FACCAT | FACULDADES INTEGRADAS DE TAQUARA

11ª Install Fest Linux da FACCAT

Segurança de Acesso á Internet com o Squid, Dansguardian e ClamAV

Como proteger o acesso á Internet com bloqueios de sites indevidos, escaneamento de conteúdo online e monitoramento com histórico de acessos utilizando Software Livre.

Tecnologia

O **Dansguardian** é um campeão na área de Filtro de conteúdo agindo como proxy. Está diponível para Linux, MacOSX, *BSD, HP-UX e Solaris. O Dansguardian utiliza um método de múltiplos níveis para filtrar o conteúdo que entra pelo proxy (squid, neste caso).

Níveis de interface:
Primeiro Nível (Baixo) – Configurações mais minuciosas de controle de acesso, considerado nível “geek” .
Segundo Nível (Moderado) – Nível mais comum onde as regras são pré-configuradas e só precisam ser habilitadas ou não – São diversos arquivos “.include” que adicionam as funcionalidade utilizando:

- Blacklists – Sites inteiros e porções identificadas
- Phraselists – Frases e palavras que devem ser completamente banidas
- Padrões de URLs – Certos padrões que identificam o conteúdo a ser bloqueado, sites com ‘xxx’ no nome, por exemplo.

Métodos de Filtragem:

- Filtragem baseada em listas classificadas como Black/White e domínio/url
- Bloqueio de expressões regulares
- Substituição por redirecionamento
- Sistema PICs de classificação de sites (http://www.w3.org/PICS/)
- Filtro com Anti-Vírus
- Filtro por Meta-tags
- Filtro por extensão ou tipo MIME de arquivo
- Filtro por palavras ou frases em sites

Squid

Um servidor de proxy com uma variedade de utilizações como aceleração de conteúdo fazendo cacheamento de requisições repetidas, adição de segurança com sistema de filtragem, entre outras.

ClamAV

Clam Anti-Vírus gratuíto para múltiplas plataformas capaz de detectar diversos tipos de software malicioso, incluindo vírus, trojans e spywares. Muito utilizado em servidores de Email.

Adicionando funcionalidades ao Dansguardian:

Blacklists:

http://www.urlblacklist.com

http://www.shallalist.de

http://www.malware.com.br

Métodos de autenticação:

Modo default:

NCSA - Autentica utilizando um arquivo com usuário/senha.

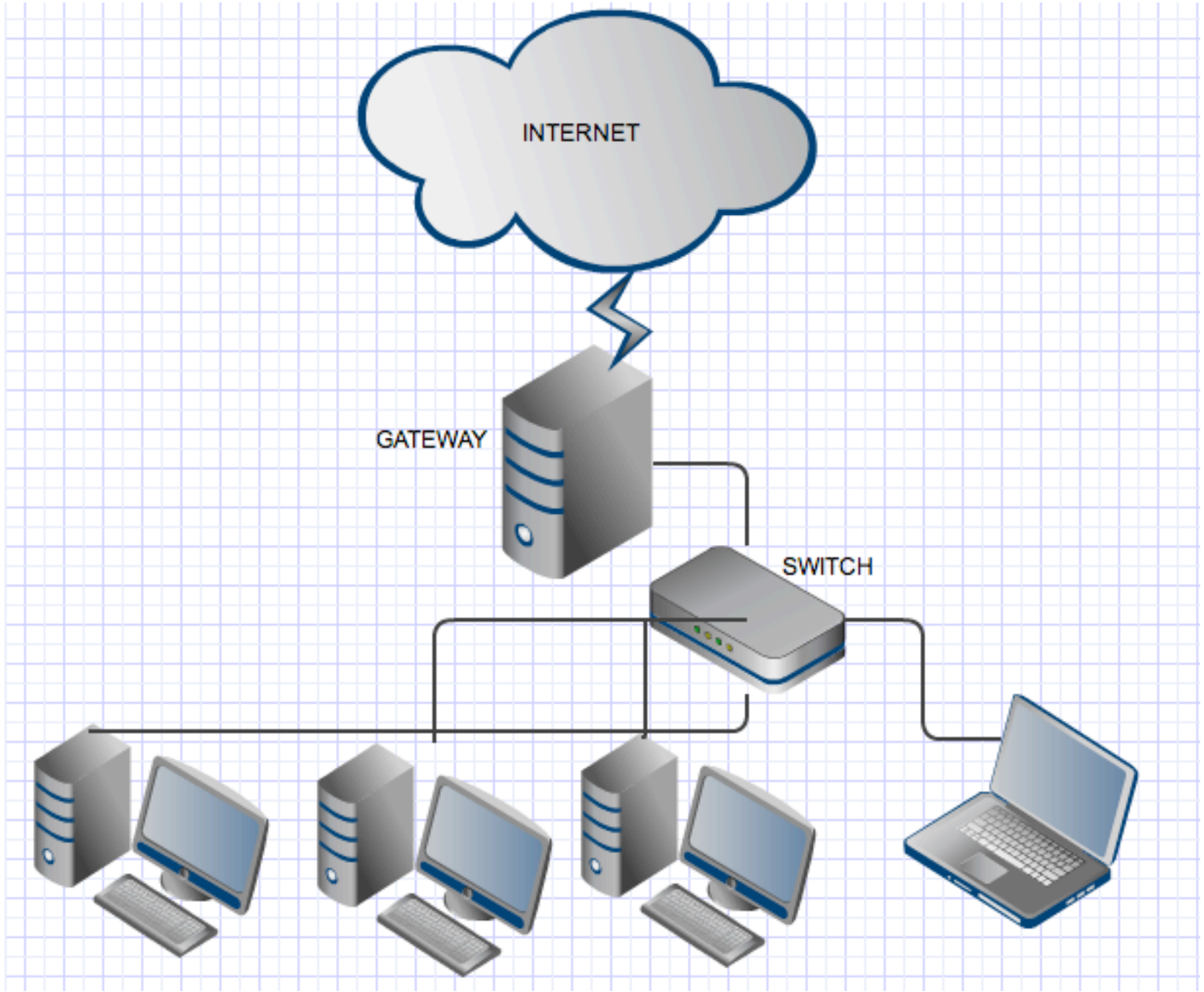
PAM - Pluggable Authentication Module. Utiliza sistemas PAM já embutidos, como o o próprio Linux.

