IpFilter
Série Firewalls

Anderson Alves de Albuquerque
José Gracia Neto
Fernando Spencer
Marita Maestrelli

2003

Prefácio

Em virtude dos diversos problemas de segurança ocorridos nos últimos anos em diversos sites na internet, iniciamos um trabalho de documentação técnica sobre firewall. Na primeira etapa, descreveremos o **ipf**(ipfilter) por ser um filtro de pacotes multi plataforma e apresentar itens satisfatórios.

Esta nota técnica apresenta conceitos básicos de segurança de rede e firewall, abordando com maior enfase as plataformas *BSD, por possuirem uma credibilidade maior no aspecto de segurança.

Todas as idéias que serão apresentadas podem ser adaptadas para qualquer ferramenta de filtro de pacotes.

Índice:

1 - NOÇÕES SOBRE FILTROS DE PACOTES (IPFILTER)

1.1 – Introdução:

Iremos abordar o software ipfilter, utilizado para construção de firewall, filtros de pacotes e NAT em sistemas operacionais UNIX e LINUX. A escolha do ipfilter foi realizada por suportar diversas plataformas como: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, SunOS, BSDI, IRIX, HP-UX e outros.

Ele pode ser implementado de duas formas: Incorporado ao kernel do sistema ou carregado através de módulos.

Esse software também possui muitas opções de configuração satisfazendo a maioria das necessidades existentes. A sintaxe de configuração é bem parecida com a maioria dos filtros usados no mercado, com isso não teremos maiores problemas.

Antes de continuarmos seria bom lembrar que a arquitetura de firewall deve ser projetada de acordo com necessidade do site, unindo diversas ferramentas, como: Filtro de pacotes, NAT, Gateway de aplicação/genérico, IDS e etc.

Este documento não tem a intenção de aprofundar–se nos assuntos relacionados acima, apenas servir como um guia de referência exemplificando tópicos básicos.

Futuras versões dos firewalls, filtros de pacotes, virão com suporte a ipv6. A versão, a partir da 3.4.14 do IPFilter já possui esse suporte.

1.2. – Definições:

Filtro de Pacotes: Software que possibilita a filtragem de pacotes na camada de transporte. São definidas regras com parâmetros como: ip de origem/destino, porta de origem/destino, proto, porta, flags, TOS, máscara de origem/destino, direção do pacote (in/out), placa de rede e outros.

Também são definidas ações como deny, pass, forward e return.

Gateway de aplicação: Proxy de aplicação, atua na camada de aplicação. Sua funcionalidade é inerente a aplicação para que foi projetada.

Gateway Genérico: Proxy de Aplicação que independe da aplicação para a qual vai ser usado. Podemos ter em mente que ele irá mudar a trajetória do pacote na camada de transporte.

Proxy Cache: Proxy de aplicação que tem como principal finalidade formar um cache das Home Pages (ou arquivos transferidos por ftp e requisições dns).

Proxy Transparente: São desvios (forward) na camada de tranporte ou aplicação independente da configuração do cliente. Como exemplos, podemos falar da opção de desviar todo o tráfego HTTP para um proxy cache, independente da configuração no browser do cliente.

NAT "Network Address Translate": O NAT mapeia as requisições da rede interna com a rede externa, com isso podemos usar na rede interna endereços inválidos. Ele atua na camada de transporte.

Muitas vezes o seu funcionamento pode ser confundido com Proxy, mas essa idéia deve ser descartada.

O NAT pode ser implementado como 1 para 1 ou 1 para N, e pode ser dividido em estático ou dinâmico.

1.3. – Instalação:

O processo de instalação pode ser divido nas etapas:

- Descompactação do ipfilter
- Instalação dos arquivos do ipfilter
- Copilação do Kernel
- Instalação do novo kernel
- Reiniciar o sitema operacional
- Ler os modulos do ipfilter (insmod)

A utilização do ipfilter neste documento será feita nos sitemas operacionais OpenBSD e Solaris 2.6.

A única diferença marcante será na momento de instalação no Solaris 2.6. No OpenBSD o ipfilter é "inerente" ao sistema, por isso não perderemos tempo no processo de instalação no OpenBSD.

2 - DOCUMENTAÇÃO

2.1. - Site:

Site oficial: http://coombs.anu.edu.au/~avalon/ip-filter.html
Atualização das documentações: http://www.obfuscation.org/ipf/

ftp://coombs.anu.edu.au/pub/net/ip-filter/
ftp.localhost.ca
ftp.tardis.ed.ac.uk
ftp.fh-koblenz.de
ftp.ntua.gr
ftp://ftp.gw.com/pub/unix/ip-filter/

Atualmente a versão corrente é ip-fil.3.4.33pre1.tar.gz

2.2 – Lista de Discussão:

http://false.net/ipfilter/

Enviar e-mail para:
majordomo@coombs.anu.edu.au
No corpo da mensagem coloque: subscribe ipfilter

2.3 – How-TO:

http://www.obfuscation.org/ipf/

2.4 – Ferramentas correlacionadas:

- Filtro de pacotes e NAT:

Ferramenta	***Site***
Ipchains	http://www.adelaide.net.au/~rustcorp/linux/ipchains
Ipfw	inerente nos sistemas freebsd 2.2.x
Ipfwadm	http://www.xos.nl/linux/ipfwadm/
Ipmasq	http://ipmasq.home.ml.org http://masqapps.home.ml.org
SINUS	http://www.ifi.unizh.ch/ikm/SINUS/firewall.html
TAMU	ftp://net.tamu.edu/pub/security/TAMU

Tabela 2.4.1

- Gateway de aplicação ou Proxys Servers:

Ferramenta	***Site***
Delegate	ftp://ftp.delegate.org/pub/DeleGate/ http://www.delegate.org
FK	http://ferret.lmh.ox.ac.uk/~weejock/fk/
Obtuse Firewall	http://www.obtuse.com
OpenSource	http://www.opensource.com
TCPWrapper	ftp://ftp.win.tue.nl/pub/security ftp://ftp.porcupine.org/pub/security/
Tis Firewall	http://www.tis.com

Tabela 2.4.2

- Gateway Genérico:

Ferramenta	***Site***
Ip_relay	http://www.stewart.com.au/ip_relay/
Ipautofw	ftp://ftp.netis.com/pub/members/rlynch/ipautofw.tar.gz
Mmtcpfwd	http://mmondor.rubiks.net/software/linux/mmtcpfwd-0.2b.tar.gz http://mmondor.rubiks.net/index.html
Portfwd	http://download.sourceforge.net/portfwd/portfwd-0.15.tar.gz http://download.sourceforge.net/portfwd/
Rinted	ftp://ftp.boutell.com/pub/boutell/rinetd/rinetd.tar.gz
Virtual Server	http://www.linuxvirtualserver.org/

Tabela 2.4.3

- Proxy Cache

Ferramenta	***Site***
Squid	http://squid.nlanr.net ftp://ftp.squid-cache.org/pub/squid-2/STABLE/
Squid Guard	http://ftp.ost.eltele.no/pub/www/proxy/squidGuard
Wwwoffle	http://www.gedanken.demon.co.uk/wwwoffle/

Tabela 2.4.4

- Gateway de circuito

Ferramenta	***Site***
Dante	http://www.inet.no/dnte/
Socks	http://www.socks.nec.com/

Tabela 2.4.5

- Ferramentas para windows

Ferramenta	***Site***
Conseal PC Firewall	http://www.signal9.com
Proxy +	http://www.proxyplus.cz
Socks	http://www.socks.nec.com/
Wingate PRO	http://wingate.deerfield.com
Winproxy	http://www.winproxy.com
Winroute PRO	http://www.tinysoftware.com

Tabela 2.4.6

Ferramenta	***Site***
Blackice Defebder	http://www.networkice.com
Esafe Desktop	http://www.esafe.com.br
Internet Guard Dog	http://www.mcafee.com.br
Languard	http://www.languard.com
Norton Internet Security	http://www.symantec.com.br
Sybergen Secure Desktop	http://www.sybergen.com
Zone Alarm	http://www.zonelabs.com/zonealarm.htm

Tabela 2.4.7

- Firewall Comercial:

Ferramenta	***Site***
Aker	http://www.aker.com.br
Altavista Firewall	http://www.altavista.software.digital.com
Ans	http://www.ans.net
Avertis	http://www.galea.com/En/Products/Avertis/Index.html
Border Manager	http://www.novell.com/text/bodermanager/index.html
Cisco (PIX Firewall)	http://www.cisco.com
Conclave	http://www.interdyn.com/fyi.html
CSM	http://www.csm-usa.com
Cyberguard	http://www.cybg.com
CyberShield	http://www.cybershield.com
Cycon's	http://www.cycon.com
Elron	http://www.elronsoftware.com
Firewall 1	http://www.checkpoint.com
Firewall Switch	http://www.fore.com
Firewall/Plus	http://www.network-1.com
Gnat	http://www.gnatbox.com
IBM Firewall	http://www.ics.raleigh.ibm.com
Interceptor Firewall	http://www.tlogic.com
Kbridge	ftp://ftp.cerias.purdue.edu/pub/tools/dos/kbridge.zip

Microsft Proxy	http://www.microsoft.com
Milkyway	http://www.milkyway.com
NetBuilder	http://www.cisco.com
NetGuard	http://www.ntguard.com
NetScreenAO	http://www.netscreen.com
Open source firewall	http://www.opensourcefirewall.com/
Raptor	http://www.raptor.com
Secure Access	http://www.ascend.com
Socks	http://www.socks.nec.com
SunScreen	http://www.sun.com
Tis Gauntlet	http://www.tis.com
Ukiah	http://www.ukiahsoft.com
WatchGuard	http://www.watchguard.com

Tabela 2.4.8

- Ferramentas Básicas para checklist:

Ferramenta	***Site***
HWA sscan2k-pre6	http://packetstorm.securify.com/advisories/hwa/
AdmHack	ftp://ADM.isp.at/
BindView	http://www.bindview.com
Cgichk	http://www.ech0.de/
Chknull	Http://www.nmrc.org/files/netware
Cops	ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/cops/
CyberCop	http://www.nai.com
Find ddos	http://www.fbi.gov/nipc/trinoo.htm
Firewallk	http://www.packetfactory.net/firewallk/
Fping	http://Packetstorm.harvard.edu/
HackerShield	http://www.bindview.com/netect/
Icmpush	http://hispahack.ccc.de/
IdentTCPscan	http://www.asmodeus.com/archive/crack-scan/
InspectorScan	http://www.shavlik.com
Iscan (Windows)	http://www.forixnt.com/iscan.zip
Iss	http://www.iss.net http://www.giga.or.at/pub/hacker/unix/
Jakal	http://www.unitedcouncil.org/c/jakal.c
Javaportscan	http://www.ccci.com/tools/portscan/index.html
Kane	http://www.intrusion.com
Nessus	http://www.nessus.com
Netcat	ftp://ftp.technotronic/unix/
Nmap	http://www.insecure.org/nmap
NSS	http://www.giga.or.at/pub/hacker/unix/
NtinfoScan	http://www.infowar.co.uk/mnemonix/
Portscanner	http://www.aneth.org/~veilleusc/

pscan	http://www.striker.ottawa.on.ca/~aland/pscan/
Queso	http://www.apostols.org/
Rscan	ftp://ftp.win.ne.jp/pub/network/security/rscan/
Saint	http://www.wwdsi.com/saint/downloads/
Satan	ftp://ftp.porcupine.org/pub/security/ ftp://ftp.win.ne.jp/pub/network/security/satan/
Sbscan	http://www.haqd.demon.co.uk/sbscan-0.03.tar.gz
Scan	http://www.prosolve.com
SolarWinds	http://www.solarwinds.net
Sshscan	http://www.monkey.org/~provos/
Strobe	ftp://suburbia.net/pub/
Tiger	ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/tiger/
Twwwscan	http://search.iland.co.kr/twww
UdpScan	http://www.giga.or.at/pub/hacker/unix/
UdpScan	ftp://ftp.technotronic/unix/
Vetescan	http://www.self-evident.com
Vlad 0.7.3	http://razor.bindview.com/tools/vlad/index.shtml
WebTrends	http://www.webtrends.com/wss/ http://www.webtrends.com
WS_Ping	http://www.ipswitch.com
Xscan	http://www.giga.or.at/pub/hacker/unix/
Yaps	http://www.tni.net/~ted/Yaps/Yaps.html

Tabela 2.4.9

Na tabela 8 colocamos diversas ferramentas para realização de checklists em hosts com filtro de pacotes ou Firewall, apesar destas ferramentas não estarem separadas por categorias e funções, essas informações podem ser facilmente obtidas nos sites relacionados.

- Ferramentas Básicas para VPN:

Ferramenta	***Site***
Free S/Wan	http://www.xs4all.nl/~freeswan/
Ippfvsadm (load Balance)	http://proxy.iinchina.net/~wensong/ippfvs
VPND	http://www.crosswinds.net/nuremberg/~anstein/unix/vpnd.html
VPS	http://www.strongcrypto.com
Tinc 1.0	http://tinc.nl.linux.org/ http://tinc.nl.linux.org/packages/tinc-1.0pre3.tar.gz

Tabela 2.4.10

- Shell Seguro:

Ferramenta	*Site*
Lsh	http://www.net.lut.ac.uk/psst
Openssh	http://www.openssh.org/
Ossh	ftp://ftp.pdc.kth.se/pub/krypto/ossh/
Psst	http://www.net.lut.ac.uk/psst/
Sftp	http://enigma.xbill.org/sftp
Ssh	http://www.ssh.org
Ssh	http://www.ssh.com
Windows Servers	http://marvin.criadvantage.com/caspian/Software/SSHD-NT/default.php

Tabela 2.4.11

- Sniffers:

Ferramenta	*Site*
Nicedump	ftp://ftp.loria.fr/pub/network/nicedump/nicedump-0.9.1b.tgz
Snort	http://www.snort.org
Tcpdump	ftp://ftp.ee.lbl.gov/

Tabela 2.4.12

- IDS:

Ferramenta	*Site*
AIDE	ftp://ftp.cs.tut.fi/pub/src/gnu/
Aps	http://www.swrtec.de/swrtec/clinux/aps-0.17.tar.gz
Delog(distributed.net)	http://kimihia.org.nz/projects/dnetc/
Fwlogwatch (5e)	http://www.kyb.uni-stuttgart.de/boris/sw/fwlogwatch-0.0.25.tar.gz
Host Sentry	http://www.psionic.com/tools/
Iplog	http://ojnk.sourceforge.net/
Ippl	http://pltplp.net/ippl/
LibNIDS (5e)	http://www.packetfactory.net/Projects/Libnids/
Log Scanner	http://logscanner.tradeservices.com
Logcheck	http://www.psionic.com/tools/
Logcolorise	http://www.linuxsupportline.com/~pgp/linux/scripts.html
LogSurfer	ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer/
Logwatch	http://logwatch.xidus.net/
Maccount	http://yasd.dhs.org/en/maccount.php3
md5mon	http://members.linuxstart.com/~winitzki/md5mon.html
Netlog	ftp://ftp.cert.dfn.de/pub/tools/audit/netlog/
NID	http://ciac.llnl.gov/cstc/nid/nid.html
Perro	http://www.grigna.com/diego/linux/perro/
PiranhaWap (Wap)	http://www.elctech.com/piranha.shtml
PortSentry	http://www.psionic.com/tools/
Samhain (5e)	http://samhain.sourceforge.net/

Snort	http://www.snort.org
Sockscan	http://dustball.com/software/sockscan/
Syslog New Generation	http://www.balabit.hu/products/syslog-ng/
tripwire	http://www.tripwiresecurity.co
Webalizer	http://www.mrunix.net/webalizer/

Tabela 2.4.13

- Outras:

Ferramenta	***Site***
Libcap	ftp://ftp.ee.lbl.gov/
Lsof	ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/
Md5	ftp://ftp.cert.org/pub/tools/md5
MRTG	http://www.mrtg.org
NetSaint	http://www.netsaint.org/
Penemo	http://www.communityprojects.org/apps/penemo/dl/
Sersniff (2 seriais)	http://www.earth.li/projectpurple/progs/sersniff.html
Socket Watcher	ftp://ftp.sgi.com/sgi/sockwatch/
Spar	http://www.isc.tamu.edu/software/man/solaris2/spar.8.html
Xinetd	http://www.xinetd.org

Tabela 2.4.14

- Sniffer detect:

Ferramenta	***Site***
Cpm	http://www.ja.net/CERT/Software/cpm/
Ifsolstat	ftp://ciac.llnl.gov/pub/ciac/sectools/unix/sniffdetect
Ifstatus	ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/ifstatus/
Neped	http://apostols.org/projectz/neped/

Tabela 2.4.15

- kernel:

Ferramenta	***Site***
Saint Jude LKM (anti-exploit)	http://www.sourceforge.net/projects/stjude

Tabela 2.4.16

2.5 – Estatísticas sobre segurança:

Alguns sites procuram manter estatísticas sobre invasões e os sistemas mais usados na internet, podemos destacar:

http://www.cert.org/stats/cert_stats.html
http://www.nbso.nic.br/stats/
http://www.attrition.org/mirror/attrition/stats.html (1999-2001)
http://www.netcraft.com/survey/
http://www.securityspace.com/s_survey/data/
http://www.attrition.org/mirror/attrition/os.html (1999-2001)

3 – Noções Básicas sobre Firewall

3.1 - Filtro de Pacotes:

Os filtros de pacotes (figura 3.1.1) podem ser implementados em roteadores ou computadores com regras (rules) que atuam na camada de transporte. O filtro de pacotes é um firewall tradicional bem simples.

As regras no filtro de pacotes são baseadas em ações (deny e allow) e parâmetros (porta origem/destino, host origem/destino, protocolo tcp/udp, sentido in/out. interface, máscara origem/destino, logs e outros). Normalmente, a implementação das regras exige um pouco de experência em cima da tecnologia onde essas regras serão implementadas.

Os filtros de pacotes possuem problemas, como: logs, autenticação, dificuldades de implementações de regras e pequeno controle fino sobre a aplicação.

É aconselhável criar uma tabela de regras genéricas, pois cada tecnolgia de firewall possui sintaxe de regra diferentes. Isso facilita a transposição de regras de um firewall para outro de tecnologia diferente.

As regras são executadas sequencialmente na ordem: *rule 1, rule 2, rule 3..., rule n* .

Alguns filtros permitem criar grupos de regras, neste caso os grupos são analisados sequencialmente e dentro dos grupos as regras são executados sequencialmente: *grupo 1 f(rule 1, rule 2, rule 3..., rule n), grupo 2 (rule 1, rule 2, rule 3..., rule n), ..., grupo N (rule 1, rule 2, rule 3..., rule n)* .

Em resumo as regras são executados na ordem $f(X_1)$, $f(X_2)$, $f(X_3)$, ..., $f(X_n)$.

Na tabela 3.1.1 mostraremos um exemplo de uma tabela genérica de regras para filtros de pacotes, o efeito do conjunto das regras desta tabela não deve ser analisada apenas devemos analisar as regras separadamente como um exemplo didático.

Regra N°	sentido	Ação	interface	Proto	IP origem/mask	IP destino/mask	Flags	Logs
1	In	Deny	Serial0	Tcp	10.10.5.1/32	192.168.1.0/24	*	*
2	Out	Allow	Ed1	Tcp	10.10.2.0/24	192.168.1.9/32	Ack/Syn	-
3	*	Allow	Eth0	Udp	10.10.1.0/24	192.168.1.9/32	-	-
4	*	Deny	Ne1	Icmp	*	*	0/8/11	*
5	*	Deny	*	Icmp	*	*	*	*

Tabela 3.1.1

Vantagens	Desvantagens
Fáceis de configurar.	Dificulta administração Segura de algumas conexões.
Baixo custo.	Recursos de logs limitados.
Transparente.	Não possui autenticação.
Inerente na maioria dos Hardware.	Não ocultam a rede interna.
Podem ser implementados em quase todos os hosts da rede.	Sucetível a exploits e overflow na rede interna.
-	Não possui ajuste fino sobre as aplicações.
-	Problemas no controle dos pacotes UDP.
-	Problemas para trabalhar com pacotes fragmentados.

Tabela 3.1.2

Para solucionar alguns problemas do filtro de pacotes criou–se o "filtro inteligente", este implementa algumas características, como: interface amigável de administração, diversos níveis de logs, autenticação de usuários, tratamento especial dos pacotes udp, mecanismo de verificação da regras, aciona a equipe técnica caso uma ocorrência pré-configurada seja detectada e outros.

Também criou–se um filtro chamado "filtro de MAC", existente atualmente para o FreeBSD.

Figura 3.1.1

3.2 - NAT (RFC 1631):

O NAT é uma forma de acesso e alocação de endereços de forma transparente para os clientes. A rede interna utiliza endereços IP não-válidos (privados), estes são traduzidos para um endereço válido (público) para o mundo externo. Os acessos versus relações de conversões, entre endereços válidos e inválidos, são guardados em uma tabela, e consultados periodicamente como mostrados na figura 3.2.1.1.

O NAT posui uma segurança maior que os filtros de pacotes, facíl de configurar e administrar, adiciona funcionalidades do proxy de aplicação e a vantagem de ser transparente para o usuário.

O NAT possui a desvantagem de dificultar auditorias de acessos dos clientes da rede interna, serviços que utilizão informações sobre o endereço IP podem necessitar de um gateway de aplicação (snmp), e alguns serviços como ftp e Real Payer podem apresentar problemas (vide figura 3.2.3.1).

3.2.1 - O NAT pode ser dividido em dois tipos: Estático ou dinâmico.

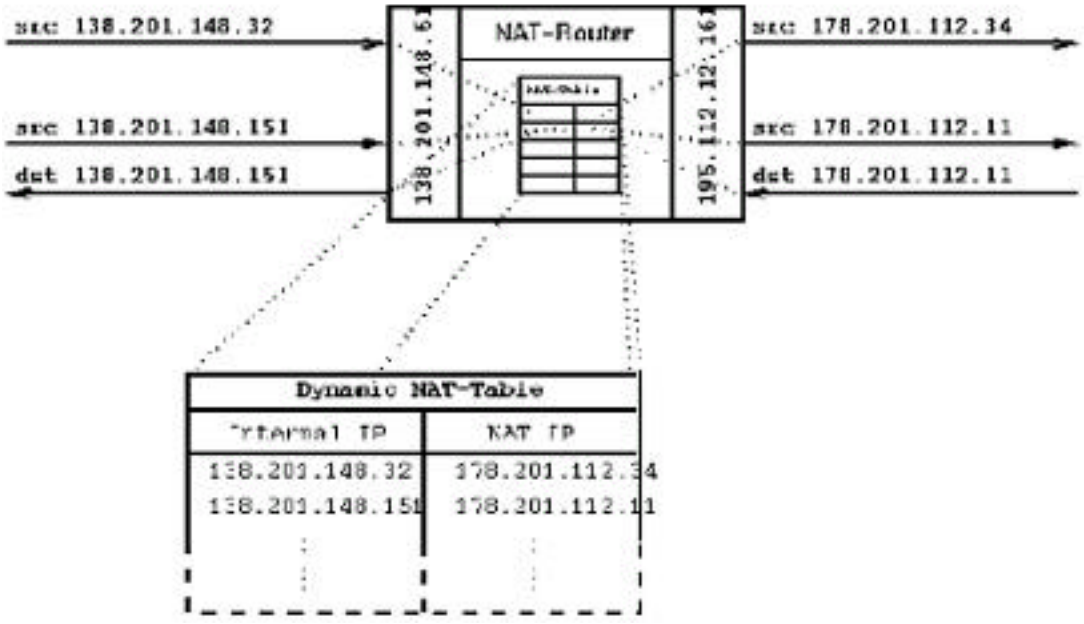
- **NAT estático:**

Tradução m:n onde m e n são maiores ou igual a 1 (um). Este NAT não economiza endereços IP.

- **NAT dinâmico:**

Tradução m:n onde m é maior ou igual a 1 (um) e m maior que n. Este NAT não economiza endereços IP. Este NAT necessita de um pacote ou feature para realizar o redirecionamento, de porta do ip externo para uma porta em um host interno, possibilitando que servidores internos sejam acessados através da rede externa. A figura abaixo exemplifica como o NAT trata a conversão de endereços IPs.

Figura 3.2.1.1



Exite o caso do o ip masquerading do linux que é um NAT dinâmico m:1, possui o máximo de economia de endereços ips, onde todos os endereços internos são representados por um endereço externo. Este também é chamado NAPT.

3.2.2 - O NAT ainda pode ou não possuir propriedades como: forward de portas ou Load Balance.

- Redirecionamento de porta:

O redirecionamento, apenas desvia o tráfego recebido por um host *A* em uma porta *A* para outro host *B* em uma porta *B*. A porta *A* pode ser diferente ou igual a *B*.

Neste exemplo (figura 3.2.2.1) os IPs 192.168.1/24 são os endereços locais ou privados, os endereços 130.102/24 são os endereços globais ou públicos.

O redirecionamento de porta também pode desviar o tráfego da rede interna para um servidor *proxy cache web* criando um proxy transparente. Este é o caso do *squid proxy cache* que possibilita esse tipo de configuração mostrada no ítem 6 exemplo 3. A vantagem é que os softwares clientes não precisarão ser configurados como é mostrado na figura 3.5.1.

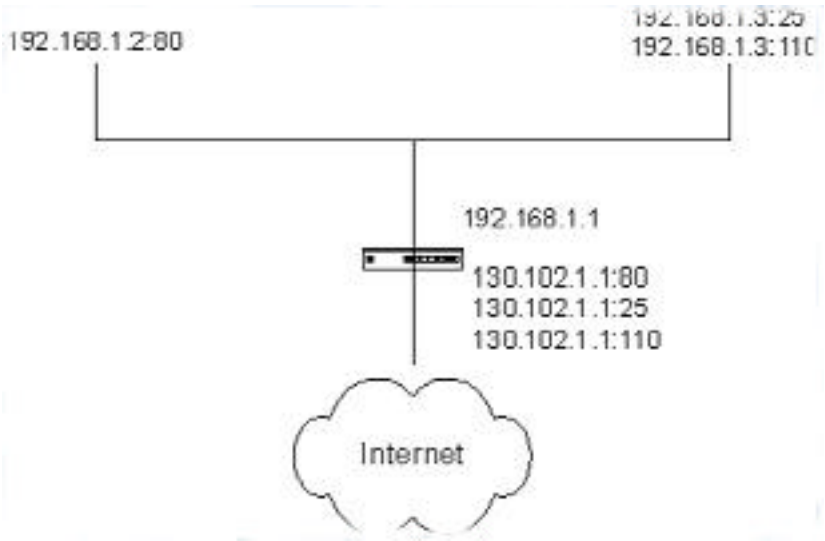


Figura 3.2.2.1

Relação de forward das portas:

Exemplo 1:

IP Externo	Host Interno	Porta A & Porta B
130.102.1.1:25	192.168.1.3:25	A = B
130.102.1.1:80	192.168.1.2:80	A = B
130.102.1.1:110	192.168.1.3:110	A = B

Tabela 3.2.2.1

Exemplo 2: O forward poderia ser entre portas diferentes.

IP Externo	Host Interno	Porta A & Porta B
130.102.1.1:25	192.168.1.3:110	A ≠ B
130.102.1.1:80	192.168.1.2:25	A ≠ B
130.102.1.1:110	192.168.1.3:80	A ≠ B

Tabela 3.2.2.2

- Load Balance:

Basicamente é levantada a vazão de tráfego, megabits/seg, e de acordo com pesos pré determinados, o tráfego pode ser direcionado para um dos links ou servidores. Isso é muito usado em sites que tem muitos acessos a Home Pages e e-mail.

Outra propriedade é o direcionamento de tráfego versus serviços acessados, podendo escoar o tráfego de e-mail pelo link1 e o de web pelo link 2. Isso é muito bom quando temos a estatística de utilização da rede interna, em média 80% dos acessos são efetuados aos serviços HTTP e e-mail.

