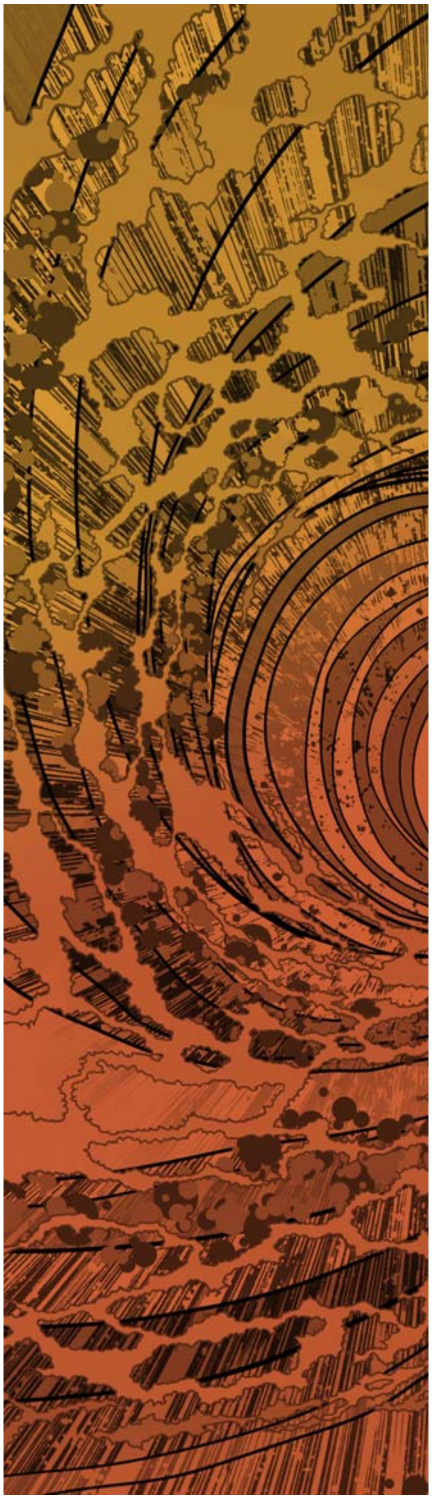


paloalto NETWORKS®

PAN-OS® Administrator's Guide

Version 7.0

Contact Information

Corporate Headquarters:

Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About this Guide

This guide takes you through the configuration and maintenance of your Palo Alto Networks next-generation firewall. For additional information, refer to the following resources:

- For information on how to configure other components in the Palo Alto Networks Next-Generation Security Platform, go to the Technical Documentation portal: https://www.paloaltonetworks.com/documentation or search the documentation.
- For access to the knowledge base and community forums, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.
- For the most current PAN-OS and Panorama 7.0 release notes, go to https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os-release-notes.html.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: May 18, 2017

Policy

Policies allow you to enforce rules and take action. The different types of policy rules that you can create on the firewall are: Security, NAT, Quality of Service (QoS), Policy Based Forwarding (PBF), Decryption, Application Override, Captive Portal, Denial of Service (DoS), and Zone protection policies. All these different policies work together to allow, deny, prioritize, forward, encrypt, decrypt, make exceptions, authenticate access, and reset connections as needed to help secure your network. The following topics describe how to work with policy:

- ▲ Policy Types
- ▲ Security Policy
- ▲ Policy Objects
- ▲ Security Profiles
- ▲ Enumeration of Rules Within a Rulebase
- ▲ Move or Clone a Policy Rule or Object to a Different Virtual System
- ▲ Use Tags to Group and Visually Distinguish Objects
- ▲ Use a Dynamic Block List in Policy
- ▲ Register IP Addresses and Tags Dynamically
- ▲ Monitor Changes in the Virtual Environment
- ▲ CLI Commands for Dynamic IP Addresses and Tags
- ▲ Identify Users Connected through a Proxy Server
- ▲ Policy-Based Forwarding

Policy Types

The Palo Alto Networks next-generation firewall supports a variety of policy types that work together to safely enable applications on your network.

Policy Type	Description
Security	Determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service. For more details, see Security Policy.
NAT	Instruct the firewall which packets need translation and how to do the translation. The firewall supports both source address and/or port translation and destination address and/or port translation. For more details, see NAT.
QoS	Identify traffic requiring QoS treatment (either preferential treatment or bandwidth-limiting) using a defined parameter or multiple parameters and assign it a class. For more details, see Quality of Service.
Policy Based Forwarding	Identify traffic that should use a different egress interface than the one that would normally be used based on the routing table. For details, see Policy-Based Forwarding.
Decryption	Identify encrypted traffic that you want to inspect for visibility, control, and granular security. For more details, see Decryption.
Application Override	Identify sessions that you do not want processed by the App-ID engine, which is a Layer-7 inspection. Traffic matching an application override policy forces the firewall to handle the session as a regular stateful inspection firewall at Layer-4. For more details, see Manage Custom or Unknown Applications.
Captive Portal	Identify traffic that requires the user to be known. The captive portal policy is only triggered if other User-ID mechanisms did not identify a user to associate with the source IP address. For more details, see Captive Portal.
DoS Protection	Identify potential denial-of-service (DoS) attacks and take protective action in response to rule matches. For more details, see DoS Protection Profiles.

Security Policy

Security policies protect network assets from threats and disruptions and aid in optimally allocating network resources for enhancing productivity and efficiency in business processes. On the Palo Alto Networks firewall, security policies determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

All traffic passing through the firewall is matched against a session and each session is matched against a security policy. When a session match occurs, the security policy is applied to bi-directional traffic (client to server and server to client) in that session. For traffic that doesn't match any defined rules, the default rules apply. The default rules—displayed at the bottom of the security rulebase—are predefined to allow all intrazone (within the zone) traffic and deny all interzone (between zones) traffic. Although these rules are part of the pre-defined configuration and are read-only by default, you can override them and change a limited number of settings, including the tags, action (allow or block), log settings, and security profiles.

Security policies are evaluated left to right and from top to bottom. A packet is matched against the first rule that meets the defined criteria; after a match is triggered the subsequent rules are not evaluated. Therefore, the more specific rules must precede more generic ones in order to enforce the best match criteria. Traffic that matches a rule generates a log entry at the end of the session in the traffic log, if logging is enabled for that rule. The logging options are configurable for each rule, and can for example be configured to log at the start of a session instead of, or in addition to, logging at the end of a session.

▲ Components of a Security Policy Rule

▲ Security Policy Best Practices

Components of a Security Policy Rule

The security policy rule construct permits a combination of the required and optional fields as detailed in the following tables:

- Required Fields
- Optional Fields

Required Fields

Required Field	Description
Name	A label that supports up to 31 characters, used to identify the rule.
Rule Type	Specifies whether the rule applies to traffic within a zone, between zones, or both: • **universal** (default)—Applies the rule to all matching interzone and intrazone traffic in the specified source and destination zones. For example, if you create a universal role 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, and all traffic from zone A to zone B and all traffic from zone B to zone A. • **intrazone**—Applies the rule to all matching traffic within the specified source zones (you cannot specify a destination zone for intrazone rules). For example, if you set the source zone 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. • **interzone**—Applies the rule to all matching traffic between the specified source and destination zones. For example, if you set the source zone 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 traffic within zones A, B, or C.
Source Zone	The zone from which the traffic originates.
Destination Zone	The zone at which the traffic terminates. If you use NAT, make sure to always reference the post-NAT zone.
Application	The application which you wish to control. The firewall uses App-ID, the traffic classification technology, to identify traffic on your network. App-ID provides application control and visibility in creating security policies that block unknown applications, while enabling, inspecting, and shaping those that are allowed.

Required Field	Description (Continued)
Action	Specifies an *Allow* or *Block* action for the traffic based on the criteria you define in the rule. When you configure the firewall to block traffic, it either resets the connection or silently drops packets. To provide a better user experience, you can configure granular options to block traffic instead of silently dropping packets, which can cause some applications to break and appear unresponsive to the user. • **Allow**—(default action) Allows the traffic. • **Deny**—Blocks traffic, and enforces the default *Deny Action* defined for the application that is being denied. To view the deny action defined by default for an application, view the application details in **Objects > Applications** or check the application details in Applipedia. • **Drop**—Silently drops the traffic; for an application, it overrides the default deny action. A TCP reset is not sent to the host/application. For Layer 3 interfaces, to optionally send an ICMP unreachable response to the client, set Action: **Drop** and enable the **Send ICMP Unreachable** checkbox. When enabled, the firewall sends the ICMP code for *communication with the destination is administratively prohibited*— ICMPv4: Type 3, Code 13; ICMPv6: Type 1, Code 1. • Reset—Resets a connection in one of the following ways. • **Reset client**—Sends a TCP reset to the client-side device. • **Reset server**—Sends a TCP reset to the server-side device. • **Reset both**—Sends a TCP reset to both the client-side and server-side devices. A reset is sent only after a session is formed. If the session is blocked before a 3-way handshake is completed, the firewall does not send a reset. For a TCP session with a reset action, the firewall does not send an ICMP Unreachable response. For a UDP session with a drop or reset action, if the **ICMP Unreachable** checkbox is selected, the firewall sends an ICMP message to the client.

Optional Fields

Optional Field	Description
Tag	A keyword or phrase that allows you to filter security rules. This is handy when you have defined many rules and wish to then review those that are tagged with a keyword such as *IT-sanctioned applications* or *High-risk applications.*
Description	A text field, up to 255 characters, used to describe the rule.
Source IP Address	Define host IP or FQDN, subnet, named groups, or country-based enforcement. If you use NAT, make sure to always refer to the original IP addresses in the packet (i.e. the pre-NAT IP address).
Destination IP Address	The location or destination for the traffic. If you use NAT, make sure to always refer to the original IP addresses in the packet (i.e. the pre-NAT IP address).
User	The user or group of users for whom the policy applies. You must have User-ID enabled on the zone. To enable User-ID, see User-ID Overview.

Optional Field	Description (Continued)
URL Category	Using the URL Category as match criteria allows you to customize security profiles (antivirus, anti-spyware, vulnerability, file-blocking, Data Filtering, and DoS) on a per-URL-category basis. For example, you can prevent.exe file download/upload for URL categories that represent higher risk while allowing them for other categories. This functionality also allows you to attach schedules to specific URL categories (allow social-media websites during lunch & after-hours), mark certain URL categories with QoS (financial, medical, and business), and select different log forwarding profiles on a per-URL-category-basis. Although you can manually configure URL categories on your device, to take advantage of the dynamic URL categorization updates available on the Palo Alto Networks firewalls, you must purchase a URL filtering license. To block or allow traffic based on URL category, you must apply a URL Filtering profile to the security policy rules. Define the URL Category as *Any* and attach a URL Filtering profile to the security policy. See Define Basic Security Rules for information on using the default profiles in your security policy and see Control Access to Web Content for more details.
Service	Allows you to select a Layer 4 (TCP or UDP) port for the application. You can choose *any*, specify a port, or use *application-default* to permit use of the standards-based port for the application. For example, for applications with well- known port numbers such as DNS, the *application-default* option will match against DNS traffic only on TCP port 53. You can also add a custom application and define the ports that the application can use. For inbound allow rules (for example, from untrust to trust), using *application-default* prevents applications from running on unusual ports and protocols. Application-default is the default option; while the device still checks for all applications on all ports, with this configuration, applications are only allowed on their standard ports/protocols.
Security Profiles	Provide additional protection from threats, vulnerabilities, and data leaks. Security profiles are only evaluated for rules that have an *allow* action.
HIP Profile (for GlobalProtect)	Allows you to identify clients with Host Information Profile (HIP) and then enforce access privileges.
Options	Allow you to define logging for the session, log forwarding settings, change Quality of Service (QoS) markings for packets that match the rule, and schedule when (day and time) the security rule should be in effect.

Security Policy Best Practices

The task of safely enabling Internet access and preventing misuse of web access privileges, and exposure to vulnerabilities and attacks is a continuous process. The key principle when defining policy on the Palo Alto Networks firewall is to use a positive enforcement approach. Positive enforcement implies that you selectively allow what is required for day-to-day business operations as opposed to a negative enforcement approach where you would selectively block everything that is not allowed. Consider the following suggestions when creating policy:

- ❐ If you have two or more zones with identical security requirements, combine them into one security rule.
- ❐ The ordering of rules is crucial to ensure the best match criteria. Because policy is evaluated top down, the more specific policy must precede the ones that are more general, so that the more specific rule is not *shadowed*. The term shadow refers to a rule that is not evaluated or is skipped because it is placed lower in the policy list. When the rule is placed lower, it is not evaluated because the match criteria was met by another rule that preceded it, thereby shadowing the rule from policy evaluation.
- ❐ To restrict and control access to inbound applications, in the security policy, explicitly define the port that the service/application will be listening on.
- ❐ Logging for broad allow rules—for example access to well known servers like DNS—can generate a lot of traffic. Hence it is not recommended unless absolutely necessary.
- ❐ By default, the firewall creates a log entry at the end of a session. However, you can modify this default behavior and configure the firewall to log at the start of the session. Because this significantly increases the log volume, logging at session start is recommended only when you are troubleshooting an issue. Another alternative for troubleshooting without enabling logging at session start is to use the session browser (**Monitor > Session Browser**) to view the sessions in real time.

Policy Objects

A *policy object* is a single object or a collective unit that groups discrete identities such as IP addresses, URLs, applications, or users. With policy objects that are a collective unit, you can reference the object in security policy instead of manually selecting multiple objects one at a time. Typically, when creating a policy object, you group objects that require similar permissions in policy. For example, if your organization uses a set of server IP addresses for authenticating users, you can group the set of server IP addresses as an *address group* policy object and reference the address group in the security policy. By grouping objects, you can significantly reduce the administrative overhead in creating policies.

You can create the following policy objects on the firewall:

Policy Object	Description
Address/Address Group, Region	Allow you to group specific source or destination addresses that require the same policy enforcement. The address object can include an IPv4 or IPv6 address (single IP, range, subnet) or the FQDN. Alternatively, a region can be defined by the latitude and longitude coordinates or you can select a country and define an IP address or IP range. You can then group a collection of address objects to create an *address group* object. You can also use dynamic address groups to dynamically update IP addresses in environments where host IP addresses change frequently.
User/User Group	Allow you to create a list of users from the local database or an external database and group them.
Application Group and Application Filter	An *Application Filter* allows you to filter applications dynamically. It allows you to filter, and save a group of applications using the attributes defined in the application database on the firewall. For example, you can Create an Application Filter by one or more attributes—category, sub-category, technology, risk, characteristics. With an application filter, when a content update occurs, any new applications that match your filter criteria are automatically added to your saved application filter. An *Application Group* allows you to create a static group of specific applications that you want to group together for a group of users or for a particular service, or to achieve a particular policy goal. See Create an Application Group.
Service/Service Groups	Allows you to specify the source and destination ports and protocol that a service can use. The firewall includes two pre-defined services—service-http and service-https—that use TCP ports 80 and 8080 for HTTP, and TCP port 443 for HTTPS. You can however, create any custom service on any TCP/UDP port of your choice to restrict application usage to specific ports on your network (in other words, you can define the default port for the application). To view the standard ports used by an application, in **Objects > Applications** search for the application and click the link. A succinct description displays.

