Palo Alto Networks® NGFW Integration Installation and Configuration Guide

Software Version 2.0

Integration Guide

April 19, 2023

30010-04 EN Rev.A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

The ThreatConnect® integration with Palo Alto Networks Next-Generation Firewall (NGFW) enables the deployment of Address and URL Indicators from ThreatConnect to Palo Alto Networks NGFW or Panorama™ devices for alerting and blocking.

Dependencies

ThreatConnect Dependencies

- ThreatConnect version 6.4 or newer
- Active ThreatConnect Application Programming Interface (API) key

Note: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Customers on Dedicated Cloud and On Premises instances can enable these settings on the **Account Settings** screen within their ThreatConnect instance.

Palo Alto Networks NGFW Dependencies

- Active Palo Alto API key
- Palo Alto Networks NGFW versions 7.0.*x* and 7.1.*x*

Configuration Parameters

Parameter Definitions

The parameters defined in Table 1 apply to the configuration parameters during the Job-creation process.

Table 1

Name	Description	Required?
Api User	The ThreatConnect API User.	Yes
Palo Alto URL	The Palo Alto API path for the Palo Alto Networks device.	Yes
Palo Alto API Key	The Palo Alto API key.	Yes
Verify SSL for Palo Alto	Select this checkbox to verify the API host's SSL certificate during the connection.	No
Indicator Types	The type(s) of Indicators that will be sent to Palo Alto Networks. Accepted values include the following: • Address • Host	No
ThreatConnect Owners	The ThreatConnect owner(s) whose Indicators will be sent to Palo Alto Networks.	No
Last Run	The last time the App ran. Data modified since this date will be included on the first run. Thereafter, the date will be automatically updated each time the job successfully completes. The default value is **30 days ago**.	No
TQL	A custom ThreatConnect Query Language (TQL) query for filtering Indicators. If using this parameter, do not use any other filter-based parameters (**Indicator Types**, **ThreatConnect Owners**, **Indicator**	No

	Types, **Include Tags**, **Minimum ThreatAssess Score**, **Minimum Threat Rating**, **Minimum Confidence Rating**, and **Maximum False Positive Count**), as doing so will cause the App to error out.	
Include Tags	The Tag(s) that Indicators must include in order to be sent to Palo Alto Networks. Indicators must include **at least one** of the specified Tags in order to be sent.	No
Minimum ThreatAssess Score	The minimum ThreatAssess score that Indicators must have in order to be sent to Palo Alto Networks.	No
Minimum Threat Rating	The minimum Threat Rating that Indicators must have in order to be sent to Palo Alto Networks.	No
Minimum Confidence Rating	The minimum Confidence Rating that Indicators must have in order to be sent to Palo Alto Networks.	No
Maximum False Positive Count	The maximum number of false positives that Indicators can have in order to be sent to Palo Alto Networks. When used, only Indicators with a false positive count less than or equal to the specified value will be sent.	No
Palo Alto Target Name (for Panorama use the device-group name)	The hostname for the Palo Alto Networks device.	No
Palo Alto URL Category (Domains)	The name of the destination URL category.	No

Palo Alto Address Group Name (IP Addresses)	The vSys or Device Group Entry Name on the Palo Alto Networks device.	No
Enable Panorama Support	Select this checkbox to enable support for Panorama.	No
Push to Panorama Device Group (Commit All)	Select this checkbox to perform a commit-all push of the configurations to the remote devices.	No
Remove Depreciated Indicators from Palo Alto Device	Select this checkbox to remove Indicators that have been deprecated in ThreatConnect from the Address Group and URL Category.	No
Logging Level	Determines the verbosity of the logging output for the application.	No

Palo Alto Address Group

For each ThreatConnect owner that is configured, there is a separate Address Group that is synced (Figure 1).

