kaspersky

# Kaspersky Network Security Threat Data Feeds для FortiGate

Версия 2.0

kaspersky

# Введение

Сетевые средства защиты – Next Generation Firewalls (NGFW), как правило, имеют функциональность фильтрации DNS/Web траффика с возможностью подключения внешних динамически обновляемых списков индикаторов компрометации.

«Лаборатория Касперского» предлагает динамически обновляемые списки индикаторов, специально разработанные для использования в таких сетевых средствах защиты.

# Потоки данных об угрозах для сетевых средств защиты «Лаборатории Касперского»

Списки индикаторов «Лаборатории Касперского» для сетевых средств защиты основаны на потоках данных об угрозах (фидах) и содержат в себе регулярно обновляемые списки индикаторов различных типов (IP-адреса, домены), с помощью которых возможно ограничить доступ к опасным ресурсам.

Доступные для загрузки следующие списки индикаторов:

| Название | Тип списка | Описание | Ссылка (URI) | Обновление, мин |
|---|---|---|---|---|
| Dangerous IPs | IP | Список опасных IP адресов | https://tip.kaspersky.com/api/feeds/dangerous_ips | 20 |
| Malicious URLs | URL | Список вредоносных доменов | https://tip.kaspersky.com/api/feeds/malicious_domains | 20 |
| Phishing URLs | URL | Список фишинговых доменов | https://tip.kaspersky.com/api/feeds/phishing_domains | 20 |
| Botnet CnC URLs | URL | Список доменов командных центров ботнетов | https://tip.kaspersky.com/api/feeds/botnet_domains | 60 |

Для возможности скачивания указанных списков индикаторов (в том числе непосредственно в сетевые средства защиты) вам потребуется API токен к Threat Intelligence порталу "Лаборатории Касперского": https://tip.kaspersky.com/Help/Doc_data/en-US/ManagingAPItoken.htm (после нажатия на ссылку закройте появившееся окно авторизации с просьбой ввести логин и пароль и перейдите на страницу справки). Данный токен вы можете запросить в вашем персональном аккаунте на Threat Intelligence портале "Лаборатории Касперского", а настроить его на доступ к указанным спискам вам поможет ваш технический менеджер "Лаборатории Касперского". Если у вас нет выделенного технического менеджера, вы можете отправьте запрос на intelligence@kaspersky.com.

Вы можете скачать списки с помощью утилиты cURL (ниже представлен синтаксис команды для Linux):

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

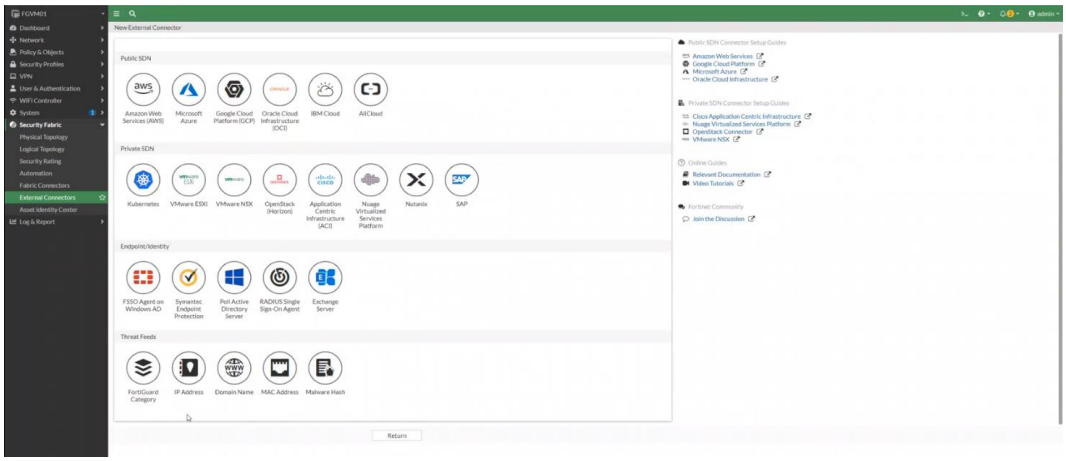
kaspersky

# Подключение потоков данных об угрозах для сетевых средств защиты к FortiGate NGFW

FortiGate NGFW реализован на базе операционной системы FortiOS. Начиная с версии 6.0, в FortiOS имеется поддержка внешних динамически обновляемых списков индикаторов (IP, URL, hash) в виде текстовых файлов, загружаемых с внешнего HTTP- или HTTPS-сервера.

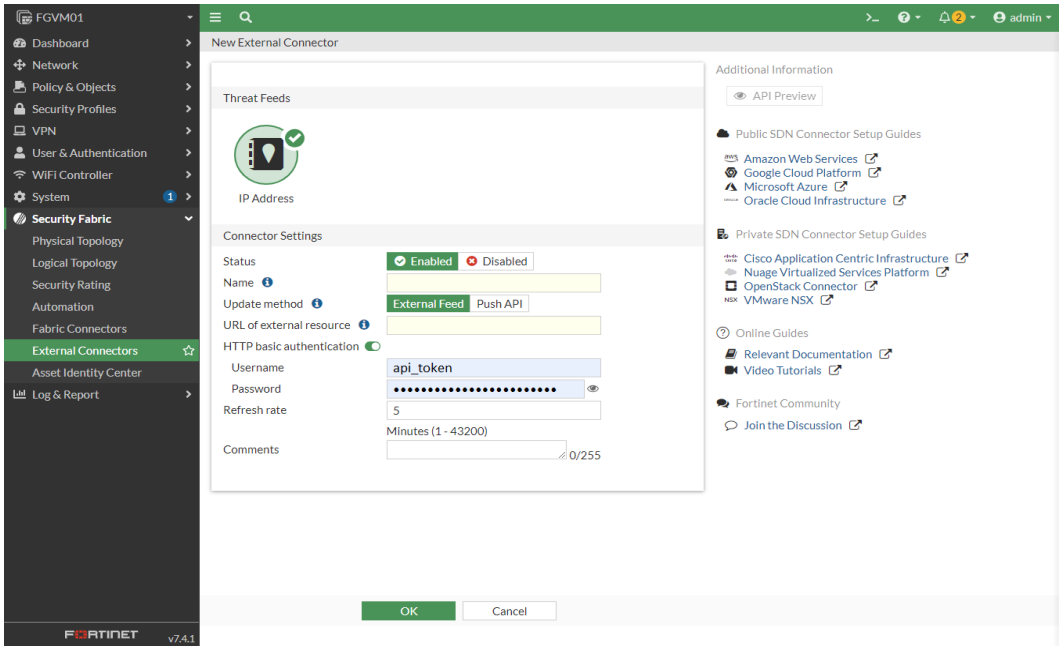
После загрузки в FortiOS списков индикаторов, в зависимости от типа, индикаторы могут быть использованы в политиках Web Filter, DNS Filter, Antivirus Profile, а также в качестве Source/Destination в политиках IPv4 и прокси. Подробное описание и примеры приведены в официальной документации Fortinet: https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/9463/threat-feeds

Для того, чтобы добавить новый источник для динамически обновляемых списков в FortiGate, необходимо перейти в раздел **Security Fabric > External Connectors** и нажать **Create new**.



Затем необходимо выбрать тип источника в зависимости от типа списка индикаторов:
- IP address – для IP списков.
- Domain name или FortiGuard Category Based Filter – для URL списков.

Для FortiOS можно создавать неограниченное количество динамически обновляемых списков индикаторов.




В окне настроек для источника динамически обновляемого списка необходимо заполнить поля:

- **Name** - название списка индикаторов, например, Botnet CnC URLs feed
- **URI of external resource** - путь к источнику, например https://tip.kaspersky.com/api/feeds/botnet_domains?limit=130000

limit – ограничение на количество записей, которое будет загружено. Параметр limit необязателен, но если его не указать - загрузятся все записи, которые есть на текущий момент в источнике.

