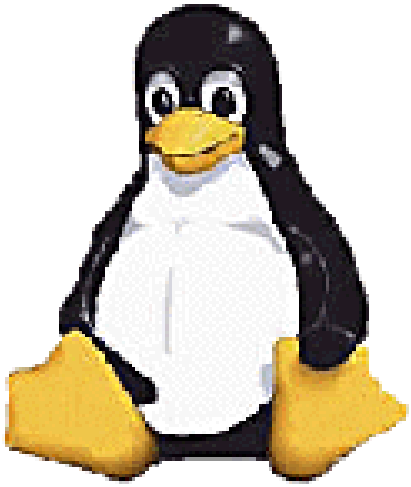
L I N U X

como servidor intranet e Internet



Palestrante:

João ERIBERTO Mota Filho

O B J E T I V O S

- Conhecer as características e possibilidades do SO Linux
- Planejar a segurança básica da rede e dos usuários
- Integrar uma intranet a um provedor Internet

S U M Á R I O

Pensamentos Iniciais

Pensamentos Iniciais

Linus Torvalds:

“Não há e nunca haverá um sistema operacional melhor que os outros em tudo.”

Pensamentos Iniciais

Linus Torvalds:

“Não há e nunca haverá um sistema operacional melhor que os outros em tudo.”

Eriberto:

**“Linux: o melhor servidor TCP/IP do mundo;
Windows 9x: um dos melhores clientes do mundo,
apesar de suas limitações técnicas.”**

Pensamentos Iniciais

Linus Torvalds:

“Não há e nunca haverá um sistema operacional melhor que os outros em tudo.”

Eriberto:

**“Linux: o melhor servidor TCP/IP do mundo;
Windows 9x: um dos melhores clientes do mundo,
apesar de suas limitações técnicas.”**

**“Administradores de sistemas devem
dominar as técnicas de shell e abandonar
o ambiente gráfico.”**

Características do Linux

Características do Linux

- ✓ Foi projetado, em 1991, para ser servidor de rede
- ✓ Possui kernel estável e independente dos processos
- ✓ Possui ambiente shell (tela preta - sem gráficos)
- ✓ Exige poucos recursos de hardware
- ✓ É rápido (o shell roda full em 486 DX4-100 / 16 MB)
- ✓ Muitos provedores mundiais utilizam Linux
- ✓ É baseado no UNIX, o pai dos SO

Principais Servidores Linux

Principais Servidores Linux

- Páginas (sites)
- Mail
- DNS
- IRC (chat)
- Roteamento
- Firewall / Proxy
- Banco de dados
- Comunicações (dial-in)
- Telnet
- FTP
- News
- DHCP
- RADIUS
- Data e hora

Hardware Necessário

para

Servidores

Hardware Necessário para Servidores

Os dados a serem aqui apresentados estão de acordo com as seguintes situações:

√ Dados práticos com base na distribuição Red Hat e nos fabricantes de daemons indicados;

√ Considera-se que não esteja instalado o ambiente gráfico;

√ Os valores a serem apresentados representam o hardware mínimo/ideal para 200 clientes de rede.

Hardware Necessário para Servidores

Servidor:	**Sites (sem banco de dados)**
Processador:	**Pentium 100 - 200**
DRAM:	**16 MB - 32 MB**
HD:	**4 GB - 10 GB**
CD-ROM:	**Necessário**
Fabricante:	**Apache**

Hardware Necessário para Servidores

Servidor:	**Sites (com banco de dados)**
Processador:	**Pentium 200 - Pentium III**
DRAM:	**32 MB - 128 MB**
HD:	**10 GB - 20 GB**
CD-ROM:	**Necessário**
Fabricante:	**Apache**

Hardware Necessário para Servidores

Servidor:	**E-mail**
Processador:	**Pentium 100**
DRAM:	**16 MB**
HD:	**6.4 GB - 30 GB**
CD-ROM:	**Desejável para instalação**
Fabricante:	**Sendmail**

Hardware Necessário para Servidores

Servidor: DNS

Processador: 486 Dx2 66

DRAM: 16 MB

HD: 270 MB - 510 MB

CD-ROM: Desejável para instalação

Fabricante: BIND

Hardware Necessário para Servidores

Servidor: IRC

Processador: 486 Dx4 100

DRAM: 16 MB - 32 MB

HD: 510 MB

CD-ROM: Desejável para instalação

Fabricante: Vários

Hardware Necessário para Servidores

Servidor:	**Roteador de rede**
Processador:	**Pentium 75**
DRAM:	**16 MB**
HD:	**270 MB - 510 MB**
CD-ROM:	**Desejável para instalação**
Fabricante:	**Nativo no kernel (forward)**

Hardware Necessário para Servidores

Servidor:	**Firewall (filtro de pacotes)**
Processador:	**Pentium 75**
DRAM:	**16 MB**
HD:	**270 MB - 510 MB**
CD-ROM:	**Desejável para instalação**
Fabricante:	**Nativo no kernel (ipchains)**

Hardware Necessário para Servidores

Servidor:	**Firewall (proxy)**
Processador:	**Pentium 200**
DRAM:	**64 MB - 128 MB**
HD:	**6.4 GB - 30 GB**
CD-ROM:	**Desejável para instalação**
Fabricante:	**Squid**

Hardware Necessário para Servidores

Servidor:	**Banco de dados**
Processador:	**Pentium 200 - Pentium III**
DRAM:	**64 MB - 128 MB**
HD:	**6.4 GB - 30 GB**
CD-ROM:	**Desejável para instalação**
Fabricante:	**MySQL / Oracle**

Hardware Necessário para Servidores

Servidor:	**Comunicações (telefônico)**
Processador:	**486 Dx2 66**
DRAM:	**8 MB**
HD:	**270 MB**
CD-ROM:	**Desejável para instalação**
Fabricante:	**Portslave / RADIUS**

Hardware Necessário para Servidores

Em caso de vários servidores em uma mesma máquina, utilizar o hardware necessário para o maior.

Ex: Servidor DNS + E-mail + RADIUS

Hardware: Pentium 100 - 16 MB DRAM

Administração do Sistema

Administração do Sistema

- √ Redirecionamento de e-mail
- √ Segurança
- √ Análise de logs
- √ Controle da banda de saída

