kaspersky

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	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
```

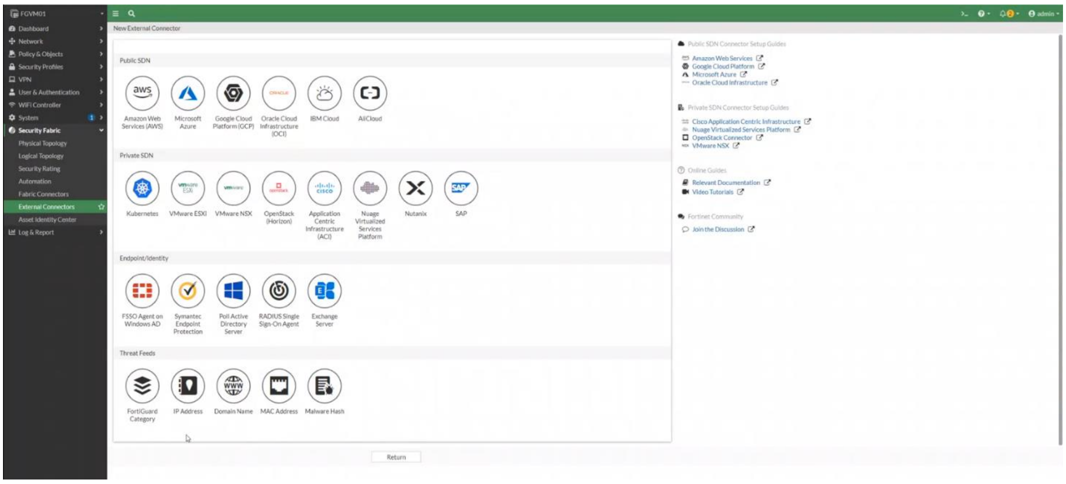
Configuring Kaspersky Network Security Threat Data Feeds in FortiGate NGFW

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: https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/9463/threat-feeds

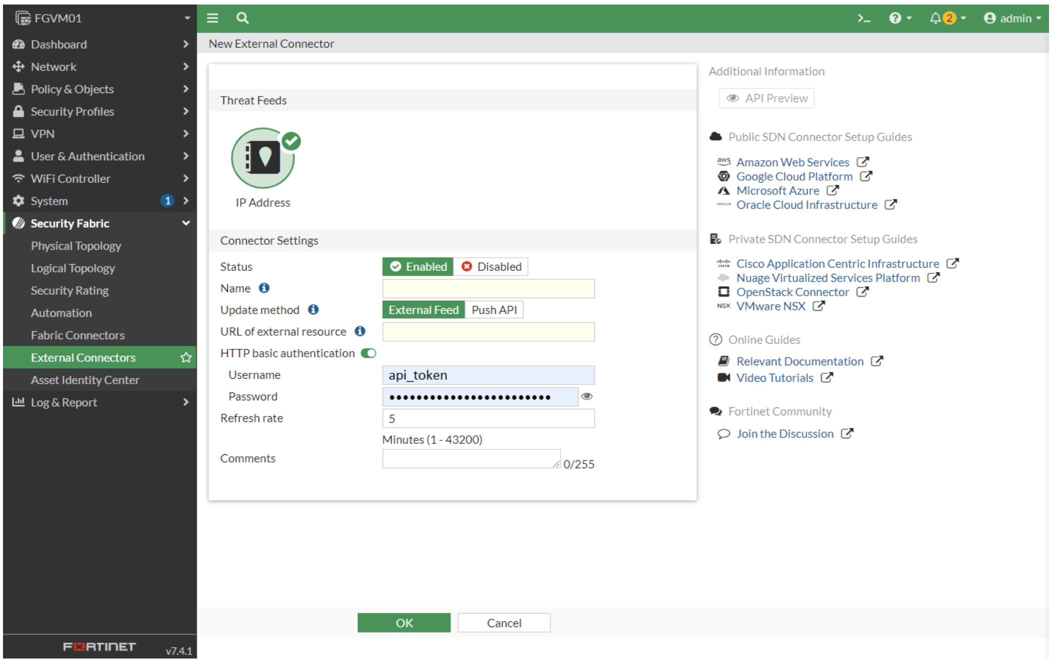
In order to add new source of dynamic lists into FortiGate, it is required to open the section **Security Fabric > External Connectors** and press **Create new**.



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.