3.2.3 - Problemas do IP Masquerading

Na utilização de NAT dinâmico (NAPT) usando o ip masquerading do linux, devemos lembrar que algumas aplicações podem apresentar problemas, como:

Nome da aplicação	Comentário
Todos programas baseados em H.323	MS Netmeeting, Intel Internet Phone Beta 2 – conectam-se, mas transmitem voz em apenas uma direção (de saída).
Intel Streaming Media Viewer Beta 1	Não conseguem conectar-se ao servidor
Netscape Cooltalk	Não conseguem conectar-se ao servidor
WebPhone	Não funciona

Lista de aplicações que não suportam NAT

figura 3.2.3.1

3.3 - Proxy Aplicação (ALG gateway a nível de Aplicação):

Os ALG's (Aplicação a nível de gateway ou proxy de aplicação) são "servidores" escritos para uma aplicação específica. A sua natureza é pertinente a aplicação com exceção do proxy de aplicação genérico, que funcionam como o redirecionador de portas no NAT deixando de atuar na camada de aplicação. Os proxy de aplicação genérico torna os

servidores internos suscetíveis a *exploit* e *buffer overflow*(estouro de memória) e não tem o mesmo grau de controle sobre a aplicação.

Como no *proxy cache* os proxys de aplicação tem um grau enorme de controle sobre as aplicações, podendo: criar logs detalhados, atenticação de usuários, verificações de vírus, controle sobre os comandos executados pelo protocolo, torna o servidor interno quase "inacessível" diretamente, diminui muito a possibilidade de *exploits* e *overflow*, tornando a rede interna oculta.

Em função do auto controle sobre a aplicação o proxy (ALG) é mais lento e mais difícil de configurar. A utilização de um serviço pelos clientes fica muito dependente da existência de um "servidor" ALG, pois sem este "servidor" ALG não podemos habilitar o serviço exceto quando utilizamos o proxy de aplicação genérico.

Podemos exemplificar, gosseiramente, o funcionamento das requisições como se fossem parecidas com o proxy cache.

Normalmente, existe uma dificuldade de localizar um proxy de aplicação Open Source, porque é mais difícil de escrevê–lo. O trabalho de pesquisa e testes é muito grande, visto que teremos um servidor para cada serviço. Podemos destacar alguns proxies de aplicação tradicionais no mundo Open Source, como o Tis Firewall e o Delegate. Em contra partida quase todos os firewalls comerciais possuem este recurso.

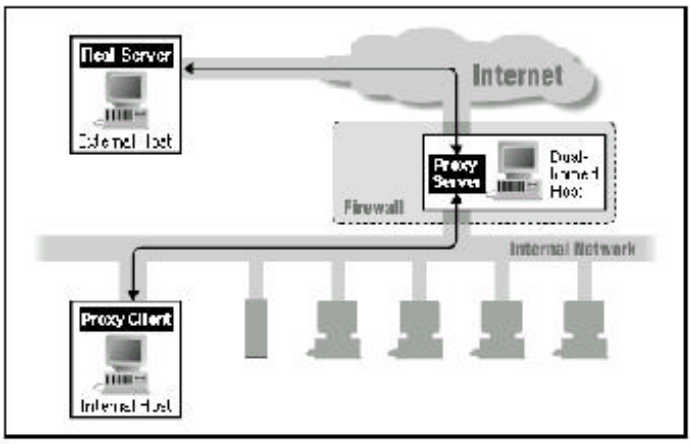
Vantagens	**Desvantagens**
Logs eficientes.	Mais lento.
Controle eficiente sobre a aplicação.	Mais difícil de configurar.
Economia de endereços IPs.	Mudança de comportamento dos usuários.
Autenticação de usuários.	Alto custo.
Limita os serviços acessados, apenas permitindo os serviços que possuem um ALG configurado.	Necessidade de um ALG específico para que o serviço funcione. Tornando –o caro.
Oculta a rede.	Upgrade constante dos "servidores" ALG, estes podem sofrer ataques DOS.
Podem evitar ataques de pacotes fragmentados.	-

Tabela 3.3.1

Podemos dividir os ALGs em:

- Gateway de aplicação específicos: São escritos para um serviço e o seu funcionamento é limitado a este serviço. Proporciona um controle maior sobre as aplicações, tornando a sua configuração e administração mais difícil.

- Gateway de aplicação genéricos: São escritos para qualquer aplicação, funciona como um redirecionador de porta. Não possui um controle tão fino sobre a aplicação, e também é sucetível a DOS.



Utilização de servidor *proxy* em um dual-homed *host*

figura 3.3.1

3.4 - Proxy (Circuito):

Este proxy cria um circuito virtual fim à fim entre o cliente e o destino final. Há necessidade do cliente tomar conhecimento do servidor proxy de circuito (SOCKS), muitas vezes implica em modificar o cliente da rede. Este proxy é totalmente transparente, atualmente os softwares Open Source mais conhecidos são o socks da *http://www.socks.nec.com* e o Dante da *http://www.inet.no/dnte*.

As grandes desvantagens do proxy de circuito é a falta de recursos para geração de logs, autenticação de usuários e controle fino sobre a aplicação.

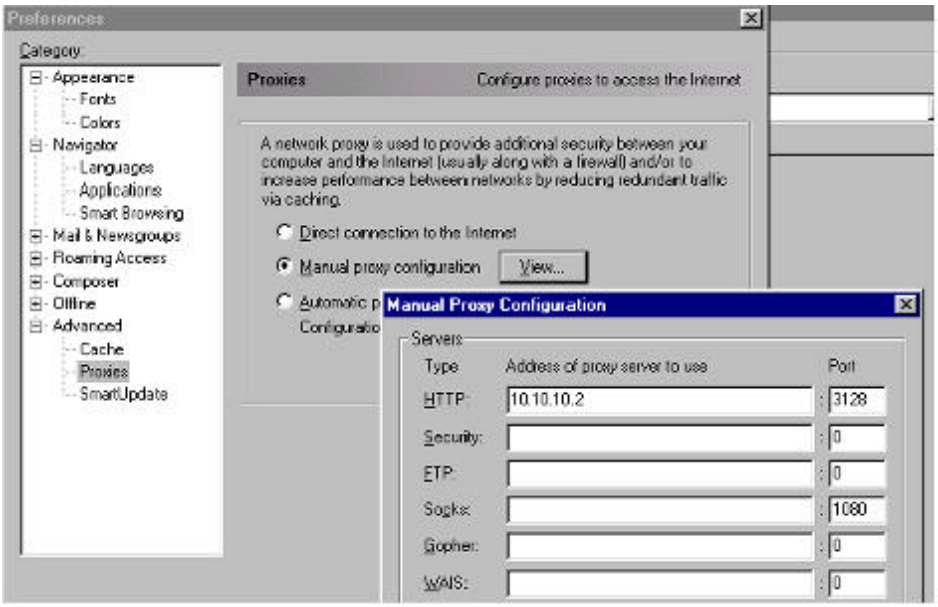
3.5 - Proxy Cache:

O proxy cache é um serviço que funciona na camada de aplicação do TCP/IP, ele permite controlar os acessos dos clientes com mais detalhes do que um simples firewall.

Outro detalhe importante do proxy cache é a geração de logs detalhados, autenticações dos clientes e caches de acesso. Tornando possível a navegação off-line do cliente, como pode ser visto no software de proxy Wwwoffle (http://www.gedanken.demon.co.uk/wwwoffle/).

O cache quando bem dimensionado pode aumentar muito a velocidade de acesso dos clientes. A grande vantagem do proxy cache é que a maioria dos clientes possuem suporte a essa ferramenta. Abaixo (figura 3.5.1) há um exemplo simples da configuração do netscape communicator (em Edit/preferences/advanced/proxies/Manual proxy configuration/), neste exemplo o servidor proxy cache é o 10.10.10.2 e a porta é a 3128/tcp .

figura 3.5.1



O acesso ao proxy cache pode ser visto na figura abaixo (figura 3.5.2). O cliente devidamente configurado envia uma requisição ao proxy cache e em seguida o proxy cache envia uma requisição ao servidor web na internet, quando a respota é recebida o proxy cache devolve a requisição ao cliente e arquiva em seu cache. O cliente não tem contato direto com o servidor web na internet e todas as páginas web sofrem uma triagem podendo negar acessos a urls específicas, palavras contidas nas páginas, sites específicos, verificação de vírus em arquivos baixados, autenticação de usuários, permissão de acessos somente em datas e horários específicos e outras verificações.

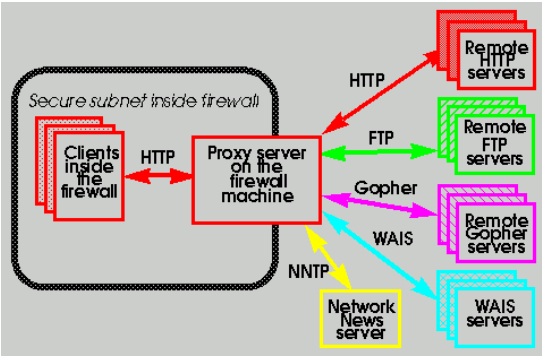


figura 3.5.2

Podemos observar abaixo (fugura 3.5.3) como a requisição é realizada através de um proxy cache.

Se o usuário digitasse a URL:

http://teste.com.br/index.htm

O browser devidamente configurado converteria para a requisição:

GET http://teste.com.br/index.htm

O proxy converteria a requisição para o servidor web desta forma:

GET /index.htm

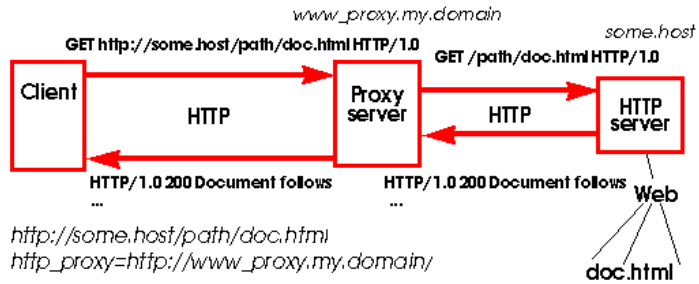
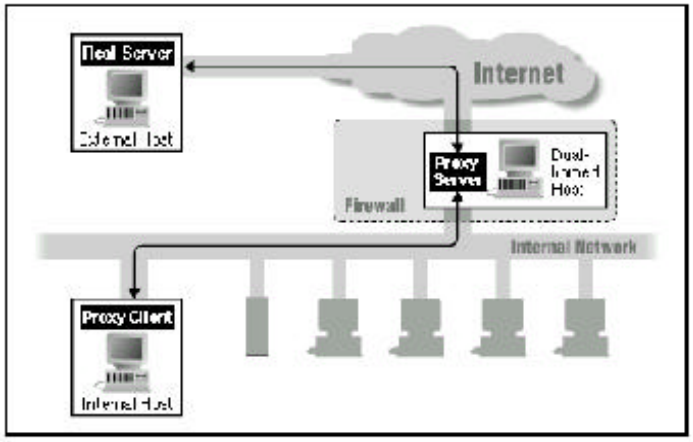


figura 3.5.3

3.6 - Arquiteturas Básicas de Firewall:

- Dual Homed:

figura 3.6.1 (Roteamento de Ip forward e ip desativado)



Utilização de servidor *proxy* em um dual-homed *host*

- Screened Host:

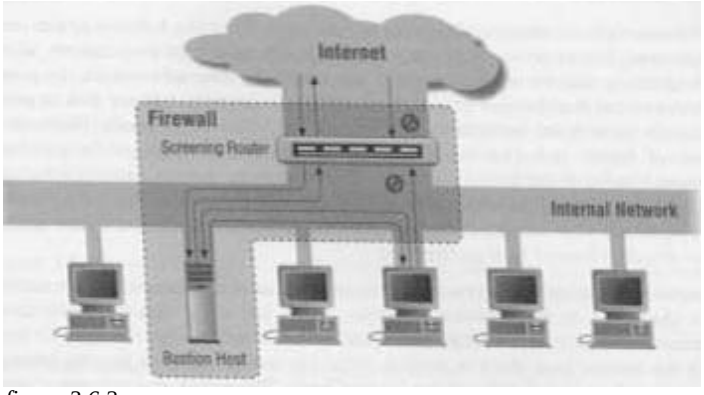


figura 3.6.2

- Sub-Rede Screened:

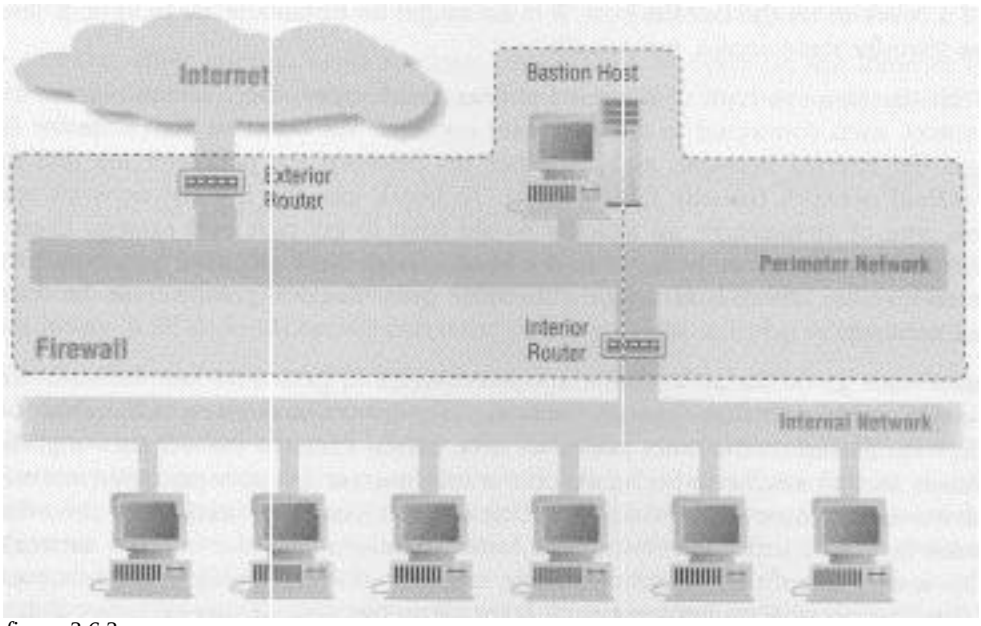


figura 3.6.3

(so permite tráfego para a DMZ)

Sentido das conexões em um creened subnet:

