

## Configurando IPSec no PIX

Daniel B. Cid [daniel@underlinux.com.br](mailto:daniel@underlinux.com.br)  
<http://www.ossec.net>

No ultimo artigo nós cobrimos a configuração básica do PIX. Neste, para complementar as informações já passadas, iremos ensinar como configurar uma VPN (site-to-site), usando senhas pré-estabelecidas (pre-shared), entre essas duas redes (fictícias) definidas abaixo:

LAN1 - FW1 - INTERNET - FW2 - LAN2

LAN1: 10.0.0.0/24

LAN2: 10.0.1.0/24

FW1: (Inside IP: 10.0.0.1, Outside IP 200.1.1.1)

FW2: (Inside IP: 10.0.1.1, Outside IP 200.2.2.2)

A configuração será dividida em 4 passos:

**Passo 1: Preparando para a VPN**

**Passo 2: Configurando IKE**

**Passo 3: Configurando IPSec**

**Passo 4: Permitindo IPSec na rede**

**Passo 1:**

Antes de começar a configuração, voce deve determinar algumas coisas:

- Quais máquinas participarão da VPN?
- Quantos pontos terá a VPN?
- Quais "IKE policieis" serão usadas.

Nesse exemplo, nós usaremos:

Authentication: pre-shared  
Encryption: 3des  
DH group:2  
Hash:md5

Os pontos e as redes já foram ditas anteriormente.

## **Passo 2:**

A configuração do IKE precisa ser feita com todo o cuidado. Erre qualquer coisa nessa parte e a sua VPN não funcionará. Siga esses seis passos:

- 2.1 - Definindo o método de autenticação.
- 2.2 - Definindo o algoritmo de encriptação.
- 2.3 - Definindo o Diffie-Hellman Group.
- 2.4 - Definindo o algoritmo de HASH a ser usado.
- 2.5 - Iniciando o isakmp
- 2.6 - Selecionando a senha compartilhada.

FW1:

```
(2.1) isakmp policy 10 authentication pre-share  
(2.2) isakmp policy 10 encryption 3des  
(2.3) isakmp policy 10 group 2 (DH group)  
(2.4) isakmp policy 10 hash md5  
(2.5) isakmp enable outside  
(2.6) isakmp identify address  
(2.6) isakmp key 123mykey 200.2.2.2 netmask 255.255.255.255
```

FW2:

```
(2.1) isakmp policy 10 authentication pre-share  
(2.2) isakmp policy 10 encryption 3des  
(2.3) isakmp policy 10 group 2 (DH group)  
(2.4) isakmp policy 10 hash md5  
(2.5) isakmp enable outside  
(2.6) isakmp identify address  
(2.6) isakmp key 123mykey 200.1.1.1 netmask 255.255.255.255
```

Para verificar a sua configuração, use:

```
show isakmp
show isakmp policy
```

### **Passo 3:**

A configuração do IPSec será sub-dividida em outros seis passos para facilitar o entendimento:

- 3.1 - Criando a lista de acesso (que tráfego será encriptado).
- 3.2 - Configurando o transform-set (a combinação de algoritmos a serem usados).
- 3.3 - Setando o IPSec SA lifetime.
- 3.4 - Criando a crypto Map entry.
- 3.5 - Aplicando a crypto map na interface de rede.
- 3.6 - Excluindo tráfego da VPN do NAT.

FW1:

```
(3.1) access-list IPSEC permit ip 10.0.0.0 255.255.255.0
10.0.1.0 255.255.255.0
(3.2) crypto ipsec transform-set FW1set esp-3des esp-md5-
hmac
(3.3) crypto ipsec security-association lifetime seconds
600
(3.4) crypto map FW1 10 ipsec-isakmp
(3.4) crypto map FW1 10 match address IPSEC (the access-
list)
(3.4) crypto map FW1 10 set transform-set FW1set (the
transform-set)
(3.4) crypto map FW1 10 set peer 200.2.2.2 (the peer)
(3.5) crypto map FW1 interface outside (applies the crypto
map)
(3.6) nat (inside) 0 access-list IPSEC (the access-list)
```

FW2:

```
(3.1) access-list IPSEC permit ip 10.0.1.0 255.255.255.0
10.0.0.0 255.255.255.0
(3.2) crypto ipsec transform-set FW2set esp-3des esp-md5-
hmac
(3.3) crypto ipsec security-association lifetime seconds
600
```

```
(3.4) crypto map FW2 10 ipsec-isakmp
(3.4) crypto map FW2 10 match address IPSEC (name of the
access list)
(3.4) crypto map FW2 10 set transform-set FW1set (transform
set name)
(3.4) crypto map FW2 10 set peer 200.1.1.1 (the peer)
(3.5) crypto map FW2 interface outside (applies the crypto
map)
(3.6) nat (inside) 0 access-list IPSEC
```

#### **Passo 4:**

Para permitir que todos os pacotes vindo do túnel IPsec sejam autorizados, use:

```
sysopt connection permit-ipsec
```

Para verificar a sua configuração, use os seguintes comandos:

```
show crypto ipsec sa
```

Ou se voce quiser monitorar as negociações IPsec, use:

```
debug crypto isakmp
debug crypto ipsec
```

#### **Resumo das configurações:**

FW1:

```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 group 2
isakmp policy 10 hash md5
isakmp enable outside
isakmp identify address
isakmp key 123mykey 200.2.2.2 netmask 255.255.255.255
```

```
access-list IPSEC permit ip 10.0.0.0 255.255.255.0 10.0.1.0
255.255.255.0
crypto ipsec transform-set FW1set esp-3des esp-md5-hmac
crypto ipsec security-association lifetime seconds 600
crypto map FW1 10 ipsec-isakmp
crypto map FW1 10 match address IPSEC
crypto map FW1 10 set transform-set FW1set
crypto map FW1 10 set peer 200.2.2.2
crypto map FW1 interface outside
nat (inside) 0 access-list IPSEC
```

FW2:

```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 group 2
isakmp policy 10 hash md5
isakmp enable outside
isakmp identify address
isakmp key 123mykey 200.1.1.1 netmask 255.255.255.255
access-list IPSEC permit ip 10.0.1.0 255.255.255.0 10.0.0.0
255.255.255.0
crypto ipsec transform-set FW2set esp-3des esp-md5-hmac
crypto ipsec security-association lifetime seconds 600
crypto map FW2 10 ipsec-isakmp
crypto map FW2 10 match address IPSEC
crypto map FW2 10 set transform-set FW2set
crypto map FW2 10 set peer 200.1.1.1
crypto map FW2 interface outside
nat (inside) 0 access-list IPSEC
```