# Kaspersky Network Security Threat Data Feeds for PaloAlto NGFW

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	Туре	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: <u>https://tip.kaspersky.com/Help/Doc data/en-US/ManagingAPItoken.htm</u> (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 <u>intelligence@kaspersky.com</u>).

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 PaloAlto NGFW

PaloAlto NGFW supports external dynamic lists of IoCs available as updatable plain text files via HTTP/HTTPs.

After import into PaloAlto NGFW IoCs can be used in traffic filtering policies.

For more information please refer to the documentation: <u>docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list</u>

In order to import a dynamic list of IoCs from Kaspersky into PaloAlto NGFW follow the steps:

1. Open **Device > Setup > Services > Service Route Configuration > Customize** and edit the service **External Dynamic Lists.** 

2. Select Objects > External Dynamic Lists.

3. Select action Add and specify the name of the list in the Name field – e.g. Kaspersky Dangerous IP.

4. Select the appropriate list **Type**. For lists with *Domain* type it is possible to set the additional option **Automatically expand to include subdomains**.

Manual V	
Addresses C	S () ⊪)→×
Regions     Departs Use Groups     Venimic Use Lists	
Applications • Disk After Networks - Authentication Portal E External Dynamic Lists	
Repetition Films Name Kaspersky, Dangerous, IP	
Services     Create List     List Entries And Exceptions	
Type (P List v)	
Charles     Description     PinObjects	
HIP Pedias Source Mtp./	
Cheternal Dynamic Lins     Server Authentication	
Dus Patients     Certificate Profile Nane	
Vulnerability     Check for updates     Every five minutes     V	
B Security Profiles     Test Source URL     OK Cancel	
Anto Sayware      Watersteiling Protection      Watersteiling Protection      Milling File Risching      File Risching	

5. In the field **Source** specify the URL of the list – e.g. <u>https://tip.kaspersky.com/api/feeds/malicious\_domains?limit=130000</u>

limit – the threshold on the number of IoCs actually being downloaded. This parameter is optional, if you do not specify it, all available IoCs will be downloaded. The actual number of downloaded IoCs can be less than the specified value, it depends on the number of available IoCs of certain type.

Full list size can exceed the threshold allowed by your PaloAlto NGFW (thresholds vary among PaloAlto NGFW models). It is recommended to set the limit according to the recommended value for your PaloAlto NGFW.

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

6. You will need to download pem files of public keys of trust chain for tip.kaspersky.com, except for the end node.

Below is the procedure for obtaining pem files of certificates using Firefox Browser 123.0 as an example:

1) Proceed to <u>https://tip.kaspersky.com</u>. You will be asked for the client's certificate. You may refuse or choose any available certificate, since no authorization is required for getting information about chain of trust.

2) Click on the 'lock' symbol next to the browser address line. Information about TLS connection to the site will be displayed:

Kaspersky Threat Intelligence	ce Pox +				
$\leftarrow \   \rightarrow \   G$	0	https://tip.kaspersky.co	m		Ś
		Site information	for tip.kaspersky.com		
		A Connection secure	>	sky Threat	
		Clear cookies and site data		ence Portal	
			Sign In		
			User name		
			Enter your user name		
			Password		
			Enter your password	SS.	
			Sign In Terms	and Conditions	
			Kaspersky Threat Intelligence by Kaspersky about cyberthre- together into a single, powerfu Get more information abou	Portal delivers all the knowledge acquired ats and their relationships, brought II web service. Kaspersky Threat Intelligence Portal	
			Request Access	<b>-</b>	

3) Click on **Connection secure**. Additional information about connection will be displayed:

🛞 Kaspersky Threat Intelligence Po X	+	-			
$\leftarrow \   \rightarrow \   G$	0	A https://tip.kaspersky.com			\$
		< Connection security for	or tip.kaspersky.com		
		A You are securely connected t	o this site.	sky Threat ence Portal	
		Подтверждено: DigiCert Inc			
		More information	Sign In		
			User name		
			Enter your user name		
			Password		
			Enter your password	\$	
			Sign In Terms	and Conditions	
			Kaspersky Threat Intelligence f by Kaspersky about cyberthrea together into a single, powerfu Get more information about	Portal delivers all the knowledge acquired Its and their relationships, brought I web service. : Kaspersky Threat Intelligence Portal	
			Request Access		

(®) ←

4) Click on More information. The Page Info - https://tip.kaspersky.com window will open:

🛯 🐸 Page Info	— https://	/tip.kaspersky.c	om/		-	. 🗆	$\times$
		ŧŏ					
General	<u>M</u> edia	Permissions	Security				
Website Ide	ntity						
Website:	tip.kasp	ersky.com					
Owner:	This we	bsite does not s	upply ownershi	p information.			
Verified by:	DigiCert	t Inc				<u>V</u> iew Cer	rtificate
Privacy & H	istory						
Have I visite	d this web	osite prior to too	day?	Yes, 24 times			
Is this websi	te storing	information on	my computer?	Yes, cookies and 216 KB of site data	<u>C</u> lear Coo	kies and Sit	te Data
Have I saved	d any pass	words for this w	vebsite?	No	Vie <u>w</u>	Saved Pas	swords
<b>Technical D</b> Connection The page yo	<b>etails</b> Encrypted ou are viev	l (TLS_ECDHE_R ving was encryp	SA_WITH_AES_2 ted before bein	256_GCM_SHA384, 256 bit keys, TLS 1.2) ig transmitted over the Internet.			
Encryption r	nakes it di	ifficult for unaut	thorized people	to view information traveling between co	mputers. It is t	nerefore ur	nlikely
that anyone	read this	page as it trave	led across the h	etwork.		н	lelp

5) Click on View Certificate. The browser will display a tab with information about chain of certificates:

sky initial intelligence in A	Certificate for up,kaspersky.com	-	
C	Sirefox about:certificate?cert=MIIG	%2FDCCBeSgAwIBAgIQBuD3NXO%2Bkod6M4KVI%2	FeiyjANBgkqhkiG9w0BAC 90%
	Certificate		
	tip.kaspersky.com Di	giCert 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	

6) For Certificate Authority (root certificate) and Intermediate certification authority download pem files of certificates. To do this, on all tabs except for **tip.kaspersky.com**, find **Miscellaneous** and select PEM (cert) in the **Download** field:

Miscellaneous	
Serial Number	06:E0:F7:35:73:BE:92:87:7A:33:82:95:97:F7:A2:CA
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

In our example, two files will be downloaded: tip-kaspersky-com.pem and tip-kaspersky-com(1).pem.

7) You will need to create a certificate profile for connecting to HTTPS server. To do this, select **New Certificate Profile**:

External Dynar	nic 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	ion —	
Certificate Profile	None (Disable Cert profile)	~
Check for updates	None (Disable Cert profile)	ê
	New 🗊 Certificate Profile	
Test Source URL	ОК Сал	icel

A window for creating certificate profile will open. Fill in the **Name** field and import the trust chain certificates obtained earlier. To do this, click **Add** in the **CA Certificates** section.

🕞 Setus 🔹 👘 🖸		Certificate P	rofile			0	1 item -
Config Audik Password Profiles Administrators		Name Username Field	Kaspersky_TIP_CA	*			BLOCI SESSII IK WITH
Admite Robes	NAME Kasperany, TIP, CA	User Domain CA Certificates	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID	UTEXPIR
VM Information Sources Troubleshooting Certificate Management			🕢 Add 💮 Delete 🍸 Mo Default OCSP URL Invest start with the	ve Up 👔 Move Down tip/Forbites/P			
Certificate Profile			Use CRL Use OCSP OCSP takes presidence over CRL	CRL Receive Timeout (sec OCSP Receive Timeout (sec Certificate Status Timeout (sec	3 5 Block s 0 5 Block s 0 5 Block s 0 5 Plock s 0 5 Plock s 0 5 Plock s 0 5 Plock s 0 S Pl	ession if certificate status is vh ession if certificate status cannot be divittini timeout vession if the certificate was not to the authenticating device	
SSH Service Prohis  Response Papes  Control Control  Service Profiles  SNMP Tape  SNMP Tape  Control  SNMP Tape  Control  Contro					Biock s	essions with expined centificates	

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

Name	Kaspersky_C	ert			
sername Field User Domain	None		~		
A Certificates		DEFAU	ILT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
		Certificate Profile			0
	Add Default OCSP Use CRL Use OCSI Use OCSI	CA Certificate Default OCSP URL OCSP Verify Certificate Template Name/OID	New 🚠 Import	Generate	of a certificate status is
				Biock	session if the certificate was not to the authenticating device sessions with expired certificates

9) In the certificate import window, fill in the following:

Certificate Name = (any name, in the example below - "Cert\_Mid")

Certificate Type = Local

**Certificate File** = select pem file of certificate public key for chain of trust.

Other fields should be unchanged.

Certificate Profile					?
Name Kaspersky	Import Certificat	te		?	
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	LATE NAME/OID
	File Format	Base64 Encoded Certificate (PEM)		$\sim$	
		Private key resides on Hardware Secur	rity Module		
		Import Private Key			
		Block Private Key Export			
(+) Add	Key File			Browse	
Default OCS	Passphrase				
	Confirm Passphrase				ertificate status is
OCSP takes					ertificate status cannot be
				incel	timeout
				ancer	the certificate was not thenticating device
			Bloc	ck sessions v	vith expired certificates

Click OK.

The above step should be performed twice – for root CA and intermediate CA trust chain certificates.

The **Test Source URL** button may not function in some PaloAlto versions. Thus, ignore the "Operation failed - URL access error" message, if appears.

							50
<ul> <li>Setup</li> <li>High Availability</li> </ul>		Certificate P	rofile			0	1 item >>>
Config Audit		Name	Kaspersky_TIP_CA				BLOCK
Administrators •	-	Username Field User Domain	None	~			JK WITH UT EXPIRED
Authentication Profile •	Kaspersky_TIP_CA	CA Certificates	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID	GERTIF
User Identification •			Cert_Mid Cert_Down				
Device Quarantine							
VM Information Sources				alla I Marchana			
Certificate Management			Default OCSP URL (must start with ht	ip:// or https://)			
Certificate Profile		1	Use CRL	CRL Receive Timeout (sec	) 5 Block s	session if certificate status is wn	
SSL/TLS Service Profile			DCSP takes precedence over CRL	Certificate Status Timeout (sec	) 5 Block s	ession if certificate status cannot be ed within timeout	
SCEP					Block sissued	ession if the certificate was not to the authenticating device	
SSH Service Profile					Block	essions with expired certificates	
Log Settings						OK Cancel	
SNMP Trap							
Syslog							

10) Click **OK**.

7. Select Client Authentication and specify Username и Password:

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

🔷 PA-VM					
				Manual	~ S ()
Addresses		External Dynamic Lists	TE PROFI	LE FREQUENC	$1$ item) $\rightarrow \times$
C Regions		Name Kaspersky_Dangerous_JP			
Applications •	Palo Alto Networks - Authentication Portal Exclude L	Create List Entries And Exceptions	- 11		
Application Filters		Type IP List	~		
Services     Service Groups     Trags		Lense ripriden			
Devices		Source https://tip.kaspersky.com/api/feeds/dangerous_jps?limit=70000			
✓ GlobalProtect		Server Authentication			
HIP Profiles		Certificate Profile Kaspersky_TIP_CA			
External Dynamic Lists		Client Authentication	5		
V 🚺 Custom Objects		Usemame api_token			
Data Patterns		Password	•		
Unerability		Confirm Password	•		
G URL Category		Check for updates Hourly V			
<ul> <li>Antivirus e</li> <li>Anti-Spyware e</li> </ul>		(Test Source URL) OK Cancel			
URL Filtering +					
Hie Blocking e	Add  Delete  Clone	😰 PDF/CSV 🌴 Move Top 🃫 Move Up 👃 Move Down 🗼 Move Bottom 🚠 Import Now 🔯 I	List Capacities	🛃 Group By Type	

8. Set **Check for updates**, and specify the frequency of updates. Recommended values are described in the table of available lists above in this document.

9. Set **OK** to save settings and **Commit** for starting download of dynamic list of indicators.

A new list will appear in the dynamic IP lists: Objects > External Dynamic Lists.

🚯 PA-VM		DASHBOARD ACC P	MONITOR POLICIES	DBJECTS NETWORK		(d	<b>⊆Commit v</b>   î= मि√ Q
							Manual 🗸 S 🕐
Addresses		(					2 items ) → ×
Regions		NAME	LOCATION	DESCRIPTION	SOURCE	CERTIFICATE PROFILE	FREQUENCY
A Dynamic User Groups	×	Dynamic IP Lists					
Applications 0		Kaspersky_Dangerous_IP			https://tip.kaspersky.com/api/fe	Kaspersky_Cert	Hourly
Application Groups	-				1000		
P Application Filters	Ľ	Dynamic URL Lists					
Service Groups		Palo Alto Networks - Authentication Portal Exclude List	Predefined	Domains and URLs to exclude from Authentication Policy. This	Palo Alto Networks - Authentication Portal Exclude List		
💊 Tags 🔹 🔹				list is managed by Palo Alto Networks.			
Devices							
V 🚱 GlobalProtect							
HIP Objects							
HIP Profiles							
Custom Objects							
Data Patterns							
😡 Spyware							
Vulnerability							
G URL Category							
<ul> <li>Security Profiles</li> </ul>							
Anti-Services a							
Vulnerability Protection							
G URL Filtering 0							
G File Blocking =			DDEICOL & Mars Top. A		Mana Ballian J. Immed Mana	Cit List Conseilling 🗖 Co	un Du Tune
11/Jullion Analysis	•	Add Clone	PUPPER T Move lop T	wove ob 1 wove nown 7	Move Bottom	iQ List Capacities 🛃 Gri	Juli ny type

In order to configure other dynamic lists of IoCs follow similar steps.

10. After applying the dynamic list in **Policies**, the entries will be displayed in **List Entries And Exceptions**.

	Name Kasper	sky_Dangerous_IP		
Cre	eate List List Entr	ies And Exceptions		
ist Er	ntries			Manual Exceptions
20		10 items $\rightarrow$ $\times$		$Q \longrightarrow X$
	LIST ENTRIES	Í		LIST ENTRIES
	62.204.41.45	De la		
	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	-		HAdd O Delete



www.kaspersky.com/ www.securelist.com

© 2024 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners