Construindo uma VPN usando IPSec

IPSec (IP Security)

- **IPSec é o protocolo de comunicação em uma VPN.**

- **IPSec é um conjunto de padrões e protocolos para segurança relacionada a uma rede VPN criada sobre uma rede IP, e foi definido pelo grupo de trabalho denominado IP Security do IETF.**

Objetivos do IPSec

- **Oferecer criptografia e autenticação para a camada de rede, em redes IP.**
- **Proteger tráfego sobre o IP, em vez de outros que apenas protegem tráfego em camadas superiores (SSH, SSL, PGP).**

Objetivos do IPSec

- **Garantir segurança entre duas máquinas.**
- **Não garante segurança das máquinas que estão na rede; a única coisa que faz é criptografar e garantir a segurança das informações (pacotes encapsulados) que estão passando pelo túnel.**

Protocolos IPSec

- AH (Authentication Header)

  Oferece serviço de autenticação para o pacote.
- ESP (Encapsulating Security Payload)

  Oferece criptografia + autenticação
- IKE (Internet Key Exchange)

  Negocia parâmetros de conexão, incluindo chaves, para os outros dois protocolos.

IPSec

- Todos os protocolos utilizam UDP **e a porta 500.**
- **O IPSec especifica os cabeçalhos AH e ESP, que podem ser usados de forma independente ou em conjunto, de maneira que um pacote IPSec poderá apresentar somente um dos cabeçalhos (AH ou ESP), ou os dois.**

IPSec

- Não autentica mensagens entre usuários **ou aplicações, no túnel.**
- Autenticação é de computador para computador **(autenticações somente de máquinas). Esse processo acontece na troca de** chaves**.**
- **Trabalha na camada de rede,** encapsulando o protocolo TCP**, ou outros, se necessário.**

Projeto FreeSwan

- **FreeSwan = Free Secure Wide Area Network**
- **1996-1999**
- **John Gilmore (gnu@toad.com)**
- **Meta: criar dentro da Internet (rede insegura) uma rede segura.**

Projeto FreeSwan

- **É uma implementação IPSec para Linux.**

- **Três partes para implementar IPSec:**

  1 - KLIPS (Kernel do IPSec) implementa AH e ESP;
  2 - PLUTO (Daemon IKE) implementa o IKE, fazendo a negociação com outros sistemas IPSec.
  3 - IKE negocia os parâmetros de conexão incluindo a troca de chaves criptográficas.

FreeSwan

- **Comunica-se com todas as VPNs construídas com IPSec.**
- **Se numa extremidade da rede tem o Linux rodando IPSec, e na outra estiver rodando também o IPSec, o FreeSwan se conectará.**

Criptografia do FreeSwan

- **É a mesma para qualquer protocolo IPSec.**
- **Primeiro usa o método assimétrico para formar o túnel.**
- **Logo após, os dados são criptografados utilizando o método simétrico, por ser mais rápido.**

FreeSwan

- **A criptografia utilizada pelo FreeSwan é a mesma de qualquer protocolo IPSec.**
- **Se utiliza da criptografia assimétrica para definir o túnel, e logo após, os dados são criptografados, utilizando o método simétrico, por ser mais rápido.**

FreeSwan

- **As máquinas (gateways) que rodam o IPSec não trocam a** chave privada**. Elas se relacionam apenas através da** chave pública **no momento da autenticação.**

FreeSwan - Tipos de Conexão

- **Desktop através de DHCP**
- **Gateway para Gateway**
  (Rede para Rede)

Montando uma VPN

- **Utilizando os gateways com** IPs fixos nas duas extremidades**:**

  conexão gateway **para** gateway

- **Utilizando os gateways com** IPs dinâmicos, através de DHCP**, nas duas extremidades.**

VPN

- **Uma VPN** não faz a segurança da máquina **(host) que está dentro da rede.**

Um Firewall para VPN

- **Então, temos que** configurar um Firewall para utilizar com a VPN**.**

Firewall para VPN

- **Inicialmente, deve-se** definir a política de segurança **utilizada no Firewall.**

- **Neste exemplo,** utilizamos a política DROP **para as três tabelas básicas de acesso no Firewall:**

```
iptables –P INPUT DROP
iptables –P OUTPUT DROP
iptables –P FORWARD DROP
```

Política de Firewall - IPTables

- DROP Nega pacote sem envio de flag Reset – R.
- ACCEPT – aceita o pacote.
- REJECT – nega pacote mas envia um flag Reset – R.
- **O envio de um flag** Reset **pode facilitar a detecção por um scanner de portas, procurando uma porta aberta. Por isso utiliza-se a política DROP.**

Montando uma VPN com IPs Fixos

- **Configurando o Firewall:**

  O Firewall não deve estar funcionando para outras aplicações.

  São liberadas apenas as portas para definir o túnel da VPN.

Montando uma VPN com IPs Fixos

- **Configurando o Firewall**

Liberando as portas apropriadas, a conexão será estabelecida apenas para os protocolos IPSec.

Montando uma VPN com IPs Fixos

- **Estrutura de regras de FIREWALL básicas para abrir conexão na VPN:**

  iptables (comando para referenciar tabelas IP no Firewall IPTables)

  -A (incluindo uma regra)
  INPUT / OUTPUT / FORWARD (a regra será incluída na tabela especificada)
  -p protocolo usado
  -s IP de origem
  -i tipo de rede na entrada do FIREWALL
  -o tipo de rede na saída do FIREWALL
  --sport porta da origem
  --dport porta de destino
  -j tratamento do pacote (ACCEPT /

Exemplo de Regra

- **Incluindo regra na tabela INPUT, para aceitar pacotes TCP, cujo IP de origem é 192.168.47.0/24 e tenham porta de destino 22:**

```
iptables -A  INPUT -p tcp
         -s 192.168.47.0/24
         --dport 22 –j ACCEPT
```

Exemplo de Firewall configurado para IPSEC

- **world=eth0**

 # negociações do IKE sobre parâmetros de conexão

```
iptables -A INPUT -p udp -i $world
         -sport 500 -dport 500 -j ACCEPT
  iptables -A OUTPUT -p udp -o $world
         -sport 500 -dport 500 -j ACCEPT
```

Exemplo de Firewall configurado para IPSEC

```
# ESP encriptação and autenticação
  # ESP é o protocolo 50 no IPSEC
  iptables -A INPUT -p 50 -i $world
           -j ACCEPT
  iptables -A OUTPUT -p 50  -o
          $world -j ACCEPT
```

Exemplo de Firewall configurado para IPSEC

 # IKE negociações sobre parâmetros de conexão

```
iptables -A INPUT  -p udp -sport 500 -dport 500
         -j ACCEPT

iptables -A OUTPUT -p udp -sport 500 -dport 500
         -j ACCEPT
```

Exemplo de Firewall configurado para IPSEC

 # ESP encriptação e autenticação
 # ESP é o protocolo 50 no IPSec

```
iptables –A INPUT –p 50 –j ACCEPT
iptables –A OUTPUT –p 50 –j ACCEPT

# AH (autentication header)
# AH é o protocolo 51 no IPSec
iptables –A INPUT –p 51 –j ACCEPT
iptables –A OUTPUT –p 51 –j ACCEPT
```

VPN

- **Mas, antes de montarmos a VPN, devemos saber:**

  - a VPN não faz controle de banda**;**

Controle de Banda

- **Controle de Banda**

Para determinar, por exemplo, quanto de banda a VPN vai utilizar**.**

O controle de banda é sempre interessante, independente da VPN, como no caso que se queira diminuir a banda de uma rede que está fazendo muito download de MP3.

Controle de Banda

- **Será possível, utilizando o sistema de controle de banda** CBQ (Class Based Queueing)

Funcionalidades CBQ

- **Controle de banda por rede, host ou mesmo, porta;**
- **Controle de banda excedente;**
- **Possibilidade de criação de classes de banda;**
- **Juntamente com o Firewall, na proteção contra ataques DoS.**

Para a Instalação do CBQ

- **Devem ser necessários os seguintes programas:**

  cbq.ini **(ftp.equinox.gu.net/pub/linux/cbq)**

  kernel-2.4.22 **(www.kernel.org)**

  iprouter2 **(www.linuxmafia.org)**
- **Todos colocados em** `/tmp`

Suporte de Kernel do Linux

- **O** CBQ **funciona como um módulo do** Linux kernel-2.4.22**.**
- **Para instalar o CBQ, primeiro deve ser dado suporte no kernel.**
- **É necessário que um** fonte do kernel **do Linux seja descompactado, por padrão, em** /usr/src **e o arquivo** `.config` **seja criado.**

Suporte de Kernel do Linux

- **Para criar o arquivo `.config`, basta digitar:**

```
make menuconfig
```

  dentro do diretório onde está o fonte do kernel e salvar.

- **Veja no que segue ... ...**

Suporte do Kernel Linux

- **O kernel em /tmp é descompactado em /usr/src e o arquivo .config é gerado:**

```
tar –xzvf linux-2.4.22.tar.gz –C /usr/src
cd /usr/src
ln –s linux-2.4.22  linux
cd linux
```

`make menuconfig` **(entra, não precisa alterar nada e salva)**

Instalando o CBQ

- **Para dar suporte ao kernel, deve-se** recompilar o kernel**.**
- **E para tal deve-se escolher a seguinte opção no** Linux Kernel v2.4.22 Configuration**:**

```
<M> CBQ packet sheduler
```

- A compilação começará imediatamente. Aparecerá:

```
cc ... ... ... ...
... ... ... ... ...
```

Instalando o CBQ

- **Depois de estar com o suporte do kernel, deve-se criar um diretório onde ficarão os** arquivos de configuração do CBQ**:**

```
mkdir /etc/cbq
```

Instalando CBQ

- **Após criar o diretório para CBQ,**
  `/etc/cbq`**,**
- **o passo seguinte será editar o arquivo**
  `cbq.ini` **(um script);**
- **atualize a variável** cbq_path **como:**

```
cbq_path = /etc/cbq
```

determinando o diretório onde foi criado os arquivos de configuração do CBQ.

Instalando o CBQ

- **Para fixar as regras para o CBQ, devemos saber que elas devem ficar dentro do diretório**

  `/etc/cbq`

- **Essas regras ficam dentro de arquivos únicos, que devem ter nomes de no mínimo 5 caracteres.**

- **Por exemplo,** `cbq-cont0001`

Estrutura de regra CBQ

DEVICE = <nome-rede>,<banda>,<peso>,<banda/10>

RATE = <velocidade>

WEITH = <peso/10>

PRIO = <prioridade> (1-8)

RULE = <IP ou rede a ser encontrada>

TIME = <limite de acesso em horários predefinidos>

BOUND = <yes/no> (Se yes, será mantido mesmo com banda excedente)

ISOLATED = yes/no (Se yes, a banda excedente não será compartilhada)

Exemplo de Regra CBQ

DEVICE = eth0,10Mbits,1Mbit
RATE = 128Kbits
WEITH = 10Kbits
PRIO = 5
RULE = 192.168.47.0/24

- **Com o Firewall e o CBQ configurados, basta configurar o FreeSwan para montarmos a VPN.**

Instalando o FreeSwan

- **O pacote pode ser baixado do link:**

  Download do pacote em ftp.xs4all.nl

  cd /tmp

  ftp://ftp.xs4all.nl/pub/crypto/freeswan/freeswan-2.02.tar.gz

  Utilizar a última versão deste aplicativo.

Instalando o FreeSwan

- **Descompactar o pacote em /tmp para o diretório** `/usr/local/src`

```
tar –xzvf freeswan-2.02.tar.gz
  -C /usr/local/src
```

- **O FreeSwan funciona como um módulo do kernel Linux.**

Instalando o FreeSwan

- **Agora com o pacote descompactado em , `/usr/local/src/freeswan-2.02` devemos incluir o módulo do FreeSwan dentro do kernel.**

- **Para isso, execute o comando:**

```
cd /usr/local/src/freeswan-2.02
make menumod
```

Instalando o FreeSwan

- **A tela do `menumod` assemelha-se à tela de configuração do kernel (a tela do `menuconfig`).**
- **Se olharmos a opção Networking Options, veremos que aparece o módulo da VPN dentro do kernel.**
- **Ver a tela do Linux Kernel v2.4.22 Configuration.**

Instalando o FreeSwan

- Selecionar **IPSec Debugging Option.**
- **Ao sair desse menu, a compilação do FreeSwan começará imediatamente.**
- **cc ... ...**
- **Ao término da compilação, se nada deu errado, deve-se executar o comando:**

```
make minstall
```

Instalando o FreeSwan

- **Havendo algum tipo de erro, é porque está faltando algum aplicativo necessário ao FreeSwan; instale esse aplicativo e execute o comando** `make menumod` **outra vez.**

Instalando o FreeSwan

- **O comando `make minstall` colocará os módulos compilados em seus devidos lugares.**
- **Para testarmos se a compilação está correta, devemos primeiramente ver se ficou algum tipo de erro de dependência no módulo do kernel.**

Instalando o FreeSwan

- **O comando para se fazer essa verificação é o** `depmod`**.**

```
depmod  -a
depmod  -ae
```

- **Esses comandos verificam se existe algum problema nos módulos associados ao kernel e também atualiza os arquivos de dependência dos mesmos.**

Instalando o FreeSwan

- **Com esses comandos executados, podemos tentar levantar o módulo do IPSec.**
- **Execute:** `modeprobe ipsec`
- **Se isso ocorrer sem problema é porque a compilação foi realizada com sucesso e o próximo passo é** gerar uma chave assimétrica para o fechamento da VPN**.**
- **Se algo deu errado, é preciso, primeiro fazer os ajustes.**

Instalando o FreeSwan

- **Gerando uma** chave assimétrica **para o estabelecimento do túnel (fechamento da VPN).**
- **O comando para gerar a chave é:**

```
ipsec newhostkey –output - --bits 1024
--hostname server1 > /etc/ipsec.secrets
```

Instalando o FreeSwan

- **1024 bits é o tamanho da chave que será gerada.**
- **Esse tamanho pode ser da escolha do administrador.**
- **Esse tamanho é usado nas duas pontas da VPN.**
- `Hostname` **é o nome da máquina de uma das pontas; no caso,** `server1`**.**

Instalando o FreeSwan: as chaves

- **As chaves (públicas e privadas) devem ser geradas nas duas pontas da VPN.**
- **As chaves públicas e privadas estão juntas em /etc/ipsec.secrets**

Instalando o FreeSwan

- **Dentro do arquivo** `ipsec.secrets` **temos uma linha comentada com** `#pubkey=<chave pública>.`

- **Esta linha tem a chave pública que iremos usar na configuração do FreeSwan.**

Instalando o FreeSwan

- **Com as chaves, pode-se editar o** arquivo de configuração do FreeSwan**, que se encontra em**

  `/etc/ipsec.conf`

- **Observar esse arquivo a partir da linha**

  `conn teste`

Observando o Arquivo de Configuração do FreeSwan (parte do ipsec.conf)

```
conn teste  (teste é o nome da conexão)
        # Gateway A
        left=192.168.50.10  (sai para a Internet)
        leftid=@clodo_trigo (nome do host)
        leftsubnet=192.168.5.0/24 (subrede do outro lado)
        leftnexthop=192.168.50.1 (gateway de aplicativo
                                  apontando para a Internet)
        leftrsasigkey=<código da chave pública usada no
                       estabelecimento do túnel-criptografia assimétrica
                       tirada do arquivo /etc/ipsec.secrets>
        leftfirewall=yes
        ... ... ...
```

Observando o Arquivo de Configuração do FreeSwan (parte do ipsec.conf)

```
# Gateway B
right=192.168.47.10  (sai para a Internet)
rightid=@honorio (nome do host)
rightsubnet=192.168.100.0/24 (subrede do outro lado)
rightnexthop=192.168.47.1 (gateway de aplicativo
                                apontando para a Internet)
rightrsasigkey=<código da chave pública usada no
                estabelecimento do túnel-criptografia assimétrica
                tirada do arquivo /etc/ipsec.secrets>
----------------------------------
rightfirewall=yes
auto=start
```

Arquivo de Configuração do FreeSwan

- **Esse esquema de configuração deve ser feito no mesmo arquivo para a outra extremidade da VPN.**
- **Deve-se trazer a chave da outra extremidade e colocar dentro do arquivo de configuração.**
- **Primeiro, foi configurado um lado chamado *left* e depois foi configurado o outro lado, *right*. Mas, esses nomes são apenas uma convenção.**

Arquivo de Configuração do FreeSwan

- **O arquivo de configuração será igual nas duas extremidades VPN.**
- **Na prática, montamos o arquivo de um lado e depois colocamos na outra ponta.**
- **O que muda entre os dois arquivos é a variável auto, que em uma será** `auto=start` **e na outra** `auto=add`**.**

Executando o IPSec

- **Inicie o IPSec**

```
/etc/init.d/ipsec stop
/etc/init.d/ipsec.start
```

- **É necessário levantar o IPSec (verificar se o túnel fechou) nas duas extremidades. Ver o arquivo de** `log`**.**

Arquivo de Log

- **Verificando o** arquivo de `log`**:**

  tail -f /var/log/autoh.log

- **Testando se o túnel está estabelecido corretamente: colocar algum tipo de programa no meio dessa conexão e verificar como está passando de um lado para o outro da VPN.**

Testando o Túnel

- **Por exemplo, colocamos o programa `etherape`, baixado de http://etherape.sourceforge.net/**

- **Caso algum erro aconteça, verifique a comunicação entre os *gateways* e se os arquivos estão de acordo com a sua rede.**

Montando uma VPN com DHCP

- **Caso, uma das extremidades seja DHCP (IP dinâmico), como ficaria o arquivo de configuração** `ipsec.conf` **?**

Montando uma VPN com DHCP

- **O arquivo** `ipsec.conf` **no lado da máquina DHCP ficaria:**

  conn road left=%defaultroute
  leftnexthop=%defaultroute
  leftid=@road.example.com
  leftrsasigkey=0sAQPIPN9uI...
  rightsubnet=10.0.0.0/24
  rightid=@xy.example.com
  rightrsasigkey=0sAQOnwiBPt...
  auto=start

- **Repetir esse arquivo na outra extremidade fazendo** auto=add **.**

Comandos IPSec

- **Testando a conexão da VPN:**
  `ipsec verify`
- **Criando as chaves pública e privada:**
  `ipsec newhostkey`
- **Mostrando as rotas criadas:**
  `ipsec look`
- **Mostra os nomes dos Hosts (left ou right)**
  `ipsec showhostkey`
- **Outros comando IPSec:**
  `ipsec -help`

Montando uma VPN com DHCP

- **Na outra extremidade, arquivo `ipsec.conf` será:**

  conn road left=%defaultroute
  leftnexthop=%defaultroute
  leftid=@road.example.com
  leftrsasigkey=0sAQPIPN9uI...
  rightsubnet=10.0.0.0/24
  rightid=@xy.example.com
  rightrsasigkey=0sAQOnwiBPt...
  auto=add