

I

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
NUCLEO DE COMPUTAÇÃO ELETRÔNICA
PÓS-GRADUAÇÃO EM GERÊNCIA DE SEGURANÇA DA
INFORMAÇÃO (MSI)

Felipe Martins Rôlla

DESENVOLVENDO FIREWALLS SEGUROS EM AMBIENTES DE
ALTA DISPONIBILIDADE UTILIZANDO SOFTWARE LIVRE

Rio de Janeiro

2009

Felipe Martins Rôlla

**DESENVOLVENDO FIREWALLS SEGUROS EM AMBIENTES DE
ALTA DISPONIBILIDADE UTILIZANDO SOFTWARE LIVRE**

Monografia apresentada como requisito parcial para a conclusão do curso de especialização em Gerência de Segurança da Informação do NCE-UFRJ.

Orientador: Alexandre Freire

Rio de Janeiro

2009

LISTA DE ANEXOS

ANEXO 1 – LEVANTAMENTO LÓGICO DE SWITCHES.....	4
ANEXO 2 – ARQUIVO ALIASES-BOND.....	6
ANEXO 3 – ARQUIVO /ETC/NETWORK/INTERFACES	6
ANEXO 4 – AUTHKEYS	7
ANEXO 5 – HA.CF	7
ANEXO 6 – HARESOURCES	7
ANEXO 7 – SCRIPT DE FIREWALL HA.....	7
ANEXO 8 – SCRIPT DE SINCRONISMO SYNC_FIREWALL.SH	18

ANEXO 1

Switch A01		Identificação dos Cabos		Hostname do Servidor Conectado (Etiqueta)	Hardware (Marca e Modelo)	OBS
Portas	Negociação	Cor	Número			
1	1000 FD	AMARELO	13487	SW-RJ1-7-A-03	SW Accton ES4625	Interconexão /p Switches de Borda
2	1000 FD	AMARELO	13489	SW-RJ1-7-A-04	SW Accton ES4625	Interconexão /p Switches de Borda
3	1000 FD	VERMELHO	13464	FWHA01	Del PowerEdge R410	Rede Internet dos nós de Firewall
4	1000 FD	VERMELHO	13479	FWHA02	Del PowerEdge R410	Rede Internet dos nós de Firewall
5	1000 FD	VERMELHO	13440	.	.	VAGA
6	1000 FD	VERMELHO	13455	.	.	VAGA
7	1000 FD	AZUL	14698	FWHA01	Del PowerEdge R410	Rede LAN dos nós de Firewall
8	1000 FD	AZUL	14698	FWHA02	Del PowerEdge R410	Rede LAN dos nós de Firewall
9	1000 FD	AZUL	13479	MAILSERVER01	Del PowerEdge R610	Servidores da LAN
10	1000 FD	AZUL	13466	WEBSERVER01	Del PowerEdge R610	Servidores da LAN
11	1000 FD	AZUL	13463	DBSERVER01	Del PowerEdge R610	Servidores da LAN
12	1000 FD	AZUL	13440	.	.	VAGA
13	1000 FD	AZUL	13480	.	.	VAGA
14	1000 FD	AZUL	13489	.	.	VAGA
15	1000 FD	AZUL	5368	.	.	VAGA
16	1000 FD	AZUL	13522	.	.	VAGA
17	1000 FD	AZUL	13477	.	.	VAGA
18	1000 FD	AZUL	13443	.	.	VAGA
19	1000 FD	AZUL	13436	.	.	VAGA
20	1000 FD	AZUL	13509	.	.	VAGA
21	1000 FD	AZUL	13453	.	.	VAGA
22	1000 FD	AZUL	SEM	.	.	VAGA
23	1000 FD	VERDE	13495	TRUNK	SW Accton ES4625	Interligação entre os dois switches
24	1000 FD	VERMELHO	13519	.	.	VAGA