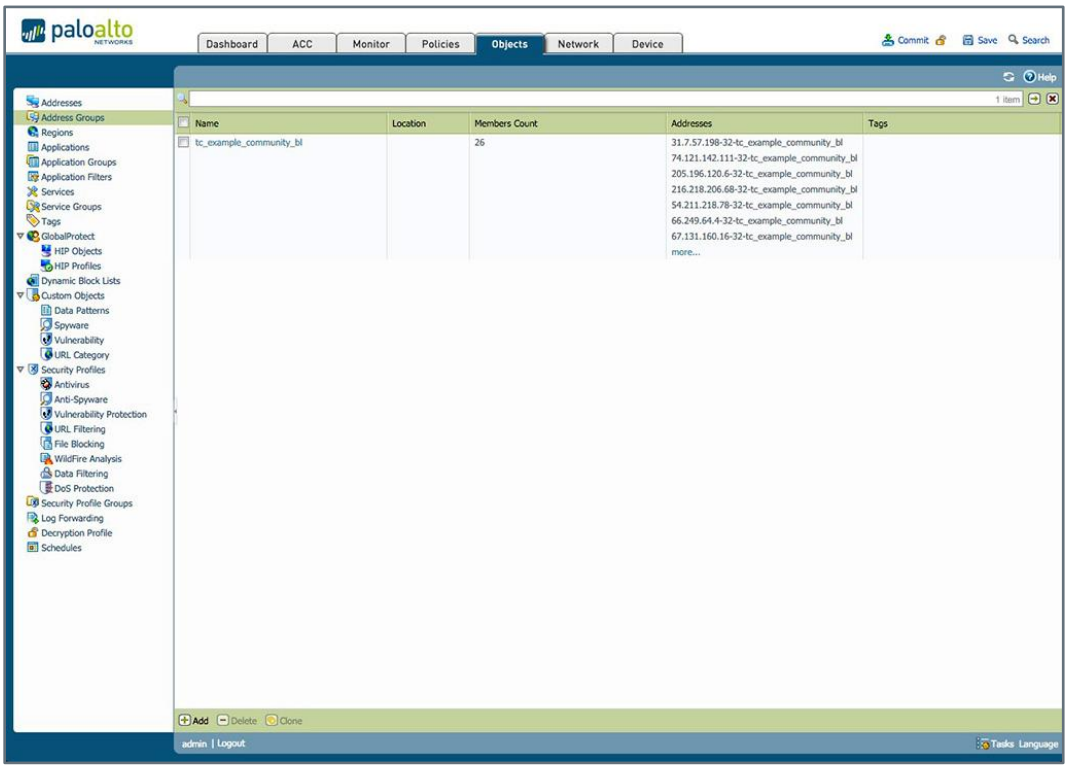

Figure 1

Palo Alto Addresses

Each Indicator added by the script as an address will be tagged with the **TC Managed** tag and will be highlighted in orange (Figure 2).