Security Profiles

While security policies enable you to allow or block traffic on your network, security profiles help you define an *allow but scan* rule, which scan allowed applications for threats, such as viruses, malware, spyware, and DDOS attacks. When traffic matches the allow rule defined in the security policy, the security profile(s) that are attached to the rule are applied for further content inspection rules such as antivirus checks and data filtering.

> Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy.

The firewall provides default security profiles that you can use out of the box to begin protecting your network from threats. See Set Up Basic Security Policies for information on using the default profiles in your security policy. As you get a better understanding about the security needs on your network, you can create custom profiles. See Scan Traffic for Threats for more information.

You can add security profiles that are commonly applied together to a security profile group; this set of profiles can be treated as a unit and added to security policies in one step (or included in security policies by default, if you choose to set up a default security profile group).

The following topics provide more detailed information about each type of security profile and how to set up a security profile group:

- Antivirus Profiles
- Anti-Spyware Profiles
- Vulnerability Protection Profiles
- URL Filtering Profiles
- Data Filtering Profiles
- File Blocking Profiles
- WildFire Analysis Profiles
- DoS Protection Profiles
- Zone Protection Profiles
- Security Profile Group

Antivirus Profiles

Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads. Using a stream-based malware prevention engine, which inspects traffic the moment the first packet is received, the Palo Alto Networks antivirus solution can 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 viruses, including support for scanning inside compressed files and data encoding schemes. If you have enabled Decryption on the firewall, the profile also enables scanning of decrypted content.

The default profile inspects all of the listed protocol decoders for viruses, and generates alerts for SMTP, IMAP, and POP3 protocols while blocking for 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:

- **Default**—For each threat signature and Antivirus 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.

Customized profiles can be used to minimize antivirus inspection for traffic between trusted security zones, and to maximize the inspection of traffic received from untrusted zones, such as the Internet, as well as 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 threats are discovered by WildFire, signatures are quickly created and then integrated into the standard antivirus signatures that can be downloaded by Threat Prevention subscribers on a daily basis (sub-hourly for WildFire subscribers).

Anti-Spyware Profiles

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:

- **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.

Vulnerability Protection Profiles

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.

To configure how the firewall responds to a threat, see Anti-Spyware Profiles for a list of supported actions.

URL Filtering Profiles

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.

Data Filtering Profiles

Data filtering profiles prevent sensitive information such as credit card or social security numbers from leaving a protected network. The data filtering profile also allows you to filter on key words, such as a sensitive project name or the word confidential. It is important to focus your profile on the desired file types to reduce false positives. For example, you may only want to search Word documents or Excel spreadsheets. You may also only want to scan web-browsing traffic, or FTP.

You can use default profiles, or create custom data patterns. There are two default profiles:

- CC# (Credit Card)—Identifies credit card numbers using a hash algorithm. The content must match the hash algorithm in order for data to be detected as a credit card number. This method will reduce false positives.
- SSN# (Social Security Number)—Uses an algorithm to detect nine digit numbers, regardless of format. There are two fields: SSN# and SSN# (no dash).

Weight and Threshold Values

It is important to understand how the weight of an object (SSN, CC#, pattern) is calculated in order to set the appropriate threshold for a condition you are trying to filter. Each occurrence multiplied by the weight value will be added together in order to reach an action threshold (alert or block).

Example: Filter for Social Security Numbers Only

For simplicity, if you only want to filter files with Social Security Numbers (SSN) and you define a weight of 3 for SSN#, you would use the following formula: each instance of a SSN x weight = threshold increment. In this case, if a Word document has 10 social security numbers you multiply that by the weight of 3, so 10 x 3 = 30. In order to take action for a file that contains 10 social security numbers you would set the threshold to 30. You may want to set an alert at 30 and then block at 60. You may also want to set a weight in the field SSN# (no dash) for Social Security Numbers that do not contain dashes. If multiple settings are used, they will accumulate to reach a given threshold.

Example: Filter for Social Security Numbers and a Custom Pattern

In this example, we will filter on files that contain Social Security Numbers and the custom pattern confidential. In other words, if a file has Social Security Numbers in addition to the word confidential and the combined instances of those items hit the threshold, the file will trigger an alert or block, depending on the action setting.

SSN# weight = 3

Custom Pattern confidential weight = 20

The custom pattern is case sensitive.

If the file contains 20 Social Security Numbers and a weight of 3 is configured, that is 20 x 3 = 60. If the file also contains one instance of the term confidential and a weight of 20 is configured, that is 1 x 20 = 20 for a total of 80. If your threshold for block is set to 80, this scenario would block the file. The alert or block action will be triggered as soon as the threshold is hit.

File Blocking Profiles

The firewall uses file blocking profiles to block specified file types over specified applications and in the specified session flow direction (inbound/outbound/both). You can set the profile to alert or block on upload and/or download and you can specify which applications will be subject to the file blocking profile. You can also configure custom block pages that will appear when a user attempts to download the specified file type. This allows the user to take a moment to consider whether or not they want to download a file.

Configure a file blocking profile with the following actions:

- **Alert**—When the specified file type is detected, a log is generated in the data filtering log.
- **Block**—When the specified file type is detected, the file is blocked and a customizable block page is presented to the user. A log is also generated in the data filtering log.
- **Continue**—When the specified file type is detected, a customizable response page is presented to the user. The user can click through the page to download the file. A log is also generated in the data filtering log. Because this type of forwarding action requires user interaction, it is only applicable for web traffic.

WildFire Analysis Profiles

Use a WildFire analysis profile to enable the firewall to forward unknown files or email links for WildFire analysis. Specify files to be forwarded for analysis based on application, file type, and transmission direction (upload or download). Files or email links matched to the profile rule are forwarded either the WildFire public cloud or the WildFire private cloud (hosted with a WF-500 appliance), depending on the analysis location defined for the rule.

You can also use the WildFire analysis profiles to set up a Wildfire hybrid cloud deployment. If you are using a WildFire appliance to analyze sensitive files locally (such as PDFs), you can specify for less sensitive files types (such as PE files) or file types that are not supported for WildFire appliance analysis (such as APKs) to be analyzed by the WildFire public cloud. Using both the WildFire appliance and the WildFire cloud for analysis allows you to benefit from a prompt verdict for files that have already been processed by the cloud, and for files that are not supported for appliance analysis, and frees up the appliance capacity to process sensitive content.

DoS Protection Profiles

DoS Protection profiles provide detailed control for Denial of Service (DoS) Protection policies. Palo Alto Networks firewalls support two DoS protection mechanisms:

- **Flood Protection**—Detects and prevents attacks where the network is flooded with packets, resulting in too many half-open sessions and/or services being unable to respond to each request. In this case the source address of the attack is usually spoofed. The flood protection defines threshold rates for incoming SYN, UDP, ICMP, and ICMPv6 packets, and other types of IP packets, which trigger an alarm, activate an action, and trigger a maximum threshold based on aggregate sessions or source and/or destination IP addresses. See DoS Protection Against Flooding of New Sessions.
- **Resources Protection**—Detects and prevents session exhaustion attacks. In this type of attack, a large number of hosts (bots) are used to establish as many fully established sessions as possible to consume all of a system's resources. The resources protection defines the maximum number of concurrent connections.

You can enable both types of protection mechanisms in a single DoS Protection profile. After you configure the DoS Protection profile, you attach it to a DoS policy.

When configuring DoS protection, it is important to analyze your environment in order to set the correct thresholds and due to some of the complexities of defining DoS protection policies, this guide will not go into detailed examples. For more information, refer to the Threat Prevention Tech Note.

Zone Protection Profiles

Zone protection profiles provide additional protection between specific network zones in order to protect the zones against attack. The profile must be applied to the entire zone, so it is important to carefully test the profiles in order to prevent issues that may arise with the normal traffic traversing the zones. When defining packets per second (pps) thresholds limits for zone protection profiles, the threshold is based on the packets per second that do not match a previously established session. For more information, refer to the Threat Prevention Tech Note.

Security Profile Group

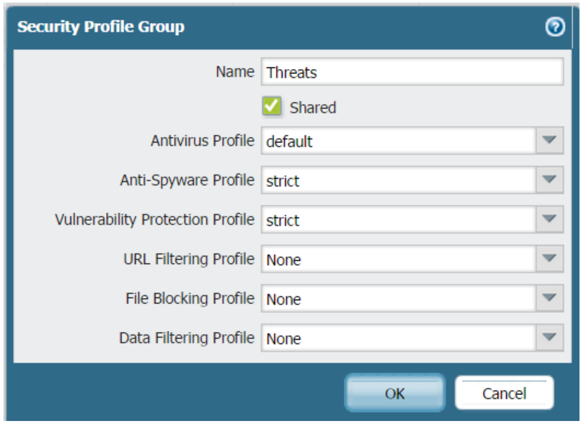
A security profile group is a set of security profiles that can be treated as a unit and then easily added to security policies. Profiles that are often assigned together can be added to profile groups to simplify the creation of security policies. You can also setup a default security profile group—new security policies will use the settings defined in the default profile group to check and control traffic that matches the security policy. Name a security profile group *default* to allow the profiles in that group to be added to new security policies by default. This allows you to consistently include your organization's preferred profile settings in new policies automatically, without having to manually add security profiles each time you create new rules.

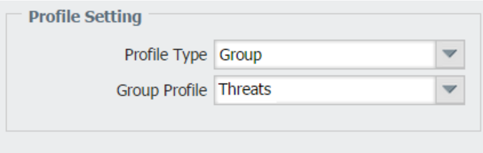
The following sections show how to create a security profile group and how to enable a profile group to be used by default in new security policies:

- Create a Security Profile Group
- Set Up or Override a Default Security Profile Group

Create a Security Profile Group

Use the following steps to create a security profile group and add it to a security policy.

Create a Security Profile Group		
Step 1	Create a security profile group.	1. Select **Objects > Security Profile Groups** and **Add** a new security profile group. 2. Give the profile group a descriptive **Name**, for example, Threats. 3. If the firewall is in Multiple Virtual System Mode, enable the profile to be **Shared** by all virtual systems. 4. Add existing profiles to the group.  Security Profile Group Name: Threats ☑ Shared Antivirus Profile: default Anti-Spyware Profile: strict Vulnerability Protection Profile: strict URL Filtering Profile: None File Blocking Profile: None Data Filtering Profile: None 5. Click **OK** to save the profile group.

Create a Security Profile Group		
Step 2	Add a security profile group to a security policy.	1. Select **Policies > Security** and **Add** or modify a security policy rule. 2. Select the **Actions** tab. 3. In the Profile Setting section, select **Group** for the **Profile Type**. 4. In the **Group Profile** drop-down, select the group you created (for example, select the Threats group):  Profile Setting Profile Type: Group Group Profile: Threats 5. Click **OK** to save the policy and **Commit** your changes.
Step 3	Save your changes.	Click **Commit**.

Set Up or Override a Default Security Profile Group

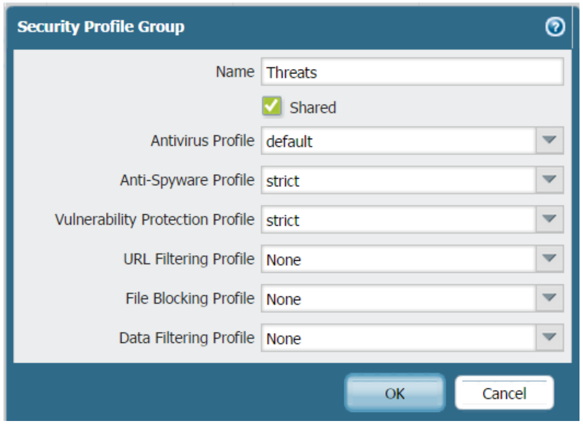
Use the following options to set up a default security profile group to be used in new security policies, or to override an existing default group. When an administrator creates a new security policy, the default profile group will be automatically selected as the policy’s profile settings, and traffic matching the policy will be checked according to the settings defined in the profile group (the administrator can choose to manually select different profile settings if desired). Use the following options to set up a default security profile group or to override your default settings.

> If no default security profile exists, the profile settings for a new security policy are set to **None** by default.

Set Up or Override a Default Security Profile Group

- Create a security profile group.

1. Select **Objects > Security Profile Groups** and Add a new security profile group.
2. Give the profile group a descriptive **Name**, for example, Threats.
3. If the firewall is in Multiple Virtual System Mode, enable the profile to be **Shared** by all virtual systems.
4. Add existing profiles to the group. For details on creating profiles, see Security Profiles.



Security Profile Group

Name: Threats

☑ Shared

Antivirus Profile: default

Anti-Spyware Profile: strict

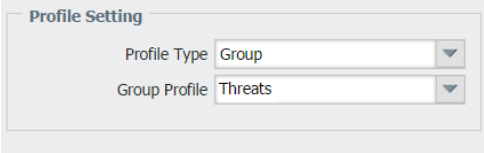
Vulnerability Protection Profile: strict

URL Filtering Profile: None

File Blocking Profile: None

Data Filtering Profile: None

5. Click **OK** to save the profile group.
6. **Add the security profile group to a security policy.**
7. **Add** or modify a security policy rule and select the **Actions** tab.
8. Select **Group** for the **Profile Type**.
9. In the **Group Profile** drop-down, select the group you created (for example, select the Threats group):

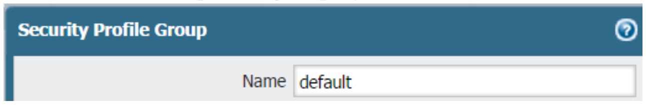
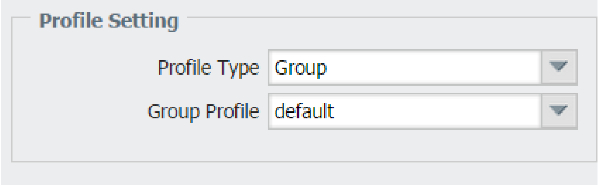


Profile Setting

Profile Type: Group

Group Profile: Threats

10. Click **OK** to save the policy and **Commit** your changes.

Set Up or Override a Default Security Profile Group	
• Set up a default security profile group.	1. Select **Objects > Security Profile Groups** and add a new security profile group or modify an existing security profile group. 2. **Name** the security profile group *default*:  Security Profile Group Name: default 3. Click **OK** and **Commit**. 4. Confirm that the *default* security profile group is included in new security policies by default: a. Select **Policies > Security** and **Add** a new security policy. b. Select the **Actions** tab and view the **Profile Setting** fields:  Profile Setting Profile Type: Group Group Profile: default By default, the new security policy correctly shows the **Profile Type** set to Group and the *default* **Group Profile** is selected.
• Override a default security profile group.	If you have an existing default security profile group, and you do not want that set of profiles to be attached to a new security policy, you can continue to modify the Profile Setting fields according to your preference. Begin by selecting a different Profile Type for your policy (**Policies > Security > Security Policy Rule > Actions**).

