Laboratório de Proxy

Objetivo

Verificar como funciona um Proxy de HTTP através da configuração e utilização do servidor Squid.

Descrição

Executaremos um servidor Web Apache na máquina *ServWeb*, que responde pelo site www.xyz.com.br, onde disponibilizaremos duas páginas HTML chamadas *índex.html* e *download.html*.

Teremos duas máquinas clientes, chamadas *Cliente1* e *Cliente2*, que vão tentar acessar as duas páginas do servidor através do Proxy instalado na máquina *Proxy*.

Será utilizada a técnica de Proxy Transparente para fazer com que as requisições dos clientes sejam redirecionadas para o Proxy. Isso será feito no roteador chamado *Roteador*.

Serão criadas regras no Proxy para que:

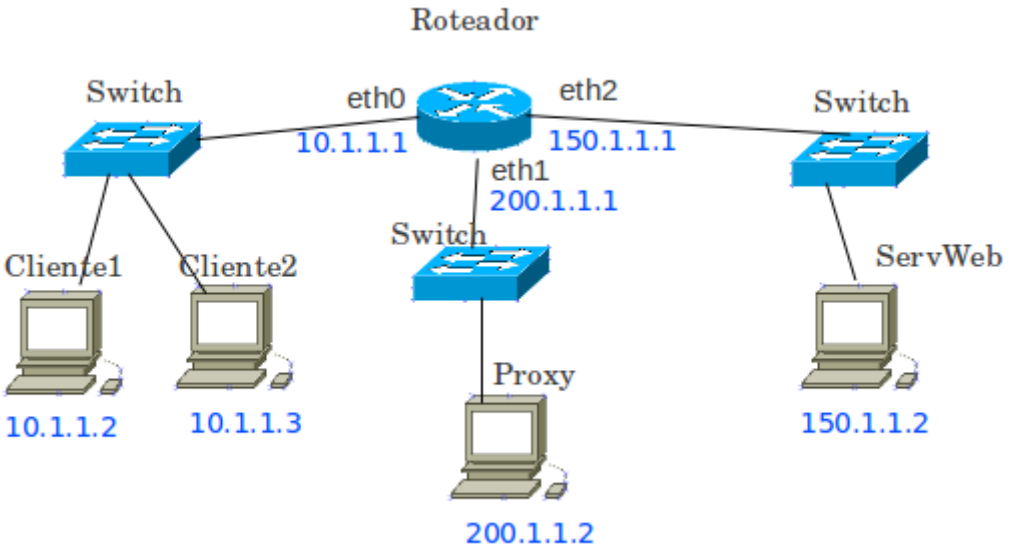
- Apenas Cliente1 possa acessar o site www.xyz.com.br.
- Ninguém consiga acessar URLs onde apareçam a palavra "download". Desse modo, ninguém conseguirá acessar a página download.html que está ServWeb.

Finalmente, olharemos as informações gravadas no arquivo de log do Proxy, decorrente das requisições feitas pelos clientes.

Para não precisarmos instalar um servidor de DNS que responda pela máquina www.xyz.com.br, inserimos uma linha no arquivo hosts de cada máquina utilizada, associando esse nome ao endereço IP 150.1.1.2, que é o endereço de *ServWeb*.