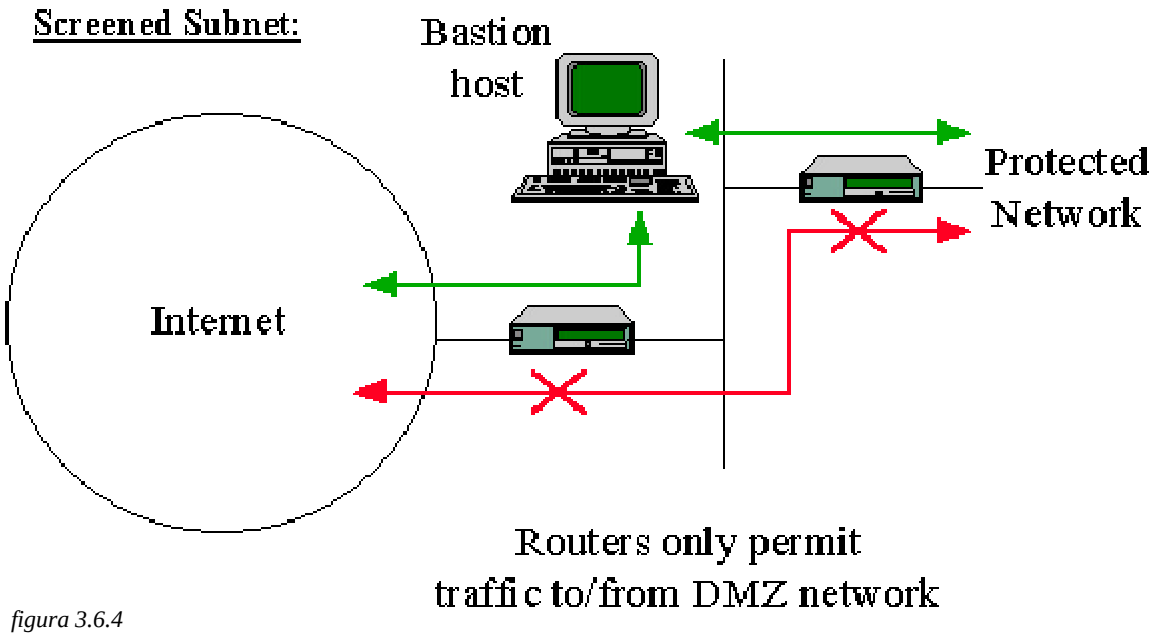
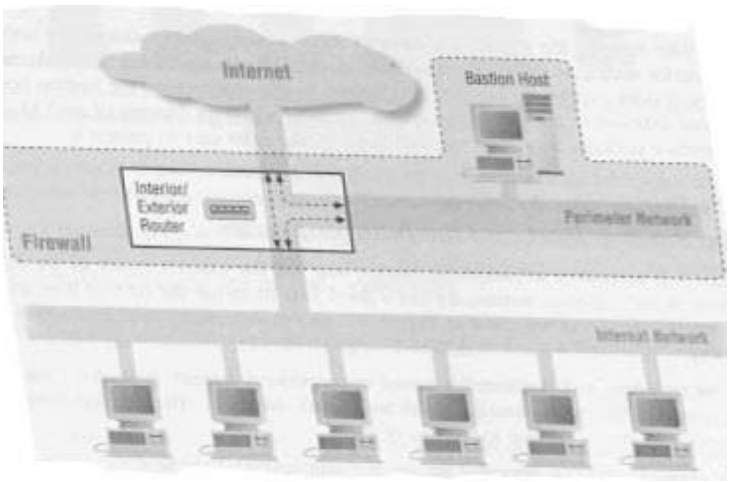


figura 3.6.4

- DMZ:

figura 3.6.5

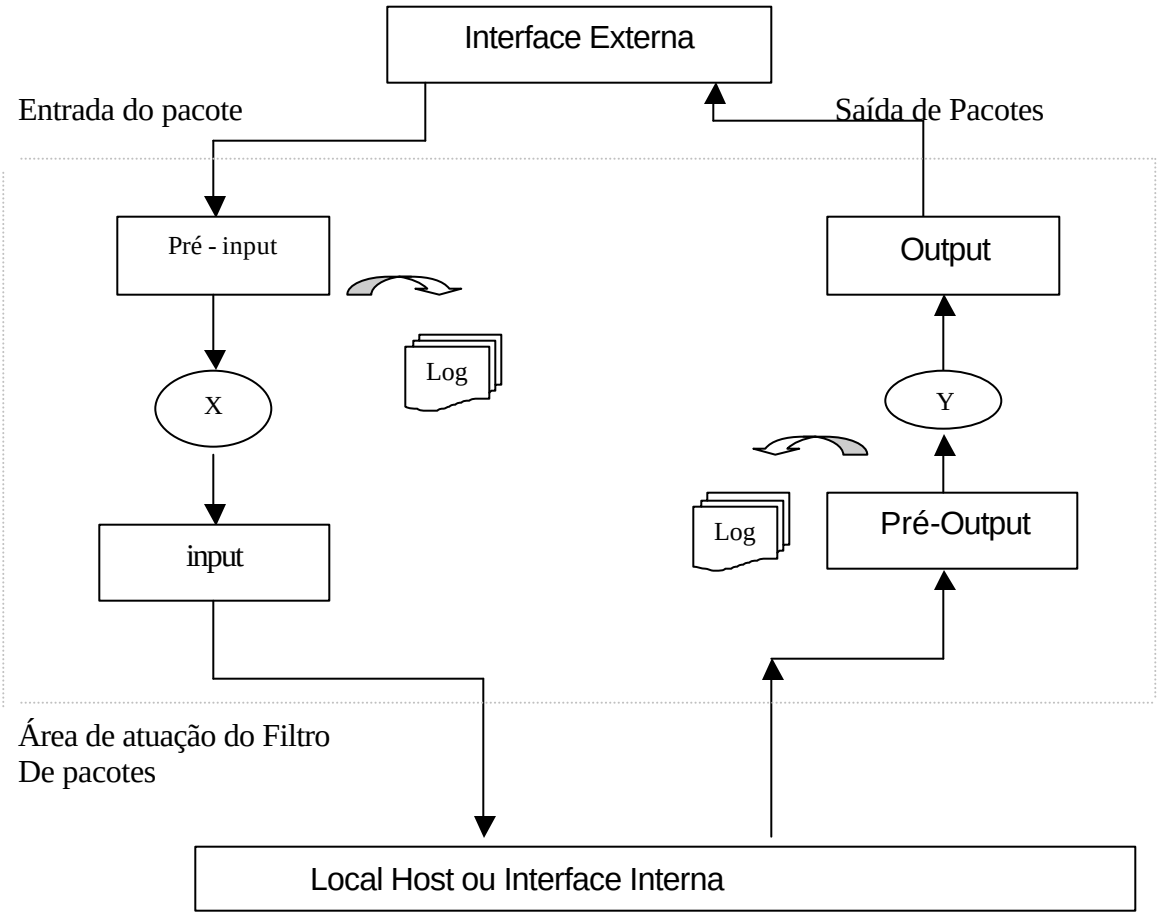


Na escolha de um firewall devemos observar a fórmula:

Firewall = [(sua necessidade) + (seu risco)] / (seu custo)

3.7 - Entendendo o filtro de pacote com diagramas de blocos:

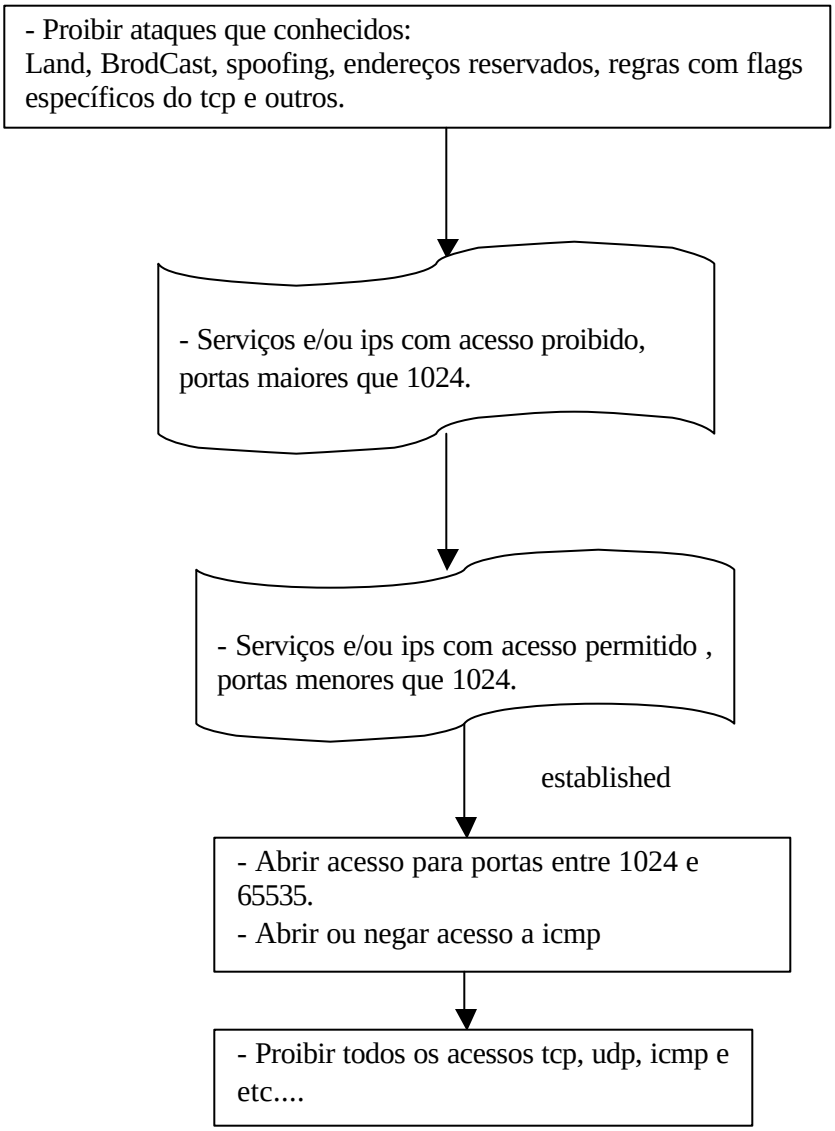
Este item irá mostrar como o filtro de pacotes funciona através de um modelo de diagrama de blocos. Esta modelo foi baseado no modelo do manual do BSD/OS. Iremos adaptá–lo para entender os diversos softwares de filtro de pacotes existentes.



Nos pontos “Pré-Input” e “Pré-Output” são executados as regras do filtro de pacote, as regras são executadas uma a uma da primeira a última. As regras são aplicadas até encontrar uma ocorrência que satisfaça a conexão, então este pacote pode ser enviado para o host (ou interface interna/externa) ou descartado. Nestes pontos são efetuados logs para um Log Hosts na rede ou conectado no console (Log Host Burro).

Nos pontos de “Pré-Input” e “Pré-Output” são usados nas configurações de proxy transparentes ou na ativação do NAT (Network Translate Adrress).

3.8 - Diagrama de blocos das linhas de comandos dos filtros de pacotes



Neste exemplo os blocos de comandos representados por retângulos geralmente não são alterados, em contrapartida os outros blocos de comandos costumam sofre alterações constantes.

O segundo e terceiro bloco podem Ter suas ordens invertidas.

4 - Instalação do IPFilter

4.1 - Visão Geral:

O ipfilter é um filtro de pacotes bastante flexível e possui portabilidade para diversas plataformas. Alguns sistemas operacionais trazem esse software "nativo" . Esse é o caso do OpenBSD, FreeBSD e NetBSD.

O Projeto do ipfilter, como a maioria dos softwares open source, sobrevive graças a doações de material e ajuda de voluntários. Maiores detalhes sobre doações: darrenr@pobox.com.

O ipfilter possui dois softwares que merecem destaques: ipf (filtro de pacotes) e o ipnat (NAT).

Softwares que compõem o pacote do ipfilter:

- ipf - Software responsável pelo filtro de pacotes;
- ipnat – Software responsável pelo NAT;
- Ipstat - Software responsável pela estatísticas dos pacotes inbound e outbound;
- Ipftest – Testa as rules do arquivo ipf;
- Iptest – Testa a configuração enviando pacotes IP;
- Ipmon – Lê os dados e armazena em logs tendo como saida: a tela, o syslogd ou arquivo;
- Ipsend – Gera arbitrários pacotes IP na maquina conectada;
- Ipresend – Lê dados salvos em arquivos e os envia.

Softwares existentes no pacote ipfilter:

- ftp-gw - Proxy transparente do Tis Firewall;
- Ipf-mrtg - Lê o ipfilter para ser usado pelo MRTG;
- Isbgraph – Program gráfico baseado no graphmaker;
- Logfilter - Filtra os logs do ipfilter;
- Plog - Filtra logs originados pelo ipfilter;
- Proxy.c – Simples Proxy Transparente.

Outros softwares:

- UCD SNMP – Suporta o ipfilter, podendo gerar estatíticas snmp
  Site relacionado: http://net-snmp.sourceforge.net/

- Squid – Proxy cache que pode ser usado na rquitetura de proxy cache transparente;

- Tis Firewall – Firewall a nível de aplicação que pode ser usado na arquitetura Sub-Rede Screened como um Bastion Host.

- Flc: Facilita a escrita das rules. Também podemos exportar e importar rules de outros filtros de pacotes como ipfilter, access-list, ipfawdm e ipfw.
  Site relacionado: http://coombs.anu.edu.au/~avalon/flc.html.

4.2 – Instalação do Pacote ipfilter em Solaris 2.6:

```
$ gunzip ip-fil3.4.10.tar.gz
$ tar –xvf ip-fil3.4.10.tar
$ cd ip_fil3.4.10
$ make solaris
$ make package
```

Será necessário reiniciar o sistema, com isso os módulos serão carregados.

No momento da incialização obteremos a seguinte saida na tela, indicando que os módulos foram carregados:

```
IP Filter: initialized.  Default = pass all, Logging = enabled
```

Os programas, manuais e exemplos estrão em /opt/ipf. Os arquivos de configuração estarão em /etc/opt/ipf/.

Para inicializar automaticamente o ipfilter basta criar um script rc no sistema.
Ex: /etc/rc.3/S93ipfilter

4.3 – Instalação do Pacote ipfilter em Linux:

Requesitos: Linux 2.0.31 ou maior e o kernel em /usr/src/linux

```
$ gunzip ip-fil3.4.10.tar.gz
$ tar –xvf ip-fil3.4.10.tar
$ cd ip_fil3.4.10
$ make  linux
$ make install-linux
$ Linux/minstall
(configura os devices do ipfilter)
$ Linux/kinstall
(aplica o patch no kernel)
```

Vá até /usr/src/linux e configure seu kernel, marque as opções referentes ao pacote do ipfilter. Salve a nova configuração e compile o novo kernel. Em seguida, instale o novo kernel e reinicialize o sistema para carregar o novo kernel.