Switch A02						
		Identificação dos Cabos				
Portas	Negociação	Cor	Número	Hostname do Servidor Conectado (Etiqueta)	Hardware (Marca e Modelo)	OBS
1	1000 FD	AMARELO	13487	SW-RJ1-7-A-03	SW Accton ES4625	Interconexão /p Switches de Borda
2	1000 FD	AMARELO	13489	SW-RJ1-7-A-04	SW Accton ES4625	Interconexão /p Switches de Borda
3	1000 FD	VERMELHO	13464	FWHA01	Del PowerEdge R410	Rede Internet dos nós de Firewall
4	1000 FD	VERMELHO	13479	FWHA02	Del PowerEdge R410	Rede Internet dos nós de Firewall
5	1000 FD	VERMELHO	13440	.	.	VAGA
6	1000 FD	VERMELHO	13455	.	.	VAGA
7	1000 FD	AZUL	14698	FWHA01	Del PowerEdge R410	Rede LAN dos nós de Firewall
8	1000 FD	AZUL	14698	FWHA02	Del PowerEdge R410	Rede LAN dos nós de Firewall
9	1000 FD	AZUL	13479	MAILSERVER01	Del PowerEdge R610	Servidores da LAN
10	1000 FD	AZUL	13466	WEBSERVER01	Del PowerEdge R610	Servidores da LAN
11	1000 FD	AZUL	13463	DBSERVER01	Del PowerEdge R610	Servidores da LAN
12	1000 FD	AZUL	13440	.	.	VAGA
13	1000 FD	AZUL	13480	.	.	VAGA
14	1000 FD	AZUL	13489	.	.	VAGA
15	1000 FD	AZUL	5368	.	.	VAGA
16	1000 FD	AZUL	13522	.	.	VAGA
17	1000 FD	AZUL	13477	.	.	VAGA
18	1000 FD	AZUL	13443	.	.	VAGA
19	1000 FD	AZUL	13436	.	.	VAGA
20	1000 FD	AZUL	13509	.	.	VAGA
21	1000 FD	AZUL	13453	.	.	VAGA
22	1000 FD	AZUL	SEM	.	.	VAGA
23	1000 FD	VERDE	13495	TRUNK	SW Accton ES4625	Interligação entre os dois switches
24	1000 FD	VERMELHO	13519	.	.	VAGA

ANEXO 2

```
# Bonding ETH0 e ETH2
alias bond0 bonding
options bond0 mode=0 miimon=100 downdelay=0 updelay=10
max_bonds=2

# Bonding ETH1 e ETH3
alias bond1 bonding
options bond1 mode=0 miimon=100 downdelay=0 updelay=10
max_bonds=2
```

ANEXO 3

1. Arquivo /etc/network/interfaces do FWHA01

```
auto bond0
iface bond0 inet static
    address 200.196.48.3
    netmask 255.255.255.0
    slaves eth0 eth2

auto bond1
iface bond1 inet static
    address 10.0.0.2
    netmask 255.255.255.0
    slaves eth1 eth3
```

1. Arquivo /etc/network/interfaces do FWHA01

```
auto bond0
iface bond0 inet static
    address 200.196.48.4
    netmask 255.255.255.0
    slaves eth0 eth2

auto bond1
iface bond1 inet static
    address 10.0.0.3
    netmask 255.255.255.0
    slaves eth1 eth3
```

ANEXO 4

```
auth 3
3 md5 fwcluster
```

ANEXO 5

```
udpport 694
bcast bond0 bond1
serial /dev/ttyS0
keepalive 3
deadtime 9
node fwha01
node fwha02
ping 200.196.48.1
debugfile /var/log/ha-debug
logfile /var/log/ha-log
auto_failback on
respawn hacluster /usr/lib/heartbeat/ipfail
```

ANEXO 6

```
casashowfwha01 IPAddr2::200.196.48.2/24/bond0:0 # VIRTUAL ACIMA FW
casashowfwha01 IPAddr2::10.0.0.1/24/bond1:0 # VIRTUAL ABAIXO FW
```