Enumeration of Rules Within a Rulebase

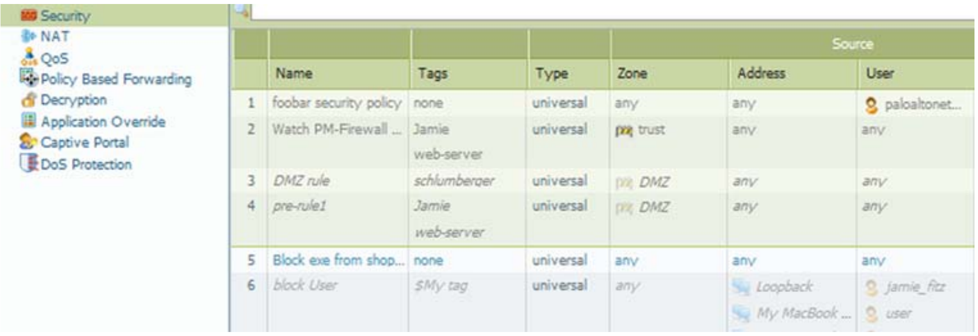
Each rule within a rulebase is automatically numbered and the ordering adjusts as rules are moved or reordered. When filtering rules to find rules that match the specified filter(s), each rule is listed with its number in the context of the complete set of rules in the rulebase and its place in the evaluation order.

On Panorama, pre-rules, post-rules, and default rules are independently numbered. When Panorama pushes rules to a firewall, the rule numbering reflects the hierarchy and evaluation order of shared rules, device-group pre-rules, firewall rules, device-group post-rules, and default rules. The **Preview Rules** option in Panorama displays an ordered list view of the total number of rules on a firewall.

View the Ordered List of Rules Within a Rulebase

- View the numbered list of rules on the firewall.

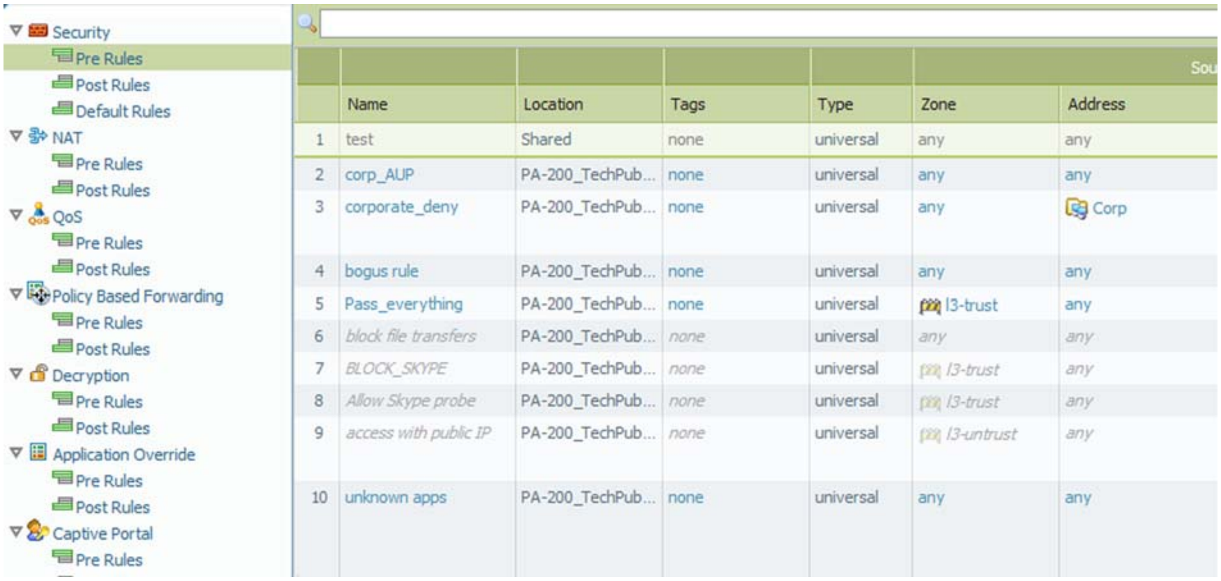
  Select **Policies** and any rulebase under it. For example, **Policies > QoS**. The left-most column in the table displays the rule number.



				Source		
	Name	Tags	Type	Zone	Address	User
1	foobar security policy	none	universal	any	any	paloaltonet...
2	Watch PM-Firewall ...	Jamie web-server	universal	trust	any	any
3	*DMZ rule*	*schlumberger*	universal	*DMZ*	*any*	*any*
4	*pre-rule1*	*Jamie* *web-server*	universal	*DMZ*	*any*	*any*
5	Block exe from shop...	none	universal	any	any	any
6	*block User*	*$My tag*	universal	*any*	*Loopback* *My MacBook ...*	*jamie_fitz* *user*

- View the numbered list of rules on Panorama.

  Select **Policies** and any rulebase under it. For example, **Policies > Security> Pre-rules**.

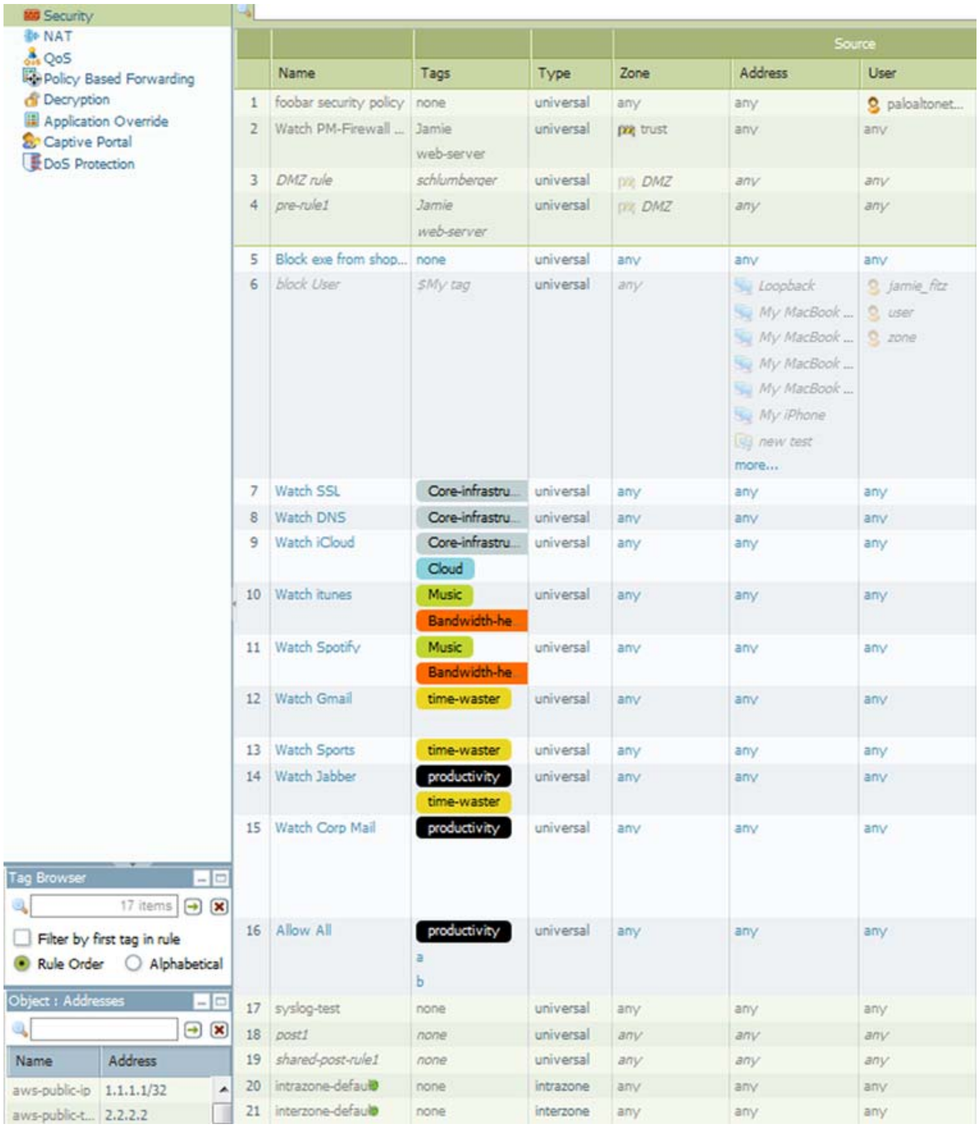


						Sou
	Name	Location	Tags	Type	Zone	Address
1	test	Shared	none	universal	any	any
2	corp_AUP	PA-200_TechPub...	none	universal	any	any
3	corporate_deny	PA-200_TechPub...	none	universal	any	Corp
4	bogus rule	PA-200_TechPub...	none	universal	any	any
5	Pass_everything	PA-200_TechPub...	none	universal	l3-trust	any
6	*block file transfers*	PA-200_TechPub...	*none*	universal	*any*	*any*
7	*BLOCK_SKYPE*	PA-200_TechPub...	*none*	universal	*l3-trust*	*any*
8	*Allow Skype probe*	PA-200_TechPub...	*none*	universal	*l3-trust*	*any*
9	*access with public IP*	PA-200_TechPub...	*none*	universal	*l3-untrust*	*any*
10	unknown apps	PA-200_TechPub...	none	universal	any	any

View the Ordered List of Rules Within a Rulebase (Continued)

- After you push the rules from Panorama, view the complete list of rules with numbers on the firewall.

  From the web interface of the firewall, select **Policies** and pick any rulebase under it. For example, select **Policies > Security** and view the complete set of numbered rules that the firewall will evaluate.



				Source		
	Name	Tags	Type	Zone	Address	User
1	foobar security policy	none	universal	any	any	paloaltonet...
2	Watch PM-Firewall ...	Jamie web-server	universal	trust	any	any
3	*DMZ rule*	*schlumberger*	universal	*DMZ*	*any*	*any*
4	*pre-rule1*	*Jamie* *web-server*	universal	*DMZ*	*any*	*any*
5	Block exe from shop...	none	universal	any	any	any
6	*block User*	*$My tag*	universal	*any*	*Loopback* *My MacBook ...* *My MacBook ...* *My MacBook ...* *My MacBook ...* *My iPhone* *new test* more...	*jamie_fitz* *user* *zone*
7	Watch SSL	Core-infrastru...	universal	any	any	any
8	Watch DNS	Core-infrastru...	universal	any	any	any
9	Watch iCloud	Core-infrastru... Cloud	universal	any	any	any
10	Watch itunes	Music Bandwidth-he...	universal	any	any	any
11	Watch Spotify	Music Bandwidth-he...	universal	any	any	any
12	Watch Gmail	time-waster	universal	any	any	any
13	Watch Sports	time-waster	universal	any	any	any
14	Watch Jabber	productivity time-waster	universal	any	any	any
15	Watch Corp Mail	productivity	universal	any	any	any
16	Allow All	productivity a b	universal	any	any	any
17	syslog-test	none	universal	any	any	any
18	*post1*	*none*	universal	*any*	*any*	*any*
19	*shared-post-rule1*	*none*	universal	*any*	*any*	*any*
20	intrazone-default	none	intrazone	any	any	any
21	interzone-default	none	interzone	any	any	any

☐ Filter by first tag in rule

● Rule Order ○ Alphabetical

Name	Address
aws-public-ip	1.1.1.1/32
aws-public-t...	2.2.2.2

Move or Clone a Policy Rule or Object to a Different Virtual System

On a firewall that has more than one virtual system (vsys), you can move or clone policy rules and objects to a different vsys or to the Shared location. Moving and cloning save you the effort of deleting, recreating, or renaming rules and objects. If the policy rule or object that you will move or clone from a vsys has references to objects in that vsys, move or clone the referenced objects also. If the references are to shared objects, you do not have to include those when moving or cloning. You can perform a Use Global Find to check for references.

Move or Clone a Policy Rule or Object to a Virtual System	
Step 1	Select the policy type (for example, **Policy > Security**) or object type (for example, **Objects > Addresses**).
Step 2	Select the **Virtual System** and select one or more policy rules or objects.
Step 3	Perform one of the following steps: • Select **Move > Move to other vsys** (for policy rules). • Click **Move** (for objects). • Click **Clone** (for policy rules or objects).
Step 4	In the **Destination** drop-down, select the new virtual system or **Shared**. The default is the **Virtual System** selected in Step 2.
Step 5	(Policy rules only) Select the **Rule order**: • **Move top** (default)—The rule will come before all other rules. • **Move bottom**—The rule will come after all other rules. • **Before rule**—In the adjacent drop-down, select the rule that comes after the Selected Rules. • **After rule**—In the adjacent drop-down, select the rule that comes before the Selected Rules.
Step 6	The **Error out on first detected error in validation** check box is selected by default. The firewall stops performing the checks for the move or clone action when it finds the first error, and displays just this error. For example, if an error occurs when the **Destination** vsys doesn't have an object that the policy rule you are moving references, the firewall will display the error and stop any further validation. When you move or clone multiple items at once, selecting this check box will allow you to find one error at a time and troubleshoot it. If you clear the check box, the firewall collects and displays a list of errors. If there are any errors in validation, the object is not moved or cloned until you fix all the errors.
Step 7	Click **OK** to start the error validation. If the firewall displays errors, fix them and retry the move or clone operation. If the firewall doesn't find errors, the object is moved or cloned successfully. After the operation finishes, click **Commit**.

Use Tags to Group and Visually Distinguish Objects

You can tag objects to group related items and add color to the tag in order to visually distinguish tagged objects. Tags can be added to the following objects: address objects, address 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 device configuration. 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 device configuration.

One or more tags can be applied to objects and to policy rules; a maximum of 64 tags can be applied to an object. Panorama supports a maximum of 10,000 tags that can be apportioned across Panorama (shared and device groups) and the managed devices (including devices with multiple virtual systems).

To use tags effectively, see the following topics:

- ▲ Create and Apply Tags
- ▲ Modify Tags
- ▲ Use the Tag Browser

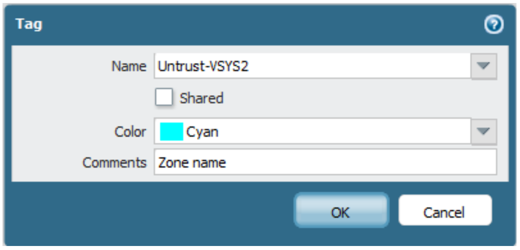
Create and Apply Tags

Create and Apply tags

Step 1 Create tags.