New External Connector

Threat Feeds

IP Address

Connector Settings

Status	[✓ Enabled] Disabled
Name	
Update method	[✓ External Feed] Push API
URL of external resource	
HTTP basic authentication	●
Username	api_token
Password	••••••••••••••••••••••••
Refresh rate	5 Minutes (1 - 43200)
Comments	0/255

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. https://tip.kaspersky.com/api/feeds/botnet_domains?limit=130000

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.

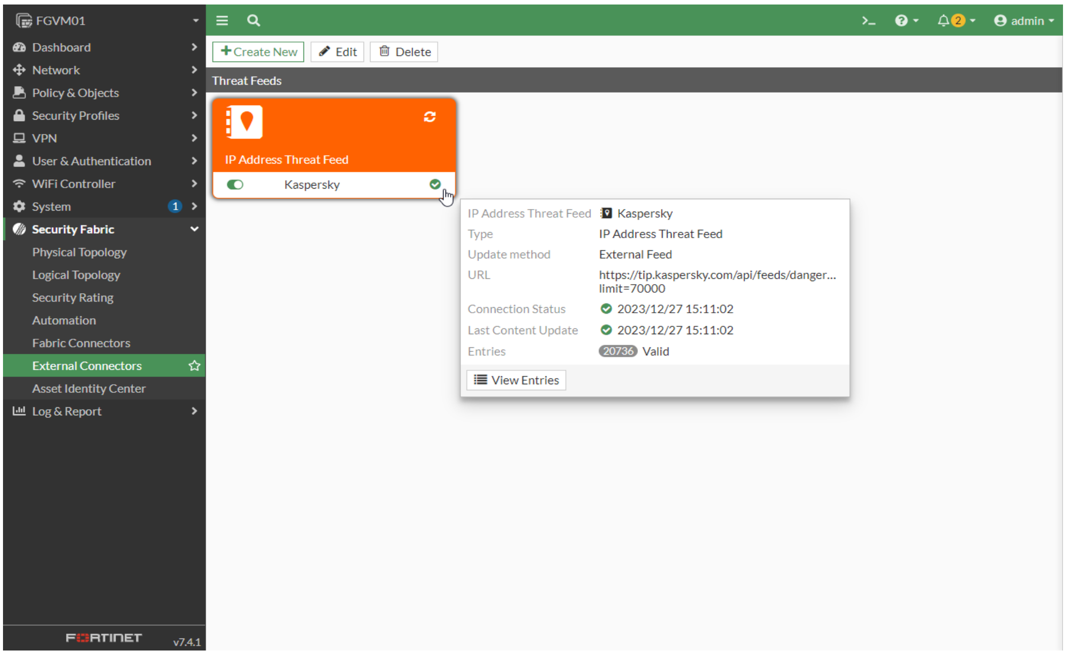
The full API specification for downloading dynamis lists of IoCs is available on Kaspersky Threat Intelligence Portal online documentation:https://tip.kaspersky.com/Help/api/?specId=tip-feeds-api (after clicking the link, close the authorization window that appears to proceed to the help page).

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

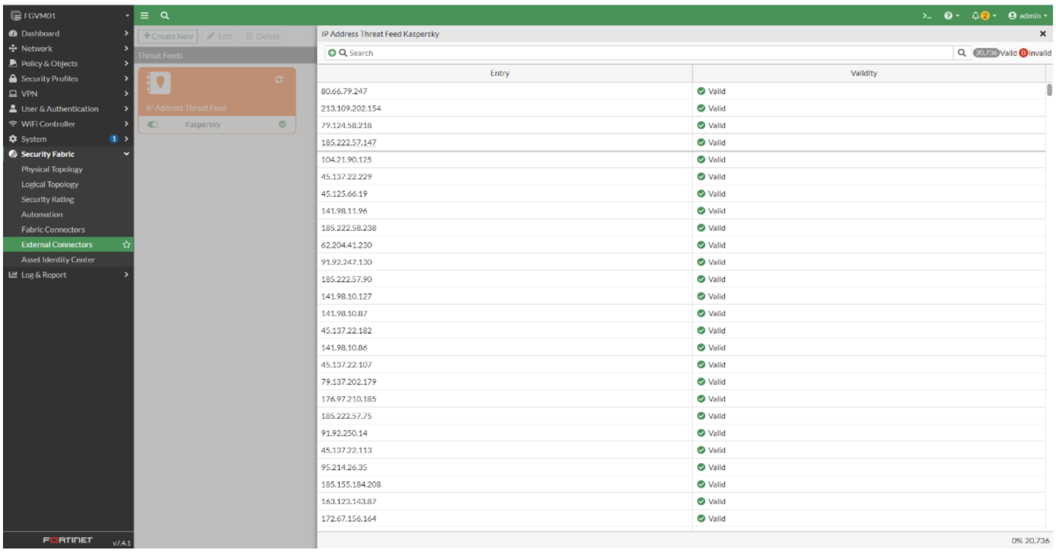
Username	api_token
Password	Your API token requested from your account in Kaspersky Threat Intelligence Portal

- **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:



IP Address Threat Feed	Kaspersky
Type	IP Address Threat Feed
Update method	External Feed
URL	https://tip.kaspersky.com/api/feeds/danger... limit=70000
Connection Status	✓ 2023/12/27 15:11:02
Last Content Update	✓ 2023/12/27 15:11:02
Entries	20736 Valid



