



Integration Guide

Integrate Fortinet Firewall with EventTracker

Publication Date:

September 16, 2022

© Copyright Netsurion. All Rights Reserved.



Abstract

This guide provides instructions to configure the Fortinet Firewall to send crucial events to the EventTracker via syslog.

Scope

The configuration details in this guide are consistent with the EventTracker version 9.3 or later, and the Fortinet Firewall with FortiOS version 4.0-6.0.

Audience

This guide is for the administrators responsible for configuring the Knowledge Packs in EventTracker.



Table of Contents

1	(Overview4
2		Prerequisites4
3	I	Enable Syslog Forwarding in the FortiOS V4.04
4		Configure Syslog over TLS
	4.1	Creating a Client Certificate
5	1	Enable Syslog Forwarding in FortiOS v5.0-6.08
6	I	EventTracker Knowledge Pack11
	6.1	L Alerts
	6.2	2 Flex Reports
	6.3	3 Dashboard
7	I	Import Fortinet Firewall Knowledge Pack25
	7.1	L Alerts
	7.2	2 Token Template
	7.3	3 Flex Reports
	7.4	4 Knowledge Objects (KO)
	7.5	5 Dashboard
8	1	Verify Fortinet Firewall Knowledge Pack32
	8.1	L Alerts
	8.2	2 Token Template
	8.3	3 Flex Reports
	8.4	4 Knowledge Objects (KO)
	8.5	5 Dashboard



1 Overview

Fortinet Firewall provides protection in various areas with other key security features such as anti-virus, intrusion prevention system (IPS), web filtering, anti-spam and traffic shaping to deliver multi-layered security for the IT environment.

Netsurion facilitates monitoring events retrieved from the Fortinet Firewall. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, collects and analyses firewall events provides details about security violations, user behavior, and traffic anomalies.

2 Prerequisites

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Fortinet Firewall with FortiOS V4.0-V6.0 must be installed.

3 Enable Syslog Forwarding in the FortiOS V4.0

Syslog is a standard for forwarding log messages in an IP network. Syslog captures the log information provided by the network devices.

- 1. To send logs to syslog server, go to Log & Report > Log Config > Log Settings.
- 2. In the Logging and Archiving section, select Syslog option.

	ITTIGATE 140D-POE	Video	Help	Logou
System	Log Settings			
Router				
Policy & Objects	Logging and Archiving			
Security Profiles	V Disk			
VPN	🖉 Enable Local Reports 🖖			
User & Device	Send Logs to FortiAnalyzer/FortiManager			
WiFi & Switch Controller	IP Address: 10.10.11.62 Test Connectivity			
Log & Report	Upload Option			
	Store & Upload Logs Daily v at 00:59			
🛡 🕙 Traffic Log	Realtime O Unreachable 5590 Logs Queued Failed: 2208548			
Event Log	C Encrypt Log Transmission			
Beport	✓ Send Logs to FortiCloud			
🖻 🕎 Log Config	Account: productmarketing@fortin lest Connectivity			
•••• Log Settings	Upload Option			
Threat Weight	Store & Upload Logs Daily t 00:00			
🛎 🖳 Monitor	© Realtime			
	Senal Logs to Systog			
	V Evenic Logging			
	Image: State of the state			
	GUI Preferences			
	Display Logs From Disk -			



- 3. After selecting the check box, the **Syslog** options appears.
- **4.** Enter the appropriate information for the following:

Option	Description
IP/FDQN	Enter the domain name or IP address of the syslog server.
Port	Enter the port number for communication with the syslog server, usually port is 514.
Minimum log level	Select a log level, the Fortinet unit will log all the messages at and above that logging severity level.
Facility	Facility indicates to the syslog server the source of a log message. By default, the Fortinet reports facility as local7. You can change the Facility if you want to distinguish log messages from other Fortinet units.
Enable set format default	Select this option to get the logs in default format. When you enable default format, the Fortinet unit produces the log in default format. If you do not enable default format, the Fortinet unit produces plain text files.

5. After providing the appropriate details, click the **Apply** button.

Note

Fortinet v4.0 does not support configuring syslog over TLS.

4 Configure Syslog over TLS

Configure Syslog over TLS using the certificate issued by a trusted Certificate Authority (CA).

4.1 Creating a Client Certificate

- 1. Log in to the Client Machine (CentOS or UBUNTU).
- **2.** Type in the below command.

Command: certtool -p --outfile ca.key.pem



- **3.** Specify the credentials to generate an RSA private key.
- **4.** Type in the below command.

Command: certtool -s --load-privkey ca.key.pem --outfile ca.crt

5. Specify the Common name, the certificate expiry date, and the other following fields as specified in the below image.

```
testuser1@R1S6-VM3:~$ sudo certtool -s --load-privkey ca.key.pem --outfile ca.cr
Generating a self signed certificate...
Please enter the details of the certificate's distinguished name. Just press ent
er to ignore a field.
Common name: centos
UID:
Organizational unit name:
Organization name:
Locality name:
State or province name:
Country name (2 chars):
Enter the subject's domain component (DC):
This field should not be used in new certificates.
E-mail:
Enter the certificate's serial number in decimal (default: 6668512171081630735):
Activation/Expiration time.
The certificate will expire in (days): 100
Extensions.
Does the certificate belong to an authority? (y/N): y
Path length constraint (decimal, -1 for no constraint): -1
Is this a TLS web client certificate? (y/N): y
Will the certificate be used for IPsec IKE operations? (y/N): y
Is this a TLS web server certificate? (y/N): y
Enter a dnsName of the subject of the certificate:
Enter a URI of the subject of the certificate:
Enter the IP address of the subject of the certificate:
Will the certificate be used for signing (DHE ciphersuites)? (Y/n): y
Will the certificate be used for encryption (RSA ciphersuites)? (Y/n): y
Will the certificate be used to sign OCSP requests? (y/N): y
Will the certificate be used to sign code? (y/N): n
Will the certificate be used for time stamping? (y/N): n
Will the certificate be used for email protection? (y/N): n
Will the certificate be used to sign other certificates? (y/N): y
Will the certificate be used to sign CRLs? (y/N): n
Will the certificate be used for signing (DHE ciphersuites)? (Y/n): n
```