ANEXO 7

```
#!/bin/bash
#####
#=====#
#=          Firewall iptables          =#
#=                                          =#
#= Autor: Felipe Martins                  =#
#= Data: 29/06/2009                      =#
#=====#
#####

function var_start()
{
```

```
iptables=/sbin/iptables
modprobe=/sbin/modprobe
sysctl=/sbin/sysctl

IF_LOC="lo"
IF_INT="eth2"
IF_EXT="eth1"
IF_DMZ="eth0"

IP_LO="127.0.0.1"
IP_INT="10.0.0.1"
IP_EXT="200.196.48.2"

NET_LOC="127.0.0.0/8"
NET_INT="10.0.0.0/24"
NET_EXT="200.196.48.0/24"

BRO_ESP="255.255.255.255"
BRO_INT="10.0.0.255"
BRO_EXT="200.196.48.255"

}

# Inicializacao dos Modulos
function modules_start()
{
    $modprobe ip_nat_ftp
    $modprobe ip_conntrack
    $modprobe ip_conntrack_ftp

    $sysctl -w net.ipv4.ip_forward=1
    $sysctl -w net.ipv4.tcp_syncookies=1
    $sysctl -w net.ipv4.rp_filter=1
    $sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
    $sysctl -w net.ipv4.accept_source_route=0
    $sysctl -w net.ipv4.secure_redirects=1
    $sysctl -w net.ipv4.log_martians=1
    $sysctl -w net.ipv4.ip_conntrack_max=300000
}
}
```

```

# Termino dos Modulos
function modules_stop()
{
    $modprobe -r ip_nat_ftp
    #$modprobe -r ip_conntrack
    $modprobe -r ip_conntrack_ftp
    $modprobe -r ip_nat_ftp
}

# Inicializacao das Politicas Padrao
function policy_start()
{
    echo -e "\n\nAbre o Firewall..."
    # define politica defaults para chains defaults
    $iptables -P INPUT DROP      # politica default para
filter
    $iptables -P FORWARD DROP    # politica default para
filter
    $iptables -P OUTPUT ACCEPT   # politica default para
filter
    $iptables -F -t filter       # flush nas regras de
filter
    $iptables -F -t nat          # flush nas regras de nat
    $iptables -F -t mangle       # flush nas regras de
mangle
    $iptables -X -t filter       # deleta chains de filter
    $iptables -X -t nat          # deleta chains de nat
    $iptables -X -t mangle       # deleta chains de mangle
    $iptables -Z -t filter       # zera contadores de
filter
    $iptables -Z -t nat          # zera contadores de nat
    $iptables -Z -t mangle       # zera contadores de
mangle
}

# Termino das Politicas Padrao
function policy_stop()
{
    echo -e "\n\nFecha o Firewall totalmente para FORWARD
e INPUT..."
}

```

```

# define politica defaults para chains defaults
filter $iptables -P INPUT ACCEPT # politica default para
filter $iptables -P FORWARD ACCEPT # politica default para
filter $iptables -P OUTPUT ACCEPT # politica default para
filter $iptables -F -t filter # flush nas regras de
filter $iptables -F -t nat # flush nas regras de nat
mangle $iptables -F -t mangle # flush nas regras de
filter $iptables -X -t filter # deleta chains de filter
filter $iptables -X -t nat # deleta chains de nat
filter $iptables -X -t mangle # deleta chains de mangle
filter $iptables -Z -t filter # zera contadores de
mangle $iptables -Z -t nat # zera contadores de nat
mangle $iptables -Z -t mangle # zera contadores de
}

# Regras do firewall
function rules_start()
{
#####
### Chain PREROUTING ###
#####

# Regras de Port Forwarding
echo "Regras para NAT 1:1 ..."
$Iiptables -t nat -A PREROUTING -i $IF_EXT -m multiport
-p tcp --dports 80,8080 -j DNAT --to $IP_WWW

#####
### Chain INPUT ###
#####

# Entrada no Firewall
echo "Regras de INPUT ..."

