Como Fazer para Bloquear o UltraSurf, Solução Definitiva [iptables + fail2ban]

Rodrigo Luis Silva

Como Fazer para Bloquear o UltraSurf, Solução Definitiva [iptables + fail2ban]

Essa semana fazendo a revisão do firewall de um cliente eu consegui bloquear o acesso as redes *BitTorrent* e ao terrível *UltraSurf*.

Vou descrever como fiz para bloquear o UltraSurf.

O problema

Em um primeiro momento eu acreditei que seria fácil bloquear o UltraSurf, porém o uso de proxy transparente obriga que a porta 443 (HTTPS) fique liberada, o BitTorrent foi bloqueado sem dificuldades.

Com o uso do *tcpdump* eu identifique que todo o acesso do *UltraSurf* sai pela porta 443, logo a solução mais obvia seria bloquea-la, porém não é possível. Bloquear o IP ou range de IP do servidor de destino seria outra opção.

Quando fiz o bloqueio pelo range de IP, descobri que o *UltraSurf* tenta uma centena de IPs diferentes até conseguir o acesso que ele precisa, e certamente devem existir novos IPs a cada nova versão.

Pesquisei pelo Google e não encontrei nenhuma forma eficiente de bloquear o *UltraSurf*, foi então que tive pensei o seguinte.

Criar uma regra no *iptables* e fazer log dos acesso ao IP do *UltraSurf*, depois criar um daemon para ler esse log e fazer um bloqueio em tempo real.

Bem, chega de bla bla e vamos por a mão na massa.

Começando

Vamos lá, esse pequeno tutorial é para tratar um problema especifico, sendo assim eu suponho que você já sabe usar o *iptables*, afinal já está aqui buscando uma forma de fazer um bloqueio mais avançado, rs

Acredito que essa solução possa ser utilizada por todos, para firewall simples até o mais complexo.

Eu estou usando Debian 5.0.3, iptables 1.4.2 e fail2ban 0.8.3.

Qualquer dúvida, problema ou sugestão podem deixar um comentário.

No final você encontra os arquivos de configuração para download.

iptables

Essa parte é bem simples, no seu script de firewall adicione a seguinte linha.

```
iptables -A FORWARD -d 65.49.14.0/24 -j LOG --log-prefix "=UltraSurf= "
```

A rede 65.49.14.0/24 é a primeira a ser contactada pelo UltraSurf quando ele é aberto, a regra acima apenas gera um LOG, não existe bloqueio do acesso, em um primeiro momento o usuário vai até pensar que está funcionando.

ATENÇÃO

Coloque essa regra antes da regra com o modulo *state* (*-m state –state ESTABLISHED,RELATED*).

Se colocar depois os pacotes das conexões já estabelecidas não irão para o LOG e pode gerar falhas no bloqueio.

fail2ban

O fail2ban é uma ferramenta muito boa para a segurança de servidores, em linhas gerais ela faz o seguinte.

Lê algum arquivo de log, compara com uma expressão regular e em caso positivo ele executa algum comando no sistema.

Por padrão ele monitora o log do SSH e em caso de falhas consecutivas no acesso ele cria uma regra no iptables para bloquear o possível invasor.

Instalando

Como eu estou utilizando o Debian e vou instalar pelo *apt-get*.

```
# apt-get install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  python-gamin
The following NEW packages will be installed:
  fail2ban
0 upgraded, 1 newly installed, 0 to remove and 100 not upgraded.
Need to get 86.2kB of archives.
After this operation, 631kB of additional disk space will be
used.
Fetched 86.2kB in 0s (419kB/s)
Selecting previously deselected package fail2ban.
(Reading database ... 38547 files and directories currently
installed.)
Unpacking fail2ban (from .../fail2ban_0.8.3-2sid1_all.deb) ...
Processing triggers for man-db ...
Setting up fail2ban (0.8.3-2sid1) ...
```

Depois de instalado vamos acessar o diretório de configuração

Aqui vamos criar um arquivo chamado *jail.local*

```
vi /etc/fail2ban/jail.local
```

Vamos adicionar o conteúdo abaixo ao arquivo *jail.local*.

```
[ultrasurf]
enabled   = true
filter    = ultrasurf
port      = all
```

```
5
 logpath   = /var/log/messages
6
 maxretry  = 6
7
 # Tempo em segundos que o IP fica bloqueado, aqui 15 minutos
8
 bantime   = 900
9
```

Vamos criar o arquivo com a expressão regular que irá filtar o log do *iptables*.

```
1vi /etc/fail2ban/filter.d/ultrasurf.local
```

Aqui vamos adicionar uma expressão regular simples ao arquivo *ultrasurf.local*.

```
1[Definition]

2failregex = (.*)=UltraSurf=(.*) SRC=<HOST>

3ignoreregex =
```

Apesar de simples, funciona

Agora o arquivo que irá executar o *iptables* e criar as regras necessárias para o bloqueio e desbloqueio.

```
1vi /etc/fail2ban/action.d/iptables-ultrasurf.local
```

Aqui é onde a magica acontece, adicione o conteúdo abaixo ao arquivo *iptables-ultrasurf.local*.

```
1 [Definition]

2 actionstart = iptables -N fail2ban-<name>

3               iptables -A fail2ban-<name> -j RETURN

4               iptables -I INPUT -j fail2ban-<name>

5               iptables -I FORWARD -j fail2ban-<name>

6 actionstop = iptables -D FORWARD -j fail2ban-<name>

7              iptables -D INPUT -j fail2ban-<name>

8              iptables -F fail2ban-<name>

9              iptables -X fail2ban-<name>

10actioncheck = iptables -n -L FORWARD | grep -q fail2ban-<name>
```

```
11
12
13
14 actionban = iptables -I fail2ban-<name> 1 -s <ip> -j REJECT
15 actionunban = iptables -D fail2ban-<name> -s <ip> -j REJECT
16 [Init]
17 name = ultrasurf
18
19
20
21
```

Agora basta reiniciar o Daemon

```
1 /etc/init.d/fail2ban restart
```

Pronto, agora é só olhar o log do fail2ban e esperar pelo primeiro bloqueio.

```
1 # tail -f fail2ban.log
2 2012-01-13 19:11:36,890 fail2ban.server : INFO   Changed logging target to /var/log/fail2ban.log for Fail2ban v0.8.3
3 2012-01-13 19:11:36,891 fail2ban.jail   : INFO   Creating new
4 jail 'ultrasurf'
5 2012-01-13 19:11:36,891 fail2ban.jail   : INFO   Jail 'ultrasurf' uses poller
6 2012-01-13 19:11:36,901 fail2ban.filter : INFO   Added logfile =
7 /var/log/messages
8 2012-01-13 19:11:36,902 fail2ban.filter : INFO   Set maxRetry = 6
9 2012-01-13 19:11:36,903 fail2ban.filter : INFO   Set findtime =
10 600
11 2012-01-13 19:11:36,903 fail2ban.actions: INFO   Set banTime = 900
12 2012-01-13 19:11:36,912 fail2ban.jail   : INFO   Creating new
```

```
jail 'ssh'

2012-01-13 19:11:36,912 fail2ban.jail   : INFO   Jail 'ssh' uses
poller

2012-01-13 19:11:36,913 fail2ban.filter : INFO   Added logfile =
/var/log/auth.log

2012-01-13 19:11:36,914 fail2ban.filter : INFO   Set maxRetry =
6

2012-01-13 19:11:36,915 fail2ban.filter : INFO   Set findtime =
600
2012-01-13 19:11:36,915 fail2ban.actions: INFO   Set banTime =
600

2012-01-13 19:11:36,985 fail2ban.jail   : INFO   Jail
'ultrasurf' started
2012-01-13 19:11:36,997 fail2ban.jail   : INFO   Jail 'ssh'
started

2012-01-13 19:11:52,029 fail2ban.actions: WARNING [ultrasurf]
Ban 10.23.134.42
2012-01-13 19:13:36,057 fail2ban.actions: WARNING [ultrasurf]
Ban 10.23.134.140

2012-01-13 19:26:52,081 fail2ban.actions: WARNING [ultrasurf]
Unban 10.23.134.42
2012-01-13 19:28:36,109 fail2ban.actions: WARNING [ultrasurf]
Unban 10.23.134.140

2012-01-13 19:33:50,137 fail2ban.actions: WARNING [ultrasurf]
Ban 10.23.134.42

2012-01-13 19:48:50,165 fail2ban.actions: WARNING [ultrasurf]
Unban 10.23.134.42

2012-01-13 19:53:44,193 fail2ban.actions: WARNING [ultrasurf]
Ban 10.23.134.140
```

Enviando email de aviso

É possível enviar um email de alerta a cada bloqueio e desbloqueio que o fail2ban faz.

Para ativar essa função você tem primeiramente que testar o envio de email na maquina, para fazer isso vamos usar o programa *mail*.

```
# mail seu-email@seu-dominio.com.br
```

```
 Subject: Teste
2
 Teste de envio de mensagem
3
 .
4
 Cc:
5
```

Atenção ao . no final da mensagem, ele finaliza o email.

O Debian por padrão utiliza o Exim, o log fica localizado em */var/log/exim4/mainlog*.

Você também pode usar o comando *mailq* para verificar a fila de email, em situações normais não deve existir nenhum email na fila.

Diversos detalhes podem impedir o envio de email, aqui não vou detalhar muito ,vou apenas colocar o conteúdo do meu arquivo */etc/exim4/update-exim4.conf.conf* para usar como referência.

```
1 dc_eximconfig_configtype='smarthost'
2 dc_other_hostnames='SERVER.DOMINIO.com.br'
3 dc_local_interfaces='127.0.0.1'
4 dc_readhost=''
5 dc_relay_domains=''
6 dc_minimaldns='false'
7 dc_relay_nets='127.0.0.1'
8 dc_smarthost='smtp.DOMINIO.com.br'
9 CFILEMODE='644'
10dc_use_split_config='false'
11dc_hide_mailname='false'
12dc_mailname_in_oh='true'
13dc_localdelivery='mail_spool'
```

Estou usando ele como smarthost e encaminhando as mensagens para o meu servidor de smtp.

Depois de ajustar o arquivo você deve executar o comando *update-exim4.conf* para atualizar a configuração, e reiniciar o Daemon do exim com o comando */etc/init.d/exim4 restart*

Pronto, se o envio de email pelo programa *mail* estiver funcionando você já pode ativar o envio de email pelo *fail2ban*, vamos lá.

Edite o arquivo */etc/fail2ban/jail.local*

```
#vi /etc/fail2ban/jail.local
```

```
[ultrasurf]
enabled   = true
filter    = ultrasurf
port      = all
banaction = iptables-ultrasurf
            sendmail-ultrasurf
logpath   = /var/log/messages
maxretry  = 6
bantime   = 900
```

Adicione a action *sendmail-ultrasurf* conforme exemplo acima.

Agora vamos criar um novo arquivo chamado /etc/fail2ban/action.d/sendmail-ultrasurf.local

```
vi /etc/fail2ban/action.d/sendmail-ultrasurf.local
```

```
 [Definition]
 actionstart =
 actionstop =
 actioncheck =
 actionban = printf %%b "Subject: Bloqueado <ip>
             From: Suporte <<sender>>
             To: <dest>\n
             \n
             O dispositivo com IP <ip> foi bloqueado depois de
```

```
9
  tentar burlar
10
              <failures> vezes o nosso sistema de seguranca.\n
11
              Acesso sera liberado automaticamente,\n
12
              Suporte" | /usr/sbin/sendmail -f <sender> <dest>
13
  actionunban = printf %%b "Subject: Liberado <ip>
14
                From: Infra <<sender>>
15
                To: <dest>\n
16
                \n
17
                O dispositivo com IP <ip> foi liberado para acesso
18normal\n
19
                Novas tentativas serao bloqueadas
  automaticamente,\n
20
                Suporte" | /usr/sbin/sendmail -f <sender> <dest>
21
  [Init]
22
  name = default
23
  dest = root
24
  sender = fail2ban
25
```

Feito isso você irá receber um email quando uma maquina for bloqueada ou desbloqueada, veja exemplo

Bloqueio

```
1
2O dispositivo com IP 10.23.134.41 foi bloqueado depois de tentar
2burlar
3
314 vezes o nosso sistema de seguranca.
4
4Acesso sera liberado automaticamente,
5
5Suporte
6
```

Desbloqueio

```
1
2O dispositivo com IP 10.23.134.41 foi liberado para acesso normal
3Novas tentativas serao bloqueadas automaticamente,
4Suporte
5
```

Você também pode alterar a mensagem a seu critério.

CentOS

O nosso amigo **Jovander** deu uma grande dica para funcionar em CentOS.

Trocando a linha

banaction = iptables-ultrasurf

por

action = iptables-ultrasurf

Ai sim o serviço funcionou e leu os logs.

Ubuntu

Nosso amigo **Angelo Figueiredo** deu uma dica pra quem utiliza o Ubuntu 12.04 LTS.

A configuração pode estar toda certinha e não estar bloqueando a solução é:

verificar o arquivo */etc/fail2ban/jail.conf*

se estiver

backend = auto

mude para

backed = polling

que irá começar a bloquear.

Agradecimento

Um forte abraço ao meu amigo **Yros Aguiar**, quando falei que eu ia criar um Daemon para ler o log, ele me lembrou que eu não precisaria re-inventar a roda, bastava usar alguma ferramenta já existente, rs.

Valeu, economizou horas de trabalho.

Conclusão

Fica ai a dica, pra mim funcionou.

Testei apenas com a versão 11.03, se em alguma outra não der certo peço que me avisem para podermos analisar como bloquear.

Com essa solução a cada tentativa de acesso utilizando o UltraSurf o usuário será bloqueado e não irá acessar mais nada pelo tempo determinado, com isso ele tem duas opções, ou entrar em contato com o suporte da empresa para reclamar ou parar de usar o UltraSurf.

Se ele reclamar você orienta a não usar mais o software, porém normalmente ele para de usar de forma natural o UltraSurf.

Download

Configuração **SEM** suporte a envio de email conf-fail2ban-ultrasurf.tar.gz
Configuração **COM** suporte a envio de email conf-fail2ban-ultrasurf-email.tar.gz

Referências

fail2ban
iptables
Bloquear Ultrasurf usando uma GPO

Rodrigo Luis Silva

Gestor de equipes especialista em sistemas GNU/Linux com vasta experiência em gerenciamento de storage, virtualização, network, desenvolvimento e outros.

http://www.dotsharp.com.br/linux/como-fazer-para-bloquear-ultrasurf-solucao-definitiva-iptables-fail2ban.html