Implantação Proxy Squid

Cenário

- 2 máquinas virtuais através o VirtualBox:
- Ubuntu 16.10
  - Squid
  - IPTables
  - ISC DHCP
  - 2 placas de rede
    - 1 – rede NAT, pegando IP por DHCP do VirtualBox
    - 2 – rede interna, IP manual
- Windows 7
  - 1 placa de rede, pegando IP pelo DHCP instalado no Ubuntu

Instalação do Squid

- Atualização dos índices dos repositórios:

 # apt-get install update

- Atualização dos pacotes do sistema:

 # apt-get install upgrade

- Instalação do pacote Squid e suas dependências:

 # apt-get install squid

ou

 # apt-get install squid3

Configuração do Squid

- Backup da configuração original do Squid:

 # mv squid.conf squid.conf-original

- Criação de um novo arquivo de configuração para o Squid:

 # gedit squid.conf

Configuração do Squid

- **auth_param basic program /usr/lib/squid/basic_pam_auth**

auth_param - parâmetro de autenticação

basic autenticação básica

program – executável do Squid que trata das autenticações, esse executável vem com squid

/usr/lib/squid3/basic_pam_auth – caminho padrão que contem as contas do Linux

Configuração do Squid

- **auth_param basic children 10**

children 10 – Define quantos processos simultâneos podem ter no servidor. No caso foi parametrizado com 10 conexões simultâneas.

- **auth_param basic realm Autentique-se para acessar a Internet**

realm – Tela de autenticação para o usuário

- **auth_param basic credentialsttl 4 hours**

credentialsttl -Tempo de vida de autenticação enquanto o browser estiver aberta

- **auth_param basic casesensitive off**

casesensitive off – Desligar o case sentitive, aceitar qualquer coisa entre maiúscula e minúscula

Configuração do Squid

- **### Controle de Acesso (ACL) ###**

- **acl all src all**

Define tudo no universo ACL

- **acl localhost src 127.0.0.1/32**

ACL Padrões

Configuração do Squid

- **### Meus Controles de Acesso###**

- **acl usuários proxy_auth REQUIRED**

ACL para autenticação de nome usuários.

REQUIRED - obriga a um usuário digitar uma autenticação

- **acl negados url_regex sexy playboy sexo xxx ultrasurf**

Não quer que passe pelo proxy. Coloca as palavras negadas

- **acl liberados url_regex libsexy computador sexoesaude**

Exceções no proxy

- **acl downloads urlpath_regex \.avi$ \.rmvb$ \.mp3$ \.avi? \.rmvb? \.mp3?**

Capturar nomes de arquivos na URL

Configuração do Squid

- **### HTTP_ACCESS ###**

Controle de acessos com as ACLs que foram criadas. Iremos informar o que deve acontecer com as ACLs e devemos colocar em ordem

- **http_access allow liberados**
- **http_access deny negados**
- **http_access deny downloads**
- **http_access allow usuarios**
- **http_access allow localhost**
- **http_access deny all**

Nega tudo para o todo tipo de ip.

Configuração do Squid

- **### Configurações gerais ###**
- **http_port 3128**

Define a porta de saída

- **cache_mem 256 MB**

Quanto de memória RAM a ser utilizado para oproxy

- **maximum_object_size_in_memory 4 MB**

Tamanho máximo por arquivo de objeto individual na memória RAM.

- **cache_dir ufs /var/spool/squid 3000 16 256**

ufs - tipo de arquivo unix

/var/spool/squid3 – local

3000 16 256 – Tamanho em Megabyte do cache, 16 subdiretórios, e 256 subdiretórios

Configuração do Squid

- **access_log /var/log/squid/access.log squid**

Log de acesso do Proxy

- **cache_mgr email@email.com**

Contado do adm do proxy para caso de probles

- **visible_hostname squid-ubuntu**

Nome da máquina

- **error_directory /usr/share/squid/errors/pt-br**

Páginas com as mensagens de erro do squid

Configuração do Squid

- **#CONFIGURACOES DNS#**

dns_nameservers 8.8.8.8

dns_nameservers 8.8.4.4

Configuração adicionado pois os endereços de DNS devem passar diretamente pelo proxy.