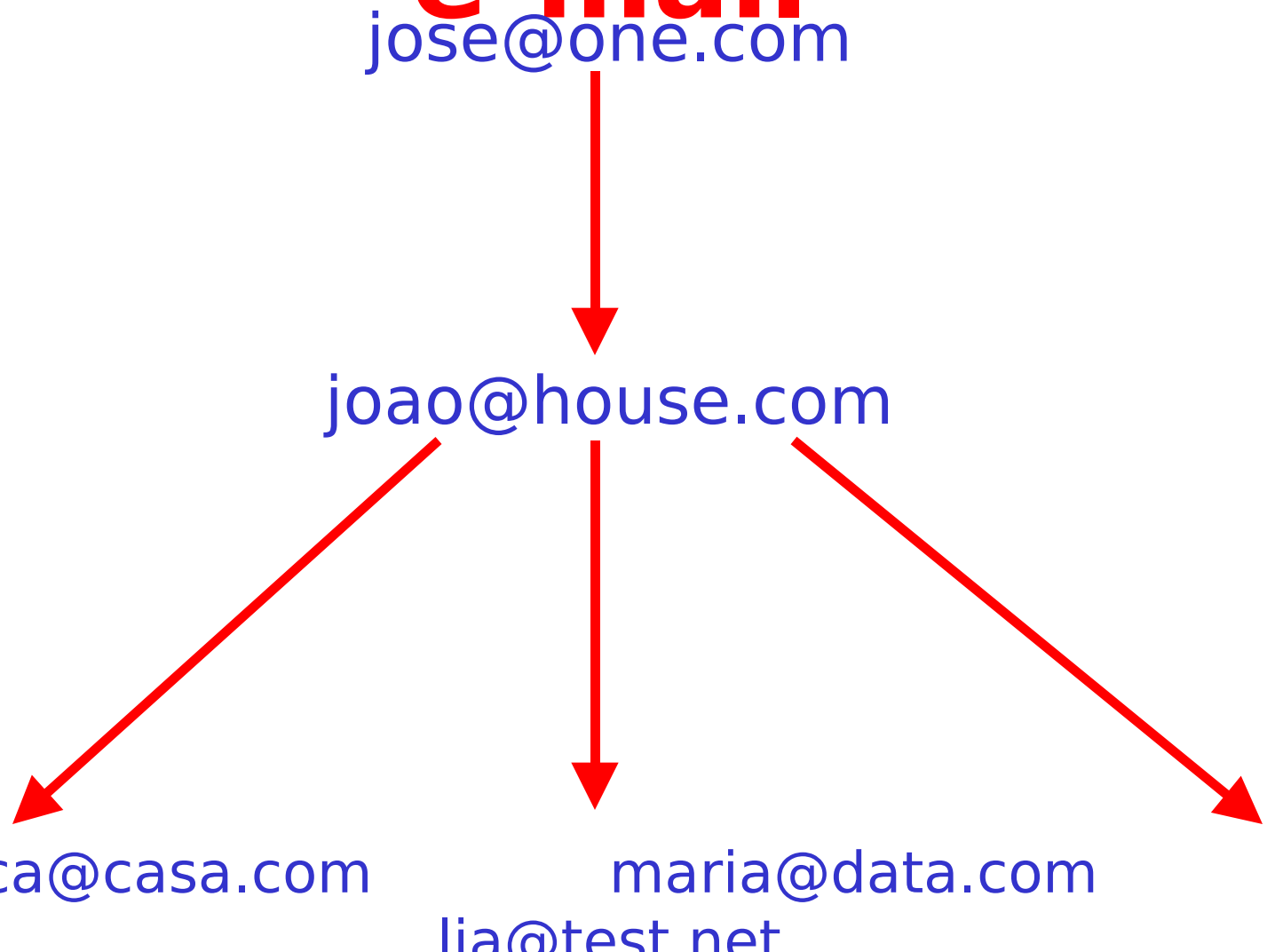
Administração do Sistema

√ **Redirecionamento de e-mail**

Redirecionamento de e-mail

Faz com que mensagens destinadas a um endereço sejam desviadas para outro(s) endereço(s). O destino original pode estar incluído ou não no redirecionamento.

Redirecionamento de e-mail



Redirecionamento de e-mail

Processamento do redirecionamento:

1. **Arquivo .forward em /home/usuário contendo os endereços de redirecionamento, ou;**

2. **Linha com endereços de redirecionamento em /etc/aliases.**

Redirecionamento de e-mail

1. Arquivo .forward em /home/usuário:

```
# cat  /home/joao/.forward
```

Redirecionamento de e-mail

1. Arquivo .forward em /home/usuário:

```
# cat  /home/joao/.forward

juca@casa.com
maria@data.com
lia@test.net
```

Redirecionamento de e-mail

2. Linha em /etc/aliases:

```
joao: juca@casa.com,maria@data.com,lia@test.net
```

Não esquecer de executar o comando

```
# newaliases
```

depois de editar o /etc/aliases.

Redirecionamentos Interessantes

webmaster → root
postmaster → root

abuso → root
abuse → root
spam → root

root → <e-mail do adm rede>

Ocorreu uma falha no kernel32.dll

Este programa executou uma operação ilegal em 00B0:0003 mas não será fechado por estar apoiando uma importante palestra sobre o Sistema Operacional Linux.

Administração do Sistema

Administração do Sistema

√ **Segurança física**

Administração do Sistema

- √ Segurança física
- √ Segurança do SO

Administração do Sistema

- √ Segurança física
- √ Segurança do SO
- √ Segurança de senhas

Administração do Sistema

- √ Segurança física
- √ Segurança do SO
- √ Segurança de senhas
- √ Segurança do usuário

Administração do Sistema

- √ Segurança física
- √ Segurança do SO
- √ Segurança de senhas
- √ Segurança do usuário

Administração do Sistema

√ Segurança física

Segurança física

- Classifique a área dos servidores como restrita;
- Somente pessoas autorizadas devem ter acesso à área dos servidores;
- Quando sozinhos, os servidores devem estar em sala trancada;

Segurança física

- Dependendo da situação, a topologia física deve estar protegida;
- O acesso local não autorizado deve ser dificultado com sensores, alarmes e câmeras;
- Deve haver uma rigorosa seleção de pessoal para evitar ações adversas.

Administração do Sistema

√ **Segurança do SO**

Segurança do SO

- Utilize um sistema eficiente de senhas;
- Realize o rodízio periódico de senhas do SO;
- Busque portas abertas no SO, utilizando programas próprios para isso;
- Desative todos os daemons que não estiverem sendo utilizados;

Segurança do SO

- Utilize firewall e criptografia, se possível;
- Firewalls mais caros possuem até sistemas de avisos por pager;
- Não execute serviços nas máquinas Firewall;
- Não cadastre usuários na máquina Firewall;
- Evite controlar remotamente o sistema (telnet, rshell, snmp etc);

Segurança do SO

- Submeta o SO a ataques de diversos tipos, buscando detectar falhas;
- Evite executar processos comuns como root;
- Inspecione periodicamente os arquivos de log;
- Utilize mensagens de abertura para serviços remotos (segurança psicológica);

Segurança do SO

- Realize upgrades regulares do SO e de seus daemons;
- Não deixe os servidores com cara de servidor;
- Utilize um servidor isca para gerar log de invasores, sem esquecer da segurança;
- Advirta e/ou puna usuários negligentes;

Segurança do SO

- Configure corretamente o seu MTA para que o mesmo não seja utilizado por spammers;
- Estude os cabeçalhos de e-mails suspeitos;
- Bloqueie, com critério, remetentes e domínios suspeitos de cometer spam;
- Retire ou restrinja o shell do usuário;
- Retire os modens clandestinos da rede;

Segurança do SO

- Utilize partições separadas para o sistema (/), caixas postais (/var/spool/mail) e diretórios de sites e do usuário (/home);
- Aplique limitação de disco (quota) nas partições /var/spool/mail e /home, para que não haja comprometimento do sistema em caso de superlotação dessas partições;

Segurança do SO

- Limite os usuários aos seus próprios diretórios, em operações de FTP;
- Coloque somente o indispensável nas configurações DNS. Não insira em DNS os firewalls, roteadores etc;
- Limite as permissões de acesso apenas aos usuários que têm necessidade delas.

Administração do Sistema

√ **Segurança de senhas**

Segurança de senhas

- Não permita que o login seja utilizado como senha;
- Utilize sempre mais de 10 caracteres nas senhas de sistema (root);
- Não utilize palavras de dicionários;
- Misture números na senha ou a mascare de alguma maneira;

Segurança de senhas

- Evite a engenharia social (pessoal ou ambiental) ao utilizar senhas;
- Tenha vários níveis de senha:
  * Pessoais de alto risco
  * Pessoais de uso geral
  * De administração de sistema
  * De cliente de sistema

Segurança de senhas

- Utilize shadow e MD5;
- Altere a senha do sistema periodicamente.

Administração do Sistema

√ **Segurança do usuário**

Segurança do usuário

- Alerte os usuários quanto aos riscos de senhas frágeis ou mal utilizadas;
- Ofereça recursos para que os usuários possam administrar suas senhas;
- Dê aos usuários condições de denunciar atos indesejados como spam etc.

Segurança total de rede

Segurança total de rede

Único sistema aprovado para segurança total de rede:

Segurança total de rede

Único sistema aprovado para segurança total de rede:

D E U S

Administração do Sistema

√ Scripts para análise de logs

Administração do Sistema

√ Scripts para análise de logs

- Acesso
- Invasão
- Disco
- Mail

Scripts para análise de logs

- Script acesso -

Mostra os acessos inetd bem sucedidos ao sistema, com exceção do POP-3, naquele dia.

Executar no cron, diariamente, às 23:59 h. O resultado será enviado para o root.

Scripts para análise de logs

- Script acesso -

```
#!/bin/bash
cat  /var/log/secure*|grep  ": conn"|grep  "`date  "+%b %e"`"|grep  -v  pop
```

Scripts para análise de logs

- Script invasão -

Mostra os acessos inetd mal sucedidos ao sistema (refused), naquele dia.

Executar no cron, diariamente, às 23:59 h. O resultado será enviado para o root.

Scripts para análise de logs

- Script invasão -

```
#!/bin/bash
cat  /var/log/secure*|grep  refused|grep  "`date  "+%b  %e"`"
```

Scripts para análise de logs

- Script disco -

Mostra utilização das partições do disco.

Executar no cron, às segundas-feiras, 30 min antes do início do expediente. O resultado será enviado para o root.

Scripts para análise de logs

- Script disco -

```
#!/bin/bash
df
```

Scripts para análise de logs

- Script mail -

Mostra utilização das caixas postais, em ordem decrescente.

Executar no cron, todos os dias, 30 min antes do início do expediente. O resultado será enviado para o root.

Scripts para análise de logs

- Script mail -

```
#!/bin/bash
ls  -shS  /var/spool/mail
```

Administração do Sistema

√ Controle da banda de saída

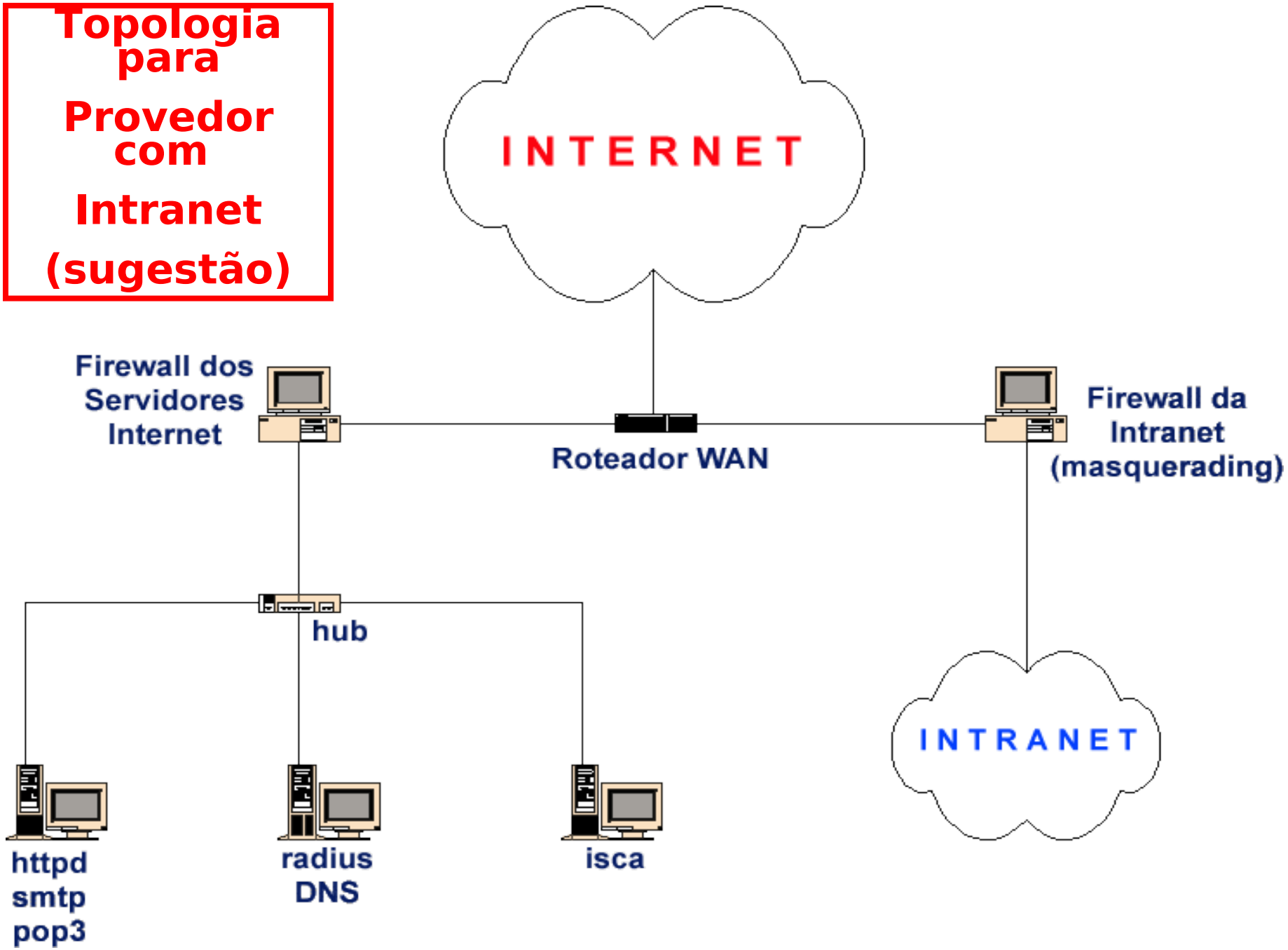
Controle da banda de saída

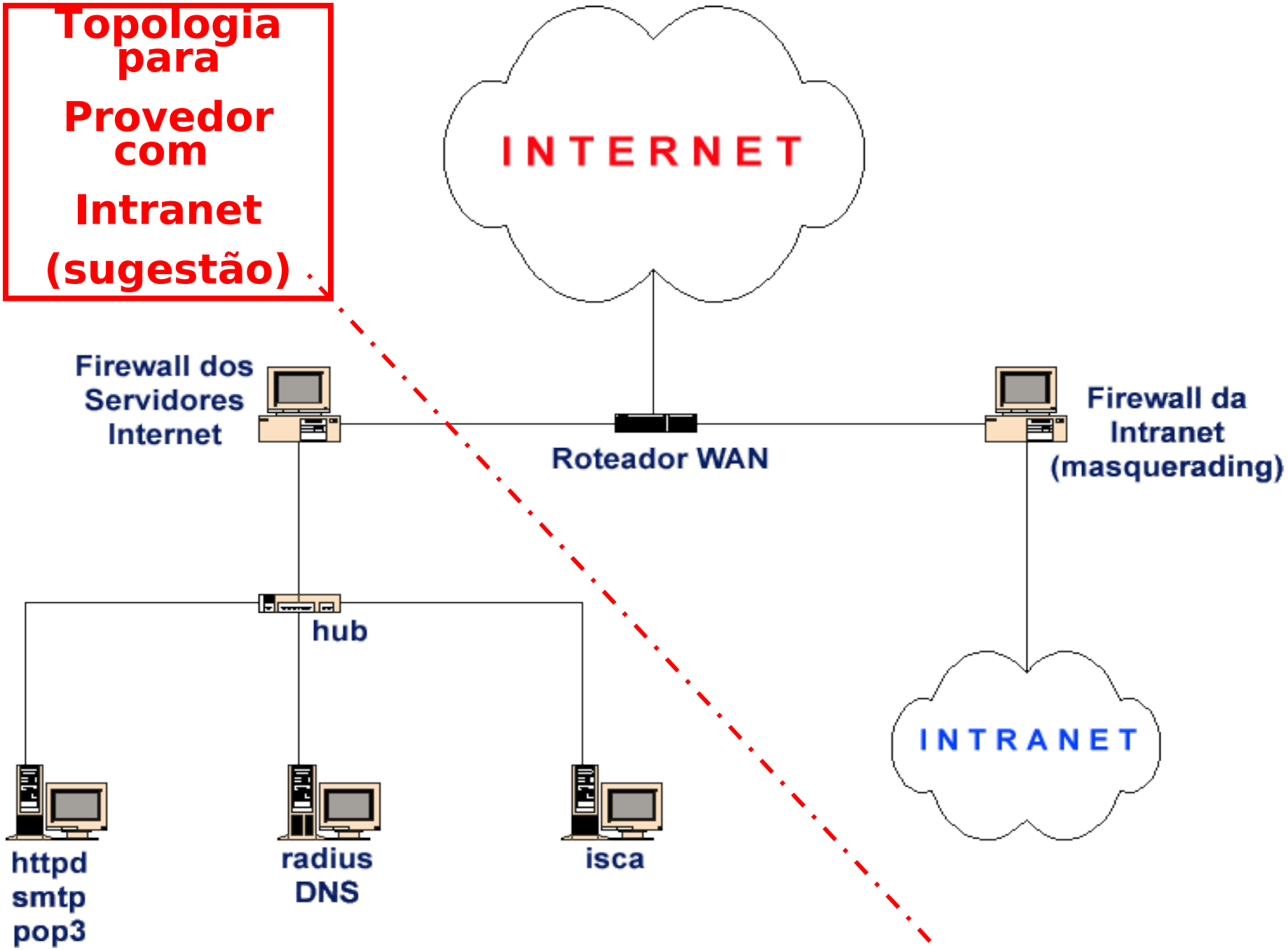
- Garante uma melhor utilização do link disponível por parte de cada um dos servidores de rede;
- Evita a queda do roteador WAN;
- O controle pode ser individual, geral ou misto;
- Sugestão: mail - 40%, sites - 30%, dns - 25%, folga/sobra - 5%.

