Roteiro

- Redes de Computadores e Internet
- Arquitetura Cliente/Servidor e Serviços Básicos de Comunicação
- Componentes do Servidor e Configuração da VM
- Sistama Operacional – Instalação e Configuração
- Roteamento no Servidor
- BIND9 – Servidor DNS
- Servidor SQUID
- Servidor DHCP
- Servidor WEB
- SARG

Redes de computadores

Conjunto de computadores interconectados a fim de compartilhar dados e/ou recursos.

Internet

A Internet é uma rede global de computadores, composta por outras redes, com características peculiares, como:

- É baseada no protocolo TCP/IP;
- É ua comunidade de pessoas que usam e desenvolvem essas redes;
- É um coleção de recursos que podem ser alcançados através destas redes.

...Internet

- A Internet não é controlada de forma central por nenhuma pessoa ou organização.
- A organização da Internet é feita pelos próprios participantes e pelos próprios usuários.
- A internet não desliga....

3 Regras para a Internet

- **Provedor de informação -** Disponibiliza informação para os usuários ou clientes.
- **Usuários ou Clientes -** Constituem a segunda regra.
- **Provedor de conexão -** Provê a conexão de rede tanto para provedores de informação quanto para usuários.

Arquitetura Cliente/Servidor

- **Um cliente, responsável por interagir com usuário.**

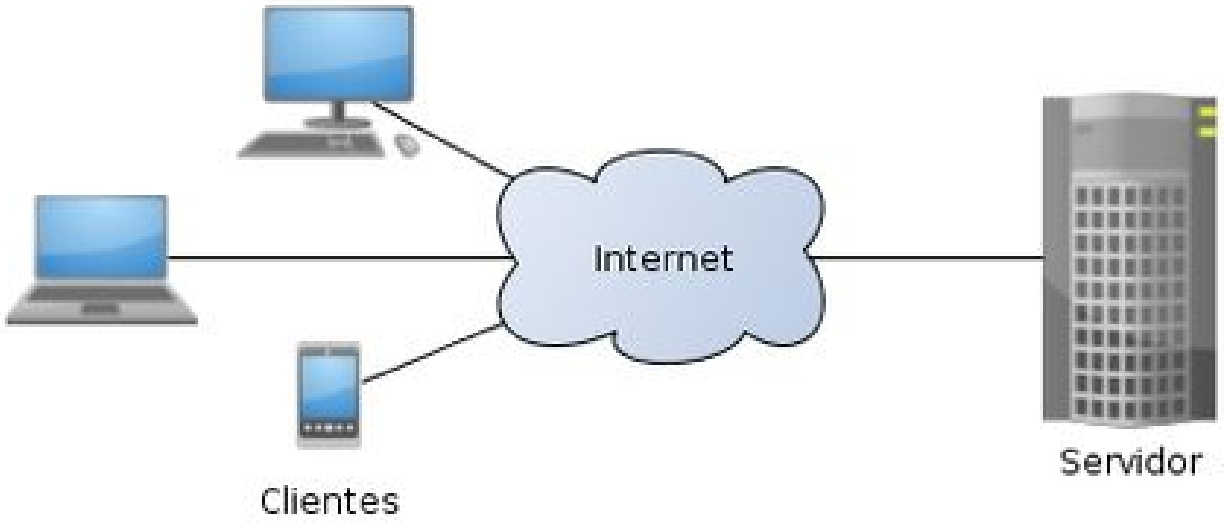
  Exemplo: Navegador de Internet, Cliente de e-mail

- **Um servidor, responsável por executar tarefas conduzidas pelo cliente;**

  - *Exemplo: acessar um dado do lado do cliente, executando cálculos e fornecendo o dado ou uma simples resposta para o cliente.*

Arquitetura Cliente/Servidor

A arquitetura cliente/servidor de serviços de informação Internet é o que torna possível para um computador conectado prover serviços para um outro.



Arquitetura TCP/IP

- Conjunto de protocolos que permite a comunicação entre redes da Internet;
- Recebe o nome dos dois principais protocolos da arquitetura:
  - ***IP (Internet Protocol) e TCP (Transmission Control Protocol)***
- Há um 3º protocolo tão importante quanto, principalmente na internet moderna.
  - ***O UDP (User Datagram Protocol).***

Serviços Básicos de Comunicação

Assíncrona - significa que um usuário pode digitar uma mensagem e enviar sem que haja necessidade do destinatário estar utilizando a rede no momento. ***Ex: Correio Eletrônico, Chat.***

- **Tempo Real ou Interativa -** significa que o usuário pode estabelecer uma conversa, em tempo real, por computador com outro usuário. ***Ex: Video Conferência, VOIP.***

Resumindo a conversa

- A **Internet** trouxe uma gama de benefícios à sociedade, todos estes atrelados a recursos e serviços que estão disponíveis em as várias redes que a compõe.

