

Squid com autenticação Windows 2003(domínio)

Bom como sempre, eu tinha uma necessidade de fazer um servidor proxy, autenticar em um servidor de domínio *Windows 2003*, procurei pela internet e achei alguns tutoriais, mas sempre, faltava algo.

No meu caso eu tinha um servidor linux *Slackware 9.1* atualizado até o *kernel 2.4.26*, com todos os patches aplicados até o momento, tinha um servidor de domínio *Windows 2003* (em produção) e tinha que colocar o mais rápido possível um servidor proxy para usar os usuários no servidor de domínio para autenticação.

Agora vamos colocar as mãos na massa:

Em primeiro lugar, eu instalei o linux *Slackware 9.1* em uma máquina que me foi disponibilizada, baixei do site todos os patches e continuo baixando sempre que sai algo novo, atualizei o kernel para a versão mais nova. Fiz todos os procedimentos de segurança e deixei o servidor bem fechado, passei o nmap nele para verificar as portas, atualizei também o kde para a última versão.

Baixei da Internet a última versão do Squid, só que baixei o código fonte, pois posso customizar a instalação de acordo como as minhas necessidades.

Descompactei o Squid em um diretório temporário como por exemplo */tmp* ,

```
$cd /tmp
```

```
$tar -zxvf squid- 2.5.STABLE5.tar.gz
```

Depois entrei no diretório criado quando da descompactação e criei um script shell para fazer a configuração.

```
$cd squid- 2.5.STABLE5
```

O conteúdo deste shell script é:

```
#!/bin/bash
```

```
./configure --prefix=/usr/local/squid \  
--enable- storeio=diskd,ufs \  
--enable- default- err- language=Portuguese
```

```
make
```

```
make install
```

note que o script vai executar a configuração do squid, depois fazer compila-lo e instala-lo no diretório */usr/local/squid* .

Feito a instalação, devemos agora compilar o programa que irá fazer a conexão com o windows, normalmente ele está no diretório *squid- 2.5.STABLE5/helpers/basic_auth/* este diretório é onde contém os programas para acesso de autenticação dentro dele iremos ver várias pastas, uma para cada tipo de autenticação, verifique se existe uma pasta de nome **MSNT**, entre nela compile o programa *msnt_auth* e depois instale-o.

```
$pwd
```

```
/tmp/squid- 2.5.STABLE5/helpers/basic_auth/MSNT
```

```
$make
```

```
$make install
```

Após compilado o Squid e o modo de autenticação e instalado está na hora de customiza- los.

Em primeiro lugar iremos configurar o acesso ao windows:
Para isto devemos ir até o diretório onde foi instalado o Squid.

```
$cd /usr/local/squid
```

Verificar se os arquivos abaixo foram criados, normalmente eles são criados no diretório **/usr/local/squid/etc** :

```
msntauth.conf  
denyusers  
allowusers
```

se não existir, não faz mal, criaremos eles, em primeiro lugar vamos editar ou criar o arquivo **msntauth.conf**.

O conteúdo do arquivo original deve ser algo como descrito abaixo:

```
# Sample MSNT authenticator configuration file.  
# Antonio Ianella, Stellar- x Pty Ltd.  
  
# Nt host to use. Best to put their IP addreses in /etc/hosts.  
server PDC BDC DOMAINNAME  
server PDC2 BDC2 OTHERDOMAINNAME  
  
denyusers    $SQUIDPREFIX/squid/etc/denyusers  
allowusers   $SQUIDPREFIX/squid/etc/allowusers
```

Agora deve- se substituir as variáveis **PDC** e **BDC** pelo nome do domínio primário e do secundário da rede. Deve ser colocado no **/etc/hosts** do servidor Squid as entradas relativas a estes servidores para resolução de nomes.

Exemplo 1: **/etc/hosts**

```
10.1.1.1      primeiro  
10.1.1.2      segundo
```

Exemplo 2: **msntauth.conf**

```
server        primeiro      segundo      nomedodominio  
  
denyusers     /usr/local/squid/etc/usuarios/denyusers  
allowusers    /usr/local/squid/etc/usuarios/allowusers
```

No caso eu coloquei os arquivos **denyuser** e **allowusers** dentro de um subdiretório **usuarios** para facilitar a administração.

Feito esta etapa, agora criaremos dentro do diretório */usr/local/squid/etc* o diretório *usuarios*, onde colocaremos os arquivos mencionados no exemplo acima.

Depois de criado o diretório e movido os arquivos *denyuser* e *allowusers*, podemos editá-lo, colocando os usuários do Squid que irão ter acesso ao proxy no arquivo *allowusers* e os que não terão acesso ao proxy no *denyuser*, note que se comentarmos as linhas onde citamos os arquivos, todos os usuários cadastrados no domínio terão acesso ao proxy.

A parte de configuração de acesso ao domínio já está configurada, agora iremos configurar o Squid.

Devemos editar o arquivo *squid.conf* que está no diretório */usr/local/squid/etc*, e procurarmos a linhas de configuração de autenticação e alterá-las.

A alteração que deve ser colocada é a seguinte:

```
auth_param basic program      /usr/local/squid/libexec/msnt_auth
auth_param basic children      5
auth_param basic realm         Squid proxy-caching web server
auth_param basic credentialsttl 5 minutes
```

Depois de alterar as configurações de autenticação, alterar o parâmetro de tipo de cacheamento.

```
cache_dir diskd /usr/local/squid/var/cache      20000 128 512
```

Agora vamos definir as configurações proprietárias para o nosso acesso, pode-se deixar os acls com as porta padrão, pois está bem dimensionado.

No meu caso eu defini um limite de simultaneidade de usuários, que no caso é um.

```
acl limit_user max_user_ip -s 1
```

Criei também acl para a minha rede de origem.

```
acl src_rede_origem src "/usr/local/squid/etc/origens/rede_origem"
```

Note que deve ser criado o arquivo *rede_origem* com o endereço da rede em questão.

Criei um acl para uma *black list*, onde contém sites de sexo.

```
acl dst_deny dstdom_auth "/usr/local/squid/etc/blacklist/deny"
```

Note que deve ser criado o arquivo *deny* com os domínios da internet com sites de sexo que se que proibir.

Criei um acl para usuários.

```
acl usr_priv proxy_auth "/usr/local/squid/etc/usuarios/especiais"
acl usr_usuario proxy_auth REQUIRED
```

Note que deve ser criado o arquivo *especiais* com os usuários que tenham acesso especial

Depois de definir as acls, podemos fazer as regras de acesso. Eu usei algumas e estão descritas abaixo.

Acesso para usuário especiais como total acesso.

```
http_access allow usr_priv
```

Proibindo acesso para site de sexo

```
http_access deny dst_deny
```

Liberando acesso com autenticação e limite de sessão.

```
http_access allow src_rede      usr_usuario !limit_user
```

mensagens de erro.

```
error_directory      /usr/local/squid/share/errors/Portuguese
```

Após feito as regras, salvar as configurações, e vamos inicializar o Squid.

```
#!/usr/local/squid/sbin/squid -k
```

O comando acima irá criar a árvore de cacheamento, após retornar para o prompt inicializaremos o Squid.

```
#!/usr/local/squid/sbin/squid
```

Agora temos que ter certeza que o domínio esta funcionando corretamente, e verificar se os usuários existem, verificar também se os serviços de *net logon e NTLM* estão ativos, depois é só abrir algum browser, configura- lo e testar os acessos.

Jorge Alexandre
Sys Admin