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 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:<BAШ API TOKEH> 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 траффика.

Подробное описание и примеры приведены в документации: <u>docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list</u>

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 **Туре**, соответствующий типу добавляемого листа. Для *Domain* списков можно включить дополнительную опцию **Automatically expand to include subdomains**

Bastrees							Manual	
Address Groops		NAME	LOCATION	DESCRIPTION	source	CERTIFICATE PROF	LE FREQUEN	cy
Regions		Synamic URL Lists						
Applications		Palo Alto Networks - Authentication Portal E	External Dynamic Lists			O		
Application Filters			Name Kaspersky_I	Dangerous_IP				
Services	*		Create List List Entries	And Exceptions				
S Tags Devices GobalProtect			Type IP List Description			<u></u>		
HIP Objects HIP Profiles External Dynamic Lists			Source http://					
Custom Objects			Server Authentication					
Data Patterns			Certificate Profile None			· •		
U spyware Vulnerability			Check for updates Every five m	inutes 🗸 🗸				
Security Protecs			Test Source URL		ОК	Cancel		
URL Filtering								

5. В поле Source введите адрес нужного списка

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: <u>https://tip.kaspersky.com/Help/api/?specId=tip-feeds-api</u> (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 <u>https://tip.kaspersky.com</u>. Будет запрошен клиентский сертфикат - 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:

🔋 Kaspersky Threat Intellig	ence PCX +		
$\leftarrow \rightarrow $ C	O A https://tij	kaspersky.com	ť
	s	te information for tip.kaspersky.com	
	🔒 Connecti	n secure > sky Threat	
	Clear cookies	and site data	
		Sign In	
		User name	
		Enter your user name	
		Password	
		Enter your password	2
		Sign In Terms and Conditions	
		Kaspersky Threat Intelligence Portal delivers all the knowledge acquire by Kaspersky about cyberthreats and their relationships, brought together into a single, powerful web service.	d
		Get more information about Kaspersky Threat Intelligence Port	al
		Request Access	

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

$\textcircled{\ensuremath{\mathbb{R}}}$ Kaspersky Threat Intelligence $\ensuremath{\mathbb{P}}\xspace \times$	+			
$\leftarrow \ \rightarrow \ G$	https://tip.kaspersky.com	m		
	< Connection security f	or tip.kaspersky.com		
	You are securely connected Подтверждено: DigiCert Inc	to this site.	sky Threat ence Portal	
	More information			
		Sign In User name		
		Enter your user name		
		Password		
		Enter your password	Ŕ	
		Sign In Term	is and Conditions	
		Kaspersky Threat Intelligence by Kaspersky about cyberthr together into a single, powerf Get more information abou	Portal delivers all the knowledge acquired sats and their relationships, brought ul web service. ut Kaspersky Threat Intelligence Portal	
		Request Access		

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

ڬ Page Info	— https:/	/tip.kaspersky.c	om/			_		\times
Gaporal	Modia	† ⊘́	Socurity					
General	ivieula	rennissions	Security					
Website Ide	ntity							
Website:	tip.kasp	ersky.com						
Owner:	This we	bsite does not s	supply ownershi	p information.				
Verified by:	DigiCer	t Inc					View Certif	icate
	2					L		
Privacy & Hi	story							
Have I visite	d this wel	bsite prior to to	day?	Yes, 24 times				
Is this websit	te storing	information or	my computer?	Yes, cookies and 216 KB of s	site data	<u>C</u> lear Cooki	es and Site	Data
Have I saved	l any pass	words for this w	vebsite?	No		Vie <u>w</u> S	aved Passw	ords
Technical De	etails							
Connection	Encrypted	I (TLS_ECDHE_R	SA_WITH_AES_2	256_GCM_SHA384, 256 bit keys, T	LS 1.2)			
The page yo	u are viev	wing was encryp	oted before beir	g transmitted over the Internet.				
Encryption n that anyone	nakes it d read this	ifficult for unau page as it trave	thorized people led across the r	to view information traveling bet etwork.	tween comp	outers. It is the	refore unlil	cely
							Help	р

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

\textcircled{P} Kaspersky Threat Intelligence P_{1} X	Certificate for tip.kaspersky.com × +
$\leftarrow \ \rightarrow \ G$	😸 Firefox about.certificate?cert=MIIG%2FDCCBeSgAwIBAgIQBuD3NXO%2Bkod6M4KVI%2FeiyjANBgkqhkiG9w0BA 90% 🏠

ertificate tip.kaspersky.com [DigiCert Global G2 TLS RSA SHA256 2020 CA1	DigiCert Global Root G2
Subject Name		
Country	СН	
Locality	Zürich	
Organization	Kaspersky Lab Switzerland GmbH	
Common Name	tip.kaspersky.com	
Issuer Name		
Country	US	
Organization	DigiCert Inc	
Common Name	DigiCert Global G2 TLS RSA SHA256 2020 CA1	
Validity		
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 рет-файлы сертификатов. Для этого во всех вкладках, кроме tip.kaspersky.com, найдите пункт Miscellaneous и в поле Download выберите PEM (cert):

