# Kaspersky Network Security Threat Data Feeds for Cisco NGFW

Version 2.0

### 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	Туре	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: <u>https://tip.kaspersky.com/Help/Doc\_data/en-US/ManagingAPItoken.htm</u> (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: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-</u> <u>v70/cisco\_threat\_intelligence\_director.html</u>

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:

Firewall Management Center Ov Integration / Intelligence / Sources	verview	Analysis	Policies	Devices	Objects	Integration			Deploy Q 💰	🔅 🞯 admin 🕶	cisco SECURE
Sources Indicators Observables						SecureX Security Analytics & Lo	gging	Intelligence Incidents		C 10 Sources	+
\$ Name						Other Integrations		Sources	ast Updated	Status	
Kasperaky IP Reputation Data Feed 3						AMP		Settings	ninute ego   Pause Updates	Completed	10
Botnet_CnC_Domain_Data_Feed						AMP Management			ninute ago   Pause Updates	Completed	10
Abuse.ch Feodo BlockIP						Dynamic Analysis Cont	rections		 tinste.ego   Pause Updates	Error	10
Abuse ch Feodo BlockIP local copy						IPv4 Flot File	URL	O Monitor -	1 minute ago   Pause Updates	Completed	10
Kaspersky IP Reputation Data Feed						IPv4 Flat File	URL	O Monitor +	1 minute ago   Pause Updates	Completed	10
Kaspersky IP Reputation Data Feed 2						IPv4 Flat File	URL	Monitor -	1 minute ago   Pause Updates	Completed	10
Kaspersky IP Reputation Data Feed TAXII						STIX	URL	O Monitor	1.minute.ego   Pause Updates	Completed	10
KL IP reputation from file						IPv4 Rat File	Upload	Monitor •	5 months ago	Ocmpleted	10
Malicious_Domain_Data_Feed						Domain Flat File	URL	O Monitor -	Never   Pause Updates	C Parsing	10
Malicious_Host_Data_Feed						Domain Flat File	URL	O Monitor -	Never   Pause Updates	C Parsing	/0

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

Add Source				?≻
DELIVERY	TAXII URL	Upload		
ТҮРЕ	Flat File	~	CONTENT	URL 🗸
URL*				SHA-256
				Domain
USERNAME				URL
PASSWORD				IPv4
				IPv6
NAME*				Email To
DESCRIPTION				Email From
				Email Sender
ACTION	🕤 Monitor 🗸 🗸			Email Subject
UPDATE EVERY (MINUTES)	1440	Neve	er Update	
TTL (DAYS)	90			
PUBLISH				
				Save

#### 4. Specify the value of the parameters:

Add Source	Ċ	Ð×
DELIVERY	TAXII URL Upload	
ТҮРЕ	Flat File V CONTENT IPv4 V	
URL*	https://tip.kaspersky.com/api/feeds/dangerous_ips?limit=130000	
	SSL Settings 🔻	-
USERNAME	api_token	
210211022		
PASSWORD		
NAME*	Kaspersky Dangerous IPs data feed	
DESCRIPTION	Kaspersky Dangerous IPs data feed	
ACTION	🔀 Block 🗸	~
UPDATE EVERY (MINUTES)	30 Never Update	
TTL (DAYS)	90	
PUBLISH		
	Save	ancel

#### Type: Flat File

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

URL: <u>https://tip.kaspersky.com/api/feeds/dangerous\_ips</u> - 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: <u>https://tip.kaspersky.com/Help/api/?specId=tip-feeds-api</u> (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).

Firewall Management Center Sources	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q 🔮	¢	🗿 admin 🔻
Sources Indicators Observables					Status Message Last Updated Next Update	Operation completed success 3 minutes ago in 20 minutes	fully C	11 Sources	•	+
¢ Name ¢	Туре	Delivery	Action	Publish	Total Indicators	20710	Stat	us		
Kaspersky Dangerous IPs data feed Kaspersky Dangerous IPs data feed	v4 Flat File	URL	Block •		Indicators Consumed	Last Update 20710	0	Completed		/ 🗇
Malicious_Domain_Data_Feed Do	omain Flat File	URL	Monitor •		Discarded Observables	0 Last Update	0	Completed		/ 🗇
Malicious_Host_Data_Feed Do	omain Flat File	URL	Monitor •		Consumed Invalid	20710 0	<b>A</b> <u>c</u>	Completed with	Errors	/ 🗇

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

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

Firev Integra	Nall Management Center ation / Intelligence / Sources	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q 💕	¢	🕘 admin 🔻	cisco SECURE
Sources II	ndicators Observables											
× Last Updated 11	Q vuor								Apply	Cancel	219,964 Indi	cators
Туре	\$ Name	¢ :	Source		Incidents	Action	Publish	▼ Last Upda	ated		Status	
IPv4	91.218.127.106 Indicator Imported From a Flat File	Ка	spersky Dangerou	us IPs data feed		Block •		Dec 29, 202	3 4:05 AM E	ST	Complete	id I
IPv4	1.171.174.39 Indicator Imported From a Flat File	Ка	spersky Dangerou	us IPs data feed		Block -		Dec 29, 202	3 4:05 AM E	ST	Complete	d
IPv4	1.171.169.160 Indicator Imported From a Flat File	Ка	spersky Dangerou	us IPs data feed		Block •		Dec 29, 202	3 4:05 AM E	ST	Complete	id.
	1 171 150 01											



www.kaspersky.com/ www.securelist.com

© 2024 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners