ManageEngine

Firewall Analyzer

# Gerenciamento de eventos de segurança: alertas em tempo real e correção instantânea

Resumo da solução

© 2012 **Zoho Corporation Pvt. Ltd**. Todos os direitos reservados

# Gerenciamento de eventos de segurança: alertas em tempo real e correção instantânea

Você pode se deparar com uma situação em que houve um ataque de vírus à sua rede de TI. Em outra situação, alguns usuários corporativos podem estar acessando sites de streaming que drenam a largura de banda da Internet. Primeiro, ele deve ser notificado instantaneamente; o Firewall Analyzer faz isso imediatamente. Os alertas por si só serão suficientes para mitigar os efeitos do ataque ou corrigir a causa da perda de largura de banda? Não. Você precisa tomar medidas rápidas e automáticas para lidar com a situação. Se você depender de medidas manuais de remediação, que são inerentemente lentas, o vírus se espalhará e paralisará toda a rede ou a empresa ficará paralisada, pois a largura de banda não estará disponível para atividades comerciais críticas. Além disso, o método de ação deve ser flexível o suficiente para lidar com diferentes cenários de segurança, como os apresentados acima. Você pode querer executar um programa ou script para encerrar um processo, bloquear uma porta, um usuário, etc. O Firewall Analyzer atende a esse requisito usando um recurso chamado "Executar Script" (Programa), que permite a remediação instantânea das ameaças à sua rede.

**Como os Alertas de Firewall e a Execução de Programas ajudam a mitigar ameaças?**

O Firewall Analyzer conta com um recurso de alerta em tempo real. Ele conta com três métodos de notificação:

- Email
- SMS
- Executar Script

As notificações por e-mail e SMS são autoexplicativas. "Executar Script" (Programa) é um recurso poderoso e flexível. Ele permite que você escreva programas personalizados, que são executados automaticamente quando um alerta é acionado. Certifique-se de que o programa que você escrever execute a ação de correção de acordo com as condições de alerta, conforme discutido acima.

**Configurando o "Executar Script" (Programa)**

Para fins de demonstração, vamos supor que você queira ser notificado sobre qualquer processo BitTorrent na rede da sua organização e encerrar esse processo imediatamente.

Crie um arquivo executável para encerrar os processos que consomem muita largura de banda (para demonstração, criamos um arquivo chamado **bit.exe**). O código de exemplo pode ser encontrado abaixo:

```
@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 para bloquear processos semelhantes ao BitTorrent*

No Firewall Analyzer, crie um perfil de alerta com a seguinte configuração:

- Insira um **nome de perfil** de sua escolha (para demonstração, selecionamos "bittorrent-blog").
- Selecione o **Tipo de Perfil** como "Alerta Normal".
- Selecione o(s) **Dispositivo(s)** de sua escolha (para demonstração, selecionamos "FGT_TEST2").
- Selecione **Critérios**, corresponda a todos os seguintes e selecione "Ataque". A condição "contém" e insira o texto "BitTorrent".

Na seção **Threshold**

- Selecione a **Prioridade** de sua escolha (para demonstração, selecionamos "Alta").
- Insira valores em **Alerta para cada 20 eventos gerados em 1 minuto** (para demonstração, selecionamos "20", "1").
- Selecione **Atribuir proprietário** de sua escolha (para demonstração, selecionamos "Convidado").
- Selecione **Aplicar threshold ao** valor como "Todos os dispositivos selecionados".

Na seção **Notificação**

- Omita a opção "**Enviar notificações uma vez**" e não envie para a seleção "Este dia, Esta semana, Este mês, Período
- personalizado".

  Selecione a opção "**Enviar notificação por e-mail**".

  Insira o ID do e-mail para o qual a notificação de alerta será enviada na caixa de texto "Enviar para:". Separe vários endereços de e-mail por vírgula (‘,’).

  Insira o assunto da notificação de alerta por e-mail na caixa de texto "Assunto:". Use a lista suspensa "Variáveis de Dados" e selecione a variável a ser adicionada ao assunto do e-mail.

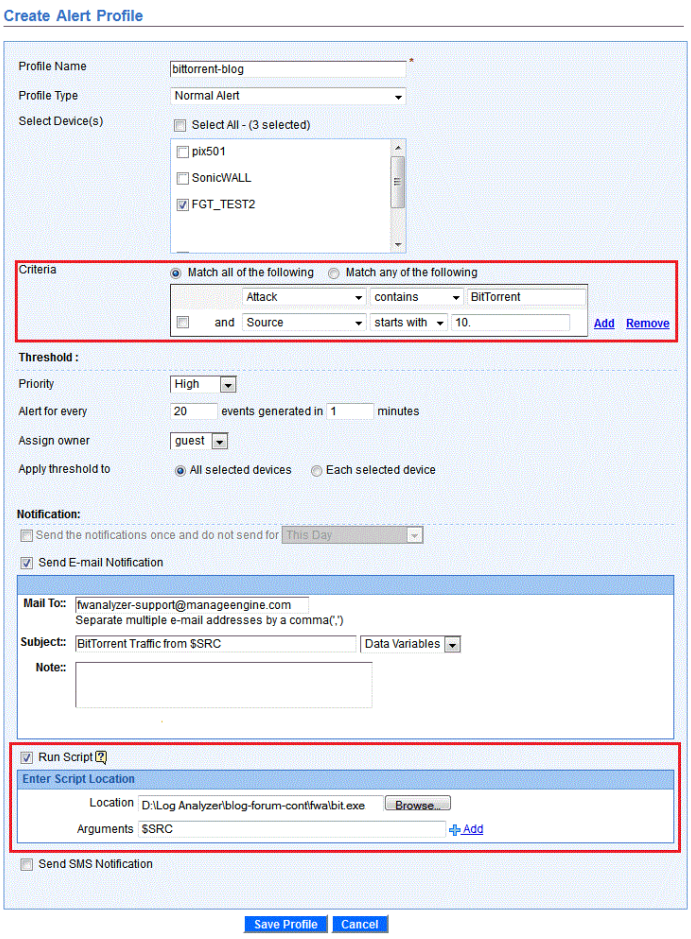
  Opcionalmente, insira a mensagem para o e-mail na caixa de texto "Observação:".

- Selecione a opção **Executar script**.
- Na seção "**Inserir local do script**",

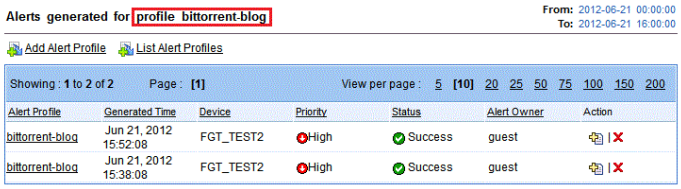
  Clique no botão **Procurar** e selecione o local do arquivo a ser executado (para o arquivo **bit.exe** de demonstração) na máquina cliente.

  Clique no link **Adicionar** para adicionar argumentos (para o campo **$SRC** de demonstração) na caixa de texto **Argumentos** que serão passados ao programa para execução.

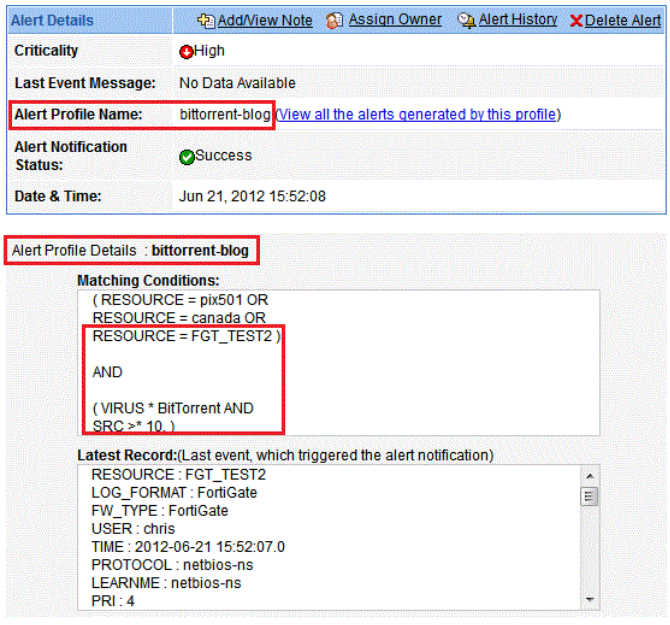
- Clique no botão **Salvar perfil** para salvar o perfil de alerta




*Crie perfil de alerta*



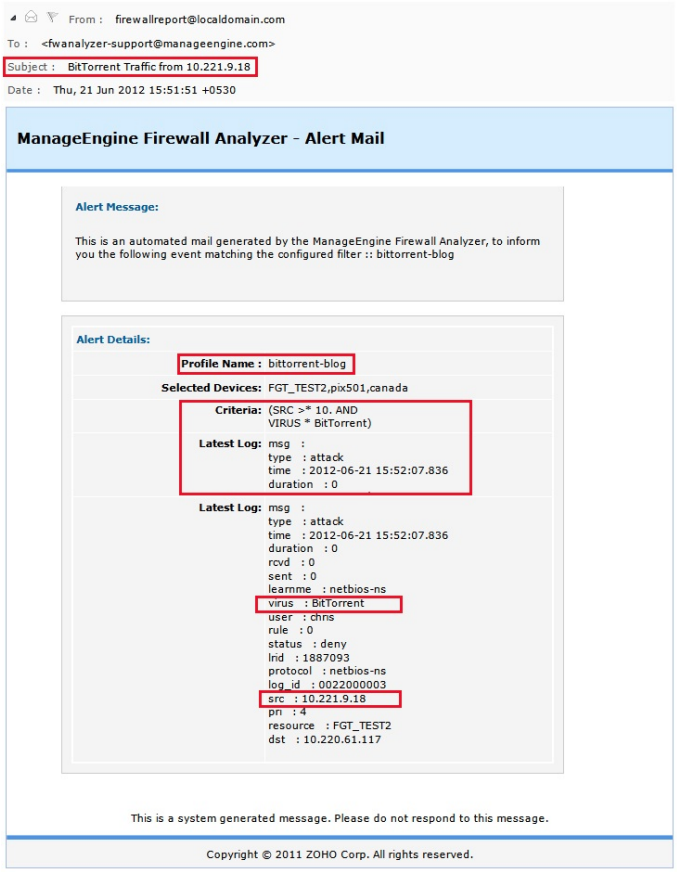

*Alerts generated for BitTorrent*




*Detalhes do alerta - 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*




*Notificação por e-mail do alerta - BitTorrent*

## Sobre o Firewall Analyzer da ManageEngine

O Firewall Analyzer é uma ferramenta automatizada de análise de logs de firewall para gerenciamento de eventos de segurança que coleta, analisa e gera relatórios sobre firewalls corporativos, servidores proxy, VPNs, IDS/IPS e outros dispositivos de perímetro de rede. Mais de 3.000 clientes em todo o mundo utilizam o Firewall Analyzer como solução de Gerenciamento de Eventos de Segurança para detectar anomalias na rede, monitorar alterações na configuração do firewall (gerenciamento de alterações de firewall), ajustar regras de firewall, mensurar o uso da largura de banda, gerenciar o acesso de usuários/funcionários à internet, auditar o tráfego e aprimorar a resposta a incidentes.

# Sobre a ManageEngine

A ManageEngine é a fornecedora líder de software de gestão de TI empresarial com excelente custo-benefício e a única a cumprir a promessa de 90% dos recursos oferecidos pelas Big 4 por apenas 10% do preço. Mais de 50.000 organizações em 200 países, de diferentes setores, setores e portes, utilizam a ManageEngine para atender às suas necessidades de gestão de TI de forma econômica. A ManageEngine é uma divisão da Zoho Corp.

ManageEngine é uma marca registrada da ZOHO Corporation. Todas as outras marcas e nomes de produtos são marcas comerciais ou marcas registradas de suas respectivas empresas.