kaspersky

Kaspersky Network Security Threat Data Feeds for Cisco NGFW

Version 2.0

kaspersky

Introduction

Network security controls – Next Generation Firewalls (NGFW), as a rule, possess the functionality of filtering DNS/Web traffic using external dynamic lists of IoCs.

Kaspersky offer dynamic lists, specifically designed to be used in such security controls.

Kaspersky Network Security Threat Data Feeds

Dynamic lists of IoCs from Kaspersky for network security controls are based on Kaspersky Threat Intelligence Data Feeds and contain regularly updated lists of IoCs of various types (IP addresses and domains). Using those lists it is possible to monitor/block user access to dangerous network resources.

The following lists of indicators are available:

Name	Type	Description	URI	Update frequency
Dangerous IPs	IP	List of dangerous IP addresses	https://tip.kaspersky.com/api/feeds/dangerous_ips	20
Malicious URLs	URL	List of malicious domains	https://tip.kaspersky.com/api/feeds/malicious_domains	20
Phishing URLs	URL	List of phishing domains	https://tip.kaspersky.com/api/feeds/phishing_domains	20
Botnet CnC URLs	URL	List of botnet C&C domains	https://tip.kaspersky.com/api/feeds/botnet_domains	60

In order to download the lists above (including direct downloading into network security controls) you will need an API token for Kaspersky Threat Intelligence Portal: https://tip.kaspersky.com/Help/Doc_data/en-US/ManagingAPItoken.htm (after clicking the link, close the authorization window that appears to proceed to the help page). You may request it in your account on Kaspersky Threat Intelligence Portal. After that make sure your token is configured for downloading dynamic lists of IoCs for network security controls (ask your Technical Manager or send the request to intelligence@kaspersky.com).

You may test downloading the lists using cURL utility (below is the syntax for Linux):

curl -v -u api_token:<YOUR API TOKEN> https://tip.kaspersky.com/api/feeds/dangerous_ips?limit=100

Configuring Kaspersky Network Security Threat Data Feeds in Cisco Firewall Management Center

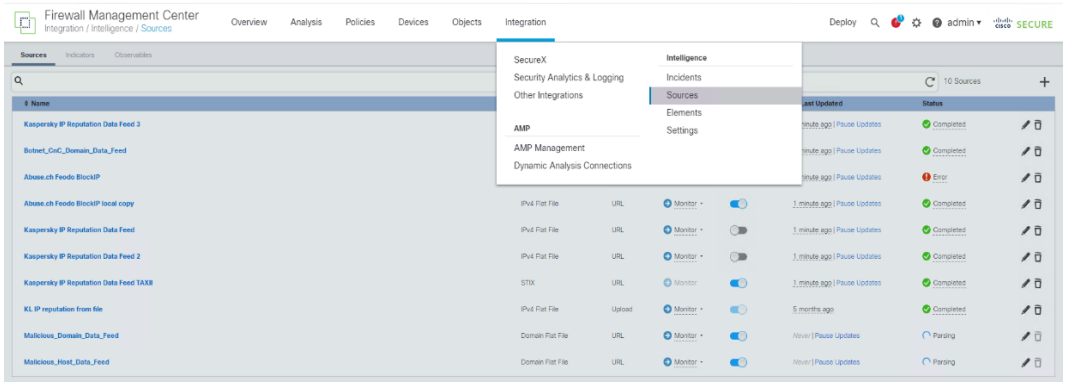
Cisco Firewall Management Center is used for managing Cisco firewalls (e.g. Cisco ASA).

Full description of external dynamic lists of IoCs configuration is available in the official documentation: https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/cisco_threat_intelligence_director.html