Disponível:

LDAP - http://www.surf.org.uk/src/squidauth.html

Autenticação do Squid por LDAP, e consequentemente Active Directory.

Topologia de rede



Neste cenário o tráfego com destino `a Internet é redirecionado no Gateway, e passa a ser filtrado pelo Dansguardian e CLAMAV.

Instalação

1. Instale o Linux Ubuntu.
2. Configure sua rede para acesso á Internet.
3. Configure sua rede para atender aos seus clientes, aplique uma regra NAT na firewall.

sudo iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
sudo echo 1 > /proc/sys/net/ipv4/ip_forward

Dica: Caso não queira adicionar o comando sudo em cada tarefa, execute "sudo su" para se tornar "root"

4. Atualize o sistema:

apt-get update

5. Instale os aplicativos necessários:

apt-get install squid clamav-daemon dansguardian apache2 sarg

6. Faça o backup do squid.conf

cd /etc/squid.conf
cp squid.conf squid.cong.original

7. Edite o squid.conf com seu editor preferido:

visible_hostname squid
http_port 3128 transparent

8. Adicione o usuário squid:

adduser squid

9. Inicie o squid:

service squid start

10. Instale o Webmin:

apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl
wget http://downloads.sourceforge.net/project/webadmin/webmin/1.510/webmin_1.510-2_all.deb?use_mirror=ufpr
dpkg -i webmin_1.510-2_all.deb

11. Configure o Dansguardian:

cd /etc/dansguardian/
cp dansguardian.conf dansguardian.conf.original

É importante editar as seguintes linhas:

#UNCONFIGURED <= Comente esta linha para habilitar o Dans
loglevel 3
language = ‘portuguese’
filterip = XXX.XXX.XXX.XX

Modifique a seguinte linha com o endereço do servidor:

accessdeniedaddress = 'http://IP/cgi-bin/dansguardian.pl'

Habilite o CLAMAV:

contentscanner = '/etc/dansguardian/contentscanners/clamav.conf'

Instale o módulo de gerenciamento do Dansguardian via Webmin:
http://downloads.sourceforge.net/project/dgwebminmodule/dgwebmin-devel/0.7.0beta1b/dgwebmin-0.7.0beta1b.wbm?use_mirror=ufpr

No nosso exemplo iremos configurar o Dans para adultos:
Em /etc/dansguardian/dansguadianf1.conf modifique a seguinte linha
naughtynesslimit = 200

Opções recomendadas:
50 = crianças
100 = adoscelentes
160 = adultos

Modifique a linha para que os arquivos sejam escaneados:
#blockdownloads = off

Todas as configurações do Dans podem ser feitas a partir do Webmin acessando a porta https://localhost:10000

O filtro de conteúdo funciona em dois níveis, ao acessar uma página o Dans checa as listas de acesso e se o endereço ou IP estiver presente, bloqueia o acesso. Caso contrário, a requisição é enviada ao squid que busca o conteúdo e novamente o Dans verifica e pontua de acordo.

12. CLAM AV

Checar se o Clam está rodando:

```
ps -ef | grep clamav
```

Testar:

```
wget http://dansguardian.org/downloads/2/Variants/AVTest/danger/eicar.com.txt

clamscan -v eicar.com.txt
```

O resultado deverá conter:

```
eicar.com.txt: Eicar-Test-Signature FOUND
---------- SCAN SUMMARY -----------
Scanned files: 1
Infected files: 1
```

13. Configure o NAT, bloqueio de acesso direto ao squid e redirecione as portas:
Para isso criamos um script que permite criar essas regras quando o sistema carrega, crie um arquivo em /etc/network/if-up.d/iptables-config
com o seguinte conteúdo:

```
#!/bin/bash
iptables -F
#Configure de acordo com sua rede eth0 para LAN e eth1 para WAN
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
iptables -A INPUT -m tcp -p tcp  ! -s 127.0.0.1 --dport 3128 -j DROP
```

Depois disso modique as permissões deste arquivo para que possa ser executado:

```
chmod +x /etc/network/if-up.d/iptables-config
```

Obrigado!

jfranco@maila.com.br