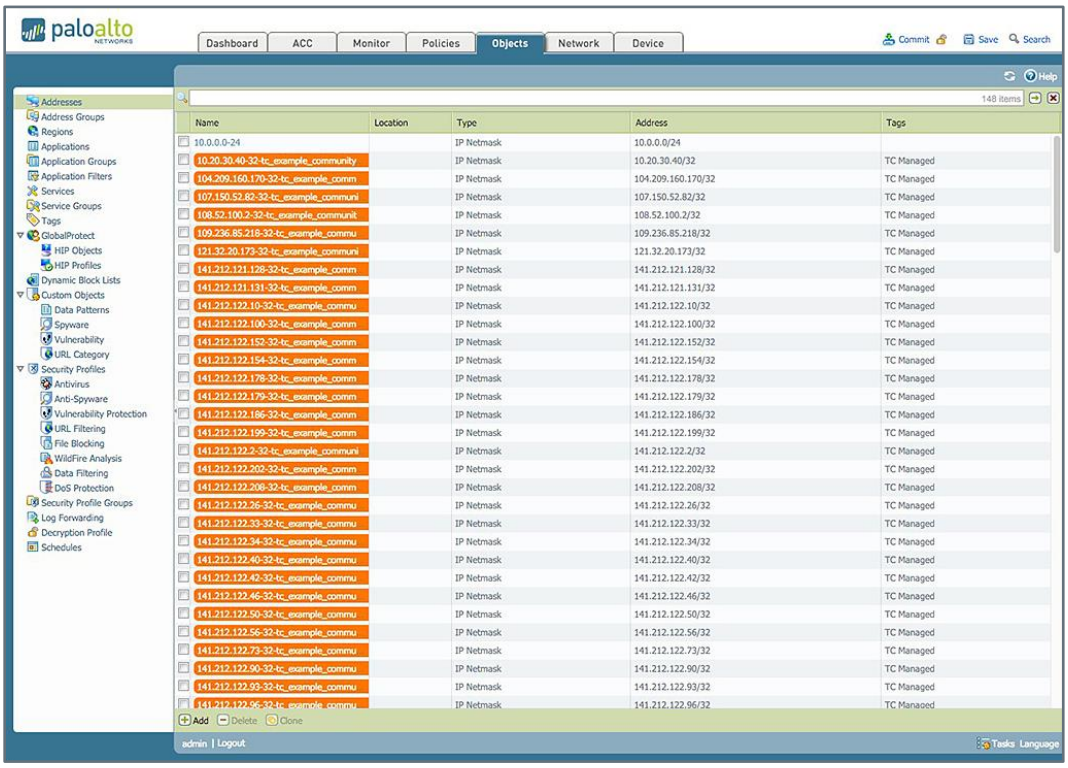

Figure 2

Palo Alto Tag

The script will create the **TC Managed** tag automatically if it does not exist. The color of the tag can be changed, if required, but the name must not be changed (Figure 3).

Figure 3

Palo Alto URL Category

For each ThreatConnect owner configured (Figure 4), there is a separate URL Category that is synced (Figure 5).

