

Universidade Federal do Rio de Janeiro

**Instituto Tércio Pacitti de Aplicações e
Pesquisas Computacionais**

Bruno Rohr da Silva

**LINUX: CONFIGURAÇÃO E
ADMINISTRAÇÃO**

Rio de Janeiro

2013

Bruno Rohr da Silva

LINUX: CONFIGURAÇÃO E ADMINISTRAÇÃO

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Paula Cyrillo Gomes, M.Sc., UPM, Espanha

Rio de Janeiro

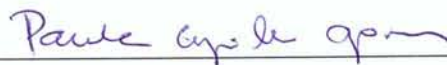
2013

Bruno Rohr da Silva

LINUX: CONFIGURAÇÃO E ADMINISTRAÇÃO

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2013.



Paula Cyrillo Gomes, M.Sc., UPM, Espanha

Dedico esta monografia aos meus pais e a minha esposa, Marcia Garibaldi Rosa, que sempre me deram muito apoio para estar dando mais este passo na vida.

AGRADECIMENTOS

Aos meus pais e irmãos, a minha esposa Marcia Garibaldi Rosa e a toda minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa da vida.

A orientadora Paula Cyrillo Gomes pela dedicação prestada na orientação deste trabalho.

Agradeço também a todos os professores que me acompanharam durante a pós-graduação, responsáveis pela realização deste trabalho, em especial o Professor Moacyr Henrique Cruz de Azevedo.

A todos meus amigos que colaboraram direta ou indiretamente para a realização deste trabalho, em especial a Gilberto Santos e Igor Jardim de Oliveira Pereira.

RESUMO

SILVA, Bruno Rohr. **LINUX: CONFIGURAÇÃO E ADMINISTRAÇÃO**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

O objetivo central deste trabalho é apresentar as principais serviços administrativos em ambiente Linux. Inicialmente, serão apresentados alguns conceitos básicos do sistema operacional. Tais como instalação e configuração do sistema, assim como, serviços de segurança e sua configuração.

ABSTRACT

SILVA, Bruno Rohr. **LINUX: CONFIGURAÇÃO E ADMINISTRAÇÃO**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

The aim of this essay is to do present the main applications and administrative tools on Linux environment. Initially we introduce some basic concepts of operating system. Such as installation and configuration, as well as security services and their configuration.

LISTA DE FIGURAS

	Página
Figura 1 – Arquivo de Configuração do LILO	16
Figura 2 – Arquivo de Configuração da rede	20
Figura 3 – Reserva de IP	25
Figura 4 – Chave Openvpn	28
Figura 5 – Arquivo de Configuração do Servidor	28
Figura 6 – Firewall	30
Figura 7 – Proxy	32
Figura 8 – Um único Domínio	33
Figura 9 – Domínio com NAT	33
Figura 10 – NAT Saída	34
Figura 11 – NAT Entrada	35

LISTA DE TABELAS

Tabela 1 – Iptables	Página
Tabela 2 – Networking	36
	38

LISTA DE ABREVIATURAS E SIGLAS

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GNUPG	GNU Privacy Guard
GPL	General Public License
GRUB	Grand Unified Bootloader
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IRQ	Interrupt Request Line
ISO	International Organization for Standardization
LILO	Linux Loader
LTS	Long Term Support
LVM	Logical Volume Manager
MAC	Media Access Control
MBR	Master Boot Recorder
NAT	Network Address Translation
NFS	Network File System
PKI	Public Key Infrastructure
RAM	Random-Access Memory
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WWW	World Wide Web

SUMÁRIO

	Página
1 INTRODUÇÃO	12
2 O SISTEMA OPERACIONAL	13
3 INSTALAÇÃO	14
3.1 ADMINISTRADORES DE BOOT E O KERNEL	14
3.1.1 GRUB	15
3.1.2 LILO	16
3.2 PARTICIONAMENTO DO DISCO	17
3.3 OS PACOTES E SERVIÇOS DURANTE A INSTALAÇÃO	18
3.4 CONFIGURAÇÕES DE REDE	19
4 APLICAÇÕES E SERVIÇOS	22
4.1 SERVIDORES DHCP	24
4.2 VPN	26
5 SEGURANÇA	30
5.1 FIREWALLS NAT E PROXY	30
5.2. IDS – SISTEMA DE DETECTAÇÃO DE INTRUSÃO	37
5.2.1 Tipos de intrusões	39
5.2.2 Exemplos de IDS	40
6 CONCLUSÕES	45
REFERÊNCIAS	46

1 INTRODUÇÃO

O Linux teve sua história iniciada em 1991, o seu idealizador foi Linus Torvalds, na Universidade de Helsinque na Finlândia. O seu principal objetivo até então era a criação de um terminal de acesso ao sistema UNIX a partir de qualquer computador independente do sistema operacional utilizado. Um sistema operacional de código aberto que poderia ser distribuído gratuitamente na internet ou em qualquer outro meio, sendo, desta forma, de fácil acesso a qualquer um.

Linus Trovalds deu início ao seu projeto tendo como referência o trabalho de Andrew Tannenbaum com o Minix, este um sistema operacional que tinha como principal alvo o setor acadêmico.

Uma das grandes vantagens do sistema Linux é a utilização do sistema de licença GPL (*General Public License*), designado para *softwares* livres.

As distribuições Linux estão cada vez mais fáceis de utilizar, seja por interface gráfica ou terminal de texto. Houve uma grande evolução no sistema em sua interface gráfica, um sistema de janelas X window.

Deste modo, o objetivo deste trabalho é contribuir para melhor desempenho do servidor com um sistema operacional Linux. Possibilitando, assim, uma configuração mais eficiente.

2 O SISTEMA OPERACIONAL

O Linux tem uma característica distinta de outros sistemas operacionais como Windows, por exemplo, que o torna, em parte, bem adaptativo as suas necessidades assim como complexo no que se diz respeito à quantidade de distribuições disponíveis. Estas podem ser desenvolvidas de forma corporativa, como é o caso do Red Hat, Mandriva e Suse ou, colaborativa, como é o caso do Debian, Ubuntu e Slackware.

As diferenças podem estar desde a interface gráfica e uso do terminal. Entretanto o uso do terminal nas distribuições pode levar a uma melhor compreensão do sistema e amenizar as diferenças para o administrador.

No decorrer do trabalho vou dar preferência à distribuição do Ubuntu 12.04 LTS (*Long Term Support*) cuja ISO (*International Organization for Standardization*) pode ser baixada gratuitamente a partir da página da Canonical. Na verdade, existem duas versões: uma com interface gráfica e a LTS. A LTS é planejada para ser atualizada e suportada durante um período mais longo, sendo esta recomendada para servidores em função do tempo maior de suporte, suporte este no qual estão incluídas atualizações críticas e de segurança do sistema por cinco anos, fato fundamental para um servidor. Mesmo utilizando a LTS nada impede que a interface gráfica seja instalada segundo a necessidade.

3 INSTALAÇÃO

A instalação do sistema estruturada de forma a atender seu propósito de servidor e a avaliação dos pacotes, a serem instalados é fundamental e, muitas vezes, determinam a partir do serviço que será utilizado no servidor, mas em geral existem algumas configurações que podem ter características comuns.

A instalação do Linux é passível de ser realizada a partir de diversos tipos de repositórios, sendo eles de um disco rígido, cd, servidores FTP (*File Transfer Protocol*), pendrive, HTTP (páginas web), Samba e NFS (*Network File System*).

Alguns servidores podem apresentar incompatibilidade no processo de instalação, a exemplo do hardware. Com intuito de resolver esse problema alguns comando podem ser utilizados, como “acpi-off”, “irqpoll”, “noapic”.

Como exemplo do uso destes comandos, poderíamos acrescentar a instrução “*linux acpi=off noapic*” no boot do sistema. Com esta instrução poderíamos desabilitar os módulos de controle térmico e conflitos de IRQ (Interrupt Request Line), muito comuns, principalmente, em computadores antigos.

3.1 ADMINISTRADORES DE BOOT E O KERNEL

Os administradores de boot são responsáveis por gerenciar a MBR (*Master Boot Recorder*). Seu código reside no primeiro setor do disco. Para entendermos a MBR, quando o computador é ligado, ele inicia sua rotina de detecção de hardware e, ao final, será carregado o primeiro setor de boot para a memória. Estes setores são chamados de MBR.

Quando instalamos vários sistemas operacionais em um computador e em caso de o último ser o Linux, este então será responsável por gerenciar a MBR, ou seja, os 512 bytes iniciais do disco rígido.

Os dois principais administradores de boot são o LILO (*Linux Loader*) e o GRUB (*Grand Unified Bootloader*), os dois permitem a escolha dos sistemas operacionais instalados em um computador, podendo ser tanto versões do Linux como outros sistemas operacionais como o Windows.

3.1.1 GRUB

O Linux, mesmo que seja o único sistema instalado no computador, instalará um gerenciador de inicialização, com uma configuração muito amigável, permitindo carregar vários sistemas operacionais.

A possibilidade de edição dos arquivos de configuração é um fator crucial, como o sistema principal que será iniciado automaticamente no boot.

Para o GRUB, às partições primárias são atribuídos os números 0 (zero) a 3 (três), e às partições lógicas, números a partir de 4 (quatro).

O arquivo de configuração do GRUB está localizado no “/boot/grub/grub.cfg”. Em versões diferentes de GRUB pode ser apresentada com diferenças na configuração.

É sempre muito importante manter uma cópia do GRUB em discos de backup, já que não é impossível a perda das informações da MBR.

3.1.2 LILO

O LILO já foi um dos principais gerenciadores de boot utilizado no Linux, e suas configurações podem ser encontradas no arquivo “/boot/boot.b” e no “/etc/lilo.conf”. Podem-se alterar configurações como vídeo, memória, mensagens de inicialização e versão do kernel (Figura 1).

```
boot=/dev/das
append='mem=1024M'
compact
install=/boot/boot.b
map=/boot/map
message=/etc/message.txt
default=LINUX
vga=normal
delay=20
lba32
prompt
image=/vmlinuz
        root=/dev/sda2
        label=LINUX v12.04
        read-only
```

Figura 1: Arquivo de configuração do LILO

3.2 PARTICIONAMENTO DO DISCO

O particionamento conta com alguns recursos como o LVM (*Logical Volume Manager*), que é baseada no uso de volumes, que permite o dimensionamento da partição segundo uma necessidade de estender a unidade lógica já criada ou o acréscimo de disco físico a uma partição lógica.

A utilização de um disco dividido em partições pode ser uma boa prática, principalmente para os diretórios “/boot”, “/home”, “/var” e “/tmp”.

As principais razões para se utilizar partições separadas para estes diretórios são:

/boot: contém o initrd e a imagem do kernel. Para este, então, será criada uma partição de 150 MB, espaço suficiente para os arquivos de configuração do GRUB.

/home: este diretório é responsável por armazenar os arquivos dos usuários e serve para evitar que o usuário crie arquivos de forma a alcançar o limite do disco “/”.

/var: o diretório é normalmente o local de armazenamento para instalações dos programas como banco de dados, logs, spool, entre outros; permite um backup mais fácil.

/tmp: é muito importante manter separada da raiz do sistema, já que muitos arquivos são criados, pelo sistema, é fundamental a criação de uma rotina de limpeza.

O volume Swap é uma extensão da memória RAM (*Random-Access Memory*), muito importante em computadores cujo a memória física é muito pequena. Em um computador com 8 GB de RAM, será usado 4 GB de Swap.

Entretanto, é bom salientar que quando o sistema chega a utilizar a Swap é necessário aumentar a memória física.

Quanto à formatação, estrutura pela qual o sistema operacional prepara o disco para gravação e leitura das informações a ser utilizada. No Linux seriam: ext4 melhor do que a ext3 e a ext2, já que tem vantagens como menor fragmentação do disco e maior desempenho. Não Além disso, utiliza um sistema *atribuir-on-flush*, apresentando, assim, melhor confiabilidade, suporte a arquivos com mais de 2 GB, tratamento a arquivos de até 16 TB, além de possuir *timestamps* (controladores de tempo) mais eficientes.

3.3 OS PACOTES E SERVIÇOS DURANTE A INSTALAÇÃO

Durante a instalação, também podem ser selecionados alguns pacotes que serão usados no servidor. Como exemplo destes pacotes, temos:

- Interface de Área de trabalho
- Servidor Web
- Servidor de Impressão
- Servidor DNS (Domain Name System)
- Servidor de Arquivos
- Servidor de Mensagens
- Base de Dados SQL
- Sistema Básico

A escolha dos aplicativos e pacotes pode facilmente ser reconfigurada após o processo de instalação com o uso do APT (aplicativo de gerenciamento de pacotes do Linux).

Contudo, é fundamental a instalação do `openssh-server`. Este permite conexão através de um terminal de acesso remoto via porta 22 pelo Secure Shell. Além disso, tem grande vantagem de tratar todo o tráfego criptografado e de seu cliente poder ser utilizado em vários outros sistemas operacionais, como Windows e IOS.

Sintaxe do comando para acesso ao servidor a partir do cliente:

```
$ssh <usuário>@<ip do servidor>
```

3.4 CONFIGURAÇÕES DE REDE

Por padrão, o sistema operacional irá tentar fazer a configuração da pilha TCP/IP do cliente por DHCP (*Dynamic Host Configuration Protocol*). Entretanto, para um servidor é recomendado que este IP (*Internet Protocol*) seja fixo, mesmo que o serviço de DHCP rode na rede.

No Linux, a rede pode ser configurada nos arquivos “`/etc/network/interfaces`” (Figura 2). Nesse arquivo pode ser configurado IP, máscara, broadcast e gateway da interface de rede, assim como, interface de loopback.

```
auto lo

iface lo inet loopback

if

# The primary network interface

auto eth0

iface eth0 inet static

address 146.164.31.141

netmask 255.255.255.128

network 146.164.31.128

broadcast 146.164.31.255

gateway 146.164.31.129
```

Figura 2: Arquivo de configuração da rede

O DNS deve ser configurado no arquivo “/etc/resolv.conf”.

Após as configurações, será necessário rodar o seguinte comando para que as alterações sejam aplicadas.

```
#/etc/init.d/network restart
```

Após a configuração da rede para internet, é fundamental manter o sistema atualizado para sua segurança. É importante a utilização das últimas versões de aplicativos, assim como a correção de problemas que foram localizados em versões anteriores ou na própria versão só que revisada. No caso do Ubuntu o processo pode ser feito com instruções no terminal de comando.

`#apt-get update` (atualiza a lista de aplicativos utilizados para atualização do sistema)

`#apt-get upgrade` (para atualizar os aplicativos instalados)

O update pode ser facilmente acrescentado como rotina ao crontab (serviço Unix que permite que tarefas sejam executadas em intervalos regulares), sendo feito automaticamente diariamente ou semanalmente, segundo a necessidade de cada servidor.

4 APLICAÇÕES E SERVIÇOS

O APT, atualmente, vem instalado por padrão em todas as versões Ubuntu disponíveis, permitindo uma série de ações, como atualização dos pacotes instalados, novas instalações e remoção.

O APT é uma ferramenta muito importante e também muito simples, trabalhando a partir de repositórios e possuindo, assim, sempre acesso às versões mais novas das aplicações.

O arquivo de referência com o endereço dos repositórios usado pelo APT é o “/etc/apt/sources.list”, Este contém todas as fontes de repositórios, onde poderá ser adicionado uma nova fonte, manualmente, caso necessário.

Instalações do aptitude (gerenciador de aplicativos do Linux) são seguras, já que o sistema conta com criptografia de chaves GNUPG (*GNU Privacy Guard*). Funciona em um sistema de chave assimétrica no qual é criada uma chave pública que é distribuída abertamente e uma chave privada que é utilizada para assinar os arquivos. Esta última deve ser mantida em sigilo absoluto.

O cache do APT está dentro do diretório “/var”, e dois arquivos fundamentais para seu funcionamento estão dentro do diretório “/var/cache/apt”. São eles pkgcache.bin e srcpkgcache.bin, sem os quais o APT não funcionará.

Para manipulação do APT serão utilizados os comandos o apt-cache e o apt-get.

O apt-cache tem a seguinte sintaxe:

```
#apt-cache [opções] comando [arquivo]
```

Para limpeza do cache:

```
#apt-get clean ou  
#apt-get autoclean
```

Para busca de um pacote que apresente uma palavra de descrição do programa a ser procurado:

```
#apt-cache search ssh
```

Para verificar arquivos corrompidos:

```
#apt-cache gencaches
```

Para mostrar os pacotes instalados:

```
#apt-cache dump
```

Para atualização dos repositórios e instalação dos pacotes existem parâmetros muito utilizados, que são:

- `update`: para atualização da lista dos repositórios;
- `upgrade`: para atualização dos pacotes instalados;
- `install`: para instalação de novos pacotes;
- `check`: para verificação de dependências quebradas;

- `clean` e `autoclean`: para limpeza onde são apagados arquivos antigos;
- `dselect-upgrade`: para seleções `dselect`;
- `dist-upgrade`: para atualização da distribuição (sistema)
- `remove`: para desinstalar aplicativos
- `source`: para baixar arquivos fonte.

4.1 SERVIDORES DHCP

O servidor DHCP é fundamental para gerenciar endereços de IP na rede, tornando o gerenciamento e, permitir a configuração automática do TCP/IP de cada estação muito mais simples.

Em grades redes, é comum que os administradores automatize as tarefas, uma delas é a distribuição automática de IPs usando o DHCP. Tentar executar esta função manualmente iria, com certeza, ocupar um longo tempo, além de aumentar a probabilidade de erros na configuração de cada host. O DHCP evita erros de configuração causados pela necessidade de digitação manual de valores em cada computador. Além disso, o DHCP tenta impedir conflitos de endereço causados por um endereço IP atribuído anteriormente e que está sendo utilizado novamente para configurar um novo computador na rede. Entretanto não impede conflitos com IPs fixados manualmente.

O serviço trabalha usando DORA (Descoberta, oferta, requerimento e reconhecimento), utilizando a porta 67 UDP (*User Datagram Protocol*) nos servidores, e 68 UDP nos clientes DHCP.

Em um servidor deve ser criado um escopo de um grupo de endereços de IP que serão configurados, onde será designada a distribuição de IPs, máscaras, gateway, DNS, como exemplo, entre os clientes, podendo ainda ser vinculado ao endereço específico de cada placa de rede MAC (*Media Access Control*).

A instalação de um servidor DHCP é simples. No Linux, o aplicativo mais usado para executar este serviço é o ISC DHCP (Serviço Linux de DHCP) e o pacote a ser instalado é o “dhcp3-server”. Para instalação basta executar o seguinte comando:

```
#apt-get install dhcp3-server
```

Com o serviço instalado ele pode ser iniciado com o seguinte comando.

```
#/etc/init.d/dhcp3-server start
```

Para configuração de reserva de IP no servidor DHCP, ou seja, vincular IP a um determinado cliente, basta acrescentar a seguinte linha no final do arquivo “dhcpd.conf”, (Figura 3), assim cada equipamento da rede, configurado, o IP será sempre o mesmo.

```
host nome {  
    hardware ethernet FF:FF:FF:FF:FF:FF;  
    fixed-address 146.164.31.141;  
}
```

Figura 3: Reserva de IP

4.2 VPN

A VPN (*Virtual Private Network*) é uma rede virtual, criada com a finalidade de interligar duas redes ou hosts distantes através da internet. A principal vantagem de criar uma VPN é a possibilidade de compartilhar recursos de forma segura entre as redes. Como exemplo destes recursos, teríamos o compartilhamento de arquivos e de equipamentos, como impressora e scanner.

As redes VPNs ainda contam com uma criptografia, que pode ser estática ou randômica. As VPNs de criptografia randômica e baseada em certificados X509, este sistema é chamado de PKI (*Public Key Infrastructure*), permitindo, assim, a configuração entre vários clientes e servidores.

As VPNs de criptografia estática são muito mais simples de se configurar. O arquivo de criptografia é em texto em claro e pode ser encontrado dentro do diretório “/etc/openvpn”. Uma outra questão no uso da criptografia estática está vinculado ao uso de apenas um cliente e um servidor por conexão, ou seja, ponto a ponto.

A instalação da VPN no Linux pode ser feita a partir do APT, e a aplicação mais usada é o openvpn. O comando para instalação do serviço é o seguinte:

```
#apt-get install openvpn
```

Após a instalação é necessário executar o módulo “tun” (túnel em modo layer 3) do kernel que é fundamental. O serviço openssh de tunelamento necessitará de interfaces virtuais para seu funcionamento. O comando para criação destas interfaces virtuais será o seguinte:

```
#modprobe tun
```

Além deste procedimento será necessário acrescentar a seguinte linha no final do arquivo de modules:

```
#echo tun >> /etc/modules (para que o modulo passe a ser carregado automaticamente na inicialização)
```

Configurando o servidor VPN:

```
#openvpn --remote 146.164.31.141 --dev tun0 --ifconfig  
192.168.1.2 192.168.1.1
```

Configurando o cliente VPN:

```
#openvpn --remote 186.25.46.15 --dev tun0 --ifconfig  
192.168.1.1 192.168.1.2
```

Criação da chave privada de 2048 bits no servidor:

```
#cd /etc/openvpn  
#openvpn --genkey --secret chave.key
```

Exemplo de um arquivo de chave gerado pelo openvpn pode ser observado na figura 4.

```

root@linux:/etc/openvpn# more chave.key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
19ab418243e3e84bcd219bf16b99e511
33b732b3ea878a81cd47e4840b4dc7dc
ef5f85dbf6af636c1f60208b2d04fbd7
abb044a577f65c8f21d753c8fb09c9b4
d1c2aa134dc38c23f896989731d04c35
4311c09866100a821a3f4461055de815
edec662a11c49a009fcab8866f59463b
7c227ef79dc6813250d31ea2def7150b
435643bb9c5d18b96ba6f3cc558f64a9
ca54e9a9fa3b4e325329bde1361c8cfc
2e736a6ec41f59be76b82a511f2e6a3e
e2126de12fa9c65c34a34804ceeaeaf
8d0b6342e9bb28a5c81c1733789db1bc
724f60d4af1a58a479d5759f998bd3c4
380d5d33c17a1c81f9d3bdcf246716a7
bba66e0f5357bba99303773e681df1e2
-----END OpenVPN Static key V1-----
root@linux:/etc/openvpn#

```

Figura 4: Chave Openvpn

O arquivo gerado no servidor, também deverá ser copiado para o diretório “/etc/openvpn” no cliente, já que os dois deverão compartilhar a mesma chave. E para iniciar a VPN, deverá ser criado um arquivo de configuração em “/etc/openvpn/” no servidor, e no cliente (Figura 5), com a extensão “. conf.

```

dev tun

ifconfig 192.168.1.1 192.168.1.2

secret chave.key

    remote 146.164.31.141

dev tun

ifconfig 192.168.1.2 192.168.1.1

secret chave.key

```

Figura 5: arquivo de configuração do Servidor

O serviço de VPN é muito útil quando temos que configurar redes remotas que necessitam utilizar os mesmos recursos, com algum grau de segurança. Podendo ser configurado inclusive em redes com IPs dinâmicos.

5 SEGURANÇA

5.1 A UTILIZAÇÃO DE FIREWALL, NAT, FILTROS E PROXY NA REDE.

O sistema Linux é complexo, e por isso o acesso ao seu sistema pode facilitar ataques provenientes da internet ou intranet, o que é fatal para os serviços utilizados e compromete as informações.

O firewall tem a função de restringir o acesso, ou determinar os tipos de acessos permitidos. Figura 6.

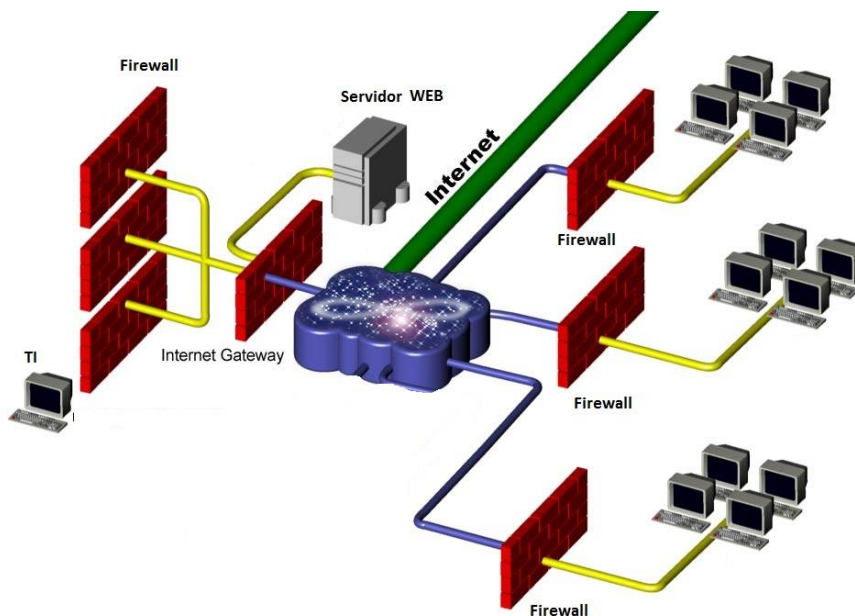


Figura 6: Firewall

Um firewall é uma tarefa importante de um planejamento de rede. A proteção do sistema pode ser ainda aprofundada com o uso do NAT. (*Network Address Translation*), funcionando como uma proteção a mais para ataques provenientes da

internet, como scanners. No Linux, o firewall está compilado no kernel, com o uso de iptables.