Netsurion

```
nter the URI of the CRL distribution point:
X.509 Certificate Information:
       Version: 3
       Serial Number (hex): 5c8b507d01b0840f
        Validity:
               Not Before: Fri Mar 15 07:13:01 UTC 2019
               Not After: Sun Jun 23 07:13:29 UTC 2019
       Subject: CN=centos
        Subject Public Key Algorithm: RSA
       Algorithm Security Level: High (3072 bits)
               Modulus (bits 3072):
                        62:1d:3f:6e:08:00:52:62:f8:0a:cc:68:98:58:36:40
                        db:4e:64:05:0a:e9:ee:12:f9:1a:d9:40:53:0d:32:76
                        4e:49:e7:59:5a:bd:16:08:0a:62:fe:7c:d9:3f:59:b1
                        20:fa:47:4c:48:57:eb:9d:8e:1a:02:4f:30:3f:ca:2e
                        92:fa:70:f4:c6:18:4c:4b:bd:bc:ed:28:54:3f:17:cc
                        61:31:88:2a:7a:41:fd:2f:4c:7b:9e:7b:c7:b8:61:cd
                        1a:77:85:57:04:12:1b:9a:a9:36:07:23:7a:46:41:fd
                        21:22:77:d3:67:60:01:d2:8f:94:ee:5a:63:06:af:39
                        2d:e6:ff:16:ed:07:a9:30:e8:58:83:5b:5d:88:fa:e0
                        d0:40:c8:ca:2c:af:29:f5:fb:e2:fa:6a:34:68:46:87
                        84:87:7e:a5:f3:a8:39:41:2c:39:34:52:fb:b3:03:43
                        9b:99:76:97:39:a5:72:7c:45:e8:b7:72:80:42:81:5e
                        57:b4:ed:d7:7f:6c:8b:64:f9:8a:c8:91:aa:ed:3b:fd
                        7c:af:15:a3:10:8b:f4:bf:bd:a0:80:4d:ce:e6:26:97
                        b1:fd:17:b1:a0:48:5f:74:bc:1b:57:ae:61:2e:2c:9d
                        28:62:5d:51:bb:3a:aa:3d:30:bd:ed:46:db:bd:22:17
                        a7:1b:10:e6:d8:b9:8d:d9:0c:d6:a7:74:b5:fc:c6:c7
                        5d:a3:d2:56:bf:ef:c5:8b:3d:bc:8d:9c:ff:f1:b4:dd
                        92:df:d1:c2:83:b9:fe:18:dc:22:95:79:eb:62:c7:3d
                        6c:72:e7:f2:4c:5b:b7:e4:0b:06:e9:c4:64:df:ff:86
               Exponent (bits 24):
                       01:00:01
       Extensions:
               Basic Constraints (critical):
                        Certificate Authority (CA): TRUE
               Key Purpose (not critical):
                       TLS WWW Client.
                        TLS WWW Server.
                        Ipsec IKE.
                        OCSP signing.
               Key Usage (critical):
                       Digital signature.
                        Non repudiation.
                        Key encipherment.
                        Certificate signing.
               Subject Key Identifier (not critical):
                       68c405e1b3bad5401735d171866f19cf3636acf3
Other Information:
       Public Key ID:
               sha1:68c405e1b3bad5401735d171866f19cf3636acf3
               sha256:7c76087403747884bffb9dfe2665aec8e42f7758f92eb465c7b101bcd
c936c89
        Public Key PIN:
               pin-sha256:fHYIdANOeIS/+53+JmWuyOQvd1j5LrRlx7EBvNyTbIk=
        Public key's random art:
                +--[ RSA 3072]---
                      o =
                      = S
                              .0.0
                      0 0
Is the above information ok? (y/N): y
Signing certificate..
```



- 6. It will generate a client certificate with the name the ca.crt
- 7. To verify, specify the command: Is

Note

Please capture the certificate location for future use.

5 Enable Syslog Forwarding in FortiOS v5.0-6.0

Use this command to configure the log settings for logging into a remote syslog server (available only in the CLI). You can configure the Fortinet unit to send logs to a remote computer running a syslog server. Using the CLI, you can send the logs up to three different syslog servers.

You can even configure additional syslog servers using syslogd2 and syslogd3 commands.

Syntax: Config log {syslogd | syslogd2 | syslogd3} setting

1. Set status to enable to allow logging to a remote syslog server.

Example: set status enable

2. Enable default format to allow the Fortinet unit to produce the logs in default format. Ifyou do not enable default format the Fortinet unit produces plain text files.

Example: set default enable

- 3. Specify the facility type. Facility identifies the source of the log message to syslog.
- 4. Set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}

Example: set facility local3

5. Specify the port number for communication with the syslog server.

Example: set port 514

6. Specify the reliable delivery of syslog messages to the syslog server.

Example: set reliable enable

7. Specify the IP address of the syslog server that stores the logs.

Example: set server 172.168.22.54



8. Specify the source IP address for syslogd, syslog2 and syslog3.

Example: set source-ip 172.168.22.50

```
Note
```

If you need to enable the TLS, please follow the below steps that are optional.

9. Specify the reliable syslog with the TLS encryption.

Example: set enc-algorithm high

10. Specify the TLS version to send logs securely.

Example: set ssl-min-proto-version TLSv1-2

Note

Captured certificate path can be utilized in the below command.

11. Specify the certificate to communicate with the Syslog server.

set certificate "<certificate local path>"

Example: set certificate "/root/CACert.crt"

Importing Certificates

- 1. Log in to the FortiGate console.
- 2. Navigate to Systems > Certificates.





- **3.** Click **Import > CA Certificate**.
- 4. Set the **Type** to File, upload the **CA** certificate file, then click **OK**.

