

**kaspersky**

# **Kaspersky Network Security Threat Data Feeds для PaloAlto NGFW**

Версия 2.0

## Введение

Сетевые средства защиты – Next Generation Firewalls (NGFW), как правило, имеют функциональность фильтрации DNS/Web трафика 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	<a href="https://tip.kaspersky.com/api/feeds/dangerous_ips">https://tip.kaspersky.com/api/feeds/dangerous_ips</a>	20
Malicious URLs	URL	Список вредоносных доменов	<a href="https://tip.kaspersky.com/api/feeds/malicious_domains">https://tip.kaspersky.com/api/feeds/malicious_domains</a>	20
Phishing URLs	URL	Список фишинговых доменов	<a href="https://tip.kaspersky.com/api/feeds/phishing_domains">https://tip.kaspersky.com/api/feeds/phishing_domains</a>	20
Botnet CnC URLs	URL	Список доменов командных центров ботнетов	<a href="https://tip.kaspersky.com/api/feeds/botnet_domains">https://tip.kaspersky.com/api/feeds/botnet_domains</a>	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](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 отправить запрос на [intelligence@kaspersky.com](mailto: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
```

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

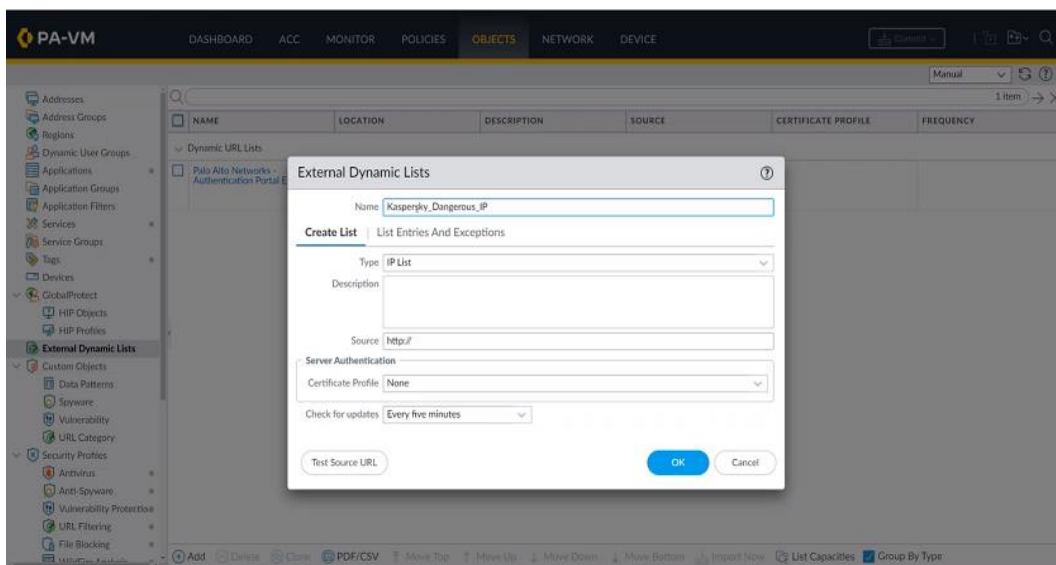
В PaloAlto NGFW имеется поддержка внешних динамически обновляемых списков индикаторов в виде текстовых файлов, загружаемых с внешнего HTTP- или HTTPS-сервера.

После загрузки в PA NGFW списков индикаторов, в зависимости от типа, могут быть использованы в политиках фильтрации трафика.

Подробное описание и примеры приведены в документации: [docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list](https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list)

Для создания динамических списков с индикаторами Лаборатории Касперского в PaloAlto выполните следующие действия:

1. Откройте **Device>Setup>Services>Service Route Configuration>Customize** и отредактируйте сервис **External Dynamic Lists**
2. Выберите **Objects > External Dynamic Lists**
3. Выберите действие **Add** и введите название вашего динамического списка в поле **Name** - например, Kaspersky Dangerous IP.
