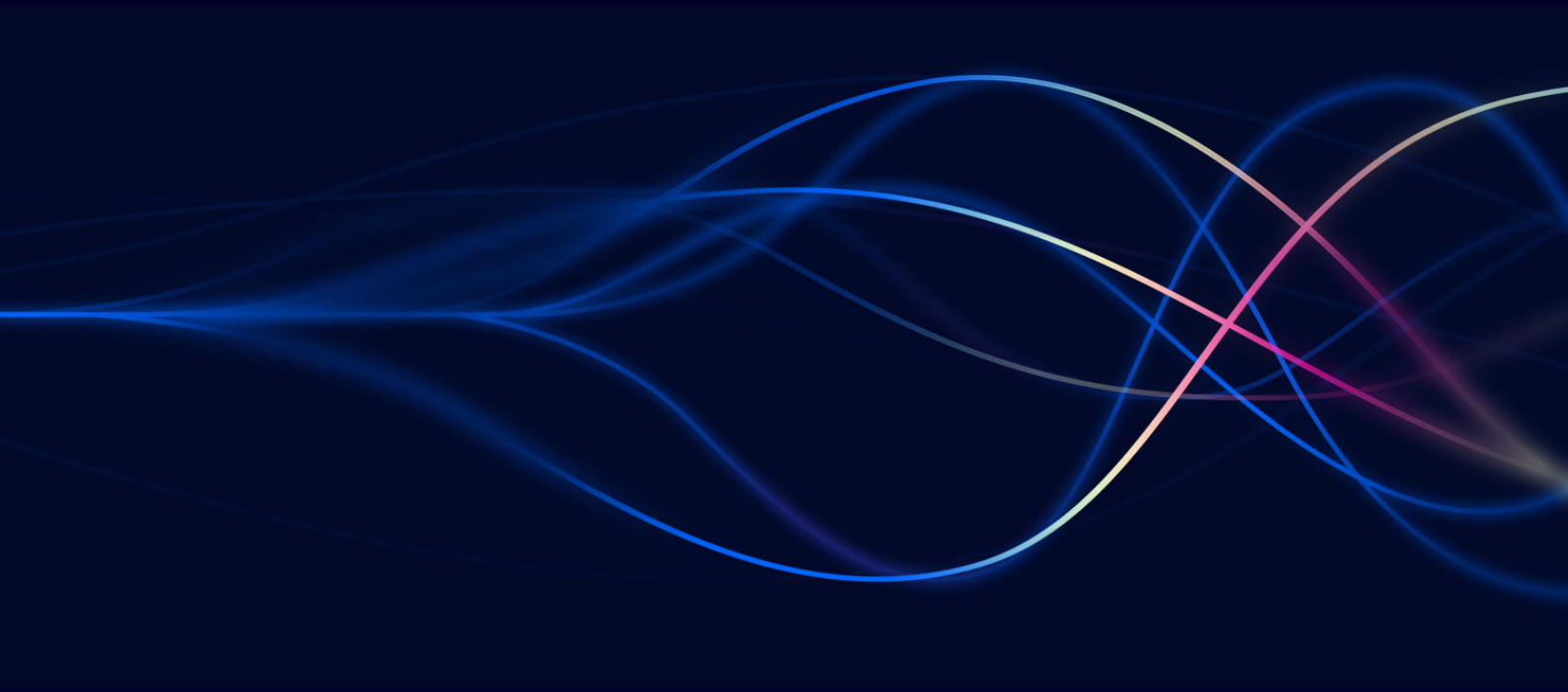
Q-FEEDS

Setup Guide
Palo Alto NGFW

Public



Version 1.0 - 12 November 2024

Introduction

In today's world, keeping your network secure is super important. Next Generation Firewalls (NGFWs) are essential tools for protecting your network. They can filter DNS and web traffic using external dynamic lists of threat indicators, known as Indicators of Compromise (IoCs).

Q-Feeds provides dynamic, up-to-date lists of these IoCs, designed specifically for use with security controls like NGFWs. By integrating Q-Feeds into your Palo Alto firewall, you can improve your network's protection against new and emerging threats. This means your firewall can automatically block harmful traffic and stay updated with the latest threat information.

This manual will show you how to set up and use Q-Feeds with your Palo Alto firewall, so you can get the best security possible. You'll learn how to configure the firewall, import Q-Feeds, and ensure everything is working correctly. With these steps, you'll be able to enhance your network's defenses and keep your data safe from cyber threats.

Using Q-Feeds for Enhanced Network Security

Q-Feeds provides dynamic lists of Indicators of Compromise (IoCs) to enhance your network security controls. These lists, based on Q-Feeds Threat Intelligence Data Feeds, are regularly updated with various types of IoCs such as IP addresses and domains. By using these lists, you can monitor and block user access to dangerous network resources effectively.

Available Lists of Indicators

Q-Feeds offers the following types of indicators:

Name	Type	Description	URI
Malware IP	IP	List of dangerous IP addresses	https://api.qfeeds.com/api?feed_type=malware_ip&limit=XXXXXX
Malware Domains	URL	List of malicious domains	https://api.qfeeds.com/api?feed_type=malware_domains&limit= XXXXXX
Phishing URLs	URL	List of phishing URLs	https://api.qfeeds.com/api?feed_type=phishing_urls&limit=XXXXXX

To optimize system performance and prevent unnecessary strain on our infrastructure, please schedule updates at the standard interval of 20 minutes. Setting the interval to less than 20 minutes is not beneficial.

