Roteiro de Atividades 9

Esta atividade pode ser feita tanto pelo cliente Windows quando pelo cliente Linux.
É importante que tanto a máquina cliente quanto o servidor estejam na mesma rede.
Teste o funcionamento da rede através do comando *ping*.

Para realizar este Roteiro de Atividades, é necessário que o servidor esteja configurado com duas placas de rede: uma delas deve possuir rota e acesso à internet.

Vamos supor que a nossa interface eth0 será a interface com acesso à internet, configurada pelo DHCP do laboratório.

1. No servidor, ative o *ip_forward*, editando o arquivo */etc/sysctl.conf* e inserindo a linha a seguir:

```
net.ipv4.ip_forward=1
```

Atividade 9.1 – Instalação e configuração do servidor proxy Squid

Nesta atividade, será feita a instalação a partir do repositório Debian. Observe que serão instalados os pacotes iptables (*firewall*), SARG (gerador de relatório de acesso) e apache2 (servidor web para publicação dos relatórios do SARG).

Caso o SARG não esteja disponível na lista padrão de repositórios, devemos incluir um novo repositório conforme orientação do instrutor. Em seguida, efetue a instalação dos pacotes squid, iptables, sarg e apache2.

1. As configurações a seguir deverão estar descritas no arquivo */etc/squid/squid.conf* com as modificações necessárias de acordo com a característica de cada rede local.

   Cada comando recebeu um comentário para facilitar o entendimento. Ainda assim, não deixe de ler o manual do Squid para obter mais informações.

```
#Porta utilizada pelo Cliente

http_port 3128

#Porta utilizada para troca de informações entre Proxies

icp_port 3130

# nome do proxy

visible_hostname cache.empresa.com.br

#Manter configuração Default

acl QUERY urlpath_regex cgi-bin \?

no_cache deny QUERY

#Configurações do Cache

cache_mem 96 MB

cache_swap_low 75
```

```
cache_swap_high 95
maximum_object_size 900 MB
minimum_object_size 0 KB
maximum_object_size_in_memory 32 KB
#Configurações do diskd
cache_dir ufs /var/spool/squid 20000 64 256
#path dos Logs
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log none
# definir o rotate log
logfile_rotate 10
#não emula o log do Apache
#emulate_httpd_log on
#opções de FTP
ftp_user admin@empresa.com.br
ftp_passive on
#Manter as configurações Default
refresh_pattern ^ftp:               1440  20%   10080
refresh_pattern ^gopher:     1440  0%   1440
refresh_pattern .            0   20%   4320
#acl defaults
acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl SSL_ports port 443 563
acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443 563
acl Safe_ports port 70
acl Safe_ports port 210
```

```
acl Safe_ports port 1025-65535
acl Safe_ports port 280
acl Safe_ports port 488
acl Safe_ports port 591
acl Safe_ports port 777
acl CONNECT method CONNECT
#Acesso à página do cache manager
http_access allow manager localhost
http_access deny manager
#Acesso Defaults
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow SSL_ports
#ACLS e regras de acesso
# Permitir o acesso ao servidor proxy a partir da rede interna
acl rede src 192.168.1.0/255.255.255.0
http_access allow rede
#regra default
http_access deny all
#Configuracoes defaults
http_reply_access allow all
icp_access allow all
miss_access allow all
never_direct allow all
```

2. Parar o serviço do squid:

```
# /etc/init.d/squid stop
```

3. Criar a árvore de diretórios de cache:

```
# squid -z
```

4. Reiniciar o serviço:

```
# /etc/init.d/squid start
```

Atividade 9.2 – Configuração dos navegadores

Nesta atividade, será feita a configuração do navegador Internet Explorer. Essa configuração deverá ser feita em todas as máquinas de usuário que acessarão a internet por meio do servidor proxy squid.

Configure o navegador para acessar a internet passando pelo servidor Proxy.

Atividade 9.3 – Configuração de listas de controle de acesso

Nesta atividade, será configurado o proxy squid com a utilização de listas de controle de acesso por endereço por MAC, IP, hora, tipo de arquivo e sites restritos.

O Squid avalia as regras de acesso por procedência, ou seja, a primeira regra com a qual a solicitação se adequar será a regra aplicada pelo servidor. Esse comportamento faz com que todas as regras listadas a seguir devam anteceder a linha *http_access deny all* do arquivo de configuração.

- Limitar o acesso à internet para o endereço MAC da estação Windows: procure pela diretiva arp;
- Limitar o acesso à internet para o endereço IP do cliente Windows: procure pela diretiva src;
- Não permitir o acesso à internet nos horários de 0h as 6h e de 19h as 23:59h, durante os dias da semana;
- Proibir o download de arquivos com extensão *.mp3* e *.avi*;
- Restringir o acesso ou pesquisa de algumas palavras, como por exemplo: sexo, playboy, sexy etc.;
- Proibir o acesso a uma lista de sites.

Atividade 9.4 – Configuração do SARG

SARG é um gerador de relatório de acesso e uso de internet. Com essa ferramenta é possível identificar e controlar os sites que os usuários estão acessando durante o dia de trabalho.

Configure o SARG para que seja possível visualizar o relatório. Fique atento aos parâmetros *output_dir* e *access_log*.

Atividade 9.5 – Proxy transparente

Altere a configuração do servidor Proxy para que os clientes possam realizar o acesso à internet de forma transparente. Lembre-se de remover a configuração de proxy dos navegadores dos clientes.

Precisaremos criar uma regra no iptables para realizar o redirecionamento dos pacotes. Exemplo:

```
# Redirecionar os pacotes da porta 80 para porta 3128

iptables -I PREROUTING -t nat -p tcp -s 192.168.1.0/24 --dport 80 -j
REDIRECT --to-port 3128

#Ativar o servico de NAT

iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
```