4. Выберите тип листа **Type**, соответствующий типу добавляемого листа. Для *Domain* списков можно включить дополнительную опцию **Automatically expand to include subdomains**



5. В поле **Source** введите адрес нужного списка

[https://tip.kaspersky.com/api/feeds/malicious\\_domains?limit=130000](https://tip.kaspersky.com/api/feeds/malicious_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.

Размер списка может превышать ограничения, установленные производителем оборудования, поэтому рекомендуем установить параметр limit в соответствии с допустимым количеством записей, указанным в документации к вашей модели оборудования.

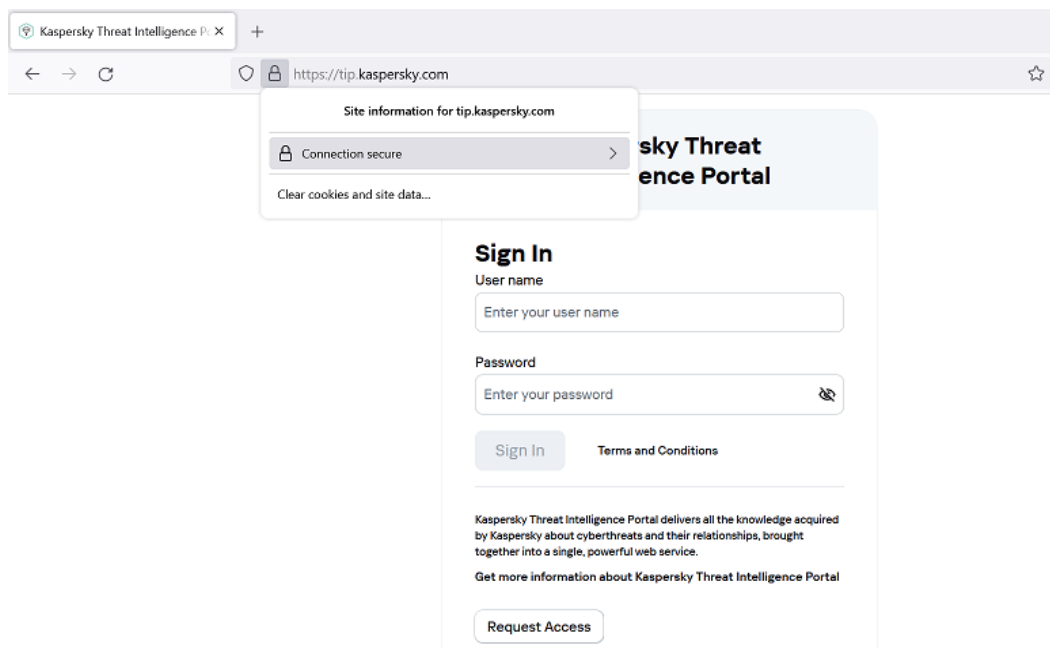
Полная спецификация API доступна по ссылке: <https://tip.kaspersky.com/Help/api/?specId=tip-feeds-api> (после нажатия на ссылку закройте появившееся окно авторизации с просьбой ввести логин и пароль и перейдите на страницу справки).

6. Необходимо скачать pem-файлы открытых ключей цепочки доверия для tip.kaspersky.com, кроме конечного узла.

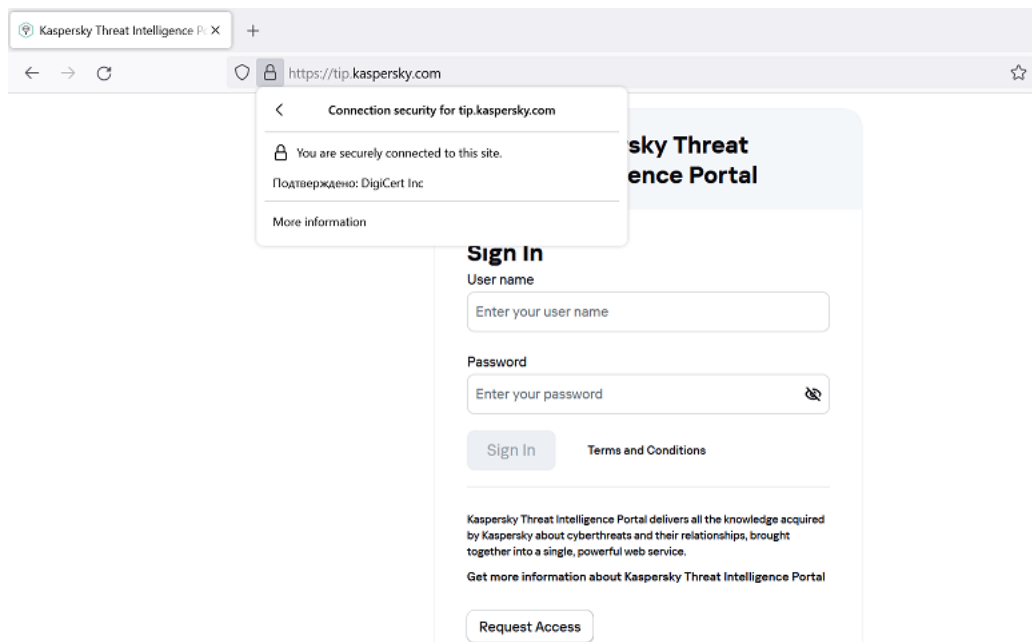
Ниже указаны шаги по получению рет-файлов сертификатов на примере браузера Firefox Browser 123.0:

1) Перейдите на сайт <https://tip.kaspersky.com>. Будет запрошен клиентский сертификат - вы можете отказаться или указать любой имеющийся, так как для получения информации о цепочки доверия авторизация в портале не потребуется.

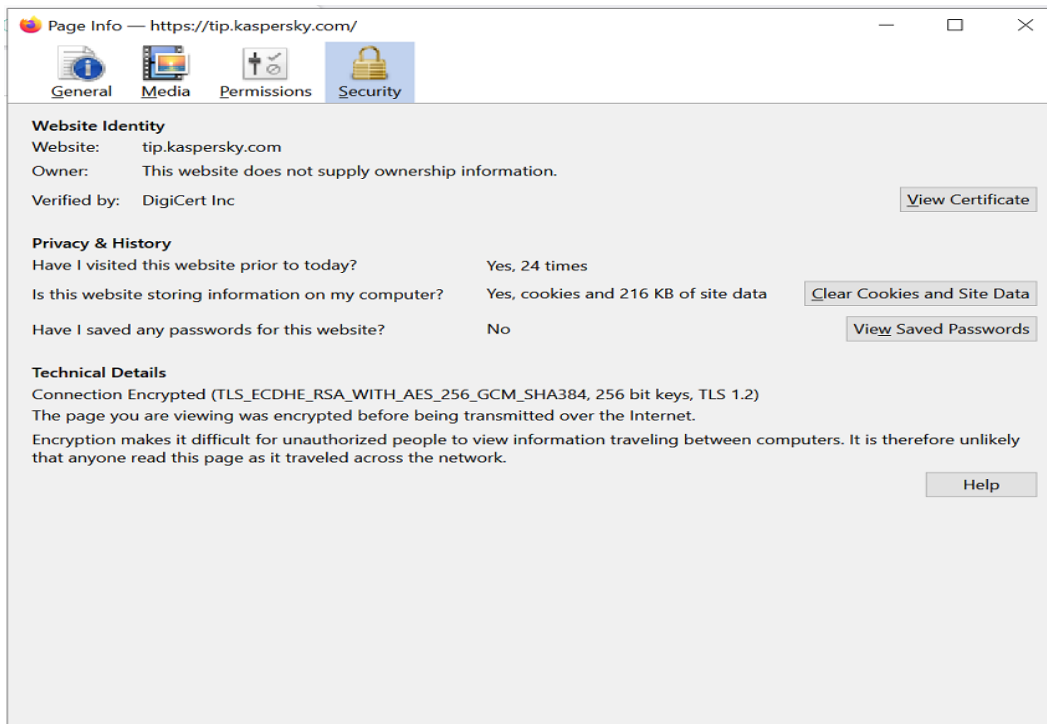
2) Нажмите на символ замочка рядом с адресной строкой браузера - откроется информация о TLS соединении с сайтом:



3) Нажмите на **Connection secure** - откроется дополнительная информация о соединении:



4) Нажмите на **More information** - откроется отдельное окно **Page Info** - <https://tip.kaspersky.com>:



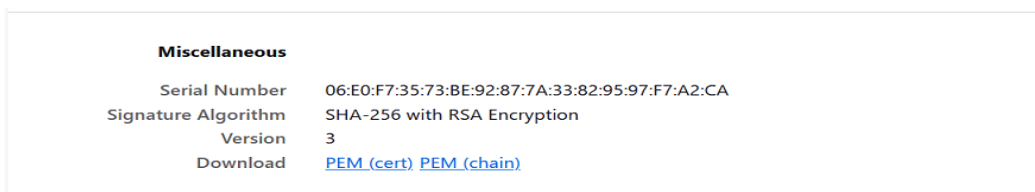
5) Нажмите **View Certificate** - в браузере появится вкладка с информацией о цепочке сертификатов:



## Certificate

<a href="#">tip.kaspersky.com</a>	DigiCert Global G2 TLS RSA SHA256 2020 CA1	DigiCert Global Root G2
<b>Subject Name</b>		
Country	CH	
Locality	Zürich	
Organization	Kaspersky Lab Switzerland GmbH	
Common Name	tip.kaspersky.com	
<b>Issuer Name</b>		
Country	US	
Organization	DigiCert Inc	