Accessing the lists—including direct downloads into your network security solutions—requires an API token from Q-Feeds. You can request this token through your account manager or by visiting our website at https://qfeeds.com/start-trial-license/.

With the trial token, you will receive 30 days of free and full access to all our indicators of compromise. If you need assistance, please contact your account manager or email us at sales@qfeeds.com.

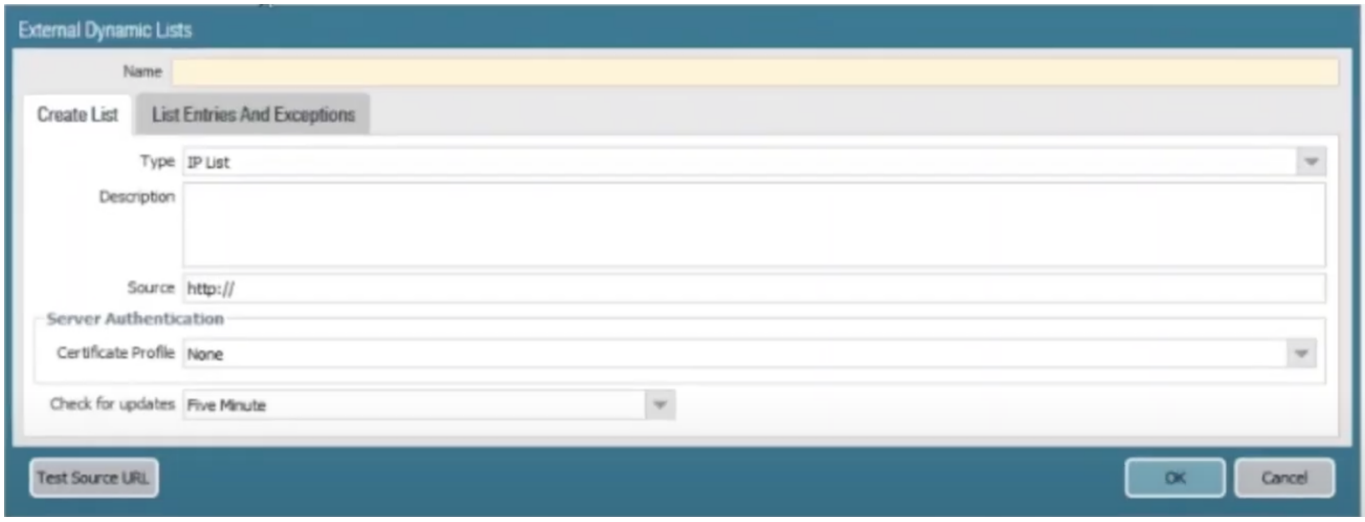
To test downloading the lists, you can use the cURL utility. Here is the syntax for Linux systems:

curl -v -u api_token:XXXXX https://api.qfeeds.com/api?feed_type=XXXX&limit=XXXXX

Setup Q-Feeds

To start we would like to refer to the documentation of Palo Alto following this link. In order to import the Q-Feed blocklists follow the steps below:

1. Open Device → Setup → Services → Service Route Configuration → Customize and edit the service External Dynamic Lists.
2. Select Objects → External Dynamic Lists
3. Select action Add and specify the name of the IoC list in the name field



4. Select the appropriate list Type as described on page 2 of this Document. For lists with Domain type it is possible to set the additional option “automatically expand to include subdomains”.
5. In the field “Source” fill in the URL as described on page 2 as well. Make sure the replace the XXXXX with your own variables. The limit variable depends on the device type:

IP address—The PA-3200 Series, PA-5200 Series, and the PA-7000 Series firewalls support a maximum of 150,000 total IP addresses; all other models support a maximum of 50,000 total IP addresses. No limits are enforced for the number of IP addresses per list. When the maximum supported IP address limit is reached on the firewall, the firewall generates a syslog message. The IP addresses in predefined IP address lists do not count toward the limit.

Model	URL List Entry Limits	Domain List Entry Limits
PA-5200 Series, PA-7000 Series (upgraded with the PA-7000 20GXM NPC, PA-7000 20GQXM NPC, or the PA-7000 100G NPC). PA-7000 appliances with mixed NPCs only support the standard capacities.	250,000	4,000,000
VM-500, VM-700	100,000	2,000,000
PA-850, PA-820, PA-3200 Series	100,000	1,000,000
PA-7000 Series (and appliances upgraded with the PA-7000 20GQ NPC or the PA-7000 20G NPC), VM-300	100,000	500,000

Model	URL List Entry Limits	Domain List Entry Limits
PA-220, VM-50, VM-50 (Lite), VM-100, VM-1000-HV	50,000	50,000

6. Download the PEM file of the API server from Q-Feeds here: https://api.qfeeds.com/download_cert_PA.php
7. You need to create a Certificate Profile. In order to do so fill in the name field and import the certificates you've downloaded in step 6. Certificate type local. This step should be repeated for all certificates you've downloaded in step 6. (could be just 1)

   If steps 6 & 7 do not work. Please follow the steps as shown in this video: https://www.youtube.com/watch?v=Vpy677VOV20

8. Select Client Authentication and specify Username and Password. The Username is "api_token" and the password is the API token provided by Q-Feeds.
9. Set the "check for updates" field to 20 minutes.
10. A new list will appear in the dynamic IP lists: Objects → External Dynamic Lists.
11. Q-Feeds can now be used within firewall policies.
12. Repeat this process for other Q-Feeds types (IPs/URLs/Domains)

Largest part of this manual is also shown in the following video: https://www.youtube.com/watch?v=QFVI4sOFoaI