Integration Guide

Integrate Fortinet Firewall with EventTracker

Publication Date:

September 16, 2022

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 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.

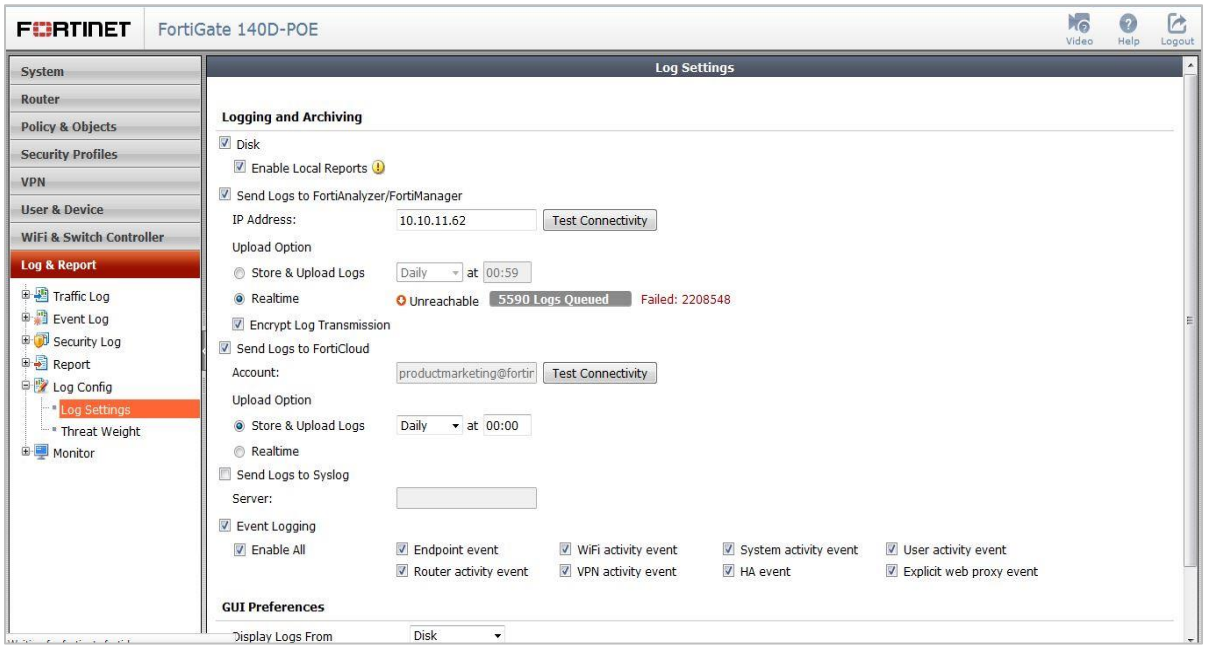
2 Prerequisites

- 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.



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.

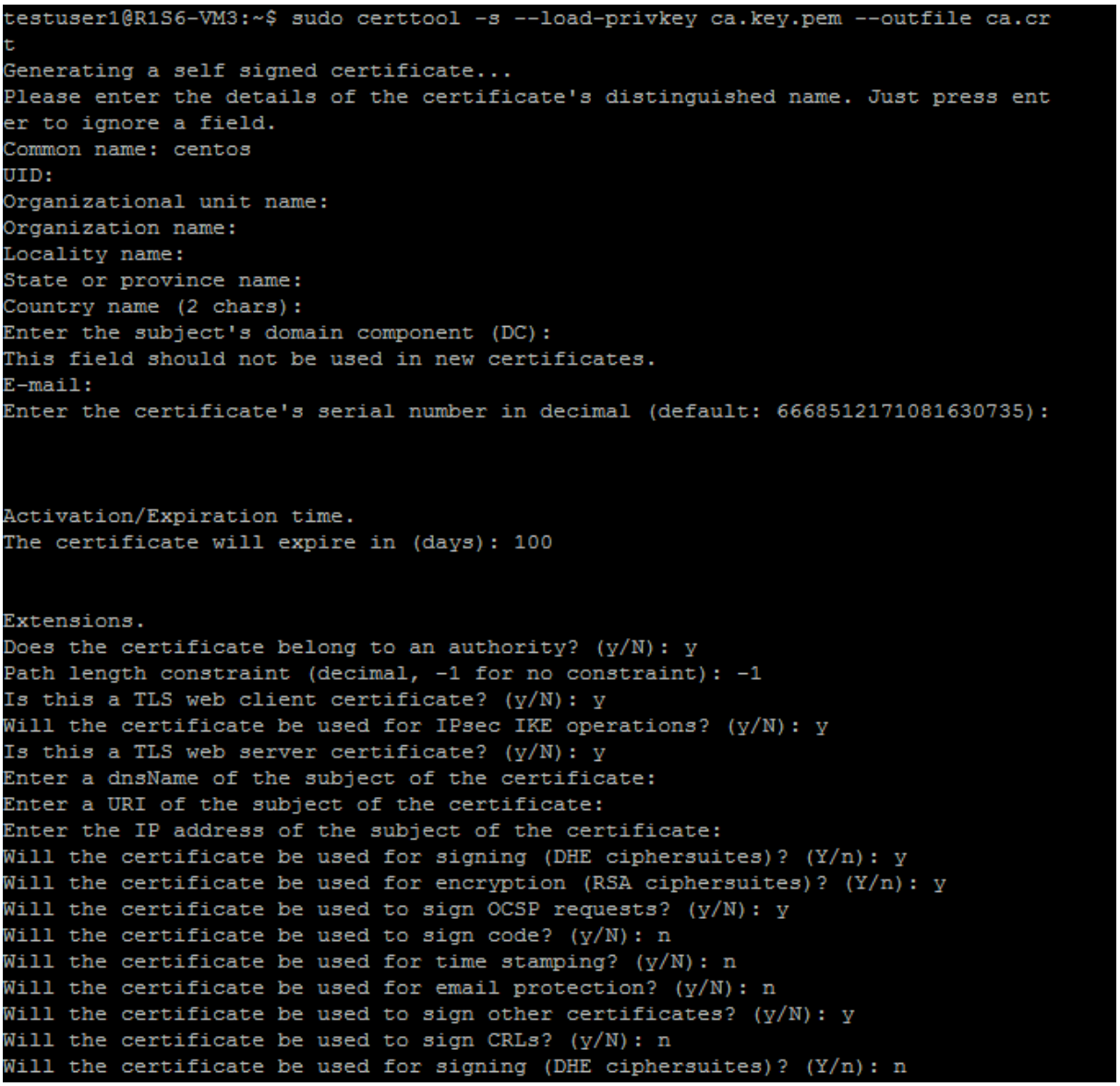
Command: `certtool -p --outfile ca.key.pem`

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.



```
Enter 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):
                        00:c8:a2:3d:a3:8e:16:88:ea:fa:bb:a4:99:d8:65:73
                        62:1d:3f:6e:08:00:52:62:f8:0a:cc:68:98:58:36:40
                        29:d2:ea:06:08:9e:74:d1:81:d9:8c:38:91:11:04:b2
                        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
                        3b:07:b0:df:84:b3:8b:bc:0c:01:2b:1b:62:cb:ae:9a
                        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
                        1d:f6:fc:b5:62:73:6d:75:a8:99:20:6f:72:38:1a:ed
                        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
                        03
                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:fHYIdAN0eIS/+53+JmWuyOQvd1j5LrRlx7EBvNyTbIk=
        Public key's random art:
                +--[ RSA 3072]----+
                |      ooo.+o.oo  |
                |     o . . .oo.  |
                |      * .    ..= |
                |     o =      +=+|
                |      = S    .o.o|
                |     o o     o   |
                |    . . .     o  |
                |     o         E |
                |    .            |
                +-----------------+

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: **ls**

> **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.

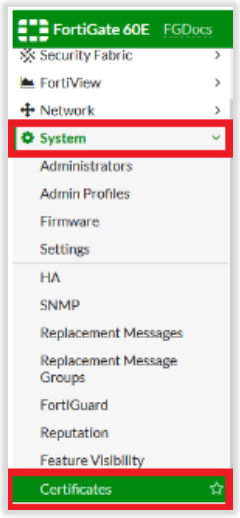
11. Specify the certificate to communicate with the Syslog server.

```
set certificate "<certificate local path>"
```

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

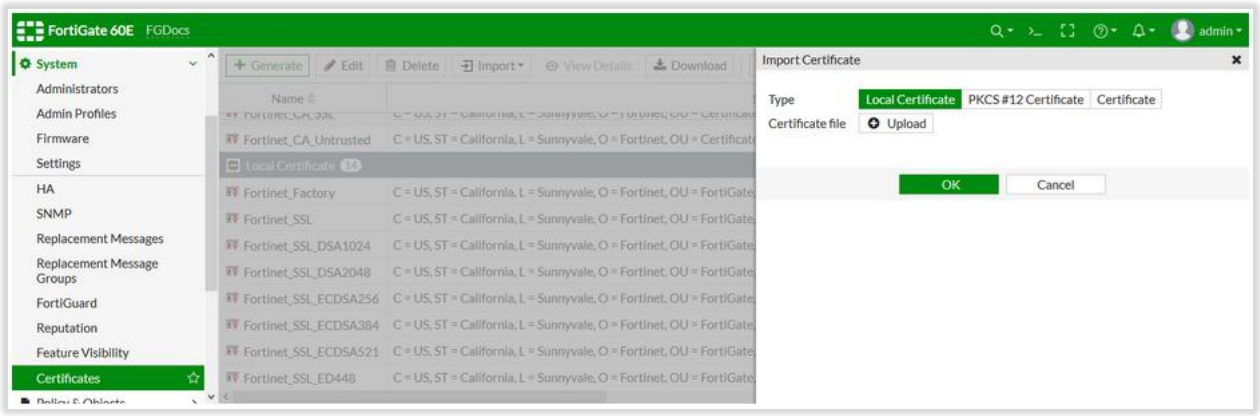
Importing Certificates

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

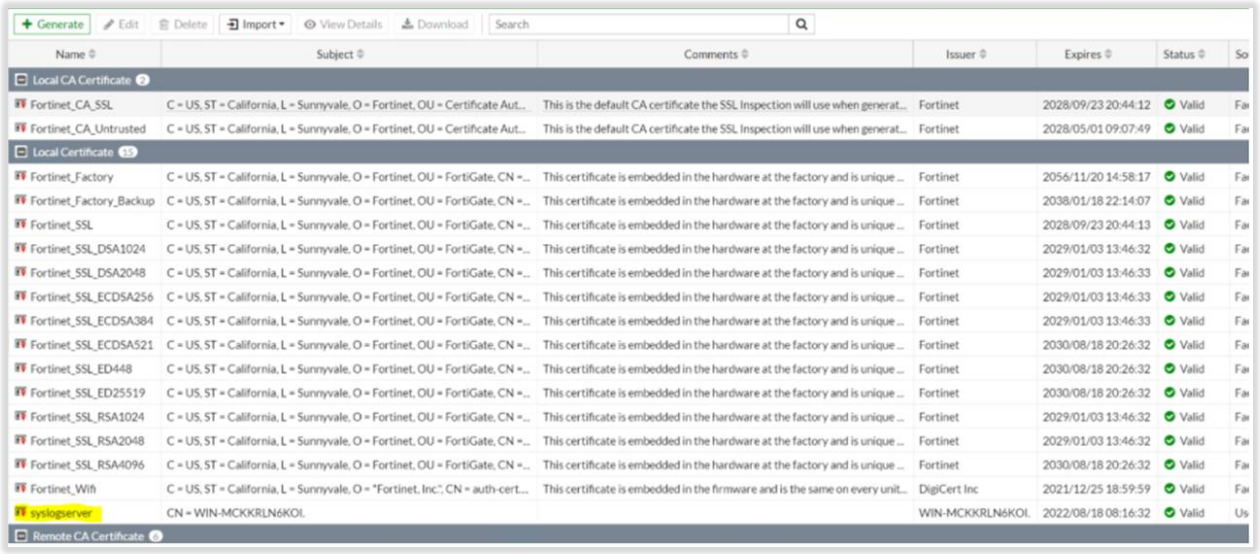


3. Click **Import** > **CA Certificate**.