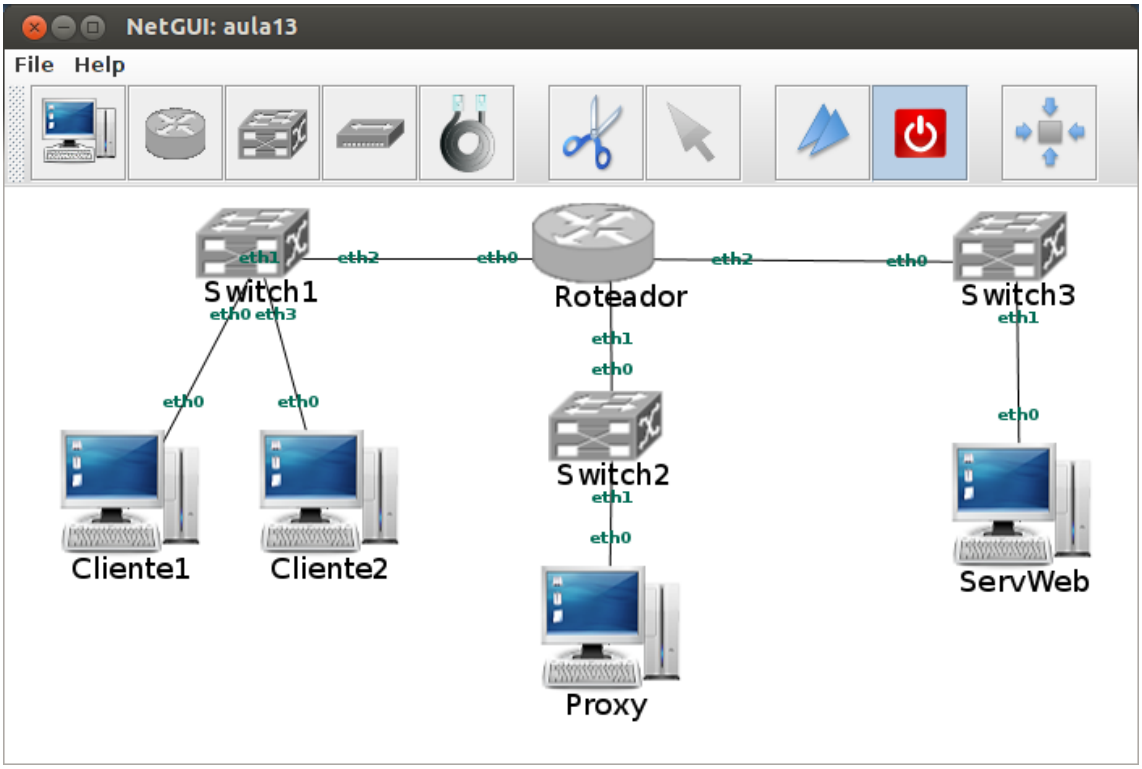
Rede Exemplo

A Figura a seguir mostra a rede utilizada neste laboratório, onde aparecem os endereços IPs de todas as máquinas e do roteador.



Roteiro Experimental

1. Inicie o NetGUI, depois clique em “File”, em seguida clique em “Open”. Na janela que aparece selecione a pasta “Tutoriais”, depois selecione a pasta “Aula13”, depois selecione a pasta “Tutorial-01”, e em seguida clique em “Open”. Isso carregará o projeto com a rede mostrada na seção anterior (Rede Exemplo). A seguinte topologia de rede deve aparecer:



Além disso, embora os endereço IP e MAC não apareçam na tela do NetGUI, os equipamentos já estão configurados com os endereços mostrados

na Rede Exemplo. Quando os equipamentos forem inicializados os endereços IP serão mostrados.

a. Inicie todos os equipamentos clicando no botão  e depois clique no equipamento. Isso irá iniciar uma nova janela com um Shell do equipamento que foi iniciado. Observe que o símbolo desse botão (dois triângulos) aparecerá sobre a figura do equipamento.

2. Inicialmente vamos editar o arquivo de configuração do Squid para fazermos as alterações necessárias, que consistem em: i) configurá-lo para trabalhar como Proxy Transparente, ii) configurar as regras de controle de acesso usando as linhas *acl* e *http_access.*
   a. Na máquina *Proxy* Abra o arquivo de configuração do Squid usando o comando a seguir.

```
# nano /etc/squid3/squid.conf
```

   b. Pesquise pela linha contendo “http_port 3128” e acrescente a palavra “transparent” ao seu final, de modo que fique como mostrado seguir.

```
http_port 3128 transparent
```

   Como o arquivo é muito grande é melhor você usar a opção de busca do editor de texto para localizar essa linha.
   Isso é tudo que precisa ser feito no arquivo de configuração para que o Squid funcione como um Proxy transparente.
   c. Vamos agora configurar as regras de controle de acesso. Pesquise a linha a seguir.

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

   Logo abaixo dela insira o texto mostrado abaixo.

```
acl redeinterna src 10.1.1.0/24
acl cliente2 src 10.1.1.3/32
acl dominio dstdomain .xyz.com.br
acl proibida url_regex download
http_access deny cliente2 dominio
http_access deny proibida
http_access allow redeinterna
```

Veja que a linha "acl proibida url_regex download" cria uma ACL chamada de *proibida*, que casa com qualquer URL que contenha a palavra *download*. Desse modo, requisições para o arquivo *download.html* do servidor web, casam com essa ACL, uma vez que a URL requisitada será "HTTP://www.xyz.com.br/download.html".

Veja também que as regras acima proíbem *Cliente2* de acessar o site em WebServ.

d. Faça com que o Squid releia o arquivo de configuração utilizando o comando a seguir.

```
# squid -k reconfigure
```

3. Agora vamos configurar o Roteador para que redirecione as requisições tcp endereçadas a porta 80 para o Proxy. Faça isso digitando o comando a seguir (todo em uma mesma linha) na máquina *Roteador*.

```
# iptables -t nat -A PREROUTING -p tcp -s 10.1.1.0/24 --dport 80 -j
DNAT --to-destination 200.1.1.2:3128
```

Veja que esse comando altera o IP de destino e a porta de todos os pacotes que chegam ao roteador vindos da rede 10.1.1.0/24 e que são destinados a porta 80 de qualquer máquina. O IP de destino é alterado para 200.1.1.2, e a porta de destino para 3128. Com isso, os pacotes são entregues ao Proxy.