Após reiniciar o sistema com o novo kernel poderemos ler o modulo do ipfilter com:

```
$ insmod if_ipl
```

Obteremos a seguinte saida na tela:

```
IP Filter: initialized.  Default = pass all, Logging = enabled
```

O processo de compilação do kernel pode ser estudado no Kernel How-to, em:

http://www.linux.org/docs/ldp/howto/Kernel-HOWTO/
http://tldp.org/HOWTO/Kernel-HOWTO.html
http://www.ibiblio.org/pub/Linux/docs/HOWTO/Kernel-HOWTO
http://www.tldp.org/
http://www.linux.com/

4.4 - Ativação do Pacote ipfilter em FreeBSD 4.7

O Freebsd 4.0 ou superior possui inerente ao sistema o ipfilter, muitas vezes é necessário apenas ativá-lo no kernel.

Inicialmente precisamos saber se o ipfilter está ativado no seu kernel, para isso verifique se as linhas abaixo estão em seu kernel no diretório /usr/src/sys/i386/conf/:

```
options     IPFILTER
options     IPFILTER_LOG
```

Caso estas linhas não estejam habilitadas edite–as e depois compile o novo kernel.Defineremos neste exemplo, que o arquivo com os parâmetros do kernel é o GENERIC.

Editando as linhas:

```
cd /usr/src/sys/i386/conf
vi      GENERIC
```

(agora edite as duas linhas "options IPFILTER" e options "IPFILTER_FILTER")

Agora compile o kernel:

```
config   GENERIC
cd ../../compile/GENERIC
make depend
make
make install
fastboot
```

Obteremos a seguinte saída na tela ao reiniciar o servidor:

```
IP Filter: initialized.  Default = pass all, Logging = enabled
```

5 – IPFilter

Como foi mencionado, o ipfilter é um pacote com grande portabilidade para os principais sistemas UNIX/LINUX, possui sintaxe de comando parecida com a maioria dos filtros e facilidde de implantação em firewalls ou Hosts.

Apesar de não ser tão utilizado no mundo Linux, o ipfilter possui uma documentação (HOW-TO) mais completa que os outros como ipfw, ipfwdm e ipchain.

O ipfilter é iniciado partindo do princípio que no final do arquivo de configuração será permitido a passagem de quaisquer pacotes de todos para todos, isso deve ser sempre observado para não termos problemas desagradáveis. Para evitarmos isso, devemos compilar o ipfilter com a opção –DIPFILTER_DEFAULT_BLOCK.

- Sintaxe do ipf: /sbin/ipf -Fa -f /etc/ipf.rules -E

- Parâmetros do ipf:

Parâmetros	***Significado***
F	Causa um flush na lista dos filtros
A	Aplica as regras ativas
E	Habilita os filtros
I	Aplica as regras inativas
D	Desabilita os filtros
d	Habilita o debug
f	Lê as rules do rquivo especificado
l	Loga os pacotes
s	Ativa swap e desabilita os rules setadas
r	Remove as rules
v	Habilita o verbose modo

Tabela 5.1

Parâmetros do ipmon:

Ex: /sbin/ipmon -Ds

Parâmetros	***Significado***
a	Habilita log em todos os devices
f	Especifica o device que irá ser logado
D	Torna um ipmon um daemon
F	Flush nos pacotes logados no buffer
N	Especifica o device que irá ser logado no NAT
o	Especifica o que será logado
s	Os logs serão enviados para o syslogd
x	Mostra o pacote em hex
X	Mostra o cabeçalho do pacote em hex

Tabela 5.2

- Rules do ipf:

Ação	**Sentido**	**log**	**Interface**	**Proto**	**Ip origem**	**Mask origem**	**Ip destino**	**Mask destino**	**porta**	**parâmetro**

- Ação: Indica como o pacote será tratado, podendo ser: pass | block

- Sentido: Sentido do pacote, tendo como referencia o slot da placa de rede, podendo ser:

in (entrada de pacotes)
out (saida de pacotes)

- Log: opções existentes para logs.

A simples existencia dessa declaração indica que a ocorrência deve ser logada.
Também podemos usar declarações enviando -as para o syslogd (/dev/ipl), opções como:

level auth.info
level auth.alert
level auth.debug

- Interface: Interface de comunicação. O device pode ser verificado pelo comando: ifconfig –a

- Proto: Protocolo usado, opções: tcp | udp | icmp | ip

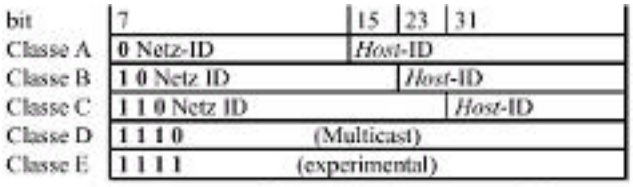
- Ip origem: Endereço ip de origem. Exemplo: 10.1.1.2

Também podemos usar a declaração any (todos).

- Máscara de origem: Máscara da rede de origem, exemplos:

/8 (classe A)
/16 (clsse B)
/24 (clsse C)
/32 (Host)

Podemos o esquema CIDR (RFCS 1518 e 1519), exemplos:
Máscara em decimal: 255.255.255.128
Máscara em Binário: 11111111. 11111111. 11111111.10000000
Máscara usada: /25
Neste exemplo poderiamos ter a rede: 192.168.12.0/25



Classes do endereçamento IP

Figura 5.1

Para evitar dúvidas colocaremos uma tabela para cada classe de rede :

Classe A				
Número de sub-redes	**Bits do host**	**Máscara de sub-rede**	**CIDR**	**Hosts / sub-rede**
01 – 02	1	255.128.0.0	/9	8.388.606
03 – 04	2	255.192.0.0	/10	4.194.302
05 – 08	3	255.224.0.0	/11	2.097.150
09 – 16	4	255.240.0.0	/12	1.048.574
17 – 32	5	255.248.0.0	/13	524.286
33-64	6	255.252.0.0	/14	262.142
65-128	7	255.254.0.0	/15	131.070
129-256	8	255.255.0.0	/16	65.534
257-512	9	255.255.128.0	/17	32.766
513-1.024	10	255.255.192.0	/18	16.382
1.025-2.048	11	255.255.224.0	/19	8.190
2.049-4.096	12	255.255.240.0	/20	4.094
4.097-8.192	13	255.255.248.0	/21	2.046
8.193-16.384	14	255.255.252.0	/22	1.022
16.385-32.768	15	255.255.254.0	/23	510
32.769-65.536	16	255.255.255.0	/24	254
65.637-131.072	17	255.255.255.128	/25	126
131.073-262.144	18	255.255.255.192	/26	62
262.145-524.288	19	255.255.255.224	/27	30
524.289-1.048.576	20	255.255.255.240	/28	14
1.048.577-2.097.152	21	255.255.255.248	/29	6
2.097.153-4.194.304	22	255.255.255.252	/30	2

Tabela 5.3

Classe B				
Número de sub-redes	**Bits do host**	**Máscara de sub-rede**	**CIDR**	**Hosts / sub-rede**
01 – 02	1	255.255.128.0	/17	32.766
03 – 04	2	255.255.192.0	/18	16.382
05 – 08	3	255.255.224.0	/19	8.190
09 – 16	4	255.255.240.0	/20	4.094
17 – 32	5	255.255.248.0	/21	2.046
33-64	6	255.255.252.0	/22	1.022
65-128	7	255.255.254.0	/23	510
129-256	8	255.255.255.0	/24	254
257-512	9	255.255.255.128	/25	126

513-1.024	10	255.255.255.192	/26	62
1.025-2.048	11	255.255.255.224	/27	30
2.049-4.096	12	255.255.255.240	/28	14
4.097-8.192	13	255.255.255.248	/29	6
8.193-16.384	14	255.255.255.252	/30	2

Tabela 5.4

Classe C				
Número de sub-redes	**Bits do host**	**Máscara de sub-rede**	**CIDR**	**Hosts / sub-rede**
01 – 02	1	255.255.255.128	/25	126
03 – 04	2	255.255.255.192	/26	62
05 – 08	3	255.255.255.224	/27	30
09 – 16	4	255.255.255.240	/28	14
17 – 32	5	255.255.255.248	/29	6
33 - 64	6	255.255.255.252	/20	2

Tabela 5.5

Classes de Endereços IP:

Nome	**IP**	**NetID**	**HostID**	**Uso**
Classe A	1 a 126	126	16.777.214	**-**
Classe B	128 a 191	16.384	65.534	**-**
Classe C	192 a 223	2.097.151	254	**-**
Classe D	224 a 239		**-**	Multicast
Classe E	240 a 247		**-**	Reservado

Tabela 5.6

Endereços reservados pela RFC1918:

Endereço inicial	**Endereço final**	**Mask**
10.0.0.0	10.255.255.255	10/8
172.16.16.0	172.31.255.255	172.16/16
192.168.0.0	192.168.255.255	192.168/16

Tabela 5.7

Endereço de Loop Back:

Endereço inicial	**Endereço final**	**Mask**
127.0.0.0	127.255.255.255	127/8

Tabela 5.8

- Ip destino: Endereço ip de destino. Exemplo: 10.1.1.2

- Máscara de destino: Máscara da rede de destino, vide exemplos de "Máscara de origem".

- Portas: Portas de serviços usadas, Exemplos:

port < 1024 - Regra validada para as portas menores que 1024
port >= 1024 - Regra validada para as portas maiores e igual à 1024
port > 1023 - Regra validada para as portas maiores que 1023
port <= 1023 - Regra validada para as portas menores e iguais á 1023
port 1023 >< 65536 - Regra validada para as portas que estao entre 1023 e 65536
port 6000 <> 6011 - Regra validada para as portas que não estão entre 6000 e 6011
port != 23 - Regra validada para as portas diferentes de 23
port = 111 - Regra validada para a porta 111

Devemos lembrar que as portas são agrupadas em três faixas:

- Well Known Ports - 0 a 1023

Está faixa é destinada a serviços já bem estabelecidos e de interesse geral. Normalmente, a ativação desses serviços exige privilégios de administrador do sistema.

- Registered Ports - 1024 a 49151

Esta faixa é usada para os programas de usuários (clientes) e outros serviços, que podem ser ativados sem privilégios de administrador. Salvo alguns casos como NFS, X-windows e outros.

- Dynamic and/or Private Ports - 49152 a 65535

Basicamente quando um cliente conecta um serviço como o smtp, ele o faz abrindo uma conexão em uma porta maior que 1023 enquanto isso o servidor escuta a requisição na porta 25. Para a maioria dos serviços este modelo e' verdadeiro. Salvo casos como nfs, X-windows, OpenWindows e etc.

- Parâmetros: Os parâmetros mais usados são:

Para o TCP:

Flags	**Significado**

S	SYN
A	ACK
R	RST
U	URG
F	FIN
P	PUSH

Tabela 5.9

Para o ICMP:

Flags	**Número**
Unreach	3
Echo	8
Echorep	0
Squench	4
Redir	5
Timex	11
Paramprob	12
Timest	13
Timestrep	14
Inforeq	15
Inforep	16
Maskreq	17
Maskrep	18

Tabela 5.10

Exemplos do ipf:

Este exemplo é para um servidor com uma placa de rede, e com os seguintes dados:

IP	x.y.z.w/24
Rede	x.y.z.0
Broadcast	x.y.z.255
Interface	ne3
Máscara	255.255.255.0
Loopback	127.0.0.1/8
Placa loopback	lo0