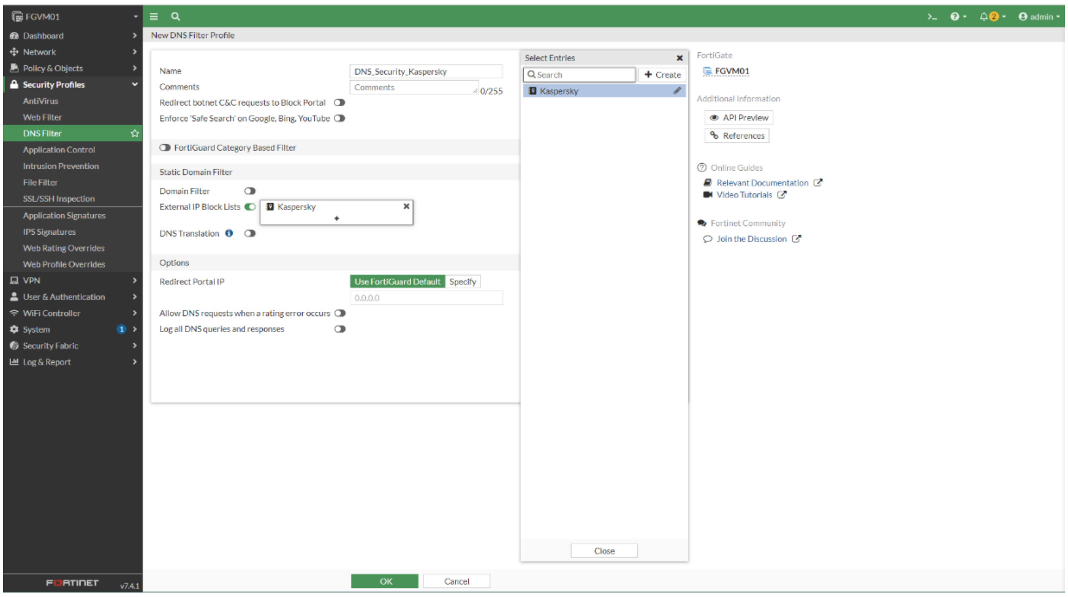
IP Address Threat Feed Kaspersky

Search — 20,736 Valid 0 Invalid

Entry	Validity
80.66.79.247	✓ Valid
213.109.202.154	✓ Valid
79.124.58.218	✓ Valid
185.222.57.147	✓ Valid
104.21.90.125	✓ Valid
45.137.22.229	✓ Valid
45.125.66.19	✓ Valid
141.98.11.96	✓ Valid
185.222.58.238	✓ Valid
62.204.41.230	✓ Valid
91.92.247.130	✓ Valid
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	✓ Valid
79.137.202.179	✓ Valid
176.97.210.185	✓ Valid
185.222.57.75	✓ Valid
91.92.250.14	✓ Valid
45.137.22.113	✓ Valid
95.214.26.35	✓ Valid
185.155.184.208	✓ Valid
163.123.143.87	✓ Valid
172.67.156.164	✓ Valid

0% 20,736

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:



New DNS Filter Profile

Name: DNS_Security_Kaspersky
Comments: Comments 0/255
Redirect botnet C&C requests to Block Portal ○
Enforce 'Safe Search' on Google, Bing, YouTube ○

○ FortiGuard Category Based Filter

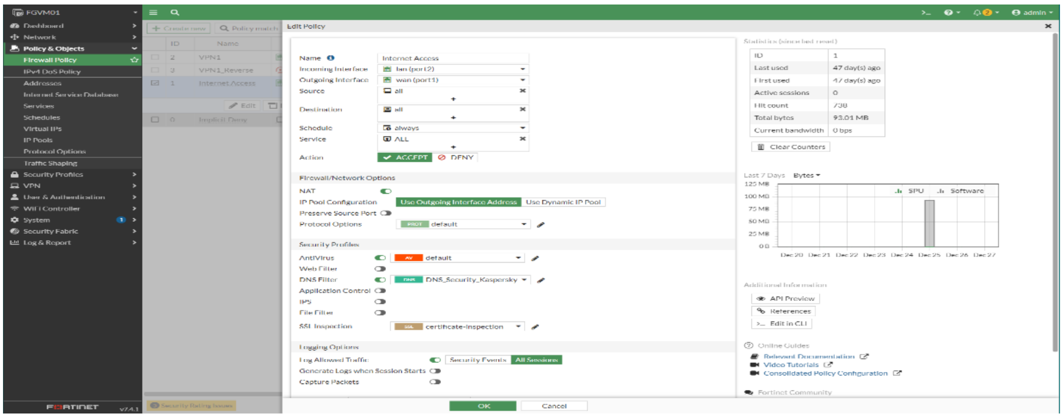
Static Domain Filter

Domain Filter ○
External IP Block Lists ● Kaspersky
DNS Translation ○

Options

Redirect Portal IP: [✓ Use FortiGuard Default] Specify — 0.0.0.0
Allow DNS requests when a rating error occurs ○
Log all DNS queries and responses ○

Select Entries — Search — Create — Kaspersky — Close



Edit Policy

Name: Internet Access
Incoming Interface: lan (port2)