Miscellaneous

Serial Number Signature Algorithm Version

06:E0:F7:35:73:BE:92:87:7A:33:82:95:97:F7:A2:CA SHA-256 with RSA Encryption 3 Download <u>PEM (cert)</u> <u>PEM (chain)</u>

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 Dyna	mic Lists	?
Name	Kaspersky_Dangerous_IP	
Create List	ist Entries And Exceptions	
Туре	IP List	\sim
Description		
Source	https://tip.kaspersky.com/api/feeds/dangerous_ips?limit=70000	
Server Authenticat	tion	
Certificate Profile	None (Disable Cert profile)	~
Check for updates	None (Disable Cert profile)	÷
	New 🔊 Certificate Profile	
Test Source URL) ок са	ancel

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**.

High Availability	Certificate I	Profile			0	
Coving Auda	Name Kaspersky_TIP_CA					
Administration *	Username Field	None	lane 😒			
Admin Roles	User Domain		pression and the	1	10.000	
Authentication Sequence . Kispersay TIP_CA	CA Certificates	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID	
User Identification *						
Device Guatantine						
VM Information Sources						
Troubleshooting		Add O Dekter † Mo	ve Up 👔 Move Down			
Certificate Management		Default OCSP URL most start with th	tip://orbitps://)			
Certificate Profile		Use CRL	CRL Receive Timeout (sec)	5 Block s	ession il certificate status is	
CCSP Responder		Use OCSP	OCSP Receive Timeout (sec)	5 United	VO analos il carbificata status casard ha	
SSL/TLS Service Profile		UCSP takes protestience over CRL	Certificate Status Timeout (sec)	5 retrieve	esson il cerencare statos carinor de id within timeout	
A SD Ownedia Berlinker				Blocks	ession if the certificate was not	
SSH Sarvice Profile				Blocks	essions with expired certificates	
Response Pages =						
à Log Settings					Carrol	

8) In the window that opens, select Import:

Name	Kaspersky_C	ert			
Isername Field User Domain	None		~		
A Certificates		DEFAU	ILT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
		Certificate Profile			0
	Add Default OCSP	CA Certificate Default OCSP URL OCSP Verify Certificate Template Name/OID	New Limport	🛃 Generate	
	Use CRL Use OCSI OCSP takes pro	-		Canc	el ertificate status is if certificate status cannot b
				Block issued	session if the certificate was not I to the authenticating device
				Block	sessions with expired certificates

9) В окне импорта сертификата необходимо заполнить:

Certificate Name = (любое имя, в примере на скриншоте ниже - "Cert_Mid")

Certificate Type = Local

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

Прочие поля остаются без изменений.

Certificate Profile		
Name Kaspersky	Import Certificate	?
Username Field None	Certificate Type 💿 Local 🔷 SCEP	
User Domain	Certificate Name Cert_Mid	
CA Certificates NAM	Certificate File C:\fakepath\tip-kaspersky-com.pem	Browse
	File Format Base64 Encoded Certificate (PEM)	~
	Private key resides on Hardware Security Module	2
	Import Private Key	
0.11	Block Private Key Export	
(+) Add	Key File	Browse
Default OCS	Passphrase	sostificato status is
	Confirm Passphrase	certificate status is
OCSP takes		certificate status can
	ок	Cancel he certificate was no henticating device
		Block sessions with expired certificat

Нажмите ОК.

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.

	🚯 PA-VM						
Image: Setup I							G ()
Repersive_TIP_CA Better Better <t< th=""><th> Methods Setup High Availability </th><th>QCertifica</th><th>ate Profile</th><th></th><th></th><th></th><th>$\textcircled{1 item} \rightarrow \times$</th></t<>	 Methods Setup High Availability 	QCertifica	ate Profile				$\textcircled{1 item} \rightarrow \times$
Admin Roles User Domain Authentication Prohie Authentication Prohie Authentication Sequence CA Certificate NAME DEFAULT OCSP URL OCSP VERIFY CERTIFICATE TEMPLATE NAME/OID Cert_Mid	Config Audit Password Profiles	N. Username F	lame Kaspersky_TIP_CA Field None	~			BLOCK SESSIO
Cert_Mid	Admin Roles	NAME User Don CA Certific CA	cates NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID	UT EXPIRED CERTIF
Des informations Cert_Down	Authentication Sequence User Identification		Cert_Mid Cert_Down				
uos ☐ Device Quarantine Ø VM Information Sources	Device Quarantine WM Information Sources						
[™] Troubleshooting [™] Confrictet Management [™] Confrictet Management	Certificate Management		Add Delete Move Default OCSP URL (must start with http://	Jp ↓ Move Down			
Certificate Certificate Profile Certifica	Certificates Certificates Certificate Profile CCSP Responder SSL/TLS Service Profile		Use CRL Use OCSP Use OCSP OCSP takes precedence over CRL	CRL Receive Timeout (sec) 5 OCSP Receive Timeout (sec) 5 Certificate Status Timeout (sec) 5	Block si unknow	ession if certificate status is vn ession if certificate status cannot b	ue i
Ta SCEP	SCEP				Block si issued t	ession if the certificate was not to the authenticating device	
Block sestions model Block sessions with copied certificates Block sessions with copied certificates Copied certificates Copied certificates Copied certificates Copied certificates Copied certificates	Response Pages Image Cog Settings Server Profiles SNMP Trap				Block s	OK Cancel	
By Syrlog By Enull • ⊕Add ⊖ Delete ⊚ Clone @ PDF/CSV	🛱 Syslog 民 Email	+ Add - Delete Clone DPDF/CSV					