Tabela 5.11

```
block in all with frag
block in quick proto tcp all with short
block in quick on ne3 all with opt lsrr
block in quick on ne3 all with opt ssrr
block in log quick on ne3 all with ipopts
block in quick on ne3 all with opt  ssrr,lsrr,rr
block in quick on ne3 proto tcp from any to any flags FUP
block in quick on ne3 proto tcp from any to any flags SF
block in quick on ne3 proto tcp from any to any flags SR
# inicio do ipf
# bloqueia a entrada pela interface ne3 de pacotes originados do ip= 192.168.0.0/16  logando estes
block in log quick on ne3 from 192.168.0.0/16 to any
# bloqueia a entrada pela interface ne3 de pacotes originados do ip= 172.16.0.0/12 logando estes
block in log quick on ne3 from 172.16.0.0/12 to any
# bloqueia a entrada pela interface ne3 de pacotes originados do ip= 10.0.0.0/8  logando estes
block in log quick on ne3 from 10.0.0.0/8 to any
# bloqueia a entrada pela interface ne3 de pacotes originados do ip= 127.0.0.1/8  logando estes
block in log quick on ne3 from 127.0.0.0/8 to any
# bloqueia a entrada pela interface lo0 de pacotes originados com o mesmo ip da interface lo0
#  usando proto tcp ou udp, logando estes
block in log quick on lo0 proto tcp/udp from x.y.z.w/32 to x.y.z.w /32
# bloqueia a saida pela interface lo0 de pacotes originados com o mesmo ip da interface lo0
# usando proto tcp ou udp, logando estes
block out  log quick on lo0 proto tcp/udp from x.y.z.w /32 to x.y.z.w /32
# bloqueia a entrada pela interface ne3 de pacotes originados com o mesmo ip da interface ne3
# usando proto tcp ou udp,  logando estes
block in  log quick on ne3 proto tcp/udp from x.y.z.w /32 to x.y.z.w /32
# bloqueia a saida pela interface ne3 de pacotes originados com o mesmo ip da interface ne3
# usando proto tcp ou udp, logando estes
block out log quick on ne3 proto tcp/udp from x. y.z.w /32 to x.y.z.w /32
# bloqueia a entrada pela interface ne3 de pacotes originados com o ip 240.0.0.0/27
# usando proto tcp ou udp, logando estes
block in  log quick on ne3  proto tcp/udp from 240.0.0.0/24 to any
# bloqueia a entrada pela interface ne3 de pacotes originados com o ip 224.0.0.0/28
# usando proto tcp ou udp, logando estes
block in  log quick on ne3  proto tcp/udp from 224.0.0.0/24 to any
# bloqueia a entrada pela interface ne3 de pacotes originados com o ip da interface lo0
#  com destino a ela mesma usando proto tcp ou udp,  logando estes
block in  log quick on ne3  proto tcp/udp from 127.0.0.0/8 to 127.0.0.0/8
# bloqueia a saida pela interface ne3 de pacotes originados com o ip da interface lo0
#  com destino a ela mesma usando proto tcp ou udp,  logando estes
block out log quick on ne3 proto tcp/udp from 127.0.0.0/8  to 127.0.0.0/8
# bloqueia a entrada pela interface ne3 de pacotes com destino a rede
# , logando estes
block in log quick on ne3 from any to x.y.z.0/32
# bloqueia a entrada pela interface ne3 de pacotes com destino ao broadcast da rede
# , logando estes
block in log quick on ne3 from any to x.y.z.255/32
# bloqueia spoof
block in log quick on ne3 from x.y.z.w/32 to any

# permite a comunicação udp na porta 53 de todos para todos, no sentido “in” pela ne3
pass in quick on ne3 proto udp from any port > 1023 to any port = 53  keep state
# permite a comunicação udp na porta 53 de todos para todos no sentido “out” pela ne3
pass out quick on ne3 proto udp from any port > 1023 to any port = 53
# bloqueia a comunicação tcp na porta 53 de todos para todos no sentido “in” pela ne3
```

```
block in log quick on ne3 proto tcp from any  to any  port = 53
# permite o ip x.y.z.31/32 acessar via ssh (porta 22) a maquina x.y.z.w /32 conexão “in” da ne3
pass in quick on ne3  proto tcp from x.y.z.31/32 port > 1023 to x.y.z.w /32 port = 22 flags S keep state
pass in quick on ne3  proto udp from x.y.z.31/32 port > 1023 to x.y.z.w/32 port = 22 keep state
# impede que  alguem abtenha acesso ao serviço de ssh (porta 22) conexão no sentido “in” da ne3
# , logando as ocorrências
block in log quick on ne3 proto tcp from any to x.y.z..34/32  port = 22
block in log quick on ne3 proto udp from any to x.y.z..34/32  port = 22

# bloqueia acesso no sentido  “in” da ne3 na porta 69 proto tcp ou udp, logando
block in log quick on ne3  proto tcp/udp from  any to any  port = 69
# bloqueia acesso no sentido  “out” da ne3 na porta 69 proto tcp ou udp, logando
block out log quick on ne3  proto tcp/udp from  any to any  port = 69
# bloqueia acesso no sentido  “in” da ne3 na porta 79 proto tcp ou udp, logando
block in log quick on ne3  proto tcp/udp from  any to any  port = 79
# bloqueia acesso no sentido  “out” da ne3 na porta 79 proto tcp ou udp, logando
block out log quick on ne3  proto tcp/udp from  any to any  port = 79
# bloqueia acesso no sentido  “in” da ne3 na porta 111 proto tcp ou udp, logando
block in log quick on ne3  proto tcp/udp from  any to any  port = 111
# bloqueia acesso no sentido  “out” da ne3 na porta 111 proto tcp ou udp, logando
block out log quick on ne3  proto tcp/udp from  any to any  port = 111
# bloqueia acesso no sentido  “in” da ne3 na porta 113 proto tcp ou udp, logando
block in log quick on ne3  proto tcp/udp from  any to any  port = 113
# bloqueia acesso no sentido  “out” da ne3 na porta 113 proto tcp ou udp, logando
block out log quick on ne3  proto tcp/udp from  any to any  port = 113
# bloqueia acesso no sentido  “in”da ne3 entre as porta 134 e 140 proto tcp ou udp
# , logando
block in log quick on ne3  proto tcp/udp from  any to any  port    134 >< 140
# bloqueia acesso no sentido  “out”da ne3 entre as porta 134 e 140 proto tcp ou udp
# , logando
block out log quick on ne3  proto tcp/udp from  any to any  port  134 >< 140
# bloqueia acesso no sentido  “in”da ne3 entre as porta 500 e 560 proto tcp ou udp
# , logando
block in log quick on ne3  proto tcp/udp from  any to any  port   500 >< 560
# bloqueia acesso no sentido  “out”da ne3 entre as porta 500 e 560 proto tcp ou udp
# , logando
block out log quick on ne3  proto tcp/udp from  any to any  port  500 >< 560
# bloqueia acesso no sentido  “in” da ne3 na porta 1524 proto tcp ou udp, logando
block in log quick on ne3  proto tcp/udp from  any to any  port = 1524
# bloqueia acesso no sentido  “out” da ne3 na porta 1524 proto tcp ou udp, logando
block out log quick on ne3  proto tcp/udp from  any to any  port = 1524
# bloqueia acesso no sentido  “in” da ne3 entre as porta 5800 e 6012 proto tcp ou udp
# , logando
block in log quick on ne3  proto tcp/udp from any to any port  5800  >< 6012
# bloqueia acesso no sentido  “in” da ne3 entre as porta 5800 e 6012 proto tcp ou udp
# , logando
block out log quick on ne3  proto tcp/udp from any to any port  5800  >< 6012
# bloqueia acesso no sentido  “in” da ne3 entre as porta 1999 e 2005 proto tcp ou udp
# , logando
block in log quick on ne3  proto tcp/udp from any to any port  1999 >< 2005
# bloqueia acesso no sentido  “out” da ne3 entre as porta 1999 e 2005 proto tcp ou udp
# , logando
block out log quick on ne3  proto tcp/udp from any to any port  1999 >< 2005
# bloqueia acesso no sentido  “in” da ne3 na porta 2049 proto tcp ou udp, logando
block in log quick on ne3  proto tcp/udp from  any to any  port =  2049
# bloqueia acesso no sentido  “out” da ne3 na porta 2049 proto tcp ou udp, logando
```

```
block out log quick on ne3  proto tcp/udp from  any to any  port = 2049
# bloqueia acesso no sentido  “in” da ne3 na porta 20034 proto tcp ou udp, logando
block in log quick on ne3  proto tcp/udp from  any to any  port = 20034
# bloqueia acesso no sentido  “out” da ne3 na porta 20034 proto tcp ou udp, logando
block out log quick on ne3  proto tcp/udp from  any to any  port = 20034
# bloqueia acesso no sentido  “in” da ne3 na porta 20034 proto tcp ou udp, logando
block in log quick on ne3  proto tcp/udp from  any to any  port = 31337
# bloqueia acesso no sentido  “out” da ne3 na porta 31337 proto tcp ou udp, logando
block out log quick on ne3  proto tcp/udp from  any to any  port = 31337

# icmp trafic
# permite acesso no sentido  “in” da ne3 do proto icmp código 0
pass in quick on ne3 proto icmp from any to any icmp-type 0
# permite acesso no sentido  “out” da ne3 do proto icmp código 8
pass out quick on ne3 proto icmp from any to any icmp-type 8
# permite acesso no sentido  “out” da ne3 do proto icmp código 11
pass out quick on ne3  proto icmp from any to any icmp-type 11
# bloqueia acesso no sentido  “out” da ne3 do proto icmp
block out log quick on ne3  proto icmp from any to any
# bloqueia acesso no sentido  “in” da ne3 do proto icmp
block in log quick on ne3  proto icmp from any to any
block in on ne3  all
# permite a saída  de conexões já estabelecidas
pass  out quick on ne3 proto tcp/udp from x.y.z.w/32  to any keep state
# bloqueia na ne3 entrada de pacotes  tcp em porta menores e iquais à 1023
# para o ip x.y.z.w/32
block in log quick on ne3 proto tcp from any to x.y.z.w /32  port <= 1023
# bloqueia na ne3 entrada de pacotes  udp em porta menores e iquais à 1023
# para o ip x.y.z.w/32
block in log quick on ne3 proto udp from any to x.y.z.w /32  port <= 1023
# permite na ne3 entrada de pacotes  tcp em porta maiores que 1023
# para o ip x.y.z.w/32
pass in quick on ne3 proto tcp from any to x.y.z.w /32  port  > 1023
# permite na ne3 entrada de pacotes  udp em porta maiores que 1023
# para o ip x.y.z.w/32
pass in  quick on ne3 proto udp from any to x.y.z.w /32  port  > 1023
# bloqueia os pacotes udp no sentido “in” de any to any
block in log quick on ne3 proto udp from  any to any
# bloqueia os pacotes tcp no sentido “in” de any to any
block in log quick on ne3 proto tcp from  any to any
# bloqueia os pacotes ip no sentido “in” de any to any
block in log quick on ne3 proto ip from any to any
```

As duas regras em negrito no final da listagem que esta acima podem ser substituídas por:

```
pass out log quick on tun0 proto tcp/udp from x.y.z.w/32  port > 1023  to any
pass in log quick on tun0 proto tcp from any to x.y.z.w/32 flags A
pass in log quick on tun0 proto tcp from any port = 20 to x.y.z.w/32 port > 1023
```

Com estas regras podemos garantir que serviços ou backdoors (tcp) em portas maiores que 1024 não serão acessadas a menos que as liberemos no filtro de pacotes

previamente. Realizando esta subistituição devemos ficar atentos a possíveis problemas nas estações clientes da rede interna. Estas regras foram baseadas no estabelecimento da conexão do TCP:

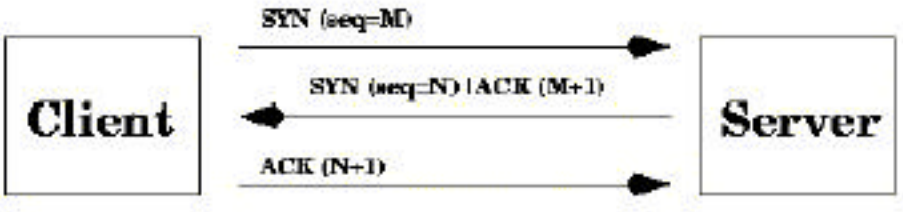


Figura 5.1

Exemplos utilizando outros parâmetros:

Bloqueia a entrada de pacote com destino rede x.y.z.0/24 pr a porta 23 enviando um reset para o ip origem.

> Block return-rst in log from any to x.y.z.0/24 proto tcp port = 23

Bloqueia a tentativa de conexão na porta 23 proto udp via tun0, enviando um icmp com código unreachable para quem o originou.

> block return-icmp(port-unr) in log quick on tun0 proto udp from any to any port = 23
ou
> block return-icmp-as-dest(port-unr) in log on tun0 proto udp from any to any port = 23

Bloqueia conexões na porta 23 via tun0 logando–as via syslogd como log information. Para isso é necessário startar o ipmon com o flag –s.

> block in log level auth.info quick on tun0 from any to any port = 23

Bloqueia conexões na porta 23 via tun0 logando –as via syslogd como log alert. Para isso é necessário startar o ipmon com o flag –s.

> block in log level auth.alert quick on tun0 proto tcp from any to any port = 23

- Manuais disponíveis

man ipf
man ipnat
man ipfstat
man ipmon
man ipftest

- Documentação:

Home Page Oficial do IPF:

http://coombs.anu.edu.au/~avalon/ip-filter.html
http://www.obfuscation.org/ipf/

6 – IPNat

- Sintaxe do ipnat: /sbin/ipnat –CF –f /etc/ipnat.rules

- Parâmetros do ipnat:

Ex:

Parâmetros	***significado***
C	Deleta todas as entradas do NAT
F	Flush nas rules do NAT
L	Mostra as rules ativadas
N	Não altera a tabela do NAT existente
S	Mostra estatítisca
V	Modo Verbose
F	Lê o file especificado

Tabela 6.1

Para startar o ipnat basta acrescentar a linha de comando mostrada acima em um rc script.

Outra forma de startar é através de um programa copilado em C:

```
/* programa start ipnat:   execnat.c */
#include <stdlib.h>
void main(void)
{ system (“
echo “ map ppp0 w.x.y.z/24 -> ªb.c.d/32 “ | /sbin/ipnat –f –
“);  }
/* fim do programa start ipnat */
Agora basta copilar o programa:
```

```
$ cc –o execnat execnat.c
$ chmod 755 execnat
$ ./execnat
$
```

- Rules do IPNAT:

Exemplo 1:

```
#   Habilita o acesso de ftp dos clientes internos em diração o server
# externo, solucionando
# o problema do reenvio do server pra o cliente
map  tun0  10.0.0.0/8  -> 0/32  proxy port  21  ftp/tcp
# mapeia todo  rede interna 10.0.0.0/8 para a interface tun0
map tun0  10.0.0.0/8 -> tun0/32
```

Exemplo2:

```
#   Mapeia todo  rede interna 10.0.0.0/8 para a interface
# com endereço x.y.z.0/24
# reservando uma range de 10000 até 60000 .
map tun0 10.0.0.0/8  -> x.y.z.0/24 portmap tcp/udp 10000:60000
```

Exemplo 3:

```
# Redireciona toda a conexão http para o proxy cache squid port 3128,
# habilitando o proxy transparente
rdr rl0  0.0.0.0/0 port 80 -> x.y.z.22  port 3128
#    Informações de como configurar o squid proxy cache para
# aceitar as conexões desviadas (forward) para a sua porta
# 3128 devem ser lidas no FAQ em http://squid.nlanr.net/
#
```

Exemplo 4:

```
#    Redireciona a conexão na porta 23 de x.y.z.7/24 interface rl1 para a
# porta 2323 do servidor interno 10.10.10.1
rdr rl1 x.y.z.7/24 port 23 -> 10.10.10.1 port 2323
```

- Documentação:

  http://www.openbsd.com/faq/faq6.html#6.2
  http://www.openbsd.org/cgi-bin/man.cgi?query=ipnat&sektion=8
  http://www.geektools.com/rfc/rfc1631.txt

7 - Variáveis de Kernel

- openbsd:

(Habilita o ipforward)
net.inet.ip.forwarding=1

(Habilita o nível de segurança do kernel)
kern.securelevel = 1

(Habilita mask reply)
net.inet.icmp.maskrepl = 0

(Não permite suid em arquivos core)
kern.nosuidcoredump = 1

(Habilita o ip source route)
net.inet.ip.sourceroute = 0

(Desabilita crtl+alt+del no console do server)
ddb.console = 0

(Habilita Broadcast)
net.inet.ip.directed-broadcast = 0

(Habilita ipv4)
net.inet.ip4.allow = 0

- freebsd:

(Habilita o ipforward)
net.inet.ip.forwarding=1

(Habilita o ip source route)
net.inet.ip.sourceroute=0

(Habilita o nível de segurança do kernel como 2)

kern.securelevel=2

(Habilita o firewall ipfw)
net.inet.ip.fw.enable = 1

(Limita o número de mensagem no processo verbose firewall)
net.inet.ip.fw.verbose_limit=0

(Habilita Broadcast)
net.ip.accept_sourceroute=0

(Loga as conexões TCP)
net.inet.tcp.log_in_vain=1

(Loga as conexões UDP)
net.inet.udp.log_in_vain=1

(Controla as mensagens debug do ipfw)
net.inet.ip.fw.debug=1

(Habilita debug mensagens do ipfw)
net.inet.ip.fw.verbose = 1

- solaris:

(Habilita o ipforward)
ndd –set /dev/ip ip_forwarding 1

(Habilita Broadcast)
ndd –set /dev/ip ip_forward_directed_broadcasts 0

(Habilita o ip source route)
ndd –set /dev/ip ip_forward_src_routed 0

(Habilita Broadcast)
ndd –set /dev/ip ip_respond_to_echo_broadcast 0

- Linux

(ignora icmp enviado para o broadcast)
$ echo “1” > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

(ignora icmp(echo) enviado)
$ echo “1” > /proc/sys/net/ipv4/icmp_echo_ignore_all

(anula ctrl+alt+del)
$ echo “1” > /proc/sys/kernel/ctrl-alt-del

(evita syn ataque DOS)
$ echo 1 > /proc/sys/net/ipv4/tcp_syncookies

8 - Filtros de pacotes alternativos (ipfw do FreeBSD)

Neste tópico tentaremos mostrar as rules do ipfw, um filtro de pacote alternativo encontrdo no Freebsd 2.x.x.

Este exemplo é para um servidor com uma placa de rede, e com os seguintes dados:

IP	x.y.z.w/24
Rede	x.y.z.0
Broadcast	x.y.z.255
Interface	ed1
Máscara	255.255.255.0
loopback	127.0.0.1/8
Placa loopback	lo0

Tabela 8.1

- Copilar o kernel com as opções:

```
# Habilita o filtro
options IPFIREWALL
options IPFIREWALL_VERBOSE
options IPFIREWALL_VERBOSE_LIMIT=100
options
IPFIREWALL_DEFAULT__TO_ACCEPT
# Habilita nat
options IPDIVERT
```

Outros parâmetros importantes do kernel:

- Retirando estas opções podemos evitar o método de descoberta do sistema operacional pelo finger print:

```
# The following options add sysctl variables for controlling how certain
# TCP packets are handled.
#
# TCP_DROP_SYNFIN adds support for ignoring TCP packets with SYN+FIN. This
# prevents nmap et al. from identifying the TCP/IP stack, but breaks support
# for RFC1644 extensions and is not recommended for web servers.
#
# TCP_RESTRICT_RST adds support for blocking the emission of TCP RST packets.
# This is useful on systems which are exposed to SYN floods (IRCservers)
# or any system which one does not want to be easily portscannable.
#
options      TCP_DROP_SYNFIN       #drop TCP packets with SYN+FIN
options      TCP_RESTRICT_RST      #restrict emission of TCP RST

# ICMP_BANDLIM enables icmp error response bandwidth limiting.   You
# typically want this option as it will help protect the machine from
# D.O.S. packet attacks.
#
options      ICMP_BANDLIM

options      IPSTEALTH
```

- Retirar a opção abaixo para evitar que as interfaces de rede fiquem em modo promisco:

```
Options  bpfilter  4
```

- Ativar as opções:

```
# ativa a contabilidade do sistema
Options sysacct
# implementa suporte a nível de segurança
C2
Options sysaudit
```

- Outras opções:

```
# Habilita a quota
```

```
Options  quota
# inibe crt+alt+del
options BOKEN_KEYBOARD_RESET
# HABILITA muli processamento
options smp
# Habilita editor userconfig
options USERCONFIG
# aplica a opção  -c no boot
options USERCONFIG_BOOT
# Habilita o visual userconfig
options VISUAL_USERCONFIG
# Habilita ccd (disco virtual)
options ccd
# Loga erros do kernel. Mandatório
options pseudo-device log
```

- Config do Freebsd:

```
/etc/rc.conf
firewall_enable="YES"
firewall_type="YES"
firewall_quiet="YES"
defaultrouter="x.y.z.1”
gateway_enable="YES"
natd_enable="YES”
natd_interface="ed1”


/etc/rc.local
/usr/sbin/ntpdate 133.100.11.8


/etc/services
natd      6668/divert
```

- Rules (/etc/rc.firewall):

```
if [ -f /etc/rc.conf ]; then
        . /etc/rc.conf
```

```
fi
if [ "x$1" != "x" ]; then
        firewall_type=$1
fi
if [ "x$firewall_quiet" = "xYES" ]; then
        fwcmd="/sbin/ipfw -q"
else
        fwcmd="/sbin/ipfw -q"
fi
$fwcmd -f flush
$fwcmd add 100 pass all from any to any via lo0
$fwcmd add 200 deny all from any to 127.0.0.0/8
net="x.y.z.0"
mask="255.255.255.0"
ip="x.y.z.w"
hostname="x.y.z.w"
backserver=”x.y.z.2”
nic=”ed1”

$fwcmd add deny  log tcp from 10.0.0.0:255.0.0.0 to any
# bloqueia pacotes origindos com ip 10/8 (tcp) , logando
$fwcmd add deny log  tcp from 172.16.0.0:255.240.0.0 to any
# bloqueia pacotes origindos com ip 172.16/16 (tcp) , logando
$fwcmd add deny  log tcp from 192.168.0.0:255.255.0.0 to any
# bloqueia pacotes origindos com ip 192.168.168/16 (tcp) , logando
$fwcmd add deny  log udp from 10.0.0.0:255.0.0.0 to any
# bloqueia pacotes origindos com ip 10/8 (udp) , logando
$fwcmd add deny  log udp from 172.16.0.0:255.240.0.0 to any
# bloqueia pacotes origindos com ip 172.16/16 (udp) , logando
$fwcmd add deny  log udp from 192.168.0.0:255.255.0.0 to any
# bloqueia pacotes origindos com ip 192.168/16 (udp) , logando
$fwcmd add deny  log tcp from x.y.z.w:255.255.255.0 to x.y.z.w:255.255.255.0
# bloqueia ataque land (tcp) , logando
$fwcmd add deny log  udp from x.y.z.w:255.255.255.0 to x.y.z.w:255.255.255.0
# bloqueia ataque land (udp) , logando
$fwcmd add deny log tcp from x.y.z.0:255.255.255.0 to any
# bloqueia pacotes destinado ao endereco de rede (tcp) , logando
$fwcmd add deny log tcp from x.y.z.255:255.255.255.255 to any
# bloqueia pacotes destinado ao endereco broadcast (tcp) , logando
$fwcmd add deny log udp from x.y.z.0:255.255.255.0 to any
# bloqueia pacotes destinado ao endereco de rede (udp) , logando
$fwcmd add deny log udp from x.y.z.255:255.255.255.255 to any
# bloqueia pacotes destinado ao endereco broadcast (udp) , logando
$fwcmd add deny log tcp from 240.0.0.0:255.255.255.0 to any
# bloqueia pacotes origindos com ip 240/24 (tcp) , logando
$fwcmd add deny log tcp from 224.0.0.0:255.255.255.0 to any
# bloqueia pacotes origindos com ip 224/24 (tcp) , logando
```

```
$fwcmd add deny log tcp from 127.0.0.0:255.0.0.0 to any
# bloqueia pacotes destinado ao loopback (tcp) , logando
$fwcmd add deny log udp from 127.0.0.0:255.0.0.0 to any
# bloqueia pacotes destinado ao loopback (udp) , logando
$fwcmd add deny log udp from 240.0.0.0:255.255.255.0 to any
# bloqueia pacotes origindos com ip 240/24 (udp) , logando
$fwcmd add deny log udp from 224.0.0.0:255.255.255.0 to any
# bloqueia pacotes origindos com ip 224/24 (udp) , logando
$fwcmd add deny log udp from 127.0.0.0:255.0.0.0 to any
# bloqueia pacotes origindos no loopback  (udp) , logando
$fwcmd add deny log tcp from any to any ipoptions ssrr,lsrr,rr
$fwcmd add deny log ip from not ${hostname} to any via ${nic} out
# bloqueia pacotes  originados na interface ${nic} que não seja o seu original , logando
$fwcmd add deny log tcp from any to ${hostname} tcpflags syn,fin
# bloqueia pacotes origindos com flags syn e fin acionados (tcp) , logando
$fwcmd add deny log tcp from any to ${hostname} tcpflags syn,rst
# bloqueia pacotes origindos com flgs rst e syn acionados (tcp) , logando
$fwcmd add deny log ip from  ${ip} to any via ${nic} in
# bloqueia tentativa  de spoof , logando
$fwcmd add pass udp from any 53 to ${ip}
$fwcmd add pass udp from ${ip} to any 53
# permite acesso so serviço de dns
$fwcmd add pass udp from any to any 123
# permite acesso ao serviço ntp port 123/udp
$fwcmd add pass tcp from x.y.z.0:255.255.255.0   to ${ip} 22 setup
$fwcmd add pass udp from x.y.z.0:255.255.255.0  to ${ip} 22 setup
# permite acessos da rede interna ao serviço de ssh port 22/tcp

$fwcmd add pass tcp from  ${backserver}to ${ip} 111,1023,1110,2049 setup
# permite acesso do server de backup a ${ip} nas portas 111,1023,1110,2049 (tcp)
$fwcmd add pass tcp from ${ip} 111,1023,1110,2049 to ${backserver} setup
# permite acesso do server de backup a ${ip} nas portas 111,1023,1110,2049 (udp)
$fwcmd add pass udp from ${backserver} to ${ip}
$fwcmd add pass udp from ${ip} to ${backserver}
# permite acesso ao server de backup (udp)

$fwcmd add deny log tcp from any to ${ip} 2049
# bloqueia acesso ao serviço nfs (tcp) , logando
$fwcmd add deny log udp from any to ${ip} 2049
# bloqueia acesso ao serviço nfs (udp) , logando
$fwcmd add deny log tcp from any to ${ip} 6000-6010
# bloqueia acesso ao X11 (tcp) , logando
$fwcmd add deny log udp from any to ${ip} 6000-6010
# bloqueia acesso ao X11 (udp) , logando
$fwcmd add deny log tcp from any to ${ip} 1999-2002
# bloqueia acesso ao Openwindows (tcp) , logando
$fwcmd add deny log udp from any to ${ip} 1999-2002
```

```
# bloqueia acesso ao Openwindows (udp) , logando
$fwcmd add deny log tcp from any to ${ip} 137-139
# bloqueia acesso ao serviço netbeui (udp) , logando
$fwcmd add deny log udp from any to ${ip} 137-139
# bloqueia acesso ao serviço netbeui (udp) , logando
$fwcmd add deny log tcp from any to ${ip} 31337,20034,1524,111,514,520,540,7777
setup
# bloqueia acesso as portas  31337,20034,1524,111,514,520,540,7777  (tcp) , logando
$fwcmd add deny log udp from any to ${ip} 31337,20034,1524,111,514,520,540,7777
# bloqueia acesso as portas  31337,20034,1524,111,514,520,540,7777  (udp) , logando

$fwcmd add deny log tcp from any to ${ip} 1-1023
# bloqueia acesso as portas  entre 1 e 1023 (tcp) , logando
$fwcmd add deny log udp from any to ${ip} 1-1023
# bloqueia acesso as portas  entre 1 e 1023 (udp) , logando

$fwcmd add pass tcp from any to any established
# permite trafego de conexões já estabelecidas
$fwcmd add pass tcp from any to ${ip}   1023-65535
# permite acesso as portas  entre 1023 e 65535 (tcp)
$fwcmd add  pass udp from any to ${ip} 1023-65535
# permite acesso as portas  entre 1023 e 65535 (tcp)
$fwcmd add deny log tcp from any to any
# bloqueia acesso proto tcp, logando
$fwcmd add deny log udp from any to any
# bloqueia acesso proto udp, logando
$fwcmd add deny icmp from any to any
# bloqueia acesso proto icmp, logando
```

- Rules NAT:

Script rc:

```
/usr/sbin/natd  -f /etc/natd.conf
```

Rules do nat:

```
log yes
#verbose
unregistered_only
use_sockets yes
interface ed1
redirect_address 10.0.0.0  x.y.z.22
```

```
# redirecionar a porta 22 para o server interno d rede
10/8
redirect_port tcp 10.0.0.3:22   x.y.z.w:22 0:0
port 6668
```

- Documentação sobre o ipfw:

  http://www.freebsd.org
  http://www.tomio.org/junior/index.htm
  http://www.free.bsd.com.br/
  http://www.freebsddiary.org
  http://www.freebsddesktop.cjb.net
  http://homepage.esoterica.pt/~jardim/Index.html
  http://www.freebsddiary.com/freebsd/ipfilter.htm#Rules

9 - Bibliografia:

Sites:

- Absoluta - "http://www.absoluta.org/seguranca/seguranca.htm"
- Aker firewall - "http://www.aker.com.br"
- Apache – "http://www.apache.org"
- Apostila - "http://apostilas.virtualave.net"
- Atrition - "http://www.attrition.org"
- BOS-BR - "http://www.sekure.org"
- Brasirc - "http://www.brasirc.net/seguranca/"
- BSD - "http://www.bsd.org"
- CERT-RS – "http://www.cert-rs.tche.br"
- CERT - "http://www.cert.org/"

