kaspersky

# Kaspersky Network Security Threat Data Feeds для UserGate NGFW

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.

# Общая информация

«Лаборатория Касперского» предоставляет возможность загрузить динамически обновляемые списки индикаторов в межсетевые экраны UserGate, повышая их возможности по обнаружению и предотвращению кибер-атак.

Загрузка динамически обновляемых списков индикаторов осуществляется с Threat Intelligence портала «Лаборатории Касперского». Данный портал содержит различные сервисы информирования о киберугрозах, в том числе потоки данных об угрозах, включающие индикаторы компрометации.

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

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

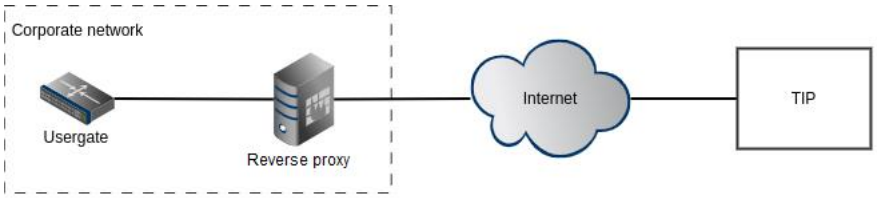
Доступные для загрузки следующие списки индикаторов:

| 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 |

# Подключение потоков данных в межсетевые экраны UserGate

**Схема интеграции**

Поскольку межсетевые экраны UserGate не поддерживают аутентификацию для загрузки списков индикаторов со сторонних ресурсов и не работают по протоколу HTTPS, интеграция с TIP на данный момент возможна только с установкой промежуточного обратного прокси-сервера. Ниже приведен пример настройки с использованием обратного прокси-сервера с открытым исходным кодом (Caddy), но можно использовать любое другое аналогичное решение.




Установка обратного прокси-сервера позволяет осуществлять безопасное соединение с Kaspersky Threat Intelligence Portal.

**Настройка Caddy**

Caddy – веб-сервер с открытым исходным кодом, который можно использовать в качестве обратного прокси-сервера.

Caddy устанавливается между межсетевым экраном UserGate и tip.kaspersky.com и обеспечивает функции авторизации и скачивания нужных файлов индикаторов для импорта в динамические списки межсетевого экрана UserGate.

Обратите внимание, что количество индикаторов в скачиваемом файле фида может быть большое, что, в свою очередь, может привести к замедлению работы межсетевого экрана UserGate.

Рекомендуем ограничивать количество скачиваемых индикаторов в зависимости от производительности устройства.

Ограничить число записей можно с помощью параметра *limit*, который можно указать в запросе списка индикаторов. Если этот параметр не указывать, будут скачаны все индикаторы.

Пример конфигурационного файла Caddy:

```
:8080 {
    route {
        # Handle path collision
        handle /api/feeds/* {
            respond 404
        }
        @list {
            path_regexp lFeed ^/(\w+)/list.zip$
        }
        rewrite @list /api/feeds/{re.lFeed.1}?format=usergate&limit=100000
        @version {
            path_regexp vFeed ^/(\w+)/version.txt$
        }
        rewrite @version /api/feeds/{re.vFeed.1}/version?format=plain
        handle /api/feeds/* {
            reverse_proxy https://tip.kaspersky.com/ {
                header_up Host {upstream_hostport}
                header_up Authorization "Bearer YourTokenHere"
            }
        }
        respond 404
    }
}
```

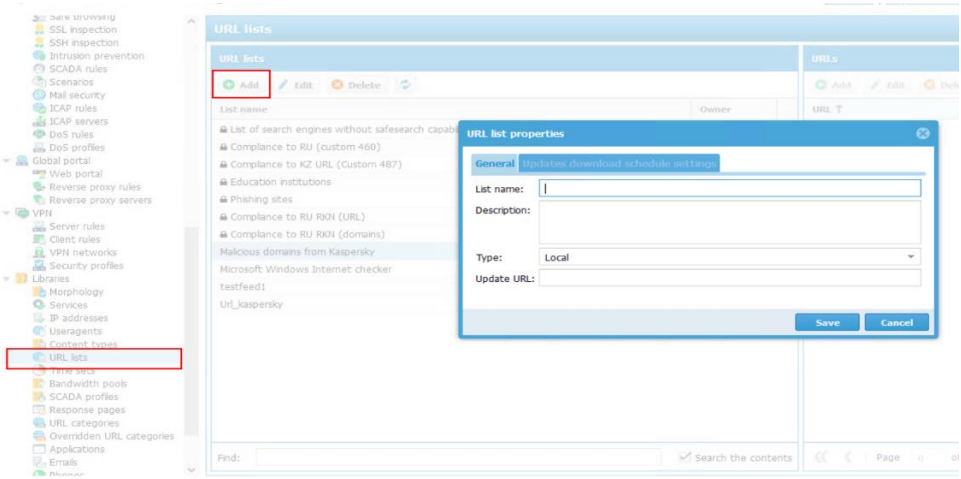
Вместо "**YourTokenHere**" необходимо указать API токен к Threat Intelligence порталу «Лаборатории Касперского».