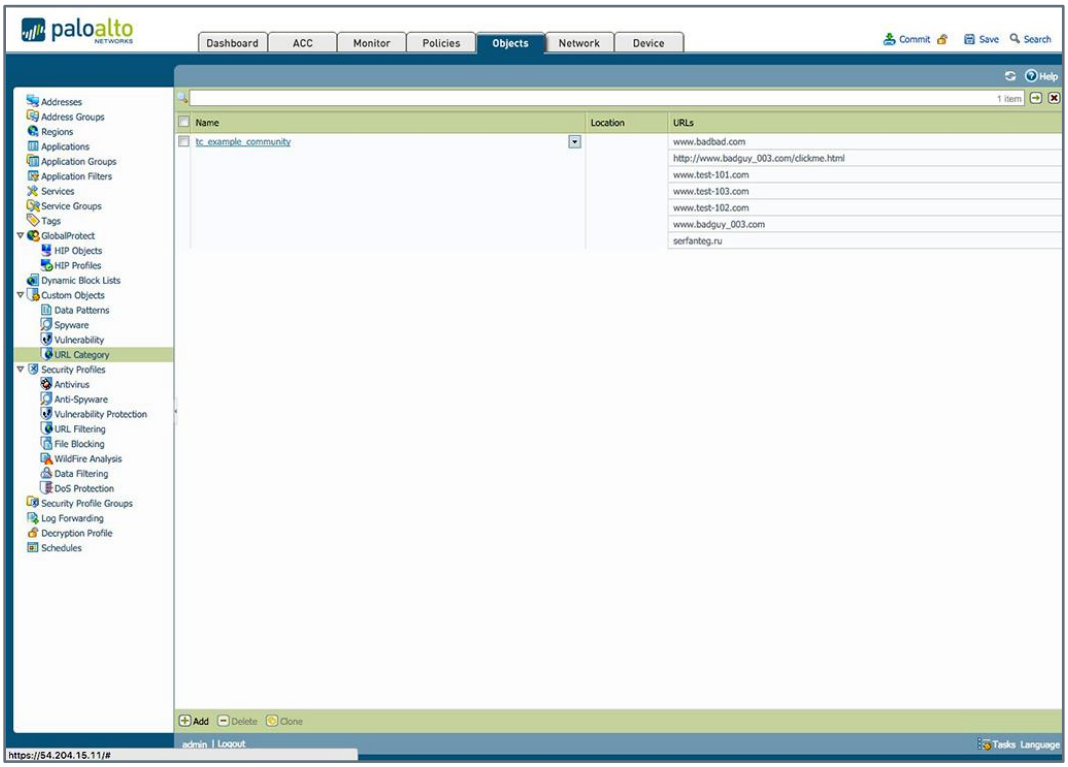

Figure 4

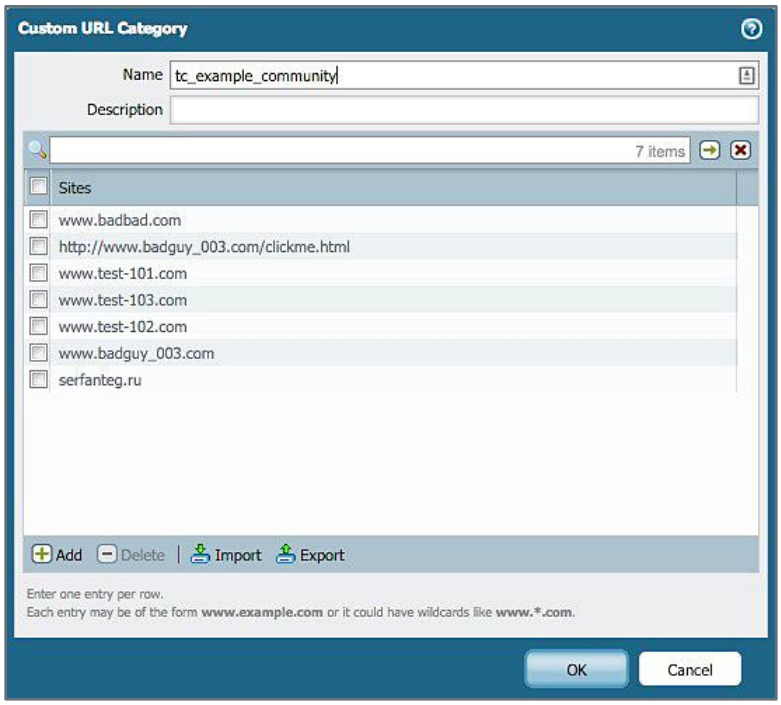
Custom URL Category
Name
tc_example_community
Description
7 items
Sites
www.badbad.com
http://www.badguy_003.com/clickme.html
www.test-101.com
www.test-103.com
www.test-102.com
www.badguy_003.com
serfanteg.ru
Add
Delete
Import
Export
Enter one entry per row.
Each entry may be of the form www.example.com or it could have wildcards like www.*.com.
OK
Cancel

Figure 5

Palo Alto URL Filters

All URL Categories can be configured under one URL filter or split between multiple URL filters, depending on the use case (Figure 6).

