Estudos de Casos de Segurança na CTBC: Firewalls em IPv6

Grupo de Trabalho em Segurança de Redes - GTS

11º Reunião

Claudio Corrêa Porto
<claudio@lintronix.com.br>

Eduardo Ascenço Reis
<eascenco@ctbc.com.br>
<eduardo@intron.com.br>

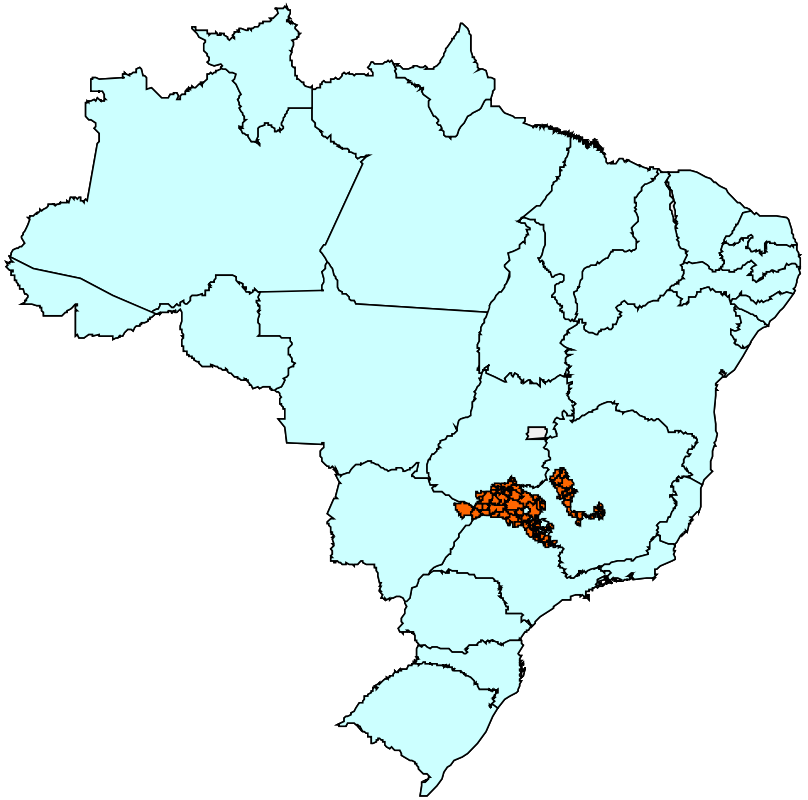
Pablo Martins Figueiredo da Costa
<pablo@cbsp.com.br>

Objetivo

O objetivo deste trabalho é apresentar algumas vulnerabilidades de segurança observadas durante a implementação de IPv6 nativo na CTBC Multimídia (AS27664) e alguns exemplos de soluções de Firewalls para IPv6 baseados em Sistemas Linux e FreeBSD.

Introdução - CTBC (Companhia de Telecomunicações do Brasil Central)

Áreas de Concessão



Áreas de Expansão

Introdução - CTBC – Serviços Internet

A CTBC é uma companhia de Telecomunicações que atua como provedor de Backbone (NSP) e de serviços Internet (ISP).

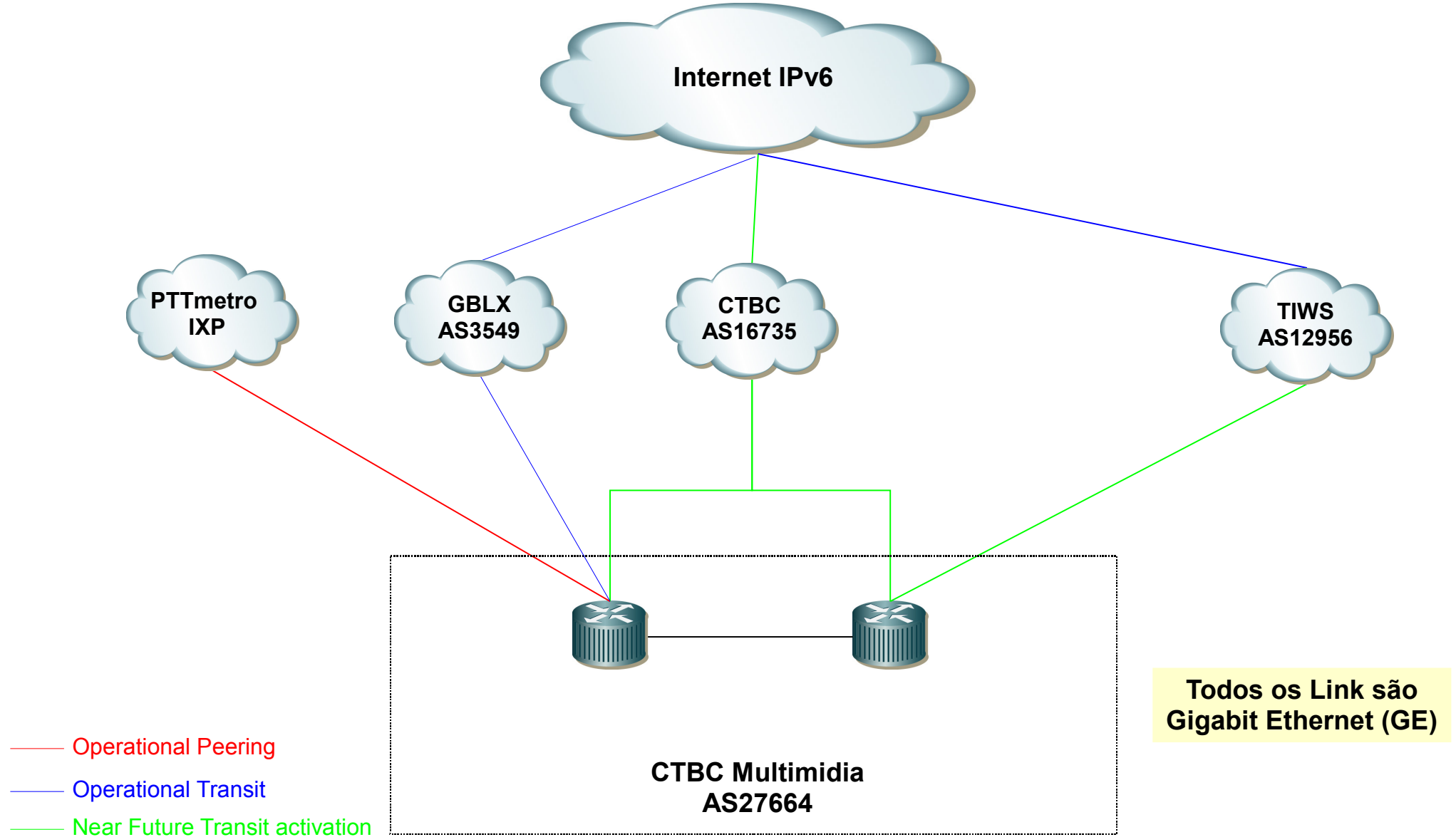
CTBC Telecom (AS16735)
Áreas Cobertas: Brasil – diferentes estados (MG, SP, RJ, etc)
Clientes: Corporativos (links dedicados) e Residencias (ADSL, etc)

CTBC Multimídia Data Net (AS27664)
Áreas Cobertas: cidade de São Paulo e vizinhança
Clientes: Corporativos (links dedicados)
Serviço Internet sobre Rede Metro Ethernet baseada em malhas de fibras ópticas enterradas cobrindo as regiões relevantes de concentração de empresas na cidade de São Paulo.

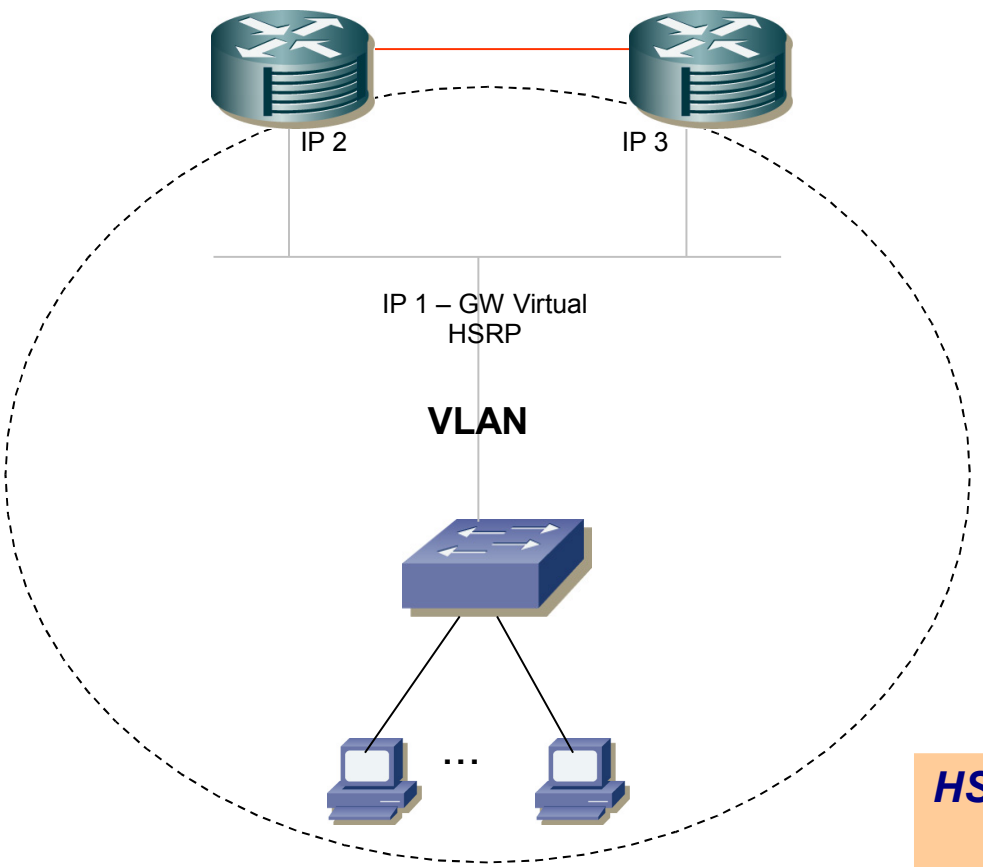
A implementação de IPv6 nativo iniciou em Janeiro de 2008 pelo AS27664 devido sua menor complexidade de rede e serviços.

Estudo de Caso de Implementação de IPv6 em São Paulo / Brasil
http://lacnic.net/pt/eventos/lacnicxi/flip6.html

CTBC AS27664 IPv6 – Atual Conectividade Externa



CTBC AS27664 IPv6 – Acesso Internet Redundante para Clientes



Modo Dual Stack

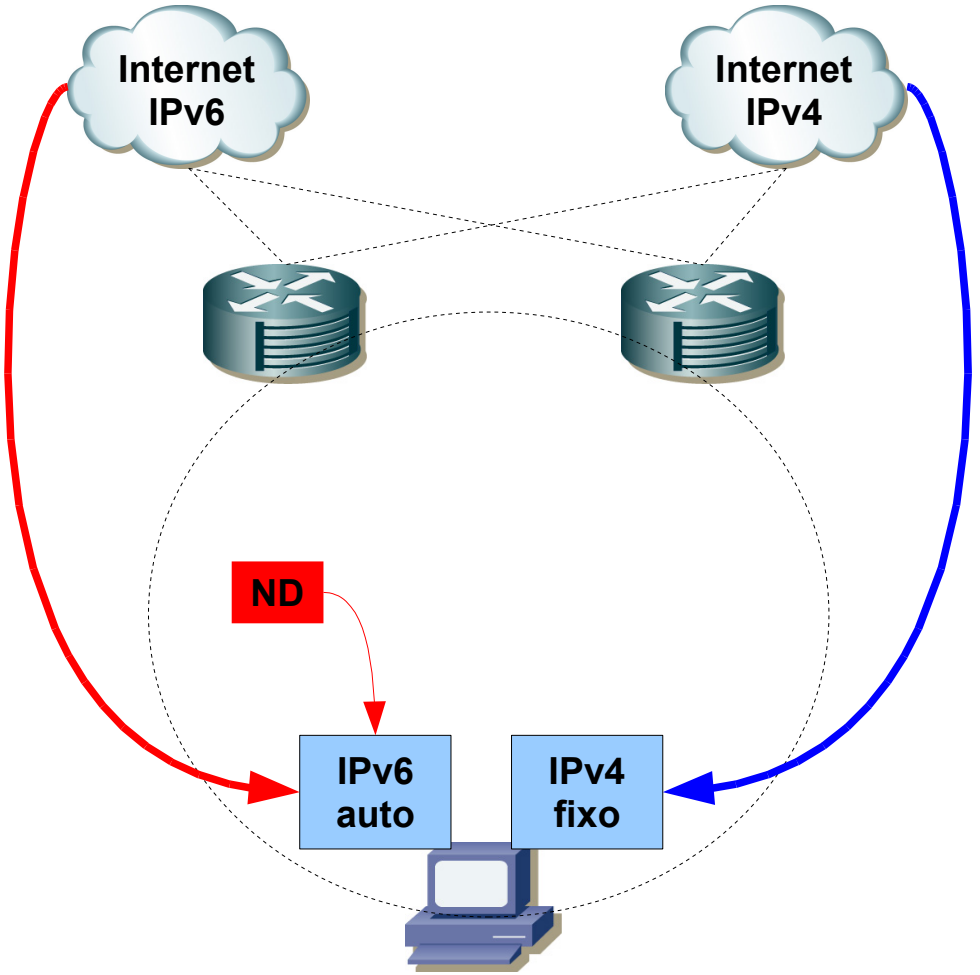
Padrão de Blocos Alocados para Cliente:

- IPv4 /28
- IPv6 /64

HSRPv2: Hot Standby Router Protocol Version 2

- Tamanho do campo de instância: de 8 para 12 bits
- Autenticação MD5
- Suporte para IPv4 e IPv6

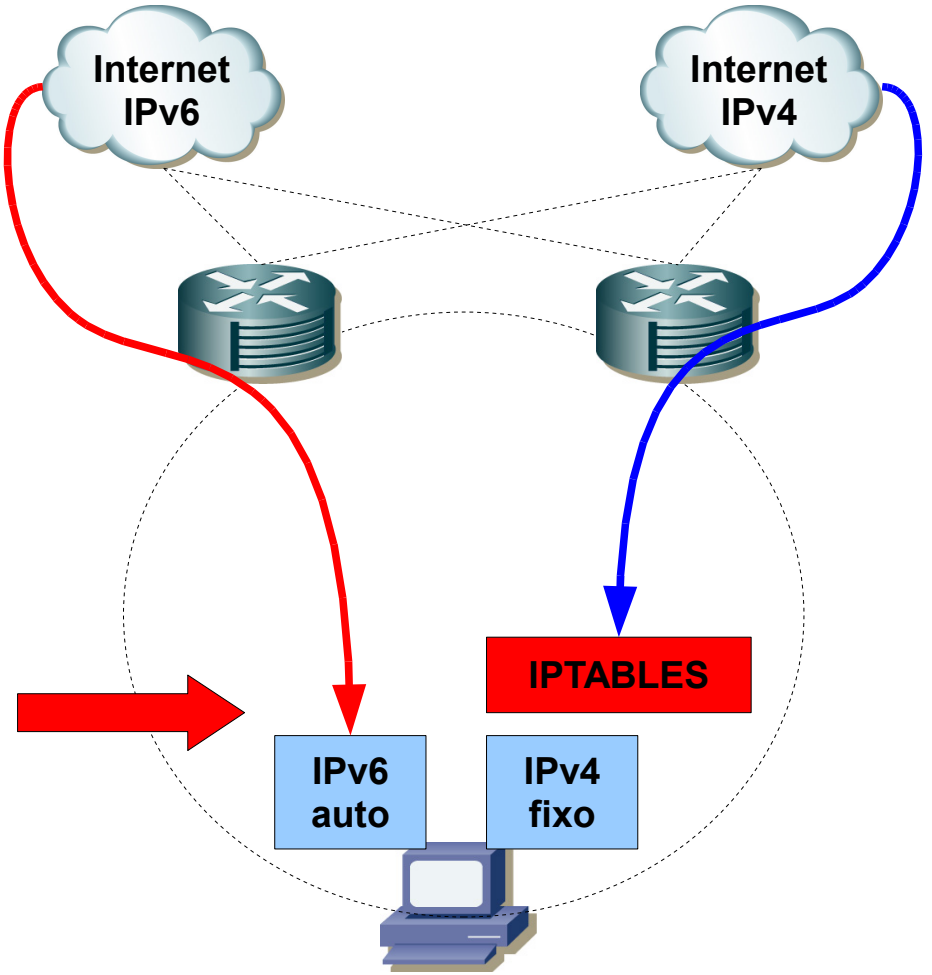
CTBC AS27664 IPv6 – Primeiro Acesso Internet Dual Stack



Estação de Trabalho com Sistema Linux
Suporte Nativo IPv6

ND: Neighbor Discovery Protocol

CTBC AS27664 IPv6 – IPv4 Protegido e IPv6 Aberto

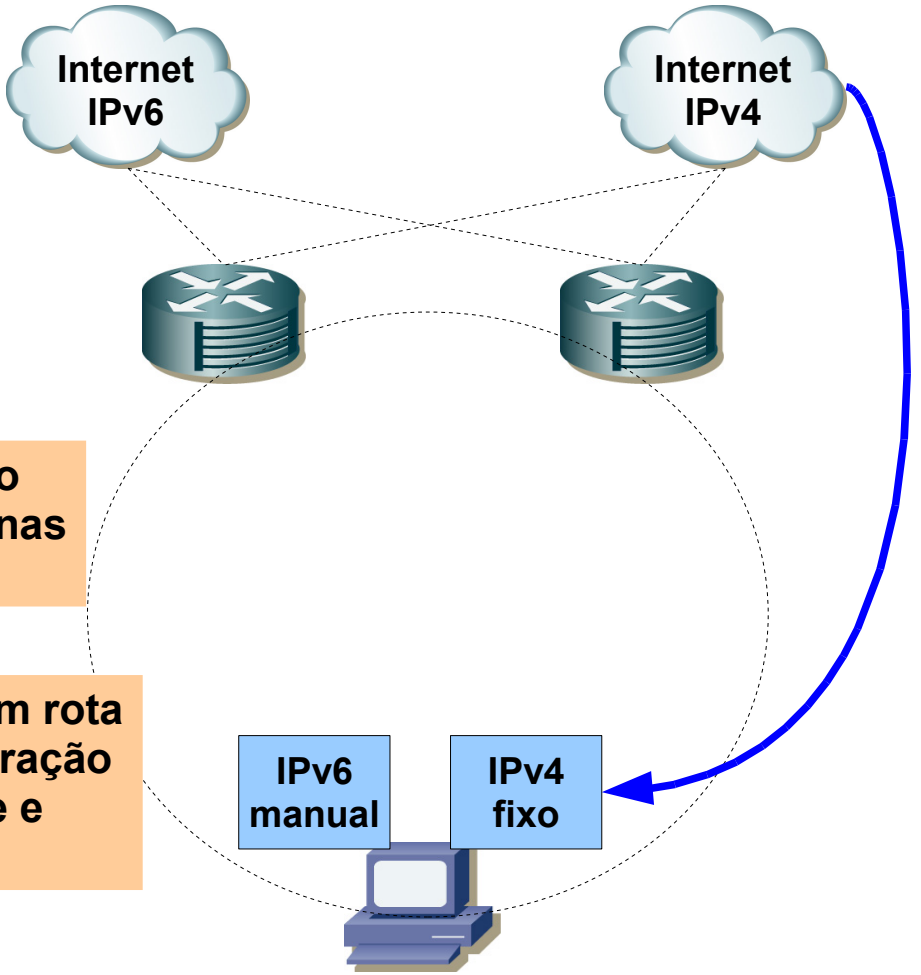


Por padrão está aberto para a Internet !!!

Estação de Trabalho com Sistema Linux
Suporte Nativo IPv6

Necessidade de estudo de Firewalls IPv6 antes de abrir rede de clientes com ND

CTBC AS27664 IPv6 – Inicialmente Desabilitado ND – Teste Configuração Manual



Inicialmente Desabilitado ND para proteger máquinas com suporte nativo IPv6

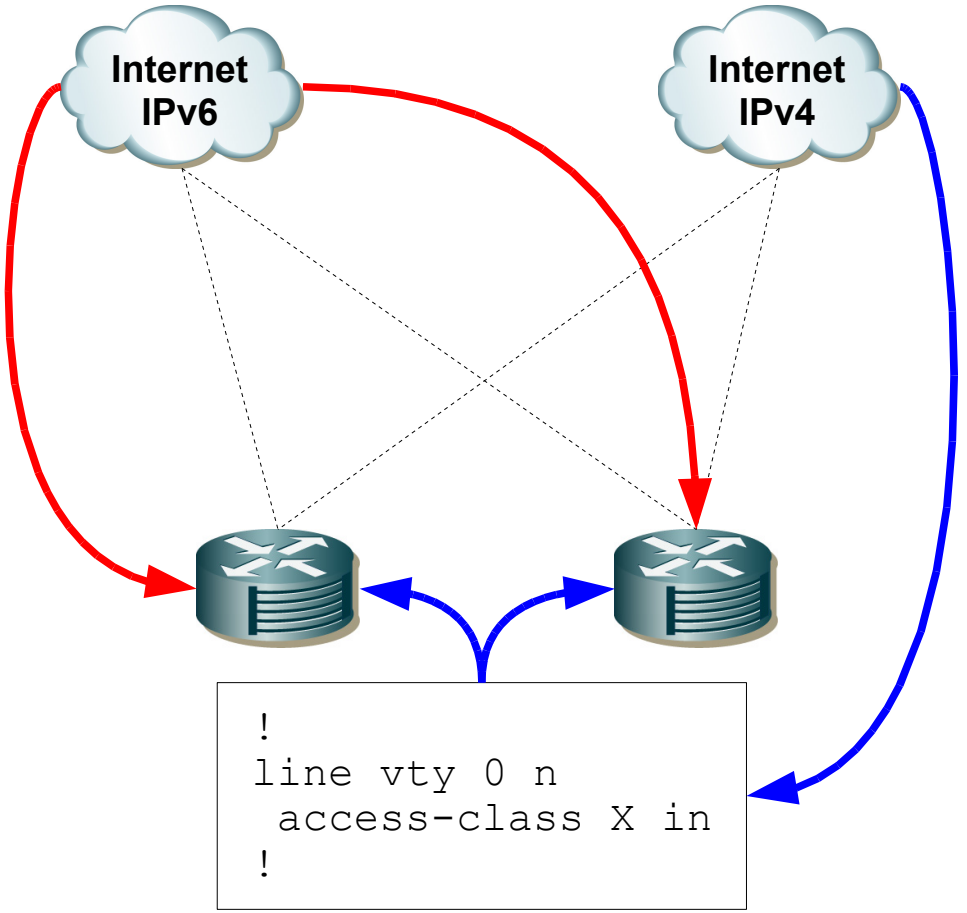
Testes iniciais com IPv6 sem rota default e utilizando configuração manual de IPv6 na interface e algumas rotas estáticas

Estação de Trabalho com Sistema Linux
Suporte Nativo IPv6

CTBC AS27664 IPv6 – Roteadores são Dual Stack – Também Aberto !!!