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, отправьте запрос на intelligence@kaspersky.com.

**Настройка UserGate**

Для создания списка необходимо:

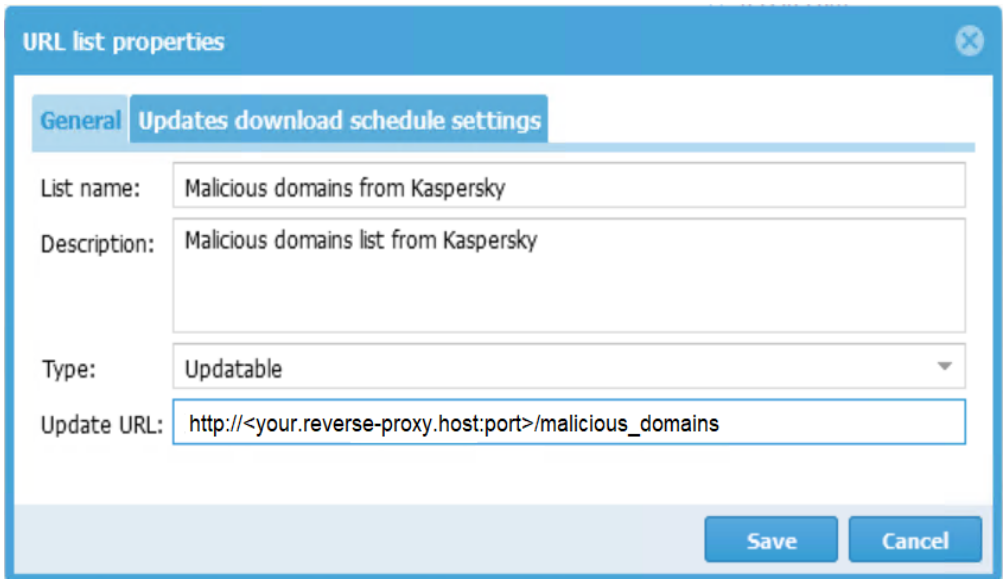
1. Перейти в раздел **Библиотеки** > **Списки URL** и нажать кнопку **Добавить**.



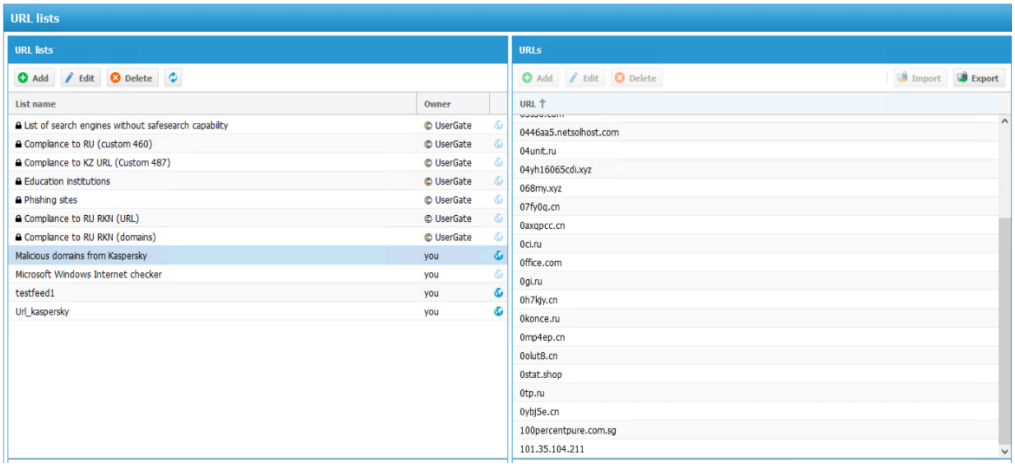

2. Необходимо задать **название** нового списка, которое будет отображаться, например, *Malicious domains from Kaspersky.*
3. Выбрать **Тип** списка — **Обновляемый**.
4. Указать **URL обновления** согласно таблице ниже.
   Вместо <your.reverse-proxy.host:port> нужно написать адрес обратного прокси-сервера, через который осуществляется интеграция с tip.kaspersky.com.

| URL | Список |
|---|---|
| http://<your.reverse-proxy.host>/dangerous_ips | Список опасных IP адресов |
| http://<your.reverse-proxy.host>/malicious_domains | Список вредоносных доменов |
| http://<your.reverse-proxy.host>/phishing_domains | Список фишинговых доменов |
| http://<your.reverse-proxy.host>/botnet_domains | Список доменов командных центров ботнетов |

5. В отдельной вкладке **Updates download schedule settings** необходимо настроить расписание скачивания обновлений. Рекомендованное время обновления приведено для каждого списка в таблице доступных для загрузки индикаторов.




После этого новый список будет отображаться в панели **URL lists**, а содержимое списка появится в панели **URLs**.




UserGate будет по расписанию проверять появление новой версии фида и обновлять список, если версия фида обновилась.

Полное руководство по работе со списками для устройств UserGate можно найти по следующей ссылке: https://docs.usergate.com/spiski-url_863.html

www.kaspersky.com/
www.securelist.com