Utilizando o Squid

- Reinicie o serviço com um dos comando abaixo

 # /etc/init.d/squid restart ou **# service squid restart**

- Log do Squid

Local que está o log de acesso:

tail -f /var/log/squid/access.log

Utilizando o Squid

- Criação de um usuário

useradd -s /bin/false -d /dev/null teste

-s /bin/false - não irá logar no Linux, somente testar o Squid

-d /dev/null – Não cria diretório home

- Alterar a senha do usuário criado

passwd teste

Alternativa de Verificação de Logs

- Para verificar o log através de um software de monitoramento, recomenda-se a utilização do aplicativo SARG.

 # apt-get install sarg

- Entrar no arquivo de configuração do SARG

 # gedit /etc/sarg/sarg.conf

Linha 144

output_dir /var/www/squid-reports

ou

output_dir /var/www/sarg

Alternativa de Verificação de Logs

- Em seguida instalar o servidor WEB caso não tenha sido instalado

 # apt-get install apache2

- Digitar sarg para rodar o programa

 # sarg

- Em seguida no browser digitar 127.0.0.1/squid-reports ou sarg

Problema

- Ubuntu com duas placas de redes não navega.
- Problemas com a rota de saída da máquina

- Solução: configurar proxy para ajustar rotas de saída, passando tráfego da segunda placa sempre pelo proxy

- Melhoria: adição do serviço de DHCP para distribuição de endereços de IP aos equipamentos clientes que utilizaram o proxy.

Configurando redirecionamento

- Habilite o redirecionamento

sudo gedit /etc/sysctl.conf

- edite a linha:

net.ipv4.ip_forward=0 para net.ipv4.ip_forward=1

- depois aplique as mudanças:

sysctl -p

Regras de Firewall

- Aplique as configurações de firewall para compartilhar e redirecionar a porta para o Squid:

 # iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

 # iptables -A FORWARD -s 192.168.0.0/24 -o eth0 -j ACCEPT

 # iptables -A FORWARD -d 192.168.0.0/24 -m state --state ESTABLISHED,RELATED -i eth0 -j ACCEPT

- No caso se for usar o Squid em modo transparente, também adicionar a regra:

 # iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to 3128

- Salve as configurações do seu firewall:

 # iptables-save > /etc/firewall.conf

Configurando 2º placa de rede no Ubuntu

- Configure as suas placas de rede:

 # gedit /etc/network/interfaces

auto lo

iface lo inet loopback

- Placa ligada à internet

auto enp0s1 <- nome da placa

iface enp0s1 inet dhcp

- Comando para restaurar as regras de firewall

pre-up iptables-restore /etc/firewall.conf

Configurando 2º placa de rede no Ubuntu

- Rede Interna

auto enp0s8

iface enp0s8 inet static

address 192.168.0.1

netmask 255.255.255.0

- Salve e saia

- Reinicie o serviço para verificar se as configurações estão corretas

#/etc/init.d/networking restart

ou

 # service networking restart

Configurando DHCP

- Instale o servidor de dhcp para configurar automaticamente a sua rede:

 # apt-get install dhcp3-server ou **# apt-get install isc-dhcp-server**

- Configure:

 # gedit /etc/isc-dhcp-server/dhcpd.conf

option domain-name-servers 8.8.8.8, 8.8.4.4;
subnet 192.168.0.0
netmask 255.255.255.0 {
range 192.168.0.10 192.168.0.220;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;}

Configurando DHCP

- Configurar o dhcp para que escute somente na rede interna.

 # gedit /etc/default/dhcp

INTERFACES="enp0s8“

- Salve e saia.

- Reinicie o serviço

#/etc/init.d/isc-dhcp-server restart ou # service ics-dhcp-server restart

Resultado

- Servidor navegando normalmente, fornecendo endereços IP para os clientes e logando as atividades realizadas através do proxy.

- Cliente obtendo IP automaticamente por DHCP e tendo todo seu tráfego direcionado ao proxy, com as devidas restrições de conteúdo.