Common Name	<a href="#">DigiCert Global G2 TLS RSA SHA256 2020 CA1</a>	
<b>Validity</b>		
Not Before	Fri, 16 Feb 2024 00:00:00 GMT	
Not After	Tue, 18 Feb 2025 23:59:59 GMT	

6) Для Certificate Authority (root certificate) и Intermediate certification authority скачайте pem-файлы сертификатов. Для этого во всех вкладках, кроме **tip.kaspersky.com**, найдите пункт **Miscellaneous** и в поле **Download** выберите PEM (cert):



В нашем случае будут скачаны 2 файла: **tip-kaspersky-com.pem** и **tip-kaspersky-com(1).pem**

7) Необходимо создать профиль сертификата для подключения к https-серверу. Для этого выберите **New Certificate Profile**:

External Dynamic Lists

Name: Kaspersky\_Dangerous\_IP

Create List | List Entries And Exceptions

Type: IP List

Description:

Source: https://tip.kaspersky.com/api/feeds/dangerous\_ips?limit=70000

Server Authentication

Certificate Profile: None (Disable Cert profile)

Check for updates: None (Disable Cert profile)

New Certificate Profile

Test Source URL OK Cancel

Откроется окно создания профиля сертификата. Необходимо заполнить поле **Name** и импортировать сертификаты цепочки доверия, полученные на предыдущем шаге. Для этого нажмите **Add** в секции **CA Certificates**.

