ManageEngine

Firewall Analyzer

Security Event Management: Real-time Alerts and Instant Remediation

Solution Brief

Security Event Management: Real-time Alerts and Instant Remediation

You may come across a situation, where there was a virus attack on you IT network. In another situation some of the corporate users may be accessing the streaming sites which drain the Internet bandwidth. First it should get notified instantly, Firewall Analyzer does this promptly. Will the alerts alone be sufficient to mitigate the effects of the attack or rectify the cause of the bandwidth drain? No. You need to take swift and automatic action to tackle the situation. If you depend on manual remediation measures, which are inherently slow, the virus will spread and will bring the whole network to a grinding halt or the business will get crippled as the bandwidth is not available for critical business activity. Also, the method of taking action should be flexible enough to address different security scenarios as given above. You may want to run a program or script to kill a process, block a port, user etc. Firewall Analyzer addresses this requirement using a feature called 'Run Script' (Program) which allows instant remediation to your network threats.

How Firewall Alerts and Program Execution help to mitigate threat?

Firewall Analyzer comes with real-time alerting feature. It is equipped with three notification methods:

- Email
- SMS
- Run Script

Email & SMS notifications are self-explanatory. 'Run Script' (Program) is a powerful and flexible feature. It allows you to write custom program, which get automatically executed when an alert gets triggered. Ensure that the program you write carries out remedial action according to the alert conditions as discussed above.

Setting up 'Run Script' (Program)

For the sake of demonstration, let us assume that you would like to be notified of any BitTorrent process in your organizations' network and immediately kill that process.

Create an executable program file to kill the bandwidth consuming processes (for demo we have created a file named **bit.exe**). The sample code can be found below:

```
@echo off
setlocal  enableextensions  enabledelayedexpansion
rem @echo %date% %time% %0  %* >> "%~dpn0-args.log"

SET EMPLOYEE="emp-"
SET USER="use-"

SET SRC=%1
FOR /F "useback tokens=*" %%a in ('%src%') do set src=%%~a
FOR /F "tokens=1,2,3 delims=/ " %%I IN ('DATE /T') DO SET date1=%%I/%%J/20%%K
FOR /F "tokens=1,2 delims=: " %%I IN ('TIME /T') DO SET time1=%%I:%%J

ping -n 1 -a %SRC% | FIND /I %STAFF% >NUL
IF NOT ERRORLEVEL 1 ( ECHO [%date1% %time%] %src% >>E:\torrent.log
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM Azureus.exe
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM BitComet.exe
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM bittorrent.exe
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM uTorrent-2-0-Beta.exe
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM uTorrent.exe
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM utorrent[1].exe
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM utorrent-3.0-latest[1].exe
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM utorrent-3.1.1-latest[1].exe
taskkill /S %src%  /U dir.uni\abc /P "xyz" /IM uTorrentPortable.exe & GOTO :EOF)

ping  -n 1 -a  %SRC% | FIND /I %STUDENT% >NUL
IF NOT ERRORLEVEL 1 ( ECHO [%date1% %time%] %src% >>E:\torrent.log
taskkill /S %src%  /U student\abc /P "xyz" /IM Azureus.exe
taskkill /S %src%  /U student\abc /P "xyz" /IM BitComet.exe
taskkill /S %src%  /U student\abc /P "xyz" /IM bittorrent.exe
taskkill /S %src%  /U student\abc /P "xyz" /IM uTorrent-2-0-Beta.exe
taskkill /S %src%  /U student\abc /P "xyz" /IM uTorrent.exe
taskkill /S %src%  /U student\abc /P "xyz" /IM utorrent[1].exe
taskkill /S %src%  /U student\abc /P "xyz" /IM utorrent-3.0-latest[1].exe
taskkill /S %src%  /U student\abc /P "xyz" /IM utorrent-3.1.1-latest[1].exe
taskkill /S %src%  /U student\abc /P "xyz" /IM uTorrentPortable.exe & GOTO :EOF)

endlocal
```

Script to block BitTorrent like processes

In Firewall Analyzer, create an alert profile with the following configuration:

- Enter a **profile name** of your choice (for demo we have given 'bittorrent-blog')
- Select **Profile Type** as 'Normal Alert'
- Select **Device(s)** of your choice (for demo we have selected 'FGT_TEST2')
- Select **Criteria**, Match all of the following and select 'Attack', condition 'contains', and enter text 'BitTorrent'

In the **Threshold** section

- Select **Priority** of your choice (for demo we have selected 'High')
- Enter values in **Alert for every 20 events generated in 1 minutes** (for demo we have selected '20', '1')
- Select **Assign owner** of your choice (for demo we have selected 'guest')
- Select **Apply threshold to** value as 'All selected devices'

In the **Notification** section

- Omit **Send the notifications once and do not send for** 'This day, This week, This month, Custom period' selection.
- Select **Send Email Notification option**

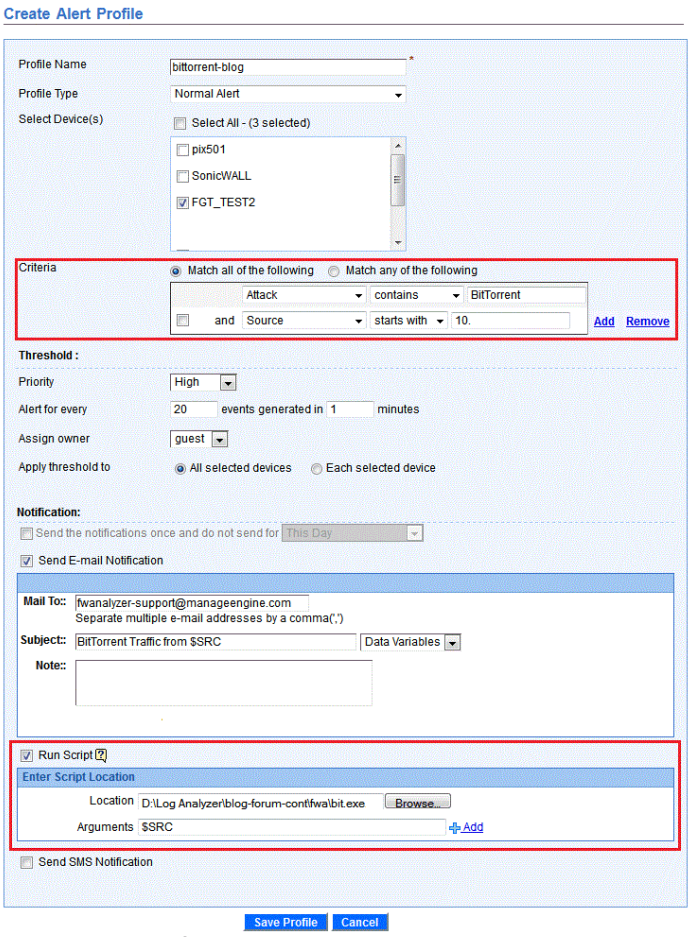
  Enter the email ID to which the alert notification to be sent in the 'Mail To:' text box. Separate multiple e-mail addresses by a comma(',')

  Enter the subject of alert email notification in the 'Subject:' text box. Use the 'Data Variables' drop down list and select the variable to add to the email subject line

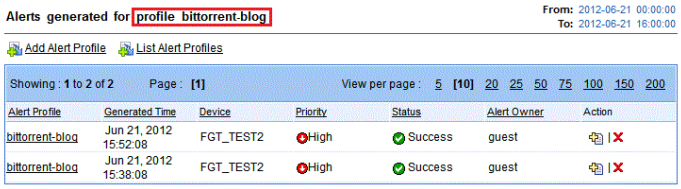
  Optionally, enter message to the email in the 'Note:' text box
- Select **Run Script** option
- In the **Enter Script Location** section,

  Click the **Browse** button and select the location of the file to be executed (for demo **bit.exe** file) in the client machine

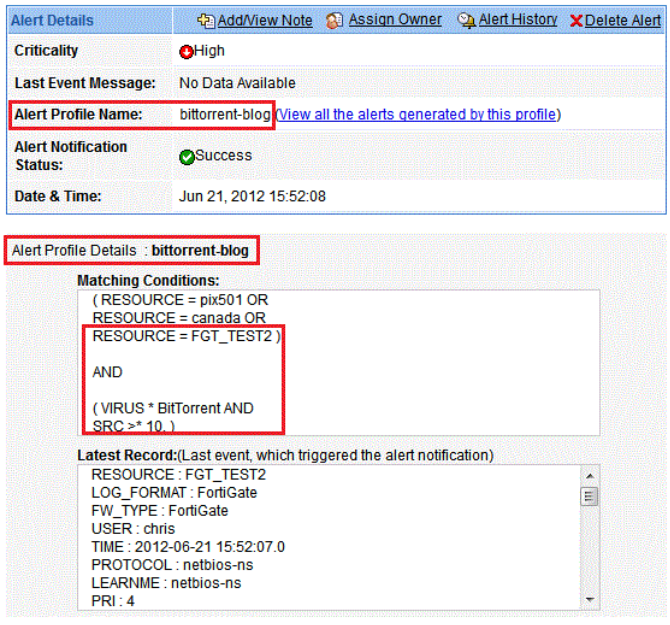
  Click **Add** link to add arguments (for demo **$SRC** field) in the **Arguments** text box which will be passed to the program for execution
- Click **Save Profile** button to save the alert profile



Create Alert Profile



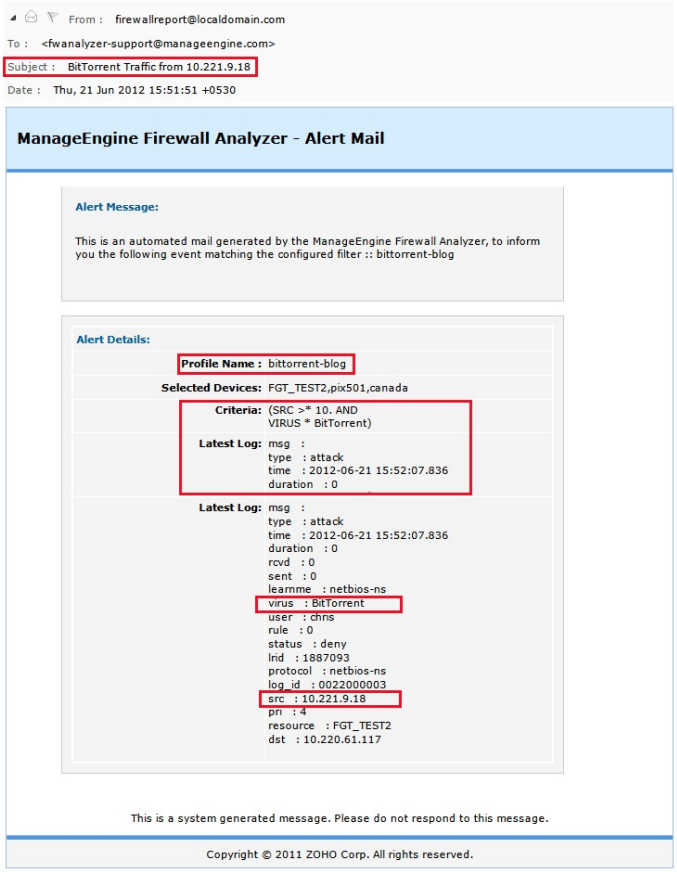
Alerts generated for BitTorrent



Details of the Alert - BitTorrent

```
RESOURCE : FGT_TEST2
LOG_FORMAT : FortiGate
FW_TYPE : FortiGate
USER : chris
TIME : 2012-06-21 15:52:07.0
PROTOCOL : netbios-ns
LEARNME : netbios-ns
PRI : 4
TYPE : attack
SRC : 10.221.9.18
SRCNAME : 10.221.9.18
SRC_PORT : 61645
DST : 10.220.61.117
DSTNAME : 10.220.61.117
DST_PORT : 137
DURATION : 0
STATUS : deny
SENT : 0
RCVD : 0
SRC_INT : 1214
DST_INT : 1215
HTTPSTATUS : 0
RULE : 0
EVENT_CODE : 0
EVENT_TYPE : 3
VIRUS : BitTorrent
POLICY_ID : web
SRC_ID : 182257938
DST_ID : 182205813
TRAN_IP : Unknown
TRAN_PORT : FaceBook
LOG_ID : 0022000003
STARTTIME : 1340274127
```

Alert details - 2


From : firewallreport@localdomain.com
To : <fwanalyzer-support@manageengine.com>
Subject : BitTorrent Traffic from 10.221.9.18
Date : Thu, 21 Jun 2012 15:51:51 +0530

ManageEngine Firewall Analyzer - Alert Mail

Alert Message:

This is an automated mail generated by the ManageEngine Firewall Analyzer, to inform you the following event matching the configured filter :: bittorrent-blog

Alert Details:

Profile Name : bittorrent-blog
Selected Devices: FGT_TEST2,pix501,canada
Criteria: (SRC >* 10. AND VIRUS * BitTorrent)
Latest Log: msg :
type : attack
time : 2012-06-21 15:52:07.836
duration : 0
Latest Log: msg :
type : attack
time : 2012-06-21 15:52:07.836
duration : 0
rcvd : 0
sent : 0
learnme : netbios-ns
virus : BitTorrent
user : chris
rule : 0
status : deny
lnd : 1887093
protocol : netbios-ns
log_id : 0022000003
src : 10.221.9.18
pri : 4
resource : FGT_TEST2
dst : 10.220.61.117

This is a system generated message. Please do not respond to this message.

Email notification of the Alert - BitTorrent

About ManageEngine Firewall Analyzer

ManageEngine Firewall Analyzer is an automated firewall log analysis tool for security event management that collects, analyses, and reports on enterprise-wide firewalls, proxy servers, VPNs, IDS/IPS, and other network perimeter devices. More than 3000 customers worldwide are using Firewall Analyzer as their Security Event Management solution to detect network anomalies, monitor firewall configuration changes (firewall change management), fine-tune firewall rules, measure bandwidth usage, manage user/employee internet access, audit traffic, and improve incident response.

About ManageEngine

ManageEngine is the leading provider of cost-effective enterprise IT management software and the only one making the 90-10 promise - to provide 90 percent of the capabilities offered by the Big 4 at just 10 percent of the price. More than 50,000 organizations in 200 countries, from different verticals, industries and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of Zoho Corp.