Linux firewalls made easy with FireHOL

Como implementar firewalls iptables não-triviais sem perder a sanidade!

Carlos Rodrigues
cefrodrigues@gmail.com

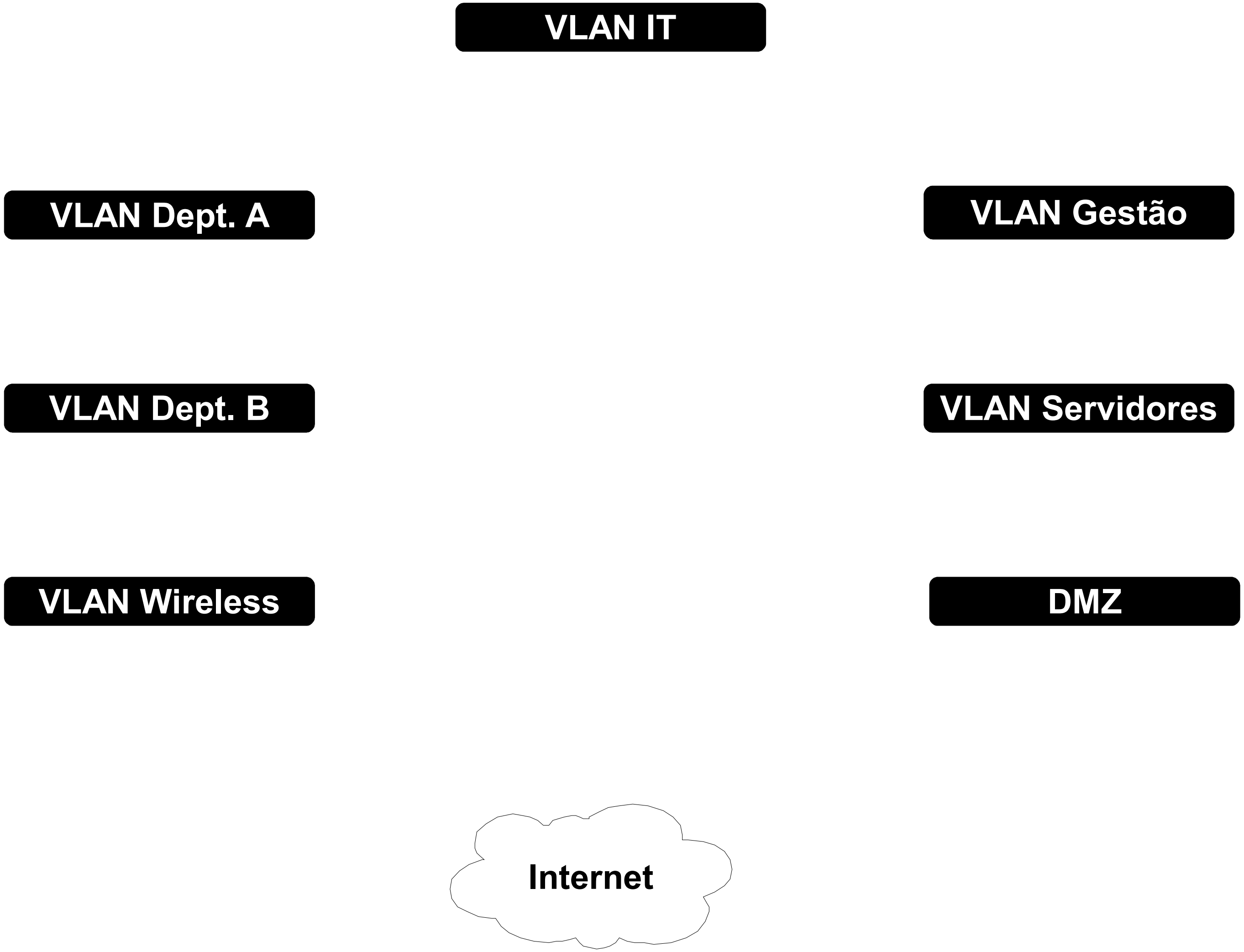
FCT barcamp
24 Maio, 2008

Porquê?

iptables

```
iptables --policy INPUT DROP
iptables --policy OUTPUT ACCEPT
iptables --policy FORWARD DROP

iptables -A INPUT -i lo -j ACCEPT

iptables -N in_lan
iptables -A INPUT -i eth0 -j in_lan

iptables -N in_world
iptables -A INPUT -i eth1 -j in_world

iptables -A in_lan -p icmp -j ACCEPT
iptables -A in_lan -p tcp --dport ssh -j ACCEPT
iptables -A in_lan -p tcp -m multiport --dport http,https -j ACCEPT
iptables -A in_lan -j REJECT

iptables -A in_world -p tcp -m multiport --dport http,https -j ACCEPT
```

Imaginem...


VLAN IT

VLAN Dept. A

VLAN Gestão

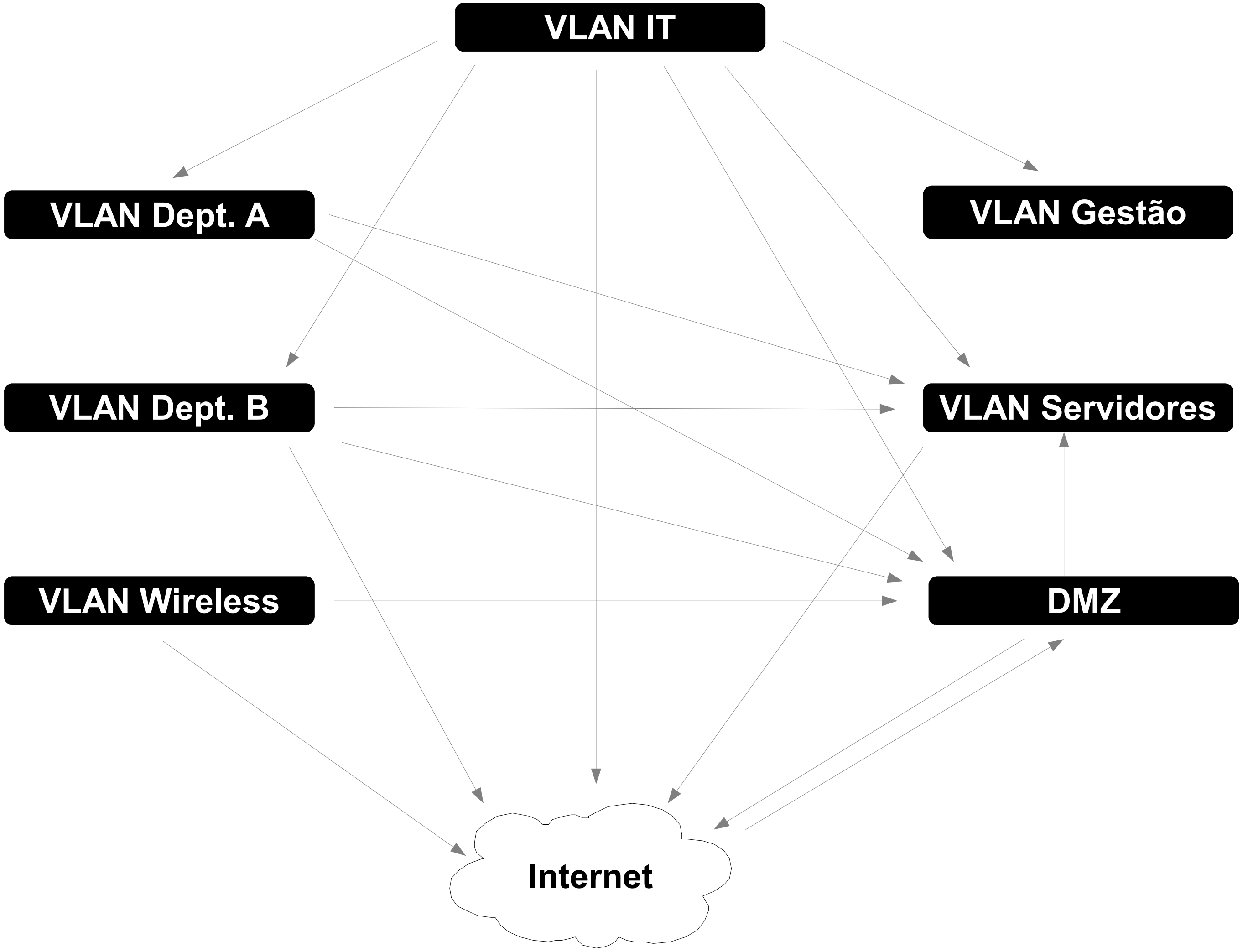
VLAN Dept. B

VLAN Servidores

VLAN Wireless

DMZ

Internet



Carlos Rodrigues
cefrodrigues@gmail.com

FireHOL

http://firehol.sourceforge.net

Carlos Rodrigues
cefrodrigues@gmail.com

Instalação

```
# Instalar...
aptitude install ulogd    # opcional
aptitude install firehol

# Activar...
sed -i s/START_FIREHOL=NO/START_FIREHOL=YES/ /etc/default/firehol

# Configurar...
cd /etc/firehol
editor firehol.conf
```