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit

Setup High Availability Config Audit Password Profiles Administrators Admin Roles Authentication Profile Authentication Sequence User Identification Data Redistribution Device Quarantine VM Information Sources Troubleshooting Certificate Management Certificates Certificate Profile OCSP Responder SSL/TLS Service Profile SCEP SSL Decryption Exclusion SSH Service Profile Response Pages Log Settings Server Profiles SNMP Trap Syslog Email

Certificate Profile

Name: Kaspersky\_TIP\_CA

Username Field: Name

User Domain:

CA Certificates

NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME /OID
------	------------------	-------------------------	--------------------

Add Delete Move Up Move Down

Default OCSP URL (must start with http:// or https://)

Use CRL CRL Receive Timeout (sec) 5

Use OCSP OCSP Receive Timeout (sec) 5

OCSP takes precedence over CRL Certificate Status Timeout (sec) 5

Block session if certificate status is unknown

Block session if certificate status cannot be retrieved within timeout

Block session if the certificate was not issued to the authenticating device

Block sessions with expired certificates

OK Cancel

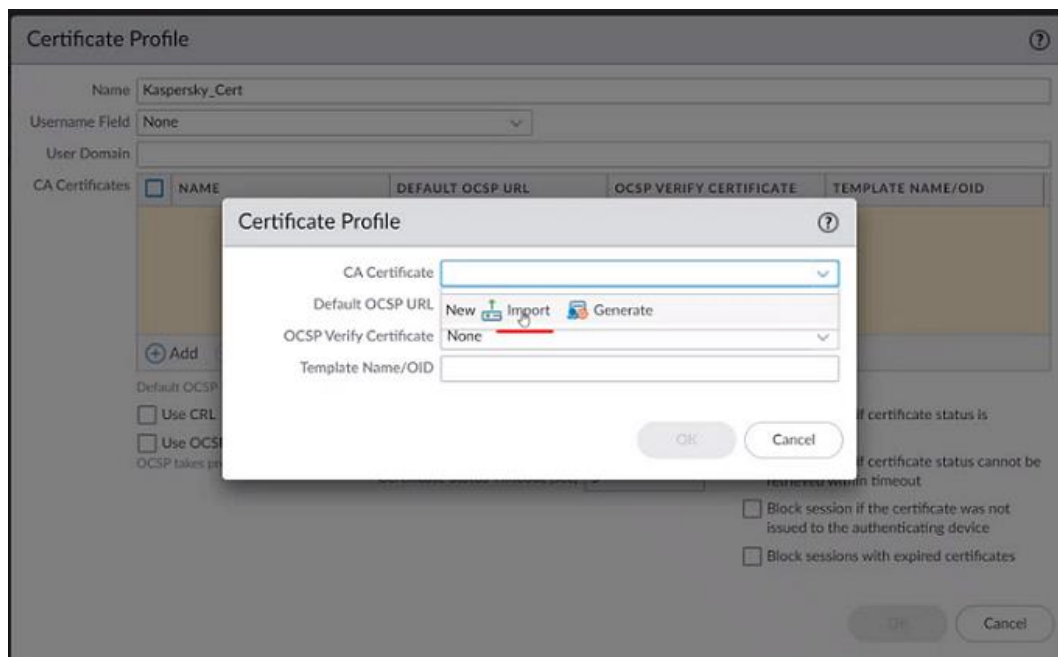
1 item

Block session with expired certificates

Admin | Logout | Last Login Time: 02/29/2024 21:50:19 | Session Expiry Time: 03/31/2024 00:04:12

Task | Language | paloalto

8) In the window that opens, select **Import**:



9) В окне импорта сертификата необходимо заполнить:

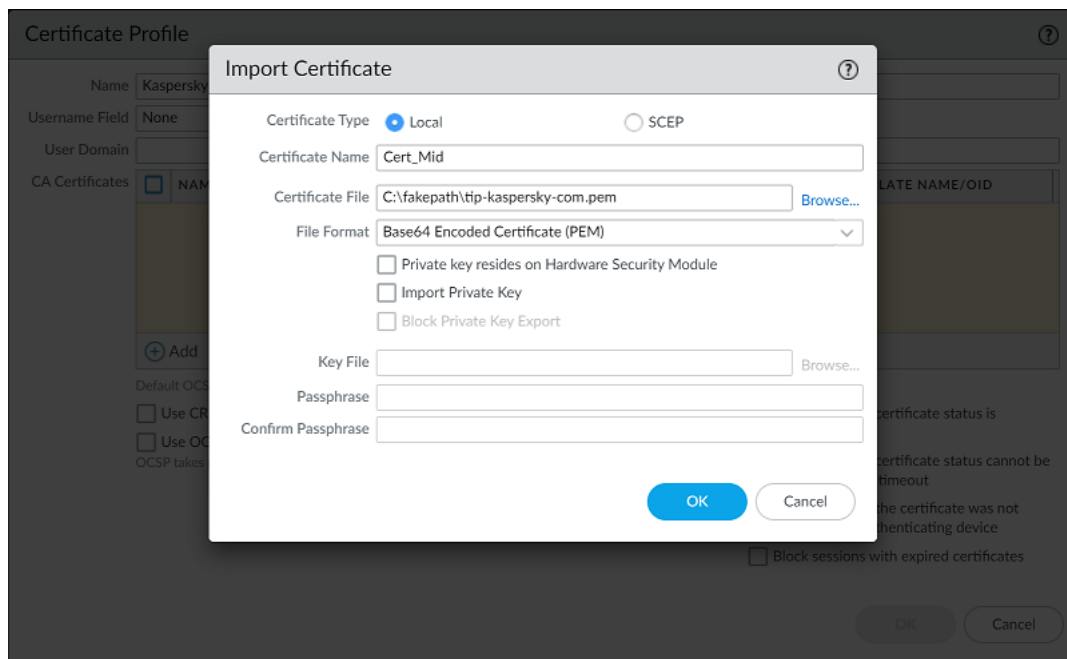
**Certificate Name** = (любое имя, в примере на скриншоте ниже - "Cert\_Mid")

**Certificate Type** = Local

**Certificate File** = выбираем pem-файл открытого ключа сертификата для цепочки доверия

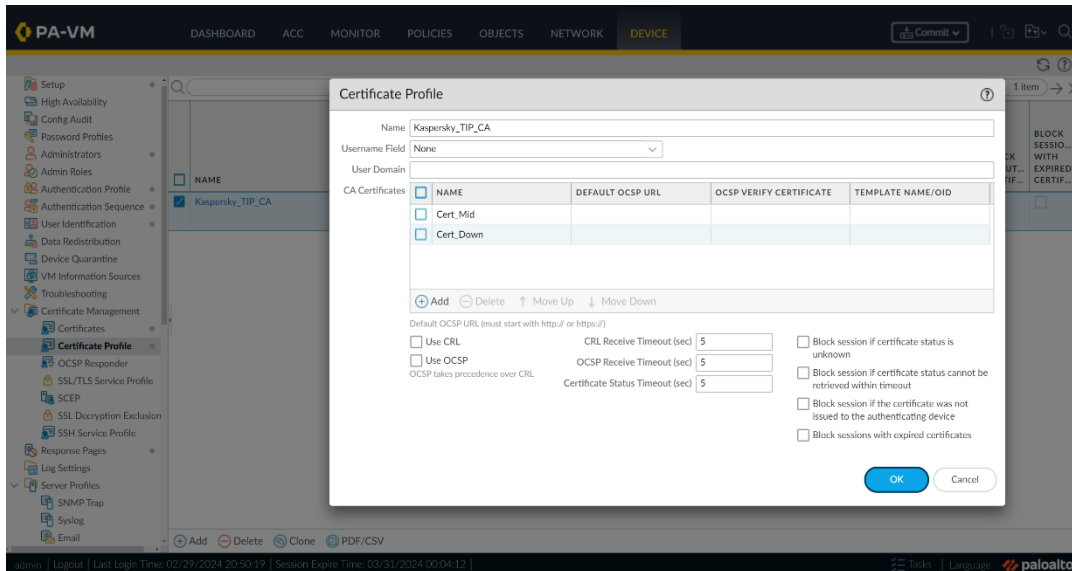
Прочие поля остаются без изменений.

Нажмите **OK**.



Операцию необходимо повторить дважды - для root CA и intermediate CA сертификатов цепочки доверия.