As zonas de firewall estão divididas em domínios baseada em um host único. Controla-se um host único com firewall, utilizando-se de filtragem de pacotes. Para esta função utiliza-se o Netfilter com base no serviço de aplicações de software e com análise de TCP (*Transmission Control Protocol*) Wrappers (utilizados para aplicar regras de acesso aos servidores).

Sendo um firewall de domínio com o papel de roteador pode-se usar na filtragem de pacotes o Netfilter junto com um servidor proxy para acessar a internet.

O Netfilter é um mecanismo de filtragem de pacotes, usando um sistema de análise de pacotes. Desta forma, pode-se analisar diretamente o pacote incluindo os endereços de hardware, software e protocolos como: MAC, IP, TCP, UDP e ICMP (*Internet Control Message Protocol*). Além destes, podem estar incluídos outros parâmetros nesta análise. Realmente, uma análise principal dos protocolos das camadas OSI 2,3 e 4. Acima destas camadas um Linux com Netfilter rodando, permite ao software iptables instruções de filtragem de pacotes muito eficientes.

O TCP Wrappers é um pacote que trabalha através de um daemon (TCPD) com uma análise do pacote instantânea capaz de entender a eminência de um possível ataque. Por exemplo, sabemos que o FTP pode operar na porta não padrão 21 para ser escutada pelo Linux embutido em um pacote TCP, onde este pacote poderá estar sujeito a restrições independente do cabeçalho FTP.

A utilização de um Proxy também pode ter muita importância como serviço de uma rede para que os administradores possam registrar informações relevantes da rede.

No exemplo da figura 7, enquanto do lado do cliente que pode ser observado fazendo um acesso para internet assim como obter dados de um provedor, o proxy controla o fluxo de dados.

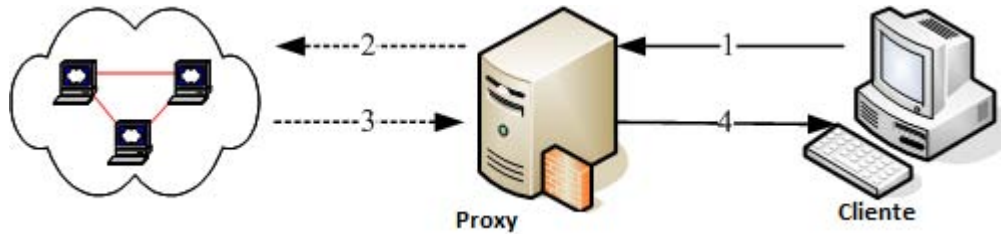


Figura 7: Proxy

1. O cliente irá requerer os dados do servidor proxy;
2. O proxy poderá analisar se o IP de origem do usuário é legítimo, se o usuário tem permissão para ir ao provedor em questão.
3. Os dados são passados para o proxy;
4. Os dados do provedor são passados para o cliente.

Em um domínio com apenas um roteador pode-se usar um Linux nativo, podendo ser configurado como roteador. Para ser eficiente, serão necessárias duas interfaces para separar o domínio interno da internet, confiável para não confiável.

Figura 8.

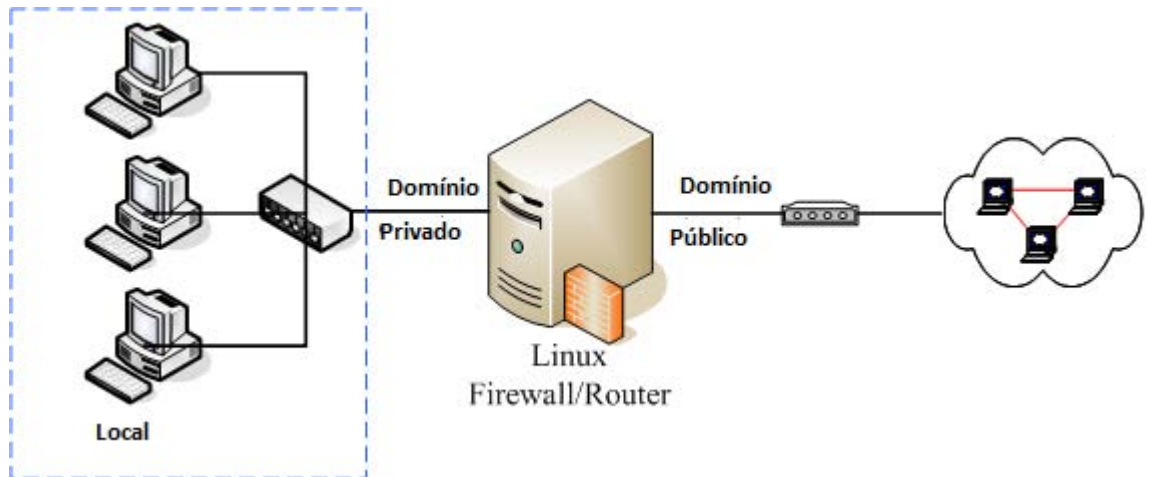


Figura 8: Um único domínio.

No modelo representado pela figura 8 o firewall, facilmente, poderá controlar todos os pacotes dentro da rede local, assim como gerir todos os pacotes provenientes da internet.

A utilização de NAT é caracterizada como uma proteção adicional, em geral no firewall, já que pode diminuir a probabilidade de brechas de confiança. Esta estrutura é formada conforme mostrado à figura 9.