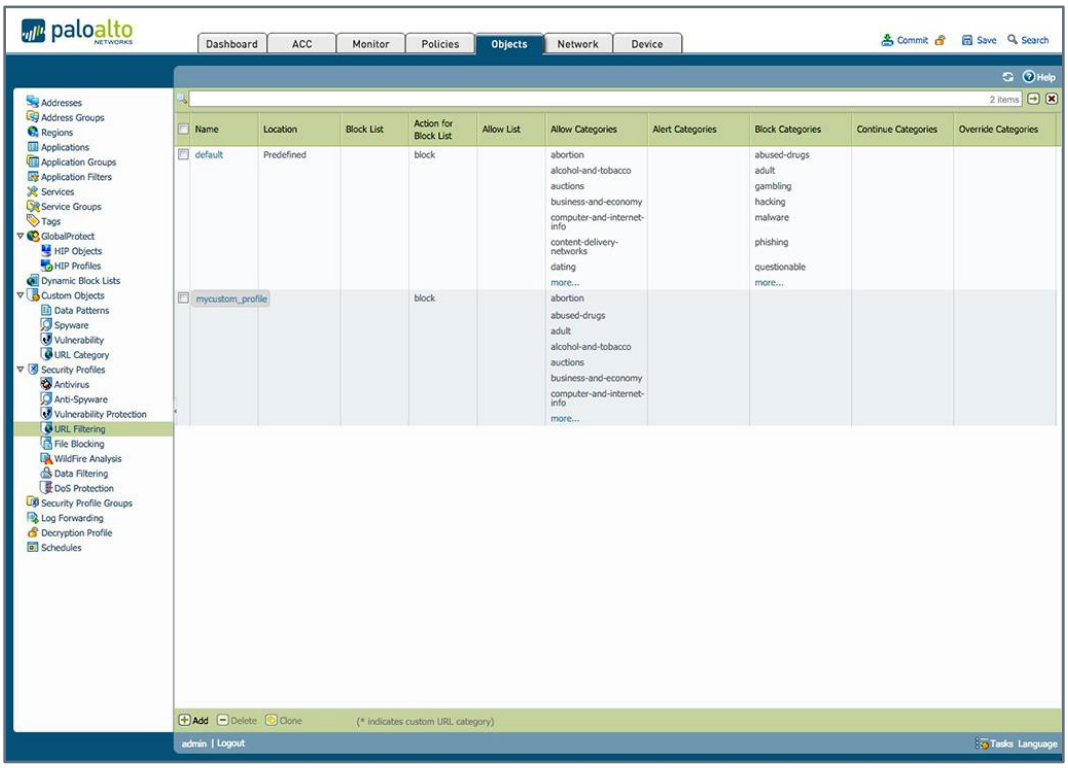

Figure 6

Palo Alto URL Filtering Profile

For each URL Category created, the action should be set in the URL filter profile to either **alert** or **block** (Figure 7).

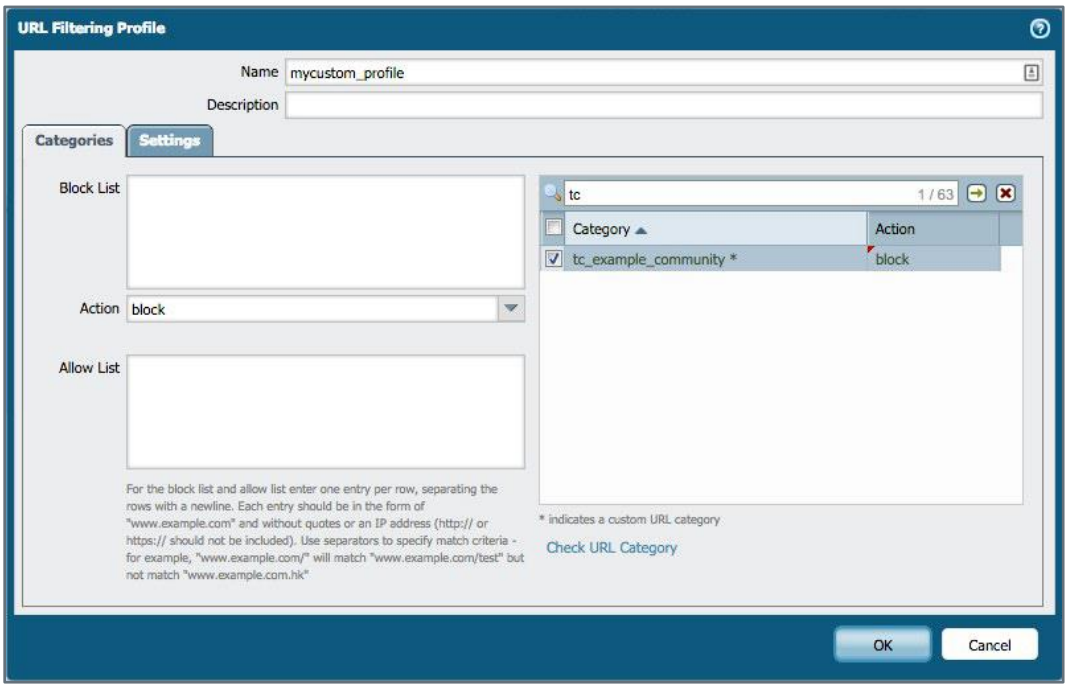

Figure 7