Controle por Endereços IPv4 de Origem para Permitir Acesso Remoto aos Roteadores

Acesso Remoto
Aberto para IPv6 !!!

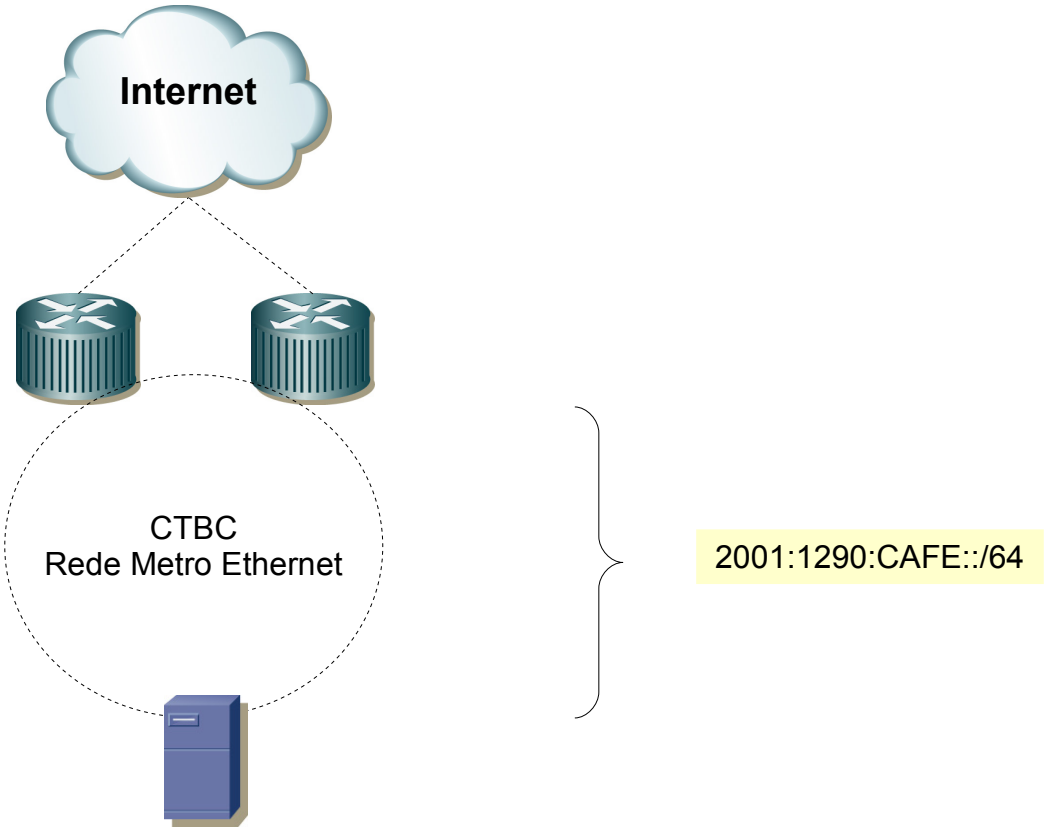


CTBC AS27664 IPv6 – Parcerias da CTBC para Apoio na Validação IPv6

Cliente
Projeto Piloto

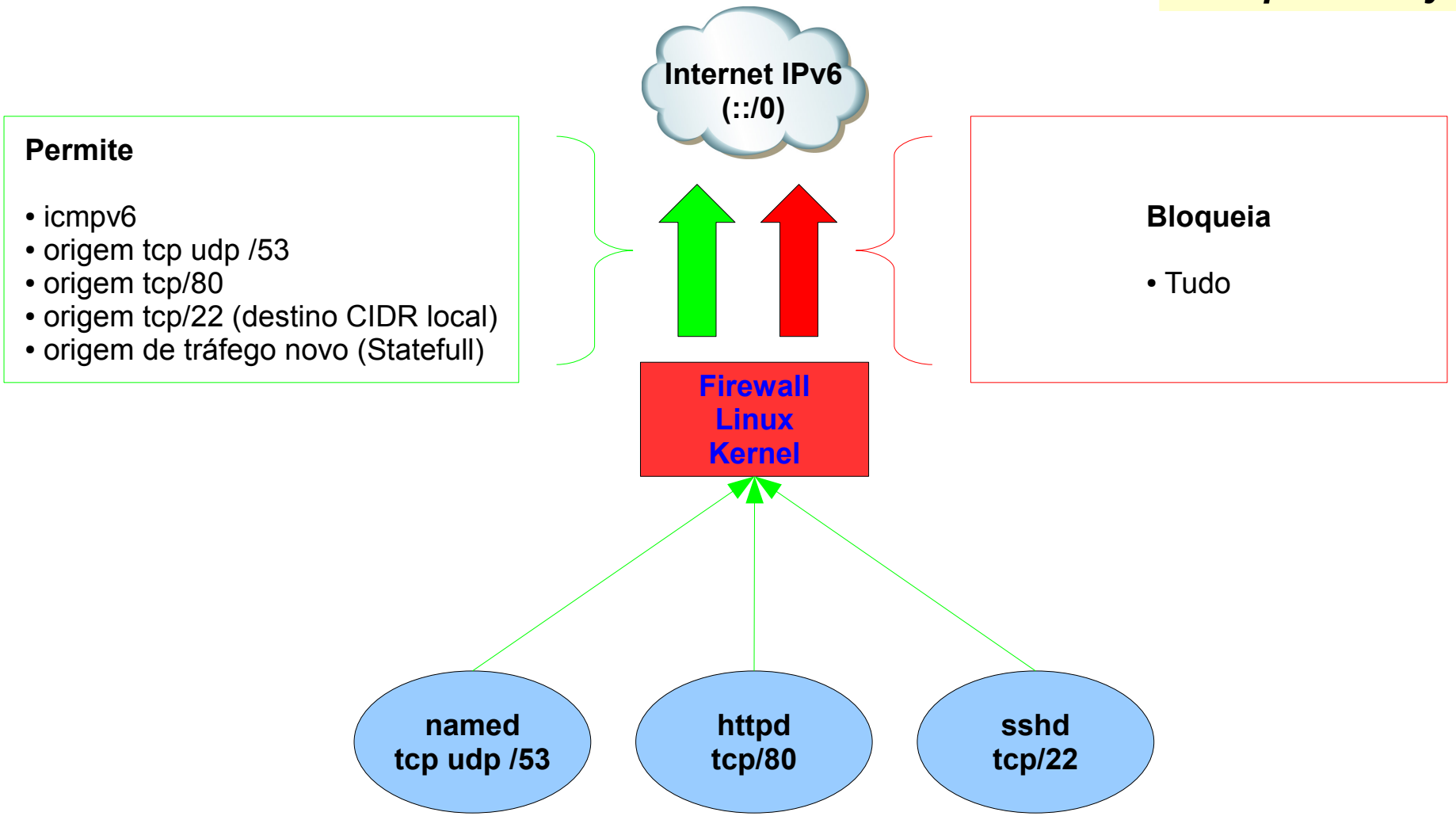
Empresa
Terceira

CTBC AS27664 IPv6 – Caso CTBC - Diagrama Lógico de Rede



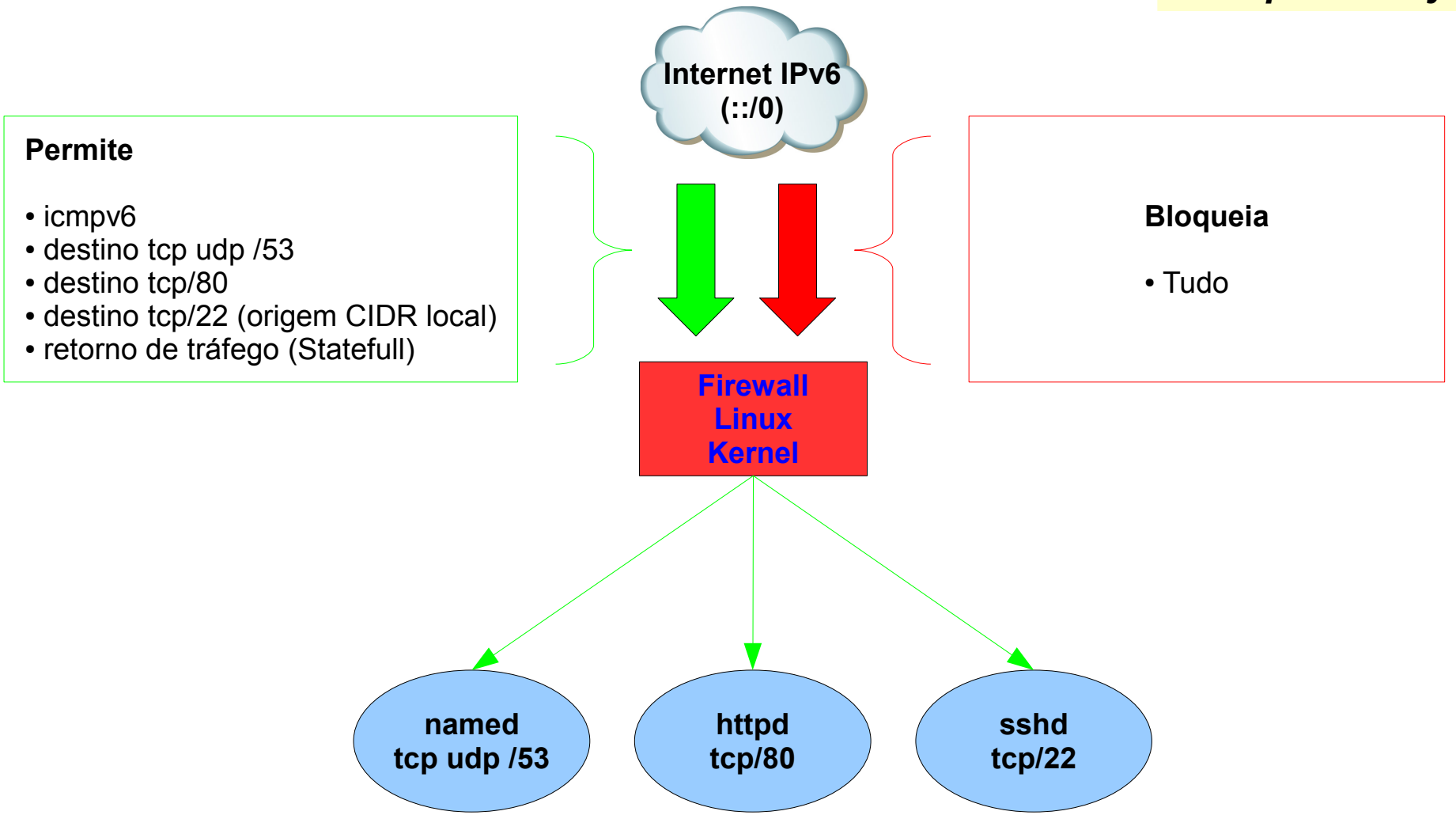
CTBC AS27664 IPv6 – Caso CTBC - Diagrama Lógico – Firewall IPv6 - 1/2

