

Openswan-BR

IPSEC Utilizando Openswan

Especificações

Nesse item serão descritas as especificações da VPN IPSEC, essa que por sua vez é provida pela implementação de ipsec do Projeto Openswan (www.openswan.org)

Fase I – Parâmetros IKE	
Método de Autenticação	RSA / PSK / Certificado
Algoritmo de Criptografia	3DES / AES / Blowfish / Serpent
Algoritmo de Integridade	MD5 / SHA1
IKE Lifetime	3.600 s
Modo de Negociação	Main mode
Perfect Forward Secrecy – PFS	Habilitado / Desabilitado

Fase II – Parâmetros IPSEC	
Algoritmo de Criptografia	3DES / AES / Blowfish / Serpent
Algoritmo de Integridade	MD5 / SHA1
IPSEC Lifetime	28.800 s

Método de Autenticação: Tipo de chave utilizada, RSA / PSK / Certificado

Algoritmo de criptografia: Algoritmo utilizado para criptografar os dados (como se fosse uma fórmula matemática utilizada pelas pontas para criptografar e descriptografar os dados transmitidos).

Algoritmo de integridade: Algoritmo utilizado para efetuar a checagem dos dados trafegados e garantir que são os mesmos que foram emitidos pela origem.

Lifetime: Tempo que o protocolo (ike ou ipsec dependendo da fase) irá aguardar para renegociar a SA

Modo de Negociação: Forma que o IKE trocara as chaves

PFS: Método de renegociação de chaves criado com o intuito de prover segurança, renegociando a chave constantemente fazendo com que a nova chave nunca seja baseada na anterior.

Para que o túnel possa ser estabelecido são utilizadas as portas 500/UDP e os protocolos AH e ESP 51 e 50

Todos esses protocolos e portas devem trafegar sem restrições pelo meio físico entre os dois VPN Gateways.

IPSEC

ISAKMP-SA (Internet Security Association Key Management Protocol Security Association)

É um "ID" obtido através do ip, id, email e DN (caso utilizados), esse id é criado automaticamente pelo isakmp durante a negociação da Fase I somados com a chave RSA/PSK utilizada.

Para que a Fase 1 seja negociada com sucesso e necessário que se utilize um método de negociação que pode ser Main Mode ou Aggressive Mode

Main Mode

Para que a Fase um seja estabelecida com sucesso é necessário que uma série de requisições seja enviada entre os Gateways vpn, o método normal dessa negociação ser feita chama-se Main Mode.

Esse Método possui uma latência maior, pois depende do envio e recebimento de vários pacotes para a negociação, devido a essa maior quantidade de requisições efetuadas sua segurança é maior.

Aggressive Mode

Muitos Fabricantes Utilizam esse modo de negociação devido ter uma menor latência, pois envia menos requisições para estabelecer a fase 1, ISAKMP-SA, que é menor, esse modo é chamado de Aggressive Mode e reduz a quantidade de pacotes enviados, esse método requer mais CPU, pois tarefas relacionadas ao Diffie Hellman precisam ser concluídas antes do primeiro pacote ser reenviado. Devido a esse problema este método de negociação está sujeito a um Denial of Service, enviando ao IPSEC simples pacotes solicitando uma ISAKMP-SA

Main Mode X Aggressive Mode

A grande Vulnerabilidade do Aggressive Mode devido a redução de requisições efetuadas o hash da chave PSK é enviado antes da Encrytação ser habilitada, esse pacote pode ser capturado e uma ferramenta de brute force ou de dicionário pode obter a Chave utilizada. Já no Main mode o hash só é enviado após a encrytação ser habilitada

Com Aggressive Mode o pacote inicial da negociação contém todos os dados necessários para a fase 1, dessa forma o IPSEC remoto apenas verifica se pode efetuar ou não a solicitação. Dessa forma também está vulnerável a um ataque man-in-the-middle, caso esse pacote seja interceptado, um atacante pode obter uma conexão VPN válida.