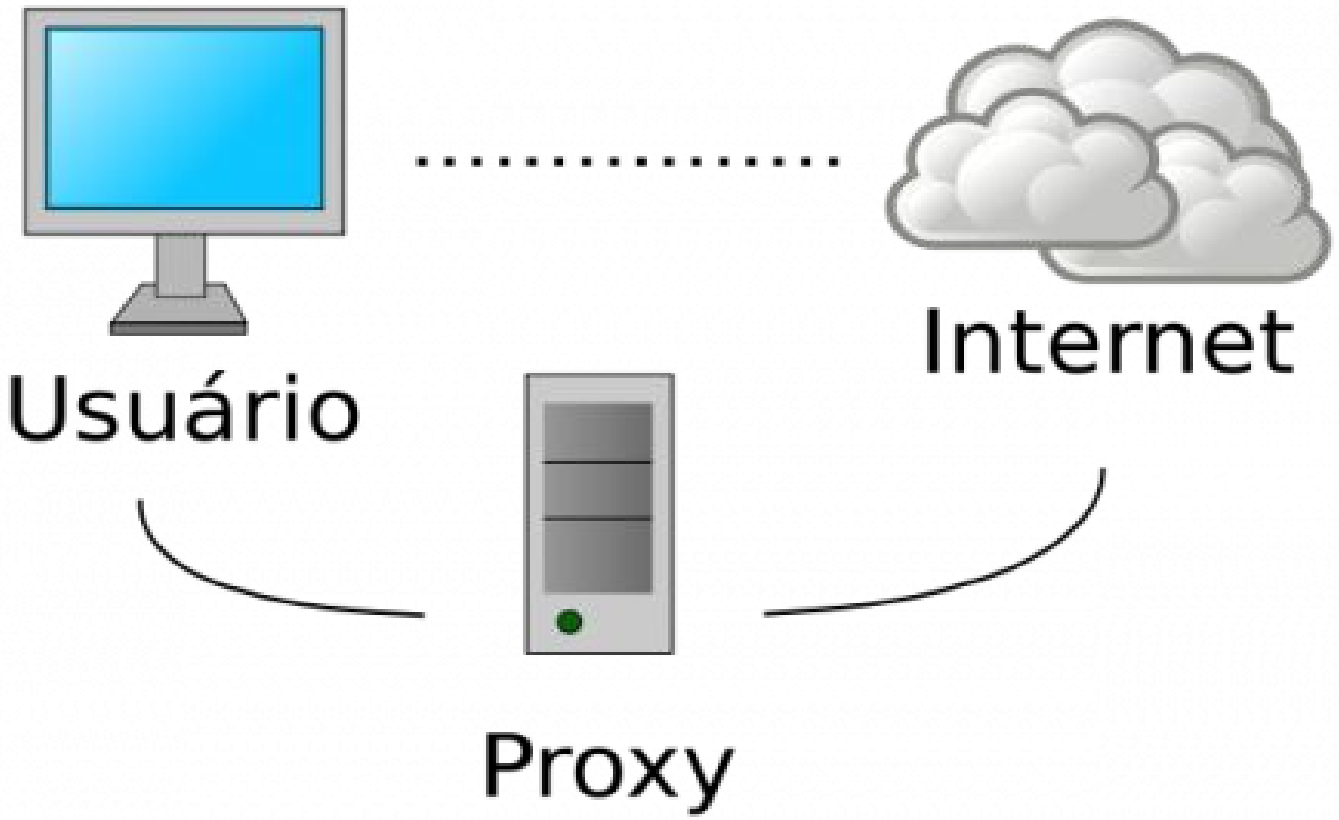
- Administrar esses benefícios de forma eficiente é uma tarefa muito delicada, e atribuida aos **Gestões de TI** e, mais especificamente, aos **NetAdmins**.

Proxy

O Proxy atua como um intermediário entre o usuário e servidores de conteúdo, seja ele local ou remoto.

Através dele, o NetAdmin pode decidir, entre outras coisas, **como**, **quando** e o **quê** cada usuário, ou grupo de usuários podem acessar, bem como estabelecer regras baseadas em **hardwares, protocolos, serviços e contéudo.**

...Proxy



Tipos de Proxy

- **Web Proxy**
- **Proxy Reverso**
- **Proxy Transparente**

Web Proxy

“Também denominado de **Web proxy/cache**, é o tipo mais comum de proxy existente, realiza o **caching** de páginas web e arquivos que estão localizadas nos servidores Web externos, possibilitando que os usuários da rede local tenham um acesso mais rápido e confiável aos conteúdos da Internet por eles requisitados, através do armazenamento em cache dos recursos Web, tais como conteúdos estáticos como figuras e gráficos”

(PONTES; HIRATA; HONÓRIO, 2008)

Proxy Reverso

“O proxy reverso funciona ao contrário do proxy. No modelo convencional de proxy se faz a interceptação das requisições dos clientes que estão localizados na rede local com destino à Internet. Enquanto que no proxy reverso a operação é inversa, interceptando requisições vindas da Internet com destino à rede local. Em suma, ambos são responsáveis por garantir que o cliente não tenha uma conexão direta com o servidor que armazena o conteúdo requisitado, a fim de garantir o anonimato das estações clientes” (SABOCINSKI NETO, 2009).

