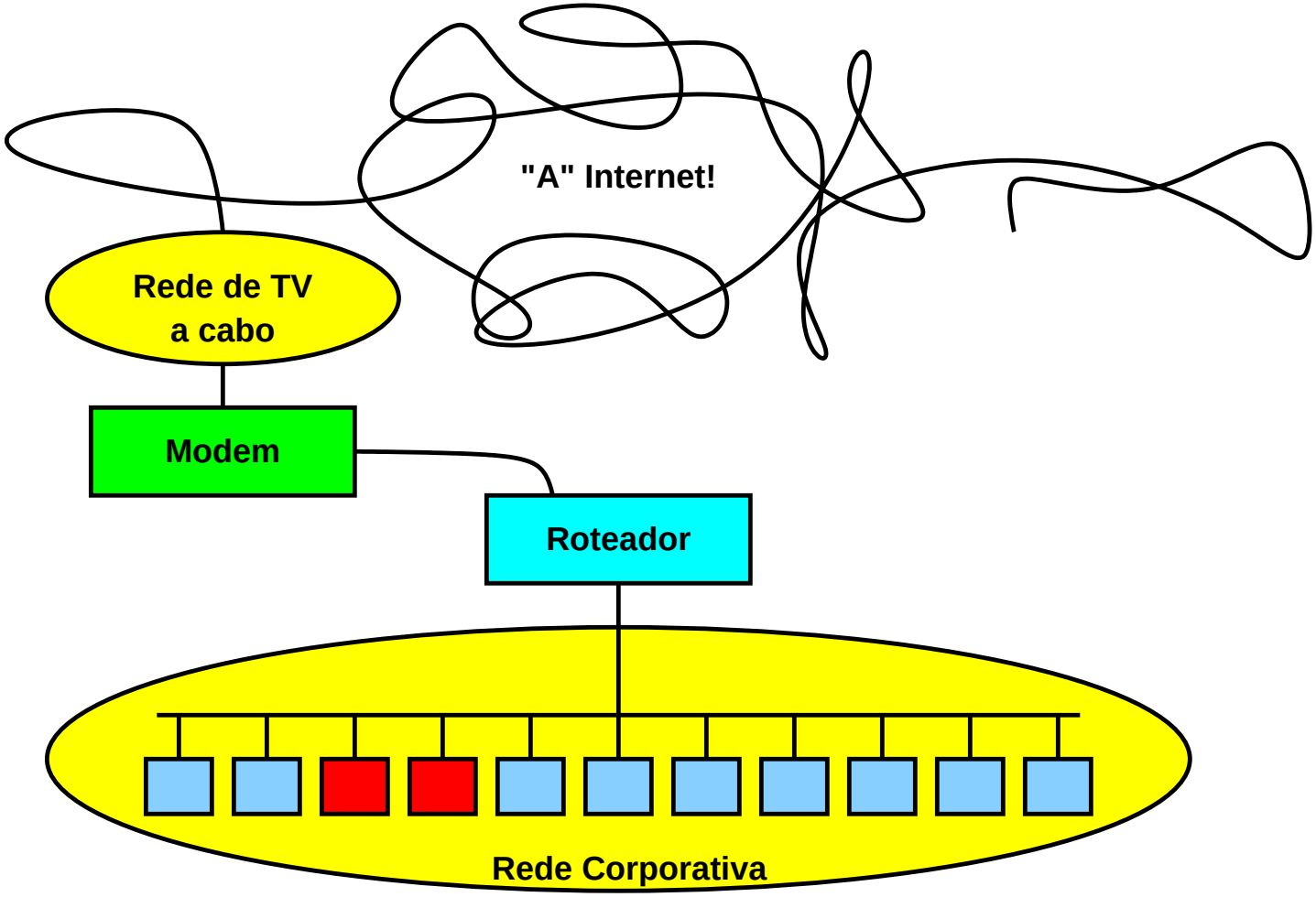
Duplo acesso de "pobre"

(poor man’s double homing)

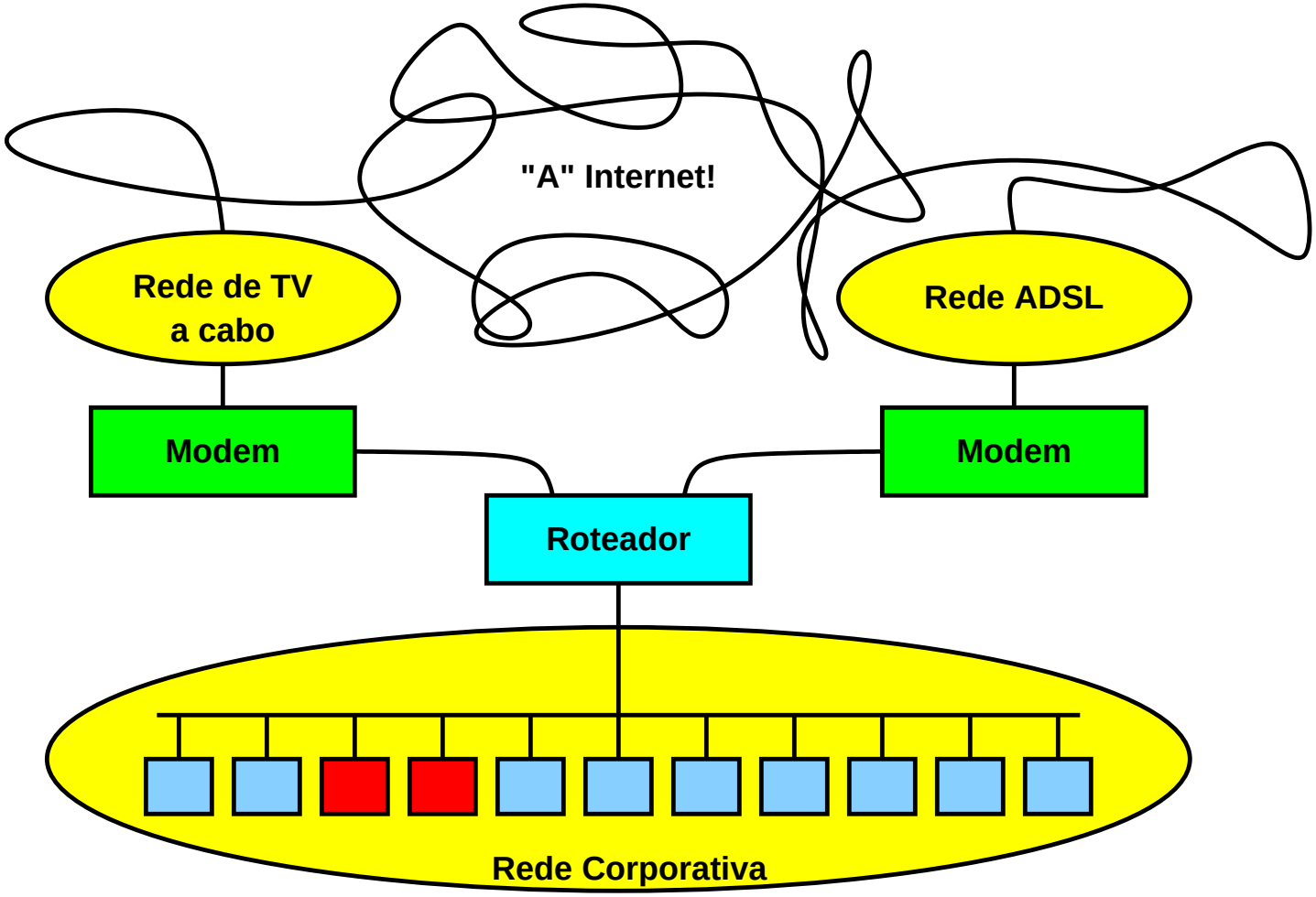
Danton Nunes, InterNexo Ltda., S.J.Campos, SP

danton.nunes@inexo.com.br

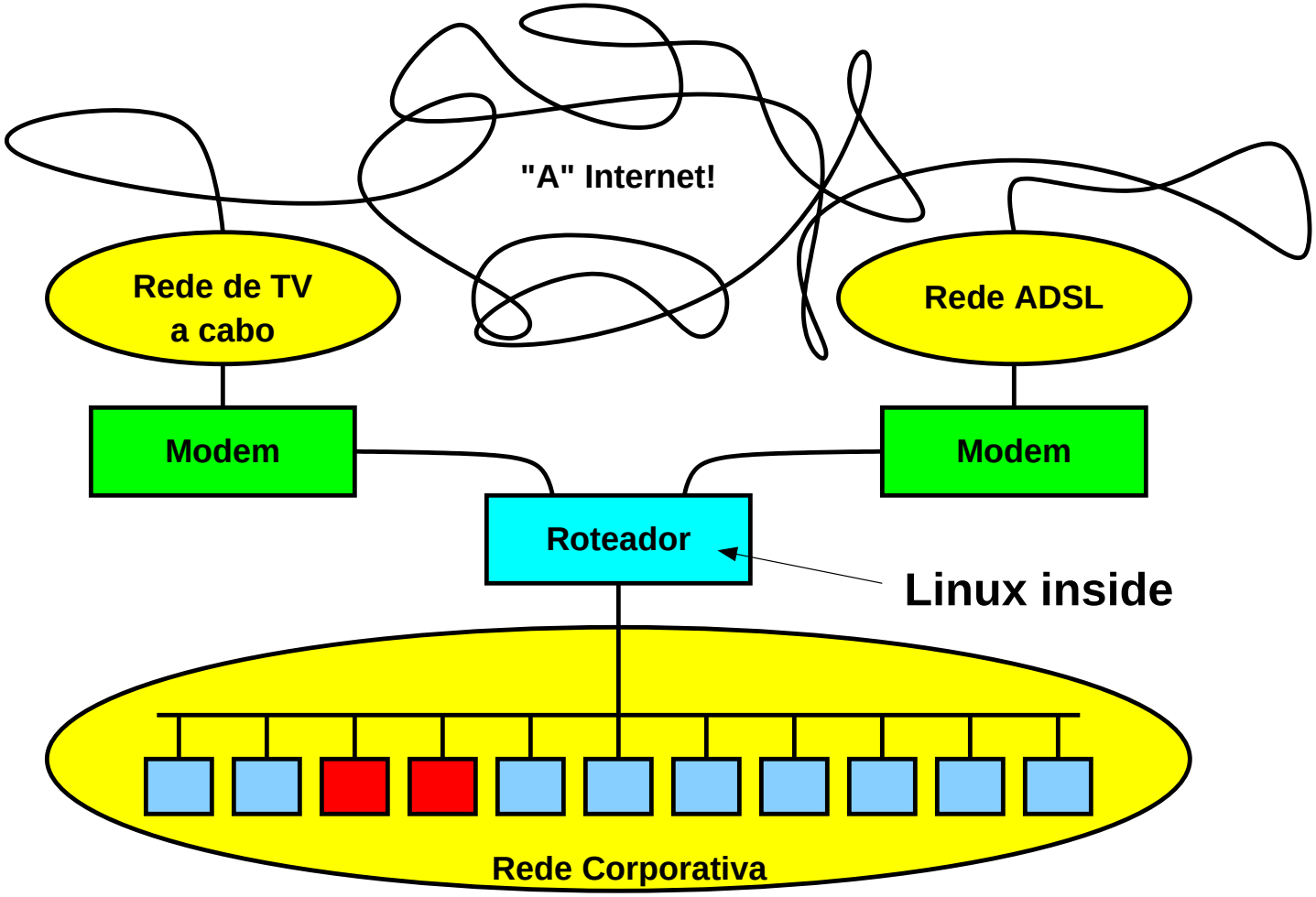
O que trataremos aqui



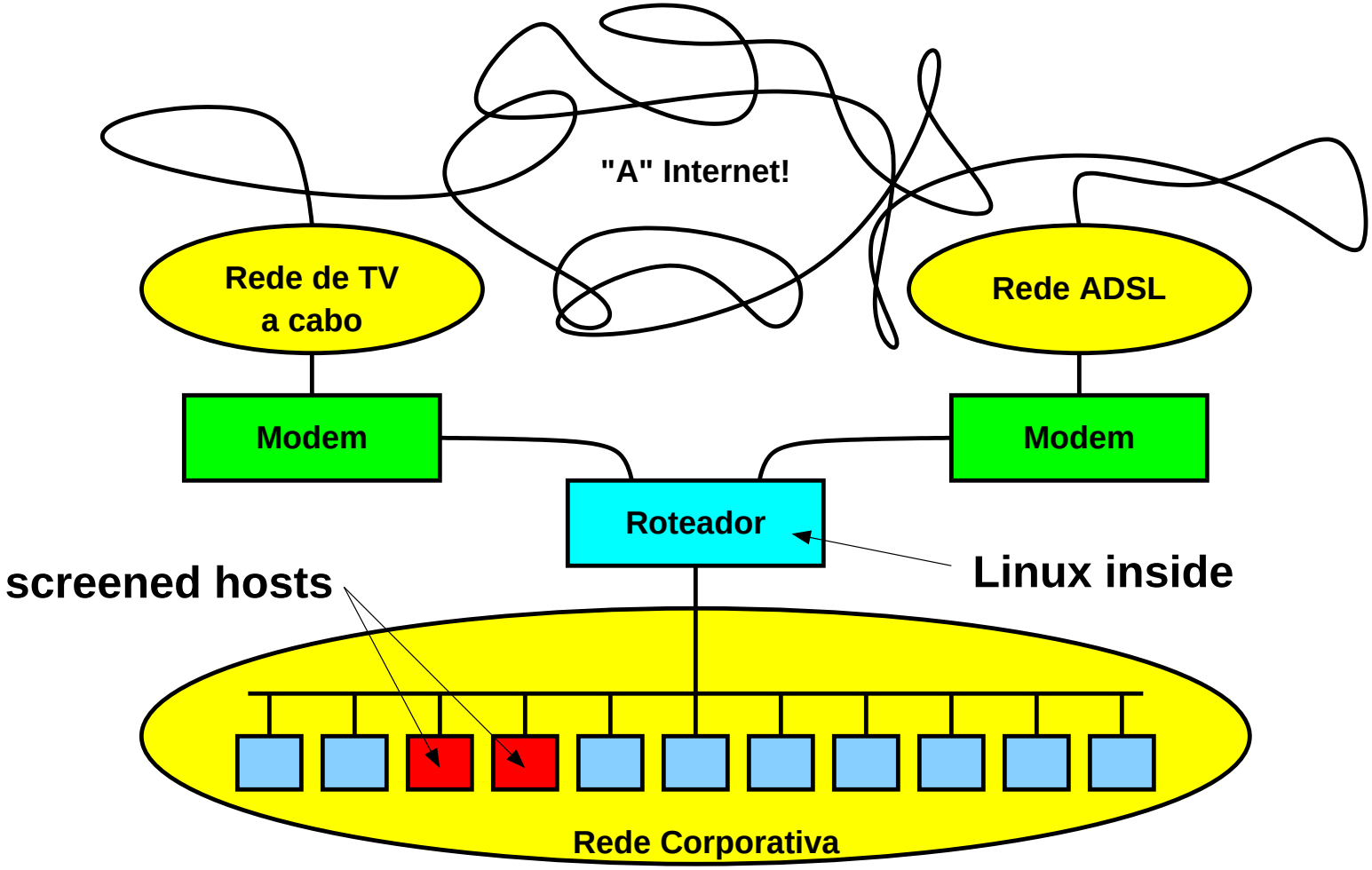
O que trataremos aqui



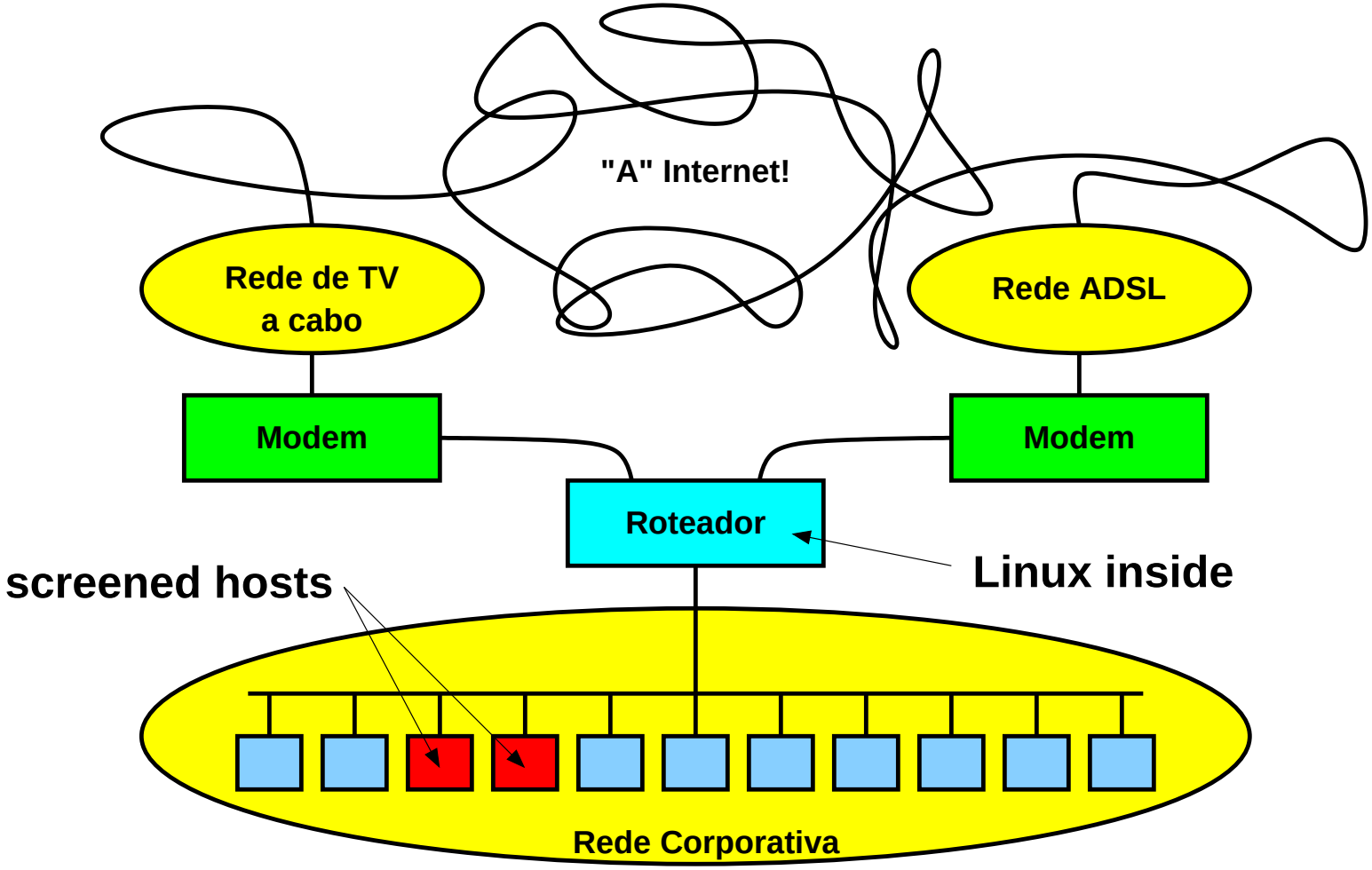
O que trataremos aqui



O que trataremos aqui



O que trataremos aqui



Rede corporativa ligada a dois provedores de acesso 'low end'.
Há 'screened hosts' dentro da rede corporativa.

O que trataremos aqui

O que trataremos aqui

- **Como disponibilizar serviços por "screened hosts" pelos dois caminhos:**
  - correio eletrônico,
  - servidor de terminais (Windows 2K3 server),
  - web corporativa (intranet).

O que trataremos aqui

- **Como disponibilizar serviços por "screened hosts" pelos dois caminhos:**
  - correio eletrônico,
  - servidor de terminais (Windows 2K3 server),
  - web corporativa (intranet).

- **Prover alguma redundância para usuários internos, dada a baixa confiabilidade individual dos dois acessos.**

O que trataremos aqui

- **Como disponibilizar serviços por "screened hosts" pelos dois caminhos:**
  - correio eletrônico,
  - servidor de terminais (Windows 2K3 server),
  - web corporativa (intranet).

- **Prover alguma redundância para usuários internos, dada a baixa confiabilidade individual dos dois acessos.**

O que NÃO trataremos aqui

O que trataremos aqui

- **Como disponibilizar serviços por "screened hosts" pelos dois caminhos:**
  - correio eletrônico,
  - servidor de terminais (Windows 2K3 server),
  - web corporativa (intranet).

- **Prover alguma redundância para usuários internos, dada a baixa confiabilidade individual dos dois acessos.**

O que NÃO trataremos aqui

- **Truques baseados em DNS,**

O que trataremos aqui

- **Como disponibilizar serviços por "screened hosts" pelos dois caminhos:**
  - correio eletrônico,
  - servidor de terminais (Windows 2K3 server),
  - web corporativa (intranet).

- **Prover alguma redundância para usuários internos, dada a baixa confiabilidade individual dos dois acessos.**

O que NÃO trataremos aqui

- **Truques baseados em DNS,**

- **Roteamento dinâmico.**

Usando as duas saídas ao mesmo tempo

Usando as duas saídas ao mesmo tempo

» Duas rotas default de acordo com o endereço IP de origem

Usando as duas saídas ao mesmo tempo

» Duas rotas default de acordo com o endereço IP de origem

» Implementado por meio de iproute2 no Linux:

```
/sbin/ip rule add from 201.6.122.4 lookup 1
/sbin/ip rule add from 200.161.131.85 lookup 2
```

Usando as duas saídas ao mesmo tempo

» Duas rotas default de acordo com o endereço IP de origem

» Implementado por meio de iproute2 no Linux:

```
/sbin/ip rule add from 201.6.122.4 lookup 1
/sbin/ip rule add from 200.161.131.85 lookup 2
/sbin/ip route add default via 201.6.122.1 src 201.6.122.4 table 1
/sbin/ip route add default via 200.161.131.65 src 200.161.131.85 table 2
```

Usando as duas saídas ao mesmo tempo

» Duas rotas default de acordo com o endereço IP de origem

» Implementado por meio de iproute2 no Linux:

```
/sbin/ip rule add from 201.6.122.4 lookup 1
/sbin/ip rule add from 200.161.131.85 lookup 2
/sbin/ip route add default via 201.6.122.1 src 201.6.122.4 table 1
/sbin/ip route add default via 200.161.131.65 src 200.161.131.85 table 2
```

Com isto garantimos que todo pacote dirigido ao endereço de uma interface será respondido por essa mesma interface.

Usando as duas saídas ao mesmo tempo

» Duas rotas default de acordo com o endereço IP de origem

» Implementado por meio de iproute2 no Linux:

```
/sbin/ip rule add from 201.6.122.4 lookup 1
/sbin/ip rule add from 200.161.131.85 lookup 2
/sbin/ip route add default via 201.6.122.1 src 201.6.122.4 table 1
/sbin/ip route add default via 200.161.131.65 src 200.161.131.85 table 2
```

Com isto garantimos que todo pacote dirigido ao endereço de uma interface será respondido por essa mesma interface.

O problema é que isto vale para servidores rodando no próprio roteador, mas nos interessa os que estão rodando nos "screened hosts".

Serviços prestados por "screened hosts"

Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

```
/sbin/iptables -A PREROUTING -i eth1 -p tcp -m tcp --dport 25
    -j DNAT --to-destination 10.1.1.50:25
```

Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

```
/sbin/iptables -A PREROUTING -i eth1 -p tcp -m tcp --dport 25
    -j DNAT --to-destination 10.1.1.50:25
```

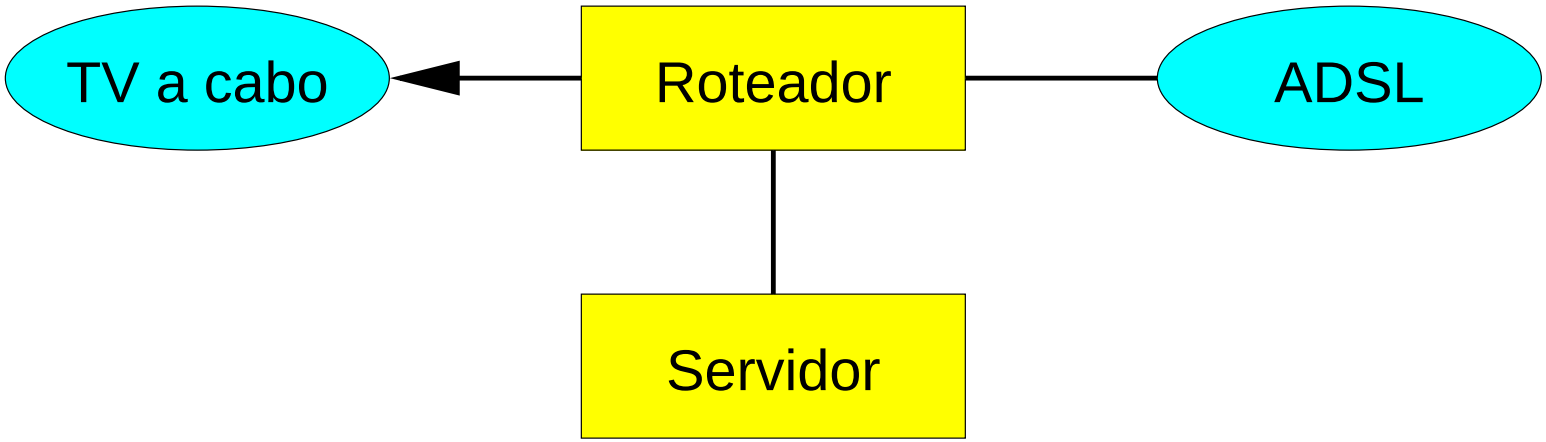
Com os dois acessos o artifício do DNAT só pode ser usado em um dos caminhos (o que tem a rota "default") senão não há caminho de volta para pacotes vindos do outro caminho.

Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

```
/sbin/iptables -A PREROUTING -i eth1 -p tcp -m tcp --dport 25
    -j DNAT --to-destination 10.1.1.50:25
```

Com os dois acessos o artifício do DNAT só pode ser usado em um dos caminhos (o que tem a rota "default") senão não há caminho de volta para pacotes vindos do outro caminho.

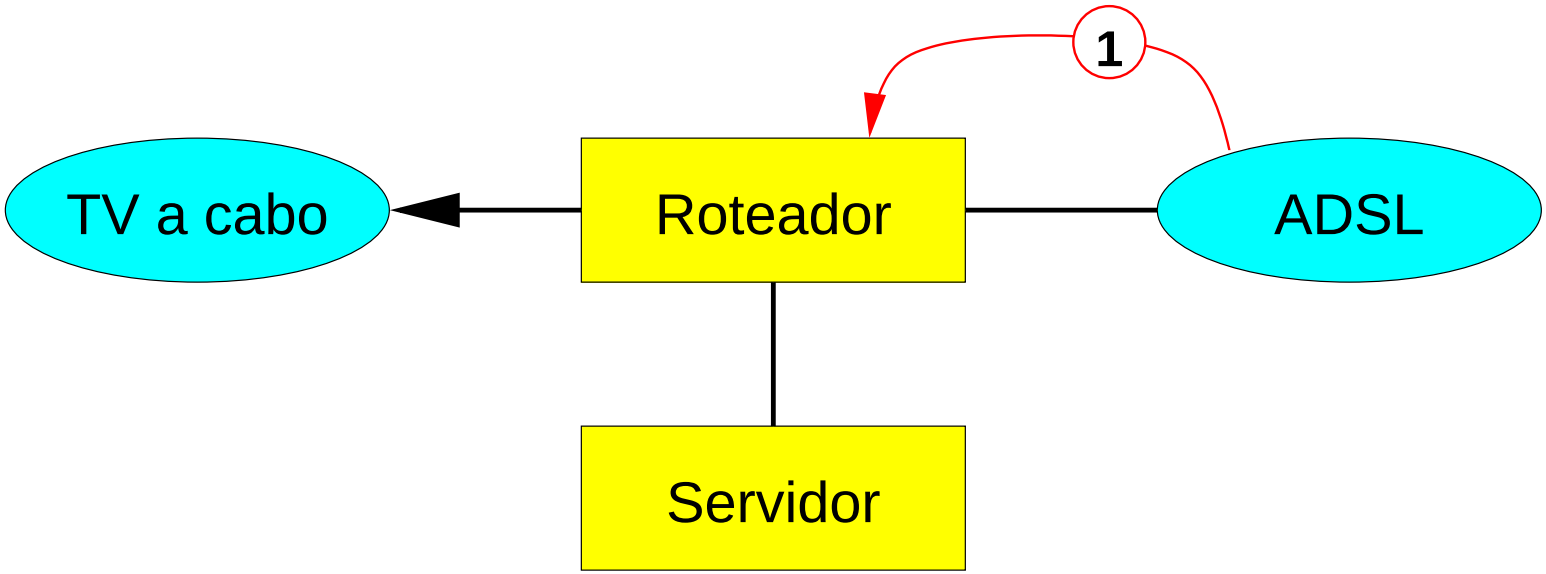


Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

```
/sbin/iptables -A PREROUTING -i eth1 -p tcp -m tcp --dport 25
    -j DNAT --to-destination 10.1.1.50:25
```

Com os dois acessos o artifício do DNAT só pode ser usado em um dos caminhos (o que tem a rota "default") senão não há caminho de volta para pacotes vindos do outro caminho.

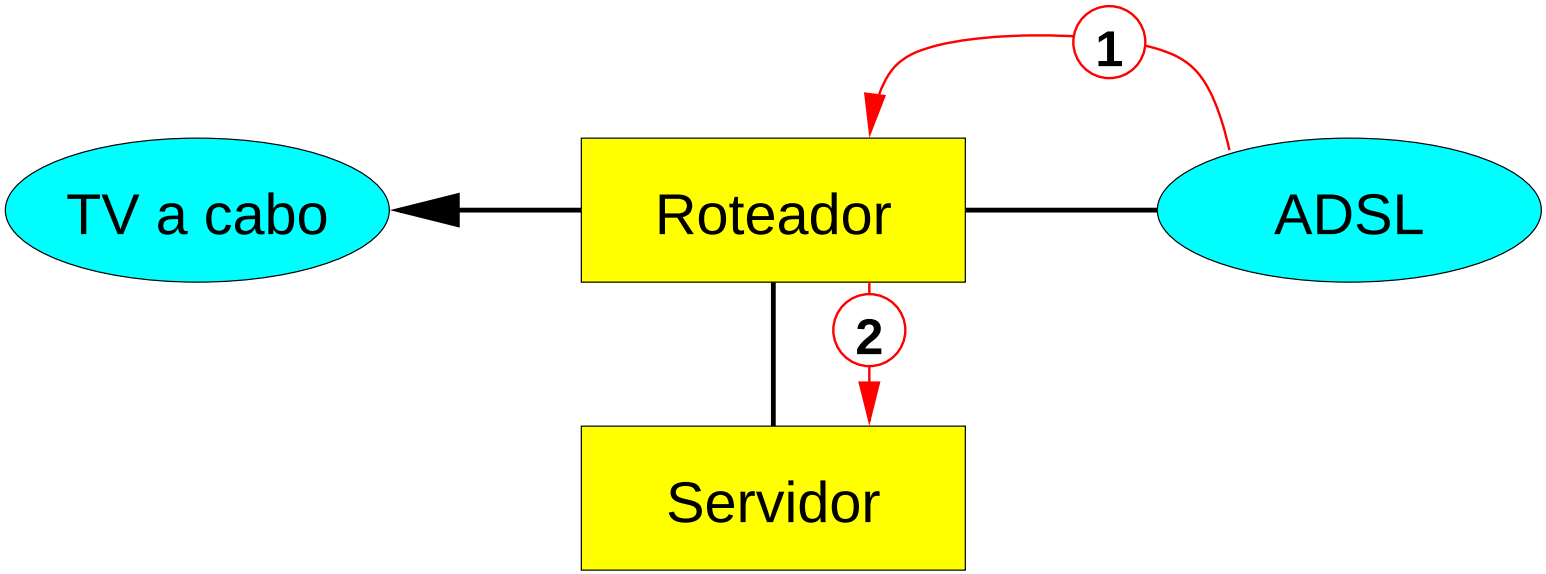


Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

```
/sbin/iptables -A PREROUTING -i eth1 -p tcp -m tcp --dport 25
    -j DNAT --to-destination 10.1.1.50:25
```

Com os dois acessos o artifício do DNAT só pode ser usado em um dos caminhos (o que tem a rota "default") senão não há caminho de volta para pacotes vindos do outro caminho.

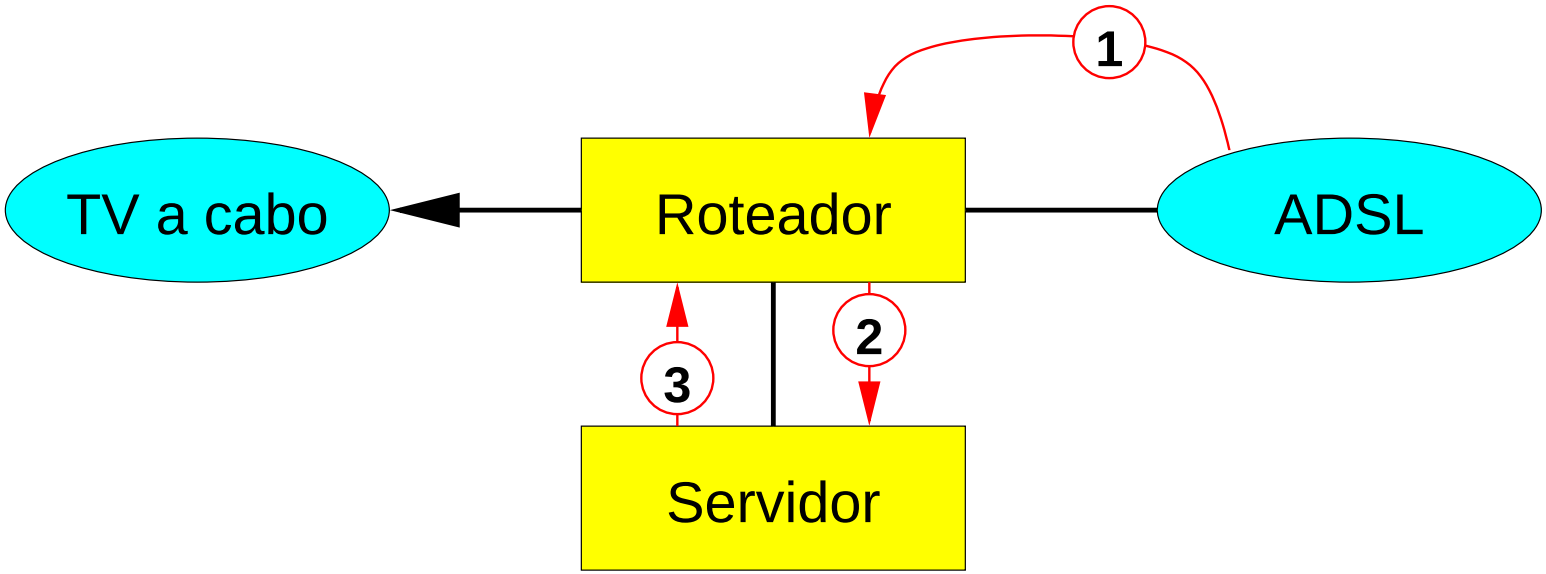


Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

```
/sbin/iptables -A PREROUTING -i eth1 -p tcp -m tcp --dport 25
    -j DNAT --to-destination 10.1.1.50:25
```

Com os dois acessos o artifício do DNAT só pode ser usado em um dos caminhos (o que tem a rota "default") senão não há caminho de volta para pacotes vindos do outro caminho.

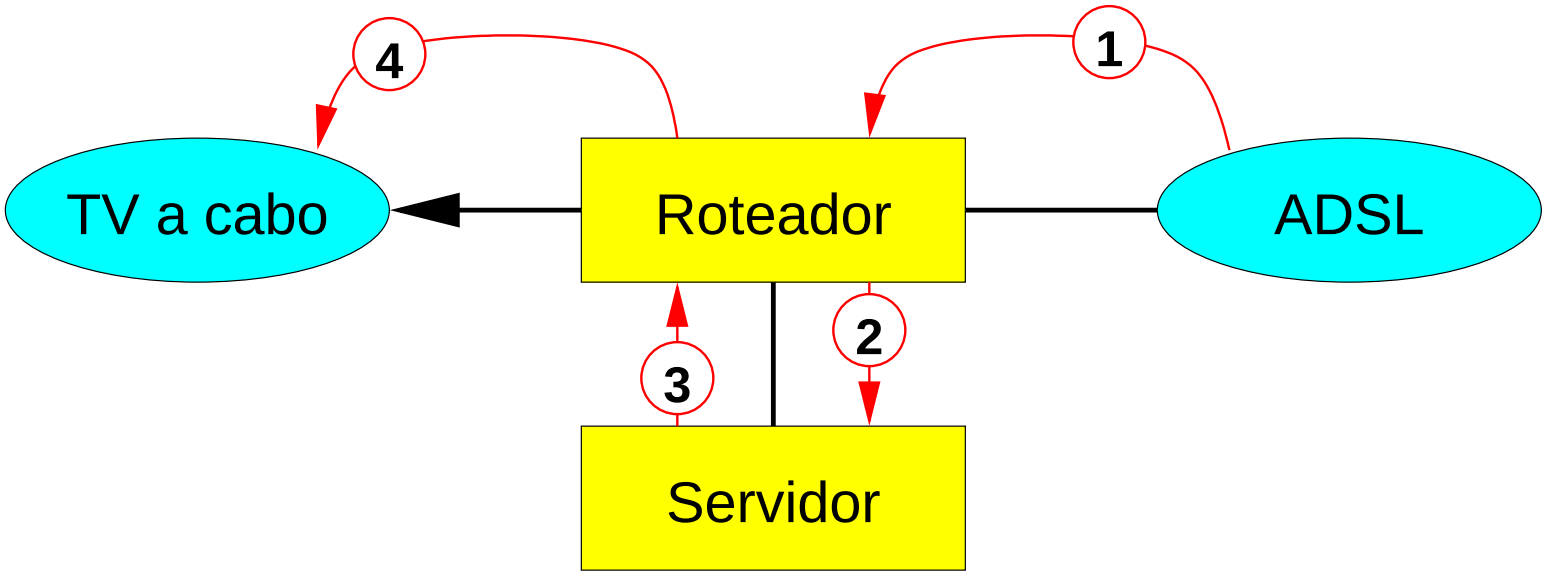


Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

```
/sbin/iptables -A PREROUTING -i eth1 -p tcp -m tcp --dport 25
    -j DNAT --to-destination 10.1.1.50:25
```

Com os dois acessos o artifício do DNAT só pode ser usado em um dos caminhos (o que tem a rota "default") senão não há caminho de volta para pacotes vindos do outro caminho.

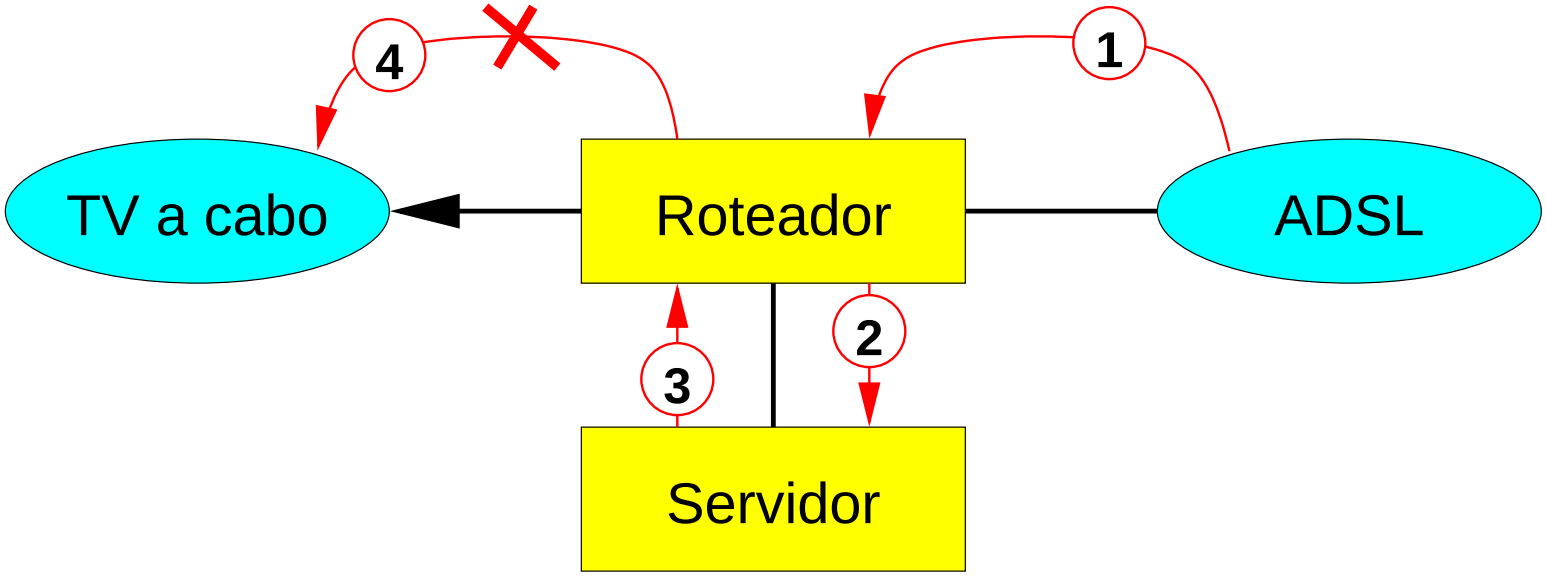


Serviços prestados por "screened hosts"

Quando havia apenas um caminho para a Internet isso era resolvido por NAT no roteador, p.ex.:

```
/sbin/iptables -A PREROUTING -i eth1 -p tcp -m tcp --dport 25
    -j DNAT --to-destination 10.1.1.50:25
```

Com os dois acessos o artifício do DNAT só pode ser usado em um dos caminhos (o que tem a rota "default") senão não há caminho de volta para pacotes vindos do outro caminho.



Solução encontrada: procurador (proxy) de aplicação

Solução encontrada: procurador (proxy) de aplicação

» Solução por NAT é possível mas pouco prática pois implica em atribuir dois endereços a cada um dos "screened hosts".

Solução encontrada: procurador (proxy) de aplicação

» Solução por NAT é possível mas pouco prática pois implica em atribuir dois endereços a cada um dos "screened hosts".

» Saída sem alterar qualquer configuração dos servidores internos: proxies de aplicação. O servidor interno "conversa" com o roteador e este com a Internet.

Solução encontrada: procurador (proxy) de aplicação

» Solução por NAT é possível mas pouco prática pois implica em atribuir dois endereços a cada um dos "screened hosts".

» Saída sem alterar qualquer configuração dos servidores internos: proxies de aplicação. O servidor interno "conversa" com o roteador e este com a Internet.

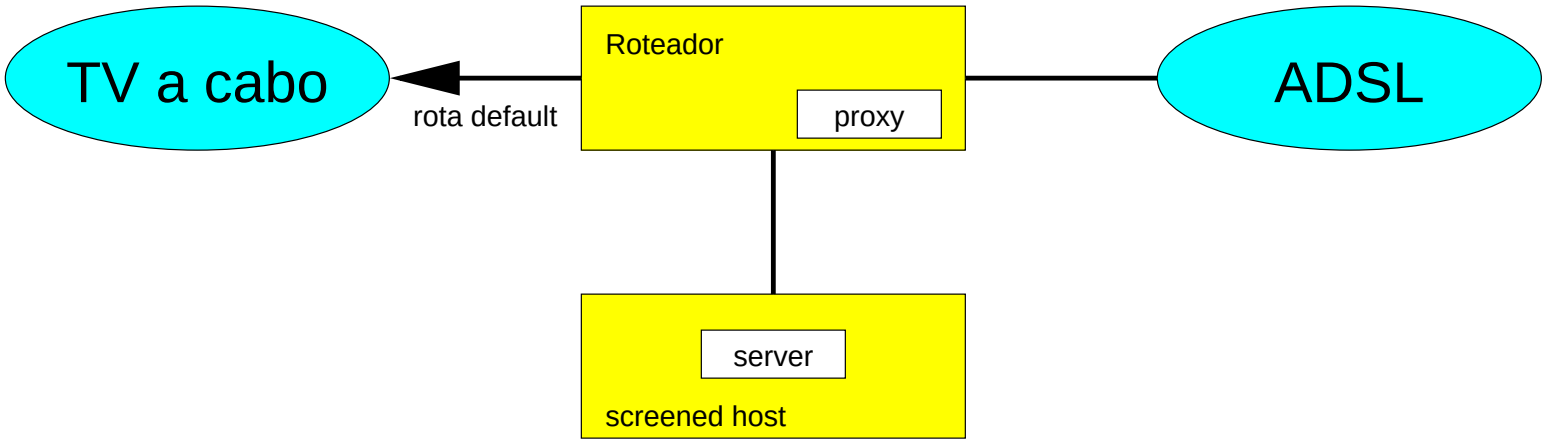
Graças ao iproute2 a resposta vai para o lado certo!

Solução encontrada: procurador (proxy) de aplicação

» Solução por NAT é possível mas pouco prática pois implica em atribuir dois endereços a cada um dos "screened hosts".

» Saída sem alterar qualquer configuração dos servidores internos: proxies de aplicação. O servidor interno "conversa" com o roteador e este com a Internet.

Graças ao iproute2 a resposta vai para o lado certo!

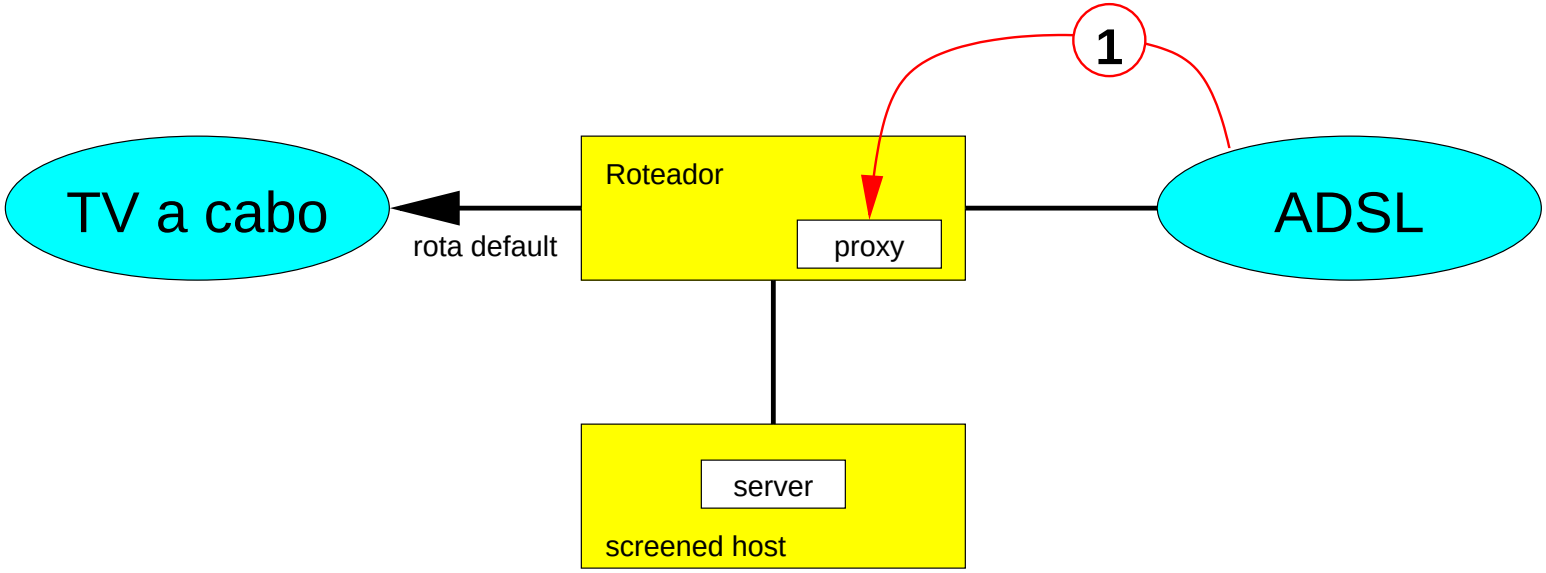


Solução encontrada: procurador (proxy) de aplicação

» Solução por NAT é possível mas pouco prática pois implica em atribuir dois endereços a cada um dos "screened hosts".

» Saída sem alterar qualquer configuração dos servidores internos: proxies de aplicação. O servidor interno "conversa" com o roteador e este com a Internet.

Graças ao iproute2 a resposta vai para o lado certo!

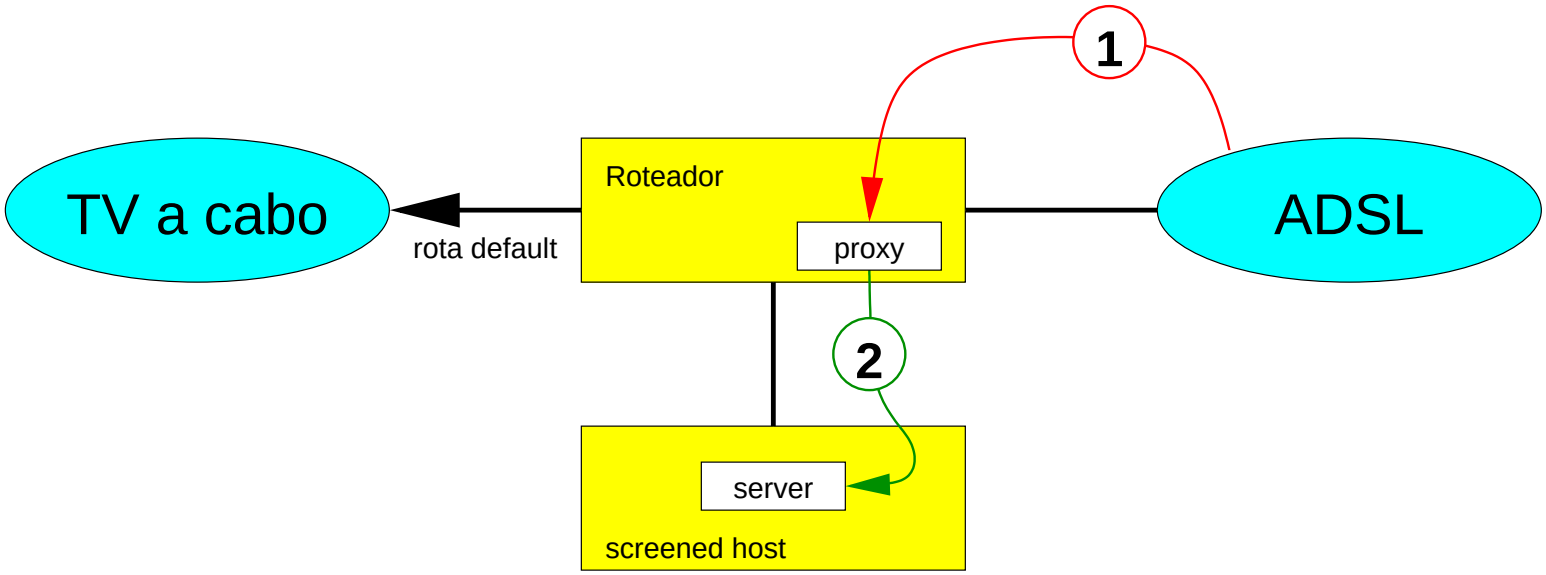


Solução encontrada: procurador (proxy) de aplicação

» Solução por NAT é possível mas pouco prática pois implica em atribuir dois endereços a cada um dos "screened hosts".

» Saída sem alterar qualquer configuração dos servidores internos: proxies de aplicação. O servidor interno "conversa" com o roteador e este com a Internet.

Graças ao iproute2 a resposta vai para o lado certo!

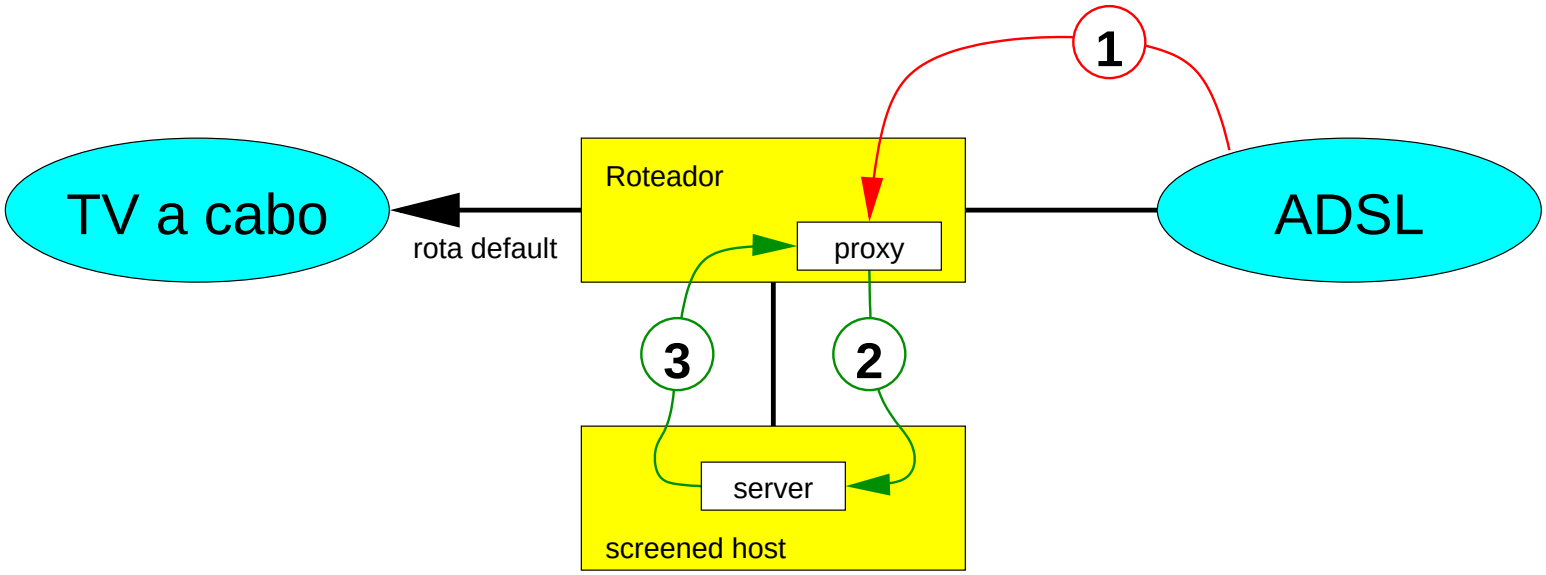


Solução encontrada: procurador (proxy) de aplicação

» Solução por NAT é possível mas pouco prática pois implica em atribuir dois endereços a cada um dos "screened hosts".

» Saída sem alterar qualquer configuração dos servidores internos: proxies de aplicação. O servidor interno "conversa" com o roteador e este com a Internet.

Graças ao iproute2 a resposta vai para o lado certo!

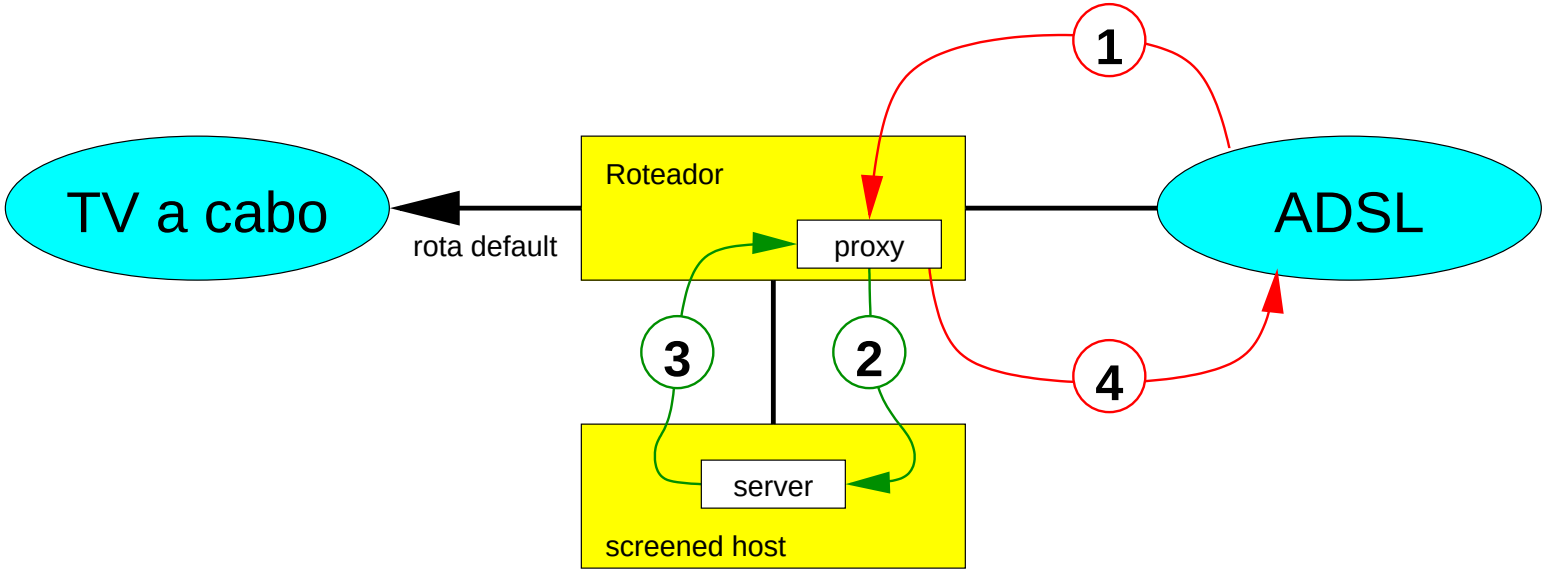


Solução encontrada: procurador (proxy) de aplicação

» Solução por NAT é possível mas pouco prática pois implica em atribuir dois endereços a cada um dos "screened hosts".

» Saída sem alterar qualquer configuração dos servidores internos: proxies de aplicação. O servidor interno "conversa" com o roteador e este com a Internet.

Graças ao iproute2 a resposta vai para o lado certo!



Primitivo mas eficiente: netpipes como proxy de aplicação!

Primitivo mas eficiente: netpipes como proxy de aplicação!

netpipes implementa algo parecido com "named pipes" através da rede e é formado por dois programas:

- **"hose" (mangueira): o lado cliente, que se conecta ao**
- **"faucet" (torneira): o lado servidor.**

Primitivo mas eficiente: netpipes como proxy de aplicação!

netpipes implementa algo parecido com "named pipes" através da rede e é formado por dois programas:

- **"hose" (mangueira): o lado cliente, que se conecta ao**
- **"faucet" (torneira): o lado servidor.**

"hose" tem um modo de operação que lembra um "telnet" primitivo, servindo como cliente genérico de TCP que lançado pelo (x)inetd é exatamente do que precisamos!

Primitivo mas eficiente: netpipes como proxy de aplicação!

netpipes implementa algo parecido com "named pipes" através da rede e é formado por dois programas:

- **"hose" (mangueira): o lado cliente, que se conecta ao**
- **"faucet" (torneira): o lado servidor.**

"hose" tem um modo de operação que lembra um "telnet" primitivo, servindo como cliente genérico de TCP que lançado pelo (x)inetd é exatamente do que precisamos!

Exemplo de configuração do xinetd:

Primitivo mas eficiente: netpipes como proxy de aplicação!

netpipes implementa algo parecido com "named pipes" através da rede e é formado por dois programas:

- "hose" (mangueira): o lado cliente, que se conecta ao
- "faucet" (torneira): o lado servidor.

"hose" tem um modo de operação que lembra um "telnet" primitivo, servindo como cliente genérico de TCP que lançado pelo (x)inetd é exatamente do que precisamos!

Exemplo de configuração do xinetd:

```
service http
{
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/local/bin/hose
        server_args     = xchange http --netslave
        log_on_failure  += USERID
        disable         = no
}
```

Parece bom, porém...

Parece bom, porém...

Há protocolos que quebram a ortogonalidade de camadas e tem seu comportamento no nível de processo alterado em função do que acontece no nível de (inter)redes. Notadamente os mecanis−mos anti−spam do correio eletrônico sofrem desse mal:

Parece bom, porém...

Há protocolos que quebram a ortogonalidade de camadas e tem seu comportamento no nível de processo alterado em função do que acontece no nível de (inter)redes. Notadamente os mecanis−mos anti−spam do correio eletrônico sofrem desse mal:

- **» SPF associa endereços IP de remententes com o que é declarado no envelope da mensagem.**

Parece bom, porém...

Há protocolos que quebram a ortogonalidade de camadas e tem seu comportamento no nível de processo alterado em função do que acontece no nível de (inter)redes. Notadamente os mecanis−mos anti−spam do correio eletrônico sofrem desse mal:

- **» SPF associa endereços IP de remententes com o que é declarado no envelope da mensagem.**
- **» Normalmene os endereços da rede interna são declarados como confiáveis, permitindo "relay" aberto sem autenticação.**

Parece bom, porém...

Há protocolos que quebram a ortogonalidade de camadas e tem seu comportamento no nível de processo alterado em função do que acontece no nível de (inter)redes. Notadamente os mecanis−mos anti−spam do correio eletrônico sofrem desse mal:

- **» SPF associa endereços IP de remententes com o que é declarado no envelope da mensagem.**
- **» Normalmene os endereços da rede interna são declarados como confiáveis, permitindo "relay" aberto sem autenticação.**

essas quebras de ortogonalidade tem efeitos desastrosos mesmo se o servidor de correio eletrônico for prefeitamente configurado!

Parece bom, porém...

Há protocolos que quebram a ortogonalidade de camadas e tem seu comportamento no nível de processo alterado em função do que acontece no nível de (inter)redes. Notadamente os mecanis−mos anti−spam do correio eletrônico sofrem desse mal:

- **» SPF associa endereços IP de remententes com o que é declarado no envelope da mensagem.**
- **» Normalmene os endereços da rede interna são declarados como confiáveis, permitindo "relay" aberto sem autenticação.**

essas quebras de ortogonalidade tem efeitos desastrosos mesmo se o servidor de correio eletrônico for prefeitamente configurado!

- **» SPF passa a ser ignorado e a quantidade de lixo recebido aumenta.**

Parece bom, porém...

Há protocolos que quebram a ortogonalidade de camadas e tem seu comportamento no nível de processo alterado em função do que acontece no nível de (inter)redes. Notadamente os mecanis−mos anti−spam do correio eletrônico sofrem desse mal:

- **» SPF associa endereços IP de remententes com o que é declarado no envelope da mensagem.**
- **» Normalmene os endereços da rede interna são declarados como confiáveis, permitindo "relay" aberto sem autenticação.**

essas quebras de ortogonalidade tem efeitos desastrosos mesmo se o servidor de correio eletrônico for prefeitamente configurado!

- **» SPF passa a ser ignorado e a quantidade de lixo recebido aumenta.**
- **» (muito pior!) o servidor se torna um retransmissor aberto!**

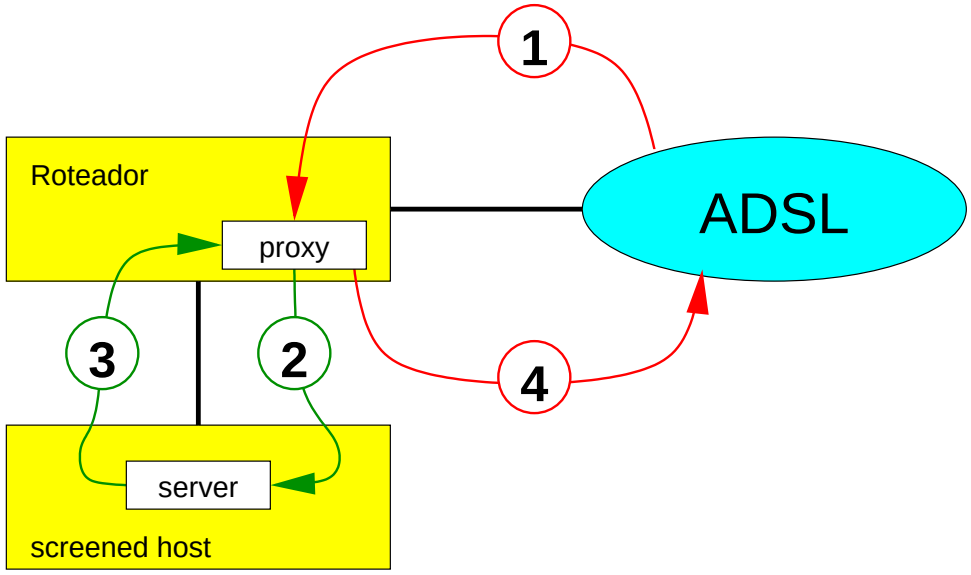
Entendendo os impactos no e−mail.

Entendendo os impactos no e−mail.

O servidor de correio recebe as conexões do proxy, com o IP interno do roteador.

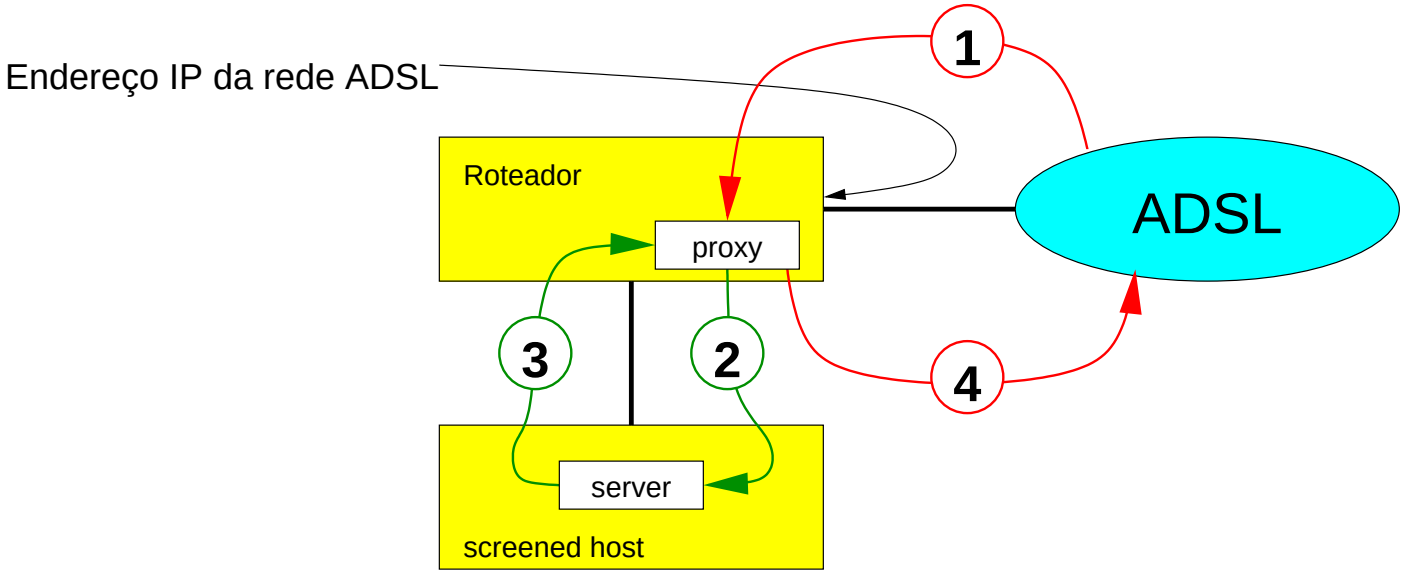
Entendendo os impactos no e−mail.

O servidor de correio recebe as conexões do proxy, com o IP interno do roteador.



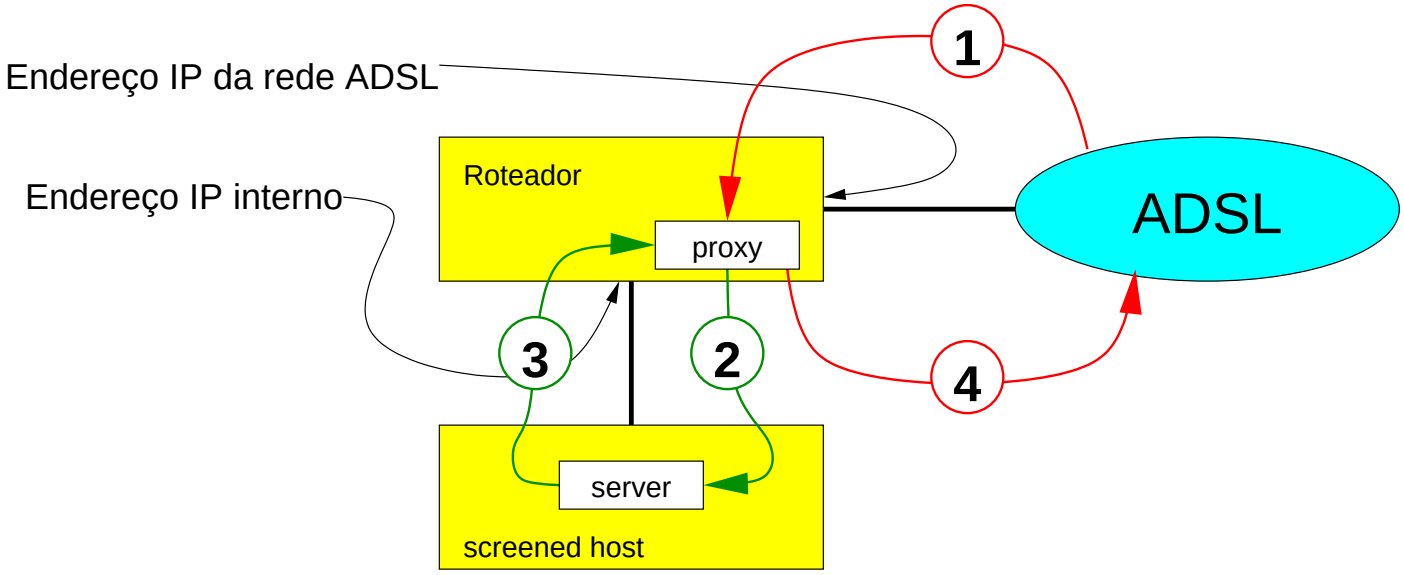
Entendendo os impactos no e−mail.

O servidor de correio recebe as conexões do proxy, com o IP interno do roteador.



Entendendo os impactos no e−mail.

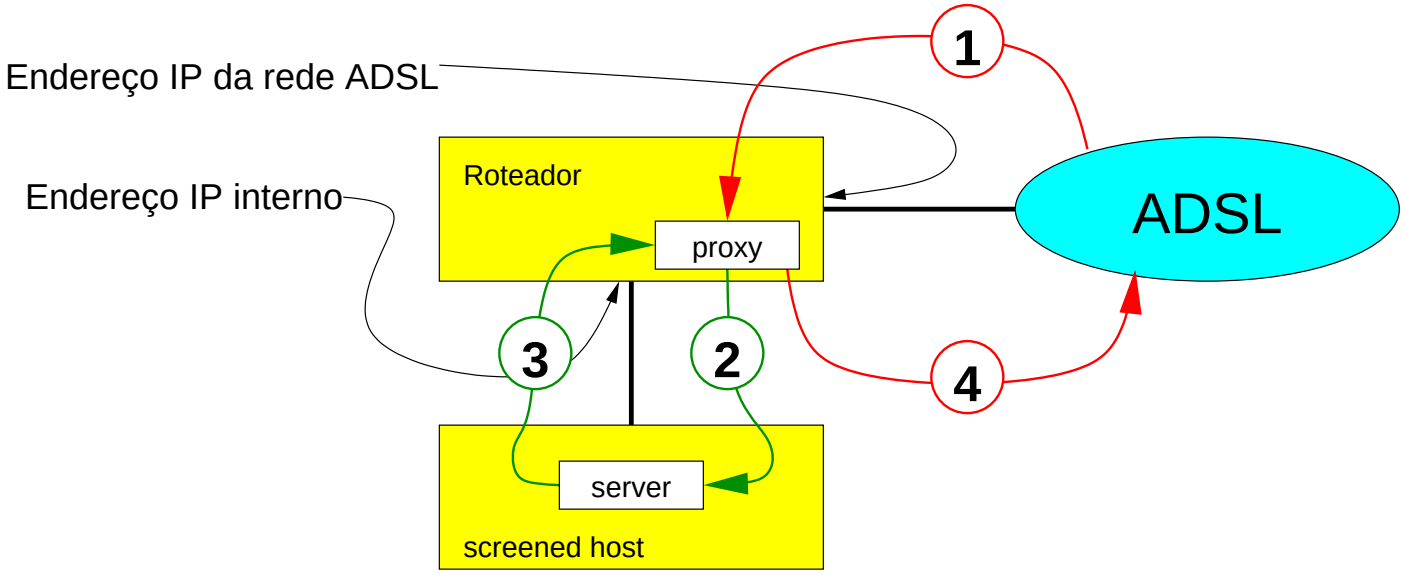
O servidor de correio recebe as conexões do proxy, com o IP interno do roteador.



Entendendo os impactos no e−mail.

O servidor de correio recebe as conexões do proxy, com o IP interno do roteador.

=> não é possível avaliar a lista de controle de acesso do SPF pois o endereço do "remetente" foi perdido; o endereço percebido é o do roteador na rede interna.

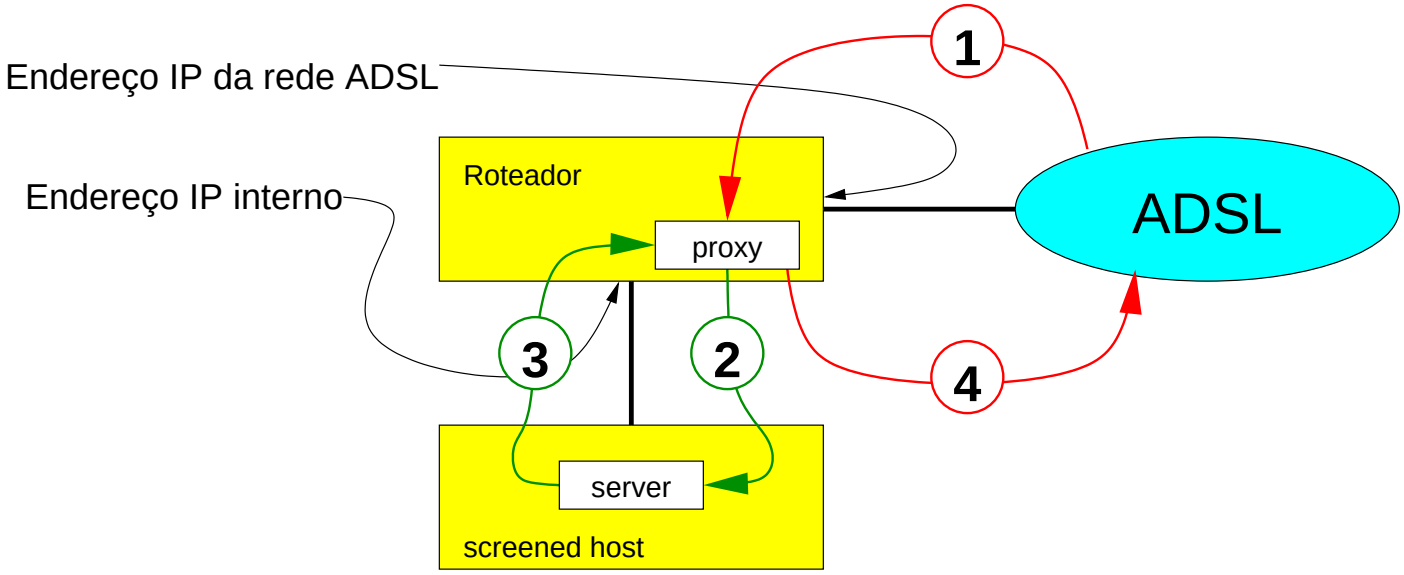


Entendendo os impactos no e−mail.

O servidor de correio recebe as conexões do proxy, com o IP interno do roteador.

=> não é possível avaliar a lista de controle de acesso do SPF pois o endereço do "remetente" foi perdido; o endereço percebido é o do roteador na rede interna.

=> como os endereços da rede interna são tratados como confiáveis, o servidor vai aceitar mensagens para qualquer lugar, passando a se comportar como um "relay" aberto!



Alternativas para contornar os problemas com e−mail.

Alternativas para contornar os problemas com e−mail.

1. **Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.**

Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.

2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.

Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.
2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.
3. Aceitar correio eletrônico por uma interface externa apenas.

Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.
2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.
3. Aceitar correio eletrônico por uma interface externa apenas.
4. Excluir o endereço do roteador da lista de confiáveis.

Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.

2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.

3. Aceitar correio eletrônico por uma interface externa apenas.

4. Excluir o endereço do roteador da lista de confiáveis.

	SPF	!Open Relay	Redundância	Simplicidade	Escolha
1					
2					
3					
4					

Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.

2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.

3. Aceitar correio eletrônico por uma interface externa apenas.

4. Excluir o endereço do roteador da lista de confiáveis.

	SPF	!Open Relay	Redundância	Simplicidade	Escolha
1					
2					
3					
4					

Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.

2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.

3. Aceitar correio eletrônico por uma interface externa apenas.

4. Excluir o endereço do roteador da lista de confiáveis.

	SPF	!Open Relay	Redundância	Simplicidade	Escolha
1					
2					
3					
4					

Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.

2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.

3. Aceitar correio eletrônico por uma interface externa apenas.

4. Excluir o endereço do roteador da lista de confiáveis.

	SPF	!Open Relay	Redundância	Simplicidade	Escolha
1					
2					
3					
4					

Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.

2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.

3. Aceitar correio eletrônico por uma interface externa apenas.

4. Excluir o endereço do roteador da lista de confiáveis.

	SPF	!Open Relay	Redundância	Simplicidade	Escolha
1					
2					
3					
4					

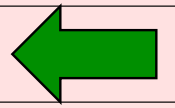
Alternativas para contornar os problemas com e−mail.

1. Voltar ao esquema de NAT, mas atribuindo dois endereços IP para o servidor de e−mail, um em correspondência a cada um dos endereços externos.

2. Processar um MTA razoavelmente bem configurado no roteador, com testes de SPF e fila próprios, isto é, um proxy mais esperto do que o feito com xinetd+hose.

3. Aceitar correio eletrônico por uma interface externa apenas.

4. Excluir o endereço do roteador da lista de confiáveis.

	SPF	!Open Relay	Redundância	Simplicidade	Escolha
1					
2					
3					
4					

Redundância fria para usuários internos

Redundância fria para usuários internos

» Os usuários internos de Web e outros serviços (ssh, ftp) usam NAT com uma única rota default.

Redundância fria para usuários internos

» Os usuários internos de Web e outros serviços (ssh, ftp) usam NAT com uma única rota default.

» Um processo testa periodicamente as duas conexões (uma saraivada de pings para os roteadores vizinhos) e comuta a rota default.

Redundância fria para usuários internos

» Os usuários internos de Web e outros serviços (ssh, ftp) usam NAT com uma única rota default.

» Um processo testa periodicamente as duas conexões (uma saraivada de pings para os roteadores vizinhos) e comuta a rota default.

Um trecho do script (Bourne shell):

Redundância fria para usuários internos

» Os usuários internos de Web e outros serviços (ssh, ftp) usam NAT com uma única rota default.

» Um processo testa periodicamente as duas conexões (uma saraivada de pings para os roteadores vizinhos) e comuta a rota default.

Um trecho do script (Bourne shell):

```
# o primário está vivo?
ping -q -c 5 ${gw1} >&/dev/null && {
 test ${defgw} = ${gw1} || {
  /sbin/ip route del ${defroute}
  /sbin/ip route add default via ${gw1} dev ${if1}
  /usr/bin/logger -p local1.warning "nova rota default: " \
    "via ${gw1} dev ${if1}"
 }
 exit
}
```

Proxy de Web

Proxy de Web

» Squid transparente (até telnet na porta 80 vai para o squid).

Proxy de Web

» Squid transparente (até telnet na porta 80 vai para o squid).

» Squid usa a rota default.

Proxy de Web

» Squid transparente (até telnet na porta 80 vai para o squid).

» Squid usa a rota default.

» Chaveamento da rota default ocorre muito rápido: o usuário regular de Web nem percebe o que está acontecendo.

Proxy de Web

» Squid transparente (até telnet na porta 80 vai para o squid).

» Squid usa a rota default.

» Chaveamento da rota default ocorre muito rápido: o usuário regular de Web nem percebe o que está acontecendo.

Proxy de outros serviços

Proxy de Web

» Squid transparente (até telnet na porta 80 vai para o squid).

» Squid usa a rota default.

» Chaveamento da rota default ocorre muito rápido: o usuário regular de Web nem percebe o que está acontecendo.

Proxy de outros serviços

» Basicamente ssh, ftp e https.

Proxy de Web

» Squid transparente (até telnet na porta 80 vai para o squid).

» Squid usa a rota default.

» Chaveamento da rota default ocorre muito rápido: o usuário regular de Web nem percebe o que está acontecendo.

Proxy de outros serviços

» Basicamente ssh, ftp e https.

» NAT convencional pela rota default.

Proxy de Web

» Squid transparente (até telnet na porta 80 vai para o squid).

» Squid usa a rota default.

» Chaveamento da rota default ocorre muito rápido: o usuário regular de Web nem percebe o que está acontecendo.

Proxy de outros serviços

» Basicamente ssh, ftp e https.

» NAT convencional pela rota default.

» Serviço interrompido ao comutar a rota default.

Conclusões

Conclusões

» **Foi implantado um esquema de acesso duplo usando dois acessos de "varejo": TV a cabo e ADSL.**

Conclusões

» Foi implantado um esquema de acesso duplo usando dois acessos de "varejo": TV a cabo e ADSL.

» O uso de "policy routing" e proxies de aplicação permitiram clientes remotos usar os dois acessos simultaneamente.

Conclusões

» Foi implantado um esquema de acesso duplo usando dois acessos de "varejo": TV a cabo e ADSL.

» O uso de "policy routing" e proxies de aplicação permitiram clientes remotos usar os dois acessos simultaneamente.

» O esquema, porém, fura em aplicações que decidem seu comportamento em função da camada de IP => e−mail!

Conclusões

» Foi implantado um esquema de acesso duplo usando dois acessos de "varejo": TV a cabo e ADSL.

» O uso de "policy routing" e proxies de aplicação permitiram clientes remotos usar os dois acessos simultaneamente.

» O esquema, porém, fura em aplicações que decidem seu comportamento em função da camada de IP => e−mail!

» Usuários da rede interna tem acesso à Web por squid em modo transparente apenas por uma das interfaces mas mal sentem as transições.

Conclusões

» Foi implantado um esquema de acesso duplo usando dois acessos de "varejo": TV a cabo e ADSL.

» O uso de "policy routing" e proxies de aplicação permitiram clientes remotos usar os dois acessos simultaneamente.

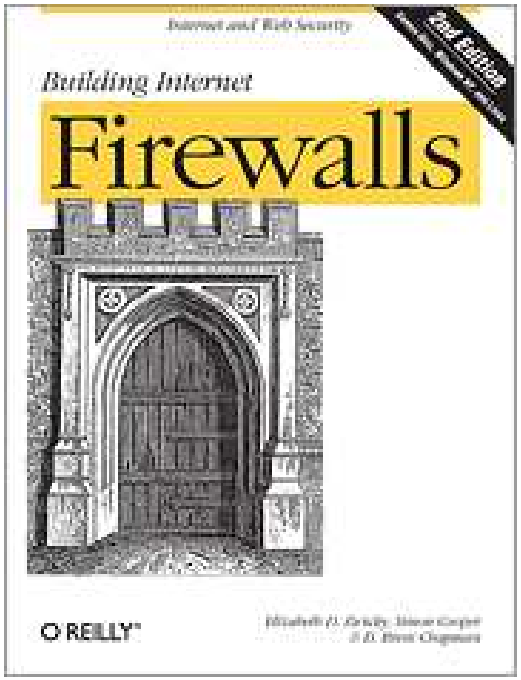
» O esquema, porém, fura em aplicações que decidem seu comportamento em função da camada de IP => e−mail!

» Usuários da rede interna tem acesso à Web por squid em modo transparente apenas por uma das interfaces mas mal sentem as transições.

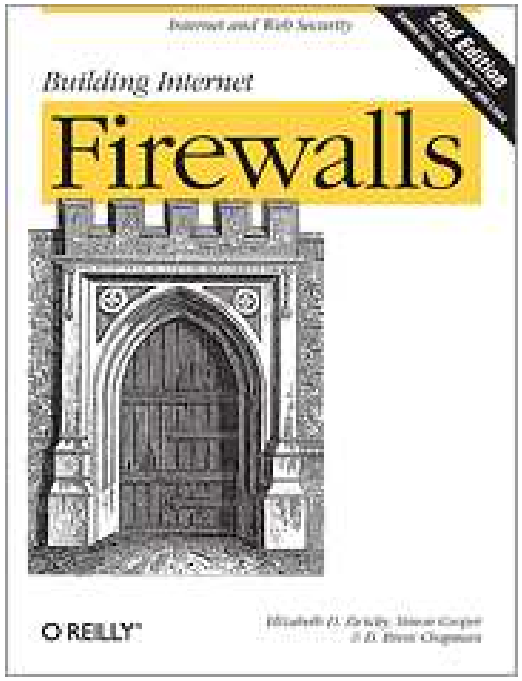
» Outros serviços encaminhados por NAT se quebram nas transições. O cliente considera fortemente simplesmente não usar NAT e rodar essas aplicações no roteador.

Referências

Referências

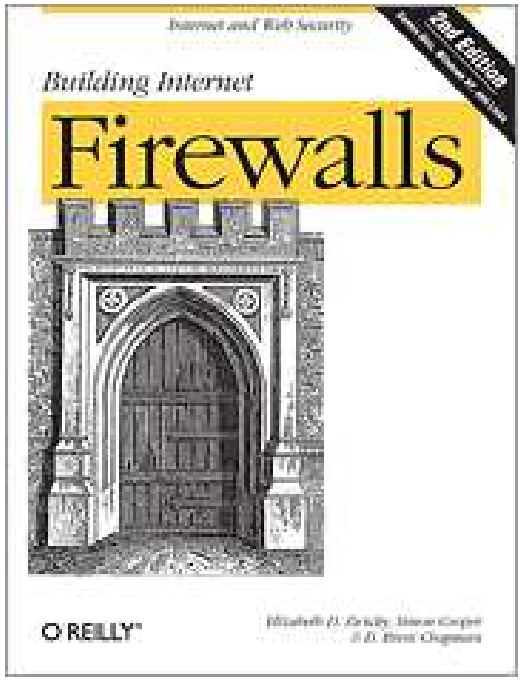


Referências



Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman
Building Internet Firewalls
ed. O'Reily

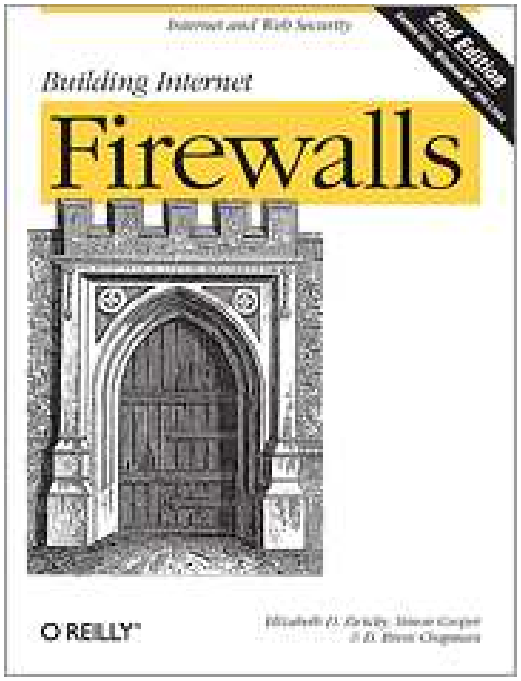
Referências



Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman
Building Internet Firewalls
ed. O'Reily

Basicamente tudo o que você queria saber sobre firewalls mas tinha medo de perguntar.

Referências

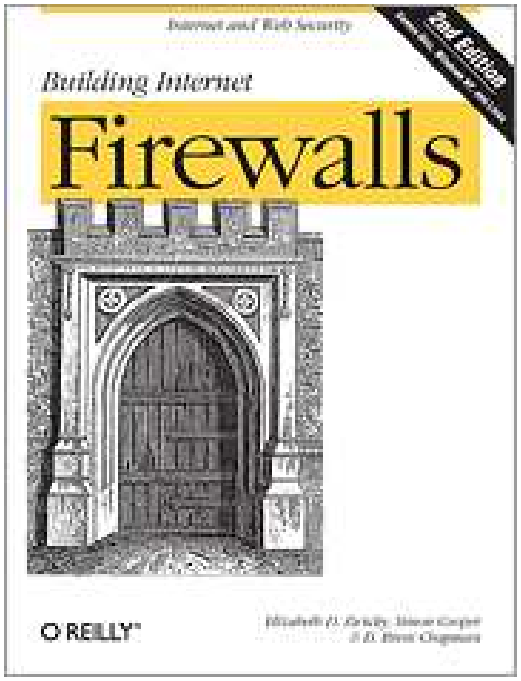


Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman
Building Internet Firewalls
ed. O'Reily

Basicamente tudo o que você queria saber sobre firewalls mas tinha medo de perguntar.

http://www.rnp.br/newsgen/0201/roteamento_linux.html
Artigo da revista da RNP sobre roteamento avançado com Linux.

Referências



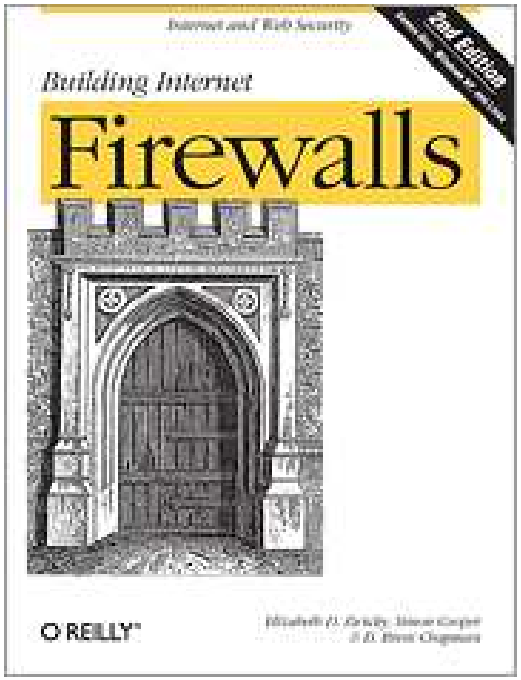
Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman
Building Internet Firewalls
ed. O'Reily

Basicamente tudo o que você queria saber sobre firewalls mas tinha medo de perguntar.

http://www.rnp.br/newsgen/0201/roteamento_linux.html
Artigo da revista da RNP sobre roteamento avançado com Linux.

http://lartc.org/howto/
Linux Advanced Routing & Traffic Control

Referências



Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman
Building Internet Firewalls
ed. O'Reily

Basicamente tudo o que você queria saber sobre firewalls mas tinha medo de perguntar.

http://www.rnp.br/newsgen/0201/roteamento_linux.html
Artigo da revista da RNP sobre roteamento avançado com Linux.

http://lartc.org/howto/
Linux Advanced Routing & Traffic Control

http://www.clintoneast.com/articles/multihomed.php
Multiple Default Gateways under Linux with iproute2