4. Agora vamos apenas conferir o conteúdo dos arquivos HTML existentes no servidor Web.
   a. O arquivo principal do site, que será mostrado quando for requisitada a URL HTTP://www.xyz.com.br, é o *índex.html*. Para vê-lo digite o comando a seguir.

```
# cat /var/www/índex.html
```

   b. Temos também o arquivo download.html, que será requisitado pelos clientes através da URL HTTP://www.xyz.com.br/download.html. Para vê-lo digite o comando a seguir.

```
# cat /var/www/download.html
```

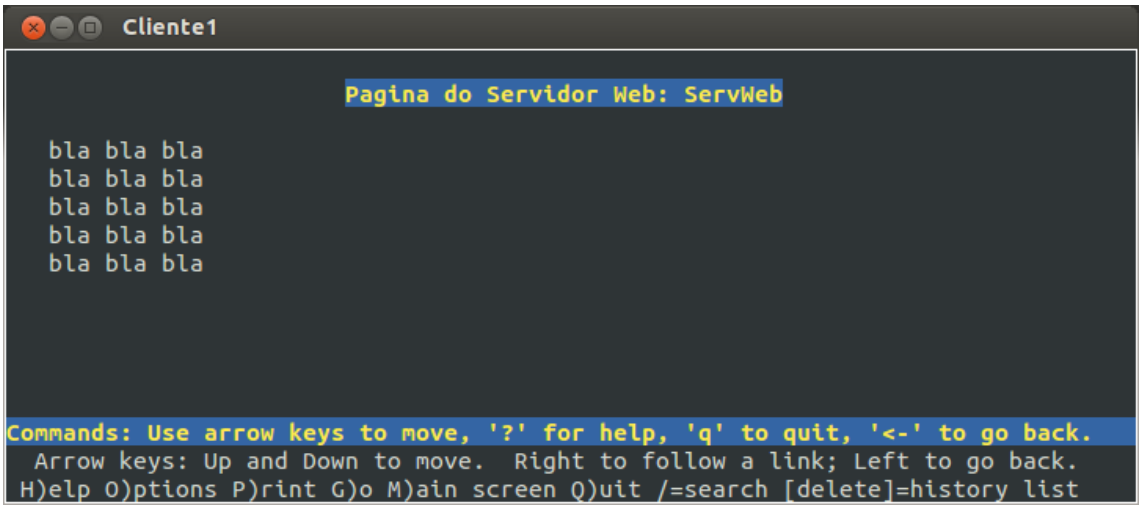
5. Finalmente vamos realizar os acessos ao servidor Web através de *Cliente1* e *Cliente2*. Tentaremos acessar cada uma das páginas de cada um dos clientes. Utilizaremos um navegador em modo texto chamado lynx.

a. Em Cliente1 digite o comando a seguir para acessar a página principal do servidor Web.

```
# lynx HTTP://www.xyz.com.br
```

A imagem a seguir mostra a execução desse comando.

Veja que a página é obtida com sucesso, conforme mostrado a seguir.

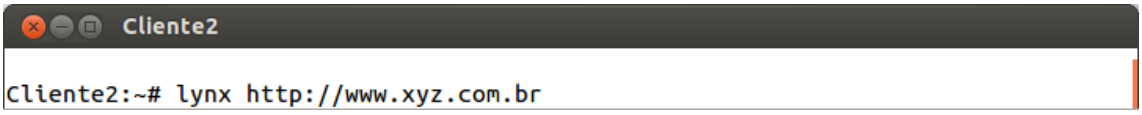


Para sair do lynx tecle a letra “q” e depois a letra “y”.