System	~ ^	🕂 Generate 🖋 Edit	💼 Delete 🔄 Import * 💿 View Det	ain 🛓 Download	Import Certifica	te			3
Administrators Admin Profiles Firmware	ł	Name ©	G = GJ, JJ = Cashorma, C = Junnyyane, G C = US, ST = California, L = Sunnyyane, G	- roconeq cro - Ceronica Fortinet, OU = Certificat	Type Certificate file	Local Certificate Upload	PKCS #12 Certificate	Certificate	
Settings	- 11	📮 Local Certificate 🖽							
HA		Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O	Fortinet, OU = FortiGate		ок	Cancel		
SNMP		W Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O	Fortinet, OU = FortiGate					
Replacement Messages		IV Fortinet_SSL DSA1024	C = US, ST = California, L = Sunnyvale, O	Fortinet, OU = FortiGate	-				
Replacement Message Groups		Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O	Fortinet, OU = FortiGate	2				
FortiGuard	11	Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O	FortInet, OU = FortiGate	-				
Reputation		Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O	Fortinet, OU = FortiGate	e,				
Feature Visibility		Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O	Fortinet, OU = FortiGate					
Certificates	슈	Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O	Fortinet, OU = FortiGate	0				

5. The CA certificate will be listed in the CA Certificates section of the certificates list.

🕇 Generate 🥒 Edit	🖹 Delete 🛃 Import • 💿 View Details 🛓 Download Search	Q				
Name 0	Subject ©	Comments ©	Issuer 0	Expires 0	Status 0	So
Local CA Certificate 🤰						
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut.,	This is the default CA certificate the SSL Inspection will use when generat	Fortinet	2028/09/23 20:44:12	O Valid	Fai
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut	This is the default CA certificate the SSL Inspection will use when generat	Fortinet	2028/05/01 09:07:49	 Valid 	Fai
Local Certificate 15						
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2056/11/20 14:58:17	 Valid 	Fai
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2038/01/18 22:14:07	 Valid 	Fai
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2028/09/23 20:44:13	 Valid 	Fai
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2029/01/03 13:46:32	 Valid 	Fai
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2029/01/03 13:46:33	 Valid 	Fai
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2029/01/03 13:46:33	 Valid 	Fai
Fortinet_SSL_ECD5A384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2029/01/03 13:46:33	 Valid 	Fai
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2030/08/18 20:26:32	 Valid 	Fai
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2030/08/18 20:26:32	 Valid 	Fai
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2030/08/18 20:26:32	 Valid 	Fai
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2029/01/03 13:46:32	 Valid 	Far
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique $_$	Fortinet	2029/01/03 13:46:32	 Valid 	Fai
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN =	This certificate is embedded in the hardware at the factory and is unique	Fortinet	2030/08/18 20:26:32	 Valid 	Fai
Fortinet_Wift	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert	This certificate is embedded in the firmware and is the same on every unit	DigiCert Inc	2021/12/25 18:59:59	 Valid 	Fai
IV syslogserver	CN = WIN-MCKKRLN6KOI.		WIN-MCKKRLN6KOI.	2022/08/18 08:16:32	O Valid	Us



6 EventTracker Knowledge Pack

After receiving the logs into the EventTracker, configure the categories and the reports into the EventTracker.

6.1 Alerts

- Fortinet: Administrator logon failed: This alert is generated when an administrator has a login failure.
- Fortinet: Attack detected: This alert is generated when the IPS alert is detected by the Fortinet firewall.
- Fortinet: Configuration changes: This alert is generated when a configuration change is done in the Fortinet firewall.
- Fortinet: Virus detected: This alert is generated when a virus is detected by the Fortinet firewall.
- Fortinet: Data leak protection: This alert is generated when a DLP event has occurred.

6.2 Flex Reports

• Fortinet- User authentication details- This report provides details about all the user authentication details.

LogTime	Computer	Priority	User Name	Action	Status	Reason	Event Details
10/30/2017 04:58:51 PM	FORTINET	notice	"user"	authentication failure	failure	"reason"	"User failed in user authentication"
10/30/2017 04:58:51 PM	FORTINET	notice	"Peter"	FSAE-auth	failure		"AD group Mobi_Tel user Peter failed in authentication"
10/30/2017 04:59:28 PM	FORTINET	notice	"user"	NTLM-author	failure	"reason"	"AD group AdGroup user user failed in authentication"



	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 10/30/2017 5:21:38 PM	3333	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio date=2 o=1 sro Mobi_1	n: 2007-07-01 time=20:29:01 devnar c=196.111.14.54:1051 dst=118.12 Fel user Peter failed in authenticat	ne=FRT123 device_ic .10.99:81 adgroup=" ion"	l=FGT000000000000 Mobi_Tel" user="Pete	1 log_id=000000001 type=event subtype=auth pri=notice vd=root prot er" ui=10.1.1.21:80(6) action=FSAE-auth status=failure msg="AD group

• Fortinet- Administrator logon details- This report provides details about all the admin login and logout activities.

LogTime	Computer	Priority	Virtual Domain	User Name	Action	Status	Profile	Event Details
10/18/2017 05:49:07 PM	FORTINET	in formation	vdom1	admin	login	failed	super_admin	Administrator admin logged in failed from console
10/18/2017 05:49:07 PM	FORTINET	in formation	vdom1	admin	login	SUCCESS	super_admin	Administrator admin logged in successfully from console

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE						
10/30/2017 4:59:28 PM	3333	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog						
Event Type: Information Log Type: Application Category Id: 0	Description: date=2014-06-28 time=13:57:36 logid=0100032002 type=event subtype=system level=alert vd="root" user="hford" ui=https(172.1 tatus=failed reason="passwd_invalid" msg="Administrator hford login failed from https(172.16.86.1) because of invalid password"										
10/30/2017 4:59:28 PM	<u>3333</u>	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog						
Event Type: Information Log Type: Application Category Id: 0	Description: date=2016-02-12 time=10:48:12 logid=0100032001 type=event subtype=system level=information vd="vdom1" logdesc="Admin login successful" sn=1 455302892 user="admin" ui=console action=login status=success reason=none profile="super_admin" msg="Administrator admin logged in successfull y from console"										

• Fortinet- Attack detected- This report provides details about all the IPS and IDS attacks that are detected by the Fortinet firewall.

