sequence. A depiction of an Authentication Sequence follows:

Authentication Sequence

Administrator Account Passwords

To ensure tighter security, you should enable minimum password complexity requirements. These global settings are applied to all local administrator accounts and help protect the firewall against unauthorized access for administrator accounts that require stricter complexity and aging requirements than do accounts for standard administrators.

A password profile can be assigned to a local administrator account, which overrides the global password settings:

Configuration Logs

Configuration logs display entries for changes to the firewall configuration. Each entry includes the date and time, the administrator username, the IP address from where the administrator made the change, the type of client (web, CLI, or Panorama), the type of command executed, the command status (succeeded or failed), the configuration path, and the values before and after the change.

2.3 Create and maintain external dynamic lists

An external dynamic list (EDL) is a text file that you host on an external web server. The firewall uses this text file to import the following objects:

- IP addresses
- URLs
- Domains

This arrangement allows the firewall to enforce policy based on the entries in the text file list. As you update the list, the firewall dynamically imports the list and enforces policy without the need to make a configuration change or a commit.

The firewall supports the following types of external dynamic lists:

- Predefined IP address
- IP address
- Domain
- URL

You can add a maximum of 30 custom EDLs on your firewall. The EDL list limit is not applicable to Panorama.

Built-In EDLs
An active Threat Prevention license is required to obtain Palo Alto Networks built-in EDLs. These built-in EDLs protect your network against malicious hosts. Built-in EDLs include the following:

- Palo Alto Networks Bulletproof IP Addresses
- Palo Alto Networks High-Risk IP Addresses
- Palo Alto Networks Known Malicious IP Addresses

With the Threat Prevention license, the firewall receives updates for these feeds in content updates. You cannot modify the contents of built-in EDLs.

2.3.1 References

- Formatting Guidelines for an External Dynamic List, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/formatting-guidelines-for-an-external-dynamic-list
- Built-in External Dynamic Lists, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edls

2.4 Configure and maintain application filters and groups

2.4.1 When to use filters versus groups

Application Filters
An administrator can dynamically categorize multiple applications into an application filter based on the specific attributes Category, Subcategory, Tags, Risk, and Characteristic. For example, if you want to allow all audio streaming applications, you could create an application filter that includes the subcategory of audio-streaming, which automatically would add all applications to the filter from the App-ID database that are subcategorized as audio-streaming. The filter then would be added as an application to a Security policy rule. Application filters simplify the process of ensuring that all applications that meet any attribute are added to a Security policy automatically.

Starting with PAN-OS 9.1, you can configure an application filter to filter for a group of applications based on their assigned application tags. Palo Alto Networks now assigns one or more predefined tags to some applications in the App-ID database. You also can create and assign your own custom tag to an application. You can build an application filter using these tags and then use the application filter in policy rules to control access to the applications. If application tags are updated and they are part of an application filter, then policy could begin to treat such applications differently.

Application Groups

An administrator can manually categorize multiple applications into an application group based on App- ID. This application group then is added to one or more Security policy rules as required, which streamlines firewall administration. Instead of a firewall administrator individually adding different applications into a Security policy, they only need to add the application group to the policy.

Application groups often are used to simplify Security, QoS, and PBF policy rule implementation.

Nesting Application Groups and Filters

An administrator can nest application groups and filters. They can combine multiple applications and multiple application filters into an application group. They can then combine one or more application groups into an application group. The final application group then can be added to a Security policy rule.

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

Application Characteristics

All applications in the App-ID database are defined by characteristics shown in the image below. The names of the characteristics are self-explanatory.

2.5 Sample Questions

Q1. Which two statements are true about a Role Based Admin Role Profile role? (Choose two.)

a. It is a built-in role.
b. It can be used for CLI commands.
c. It can be used for XML API.
d. Superuser is an example of such a role.

Q2. The management console supports which two authentication types? (Choose two.)

a. RADIUS
b. SMB
c. LDAP
d. TACACS+
e. AWS

Q3. Which two Dynamic Admin Role types are available on the PAN-OS software? (Choose two.)

a. Superuser
b. Superuser (write-only)
c. Device user
d. Device administrator (read-only)

Q4. Which type of profile does an authentication sequence include?

a. Security
b. Authorization
c. Admin
d. Authentication

Q5. An Authentication profile includes which other type of profile?

a. Server
b. Admin
c. Customized
d. Built-In

Q6. True or false? Dynamic Admin Roles are called “dynamic” because you can customize them.

a. true
b. false

Q7. Which profile is used to override global minimum password complexity requirements?

a. Authentication
b. Local
c. User
d. Password

Q8. What does an application filter enable an administrator to do?

a. Manually categorize multiple service filters.
b. Dynamically categorize multiple service filters.
c. Dynamically categorize multiple applications.
d. Manually categorize multiple applications.

`

Q9. Which two items can be added to an application group? (Choose two.)

a. Application groups
b. Application services
c. Application filters
d. Application categories

Q10. What are two application characteristics? (Choose two.)

a. Stateful
b. Excessive bandwidth use
c. Intensive
d. Evasive

`

Domain 3: Policy Evaluation and Management

3.1 Develop the appropriate application-based Security policy

3.1.1 Create an appropriate App-ID rule

Policy Optimizer provides a simple workflow to migrate your legacy Security policy rulebase to an App-ID-based rulebase, which improves your security by reducing the attack surface and offering visibility into applications so you can safely enable them. Policy Optimizer identifies port-based rules so you can convert them to application-based allow list rules or add applications from a port-based rule to an existing application-based rule without compromising application availability. It also identifies overprovisioned App-ID-based rules (App-ID rules configured with unused applications). Policy Optimizer helps you prioritize which port-based rules to migrate first, identify application-based rules that allow applications you do not use, and analyze rule-usage characteristics such as hit count.

Conversion of port-based rules to application-based rules improves your security posture because you select the applications you want to allow list and deny all other applications. You therefore eliminate unwanted and potentially malicious traffic from your network. The combination of restricting application traffic to its default ports (set the **Service** to **application-default**) and conversion to application-based rules also prevents evasive applications from running on nonstandard ports.

Using the Policy Optimizer
Begin by identifying existing port-based rules.

Use the displayed information to determine which applications were seen in a specific rule. Click Compare to display the list and application usage information:

`

You can add the discovered App-IDs to your Security policy rules using one of the four selections at the bottom of the **Application & Usage** display. Select a listed **Application** by checking the box to make the options available.

- Create Cloned Rule: Creates a duplicate of the Security policy rule being examined, adding the selected App-ID.
- Add to This Rule: Adds the selected Application(s) to the existing Security policy rule being evaluated.
- Add to Existing Rule: Adds the selected Application(s)to an existing Security policy rule of your choice.
- Match Usage: Replaces the selected Security policy rule with a new, App-ID-based version in the same Security policy rule list position.

The Policy Optimizer also can display existing App-IDs in Security policy rules that have not been used, and it can identify Security policy rules that have not matched traffic at intervals of 30 days, 60 days, and never.

App-ID Updates and Impact

Firewall administrators must be careful when they install any App-ID updates because some applications might have changed since the last App-ID update (content update). For example, an application that previously was categorized under web-browsing now might be categorized under its own unique App-ID. Categorization of applications into more specific applications enables more granularity and control of applications within Security policy rules. Because the new App-ID no longer will be categorized as web-browsing, no Security policy rule now will contain this new App-ID. Consequently, the new App-ID will be blocked.

You can minimize this risk by using the **Disable new apps in content update feature**. New updates will be downloaded and installed according to the schedule, but they will be disabled until they are

manually enabled. Be aware that this action will force you to track disabled applications, which increases your administrative burden. You may want to examine the effect of any new applications on your Security policy and make any required policy updates without disabling new application signatures.

Content Update Absorption

To see the applications that have been modified since the last content release, select **Review Apps** in the **Action** column. The screen will display details about the modified application.

Select **Review Policies** to display the Security policy rules that might enforce traffic differently after the application is modified:

Always review content release notes for the list of newly identified and modified applications and threat signatures that the content release introduces. Content release notes also describe how the update might impact existing Security policy enforcement, and they provide recommendations on how you can modify your Security policy to best leverage what's new. Installation of new App-IDs included in a content release version sometimes can cause a change in policy enforcement for the application that now is uniquely identified.

3.1.2 Rule shadowing

A shadow-rule warning indicates that a broader rule matching the criteria is configured above a more specific rule.

The following screenshot shows that no traffic ever will match the second rule, which specifically allows Skype and Dropbox, because all applications already have been allowed by the first rule. Rule 2's "skype" shadows rule 3's "skype."

3.1.3 Group rules by tag

Application Tags

Starting with the release of PAN-OS 9.1, Palo Alto Networks adds predefined tags to many applications listed in the App-ID database. The predefined tags are assigned to applications based on each application's characteristics. For example, web-based applications are assigned the tag

`

Web App, and VoIP applications are assigned the tag Enterprise VoIP. Predefined tags are updated and maintained by the Applications and Threats dynamic updates.

You can view application tags in the web interface by browsing to **Objects > Applications** and then opening an application's details window (see the following image). You can create custom tags using **Objects > Tags** and then assign your custom tag to an application. To assign a custom tag to an application, use the **Edit** link in the application's details window, as shown in the following screenshot:

You can use application tags as policy rule match criteria. First, create an application filter using one or more application tags as filter criteria. Then add the application filter to a policy rule. If the tags associated with applications are updated, then the behavior of application filters and policy rules also will be automatically updated. An example Security policy rule with an application filter is shown in the following screenshot:

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

Newly-categorized and modified App-IDs can change the way the firewall enforces traffic. Perform a content update policy review to see how new and modified App-IDs impact your security policy, and to easily make any necessary adjustments. You can perform a content update policy review for both downloaded and installed content.

Step 1: Select **Device > Dynamic Updates**

Step 2: See the New and Modified App-IDs in a Content Release to learn more about each App-ID that a content release introduces or modifies.

Step 3: For a downloaded or currently installed content release, click **Review Policies** in the Action column. The **Policy review based on candidate configuration** dialog allows you to filter by **Content Version** and view either new or modified App-IDs introduced in a specific release (you can also filter the policy impact of new App-IDs according to **Rulebase**, **Virtual System**, and **Application**).

Step 4: Select an App-ID from the **Application** drop-down to view policy rules that currently enforce the application. The rules displayed are based on the App-IDs that match to the application before the new App-ID is installed (view application details to see the list of application signatures that an application was **Previously Identified As** before the new App-ID).

Step 5: Use the detail provided in the policy review to plan policy rule updates to take effect when the App-ID is installed, or if the content release version that included the App-ID is currently installed, the changes you make take effect immediately.

You can **Add app to selected policies** or **Remove app from selected policies**.

3.1.5 Policy usage statistics

The Panorama and firewall web interfaces now display the hit count for traffic that matches a policy rule to help keep your firewall policies up to date as your environment and security needs change over time. To prevent attackers from exploiting over-provisioned access, such as when a server is decommissioned or when you no longer require temporary access to a service, the rule usage tracking feature helps you -identify and remove unused rules. Additionally, this feature provides the ability to validate rule additions and rule changes and to monitor the time frame when a rule was used. For example, when you migrate port-based rules to app-based rules, you create an app-based rule above the port-based rule and then check for any traffic that matches the port-based rule. After migration, the hit-count data helps you determine whether it is safe to remove the port-based rule by confirming that traffic is matching the app-based rule instead of the port-based rule.

On the firewall, rule-usage tracking allows you to view the rule usage hit count and the last timestamp of the last hit. On Panorama, the rule usage tracking data allows you to view whether a policy rule pushed to firewalls in a specific device group has traffic matches. The rule usage tracking data gives you the information you need to determine whether a rule is effective for access enforcement. For more information, see Monitor Policy Rule Usage.