Proxy Transparente

Este é um tipo de proxy onde o cliente está isento de qualquer configuração adiconal em função do servidor. Em suma, basta que o cliente tenho o servidor como seu **Gateway Padrão,** fazendo uma combinação entre o NAT e o Proxy, de fato.

Servidor Proxy SQUID

O Squid é um software desenvolvido por voluntários e oferecido a todos sob a GNU General Public License (GPL), que encoraja o compartilhamento e reutilização **software livre**.

“Não cobramos de qualquer maneira pelo nosso software, e qualquer um pode baixar, usar e modificar Squid.”

Squid Software Foundation

Benefícios do Servidor Proxy SQUID

- **Autenticação;**
- **Registro de acessos;**
- **Controle centralizado;**
- **Segurança.**

Autenticação

É possível restringir o acesso ao servidor proxy com o uso da autenticação de usuários, de forma que seja melhorada a segurança, já que somente usuários autorizados poderão acessar a Internet.

Este recurso é bastante flexível e pode ser implementado de várias maneiras, como uso do protocolo LDAP, SMB, módulos PAM, etc.

Registro de acessos;

Os acessos são registrados em arquivos de log, podendo esses serem utilizados para as mais diversas finalidades, que vão desde a análise de performance do servidor, até a geração de relatórios detalhados dos acessos à Internet.

Existem vários softwares analisadores de logs do Squid capazes de gerar relatórios tão bons, que por si já justificariam o uso do Squid, em razão do controle proporcionado;

Controle centralizado

Com o uso do proxy temos a facilidade de um único ponto centralizador do acesso à Internet, o que torna a gerência da rede mais fácil e eficiente.

Uma única máquina é capaz de prover acesso a várias outras.

Segurança

Como apenas o proxy está diretamente ligado à Internet, temos apenas uma (ou mesmo poucas, caso tenhamos mais de um servidor proxy) máquina potencialmente vulnerável. Desta forma fica mais fácil concentrar esforços na melhoria da segurança de apenas um ponto na rede.

O Servidor (Componentes)

- **Oracle VM Virtual Box –** Virtualizador de Sistemas Operacionais.
- **DHCP Server** – Atribui endereços dinâmicos para os hosts da rede.
- **SQUID –** O Servidor Proxy.
- **Apache + SARG –** Servidor WEB e Gerador de relatórios do SQUID
- **IPTABLES** – Firewall (Netfilter)

Sistema Operacional

Gnu/Linux Debian7 ou superior – S. O. de grande utilização em todos os servidores do mundo.

- Fácil de interagir;
- Fácil gerenciamento de pacotes (APT);
- A maior comunidade de Software Livre do Mundo.
- Derivados: UBUNTU, MINT, entre outros.

Configuração da VM

- **Disco Rigido:** 20 Gb - Recomendado
- **Memória RAM:** 512 MB - Recomendado
- **CPU:** 1 núcleo – é o suficiente
- **Placa de Rede:** Em modo Bridge

Prática

Configuração da rede

- **Ative as placas de rede**
  - # ifconfig eth**”0”** up
- **Dentro do interfaces, configure as placas**
  - # nano /etc/network/interfaces
  -
- **Reinicie as placas de rede**
  - # /etc/network/networking restart

Arquivo /etc/network/interfaces

auto **eth0**

iface **eth0** inet dhcp

address 10.0.0.1

netmask 255.255.255.0

network 10.0.0.0

broadcast 10.0.0.255

gateway 10.0.0.254

Ativando o roteamento no servidor

O Arquivo ip_forward é responsável pela ativação do roteamento no servidor. A ativação é feita através de inserção dos valores **1 para ativar** e **0 para desativar**

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Instalação do BIND9 (opcional)

- O **BIND9** é o serviço de DNS do servidor. Ao instalar o **BIND9** o servidor DNS já funcionará como **DNS Cacher** automáticamente.

- O **BIND9** proverá para os clientes da rede um cache de DNS, ou seja, consultas já realizada ficarão em cache. No entanto, este servidor não será capaz de resolver nenhuma requisição, sendo essas encaminhadas a um DNS resolver.

