Palo Alto Networks® Firewall connector v1.0.1

About the connector

Palo Alto Networks® Firewall is a next-generation firewall by Palo Alto Networks®, which contains application awareness, full stack visibility, extra-firewall intelligence, and upgrade paths in addition to the full capabilities of both traditional firewalls and intrusion prevention systems. Additionally, the company defines its firewall technology by the following abilities:

- Identify applications regardless of port, protocol, evasive tactic, or Secure Sockets Layer.
- Identify and control users regardless of IP address, location, or device.
- Protect against known and unknown application-borne threats.
- Fine-grained visibility and policy control over application access and functionality.

The PaloAlto Firewall connector allows the user to block and unblock both the IP and the application, thereby protecting against known and unknown threats and blocking the communication with malicious IPs. Palo Alto Networks® help security analysts turn thread data into thread intelligence. It take indicators from network, like domain names and IPs and connects them with nearly every active domain on the Internet. These connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

This document provides information about the PaloAlto Firewall connector, which facilitates automated interactions, with a Palo Alto Networks® server using CyOPs™ playbooks. Add the PaloAlto Firewall connector as a step in CyOPs™ playbooks and perform automated operations, such as blocking and unblocking IPs, URLs and applications.

Version information

Connector Version: 1.0.1

CyOPs™ Version Tested on: 4.11.0-1161

PaloAlto Versions Tested on: The PaloAlto Firewall connector has been tested on the following: Model: PA-VM version 8.0.0 Application version: 655-3816

Authored By: CyberSponse, Inc.

Certified: Yes

Release Notes for version 1.0.1

Following enhancements have been made to the PaloAlto Firewall connector in version 1.0.1:

- Masked the text entered in the **API Key** field on the `Configuration` page.
- Added a link to the online help.
- Added a new configuration parameter, named **Verify SSL**.

- Updated the name of the connector from PaloAlto to PaloAlto Firewall.
- In the Block IP and Unblock IP operation, renamed the IP to Block and IP to Unblock parameter to IP Address.
- Updated the input parameter name IP to IP Address in the Block IP and Unblock IP operations.
- Updated the input parameter name app to Application Name in Block Application and Unblock Application operations.

Installing the connector

All connectors provided by CyOPs™ are delivered using a CyOPs™ repository. Therefore, you must set up your CyOPs™ repository and use the `yum` command to install connectors:

```
yum install cyops-connector-paloalto-firewall
```

For the procedure to install a connector, click here.

Prerequisites to configuring the connector

- You must have the IP address or hostname of the Palo Alto Networks® Firewall to which you will connect and perform the automated operations.
- You must also have the username and password to access the Palo Alto Networks® Firewall.
- To access the CyOPs™ UI, ensure that port 443 is open through the firewall for the CyOPs™ instance.

Configuring the connector

For the procedure to configure a connector, click here.

Configuration parameters

In CyOPs™, on the Connectors page, select the **PaloAlto Firewall** connector and click **Configure** to configure the following parameters:

Parameter	Description
Server URL	IP address or Hostname of the PaloAlto Firewall.
Username	Username to access the PaloAlto Firewall.
Password	Password to access the PaloAlto Firewall.

Parameter	Description
Security Policy Name for Blocking IP	Security Policy Name that has been pre-configured in PaloAlto for blocking an IP.
IP Address Group	Name of the IP Address Group that is linked to the Security Policy Name for Blocking IP.
Security Policy Name for Blocking URL	Security Policy Name that has been pre-configured in PaloAlto for blocking a URL.
URL Group	Name of the URL Group that is linked to the Security Policy Name for Blocking URL.
Security Policy Name for Blocking Application	Security Policy Name that has been pre-configured in PaloAlto for blocking a Application.
Application Group	Name of the Application Group that is linked to the Security Policy Name for Blocking Application.
Verify SSL	Specifies whether the SSL certificate for the server is to be verified or not. By default, this option is set as True.

Actions supported by the connector

The following automated operations can be included in playbooks, and you can also use the annotations to access operations from CyOPs™ release 4.10.0 onward:

Function	Description	Annotation and Category
Block IP	Blocks the specified IP address.	block_ip Containment

Function	Description	Annotation and Category
Unblock IP	Unblocks the specified IP address.	unblock_ip Remediation
Block URL	Blocks the specified URL.	block_url Containment
Unblock URL	Unblocks the specified URL.	unblock_ip Remediation
Block Application	Blocks the specified application.	block_app Containment
Unblock Application	Unblocks the specified Application.	unblock_app Remediation