Follow the steps below:

Step 1: Launch the firewall or Panorama web interface.

- On a firewall
  - Launch the web interface and select Policies.
  - View the rule usage statistics for each policy rule. The following information is displayed:
    - Hit Count—The number of times traffic matched the criteria you defined in the policy rule. Persists through reboot, data-plane restarts, and upgrades unless you manually reset or rename the rule.
    - Last Hit—The most recent timestamp for when traffic matched the rule.
    - First Hit—The first instance when traffic was matched to this rule.

	Name	Tags	Type	Rule Usage			Application
				Hit Count	Last Hit	First Hit	
7	Allowed IM	none	universal	251689793	2017-11-20 03:1...	2017-08-15 02:31:57	irc-base skype skype-probe yahoo-voice
8	Corp Mail	none	universal	4839264	2017-11-20 03:1...	2017-08-15 02:31:57	pop3 smtp
9	Monitor	none	universal	482226722	2017-11-20 03:1...	2017-08-15 02:31:57	any
10	LS_Allow	none	universal	0	-	-	any
11	branch1-test	none	universal	0	-	-	any
12	test	none	universal	10586680	2017-08-14 23:3...	2017-08-14 06:26:09	any
13	intrazone-default	none	intrazone	21108459	2017-11-20 03:1...	2017-08-14 06:26:09	any
14	interzone-default	none	interzone	0	-	-	any

- On Panorama
  - Launch the web interface and select Policies.
  - Determine whether the rule is being used (Rule Usage column). The policy rule usage status is one of the following:
    Firewalls must run PAN-OS 8.1 or later release with Policy Rule Hit Count enabled for Panorama to determine rule usage.

    Used-When all firewalls in the device group—to which you pushed the policy rule—have traffic matches for the policy rule.

Partially Used-When some of the firewalls in the device group—to which you pushed the policy rule—have traffic matches for the policy rule.

Unused-When no firewalls in the device group—to which you pushed the policy rule—have traffic matches for the policy rule.

Em-dash (—)-When no firewalls in the device group—to which you pushed the policy rule—have Policy Rule Hit Count enabled or available for Panorama to determine the rule usage.

Modified-The date and time the policy rule was last modified.

Created-The date and time the policy rule was created.

Rule Usage				
RULE USAGE	APPS SEEN	DAYS WITH NO NEW APPS	MODIFIED	CREATED
Used	6	150	2020-06-24 10:34:...	2020-04-09 11:34:03
Unused	0	-	2020-06-24 10:34:...	2020-04-16 11:42:46
Used	11	57	2020-06-24 10:34:...	2020-04-16 11:42:46
Partially Used	3	111	2020-06-24 10:34:...	2020-05-22 17:26:44
Unused	0	-	2020-06-24 10:34:...	2020-05-22 22:45:53

- The Rule Usage column displays rule usage for each appliance in the device group. The rule usage information displayed persists through reboot, data-plane restarts, and upgrades.
  - Used—When all appliances in the device group—to which you pushed the policy rule—have traffic matches for the policy rule.
  - Partially Used—When some of the appliances in the device group—to which you pushed the policy rule—have matches for the policy rule.
  - Unused—When no appliances in the device group—to which you pushed the policy rule—have traffic matches for the policy rule.

- To view the firewall-specific policy rule usage data, navigate to Preview Rules and select a specific firewall managed by Panorama. If needed, you can reset the firewall hit-count data for individual rules. Panorama retrieves rule usage information from managed firewalls every five minutes.

Step 2: Reset the rule usage tracking count data.
You can reset the rule hit-count data to validate an existing rule or to gauge rule usage within a specified period of time. Policy rule hit-count data is not stored on the firewall or Panorama, so after you clear the hit count using the reset option, that data is no longer available.

- Identify any rules you need to reset and navigate to the Hit Count column.
- Select Reset from the drop-down. If you previously reset a rule policy hit count, you can also view the Last Reset Time from the drop-down.

`

3.1.6 Reference

- Resolve Application Dependencies, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies

3.2 Differentiate specific security rule types

3.2.1 Interzone rules

Interzone • Default rule • Displayed at the bottom of the security rulebase	A Security policy rule allowing traffic between two different zones is called an interzone rule. However, the traffic within the same zone will not be allowed when the policy is created as type Interzone. Interzone rule types apply to all matching traffic between the specified source and destination zones. For example, if the source zone is set to A, B, and C and the destination zone to A and B, the rule would apply to traffic from zone A to zone B, from zone B to zone A, from zone C to zone A, and from zone C to zone B, but not to traffic within zones A, B, or C. Traffic logging is not enabled by default. However, best practice is to log the traffic.

Interzone Security Policy

`

3.2.2 Intrazone rules

RULE TYPE	DESCRIPTION
Intrazone • Default rule • Displayed at the bottom of the security rulebase	A Security policy rule allowing traffic within the same zone is called an intrazone rule. Intrazone rule types apply to all matching traffic within the specified source zones (a destination zone cannot be specified for intrazone rules). For example, if the source zone is set to A and B, the rule would apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B. Traffic logging is not enabled by default. However, best practice is to log the end-of-session traffic.

Intrazone Security Policy

3.2.3 Universal rules

Universal • Exists above the intrazone and interzone Security policies	In universal rule, by default, all the traffic is destined between two zones, regardless of whether it is from the same zone or different zone. Universal rule types apply to all matching interzone and intrazone traffic in the specified source and destination zones. For example, if a universal rule is created with source zones A and B and destination zones A and B, the rule would apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B and all traffic from zone B to zone A. Traffic logging is enabled by default.

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

Implicit and Explicit Rules

Two implicit (predefined) Security policy rules come with the PAN-OS software: intrazone and interzone. The intrazone Security policy rule allows traffic within a zone by default. The interzone Security policy does not allow traffic between zones by default. These two predefined Security policy rule types reside at the bottom of the security rulebase set and are processed after all other

`

preceding Security policy rules are processed. All preceding security rules must be explicitly defined by an administrator. Note that traffic is not logged by default for the predefined rules and that traffic is logged by default for explicitly defined rules. Best practice is to log for all Security policy rules, whether implicit or explicit.

A shadow-rule warning indicates that a broader rule matching the criteria is configured above a more specific rule.

The following screenshot shows that no traffic ever will match the second rule, which specifically allows skype and dropbox, because all applications already have been allowed by the first rule. Rule 2's "skype" shadows rule 3's "skype."

	NAME	TYPE	ACTION	Source ZONE	Destination ZONE	APPLICATI...	SERVICE	PROFI...	OPTIONS
1	Explicit Allow Everything	universal	Allow	Users	Internet	any	application-default	none	
2	Shadowed	universal	Allow	Users	Internet	dropbox skype	application-default	none	
3	Another Shadow	universal	Allow	Users	Internet	skype	application-default	none	
4	intrazone-default	intrazone	Allow	any	(intrazone)	any	any	none	none
5	interzone-default	interzone	Deny	any	any	any	any	none	none

Security Rule Hit Count

The PAN-OS software enables you to monitor hit count. The three components of Rule Usage are as follows:

- **Hit Count**: The number of times traffic matched the criteria you defined in the policy rule. It persists through reboot, data plane restarts, and upgrades unless you manually reset or rename the rule.
- **Last Hit**: The most recent timestamp for when traffic matched the rule.
- **First Hit**: The first instance when traffic was matched to this rule.

In the following screenshot, note that the hit counts have not incremented because this example has no live traffic:

Application Properties

All applications in the App-ID database are defined by six properties:

PROPERTY	DEFINITION
Category	Used to generate the Top Ten Application Categories chart within the ACC and is available for filtering.
Subcategory	Also used to generate the Top Ten Application Categories chart within the ACC and is available for filtering.
Technology	Technology most closely associated with the application.
Parent App	Specify a parent application for this application. This setting applies when a session matches both the parent and the custom applications; however, the custom application is reported because it is more specific.
Risk	A relative risk rating from 1 to 5, with 5 being the most risky.
Characteristics	Identifies some application property or behavior, like certified for FEDRAMP, or can be used for evasion, or can use excessive bandwidth, and so on.

Application Characteristics

All applications in the App-ID database are defined by characteristics shown in the image below. The names of the characteristics are self-explanatory.

`

Application Timeouts

ITEM	DEFINITION
Timeout	Number of seconds before an idle application flow is terminated. A zero indicates that the default timeout of the application will be used. This value is used for protocols other than TCP and UDP in all cases, and for TCP and UDP timeouts when the TCP timeout and UDP timeout are not specified.
TCP Timeout	Number of seconds before an idle TCP application flow is terminated. A zero indicates that the default timeout of the application is used.
UDP Timeout	Number of seconds before an idle UDP application flow is terminated. A zero indicates that the default timeout of the application is used.
TCP Half Closed	Maximum length of time that a session remains in the session table between reception of the first FIN and reception of the second FIN or RST. If the timer expires, the session is closed.
TCP Time Wait	Maximum length of time that a session remains in the session table after the second FIN or RST is received. If the timer expires, the session is closed. If this time is not configured at the application level, the global setting is used (range is 1 to 600 seconds). If this value is configured at the application level, it overrides the global TCP Time Wait setting.

3.3.1 Use Application Filters and Groups

Application Filter

An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter.

Create an Application Filter

Step 1: Select **Objects > Application Filters**.

Step 2: Add a filter and give it a descriptive **Name**.

Step 3: (Optional) Select **Shared** to create the object in a shared location for access as a shared object in Panorama or for use across all virtual systems in a multiple virtual system firewall.

Step 4: Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections. As you select values, notice that the list of matching applications at the bottom of the dialog narrows. When you have adjusted the filter attributes to match the types of applications you want to safely enable, click **OK**.

Step 5: Commit the configuration.

Application Group

An application group is an object that contains applications that you want to treat similarly in policy. Application groups are useful for enabling access to applications that you explicitly sanction for use within your organization. Grouping sanctioned applications simplifies administration of your rulebases. Instead of having to update individual policy rules when there is a change in the applications you support, you can update only the affected application groups.

When deciding how to group applications, consider how you plan to enforce access to your sanctioned applications and create an application group that aligns with each of your policy goals. For example, you might have some applications that you will only allow your IT administrators to access, and other applications that you want to make available for any known user in your organization. In this case, you would create separate application groups for each of these policy goals. Although you generally want to enable access to applications on the default port only, you may want to group applications that are an exception to this and enforce access to those applications in a separate rule.

Create an Application Group

Step 1: Select **Objects > Application Groups**.

Step 2: Add a group and give it a descriptive **Name**.

Step 3: (Optional) Select **Shared** to create the object in a shared location for access as a shared object in Panorama or for use across all virtual systems in a multiple virtual system firewall.

Step 4: Add the applications you want in the group and then click **OK**.

Step 5: Commit the configuration.

3.3.2 Use logging options

The **HTTP Header Logging** feature provides visibility into the attributes included in the HTTP request sent to a server. When HTTP Header Logging is enabled, one or more of the following attributes are recorded in the URL Filtering log:

- **User Agent**: The web browser that the user used to access the URL. This information is sent in the HTTP request to the server. For example, the User Agent can be Internet Explorer or Firefox.
- **Referrer**: The URL of the webpage that linked the user to another webpage. It is the source that redirected (referred) the user to the webpage that is being requested.
- **X-Forward-For**: The header field option that preserves the IP address of the user who requested the webpage. It enables you to identify the IP address of the user, which is

particularly useful if you have a proxy server on your network or you have implemented source NAT that is masking the user's IP address such that all requests seem to originate from the proxy server's IP address or a common IP address.