Topologia de Rede

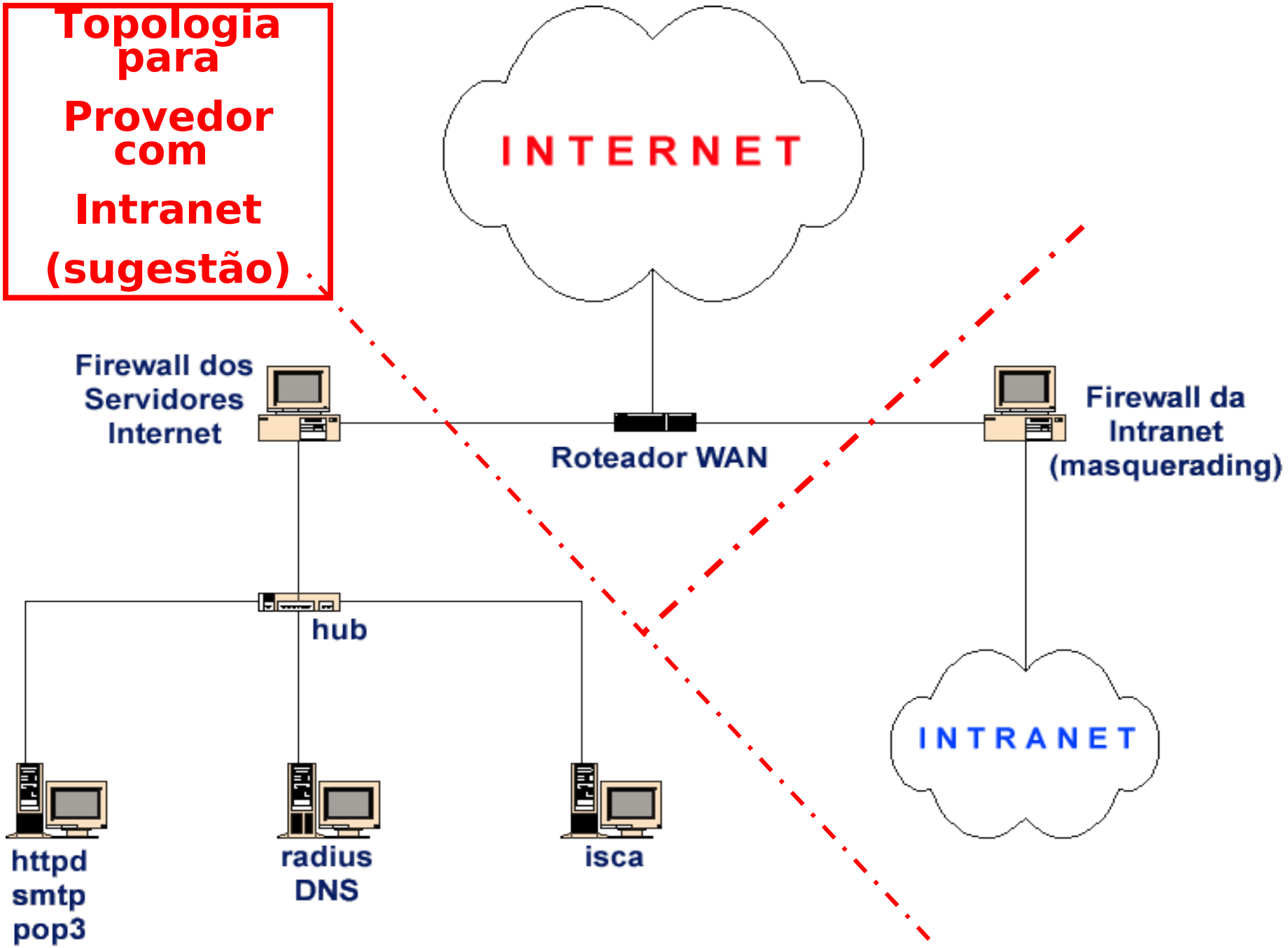
Provedor Internet com intranet

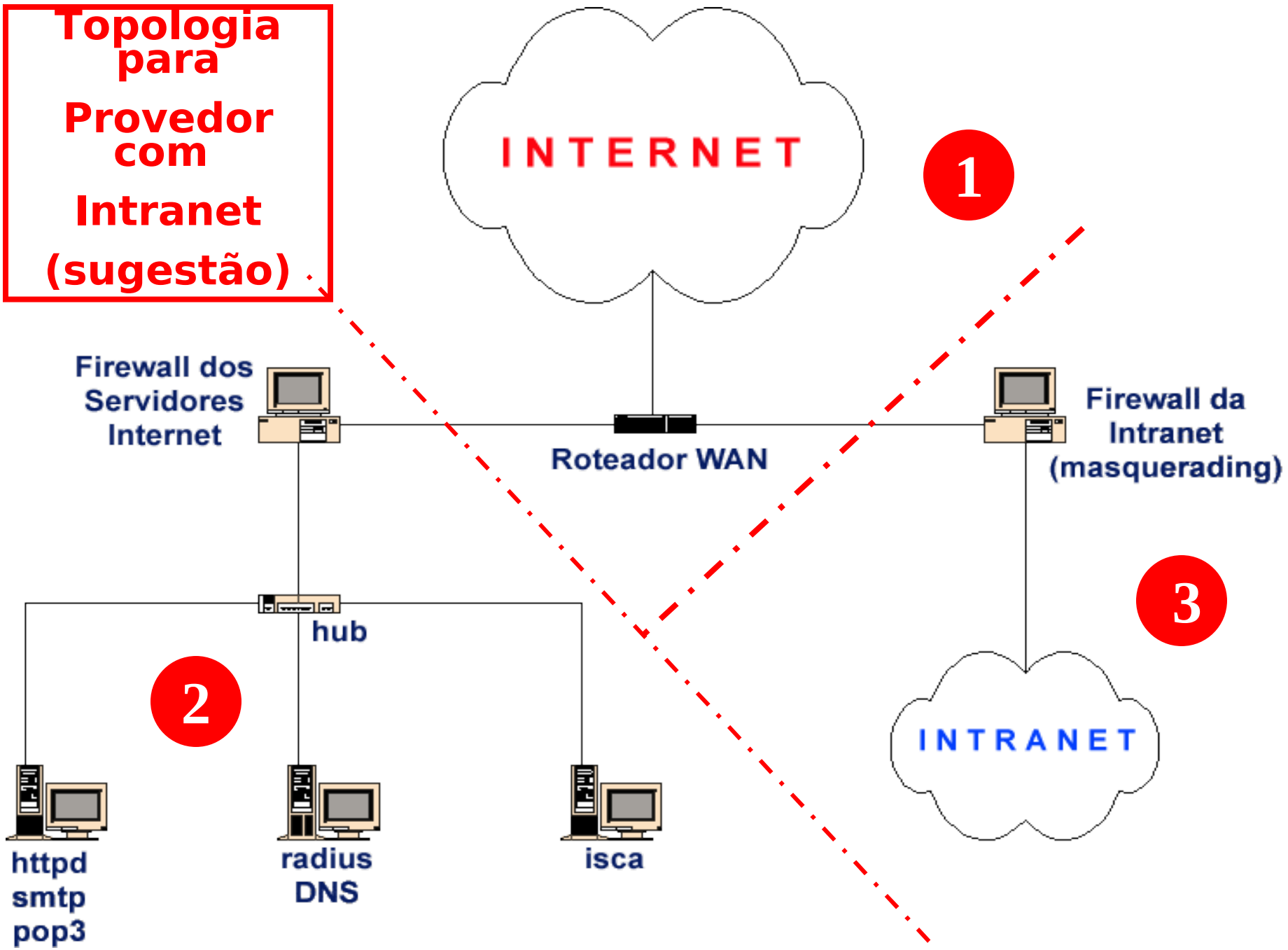
Topologia para Provedor com Intranet (sugestão)




Topologia para Provedor com Intranet (sugestão)
INTERNET
Firewall dos Servidores Internet
Roteador WAN
Firewall da Intranet (masquerading)
hub
INTRANET
httpd
smtp
pop3
radius
DNS
isca