Regras de Saída
Output Policy



CTBC AS27664 IPv6 – Caso CTBC - Diagrama Lógico – Firewall IPv6 - 2/2

Regras de Entrada
Input Policy



CTBC AS27664 IPv6 – Caso CTBC - Regras de Firewall Linux (ip6tables) 1/3

```
# Politica default eh negar tudo
ip6tables -F
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# Trafego para a interface de loopback
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT

# ICMPv6
ip6tables -A INPUT -p icmpv6 -j ACCEPT
ip6tables -A OUTPUT -p icmpv6 -j ACCEPT
```

CTBC AS27664 IPv6 – Caso CTBC - Regras de Firewall Linux (ip6tables) 2/3

```
# Servidor DNS
ip6tables -A INPUT -p udp -s ::/0 --dport 53 -j ACCEPT
ip6tables -A OUTPUT -p udp --sport 53 -d ::/0 -j ACCEPT
ip6tables -A INPUT -p tcp -s ::/0 --dport 53 -j ACCEPT
ip6tables -A OUTPUT -p tcp --sport 53 -d ::/0 -j ACCEPT

# Servidor SSH (22)
ip6tables -A INPUT -p tcp -s 2001:1290::/32 --dport 22 -j ACCEPT
ip6tables -A OUTPUT -p tcp --sport 22 -d 2001:1290::/32 -j ACCEPT

# Servidor HTTP (80)
ip6tables -A INPUT -p tcp -s ::/0 --dport 80 -j ACCEPT
ip6tables -A OUTPUT -p tcp --sport 80 -d ::/0 -j ACCEPT
```

CTBC AS27664 IPv6 – Caso CTBC - Regras de Firewall Linux (ip6tables) 3/3

```
# StateFull Firewall

ip6tables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT
```

CTBC AS27664 IPv6 – Caso CTBC - NTP – Sincronização de Relógio em IPv6

```
# host -t AAAA a.ntp.br
a.ntp.br has IPv6 address 2001:12ff::8
#


# ntpq
ntpq> peers
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*a.ntp.br        200.160.7.192    2 u   20   64    7    0.667    9.525   0.983
ntpq>
ntpq> quit


# grep "^server" /etc/ntp.conf
server 2001:12ff::8 iburst
#


# tcpdump -i eth1 -n -v port 123
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
01:15:09.341332 IP6 (hlim 64, next-header: UDP (17), length: 56) 2001:1290:cafe::2002.123 >
 2001:12ff::8.123: NTPv4, length 48
        Client, Leap indicator: clock unsynchronized (192), Stratum 0, poll 6s, precision -20
        Root Delay: 0.000000, Root dispersion: 0.000000, Reference-ID: (unspec)
          Reference Timestamp:  0.000000000
          Originator Timestamp: 0.000000000 [|ntp]
01:15:09.342071 IP6 (hlim 60, next-header: UDP (17), length: 56) 2001:12ff::8.123 >
2001:1290:cafe::2002.123: NTPv4, length 48
        Server, Leap indicator:  (0), Stratum 2, poll 6s, precision -18
        Root Delay: 0.000396, Root dispersion: 0.006576, Reference-ID: 200.160.7.192
          Reference Timestamp:  3421109631.577830530 (2008/05/30 01:13:51)
          Originator Timestamp: 3421109709.341292907 (2008/05/30 01:15:09) [|ntp]

(...)
```

CTBC AS27664 IPv6 – Caso CTBC – Teste Servidor Apache 80 e 8080 /tcp - 1/3

```
# cat /etc/apache2/ports.conf
Listen 80
Listen 8080

<IfModule mod_ssl.c>
    Listen 443
</IfModule>
#


# netstat -antp | grep apache
tcp6       0      0 :::8080                 :::*                    LISTEN      10991/apache2
tcp6       0      0 :::80                   :::*                    LISTEN      10991/apache2

#
```

CTBC AS27664 IPv6 – Caso CTBC – Teste Servidor Apache 80 e 8080 /tcp - 2/3

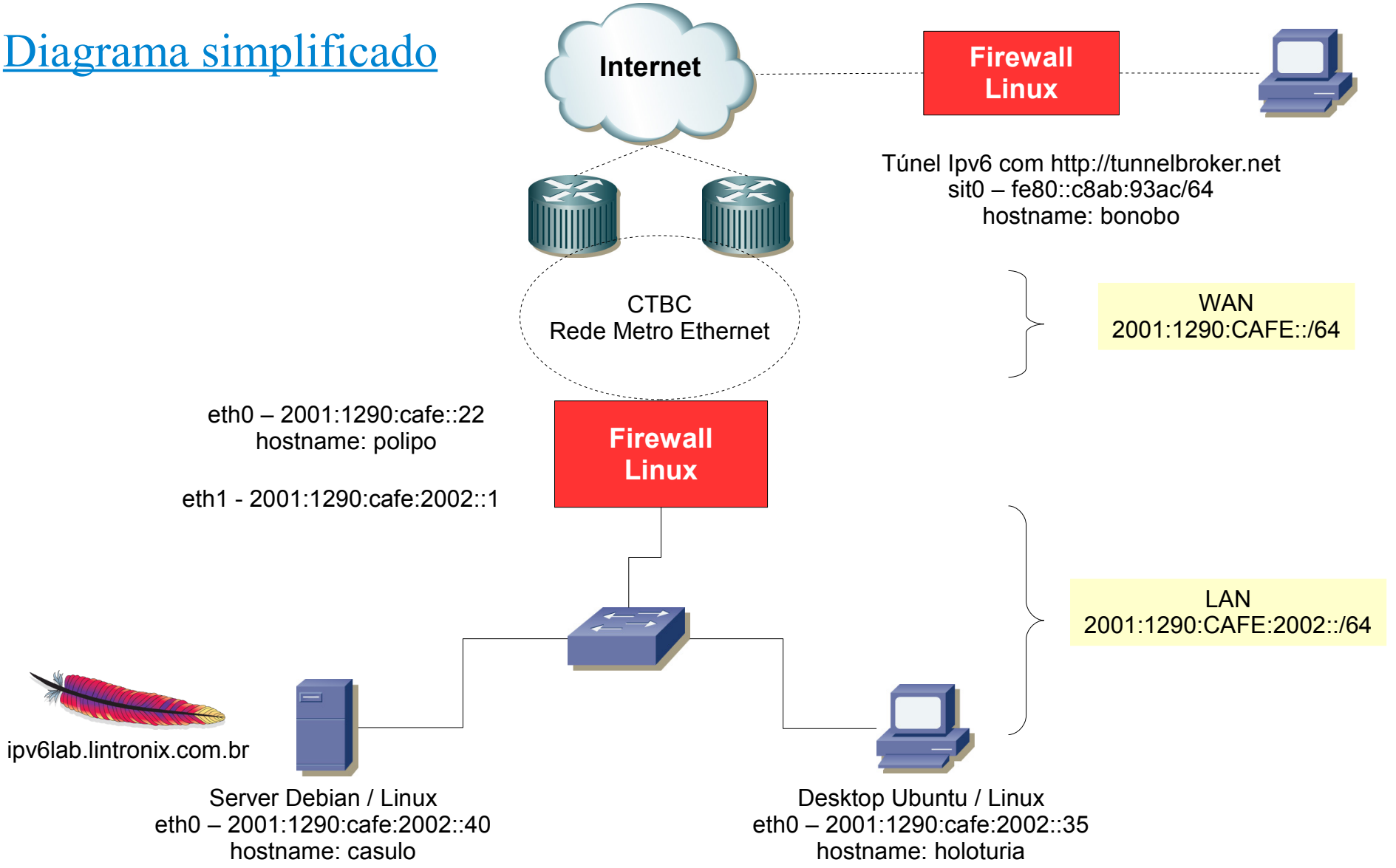
```
# ip6tables -v -n -L
Chain INPUT (policy DROP 7 packets, 560 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0        lo     *       ::/0       ::/0
   11   752 ACCEPT     icmpv6    *      *       ::/0       ::/0
   14  1145 ACCEPT     udp      *      *       ::/0       ::/0       udp dpt:53
    0     0 ACCEPT     tcp      *      *       ::/0       ::/0       tcp dpt:53
   21  2225 ACCEPT     tcp      *      *       ::/0       ::/0       tcp dpt:80
    0     0 ACCEPT     tcp      *      *       ::/0       ::/0       tcp dpt:80
    0     0 ACCEPT     0        *      *       ::/0       ::/0       state RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0        *      lo      ::/0                 ::/0
   11   744 ACCEPT     icmpv6    *      *       ::/0                 ::/0
   14  2567 ACCEPT     udp      *      *       ::/0                 ::/0          udp spt:53
    0     0 ACCEPT     tcp      *      *       ::/0                 ::/0          tcp spt:53
   21  4304 ACCEPT     tcp      *      *       ::/0                 ::/0          tcp spt:80
    0     0 ACCEPT     tcp      *      *       ::/0                 ::/0          tcp spt:80
    0     0 ACCEPT     0        *      *       ::/0                 ::/0          state NEW,ESTABLISHED
#
```

CTBC AS27664 IPv6 – Caso CTBC – Teste Servidor Apache 80 e 8080 /tcp - 3/3

```
From: inet6 addr: 2001:1290:cafe::20

$ telnet ctbcv6.com.br 80
Trying 2001:1290:cafe::1001...
Connected to ctbcv6.com.br.
Escape character is '^]'.
GET /
<html>
<body>

<h1>CTBCv6.com.br</h1>

</body>
</html>
Connection closed by foreign host.
$


$ telnet ctbcv6.com.br 8080
Trying 2001:1290:cafe::1001...
$
```

Caso Lintronix - IPv6 – Laboratório e testes.

Diagrama simplificado



Host: polipo

ifconfig

```
root@polipo:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:15:C5:EB:D4:49
          inet addr:189.39.63.22  Bcast:189.39.63.31  Mask:255.255.255.240
          inet6 addr: 2001:1290:cafe::22/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:425778 errors:0 dropped:0 overruns:0 frame:0
          TX packets:299787 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:371148285 (353.9 MB)  TX bytes:38274700 (36.5 MB)
          Interrupt:16 Memory:f8000000-f8012100
```

** *Em vermelho, destaca-se o endereço IPv6 desta interface*

Host: polipo

ifconfig

```
root@polipo:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:15:C5:EB:D4:4B
          inet addr:189.39.63.33  Bcast:189.39.63.47  Mask:255.255.255.240
          inet6 addr: 2001:1290:cafe:2002::1/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:254148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:384914 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30087689 (28.6 MB)  TX bytes:387193430 (369.2 MB)
          Interrupt:16 Memory:f4000000-f4012100
```

** *Em vermelho, destaca-se o endereço IPv6 desta interface*

Host: polipo – interface loopback - ::1/128

ifconfig

```
root@polipo:~# ifconfig lo
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:90 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12720 (12.4 KB)  TX bytes:12720 (12.4 KB)
```

** *Em vermelho, destaca-se o endereço IPv6 desta interface*

Host: bonobo – Túnel criado com http://tunnelbroker.net

ifconfig

```
root@bonobo:~# ifconfig sit1
sit1   Encapsulamento do Link: IPv6 sobre Ipv4                  <---- Túnel
          endereço inet6: 2001:470:1f06:5d9::2/64 Escopo:Global
          UP POINTOPOINT RUNNING NOARP  MTU:1480  Métrica:1
          RX packets:14870 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23540 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:0
          RX bytes:1923335 (1.8 MiB)  TX bytes:25521844 (24.3 MiB)
```

** *Em vermelho destaca-se o endereço IPv6 desta interface.*
** *Ao iniciar o túnel, cria-se uma interface sit1 (IPv6 sobre IPv4)*