3.3.3 App-ID

App-ID, a patented traffic-classification system only available in Palo Alto Networks firewalls, determines what an application is, irrespective of port, protocol, encryption (SSH or SSL), or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications.

Here's how App-ID identifies applications traversing your network:

- Traffic is matched against policy to check whether it is allowed on the network.
- Signatures are then applied to allowed traffic to identify the application based on unique application properties and related transaction characteristics. The signature also determines whether the application is being used on its default port or is using a nonstandard port. If the traffic is allowed by policy, the traffic is then scanned for threats and further analyzed for identifying the application more granularly.
- If App-ID determines that encryption (SSL or SSH) is in use, and a Decryption policy rule is in place, the session is decrypted and application signatures are applied again on the decrypted flow.
- Decoders for known protocols are then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol (for example, Yahoo! Instant Messenger used across HTTP). Decoders validate that the traffic conforms to the protocol specification and provide support for NAT traversal and opening dynamic pinholes for applications such as SIP and FTP.

- For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, App-ID may use heuristics or behavioral analysis to determine the identity of the application.

When the application is identified, the policy check determines how to treat the application—for example, block or allow and scan for threats, inspect for unauthorized file transfer and data patterns, or shape using QoS.

All applications in the App-ID database are defined by six properties:

PROPERTY	DEFINITION
Category	Used to generate the Top Ten Application Categories chart within the ACC and is available for filtering.
Subcategory	Also used to generate the Top Ten Application Categories chart within the ACC and is available for filtering.
Technology	Technology most closely associated with the application.
Parent App	Specify a parent application for this application. This setting applies when a session matches both the parent and the custom applications; however, the custom application is reported because it is more specific.
Risk	A relative risk rating from 1 to 5, with 5 being the most risky.
Characteristics	Identifies some application property or behavior, like certified for FEDRAMP, or can be used for evasion, or can use excessive bandwidth, and so on.

3.3.4 User-ID

User-ID enables you to identify all users on your network using a variety of techniques to ensure that you can identify users in all locations who are using a variety of access methods and operating systems, including Microsoft Windows, Apple iOS, macOS, Android, and Linux®/UNIX. Knowing who your users are instead of just their IP addresses enables:

Visibility—Improved visibility into application usage based on users gives you a more relevant picture of network activity. The power of User-ID becomes evident when you notice a strange or unfamiliar application on your network. Using either ACC or the log viewer, your security team can discern what the application is, who the user is, the bandwidth and session consumption, the source and destination of the application traffic, and any associated threats.

Policy control—Tying user information to Security policy rules improves safe enablement of applications traversing the network and ensures that only those users who have a business need for an application have access. For example, some applications, such as SaaS applications that enable access to Human Resources services (such as Workday or Service Now) must be available to any known user on your network. However, for more sensitive applications, you can reduce your attack surface by ensuring that only users who need these applications can access them. For example, while IT support personnel may legitimately need access to remote desktop applications, the majority of your users do not.

Logging, reporting, forensics—If a security incident occurs, forensic analysis and reporting based on user information rather than just IP addresses provides a more complete picture of the incident. For example, you can use the predefined User/Group Activity to see a summary of the web activity of individual users or user groups. Alternatively, you can use the SaaS Application Usage report to see which users are transferring the most data over unsanctioned SaaS applications.

To enforce user- and group-based policies, the firewall must be able to map the IP addresses in the packets it receives to usernames. User-ID provides many mechanisms to collect this user-mapping information. For example, the User-ID agent monitors server logs for login events and listens for syslog messages from authenticating services. To identify mappings for IP addresses that the agent didn't map, you can configure Authentication policy to redirect HTTP requests to a Captive Portal login. You can tailor the user-mapping mechanisms to suit your environment and even use different mechanisms at different sites to ensure that you are safely enabling access to applications for all users, in all locations, all the time.

To enable user- and group-based policy enforcement, the firewall requires a list of all available users and their corresponding group memberships so that you can select groups when defining your policy rules. The firewall collects group mapping information by connecting directly to your LDAP directory server, or using XML API integration with your directory server.

3.3.5 Device-ID

According to the 2020 Unit 42 IoT Threat Report, 30 percent of all network-connected devices in an average enterprise are IoT. This presents a constantly growing area of risk with many possibilities for exploitation by malicious users. Additionally, once you identify these devices, how do you secure them from vulnerabilities such as outdated operating software? Using Device-ID™ on your firewall

or to push policy from Panorama, you can get device context for events on your network, obtain policy rule recommendations for those devices, write policies based on devices, and enforce Security policy based on the recommendations.

Similar to how User-ID provides user-based policy and App-ID provides app-based policy, Device-ID provides policy rules that are based on a device, regardless of changes to its IP address or location. By providing traceability for devices and associating network events with specific devices, Device-ID allows you to gain context for how events relate to devices and write policies that are associated with devices, instead of users, locations, or IP addresses, which can change over time. You can use Device-ID in Security, Decryption, Quality of Service (QoS), and Authentication policies.

For Device-ID features to be available on a firewall, you must purchase an IoT Security subscription and select the firewall during the IoT Security onboarding process. There are two types of IoT Security subscriptions:

- IoT Security Subscription
- IoT Security – Does not require Data Lake (DRDL) Subscription

3.3.6 Include an application filter in policy

Create an Application Filter

Step 1: Select **Objects > Application Filters**.

Step 2: Add a filter and give it a descriptive Name

Step 3: (Optional) Select **Shared** to create the object in a shared location for access as a shared object in Panorama or for use across all virtual systems in a multiple virtual system firewall.

Step 4: Define the filter by selecting attribute values from the Category, Subcategory, Technology, Risk, and Characteristic sections. As you select values, notice that the list of matching applications at the bottom of the dialog narrows. When you have adjusted the filter attributes to match the types of applications you want to safely enable, click **OK**.

`

Step 5: Commit the configuration.

3.3.7 Include an application group in policy

An administrator can manually categorize multiple applications into an application group based on App- ID. This application group then is added to one or more Security policy rules as required, which streamlines firewall administration. Instead of a firewall administrator individually adding different applications into a Security policy, only the application group needs to be added to the policy.

Application groups often are used to simplify security, QoS, and PBF policy rule implementation.

Nesting Application Groups and Filters

An administrator can nest application groups and filters. They can combine multiple applications and multiple application filters into an application group. They can also combine one or more application groups into one application group. They can then add the final application group to a Security policy rule.

`

3.3.8 EDLs

An External Dynamic List is a text file that is hosted on an external web server so that the firewall can import objects—IP addresses, URLs, domains—included in the list and enforce policy. To enforce policy on the entries included in the external dynamic list, you must reference the list in a supported policy rule or profile. When multiple lists are referenced, you can prioritize the order of evaluation to make sure the most important EDLs are committed before capacity limits are reached. As you modify the list, the firewall dynamically imports the list at the configured interval and enforces policy without the need to make a configuration change or a commit on the firewall. If the web server is unreachable, the firewall uses the last successfully retrieved list for enforcing policy until the connection is restored with the web server. In cases where authentication to the EDL fails, the security policy stops enforcing the EDL. To retrieve the external dynamic list, the firewall uses the interface configured with the Palo Alto Networks Services service route.

3.3.9 References

- External Dynamic Lists, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list

3.4 Identify and implement proper NAT policies

3.4.1 Destination NAT

DNAT is used to replace the original destination IP address in a packet. A typical scenario for DNAT is when a packet originates from the internet and then is forwarded to a company's internal network. The original destination IP is routable within the internet. When the packet arrives at the firewall, the routable IP address is replaced with the real IP address of the destination device (usually an RFC 1918 IP address) and then is forwarded to the destination device.

DNAT can be used in other scenarios such as when subnets overlap.

Destination NAT (DNAT) typically is used to allow an external client to initiate access to an internal host such as a web server. The two types of destination NAT are as follows:

DESTINATION NAT TYPE	DESCRIPTION
Static	You can set the translated address as an IP address or range of IP addresses and a translated port number (1 – 65,535), to which the original destination address and port number are translated. If the Translated Port field is blank, the destination port is not changed.
Dynamic IP (with session distribution)	You can enter a translated address that is an FQDN, an address object, or an address group from which the firewall selects the translated address. If the DNS server returns more than one address for an FQDN, or if the address object or address group translates into more than one IP address, the firewall distributes sessions among those addresses using the specified session distribution method.

`

Destination NAT and Security Policies

A Security policy rule requires a source IP, destination IP, source zone, and destination zone. If you use an IP address in a Security policy rule, you must add the IP address value that existed before NAT was implemented, which is called the pre-NAT IP. After the destination IP address is translated (post-NAT IP), determine the zone where the post-NAT IP address would exist. This post-NAT zone is used in the Security policy rule.

A simple way to remember how to configure Security policy rules where NAT was implemented is to memorize the following: "pre-NAT IP; post-NAT zone."

Configuring Dynamic IP Address Support for DNAT

You can enter a translated address that is an FQDN, an address object, or an address group from which the firewall selects the translated address. If the DNS server returns more than one address for an FQDN or if the address object or address group translates into more than one IP address, the firewall distributes sessions among those addresses using the specified session distribution method.

`

Configuring Destination NAT Port Forwarding

3.4.2 Source NAT

SNAT is used to replace the original source IP address in a packet. A typical scenario for SNAT is when a packet originates from within a company's network and then is forwarded out to the internet. The original source IP address usually is an RFC 1918 IP address that is not routable within the internet.

Source NAT Types

The following table describes the three source NAT types: static IP, dynamic IP, and dynamic IP and port:

SOURCE NAT TYPE	DESCRIPTION
Static IP	The same address is always used for the translation, and the port is unchanged. For example, if the source range is 192.168.0.1 – 192.168.0.10, and the translation range is 10.0.0.1 – 10.0.0.10, address 192.168.0.2 always is translated to 10.0.0.2. The address range usually is limited. This concept applies if only a host /32 IP address is used.
Dynamic IP	The original source IP address translates to the next available address in the specified range, but the port number remains unchanged. Up to 32,000 consecutive IP addresses are supported. A dynamic IP pool can contain multiple subnets, so you can translate your internal network addresses to two or more separate public subnets.
Dynamic IP and port	This is the most commonly used source NAT type. Address selection is based on a hash of the source IP address. For a given source IP address, the firewall uses the same translated source address for all sessions.

`

Source NAT and Security Policies

A Security policy rule requires a source IP, destination IP, source zone, and destination zone. If you use an IP address in a Security policy rule, you must add the IP address value that existed before NAT was implemented, which is called the pre-NAT IP. After the IP address is translated (post-NAT IP), determine the zone where the post-NAT IP address would exist. This post-NAT zone is used in the Security policy rule.

A simple way to remember how to configure Security policy rules where NAT was implemented is to memorize the following: "pre-NAT IP; post-NAT zone."

Configuring Source NAT

Configuring Bidirectional Source NAT

For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure. If you are configuring static source NAT, bidirectional NAT eliminates the need to create an additional NAT policy rule for the incoming traffic.

If you enable bidirectional translation, you must ensure that you have Security policy rules in place to control the traffic in both directions. If there are no such rules, the bidirectional feature allows packets to be translated automatically in both directions.

3.5 Optimize Security policies using appropriate tools

3.5.1 Policy text match tool

Test the policy rules in your running configuration to ensure that your policies appropriately allow and deny traffic and access to applications and websites in compliance with your business needs

`

and requirements. You can test and verify that your policy rules are allowing and denying the correct traffic by executing policy match tests for your firewalls directly from the web interface.

Step 1: Launch the web interface.

Step 2: Select **Device > Troubleshooting** to perform a policy match or connectivity test.

Step 3: Enter the required information to perform the policy match test. In this example, we run a NAT policy match test.

- **Select Test**—Select **NAT Policy Match**.
- **From**—Select the zone from which traffic is originating.
- **To**—Select the target zone of the traffic.
- **Source**—Enter the IP address from which traffic originated.
- **Destination**—Enter the IP address of the target device for the traffic.
- **Destination Port**—Enter the port used for the traffic. This port varies depending on the IP protocol used in the following step.
- **Protocol**—Enter the IP protocol used for the traffic.
- If necessary, enter any additional information relevant for your NAT policy rule testing.

Step 4: Execute the NAT policy match test.

Step 5: Review the NAT Policy Match Result to see the policy rules that match the test criteria.

3.5.2 Policy Optimizer

Policy Optimizer provides a simple workflow to migrate your legacy Security policy rulebase to an App-ID based rulebase, which improves your security by reducing the attack surface and gaining visibility into applications so you can safely enable them. Policy Optimizer identifies port-based rules so you can convert them to application-based allow rules or add applications from a port-based rule to an existing application-based rule without compromising application availability. It also identifies over-provisioned App-ID based rules (App-ID rules configured with unused applications). Policy Optimizer helps you prioritize which port-based rules to migrate first, identify application-based rules that allow applications you don't use, and analyze rule usage characteristics such as hit count.

`

Converting port-based rules to application-based rules improves your security posture because you select the applications you want to allow and deny all other applications, so you eliminate unwanted and potentially malicious traffic from your network. Combined with restricting application traffic to its default ports (set the Service to **application-default**), converting to application-based rules also prevents evasive applications from running on non-standard ports.

You can use this feature on:

- Firewalls that run PAN-OS version 9.0 and have App-ID enabled.
- Panorama running PAN-OS version 9.0. You don't have to upgrade firewalls that Panorama manages to use the Policy Optimizer capabilities. However, to use the **Rule Usage** capabilities (Monitor Policy Rule Usage), managed firewalls must run PAN-OS 8.1 or later. If managed firewalls connect to Log Collectors, those Log Collectors must also run PAN-OS version 9.0. Managed PA-7000 Series firewalls that have a Log Processing Card (LPC) can also run PAN-OS 8.1 (or later).
- For Cortex Data Lake compatibility, Panorama running PAN-OS 10.0.3 or later with the Cloud Services plugin 2.0 Innovation or later installed.

Use this feature to:

- **Migrate port-based rules to application-based rules**—Instead of combing through traffic logs and manually mapping applications to port-based rules, use Policy Optimizer to identify port-based rules and list the applications that matched each rule, so you can select the applications you want to allow and safely enable them. Converting your legacy port-based rules to application-based allow rules supports your business applications and enables you to block any applications associated with malicious activity.

- **Identify over-provisioned application-based rules**—Rules that are too broad allow applications you don't use on your network, which increases the attack surface and the risk of inadvertently allowing malicious traffic.

- **Add App-ID Cloud Engine (ACE) applications to Security policy rules**—If you have a SaaS Security Inline subscription, you can use Policy Optimizer's New App Viewer to manage cloud-delivered App-IDs in Security policy. The ACE documentation describes how to use Policy Optimizer to gain visibility into and control cloud-delivered App-IDs.

You can't sort Security policy rules in **Security > Policies** because sorting would change the rule order in the rulebase. However, under **Policies > Security > Policy Optimizer**, Policy Optimizer provides sorting options that don't affect the rule order, so you can sort rules to prioritize which rules to convert or clean up first. You can sort rules by the amount of traffic during the past 30 days, the number of applications seen on the rule, the number of days with no new applications, and the number of applications allowed (for over-provisioned rules).

You can use Policy Optimizer in other ways as well, including validating pre-production rules and troubleshooting existing rules. Note that Policy Optimizer honors only **Log at Session End** and ignores **Log at Session Start** to avoid counting transient applications on rules.

`

3.6 Sample Questions

Q1. What will be the result of one or more occurrences of shadowing?

a. A failed commit
b. An invalid configuration
c. A warning
d. An alarm window

Q2. Which column in the Applications and Threats screen includes the options Review Apps and Review Policies?

a. Features
b. Type
c. Version
d. Action

Q3. Which link can you select in the web interface to minimize the risk of installing new App-ID updates?

a. Enable new apps in content update.
b. Disable new apps in App-ID database.
c. Disable new apps in content update.
d. Enable new apps in App-ID database.

Q4. Which two protocols are implicitly allowed when you select the facebook-base application? (Choose two.)

a. Web-browsing
b. Chat
c. Gaming
d. SSL

Q5. What are the two default (predefined) Security policy rule types in PAN-OS software? (Choose two.)

a. Universal
b. Interzone
c. Intrazone
d. Extrazone

Q6. Which type of Security policy rules most often exist above the two predefined Security policies?

a. Intrazone
b. Interzone
c. Universal
d. Global

Q7. What does the TCP Half Closed setting mean?

a. Maximum length of time that a session remains in the session table between reception of the first FIN and reception of the third FIN or RST.
b. Minimum length of time that a session remains in the session table between reception of the first FIN and reception of the second FIN or RST.

`

c. Maximum length of time that a session remains in the session table between reception of the first FIN and reception of the second FIN or RST.
d. Minimum length of time that a session remains in the session table between reception of the first FIN and reception of the third FIN or RST.

Q8. What are two application characteristics? (Choose two.)
a. Stateful
b. Excessive bandwidth use
c. Intensive
d. Evasive

Q9. Which two HTTP Header Logging options are within a URL Filtering profile? (Choose two.)
a. User-Agent
b. Safe Search
c. URL redirection
d. X-Forwarded-For

Q10. What are two source NAT types? (Choose two.)
a. Universal
b. Static
c. Dynamic
d. Extrazone

Q11. Which phrase is a simple way to remember how to configure Security policy rules where NAT was implemented?
a. Post-NAT IP, pre-NAT zone
b. Post-NAT IP, post-NAT zone
c. Pre-NAT IP, post-NAT zone
d. Pre-NAT IP, pre-NAT zone

Q12. What are two types of destination NAT? (Choose two.)
a. Dynamic IP (with session distribution)
b. DIPP
c. Global
d. Static

Q13. What are two possible values for DIPP (Dynamic IP and Port NAT) oversubscription? (Choose two.)
a. 1x
b. 4x
c. 16x
d. 32x

`

Q14. Which statement is true regarding bidirectional NAT?

a. For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure.
b. For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the same direction as the translation you configure.
c. For dynamic translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure.
d. For dynamic translations, bidirectional NAT enables the firewall to create a corresponding translation in the same direction as the translation you configure.

Q15. The Policy Optimizer does not analyze which statistics?

a. Applications allowed through port-based Security policy rules.
b. The usage of existing App-IDs in Security policy rules.
c. Which users matched Security policies.
d. Existing Security policy rule App-IDs that have not matched processed traffic.
e. Days since the latest new application discovery in a port-based Security policy rule.

`

Domain 4: Securing Traffic

4.1 Compare and contrast different types of Security profiles

4.1.1 Antivirus

Antivirus Security profiles protect against viruses, worms, and Trojans, along with spyware downloads. The Palo Alto Networks antivirus solution uses a stream-based malware prevention engine that inspects traffic the moment the first packet is received to provide protection for clients without significantly impacting the performance of the firewall. This profile scans for a wide variety of malware in executables, PDF files, HTML, and JavaScript, and it includes support for scanning inside compressed files and data-encoding schemes. The profile also enables scanning of decrypted content if decryption is enabled on the firewall.

The *default* profile inspects all listed protocol decoders for viruses and generates alerts for SMTP, IMAP, and POP3 protocols while blocking FTP, HTTP, and SMB protocols. You can configure the action for a decoder or antivirus signature and specify how the firewall responds to a threat.

Customized profiles can be used to minimize antivirus inspection for traffic between more trusted security zones. They also can be used to maximize the inspection of traffic received from less trusted zones, such as the internet, and the traffic sent to highly sensitive destinations such as server farms.

The Palo Alto Networks WildFire system also provides signatures for persistent threats that are more evasive and have not yet been discovered by other antivirus solutions. As WildFire discovers threats, signatures are quickly created and then are integrated into the standard antivirus signatures, which Threat Prevention subscribers can then download daily (sub-hourly for WildFire subscribers).

4.1.2 Anti-Spyware

Anti-Spyware Security profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between security zones. For example, you might want to have custom Anti-Spyware profiles that minimize inspection between more trusted zones while maximizing inspection on traffic received from less trusted zones such as internet-facing zones.

4.1.3 Vulnerability Protection

Vulnerability Protection Security profiles stop attempts to exploit system flaws or gain unauthorized access to systems. Anti-Spyware Security profiles identify infected hosts as traffic leaves the network, but Vulnerability Protection Security profiles protect against threats entering the network. For example, Vulnerability Protection Security profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The *default* Vulnerability Protection Security profile protects clients and servers from all known critical-, high-, and medium-severity

`

threats. You also can create exceptions that enable you to change the response to a specific signature.

4.1.4 URL Filtering

The URL Filtering Security profile determines web access and credential-submission permissions for each URL category. By default, site access for all URL categories is set to “allow” when you create a new URL Filtering Security profile. By default, no allowed traffic will be logged. You can customize the URL Filtering Security profile with custom site access settings for each category, or use the predefined *default* URL Filtering Security profile on the firewall to allow access to all URL categories except the following threat-prone categories, which the profile blocks: abused-drugs, adult, gambling, hacking, malware, phishing, questionable, and weapons.

For each URL category, select **User Credential Submissions** to allow or disallow users from submitting valid corporate credentials to a URL in that category. This action will prevent credential phishing.

Management of the sites to which users can submit credentials requires User-ID, and you must first set up credential phishing prevention. URL categories with the **Site Access** set to “block” automatically are set to block user credential submissions, as well.

4.1.5 WildFire analysis

WildFire turns every Palo Alto Networks platform deployment into a distributed sensor and enforcement point to stop zero-day malware and exploits before they can spread and become successful. Within the WildFire environment, threats are detonated, intelligence is extracted, and preventions are automatically orchestrated across the Palo Alto Networks next-generation security product portfolio as soon as a signature is generated, thus minimizing the window in which malware can infiltrate your network. WildFire goes beyond traditional approaches. The service employs a unique, multitechnique approach that combines dynamic and static analysis, innovative machine-learning techniques, and a groundbreaking bare metal analysis environment to detect unknown threats and prevent even the most evasive threats. The following illustration depicts WildFire, its information sources, and the services it supports.

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

4.2.1 Antivirus

The *default* profile inspects the listed protocol decoders for viruses and generates alerts for SMTP, IMAP, and POP3 protocols while blocking FTP, HTTP, and SMB protocols. You can configure the action for a decoder or antivirus signature and specify how the firewall responds to a threat event; see the following table:

ACTION	DESCRIPTION
Default	For each threat signature and Antivirus signature Palo Alto Networks defines, a default action is specified internally. The default action typically is an “alert” or a “reset-both.” The default action is displayed in parentheses in the threat or antivirus signature—for example, default (alert).
Allow	Permits the application traffic.
Alert	Generates an alert for each application traffic flow. The alert is saved in the Threat log.
Drop	Drops the application traffic.
Reset Client	For TCP, resets the client-side connection. For UDP, drops the connection.
Reset Server	For TCP, resets the server-side connection. For UDP, drops the connection.
Reset Both	For TCP, resets the connection on both the client and server ends. For UDP, drops the connection.