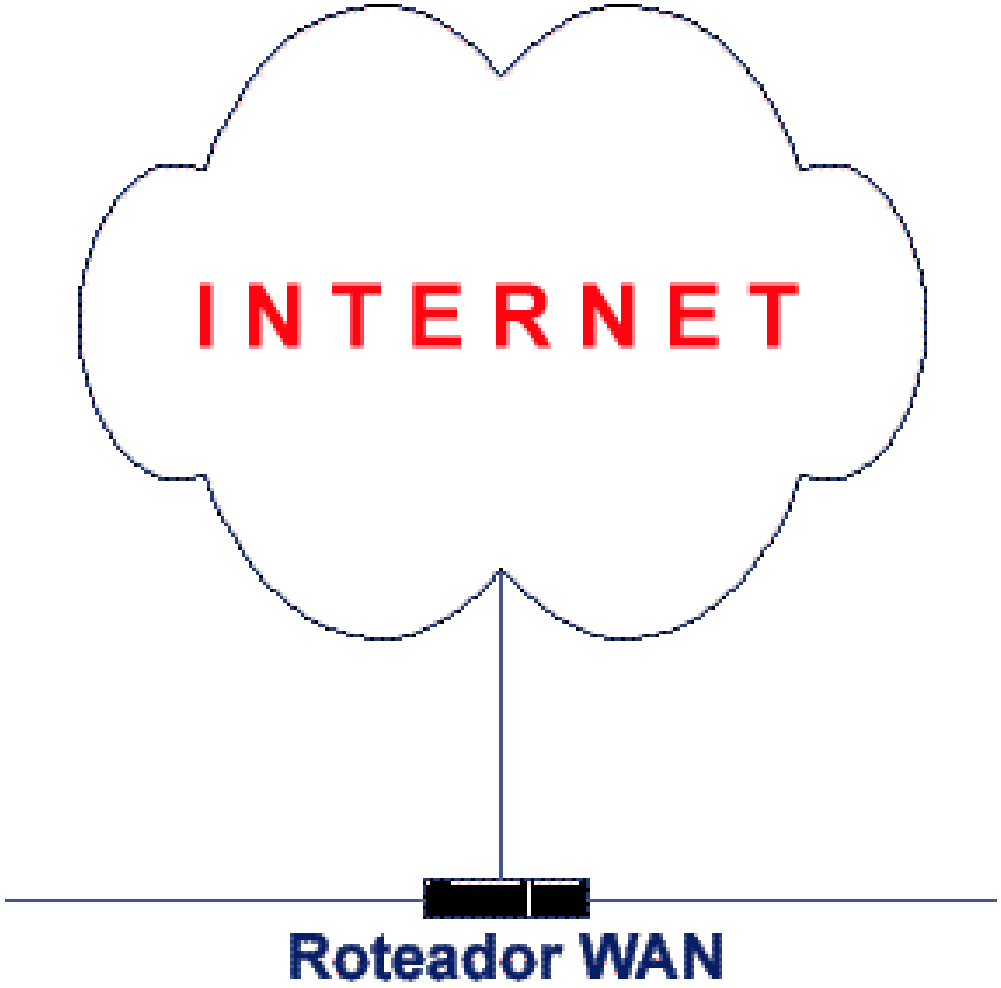
Topologia para Provedor com Intranet (sugestão)




Topologia para Provedor com Intranet (sugestão)
INTERNET
1
Firewall dos Servidores Internet
Roteador WAN
Firewall da Intranet (masquerading)
3
hub
2
INTRANET
httpd
smtp
pop3
radius
DNS
isca

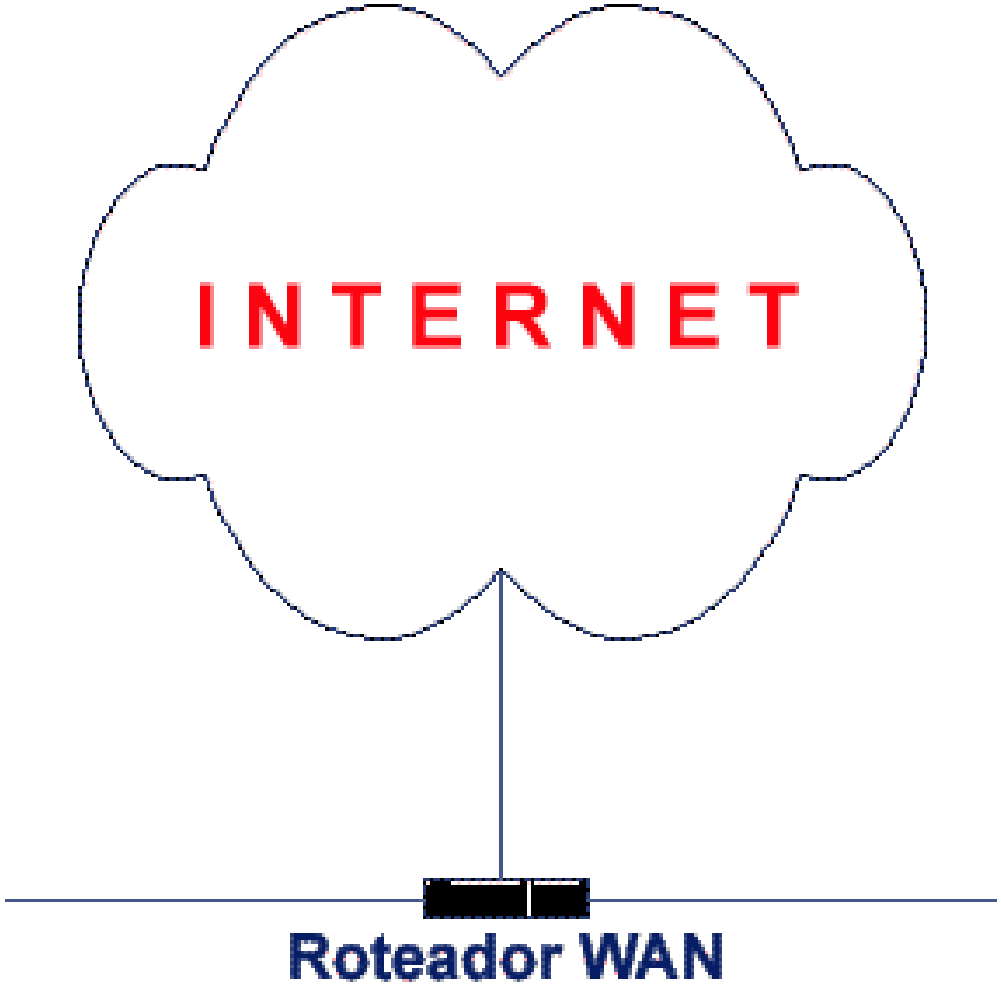
Topologia para Provedor com Intranet (sugestão)

1



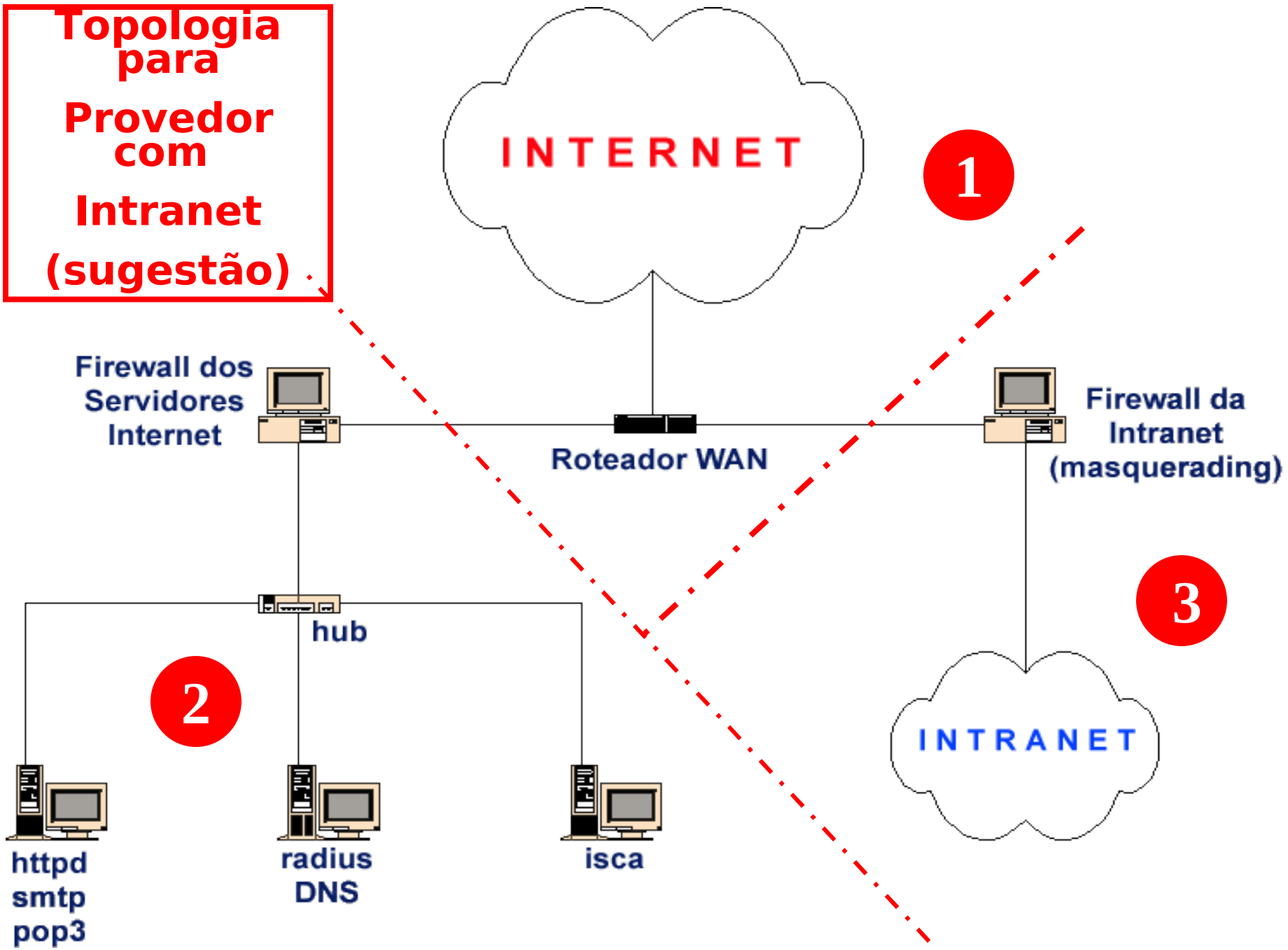
Topologia para Provedor com Intranet (sugestão)

1

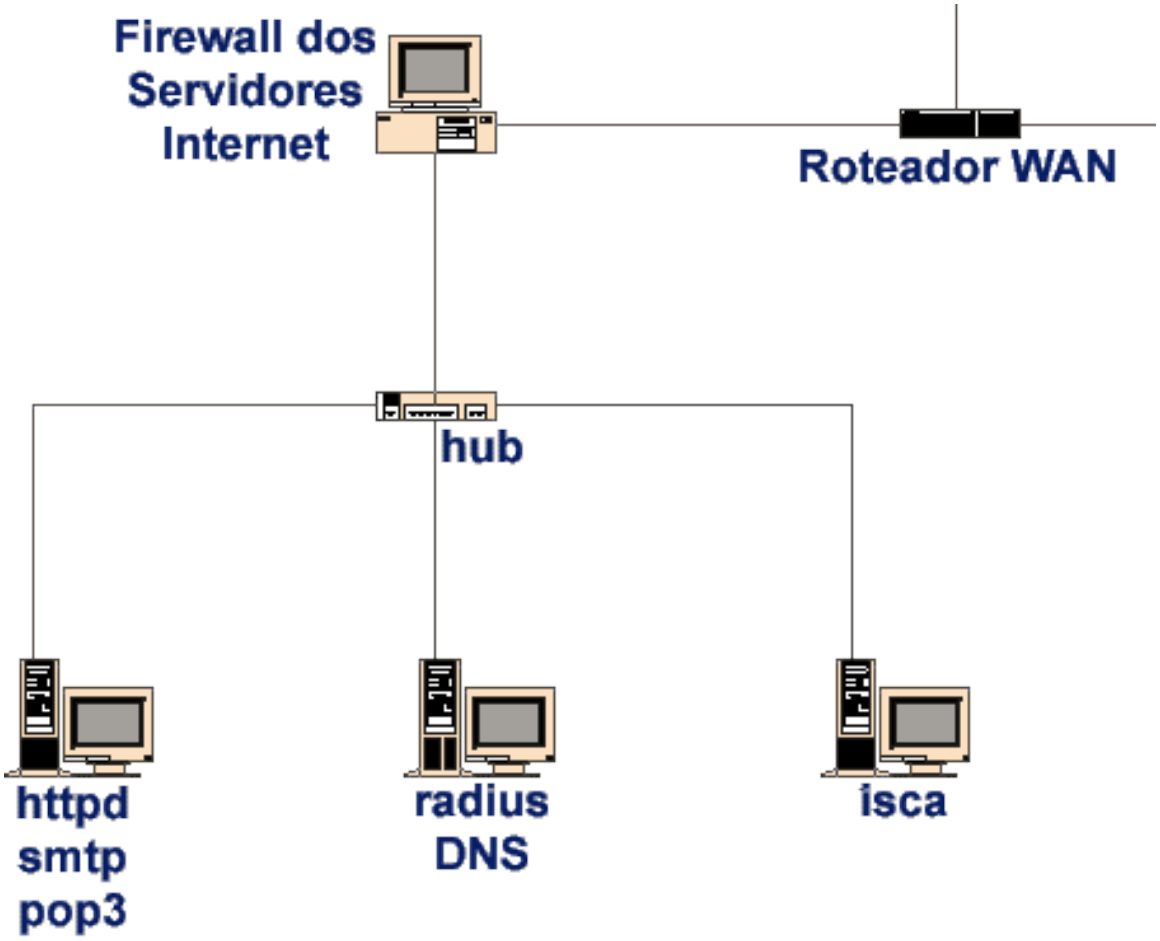


CARACTERÍSTICAS

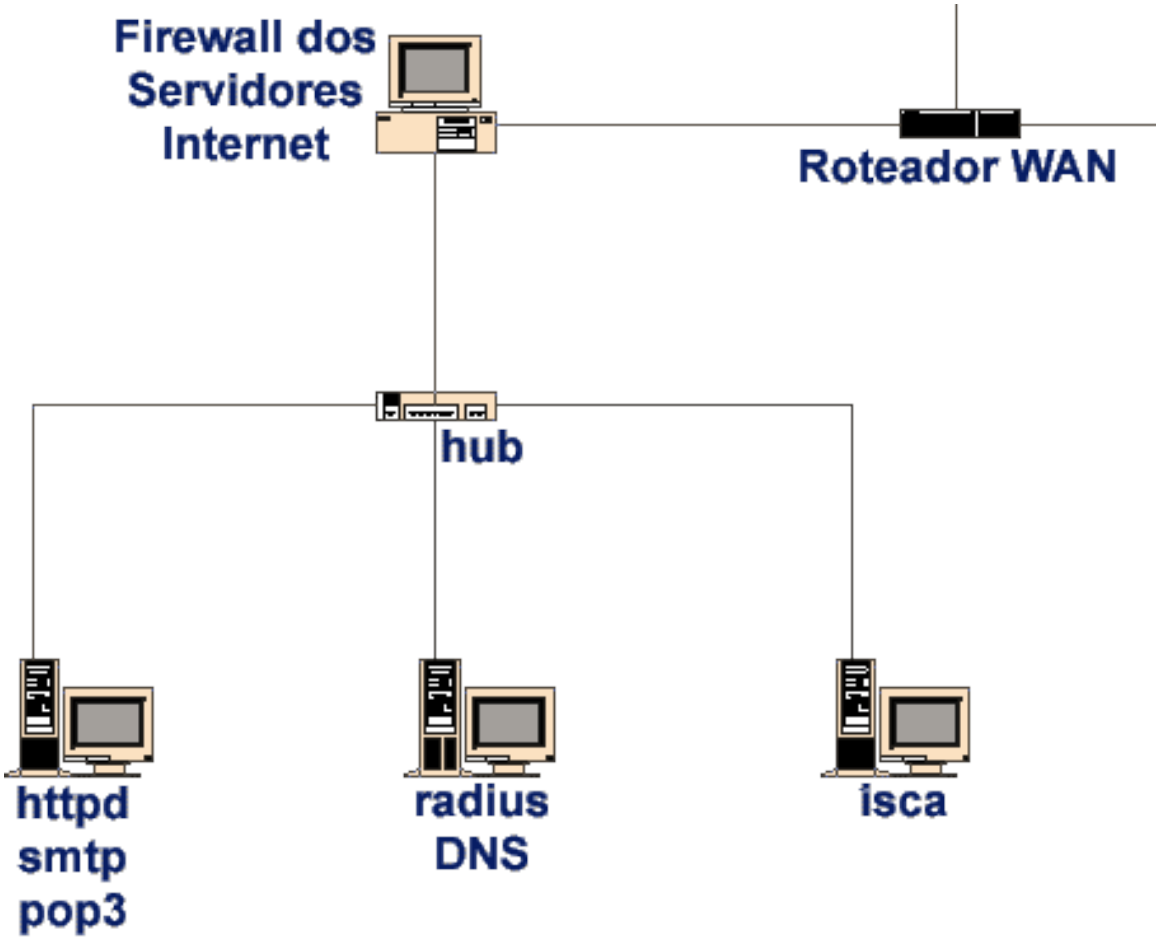
- Recebimento de dados
- Envio de dados


Topologia para Provedor com Intranet (sugestão)
INTERNET
1
Firewall dos Servidores Internet
Roteador WAN
Firewall da Intranet (masquerading)
3
hub
2
INTRANET
httpd
smtp
pop3
radius
DNS
isca

Topologia para Provedor com Intranet (sugestão)



Topologia para Provedor com Intranet (sugestão)

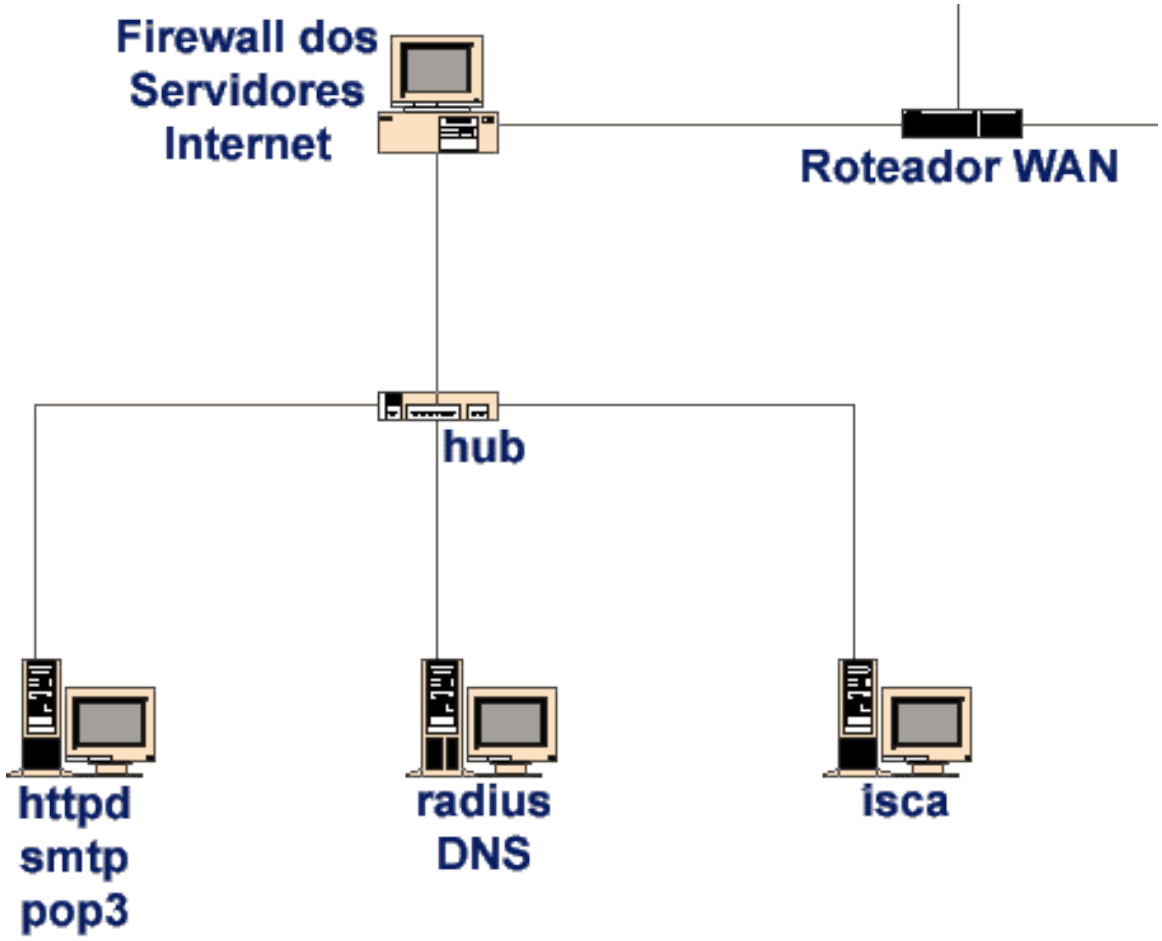


CARACTERÍSTICAS

- Limitação mista (banda)
- Maior banda de saída por máquina
- Firewall de passagem dando acesso somente às portas e serviços necessários
- Melhor controle da isca

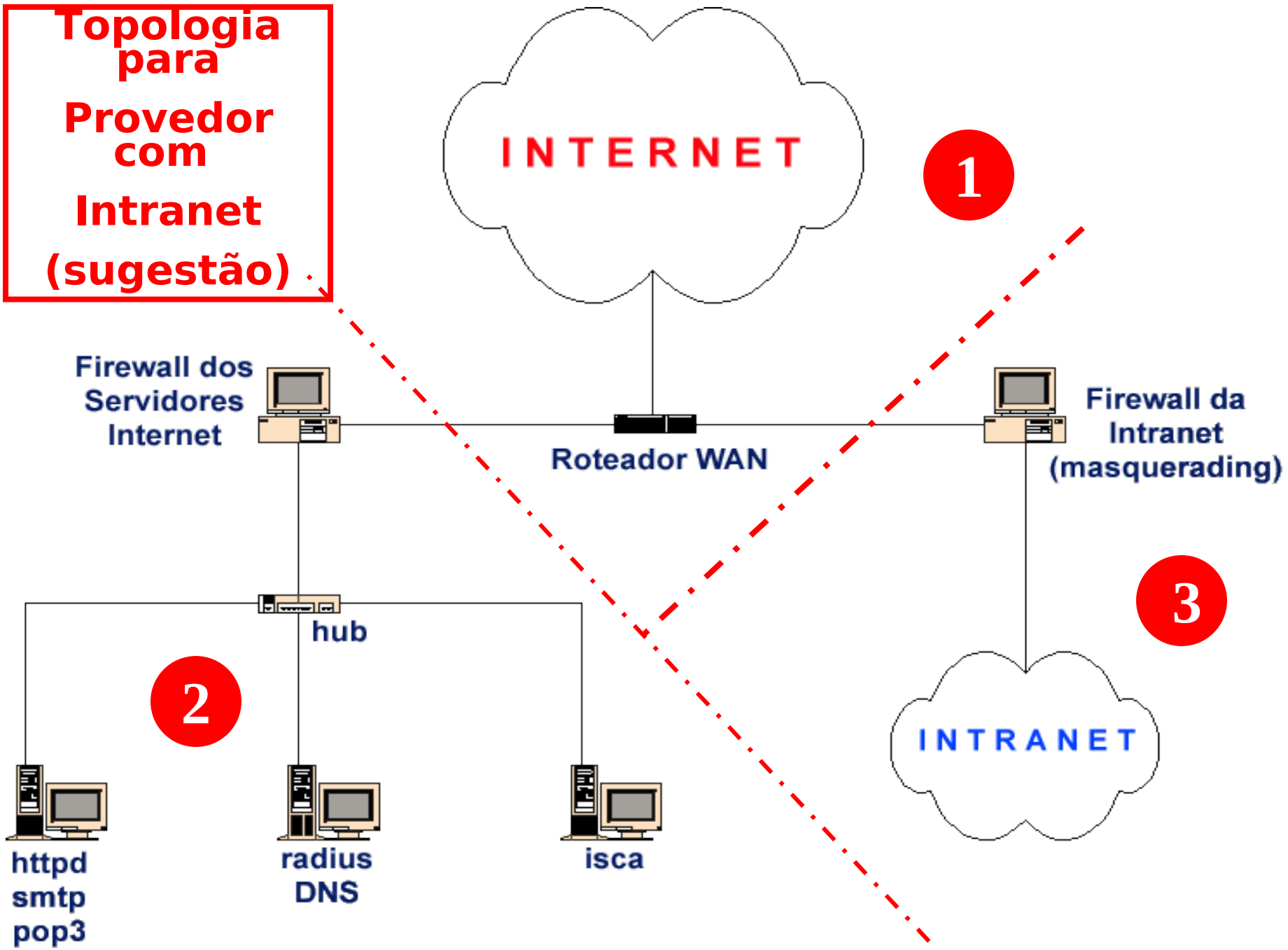
Topologia para Provedor com Intranet (sugestão)

2

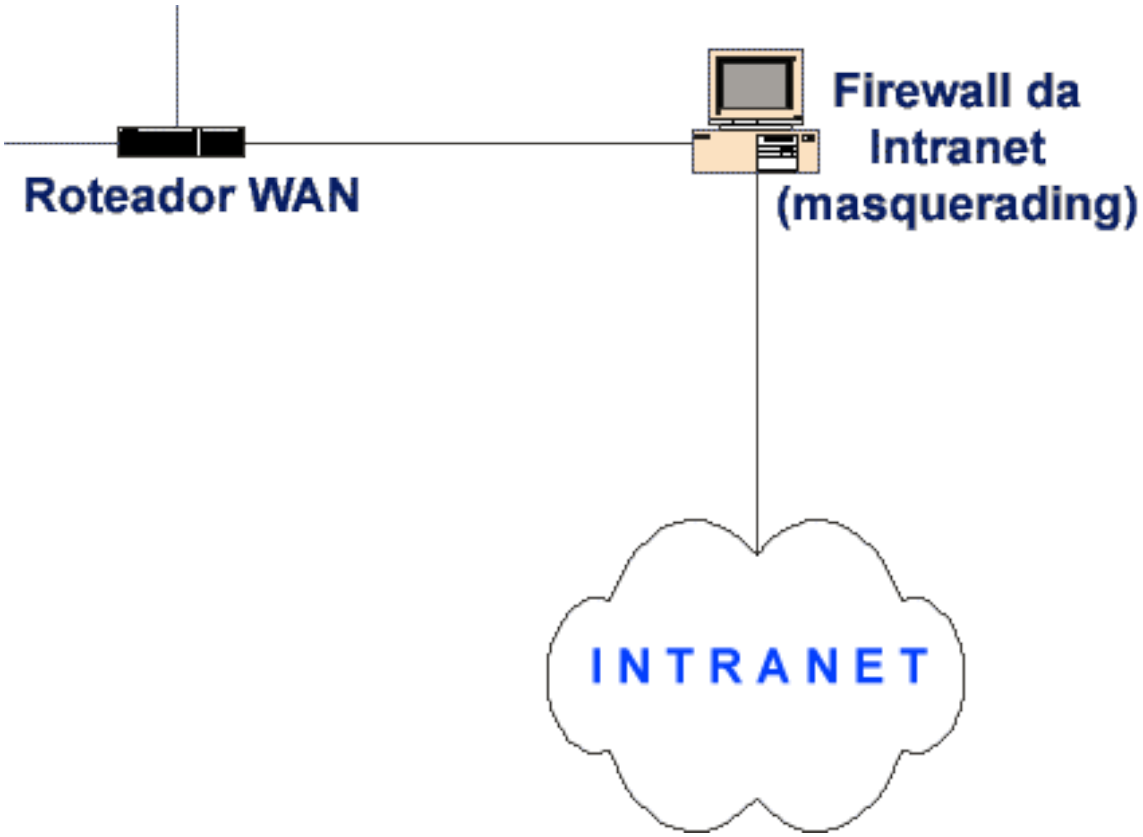


Portas Importantes

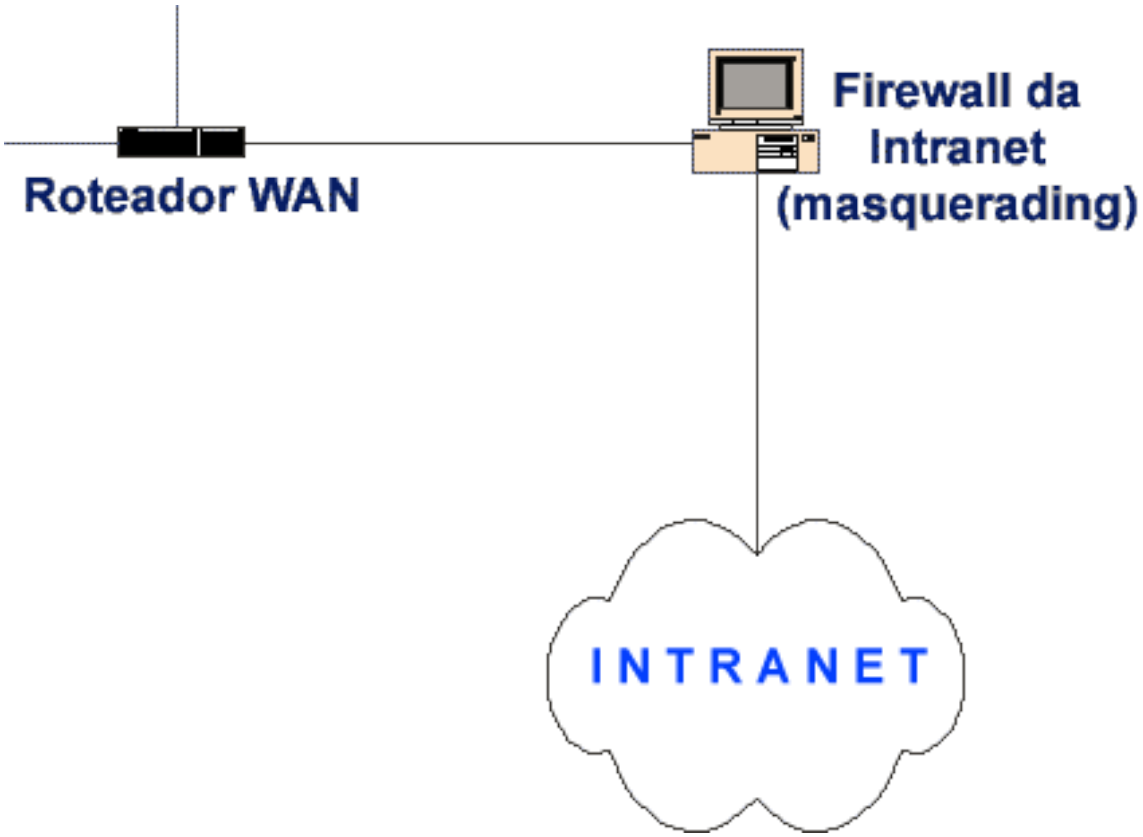
20 - ftp-data server
21 - ftp server
23 - telnet server
25 - smtp server
37 - time server
53 - dns server
79 - finger server
80 - http server
110 - pop3 server
139 - NetBIOS session
220 - imap server
443 - https server
513 - rlogin, rwho
514 - rshell
1812 - radius server
1813 - radius accounting
6667 - irc server


Topologia para Provedor com Intranet (sugestão)
INTERNET
1
Firewall dos Servidores Internet
Roteador WAN
Firewall da Intranet (masquerading)
3
hub
2
INTRANET
httpd
smtp
pop3
radius
DNS
isca

Topologia para Provedor com Intranet (sugestão)



Topologia para Provedor com Intranet (sugestão)



CARACTERÍSTICAS

- Limitação geral (banda)
- Firewall de mascara-mento ocultando, da Internet, toda a rede interna
- Ao contrário do que se pensa, a banda de saída do firewall de intranet não precisa ser grande.

Conclusão

O Sistema Operacional Linux é simples, leve, estável, seguro e possui muitos recursos. É extremamente viável a sua utilização como servidor em pequenas e grandes redes de computadores.

Referências e Apoio

Bibliografia Básica

- **Linux & Seus Servidores - João Eriberto M. Filho - Ciência Moderna**
- **Servidores de Rede com Linux - Craig Hunt - Market Books**
- **TCP/IP Internet - Fernando Albuquerque - Axcel Books**
- **Linux - Programação Shell - Julio Cezar Neves - Brasport**

Listas de Discussão

- **Servidores Linux: servux-subscribe@egroups.com**
- **LinUSP (genérica): http://linusp.usp.br/listas/linusp-gen**
- **Linux Networking: linux-networking-subscribe@egroups.com**
- **Sendmail-BR: http://listas.linkway.com.br**
- **Rede WAN: redewan-subscribe@listbot.com**