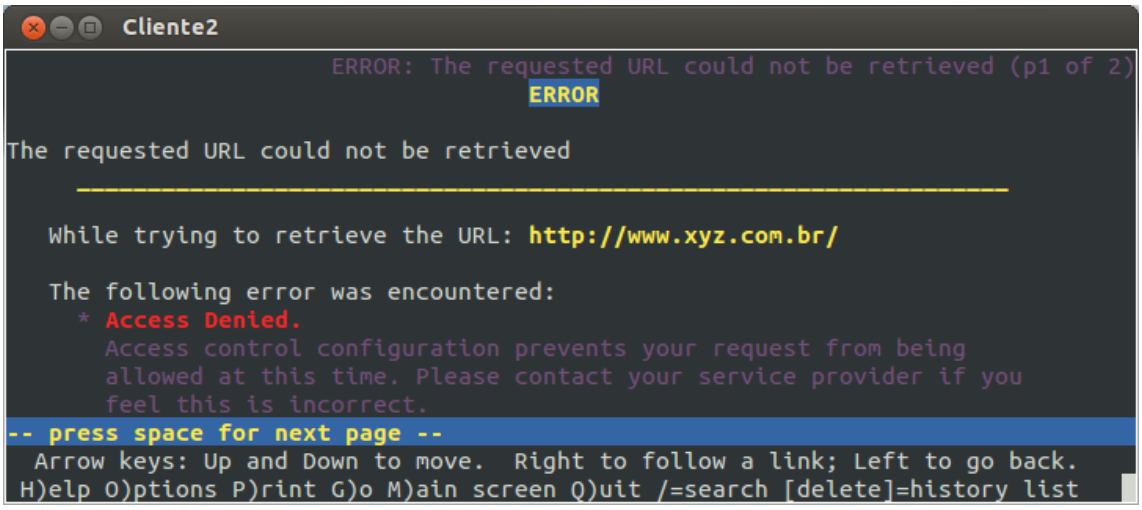
b. Vamos agora tentar acessar a página principal do servidor Web a partir de *Cliente2*. Vá para aquela máquina e digite o comando a seguir.

```
# lynx HTTP://www.xyz.com.br
```

A imagem a seguir mostra a execução desse comando.



Veja que após aparecer a mensagem “*Alert!: HTTP/1.0 403 Forbidden*”, será mostrada uma tela semelhante a que vemos a seguir, indicando “*Access Denied*”, ou seja, acesso negado.

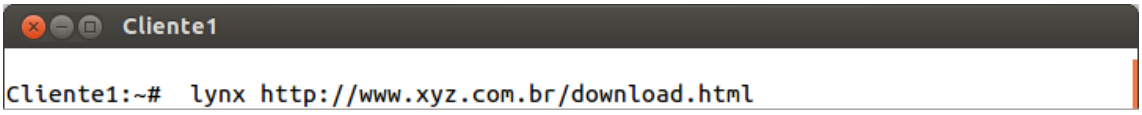


Como era esperado, o Proxy não permitiu que *Cliente2* acessasse o site www.xyz.com.br

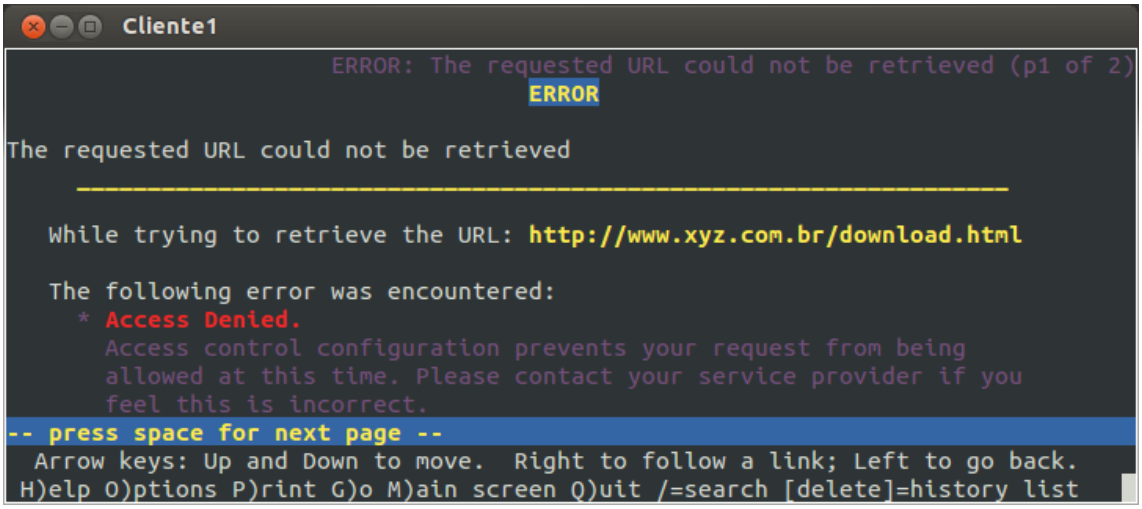
c. Vamos agora tentar acessar a página *download.html* do servidor Web a partir de *Cliente1*. Vá para aquela máquina e digite o comando a seguir.

```
# lynx HTTP://www.xyz.com.br/download.html
```

A imagem a seguir mostra a execução desse comando.