```

```

        #Iptables -A INPUT -j END_INVALID -m state --state
INVALID
        $iptables -A INPUT -m state --state
ESTABLISHED,RELATED -j ACCEPT
        $iptables -A INPUT -i $IF_LOC -s $NET_LOC -j ACCEPT
        $iptables -A OUTPUT -m state --state
ESTABLISHED,RELATED -j ACCEPT

        # Regras para VPN PPTP e IPsec
        #####-VPN PPTPD-
#####
        $iptables -A INPUT -p tcp --dport 1723 -j ACCEPT
#
        $iptables -A INPUT -p 47 -j ACCEPT
#
        $iptables -A FORWARD -s $NET_VPN -d $NET_INT -j ACCEPT
#

#####
#####

        # Acesso SSH apenas da REDE INTERA E REDE VPN
        $iptables -A INPUT -s $NET_INT -p tcp --dport 22 -j
ACCEPT      # SSH Rede Interna
        $iptables -A INPUT -s $NET_VPN -p tcp --dport 22 -j
ACCEPT      # SSH Rede VPN

        $iptables -A INPUT -p tcp --dport 21 -j ACCEPT
# FTP
        $iptables -A INPUT -i $IF_INT -s 10.1.1.204 -p tcp --
dport 80 -j ACCEPT      # HTTP (Relatorios SARG)
        $iptables -A INPUT -i $IF_INT -s 10.1.1.11 -p tcp --
dport 80 -j ACCEPT      # HTTP (Relatorios SARG)
        $iptables -A INPUT -i $IF_INT -s $NET_INT -p tcp --
dport 10000 -j ACCEPT      # WEBMIN

        $iptables -A INPUT -i $IF_INT -s 10.1.1.1 -j ACCEPT
        $iptables -A INPUT -i $IF_INT -s 10.1.1.2 -j ACCEPT

        # Squid Transparente - Regra de Entrada no FW
        $iptables -A INPUT -i $IF_INT -s $NET_INT -p tcp --
dport 3128 -j ACCEPT

```

```

#####
### Chain FORWARD ###
#####

# Regras de Passagem
echo "Regras de FORWARD ..."
$Iptables -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT
$Iptables -A FORWARD -s $NET_INT -j ACCEPT
$Iptables -A FORWARD -i eth1 -d $NET_INT -j ACCEPT
$Iptables -A FORWARD -s $NET_VPN -d $NET_INT -j ACCEPT

#####
# Chain POSTROUTING (SAIDA) ###
#####

# Saida da Rede Interna para a Internet
$Iptables -A POSTROUTING -t nat -s $NET_INT -j SNAT --
to $IP_EXT
}

#####
### MAIN ###
#####

case "$1" in
    start)
        var_start
        modules_start
        policy_start
        rules_start
        ;;
    stop)
        var_start
        policy_stop
        modules_stop
        ;;
    restart)
        var_start
        policy_stop

```

```

modules_stop
modules_start
policy_start
rules_start
;;
status)
echo "STATUS das Regras de Firewall";
echo "=====";
echo;
$iptables -L -n
;;
*)
echo "Use o Comando:"
echo "    iptables
(status|start|stop|free|backup|restore) "
;;
esac

```

ANEXO 7

```

#!/bin/bash
#####
#=====#
#=          Sincronimos de Firewall          =#
#=          =#
#= Autor: Felipe Martins Rolla              =#
#=====#
#####

RSYNC=`which rsync`
MD5=`which md5sum`
SSHPASS=`which sshpass`

#insira os arquivos
fileconf[1]="/etc/init.d/firewall";command[1]="/etc/init.d/firewall restart"
fileconf[2]="/etc/ipsec.conf";command[2]="/etc/init.d/ipsec restart"
fileconf[3]="/etc/ipsec.secrets";command[3]="/etc/init.d/ipsec restart"

```

```
#Conta array ativos
count=${#fileconf[@]}

for i in `seq 1 $count`
do

    md5sum1=`$MD5 ${fileconf[$i]} | awk -F " " '{print
$1}`

    $SSHPPASS -p "we^3k4SD*$#d" ssh 200.196.48.2 -l
fwoperator sudo cat ${fileconf[$i]} > ${fileconf[$i]}

    md5sum2=`$MD5 ${fileconf[$i]} | awk -F " " '{print
$1}`

    if [ "$md5sum1" != "$md5sum2" ];then
    ${command[$i]}
    fi
done
```