INTERNEXO

Ativando IPv6 em uma rede corporativa

Danton Nunes
danton.nunes@inexo.com.br

Ativando IPv6 em uma rede corporativa

Danton Nunes
danton.nunes@inexo.com.br

Parte 1
Roteamento

O Problema

O Problema

Rede corporativa:

O Problema

Rede corporativa:
– 12+ servidores;

O Problema

Rede corporativa:

– 12+ servidores;

– um montão de estações de trabalho

O Problema

Rede corporativa:

– 12+ servidores;

– um montão de estações de trabalho

ISP oferece um bloco /64, porém:

O Problema

Rede corporativa:
– 12+ servidores;
– um montão de estações de trabalho

ISP oferece um bloco /64, porém:
– sem delegação de prefixo

O Problema

Rede corporativa:

– 12+ servidores;

– um montão de estações de trabalho

ISP oferece um bloco /64, porém:

– sem delegação de prefixo

– sem autoconfiguração

O Problema

Rede corporativa:
- *12+ servidores;*
- *um montão de estações de trabalho*

ISP oferece um bloco /64, porém:
- *sem delegação de prefixo*
- *sem autoconfiguração*
- *sem firewall*

O Problema

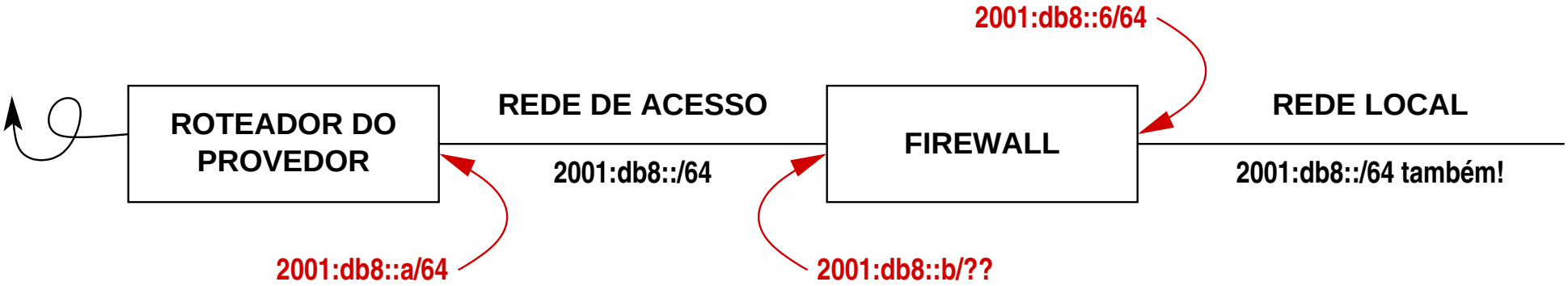
Rede corporativa:

- 12+ servidores;
- um montão de estações de trabalho

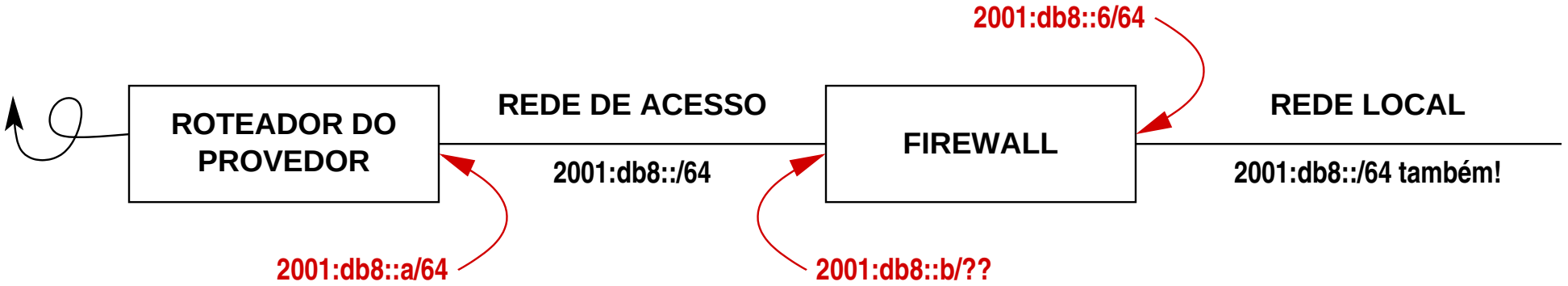
ISP oferece um bloco /64, porém:

- sem delegação de prefixo
- sem autoconfigura
- sem firewall

O Problema

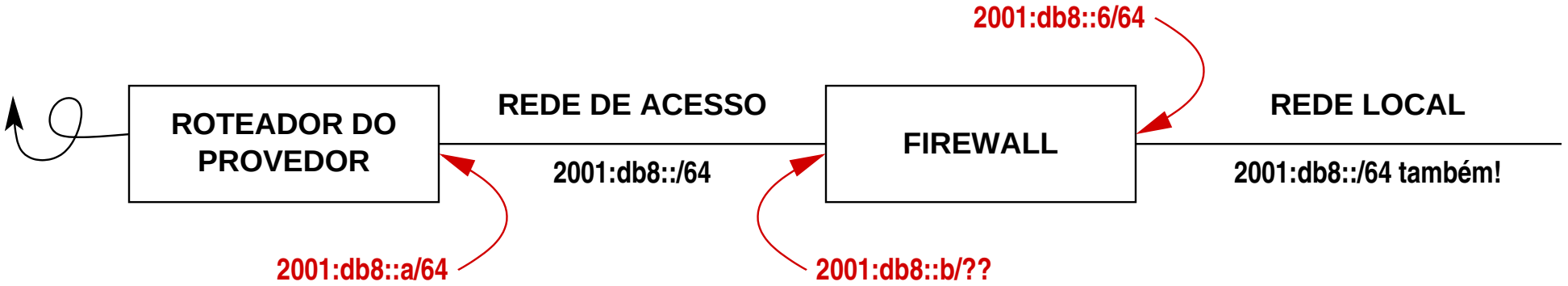

2001:db8::6/64
ROTEADOR DO PROVEDOR
REDE DE ACESSO
2001:db8::/64
FIREWALL
REDE LOCAL
2001:db8::/64 também!
2001:db8::a/64
2001:db8::b/??

O Problema



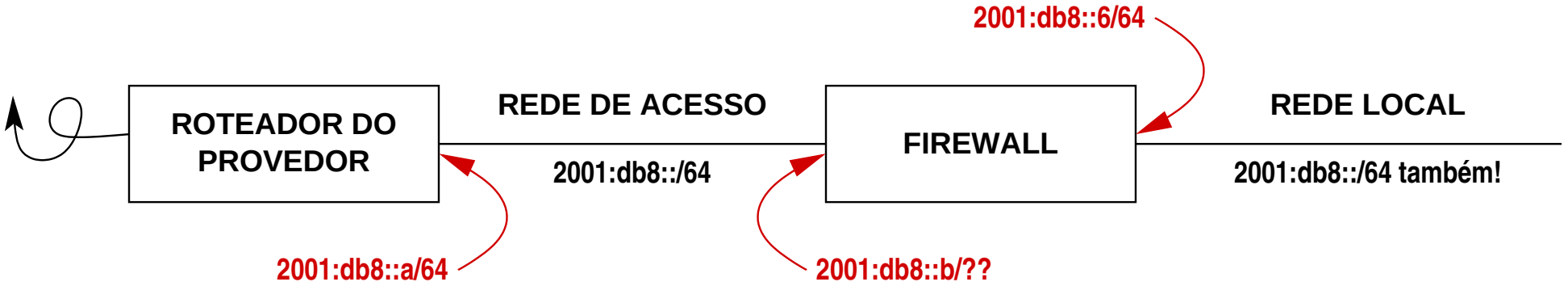
Um dia na vida de um pacote

O Problema



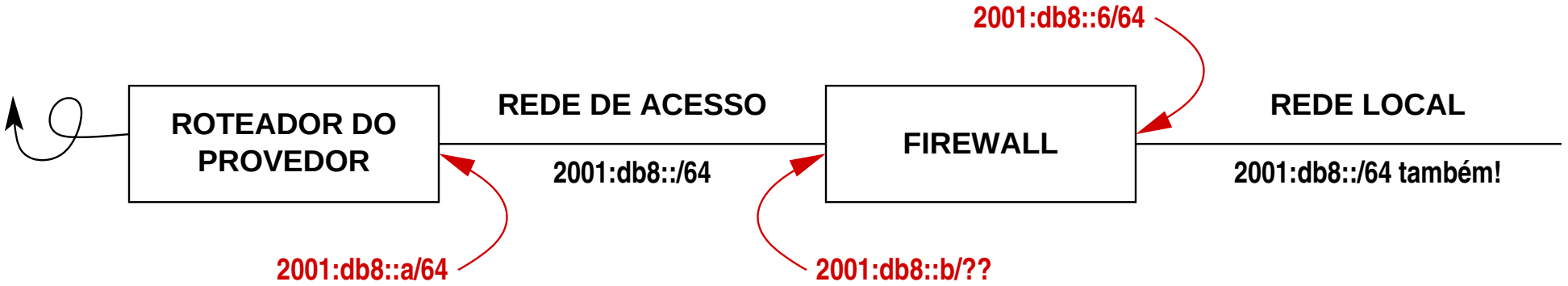
Um dia na vida de um pacote

O Problema



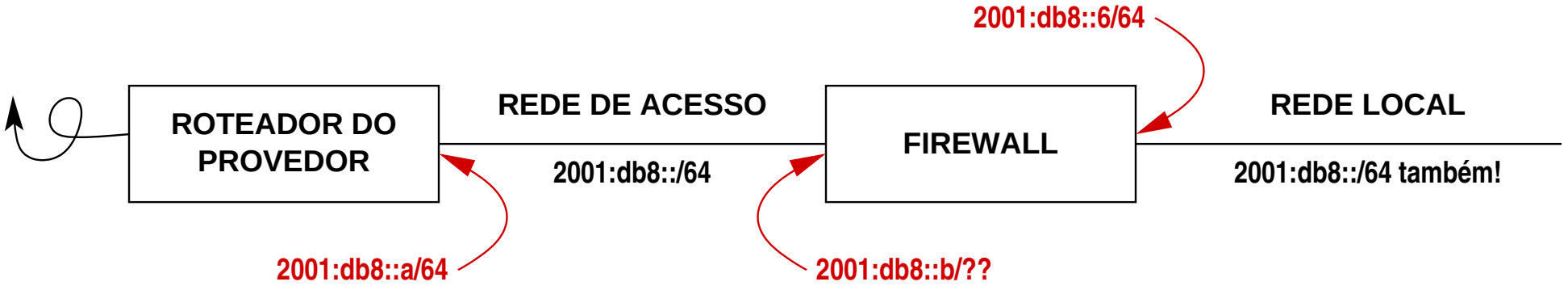
Um dia na vida de um pacote

O Problema

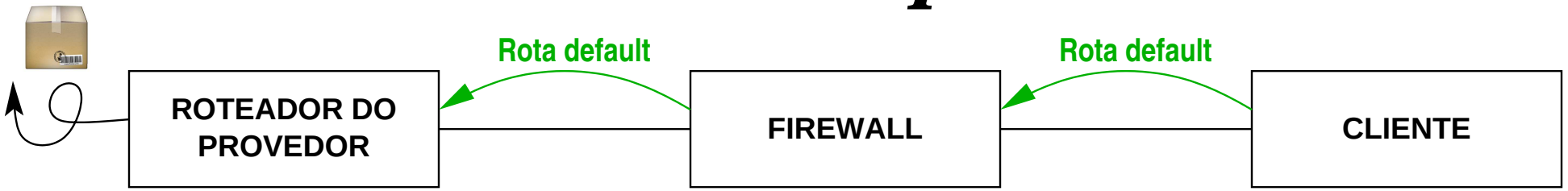


Um dia na vida de um pacote

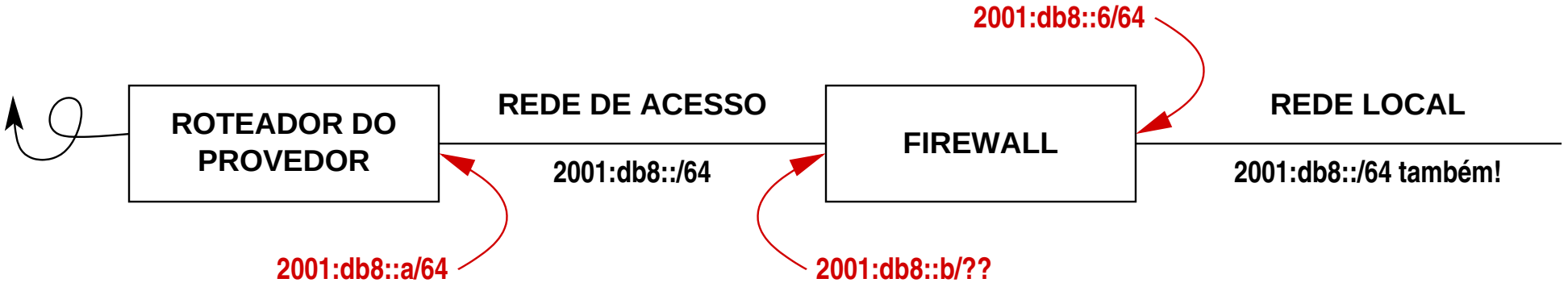
O Problema



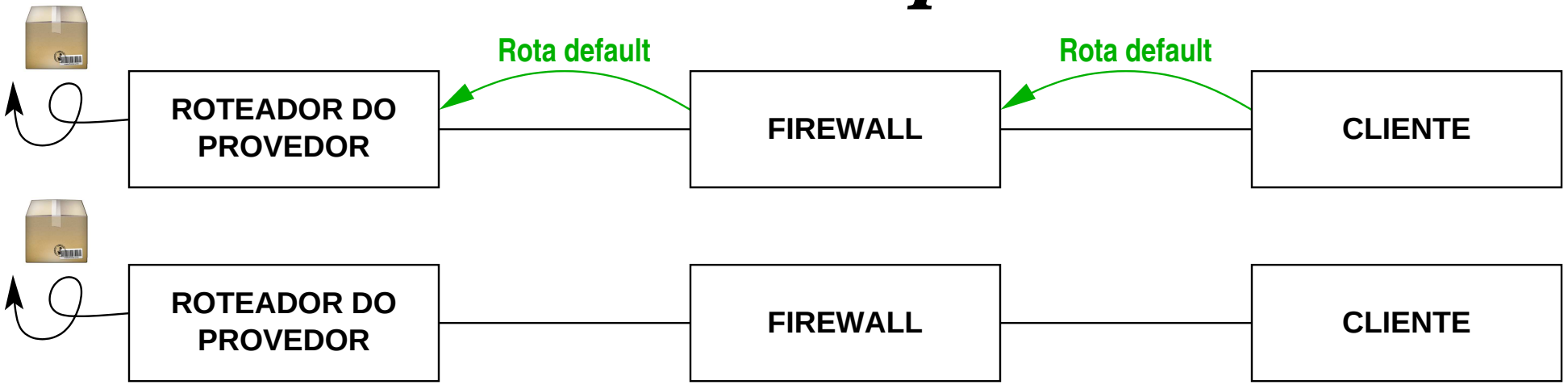
Um dia na vida de um pacote



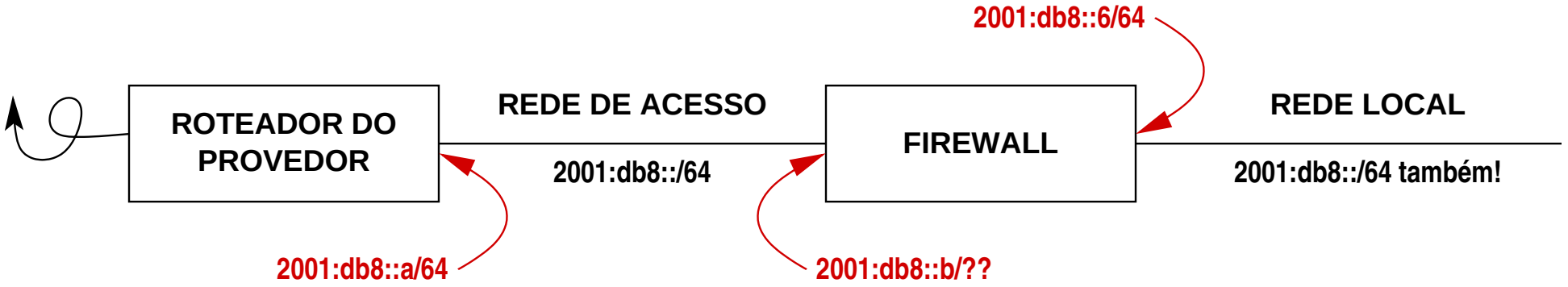
O Problema



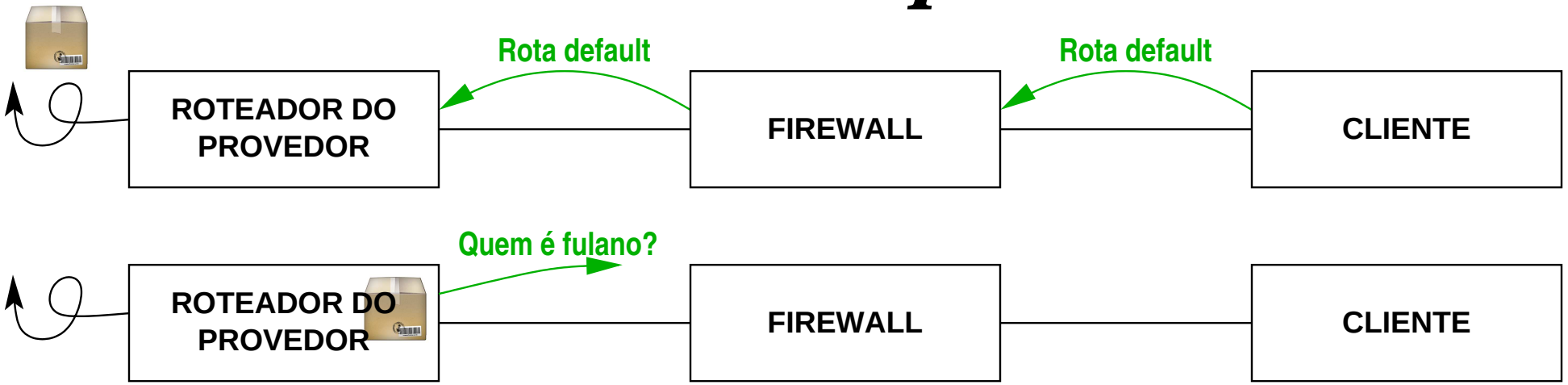
Um dia na vida de um pacote



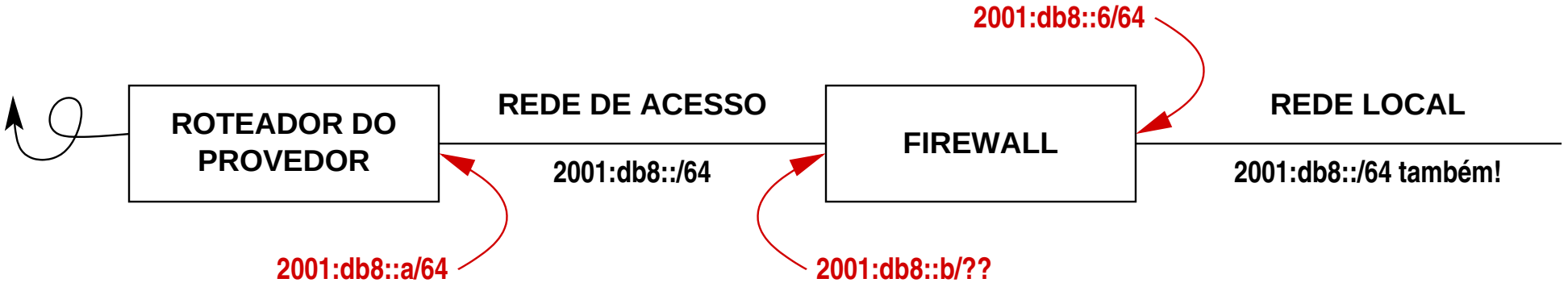
O Problema



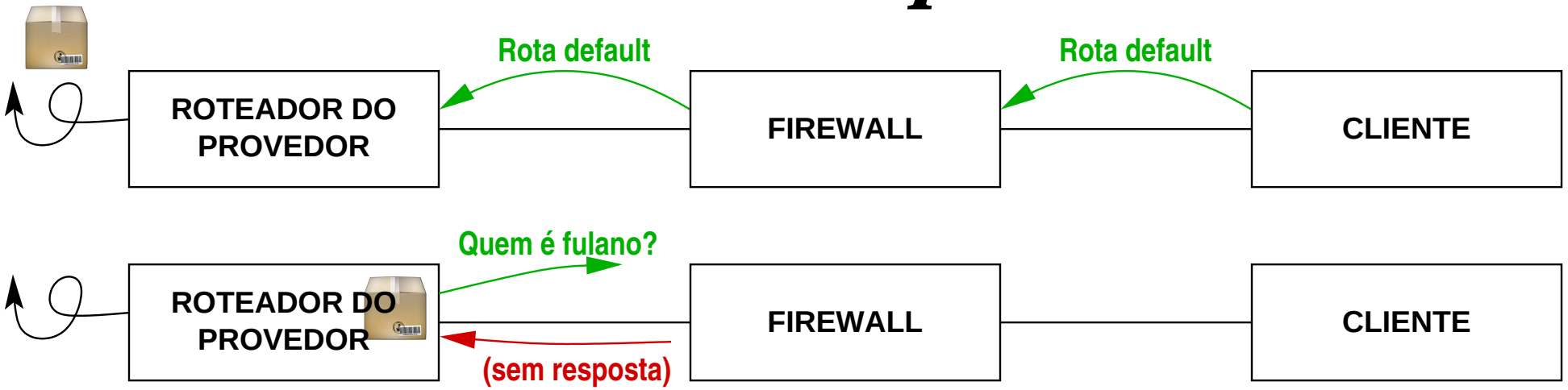
Um dia na vida de um pacote



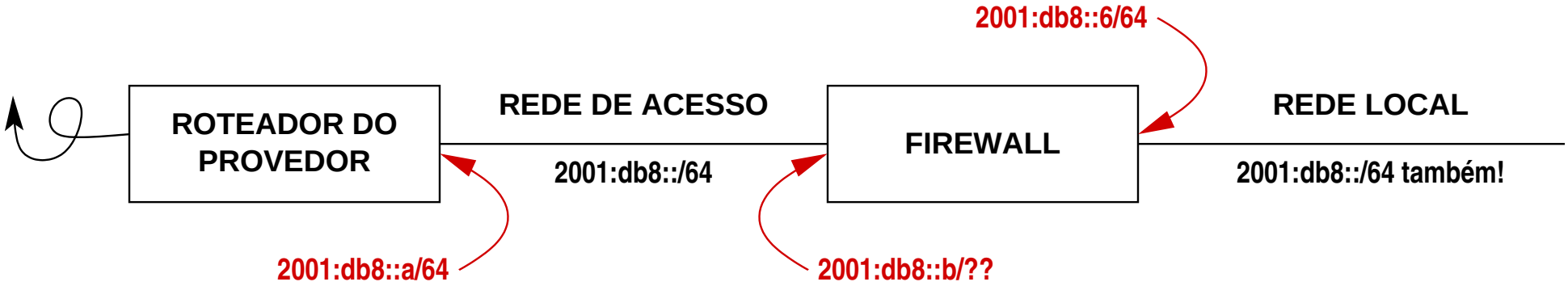
O Problema



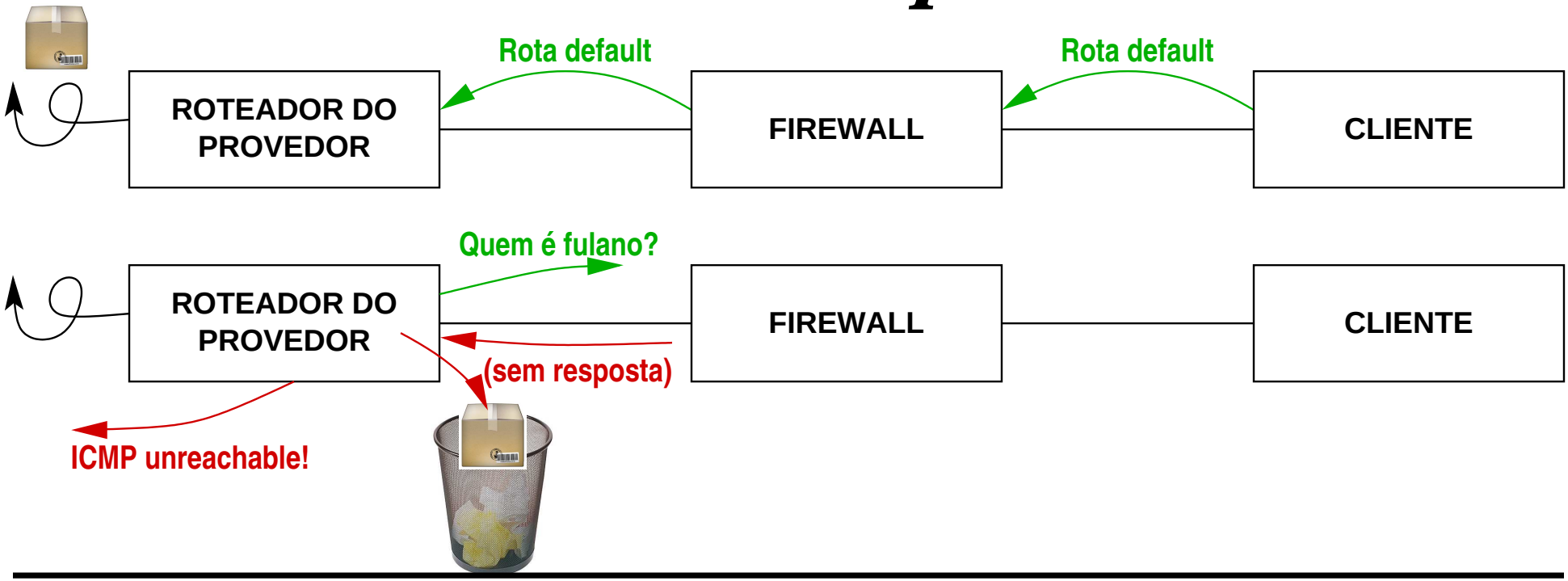
Um dia na vida de um pacote



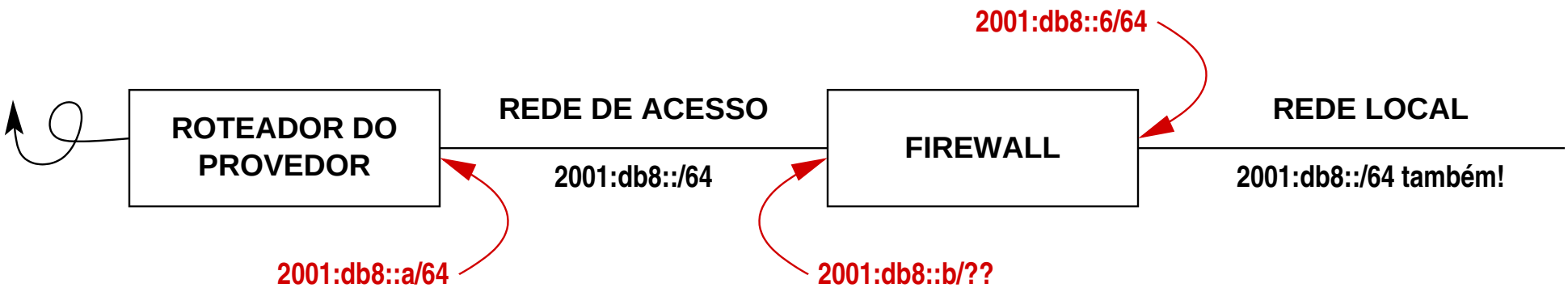
O Problema



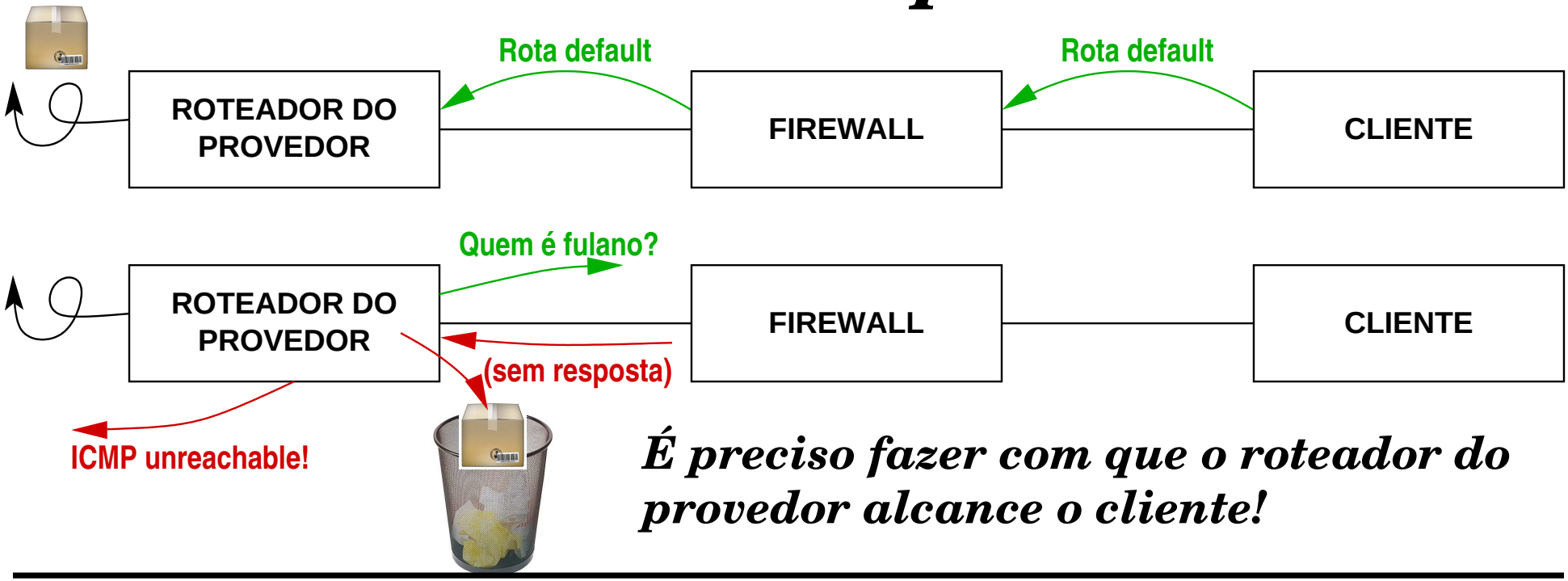
Um dia na vida de um pacote



O Problema



Um dia na vida de um pacote

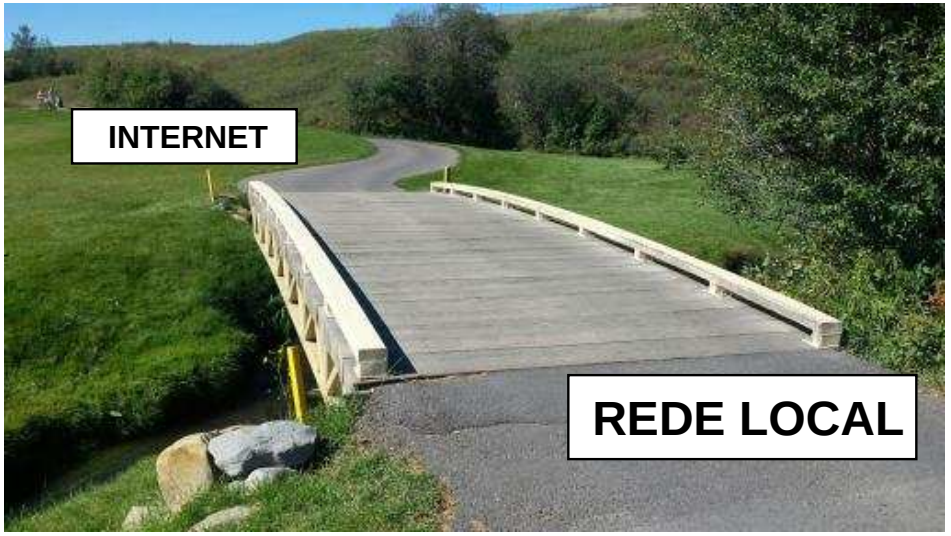


É preciso fazer com que o roteador do provedor alcance o cliente!

Possíveis soluções

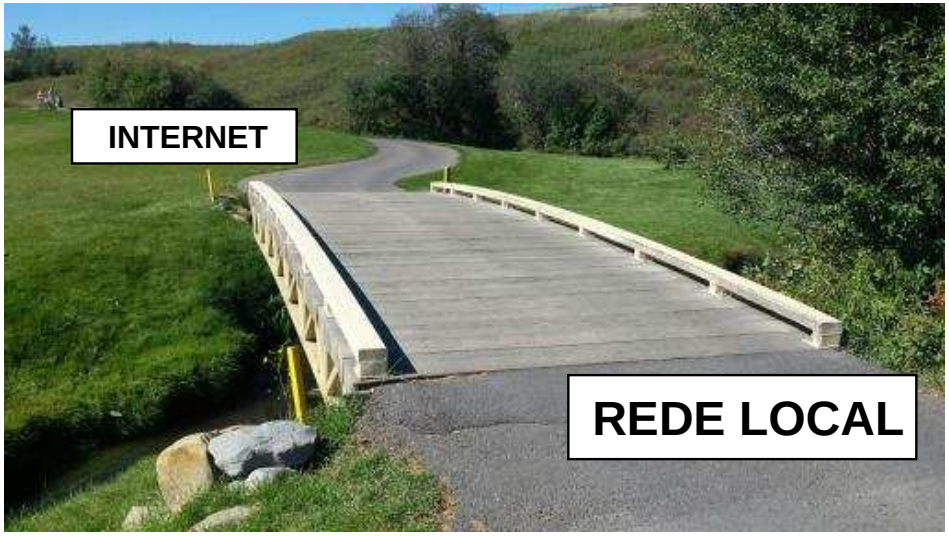
Possíveis soluções

1 – uma ponte (bridge)



Possíveis soluções

1 – uma ponte (bridge)

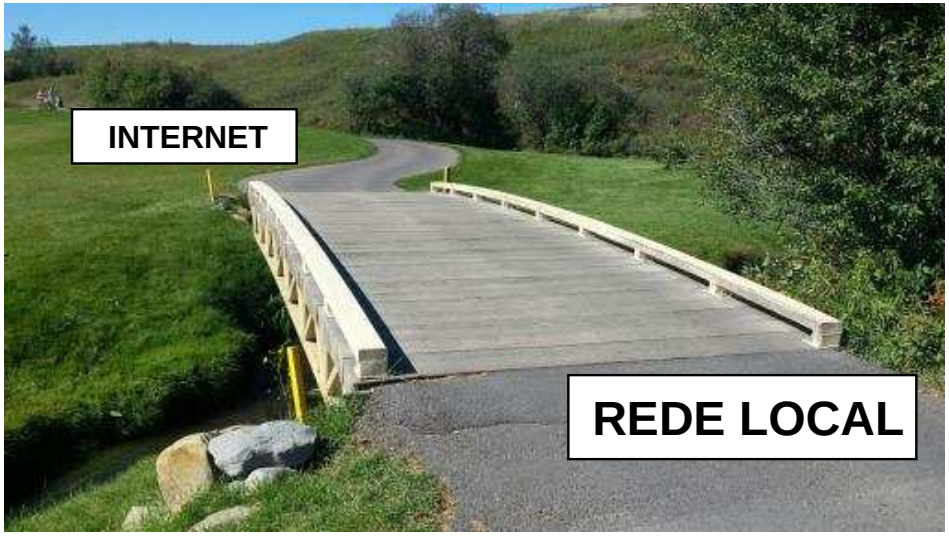


É simples e funciona!

Permite filtragem de pacotes (ip6tables).

Possíveis soluções

1 – uma ponte (bridge)



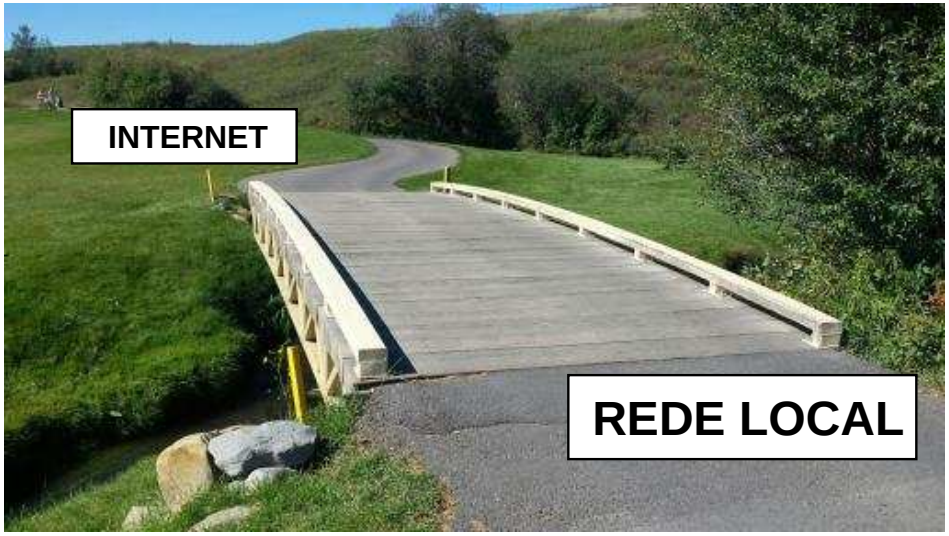
É simples e funciona!

Permite filtragem de pacotes (ip6tables).

Porém expõe a rede de acesso completamente aos clientes e há coisas "feias" lá.

Possíveis soluções

1 – uma ponte (bridge)



É simples e funciona!

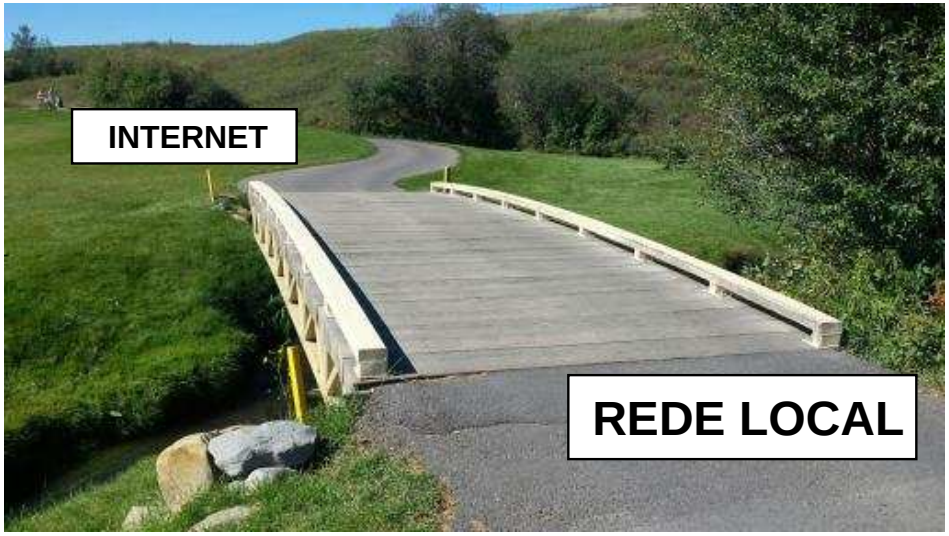
Permite filtragem de pacotes (ip6tables).

Porém expõe a rede de acesso completamente aos clientes e há coisas "feias" lá.

Complica a coexistencia com IPv4 pré–existente (e no qual não podemos mexer!)

Possíveis soluções

1 – uma ponte (bridge)



É simples e funciona!

Permite filtragem de pacotes (ip6tables).

Porém expõe a rede de acesso completamente aos clientes e há coisas "feias" lá.

Complica a coexistencia com IPv4 pré–existente (e no qual não podemos mexer!)

Possíveis soluções

2 – Proxy NDP, ou o roteador de pobre, ou ainda ai que saudade do proxy–arp do IPv4.

Possíveis soluções

2 – Proxy NDP, ou o roteador de pobre, ou ainda ai que saudade do proxy–arp do IPv4.

Consiste em responder às solicitações de MAC de vizinhos por procuração.

Possíveis soluções

2 – Proxy NDP, ou o roteador de pobre, ou ainda ai que saudade do proxy–arp do IPv4.

Consiste em responder às solicitações de MAC de vizinhos por procuração.

Exige ajuste nos parâmetros do kernel e um programa na "userland" para gerenciar a tabela de vizinhos.

Possíveis soluções

2 – Proxy NDP, ou o roteador de pobre, ou ainda ai que saudade do proxy–arp do IPv4.

Consiste em responder às solicitações de MAC de vizinhos por procuração.

Exige ajuste nos parâmetros do kernel e um programa na "userland" para gerenciar a tabela de vizinhos.

Quais endereços podem ser resolvidos são configurados manualmente.

Possíveis soluções

2 – Proxy NDP, ou o roteador de pobre, ou ainda ai que saudade do proxy–arp do IPv4.

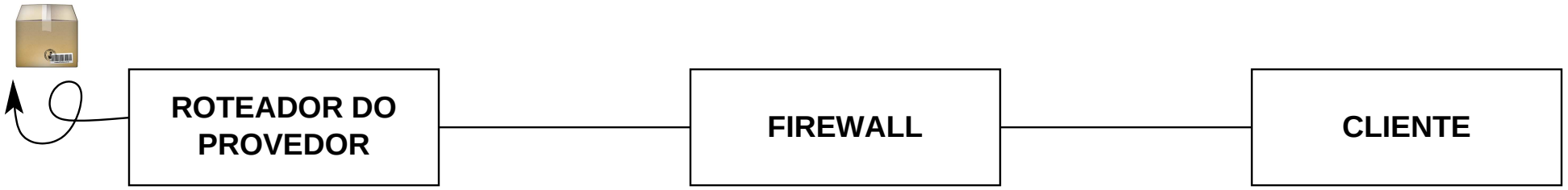
Consiste em responder às solicitações de MAC de vizinhos por procuração.

Exige ajuste nos parâmetros do kernel e um programa na "userland" para gerenciar a tabela de vizinhos.

Quais endereços podem ser resolvidos são configurados manualmente.

Um dia na vida de um pacote – mas agora com proxy–NDP!

Um dia na vida de um pacote – mas agora com proxy–NDP!

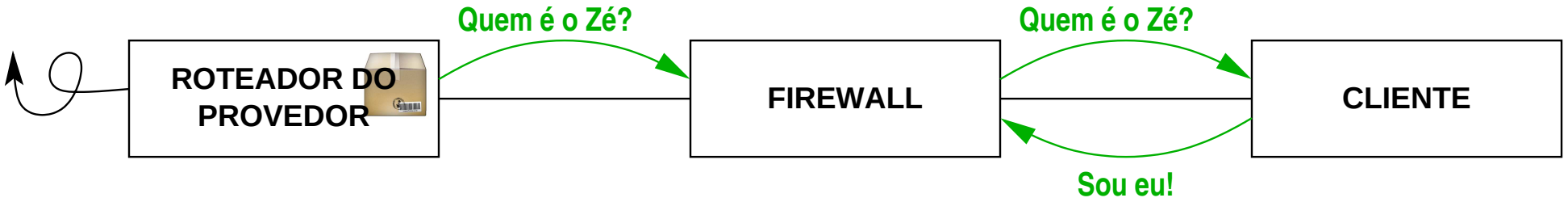


Um dia na vida de um pacote – mas agora com proxy–NDP!

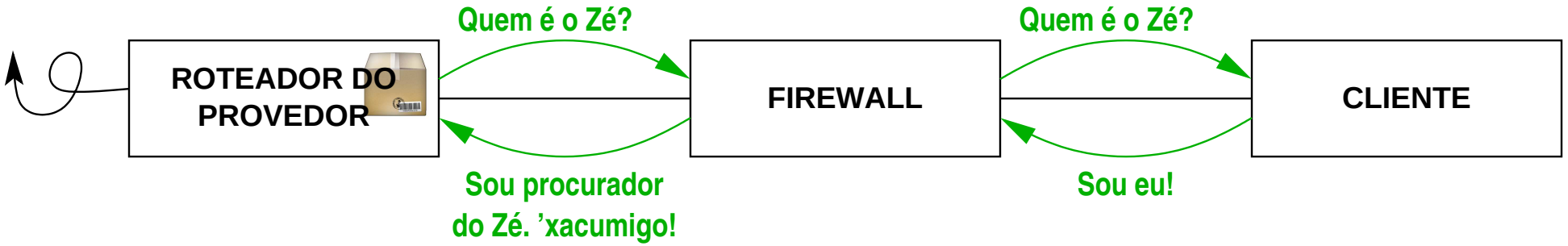
Um dia na vida de um pacote – mas agora com proxy–NDP!

Um dia na vida de um pacote – mas agora com proxy–NDP!

Um dia na vida de um pacote – mas agora com proxy–NDP!

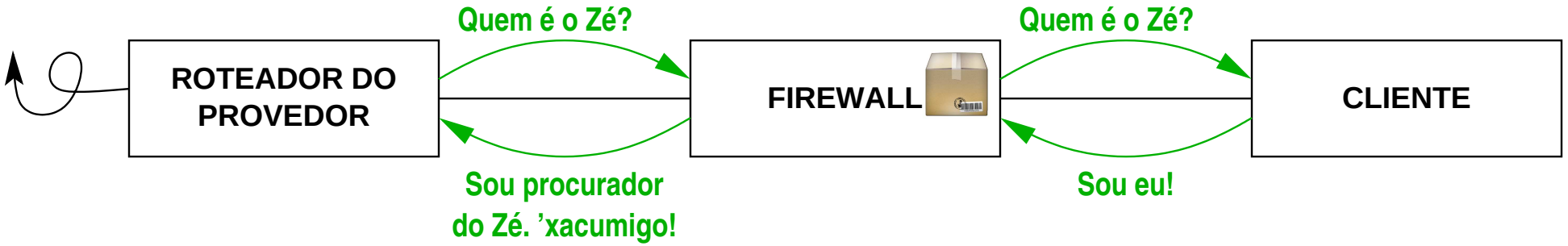


Um dia na vida de um pacote – mas agora com proxy–NDP!

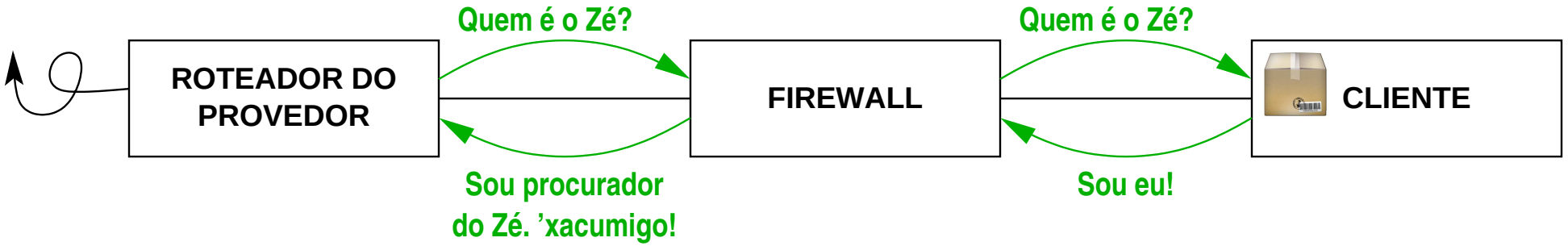


Um dia na vida de um pacote – mas agora com proxy–NDP!

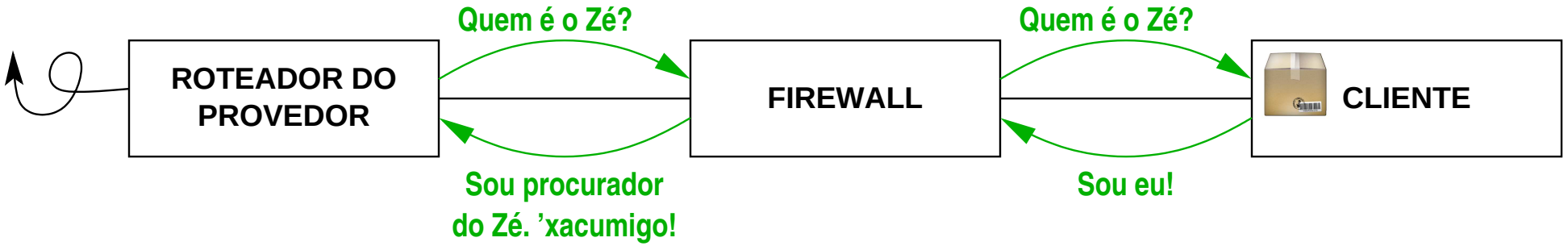
Um dia na vida de um pacote – mas agora com proxy–NDP!



Um dia na vida de um pacote – mas agora com proxy–NDP!

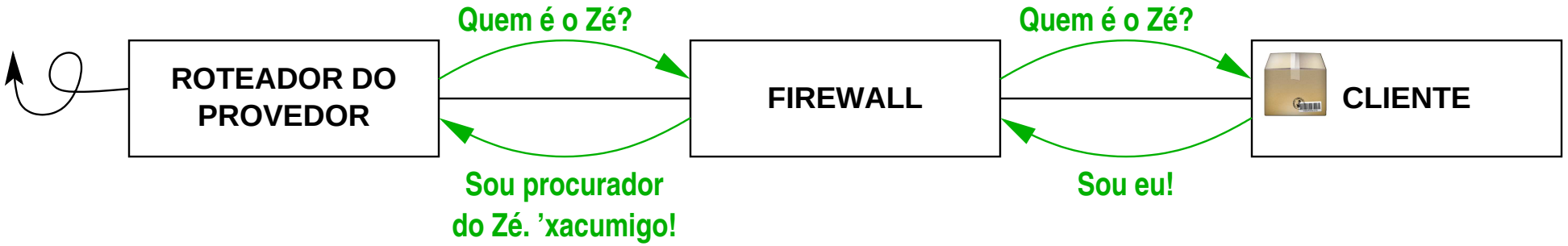


Um dia na vida de um pacote – mas agora com proxy–NDP!



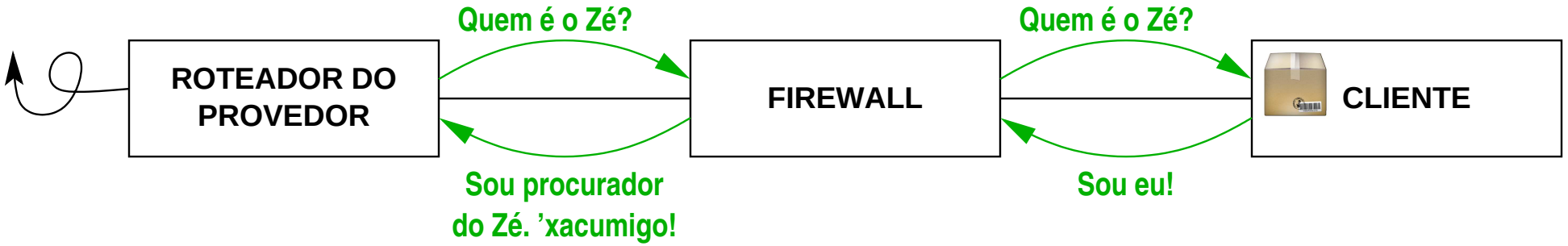
Resumo da ópera

Um dia na vida de um pacote – mas agora com proxy–NDP!



Resumo da ópera – roteador envia uma solicitação de vizinho.

Um dia na vida de um pacote – mas agora com proxy–NDP!

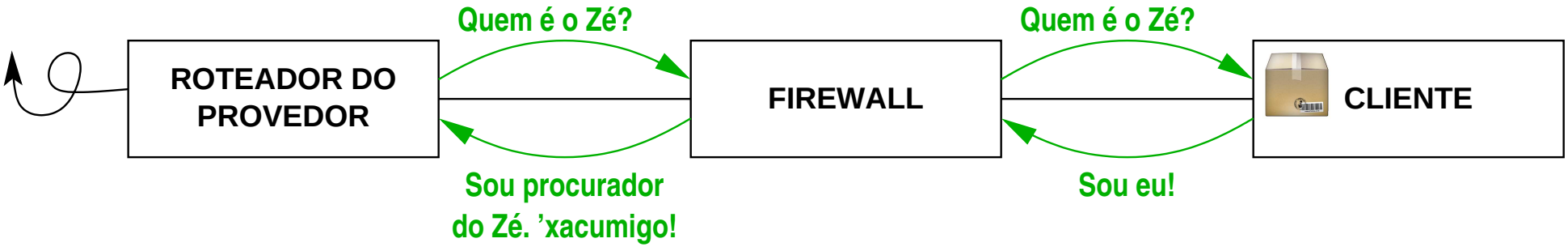


Resumo da ópera

– roteador envia uma solicitação de vizinho.

– firewall responde em nome do cliente (por isso ele é um procurador – proxy).

Um dia na vida de um pacote – mas agora com proxy–NDP!



Resumo da ópera

– roteador envia uma solicitação de vizinho.

– firewall responde em nome do cliente (por isso ele é um procurador – proxy).

– se necessário o firewall atualiza sua própria tabela de vizinhos.

Proxy NDP no Linux

Proxy NDP no Linux

Requer ajuste no kernel

/etc/sysctl.d/99-sysctl.conf

```
net.ipv6.conf.all.proxy_ndp = 1
net.ipv6.conf.default.proxy_ndp = 1
```

Proxy NDP no Linux

Requer ajuste no kernel

/etc/sysctl.d/99-sysctl.conf

```
net.ipv6.conf.all.proxy_ndp = 1
net.ipv6.conf.default.proxy_ndp = 1
```

Usa um "daemon" chamado ndppd

/etc/ndppd.conf

```
proxy home {
        rule 2001:db8::a/127 {
                static
        }
}
proxy jungle {
        rule 2001:db8::/64 {
                static
        }
}
```

Proxy NDP no Linux

Requer ajuste no kernel

/etc/sysctl.d/99-sysctl.conf

```
net.ipv6.conf.all.proxy_ndp = 1
net.ipv6.conf.default.proxy_ndp = 1
```

Usa um "daemon" chamado ndppd

/etc/ndppd.conf

rede local

```
proxy home {
        rule 2001:db8::a/127 {
                static
        }
}
proxy jungle {
        rule 2001:db8::/64 {
                static
        }
}
```

Proxy NDP no Linux

Requer ajuste no kernel

/etc/sysctl.d/99-sysctl.conf

```
net.ipv6.conf.all.proxy_ndp = 1
net.ipv6.conf.default.proxy_ndp = 1
```

Usa um "daemon" chamado ndppd

/etc/ndppd.conf

```
proxy home {
        rule 2001:db8::a/127 {
                static
        }
}
proxy jungle {
        rule 2001:db8::/64 {
                static
        }
}
```

rede local

rede de acesso

Autoconfiguração de endereços IP

Autoconfiguração de endereços IP

Os clientes obtém o endereço IP por SLAAC.

Autoconfiguração de endereços IP

Os clientes obtém o endereço IP por SLAAC.

O serviço é prestado pelo radvd

Autoconfiguração de endereços IP

Os clientes obtém o endereço IP por SLAAC.

O serviço é prestado pelo radvd

/etc/radvd.conf

```
interface home {
        AdvSendAdvert on;
        MinRtrAdvInterval 5;
        MaxRtrAdvInterval 10;
        prefix 2001:db8::/64 {
                AdvAutonomous on;
        };
        RDNSS 2001:db8::1bd {
                AdvRDNSSPreference 8;
        };
};
```

Autoconfiguração de endereços IP

Os clientes obtém o endereço IP por SLAAC.

O serviço é prestado pelo radvd

/etc/radvd.conf

```
interface home {
        AdvSendAdvert on;
        MinRtrAdvInterval 5;
        MaxRtrAdvInterval 10;
        prefix 2001:db8::/64 {
                AdvAutonomous on;
        };
        RDNSS 2001:db8::1bd {
                AdvRDNSSPreference 8;
        };
};
```

porque roda "unbound"!

Parte 2
Firewall

Firewall

Firewall

Modelo: Screened Hosts

Firewall

Modelo: Screened Hosts

permite acesso externo a endereços/portas previamente escolhidos na rede interna

bloqueia o acesso para qualquer outro host.

Firewall

Modelo: Screened Hosts

permite acesso externo a endereços/portas previamente escolhidos na rede interna

bloqueia o acesso para qualquer outro host.

Lógica de filtragem

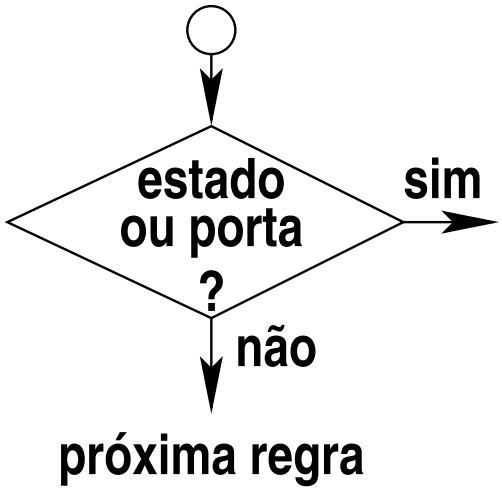
Firewall

Modelo: Screened Hosts

permite acesso externo a endereços/portas previamente escolhidos na rede interna

bloqueia o acesso para qualquer outro host.

Lógica de filtragem



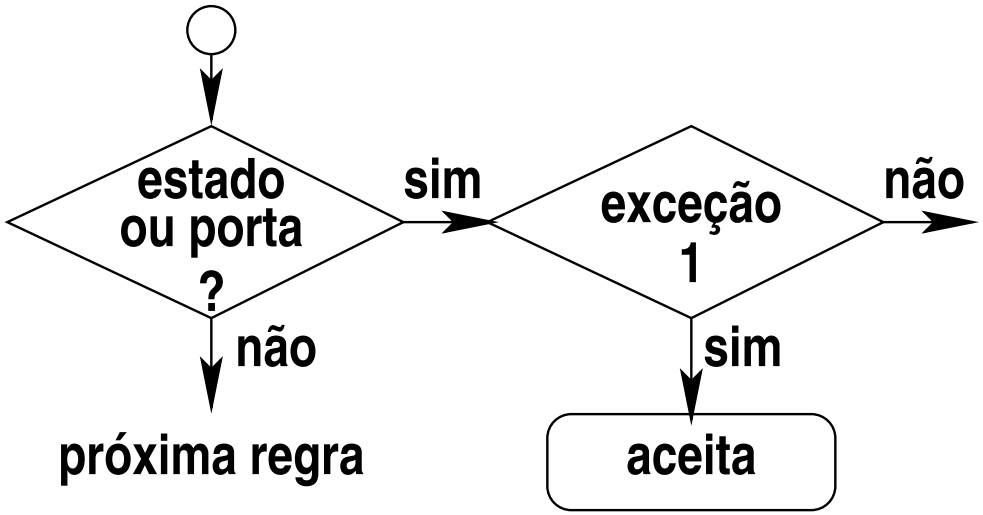
Firewall

Modelo: Screened Hosts

permite acesso externo a endereços/portas previamente escolhidos na rede interna

bloqueia o acesso para qualquer outro host.

Lógica de filtragem



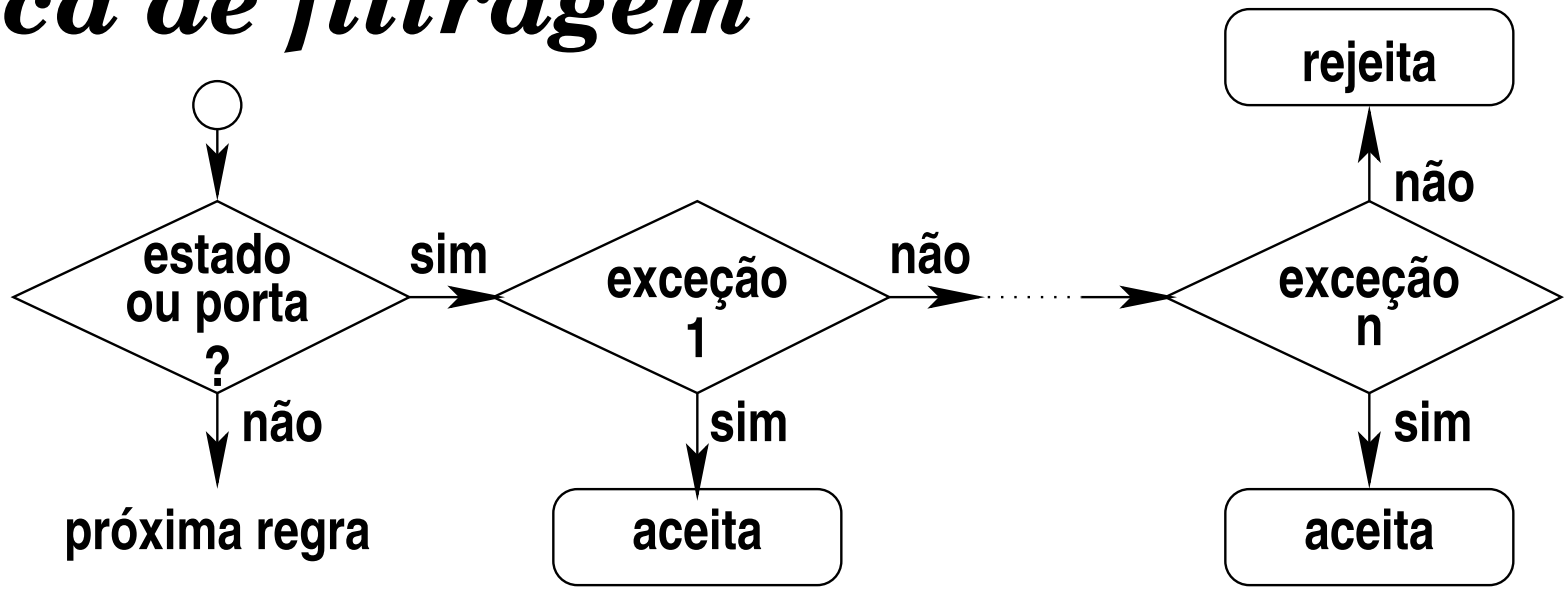
Firewall

Modelo: Screened Hosts

permite acesso externo a endereços/portas previamente escolhidos na rede interna

bloqueia o acesso para qualquer outro host.

Lógica de filtragem



Firewall – política de entrada

Firewall – política de entrada

```
-N INBOUND
-A INBOUND -m comment --comment "Rules for incoming packets"
-A INBOUND -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INBOUND -p tcp -m multiport --dports 80,443 -j WEB-SERVERS
-A INBOUND -p tcp -m multiport --dports 25,110,143,587,993 -j MAIL
-A INBOUND -p tcp -m tcp --dport 53 -j DNS-SERVERS
-A INBOUND -p udp -m udp --dport 53 -j DNS-SERVERS
-A INBOUND -p tcp -m tcp --dport 3389 -j TS-WINDOWS
-A INBOUND -p tcp -m tcp --dport 22 -j SSH-SERVERS
-A INBOUND -p tcp -m tcp --dport 445 -j LOG+DROP
-A INBOUND -j DROP
```

Firewall – política de entrada

```
-N INBOUND
-A INBOUND -m comment --comment "Rules for incoming packets"
-A INBOUND -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INBOUND -p tcp -m multiport --dports 80,443 -j WEB-SERVERS
-A INBOUND -p tcp -m multiport --dports 25,110,143,587,993 -j MAIL
-A INBOUND -p tcp -m tcp --dport 53 -j DNS-SERVERS
-A INBOUND -p udp -m udp --dport 53 -j DNS-SERVERS
-A INBOUND -p tcp -m tcp --dport 3389 -j TS-WINDOWS
-A INBOUND -p tcp -m tcp --dport 22 -j SSH-SERVERS
-A INBOUND -p tcp -m tcp --dport 445 -j LOG+DROP
-A INBOUND -j DROP
```

```
-N MAIL
-A MAIL -m comment --comment "mail servers come here."
-A MAIL -d 2001:db8::25/128 -j RETURN
-A MAIL -j DROP
```

Firewall – política de entrada

```
-N INBOUND
-A INBOUND -m comment --comment "Rules for incoming packets"
-A INBOUND -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INBOUND -p tcp -m multiport --dports 80,443 -j WEB-SERVERS
-A INBOUND -p tcp -m multiport --dports 25,110,143,587,993 -j MAIL
-A INBOUND -p tcp -m tcp --dport 53 -j DNS-SERVERS
-A INBOUND -p udp -m udp --dport 53 -j DNS-SERVERS
-A INBOUND -p tcp -m tcp --dport 3389 -j TS-WINDOWS
-A INBOUND -p tcp -m tcp --dport 22 -j SSH-SERVERS
-A INBOUND -p tcp -m tcp --dport 445 -j LOG+DROP
-A INBOUND -j DROP
```

```
-N MAIL
-A MAIL -m comment --comment "mail servers come here."
-A MAIL -d 2001:db8::25/128 -j RETURN
-A MAIL -j DROP
```

```
-N TS-WINDOWS
-A TS-WINDOWS -m comment --comment "MS Terminal servers."
-A TS-WINDOWS -d 2001:db8::15a1/128 -j RETURN
-A TS-WINDOWS -d 2001:db8::15a2/128 -j RETURN
-A TS-WINDOWS -j DROP
```

Firewall – política de saída

Firewall – política de saída

```
-N OUTBOUND
-A OUTBOUND -m comment --comment "Rules for outbound packets"
-A OUTBOUND -j INGRESS
-A OUTBOUND -p tcp -m tcp --dport 25 -j ANTI-SPAM
-A OUTBOUND -m conntrack --ctstate NEW,RELATED,ESTABLISHED -j ACC
-A OUTBOUND -j DROP
```

Firewall – política de saída

```
-N OUTBOUND
-A OUTBOUND -m comment --comment "Rules for outbound packets"
-A OUTBOUND -j INGRESS
-A OUTBOUND -p tcp -m tcp --dport 25 -j ANTI-SPAM
-A OUTBOUND -m conntrack --ctstate NEW,RELATED,ESTABLISHED -j ACC
-A OUTBOUND -j DROP
```

```
-N INGRESS
-A INGRESS -m comment --comment "Ingress filter"
-A INGRESS -s 2001:db8::/64 -j RETURN
-A INGRESS -s fe80::/64 -j RETURN
-A INGRESS -j LOG+DROP
```

Firewall – política de saída

```
-N OUTBOUND
-A OUTBOUND -m comment --comment "Rules for outbound packets"
-A OUTBOUND -j INGRESS
-A OUTBOUND -p tcp -m tcp --dport 25 -j ANTI-SPAM
-A OUTBOUND -m conntrack --ctstate NEW,RELATED,ESTABLISHED -j ACC
-A OUTBOUND -j DROP
```

```
-N INGRESS
-A INGRESS -m comment --comment "Ingress filter"
-A INGRESS -s 2001:db8::/64 -j RETURN
-A INGRESS -s fe80::/64 -j RETURN
-A INGRESS -j LOG+DROP
```

```
-N ANTI-SPAM
-A ANTI-SPAM -m comment --comment "Port 25/tcp screening."
-A ANTI-SPAM -s 2001:db8::25/128 -j RETURN
-A ANTI-SPAM -s 2001:db8::a17f/128 -j RETURN
-A ANTI-SPAM -j LOG+DROP
```

Comentários e conclusões

Comentários e conclusões

Bem que o provedor de serviços IP poderia caprichar um pouco mais...

Comentários e conclusões

Bem que o provedor de serviços IP poderia caprichar um pouco mais...

Bridge ou proxy–NDP permitem interpor um filtro/firewall.

Comentários e conclusões

Bem que o provedor de serviços IP poderia caprichar um pouco mais...

Bridge ou proxy–NDP permitem interpor um filtro/firewall.

Optamos pelo proxy–NDP por ser mais compatível com a infra atual.

Comentários e conclusões

Bem que o provedor de serviços IP poderia caprichar um pouco mais...

Bridge ou proxy–NDP permitem interpor um filtro/firewall.

Optamos pelo proxy–NDP por ser mais compatível com a infra atual.

Autoconfiguração (SLAAC).

Comentários e conclusões

Bem que o provedor de serviços IP poderia caprichar um pouco mais...

Bridge ou proxy–NDP permitem interpor um filtro/firewall.

Optamos pelo proxy–NDP por ser mais compatível com a infra atual.

Autoconfiguração (SLAAC).

Atenção ao limite de tamanho da tabela de vizinhos, especialmente em redes grandes (não é nosso caso).

Referencias úteis

Referencias úteis

IPv6 – Proxy the neighbors (or come back ARP – we loved you really)

https://www.ipsidixit.net/2010/03/24/239/

Referencias úteis

IPv6 – Proxy the neighbors (or come back ARP – we loved you really)

https://www.ipsidixit.net/2010/03/24/239/

DanielAdolfsson/ndppd (github)

https://github.com/DanielAdolfsson/ndppd

Referencias úteis

IPv6 – Proxy the neighbors (or come back ARP – we loved you really)

https://www.ipsidixit.net/2010/03/24/239/

DanielAdolfsson/ndppd (github)

https://github.com/DanielAdolfsson/ndppd