LogTime	Source IP Address	Destination IP Address	Destination Port	Action	Attack ID	Attack Details	Service Name	Reference Url	Virtual Domain	Source Interface	Critical Level	Critical Score
10/18/2017 05:49:07 PM	192.168.1.183	192.168.70.184	20882	clear_ sessio n	16777316	icmp_flood	icmp/146/81	http://www.fort inet.com/ids/VID 16777316	vdom1	port15	critical	50



	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
10/30/2017 5:21:38 PM	3333	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Descriptio date=2 p=172. ptype= > thres	on: 2016-02-12 time=14:10:42 logid .160.45.111 srcintf="port15" ses =0x92 icmpcode=0x51 attackid= shold 25, repeats 306 times" crs4	=0720018433 type sionid=0 action=cle 16777316 profile= core=50 crlevel=crit	=anomaly subtype=anor ear_session proto=1 serv 'DoS-policy1" ref="http:/ ical	naly level=alert vd="vdom1" severity=critical sn ice="icmp/146/81" count=306 attack="icmp_flc //www.fortinet.com/ids/VID16777316" msg="ar	cip=192.168.11.101 dsti bod" dstport=20882 icm bomaly: icmp_flood, 34

• Fortinet- Suspicious web content detected- This report provides details about all the suspicious web traffic content that is detected by the Fortinet firewall.

LogTime Source IP Address	Source Port	Destination Host Address	Destination IP Address	Destination Port	Action	Service Name	Requested URL	Source Interface	Destination Inteface	Direction	Bytes Sent	Bytes Received	Event Details	Critical Level	Critical Score
10/18/2017 05:49:07 PM 192.168.1.183	48676	www.youku.com	202.46.41.172	80	blocked	HTTP	I	port15	port19	outgoing	120	948	URL belongs to a denied category in policy	high	30

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
Event Type: Information Log Type: Application Category Id: 0	Descriptio date=2 =" rool er=" bj ervice= =" refe	n: 2013-10-30 time=11:14:50 dev t° policyid=30 identidx=0 sess " unauthusersource=" forticlie e" http" hostname=" nagios.fo rral" url=" /nagios3/images/ci	name=FRT123 devid= ionid=21843402 srcna nt" srcip=192.168.11. o.net" profiletype=" V omment.gif" sentbyte=	=FG100D3 logid=0315013 ame=" MacBook-MacBoo 101.8 srcport=60038 srcir Vebfilter_Profile" profile= =633 rcvdbyte=18msg="	3317 type=utm subtype=webfilter e sk-Pro-de-B.local" osname=" Mac C htf=" internal2" dstip=172.160.45.11 " default" [b][color=#FF0000]status URL has been visited" method=dor	eventtype=urfilter level=notice vd S X" osversion=" 10.8.5" unauthus 11 dstport=80 dstintf=" ISP-Colt" s =passthrough [/color][/b] reqtype main class=0 cat=255

• **Fortinet- Suspicious email content detected-** This report provides details about all the suspicious email traffic content that is detected by the Fortinet firewall.

LogTime Computer Actio	Source IP So n Address Po	ource l	Destination IP Address	Destination Port	Service Name	Sender Address	Recipient Address	Mail Subject	Mail Attach ment	Event Details
10/18/2017 05:49:07 PM FORTINET tagge	J 192.168.1.183 ⁵ 3	3244 1	192.168.70.184	110	POP3	jj@fortinet.com	mm@fortinet. com	[SMTP]: MyTest	no	email is reported as spam by ASE



	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 10/30/2017 5:21:38 PM	3333	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description date=20 srcip=19 =tagged spam by	n: 016-02-12 time=14:01:12 logid=05(92.168.11.101 srcport=33244 srcint: d from="jj@fortinet.com" to="mm(y ASE" subject="[SMTP]: MyTest" at	09020482 type=utm f="port15" dstip=17 @fortinet.com" recip tachment=no	subtype=emailfilter eventtype 2.160.45.111 dstport=110 dsti ient="testpc3" sentbyte=27 rc	=pop3 level=notice vd="vdom1" sessionid=64465 user="" ntf="port19" proto=6 service=POP3 profile="default" action vdbyte=1592 direction=incoming msg="email is reported as

• Fortinet- Data leak detected- This report provides details about all the DLP event detected by the Fortinet firewall.

LogTime	Source IP Address	Source Port	Destination IP	Destination Port	Action	File Type	File Name	Requested URI	Source Interface	Destination Inteface	Protocol	Service Name	Bytes Sent	Bytes Received	Direction	User Agent
10/18/2017 05:49:07 PM	192.168.1.183	36171	192.168.70.184	80	block	unknown	ssn-docx- pdf-valid.tar	/dlp/ssn/ssn- docx-pdf- valid.tar	port15	port19	6	HTTP	151	90170	incoming	Wget/1.10.2

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
10/30/2017 5:21:38 PM Event Type: Information Log Type: Application Category Id: 0	3333 Descriptio date=2 vd="ro 92.168.	NTPLDTBLR38 / <u>Fortin</u> n: 2014-05-01 time=11:54:37 devna ot' filteridx=0 filtertype=none fil 11.101 srcport=60439 srcintf="ir	N/A me=FRT123D devi tercat=none policy iternal" dstip=172.	N/A d=FG100D3G12812498 yid=8 identidx=1 session 160.45.111 dstport=80 d	Syslog ogid=0954024577 type=utm subtype=dlp ever id=8774608 epoch=2043380188 eventid=0 use stintf="wan2" service=http filetype="unknown	nttype=dlp level=notice er="USRNAME" srcip=1 " sentbyte=0 rcvdbyte=
	0 hostr	name="1.2.com" url="/ws/ps.asm	x/GetMailcount" fi	ile="GetMailcount" actio	n="log-only" profile="default"	

• Fortinet-Virus detected- This report provides details about all the virus detected by the Fortinet firewall.

LogTime	Source IP Address	Source Port	Destination IP Address	Destination Port	Virus Name	Priority	Intrusion type	Reference Url	Requested URL	Action	Direction	File Name	Virtual Domain	Event Details	User Agent	Service Name	Source Interface	Destination Inteface	Critical Score	Critical Level
10/18/2017 05:49:07 PM	192.168.1.183	45719	192.168.70.184	80	EICAR_TEST _FILE	warning	Virus	http://www.for inet.com/ve?vn =EICAR_TEST_ FILE	http://192.168. 70.184/eicar.c om	blocked	incoming	eicar.com	vdom1	File is infected	Wget/1.1 0.2	нттр	port15	port19	50	critical

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
— 10/30/2017 5:21:39 PM	<u>3333</u>	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Descriptio date=2 on=blo to=6 di et.com, 1f95c5	n: 016-02-12 time=11:11:25 logid cked service=HTTP sessionid=5 irection=incoming filename="ei /ve?vn=EICAR_TEST_FILE" virusik 1cc819465fa1797f6ccacf9d494a	=0211008192 type= 6633 srcip=192.168 car.com" checksum: d=2172 url="http:// aaff46fa3eac73ae63	utm subtype=virus eve .11.101 dstip=172.160. ="1dd02bdb" quarskip= 192.168.70.184/eicar.co ffbdfd8267" analyticssu	nttype=infected level=warning vd="vda 45.111 srcport=45719 dstport=80 srcint =No-skip virus="EICAR_TEST_FILE" dtyp m" profile="default" user="" agent="Wather" bmit=false crscore=50 crlevel=critical	om1" msg="File is infected." acti f="port15" dstintf="port19" pro e="Virus" ref="http://www.fortin get/1.10.2" analyticscksum="13



• Fortinet- Traffic allowed details- This report provides details about all the traffic allowed by the Fortinet firewall.

LogTime A	Action	Application Category	Application Name	Bytes Received	Bytes Sent	Destinatio n Country	Destination IP Address	Destination Port	NAT Destination	NAT Source IP Address	Priority	Protocol	Source Country	Source IP Address	Source Port	Traffic Type	Virtual Domain
10/18/2017 05:49:07 PM c	close	General.Interest	Wget.Like	1605	398	Reserved	192.168.70.184	80	snat	192.168.70.214	notice	6	Reserved	192.168.1.183	45719	forward	vdom1

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
10/30/2017 5:21:39 PM Event Type: Information	<u>3333</u> Descriptio	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog
Log Type: Application Category Id: 0	Feb 19 vel=no o=6 ac 0 crsco	23:26:11 cpsutmfw01 time=23:26 tice vd=root srcip=192.168.11.101 tion=allow policyid=0 dstcountry: re=30 craction=131072 crlevel=hi	:11 devname=FG-M srcport=54256 srci ="Brazil" srccountry igh devtype="Error"	latera-Matriz devid=FC intf="wan1" dstip=172 ="United States" trand ' mastersrcmac=b8:af:	G200D3913805186 logid=000000013 type=traffic subtype=forward l 2.160.45.111 dstport=3389 dstintf="port16" sessionid=193737894 pro disp=noop service="RDP" duration=0 sentbyte=0 rcvdbyte=0 sentpkt 67:f6:06:d9 srcmac=b8:af:67:f6:06:d9

• **Fortinet- Traffic denied details-** This report provides details about all the traffic denied by the Fortinet firewall.

LogTime Device Name	Bytes B Sent R	lytes leceived	Source IP Address	Source Port	Destination IP Address	Destination Port	Priority	Action	Source Interface	Destination Inteface	Source Country	Destination Country	Virtual Domain
10/18/2017 05:49:07 PM FG-Matera- Matriz	00		108.166.82.18 1	54256	201.16.252.12	3389	notice	deny	wan1	port16	United	Brazil	root

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
 10/30/2017 5:21:39 PM Event Type: Information Log Type: Application Category Id: 0 	3333 Descriptio Feb 19 vel=no o=6 ac	NTPLDTBLR38 / Fortin n: 23:26:11 cpsutmfw01 time=23:26 titce vd=root srcip=192.168.11.10 tition=deny policyid=0 dstcountry: w=30 craction=131072 crawel=b	N/A :11 devname=FG-N 1 srcport=54256 src ="Brazil" srccountry inh devtypa="From	N/A Matera-Matriz devid=F(cintf="wan1" dstip=17/ /="United States" trand " macters:rmar=b8:8f	Syslog S200D3913805186 logid=0000000013 type=traffic subtype=forward le 2.160.45.111 dstport=3389 dstintf="port16" sessionid=193737894 prot lisp=noop service="RDP" duration=0 sentbyte=0 rcvdbyte=0 sentpkt= 6.7fc96v9 scrmac=b8aff57fc96v9



• Fortinet- VPN logon details- This report provides details of all the VPN logon details.

LogTime	Computer	Device Name	User Name	Source IP Address	Source Port	Destination IP Address	Destination Port	Action	Status	Event Details
10/30/2017 04:58:51 PM	FORTINET	FG300C39136 06597	"N/A"	1270.0.1	4500	1270.0.2	1659	negotiate	failure	"progress IPsec phase 1"
10/30/2017 04:58:51 PM	FORTINET	FG300C39136 06597	"N/A"	1270.0.1	4500	1270.0.2	1 659	negotiate	negotiate_ error	"IPsec phase 1 error"
10/30/2017 04:58:51 PM	FORTINET	FG300C39136 06597	"jens.weber "			1270.0.1		"ssl-login- fail"		"SSL user failed to logged in"

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
 10/30/2017 5:21:38 PM Event Type: Information Log Type: Application Category Id: 0 	3333 Descriptio date=2 ="prog 000000	NTPLDTBLR38 / <u>Fortin</u> n: 015-04-10 time=20:26:33 devname ress IPsec phase 1° action=negotia 0000000000° user="N/A° group="	N/A e=FRT123 devid=FG: te remip=1270.0.2 k N/A" xauthuser="N/	N/A 300C3913606597 logid=01010 ocip=1270.0.1 remport=1659 l A" xauthgroup="N/A" vpntun	Syslog 137128 type=event subtype=vpn level=error vd="root" msg ocport=4500 outintf="port10" cookies="38c1bf7739f47688/ nel="N/A" status=failure init=remote mode=main dir=inbou
	nd stag	e=1 role=responder result=ERROF	2		

• **Fortinet- Configuration changes-** This report provides details of all the configuration changes done in the Fortinet firewall.