4. Set the **Type** to File, upload the **CA** certificate file, then click **OK**.



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



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"

Logs Considered:

LOG TIME	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=2007-07-01 time=20:29:01 devname=FRT123 device_id=FGT0000000000001 log_id=000000001 type=event subtype=auth pri=notice vd=root prot o=1 src=196.111.14.54:1051 dst=118.12.10.99:81 adgroup="Mobi_Tel" user="Peter" ui=10.1.1.21:80(6) action=FSAE-auth status=failure msg="AD group Mobi_Tel user Peter failed in authentication"

- **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	information	vdom1	admin	login	failed	super_admin	Administrator admin logged in failed from console
10/18/2017 05:49:07 PM	FORTINET	information	vdom1	admin	login	success	super_admin	Administrator admin logged in successfully from console

Logs Considered:

LOG TIME	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(172.16.86.1) action=login s 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	3333	NTPLDTBLR38 / Fortin...	N/A	N/A	Syslog

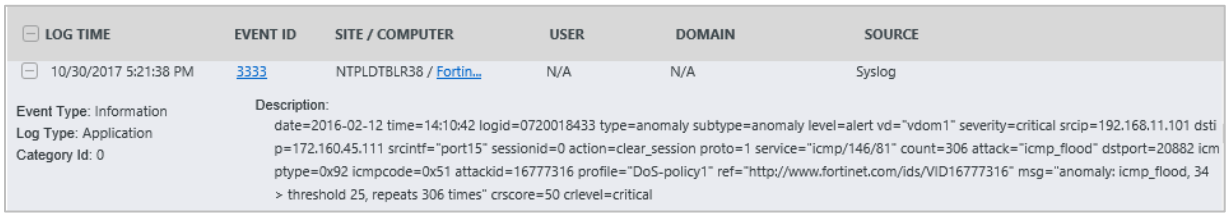
Event Type: Information
Log Type: Application
Category Id: 0

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_session	16777316	icmp_flood	icmp/146/81	http://www.fortinet.com/ids/VID16777316	vdom1	port15	critical	50

Logs Considered:

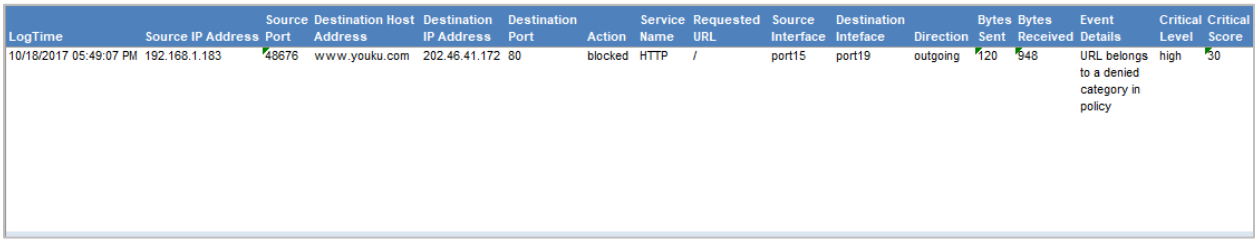


LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
10/30/2017 5:21:38 PM	3333	NTPLDTBLR38 / Fortin...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

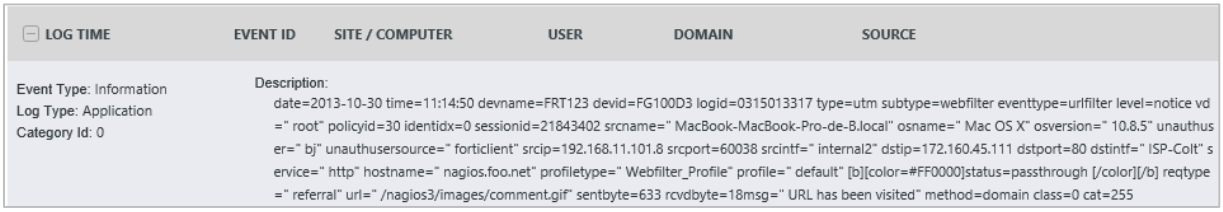
Description:
date=2016-02-12 time=14:10:42 logid=0720018433 type=anomaly subtype=anomaly level=alert vd="vdom1" severity=critical srcip=192.168.11.101 dstip=172.160.45.111 srcintf="port15" sessionid=0 action=clear_session proto=1 service="icmp/146/81" count=306 attack="icmp_flood" dstport=20882 icmptype=0x92 icmpcode=0x51 attackid=16777316 profile="DoS-policy1" ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 34 > threshold 25, repeats 306 times" crscore=50 crlevel=critical

- **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	/	port15	port19	outgoing	120	948	URL belongs to a denied category in policy	high	30

Logs Considered:

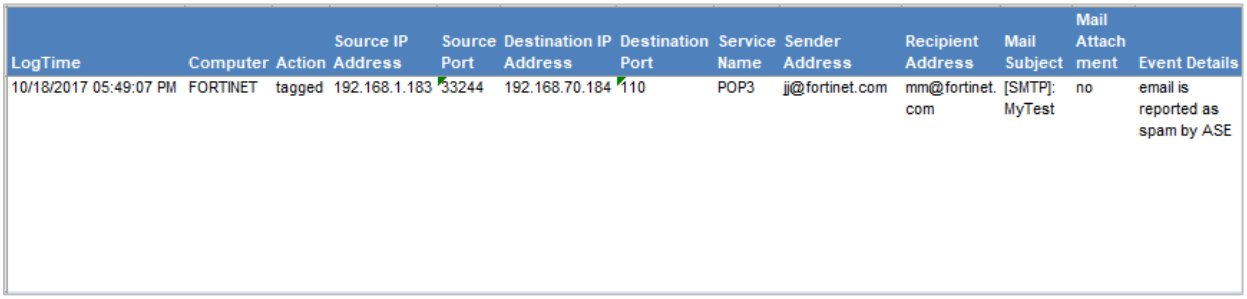


LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE

Event Type: Information
Log Type: Application
Category Id: 0

Description:
date=2013-10-30 time=11:14:50 devname=FRT123 devid=FG100D3 logid=0315013317 type=utm subtype=webfilter eventtype=urlfilter level=notice vd=" root" policyid=30 identidx=0 sessionid=21843402 srcname=" MacBook-MacBook-Pro-de-B.local" osname=" Mac OS X" osversion=" 10.8.5" unauthuser=" bj" unauthusersource=" forticlient" srcip=192.168.11.101.8 srcport=60038 srcintf=" internal2" dstip=172.160.45.111 dstport=80 dstintf=" ISP-Colt" service=" http" hostname=" nagios.foo.net" profiletype=" Webfilter_Profile" profile=" default" [b][color=#FF0000]status=passthrough [/color][/b] reqtype=" referral" url=" /nagios3/images/comment.gif" sentbyte=633 rcvdbyte=18msg=" URL has been visited" method=domain 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	Action	Source IP Address	Source Port	Destination IP Address	Destination Port	Service Name	Sender Address	Recipient Address	Mail Subject	Mail Attachment	Event Details
10/18/2017 05:49:07 PM	FORTINET	tagged	192.168.1.183	33244	192.168.70.184	110	POP3	jj@fortinet.com	mm@fortinet.com	[SMTP]: MyTest	no	email is reported as spam by ASE

Logs Considered:

LOG TIME	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=2016-02-12 time=14:01:12 logid=0509020482 type=utm subtype=emailfilter eventtype=pop3 level=notice vd="vdom1" sessionid=64465 user="" srcip=192.168.11.101 srcport=33244 srcintf="port15" dstip=172.160.45.111 dstport=110 dstintf="port19" proto=6 service=POP3 profile="default" action =tagged from="jj@fortinet.com" to="mm@fortinet.com" recipient="testpc3" sentbyte=27 rcvdbyte=1592 direction=incoming msg="email is reported as spam by ASE" subject="[SMTP]: MyTest" attachment=no

- **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 Address	Destination Port	Action	File Type	File Name	Requested URL	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	30170	incoming	Wget/1.10.2

Logs Considered:

LOG TIME	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=2014-05-01 time=11:54:37 devname=FRT123D devid=FG100D3G12812498 logid=0954024577 type=utm subtype=dlp eventtype=dlp level=notice vd="root" filteridx=0 filtertype=none filtercat=none policyid=8 identidx=1 sessionid=8774608 epoch=2043380188 eventid=0 user="USRNAME" srcip=192.168.11.101 srcport=60439 srcintf="internal" dstip=172.160.45.111 dstport=80 dstintf="wan2" service=http filetype="unknown" sentbyte=0 rcvdbyte=0 hostname="1.2.com" url="/ws/ps.asmx/GetMailcount" file="GetMailcount" action="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.fortinet.com/ve?vn=EICAR_TEST_FILE	http://192.168.70.184/eicar.com	blocked	incoming	eicar.com	vdom1	File is infected.	Wget/1.10.2	HTTP	port15	port19	50	critical

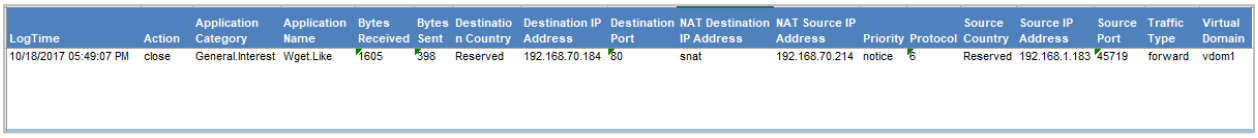
Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
10/30/2017 5:21:39 PM	3333	NTPLDTBLR38 / Fortin...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

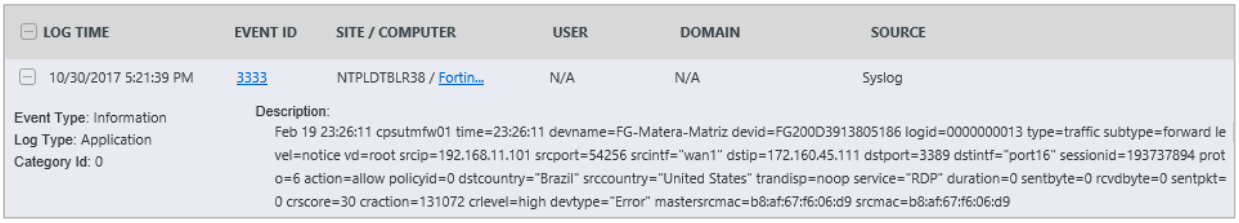
Description:
date=2016-02-12 time=11:11:25 logid=0211008192 type=utm subtype=virus eventtype=infected level=warning vd="vdom1" msg="File is infected." action=blocked service=HTTP sessionid=56633 srcip=192.168.11.101 dstip=172.160.45.111 srcport=45719 dstport=80 srcintf="port15" dstintf="port19" proto=6 direction=incoming filename="eicar.com" checksum="1dd02bdb" quarskip=No-skip virus="EICAR_TEST_FILE" dtype="Virus" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172 url="http://192.168.70.184/eicar.com" profile="default" user="" agent="Wget/1.10.2" analyticscksum="131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267" analyticssubmit=false crscore=50 crlevel=critical

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



LogTime	Action	Application Category	Application Name	Bytes Received	Bytes Sent	Destination Country	Destination IP Address	Destination Port	NAT Destination IP Address	NAT Source IP Address	Priority	Protocol	Source Country	Source IP Address	Source Port	Traffic Type	Virtual Domain
10/18/2017 05:49:07 PM	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:



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
10/30/2017 5:21:39 PM	3333	NTPLDTBLR38 / Fortin...	N/A	N/A	Syslog

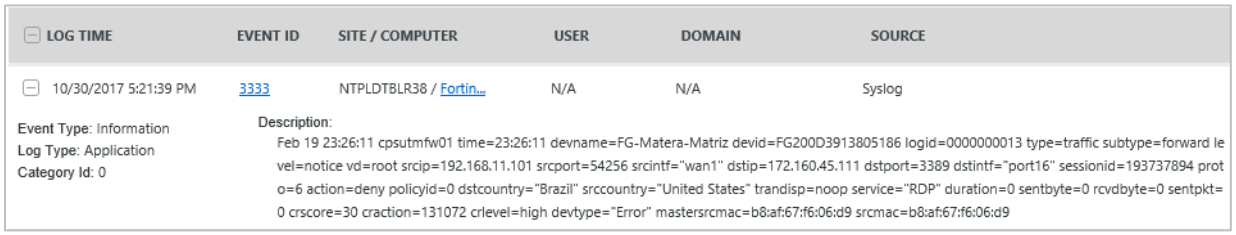
Event Type: Information
Log Type: Application
Category Id: 0

Description:
Feb 19 23:26:11 cpsutmfw01 time=23:26:11 devname=FG-Matera-Matriz devid=FG200D3913805186 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=192.168.11.101 srcport=54256 srcintf="wan1" dstip=172.160.45.111 dstport=3389 dstintf="port16" sessionid=193737894 proto=6 action=allow policyid=0 dstcountry="Brazil" srccountry="United States" trandisp=noop service="RDP" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 crscore=30 craction=131072 crlevel=high devtype="Error" mastersrcmac=b8:af: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 Sent	Bytes Received	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	0	0	108.166.82.181	54256	201.16.252.12	3389	notice	deny	wan1	port16	United	Brazil	root

Logs Considered:



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
10/30/2017 5:21:39 PM	3333	NTPLDTBLR38 / Fortin...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Feb 19 23:26:11 cpsutmfw01 time=23:26:11 devname=FG-Matera-Matriz devid=FG200D3913805186 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=192.168.11.101 srcport=54256 srcintf="wan1" dstip=172.160.45.111 dstport=3389 dstintf="port16" sessionid=193737894 proto=6 action=deny policyid=0 dstcountry="Brazil" srccountry="United States" trandisp=noop service="RDP" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 crscore=30 craction=131072 crlevel=high devtype="Error" mastersrcmac=b8:af:67:f6:06:d9 srcmac=b8:af:67:f6:06:d9

- **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	FG300C3913606597	"N/A"	1270.0.1	4500	1270.0.2	1659	negotiate	failure	"progress IPsec phase 1"
10/30/2017 04:58:51 PM	FORTINET	FG300C3913606597	"N/A"	1270.0.1	4500	1270.0.2	1659	negotiate	negotiate_error	"IPsec phase 1 error"
10/30/2017 04:58:51 PM	FORTINET	FG300C3913606597	"jens.weber"			1270.0.1		"ssl-login-fail"		"SSL user failed to logged in"

Logs Considered:

LOG TIME	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=2015-04-10 time=20:26:33 devname=FRT123 devid=FG300C3913606597 logid=0101037128 type=event subtype=vpn level=error vd="root" msg="progress IPsec phase 1" action=negotiate remip=1270.0.2 locip=1270.0.1 remport=1659 locport=4500 outintf="port10" cookies="38c1bf7739f47688/0000000000000000" user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" vpntunnel="N/A" status=failure init=remote mode=main dir=inbound stage=1 role=responder result=ERROR

- **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"

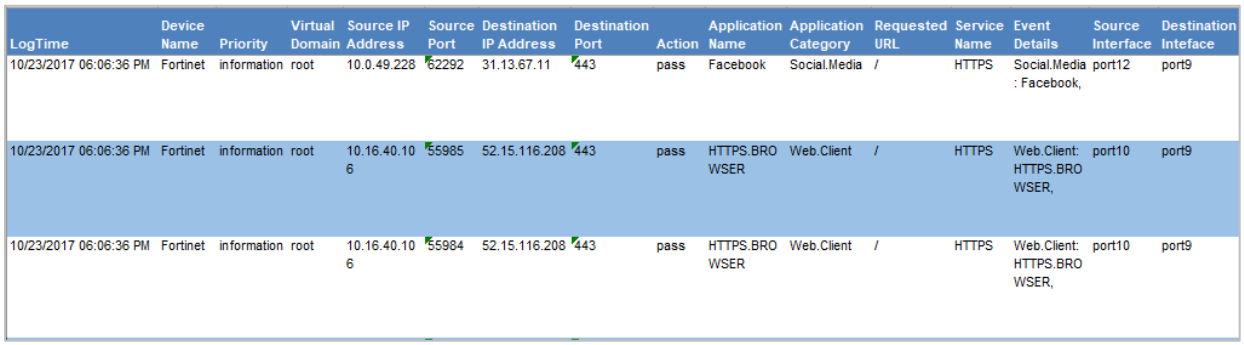
Logs Considered:

LOG TIME	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

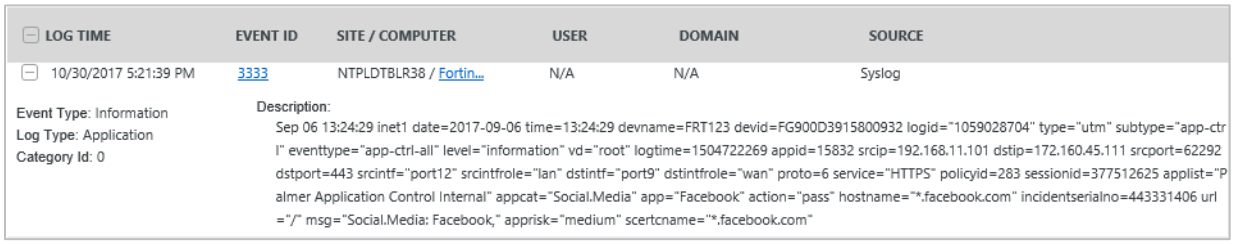
Description:
date=2015-05-18 time=14:13:48 devname=FRT123XXXX devid=FG140XXXXT logid=0100044547 type=event subtype=system level=information vd="VirtualDomain" logdesc="Configure object attribute" user="user1" ui="jsconsole" action=Edit cfgtid=1790967809 cfgpath="system.wccp" cfgobj="101" cfgattr="password[ENC K7taRRarXYdpNvARTqktleNcecPbJB6gsRQPLKjjftFAj81qnhoGStE4PKl9PGjYodn/Z/f26bcGG0FDpsq4scGzMONwrNuV973xkizVF/YawO8kDmdAlCJeFVHJG99J1gwVhxqjz6cmWSF5al6FcgAfyk4gjh4yJe0p/oWks3bXxCT2Q/6juahXAlqBtlY9ZJCMJw==->ENC K7taRTt0SmYF1SbAdZes1UJbKzwzFyD/0nrlQ6JHH0Dir6kdtDCtdrT5f9/GfwxmkmAS7hNS+Tidmrrczxf1FNdedgIQlt6gVx+C1J63RWtOp+D68aDScOgBXkO05An3o8EGo4+GyYlr1yUtG1QEGYlbJ7ZhTkYNmpxCi55PdHFZeGROMjvhfB7cSwsGjHpskFk4ug==]" msg="Edit system.wccp 101"

- **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	information	root	10.0.49.228	62292	31.13.67.11	443	pass	Facebook	Social.Media	/	HTTPS	Social.Media: Facebook,	port12	port9
10/23/2017 06:06:36 PM	Fortinet	information	root	10.16.40.106	55985	52.15.116.208	443	pass	HTTPS.BROWSER	Web.Client	/	HTTPS	Web.Client: HTTPS.BROWSER,	port10	port9
10/23/2017 06:06:36 PM	Fortinet	information	root	10.16.40.106	55984	52.15.116.208	443	pass	HTTPS.BROWSER	Web.Client	/	HTTPS	Web.Client: HTTPS.BROWSER,	port10	port9

Logs Considered:



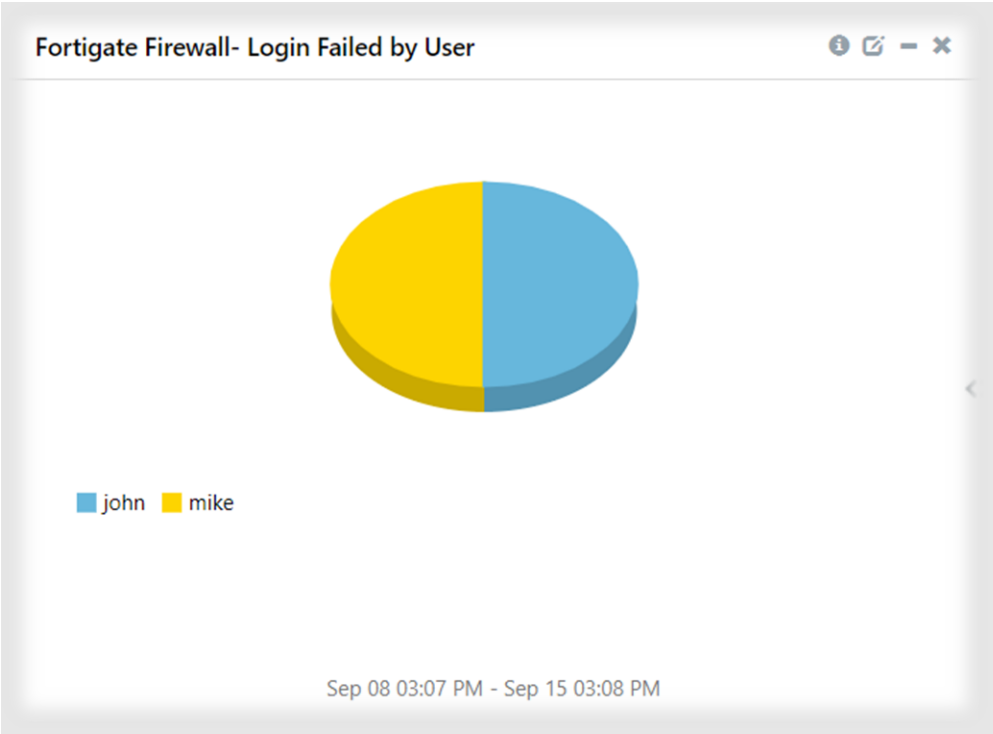
LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
10/30/2017 5:21:39 PM	3333	NTPLDTBLR38 / Fortin...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

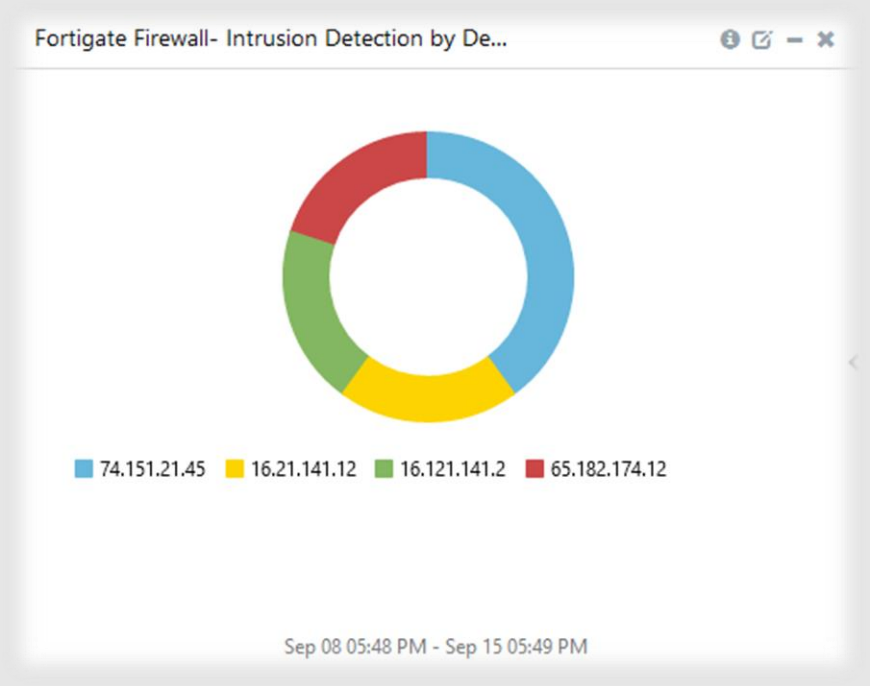
Description:
Sep 06 13:24:29 inet1 date=2017-09-06 time=13:24:29 devname=FRT123 devid=FG900D3915800932 logid="1059028704" type="utm" subtype="app-ctrl" eventtype="app-ctrl-all" level="information" vd="root" logtime=1504722269 appid=15832 srcip=192.168.11.101 dstip=172.160.45.111 srcport=62292 dstport=443 srcintf="port12" srcintfrole="lan" dstintf="port9" dstintfrole="wan" proto=6 service="HTTPS" policyid=283 sessionid=377512625 applist="Palmer Application Control Internal" appcat="Social.Media" app="Facebook" action="pass" hostname="*.facebook.com" incidentserialno=443331406 url="/" msg="Social.Media: Facebook," apprisk="medium" scertcname="*.facebook.com"

6.3 Dashboard

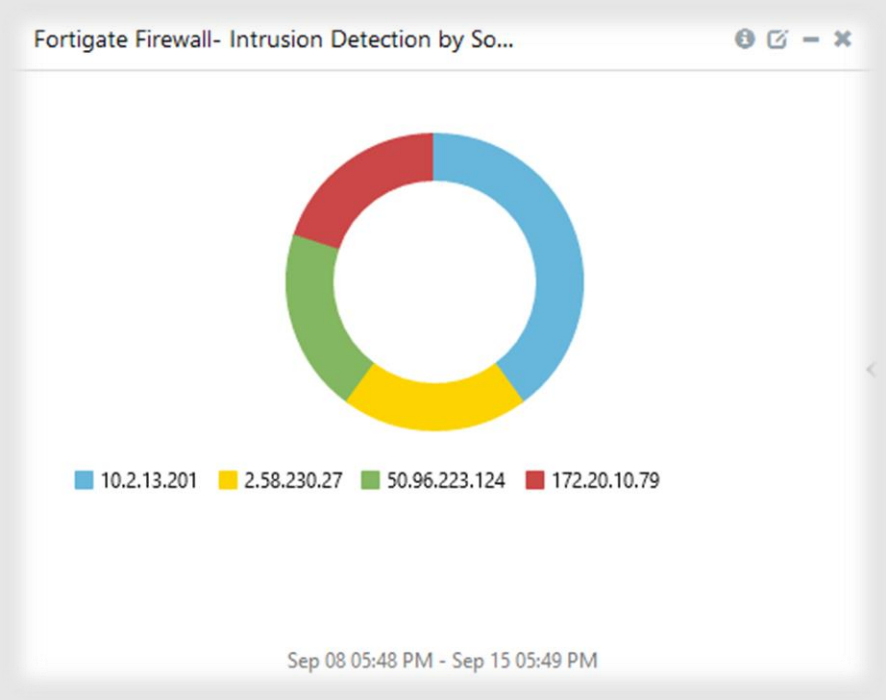
- **Fortigate Firewall- Login Failed by User**



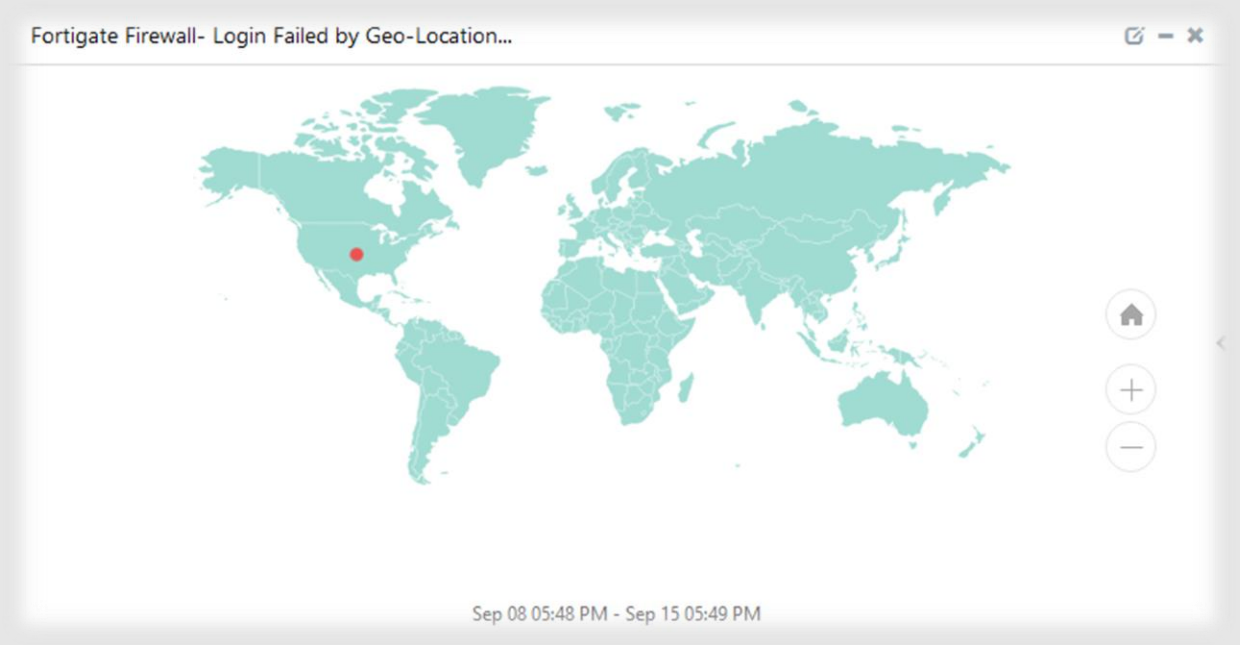
- **Fortigate Firewall- Intrusion Detection by Destination IP Address**



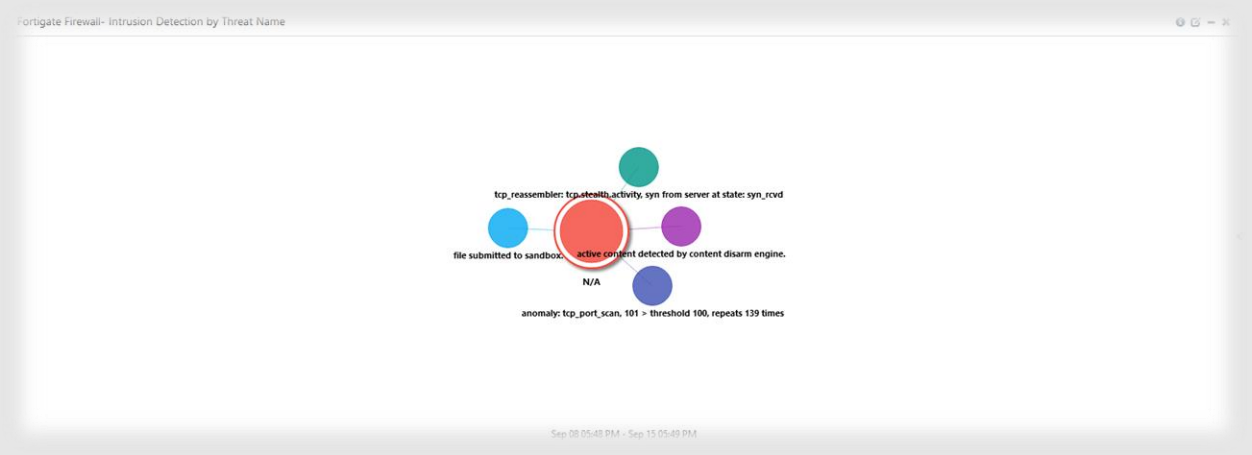
- **Fortigate Firewall- Intrusion Detection by Source IP Address**



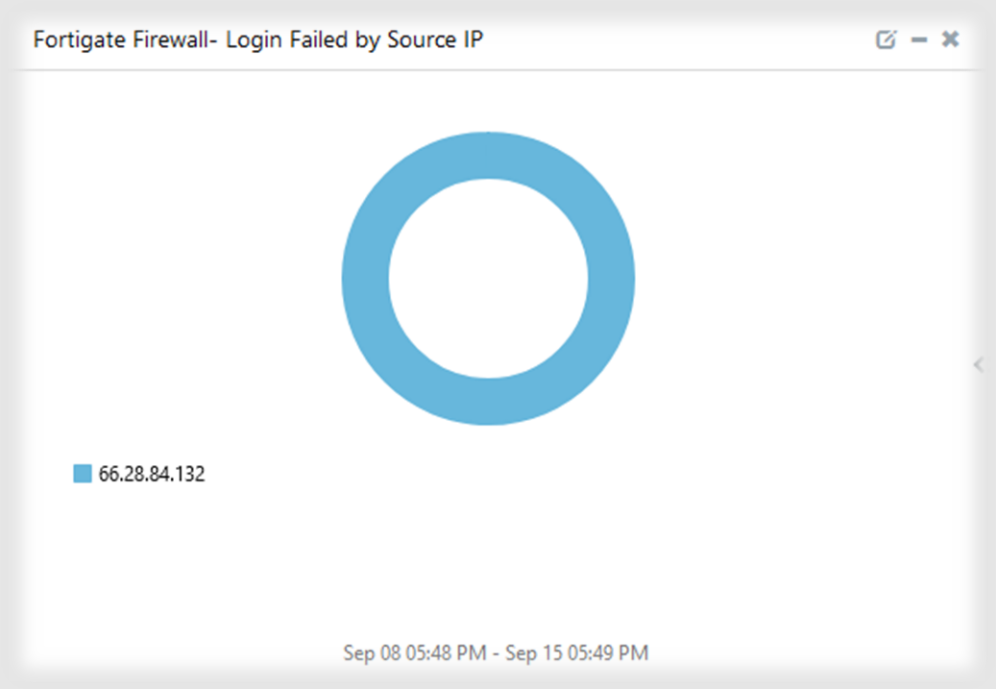
- **Fortigate Firewall- Login Failed by Geo-Location**



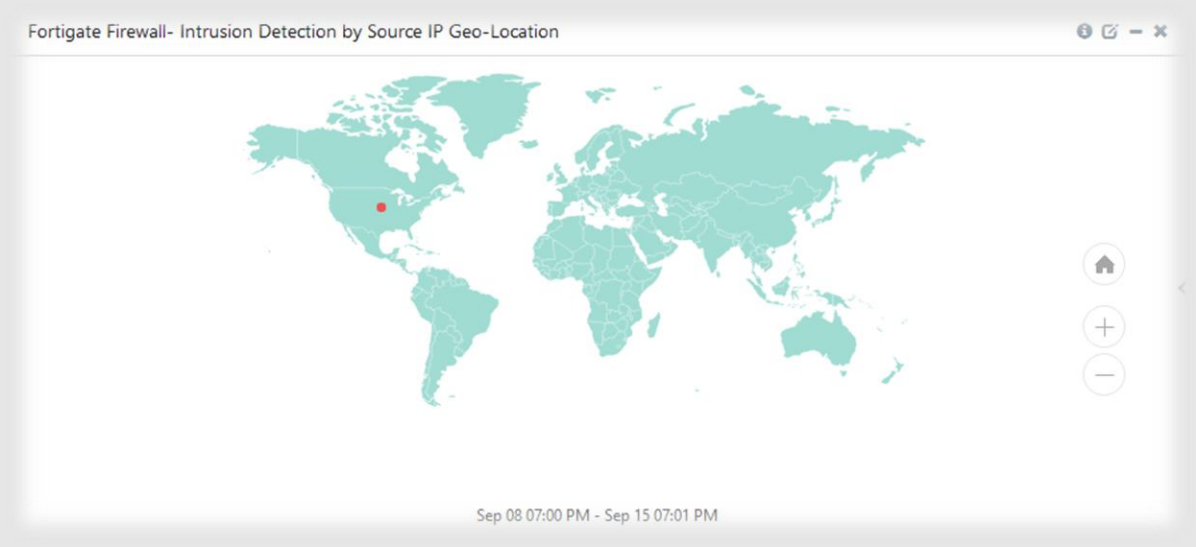
- **Fortigate Firewall- Intrusion Detection by Threat Name**



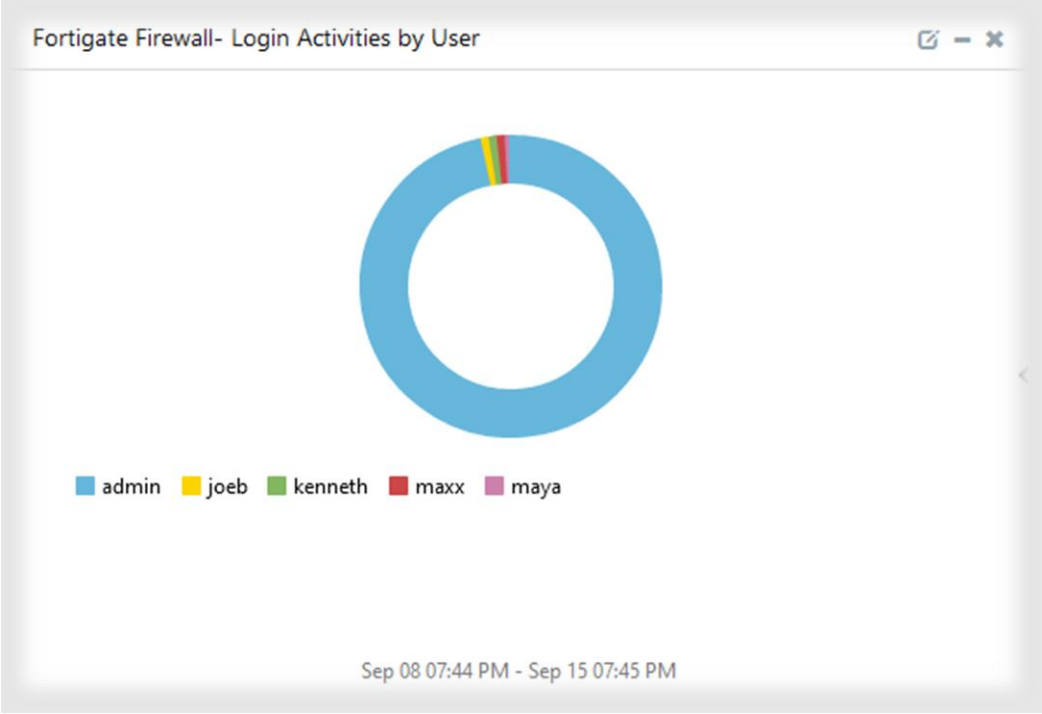
- **Fortigate Firewall- Login Failed by Source IP**



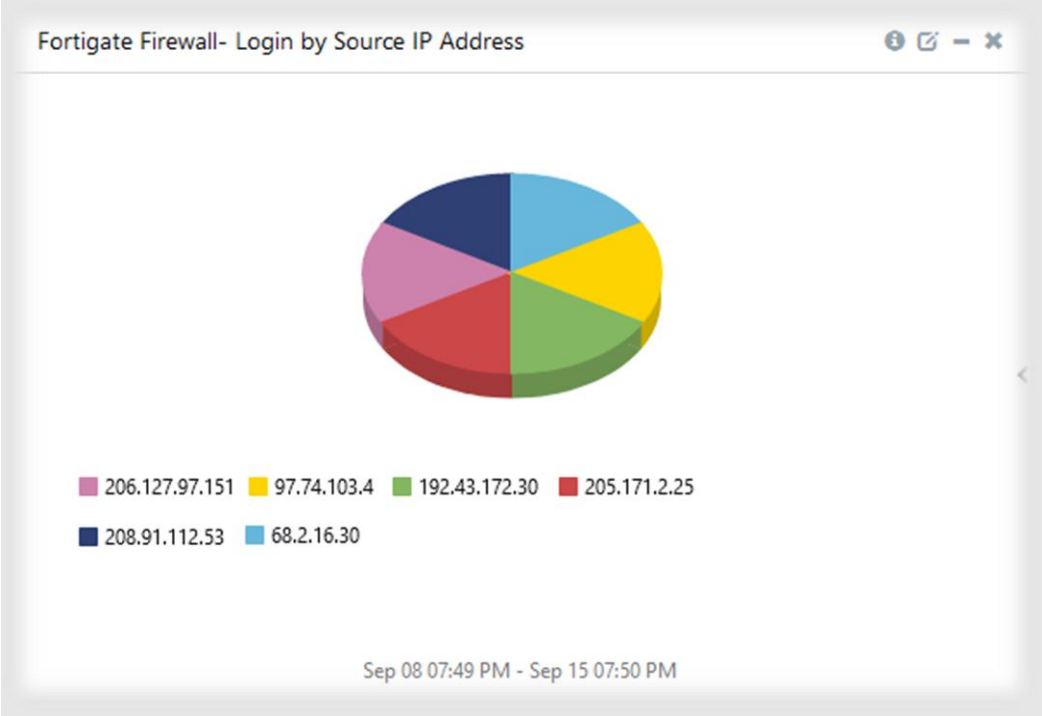
- **Fortigate Firewall- Intrusion Detection by Source IP Geo-Location**



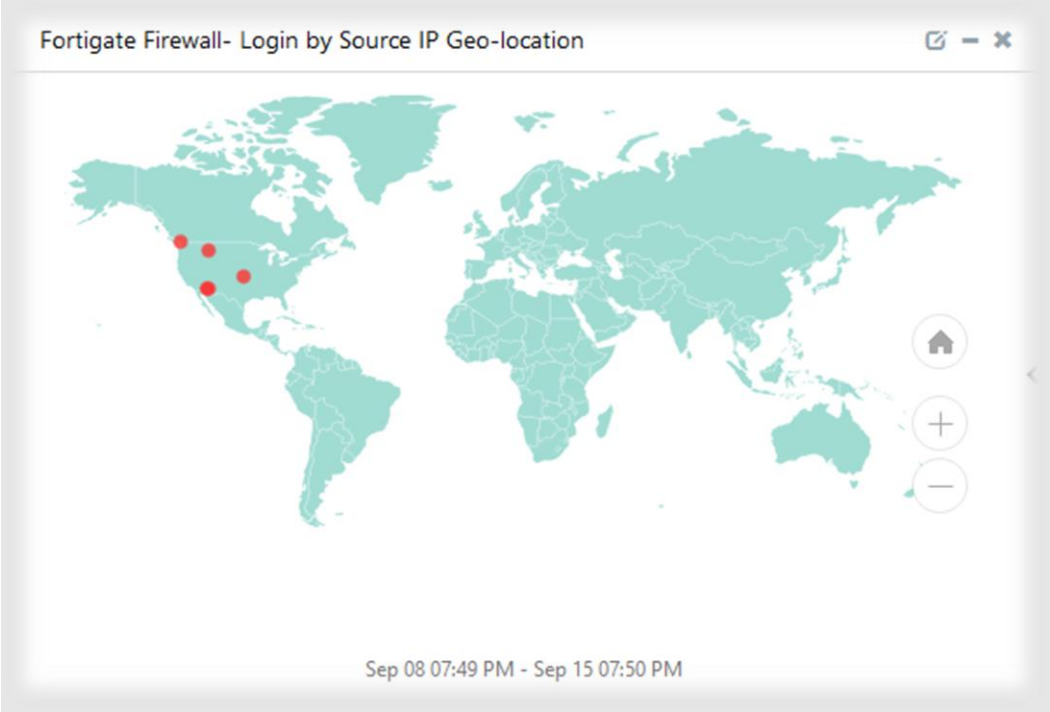
- **Fortigate Firewall – Login Activities by User**



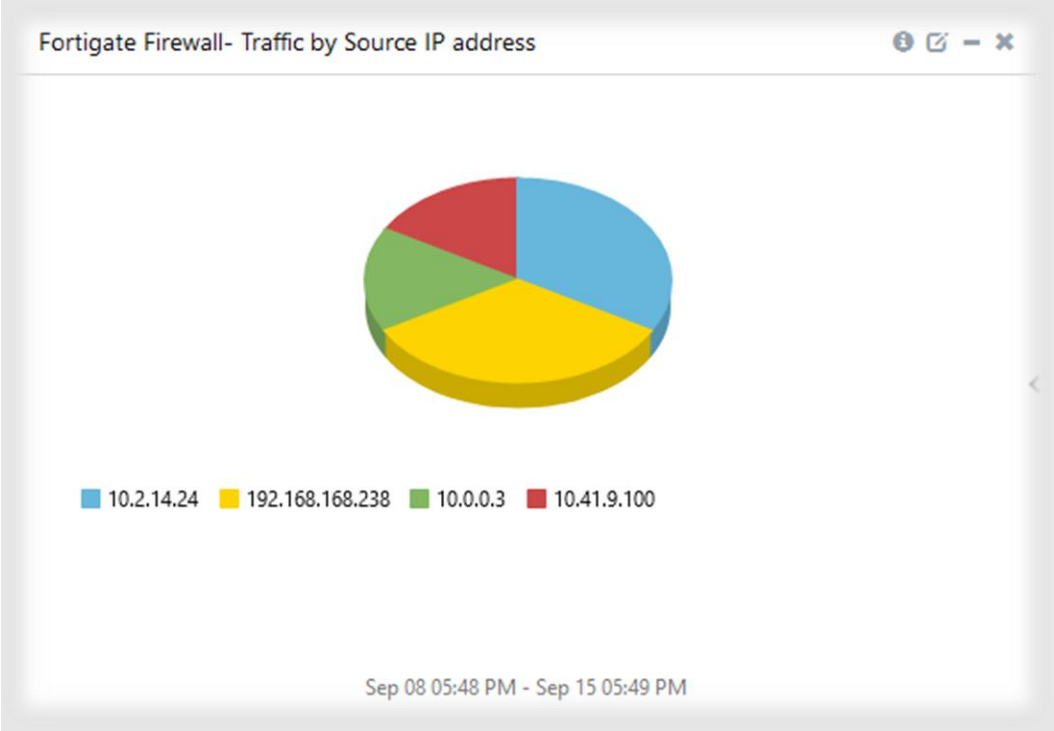
- **Fortigate Firewall- Login by Source IP Address**



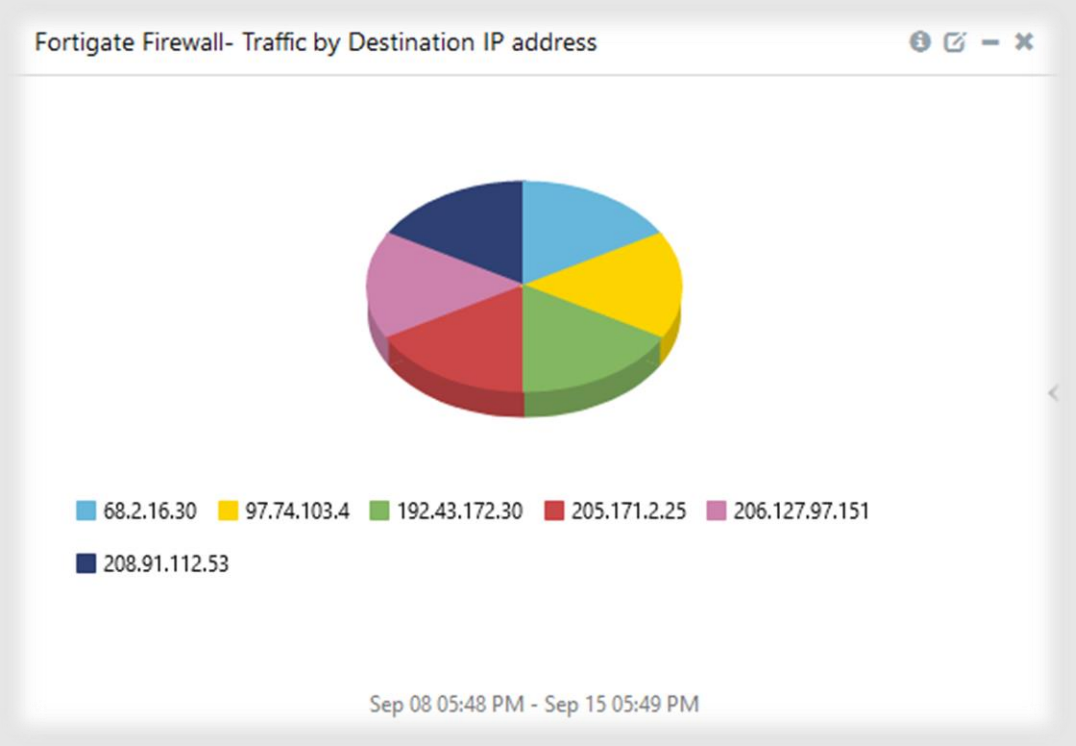
- **Fortigate Firewall- Login by Source IP Geo-location**



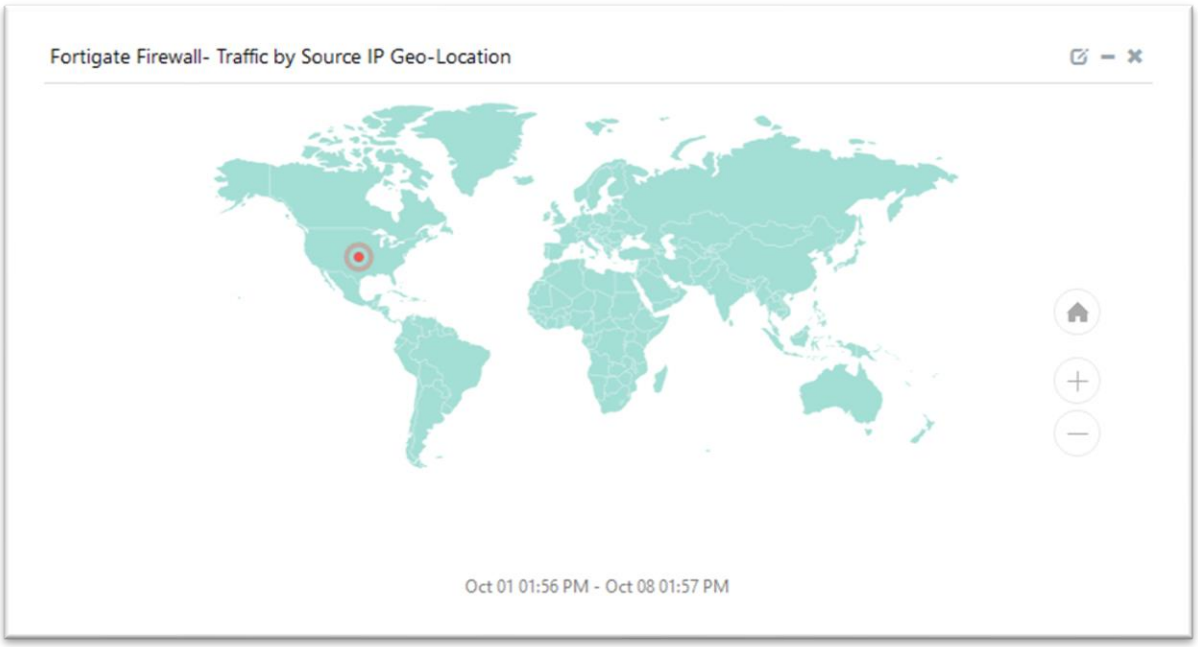
- **Fortigate Firewall- Traffic by Source IP address**



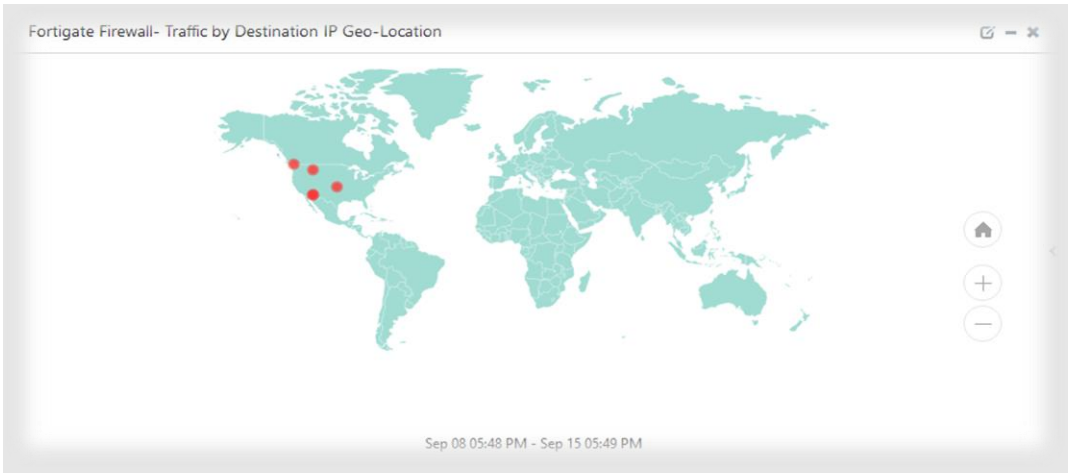
- **Fortigate Firewall- Traffic by Destination IP address**



- **Fortigate Firewall- Traffic by Source IP Geo-Location**



- **Fortigate Firewall- Traffic by Destination IP Geo-Location**

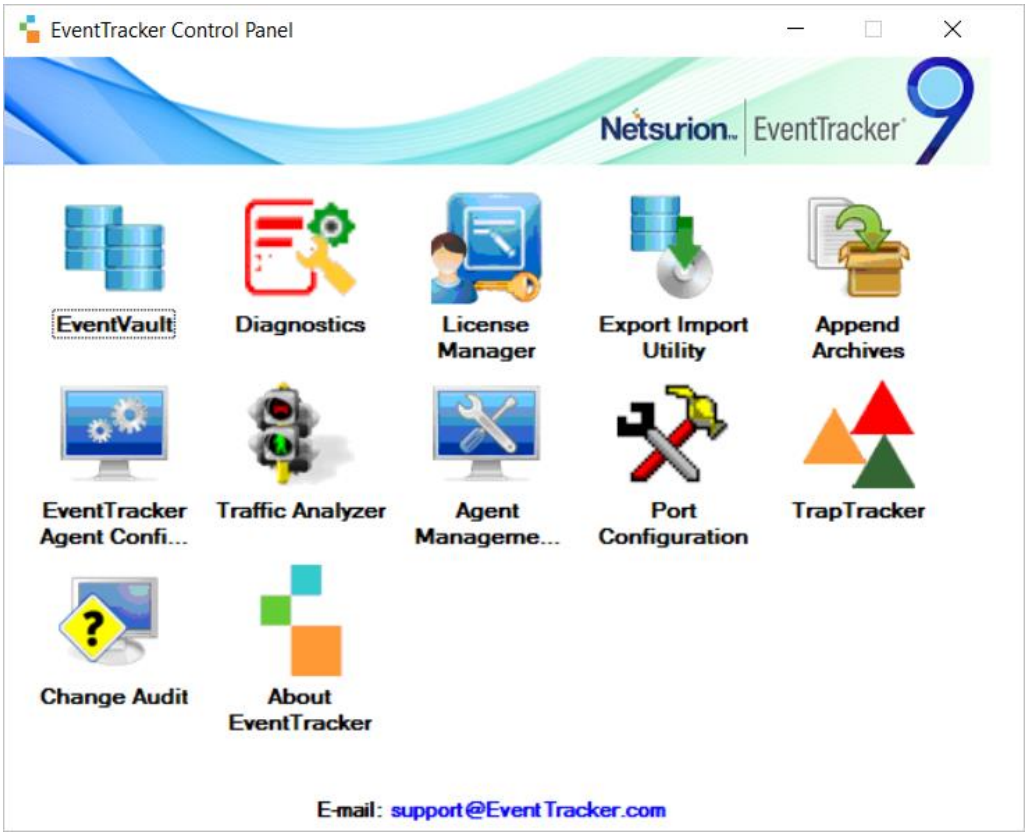


7 Import Fortinet Firewall Knowledge Pack

Import the Knowledge Pack items in the following sequence.

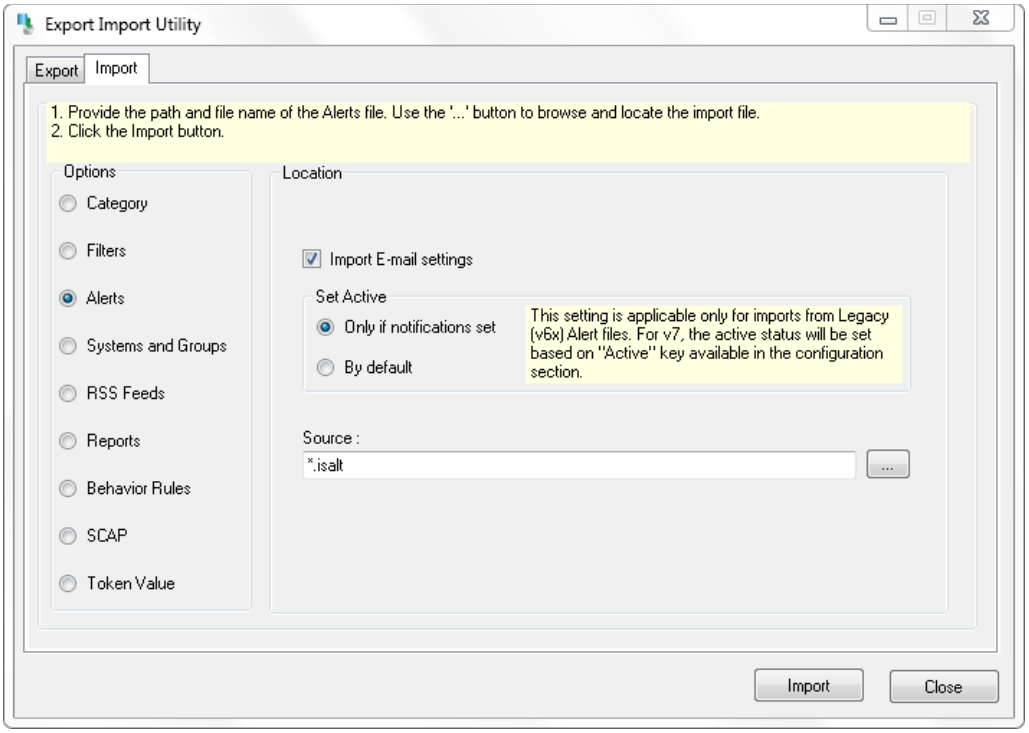
- Category
- Alerts
- Token Template
- Flex Reports
- Knowledge Objects
- Dashboards

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.



2. In the **Browse** window, locate the **Fortinet Firewall.isalt** file, and then click **Open**.

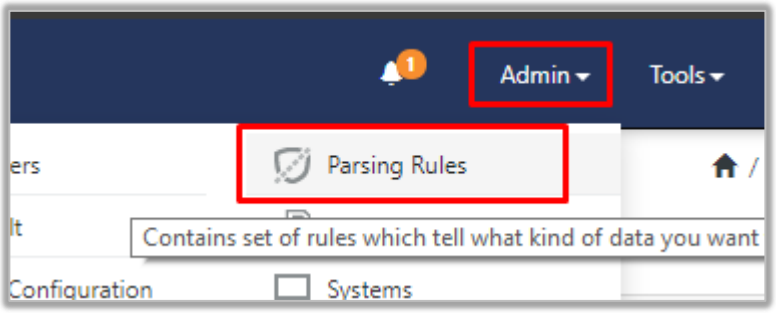
3. To import alerts, click **Import**.

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.

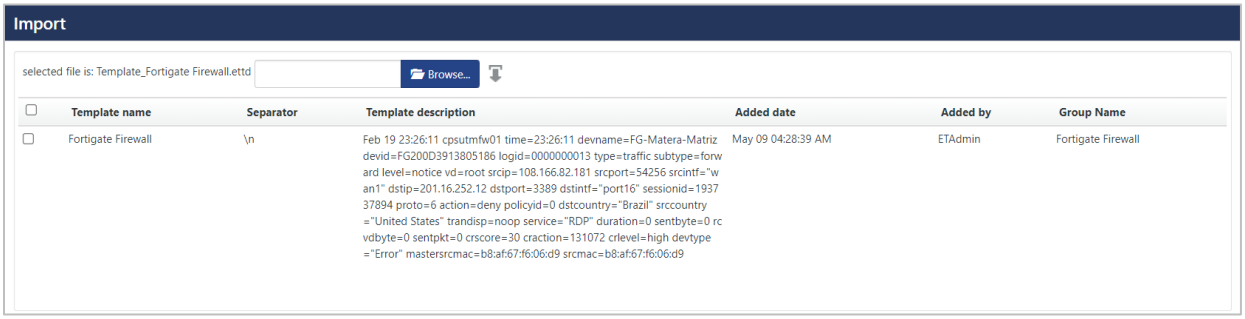
7.2 Token Template

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



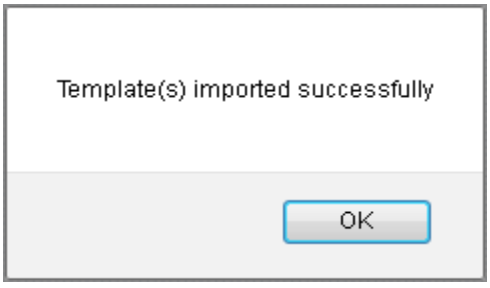
2. In the **Parsing Rules** interface, click the **Template** tab.

3. Click the **Browse** button and locate the **.ettd** file, and then click **Open**.



4. Select the template check box and then click the **Import** button.

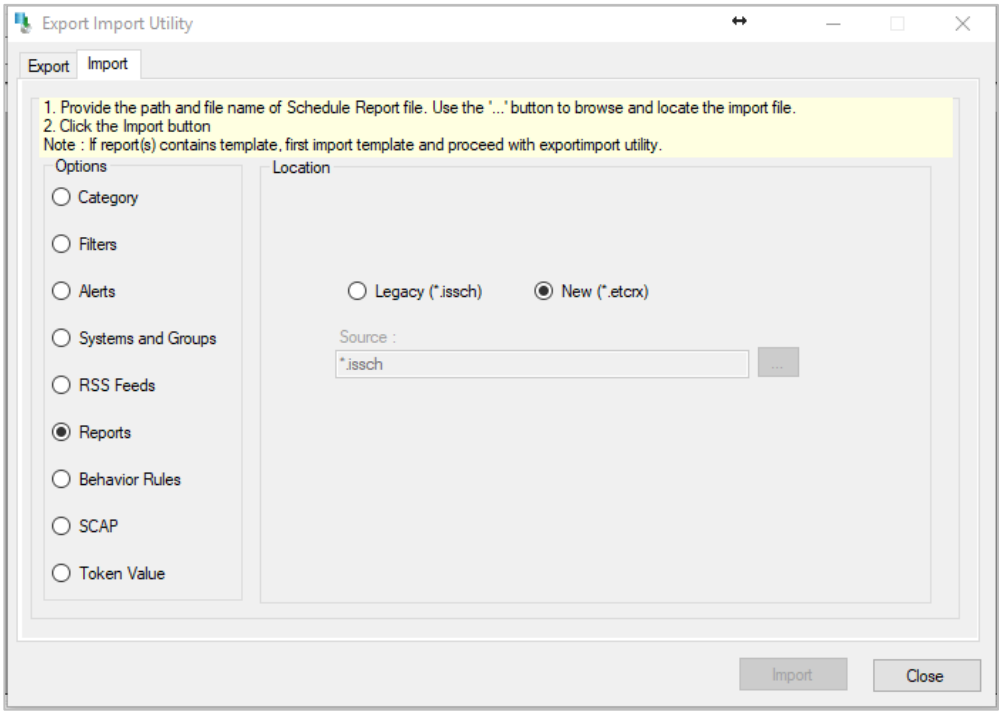
5. EventTracker displays a successful message on successfully importing the selected Template file in **Template**.



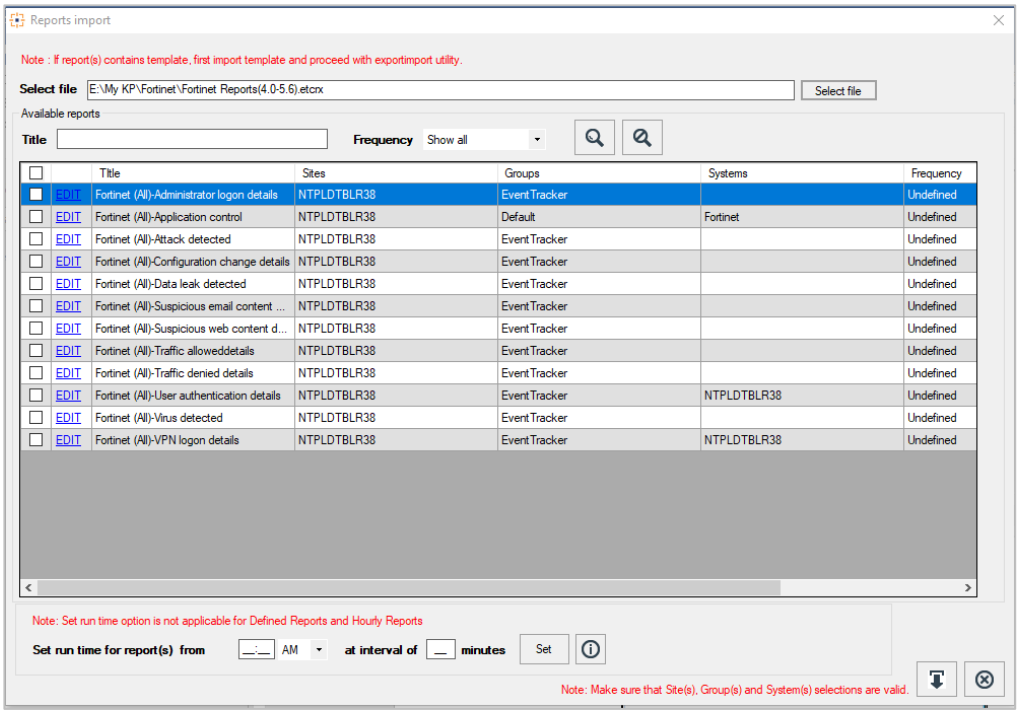
6. Click **OK** or the **Close** button to complete the process.

7.3 Flex Reports

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

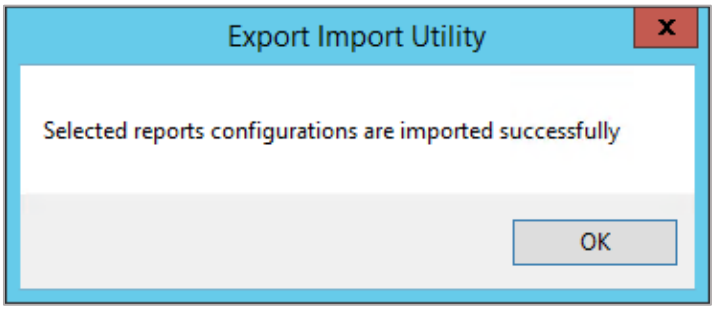


2. In the **Reports Import** window, click **Select file** to locate the **Fortinet Firewall.issch** file, and then click **Open**.



3. Select the check box of all the files and click the **Import** button to import the selected files.

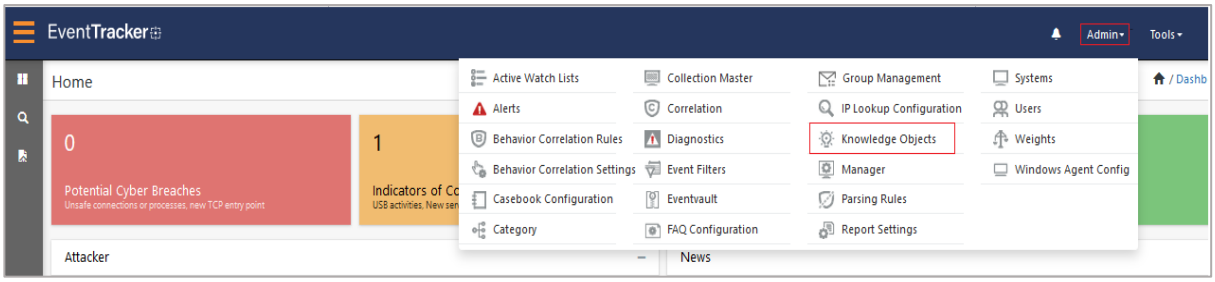
4. EventTracker displays a success message on successful importing of the selected file in **Reports**.



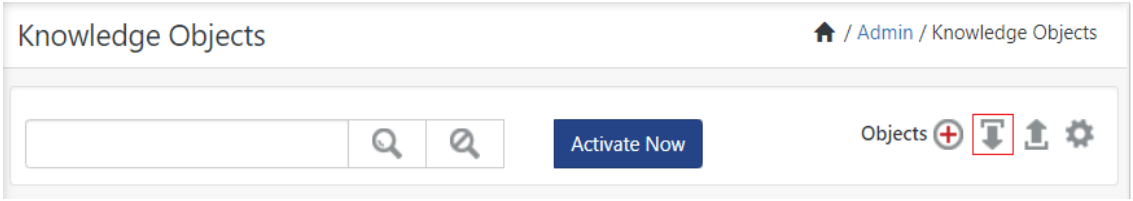
5. Click **OK** or the **Close** button to complete the process.

7.4 Knowledge Objects (KO)

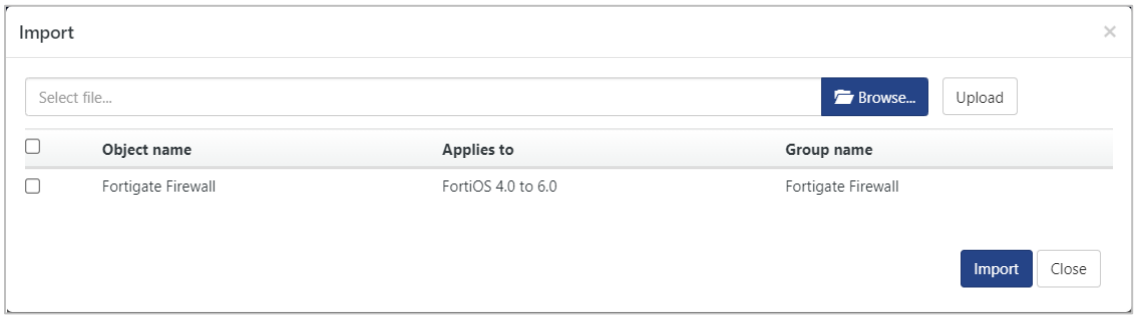
1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Knowledge Objects**.



2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.

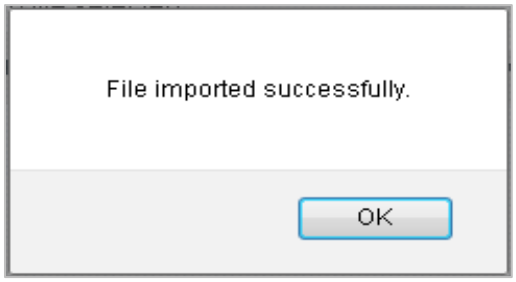


3. In the **Import** window, click **Browse** and locate the **.etko** file.



4. Select the check box and then click the **OVERWRITE** option.

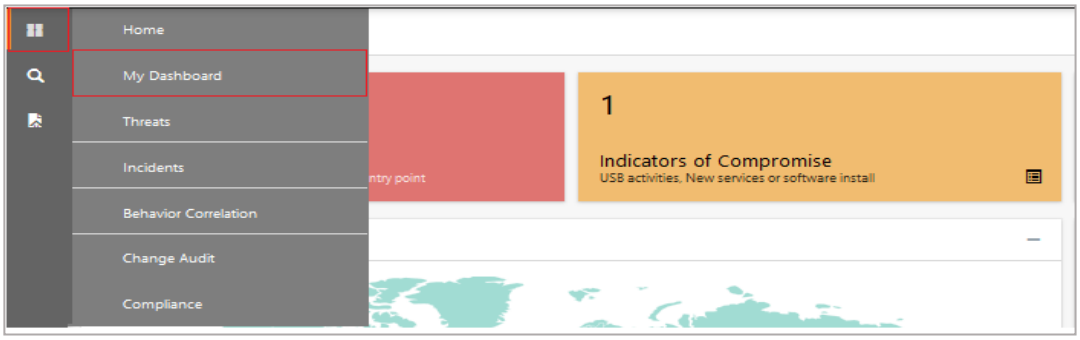
5. EventTracker displays a successful message on successfully importing the selected file in **Knowledge Objects**.



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

7.5 Dashboard

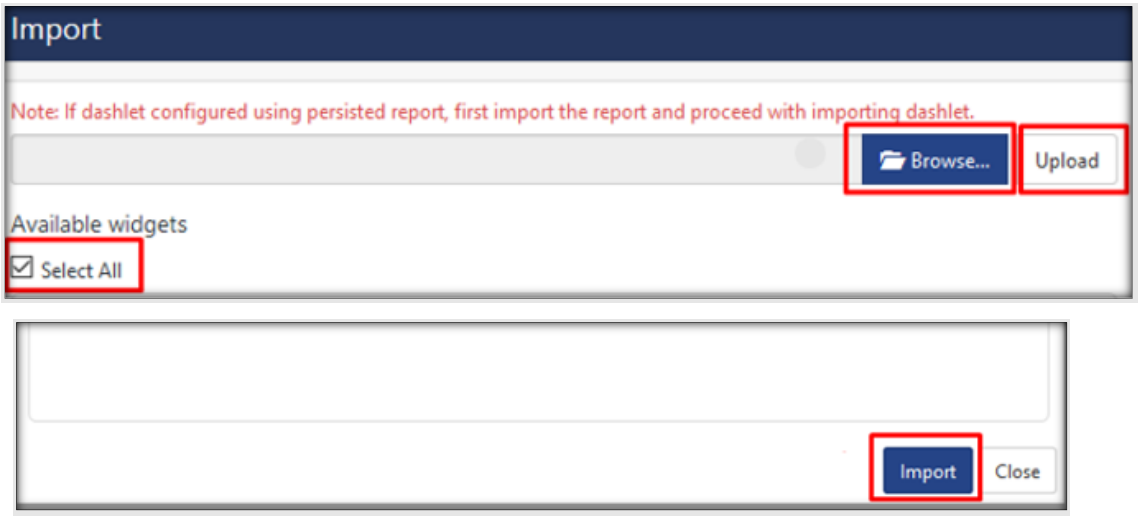
1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.



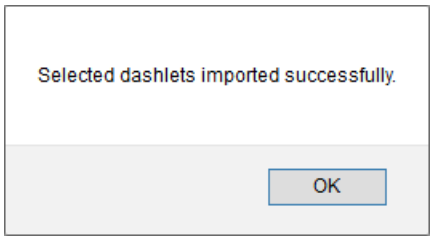
2. In the **My Dashboard** interface, click the **Import** button to import the dashlet files.

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.



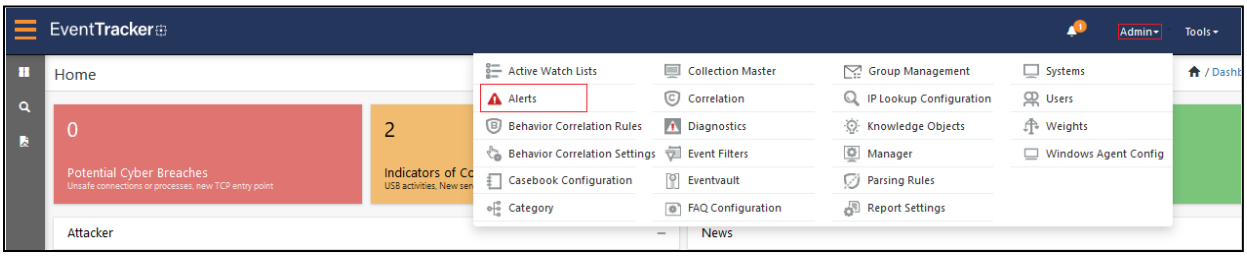
5. The EventTracker displays the success message on successfully importing the dashlet files.



8 Verify Fortinet Firewall Knowledge Pack

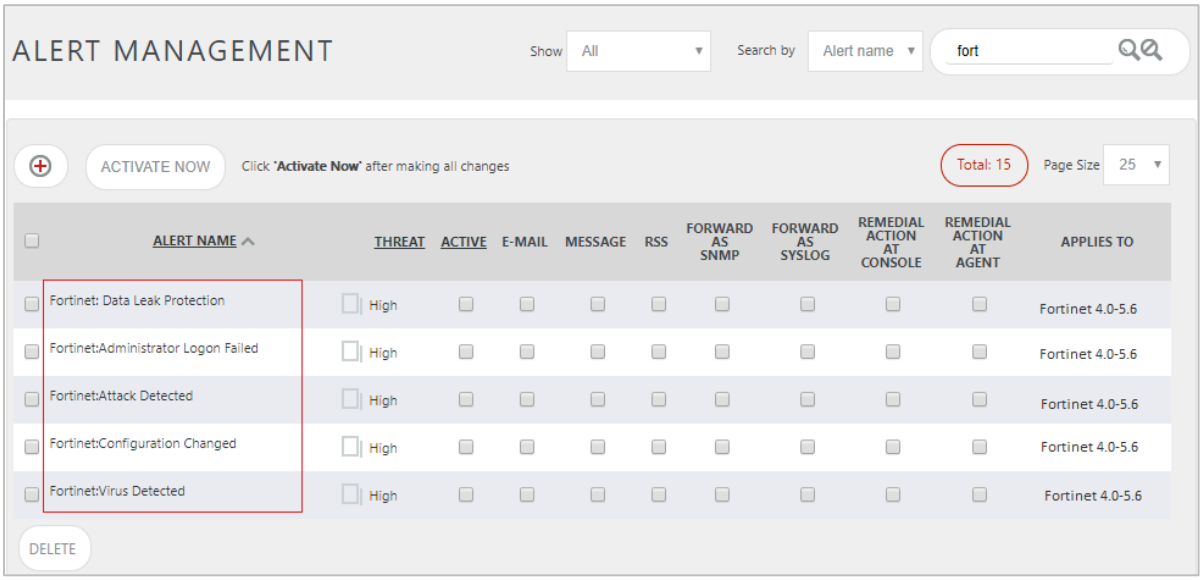
8.1 Alerts

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



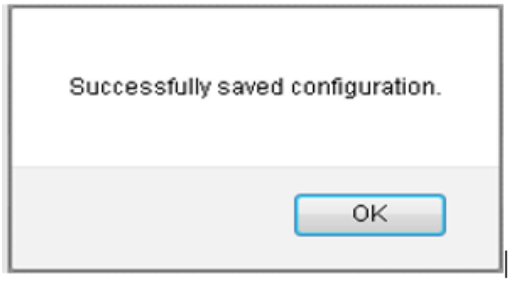
2. In the **Alerts** interface, type **Fortinet** in the search field, and click the **Search** button.

3. The **Alerts** interface will display all the imported **Fortinet** alerts.



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.

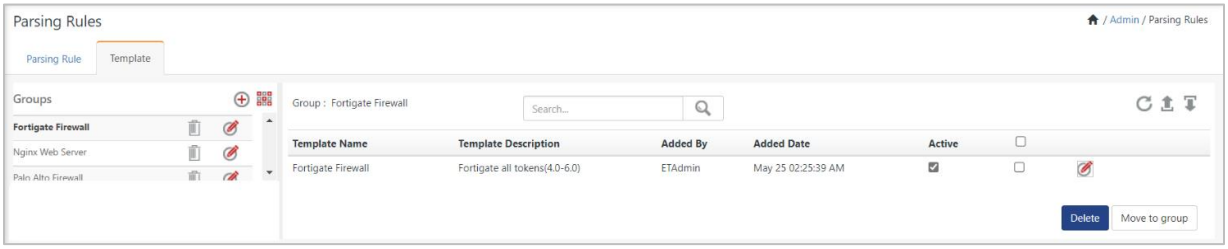
> **Note**
>
> You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

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

8.2 Token Template

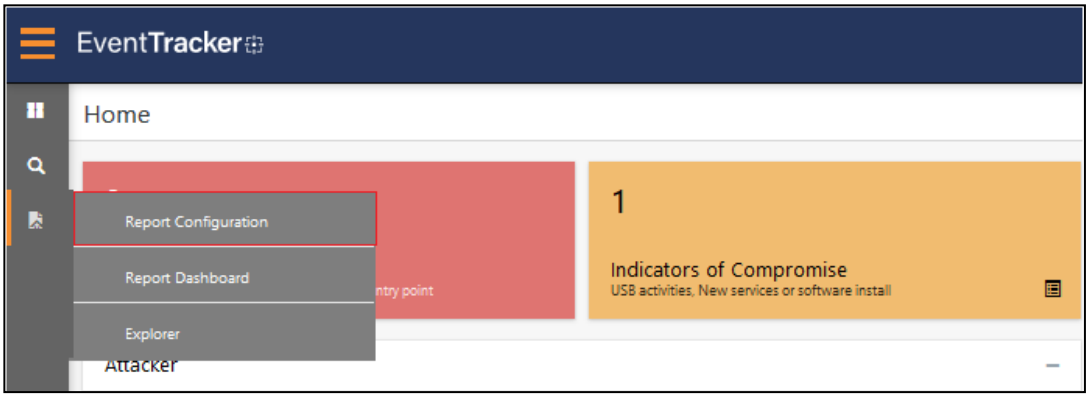
1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Parsing Rules**.

2. Go to the **Template** tab and click the **Fortinet Firewall** group folder to view the imported Token template.



8.3 Flex Reports

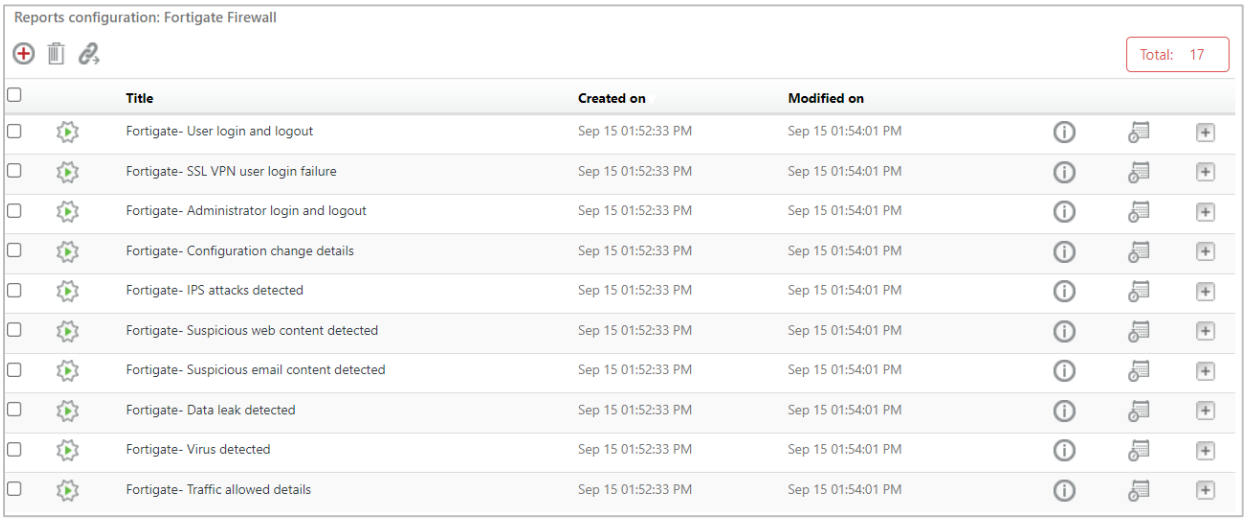
1. In the **EventTracker** web interface, click the **Reports** menu, and then click **Report Configuration**.



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.



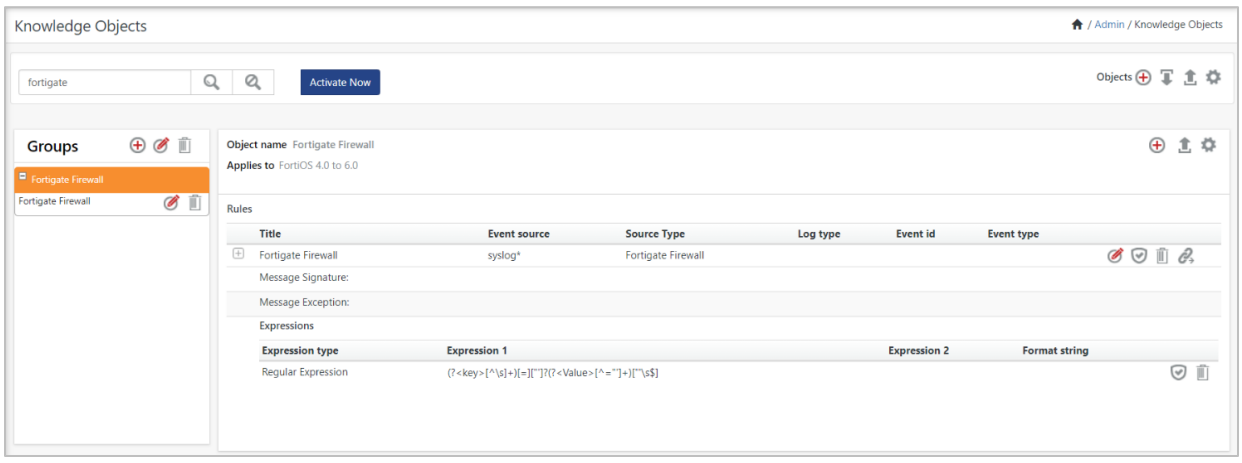
Note

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

8.4 Knowledge Objects (KO)

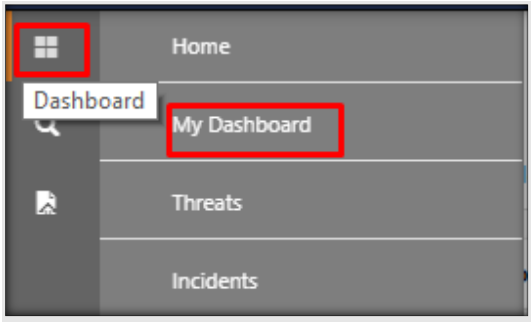
1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Knowledge Objects.**

2. Scroll down and select **FortiGate** in **Objects** pane, and the imported FortiGate object details will be displayed.

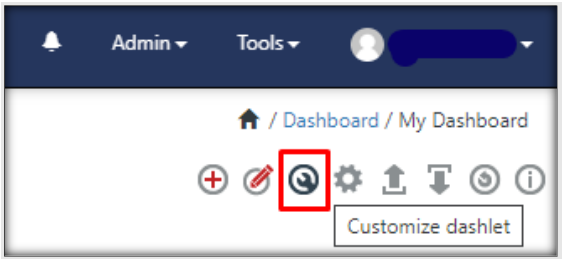


8.5 Dashboard

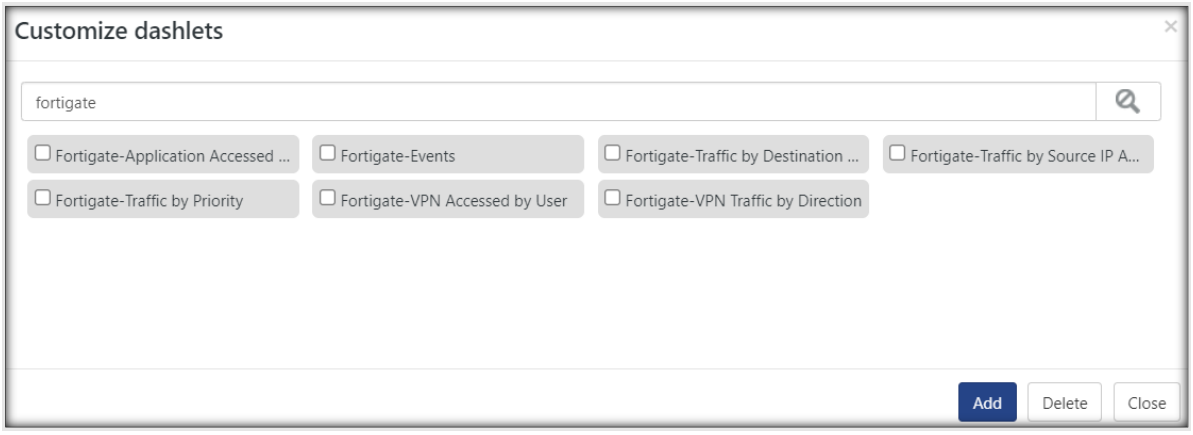
1. In the **EventTracker** web interface, go to **Home** > **My Dashboard**, and click the **Customize dashlets** button.



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



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



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 netsurion.com.

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