To tag a zone, you must create a tag with the same name as the zone. When the zone is attached in policy rules, the tag color automatically displays as the background color against the zone name.

1. Select **Objects > Tags**.
2. On Panorama or a multiple virtual system firewall, select the **Device Group** or the **Virtual System** to which this object must belong.
3. Click **Add** and enter a **Name** to identify the tag. The maximum length is 127 characters.
4. (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.
5. (Optional) Assign one of the 16 predefined colors to the tag. By default, no color is selected.



Tag

Name: Untrust-VSYS2

□ Shared

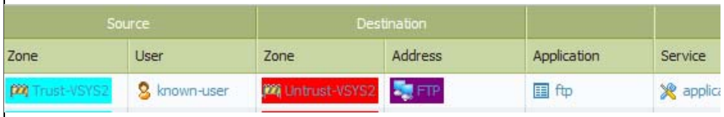
Color: Cyan

Comments: Zone name

6. Click **OK** and **Commit** to save the changes.

Step 2 Apply tags to policy.

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



Source		Destination			
Zone	User	Zone	Address	Application	Service
Trust-VSYS2	known-user	Untrust-VSYS2	FTP	ftp	applica

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

1. Create the object.

   For example to create a service group, select **Objects > Service Groups > Add**.
2. Select the tag(s) from the **Tag** drop-down or enter a phrase to create a new tag.

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

Modify Tags

Modify Tags
• Select **Objects > Tags** to perform any of the following operations with tags: • Click the link in the **Name** column to edit the properties of a tag. • Select a tag in the table, and click **Delete** to remove the tag from the firewall. • Click **Clone** to create a duplicate tag with the same properties. A numerical suffix is added to the tag name. For example, FTP-1.

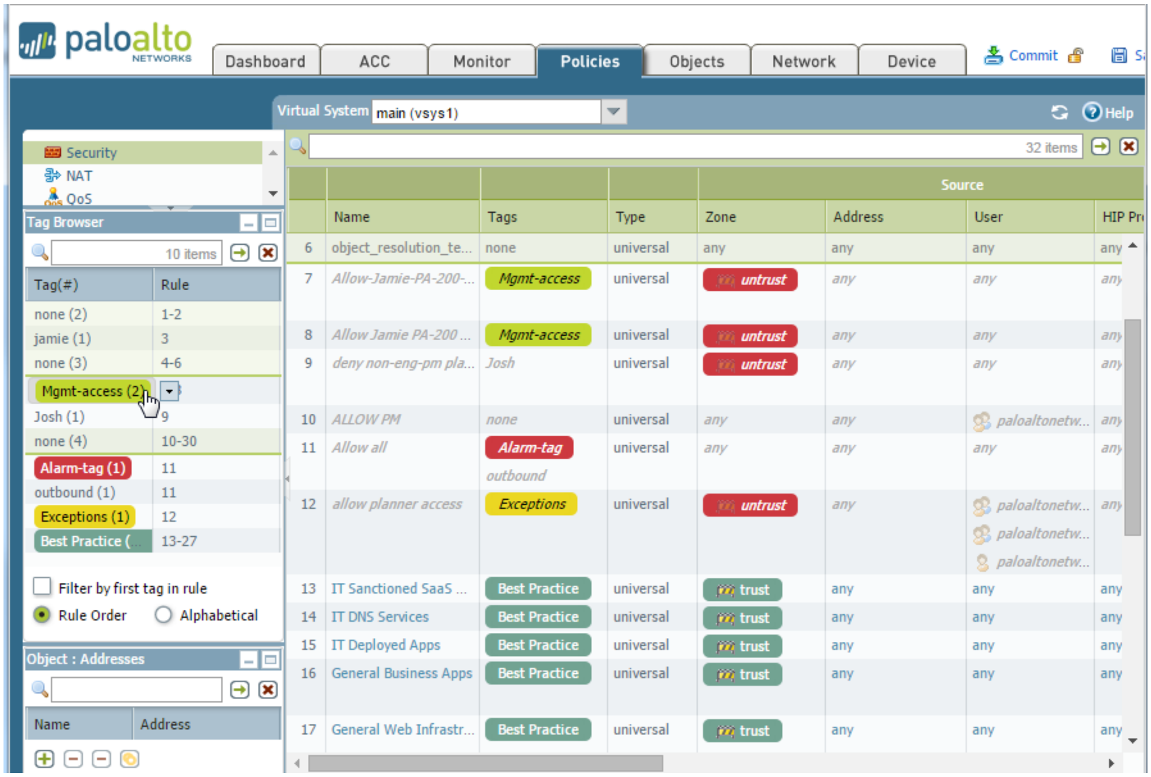
For details on creating tags, see Create and Apply Tags. For information on working with tags, see Use the Tag Browser.

Use the Tag Browser

The tag browser provides a way to view all the tags used within a rulebase. In rulebases with a large number of rules, the tag browser simplifies the display by presenting the tags, the color code, and the rule numbers in which the tags are used.

It also allows you to group rules using the first tag applied to the rule. As a best practice, use the first tag to identify the primary purpose for a rule. For example, the first tag can identify a rule by a high-level function such as best practice, or Internet access or IT sanctioned applications or high-risk applications. In the tag browser, when you **Filter by first tag in rule**, you can easily identify gaps in coverage and move rules or add new rules within the rulebase. All the changes are saved to the candidate configuration until you commit the changes on the firewall and make them a part of the running configuration.

For devices that are managed by Panorama, the tags applied to pre-rules and post-rules that have been pushed from Panorama, display in a green background and are demarcated with green lines so that you can identify these tags from the local tags on the device.



Virtual System main (vsys1)

10 items

Tag(#)	Rule
none (2)	1-2
jamie (1)	3
none (3)	4-6
Mgmt-access (2)	
Josh (1)	9
none (4)	10-30
Alarm-tag (1)	11
outbound (1)	11
Exceptions (1)	12
Best Practice (...	13-27

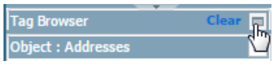
□ Filter by first tag in rule

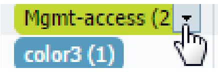
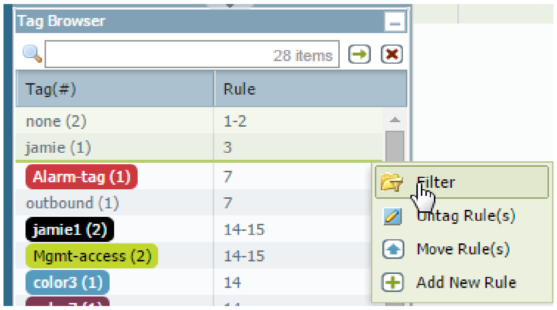
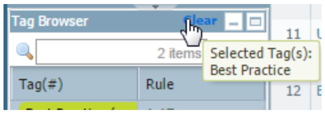
● Rule Order ○ Alphabetical

Name	Address

32 items

				Source			
	Name	Tags	Type	Zone	Address	User	HIP Pr
6	object_resolution_te...	none	universal	any	any	any	any
7	Allow-Jamie-PA-200-...	Mgmt-access	universal	untrust	any	any	any
8	Allow Jamie PA-200 ...	Mgmt-access	universal	untrust	any	any	any
9	deny non-eng-pm pla...	Josh	universal	untrust	any	any	any
10	ALLOW PM	none	universal	any	any	paloaltonetw...	any
11	Allow all	Alarm-tag outbound	universal	any	any	any	any
12	allow planner access	Exceptions	universal	untrust	any	paloaltonetw... paloaltonetw... paloaltonetw...	any
13	IT Sanctioned SaaS ...	Best Practice	universal	trust	any	any	any
14	IT DNS Services	Best Practice	universal	trust	any	any	any
15	IT Deployed Apps	Best Practice	universal	trust	any	any	any
16	General Business Apps	Best Practice	universal	trust	any	any	any
17	General Web Infrastr...	Best Practice	universal	trust	any	any	any

Use the Tag Browser	
• Explore the tag browser.	1. Access the **Tag Browser** on the left pane of the **Policies >** tab. The tag browser displays the tags that have been used in the rules for the selected rulebase, for example **Policies > Security**. 2. **Tag (#)**—Displays the label and the rule number or range of numbers in which the tag is used contiguously. Hover over the label to see the location where the rule was defined, it can be inherited from a shared location, a device group, or a virtual system. 3. **Rule**—Lists the rule number or range of numbers associated with the tags. 4. Sort the tags. • **Filter by first tag in rule**—Sorts rules using the first tag applied to each rule in the rulebase. This view is particularly useful if you want to narrow the list and view related rules that might be spread around the rulebase. For example if the first tag in each rule denotes its function—best practices, administration, web-access, data center access, proxy—you can narrow the result and scan the rules based on function. • **Rule Order**—Sorts the tags in the order of appearance within the selected rulebase. When displayed in order of appearance, tags used in contiguous rules are grouped. The rule number with which the tag is associated is displayed along with the tag name. • **Alphabetical**—Sorts the tags in alphabetical order within the selected rulebase. The display lists the tag name and color (if a color is assigned) and the number of times it is used within the rulebase. The label **None** represents rules without any tags; it does not display rule numbers for untagged rules. When you select **None**, the right pane is filtered to display rules that have no tags assigned to them. 5. **Clear**—Clears the filter on the currently selected tags in the search bar. 6. **Search bar**—To search for a tag, enter the term and click the green arrow icon to apply the filter. It also displays the total number of tags in the rulebase and the number of selected tags. 7. Expand or collapse the tag browser. 

Use the Tag Browser (Continued)	
• Tag a rule.	1. Select a rule on the right pane. 2. Do one of the following: • Select a tag in the tag browser and select **Apply the Tag to the Selection(s)** from the drop-down.  • Drag and drop tag(s) from the tag browser on to the Tags column of the rule. When you drop a tag, a confirmation dialog displays. 3. **Commit** the changes.
• View rules that match the selected tags. You can filter rules based on tags with an AND or an OR operator.	• OR filter: To view rules that have specific tags, select one or more tags in the tag browser; the right pane only displays the rules that include any of the currently selected tags. • AND filter: To view rules that have all the selected tags, hover over the number associated with the tag in the **Rule** column of the tag browser and select **Filter**. Repeat to add more tags.  Tag Browser 28 items Tag(#) Rule none (2) 1-2 jamie (1) 3 Alarm-tag (1) 7 outbound (1) 7 jamie1 (2) 14-15 Mgmt-access (2) 14-15 color3 (1) 14 Click the apply filter icon in the search bar on the right pane. The results are displayed using an AND operator.
• View the currently selected tags.	To view the currently selected tags, hover over the **Clear** label in the tag browser.  Tag Browser Clear 2 items Selected Tag(s): Best Practice Tag(#) Rule
• Untag a rule.	Hover over the rule number associated with a tag in the **Rule** column of the tag browser and select **Untag Rule(s)**. Confirm that you want to remove the selected tag from the rule. **Commit** the changes.
• Reorder rules using tags.	Select one or more tags and hover over the rule number in the Rule column of the tag browser and select **Move Rule(s)**. Select a tag from the drop-down in the move rule window and select whether you want to **Move Before** or **Move After** the tag selected in the drop-down. **Commit** the changes.

Use the Tag Browser (Continued)	
• Add a new rule that applies the selected tags.	Select one or more tags and hover over the rule number in the **Rule** column of the tag browser, and select **Add New Rule**. Define the rule and **Commit** the changes. The numerical order of the new rule varies by whether you selected a rule on the right pane. If you did not select a rule on the right pane, the new rule will be added after the rule to which the selected tag(s) belongs. Otherwise, the new rule is added after the selected rule.
• Search for a tag.	In the tag browser, enter the first few letters of the tag name you want to search for and click the Apply Filter icon. The tags that match your input will display.

Use a Dynamic Block List in Policy

The firewall or Panorama typically enforce policy for a source or destination IP address that is defined as a static object on the firewall. If you need agility in enforcing policy for a list of source/destination IP addresses that emerge ad hoc, you can use dynamic block lists.

A dynamic block list is a text file that contains a list of IP addresses, IP ranges, or IP subnets, and is hosted on a web server. The dynamic block list can be used to deny or allow access to the IP addresses (IPv4 and IPv6) included in the list. For example, you can use it as a whitelist for allowing a set of IP addresses or as a blacklist to disallow access to the specified IP addresses. At a configured interval, the firewall dynamically imports the list and enforces policy for the IP addresses included in the list. When you modify the list, the firewall retrieves the updates; a configuration change or commit is not required on the firewall. If the web server is unreachable, the firewall or Panorama will use the last successfully retrieved list for enforcing policy until the connection is restored with the web server that hosts the list.

- View the IP Address Limit For Your Firewall Model
- Formatting Guidelines for Dynamic Block Lists
- Enforce Policy with a Dynamic Block List
- View the List of IP addresses in the Dynamic Block List
- Retrieve a Dynamic Block List from Web Server

View the IP Address Limit For Your Firewall Model

Irrespective of the firewall model, each firewall supports a maximum of 10 Dynamic Block Lists.

To find the maximum number of addresses, address groups, and IP addresses per group, for your model of the firewall, use the following CLI command:

```
show system state | match cfg.general.max-address
```

For example:

```
admin@PA-7050> show system state | match cfg.general.max-address
cfg.general.max-address: 80000
cfg.general.max-address-group: 8000
cfg.general.max-address-per-group: 500
```

Each list can contain the maximum number of addresses supported by your firewall model minus 300. Up to 300 IP addresses are reserved for internal use on the firewall and are deducted from the available limit. Therefore, in the example above, the firewall can have a maximum of 79,700 IP addresses.

Formatting Guidelines for Dynamic Block Lists

The dynamic block list can include individual IP addresses, subnet addresses (address/mask), or range of IP addresses. In addition, the block list can include comments and special characters such as `*` , `:` , `;` , `#`, or `/`. The syntax for each line in the list is `[IP address, IP/Mask, or IP start range-IP end range] [space] [comment]`.

Because the firewall ignores incorrectly formatted lines, use these guidelines when defining the list:

- Enter each IP address/range/subnet in a new line; URLs are not supported in this list.
- If you add comments, the comment must be on the same line as the IP address/range/subnet. The space at the end of the IP address is the delimiter that separates a comment from the IP address.

An example:

```
192.168.20.10/32
2001:db8:123:1::1 #test IPv6 address
192.168.20.0/24 ; test internal subnet
2001:db8:123:1::/64 test internal IPv6 range
192.168.20.40-192.168.20.50
```

For an IP address that is blocked, you can display a notification page only if the protocol is HTTP.