10) Нажмите ОК.

7. Выберите Client Authentication и введите Username и Password.

Username	api_token
Password	Токен для доступа к API Threat Intelligence портала

🚺 PA-VM									
								Manual	~ G ()
Addresses		E L L D L L L							1 item \rightarrow \times
Address Groups	NAME	External Dynamic Lis	sts			(U	TE PROFILE	FREQUENCY	
Regions	- Dynamic URL Lists	Name Kaspers	sky_Dangerous_IP						
Applications •	Palo Alto Networks -	Create List List Entri	ies And Exception	15					
Application Groups	Authentication Portal Exclude L								
Application Filters		Type IP List				~			
Services •		Description							
M Service Groups									
 Iags Devices 		Courses [https://d	No barnamlas com /or	Meade Manmarn in	in dinite 70000				
 GlobalProtect 		- Separ Authentication	opsaspersky.com/ap	in recust dangerous_	ps:mm-70000				
HIP Objects		Server Mannenfranton							
HIP Profiles		Cerbhcate Prohle Kaspers	sky_TIP_CA			Y			
External Dynamic Lists		Client Authentication -							
V 🐻 Custom Objects		Username api_to	ken						
Data Patterns		Password							
 Spyware Weborshilts 		Confirm Password							
WILL Category									
V Security Profiles		Check for updates Hourly		~					
Antivirus e									
AntS-Spyware e		Test Source URL				OK Cancel			
Vulnerability Protection									
G URL Filtering •									
In the blocking •	Add Delete Clone	PDF/CSV T Move Top				Import Now 🔀 List C	Capacities 🗾 Gro	up By Type	
			ac t						

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

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

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

🔶 PA-VM		DASHBOARD ACC	MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE		(t=Commit v	î⊐ 🖭~ Q
									Manual	- S ()
Addresses	Q									2 items)→ ×
Address Groups		NAME	LOCATION		DESCRIPTI	ON	SOURCE	CERTIFICATE PROFILI	E FREQUENC	Y
Regions	-									-
😤 Dynamic User Groups	~	Dynamic IP Lists								
Applications +		Kaspersky_Dangerous_IP					https://tip.kaspersky.com/api/fe	Kaspersky_Cert	Hourly	
Application Groups	-									
Application Filters	~	Dynamic URL Lists								
Services •		Palo Alto Networks - Authentication Portal Exclude List	Predefined		Domains an from Author	d URLs to exclude atication Policy. This	Palo Alto Networks - Authentication Portal Exclude List			
Terr 0					list is mana Notworks	ged by Palo Alto				
Devices										
V 🚱 GlobalProtect										
HIP Objects										
HIP Profiles										
🚱 External Dynamic Lists 🔹	ŀ.									
V G Custom Objects										
Data Patterns										
Spyware	1									
Vulnerability										
URL Category										
Security Promes										
Anti-Snoware a										
Vulnerability Protection										
G URL Filtering •										
G File Blocking =										
14/2dCies Association of a	• 🕀	Add 🕞 Delete 💿 Clone 🄇	PDF/CSV	Move Top	Move Up	↓ Move Down ↓	Move Bottom	🛛 List Capacities	Group By Type	

Для загрузки других списков индикаторов выполните аналогичные действия.

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

Ext	ernal Dynamic Li	sts			(?
	Name Kasper	sky_Dangerous_IP			
Cro	eate List List Entr	ries And Exceptions			
List E	intries			Manual Exceptions	
Q.(10 items \rightarrow \times		Q 0 items → >	<
	LIST ENTRIES	i		LIST ENTRIES	
	62.204.41.45	De			
	194.26.135.119				
	185.224.128.191				
	2.57.149.235		\rightarrow		
	62.204.41.230				
	80.66.79.247				
	45.137.22.156				
	405 000 50 (7	-		H Add Belete	
Т	est Source URL			OK Cance	I



www.kaspersky.com/ www.securelist.com

 $\ensuremath{\mathbb{C}}$ 2024 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners