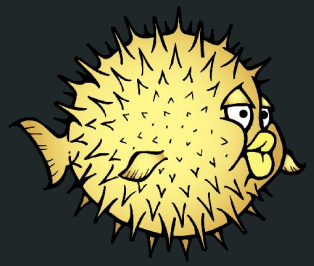


Firewall com OpenBSD

Luis Henrique Fonseca
Weslei de Paula Pinto
Felipe Menino

Agenda

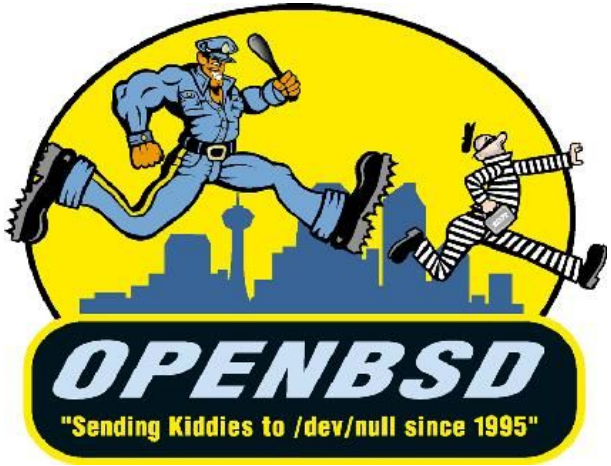
- Motivação
- O que é OpenBSD
- Porquê o OpenBSD
- Diferenças entre FreeBSD, OpenBSD e NetBSD
- O que é o PF
- Criação e configuração do Firewall

Motivação

- Depois do sofrimento com uma quantidade elevada de regras no IPtables, decidimos buscar novas formas de realizar a configuração dos firewalls livres que estávamos fazendo.

O que é OpenBSD

- OpenBSD é um sistema operacional baseado em UNIX, que tem suporte a uma vasta quantidade de arquiteturas.
- Desde sua primeira versão, se focou no desenvolvimento seguro, o que lhe gerou apenas duas falhas em 22 anos.
- É um *fork* do projeto BSD



Porquê o OpenBSD

- Como citado o OpenBSD tem seu ecossistema completamente desenvolvido em meio a segurança, isso faz com que ele seja um sistema bastante seguro, e ainda, a implementação de muitas ferramentas são facilitadas, para evitar configurações que causem dano à segurança.

Diferenças entre FreeBSD, OpenBSD e NetBSD

A diferença do OpenBSD para os outros Sistema Operacionais da família BSD é que:

- NetBSD: tem a característica de suportar diversas plataformas e sua segurança também é forte outras características são, a qualidade e correção do código, adesão aos padrões e pesquisa e inovação
- FreeBSD: O Freebsd tem a sua característica por ter excelente performance em aplicações para servidores Web e de banco de dados.
  O que deixa a desejar no FreeBSD é a arquitetura que roda apenas em plataforma Intel 32 bits

O que é o PF

- O PF ou *packet filter* é o sistema de *firewall* utilizado nos sistemas BSD;
- Permite realizar a criação de:
  - NAT
  - DMZ
  - Priorização de pacotes
  - Control de banda
- A facilidade é sua maior vantagem

PF vs IPTables

- PF
  - Regras menores;
  - Maior organização com listas, variáveis;
  - Análise *stateful* dos pacotes;
  - Análise sequencial das regras;
  - Lento em muitos casos se comparado ao IPTables
- IPTables
  - Rápido;
  - Em certos ambientes, as muitas regras causam confusão;
  - Não realiza análise stateful
  - Análise das regras feita de forma não estruturada

Criação e configuração do Firewall

Instalando VIM

- Antes de qualquer ação, é necessário instalar o VIM, ou utilizar o VI
- Os comandos são bastante simples, veja

```
# export PKG_PATH=http://ftp.openbsd.org/pub/OpenBSD/`uname -r`/packages/`arch>
# echo $PKG_PATH
http://ftp.openbsd.org/pub/OpenBSD/6.1/packages/i386
#
```

Instalando VIM

```
# pkg_add vim
quirks-2.304 signed on 2017-04-04T09:09:10Z
quirks-2.304: ok
Ambiguous: choose package for vim
a       0: <None>
        1: vim-8.0.0388-gtk2
        2: vim-8.0.0388-gtk2-lua
        3: vim-8.0.0388-gtk2-perl-python-ruby
        4: vim-8.0.0388-gtk2-perl-python3-ruby
        5: vim-8.0.0388-no_x11
        6: vim-8.0.0388-no_x11-lua
        7: vim-8.0.0388-no_x11-perl-python-ruby
        8: vim-8.0.0388-no_x11-perl-python3-ruby
        9: vim-8.0.0388-no_x11-ruby
Your choice:
```

Configurando as interfaces

- Vamos agora configurar a interface LAN, já que neste caso a WAN está com IP dinâmico;
- Neste cenário temos:
  - em0 -> WAN
  - em1 -> LAN

```
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        lladdr 08:00:27:e8:4b:f7
        index 1 priority 0 llprio 3
        groups: egress
        media: Ethernet autoselect (1000baseT full-duplex)
        status: active
        inet 192.168.0.5 netmask 0xffffff00 broadcast 192.168.0.255
em1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
        lladdr 08:00:27:eb:14:4c
        index 2 priority 0 llprio 3
        media: Ethernet autoselect (1000baseT full-duplex)
        status: active
```

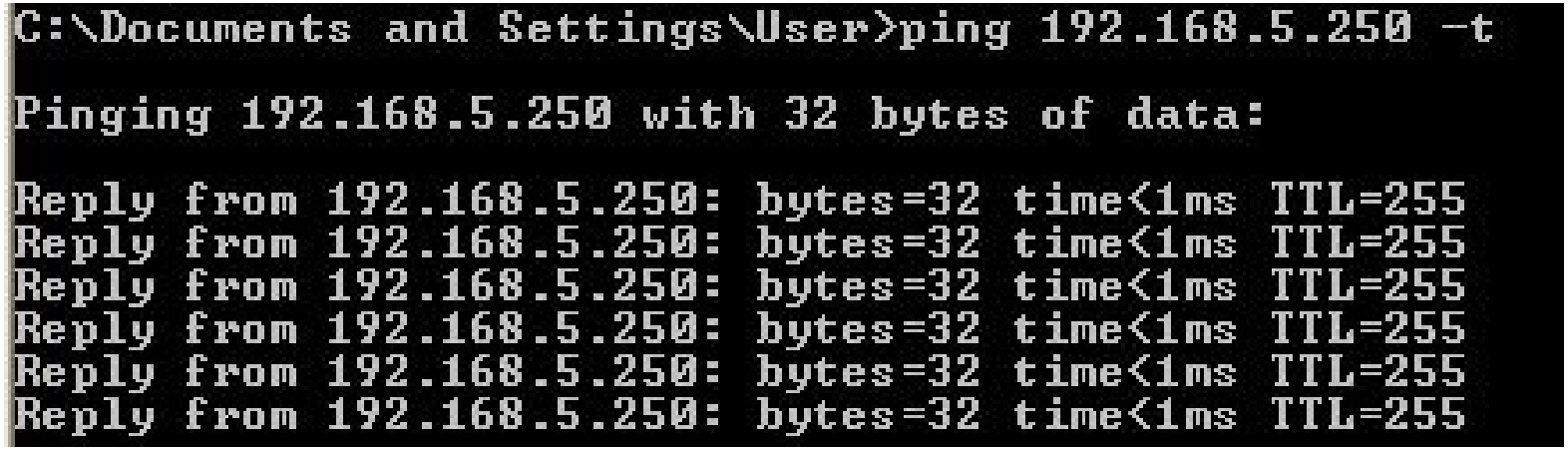
Configurando as interfaces

- Para configurar a interface é necessário criar um arquivo de configuração para a interface.
  - vim /etc/hostname.NOME_DA_INTERFACE
  - exemplo: vim /etc/hostname.em1
- Dentro deste arquivo, inserir as configurações da interface. No caso de ip fixo usa-se:
  - inet 192.168.x.x 255.255.255.0 192.168.x.255
- Já nos ips dinâmicos:
  - dhcp