You can use customized profiles to minimize antivirus inspection for traffic between trusted security zones. You can also use them to maximize the inspection of traffic received from more untrusted zones such as the internet and of traffic sent to highly sensitive destinations such as server farms. The Palo Alto Networks WildFire product also provides signatures for persistent threats that are more evasive and have not yet been discovered by other antivirus solutions. As threats are discovered by WildFire, signatures are quickly created and then integrated into the standard antivirus signatures that can be downloaded daily by Threat Prevention subscribers (sub-hourly for WildFire subscribers).

4.2.2 Anti-Spyware

Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between zones. For example, you may want to have custom Anti-Spyware profiles that minimize inspection between trusted zones, while maximizing inspection on traffic received from an untrusted zone, such as internet-facing zones.

You can define your own custom Anti-Spyware profiles, or choose one of the following predefined profiles when applying Anti-Spyware to a Security policy rule:

`

- **Default**—Uses the default action for every signature, as specified by Palo Alto Networks when the signature is created.
- **Strict**—Overrides the default action of critical, high, and medium severity threats to the block action, regardless of the action defined in the signature file. This profile still uses the default action for low and informational severity signatures.

When the firewall detects a threat event, you can configure the following actions in an Anti-Spyware profile:

- **Default**—For each threat signature and Anti-Spyware signature that is defined by Palo Alto Networks, a default action is specified internally. Typically the default action is an alert or a reset-both. The default action is displayed in parenthesis, for example default (alert) in the threat or Antivirus signature.
- **Allow**—Permits the application traffic.
- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Drop**—Drops the application traffic.
- **Reset Client**—For TCP, resets the client-side connection. For UDP, drops the connection.
- **Reset Server**—For TCP, resets the server-side connection. For UDP, drops the connection.
- **Reset Both**—For TCP, resets the connection on both client and server ends. For UDP, drops the connection.
- **Block IP**—This action blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

In addition, you can enable the DNS Sinkholing action in Anti-Spyware profiles to enable the firewall to forge a response to a DNS query for a known malicious domain, causing the malicious domain name to resolve to an IP address that you define. This feature helps to identify infected hosts on the protected network using DNS traffic. Infected hosts can then be easily identified in the traffic and threat logs because any host that attempts to connect to the sinkhole IP address are most likely infected with malware.

Anti-Spyware and Vulnerability Protection profiles are configured similarly.

4.2.3 Vulnerability protection

Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network. For example, Vulnerability Protection profiles help protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection profile protects clients and servers from all known critical, high, and medium-severity threats. You can also create exceptions, which allow you to change the response to a specific signature.

When the firewall detects a threat event, you can configure the following actions in an Anti-Spyware profile:

- **Default**—For each threat signature and Anti-Spyware signature that is defined by Palo Alto Networks, a default action is specified internally. Typically the default action is an alert or a reset-both. The default action is displayed in parenthesis, for example default (alert) in the threat or Antivirus signature.
- **Allow**—Permits the application traffic.

`

- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Drop**—Drops the application traffic.
- **Reset Client**—For TCP, resets the client-side connection. For UDP, drops the connection.
- **Reset Server**—For TCP, resets the server-side connection. For UDP, drops the connection.
- **Reset Both**—For TCP, resets the connection on both client and server ends. For UDP, drops the connection.
- **Block IP**—This action blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

4.2.4 URL filtering

URL Filtering profiles enable you to monitor and control how users access the web over HTTP and HTTPS. The firewall comes with a default profile that is configured to block websites such as known malware sites, phishing sites, and adult content sites. You can use the default profile in a security policy, clone it to be used as a starting point for new URL filtering profiles, or add a new URL profile that will have all categories set to allow for visibility into the traffic on your network. You can then customize the newly added URL profiles and add lists of specific websites that should always be blocked or allowed, which provides more granular control over URL categories.

4.2.5 WildFire analysis

WildFire turns every Palo Alto Networks platform deployment into a distributed sensor and enforcement point to stop zero-day malware and exploits before they can spread and become successful. Within the WildFire environment, threats are detonated, intelligence is extracted, and preventions are automatically orchestrated across the Palo Alto Networks next-generation security product portfolio as soon as a signature is generated, thus minimizing the window in which malware can infiltrate your network. WildFire goes beyond traditional approaches. The service employs a unique, multi-technique approach that combines dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect unknown threats and prevent even the most evasive threats. The following illustration depicts WildFire, its information sources, and the services it supports.

4.2.6 Configure Threat Prevention policy

Because threats do not discriminate between application delivery vectors, an approach to security is needed that has full visibility into all application traffic, including SSL-encrypted content, with full user context. Threat Prevention leverages the visibility of the Palo Alto Networks Next-Generation Firewall to inspect all traffic; it thus automatically prevents known threats regardless of port, protocol, or SSL encryption. Threat Prevention automatically stops vulnerability exploits with IPS (Intrusion Prevention Systems) capabilities, offers inline malware protection, and blocks outbound command-and-control traffic. When these protections are combined with WildFire and URL Filtering, owning organizations are shielded at every stage of the attack lifecycle. Protection from both known and zero-day threats is provided.

4.3 Differentiate between Security profile actions

Security Policy Actions and Security Profile Actions

When packets traverse a firewall, they are inspected in two primary stages:

- Security Policy Stage
- Security Profile Stage

In the Security Policy Stage, packets must meet all the criteria in a Security policy rule to match the Security policy rule. If all the criteria match, the Security policy rule's action is applied. If the Security policy action is "allow," the packet is inspected by the Security profiles attached to the Security policy rule. If all the Security profile criteria do not match, or the Security policy is any action other than "allow," the packet is evaluated against the next Security policy rule, and so on. You can create

a Security profile group that includes one or more Security profiles, which simplifies the task of adding Security profiles to a Security policy rule.

Antivirus Security Profile Actions

The *default* profile inspects the listed protocol decoders for viruses and generates alerts for SMTP, IMAP, and POP3 protocols while blocking FTP, HTTP, and SMB protocols. You can configure the action for a decoder or antivirus signature and specify how the firewall responds to a threat event; see the following table:

ACTION	DESCRIPTION
Default	For each threat signature and Antivirus signature that is defined by Palo Alto Networks, a default action is specified internally. The default action typically is an "alert" or a "reset-both." The default action is displayed in parentheses, for example, default (alert), in the threat or antivirus signature.
Allow	Permits the application traffic.

Alert	Generates an alert for each application traffic flow. The alert is saved in the Threat log.
Drop	Drops the application traffic.
Reset Client	For TCP, resets the client-side connection. For UDP, drops the connection.
Reset Server	For TCP, resets the server-side connection. For UDP, drops the connection.
Reset Both	For TCP, resets the connection on both the client and server ends. For UDP, drops the connection.

You also can use customized profiles to minimize antivirus inspection for traffic between trusted security zones. They also can be used to maximize the inspection of traffic received from more untrusted zones such as the internet and of traffic sent to highly sensitive destinations such as server farms. The Palo Alto Networks WildFire product also provides signatures for persistent threats that are more evasive and have not yet been discovered by other antivirus solutions. As threats are discovered by WildFire, signatures are quickly created and then integrated into the standard antivirus signatures that can be downloaded daily by Threat Prevention subscribers (sub-hourly for WildFire subscribers).

Anti-Spyware Security Profile Actions

You can create custom Anti-Spyware profiles, or you can choose one of the two following predefined profiles when you apply Anti-Spyware to a Security policy rule:

`

PROFILE	DESCRIPTION
Default	Uses the default action for every signature, as specified by Palo Alto Networks when the signature is created.
Strict	Overrides the default action of critical-, high-, and medium-severity threats to the "block" action, regardless of the action defined in the signature file. This profile still uses the default action for low- and informational-severity signatures.

After the firewall detects a threat event, you can configure the following actions in an Anti-Spyware profile:

ACTION	DESCRIPTION
Default	For each threat signature and anti-spyware signature that Palo Alto Networks defines, a default action is specified internally. The default action typically is an "alert" or a "reset-both." The default action is displayed in parentheses in the threat or antivirus signature—for example, default (alert).
Allow	Permits the application traffic.
Alert	Generates an alert for each application traffic flow. The alert is saved in the Threat log.
Drop	Drops the application traffic.
Reset Client	For TCP, resets the client-side connection. For UDP, drops the connection.
Reset Server	For TCP, resets the server-side connection. For UDP, drops the connection.
Reset Both	For TCP, resets the connection on both the client and server ends. For UDP, drops the connection.
Block IP	Blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

You also can enable the DNS Sinkholing action in Anti-Spyware profiles to enable the firewall to create a response to a DNS query for a known malicious domain, thus causing the malicious domain name to resolve to a sinkhole IP address that you define. This feature helps to identify infected hosts on the protected network using DNS traffic. Infected hosts then easily can be identified in the Traffic and Threat logs because any host that attempts to connect to the sinkhole IP address most likely is infected with malware. Anti-Spyware and Vulnerability Protection profiles are configured similarly.

Two Predefined Antivirus Security Profiles

			Decoders				Dynamic Classification			
NAME	PACKET CAPTURE	NAME	ACTION	WILDFIRE ACTION	DYNAMIC CLASSIFICATION ACTION	NAME	POLICY ACTION	THREAT EXCEPTIONS	DYNAMIC CLASSIFICATION EXCEPTIONS
default		http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	enable	0	0
		http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	enable		
		smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	enable		
		imap	default (alert)	default (alert)	default (alert)				
		pop3	default (alert)	default (alert)	default (alert)				
		ftp	default (reset-both)	default (reset-both)	default (reset-both)				
		smb	default (reset-both)	default (reset-both)	default (reset-both)				
Corp-AV		http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	enable	0	0
		http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	enable		
		smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	enable		
		imap	default (alert)	default (alert)	default (alert)				
		pop3	default (alert)	default (alert)	default (alert)				
		ftp	default (reset-both)	default (reset-both)	default (reset-both)				
		smb	default (reset-both)	default (reset-both)	default (reset-both)				

Two default profiles

Vulnerability Protection Security Profile Actions

The *default* Vulnerability Protection Security profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

Two Predefined Vulnerability Protection Security Profiles

NAME	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
strict	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
		simple-client-high	any	client	high	reset-both	disable
		simple-client-medium	any	client	medium	reset-both	disable
		simple-client-informational	any	client	informational	default	disable
		simple-client-low	any	client	low	default	disable
		simple-server-critical	any	server	critical	reset-both	disable
		simple-server-high	any	server	high	reset-both	disable
		more...					
default	Rules: 6	simple-client-critical	any	client	critical	default	disable
		simple-client-high	any	client	high	default	disable
		simple-client-medium	any	client	medium	default	disable
		simple-server-critical	any	server	critical	default	disable
		simple-server-high	any	server	high	default	disable
		simple-server-medium	any	server	medium	default	disable

Two default profiles

URL Filtering Security Profile Actions

ACTION	DESCRIPTION
alert	The website is allowed, and a log entry is generated in the URL Filtering log.
allow	The website is allowed, and no log entry is generated.

`

block	The website is blocked. The user will see a response page and will not be able to continue to the website. A log entry is generated in the URL Filtering log. Blocking of site access for a URL category also sets User Credential Submissions for that URL category to “block.”
continue	The user will see a response page indicating that the site has been blocked due to company policy, but the user is prompted with the option to continue to the website. The “continue” action typically is used for categories that are considered benign and is used to improve the user experience by giving the user the option to continue if they consider the site to be incorrectly categorized. The response page’s message can be customized to contain details specific to your company. A log entry is generated in the URL Filtering log. The Continue webpage doesn’t display properly on client systems configured to use a proxy server.
override	The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security administrator or help-desk person would provide a password granting temporary access to all websites in the given category. A log entry is generated in the URL Filtering log. The Override webpage doesn’t display properly on client systems configured to use a proxy server.
none	The “none” action applies only to custom URL categories. Select none to ensure that, if multiple URL Filtering profiles exist, the custom category will not have any impact on other profiles. For example, if you have two URL Filtering profiles and the custom URL category is set to “block” in one profile, if you do not want the “block” action to apply to the other profile, you must set the action to none. Also, to delete a custom URL category, the category must be set to none in any profile where it is used.