LogTime	Device Name	User Name	Event Details	Action	Changed Object Name	Changed Object Type
10/30/2017 04:58:51 PM	FG140XXXX	"user1"	"Edit system.wccp 101"	Edit	"101"	"system.wccp"
10/30/2017 04:59:28 PM	FG140XXXX	"user1"	"Edit system.wccp 101"	Edit	"101"	"system.wccp"
10/30/2017 05:21:38 PM	FRT123XXXX	"user1"	"Edit system.wccp 101"	Edit	"101"	"system.wccp"



	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 10/30/2017 5:21:38 PM	3333	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	date=20 ualDom ttr="pas 8kDmd/ yD/0nrli 7ZhTkYI	n: 015-05-18 time=14:13:48 devname iain" logdesc="Configure object att ssword[ENC K7taRRarXYdpNvARTq AICJeFVHJG99J1gwVhxqjz6cmWSF5 Q6JHH0Dir6kdtDCtdrT5f9/Gfwxmkd NmpxCI55PdHFZeGROMjvhf87cSw	=FRT123XXXX devid iribute" user="user1" ktleNcecPbJB6gsRQJ 5al6FcgAfyk4gjh4yJe mAS7hNS+Tidmrrcz sGjHpskFk4ug==]" n	=FG140XXXXT logid=0100044 ui="jsconsole" action=Edit cft PLKjjftFAj81qnhoGStE4PKI9PGj 0p/oWks3bXxCT2Q/6juahXAlq cf1FNdedglQlt6gVx+C1J63RW nsg="Edit system.wccp 101"	547 type=event subtype=system level=information vd="Virt tid=1790967809 cfgpath="system.wccp" cfgobj="101" cfga Yodn/Z/f26bcGG0FDpsq4scG2MONwrNuV973xkizVF/YawO IBtIY9ZJCMJw==->ENC K7taRTt0SmYF1SbAdZes1UJbKzwzF tOp+D68aDScOgBXkO05An3o8EGo4+GyYIr1yUtG1QEGYIbJ

• **Fortinet- Application control-** This report provides details about all the application control policies and the rules defined by the Fortinet firewall.

LogTime	Device Name	Priority	Virtual Domain	Source IP Address	Source Port	Destination IP Address	Destination Port	Action	Application Name	Application Category	Requested URL	Service Name	Event Details	Source Interface	Destination Inteface
10/23/2017 06:06:36 PM	Fortinet	in formation	root	10.0.49.228	62292	31.13.67.11	443	pass	Facebook	Social.Media	1	HTTPS	Social.Media : Facebook,	port12	port9
10/23/2017 06:06:36 PM	Fortinet	in formation	root	10.16.40.10 6	55985	52.15.116.208	443	pass	HTTPS.BRO WSER	Web.Client	1	HTTPS	Web.Client: HTTPS.BRO WSER,	port10	port9
10/23/2017 06:06:36 PM	Fortinet	in formation	root	10.16.40.10 6	55984	52.15.116.208	443	pass	HTTPS.BRO WSER	Web.Client	1	HTTPS	Web.Client: HTTPS.BRO WSER,	port10	port9

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
10/30/2017 5:21:39 PM	<u>3333</u>	NTPLDTBLR38 / Fortin	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Descriptio Sep 06 I" even dstport almer / ="/" m:	n: 13:24:29 inet1 date=2017-09-06 ttype="app-ctrl-all" level="inforr t=443 srcintf="port12" srcintfrole Application Control Internal" app sg="Social.Media: Facebook," ap	time=13:24:29 de nation" vd="root" ="lan" dstintf="po cat="Social.Media" prisk="medium" so	vname=FRT123 devid=F logtime=1504722269 ap rt9" dstintfrole="wan" p ' app="Facebook" action certcname="*.facebook.c	G900D3915800932 logid="1059028704" type="ut pid=15832 srcip=192.168.11.101 dstip=172.160.4 roto=6 service="HTTPS" policyid=283 sessionid=: ="pass" hostname="*.facebook.com" incidentseria .com"	m" subtype="app-ctr 5.111 srcport=62292 377512625 applist="P alno=443331406 url



6.3 Dashboard

• Fortigate Firewall- Login Failed by User





• Fortigate Firewall- Intrusion Detection by Destination IP Address





• Fortigate Firewall- Intrusion Detection by Source IP Address

Fortigate Firewall- Login Failed by Geo-Location.. C → × Image: Comparison of the comparison of t

• Fortigate Firewall- Login Failed by Geo-Location



• Fortigate Firewall- Intrusion Detection by Threat Name



• Fortigate Firewall- Login Failed by Source IP





• Fortigate Firewall- Intrusion Detection by Source IP Geo-Location



Fortigate Firewall- Login Activities by User

• Fortigate Firewall – Login Activities by User





• Fortigate Firewall- Login by Source IP Address



• Fortigate Firewall- Login by Source IP Geo-location







Image: Sep 08 05:48 PM - Sep 15 05:49 PM

• Fortigate Firewall- Traffic by Destination IP address



• Fortigate Firewall- Traffic by Source IP Geo-Location



• Fortigate Firewall- Traffic by Destination IP Geo-Location





7 Import Fortinet Firewall Knowledge Pack

Import the Knowledge Pack items in the following sequence.

- Category
- Alerts
- Token Template
- Flex Reports
- Knowledge Objects
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click the Export Import Utility, and click the Import tab.





7.1 Alerts

1. In the **Import** tab, click **Alerts**, and then click the **Browse** button to locate the file.

I. Provide the path and file na 2. Click the Import button.	ame of the Alerts file. Use the '' buttor	to browse and locate the import file.	
Options	Location		
Category			
Filters	👿 Import E-mail settings		
Alerts	Set Active		
	Only if notifications set	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set	
Systems and Groups	Bu default	based on "Active" key available in the configuration	
RSS Feeds		section.	
Reports	Source :		
	*.isalt		
Behavior Hules			
SCAP			
🔘 Token Value			

- 2. In the Browse window, locate the Fortinet Firewall.isalt file, and then click Open.
- **3.** To import alerts, click **Import**.
- 4. EventTracker displays a success message on successfully importing the selected file in Alerts.