Host: polipo

ip

```
root@polipo:~# ip -6 route show
2001:1290:cafe::/64 dev eth0  metric 256  expires -593067sec mtu 1500 advmss
1440 hoplimit 4294967295
2001:1290:cafe:2002::/64 dev eth1  metric 256  expires -593067sec mtu 1500
advmss 1440 hoplimit 4294967295
fe80::/64 dev eth0  metric 256  expires -593066sec mtu 1500 advmss 1440
hoplimit 4294967295
fe80::/64 dev eth1  metric 256  expires -593066sec mtu 1500 advmss 1440
hoplimit 4294967295
default via 2001:1290:cafe::1 dev eth0  metric 1  expires -593066sec mtu 1500
advmss 1440 hoplimit 4294967295
```

** *Em vermelho destaca-se a rota default*
Ver: http://tldp.org/HOWTO/Linux+IPv6-HOWTO/x1070.html

Host: polipo

ping6

```
root@polipo:~# ping6 -c 5 2001:1290:cafe:2002::40
PING 2001:1290:cafe:2002::40(2001:1290:cafe:2002::40) 56 data bytes
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=1 ttl=64 time=3.97 ms
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=2 ttl=64 time=0.343 ms
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=3 ttl=64 time=0.494 ms
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=4 ttl=64 time=0.417 ms
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=5 ttl=64 time=0.625 ms

--- 2001:1290:cafe:2002::40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.343/1.170/3.972/1.404 ms
```

Host: bonobo

ping6

```
root@bonobo:~# ping6 -c 5 2001:1290:cafe:2002::40
PING 2001:1290:cafe:2002::40(2001:1290:cafe:2002::40) 56 data bytes
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=1 ttl=57 time=382 ms
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=2 ttl=57 time=375 ms
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=3 ttl=57 time=374 ms
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=4 ttl=57 time=378 ms
64 bytes from 2001:1290:cafe:2002::40: icmp_seq=5 ttl=57 time=375 ms

--- 2001:1290:cafe:2002::40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 374.474/377.232/382.060/2.753 ms
```

** *Observa-se alta latência devido ao túnel.*

Host: bonobo

ping6 – Captura de pacotes com tcpdump

```
root@bonobo:~#
tcpdump -n -s0 -i sit1 -w tcpdump-ping6-cafe22.tcp host 2001:1290:cafe::22
```

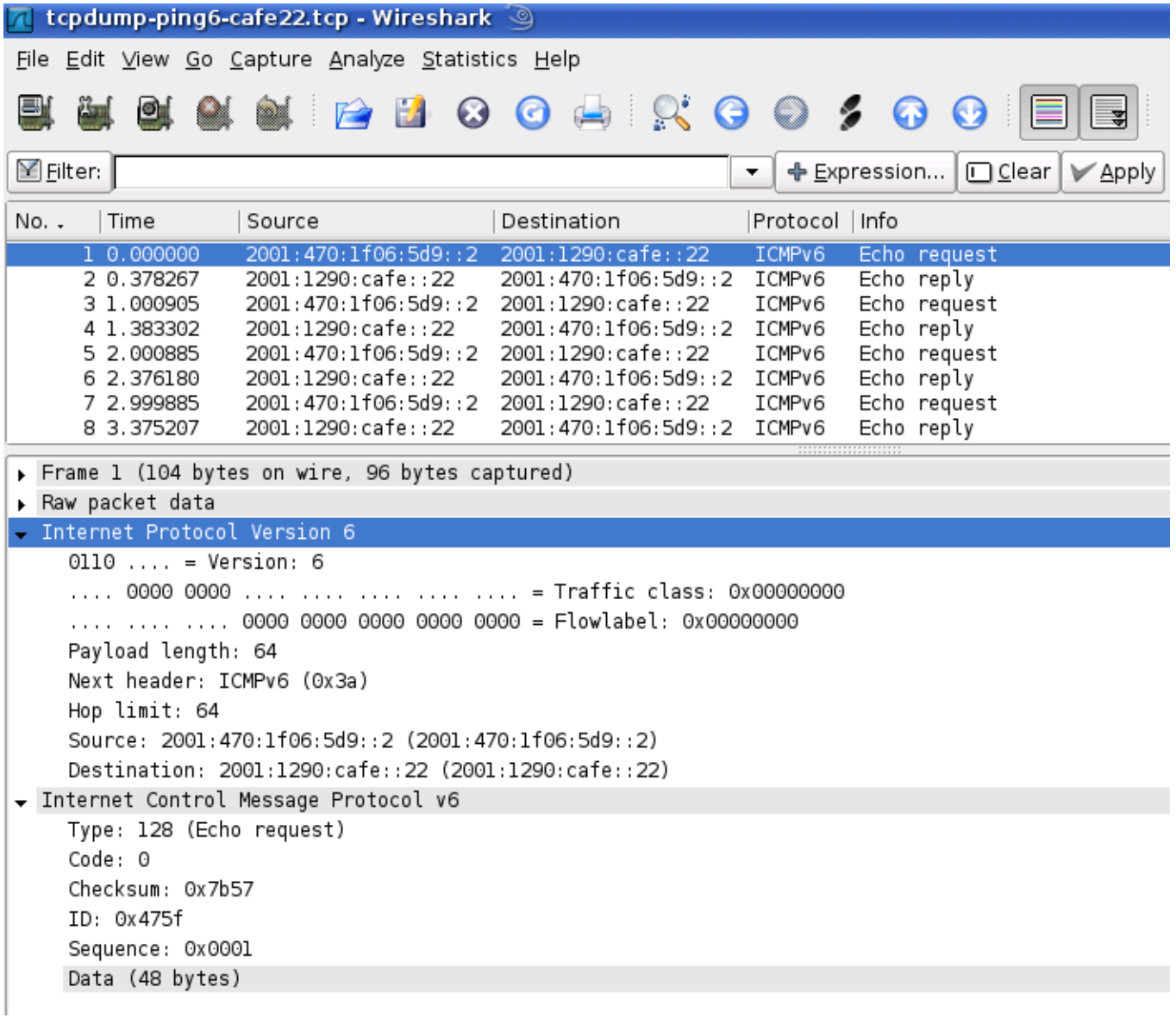
O comando acima escuta na interface sit0, e escreve o conteúdo em um arquivo chamado tcpdump-ping6-cafe22.tcp, filtrando apenas os pacotes com destino ao host polipo (2001:1290:cafe::22). O conteúdo pode ser visualizado com o aplicativo gráfico Wireshark.

Caso Lintronix - IPv6 – Linha de comando

Host: bonobo

ping6

Wireshark:



Host: polipo

ssh

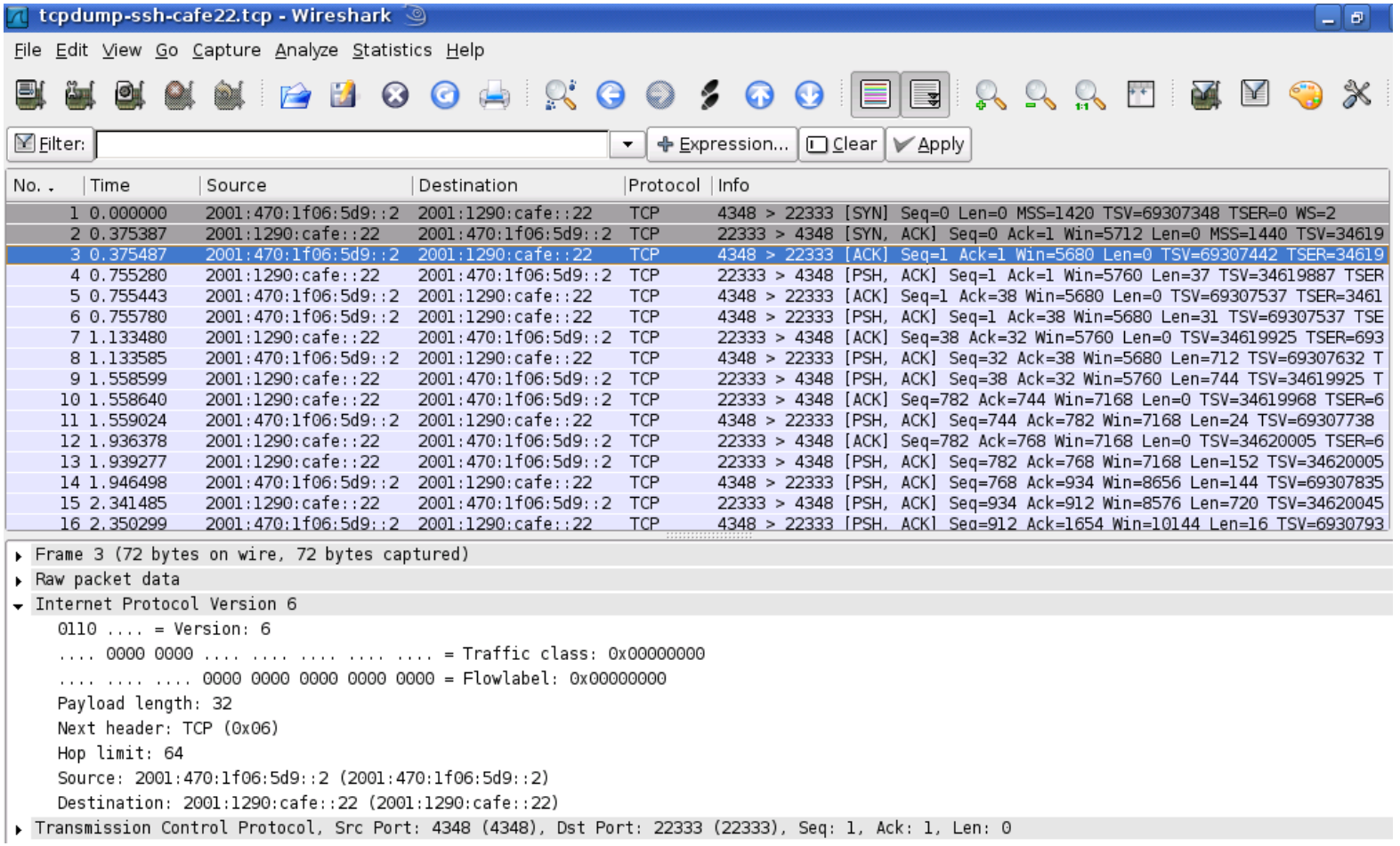
```
root@polipo:~# ssh 2001:1290:cafe:2002::40 -l userlab -p 22
userlab@2001:1290:cafe:2002::40's password:
Linux casulo 2.6.18-6-686 #1 SMP Sun Feb 10 22:11:31 UTC 2008 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat May 24 11:05:33 2008 from coral.lintronix.com.br
userlab@casulo:~$
```