File Blocking Security Profile Actions

`

FIELD	DESCRIPTION
Name	Enter a rule name (up to 31 characters in length).
Applications	Select the applications to which the rule applies, or select Any.
File Types	Click in the field and then click **Add** to display a list of supported file types. Click a file type to add it to the profile, and continue to add file types as needed. If you select **Any**, the defined action is taken on all supported file types.
Direction	Select the direction of the file transfer (upload, download, or both).
Action	Select the action taken when the selected file types are detected: **alert**: An entry is added to the Threat log. **block**: The file is blocked. **continue**: A message to the user indicates that a download has been requested and asks the user to confirm whether to continue. The purpose is to warn the user of a possible unknown download (also known as a drive-by download) and to give the user the option of continuing or stopping the download.

When you create a File Blocking profile with the action "continue," you can only choose the application web-browsing. If you choose any other application, traffic that matches the Security policy will not flow through the firewall because the users will not be prompted with a continue page.

4.4 Use information available in logs

4.4.1 Traffic

Traffic logs display an entry for the start and end of each session. Each entry includes the following information: date and time; source and destination zones, addresses and ports; application name; security rule applied to the traffic flow; rule action (allow, deny, or drop); ingress and egress interface; number of bytes; and session end reason.

The Type column indicates whether the entry is for the start or end of the session. The Action column indicates whether the firewall allowed, denied, or dropped the session. A drop indicates that the security rule that blocked the traffic specified any application, while a deny indicates that the rule identified a specific application. If the firewall drops traffic before identifying the application, such as when a rule drops all traffic for a specific service, the Application column displays not-applicable.

Click beside an entry to view additional details about the session, such as whether an ICMP entry aggregates multiple sessions between the same source and destination (in which case the Count column value is greater than one).

4.4.2 Threat

Threats are recorded and logged in the Threat log. A Threat log displays entries when traffic matches one of the Security profiles attached to a Security policy rule on the firewall. Each entry includes the following information: date and time; type of threat (such as virus or spyware); threat description or URL (**Name** column); source and destination zones, addresses, and ports; application name; alarm action (such as allow or block); and severity level. The Threat log is used as the source of information that is displayed on the **ACC** tab (Application Control Center).

Threat levels are based on severity. There are five levels of severity:

- **Critical**: Critical threats are serious threats such as those that affect default installations of widely deployed software and result in the compromise of servers. Critical threats include those where the exploit code is widely available to attackers. The attacker usually does not need any special authentication credentials or knowledge about the individual victims, and the target does not need to be manipulated into performing any special functions.
- **High**: High threats are those that can become critical but have mitigating factors; for example, they might be difficult to exploit, do not result in elevated privileges, or do not have a large victim pool.
- **Medium**: Medium threats are minor threats and those that pose minimal impact. Examples include DoS attacks that do not compromise the target or exploits that require an attacker to reside on the same LAN as the victim. Medium threats affect only nonstandard configurations or obscure applications, or they provide very limited access.

- **Low**: Low threats are warning-level threats that have little impact on an organization's infrastructure. They usually require local or physical system access and often might result in victim privacy or DoS issues and information leakage. Data Filtering profile matches are logged as Low.
- **Informational**: Informational threats are suspicious events that do not pose an immediate threat but that are reported to call attention to deeper problems that could exist. URL Filtering log entries are logged as Informational. Log entries with any verdict and an action set to “block” also are logged as Informational.

4.4.3 Data

Data Filtering logs display entries for the security rules that help prevent sensitive information such as credit-card numbers from leaving the area that the firewall protects. See Set Up Data Filtering for information on defining Data Filtering profiles.

This log type also shows information for File Blocking Profiles. For example, if a rule blocks .exe files, the log shows the blocked files.

4.4.4 System logs

System logs display entries for each system event on the firewall. Each entry includes the date and time, event severity, and event description. The following table summarizes the System log severity levels. For a partial list of System log messages and their corresponding severity levels, refer to System Log Events.

SEVERITY	DESCRIPTION
Critical	Hardware failures, including high availability (HA) failover and link failures.
High	Serious issues, including dropped connections with external devices, such as LDAP and RADIUS servers.
Medium	Mid-level notifications, such as antivirus package upgrades.
Low	Minor-severity notifications, such as user password changes.
Informational	Log in/log off, administrator name or password change, any configuration change, and all other events not covered by the other severity levels.

4.5 Enable DNS Security to control traffic based on domains

4.5.1 Where to configure DNS Security

DNS Security subscription enables users to access real-time protections using advanced predictive analytics. When techniques such as DGA/DNS tunneling detection and machine learning are used, threats hidden within DNS traffic can be proactively identified and shared through an infinitely

scalable cloud service. Because the DNS signatures and protections are stored in a cloud-based architecture, you can access the full database of ever-expanding signatures that have been generated using a multitude of data sources. This list of signatures allows you to defend against an array of threats using DNS in real time against newly generated malicious domains. To combat future threats, updates to the analysis, detection, and prevention capabilities of the DNS Security service will be available through content releases. To access the DNS Security service, you must have a Threat Prevention license and DNS Security license.

4.5.2 How to apply DNS Security in policy

Enable DNS Security

To enable DNS Security, domain queries using DNS Security that are found to be threats are remediated with an Anti-Spyware Security profile. Edit an existing or open a new Anti-Spyware profile at **Objects > Security Profiles > Anti-Spyware**.

Click the **DNS Policies** tab and expand the **DNS Security** group item in the list of signature sources. Each list item is a cloud-based collection of DNS identifying information of the threat type indicated in the list item name. The **Policy Action** column shows the selected remediation when a threat is found in a list. An explanation of these actions, including Sinkholing, can be found in Section 4.2 of this study guide, under Anti-Spyware Security Profile Actions. Anti-Spyware profiles configured for DNS Security protections are added to Security profiles that allow traffic to be inspected.

`

4.6 Create and deploy URL Filtering-based controls

4.6.1 Apply a URL profile in a Security policy

You can use URL filtering profiles to not only control access to web content, but also to control how users interact with web content.

WHAT ARE YOU LOOKING FOR?	SEE:
Control access to websites based on URL category.	URL Filtering Categories
Detect corporate credential submissions, and then decide the URL categories to which users can submit credentials.	User Credential Detection URL Filtering Categories
Block search results if the end user is not using the strictest safe search settings.	URL Filtering Settings
Enable logging of HTTP headers.	URL Filtering Settings
Control access to websites using custom HTTP Headers.	HTTP Header Insertion
Enable cloud and local inline categorization to analyze web pages in real-time for malicious content.	Inline Categorization
Looking for more?	• Learn more about how to configure URL Filtering. • Use URL categories to prevent credential phishing. • To create custom URL categories, select Objects > Custom Objects > URL Category. • To import a list of URLs that you want to enforce, select Objects > External Dynamic Lists.

4.6.2 Create a URL Filtering profile

A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules to enforce your web access policy. The firewall comes with a default profile that is configured to block threat-prone categories, such as malware, phishing, and adult. You can use the default profile in a Security policy, clone it to be used as a starting point for new URL Filtering profiles, or add a new URL Filtering profile. You can then customize the newly added URL profiles and add lists of specific websites that should always be blocked or allowed. For example, you may want to block social-networking sites but allow some websites that are part of the social-networking category.

After you determine URL Filtering policy requirements, you should have a basic understanding of the types of websites and website categories your users are accessing. Use this information to create custom URL Filtering profiles and attach them to the Security policy rules that allow web

access. In addition to managing web access with a URL Filtering profile, if you configure User-ID, you can manage the sites to which users can submit corporate credentials.

Step 1: Create a URL Filtering profile.

Select **Objects > Security Profiles > URL Filtering** and Add or modify a URL Filtering profile.

Step 2: Define site access for each URL category.

Select Categories and set the Site Access for each URL category:

- Allow traffic destined for that URL category; allowed traffic is not logged.
- Select **alert** to have visibility into sites that users are accessing. Traffic matching that category is allowed, but a URL Filtering log is generated to record when a user accesses a site in that category.
- Select **block** to deny access to traffic that matches that category and to enable logging of the blocked traffic.
- Select **continue** to display a page to users with a warning and require them to click Continue to proceed to a site in that category.
- To only allow access if users provide a configured password, select **override**. For more details, see Allow Password Access to Certain Sites.

Step 3: Configure the URL Filtering profile to detect corporate credential submissions to websites that are in allowed URL categories.

- Select **User Credential Detection**.
- Select one of the methods to check for corporate credential submissions to web pages from the User Credential Detection drop-down:
    - Use IP User Mapping—Checks for valid corporate username submissions and verifies that the username matches the user logged in to the source IP address of the session. To use this method, the firewall matches the submitted username against its IP-address-to-username mapping table. To use this method, you can use any of the user-mapping methods described in Map IP Addresses to Users.
    - Use Domain Credential Filter—Checks for valid corporate usernames and password submissions and verifies that the username maps to the IP address of the logged-in user. See Configure User Mapping Using the Windows User-ID Agent for instructions on how to set up User-ID to enable this method.
    - Use Group Mapping—Checks for valid username submissions based on the user-to-group mapping table populated when you configure the firewall to map users to groups. With group mapping, you can apply credential detection to any part of the directory or to a specific group, such as groups like IT that have access to your most sensitive applications.
- Set the Valid Username Detected Log Severity that the firewall uses to log detection of corporate credential submissions (default is medium).

`

Step 4: Allow or block users from submitting corporate credentials to sites based on URL category to prevent credential phishing.

- For each URL category to which you allow Site Access, select how you want to treat User Credential Submissions:
  - alert—Allow users to submit credentials to the website, but generate a URL filtering alert log each time a user submits credentials to sites in this URL category.
  - allow (default)—Allow users to submit credentials to the website.
  - block—Displays the Anti-Phishing Block Page to block users from submitting credentials to the website.
  - continue—Present the Anti-Phishing Continue Page to require users to click Continue to access the site.
- Configure the URL Filtering profile to detect corporate credential submissions to websites that are in allowed URL categories.

Step 5: Define URL category exception lists to specify websites that should always be blocked or allowed, regardless of URL category.

For example, to reduce URL Filtering logs, you may want to add your corporate websites to the allow list so that no logs are generated for those sites. Or, if there is a website that is being overly used and is not work-related, you can add that site to the block list.

The policy actions configured for custom URL categories have priority enforcement over matching URLs in external dynamic lists.

Traffic to websites in the block list is always blocked, regardless of the action, for the associated category; traffic to URLs in the allow list is always allowed.

For more information on the proper format and wildcard usage, see URL Category Exception Lists.

Step 6: Enable Safe Search Enforcement.

Step 7: Log only Container Pages for URL filtering events.

- Select **URL Filtering Settings**. Enable **Log container page only (default)** so that the firewall logs only the main page that matches the category, not subsequent pages or categories that load within the container page.
- To enable logging for all pages and categories, disable the **Log container page only** option.

Step 8: Enable HTTP Header Logging for one or more of the supported HTTP header fields.

Select **URL Filtering Settings** and select one or more of the following fields to log:

- User-Agent
- Referer
- X-Forwarded-For

Step 9: Save the URL Filtering profile and commit your changes.

`

- Click **OK**.
- Click **Commit**.

Step 10: Test your URL Filtering policy configuration.

- Access a website in the desired URL category and observe the firewall's behavior.
- Use Palo Alto Networks URL Filtering Test Pages (urlfiltering.paloaltonetworks.com/test-<url-category>) if you want to avoid directly accessing a site. Palo Alto Networks has test URLs for benign and malicious URL categories. For example, to test your block policy for malware, visit https://urlfiltering.paloaltonetworks.com/test-malware.
- Review the Traffic and URL Filtering logs (MonitorLogs) to confirm that the correct policy rule is logged.

Step 11: (PAN-OS 9.0.4 and later PAN-OS 9.0 releases only) Enable hold-client-request to block client requests while the firewall performs URL category lookups.

- Access the CLI.
- Enter **`configure`** to access Configuration Mode.
- Enter **`set deviceconfig setting ctd hold-client-request yes`** to enable the feature.
- Commit your changes.

Step 12: Set the amount of time before a URL category lookup times out.

- Access the CLI.
- Enter the **`configure`** command to access configuration mode.
- Enter the **`set deviceconfig setting ctd url-wait-timeout`** command followed by a number of seconds (default is 5).
- Commit your changes.

4.6.3 Create a custom URL category

Custom URL Filtering Categories
Use the **Custom URL Category** page to create your custom list of URLs and use it in a URL Filtering profile or as a match criterion in policy rules. In a custom URL category, you can add URL entries individually or import a text file that contains a list of URLs. URL entries added to custom categories are case-insensitive.

Custom URL category settings are as follows:

- **Name**: Enter a name to identify the custom URL category (up to 31 characters in length). This name displays in the category list when URL Filtering profiles are defined and in the match criteria for URL categories in policy rules. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
- **Description**: Enter a description for the URL category (up to 255 characters in length).
- **Sites**:
    - Click **Add** to enter URLs, only one in each row. Each URL can be in the format "www.example.com" or can include wildcards ("*.example.com").

`

- Click **Import** and browse to select the text file that contains the list of URLs. Enter only one URL per row. Each URL can be in the format "www.example.com" or can include wildcards ("*.example.com").
- Click **Export** to export the custom URL entries included in the list. The URLs are exported as a text file.
- Select an entry and click **Delete** to remove the URL from the list. Before you can delete a custom category that you have used in a URL Filtering profile, you must set the action to **None**. Go to Category actions in **Objects > Security Profiles > URL Filtering**.

4.6.4 Control traffic based on a URL category

Block or allow traffic based on URL category—You can create a URL Filtering profile that specifies an action for each URL category and attach the profile to a policy. Traffic that matches the policy would then be subject to the settings in the profile. For example, to block all gaming websites, you would configure a URL Filtering profile with the "block" action set for the games URL category and apply the profile to the Security policy rule(s) that allow web access. See Configure URL Filtering for more information.

4.6.5 Why a URL was blocked

Basic Guidelines for URL Category Exception Lists

- Enter the IP addresses or URLs of websites that you want to enforce separately from the associated URL category.
- List entries must be an exact match but are case-insensitive.
- You can enter a string that is an exact match to the website (and possibly, specific subdomain) for which you want to control access, or you can use wildcard characters to allow an entry to match to more than one website subdomain. For details on using wildcard characters, review Wildcard Guidelines for URL Category Exception Lists.
- Omit http and https from URL entries.
- Each URL entry can be up to 255 characters in length.

Wildcard Guidelines for URL Category Exception Lists

You can use wildcards in URL category exception lists to easily configure a single entry to match to multiple website subdomains and pages, without having to specify exact subdomains and pages.

Follow these guidelines when creating wildcard entries:

`

- The following characters are considered token separators: . / ? & = ; +

  Every string separated by one or two of these characters is a token. Use wildcard characters as token placeholders, indicating that a specific token can contain any value.

- In place of a token, use either an asterisk (*) or a caret (^) to indicate a wildcard value.
- Wildcard characters must be the only character within a token. For example, www.gmail*.com would be invalid because the asterisk follows other characters. An entry can contain multiple wildcards, however.

4.6.6 How to allow a blocked URL

Define URL category exception lists to specify websites that should always be blocked or allowed, regardless of URL category.

For example, to reduce URL Filtering logs, you may want to add your corporate websites to the allow list so that no logs are generated for those sites. Or, if there is a website that is being overly used and is not work-related, you can add that site to the block list.

The policy actions configured for custom URL categories have priority enforcement over matching URLs in external dynamic lists.

Traffic to websites in the block list is always blocked, regardless of the action, for the associated category; traffic to URLs in the allow list is always allowed.

Add the IP addresses or URLs of the sites you want to block or allow directly to a URL Filtering profile (Objects > Security Profiles > URL Filtering > Overrides). Then, attach the profile to a Security policy rule.

4.6.7 How to request a URL recategorization

If you think that a URL is not categorized accurately, you can request for Palo Alto Networks to categorize it differently. Submit a change request directly in the firewall, or use Test A Site. A change request triggers PAN-DB—the URL Filtering cloud—to do an immediate analysis of the URL for which you are suggesting a category change. If PAN-DB validates that the new category suggestion is accurate, the change request is approved. If PAN-DB does not find the new category suggestion to be accurate, the change request is then reviewed by human editors from the Palo Alto Networks threat research and data science teams.

After you've submitted a change request, you'll receive an email from us confirming that we've received your request. When we've completed our investigation, you'll receive a second email confirming the results.

You cannot request to change the risk category a URL receives (high risk, medium risk, or low risk), or request to change the URLs categorized as insufficient content or newly-registered domains.

Make a Change Request Online

Visit Palo Alto Networks URL Filtering Test A Site to make a change request online.

Step 1: Go to Test A Site.

You do not need to log in to submit a change request, though you will need to provide your email as part of the change request form. If you decide not to log in, you'll need to take a CAPTCHA test to confirm that you're a human being (log in to avoid the CAPTCHA test).

Step 2: Enter a URL to check its categories:

Step 3: Review the URL categories, and if you don't think that they're accurate, select Request Change.

Step 4: Continue to populate and submit the change request form.

Include at least one (and up to two) new category suggestions, and leave an (optional) comment to tell us more about your suggestion.

`

Make a Bulk Change Request

You can also use Test A Site to make a bulk change request, where you want to submit change requests for multiple URLs at a single time.

Step 1: Go to Test A Site.

You don't need to log in to make a change request; however, you'll need to provide your email as part of completing the change request form. If you decide not to log in, you'll need to take a CAPTCHA test to confirm that you're a human being (log in to avoid the CAPTCHA test).

Step 2: Choose the option to submit a bulk change request:

Step 3: Complete and submit the bulk change request form.

Make a Change Request from the Firewall

You can also submit a URL category change request directly from the firewall. In the URL Filtering logs, the details for each log entry include an option to Request Categorization Change (Monitor > Logs > URL Filtering).

From here, you can complete the request form and submit it.

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

An Interface Management profile protects the firewall from unauthorized access by defining the protocols, services, and IP addresses that a firewall interface permits for management traffic. For example, you might want to prevent users from accessing the firewall web interface over the ethernet1/1 interface but allow that interface to receive SNMP queries from your network monitoring system. In this case, you would enable SNMP and disable HTTP/HTTPS in an Interface Management profile and assign the profile to ethernet1/1.

You can assign an Interface Management profile to Layer 3 Ethernet interfaces (including subinterfaces) and to logical interfaces (aggregate group, VLAN, loopback, and tunnel interfaces). If you do not assign an Interface Management profile to an interface, the profile denies access for all IP addresses, protocols, and services by default.

4.7.2 How to apply the specific policies

Several options must be configured before User-ID can function. The LDAP Server profile is the most important item to configure. The LDAP Server profile is used to connect the firewall to an LDAP server and retrieve a list of usernames and groups. The LDAP Server profile will require different information, depending on what is used.

After configuring the LDAP Server profile, you need to configure the group mapping:

4.7.3 Identify users within the ACC and the monitor tab

Administrators should select the LDAP Server profile they configured earlier and complete the domain settings. The **Group Include List** tab will show the available groups in the domain. The administrator can choose which groups to monitor and which ones to ignore:

`

To learn more about the methods to map users and groups to collect User-ID information, see the following information:

- The "Block Threats by Identifying Users" module in the EDU-210 training, Firewall Essentials: Configuration and Management
- User-ID in the *PAN-OS Administrator's Guide*

4.8 Sample Questions

Q1. If you have a Threat Prevention subscription but not a WildFire subscription, how long must you wait for the WildFire signatures to be added into the antivirus update?

a. 1 to 2 hours
b. 2 to 4 hours
c. 10 to 12 hours
d. 24 to 48 hours

Q2. What are two benefits of Vulnerability Protection Security profiles? (Choose two.)

a. They prevent compromised hosts from trying to communicate with external C2 servers.
b. They protect against viruses, worms, and Trojans.
c. They prevent exploitation of system flaws.
d. They prevent unauthorized access to systems.

Q3. Which two actions are available for Antivirus Security profiles? (Choose two.)

a. Continue
b. Allow
c. Block IP
d. Alert

Q4. Which two actions are required to implement DNS Security inspections of traffic? (Choose two.)

a. Add an Anti-Spyware Security profile with DNS remediations to a Security policy.
b. Enable the Advanced DNS Security check box in General Settings.
c. Configure an Anti-Spyware Security profile with DNS remediations.
d. Enter the address for the Secure DNS service in the firewall's DNS settings.

Q5. Which two types of attacks does the PAN-DB prevent? (Choose two.)

a. Phishing site
b. HTTP-based command and control
c. Infected JavaScript
d. Flood attacks

Q6. Which two valid URLs can be used in a custom URL category? (Choose two.)

a. ww.youtube.**
b. www.**.com
c. www.youtube.com
d. *youtube*
e. *.youtube.com

`

Appendix A: Sample Questions with Answers

Below are the questions offered throughout the study guide, with the correct answers indicated.

Domain 1

Q1. What are two firewall management methods? (Choose two.)

- **a. CLI**
- b. RDP
- c. VPN
- **d. XML API**

Q2. Which two devices are used to connect a computer to the firewall for management purposes? (Choose two.)

- a. Rollover cable
- **b. Serial cable**
- **c. RJ-45 Ethernet cable**
- d. USB cable

Q3. What is the default IP address assigned to the MGT interfaces of a Palo Alto Networks firewall?

- **a. 192.168.1.1**
- b. 192.168.1.254
- c. 10.0.0.1
- d. 10.0.0.254

Q4. What are the two default services that are available on the MGT interface? (Choose two.)

- **a. HTTPS**
- **b. SSH**
- c. HTTP
- d. Telnet

Q5. True or false? Service route traffic has Security policy rules applied against it.

- **a. true**
- b. false

Q6. Service routes may be used to forward which two traffic types out of a data port? (Choose two.)

- **a. External dynamic lists**
- b. MineMeld
- c. Skype
- **d. Palo Alto Networks updates**

Q7. Which command must be performed on the firewall to activate any changes?

- **a. Commit**
- b. Save
- c. Load
- d. Import

Q8 Which command backs up configuration files to a remote network device?

- a. Import
- b. Load

`

c. Copy
d. Export

Q9. The command load named configuration snapshot overwrites the current candidate configuration with which three items? (Choose three.)

a. Custom-named candidate configuration snapshot (instead of the default snapshot)
b. Custom-named running configuration that you imported
c. Snapshot.xml
d. Current running configuration (running-config.xml)
e. Palo Alto Networks updates

Q10. What are two firewall management methods? (Choose two.)

a. CLI
b. RDP
c. VPN
d. XML API

Q11. True or false? A Palo Alto Networks firewall automatically provides a backup of the configuration during a software upgrade.

a. true
b. false

Q12. If you have a Threat Prevention subscription but not a WildFire subscription, how long must you wait for the WildFire signatures to be added into the antivirus update?

a. 1 to 2 hours
b. 2 to 4 hours
c. 10 to 12 hours
d. 24 to 48 hours

Q13. Which three actions should you complete before you upgrade to a newer version of software? (Choose three.)

a. Review the release notes to determine any impact of upgrading to a newer version of software.
b. Ensure that the firewall is connected to a reliable power source.
c. Export the device state.
d. Create and externally store a backup before you upgrade.
e. Put the firewall in maintenance mode.

Q14. Which two default zones are included with the PAN-OS software? (Choose two.)

a. Interzone
b. Extrazone
c. Intrazone
d. Extranet

Q15. Which two zone types are valid options? (Choose two.)

a. Trusted
b. Tap
c. Virtual wire
d. Untrusted
e. DMZ

`

Q16. Which two statements about interfaces are correct? (Choose two.)

a. Interfaces must be configured before you can create a zone.
b. Interfaces do not have to be configured before you can create a zone.
c. An interface can belong to only one zone.
d. An interface can belong to multiple zones.

Q17. Which two interface types can belong in a Layer 3 zone? (Choose two.)

a. Loopback
b. Tap
c. Tunnel
d. Virtual Wire

Q18. What are used to control traffic through zones?

a. Access lists
b. Security policy lists
c. Security policy rules
d. Access policy rules

Q19. For inbound inspection, which two actions can be done with a Tap interface? (Choose two.)

a. Encrypt traffic
b. Decrypt traffic
c. Allow or block traffic
d. Log traffic

Q20. Which two actions can be done with a Virtual Wire interface? (Choose two.)

a. NAT
b. Route
c. Switch
d. Log traffic

Q21. Which two actions can be done with a Layer 3 interface? (Choose two.)

a. NAT
b. Route
c. Switch
d. Create a virtual wire object

Q22. Layer 3 interfaces support which two items? (Choose two.)

a. NAT
b. IPv6
c. Switching
d. Spanning tree

Q23. Layer 3 interfaces support which three advanced settings? (Choose three.)

a. IPv4 addressing
b. IPv6 addressing
c. NDP configuration
d. Link speed configuration
e. Link duplex configuration

Q24. Layer 2 interfaces support which three items? (Choose three.)

`

a. Spanning tree blocking
b. Traffic examination
c. Forwarding of spanning tree BPDUs
d. Traffic shaping via QoS
e. Firewall management
f. Routing

Q25. Which two interface types support subinterfaces? (Choose two.)
a. Virtual Wire
b. Layer 2
c. Loopback
d. Tunnel

Q26. Which two statements are true regarding Layer 3 interfaces? (Choose two.)
a. You can configure a Layer 3 interface with one or more IP addresses as a DHCP client.
b. A Layer 3 interface can only have one DHCP assigned address.
c. You can assign only one IPv4 address to the same interface.
d. You can enable an interface to send IPv4 router advertisements by selecting the Enable Router Advertisement check box on the Router Advertisement tab.
e. You can apply an Interface Management profile to the interface.

Q27. Which statement is true regarding aggregate Ethernet interfaces?
a. Members of an aggregate interface group can be of different media types.
b. An aggregate interface group can be set to a type of tap.
c. Ethernet interfaces that are members of an aggregate interface group must have the same transmission speeds.
d. A Layer 3 aggregate interface group can have more than one IP assigned to it.
e. Members of aggregate Ethernet interfaces can be assigned to different virtual routers.

Q28. What is the default administrative distance of a static route within the PAN-OS software?
a. 1
b. 5
c. 10
d. 100

Q29. Which two dynamic routing protocols are available in the PAN-OS software? (Choose two.)
a. RIP1
b. RIPv2
c. OSPFv3
d. EIGRP

Q30. Which value is used to distinguish the preference of routing protocols?
a. Metric
b. Weight
c. Distance
d. Cost
e. Administrative distance

Q31. Which value is used to distinguish the best route within the same routing protocol?
a. Metric

`

b. Weight
c. Distance
d. Cost
e. Administrative distance

Q32. In path monitoring, what is used to monitor remote network devices?
a. Ping
b. SSL
c. HTTP
d. HTTPS
e. Link state

Domain 2

Q1. Which two statements are true about a Role Based Admin Role Profile role? (Choose two.)
a. It is a built-in role.
b. It can be used for CLI commands.
c. It can be used for XML API.
d. Superuser is an example of such a role.

Q2. The management console supports which two authentication types? (Choose two.)
a. RADIUS
b. SMB
c. LDAP
d. TACACS+
e. AWS

Q3. Which two Dynamic Admin Role types are available on the PAN-OS software? (Choose two.)
a. Superuser
b. Superuser (write-only)
c. Device user
d. Device administrator (read-only)

Q4. Which type of profile does an authentication sequence include?
a. Security
b. Authorization
c. Admin
d. Authentication

Q5. An Authentication profile includes which other type of profile?
a. Server
b. Admin
c. Customized
d. Built-In

Q6. True or false? Dynamic Admin Roles are called “dynamic” because you can customize them.
a. true
b. false

`

Q7. Which profile is used to override global minimum password complexity requirements?

a. Authentication
b. Local
c. User
d. Password

Q8. What does an application filter enable an administrator to do?

a. Manually categorize multiple service filters.
b. Dynamically categorize multiple service filters.
c. Dynamically categorize multiple applications.
d. Manually categorize multiple applications.

Q9. Which two items can be added to an application group? (Choose two.)

a. Application groups
b. Application services
c. Application filters
d. Application categories

Q10. What are two application characteristics? (Choose two.)

a. Stateful
b. Excessive bandwidth use
c. Intensive
d. Evasive

Domain 3

Q.1 What will be the result of one or more occurrences of shadowing?

a. A failed commit
b. An invalid configuration
c. A warning
d. An alarm window

Q2. Which column in the Applications and Threats screen includes the options Review Apps and Review Policies?

a. Features
b. Type
c. Version
d. Action

Q3. Which link can you select in the web interface to minimize the risk of installing new App-ID updates?

a. Enable new apps in content update.
b. Disable new apps in App-ID database.
c. Disable new apps in content update.
d. Enable new apps in App-ID database.

Q5. Which two protocols are implicitly allowed when you select the facebook-base application? (Choose two.)

`

a. Web-browsing
b. Chat
c. Gaming
d. SSL

Q7. What are the two default (predefined) Security policy rule types in PAN-OS software? (Choose two.)
a. Universal
b. Interzone
c. Intrazone
d. Extrazone

Q8. Which type of Security policy rules most often exist above the two predefined Security policies?
a. Intrazone
b. Interzone
c. Universal
d. Global

Q9. What does the TCP Half Closed setting mean?
a. Maximum length of time that a session remains in the session table between reception of the first FIN and reception of the third FIN or RST.
b. Minimum length of time that a session remains in the session table between reception of the first FIN and reception of the second FIN or RST.
c. Maximum length of time that a session remains in the session table between reception of the first FIN and reception of the second FIN or RST.
d. Minimum length of time that a session remains in the session table between reception of the first FIN and reception of the third FIN or RST.

Q10. What are two application characteristics? (Choose two.)
a. Stateful
b. Excessive bandwidth use
c. Intensive
d. Evasive

Q11. Which two HTTP Header Logging options are within a URL Filtering profile? (Choose two.)
a. User-Agent
b. Safe Search
c. URL redirection
d. X-Forwarded-For

Q12. What are two source NAT types? (Choose two.)
a. Universal
b. Static
c. Dynamic
d. Extrazone

`

Q13. Which phrase is a simple way to remember how to configure Security policy rules where NAT was implemented?

a. Post-NAT IP, pre-NAT zone
b. Post-NAT IP, post-NAT zone
c. Pre-NAT IP, post-NAT zone
d. Pre-NAT IP, pre-NAT zone

Q14. What are two types of destination NAT? (Choose two.)

a. Dynamic IP (with session distribution)
b. DIPP
c. Global
d. Static

Q15. What are two possible values for DIPP (Dynamic IP and Port NAT) oversubscription? (Choose two.)

a. 1x
b. 4x
c. 16x
d. 32x

Q16. Which statement is true regarding bidirectional NAT?

a. For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure.
b. For static translations, bidirectional NAT enables the firewall to create a corresponding translation in the same direction as the translation you configure.
c. For dynamic translations, bidirectional NAT enables the firewall to create a corresponding translation in the opposite direction of the translation you configure.
d. For dynamic translations, bidirectional NAT enables the firewall to create a corresponding translation in the same direction as the translation you configure.

Q17. The Policy Optimizer does not analyze which statistics?

a. Applications allowed through port-based Security policy rules.
b. The usage of existing App-IDs in Security policy rules.
c. Which users matched Security policies.
d. Existing Security policy rule App-IDs that have not matched processed traffic.
e. Days since the latest new application discovery in a port-based Security policy rule.

Domain 4

Q1. If you have a Threat Prevention subscription but not a WildFire subscription, how long must you wait for the WildFire signatures to be added into the antivirus update?

a. 1 to 2 hours
b. 2 to 4 hours
c. 10 to 12 hours
d. 24 to 48 hours

Q2. What are two benefits of Vulnerability Protection Security profiles? (Choose two.)

a. They prevent compromised hosts from trying to communicate with external C2 servers.

`

b. They protect against viruses, worms, and Trojans.
c. They prevent exploitation of system flaws.
d. They prevent unauthorized access to systems.

Q3. Which two actions are available for Antivirus Security profiles? (Choose two.)
a. Continue
b. Allow
c. Block IP
d. Alert

Q4. Which two actions are required to implement DNS Security inspections of traffic? (Choose two.)
a. Add an Anti-Spyware Security profile with DNS remediations to a Security policy.
b. Enable the Advanced DNS Security check box in General Settings.
c. Configure an Anti-Spyware Security profile with DNS remediations.
d. Enter the address for the Secure DNS service in the firewall's DNS settings.

Q5. Which two types of attacks does the PAN-DB prevent? (Choose two.)
a. Phishing site
b. HTTP-based command and control
c. Infected JavaScript
d. Flood attacks

Q6. Which two valid URLs can be used in a custom URL category? (Choose two.)
a. ww.youtube.**
b. www.**.com
c. www.youtube.com
d. *youtube*
e. *.youtube.com

`

Continuing Your Learning Journey with Palo Alto Networks

Training from Palo Alto Networks and our Authorized Training Partners delivers the knowledge and expertise to prepare you to protect our way of life in the digital age. Our trusted security certifications give you the Palo Alto Networks product portfolio knowledge necessary to prevent successful cyberattacks and to safely enable applications.

Digital Learning

For those of you who want to keep up to date on our technology, a learning library of *free* digital learning is available. These on-demand, self-paced digital-learning classes are a helpful way to reinforce the key information for those who have been to the formal hands-on classes. They also serve as a useful overview and introduction to working with our technology for those unable to attend a hands-on, instructor-led class.

Simply register in Beacon and you will be given access to our digital-learning portfolio. These online classes cover foundational material and contain narrated slides, knowledge checks, and, where applicable, demos for you to access.

New courses are being added often, so check back to see new curriculum available.

Instructor-Led Training

Looking for a hands-on, instructor-led course in your area?

Palo Alto Networks Authorized Training Partners (ATPs) are located globally and offer a breadth of solutions from onsite training to public, open-environment classes. About 42 authorized training centers are delivering online courses in 14 languages and at convenient times for most major markets worldwide. For class schedule, location, and training offerings, see https://www.paloaltonetworks.com/services/education/atc-locations.

Learning Through the Community

You also can learn from peers and other experts in the field. Check out our communities site at https://live.paloaltonetworks.com, where you can:

- Discover reference material
- Learn best practices
- Learn what is trending

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.