- CIAC - "http://ciac.llnl.gov/ciac/"
- Conectiva - "http://www.conectiva.com.br"
- CEFET-RJ - "http://www.cefet-rj.br/Ensino/Engenharia/redeslocais/"
- CEFET-RJ - "http://www.cefet-rj.br/Ensino/Engenharia/redeslocais/default.htm"
- CEFET-RJ - "http://www.cefet-rj.br/Nucleo/Seminario/seminarios.htm"
- Defecon - "http://www.defcon.org"
- FreeBSD - "http://www.freebsd.org"
- Freshmeat - "http://www.freshmeat.net"
- Forbidden.net-security - "http://forbidden.net-security.org"
- ftp unicamp - "ftp://ftp.unicamp.br"
- GNU Project - "http://www.gnu.org"
- GTA UFRJ - "http://www.gta.ufrj.br"
- Hacker - "http://www.hacker.com.br"
- Hackers - "http://www.hackers.com.br"
- HackerNews - "http://www.hackernews.com.br"
- HackersNews - "http://www.hackersnews.com.br"
- IPF - "http://coombs.anu.edu.au/~avalon/ip-filter.html"
- ISS - "http://www.iss.net"
- LDP - "http://ldp.conectiva.com.br"
- Linux.com – "http://www.linux.com"
- Linux.org - "http://www.linux.org"
- Linux Security - "http://www.linuxsecurity.com.br"
- Linux Unicamp - "http://www.linux.unicamp.br"
- Linux Usp - "http://www.linux.usp.br"

- Modulo - “http://www.modulo.com.br”
- NetBSD - “http://www.netbsd.org”
- Net-Security - “http://www.net-security.org”
- NIC - “http://www.nic.br”
- Olinux - “http://www.olinux.com.br”
- OpenBSD – “http://www.openbsd.org”
- OpenSSL - “http://www.openssl.org”
- OpenWap - “http://www.openwap.org”
- Packetstorm - “http://packetstorm.securify.com/”
- Penta UFRGS - “http://www.penta.ufrgs.br”
- RedHat - “http://www.redhat.com”
- RNP – “http://www.rnp.br”
- RootSheel - “http://www.rootshell.com”
- Search Lycos - “http://ftpsearch.lycos.com/”
- SecureNet - “http://www.securenet.com.br”
- Security focus - “http://www.securityfocus.com”
- security.linuxtoday - “http://security.linuxtoday.com”
- Security Portal - “http://www.securityportal.com”
- Segurança NT - “http://www.segurancant.com/”
- SQUID CACHE – “http://squid.nlanr.net”
- SSL - “http://www.ssl.org”
- Sunsite - “ftp://sunsite.unc.edu/”
- Technotronic – “http://www.technotronic.com”

- Unicamp - “http://www.security.unicamp.br”
- Wap master - “http://www.wapmaster.com.br”
- Wapresources - “http://www.wap-resources.net”
- Wwsecurity - “http://www.wwsecurity.net”

Livros:

- Computer Networks; Andrew S. Tanenbaum, Prentice Hall PTR, 1996;
- Segurança na Internet; Marcus Gonçalves; Axcel Books, 1997;
- Comércio & segurança na Web; Simson Garfinkel; Market Books Brasil, 1999;
- Segurança na Internet; Terry Bernstein; Editora Campus, 1997;
- Firewalls Complete; Marcus Gonçalves; MacGraw-Hill, 1998.

How-to, Faqs e manuais:

- Ip-filter – http://coombs.anu.edu.au/~avalon/ip-filter.html;
- Implementações de soluções para segurança de redes; Leonardo G. de Mello;
- How-To Linux - “Firewalling and Proxy Server HOWTO”; Mark Grennan;

  http://okcforum.org/~markg/Firewall-HOWTO.html
  http://sunsite.unc.edu/mdw/linux.html

- How-To Linux – “Linux Security HOWTO”; Kevin Fenzi;

  ftp://sunsite.unc.edu/pub/Linux/docs/HOWTO

- OpenBSD Manual – http://www.openbsd.org ;

- Curso de segurança em redes linux; Renato Martini; Março de 2000;

  http://www.cipsga.org.br

Listas de discussão:

- BugTraq

  E-mail: BUGTRAQ@SECURITYFOCUS.COM
  Site: www.securityfocus.com

Revistas:

- PC Master; Ano3 número 7; Editora Europa, 1999;
- Security Magazine - "http://www.securitymagazine.com.br"
- Revista do Linux - "http:// www.revistadolinux.com.br"

10 - Glossário:

802.3
Padrão IEEE para ethernet.

ACK
Abreviatura para acknowledgement, confirmação.

Active X
Ambiente de Programação baseado em programação por objetos, arquitetura compatível com o Microsoft Windows, criado pela microsoft; objetivando criar mais agilidades e opções de novas aplicações mais pesadas.

ALG
gateway a nível de Aplicação.

Allow
Regra (ação) que permite uma ocorrência pré-determinada.

ANSI (American National Standards Institute)
Grupo que define padrões nos EUA.

ARP (Address Resolutions Protocol)
Vículo entre o endereço IP e o endereço de nível físico.

Apache
Servidor de HTTP desenvolvido pela "The Apache Software Foundation". Atualmente é o servidor de web mas usado na internet. Suportado por plataformas Linux, Unix, OS/2, Windows e etc....

Applet
Uma página da www pode fazer referência a um programa escrito em *Java*. Desta forma, o programa é trascrito junto com a página. Chama-se este programa de *"Applet"*.

Binário
Sistema numérico que utiliza a base 2.

Bit
A menor unidade dentro de uma posição de memória.

Browsers
São programas que possibilitam a visualizam de Home Pages.

BSD
Linha (sabor) de unix desenvolvido na universidade de Berkley da California EUA. Possui basicamente quatro distribuições: BSDI, FreeBSD, NetBSD e OpenBSD.

BUG
Expressão que caracteriza falha de programação em software ou em um sistema operacional.

C
Linguagem de programação muito utilizada no meio científico, usada para escrever 99% do código do UNIX, Linux e outros sistemas operacionais. Pode ser usada em computadores de pequeno porte ou em super computadores.

CGI (*Common Gaytway Interface)*
Programas que possibilitam real possibilidade de interagir com o usuário.

Chave privada
Chave mantida em sigilo no sistema de criptografia assimétrico.

Chave publica
Chave distribuida para o mundo.

checksum
Um valor calculado com a finalidade de testar a integridade dos dados.

chroot
Possibilita a alteração da raiz do sistema tendo como referencial um o software que foi startado pelo chroot.

Conectiva Linux
Empresa brasileira que distribui uma versão do linux baseada no linux Red Hat.

Compilador
Programa usado para traduzir uma informação em linguagem de máquina

Criptografia
Arte de codificar e decodificar mensagens.

Criptografia chave pública
Técnica de criptografia onde uma chave deve ser mantida em sigilo e a outra distribuida.

Criptografia assimétrica
Algorítmo onde chaves diferentes são utilizadas no processo de criptografia de descriptografia.

Criptografia simétrica
Algorítmo onde a mesma chave é utilizada no processo de criptografia de descriptografia.

Decimal
Sistema numérico que utiliza a base 10.

Deny
Regra (ação) que impede uma ocorrência pré-determinada.

DNS (Domain name system)
Base de dados que converte endereço ips em nomes ou endereços ips em nomes. Porta 53/udp. Também pode fornecer outras informações como: localização do servidor de e-mail, função dos servidores, sistema operacional dos servidores e outras informações.

DOS (denial of service)
Negação de serviços.

EAD
Vide ensino a distância.

Endereço IP
Endereço com 32 bits (IPV4) , este caracteriza um host na rede. Também é dividido em redes classe A, B, C, D e E.

Ensina a Distância
Utilização de recursos da internet para prover ensino, abramgendo desde o ensino fundamental até a pós-graduação.

Exploit
Programa utilizado por intrusos com a finalidade de explorar vulnerabilidades nos diversos sistemas, afim de obter privilégios de super usuário.

Filtro de pacotes
Equipamento que encaminham ou descartam pacotes em função de regras pré-definidas.

Filtro de pacotes Inteligente
Filtro de pacotes aprimorado, onde alguns problemas do filtro de pacotes são sanados.

Firewall
Equipamento usado para proteger uma rede, pode ser dividido basicamente em firewall de filtro de pacotes, NAT, proxy (gateway de aplicação) e gateway de circuito.

Forward de portas
Desvio transparente do pacote TCP/IP para um segundo host. Os parâmetros necessários são: porta de origem, host destino e porta destino.

FreeBSD
Sistema operacional baseado nos BSD de Berkley, voltado para as plataforma I386.

Freeware
Software distribuído com licença gratuita, apenas resguardando os direitos autorais.

FTP (File Transfer Protocol)
Protocolo para transferência de arquivos, porta 21/tcp.

Gateway
Equipamento responsável pelo roteamento de pacotes entre duas ou mais redes.

Gzip
Compactador muito usado no unix.

Gopher
Serviço precursor do WWW.

Gunzip
Descompactador muito usado no unix.

Handshake Sequence
Sequência de comunicação do protocolo(s) que caracteriza(m) estabelecimento da conexão entre cliente e servidor.

HOME PAGE
Um local na web que representa a presença de uma organização.

HOST
Qualquer computador, equipamento, de usuário final que conecta à rede.

How-To
Documento que descreve um procedimento para implementação de um serviço ou característica no Linux. Estes documentos podem também descrever uma teoria sobre o sistema operacional, uma teoria sobre rede de computadores ou relatos históricos.

HTTP (Hyper Text Transfer Protocol)
Protocolo da World Wide Web.

ICMP (Internet Control Message Protocol)
Integrante do protocolo IP e lida com mensagens de controle e erro.

IDS
Sistema de detcção de invasão.

IEEE 802.3
Vide 802.3 .

Internet
Conjunto de hosts, redes e roteadores que utiliza o protocolo TCP/IP unindo mais de 61 paises. Formando uma única rede.

INTERNIC
Organização que fornece informações sobre serviços e protocolos. Também é responsável pelo registro de IP e nomes na internet.

Inetd
Software que gerencia o processo inicializado por um servidor. Chamado de super servidor.

IP (Internet Protocol)
Protocolo usado para identificar os computadores com endereços ips de origem e destino.

IPV4
Versão atual do ip.

IPV6
Versão da nova versão do IP.

ISP
Internet Service Provider, Provedor de Serviço Internet.

JAVA
Linguagem de script que independe da plataforma. Esta é uma poderosa linguagem orientada a objeto criada pela SUN.

JAVA SCRIPT
É uma adaptação da *Java*, de forma a ser interpretada pelo Browser, sem necessidade de ser compilada pelo autor.

Kernel
O kernel é o núcleo essencial de um sistema operacional, o centro que provê os serviços básicos para todas as outras partes deste sistema operacional. Kernel é um termo usado com mais freqüência no Unix.

Linux
Sistema operacional baseado no minix desenvolvido por Linus Trovald no início da década de 90. Hoje este sistema operacional possui diversas distribuições pelo mundo.

LOG
Armazenamento de ocorrências para realização de auditorias.

Mapa Sensitivo
São figurar onde são definidas zonas através de coordenadas de forma a selecionar áreas que ao serem acionadas funcionam como links.

Mask
Máscara da rede.

NetBSD
Sistema operacional baseado nos BSD de Berkley, voltado aspectos de segurança e multiplataforma.

NAT
Network address Translation.

NEWS
É composto por informações agrupadas por categorias.

NFS (Network file system)
Possibilita a compartilhamento de file system entre duas ou mais maquinas UNIX/Linux. Porta 2049/tcp e udp.

OpenBSD
Sistema operacional baseado nos BSD de Berkley, voltado para aspectos de segurança. Possui grande suporte a criptografia, VPN e firewall. Considerado um dos sitemas mais seguros entre os sitemas free e pagos em ambiente standard.

Open Source
Software distribuído normalmente com licença gratuita e com o código aberto, normalmente sobre alguma licença como a GPL resguardando os direitos autorais.

OS/2
Sistema operacional desenvolvido pela IBM voltado para o mercado coorporativo e domético.

Pacote
Um conjunto de informações, dados e cabeçlhos, que são usados na transmissão de dados.

Perl
Linguagem interpletada voltada para o processamento de texto, muito utilizada em CGI's na WEB. Também facilita a depuração de logs do sistema.

Plugins
São módulos que podem ser conectados (instalados) ao browser, de forma que este passe a reconhecer os mais diversos formatos de informação. Diversas empresas criaram *Plugins*, permitindo assim ao browser visualizar gráficos vetoriais, vídeos, som, planilhas, *VRML*, *Flash* e outros.

Proto
Vide protocolo. Em um firewall este termo é usado para descrever a ocorrência de pacotes udp, tcp e icmp.

Protocolo
Descrição formal das regras que possibilitam a troca de informações entre os dispositivos de rede.

Provedores de Backbone Internet
São instituições que disponibilizam acesso a internet para redes locais.

Proxy
Um servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet.

Raiz
Em UNIX é a conta que detem o controle do sistema.

Red Hat
Distribuição do Linux.

RFC
Request for comments. Documento que descreve um protocolo internet. Podem ser informativas, históricas e de padronização.

rlogin
Protocolo de acesso remoto.

Root
Raiz do sistema. Conta que possui o controle sobre o sistema.

Rules
Regras de acesso em um firewall ou proxy.

Sendmail
Implementação mais comum do SMTP.

SMTP (Simple Mail Transport Protocolo)
Protocolo de transmissão de e-mails. Porta 25/tcp.

SSL (Secure Socks Layer)
Protocolo desenvolvido pela netscape que oferece serviço de segurança acima do protocolo tcp.

Standalone
Um servidor é startado, ou processo, sem auxílio de algum software "gerenciador" como o inetd.

SSH (Secure Shell)
Protocolo de acesso remoto que possui um canal encriptado. Possui as versões ssh1 e ssh2 estas versões de ssh utilizam algorítimo de encriptação RSA e DSA respectivamente. Porta 22/tcp.

SQUID
Software proxy cache para acessos a WEB.

Tar
Aglomerador de arquivos muito usado em UNIX/Linux.

TCP (Transmission Control Protocol)
Protocolo orientado a comunicação e atua na camada de transporte .

TELNET
Protocolo que possibilita a emulação de terminal entre duas maquinas. Porta 23/tcp.

UDP (User Datagram Protocol)
Protocolo não orientado a comunicação e atua na camada de transporte .

VPN (Virtual Private Netwaork)
Canal de comunicação encriptado gerado através de uma rede de ip pública não confiável.

Wais
Sistema de banco de dados de acesso remoto usado na internet.

Windows
Sistema operacional desenvolvido pela microsoft, possuidor de vários problemas de estabilidade e segurança. Mas, possui recursos que tornam o sistema amigável.

WWW (Word Wide Web)
Recurso de hipermídia para acessar a internet. Desenvolvido pelo CERN.