Enforce Policy with a Dynamic Block List

Enforce Policy with a Dynamic Block List		
Step 1	Create the dynamic block list and host it on a web server, so that the firewall can retrieve the list for policy evaluation.	1. Create a text file and enter the IP addresses for which you want to enforce policy. For syntax, see Formatting Guidelines for Dynamic Block Lists.
Step 2	Create a dynamic block list object on the firewall.	1. Select **Objects > Dynamic Block Lists**. 2. Click **Add** and enter a descriptive **Name** for the list. 3. (Optional) Select **Shared**, to share the list with all virtual systems on a device that is enabled for multiple virtual systems. By default, the object is created on the virtual system that is currently selected in the **Virtual Systems** drop-down. 4. Enter the **Source** URL (hostname or IP address and the path) for the list you just created on the web server. For example, https://1.2.3.4/DBL_2014 5. Click **Test Source URL** to verify that the firewall or Panorama can connect to the web server. 6. (Optional) Specify the **Repeat** frequency at which the firewall or Panorama must retrieve the list. By default the list is retrieved ever hour. 7. Click **OK** to save the changes.

Enforce Policy with a Dynamic Block List		
Step 3	Use the dynamic block list as a source or destination address object in policy. Create separate dynamic block lists if you want to specify allow and deny actions for specific IP addresses. The list can be referenced in any policy type. In this example, we attach it as a destination object in security policy.	1. Select **Policies > Security**. 2. Click **Add** and give the rule a descriptive name in the **General** tab. 3. In the **Source** tab, select the **Source Zone**. 4. In the **Destination** tab, select the **Destination Zone** and select the dynamic block list as the Destination Address. 5. In the **Service/ URL Category** tab, make sure the **Service** is set to **application-default**. 6. In the **Actions** tab, set the **Action Setting** to Allow or Deny. 7. Leave all the other options at the default values. 8. Click **OK** to save the changes. 9. **Commit** the changes.
Step 4	Test that the policy action is enforced.	1. Access a IP address that is included in the dynamic block list and verify that action you defined is enforced. 2. Select **Monitor > Logs > Traffic** and see the log entry for the session. 3. To verify the policy rule that matches a flow, use the following CLI command: `test security-policy-match source <IP_address> destination <IP_address> destination port <port_number> protocol <protocol_number>`

View the List of IP addresses in the Dynamic Block List

View the IP Addresses Included in the Dynamic Block List

To view the list of IP addresses that the firewall has retrieved from the web server enter the following CLI command:

```
request system external-list show name <name>
```

For example, for a list named case DBL_2014, the output is:

```
vsys1/DBL_2014:
  Next update at: Wed Aug 27 16:00:00 2014
  IPs:
  1.1.1.1
  1.2.2.2/20 #test China
  192.168.255.0; test internal
  192.168.254.0/24 test internal range
```

Retrieve a Dynamic Block List from Web Server

The firewall or Panorama can be configured to retrieve the list from the web server on an hourly, daily, weekly, or monthly basis. If you have added or deleted IP addresses on the list and need to trigger an immediate refresh, you must use the Command Line Interface.

Retrieve a Dynamic Block List
1. Enter the command: **`request system external-list refresh name <name>`** For example, `request system external-list refresh name DBL_2014`
2. Get the job ID for the refresh job using the CLI command: **`show jobs all`** Look for the last EBL Refresh job in the list.
3. View the details for the job ID. Use the command **`show jobs id <number>`** A message indicating the success or failure displays. For example:

```
admin@PA-200> show jobs id 55
Enqueued                     ID              Type    Status Result Completed
--------------------------------------------------------------------------
2014/08/26 15:34:14          55       EBLRefresh       FIN     OK 15:34:40
Warnings:
Details:
```

Register IP Addresses and Tags Dynamically

To mitigate the challenges of scale, lack of flexibility and performance, the architecture in networks today allows for clients, servers, and applications to be provisioned, changed, and deleted on demand. This agility poses a challenge for security administrators because they have limited visibility into the IP addresses of the dynamically provisioned clients and servers, and the plethora of applications that can be enabled on these virtual resources.

The firewall (hardware-based platforms and the VM-Series) supports the ability to register IP addresses and tags dynamically. The IP addresses and tags can be registered on the firewall directly or registered on the firewall through Panorama.This dynamic registration process can be enabled using any of the following options:

- **User-ID agent for Windows**—In an environment where you've deployed the User-ID agent, you can enable the User-ID agent to monitor up to 100 VMware ESXi and/or vCenter Servers. As you provision or modify virtual machines on these VMware servers, the agent can retrieve the IP address changes and share them with the firewall.
- **VM Information Sources**—Allows you to monitor VMware ESXi and vCenter Server, and the AWS-VPC to retrieve IP address changes when you provision or modify virtual machines on these sources. VM Information Sources polls for a predefined set of attributes and does not require external scripts to register the IP addresses through the XML API. See Monitor Changes in the Virtual Environment.
- **VMware Service Manager** (only available for the integrated NSX solution)—The integrated NSX solution is designed for automated provisioning and distribution of Palo Alto Networks next-generation security services and the delivery of dynamic context-based security policies using Panorama. The NSX Manager updates Panorama with the latest information on the IP addresses and tags associated with the virtual machines deployed in this integrated solution. For information on this solution, see Set Up a VM-Series NSX Edition Firewall.
- **XML API**—The firewall and Panorama support an XML API that uses standard HTTP requests to send and receive data. You can use this API to register IP addresses and tags with the firewall or Panorama. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports REST-based services. Refer to the PAN-OS XML API Usage Guide for details.

For information on creating and using Dynamic Address Groups, see Use Dynamic Address Groups in Policy.

For the CLI commands for registering tags dynamically, see CLI Commands for Dynamic IP Addresses and Tags.

Monitor Changes in the Virtual Environment

To secure applications and prevent threats in an environment where new users and servers are constantly emerging, your security policy must be nimble. To be nimble, the firewall must be able to learn about new or modified IP addresses and consistently apply policy without requiring configuration changes on the firewall.

This capability is provided by the coordination between the **VM Information Sources** and **Dynamic Address Groups** features on the firewall. The firewall and Panorama provide an automated way to gather information on the virtual machine (or guest) inventory on each monitored source and create policy objects that stay in sync with the dynamic changes on the network.

- ▲ Enable VM Monitoring to Track Changes on the Virtual Network
- ▲ Attributes Monitored in the AWS and VMware Environments
- ▲ Use Dynamic Address Groups in Policy

Enable VM Monitoring to Track Changes on the Virtual Network

VM information sources provides an automated way to gather information on the Virtual Machine (VM) inventory on each monitored source (host); the firewall can monitor the VMware ESXi and vCenter Server, and the AWS-VPC. As virtual machines (guests) are deployed or moved, the firewall collects a predefined set of attributes (or metadata elements) as tags; these tags can then be used to define Dynamic Address Groups (see Use Dynamic Address Groups in Policy) and matched against in policy.

Up to 10 VM information sources can be configured on the firewall or pushed using Panorama templates. By default, the traffic between the firewall and the monitored sources uses the management (MGT) port on the firewall.

VM Information Sources offers easy configuration and enables you to monitor a predefined set of 16 metadata elements or attributes. See Attributes Monitored in the AWS and VMware Environmentsfor the list.

Set up the VM Monitoring Agent

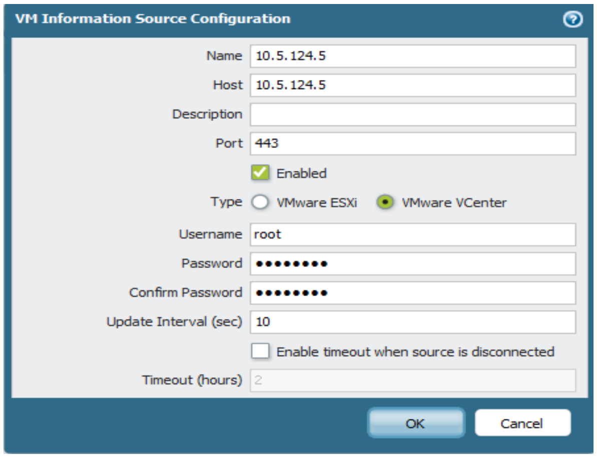
Step 1 Enable the VM Monitoring Agent.

Up to 10 sources can be configured for each firewall, or for each virtual system on a multiple virtual systems capable firewall.

If your firewalls are configured in a high availability configuration:

- An active/passive setup, only the active firewall monitors the VM sources.
- An active/active setup, only the firewall with the priority value of primary monitors the VM sources.

1. Select **Device > VM Information Sources**.
2. Click **Add** and enter the following information:
   - A **Name** to identify the VMware ESX(i) or vCenter Server that you want to monitor.
   - Enter the **Host information for the server—**hostname or IP address and the **Port** on which it is listening.
   - Select the **Type** to indicate whether the source is a **VMware ESX(i)** server or a **VMware vCenter** Server.
   - Add the credentials (**Username** and **Password**) to authenticate to the server specified above.
   - Use the credentials of an administrative user to enable access.
   - (Optional) Modify the **Update interval** to a value between 5-600 seconds. By default, the firewall polls every 5 seconds. The API calls are queued and retrieved within every 60 seconds, so updates may take up to 60 seconds plus the configured polling interval.



VM Information Source Configuration

Name 10.5.124.5

Host 10.5.124.5

Description

Port 443

☑ Enabled

Type ○ VMware ESXi ● VMware VCenter

Username root

Password ••••••••

Confirm Password ••••••••

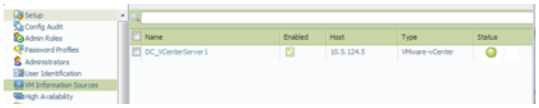
Update Interval (sec) 10

□ Enable timeout when source is disconnected

Timeout (hours) 2

   - (Optional) Enter the interval in hours when the connection to the monitored source is closed, if the host does not respond. (default: 2 hours, range 2-10 hours)
     To change the default value, select the check box to **Enable timeout when the source is disconnected** and specify the value. When the specified limit is reached or if the host cannot be accessed or does not respond, the firewall will close the connection to the source.
   - Click **OK**, and **Commit** the changes.
   - Verify that the connection **Status** displays as connected ●.

<table>
<tr><th colspan="2">Set up the VM Monitoring Agent (Continued)</th></tr>
<tr>
<td>Step 2 Verify the connection status.</td>
<td>
Verify that the connection <b>Status</b> displays as ● connected.



<table>
<tr><th>□</th><th>Name</th><th>Enabled</th><th>Host</th><th>Type</th><th>Status</th></tr>
<tr><td>□</td><td>DC_VCenterServer1</td><td>☑</td><td>10.5.124.5</td><td>VMware-vCenter</td><td>●</td></tr>
</table>

If the connection status is pending or disconnected, verify that the source is operational and that the firewall is able to access the source. If you use a port other than the MGT port for communicating with the monitored source, you must change the service route (<b>Device > Setup > Services</b>, click the <b>Service Route Configuration</b> link and modify the <b>Source Interface</b> for the <b>VM Monitor</b> service).
</td>
</tr>
</table>

Attributes Monitored in the AWS and VMware Environments

Each VM on a monitored ESXi or vCenter server must have VMware Tools installed and running. VMware Tools provide the capability to glean the IP address(es) and other values assigned to each VM.

In order to collect the values assigned to the monitored VMs, the firewall monitors the following predefined set of attributes:

Attributes Monitored on a VMware Source	Attributes Monitored on the AWS-VPC
• UUID	• Architecture
• Name	• Guest OS
• Guest OS	• Image ID
• VM State — the power state can be poweredOff, poweredOn, standBy, and unknown.	• Instance ID
• Annotation	• Instance State
• Version	• Instance Type
• Network — Virtual Switch Name, Port Group Name, and VLAN ID	• Key Name
• Container Name —vCenter Name, Data Center Object Name, Resource Pool Name, Cluster Name, Host, Host IP address.	• Placement—Tenancy, Group Name, Availability Zone
	• Private DNS Name
	• Public DNS Name
	• Subnet ID
	• Tag (key, value) (up to5 tags supported per instance
	• VPC ID

Use Dynamic Address Groups in Policy

Dynamic address groups are used in policy. They allow you to create policy that automatically adapts to changes—adds, moves, or deletions of servers. It also enables the flexibility to apply different rules to the same server based on *tags* that define its role on the network, the operating system, or the different kinds of traffic it processes.

A dynamic address group uses tags as a filtering criteria to determine its members. The filter uses logical *and* and *or* operators. All IP addresses or address groups that match the filtering criteria become members of the dynamic address group. Tags can be defined statically on the firewall and/or registered (dynamically) to the firewall. The difference between static and dynamic tags is that static tags are part of the configuration on the firewall, and dynamic tags are part of the runtime configuration. This implies that a commit is not required to update dynamic tags; the tags must however be used by Dynamic Address Groups that are referenced in policy, and the policy must be committed on the device.

To dynamically register tags, you can use the XML API or the VM Monitoring agent on the firewall or on the User-ID agent. Each tag is a metadata element or attribute-value pair that is registered on the firewall or Panorama. For example, IP1 {tag1, tag2,.....tag32}, where the IP address and the associated tags are maintained as a list; each registered IP address can have up to 32 tags such as the operating system, the datacenter or the virtual switch to which it belongs. Within 60 seconds of the API call, the firewall registers the IP address and associated tags, and automatically updates the membership information for the dynamic address group(s).

The maximum number of IP addresses that can be registered for each platform is different. Use the following table for specifics on your platform:

Platform	Maximum number of dynamically registered IP addresses
PA-7000 Series, PA-5060, VM-1000-HV	100,000
PA-5050	50,000
PA-5020	25,000
PA-4000 Series, PA-3000 Series	5,000
PA-2000 Series, PA-500, PA-200, VM-300, VM-200, VM-100	1,000

The following example shows how dynamic address groups can simplify network security enforcement. The example workflow shows how to:

- Enable the VM Monitoring agent on the firewall, to monitor the VMware ESX(i) host or vCenter Server and register VM IP addresses and the associated tags.
- Create dynamic address groups and define the tags to filter. In this example, two address groups are created. One that only filters for dynamic tags and another that filters for both static and dynamic tags to populate the members of the group.
- Validate that the members of the dynamic address group are populated on the firewall.
- Use dynamic address groups in policy. This example uses two different security policies:
  - A security policy for all Linux servers that are deployed as FTP servers; this rule matches on dynamically registered tags.

  - A security policy for all Linux servers that are deployed as web servers; this rule matches on a dynamic address group that uses static and dynamic tags.

- Validate that the members of the dynamic address groups are updated as new FTP or web servers are deployed. This ensure that the security rules are enforced on these new virtual machines too.