Максимальный размер динамически обновляемого списка индикаторов, который можно загрузить в устройство: 10 MB или 128×1024 (131072) записей, поэтому рекомендуется указывать ограничение в 130000 записей. Итоговое количество скачанных записей об индикаторах может быть меньше, если в источнике содержится меньшее количество записей.

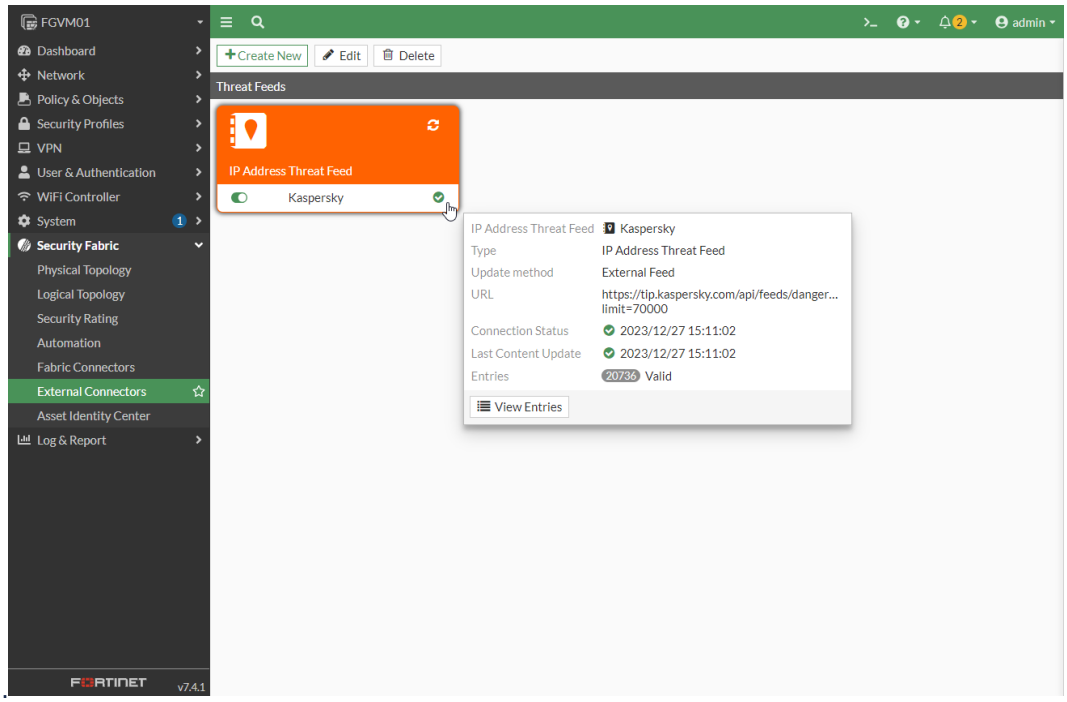
Полная спецификация API доступна по ссылке: https://tip.kaspersky.com/Help/api/?specId=tip-feeds-api (после нажатия на ссылку закройте появившееся окно авторизации с просьбой ввести логин и пароль и перейдите на страницу справки).

- **HTTP basic authentication** - необходимо включить для авторизации через API и указать данные, полученные у технического менеджера.