Aggressive Mode consome menos recursos de rede, devido fazer menos requisições porem requer mais CPU por ter que processar a SA inteira antes de terminar a Fase I

Main Mode consome mais recursos de rede, por enviar mais requisições, por outro lado consome menos cpu, por processar a SA aos poucos, conforme as requisições são recebidas/enviadas

Quick Mode

Após a fase I , ISAKMP SA, ser concluída a Fase 2, IPsec SA, pode iniciar, para isso ela utiliza o Quick Mode para negociar parâmetros de criptografia, assim como

Arquivos de Configuração

O openswan é composto basicamente por dois arquivos de configuração são eles:

ipsec.conf – Principal arquivo de configuração do openswan
ipsec.secrets – Arquivo que contém as chaves RSA/PSK dos túneis

fora esses dois arquivos existe também os diretórios aacerts cacerts certs crls ocspcerts, que contem os certificados do openswan, caso configurado para trabalhar com suporte ao mesmo.

O principal arquivo de configuração do openswan ipsec.conf é composto por uma sintaxe simples, mas que deve ser respeitada para não haver erros.

Exemplo:

Bloco

Opção 1=opção
Opção 2=opção

Bloco 2

Opção 1=Opção
Opção 2=Opção

A Tabulação deve ser respeitada para não haver erros, e também não deve existir espaço antes e depois do sinal de igualdade.

Exemplo de uma conexão criada no ipsec.conf

```
conn gw1-gw2
    authby=rsasig
    esp=3des-md5
    ike=3des-md5
    ikelifetime=3600
    keylife=28800
    left=200.1.1.2
    leftid=@gw1.openswan
    leftnexthop=200.1.1.1
    leftrsasigkey=xEejhas4f.....
    leftsubnet=192.168.0.0/24
    right=201.1.1.2
    rightid=@gw2.openswan
    rightnexthop=201.1.1.1
    rightsakey=e654yr12a....
    rightrsasigkeysubnet=172.16.0.0/16
    pfs=no
```

Observações:

Os algoritmos de criptografia utilizados vão depender do suporte ao mesmo em seu kernel, o openswan suporta DES, 3DES, AES, Blowfish, entre outros menos utilizados, bastando ter suporte no kernel.

Opções relevantes:

Parâmetros Fase 1	
Algoritmos de Criptografia	ike=3des, ike=AES, ike=blowfish
Algoritmos de Integridade	ike=md5, ike=sha1
Ambos	ike=3des-md5, ike=aes-sha1
Lifetime	ikelifetime=3600, ikelifetime=8h
pfs	pfs=no, pfs=yes
Grupo diffie-hellman (caso pfs=yes)	ike=3des-sha1-modp1024
Parâmetros Fase 2	
Algoritmos de Criptografia	esp=3des, esp=aes, esp=blowfish
Algoritmos de Integridade	esp=md5, esp=sha1
Lifetime	Keylife=28800, keylife=8h
Parâmetros Diversos	
Compressão de dados	compression=yes
Tipo de autenticação	authby=rsasig, authby=secret
Status	auto=add, auto=start, auto=route
Aggressive Mode	aggrmode=yes, aggrmode=no

Sessões do Ipsec.conf

O arquivo ipsec.conf é dividido em algumas sessões, utilizadas para organizar e diferenciar os parâmetros de configuração (Alguns parâmetros só funcionam em uma sessão específica). São Elas:

Sessão Setup:

A sessão setup contém opções de inicialização do daemon, como por exemplo, qual interface utilizará para a vpn, opções de debug, nat-t, etc..

Exemplo:

```
config setup
    interfaces="ipsec0=eth0 ipsec1=eth1 ipsec2=ppp0"
    klipsdebug=none
    plutodebug=none
```

Sessão conn:

Nesta sessão constam os túneis VPN configurados, bem como algumas configurações Default.

conn %default é a conexão que pode ser criada para simplificar a configuração dos túneis, setando uma configuração padrão e que caso omitido algum parâmetro em uma conexão subsequente essa utilizará os parâmetros da conn %default

```
conn %default
    esp=3des:sha1
    ike=3des:sha1
    keylife=8h
    ikelifetime=3600
```

Polices

Além das configurações citadas acima existem as polices do ipsec, que são configurações adicionais que permitem refinar o controle efetuado através do ipsec.conf

são elas:

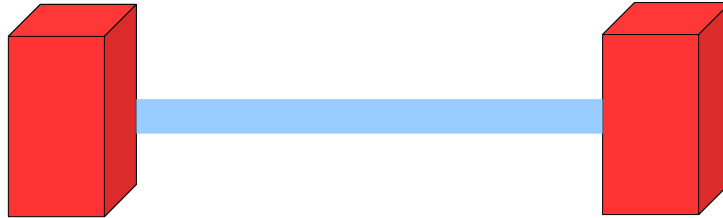
clear – Estipula ips/redes que não devem ser encriptados, como por exemplo os Servers root

clear-or-private private-or-clear private – Estipula conexões que não devem ser criptografadas, geralmente utilizado com opportunistic encryption devem

block – Estipula conexões que devem ser ignoradas pelo tunel vpn, caso algum ip ou rede não deva acessar ou ser acessado através da VPN

Exemplos de Configuração

Host-to-Host



Utilizado para comunicação entre dois hosts permitindo apenas o tráfego entre eles, caso seja necessário que outro equipamento seja acessado esse deve ser mascarado com o ip local do servidor (lan)

Exemplo de configuração:

<pre>conn matriz-filial auto=start type=tunnel authby=secret ike=3des-md5-modp1024 ikelifetime=3600 esp=3des-md5 keylife=28800 pfs=yes left=192.168.0.2 leftnexthop=192.168.0.1 right=192.168.1.2 rightnexthop=192.168.1.1</pre>	<pre>conn filial-matriz auto=start type=tunnel authby=secret ike=3des-md5-modp1024 ikelifetime=3600 esp=3des-md5 keylife=28800 pfs=yes left=192.168.1.2 leftnexthop=192.168.1.1 right=192.168.0.2 rightnexthop=192.168.0.1</pre>
--	--

Ipsec.secrets

192.168.0.2 192.168.1.2: PSK "ChavePSK"

192.168.1.2 192.168.0.2: PSK "ChavePSK"

Lan-to-lan



Utilizada quando existe q necessidade de comunicação entre as redes/hosts que estão conectadas ao gateway vpn, permitindo a comunicação somente das redes estipuladas

Exemplo de configuração:

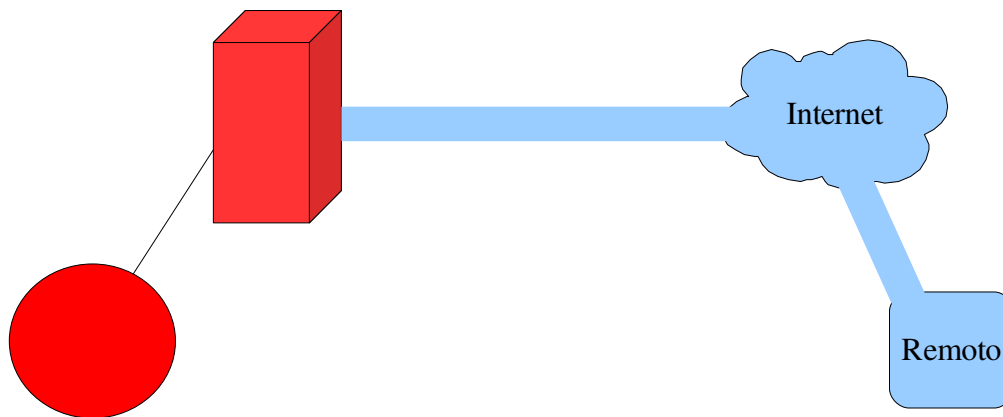
<pre>conn matriz-filial auto=start type=tunnel authby=secret ike=3des-md5-modp1024 ikelifetime=3600 esp=3des-md5 keylife=28800 pfs=yes left=192.168.0.2 leftnexthop=192.168.0.1 leftsubnet=172.16.0.0/24 right=192.168.1.2 rightnexthop=192.168.1.1 rightsubnet=172.16.1.0/24</pre>	<pre>conn filial-matriz auto=start type=tunnel authby=secret ike=3des-md5-modp1024 ikelifetime=3600 esp=3des-md5 keylife=28800 pfs=yes left=192.168.1.2 leftnexthop=192.168.1.1 leftsubnet=172.16.1.0/24 right=192.168.0.2 rightnexthop=192.168.0.1 rightsubnet=172.16.0.0/24</pre>
---	---

Ipsec.secrets

192.168.0.2 192.168.1.2: PSK "ChavePSK"

192.168.1.2 192.168.0.2: PSK "ChavePSK"

Road Warrior



Conexão sob demanda, o servidor fica apenas aguardando uma conexão, nunca a inicia e a ponta remota (uma conexão de ip dinâmico por exemplo) quem inicia essa conexão. (tambem pode ser utilizado caso uma das pontas não possua ip válido).

Exemplo de configuração

<pre>conn matriz-filial (IP Fixo) auto=add type=tunnel authby=secret ike=3des-md5-modp1024 ikelifetime=3600 esp=3des-md5 keylife=28800 pfs=yes left=192.168.0.2 leftnexthop=192.168.0.1 leftsubnet=172.16.0.0/24 right=%any rightnexthop= rightsubnet=172.16.1.0/24</pre>	<pre>conn filial-matriz auto=start type=tunnel authby=secret ike=3des-md5-modp1024 ikelifetime=3600 esp=3des-md5 keylife=28800 pfs=yes left=%defaultroute leftnexthop= leftsubnet=172.16.1.0/24 right=192.168.0.2 rightnexthop=192.168.0.1 rightsubnet=172.16.0.0/24</pre>
---	--

Ipsec.secrets

```
192.168.0.2 %any: PSK "ChavePSK"
```

```
%defaultroute 192.168.0.2: PSK "ChavePSK"
```

Por questões de segurança, evitar criar conexões RoadWarrior com chaves PSK, usar preferencialmente RSA, esse exemplo so deve ser utilizado caso o outro equipamento não tenha suporte a chaves RSA ou autenticação via Certificado.

Gerando uma nova chave RSA

```
#ipsec newhostkey --random /dev/urandom --bits 1024 --output teste.key
```

Com isso uma nova chave será gerada no arquivo teste.key, para a configuração do túnel será necessário utilizar a chave publica que fica contida no item pubkey= dentro do arquivo, exemplo:

```
[root@krl24 root]# cat /etc/ipsec.secrets
: RSA {
    # RSA 512 bits  krl24.rasputtin.com.br  Fri Sep 5 03:34:26 2008
    # for signatures only, UNSAFE FOR ENCRYPTION
    #pubkey=0sAQNiIX9nlTSJa4E6FtFzsYAAbS/eirIWMLGXi3WlbsgnOg14k46OmSCM7X
XscafV48osWnf21zwT9FsWRjov7ELx
    Modulus: 0x62897f679534896b813a16d173b180006d2fde8ab21
    PublicExponent: 0x03
    # everything after this point is secret
    PrivateExponent:
0x106c3fe698de16e740345922e89d95556787fa6c7303b2c843ec939b9276b134228aaf329fc1c1a928
    Prime1: 0xa8a0c82d68a4f57563b8f58416480d4850bee7bd8e84e4e48ac70433858d2b85
    Prime2: 0x9597b0316769a12097a8d98db40c2db2b2596684ef1100daddeff47acfa5e77d
    Exponent1: 0x706b301e45c34e4e427b4e580edab3858b29efd3b45898985c84ad77ae5e1d03
    Exponent2: 0x63ba757644f11615ba70910922b2c921cc3b99adf4b60091e94aa2fc8a6e9a53
    Coefficient: 0x6264d65f75462fbb72932173c6fd89bc0509e2e3dd40074337f76b37fc5797c5
}
```

esse é o conteúdo de um arquivo gerado pelo ipsec newhostkey, como demonstrado acima, o item pubkey deve ser utilizado para a configuração do tunel que sera descrita abaixo.