Use Dynamic Address Groups in Policy

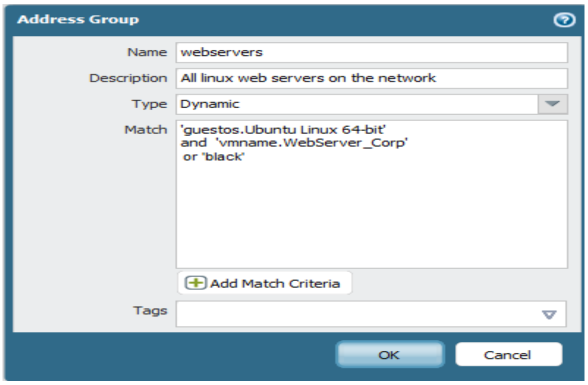
Step 1 Enable VM Source Monitoring.

See Enable VM Monitoring to Track Changes on the Virtual Network.

Step 2 Create dynamic address groups on the firewall.

View the tutorial to see a big picture view of the feature.

1. Log in to the web interface of the firewall.
2. Select **Object > Address Groups**.
3. Click **Add** and enter a **Name** and a **Description** for the address group.
4. Select **Type** as **Dynamic**.
5. Define the match criteria. You can select dynamic and static tags as the match criteria to populate the members of the group. Click **Add Match Criteria**, and select the **And** or **Or** operator and select the attributes that you would like to filter for or match against. and then click **OK**.



Address Group

Name webservers

Description All linux web servers on the network

Type Dynamic

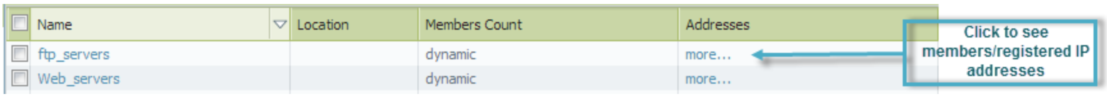
Match 'guestos.Ubuntu Linux 64-bit'
and 'vmname.WebServer_Corp'
or 'black'

6. Click **Commit**.

The match criteria for each dynamic address group in this example is as follows:

ftp_server: matches on the guest operating system “Linux 64-bit” and annotated as “ftp” ('guestos.Ubuntu Linux 64-bit' and 'annotation.ftp').

web-servers: matches on two criteria—the tag black or if the guest operating system is Linux 64-bit and the name of the server us Web_server_Corp. ('guestos.Ubuntu Linux 64-bit' and 'vmname.WebServer_Corp' or 'black')



□	Name	Location	Members Count	Addresses
□	ftp_servers		dynamic	more...
□	Web_servers		dynamic	more...

Click to see members/registered IP addresses

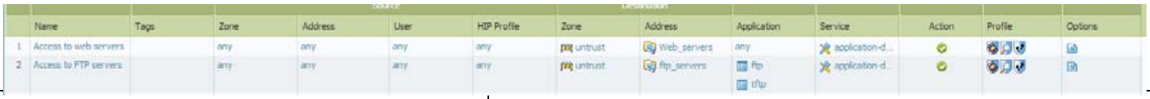
Use Dynamic Address Groups in Policy (Continued)

Step 3 Use dynamic address groups in policy.

View the tutorial.

1. Select **Policies > Security**.
2. Click **Add** and enter a **Name** and a **Description** for the policy.
3. Add the **Source Zone** to specify the zone from which the traffic originates.
4. Add the **Destination Zone** at which the traffic is terminating.
5. For the **Destination Address**, select the Dynamic address group you created in Step 2 above.
6. Specify the action— **Allow** or **Deny**—for the traffic, and optionally attach the default security profiles to the rule.
7. Repeats Steps 1 through 6 above to create another policy rule.
8. Click **Commit**.

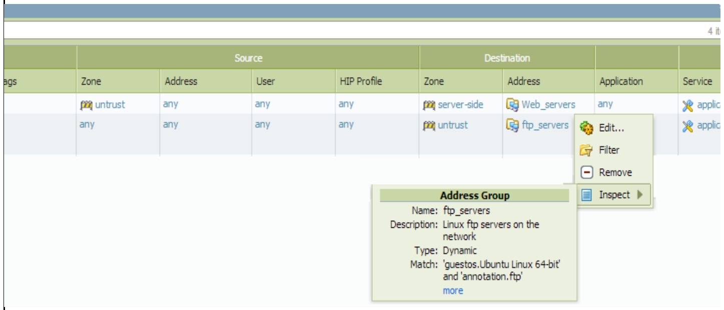
This example shows how to create two policies: one for all access to FTP servers and the other for access to web servers.



			Source				Destination						
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
1	Access to web servers		any	any	any	any	untrust	Web_servers	any	application-d...	✓		
2	Access to FTP servers		any	any	any	any	untrust	ftp_servers	ftp tftp	application-d...	✓		

Step 4 Validate that the members of the dynamic address group are populated on the firewall.

1. Select **Policies > Security**, and select the rule.
2. Select the drop-down arrow next to the address group link, and select **Inspect**. You can also verify that the match criteria is accurate.

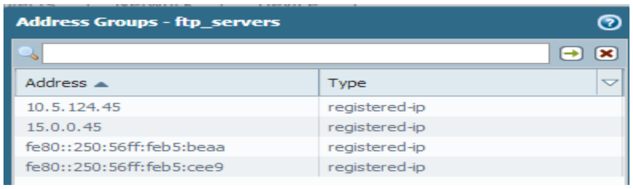


	Source				Destination			
ags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service
	untrust	any	any	any	server-side	Web_servers	any	applic
	any	any	any	any	untrust	ftp_servers		applic

Address Group

Name: ftp_servers
Description: Linux ftp servers on the network
Type: Dynamic
Match: 'guestos.Ubuntu Linux 64-bit' and 'annotation.ftp'
more

3. Click the **more** link and verify that the list of registered IP addresses is displayed.



Address Groups - ftp_servers

Address	Type
10.5.124.45	registered-ip
15.0.0.45	registered-ip
fe80::250:56ff:feb5:beaa	registered-ip
fe80::250:56ff:feb5:cee9	registered-ip

Policy will be enforced for all IP addresses that belong to this address group, and are displayed here.

CLI Commands for Dynamic IP Addresses and Tags

The Command Line Interface on the firewall and Panorama give you a detailed view into the different sources from which tags and IP addresses are dynamically registered. It also allows you to audit registered and unregistered tags. The following examples illustrate the capabilities in the CLI.

Example	CLI Command

View all registered IP addresses that match the tag, `state.poweredOn` or that are not tagged as `vSwitch0`	`show log iptag tag_name equal state.poweredOn`
	`show log iptag tag_name not-equal switch.vSwitch0`

View all dynamically registered IP addresses that were sourced by VM Information Source with name `vmware1` and tagged as `poweredOn`	`show vm-monitor source source-name vmware1 tag state.poweredOn registered-ip all`
	
	`registered IP                          Tags`
	`---------------------------- -----------------`
	`fe80::20c:29ff:fe69:2f76      "state.poweredOn"`
	`10.1.22.100                   "state.poweredOn"`
	`2001:1890:12f2:11:20c:29ff:fe69:2f76`
	`"state.poweredOn"`
	`fe80::20c:29ff:fe69:2f80       "state.poweredOn"`
	`192.168.1.102                 "state.poweredOn"`
	`10.1.22.105                   "state.poweredOn"`
	`2001:1890:12f2:11:2cf8:77a9:5435:c0d`
	`"state.poweredOn"`
	`fe80::2cf8:77a9:5435:c0d       "state.poweredOn"`

Clear all IP addresses and tags learned from a specific VM Monitoring source without disconnecting the source.	`debug vm-monitor clear source-name <`*`name`*`>`
Display IP addresses registered from all sources.	`show object registered-ip all`
Display the count for IP addresses registered from all sources.	`show object registered-ip all option count`
Clear IP addresses registered from all sources	`debug object registered-ip clear all`
Add or delete tags for a given IP address that was registered using the XML API.	`debug object test registered-ip [<register/unregister>] <ip/netmask> <tag>`

Example	CLI Command

View all tags registered from a specific information source.	`show vm-monitor source source-name vmware1 tag all`
	`vlanId.4095`
	`vswitch.vSwitch1`
	`host-ip.10.1.5.22`
	`portgroup.TOBEUSED`
	`hostname.panserver22`
	`portgroup.VM Network 2`
	`datacenter.ha-datacenter`
	`vlanId.0`
	`state.poweredOn`
	`vswitch.vSwitch0`
	`vmname.Ubuntu22-100`
	`vmname.win2k8-22-105`
	`resource-pool.Resources`
	`vswitch.vSwitch2`
	`guestos.Ubuntu Linux 32-bit`
	`guestos.Microsoft Windows Server 2008 32-bit`
	`annotation.`
	`version.vmx-08`
	`portgroup.VM Network`
	`vm-info-source.vmware1`
	`uuid.564d362c-11cd-b27f-271f-c361604dfad7`
	`uuid.564dd337-677a-eb8d-47db-293bd6692f76`
	`Total: 22`

View all tags registered from a specific data source, for example from the VM Monitoring Agent on the firewall, the XML API, Windows User-ID Agent or the CLI.	• To view tags registered from the CLI:
	`show log iptag datasource_type equal unknown`
	• To view tags registered from the XML API:
	`show log iptag datasource_type equal xml-api`
	• To view tags registered from VM Information sources:
	`show log iptag datasource_type equal vm-monitor`
	• To view tags registered from the Windows User-ID agent:
	`show log iptag datasource_type equal xml-api datasource_subtype equal user-id-agent`

View all tags that are registered for a specific IP address (across all sources).	`debug object registered-ip show tag-source ip` *`ip_address`* `tag all`

Identify Users Connected through a Proxy Server

If you have a proxy server deployed between the users on your network and the firewall, in HTTP/HTTPS requests the firewall might see the proxy server IP address as the source IP address in the traffic that the proxy forwards rather than the IP address of the client that requested the content. In many cases, the proxy server adds an X-Forwarded-For (XFF) header to traffic packets that includes the actual IPv4 or IPv6 address of the client that requested the content or from whom the request originated. In such cases, you can configure the firewall to read the XFF header values and determine the IP addresses of the client who requested the content. The firewall matches the XFF IP addresses with usernames that your policy rules reference so that those rules can control access for the associated users and groups. The firewall also uses the XFF-derived usernames to populate the source user fields of logs so you can monitor user access to web services.

You can also configure the firewall to add XFF values to URL Filtering logs. In these logs, an XFF value can be the client IP address, client username (if available), the IP address of the last proxy server traversed in a proxy chain, or any string of up to 128 characters that the XFF header stores.

XFF user identification applies only to HTTP or HTTPS traffic, and only if the proxy server supports the XFF header. If the header has an invalid IP address, the firewall uses that IP address as a username for group mapping references in policies. If the XFF header has multiple IP addresses, the firewall uses the first entry from the left.

▲ Use XFF Values for Policies and Logging Source Users

▲ Add XFF Values to URL Filtering Logs

Use XFF Values for Policies and Logging Source Users

You can configure the firewall to use XFF values in user-based policies and in the source user fields of logs. To use XFF values in policies, you must also Map IP Addresses to Users, Map Users to Groups (if you have group-based policies), and configure policies based on users or groups.

> Logging XFF values doesn’t populate the source IP address values of logs. When you view the logs, the source field displays the IP address of the proxy server if one is deployed between the user clients and the firewall. However, you can configure the firewall to Add XFF Values to URL Filtering Logs so that you can see user IP addresses in those logs.

To ensure that attackers can’t read and exploit the XFF values in web request packets that exit the firewall to retrieve content from an external server, you can also configure the firewall to strip the XFF values from outgoing packets.

These options are not mutually exclusive: if you configure both, the firewall zeroes out XFF values only after using them in policies and logs.

Use XFF Values for Policies and Logging Source Users		
Step 1	Enable the firewall to use XFF values in policies and in the source user fields of logs.	1. Select **Device > Setup > Content-ID** and edit the X-Forwarded-For Headers settings. 2. Select the **Use X-Forwarded-For Header in User-ID** check box.
Step 2	Remove XFF values from outgoing web requests.	1. Select the **Strip X-Forwarded-For Header** check box. 2. Click **OK** and **Commit**.

Use XFF Values for Policies and Logging Source Users (Continued)		
Step 3	Verify the firewall is populating the source user fields of logs.	1. Select a log type that has a source user field (for example, **Monitor > Logs > Traffic**). 2. Verify that the Source User column displays the usernames of users who access the web.

Add XFF Values to URL Filtering Logs

You can configure the firewall to add the XFF values from web requests to URL Filtering logs. The XFF values that the logs display can be client IP addresses, usernames if available, or any values of up to 128 characters that the XFF fields store.

This method of logging XFF values doesn't add usernames to the source user fields in URL Filtering logs. To populate the source user fields, see Use XFF Values for Policies and Logging Source Users.

Add XFF Values to URL Filtering Logs		
Step 1	Configure a URL Filtering profile.	1. Select **Objects > Security Profiles > URL Filtering**. 2. Select an existing profile or **Add** a new profile and enter a descriptive **Name**. You can't enable XFF logging in the default URL Filtering profile. 3. In the **Categories** tab, Define how to control access to web content. 4. Select the **Settings** tab and select the **X-Forwarded-For** check box. 5. Click **OK** to save the profile.
Step 2	Attach the URL Filtering profile to a policy rule.	1. Select **Policies > Security** and click the rule. 2. Select the **Actions** tab, set the **Profile Type** to **Profiles**, and select the **URL Filtering** profile you just created. 3. Click **OK** and **Commit**.
Step 3	Verify the firewall is logging XFF values.	1. Select **Monitor > Logs > URL Filtering**. 2. Display the XFF values in one of the following ways: • To display the XFF value for a single log—Click the 🔍 icon for the log to displays its details. The HTTP Headers section displays the X-Forwarded-For value. • To display the XFF values for all logs—Open the drop-down in any column header, select **Columns**, and select the **X-Forwarded-For** check box. The page then displays an X-Forwarded-For column.

Policy-Based Forwarding

Normally, the firewall uses the destination IP address in a packet to determine the outgoing interface. The firewall uses the routing table associated with the virtual router to which the interface is connected to perform the route lookup. Policy-Based Forwarding (PBF) allows you to override the routing table, and specify the outgoing or *egress* interface based on specific parameters such as source or destination IP address, or type of traffic.

▲ PBF

▲ Create a Policy-Based Forwarding Rule

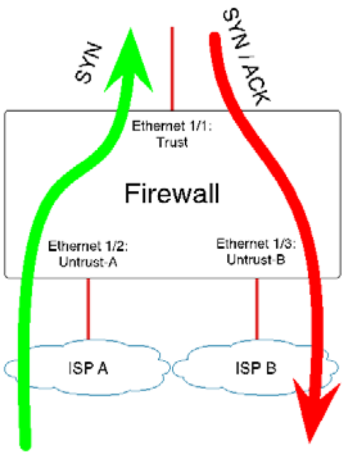
▲ Use Case: PBF for Outbound Access with Dual ISPs

PBF

PBF rules allow traffic to take an alternative path from the next hop specified in the route table, and are typically used to specify an egress interface for security or performance reasons. Let's say your company has two links between the corporate office and the branch office: a cheaper Internet link and a more expensive leased line. The leased line is a high-bandwidth, low-latency link. For enhanced security, you can use PBF to send applications that aren't encrypted traffic, such as FTP traffic, over the private leased line and all other traffic over the Internet link. Or, for performance, you can choose to route business-critical applications over the leased line while sending all other traffic, such as web browsing, over the cheaper link.