5. Click **OK** or the **Close** button to complete the process.



7.2 Token Template

1. In the EventTracker Manager console, hover over the Admin menu and click Parsing Rules.



- 2. In the Parsing Rules interface, click the Template tab.
- 3. Click the Browse button and locate the .ettd file, and then click Open.

Impo	Import									
selecte	d file is: Template_Fortigate F	irewall.ettd	🖀 Browse							
	Template name	Separator	Template description	Added date	Added by	Group Name				
	Fortigate Firewall	\n	Feb 19 23:26:11 cpsutmfw01 time=23:26:11 devname=FG-Matera-Matriz devid=FG200D3913005186 logid=0000000013 type=traffic subtype=forw and level-notice vd-root scrip=10.8:16:86:2181 srcpot=5255 scrintf="v an1" dstip=201.16:25:21 dstport=3389 dstintf="port16" sessionid=1937 37894 proto=6 action=deny policyid=0 dstcountry="Brazil" srccountry ="United States" transfig=noop service=TDP" duration=0 sentbyte=0 to vdbyte=0 sentpkt=0 crscore=30 craction=131072 crlevel=high devtype = "Error" mastersrcmac=b8:a67/f6:06:d9 srcmac=b8:a667/f6:06:d9	May 09 04:28:39 AM	ETAdmin	Fortigate Firewall				

- **4.** Select the template check box and then click the **Import** I button.
- 5. EventTracker displays a successful message on successfully importing the selected Template file in **Template**.

Template(s) importe	d successfully
	ОК

6. Click **OK** or the **Close** button to complete the process.



7.3 Flex Reports

Note : If report(s) contains temp	olate, first im	port template and proceed	with exportimport utility.		
Options	Location	1			
Category					
O Filters					
◯ Alerts		O Legacy (*.issch)	• New (*.etcrx)		
O Systems and Groups		Source :			
O RSS Feeds		".issch			
 Reports 					
O Behavior Rules					
⊖ SCAP					
O Token Value					

1. In the Import tab, click Reports and then click New (*.etcrx).

2. In the **Reports Import** window, click **Select file** to locate the **Fortinet Firewall.issch** file, and then click **Open**.

3 Rep	orts im	port				>
Note :	If report	t(s) contains template, first import template a	nd proceed with exportimport utility.			
Selec	t file	E:\My KP\Fortinet\Fortinet Reports(4.0-5.6).etcrx		Select file	
Availa	ble repo	rts				
Title			Frequency Show all	- Q Q		
		77.1				-
H	CDIT	litie	Sites	Groups	Systems	Frequency
	EDIT	Fortinet (All) Administrator logon details	NTPLUTBLR38	Event fracker	Fasters	Undefined
	EDIT	Fortinet (All) Attack detected		Event Tracker	Fortinet	Undefined
	EDIT	Fortinet (All)-Configuration change details		EventTracker		Undefined
	EDIT	Fortinet (All)-Data leak detected	NTPLDTBLB38	EventTracker		Undefined
Π	FDIT	Fortinet (All)-Suspicious email content	NTPLDTBLR38	EventTracker		Undefined
П	EDIT	Fortinet (AII)-Suspicious web content d	NTPLDTBLR38	EventTracker		Undefined
Π	EDIT	Fortinet (All)-Traffic alloweddetails	NTPLDTBLR38	EventTracker		Undefined
	EDIT	Fortinet (All)-Traffic denied details	NTPLDTBLR38	EventTracker		Undefined
	EDIT	Fortinet (AII)-User authentication details	NTPLDTBLR38	EventTracker	NTPLDTBLR38	Undefined
	<u>EDIT</u>	Fortinet (AII)-Virus detected	NTPLDTBLR38	EventTracker		Undefined
	EDIT	Fortinet (All)-VPN logon details	NTPLDTBLR38	EventTracker	NTPLDTBLR38	Undefined
<						>
Not Sel	e: Set ru t run ti r	In time option is not applicable for Defined F ne for report(s) from	Reports and Hourly Reports	es Set		
				Note: Make sure that Site(s)	Group(s) and System(s) selections are vali	d. 耳 🛛 😣



- 3. Select the check box of all the files and click the **Import** \mathbb{T} button to import the selected files.
- 4. EventTracker displays a success message on successful importing of the selected file in **Reports**.

Export Import Utility	x
Selected reports configurations are imported successfully	
ОК	

5. Click **OK** or the **Close** button to complete the process.

7.4 Knowledge Objects (KO)

1. In the EventTracker Manager console, hover over the Admin menu and click Knowledge Objects.

≡	Event Tracker ⊕					. Admin∙	Tools +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
Q		_	Alerts	Correlation	🔍 IP Lookup Configuration	🙊 Users	_
	0	1	Behavior Correlation Rules	Diagnostics	☆ Knowledge Objects	r Weights	
			🏷 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Seventvault	🕖 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Knowledge Objects interface, click the Import \mathbb{T} button to import the KO files.





3. In the Import window, click Browse and locate the .etko file.

Import			×
Select	file		The Browse Upload
	Object name	Applies to	Group name
	Fortigate Firewall	FortiOS 4.0 to 6.0	Fortigate Firewall
			Import Close

- 4. Select the check box and then click the **OVERWRITE** option.
- 5. EventTracker displays a successful message on successfully importing the selected file in Knowledge Objects.

File imported successfully.	
ОК	

6. Click **OK** or the **Close** button to complete the process.

7.5 Dashboard

1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.

-	Home			
٩	My Dashboard			
2	Threats		1	
	Incidents	ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit			-
	Compliance			



2. In the My Dashboard interface, click the Import \mathbb{T} button to import the dashlet files.



- **3.** In the **Import** window, click **Browse** to locate the file with the **.etwd** extension (for example **Dashboards_Fortinet Firewall.etwd**) and then click **Upload**.
- **4.** Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.