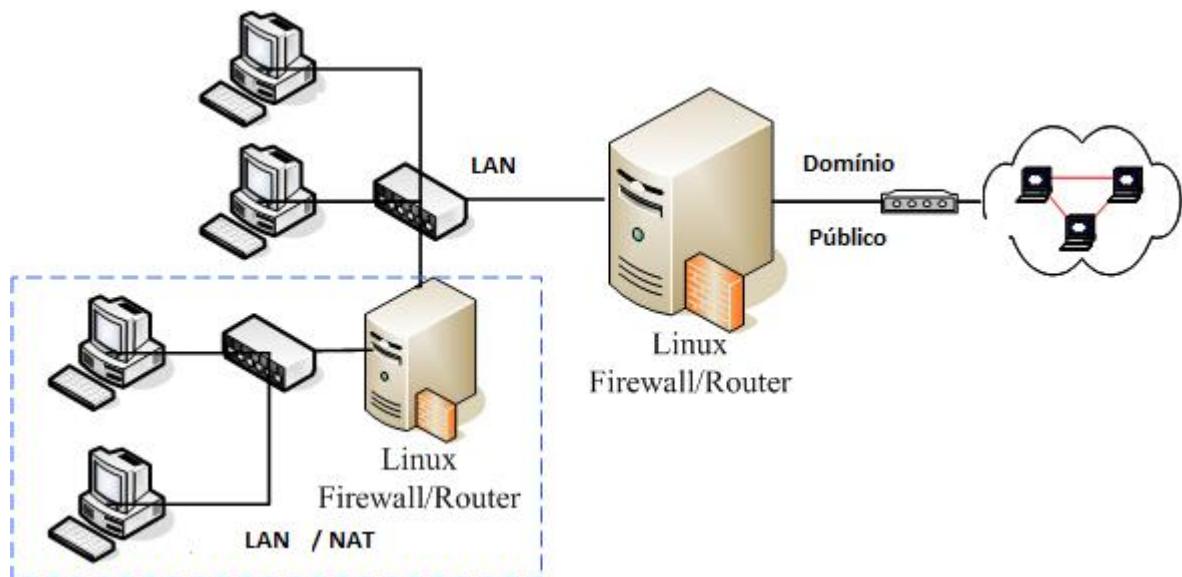


Figura 9: Domínio com NAT

O NAT acaba oferecendo uma barreira adicional, pois não envia o IP do host para a internet, como pode ser mais bem entendido com a representação da figura 10, e também não tem acesso direto ao host baseando-se na configuração dentro do NAT representado na figura 11.

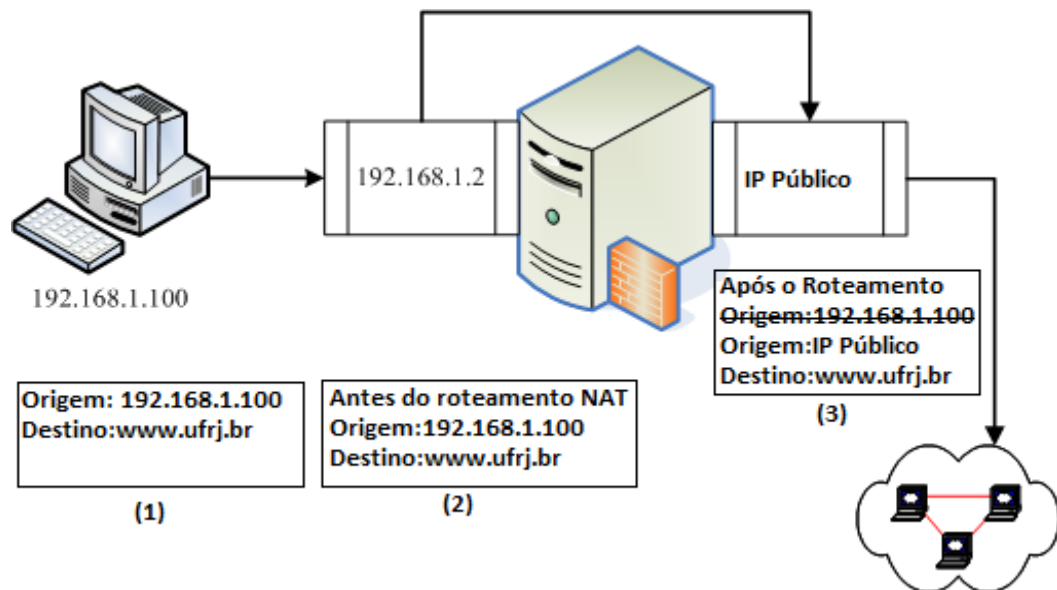


Figura 10: NAT Saída

1. Emitido pelo cliente no cabeçalho do pacote, fonte 192.168.1.100, então enviá-lo para o servidor NAT;
2. A interface interna NAT (192.168.1.2) irá iniciar a análise de dados do cabeçalho, o encaminhamento deste pacote será feito para interface de IP Público.
3. O IP privado e IP público não podem ser trocados, o host Linux via tabela NAT dentro de um processo pós roteamento de cabeçalho faz uma camuflagem para a interface Pública do host com dois IPs diferentes (192.168.1.100 e IP Público), encaminhado um controle para memória e enviando para internet.