Egress Path and Symmetric Return

Using PBF, you can direct traffic to a specific interface on the firewall, drop the traffic, or direct traffic to another virtual system (on systems enabled for multiple virtual systems).



In networks with asymmetric routes, such as in a dual ISP environment, connectivity issues occur when traffic arrives at one interface on the firewall and leaves from another interface. If the route is asymmetrical, where the forward (SYN packet) and return (SYN/ACK) paths are different, the firewall is unable to track the state of the entire session and this causes a connection failure. To ensure that the traffic uses a symmetrical path, which means that the traffic arrives at and leaves from the same interface on which the session was created, you can enable the *Symmetric Return* option.

With symmetric return, the virtual router overrides a routing lookup for return traffic and instead directs the flow back to the MAC address from which it received the SYN packet (or first packet). However, if the destination IP address is on the same subnet as the ingress/egress interface's IP address, a route lookup is performed and symmetric return is not enforced. This behavior prevents traffic from being blackholed.

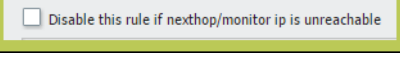
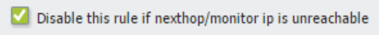
To determine the next hop for symmetric returns, the firewall uses an Address Resolution Protocol (ARP) table. The maximum number of entries that this ARP table supports is limited by the firewall model and the value is not user configurable. To determine the limit for your model, use the CLI command: `show pbf return-mac all`.

Path Monitoring

Path monitoring allows you to verify connectivity to an IP address so that the firewall can direct traffic through an alternate route, when needed. The firewall uses ICMP pings as *heartbeats* to verify that the specified IP address is reachable.

A monitoring profile allows you to specify the threshold number of heartbeats to determine whether the IP address is reachable. When the monitored IP address is unreachable, you can either disable the PBF rule or specify a *fail-over* or *wait-recover* action. Disabling the PBF rule allows the virtual router to take over the routing decisions. When the fail-over or wait-recover action is taken, the monitoring profile continues to monitor whether the target IP address is reachable, and when it comes back up, the firewall reverts back to using the original route.

The following table lists the difference in behavior for a path monitoring failure on a new session versus an established session.

Behavior of a session on a monitoring failure	**If the rule stays enabled when the monitored IP address is unreachable**  ☐ Disable this rule if nexthop/monitor ip is unreachable	**If rule is disabled when the monitored IP address is unreachable**  ☑ Disable this rule if nexthop/monitor ip is unreachable
For an established session	**wait-recover**—Continue to use egress interface specified in the PBF rule	**wait-recover**—Continue to use egress interface specified in the PBF rule
	fail-over—Use path determined by routing table (no PBF)	**fail-over**—Use path determined by routing table (no PBF)
For a new session	**wait-recover**—Use path determined by routing table (no PBF)	**wait-recover**—Check the remaining PBF rules. If no match, use the routing table
	fail-over—Use path determined by routing table (no PBF)	**fail-over**—Check the remaining PBF rules. If no match, use the routing table

Service Versus Applications in PBF

PBF rules are applied either on the first packet (SYN) or the first response to the first packet (SYN/ACK). This means that a PBF rule may be applied before the firewall has enough information to determine the application. Therefore, application-specific rules are not recommended for use with PBF. Whenever possible, use a service object, which is the Layer 4 port (TCP or UDP) used by the protocol or application.

However, if you specify an application in a PBF rule, the firewall performs *App-ID caching*. When an application passes through the firewall for the first time, the firewall does not have enough information to identify the application and therefore cannot enforce the PBF rule. As more packets arrive, the firewall determines the application and creates an entry in the App-ID cache and retains this App-ID for the session.When a new session is created with the same destination IP address, destination port, and protocol ID, the firewall could identify the application as the same from the initial session (based on the App-ID cache) and apply the PBF rule. Therefore, a session that is not an exact match and is not the same application, can be forwarded based on the PBF rule.

Further, applications have dependencies and the identity of the application can change as the firewall receives more packets. Because PBF makes a routing decision at the start of a session, the firewall cannot enforce a change in application identity. YouTube, for example, starts as web-browsing but changes to Flash, RTSP, or YouTube based on the different links and videos included on the page. However with PBF, because the firewall identifies the application as web-browsing at the start of the session, the change in application is not recognized thereafter.

You cannot use custom-applications, application-filters or application groups in PBF rules.

Create a Policy-Based Forwarding Rule

Use a PBF rule to direct traffic to a specific egress interface on the firewall, and override the default path for the traffic.

Create a PBF Rule		
Step 1	Create a PBF rule. When creating a PBF rule you must specify a name for the rule, a source zone or interface, and an egress interface. All other components are either optional or have a default value provided. You can specify the source and destination addresses using an IP address, an address object, or a FQDN. For the next hop, however, you must specify an IP address.	1. Select **Policies > Policy Based Forwarding** and click **Add.** 2. Give the rule a descriptive name in the **General** tab. 3. In the **Source** tab, select the following: a. Select the **Type—Zone** or **Interface—** to which the forwarding policy will be applied, and the relevant zone or interface. If you have an asymmetric routing environment and want to enforce symmetric return, you must select a source interface. PBF is only supported on Layer 3 interfaces; loopback interfaces do not support PBF. b. (Optional) Specify the **Source Address** to which PBF will apply. For example, a specific IP address or subnet IP address from which you want to forward traffic to the interface or zone specified in this rule. Use the **Negate** option to exclude a one or more source IP addresses from the PBF rule. For example, if your PBF rule directs all traffic from the specified zone to the Internet, **Negate** allows you to exclude internal IP addresses from the PBF rule. The evaluation order is top down. A packet is matched against the first rule that meets the defined criteria; after a match is triggered the subsequent rules are not evaluated. c. (Optional) **Add** and select the **Source User** or groups of users to whom the policy applies. 4. In the **Destination/Application/Service** tab, select the following: a. **Destination Address**. By default the rule applies to **Any** IP address. Use the **Negate** option to exclude one or more destination IP addresses from the PBF rule. b. Select the Application(s) or Service(s) that you want to control using PBF. Application-specific rules are not recommended for use with PBF. Whenever possible, use a service object, which is the Layer 4 port (TCP or UDP) used by the protocol or application. For more details, see Service Versus Applications in PBF.

Create a PBF Rule

Step 2 Define the forwarding rules.

If you are configuring PBF in a multi-VSYS environment, you must create separate PBF rules for each virtual system (and create the appropriate Security policy rules to enable the traffic).

5. In the **Forwarding** tab, select the following:

   a. Set the **Action.** The options are as follows:

   – **Forward**—Directs the packet to a specific **Egress Interface**. Enter the **Next Hop** IP address for the packet (you cannot use an FQDN for the next hop).

   – **Forward To VSYS**—(On a device enabled for multiple virtual systems) Select the virtual system to which to forward the packet.

   – **Discard**—Drop the packet.

   – **No PBF**—Exclude the packets that match the criteria for source/destination/application/service defined in the rule. Matching packets use the route table instead of PBF; the firewall uses the route table to exclude the matched traffic from the redirected port.

   To trigger the specified action at a daily, weekly or non-recurring frequency, create and attach a **Schedule**.

   b. (Optional) Enable Monitoring to verify connectivity to a target IP address or to the next hop IP address. Select **Monitor** and attach a monitoring **Profile** (default or custom) that specifies the action when the IP address is unreachable.

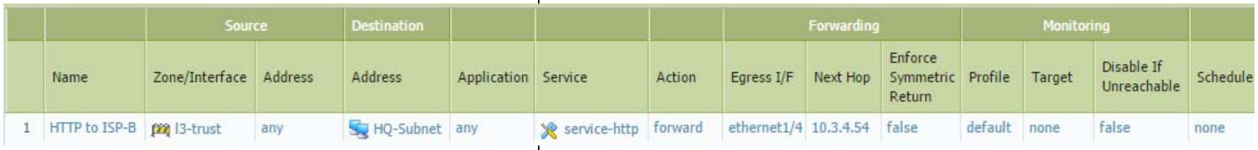
   c. (Optional, required for asymmetric routing environments) Select **Enforce Symmetric Return** and enter one or more IP addresses in the **Next Hop Address List** (you cannot use an FQDN as the next hop). You can add up to 8 next-hop addresses per rule; tunnel and PPoE interfaces are not available as a next-hop IP address

   Enabling symmetric return ensures that return traffic (say, from the Trust zone on the LAN to the Internet) is forwarded out through the same interface through which traffic ingresses from the Internet.

Step 3 Save the policies to the running configuration on the device.

Click **Commit**.

The PBF rule is in effect.

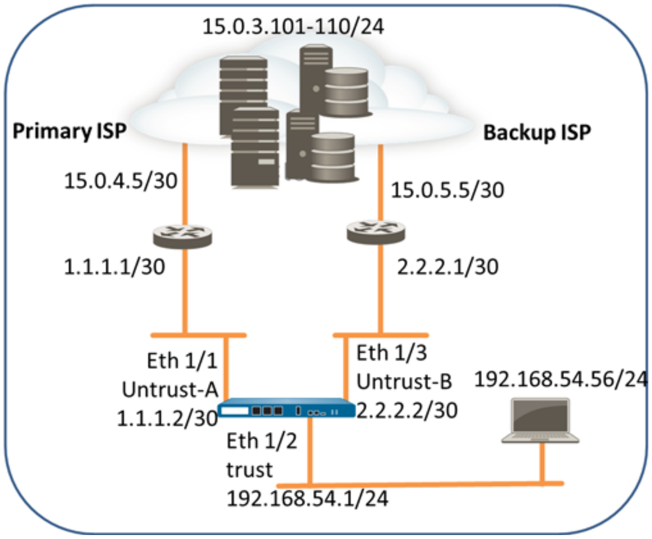


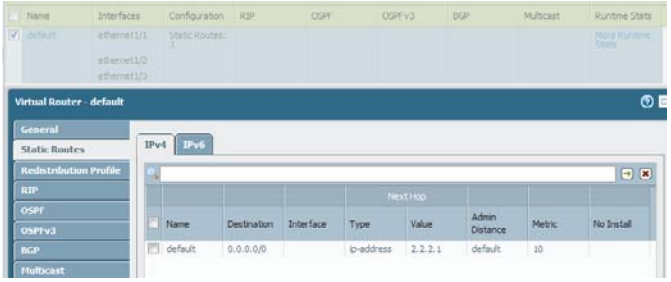
		Source		Destination				Forwarding			Monitoring			
	Name	Zone/Interface	Address	Address	Application	Service	Action	Egress I/F	Next Hop	Enforce Symmetric Return	Profile	Target	Disable If Unreachable	Schedule
1	HTTP to ISP-B	l3-trust	any	HQ-Subnet	any	service-http	forward	ethernet1/4	10.3.4.54	false	default	none	false	none

Use Case: PBF for Outbound Access with Dual ISPs

In this use case, the branch office has a dual ISP configuration and implements PBF for redundant Internet access. The backup ISP is the default route for traffic from the client to the web servers. In order to enable redundant Internet access without using an internetwork protocol such as BGP, we use PBF with destination interface-based source NAT and static routes, and configure the firewall as follows:

- Enable a PBF rule that routes traffic through the primary ISP, and attach a monitoring profile to the rule. The monitoring profile triggers the firewall to use the default route through the backup ISP when the primary ISP is unavailable.
- Define Source NAT rules for both the primary and backup ISP that instruct the firewall to use the source IP address associated with the egress interface for the corresponding ISP. This ensures that the outbound traffic has the correct source IP address.
- Add a static route to the backup ISP, so that when the primary ISP is unavailable, the default route comes into effect and the traffic is directed through the backup ISP.



PBF for Outbound Access with Dual ISPs		
Step 1	Configure the ingress and the egress interfaces on the firewall. Egress interfaces can be in the same zone. In this example we assign the egress interfaces to different zones.	1. Select **Network > Interfaces** and then select the interface you want to configure, for example, Ethernet1/1 and Ethernet1/3. The interface configuration on the firewall used in this example is as follows: • Ethernet 1/1 connected to the primary ISP: – Zone: ISP-East – IP Address:1.1.1.2/30 – Virtual Router: Default • Ethernet 1/3 connected to the backup ISP: – Zone: ISP-West – IP Address:2.2.2.2/30 – Virtual Router: Default • Ethernet 1/2 is the ingress interface, used by the network clients to connect to the Internet: – Zone: Trust – IP Address:192.168. 54.1/24 – Virtual Router: Default 2. To save the interface configuration, click **OK**.
Step 2	On the virtual router, add a static route to the backup ISP.	1. Select **Network > Virtual Router** and then select the **default** link to open the Virtual Router dialog. 2. Select the **Static Routes** tab and click **Add**. Enter a **Name** for the route and specify the **Destination** IP address for which you are defining the static route. In this example, we use 0.0.0.0/0 for all traffic. 3. Select the **IP Address** radio button and set the **Next Hop** IP address (you cannot use an FQDN) for your router that connects to the backup Internet gateway. In this example, 2.2.2.1. 4. Specify a cost metric for the route. In this example, we use 10.  Virtual Router - default Static Routes — IPv4 Name: default; Destination: 0.0.0.0/0; Interface: ; Next Hop Type: ip-address; Next Hop Value: 2.2.2.1; Admin Distance: default; Metric: 10; No Install: 5. Click **OK** twice to save the virtual router configuration.

PBF for Outbound Access with Dual ISPs

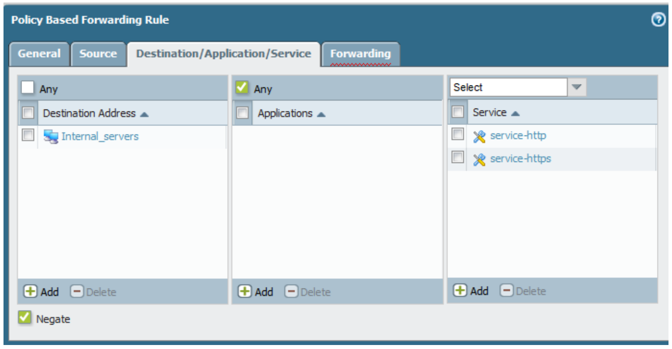
Step 3 Create a PBF rule that directs traffic to the interface that is connected to the primary ISP.