Import		
Note: If dashlet configured using persisted report, first import the report and proceed with im	porting dashlet.	
	🗁 Browse	Upload
Available widgets		
	Import Clo	ose

5. The EventTracker displays the success message on successfully importing the dashlet files.





8 Verify Fortinet Firewall Knowledge Pack

8.1 Alerts

1. In the EventTracker web interface, hover over the Admin menu and click Alerts.

≡	Event Tracker ⊕					🔎 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
a			Alerts	Correlation	🔍 IP Lookup Configuration	였 Users	
	0	2	Behavior Correlation Rule	Diagnostics	💮 Knowledge Objects	r Weights	
			🗞 Behavior Correlation Sett	ings Event Filters	😟 Manager	Windows Agent Config	
	Potential Cyber Breaches Indicators of Unsafe connections or processes, new TCP entry point USB activities. New		Casebook Configuration	Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

- 2. In the Alerts interface, type Fortinet in the search field, and click the Search Search button.
- 3. The Alerts interface will display all the imported Fortinet alerts.

AL	ERT MANAGEMEN	NT		Sho	w All		▼ Sea	rch by Ale	ert name 🔻	fort	୍ଦ୍
•	ACTIVATE NOW Click 'Activ	vate Now' after makin	ig all chang	ges						Total: 15	Page Size 25 V
	ALERT NAME	THREAT	<u>ACTIVE</u>	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
	Fortinet: Data Leak Protection	High									Fortinet 4.0-5.6
	Fortinet:Administrator Logon Failed	High									Fortinet 4.0-5.6
	Fortinet:Attack Detected	High									Fortinet 4.0-5.6
	Fortinet:Configuration Changed	High									Fortinet 4.0-5.6
	Fortinet:Virus Detected	High									Fortinet 4.0-5.6
DE	LETE										

- 4. To activate the imported alerts, click **Active**, which is available next to the respective alert name.
- 5. EventTracker displays a success message on successfully configuring the alerts.





6. Click OK and click Activate now to activate the alerts after making the required changes.

Note

You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

In the Alert Configuration interface, specify the appropriate System for better performance.

8.2 Token Template

- 1. In the EventTracker web interface, hover over the Admin menu and click Parsing Rules.
- 2. Go to the **Template** tab and click the **Fortinet Firewall** group folder to view the imported Token template.

Parsing Rules									† /	Admin / Parsing Rules
Parsing Rule Template										
Groups		Ð		Group : Fortigate Firewall	Search	Q				CİI
Fortigate Firewall	前	Ø	*			•				
Nginx Web Server	Û	Ø		Template Name	Template Description	Added By	Added Date	Active		
Palo Alto Firewall	前	(A)	•	Fortigate Firewall	Fortigate all tokens(4.0-6.0)	ETAdmin	May 25 02:25:39 AM		Ø	
									Delete	Move to group

8.3 Flex Reports

1. In the EventTracker web interface, click the Reports menu, and then click Report Configuration.

	Event Tracker ⊕			
-	Home			
٩				
R	Report Configuration		1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer			
	Аπаскег	1		-

2. In the Reports Configuration interface, select the Defined option.



- 3. In the **Report Groups Tree** scroll down and click the **Fortinet Firewall** group folder to view the imported **Scheduled Reports**.
- 4. EventTracker displays the reports for Scheduled Reports in the Reports configuration pane.

Repo	Reports configuration: Fortigate Firewall											
Ð	Ē <i>2</i> ,					Total:	17					
		Title	Created on	Modified on								
	2	Fortigate- User login and logout	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	()	5	+					
	£ 5 3	Fortigate- SSL VPN user login failure	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	8	+					
	£ 5 3	Fortigate- Administrator login and logout	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	8	+					
	£\$3	Fortigate- Configuration change details	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	5	+					
	££3	Fortigate- IPS attacks detected	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	8	+					
	£ £ 3	Fortigate- Suspicious web content detected	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	5	+					
	£ 3 3	Fortigate- Suspicious email content detected	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	5	+					
	£ 3 3	Fortigate- Data leak detected	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	5	+					
	₹ £ 3	Fortigate- Virus detected	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	5	+					
	2	Fortigate- Traffic allowed details	Sep 15 01:52:33 PM	Sep 15 01:54:01 PM	(i)	8	+					

Note

Specify the appropriate **systems** in the **report wizard** for better performance.

8.4 Knowledge Objects (KO)

- 1. In the EventTracker web interface, hover over the Admin menu and click Knowledge Objects.
- 2. Scroll down and select **FortiGate** in **Objects** pane, and the imported FortiGate object details will be displayed.

Knowledge Ob	jects						♠ /	Admin / Knowledge Ob	jects
fortigate	C	Activate Now						Objects 🕂 🖡 🏦	۵
Groups	⊕ Ø Î	Object name Fortigate Firewall Applies to FortiOS 4.0 to 6.0						÷ 1	¢
Fortigate Firewall	Ø 🗓	Rules							
		Title	Event source	Source Type	Log type	Event id	Event type		
		+ Fortigate Firewall	syslog*	Fortigate Firewall				🧭 🕑 🗓 🔗	
		Message Signature:							
		Message Exception:							
		Expressions							
		Expression type	Expression 1			Expression 2	Format string		
		Regular Expression	(? <key>[^\s]+)[=][""]?(?<value< td=""><td>>[^=*]+)[**\\$]</td><td></td><td></td><td></td><td></td><td>Ĩ</td></value<></key>	>[^=*]+)[**\\$]					Ĩ



8.5 Dashboard

In the EventTracker web interface, go to Home > My Dashboard, and click the Customize dashlets
 button.



2. In the **Customize dashlets** interface, search for **Fortigate** in the search field.



3. The following Fortinet Firewall dashlet files will get displayed.

Customize dashlets			×
fortigate			Q
Generation Accessed	Fortigate-Events	□ Fortigate-Traffic by Destination	□ Fortigate-Traffic by Source IP A
□ Fortigate-Traffic by Priority	Fortigate-VPN Accessed by User	□ Fortigate-VPN Traffic by Direction	
			Add Delete Close



About Netsurion

Netsurion[®] delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with yourIT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at <u>netsurion.com</u>.

Contact Us

Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2) EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3) EventTracker Essentials SOC: 877-333-1433 (Option 4) EventTracker Software Support: 877-333-1433 (Option 5) https://www.netsurion.com/eventtracker-support