Kaspersky Network Security Threat Data Feeds for FortiGate

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

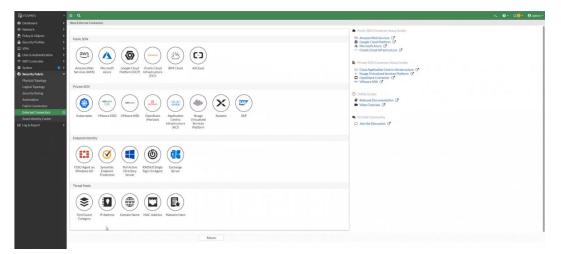
Configuring Kaspersky Network Security Threat Data Feeds in FortiGate NGFW

FortiGate NGFW is based on FortiOS operation system. Starting from the version 6.0 FortiOS supports external dynamic lists of IoCs in the form of updateable text files located on a web server, accessible via HTTP/HTTPs.

After importing IoCs into FortiGate it is possible to use them in various policies depending on IoC type: Web Filter, DNS Filter, Antivirus Profile, and also as Source/Destination in IPv4 and proxy policies.

The detailed description and the examples are specified in the official Fortinet documentation: <u>https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/9463/threat-feeds</u>

In order to add new source of dynamic lists into FortiGate, it is required to open the section **Security Fabric > External Connectors** and press **Create new**.



Then it is needed to select the Connector type depending on the IoC type:

- IP address for IP Address list.
- Domain name or FortiGuard Category Based Filter for URL list.

It is possible to create any number of dynamic lists in FortiOS without limitation.

FGVM01	-	≡ Q.			>_ 😯 ▾ 🗘 2 ▾ 😝 admin ▾
Dashboard		New External Connector			
Network					Additional Information
💄 Policy & Objects					API Preview
Security Profiles		Threat Feeds			C API Preview
묘 VPN					Public SDN Connector Setup Guides
User & Authentication					Mazon Web Services
↔ WiFi Controller					Google Cloud Platform C
🏟 System		IP Address			▲ Microsoft Azure → Oracle Cloud Infrastructure
Security Fabric					
Physical Topology		Connector Settings			Private SDN Connector Setup Guides
Logical Topology		Status	Enabled Obsabled		 Cisco Application Centric Infrastructure Nuage Virtualized Services Platform
Security Rating		Name 🚯			OpenStack Connector C
Automation		Update method 🚯	External Feed Push API		NSX VMware NSX 🖸
Fabric Connectors		URL of external resource ()			⑦ Online Guides
External Connectors		HTTP basic authentication C)		Relevant Documentation C
Asset Identity Center		Username	api_token		Video Tutorials 🖸
Log & Report		Password	•••••	۲	Fortinet Community
		Refresh rate	5		Join the Discussion
			Minutes (1 - 43200)		C Join the Discussion 🖸
		Comments	h	0/255	
			OK Cancel		
FCRTINET					

Set the values for the following parameters:

- Name list name e.g., Dangerous IPs List
- **URI of external resource** the link to the list on Kaspersky Threat Intelligence Portal, e.g. <u>https://tip.kaspersky.com/api/feeds/botnet_domains?limit=130000</u>

limit – the threshold on the number of IoCs actually being downloaded. This parameter is optional, however it is recommended to use it in order to fit the allowed list capacity. Otherwise all available IoCs will be downloaded and it may not be accepted by the appliance.

Maximum allowed dynamic list size for FortiGate is: 10 MB or 128×1024 (131072) IoCs. So it is recommended to set limit=130000. The actual number of downloaded IoCs can be less, it depends on the number of available IoCs of certain type.

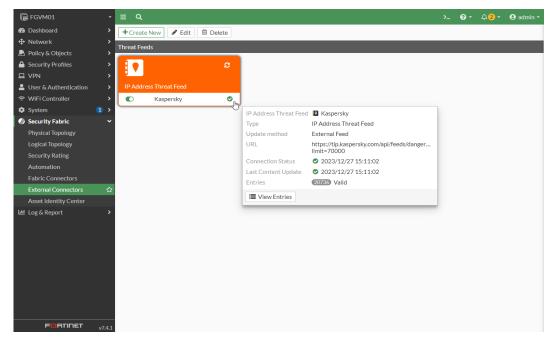
The full API specification for downloading dynamis lists of IoCs is available on Kaspersky Threat Intelligence Portal online documentation: <u>https://tip.kaspersky.com/Help/api/?specId=tip-feeds-api</u> (after clicking the link, close the authorization window that appears to proceed to the help page).

• **HTTP basic authentication** – switch on for authorization via API and specify your Username and Password:

Username	api_token
Password	Your API token requested from your account in Kaspersky Threat Intelligence Portal

- Refresh rate list update frequency in minutes (see recommended values in the table above)
- **Comments** comments (the field is optional)
- Status switch on

After filling in all the required settings press "Ok", the connector will be created:



a Dashboard 🔹 💦		IP Address Threat Feed Kaspersky	
Notwork	reat Feeds	O Q. Search	Q. 200733 Valid () m
Policy & Objects >		Entry	Validity
Security Profiles >	۵ 🕈	80.66.79.247	S Valid
VPN >		213.109.202.154	© Valid
		213.109.202.134	S Valid
System (1)	C Kaspersky O		© Valid
Security Fabric Y		185.222.57.147	
Physical Topology		104.21.90.125	S Valid
Logical Topology		45.137.22.229	O Valid
Security Rating		45.125.66.19	Valid
Automation		141.98.11.96	🖉 Valid
Fabric Connectors		185.222.58.238	Valid
External Connectors 📅		62.204.41.230	S Valid
Asset Identity Center		91.92.247.130	S Valid
Log & Report >		185.222.57.90	Valid
		141.98.10.127	🖉 Valid
		141.98.10.87	🖉 Valid
		45.137.22.182	🖉 Valid
		141.98.10.86	🖉 Valid
		45.137.22.107	S Valid
		79.137.202.179	S Valid
		176.97.210.185	S Valid
		185.222.57.75	S Valid
		91.92.250.14	S Valid
		45.137.22.113	Valid
		95.214.26.35	© Valid
		185.155.184.208	© Volid
		163.135.164.208	♥ Valid
		172.67.156.164	Valid