Caso Lintronix - IPv6 – Linha de comando

Host: polipo

ssh

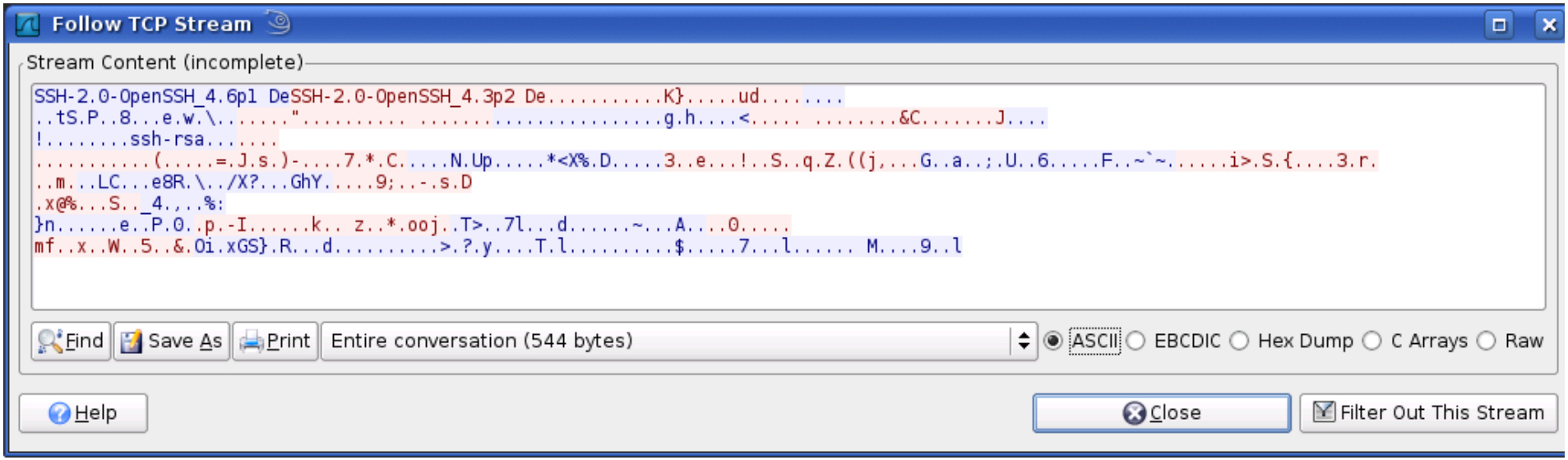
Wireshark



Host: polipo

ssh

Wireshark



Host:bonobo

scp

```
root@bonobo:~# scp -P 22 arquivo.tar.gz userlab@\
[2001:1290:cafe:2002::40\]:/home/userlab
userlab@2001:1290:cafe:2002::40's password:
arquivo.tar.gz                                100% 75360KB  33.3KB/s   10:08
ETA
root@bonobo:~#
```

Host:casulo

netstat

```
casulo:~# netstat -ant
Active Internet connections (servers and established)
Proto   Local Address                Foreign Address      State   PID/Program
name
tcp     0.0.0.0:37634                0.0.0.0:*            LISTEN  2127/rpc.statd
tcp     0.0.0.0:111                  0.0.0.0:*            LISTEN  1640/portmap
tcp     189.39.63.40:80              0.0.0.0:*            LISTEN  2254/apache2
tcp     0.0.0.0:113                  0.0.0.0:*            LISTEN  2098/inetd
tcp     127.0.0.1:25                 0.0.0.0:*            LISTEN  2086/exim4
tcp     189.39.63.40:443             0.0.0.0:*            LISTEN  2254/apache2
tcp6    2001:1290:cafe:2002::80      :::*                 LISTEN  2254/apache2

tcp6    2001:1290:cafe:2002:443      :::*                 LISTEN  2254/apache2

tcp6    :::22                        :::*                 LISTEN  2108/sshd
```

Host:casulo

nmap

```
casulo:~# nmap  -6 -sT 2001:1290:cafe:2002::40

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2008-05-24 11:44 BRT
Interesting ports on ipv6lab.lintronix.com.br (2001:1290:cafe:2002::40):
Not shown: 1678 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap finished: 1 IP address (1 host up) scanned in 0.174 seconds
casulo:~#
```

Host:casulo

nmap

```
casulo:~# nmap  -6 -sT 2001:1290:cafe::22

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2008-05-24 11:46 BRT
All 1680 scanned ports on polipo.lintronix.com.br (2001:1290:cafe::22) are
closed

Nmap finished: 1 IP address (1 host up) scanned in 1.403 seconds
casulo:~#
```

Host:casulo

lynx

Testamos o aplicativo lynx para navegação em modo texto e acesso ao sítio ipv6lab.lintronix.com.br hospedado na máquina casulo, a partir da máquina bonobo.

O aplicativo navega sem problemas, ou necessidade de configurações adicionais.

Para Navegar digitando o IP:

http://[2001:1290:cafe:2002::40]/

```
root@firewall:~# lynx http://[2001:1290:cafe:2002::40]/
```

Host: polipo

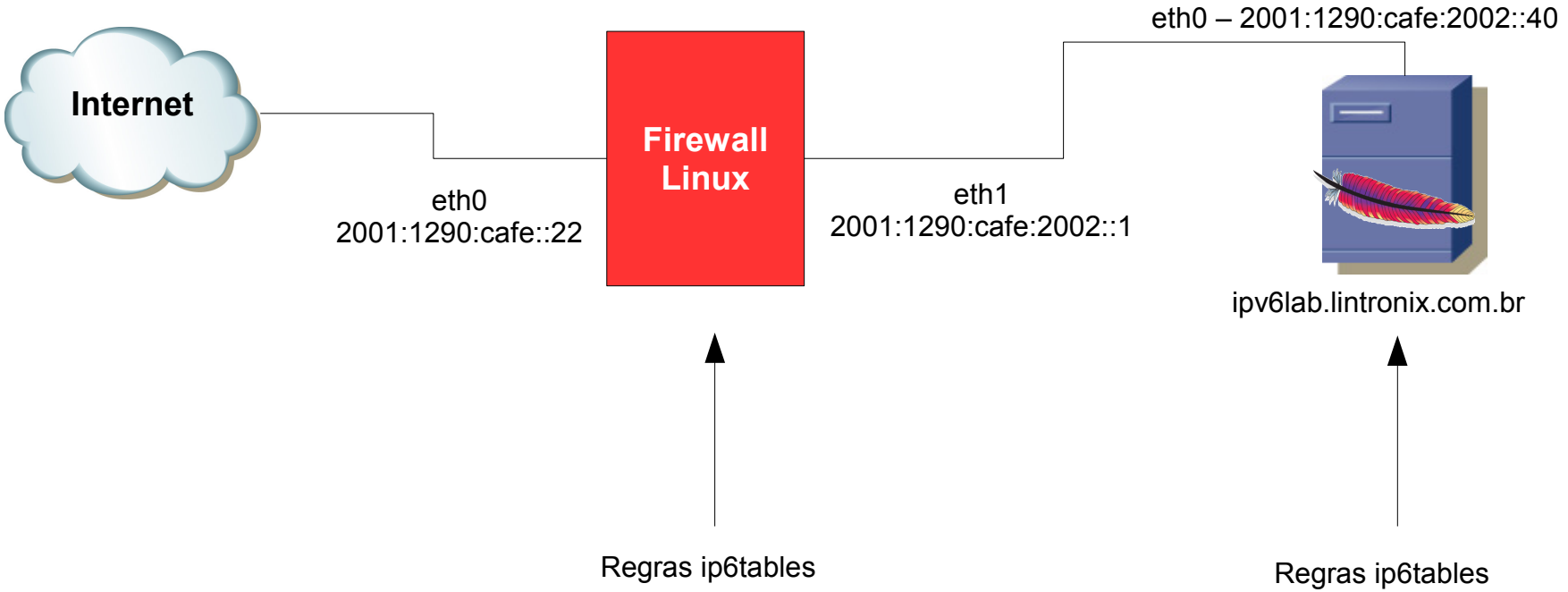
ip6tables

Para criação das regras de firewall em IPv6, utilizamos no LINUX o ip6tables, o qual já acompanha o iptables – v1.3.6

De modo geral, a grafia das regras ip6tables é idêntica à do iptables.

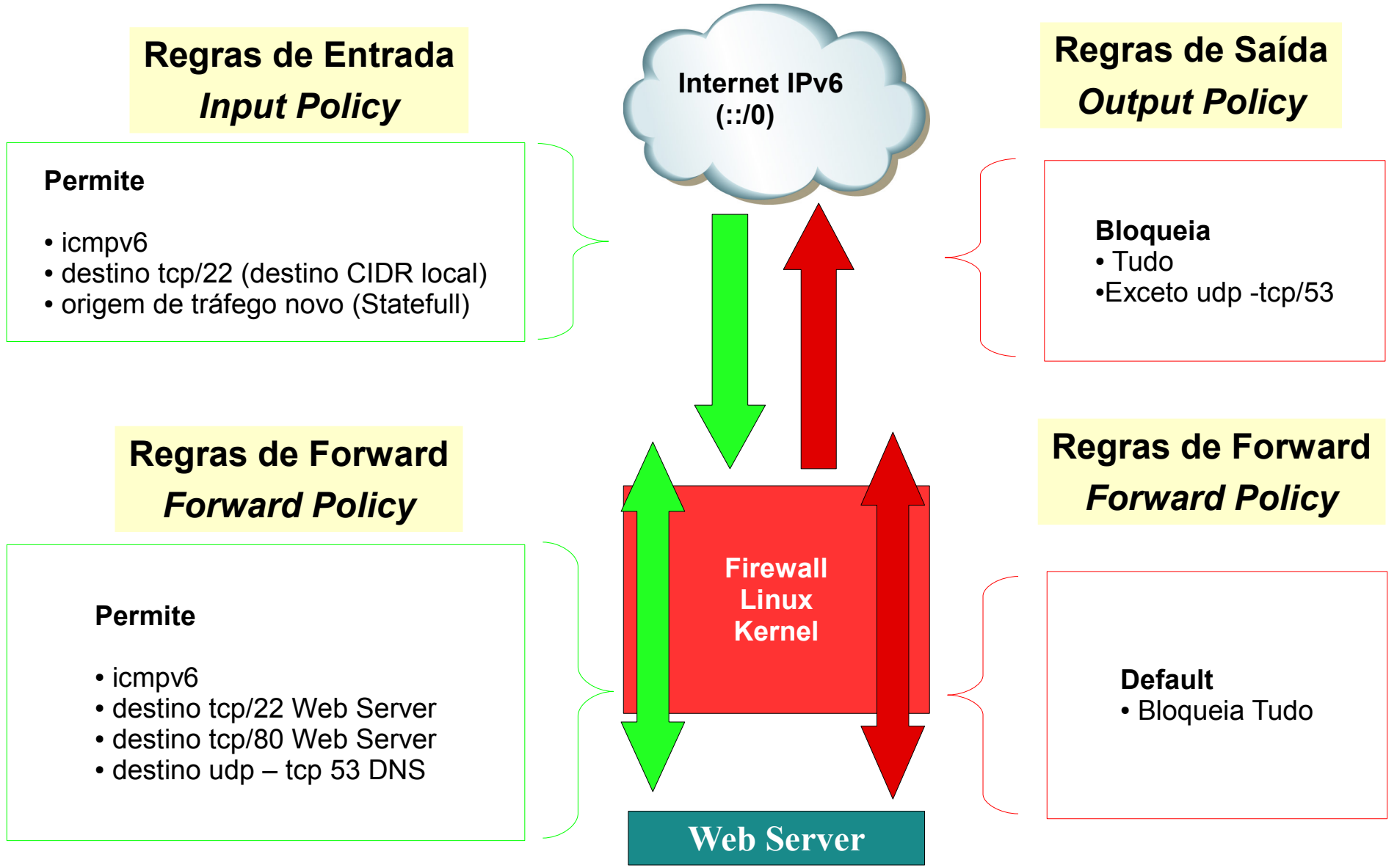
```
root@firewall:~# lynx http://[2001:1290:cafe:2002::40]/
```

Caso Lintronix - IPv6 – Firewall



Por tratar-se de um laboratório, simplificamos ao máximo as regras.
Avaliamos algumas regras bem simplificadas apenas para fins didátios.
Os scripts em bash funcionaram normalmente, podendo designar variáveis.
Não recomendamos rodar um firewall apenas com estas regras.