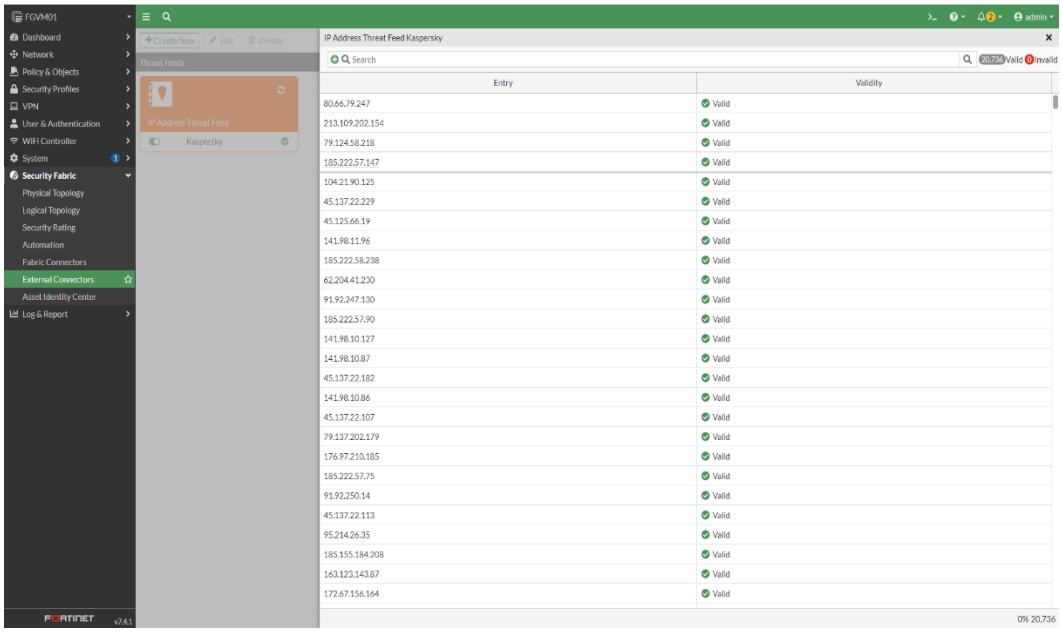
| | |
|---|---|
| **Username** | api_token |
| **Password** | Токен для доступа к API, запрошенный через Threat Intelligence портал |

- **Refresh rate** - период обновления списка в минутах, рекомендуемые значения указаны в таблице
- **Comments** - комментарии (опционально)
- **Status** - включить

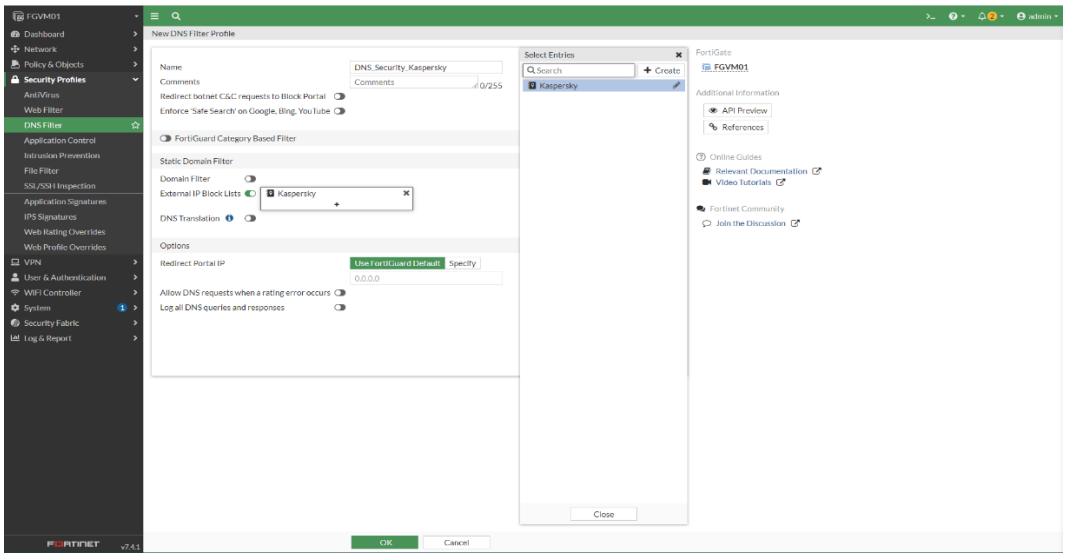
После заполнения всех необходимых полей нажать «ОК»