Configure o /etc/resolv.conf

- **Configurando o resolv.conf para usar o DNS local, escrevendo dentro de /etc/resolv.conf:**

  - #nano /etc/resolv.conf
  - nameserver 127.0.0.0 –-> direciona as requisições para o **loopback**

Servidor DHCP

- O servidor **DHCP** será responsável por fornecer endereços dinâmicos aos host da rede. Desta forma, nenhuma máquina precisa ser configurada manualmente na rede. Instale-o com o comando:
  - #apt-get install isc-dhcp-server
  - Obs: As configurações do ISC-DHCP-SERVER são feitas no arquivo /etc/dhcp3/dhcpd.conf .

/etc/dhcp3/dhcpd.conf

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.0.0.0;
option broadcast-address 10.255.255.255;
option routers 10.0.0.10;
option domain-name-servers 10.0.0.10;
subnet 10.0.0.0 netmask 255.0.0.0 {
range 10.0.1.1 10.0.1.100;
}
```

Reinicie o DHCP

#service isc-dhcp-server restart

SQUID no Debian 7 ou +

- **Instalação do SQUID via APT**
  - #apt-get install squid

- **O SQUID tem suas configuração realizadas no arquivo /etc/squid/squid.conf.**

Obs: Faça o backup do squid.conf para posteriores consultas

  - #cd /etc/squid/
  - #mv squid.conf squid.conf.bkp

squid.conf

Acesse o endereço abaixo e baixe os arquivos de configuração:

http://roitier.pro.br/tutoriais/

Apache 2

O **Apache** é o servidor WEB mais utilizado entre os servidores do mundo. No nosso servidor ele será responsável por permitir que tenhamos acesso ao relatório gerado pelo **SARG**, visto que este será web.

Instale o apache, versão 2

- #apt-get install apache2

Por padrão, o apache2, logo após a instalação, já está pronto para uso.

SARG - Squid Analysis Report Generator

O **SARG** é o gerador de relatórios do **SQUID**. Sem ele, o **SQUID** seria um tiro no escuro, onde todas as decisões tomadas a partir do uso passariam as ser apenas **intuitivas**. Ele nos permitirá conhecer:

Quem? O quê? e Quando acessou?

Configurando o SARG

- **Entre no sarg.conf:**
  - # nano /etc/sarg/sarg.conf
- **Edite a linha output_dir, da forma que fique assim:**
  - output_dir /var/www/squid-reports

...SARG

- Dentro do mesmo arquivo, procure a linha que esteja escrito "RELATORIO DE ACESSO" e personalize. No meu caso: "Relatorio de acesso [nome da empresa]".
-

Configurando a página de erro

- Crie o arquivo que será lido quando o squid negar acesso a um usuário:
  - #mkdir /usr/share/squid/errors/portuguese
  - #nano /usr/share/squid/errors/portuguese

```
<html><head><body></br>

</br>

<b><center><font size=7 color=red>A Pagina que voce esta tentando acessar esta bloqueada!!!</font>

<div align=center><img src=http://10.0.0.10/bloqueio.jpg></div>

</head></body></html>
```

IPtables

- O **IPTABLES** é Filtro de Pacotes, Firewall, baseado no módulo **NETFILTER** presente no kernel do linux.
- No Servidor proxy o **IPTABLES** tem o papel de redirecionar todos pacotes que chegam na porta **80 (http)** para a porta **3128 (squid)**. Essa prática faz com que o proxy se torne transparente aos clientes.

Configurando o IPTABLES

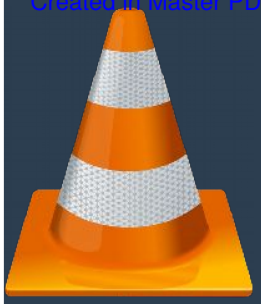
- **Inserindo o NAT GLOBAL:**
  - # iptables -t nat -A POSTROUTING -o eth(internet) -p tcp -j MASQUERADE

- **Redirecionando o conteúdo que PREROUTING da porta 80 para a porta 3128:**
  - # iptables -t nat -A PREROUTING -s (seu net id/mascara) -p tcp --dport 80 -j REDIRECT --to-port 3128
  -

- Não há problemas em utilizar regras complementares no IPTABLES, mesmo utilizando o SQUID como Proxy da rede. Exemplo:
  - # iptables -A POSTROUTING -s (sua rede / mascara) -m string --algo bm --string "facebook.com" -J DROP

Conclusão

- O Gnu/Linux Debian é uma excelente opção de Sistema Operacional para o seu servidor;
- SQUID+SARG+IPTABLES+VirtuaBOX são uma ótima combinação para o seu servidor, doméstico ou corporativo;
- Softwares Livres são a expressão da excelência a partir da colaboração. Use, Modifique, Compartilhe!



Roitier Campos Gonçalves

 **@roitier**

 **/roitier**

http://roitier.pro.br

roitier1@hotmail.com