Configurando as interfaces

```
# echo "inet 192.168.5.250 255.255.255.0 192.168.5.255" > /etc/hostname.em1
# cat /etc/hostname.em1
inet 192.168.5.250 255.255.255.0 192.168.5.255
#
```

Configurando as interfaces



DHCP

- A configuração do DHCP no OpenBSD é bastante simplificada, quando comparada a outras, como o Debian
- Para habilitar o DHCP, basta executar os comandos:

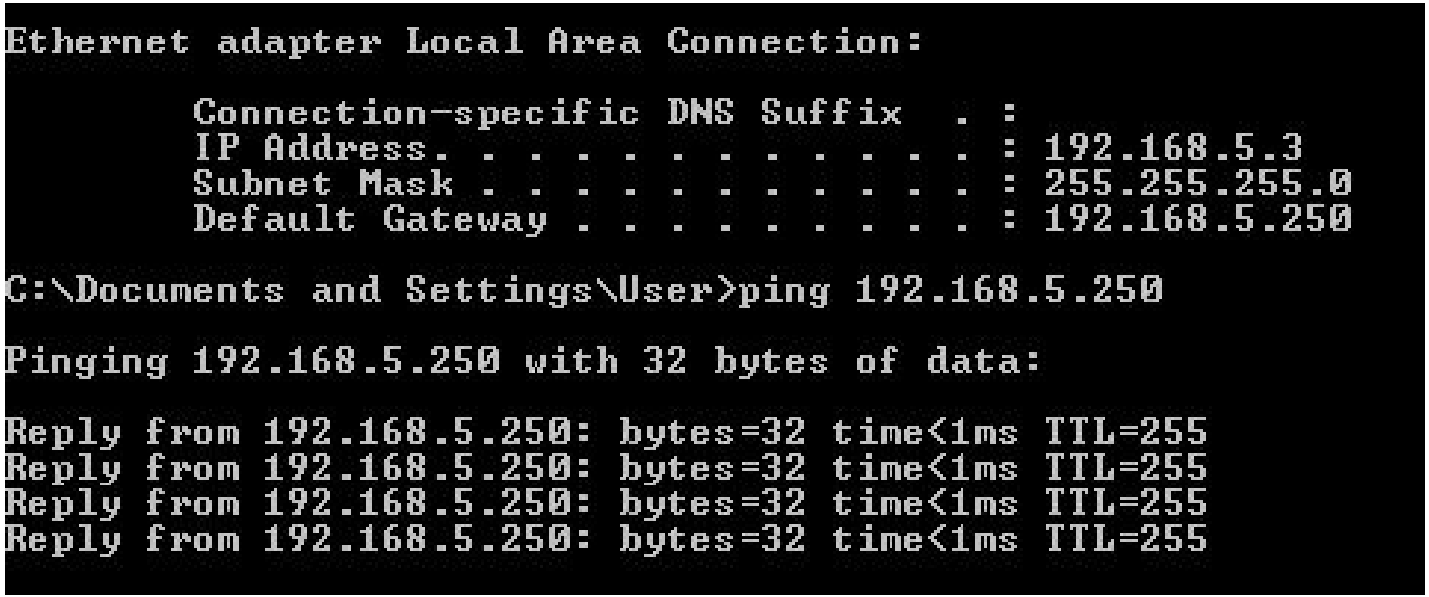
```
# rcctl enable dhcpd
# rcctl set dhcpd flags em1
# 
```

DHCP

- vim /etc/dhcpd.conf

```
subnet 192.168.5.0 netmask 255.255.255.0 {
        option domain-name-servers 8.8.8.8;
        option routers 192.168.5.250;
        range 192.168.5.3 192.168.5.50;
}
```

DHCP


Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.5.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.5.250
C:\Documents and Settings\User>ping 192.168.5.250
Pinging 192.168.5.250 with 32 bytes of data:
Reply from 192.168.5.250: bytes=32 time<1ms TTL=255
Reply from 192.168.5.250: bytes=32 time<1ms TTL=255
Reply from 192.168.5.250: bytes=32 time<1ms TTL=255
Reply from 192.168.5.250: bytes=32 time<1ms TTL=255