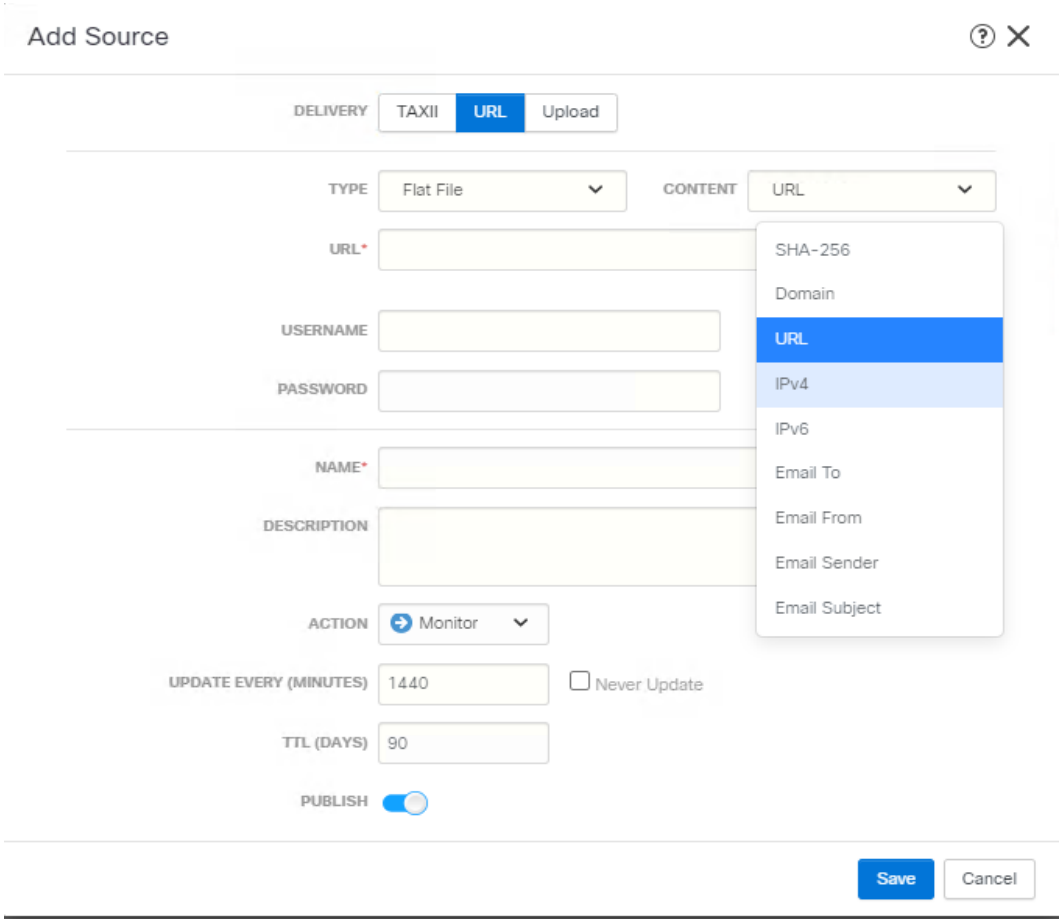
In order to import dynamic lists of IoCs from Kaspersky into Cisco Firewall Management Center follow the steps below:

1. Open web console of Cisco Firewall Management Center in your web browser.

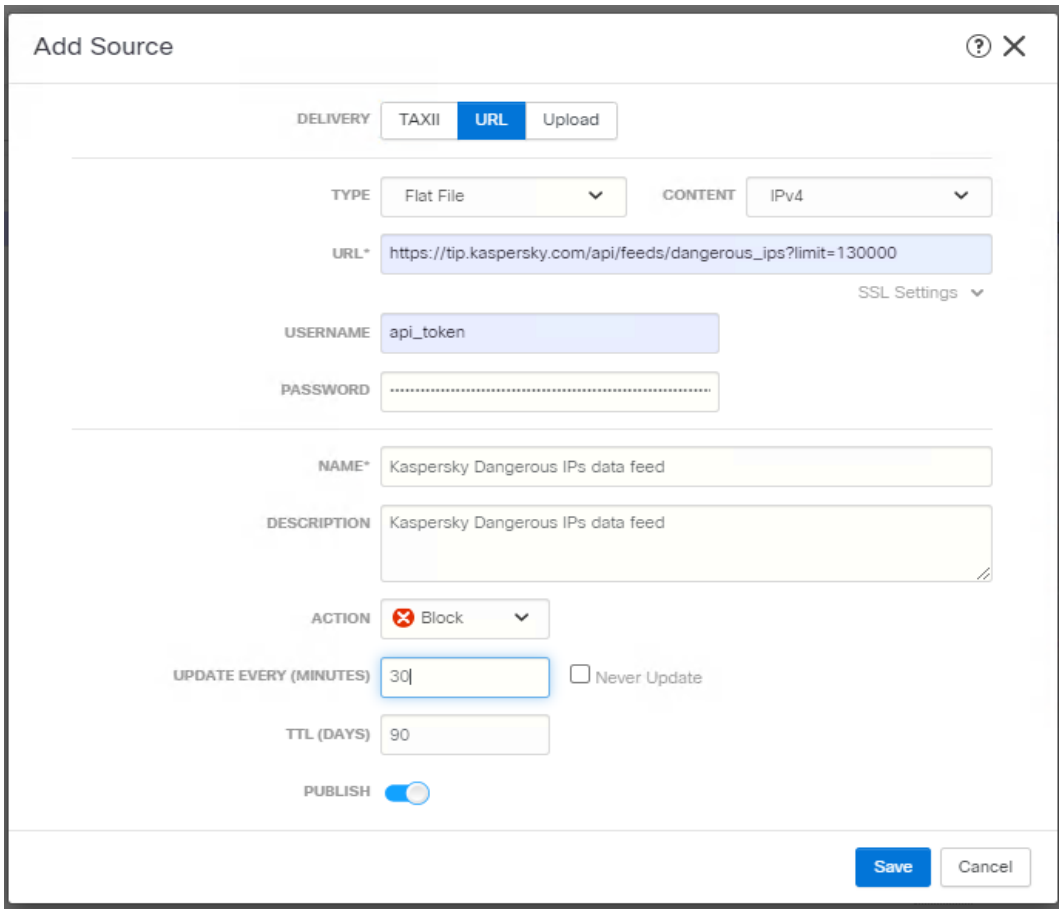
2. Go to **Integration** > **Intelligence** > **Sources**:



3. Select **Add a new source *(+)***.



4. Specify the value of the parameters:



Type: Flat File

Content: IPv4 or URL (the type is specified in the table of available lists, see above in this document)

URL: https://tip.kaspersky.com/api/feeds/dangerous_ips - URL, where the list is available

limit – the threshold on the number of IoCs actually being downloaded. This parameter is optional, if you do not specify it, all available IoCs will be downloaded. The actual number of downloaded IoCs can be less than the specified value, it depends on the number of available IoCs of certain type.

Maximum allowed dynamic list size to be imported into Cisco Firewall Management Center is: 500 Mb. Limit 130000 is given above as an example; the actual limitation should be chosen before using in production.

The full API specification for downloading dynamis lists of IoCs is available on Kaspersky Threat Intelligence Portal online documentation:https://tip.kaspersky.com/Help/api/?specId=tip-feeds-api (after clicking the link, close the authorization window that appears to proceed to the help page).

Username: api_token

Password: your API token requested in your account on Kaspersky Threat Intelligence portal

Name: Kaspersky Dangerous IP – the name of dynamic list of IoCs

Description: Kaspersky Dangerous IP data feed – optional field

Action: select the action to be performed on Cisco NGFW on the detection of IoC from the list:
- Monitor
- Block

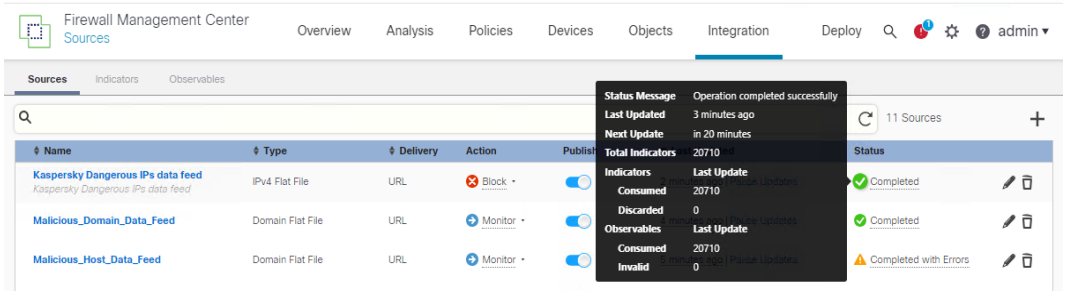
Update every (minutes): 30 – update frequency interval for the list. See the recommended frequency values for each list in the table above in this document.

TTL (days): 1

Publish: Yes

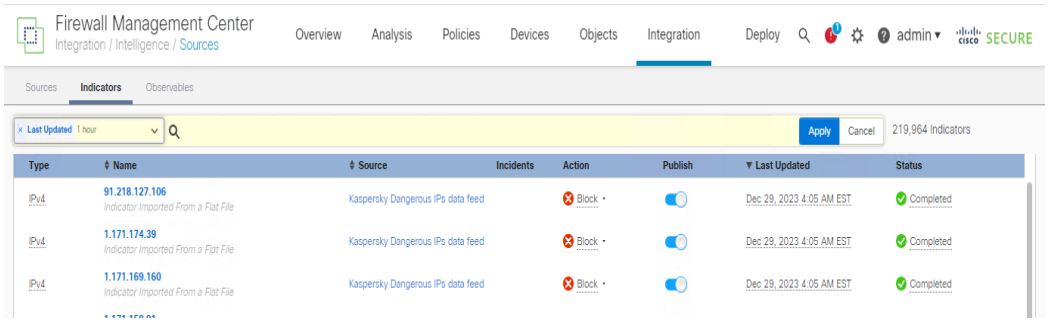
5. Press **Save.**

After that Cisco Firewall Management Center will start importing IoCs from the list and will update the list every 30 minutes. After successful import of the list the following message will be shown (status Completed and statistics of IoCs).



In order to import other lists of IoCs follow similar steps.

You can see the list of imported IoCs on **Indicators** tab:



www.kaspersky.com/
www.securelist.com