/etc/firehol/firehol.conf

```
version 5

FIREHOL_LOG_MODE="ULOG"
FIREHOL_LOG_FREQUENCY="6/minute"
FIREHOL_LOG_BURST="3"

interface eth0 lan
    policy reject
    protection strong 100/sec 50

    server icmp accept

    server ssh accept
    server “http https“ accept

    client all accept

interface eth1 world
    policy drop
    protection strong 100/sec 50

    server “http https“ accept

    client all accept
```

/etc/firehol/firehol.conf

```
interface eth0 lan
    policy reject
    protection strong 100/sec 50

    server icmp accept
    server ssh accept

    client all accept

interface eth1 world
    policy drop

    client all accept


router lan-to-world inface eth0 outface eth1
    masquerade

    route all accept
```

/etc/firehol/firehol.conf

```
lan_if=”eth0”
world_if=”eth1”

interface “${lan_if}” lan
    policy reject
    protection strong 100/sec 50

    server icmp accept
    server ssh accept

    client all accept

interface “${world_if}” world
    policy drop

    client all accept


router lan-to-world inface “${lan_if}” outface “${world_if}”
    masquerade

    route all accept
```

/etc/firehol/firehol.conf

```
lan_network=”192.168.1.0/24”
...

interface “${lan_if}” lan dst “${lan_ip}”
    policy reject
    protection strong 100/sec 50

    server icmp accept
    server ssh accept

    client all accept

interface “${world_if}” world src not "${lan_network}"
    policy drop

    client all accept


router lan-to-world inface “${lan_if}” outface “${world_if}” src “${lan_network}”
    masquerade

    route all accept
```

/etc/firehol/firehol.conf

```
...
snat to "${nat_address}" outface "${world_if}" src "${lan_network}”

interface “${lan_if}” lan dst “${lan_ip}”
    policy reject
    protection strong 100/sec 50

    server icmp accept
    server ssh accept

    client all accept

interface “${world_if}” world dst “${world_ip}” src not "${lan_network}"
    policy drop

    client all accept


router lan-to-world inface “${lan_if}” outface “${world_if}” src “${lan_network}”
    route all accept
```

/etc/firehol/firehol.conf

```
...
router dmz-to-world inface “${dmz_if}” outface “${world_if}” src “${dmz_network}”
    protection strong 100/sec 50

    route smtp accept src “${mail_server}”
    route “http https” accept

router world-to-dmz inface “${world_if}” outface “${dmz_if}” src not “${dmz_network}”
    protection strong 1000/sec 500

    group with dst “${mail_server}”
        route smtp accept
        route imap accept
    group end

    group with dst “${web_server}”
        route “http https” accept
    group end

    group with dst “${ftp_server}”
        route ftp accept
    group end
...
```

/etc/firehol/firehol.conf

```
...
router world-to-dmz inface “${world_if}” outface “${dmz_if}” src not “${dmz_network}”
    ...

    group with dst “${web_server}”
        route “http https” accept
        route custom ws “tcp/8880” “default” accept src “${business_partner}”
    group end
...
```

/etc/firehol/firehol.conf

```
server_ws_ports="tcp/8880"
client_ws_ports="default"

...
router world-to-dmz inface “${world_if}” outface “${dmz_if}” src not “${dmz_network}”
    ...

    group with dst “${web_server}”
        route “http https” accept
        route ws accept src “${business_partner}”
    group end
...
```

/etc/firehol/firehol.conf

```
... (variaveis)

iptables -N in_protect_ssh
iptables -A in_protect_ssh --match recent --name SSH --set
iptables -A in_protect_ssh --match recent --name SSH --update --seconds 30 \
                                                     --hitcount 4 -j DROP

for c in INPUT FORWARD; do
    iptables -A $c -i $world_iface -p tcp --dport ssh \
                   -m state --state NEW -j in_prot_ssh
done

...

interface “${world_if}” world dst “${world_ip}” src not "${lan_network}"
    ...
    server accept ssh with recent SSH 30 4
    ...
...
```

The End!