Bloqueando redes da China e da Koreia
Ataliba Teixeira < ataliba em ataliba ponto eti ponto br >

http://www.ataliba.eti.br

Hoje, fazendo uma pequena busca sobre bloqueio de spam e redes, acabei caindo em um site interessante, que é o site do Mateus Lamberti[1] onde ele fala sobre uma solução não muito bonita, mas em compensação funcional, em que se bloqueia, através de uma lista mantida por um site, as redes vindas da China. Não é a solução ideal, tendo em vista que vai se bloquear dois países inteiros para o acesso a seu servidor. Mas em compensação se torna funcional, pois boa parte dos spammers utilizam servidores hospedados nestes dois países.

Assim, vou cobrir neste artigo as soluções que implementei em cima desta lista para iptables e Cisco (acls do roteador). Todas utilizam um script sh para gerar as regras. Um problema que quem utiliza Windows vai achar, talvez seja isto. Por ser em sh (shell do Unix), não vão conseguir implementar por exemplo, as regras para o roteador Cisco. Mas, com o cygwin[2], seus problemas acabaram. É só instalar ele em sua máquina e aproveitar as dicas do artigo.

Em Linux, a coisa é bem fácil. Bloquear o pessoal da China é algo bem trivial e tranquilo. O script disponível no site[3] já fornece um script iptables prontinho para uso. O grande problema é : o script de iptables fornecido lá foi pensado simplesmente para o bloqueio de smtp.

Pensando nisto, acabei criando um script para crontab onde pode ser feito o download das regras e criado também as regras para o ssh.

O script é o seguinte :

```
#!/bin/sh
{
TMP=/tmp/korea
mkdir $TMP
cd $TMP

sed 's/-A/-D/g' /root/rc.firewall.sinokorea > /root/tmprc.firewall.sinokorea

sh /root/tmprc.firewall.sinokorea

wget http://www.okean.com/antispam/iptables/rc.firewall.sinokorea

cat rc.firewall.sinokorea > /root/rc.firewall.sinokorea

sed 's/dport 25/dport 22/g' rc.firewall.sinokorea  | grep -v "#" >> /root/rc.firewall.sinokorea


cd ~

rm -rf $TMP

rm -f /root/tmprc.firewall.sinokorea

sh /root/rc.firewall.sinokorea

} &
```

Este script foi feito pensando na estrutura do Slackware[4]. Mas pode ser traduzido para qualquer distro, com uma ou outra edição da dica. Mas, vamos explicar o que está sendo feito acima, onde pode ser boservado que foram utilizados somente recursos do próprio shell e o programa wget .

Entendendo o script. Primeiro, ele cria um arquivo para deletar as regras que foram adicionadas anteriormente, utilizando o sed e o executa. Após isto, efetua o download do arquivo com as regras do iptables para uma pasta temporária dentro do diretório /tmp . Após isto, ele dá um cat no arquivo e dentro do diretório /etc/rc.d cria um arquivo chamado rc.firewall.sinokorea .

Logo após, um sed substitui a porta 25 pela 22, e um grep retira o símbolo “#” do resultado, e grava no arquivo /etc/rc.d/rc.firewall.sinokorea e depois o executa para adicionar as regras ao seu firewall.

Assim, você tem um arquivo pronto de iptables para adicionar ao seu firewall.

Aí, vem a parte interessante. No seu firewall, ou seja, o arquivo rc.firewall ou outro que você utilize, coloque a seguinte linha (em algum lugar que as regras façam sentido).

```
sh /etc/rc.d/rc.firewall.sinokorea
```

Isto vai garantir que toda a vez que sua máquina for reiniciada as regras do firewall sinokorea vão estar sendo carregadas no seu servidor.

Como pode ser visto, no Linux, a coisa é bem fácil.

No Cisco a coisa é um pouco diferente. Infelizmente, não tem como carregar as regras dele via um script shell ou coisa parecida (aliás, algo que os roteadores deveria melhorar é a tal interface shell deles), mas dá para pelo menos você criar o script ou melhor, as acls sem ter que gastar muita mão para ficar carregando-as.

Bom, no caso da Cisco, o site fornece as regras totalmente prontas também[5], o que ajuda em demasia. Mas, logicamente, caso você não queira usar um editor de texto para fazer a edição do que está lá, você pode simplesmente utilizar o script que segue abaixo.

Os passos que o pessoal da da Okean pedem para seguir são :

- Procure e troque “tcp” por “ip” (este passo bloquea todo o tráfego, incluindo tcp, udp e icmp) .
- Procure e troque “eq smtp” por “” - isto fornece a regra possibilidade de bloquear todas as portas para o host em contraposição a somente a porta 25.

Agora, as instruções para o arquivo em si :

- Modifique o “yyy” para o número da sua access-list de entrada.
- Modifique o “zzz.zzz.zzz.zzz” para o endereço ip do seu SMTP-SERVER (ou qualquer outra máquina que você queira proteger).
- Adicione a access list ao seu roteador (esta parte vou cobrir em parte neste artigo).

Como pode ser visto, este arquivo que contém as access-lists é algo que pode ser utilizado de diversas formas. E, assim, tentar parar um pouco a loucura que são os spams. No caso deste script, criei da forma seguinte : ele bloquea por padrão as portas tcp e all, mas vai te perguntar o que modificar. Te pergunta o número da regra e ip do seu servidor. E, assim, bloqueia tudo. Um

porém : tem como eu bloquear todo o tráfego vindo dos ips da Koreia e China, para meus servidores, sem exceção. Tem, e após este script, eu vou mostar como utilizar estas regras para este fim.

```
#!/bin/sh
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

mkdir /tmp/ciscosinokorea

cd /tmp/ciscosinokorea

# baixa o arquivo

wget http://www.okean.com/antispam/cisco/sinokoreaacl.txt

# aqui comeÃ§a a brincadeira



# E DA-LHE SED
# modifique aqui para os dados dos seus servidores

sed 's/yyy/numero_das_suas_regras_deentrada/g' sinokoreaacl.txt > tmp1.txt
sed 's/zzz.zzz.zzz.zzz/seu_ip_do_servidor/g' tmp1.txt > tmp2.txt

sed 's/tcp/ip/g' tmp2.txt > tmp3.txt

cat tmp3.txt > $HOME/sinokoreaacl.txt

cd $HOME

rm -rf /tmp/ciscosinokorea

less sinokoreaacl.txt
```

Listagem 2

Para bloquear o tráfego para todos os seus servidores, é só tornar a ACL mais radical. Para isto, é somente digitar a acl do seguinte modo :

```
access-list yyy deny tcp 58.14.0.0 0.1.255.255   !China
```

A regra acima bloquea todo o tráfego destes ips para todas as máquinas da sua rede. E como posso fazer isto no arquivo, para eliminar tornar o arquivo deste modo. O script abaixo, faz o que você precisa, e permitindo que você não precise, novamente, gastar braço para digitar as regras no seu roteador.

```
#!/bin/sh
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

mkdir /tmp/ciscosinokorea

cd /tmp/ciscosinokorea

# baixa o arquivo

wget http://www.okean.com/antispam/cisco/sinokoreaacl.txt

# aqui comeÃ§a a brincadeira



# E DA-LHE SED
# modifique aqui para os dados dos seus servidores

sed 's/yyy/numero_das_suas_regras_deentrada/g' sinokoreaacl.txt > tmp1.txt
sed 's/host zzz.zzz.zzz.zzz eq smtp//g' tmp1.txt > tmp2.txt

sed 's/tcp/ip/g' tmp2.txt > tmp3.txt

cat tmp3.txt > $HOME/sinokoreaacl.txt

cd $HOME

rm -rf /tmp/ciscosinokorea

less sinokoreaacl.txt
```

Listagem 3

De posse das regras prontas, é só colocar no roteador e ir para o abraço ...

E, finalmente, há como utilizar esta lista de ips para proteger o seu site, simplesmente negando a conexão dos mesmos via apache. Em geral, todos os provedores de hospedagem, fornecem a possibilidade de você utilizar um arquivo chamado htaccess.

O .htaccess é um arquivo especial para o Apache. Quando um usuário está navegando por alguma página do seu servidor Apache, para todo diretório que ele tentar acessar (e se o servidor estiver configurado para isso), o Apache procura pelo tal do .htaccess e se encontrar, verifica alguma restrição ou liberação para o usuário.

E como aproveitar este arquivo para utilização no seu apache ? Simplesmente, fazendo uso de dois scripts no seu cron. O primeiro, baixa a lista de ips sinokorea (listagem 4) do servidor e cria uma lista padrão, para ser lida pelo outro script, que insere esta listagem no seu arquivo .htaccess (listagem 5).

Ou seja, nada muito difícil, mas que vai diminuir em demasia o número de spams que você vai receber via comentários no seu site.

```
#!/bin/sh

cd ~/db

wget http://www.okean.com/sinokoreacidr.txt

cat sinokoreacidr.txt | grep -v "#"  | cut -d ' ' -f 1 > china_and_korea.cidr

rm -f sinokoreacidr.txt
```

Listagem 4

```
#!/bin/sh
$HTACCESS=/localizacao/do/seu/htaccess
 echo "order allow,deny" > $HTACCESS

for i in `cat ~/pastaqualquer/china_and_korea.cidr`; do
   echo "deny from $i " >> $HTACCESS
done

 echo "allow from all" >> $HTACCESS
```

Listagem 5

Como pode ser visto, a listagem fornecida por este site pode lhe dar n possibilidades de criação de scripts para tentar parar um pouco dos spams no seu site. E, garantidamente, estes scripts diminuem, e muito, a incidência de spams e afins na sua rede computacional ou até, um simples blog.

Espero que este artigo seja útil a alguém e caso tenha alguma sugestão ou correção, mande um email :-)

Bibliografia

[1] http://matheuslamberti.wordpress.com/2006/08/23/bloqueando-ips-vindos-da-chinakorea/

[2] http://www.aurelio.net/cygwin

[3] http://www.okean.com/thegoods.html

[4] http://www.slackware.com

[5] http://www.okean.com/antispam/cisco/sinokoreanacl.html