Make sure to exclude traffic destined to internal servers/IP addresses from PBF. Define a negate rule so that traffic destined to internal IP addresses is not routed through the egress interface defined in the PBF rule.

1. Select **Policies > Policy Based Forwarding** and click **Add.**
2. Give the rule a descriptive **Name** in the **General** tab.
3. In the **Source** tab, set the **Source Zone** to Trust.
4. In the **Destination/Application/Service** tab, set the following:
   a. In the Destination Address section, **Add** the IP addresses or address range for servers on the internal network or create an address object for your internal servers. Select **Negate** to exclude the IP addresses or address object listed above from using this rule.

   b. In the Service section, **Add** the **service-http** and **service-https** services to allow HTTP and HTTPS traffic to use the default ports. For all other traffic that is allowed by security policy, the default route will be used.

   To forward all traffic using PBF, set the Service to **Any**.



Policy Based Forwarding Rule

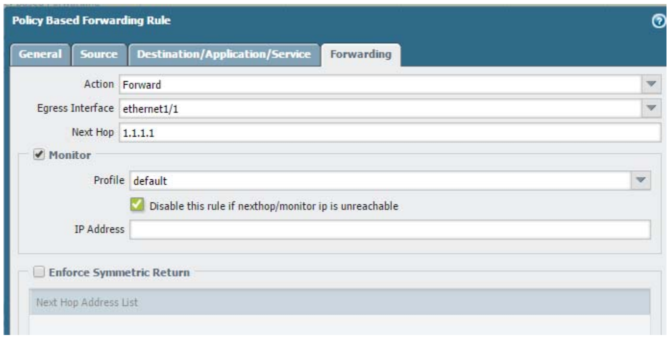
General | Source | Destination/Application/Service | Forwarding

□ Any
□ Destination Address
□ Internal_servers
☑ Negate

☑ Any
□ Applications

Select
□ Service
□ service-http
□ service-https

5. In the **Forwarding** tab, specify the interface to which you want to forward traffic and enable path monitoring.
   a. To forward traffic, set the **Action** to **Forward**, and select the **Egress Interface** and specify the **Next Hop**. In this example, the egress interface is ethernet1/1, and the next hop IP address is 1.1.1.1.



Policy Based Forwarding Rule

General | Source | Destination/Application/Service | Forwarding

Action: Forward
Egress Interface: ethernet1/1
Next Hop: 1.1.1.1
☑ Monitor
Profile: default
☑ Disable this rule if nexthop/monitor ip is unreachable
IP Address:
□ Enforce Symmetric Return
Next Hop Address List

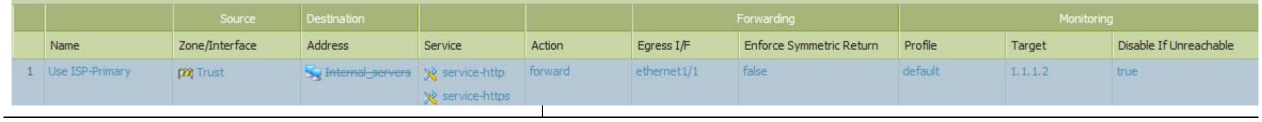
PBF for Outbound Access with Dual ISPs

b. Enable **Monitor** and attach the default monitoring profile, to trigger a failover to the backup ISP. In this example, we do not specify a target IP address to monitor. The firewall will monitor the next hop IP address; if this IP address is unreachable the firewall will direct traffic to the default route specified on the virtual router.

c. (Required if you have asymmetric routes). Select **Enforce Symmetric Return** to ensure that return traffic from the Trust zone to the Internet is forwarded out on the same interface through which traffic ingressed from the Internet.

NAT ensures that the traffic from the Internet is returned to the correct interface/IP address on the firewall.

d. Click **OK** to save the changes.



		Source	Destination			Forwarding		Monitoring		
	Name	Zone/Interface	Address	Service	Action	Egress I/F	Enforce Symmetric Return	Profile	Target	Disable If Unreachable
1	Use ISP-Primary	Trust	~~Internal_servers~~	service-http service-https	forward	ethernet1/1	false	default	1.1.1.2	true

PBF for Outbound Access with Dual ISPs

Step 4 Create NAT rules based on the egress interface and ISP. These rules ensure that the correct source IP address is used for outbound connections.

1. Select **Policies > NAT** and click **Add**.
2. In this example, the NAT rule we create for each ISP is as follows:

NAT for Primary ISP

In the **Original Packet** tab,

- **Source Zone**: Trust
- **Destination Zone**: ISP-West

In the **Translated Packet** tab, under Source Address Translation

- **Translation Type**: Dynamic IP and Port
- **Address Type**: Interface Address
- **Interface**: ethernet1/1
- **IP Address**: 1.1.1.2/30

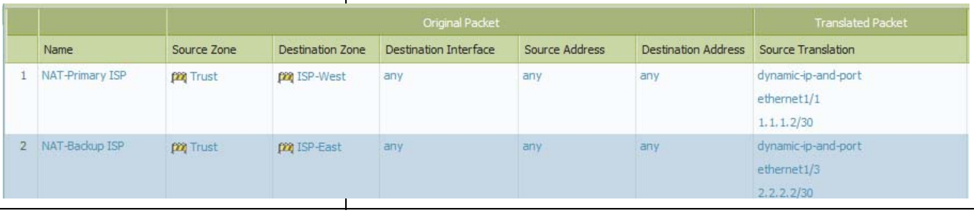
NAT for Backup ISP

In the **Original Packet** tab,

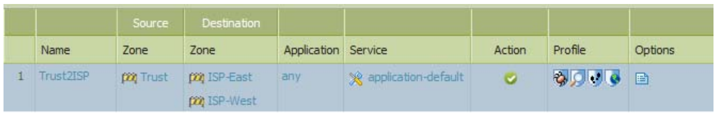
- **Source Zone**: Trust
- **Destination Zone**: ISP-East

In the **Translated Packet** tab, under Source Address Translation

- **Translation Type**: Dynamic IP and Port
- **Address Type**: Interface Address
- **Interface**: ethernet1/3
- **IP Address**: 2.2.2.2/30



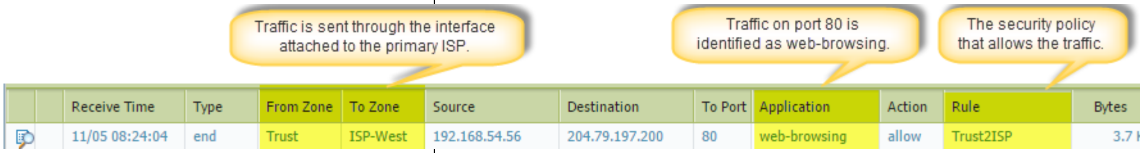
		Original Packet					Translated Packet
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Source Translation
1	NAT-Primary ISP	Trust	ISP-West	any	any	any	dynamic-ip-and-port ethernet1/1 1.1.1.2/30
2	NAT-Backup ISP	Trust	ISP-East	any	any	any	dynamic-ip-and-port ethernet1/3 2.2.2.2/30

<table>
<tr><th colspan="3">PBF for Outbound Access with Dual ISPs</th></tr>
<tr><td>Step 5</td><td>Create security policy to allow outbound access to the Internet.</td><td>To safely enable applications, create a simple rule that allows access to the Internet and attach the security profiles available on the firewall.
1. Select <b>Policies > Security</b> and click <b>Add</b>.
2. Give the rule a descriptive <b>Name</b> in the <b>General</b> tab.
3. In the <b>Source</b> tab, set the <b>Source Zone</b> to Trust.
4. In the <b>Destination</b> tab, Set the <b>Destination Zone</b> to ISP-East and ISP-West.
5. In the <b>Service/ URL Category</b> tab, leave the default <b>application-default</b>.
6. In the <b>Actions</b> tab, complete these tasks:
a. Set the <b>Action Setting</b> to <b>Allow</b>.
b. Attach the default profiles for antivirus, anti-spyware, vulnerability protection and URL filtering, under <b>Profile Setting.</b>
7. Under <b>Options</b>, verify that logging is enabled at the end of a session. Only traffic that matches a security rule is logged.

<table>
<tr><th></th><th></th><th>Source</th><th>Destination</th><th></th><th></th><th></th><th></th><th></th></tr>
<tr><th></th><th>Name</th><th>Zone</th><th>Zone</th><th>Application</th><th>Service</th><th>Action</th><th>Profile</th><th>Options</th></tr>
<tr><td>1</td><td>Trust2ISP</td><td>Trust</td><td>ISP-East
ISP-West</td><td>any</td><td>application-default</td><td>✓</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Step 6</td><td>Save the policies to the running configuration on the device.</td><td>Click <b>Commit</b>.</td></tr>
</table>

PBF for Outbound Access with Dual ISPs

Step 7 Verify that the PBF rule is active and that the primary ISP is used for Internet access.

1. Launch a web browser and access a web server. On the firewall check the traffic log for web-browsing activity.



Traffic is sent through the interface attached to the primary ISP.

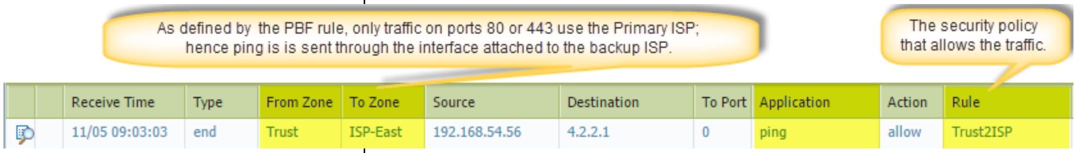
Traffic on port 80 is identified as web-browsing.

The security policy that allows the traffic.

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule	Bytes
		11/05 08:24:04	end	Trust	ISP-West	192.168.54.56	204.79.197.200	80	web-browsing	allow	Trust2ISP	3.7 k

2. From a client on the network, use the ping utility to verify connectivity to a web server on the Internet. and check the traffic log on the firewall.

```
C:\Users\pm-user1>ping 4.2.2.1
Pinging 4.2.2.1 with 32 bytes of data:
Reply from 4.2.2.1: bytes=32 time=34ms TTL=117
Reply from 4.2.2.1: bytes=32 time=13ms TTL=117
Reply from 4.2.2.1: bytes=32 time=25ms TTL=117
Reply from 4.2.2.1: bytes=32 time=3ms TTL=117
Ping statistics for 4.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 34ms, Average = 18ms
```



As defined by the PBF rule, only traffic on ports 80 or 443 use the Primary ISP; hence ping is is sent through the interface attached to the backup ISP.

The security policy that allows the traffic.

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
		11/05 09:03:03	end	Trust	ISP-East	192.168.54.56	4.2.2.1	0	ping	allow	Trust2ISP

3. To confirm that the PBF rule is active, use the CLI command **`show pbf rule all`**

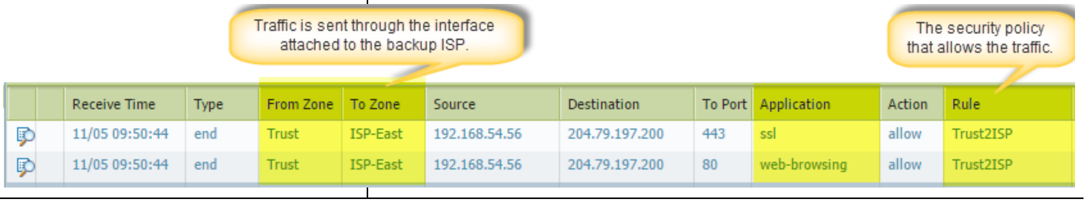
```
admin@PA-NGFW> show pbf rule all
Rule       ID    Rule State Action   Egress IF/VSYS  NextHop
========== === ========== ====== ============== =======
Use ISP-Pr 1     Active     Forward ethernet1/1     1.1.1.1
```

Step 8 Verify that the failover to the backup ISP occurs and that the Source NAT is correctly applied.

1. Unplug the connection to the primary ISP.
2. Confirm that the PBF rule is inactive with the CLI command **`show pbf rule all`**

```
admin@PA-NGFW> show pbf rule all
Rule       ID    Rule State Action   Egress IF/VSYS  NextHop
========== === ========== ====== ============== =======
Use ISP-Pr 1   Disabled   Forward   ethernet1/1     1.1.1.1
```

3. Access a web server, and check the traffic log to verify that traffic is being forwarded through the backup ISP.



Traffic is sent through the interface attached to the backup ISP.

The security policy that allows the traffic.

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
		11/05 09:50:44	end	Trust	ISP-East	192.168.54.56	204.79.197.200	443	ssl	allow	Trust2ISP
		11/05 09:50:44	end	Trust	ISP-East	192.168.54.56	204.79.197.200	80	web-browsing	allow	Trust2ISP

PBF for Outbound Access with Dual ISPs

4. View the session details to confirm that the NAT rule is working properly.

```
admin@PA-NGFW> show session all
---------------------------------------------------------
ID Application    State   Type Flag Src[Sport]/Zone/Proto
  (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
  IP[Port])
---------------------------------------------------------
87212 ssl ACTIVE  FLOW  NS   192.168.54.56[53236]/Trust/6
  (2.2.2.2[12896]) vsys1 204.79.197.200[443]/ISP-East
  (204.79.197.200[443])
```

5. Obtain the session identification number from the output and view the session details. Note that the PBF rule is not used and hence is not listed in the output.

```
admin@PA-NGFW> show session id 87212

Session           87212

        c2s flow:
                source:      192.168.54.56 [Trust]
                dst:         204.79.197.200
                proto:       6
               sport:       53236          dport:      443
               state:       ACTIVE         type:       FLOW
                src user:    unknown
                dst user:    unknown

        s2c flow:
                source:      204.79.197.200 [ISP-East]
                dst:         2.2.2.2
                proto:       6
              sport:       443            dport:      12896
               state:       ACTIVE         type:       FLOW
                src user:    unknown
                dst user:    unknown
start time                    : Wed Nov5 11:16:10 2014
        timeout                       : 1800 sec
        time to live                  : 1757 sec
        total byte count(c2s)         : 1918
        total byte count(s2c)         : 4333
        layer7 packet count(c2s)      : 10
        layer7 packet count(s2c)      : 7
        vsys                          : vsys1
        application                   : ssl
        rule                          : Trust2ISP
        session to be logged at end   : True
        session in session ager       : True
        session synced from HA peer   : False
        address/port translation      : source
       nat-rule                    : NAT-Backup ISP(vsys1)
        layer7 processing             : enabled
        URL filtering enabled         : True
        URL category                  : search-engines
        session via syn-cookies       : False
        session terminated on host    : False
        session traverses tunnel      : False
        captive portal session        : False
        ingress interface             : ethernet1/2
        egress interface              : ethernet1/3
        session QoS rule              : N/A (class 4)
```