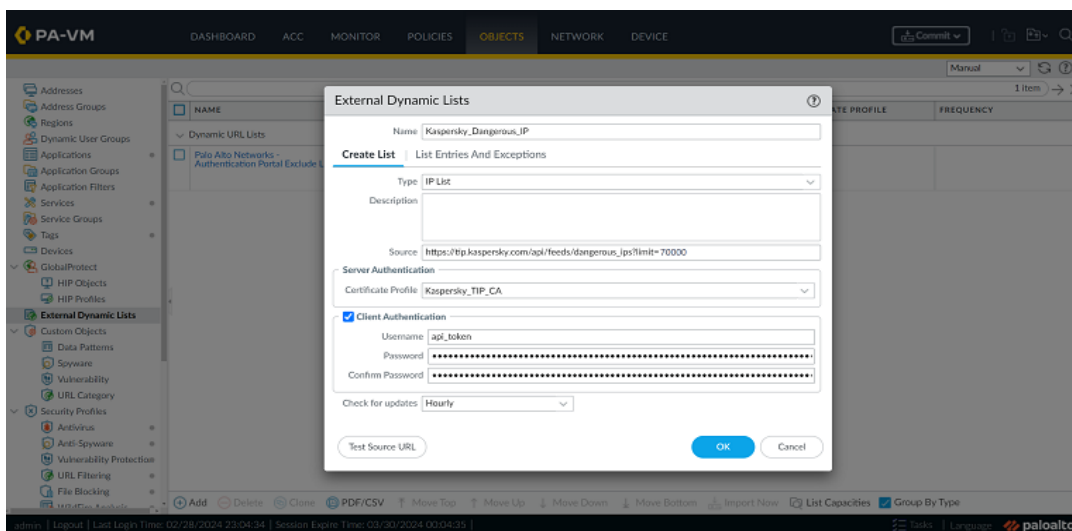
Кнопка **Test Source URL** в некоторых версиях PaloAlto может не работать. Поэтому при получении ошибки "Operation failed - URL access error" проигнорируйте ее.



10) Нажмите **OK**.

7. Выберите **Client Authentication** и введите **Username** и **Password**.

<b>Username</b>	api_token
<b>Password</b>	<a href="#">Токен для доступа к API</a> Threat Intelligence портала

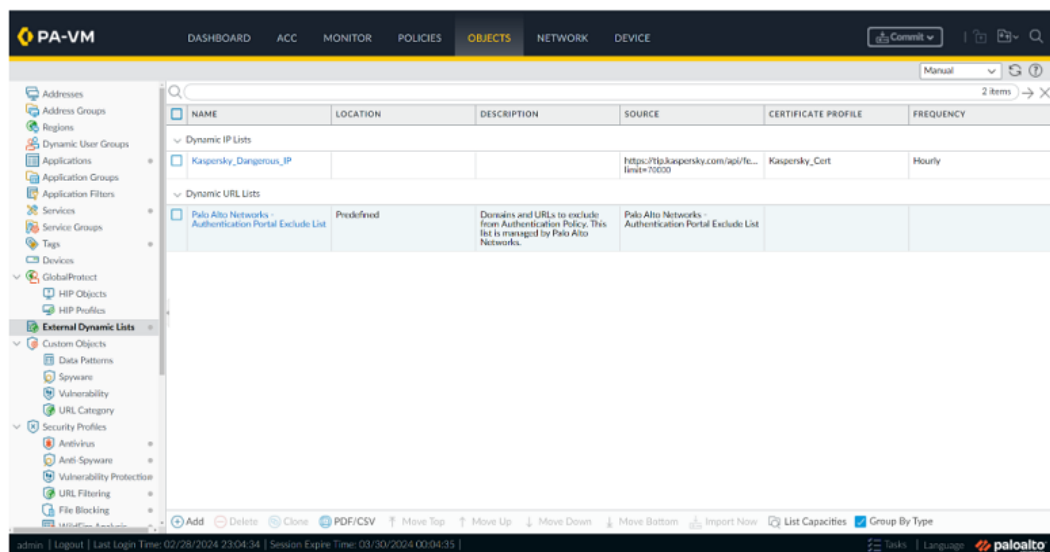


8. Установите значение **Check for updates**, рекомендуемые значения приведены в таблице доступных списков.

9. Нажмите **OK** для сохранения настроек и **Commit** для старта загрузки динамического списка индикаторов.

Новый список появится в списке динамических IP листов: **Objects > External Dynamic Lists**.





Для загрузки других списков индикаторов выполните аналогичные действия.

10. После применения динамического листа в **Policies** появятся записи в **List Entries And Exceptions**.