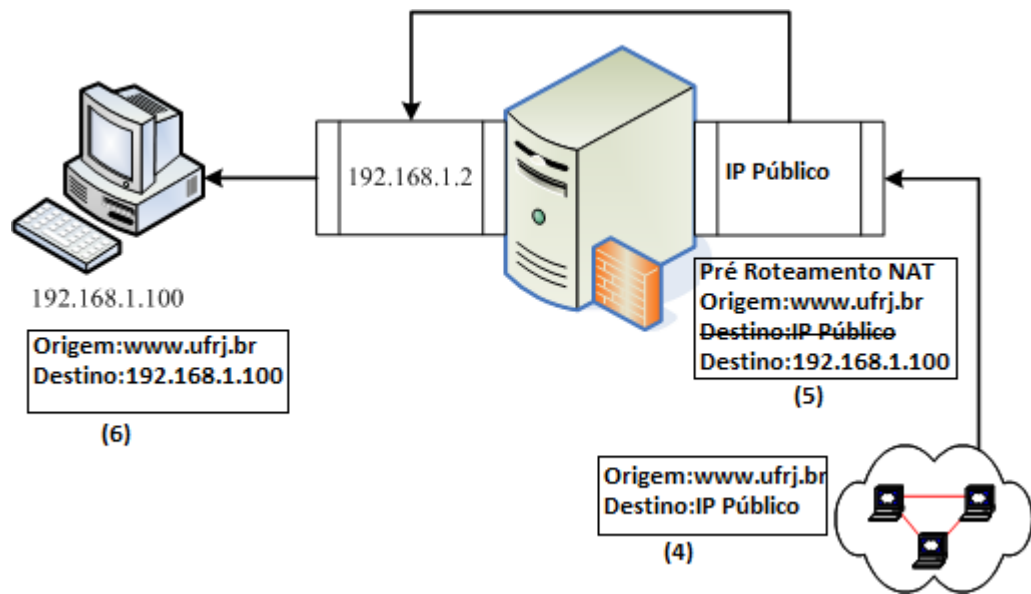


Figura 11: NAT Entrada

4. O servidor recebe o pacote onde será enviada uma resposta para o requerente.
5. Quando servidor NAT recebe os pacotes de resposta a partir da internet, vai analisar o número de sequência dos pacotes e os dados que foram gravados na memória junto ao pacote enviado antes pelo servidor. O IP destino será modificado para se tornar o servidor final de volta, o que é 192.168.1.100, verificando que então o IP Público não é nativo. Assim sendo, os pacotes sempre passam por uma análise de encaminhamento.
6. Os pacotes serão enviados para 192.168.1.2, interface interna, e em seguida enviados para o host final 192.168.1.100.

Escrever regras de firewall é complexo no Iptables, mas existem vários firewalls gráficos no Linux, assim como o Firestarter e o Shorewall. O nível de dificuldade deles varia, mas oferecem uma interface amigável, gerando de maneira

mais simples regras de Iptables. Os comandos básicos de Iptable pode ser conferido na tabela 1. Sintaxe do iptables:

```
#iptables -t [tabela] <ordem> <chain> [condições] -j <ação>
```

Tabela 1: Iptables

Regra	<i>iptables -A</i> <i>iptables --append</i>
Regra em prioridade	<i>iptables --insert [linha]</i> <i>iptables -I [linha]</i>
Remover regra	<i>iptables -D [Regra]</i> <i>iptables --delete [Regra]</i>
Substituindo regra	<i>iptables --replace [Regra]</i> <i>iptables -R [regra]</i>
Listar Regras	<i>iptables -L</i> <i>iptables --list</i> <i>iptables -L OUTPUT</i> <i>iptables -t nat -L</i>
Zerar contadores	<i>iptables -Z</i> <i>iptables --zero</i> <i>iptables -Z INPUT</i>
Nova CHAIN	<i>iptables -N NOVACHAIN</i> <i>iptables --new-chain NOVACHAIN</i> <i>iptables -t nat -N novachain</i>
Renomeando CHAINS	<i>iptables -E ANTIGACHAIN NOVACHAIN</i> <i>iptables --rename-chain ANTIGACHAIN NOVACHAIN</i>
Deletando CHAINS	<i>iptables -X NAMEDACHAIN</i> <i>iptables --delete-chain NAMEDACHAIN</i>
Regras padrão	<i>iptables -P</i> <i>iptables --policy</i>

5.2 IDS – SISTEMA DE DETECÇÃO DE INTRUSÃO

A cada novo dia surgem novas tecnologias que prometem projetar um sistema de segurança cuja eficiência se aproxima de 100%.

Todos os tipos de criptografias conhecidos podem de uma maneira ou outra, serem quebrados. Todos os sistemas, por mais seguros, estão propícios a ataques, que podem ser originados tanto externamente, como internamente. Então, quanto mais rápido forem descobertos estes ataques, mais rápido serão tomadas providências para sua anulação. Este é o princípio de uma ferramenta IDS (*Intrusion Detection System*).

Um IDS trabalha em tempo real, proporcionando à rede monitoramento de tráfego e armazenando dados. Sua utilização é feita de maneira a alertar as possíveis falhas de segurança.

A análise dos pacotes é baseada em regras de segurança armazenadas em seu banco de dados, tendo o administrador a liberdade de criar e adicionar regras que atendam às necessidades de segurança de sua rede.

Existem dois tipos de soluções que podem ser aplicadas a IDS: baseado em “host” e em “rede”.

- NIDS – Sistema de detecção de intrusos por rede.
- HIDS – Sistema de detecção de intrusos por hosts.

Ambas as soluções contam com vantagens e desvantagens. Apesar do sistema por rede ser o mais utilizado. A tabela 2 mostra as principais diferenças entre ambos.

Tabela 2: Networking

	HIDS	NIDS
Protege múltiplas estações com análise apenas de um pacote	Não	Sim
Analisa o trafego de forma individual	Sim	Não
Monitora apenas uma máquina	Sim	Não
Monitora toda a rede	Não	Sim
Pode trabalhar com vários pontos espalhados pela rede	Não	Sim
Pouco impacto sobre o desempenho da rede, pois trabalham em modo de escuta.	Sim	Sim
Monitoram redes com muito tráfego com facilidade	Não	Não
Analisa tráfego criptografado	Sim	Não
Verifica se o ataque sofrido foi bem sucedido	Sim	Não
Funciona bem com análise de pacotes fragmentados.	Sim	Não
Precisa ser configurado em cada computador	Sim	Não
Reconhece ataque destinado a rede	Não	Sim
Influência no desempenho do host	Sim	Não

5.2.1 Tipos de intrusões

As intrusões podem ser classificadas em dois grandes grupos:

- Anomalias
- Abusos

ANOMALIAS - Como o nome sugere, são feitas comparações dos pacotes com seu banco de dados e por seus conjuntos de regras, são considerados anomalias.

Este tipo de procedimento deve ser analisado com cuidado, pois é passível de erro, já que se pode criar a falsa impressão de ataque, ou mesmo, mascarar um possível ataque.

Estes erros são classificados em três tipos:

- Falso positivo – Ocorre o falso positivo quando a ferramenta identifica uma intrusão, por não conhecer o pacote analisado, porém trata-se de uma atividade normal.
- Falso negativo – Ocorre o falso negativo quando acontece uma intrusão e a ferramenta não identifica o tráfego positivo.
- Subversão – Ocorre quando a intrusão tem o propósito de mudar as regras da ferramenta IDS. O intruso modifica as regras criando falsos negativos e falsos positivos.

ABUSOS - São procedimentos de defesa que utilizam um padrão conhecido. Mesmo que o ataque utilize variações, serão descobertos. Para isso será necessário que as regras cubram todas as variações possíveis.