Outgoing Interface: wan (port1)
Source: all
Destination: all
Schedule: always
Service: ALL
Action: [✓ ACCEPT] DENY

Firewall/Network Options

NAT ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options: PROT default

Security Profiles

AntiVirus ● AV default
Web Filter ○
DNS Filter ● DNS DNS_Security_Kaspersky
Application Control ○
IPS ○
File Filter ○
SSL Inspection: SSL certificate-inspection

Logging Options

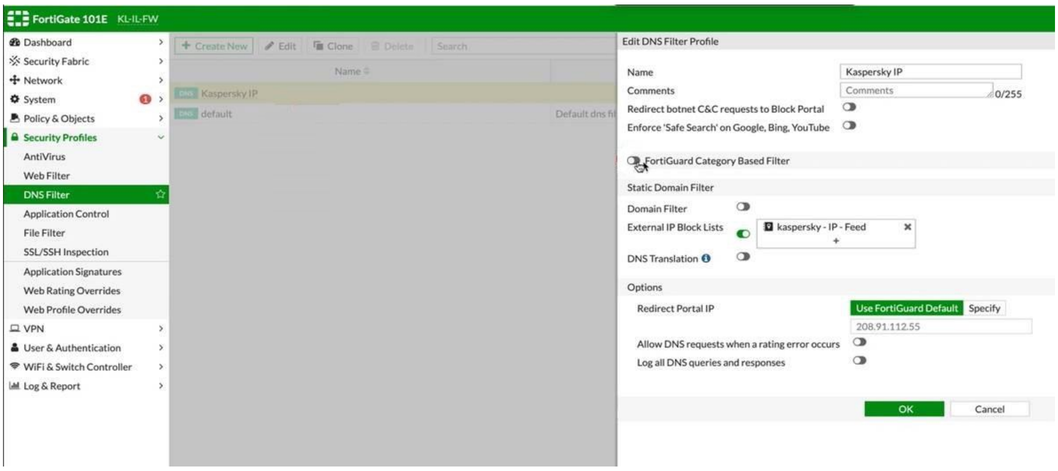
Log Allowed Traffic ● Security Events [✓ All Sessions]
Generate Logs when Session Starts ○
Capture Packets ○

Statistics (since last reset)

ID	1
Last used	47 day(s) ago
First used	47 day(s) ago
Active sessions	0
Hit count	738
Total bytes	93.01 MB
Current bandwidth	0 bps

Clear Counters

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



Edit DNS Filter Profile

Name: Kaspersky IP

Comments: Comments 0/255

Redirect botnet C&C requests to Block Portal ○

Enforce 'Safe Search' on Google, Bing, YouTube ○

○ FortiGuard Category Based Filter

Static Domain Filter

Domain Filter ○

External IP Block Lists ● kaspersky - IP - Feed ✕ +

DNS Translation ○

Options

Redirect Portal IP: [✓ Use FortiGuard Default] Specify

208.91.112.55

Allow DNS requests when a rating error occurs ○

Log all DNS queries and responses ○

OK Cancel

www.kaspersky.com/
www.securelist.com