Caso Lintronix - IPv6 – Firewall – Diagrama Lógico



Caso Lintronix - IPv6 – Firewall – Regras

```
# Loopback
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT


# Statefull Firewall
ip6tables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT
```

Caso Lintronix - IPv6 – Firewall – Regras

```
# Politica default
ip6tables -F
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# Trafego para a interface de loopback
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT

# ICMPv6
ip6tables -A INPUT -p icmpv6 -m limit --limit 1/second -j ACCEPT
ip6tables -A OUTPUT -p icmpv6 -m limit --limit 1/second -j ACCEPT
```

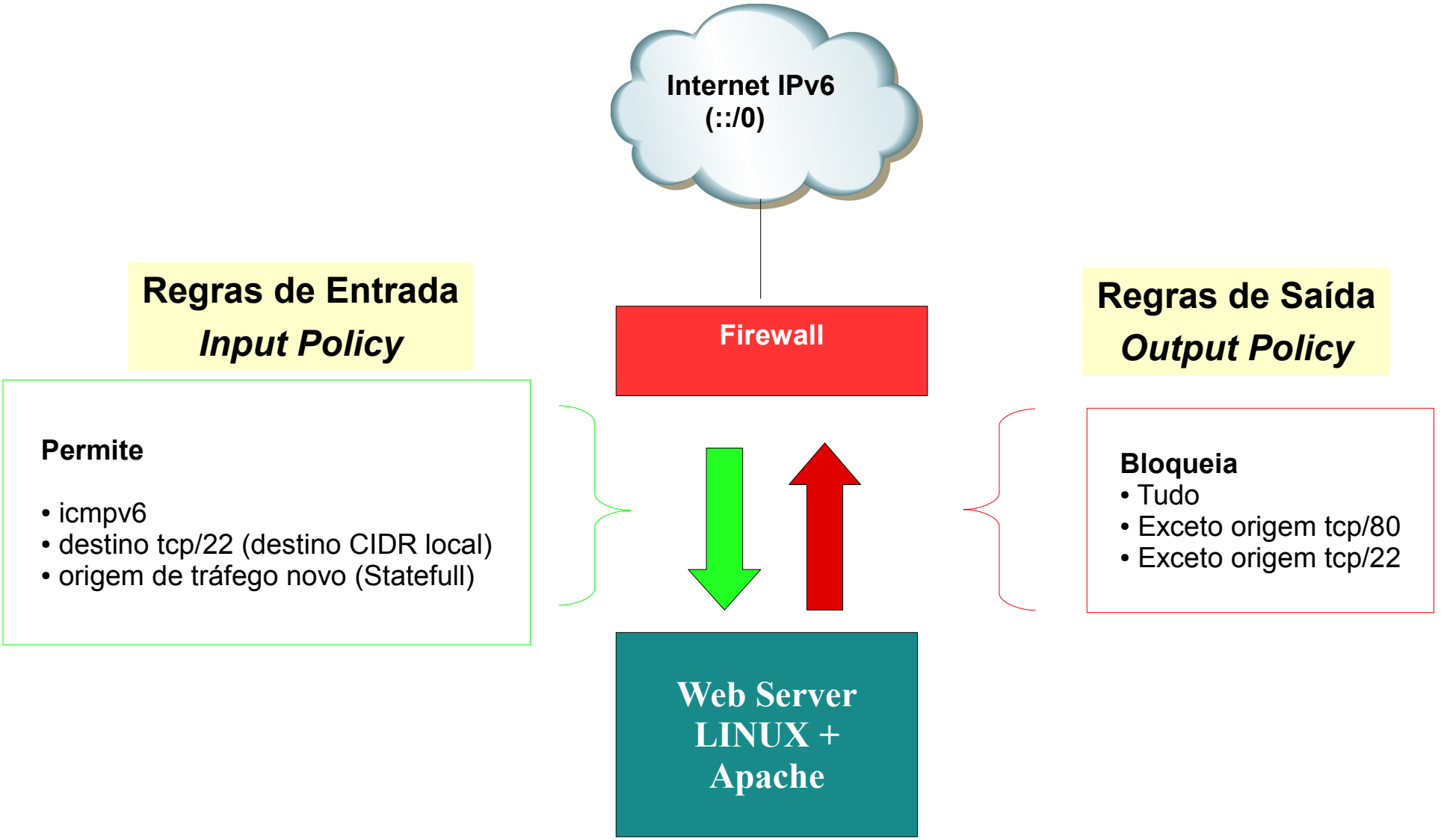
Caso Lintronix - IPv6 – Firewall – Regras

```
# Ping da Internet para o servidor WEB
ip6tables -A FORWARD -d 2001:1290:cafe:2002::40 -p icmpv6 \
-m limit --limit 1/second -j ACCEPT

# Ping do Servidor WEB para Internet
ip6tables -A FORWARD -s 2001:1290:cafe:2002::40 -p icmpv6 \
-m limit --limit 1/second -j ACCEPT
```

Caso Lintronix - IPv6 – Firewall – Regras

```
# Acesso da Internet ao servidor WEB (porta 80)
ip6tables -A FORWARD -s 2001:1290:cafe:2002::40 -p tcp --sport 80 -j ACCEPT
ip6tables -A FORWARD -d 2001:1290:cafe:2002::40 -p tcp --dport 80 -j ACCEPT

# Acesso ao serviço SSH (porta 22)
ip6tables -A FORWARD -s 2001:1290:cafe:2002::40 -p tcp --sport 22 -j ACCEPT
ip6tables -A FORWARD -d 2001:1290:cafe:2002::40 -p tcp --dport 22 -j ACCEPT
```

Caso Lintronix - IPv6 – Firewall – Diagrama Lógico



Caso Lintronix - IPv6 – Web Server – Regras

```
# Loopback
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT


# Statefull Firewall
ip6tables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT
```

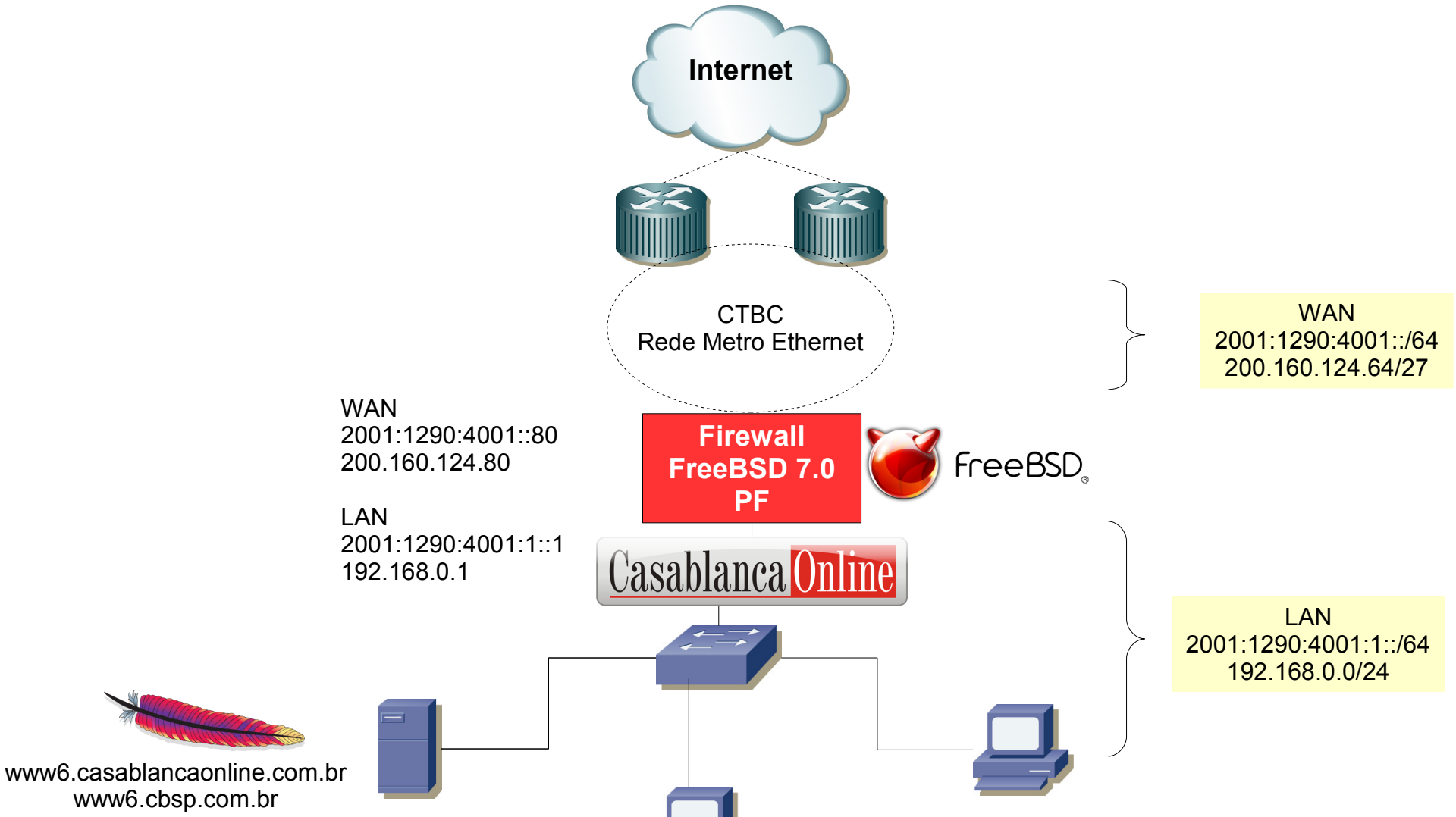
Caso Lintronix - IPv6 – Web Server – Regras

```
# Politica default
ip6tables -F
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# Trafego para a interface de loopback
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT

# ICMPv6
ip6tables -A INPUT -p icmpv6 -m limit --limit 1/second -j ACCEPT
ip6tables -A OUTPUT -p icmpv6 -m limit --limit 1/second -j ACCEPT
```

