"Iptables: uma solução de baixo custo para implantação de firewalls"

Sumário

Introdução e Conceitos

Regras do Netfilter

Exemplos

Ferramentas

Introdução

- O que proteger? Quais os objetivos?
  - Dados que trafegam pela rede
    - Confidencialidade, integridade e disponibilidade
  - Os recursos ligados à rede
  - Sua reputação :-(

Conceitos

O que é um Firewall?

Mecanismo de rede capaz de classificar o tráfego em aceitável ou não-aceitável.

Dispositivo que toma decisões sobre o tráfego da rede.

Dispositivo usado para filtragem e NAT

Lógicamente: separa, restringe e analiza datagramas IP.

Fisicamente: hardware dedicado, roteador, computador ou uma combinação desses.

Filtragem de pacotes

(*Packet filtering*)

Controle seletivo do fluxo de dados de, e para uma rede.

Permite ou bloqueia pacotes.

Conjunto de “regras”

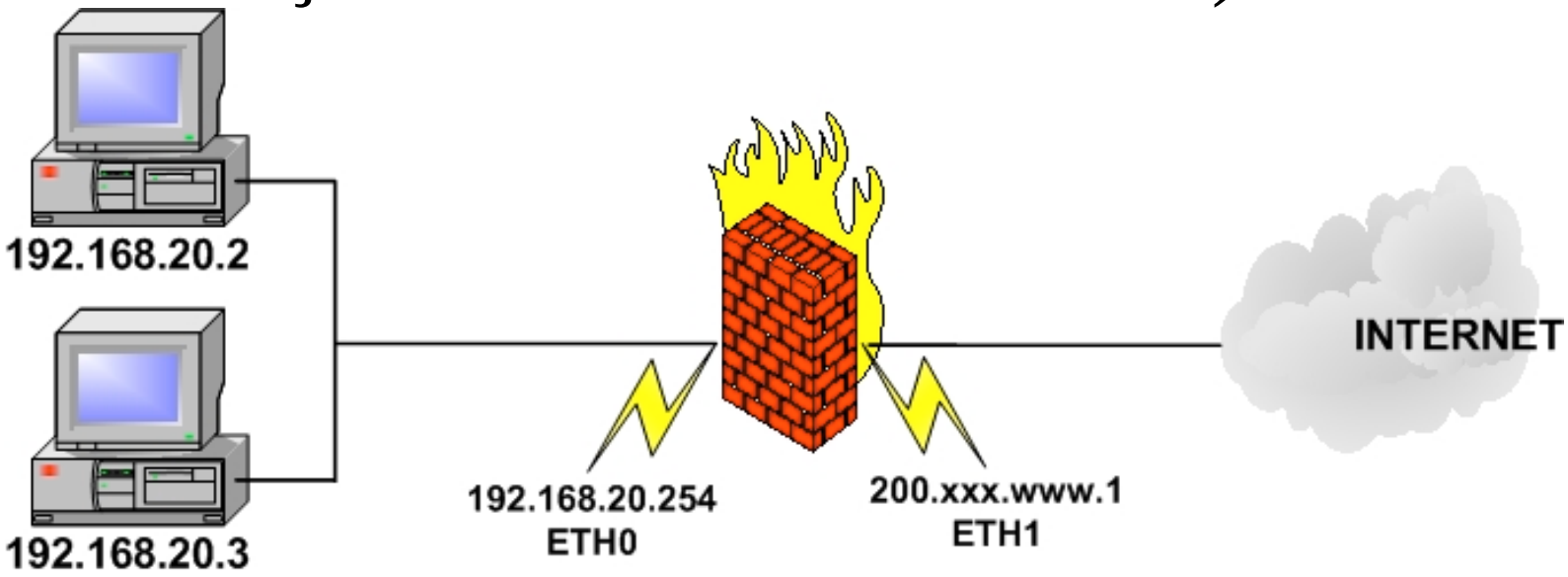
Baseada em:

- Endereços Ips;
- Protocolos (portas);
- Conteúdo

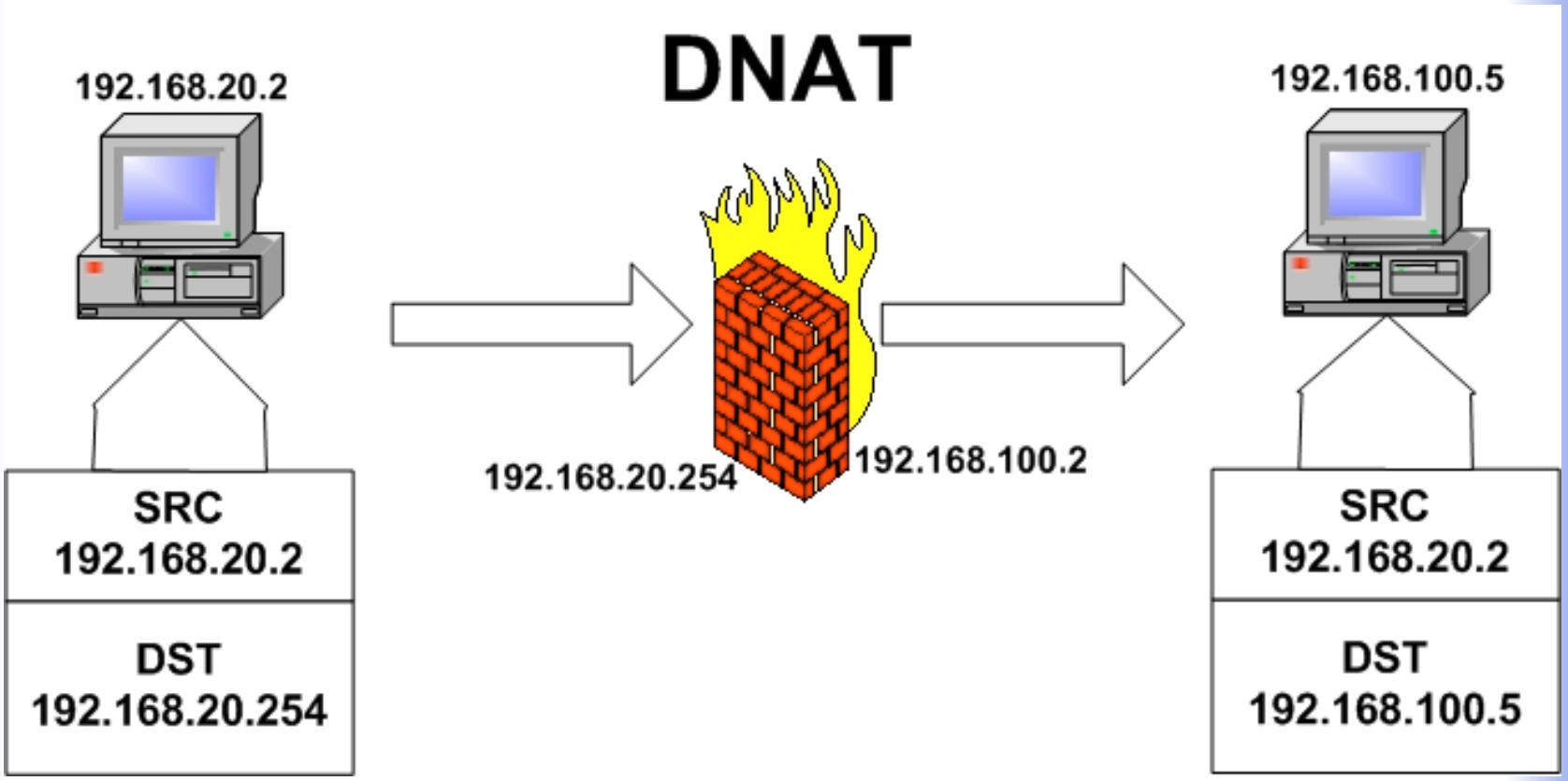
NAT (1/2)

Network Address Translation

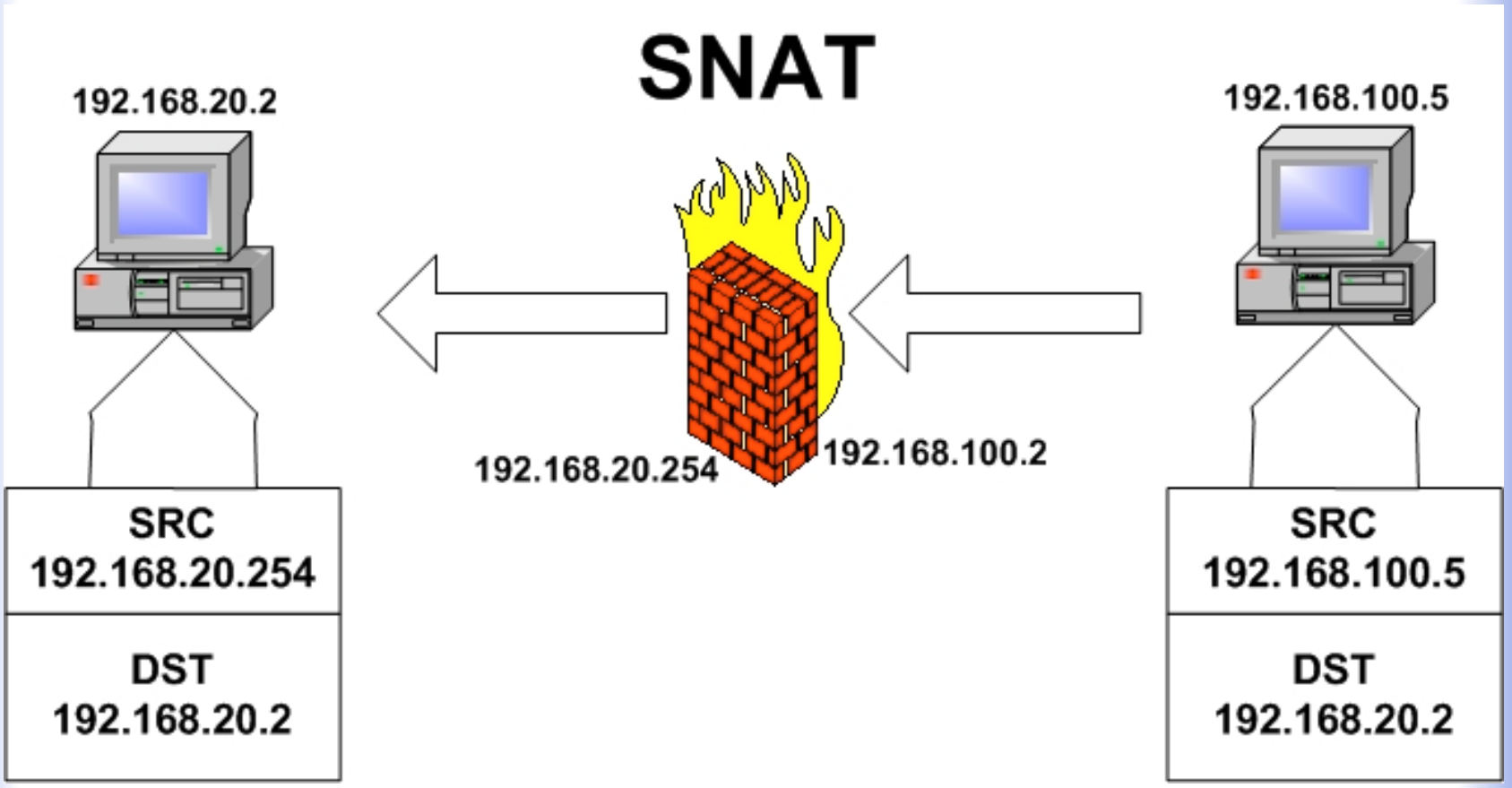
Mascaramento de endereços IPs (geralmente de endereços reservados ou inválidos).



NAT (2/4)


DNAT
192.168.20.2
192.168.100.5
192.168.20.254
192.168.100.2
SRC
192.168.20.2
DST
192.168.20.254
SRC
192.168.20.2
DST
192.168.100.5

NAT (3/4)


SNAT
192.168.20.2
192.168.100.5
192.168.20.254
192.168.100.2
SRC
192.168.20.254
DST
192.168.20.2
SRC
192.168.100.5
DST
192.168.20.2

NAT (4/4)

Masquerade

NAT (SNAT e DNAT) utilizado quando utiliza-se um IP dinâmico para o firewall.

DHCP, BOOTP, PPP, PPPoE...

Interconexão de Rede

- Gateway
  - Por onde sai o tráfego da rede interna
  - Interface entre as redes interna e externa
  - Roteamento
- Bridge
  - Interconecta duas redes, podendo estas utilizarem protocolos diferentes

Stateful

Stateful Firewalling – mantém o estado das conexões

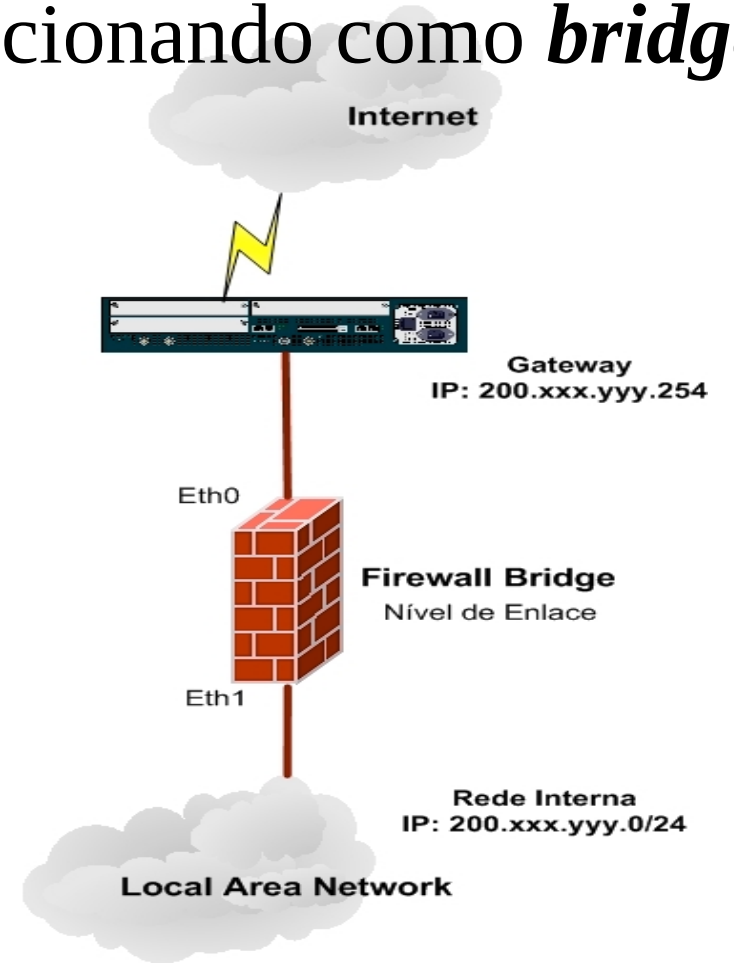
Máquinas de estados

Detecção e bloqueio de *stealth scans*

Ftp

Stealth Firewall

Firewall funcionando como ***bridge***



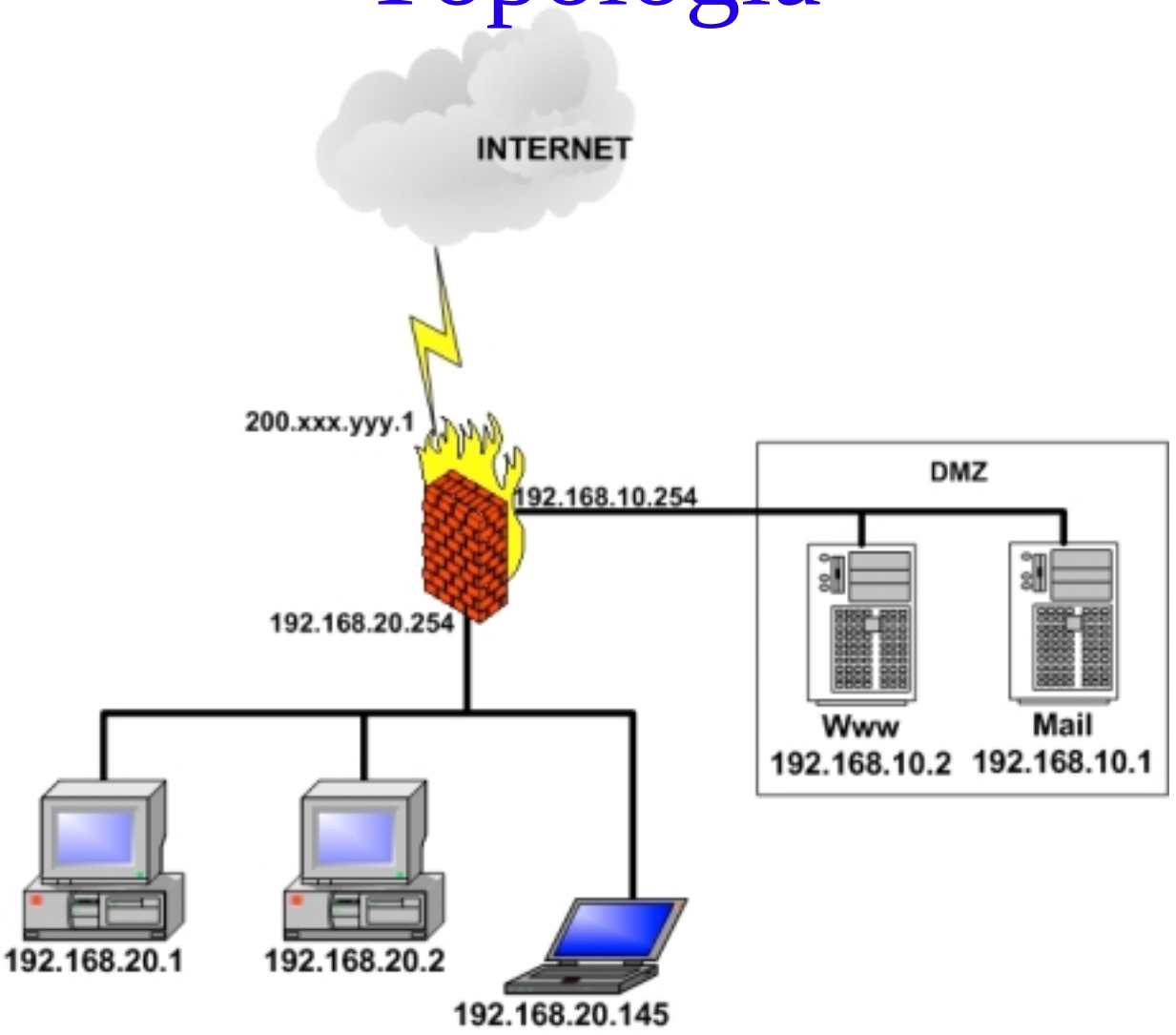
Conceitos Relevantes

Host **–** um computador ligado a uma rede;

Bastion host **–** um computador que deve possuir segurança maior (exemplo: servidores)

DMZ **–** Zona desmilitarizada – rede entre uma rede protegida e a rede externa, normalmente composta por *bastion hosts*

Topologia


INTERNET
200.xxx.yyy.1
192.168.10.254
DMZ
192.168.20.254
Www
192.168.10.2
Mail
192.168.10.1
192.168.20.1
192.168.20.2
192.168.20.145

Cuidados Básicos

Spoofing – falsificação de endereços (IP, MAC, DNS)

Scan – prospecção ou varredura

Stealth scan – prospecção que utiliza combinação de *flags* do TCP (XMAS, NULL, SYN+FIN)

DoS – negativa de serviço – limitação do número de conexões de um *host*.

Comparações

- Firewalls comerciais
  - Cisco PIX, Checkpoint FW-1, SonicWall, Alker
- Firewalls Livres
  - Ipfilter
  - Ipfwadm
  - Ipchains
  - Packet Filter
  - **Netfilter**

Ipfilter

É um filtro de pacotes baseado muito potente e versátil.

Permite fazer *transparent proxying*.

Possibilita fazer *round-robim forward* (balanceamento de carga)

SO: FreeBSD

Ipfwadm

Antigo firewall dos sistemas Linux.

Não possui controle de estado da conexão.

Linux kernel 2.0

Ipchains

Firewall que pode ser integrado ao kernel do linux.

Filtragem de pacotes, masquerading e roteamento

Não possui controle de estado de conexões

Linux kernel 2.2

Packet Filter

É um filtro de pacotes baseado muito potente e versátil.

Stateful Firewall

Regras de fácil entendimento

SO: OpenBSD

Iptables Netfilter (1/5)

Primeiro sistema *stateful firewall* no linux

NAT

Consegue fazer matches em diferentes camadas.

Linux kernel 2.4

Iptables Netfilter (2/5)

Porque escolhemos o Netfilter?

- Ambiente Universitário
- Software Free!!!
- Estável
- Leve
- Controle de estado de conexão
- Linux

Iptables Netfilter (3/5)

Como Instalar

Adicionar os *patches* do Iptables ao Kernel

- patch-o-matic-versão.tar.bz2
  - Descompacte o arquivo entre no diretório

    KERNEL_DIR=<<where-you-built-your-kernel>> ./runme pending

    KERNEL_DIR=<<where-you-built-your-kernel>> ./runme base

    KERNEL_DIR=<<where-you-built-your-kernel>> ./runme extra

Obs.: Responda as questões dos scripts cuidadosamente, pois determinados patches sobrescrevem ou são incompatíveis com outros patches.

Compilar o Kernel

Iptables Netfilter (4/5)

- Compilando o Kernel
  - Comandos:
    - make menuconfig (modo texto) ou
    - make xconfig (modo gráfico)
  - Escolher as opções do kernel compatíveis com a necessidade do sistema.

Iptables Netfilter (5/5)

Salvar e iniciar a compilação

Comandos:

make dep; make clean; make bzImage

make modules; make modules_install; make install

Nem sempre isso dá certo :-) mas não desista!

Entendendo Patches (1/5)

Aplicar os patches ao kernel:

"Alguns" patches disponíveis - Adicionam funções:

ah-esp patch: Adiciona capacidade de reconhecer características do IPSEC.

condition match: Possibilita habilitar ou desabilitar uma regra baseado em um arquivo armazenado no diretório "/proc/net/ipt_condition/".

Entendendo Patches (2/5)

Contrack patch: Possibilita identificar informações adicionais relacionadas a tabela de conexões. Possibilita identificar como SNAT e DNAT.

fuzzy patch: Adiciona um FLC (Fuzzy Logic Controler) simples.

iplimit patch: Limita/aceita determinado número de conexões paralelas.

Ipv4options patch: Habilita identificações baseadas nas opções do protocolo IP.

Entendendo Patches (3/5)

length patch: Com este patch pode-se aceitar ou rejeitar um pacote, baseando-se no seu tamanho.

mport patch: Permite mesclar conjunto de (ou seqüencias de) portas.

nth patch: Habilita regras que serão acionadas a cada n pacotes.

pkttype patch: Identifica pacotes baseados nos tipos: host, broadcast, multcast.

Entendendo Patches (4/5)

psd patch: Possibilita identificar port scans.

quota patch: Permite limitar quotas (Mbytes que passaram pela regra).

random patch: Este patch permite selecionar um pacote aleatoriamente.

recent patch: Permite estabelecer e filtrar uma lista de endereços IPs.

record-rpc patch: Verifica conexões de rpc.

Entendendo Patches (5/5)

string patch: Permite procurar por uma string qualquer em um pacote.

time patch: Identifica pacotes baseados no seu timestamp.

ttl patch: Faz filtragem baseada no TTL do pacote.

Entendendo os Módulos (1/6)

CONFIG_PACKET: Permite aplicações (tcpdump, snort) trabalharem com dispositivos de rede.

CONFIG_NETFILTER: Habilita o Netfilter.

Entendendo os Módulos (2/)

CONFIG_IP_NF_CONNTRACk: Módulo responsável pela tabela de conexões. NAT, Masquerading, estado de uma conexão.

CONFIG_IP_NF_FTP: É necessário para controlar conexões FTP.

Entendendo os Módulos (2/6)

CONFIG_IP_NF_IPTABLES: Adiciona o suporte ao Iptables ao kernel. É preciso para as ações de filtragem e NAT.

CONFIG_IP_NF_MATCH_LIMIT: Possibilita um controle de quantos pacotes por determinado intervalo de tempo são aceitos/negados.

Entendendo os Módulos (3/)

CONFIG_IP_NF_MATCH_MAC: Identifica pacotes baseados em seu endereço MAC.

CONFIG_IP_NF_MATCH_MULTIPORT: Possibilita elaborar regras que utilizem um intervalo (range) de portas, tanto de origem quanto de destino.

Entendendo os Módulos (3/6)

CONFIG_IP_NF_MATCH_TOS: Possibilita identificar pacotes baseado em seu campo TOS (Type Of Service).

CONFIG_IP_NF_MATCH_TCPMSS: Adiciona suporte à identificação de pacotes TCP baseados no campo MSS. -

Entendendo os Módulos (4/)

CONFIG_IP_NF_MATCH_STATE: Este módulo permite que sejam feitos filtros baseados no estado das coneções. Esse é uma das mais importantes funcionalidades do Iptables/Netfilter.

CONFIG_IP_NF_MATCH_UNCLEAN: - Experimental - Identifica pacotes inválidos, ou que não foram "entendidos".

Entendendo os Módulos (4/6)

CONFIG_IP_NF_MATCH_OWNER: - Experimental - Faz idenficação de pacotes baseados no "dono" (Ex.: root) do socket.

Processos locais!

CONFIG_IP_NF_FILTER - Adiciona ao kernel, a tabela de filter. Isso irá habilitar a filtragem de pacotes Ips.

Entendendo os Módulos (5/)

CONFIG_IP_NF_TARGET_REJECT: Permite especificar uma mensagem de erro ICMP que será enviado quando uma conexão necessitar ser cancelada.

CONFIG_IP_NF_TARGET_MIRROR: Permite que pacotes sejam enviados de volta à sua origem.

Entendendo os Módulos (5/6)

CONFIG_IP_NF_NAT: Este módulo habilita network address translation - NAT (SNAT e DNAT). Adicina ao kernel a tabela nat. (Port forwarding).

CONFIG_IP_NF_TARGET_MASQUERADE: Adiciona a opção Masquerade. Utilizado com IP dinâmico. DHCP, PPP, SLIP, PPPoE, etc.

Entendendo os Módulos (6/)

CONFIG_IP_NF_TARGET_REDIRECT: Possibilita fazer um proxy transparente. Ele redireciona o pacote.

CONFIG_IP_NF_TARGET_LOG: Adicina a funcionalidade de gerar logs ao iptables. Integração com o syslog.

Entendendo os Módulos (6/6)

CONFIG_IP_NF_TARGET_TCPMSS: Utilizado contra ISP (Internet Service Providers) que bloqueiam pacotes do tipo ICMP Fragmentation Needed. (Ver isso um pouco melhor)

CONFIG_IP_NF_COMPAT_IPCHAINS: Adiciona ao Netfilter compatibilidade com o ipchains. Cuidado!

CONFIG_IP_NF_COMPAT_IPFWADM: Adiciona ao Netfilter compatibilidade com o ipfwadm. Cuidado!

Tabela de conexão (1/)

(*Conection Tracking*)

Mantém em memória uma tabela com as conexões ativas.

IP origem e destino, portas origem e destino, protocolo, estado da conexão, timeout

Stateful firewall

Tabela de conexão (2/)

(*Conection Tracking*)

O controle de conexão é feito nas chains PREROUTING e OUTPUT (pacotes gerados pelo firewall).

Desfragmenta todos os pacotes.

/proc/net/ip_conntrack

Tabela de conexão (2/)

(*Conection Tracking*)

```
# cat /proc/net/ip_conntrack

 tcp      6 431989 ESTABLISHED src=192.168.20.145
dst=192.168.10.5 sport=32768 dport=22 src=192.168.10.5
dst=192.168.20.145 sport=22 dport=32768 [ASSURED] use=1

 udp      17 140 src=192.168.20.145 dst=192.168.10.1 sport=32768
dport=53 src=192.168.10.1 dst=192.168.20.145 sport=53
dport=32768 [ASSURED] use=1
```

Tabela de conexão (4/)

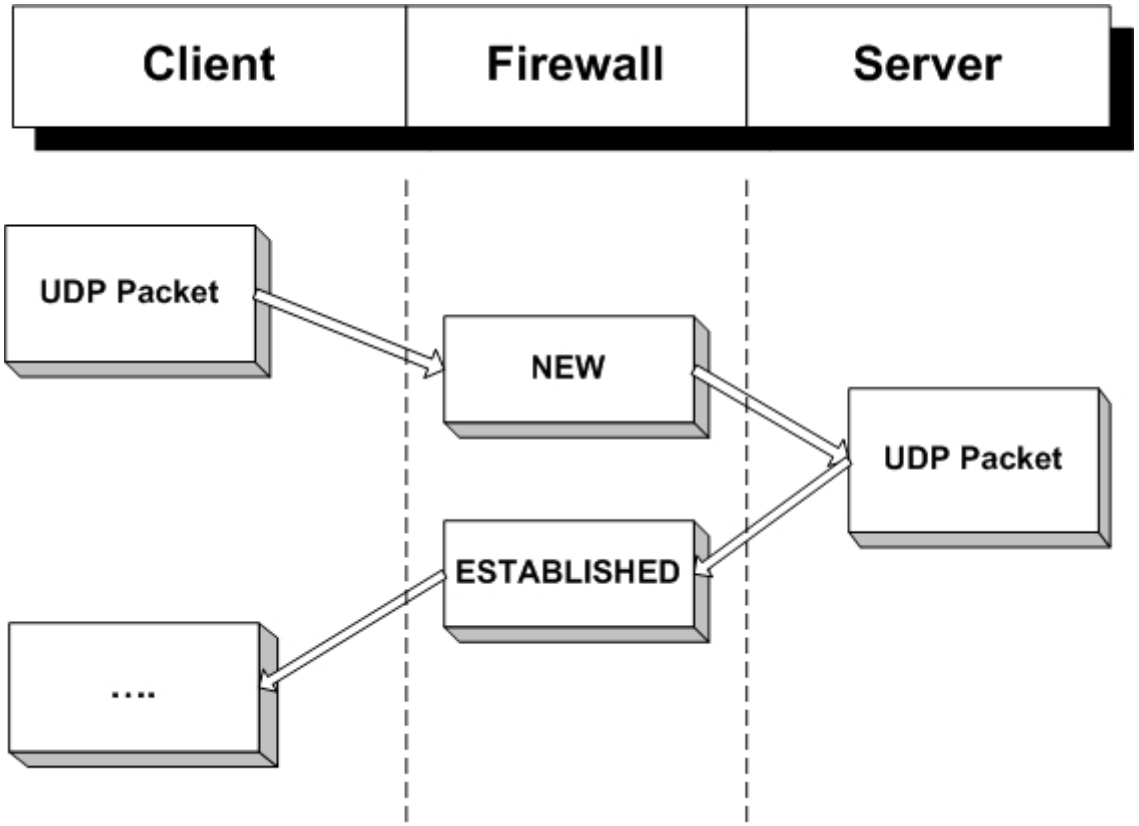
(*Conection Tracking*)

TIMEOUT

- SYN Sent - 2 minutos
- ESTABLISHED - 5 dias

NEW, ESTABLISHED, RELATED e INVALID

UDP (1/3)


Client
Firewall
Server
UDP Packet
NEW
UDP Packet
ESTABLISHED
....

UDP (2/3)

O controle é baseado em request/replie.

udp 17 19 src=AAA.AAA.AAA.AAA dst=BBB.BBB.BBB.BBB sport=CC dport=DD [UNREPLIED] src=BBB.BBB.BBB.BBB dst=AAA.AAA.AAA.AAA sport=DD dport=CC use=1

17: protocolo UDP

19: timeout restante

UDP (3/3)

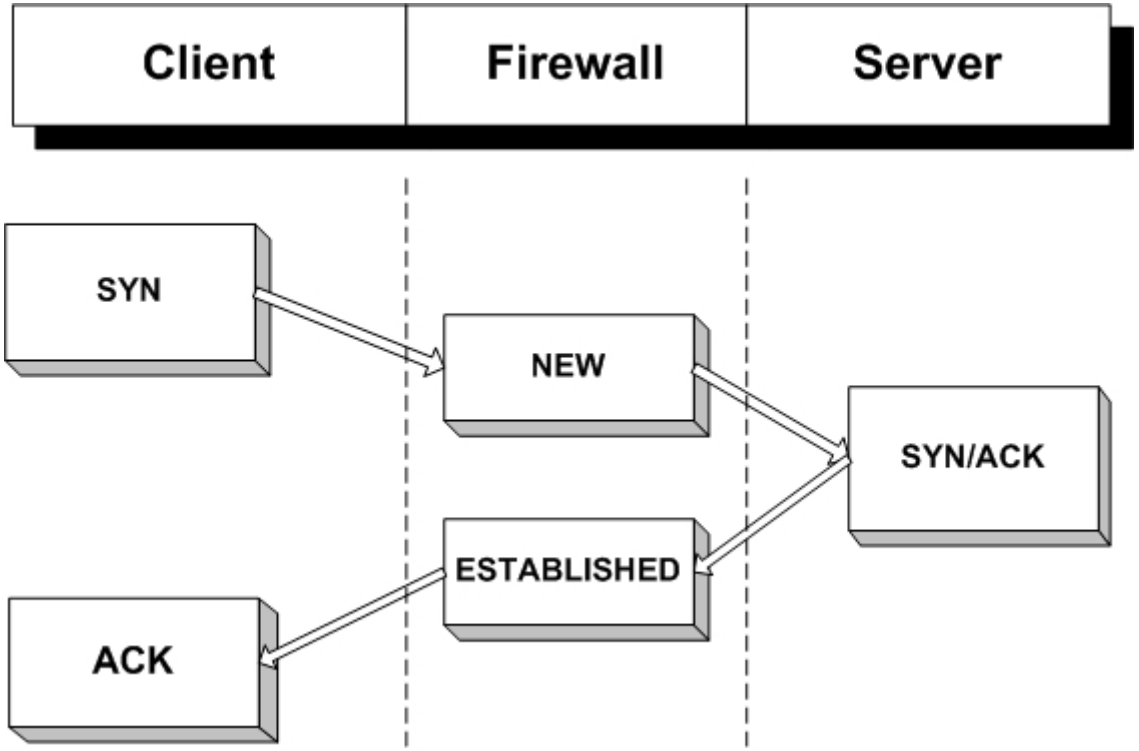
TIMEOUT = 30 segundos

UDP Stream - multiplas requisições/repostas ocorridas entre o mesmo "socket pairs"

TIMEOUT - 180 segundos

TCP (1/2)

O controle é baseado no handshake de três vias.



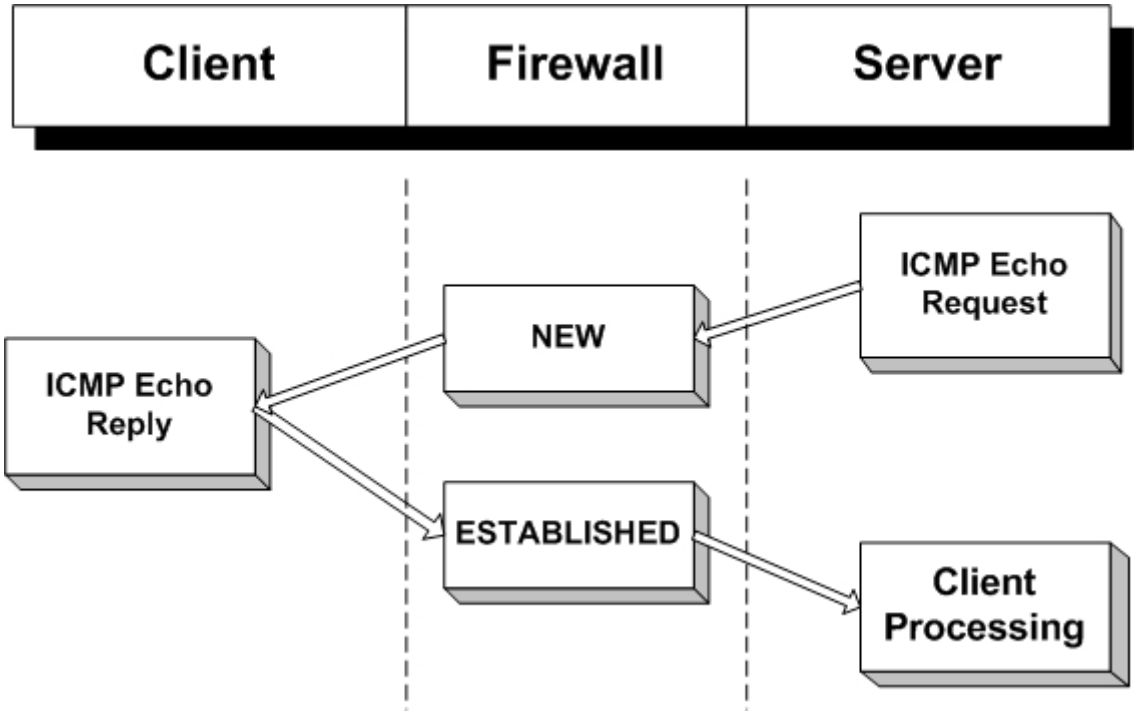
TCP (2/2)

Importante: O estado NEW não quer dizer que foi um pacote com SYN.

SYN+ACK -> ESTABLISHED. Não é igual ao TCP.

```
tcp      6 431989 ESTABLISHED src=192.168.20.145
dst=192.168.10.5 sport=32768 dport=22 src=192.168.10.5
dst=192.168.20.145 sport=22 dport=32768 [ASSURED] use=1
```

ICMP (1/2)


Client
Firewall
Server
ICMP Echo Request
NEW
ICMP Echo Reply
ESTABLISHED
Client Processing

ICMP (2/2)

NEW/ESTABLISHED

- Echo request(8) -> Echo reply(0)
- Timestamp request(13) -> Timestamp reply(14)
- Information request(15) -> Information reply(16)
- Address mask request(17) -> Address mask reply(18)
- Outros tipos de ICMP -> RELATED

Problema da ip_conntrack (1/2)

Protocolos que utilzam mais de uma conexão.

Conexão FTP

FTP Passivo - Dados e comandos são enviados pela porta 21.

FTP Ativo - Problema! Comandos são enviados pela porta TCP 21. Dados são enviados pela porta TCP 20 do servidor.

É estabelecida uma conexão do servidor para o cliente.

14:53:04.626786 CLIENTE.32946 > SERVIDOR.21: S 4191272088:4191272088(0) win 5840 <mss 1460,sackOK,timestamp 8288590 0,nop,wscale 0> (DF)

14:53:04.652930 SERVIDOR.21 > CLIENTE.32946: S 1238074047:1238074047(0) ack 4191272089 win 57344 <mss 1460,nop,wscale 0,nop,nop,timestamp 76112648 8288590> (DF)

14:53:04.653061 CLIENTE.32946 > SERVIDOR.21: . ack 1 win 5840 <nop,nop,timestamp 8288603 76112648> (DF)

14:53:04.691791 SERVIDOR.21 > CLIENTE.32946: P 1:28(27) ack 1 win 57920 <nop,nop,timestamp 76112652 8288603> (DF)

14:53:04.691893 CLIENTE.32946 > SERVIDOR.21: . ack 28 win 5840 <nop,nop,timestamp 8288623 76112652> (DF)

...

14:53:06.563236 SERVIDOR.20 > CLIENTE.32947: S 83185498:83185498(0) win 57344 <mss 1460,nop,wscale 0,nop,nop,timestamp 76112839 0> (DF)

14:53:06.563347 CLIENTE.32947 > SERVIDOR.20: S 4196113913:4196113913(0) ack 83185499 win 5792 <mss 1460,nop,nop,timestamp 8289581 76112839,nop,wscale 0> (DF)

Problema da ip_conntrack (2/2)

Solução: ip_conntrack_ftp

No ftp ativo, a conexão com a porta 21 do servidor será considerada RELATED.

CHAINS (1/3)

São os possíveis repositórios dentro do kernel, onde regras que atuam em uma direção "semelhante" sao aplicadas/checadas.

INPUT: Pacotes roteados para o firewall (destino é o firewall).

OUTPUT: Pacotes gerados localmente pelo firewall.

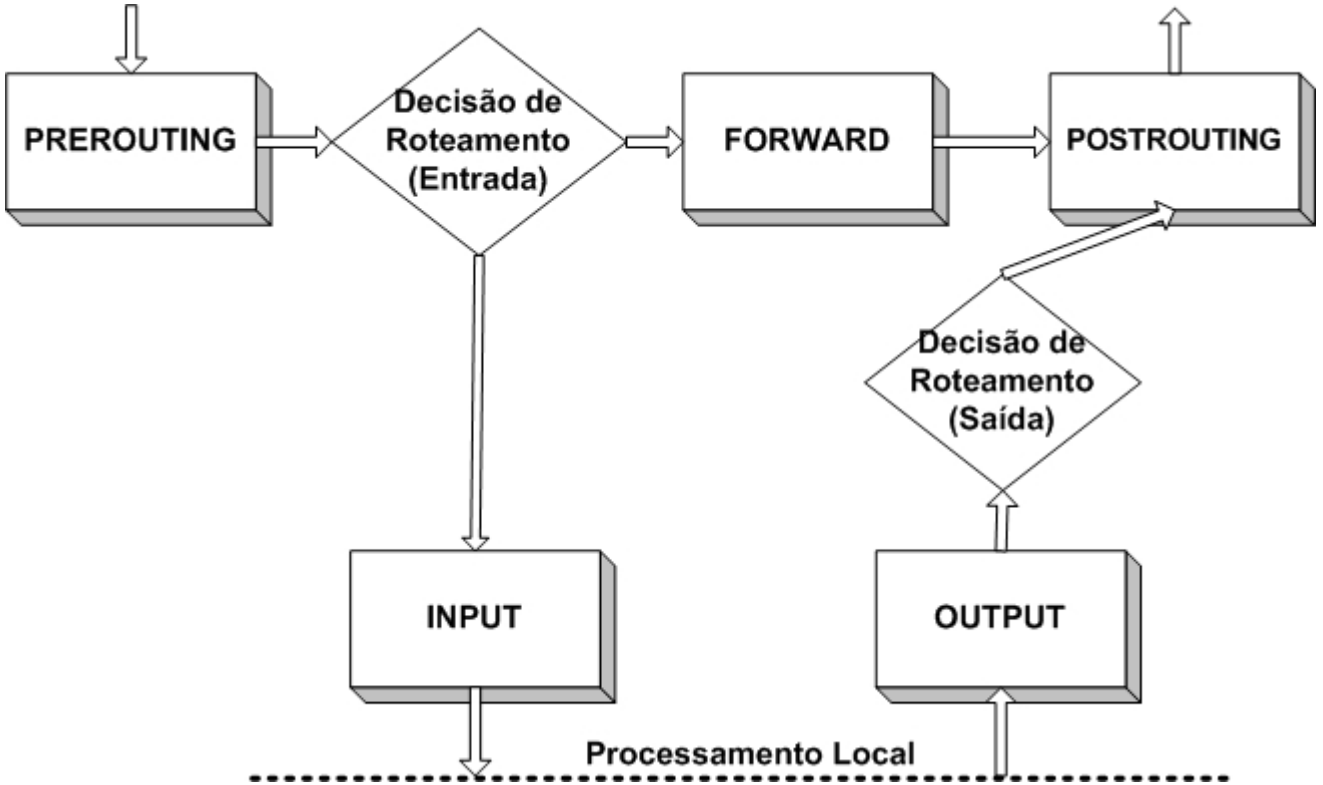
CHAINS (2/3)

PREROUTING: Pacote entrando pelo firewall (antes da decisão de roteamento)

FORWARD: Passam os pacotes que não tem nem origem nem destino no firewall.

POSTROUTING: Saída dos pacotes. Depois de todas as decisões de roteamento.

CHAINS (3/3)


PREROUTING
Decisão de Roteamento (Entrada)
FORWARD
POSTROUTING
Decisão de Roteamento (Saída)
INPUT
OUTPUT
Processamento Local

Tabelas (1/5)

(*Tables*)

Tables: tabelas que agrupam chains com decisões da mesma natureza.

- FILTER: Única e exclusiva para chains que aceitam ou rejeitam pacotes.
- NAT: Controle do mascaramento de endereços IPs.
- MANGLE: Alteracoes "low-level" (modificar TTL, TOS, ...)

Tabelas (2/5)

(*Tables*)

Tabela mangle

- TOS - Type Of Service
- TTL - Time to Live
- MARK – reconhecidos pelo iproute2

Tabelas (3/5)

(*Tables*)

Tabela nat

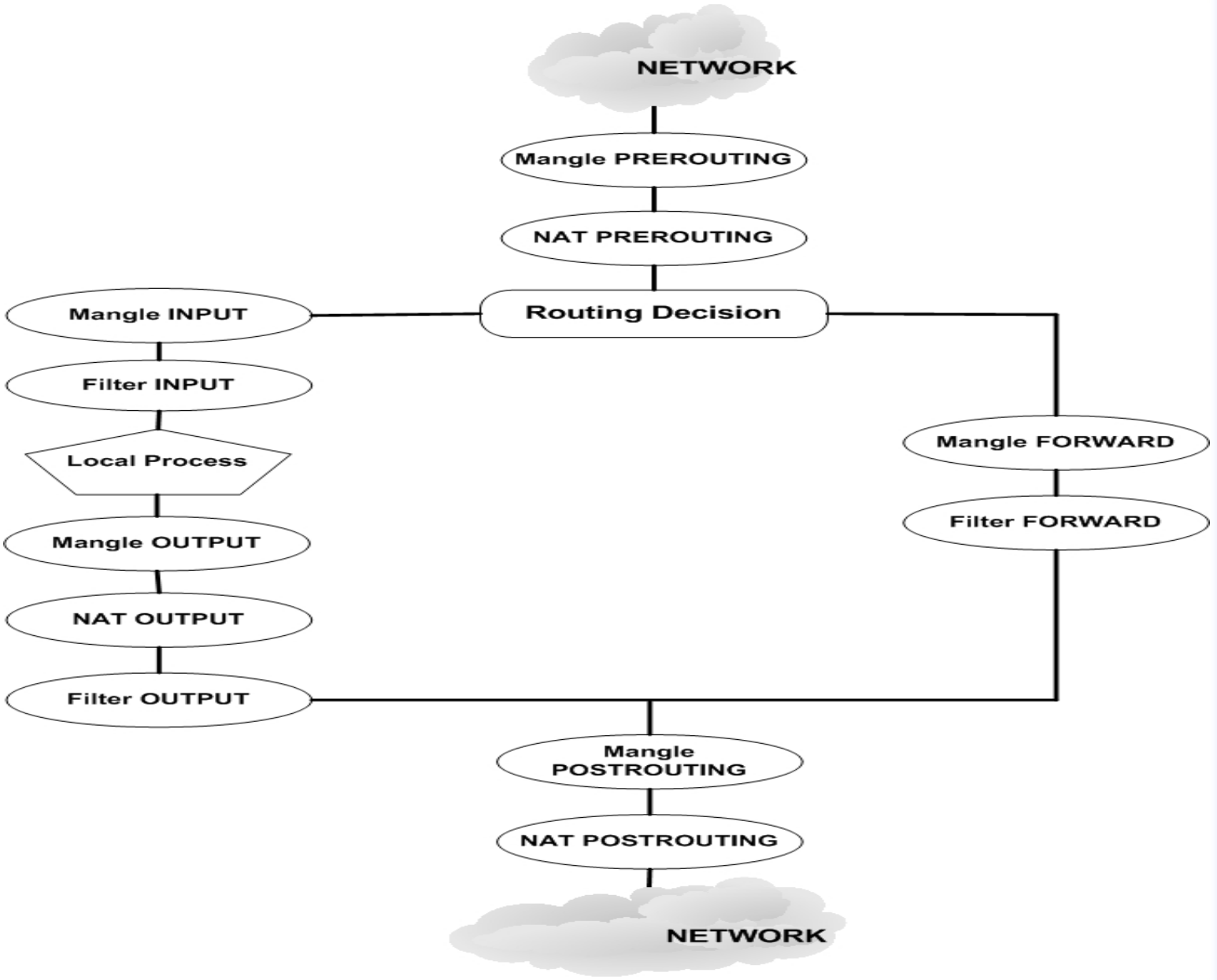
- DNAT
- SNAT
- MASQUERADE

Tabelas (4/5)

(*Tables*)

Tabela filter (Default)

- DROP
- ACCEPT
- LOG
- REJECT


NETWORK
Mangle PREROUTING
NAT PREROUTING
Routing Decision
Mangle INPUT
Filter INPUT
Local Process
Mangle OUTPUT
NAT OUTPUT
Filter OUTPUT
Mangle FORWARD
Filter FORWARD
Mangle POSTROUTING
NAT POSTROUTING
NETWORK

Comandos (1/11)

-A, --apend

Iptables -A INPUT

Insere uma regra no final da chain

Comandos (2/11)

-D, --delete

iptables -D INPUT --dport 80 -j ACCEPT

iptables -D INPUT 1 -> número da regra

Apaga um regra de uma chain.

Comandos (3/11)

-R, --replace

iptables -R INPUT 1 -s 192.168.30.1 -j DROP

Troca o conteúdo de uma regra.

Comandos (4/11)

-I, --insert

iptables -I INPUT 1 --dport 80 -j ACCEPT

Insere uma regra no número especificado.

Comandos (5/11)

-L, --list

iptables -L INPUT

Lista as regras de um chain.

Comandos (6/11)

-F, --flush

iptables -F INPUT

Apaga todas as regras de uma chain.

Comandos (7/11)

-Z, --zero

iptables -Z INPUT

Zera o contador de ocorrência de uma regra.

Comandos (8/11)

-N, --new-chain

iptables -N TESTE

Cria uma nova chain.

Comandos (9/11)

-X, --delete-chain

iptables -X TESTE

Apaga um chain.

Comandos (10/11)

-P, --policy

iptables -P INPUT DROP

Coloca uma regra default em uma chain (política).

Comandos (11/11)

-E, --rename-chain

iptables - E TESTE teste

Troca o nome de uma chain.

OPÇÕES (1 /2)

-v, --verbose

Coloca o comando em modo prolixo, ou seja, mostra na tela informações mais detalhadas.

-x, --exact

Expande a representação de números. Não apresenta os prefixos K, M ou G.

OPÇÕES (2/2)

-n, --numeric

Apresenta os endereços IPs e portas em valores numéricos. Não apresenta host-names ou nome de serviços.

--line-numbers

Mostra o número da linha (regra).

MATCHES (1/)

-p, --protocol

Iptables -A INPUT -p tcp

Seleciona protocolos (Ex. TCP, UDP, ICMP).

/etc/protocols

MATCHES (2/)

-s, --src, --source

Iptables -A INPUT -s 192.168.20.254

Identifica pacotes baseados no seu endereço IP de origem. Opcionalmente, pode-se colocar a máscara do endereço (/24, /32, /255.255.255.0).

MATCHES (3/)

-d, --dst, --destination

Iptables -A INPUT -d 192.168.20.254

Identifica pacotes baseados no seu endereço IP de destino. Opcionalmente, pode-se colocar a máscara do endereço (/24, /32, /255.255.255.0).

MATCHES (4/)

-i, --in-interface

Iptables -A INPUT -i eth0

Seleciona a interface por onde o pacote é recebido. Deve ser utilizada nas chains INPUT, FORWARD e PREROUTING

MATCHES (5/)

-o, --out-interface

Iptables -A OUTPUT -o eth0

Seleciona a interface por onde o pacote será enviado. Deve ser utilizada nas chains OUTPUT, FORWARD e POSTROUTING

MATCHES

CONDITION

iptables -A FORWARD -p tcp -d 192.168.30.1 --dport 80 -m condition acesso_web -J ACCEPT

Esta regra é habilitada se o conteúdo do arquivo "/proc/net/ipt_condition/accesso_web" for "1".

Os arquivos devem sempre estar no diretório "/proc/net/ipt_condition/"

MATCHES

CONTRACK

iptables -A FORWARD -m conntrack --ctstate SNAT --ctproto tcp -j ACCEPT

São adicionados os estados SNAT e DNAT. Além disso podem ser utilizados as seguintes opções:

--ctproto protocolo - protocolo

--ctorigsrc endereço - endereço de origem original

MATCHES

--ctorigdst endereço - endereço de destino original

--ctreplsrc endereço - endereço de origem de resposta

--ctrepldst endereço - endereço de destino de resposta

MATCHES

FUZZY

Iptables -A INPUT -m fuzzy --lower-limit 100 --upper-limit 1000 -j REJECT

Quando a taxa de pacotes está abaixo do limite inferior, a regra nunca é habilitada.

Quando está entre o limite inferior e superior, a regra é habilitada com probabilidade proporcionalmente.

Continua

MATCHES

Quando está acima do limete superior, a regra é habilitada com uma probabilidadede 99%.

Medidas em pacotes por segundo.

MATCHES

IPLIMIT

iptables -A INPUT -p tcp --syn --dport 80 -m iplimit --limit-above 10 -j REJECT

Limita o número de conexões paralelas originadas em determinado host. Também pode ser utilizada a opção --iplimit-mask [n] para utilizar máscara de rede.

MATCHES

LENGTH

iptables -A INPUT -p icmp --icmp-type echo-request -m length --length 86:0xffff -j DROP

Identifica pacotes baseados no tamanho do pacote. Esse tamanha é especicado por um intervalo de valores.

MATCHES

MPORT

iptables -A INPUT -p tcp -mport --ports 20:50,70:90 -j DROP

Permite especificar regras com um conjunto de (intervalos de) portas. Ainda são suportadas as opções:

--source-ports portas

Continua

MATCHES

--sport portas

--destination-ports portas

--dports portas

MATCHES

NTH

iptables -A INPUT -p icmp --icmp-type echo-request -m nth --every 2 -j DROP

A regra é habilitada a cada n pacotes. Ainda são suportadas as opções:

--start número - Inicializa o contador de pacotes.

Continua

MATCHES

--counter número (entre 0 e 15) - Define qual contador utilizar.

--packet número - Define qual pacote identificar.

MATCHES

Balanceamento de carga entre 2 hosts:

iptables -t nat -A POSTROUTING -o eth0 -m nth --counter 1 --every 2 --packet 0 -j SNAT --to-destination 192.168.10.1

iptables -t nat -A POSTROUTING -o eth0 -m nth --counter 1 --every 2 --packet 1 -j SNAT --to-destination 192.168.10.2

Metade dos pacotes vai para 192.168.10.1 e metade vai para 192.168.10.2

MATCHES

PKTTYPE

iptables -A INPUT -m pkttyep -pkt-type broadcast -j DROP

Identifica pacotes baseados no tipo de destino do endereço IP. Esse tipo pode ser: broadcast, multcast ou host.

MATCHES

PSD

iptables -A INPUT -m psd -j DROP

Identifica portscans. Podem ainda ser utilizadas as seguintes opções:

--psd-weigth-threshould

--psd-delay-threshould

--psd-lo-ports-weight lo

--psd-hi-ports-weight hi

MATCHES

QUOTA

iptables -A INPUT -p tcp --dport 80 -m quota --quota 52428800 -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -j DROP

Faz regras baseadas em uma quota. Nesse exemplo, apenas os primeiros 50Mb seríam aceitos.

MATCHES

RANDOM

iptables -A INPUT -p icmp --icmp-type echo-request -m random --average 50 -j DROP

A regra é "ativada" com uma probabilidade estipulada.

MATCHES

RECENT

iptables -A FORWARD -m recent --name black_list --rcheck --seconds 60 -j DROP

iptables -A FORWARD -p tcp -i eth0 --dport 139 -m recent --name black_list --set -j DROP

Continua

MATCHES

Identifica pacotes baseados em uma lista de endereços IP de origem. São suportadas as seguintes opções:

--name nome_da_lista - marca o nome da lista.

--set - envia o endereço IP de origem do pacote para a lista.

--recheck - verifica se o endereço IP de origem do pacote está na lista.

Continua

MATCHES

--update - semelhante ao recheck, mas faz um update na lista.

--remove - remove um endereço IP de uma lista.

--seconds segundos - estabelece um limite de tempo para o endereço estar na lista. Deve ser utilizada junto com recheck ou update.

Continua

MATCHES

--hitcount número - estabelece um limite mínimo de pacotes que devem "casar" com a regra (IP) antes que essa comece a ser utilizada.

--rttl - compara os TTLs dos pacotes que foram para a regra.

MATCHES

STRING

iptables -A INPUT-m string --string 'cmd.exe' -j DROP

Faz filtragem baseada no conteúdo dos pacotes.

Cuidado! Esse tipo de match pode causar uma degradação na performance do firewall.

MATCHES

TIME

iptables -A INPUT -m time --timestart 8:00 --timestop 18:00 --days Mon,Tue,Wed,Thu,Fri -j ACCEPT

Continua

MATCHES

Essa regra permite fazer filtragem baseada no tempo de chegada (local) dos pacotes. Estão disponíveis as seguintes opções:

--timestart

--timestop

--days - Mon,Tue,Wed,Thu,Fri,Sat,Sun

MATCHES – TTL

TTL

iptables -A INPUT -m ttl --ttl-lt 5 -j LOG

Faz filtragem baseada no TTL do pacote. Podem ser utilizadas:

--ttl-eq número - igual

--ttl-lt número - menor que

--ttl-gt número - maior que

MATCHES - TCP (1/3)

--sport, --source-port

iptables -A INPUT -p tcp --sport 12345

Identifica pacotes baseados na porta de origem da conexão.

--dport, --destination-port

iptables -A INPUT -p tcp –dport 22

Essa regra procura por pacotes baseado na porta de destino.

MATCHES – TCP (2/3)

--tcp-flags

iptables -p tcp --tcp-flags SYN,FIN,ACK SYN,FIN

Identifica pacotes baseando nas flags do cabeçalho TCP. O primeiro argumento é uma lista de quais flags procurar, e o segundo, quais flags devem estar marcadas para que a regra seja ativada.

MATCHES – TCP (3/3)

--syn

iptables -p tcp -syn

Procura por pacotes que tenham a flag syn marcada e não tenha as flags ACK e RST ligadas.

MATCHES – UDP

--sport, --source-port

iptables -A INPUT -p udp --sport 12345

Identifica pacotes baseados na porta de origem da conexão.

--dport, --destination-port

iptables -A INPUT -p udp --dport 22

Essa regra procura por pacotes baseado na porta de destino.

MATCHES – ICMP

--icmp-type

iptables -A INPUT -p icmp --icmp-type 8

Regras baseadas no tipo do pacote icmp.

MATCHES – LIMIT

--limit

Iptables -A INPUT -m limit --limit 3/hour

Faz um limite da taxa media de pacotes. Pode ser utilizada com as unidades: second, minute, hour, day.

--limit-burst

iptables -A INPUT -m limit --limit-burst 5

Limita a quantidade de pacotes em uma rajada. Trabalha em conjunto com uma regra --limit.

MATCHES – MAC

--mac-source

Iptables -A INPUT -m mac --mac-source 3a:40:30:00:e2:1f

Identifica pacotes baseados no endereço MAC de origem.

Essa regra funcionrá nas chains INPUT, FORWARD e PREROUTING

MATCHES – MARK

--mark

iptables -t mangle -A INPUT -m mark --mark 1

Identifica pacotes que foram anteriormente marcados.

MATCHES – MULTPORT (1/3)

--source-port

Iptables -A INPUT -p tcp -m multiport --source-port 22,80,443

Permite utilizar multiplas portas de origem (máximo de 15) com os protocolos TCP e UDP.

MATCHES – MULTPORT (2/3)

--destination-port

Iptables -A INPUT -p tcp -m multiport --destination-port 22,80,443

Permite utilizar multiplas portas de destino (máximo de 15) com os protocolos TCP e UDP.

MATCHES – MULTPORT (3/3)

--port

Iptables -A INPUT -p tcp -m multiport --port 22,80,443

Permite utilizar multiplas portas de origem e destino (máximo de 15) com os protocolos TCP e UDP.

MATCHES – OWNER (1/2)

--uid-owner

Iptables -A OUTPUT -m owner --uid-owner 500

Identifica pacotes baseados no ID criador do processo.

--gid-owner

iptables -A OUTPUT -m owner --gid-owner 0

Procura por pacotes baseados no ID do grupo.

MATCHES – OWNER (2/2)

--pid-owner

iptables -A OUTPUT -m owner --pid-owner 78

Procura por pacotes baseados no ID do processo.

--sid-owner

iptables -A OUTPUT -m owner --sid-owner 100

Procura por pacotes baseados no ID da sessão. Todos os threads de um processo devem ter o mesmo SID.

MATCHES – STATE

--state

Iptables -A INPUT -m state --state RELATED,ESTABLISHED

Trata os pacotes baseados no estado da conexão. Os possíveis estados são: INVALID, ESTABLISHED, NEW e RELATED.

MATCHES – TOS

--tos

Iptables -A INPUT -p tcp -m tos --tos 0x16

Identifica pacotes baseados no TOS (*Type Of Service*).

Minimize-Delay 16 (0x10)

Maximize-Throughput 8 (0x08)

Maximize-Reliability 4 (0x04)

Minimize-Cost 2 (0x02)

Normal-Service 0 (0x00)

MATCHES – TTL

--ttl

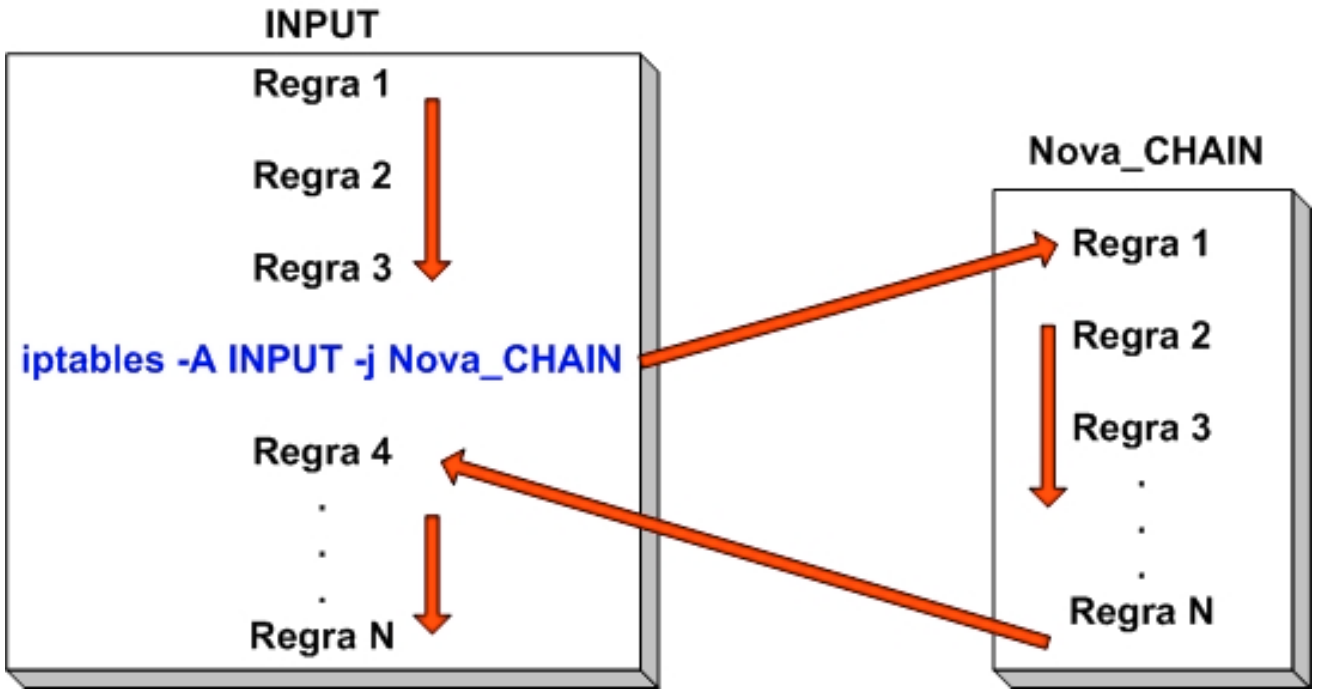
Iptables -A OUTPUT -m ttl --ttl60

Procura por pacotes baseados no seu TTL (*Time To Live*).

Targets

iptables -N Nova_CHAIN

iptables -A INPUT -j Nova_CHAIN



Targets

ACCEPT

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

Aceita um pacote. Permite que o pacote seja encaminhado ao seu destino

Targets

DNAT

iptables -t nat -A PREROUTING -p tcp -d 192.168.20.1 --dport 80 -j DNAT --to-destination 192.168.30.2

iptables -t nat -A PREROUTING -p tcp -d 192.168.20.1 --dport 80 -j DNAT --to-destination 192.168.30.2-192.168.30.5

iptables -t nat -A PREROUTING -p tcp -d 192.168.20.1 --dport 22 -j DNAT –to-destination 192.168.30.2:22000

Targets

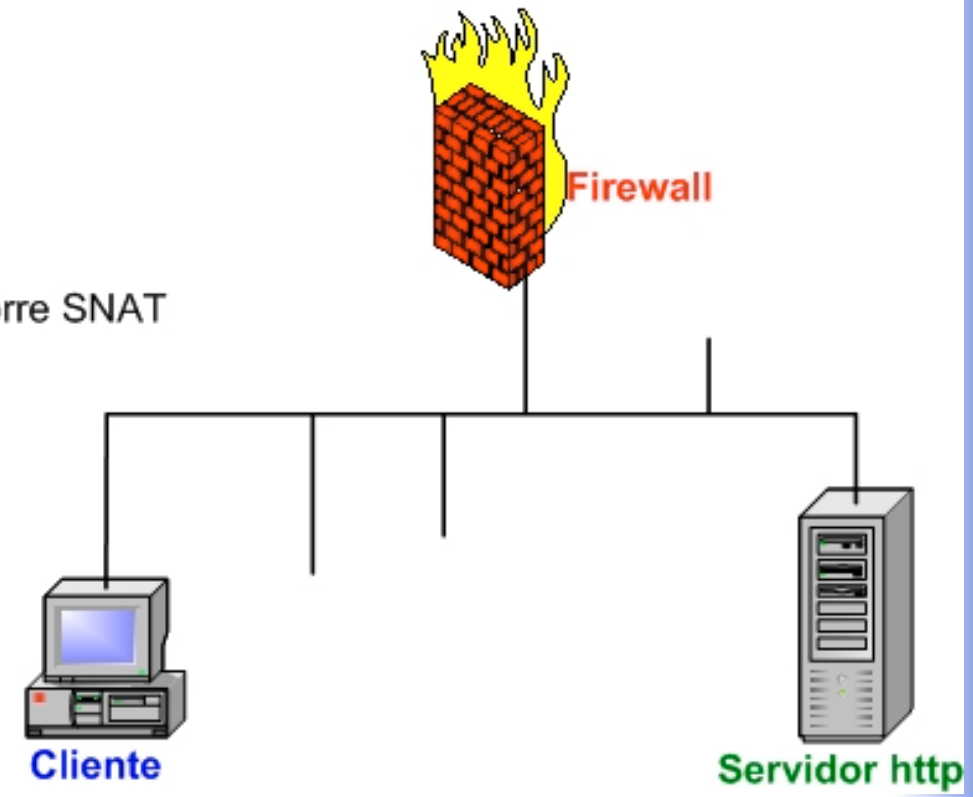
PROBLEMA

Quando um hoste da rede interna (que normalmente sofre um SNAT) tenta se conectar com um serviço que o firewall faz DNAT.

Problema: como o pacote vai para um endereco da rede interna, ele não sofre SNAT, então o servidor responde diretamente para o cliente (sem passar pelo firewall) e o cliente manda um reset para a conexão.

Targets

1. Cliente → Firewall
2. Firewall → Servidor http - Não ocorre SNAT
3. Servidor http → Cliente
4. Client → Servidor http - Reset



Targets

SNAT

iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to-source

192.168.30.1

Tem como função alterar o valor do endereço de origem dos pacotes.

Targets

MASQUERADE

iptables -t nat -A POSTROUTING -p tcp -j MASQUERADE

iptables -t nat -A POSTROUTING -p tcp -j MASQUERADE --to-ports 2000

Mesma função do SNAT, mas não necessita da opção --to-souce, é buscado o enderço da maquina. Essa regra é utilizada em quando o enderço IP do firewall é dinamico: DHCP, ppp, PPPoE

Targets

DROP

iptables -A INPUT -p tcp --dport 139 -j DROP

Descarta um pacote. O pacote não é processado por nenhuma outra regra.

Targets

LOG

Faz log de pacotes. Envia informações do pacote para o kernel, onde pode ser lido pelo syslog.

Targets

--log-level

iptables -A FORWARD -p tcp -j LOG --log-level debug

Essa opcão diz ao iptables qual nível de log (log level) usar.

debug, info, notice, warning, error, crit, alert, emerg e panic.

Targets

--log-prefix

iptables -A INPUT -p tcp -j LOG --log-prefix "INPUT packets"

Coloca a string em questão com prefixo do log. Facilita a busca por logs com o

grep ou swatch.

Targets

--log-tcp-sequence

iptables -A INPUT -p tcp -j LOG --log-tcp-sequence

Essa opção irá adicionar o número de seqüencia TCP ao log do pacote.

Targets

--log-tcp-options

iptables -A INPUT -p tcp -j LOG --log-tcp-options

Adiciona ao log as opções do cabeçalho TCP

Targets

--log-ip-options

iptables -A INPUT -p tcp -j LOG --log-ip-options

Adiciona ao log as opções do cabeçalho IP

Targets

MARK

iptables -t mangle -A PREROUTING -p tcp -dport22 -j MARK --set-mark 2

Faz uma marcação no pacote. Essa marcação pode ser utilizada pelo própria máquina para realizar roteamento de pacotes.

Obs.: Essa marca não é adicionada ao pacote! Não pode ser reconhecida em outra máquina

Targets

QUEUE

iptables -A INPUT -p tcp -j QUEUE

Envia o pacote para o userspace (espaço do usuário), onde outros programas podem utilizar/analizar este pacote

Targets

REDIRECT

iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080

Faz um DNAT no pacote, enviando este para o próprio firewall (127.0.0.1). Essa regra deve ser utilizada apenas nas chains PREROUTING e OUTPUT e na tabela nat.

Utilizada para fazer Proxy transparente

Targets

REJECT

iptables -A FORWARD -p tcp -dport 22 -j REJECT --reject-with tcp-reset

Mesma função que DROP, mas envia uma mensagem de erro para o origem do pacote.

icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable,

icmp-proto-unreachable, icmp-net-prohibited, icmp-host-prohibited, tcp-reset

Targets

RETURN

iptables -A SPOOFING_TEST -p tcp -j RETURN

Envia o pacote para a chain imediatamente superior, como se nada tivesse ocorrido. Se for utilizada em uma das chains default (INPUT, FORWARD), será aplicado ao pacote a política default

Targets

TOS

iptables -t mangle -A PREROUTING -p tcp --dport 22 -j TOS --set-tos 0x10

Ajusta o TOS (Type Of Service) do pacote. Deve sempre ser utilizado na tabela mangle.

- Minimize-Delay 16 (0x10)
- Maximize-Throughput 8 (0x08)
- Maximize-Reliability 4 (0x04)
- Minimize-Cost 2 (0x02)
- Normal-Service 0 (0x00)

Targets

TTL

iptables -t mangle -A PREROUTING -i eth0 -j TTL --ttl-set 64

Essa regra irá definir o TTL do pacote. Útil para mascarar várias maquinas com

sistemas operacionais diferentes

Targets

iptables -t mangle -A PREROUTING -i eth0 -j TTL --ttl-dec 3

Decrementa o TTL do pacote.

iptables -t mangle -A PREROUTING -i eth0 -j TTL --ttl-inc 1

Incrementa o valor do TTL do pacote.

Sempre deve ser utilizda na tabela mangle.

Ferramentas

connwatcher.pl

Fwlogwatch

Pigmelt

Tuxfrw

Fwbuilder

connwatcher.pl

Processa a lista de conexões da contrack

Mais legível

“Refresh” automático

http://prdownloads.sourceforge.net/fwbuilder/connwatcher.pl?download

Fwlogwatch

Analizador de logs

Escrito em C por Boris Wesslowski - RUS-CERT

- Ipchains
- Netfilter
- Ipfilter
- Cisco IOS
- Snort

Fwlogwatch

Aceita compressão de logs (gzip)

Gera sumários em HTML ou texto

Pode enviar *reports* via e-mail

http://cert.uni-stuttgart.de/projects/fwlogwatch/

Pigmeat

Bloqueio por Firewall em tempo real

Utiliza logs do Snort

Listas de IPs bloqueados e ignorados

Pode ser executado em modo interativo

http://pigmeat.linuxinfo.com.br/

TuxFrw

Gerador de regras para o Netfilter

Criação de scripts de inicialização que configuram o Netfilter

Divisão em módulos dos scripts

Desenvolvido por brasileiros

Marcelo de Souza <marcelo@acmesecurity.org>

Marcelo Gondim <gondim@linuxinfo.com.br>

http://tuxfrw.sourceforge.net/

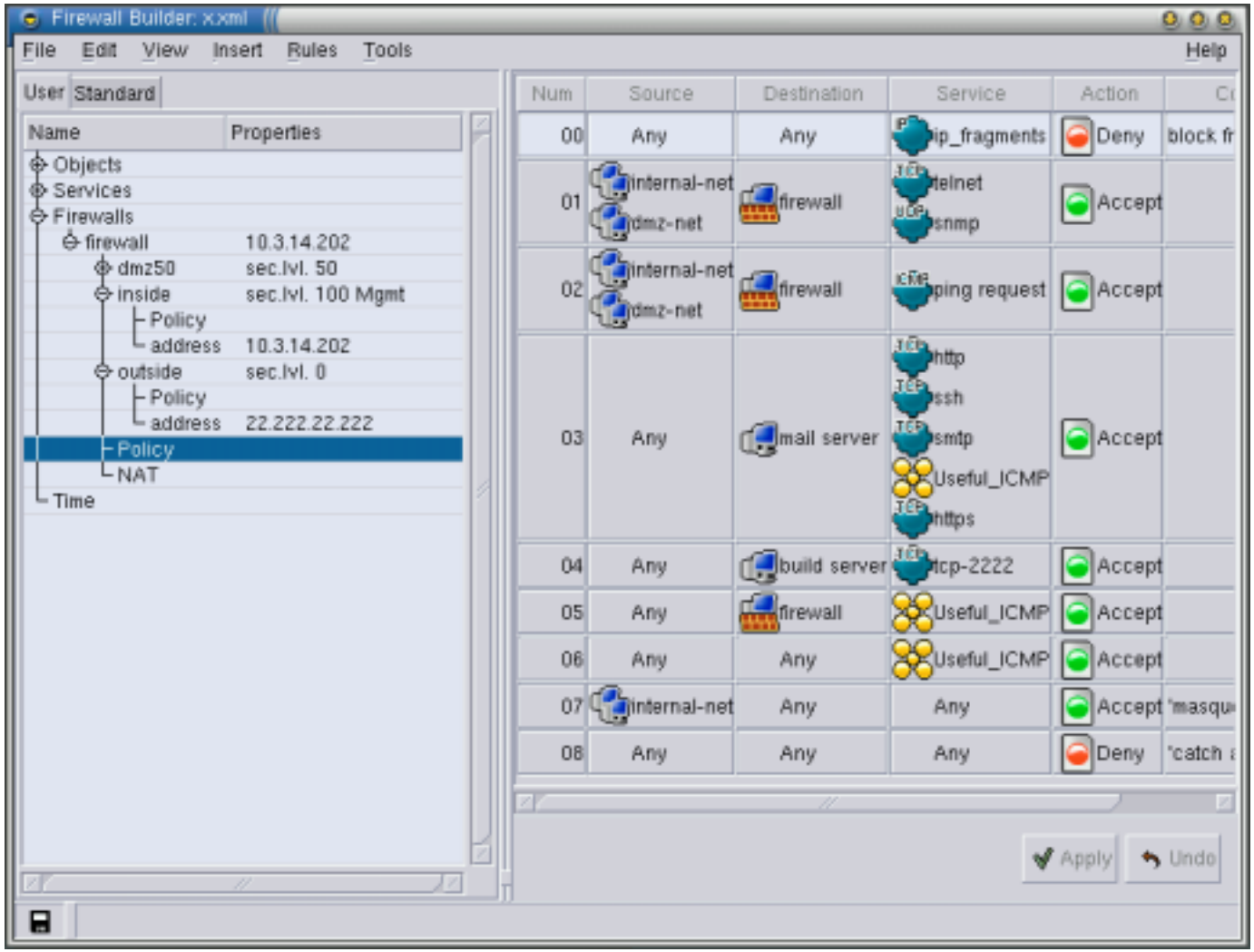
Fwbuilder

Ferramenta gráfica para geração de regras para diversos firewalls

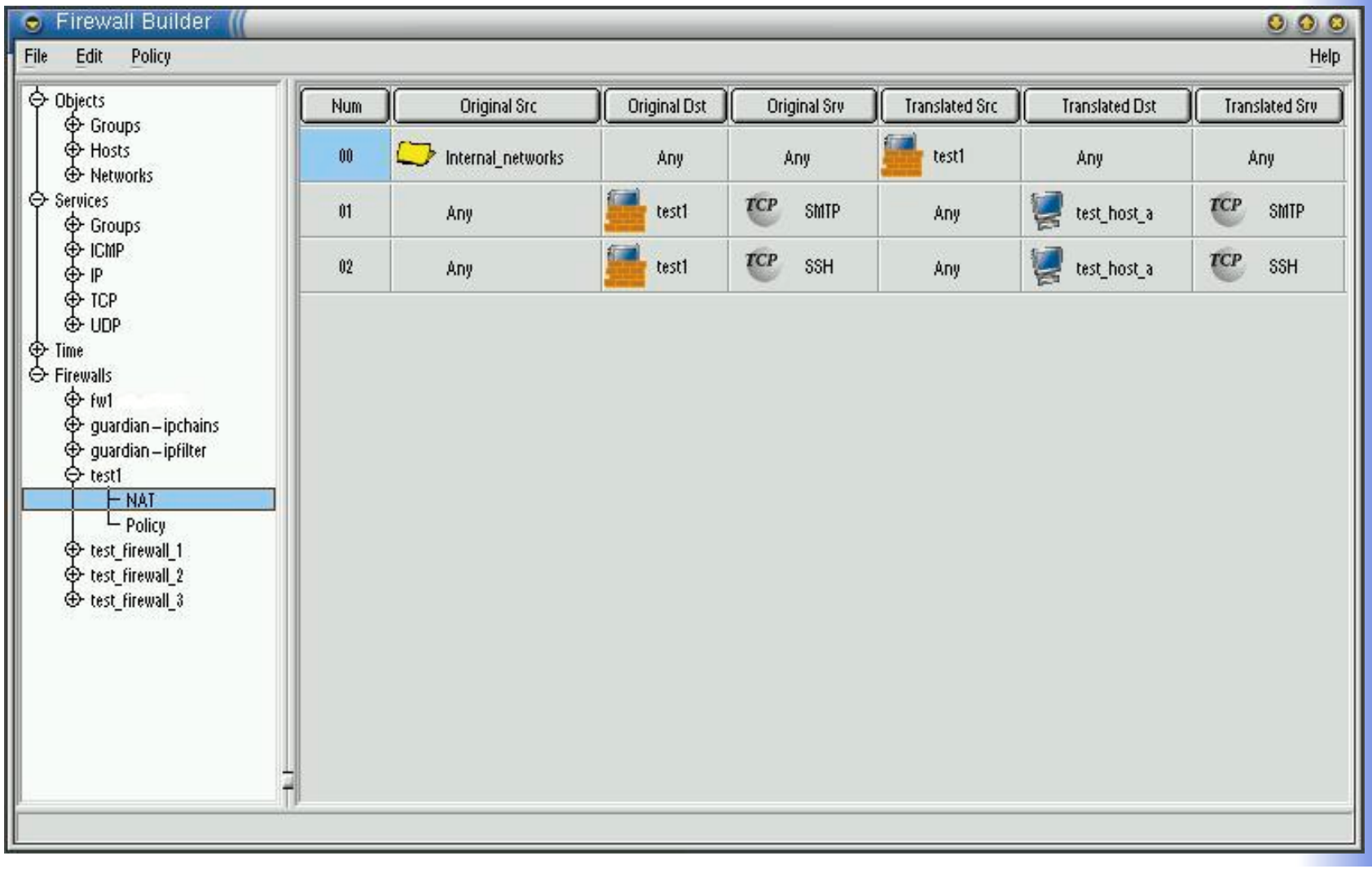
- Iptables
- Ipfilter
- Packet Filter
- Cisco PIX.

http://www.fwbuilder.org/

Fwbuilder


Firewall Builder: x.xml
File Edit View Insert Rules Tools Help
User Standard
Name Properties
Objects
Services
Firewalls
firewall 10.3.14.202
dmz50 sec.lvl. 50
inside sec.lvl. 100 Mgmt
Policy
address 10.3.14.202
outside sec.lvl. 0
Policy
address 22.222.22.222
Policy
NAT
Time
Num Source Destination Service Action
00 Any Any ip_fragments Deny block fr
01 internal-net dmz-net firewall telnet snmp Accept
02 internal-net dmz-net firewall ping request Accept
03 Any mail server http ssh smtp Useful_ICMP https Accept
04 Any build server tcp-2222 Accept
05 Any firewall Useful_ICMP Accept
06 Any Any Useful_ICMP Accept
07 internal-net Any Any Accept
08 Any Any Any Deny
Apply Undo

Fwbuilder


Firewall Builder
File
Edit
Policy
Help
Objects
Groups
Hosts
Networks
Services
Groups
ICMP
IP
TCP
UDP
Time
Firewalls
fw1
guardian – ipchains
guardian – ipfilter
test1
NAT
Policy
test_firewall_1
test_firewall_2
test_firewall_3
Num
Original Src
Original Dst
Original Srv
Translated Src
Translated Dst
Translated Srv
00
Internal_networks
Any
Any
test1
Any
Any
01
Any
test1
TCP
SMTP
Any
test_host_a
TCP
SMTP
02
Any
test1
TCP
SSH
Any
test_host_a
TCP
SSH

Links

http://forum.acmesecurity.org

http://www.netfilter.org

http://iptables-tutorial.frozentux.net/

http://www.kernel.org

Autores

Prof. Dr. Adriano Mauro Cansian

<adriano@acmesecurity.org>

Artur Renato Araujo da Silva

<artur@acmesecurity.org>

Jarbas de Freitas Peixoto

<jarbas@acmesecurity.org>