Kaspersky Network Security Threat Data Feeds для FortiGate

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 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: <u>https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/9463/threat-feeds</u>

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

FGVM01 -		>_ 0 - 0 0 - 0 admin -
Dashboard >	New External Connector	
Network >		Public SDN Connector Setup Guides
🕭 Policy & Objects 🔷 🔸	Durity STM	🖽 Amazon Web Services 🕜
Security Profiles	T MARK ANY	Geogle Cloud Platform (2)
Q VPN >		- Oracle Cloud Infrastructure (2*
Liser & Authentication	(🖤)((()(()()()()()()()()()()()()()()()(
♥ WiFi Controller >		R. Private SDN Connector Setup Guides
O System	Anazon Web Microsoft Geogle Cloud Oracle Cloud IBM Cloud All-Cloud Services (AMS) Azure PlatformICCPI Infestructure	Cisco Application Centric Infrastructure
Security Fabric •	1001	Pruge Virbalded Services Patronii (2) OpenStack Connector (2)
Physical lopology	Delasta SDM	** VMware NSK @
Security Dation	FIREW INT	0.0000
Automation		Origination Commentation C
Fabric Connectors		Video Tutoriais C
External Connectors		
Asset Identity Center	Kubernetes VMware ESQ VMware NSX OpenStack Application Nuage Nutanix SAP	Sectional Community
Ltd Log & Report >	Infrastructure Services Beatroom	O Join the Discussion C
	a manage a second and a second a	
	Endpoint/Identity	
	FSSO Agent on Symantic Poll Active RADIUS Single Exchange	
	Windows AD Endpoint Directory Sign-On Agent Server Protection Server	
	Threat Feeds	
	FortiGuard IP Address Domain Name MAC Address Matware Hash	
	Category	
	▶	
	Return	
	7654411	

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.

🕞 FGVM01	-	≡ Q.			>_	0 -		⊖ admin •
Dashboard		New External Connector						
Network					Additional Information			
🖹 Policy & Objects		-			(A) A DI Draviour			
Security Profiles		Inreat Feeds			W AFIFICVICW			
D VPN					Public SDN Connector Setup	Guides		
User & Authentication					🦥 Amazon Web Services 🏹			
☆ WiFi Controller					Google Cloud Platform			
🌣 System		IP Address			Microsoft Azure Oracle Cloud Infrastructur	e 🕑		
Ø Security Fabric					_			
Physical Topology		Connector Settings			Private SDN Connector Setu	p Guides		
Logical Topology		Status	Enabled S Disabled		Cisco Application Centric I	nfrastruc Platforn	ture 🖸	
Security Rating		Name 🚯			OpenStack Connector II	Flation		
Automation		Update method	External Feed Push API		NSX VMware NSX 🗹			
Fabric Connectors		URL of external resource 0			⑦ Online Guides			
External Connectors		HTTP basic authentication C			Relevant Documentation	2		
Asset Identity Center		Username	api_token		Video Tutorials			
ഥ Log & Report		Password	••••••		Fortloot Community			
		Refresh rate	5		For the Community			
			Minutes (1 - 43200)		Solutine Discussion			
		Comments	/ 0/255	5				
			OK Cancel					
FORTIDET	v7.4.1							

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 МВ 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: <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).

• **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»

🕞 FGVM01		≣ વ					• •	<mark> </mark>	\rm e admin 🝷
Dashboard		+Create	New 🖋 Edit	1 Delete					
Network		Throat Foo	ode						_
💄 Policy & Objects		Threat Fee	sus						_
Security Profiles				C					
묘 VPN									
User & Authentication		IP Addre	ess Threat Feed						
			Kaspersky	o.					
🌣 System					IP Address Threat Feed	Kaspersky			
Security Fabric					Туре	IP Address Threat Feed			
Physical Topology					Update method	External Feed			
Logical Topology					URL	https://tip.kaspersky.com/api/feeds/danger limit=70000			
Security Rating					Connection Status	2023/12/27 15:11:02			
Automation					Last Content Update	2023/12/27 15:11:02			
Fabric Connectors					Entries	(20736) Valid			
External Connectors	ជ				i≣ View Entries				
Asset Identity Center									
🕮 Log & Report	,								
EBRIDET		-							
	v7.4.1								

FGVM01	-	≡ Q.		>_ @ • Q • 🖯 ed admin •
Dashboard	`	+Create New 🖋 Edit 🗍 Delete	IP Address Threat Feed Kaspersky	×
Network	`		O Q Search	Q. (20,733)Valid () invalid
Policy & Objects	2		Entry	Validity
 Security Profiles VON 	``		80.66.79.247	Ø Valid
LUSer & Authentication	,		213.109.202.154	Ø Valid
←	,	C Kaspersky O	79.124.58.218	✓ Valid
🕸 System	1 >		185.222.57.147	Valid
Security Fabric	۰		104.21.90.125	🖉 Valid
Physical Topology			45.137.22.229	Valid
Logical Topology			45.125.66.19	🖉 Valid
Automation			141,98,11,96	S Valid
Fabric Connectors			185.222.58.238	🖉 Valid
External Connectors	슈		62.204.41.230	🐼 Valid
Asset Identity Center			91.92.247.130	S Valid
네 Log & Report	•		185.222.57.90	S Valid
			141.98.10.127	S Valid
			141,98,10,87	S Valid
			45.137.22.182	S Valid
			141,98,10,86	S Valid
			45.137.22.107	👁 Valid
			79.137.202.179	S Valid
			176,97,210,185	👁 Valid
			185.222.57.75	🖉 Valid
			91.92.250.14	🖉 Valld
			45.137.22.113	Ø Valid
			95.214.26.35	🖉 Valid
			185.155.184.208	🛛 Valid
			163.123.143.87	Valid
			172.67.156.164	Valid
FURTIDET	v7.4.1			0% 20,736

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:

different and the second secon						>_ �• ↓ <mark>2</mark> • ⊖ admin •
Dashboard		New DNS Filter Profile				
Network >				Select Entries	×	FortiGate
💄 Policy & Objects 🔹 🔸		Name	DNS_Security_Kaspersky	O Search	+ Create	FGVM01
Security Profiles ~	-	Comments	Comments 0/255	Kasnersky	. 010010	
AntiVirus		Redirect botnet C&C requests to Block Portal		and the part any		Additional Information
Web Filter		Enforce 'Safe Search' on Google, Bing, YouTube 🕥				API Preview
DNS Filter 술	≿					% References
Application Control		FortiGuard Category Based Filter				
Intrusion Prevention		Static Domain Filter				⑦ Online Guides
File Filter		Domain Eliter				Relevant Documentation C
SSL/SSH Inspection		External IP Block Lists	×			Video Iutoriais 🕑
Application Signatures		+				Earlinet Community
IPS Signatures		DNS Translation 🚯				O Join the Discussion
Web Rating Overrides						-
Web Profile Overrides		Options				
₽ VPN >		Redirect Portal IP	Use FortiGuard Default Specify			
User & Authentication >			0.0.0.0			
♥ WIFI Controller >	·	Allow DNS requests when a rating error occurs <a>>				
🕸 System 🔹 🔹	1	Log all DNS queries and responses O				
Security Fabric >						
네 Log & Report >	1					
				Close		
	1		OK Cancel			

FGVM01		≡ ۹.								>_ @ • 4
Dashboard	.			Edit Bollov						
4 Nelwark	;	- Creat	e new Q Policy match	Loncroncy						
Policy & Objects							Sta	tistics (since last re	ret)	
Elrewall Policy	-			Name 0	Internet Access			(D)	1	
IPv4 DroS Drolie v			VPN1_Reverse	Incoming Interface	Ian (port2)	-		Last used	47 day(s) ago	
Addresses				Outgoing Interface	💌 wan (port1)	-		First used	47 day(s) ago	
				Source	📼 all	×		Active sessions	0	
Services			/ Edit	Destination	* 177 - 11	~		Hit count	730	
Schedules				Contraction	+	-		Total bytes	93.01 MB	
Virtual IPs	_			Schedule	Co atways	-		Current bandwidth	0 bps	
IP Pools				Service	@ ALL	×				
Protocol Options					+			Clear Counters		
Traffic Shaping				Action	V ACCEPT Ø DENY					
Security Profiles	>			Firewall/Network O	tions		Las	it 7 Days Bytes -		
	>			NAT	•		12	S M8		In SPLL In Softwa
User & Authentication	>			IP Pool Configuration	Use Outeoing Interface Ad	Itess Use Dynamic IP Pool	10	D MB		
	•			Preserve Source Por			7	5 MB		
System	● *			Protocol Options	default	- /	51	1MB		
Security Fabric	•						2	5 MB		
🗠 Log & Report	•			Security Profiles				08		
				AntiVirus	C default	- /		Dec 20 Dec 2	1 Dec22 Dec23	Dec24 Dec25 Dec26
				Web Filter	3					
				DN5 Filter	DNS_Security_Kasp	ersky 👻 🥜	Ad	ditional Information		
				Application Control	3			ABI Broudows		
				025	0			St. Deferments		
				TileTilter				6 Nererences		
				SSL Inspection	ss cortificate inspectio	n - 🌶		>_ Edit in GU		
				Logging Options			٢	Online Guides		
				Log Allowed Traffic	C Security Ever	All Sessions	4	Relevant Docum	ntation 12	
				Generate Logs when	Session Starts 🗇			Consolidated Pol	Sicy Configuration	0
				Capture Packets	3					
								Fortinet Communi	y.	

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

20 Dashboard	>	+ Create New / Edit Ta Clone B Delete Search		Edit DNS Filter Profile	
Security Fabric	>			Name	Kasparelo ID
Network	>			Kane	Commente
System (•			Comments	Comments A0/255
Policy & Objects	>	6455 default	Default dos fil	Redirect bothet C&C requests to Block Portal	2
Security Profiles	~			Enforce Safe Search on Google, Bing, YouTube	
AntiVirus Web Filter				FortiGuard Category Based Filter	
DNS Filter	合			Static Domain Filter	
Application Control				Domain Filter	
File Filter				External IP Block Lists 💿 📱 kaspersky - IP	- Feed 🗙
SSL/SSH Inspection				DNS Translation 🚯 🛛 🕥	
Application Signatures				Ontions	
Web Rating Overrides				Dedicat Destal ID	Line Contri Countri Default - Specific
Web Profile Overrides				Redirect Portai iP	208.91.112.55
	2			Allow DNS requests when a rating error occurs	0
User & Authentication	>			Log all DNS queries and responses	0
WiFi & Switch Controller	~			EQUAL DIS QUELES AND RESPONSES	
🛍 Log & Report	>				
					OK Cancel



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