Veja que após aparecer a mensagem "*Alert!: HTTP/1.0 403 Forbidden*", será mostrada uma tela semelhante a que vemos a seguir, indicando "*Access Denied*", ou seja, acesso negado.

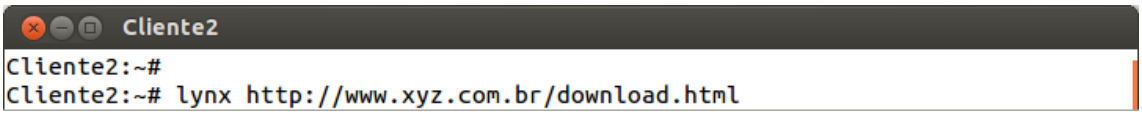


Como era esperado, o Proxy não permitiu que *Cliente1* acessasse a URL HTTP://www.xyz.com.br/download.html, uma vez que essa URL contém a palavra *download*.

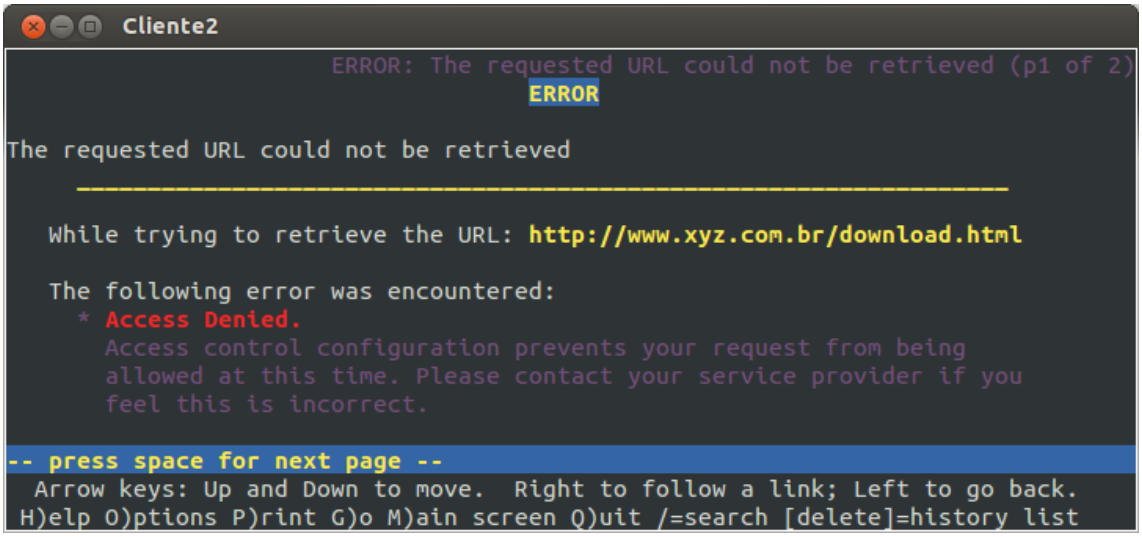
d. Vamos agora tentar acessar a mesma página *download.html* do servidor Web a partir de *Cliente2*. Vá para aquela máquina e digite o comando a seguir.

```
# lynx HTTP://www.xyz.com.br/download.html
```

A imagem a seguir mostra a execução desse comando.



Veja que após aparecer a mensagem "*Alert!: HTTP/1.0 403 Forbidden*", será mostrada uma tela semelhante a que vemos a seguir, indicando "*Access Denied*", ou seja, acesso negado.



Como era esperado, o Proxy também não permitiu que *Cliente2* acessasse a URL *HTTP://www.xyz.com.br/download.html*, uma vez que essa URL contém a palavra *download*.

6. Agora vamos ver o arquivo de log do Squid, onde ele armazena as requisições recebidas. Esse arquivo se chama Access.log e fica na pasta /var/log/squid. Digite o comando a seguir para ver apenas as quatro últimas linhas do arquivo.

```
# tail -n 4 /var/log/squid/access.log
```

A saída é algo semelhante a mostrada a seguir, onde podemos ver as quatro requisições que fizemos anteriormente. Vemos também que apenas a primeira requisição foi atendida, que foi a requisição do *Cliente1* (10.1.1.2) pela URL HTTP://www.xyz.com.br.

7. Desligue todos os equipamentos, clicando no botão  do NetGUI e depois na Figura que representa o equipamento a ser desligado. Repita isso para os três equipamentos.
    a. Nunca feche a janela do terminal de uma máquina virtual clicando no  da janela.