NAT

- echo “pf=YES” >> /etc/rc.conf.local
- echo “net.inet.ip.forwarding=1” >> /etc/sysctl.conf
- vim /etc/pf.conf

```
## Interfaces, externas e internas
ExtIf = "INTERFACE_EXTERNA" #Exemplo: ExtIf="em0"
IntIf = "INTERFACE_INTERNA" #Exemplo: IntIf="em1"

## Rede privada que recebe o NAT
PrivNet = "192.168.5.0/24" #Rede que será utilizada

## Our NAT
match out log on $ExtIf from $PrivNet to any received-on $IntIf tag EGRESS nat-to ($ExtIf:0)
```

Squid

- Para instalar execute:

```
#  export PKG_PATH=http://ftp.openbsd.org/pub/OpenBSD/`uname -r`/packages/`arch -s`
# pkg_add -i squid
```

Squid

- vim /etc/squid/squid.conf

```
#Porta padrão do squid
http_port   3128

#Nome do servidor
visible_hostname SquidOpenBSD

#Caminho do diretório de cache
cache_dir   ufs /var/squid/cache 100 16 256

#Cache Admin
cache_mgr  administrador@VoIP.com

#Log de acesso
access_log /var/log/squid/access.log squid

#Bloqueio de sites por URL
acl sites_proibidos url_regex -i etc/squid/sites_proibidos
http_access deny sites_proibidos
```

Squid

- vim /etc/squid/squid.conf

```
#Portas Seguras

#Porta SSL
acl SSL_ports port 443
acl Safe_ports port 80 #HTTP
acl Safe_ports port 443 #HTTPS
acl Safe_ports port 3128 #Squid
acl Safe_ports port 22 #SSH

acl CONNECT method CONNECT

#Redes que vão se conectar ao squid
acl manager proto cache_object
acl redelocal src 10.20.30.0/24

#Bloqueio de portas e endereços
http_access allow redelocal
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access deny all
```

Squid

- > /etc/squid/sites_proibidos
- mkdir /var/log/squid
- > /var/log/squid/access.log
- Para verificar se há erros na configuração, execute:
  - squid -d 1 -N

SquidGuard

- O SquidGuard trabalha como uma extensão do Squid, esse ajuda na adição de regras, para aumentar o *range* de sites bloqueados
- export PKG_PATH=http://ftp.openbsd.org/pub/OpenBSD/`uname -r`/packages/`arch -s`

```
# pkg_add -i squidGuard
quirks-2.304 signed on 2017-04-04T09:09:10Z
Ambiguous: choose package for squidGuard
a       0: <None>
        1: squidGuard-1.4p14
        2: squidGuard-1.4p14-ldap
Your choice: 1
squidGuard-1.4p14: ok
# pkg_add -i wget
quirks-2.304 signed on 2017-04-04T09:09:10Z
wget-1.19.1:libpsl-0.17.0: ok
wget-1.19.1:pcre-8.38p0: ok
wget-1.19.1: ok
```

SquidGuard

- Baixando e configurando a blacklist
- wget http://www.shallalist.de/Downloads/shallalist.tar.gz
- tar zxvf shallalist.tar.gz -C /var/db/squidGuard/db/
- chown -R _squid /var/db/squidGuard
- vim /etc/squid/squid.conf

```
#SquidGuard config

url_rewrite_program   /usr/local/bin/squidGuard
url_rewrite_children  5
url_rewrite_access    deny  localhost
```

SquidGuard

- vim /etc/squidguard/squidguard.conf

```
#
# SOURCE ADDRESSES:
#

src clients {
        ip                      192.168.5.1-192.168.5.240
}
```

SquidGuard

- vim /etc/squidguard/squidguard.conf

```
#
# DESTINATION CLASSES:
#

dest porn {
        domainlist BL/porn/domains
        urllist  BL/porn/urls
}

src lan {
        ip      192.168.0.5/24
}


acl {
        lan {
                pass !porn all
        }

        default {
                pass !porn all
        }
}
```

Obrigado