operation: Block IP

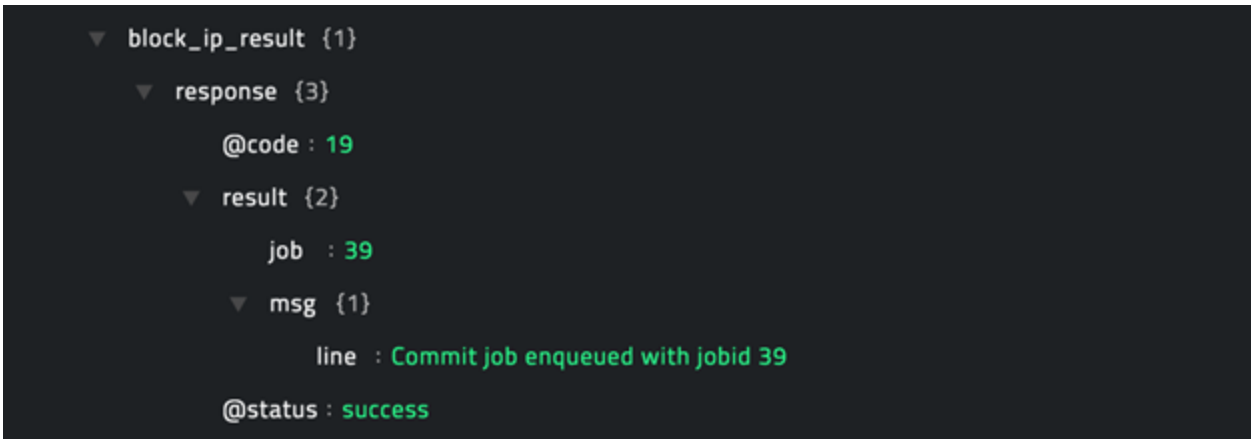
Input parameters

Parameter	Description
IP Address	IP address that you want to block.

Output

The JSON output returns a `Success` message if the IP is successful blocked or an `Error` message containing the reason for failure if the IP is not blocked.

Following image displays a sample output:



operation: Unblock IP

Input parameters

Parameter	Description
IP Address	IP address that you want to unblock.

Output

The JSON output returns a `Success` message if the IP is successful unblocked or an `Error` message containing the reason for failure if the IP is not unblocked.

Following image displays a sample output:

operation: Block URL

Input parameters

Parameter	Description
url	URL that you want to block.

Output

The JSON output returns a `Success` message if the URL is successful blocked or an `Error` message containing the reason for failure if the URL is not blocked.

Following image displays a sample output:

operation: Unblock URL

Input parameters

Parameter	Description
url	URL that you want to unblock.

Output

The JSON output returns a `Success` message if the URL is successful unblocked or an `Error` message containing the reason for failure if the URL is not unblocked.

Following image displays a sample output:

operation: Block Application

Input parameters

Parameter	Description
Application Name	Name of the application that you want to block.

Output

The JSON output returns a `Success` message if the application is successful blocked or an `Error` message containing the reason for failure if the application is not blocked.

Following image displays a sample output:

operation: Unblock Application

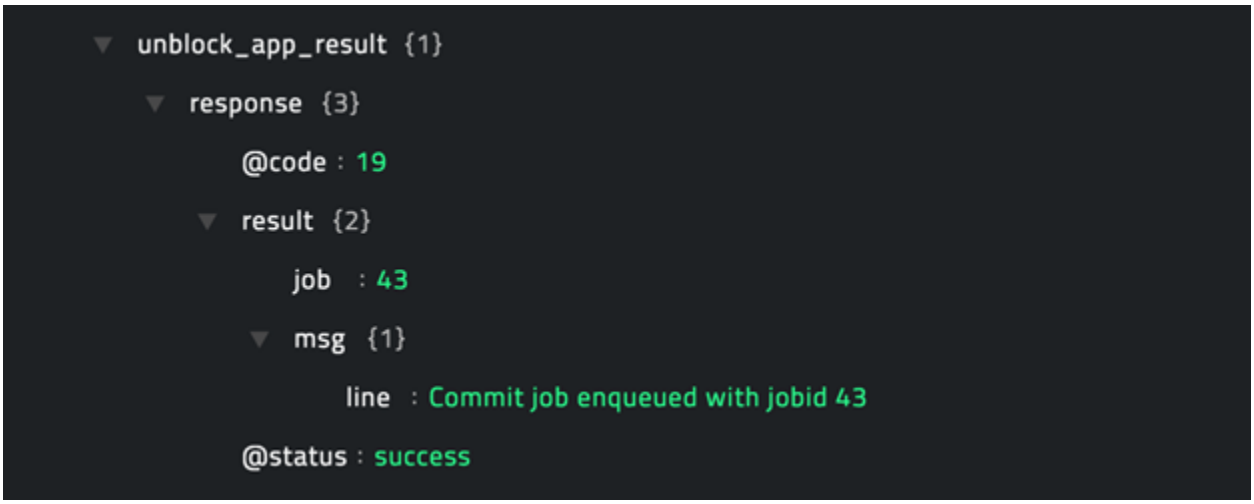
Input parameters

Parameter	Description
Application Name	Name of the application that you want to unblock.

Output

The JSON output returns a `Success` message if the application is successful unblocked or an `Error` message containing the reason for failure if the application is not unblocked.

Following image displays a sample output:



Included playbooks

The *`Sample - PaloAlto-Firewall - 1.0.1`* playbook collection comes bundled with the PaloAlto Firewall connector. This playbook contains steps using which you can perform all supported actions. You can see the bundled playbooks in the **Automation** > **Playbooks** section in CyOPs™ after importing the PaloAlto Firewall connector.

- Block Application
- Block IP
- Block URL
- Unblock Application
- Unblock IP
- Unblock URL

Note: If you are planning to use any of the sample playbooks in your environment, ensure that you clone those playbooks and move them to a different collection since the sample playbook collection gets deleted during connector upgrade and delete.