After importing the list it is possible to use it in policies such as Web Filter, DNS, Firewall, Antivirus profile, and also for Source/Destination in IPv4 and proxy policies:

FGVM01 •					>_ 😧 •
Dashboard	New DNS Filter Profile				
Network			Select Entries	×	FortIGate
Policy & Objects >	Name	DNS_Security_Kaspersky		+ Create	FGVM01
🚔 Security Profiles 🛛 🗸	Comments	Comments // 0/255	Kaspersky	I CICULC	
AntiVirus	Redirect botnet C&C requests to Block Portal		- Hooporoky		Additional Information
Web Filter	Enforce 'Safe Search' on Google, Bing, YouTube 🖸	•			API Preview
DNS Fliter ☆					% References
Application Control	FortiGuard Category Based Filter				
Intrusion Prevention	Static Domain Filter				② Online Guides
File Filter	Domain Filter				Relevant Documentation 🗹
SSL/SSH Inspection	External IP Block Lists Kaspersky	×			Video Tutoriais C
Application Signatures	+	^			Second Se
IPS Signatures	DNS Translation ()				○ Join the Discussion
Web Rating Overrides					C Jon the Distance (B
Web Profile Overrides	Options				
묘 VPN >	Redirect Portai IP	Use FortiGuard Default Specify			
🚨 User & Authentication 🔷 🔸					
♥ WiFi Controller >	Allow DNS requests when a rating error occurs				
🕸 System 🔹 🕽 🕨	Log all DNS queries and responses	•			
Security Fabric >					
ഥ Log & Report >					
			Close		
			Ciose		
FURTINET V7.4.1		OK Cancel			

🕞 FGVM01 -												
De Dashboard →	+	DRW Q. Policy match	Edit Policy									
₽ Network >							Contract Inc.	ics (since last re-				
Policy & Objects ~							ID		1			
Firewall Policy th			Name 0	Internet Access								
IPv4 DoS Policy			Incoming Interface	Inn (port2)	-			t used	47 day(s) ago			
Addresses			Outgoing Interface	wan (port1)	*			t used	47 day(s) ago			
Internet Service Detabase			Source	u all +	*		Act	ive sessions	0			
Services		Sedit 🗔	Destination	🖾 sli	×		Filt	count	730			
Schedules				+			Tot	al bytes	93.01 MB			
Virtual IPs			Schedule	Co always	-		Cur	rent bandwidth	Obps			
IP Pools			Service	CO ALL	ж		10	Clear Counters				
Protocol Options			Action	ACCEPT O DENY								
Trathc Shaping												
Socurity Profiles >			Firewall/Network Op	tions			Last 7 125 M	Days Bytes *				
VPN ≻ User & Authentication >			NAT	•			100 M			Ji SPU	.l. Software	
Will Controller >			IP Pool Configuration	Use Outgoing Interfac	e Address	e Dynamic IP Pool	25 M			1	1	
System 3			Preserve Source Port				50 M					
Socurity Fabric			Protocol Options	enor default	-	/						
Log & Report >							25 M					
rod a prime b			Security Profiles				01		1 Dec 22 Dec 23			
				C default	-	•		DREAD DREA	a these these	1.000204 1.000	25 LINE 26 LINE	
				DNS_Socurity_I								
			Application Control		Kasporsky •		Additi	real Information				
				3				API Proview				
							90	References				
			55L Inspection	certificate-insp			2	Edit in CLI				
			554 inspection	certificate-insp	ection •	·						
			Logging Options				00	illne Guldes				
			Los Allowed Torffe	Security	Events All	s suite an an		belevant Docum				
			Generate Logs when					/ideo Tutorials (2 Icy Continuatio			
			Capture Packets	0			-	onsonoated Pol	icy configuratio	n LIS.		
							🗨 Fo	rtinct Communi	EV.			
	-				ж	Cancel						

For proper feeds functioning, do not enable **FortiGuard Category Based Filter** concurrently in several profiles of DNS filter (default profile and additionally created profiles).

Dashboard	>	+ Create New / Edit Ta Clone B Delete Search		Edit DNS Filter Profile	
Security Fabric	>	Name =			Kaspersky IP
• Network	>			Name	
System (•	Chos Kaspersky IP		Comments	Comments 0/25
Policy & Objects	>	EASE default	Default dns fil	Redirect botnet C&C requests to Block Portal	0
Security Profiles	~			Enforce 'Safe Search' on Google, Bing, YouTube	3
AntiVirus				FortiGuard Category Based Filter	
Web Filter					
DNS Filter	合			Static Domain Filter	
Application Control				Domain Filter	
File Filter				External IP Block Lists 💿 📱 kaspersky - IP	- Feed 🛛 🗶
SSL/SSH Inspection				DNS Translation 0	
Application Signatures				DNS Translation ()	
Web Rating Overrides				Options	
Web Profile Overrides				Redirect Portal IP	Use FortiGuard Default Specify
2 VPN					208.91.112.55
User & Authentication				Allow DNS requests when a rating error occurs	0
WiFi & Switch Controller	>			Log all DNS queries and responses	3
Log & Report					
LOG OL NEDOLI	~				
					OK Cancel



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