Utilizando chaves RSA

A configuração funciona em todos os ambientes citados anteriormente apenas alterando o parâmetro `authby=secret` para `authby=rsasig`, segue exemplo de configuração:

<pre>conn matriz-filial (IP Fixo) auto=start type=tunnel authby=secret ike=3des-md5-modp1024 ikelifetime=3600 esp=3des-md5 keylife=28800 pfs=yes left=192.168.0.2 leftnexthop=192.168.0.1 leftsubnet=172.16.0.0/24 leftrsasigkey=0sAQNiiX9nITSJa4E6FtFzs YAAbS/eirIWMLGXi3WlbsgnOg14k46OmSCM7X XscafV48osWnf21zwT9FsWRjov7ELx right=192.168.1.2 rightrightnexthop=192.168.1.1 rightsubnet=172.16.1.0/24 rightrsasigkey=0sAQNiasdghjjhewgfgdf ghghderw3746g542f323r3gbn467ukk5I80812 d124h6h6h6yuow4ggjjsstQWTQrt</pre>	<pre>conn filial-matriz auto=start type=tunnel authby=secret ike=3des-md5-modp1024 ikelifetime=3600 esp=3des-md5 keylife=28800 pfs=yes left=192.168.1.2 leftnexthop=192.168.1.1 leftsubnet=172.16.1.0/24 leftrsasigkey=0sAQNiasdghjjhewgfgdfg hghderw3746g542f323r3gbn467ukk5I80812d 124h6h6h6yuow4ggjjsstQWTQrt right=192.168.0.2 rightrightnexthop=192.168.0.1 rightsubnet=172.16.0.0/24 rightrsasigkey=0sAQNiiX9nITSJa4E6FtF zsYAAbS/eirIWMLGXi3WlbsgnOg14k46OmSCM 7XXscafV48osWnf21zwT9FsWRjov7ELx</pre>
--	--

Facilitando a configuração:

Em servidores com diversos túneis criados, existem algumas formas de poupar trabalho para o administrador, criando uma conn %default ou utilizando a opção also:

Utilizando conn %default

```
conn %default
    auto=start
    type=tunnel
    authby=secret
    ike=3des-md5-modp1024
    ikelifetime=3600
    esp=3des-md5
    keylife=28800
    pfs=yes
```

Com isso todas as outras conexões não precisam estipular esses valores, somente devem estipular caso necessitem alterá-los.

Utilizando o parametro also:

Com esse parâmetro é possível reutilizar um tunel já criado e setar apenas o que é necessário ser alterado, muito útil quando por exemplo uma das pontas possui duas, três, quatro redes atrás do gateway VPN

ex.:

```
conn matriz-filial
    auto=start
    type=tunnel
    authby=secret
    ike=3des-md5-modp1024
    ikelifetime=3600
    esp=3des-md5
    keylife=28800
    pfs=yes
    left=192.168.0.2
    leftnexthop=192.168.0.1
    leftsubnet=172.16.0.0/24
    right=192.168.1.2
    rightnexthop=192.168.1.1
    rightsubnet=172.16.1.0/24
```

```
conn matriz-filial2
    also=matriz-filial
    rightsubnet=172.16.2.0/24
```

Fontes:

Building and Integrating Virtual Private Networks with Openswan

Ken Bantoft, Paul Wouters

www.openswan.org

wiki.openswan.org

Felipe Santos – Rasputin

felipe.nix@gmail.com

www.rasputintech.blogspot.com

Openswan-BR

<http://br.groups.yahoo.com/group/openswan-br>