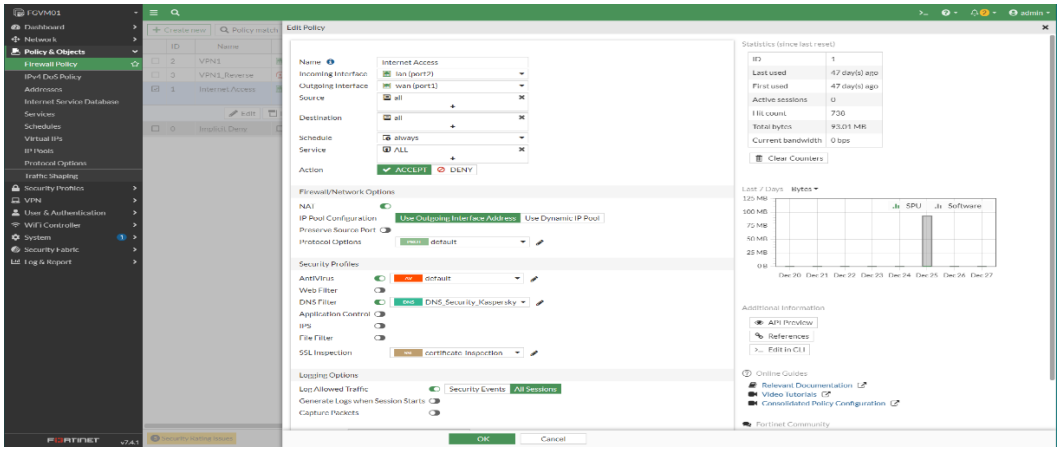


kaspersky

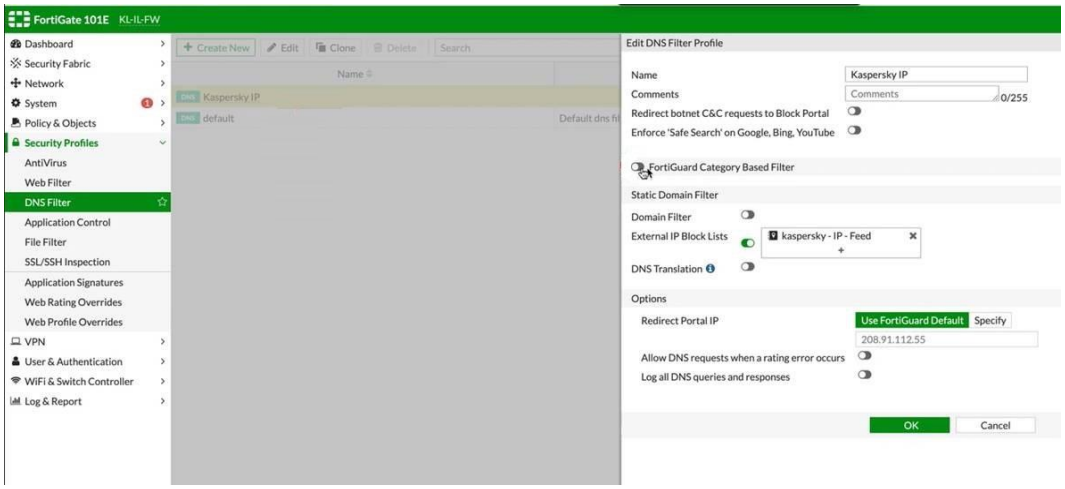



После полной загрузки динамически обновляемого списка индикаторов его можно использовать в политиках Web Filter, DNS, Firewall, Antivirus profile, а также в качестве Source/Destination в политиках IPv4 и прокси:



Для корректной работы фидов не включайте опцию **FortiGuard Category Based Filter** одновременно в нескольких профилях DNS Filter (профиле по умолчанию и дополнительно созданных профилях).




www.kaspersky.com/
www.securelist.com