5.2.2 Exemplos de IDS

Existem várias ferramentas IDS, pagas, *free* e *open source*, que oferecem segurança às redes. Eis alguns exemplos: Checkpoint, IDS/IPS, Snort, OSSEC, Prelude, entre outros.

Porém, qual seria a melhor solução?

Isso dependerá de vários fatores, tais como: o cenário, o conhecimento que o administrador terá para configurar a ferramenta, o custo.

Como exemplo usará o Snort, já que a ferramenta é usada amplamente em todo mundo.

SNORT - Criado em 1998 por Martin Roesch, ele é capaz de checar o tráfego, da rede em tempo real, fazendo o registro destes dados por IP. O Snort é grátis, além de ter seu código fonte aberto a desenvolvedores (*open source*), contando hoje com mais de 4 milhões de downloads e sendo hoje a tecnologia de prevenção de intrusão mais utilizada no mundo.

INSTALANDO SNORT

Instalação:

```
#apt-get install mysql-server mysql-client
```

Durante a instalação será pedido que fosse preenchido o campo com a senha do administrador do mysql.

```
#mysql -u root -p
```



```
mysql> create database snort;
mysql> grant all privileges on snort.* to snort@localhost
identified by 'senha_adm_mysql';
mysql> flush privileges;
mysql> quit
```

Configurando a base de dados:

```
#zcat /usr/share/doc/snort-mysql/create_mysql.gz | mysql -u
root -h localhost -p snort
#apt-get install snort-mysql snort-rules-default
```

Editar algumas configurações do snort:

```
#vi /etc/snort/snort.debian.conf

debian_snort_home_net="127.0.0.0/8,192.168.1.0/24"
debian_snort_interface="eth0"
---
```

Configurar o snort para usar o mysql:

```
#vi /etc/snort/database.conf

database: log, mysql, user=snort password=senha_snort_mysql
dbname=snort host=localhost

---
```

Remover o arquivo db-pending-config sem o qual não seria possível iniciar o snort.:

```
#rm /etc/snort/db-pending-config
```

Reiniciar o snort:

```
#/etc/init.d/snort restart
```

Instalar o BASE (*Basic Analysis and Security Engine*) para a análise de alertas gerado pelo snort.

Instalar alguns pacotes necessários:

```
#apt-get install php5 php5-mysql php5-gd php-pear libapache2-  
mod-php5 zip unzip
```

Reiniciar o apache2 para ter suporte ao php:

```
#/etc/init.d/apache2 restart
```

Download do BASE:

```
#WGET  
HTTP://SOURCEFORGE.NET/PROJECTS/SECUREIDEAS/FILES/BASE/BASE-  
1.4.5/BASE-1.4.5.TAR.GZ
```

Descompactar o arquivo:

```
#tar xzvf base-1.4.5.tar.gz -c /var/www  
#cd /var/www  
#mv base-1.4.5/ base
```

Trocar o dono/grupo:

```
#chown www-data:www-data base -r
```

Baixar o adodb para acesso a base de dados:

```
#wget http://sourceforge.net/projects/adodb/files/adodb-php5-  
only/adodb-513-for-php/adodb513.zip
```

Descompactar:

```
# unzip -d /var/www adodb513.zip
# chown www-data:www-data adodb5 -r
```

Configurar o BASE:

```
# cd /var/www/base
# cp -a base_conf.php.dist base_conf.php
# vi base_conf.php
$base_urlpath = '/base';
$dblib_path = '/var/www/adodb5';
$alert_dbname = 'snort';
$alert_host = 'localhost';
$alert_port = "";
$alert_user = 'snort';
-----
```

Instalar dependências pear Image_Canvas e Image_Graph:

```
#pear install -a pear/image_graph-0.8.0
```

Ao invés de trazer o que foi pedido ele trouxe o Numbers_Words, mas precisamos dela então vamos resolver outra dependência:

```
#pear install -a pear/image_canvas-0.3.0
```

E agora o Image_Graph:

```
#pear install -a pear/image_graph-0.8.0
```

Abrir o navegador para verificação no seguinte endereço:
<http://10.1.1.11/base>

Agora fica mais fácil analisar os alertas gerados pelo SNORT, o BASE não é o único com esse propósito. Existem outras ferramentas que podem ser utilizadas.

6 – CONCLUSÕES

O objetivo deste trabalho foi implementar de forma segura e adequada um Servidor.

Em geral, é possível montar um servidor que forneça segurança aos serviços fornecidos na rede. Não há dúvidas sobre a eficiência e flexibilidade do uso do Linux, quando comparado a outros sistemas operacionais. E, embora não pareça, a filosofia do *opensource* proporciona aos profissionais a possibilidade de adequar a estrutura da rede às necessidades corporativas do mundo atual.

Hoje, as referências demonstram que nos provedores de serviços e no datacenters espalhados pela rede mundial, o Linux é o sistema operacional mais utilizado. Com efeito, o servidor Linux deixou de ser uma opção e passou a ser a solução em diversos serviços da área de TI.

A sua segurança é um dos fatores que garante a sua preferência nos serviços voltados para a WEB.

Em suma, concluímos que o conjunto de ferramentas disponíveis no Linux viabiliza a configuração de servidores altamente eficientes e seguros; capazes de atender a todas as demandas provenientes do ambiente de TI, provendo, assim, soluções e serviços adequados às necessidades existentes.

REFERÊNCIAS

BONAN, ADILSON RODRIGUES. **LINUX: Fundamentos, Prática & Certificação LPI – Exame 117-101**. 1. Ed. Rio de Janeiro, Alta Books, 2010.

JUCÁ, Humberto L. **Técnicas Avançadas de Conectividade e Firewall: em GNU/Linux**. Rio de Janeiro: Brasport, 2005.

MORIMOTO, Carlos Eduardo. **Servidores Linux – Guia prático**. Porto Alegre: Meridional, 2008

SISTEMA OPERACIONAL LINUX – **Sistemas Operacionais**. Disponível em: <<http://www.inf.ufrgs.br/~asc/livro/secao94.pdf>>. Acessado dia 12 Nov. 2012

TANENBAUM, Andrew, S. **Sistemas Operacionais**, 1999.

ZWICHY, Elizabeth D.; COOPER, Simon; CHAPMAN, D. Brent. **Construindo Firewalls para a Internet**. 2ª ed. Rio de Janeiro: Campus, 2000