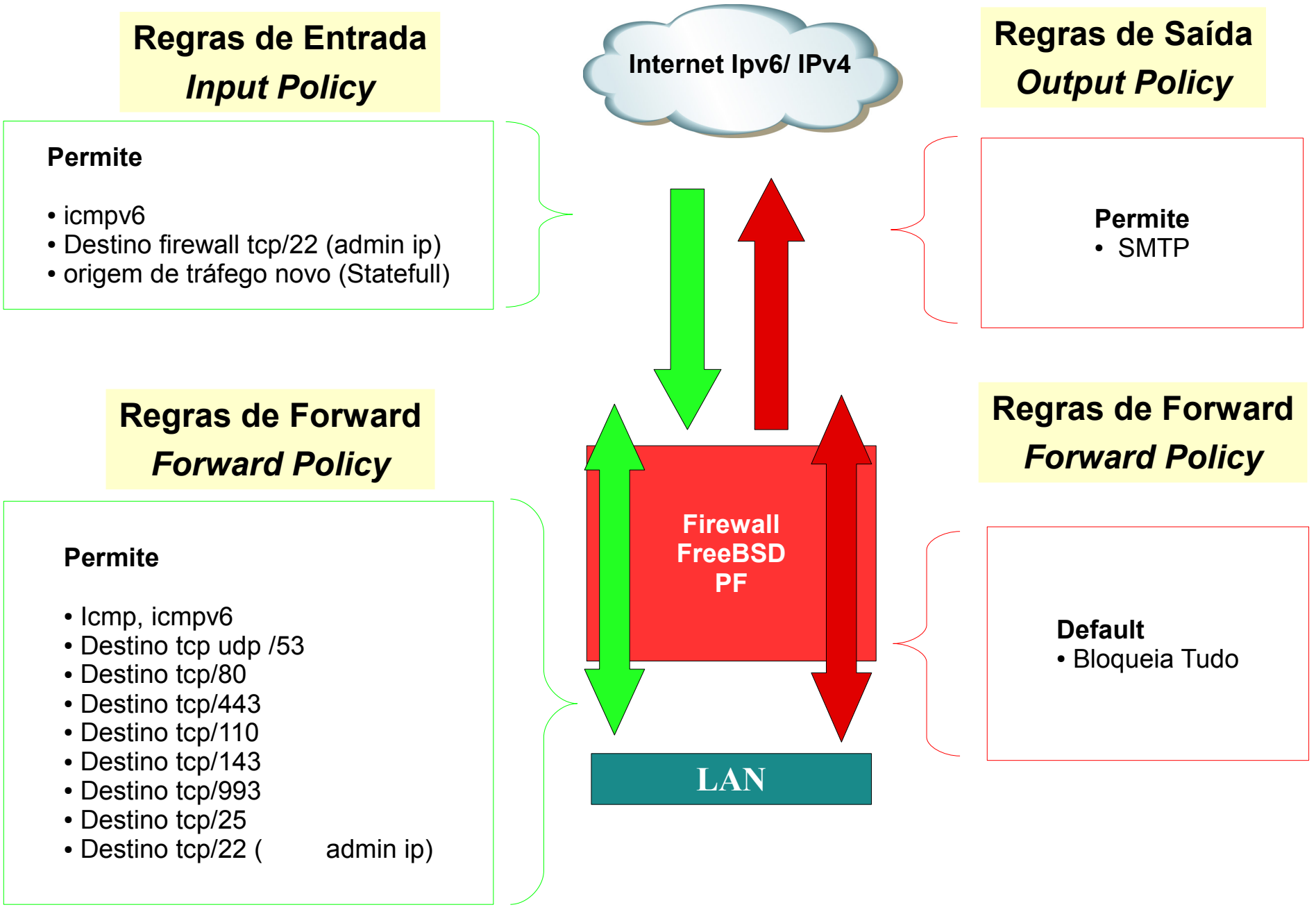
Caso Lintronix - IPv6 – Web Server – Regras

```
# Input
# SSH
ip6tables -A INPUT -p tcp -m tcp -d 2001:1290:cafe:2002::40 \
--dport 22 -j ACCEPT
# HTTP
ip6tables -A INPUT -p tcp -m tcp -d 2001:1290:cafe:2002::40 \
--dport 80 -j ACCEPT


#Output
# SSH
ip6tables -A OUTPUT -p tcp -m tcp -s 2001:1290:cafe:2002::40 \
 --sport 22 -j ACCEPT
# HTTP
ip6tables -A OUTPUT -p tcp -m tcp -s 2001:1290:cafe:2002::40 \
--sport 80 -j ACCEPT
```

Casablanca Online (dualstacked firewall) – Diagrama Lógico de Rede



Casablanca Online – Diagrama Lógico – Firewall Ipv6, IPv4



Casablanca Online – Regras de Firewall FreeBSD (Packet filter) 1/6

```
# Dualstacked firewall baseado em  https://solarflux.org/pf/pf+IPv6.php
# * = Consultar topico no documento acima

extif = "xl0"                              # Interface externa (WAN)
intif = "xl1"                              # Interface intena  (LAN)

# * Vide 3.3.1.a Macros
# IPV6 macros
extip6    = "2001:1290:4001::80"           # IPv6 externo (WAN)
intip6    = "2001:1290:4001:1::1"          # IPv6 interno (LAN)
intnet6   = "2001:1290:4001:1::/64"        # IPV6 Endereco de rede (LAN)
ispdns6   = "2001:1290:4001::cb"           # IPv6 Servidor de dns
intwww6   = "2001:1290:4001:1::cb"         # IPv6 servidor web (LAN)
intadmin6 = "2001:1290:4001:1::50"         # IPv6 Computador SysAdmin (LAN)
extadmin6 = "xxx:xxx:xxx::xx"              # IPv6 Computador SysAdmin (LAN)

# IPV4 macros
extip4="200.160.124.80"                    # IPv4 externo (WAN)
intip4="192.168.0.1"                       # Ipv4 interno (LAN)
intnet4="192.168.0.0/24"                    # IPv4 Endereco de rede (LAN)
ispdns4="200.160.124.69"                   # IPv6 Servidor de dns
intwww4="192.168.0.10"                      # IPv4 servidor web (LAN)
intadmin4="192.168.0.50"                    # IPv4 Computador SysAdmin (LAN)
extadmin4="xxx.xxx.xxx.xxx"                  # IPv4 Computador SysAdmin (WAN)

# Protocolos permitidos para acesso externo: WWW, SSL, POP3, IMAP, IMAPS, SMTP
# * Vide 3.3.2.b State Modulation
allowed_ports = "{ 80, 443, 110, 143, 993, 25 }"
```

Casablanca Online – Regras de Firewall FreeBSD (Packet filter) 2/6

```
# http://www.openbsd.org/faq/pf/scrub.html
scrub in all

# Habilita nat IPv4
nat on $extif inet from $intnet4 to any -> $extip4

# Port Forward para www interno (IPv4)
rdr on $extif inet proto tcp from any to $extip4 port 80 -> $intwww4 port 80

# * Vide: 3.3.2.c Antispoofing
antispoof for lo0
antispoof for sk0 inet
antispoof for xl1 inet

# Nega tudo
block in log all


# Avisa daemons que tentam conectar no identd que o servico esta bloqueado e evita delay
# * Vide: 3.3.1.c Block return-rst
block return-rst in log on $extif inet6 proto tcp from any to any port = 113
block return-rst in log on $extif inet  proto tcp from any to any port = 113
```

Casablanca Online – Regras de Firewall FreeBSD (Packet filter) 3/6

```
# Permite passar/entrar consulta dns pela interface LAN
pass in on $intif inet6 proto udp from $intnet6 to $ispdns6 port = 53
pass in on $intif inet  proto udp from $intnet4 to $ispdns4 port = 53

# Permite passar/sair consulta dns pela interface WAN
pass out on $extif inet6 proto udp from { $extip6, ::1, $intnet6 }       to $ispdns6 port = 53 keep state
pass out on $extif inet  proto udp from { $extip4, 127.0.0.1, $intnet4 } to $ispdns4 port = 53 keep state

# Permite firewall enviar emails
pass out on $extif inet6 proto tcp from { $extip6, ::1 }       to any port = 25 keep state
pass out on $extif inet  proto tcp from { $extip4, 127.0.0.1 } to any port = 25 keep state

# Permite passar/entrar protocolo icmp pela interface LAN
pass in on $intif inet6 proto ipv6-icmp all icmp6-type { 128, 129, 135, 136 }
pass in on $intif inet  proto icmp      all icmp-type  8 code 0

# Permite passar entrada/saida protocolo icmp pela interface WAN
pass in  on $extif inet6 proto ipv6-icmp all icmp6-type { 134, 135, 136 }
pass in  on $extif inet  proto icmp      all
pass out on $extif inet6 proto ipv6-icmp all icmp6-type { 128, 136 } keep state
pass out on $extif inet  proto icmp      all icmp-type 8 code 0 keep state
```

Casablanca Online – Regras de Firewall FreeBSD (Packet filter) 4/6

```
# Permite computador do SysAdmin trafegar ssh (para ofirewall inclusive)

pass in log on $intif inet6 proto tcp from $intadmin6 to any port = 22 keep state
pass in log on $intif inet  proto tcp from $intadmin4 to any port = 22 keep state

# Permite acesso remoto do SysAdmin via ssh no firewall a partir da WAN
pass in on $extif inet6 proto tcp from $extadmin6 to $extip6 port = 22
pass in on $extif inet  proto tcp from $extadmin4 to $extip4 port = 22
```

Casablanca Online – Regras de Firewall FreeBSD (Packet filter) 5/6

```
# Permite passagem pelo firewall dos protocolos permitidos
pass in  on $intif inet6 proto tcp from $intnet6 to any port $allowed_ports
pass in  on $intif inet  proto tcp from $intnet4 to any port $allowed_ports
pass out on $extif inet6 proto tcp from $intnet6 to any port $allowed_ports keep state
pass out on $extif inet  proto tcp from $intnet4 to any port $allowed_ports keep state
```

Casablanca Online – Regras de Firewall FreeBSD (Packet filter) 6/6

```
# Permite acesso ao servior web interno via IPv6
pass in on $intif inet6 proto tcp from $intwww6 port = 80 to any keep state
pass in on $extif inet6 proto tcp from any to $intwww6 port = 80 keep state
```

Casablanca Online – Testes NMAP 1/2

```
Teste IPV6: A partir da rede Interna (Maquina do SysAdmin)

nmap -P0 -sT -6 2001:1290:4001:1::1

Starting Nmap 4.53 ( http://insecure.org ) at 2008-05-31 18:55 BRT
Interesting ports on fw6lan.casablancaonline.com.br (2001:1290:4001:1::1):
Not shown: 1712 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
```

Casablanca Online – Testes NMAP 2/2

```
Teste IPV6: A partir da rede externa

nmap -P0 -sT -6 2001:1290:4001::80

Starting Nmap 4.53 ( http://insecure.org ) at 2008-05-31 19:03 BRT
Interesting ports on fw6.casablancaonline.com.br (2001:1290:4001::80):
Not shown: 1713 filtered ports
PORT    STATE  SERVICE
113/tcp closed auth
```

Casablanca Online – Instalação de pacotes

```
Antes de configurar Ipv4 a configuracao estava assim:

#ifconfig xl0
xl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=b<RXCSUM,TXCSUM,VLAN_MTU>
        ether 00:60:08:cb:87:2f
        inet6 fe80::213:d4ff:fe6c:dd21%sk0 prefixlen 64 scopeid 0x3
        inet6 2001:1290:4001::80 prefixlen 64
        media: Ethernet autoselect (100baseTX <full-duplex>)
        status: active

# netstat -rn | grep default

Destination                       Gateway                       Flags      Netif Expire
default                           2001:1290:4001::1             UGS         xl0

# host www.freebsd.org
www.freebsd.org has address 69.147.83.33
www.freebsd.org has IPv6 address 2001:4f8:fff6::21

# host ftp.freebsd.org
ftp.freebsd.org has address 204.152.184.73
ftp.freebsd.org has address 62.243.72.50
ftp.freebsd.org has IPv6 address 2001:4f8:0:2::e
ftp.freebsd.org has IPv6 address 2001:6c8:6:4::7

Desta forma foi possivel instalar programas sem necessidade de Ipv4, uma vez que os servidores de ftp
do projeto FreeBSD possuem suporte a Ipv6

Ex:

# pkg_add -r nmap
Fetching ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-stable/Latest/nmap.tbz... Done.
Fetching ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-stable/All/libdnet-1.11_1.tbz... Done.
Fetching ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7-stable/All/pcre-7.7.tbz... Done.
```

CTBC AS27664 IPv6 – Sugestões de URL & Agradecimentos

CTBC - *Eduardo Ascenço Reis*

http://ctbcv6.com.br/

http://lg.ctbcv6.com.br/

Casablanca - *Pablo Martins Figueiredo da Costa*

http://www6.cbsp.com.br/

http://www6.casablancaonline.com.br/

http://ipv6.casablancaonline.com.br/

Lintronix - *Claudio Corrêa Porto*

http://ipv6lab.lintronix.com.br/

http://www.ipv6forum.com.br/