Configuring IPSec on PIX

Daniel B. Cid daniel@underlinux.com.br
http://www.ossec.net

In the last article, we covered the basic PIX configuration. In this one, we will talk about the setup of a VPN (site-to-site), using pre-shared keys, between the two networks defined bellow:

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)

The configuration will be completed in four steps:

Step 1: Preparing to the VPN

Step 2: Configuring IKE

Step 3: Configuring IPSec

Step 4: Allowing IPSec traffic

Step 1:

Before starting the hands on configuration, you need to determine some options that you will use:

-Which hosts will be in the VPN?
-How many peers will be.
-What IKE policies to use (like hash algorithm, DH group, etc).

In this example, we are going to use:

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

Step 2:

The IKE configuration needs to be very well done. If you
miss any step here, your VPN will not work.

2.1 – Specifying the peer authentication method (we are
going to use pre-shared, which requires a key to be
manually configured).
2.2 – Specifying the encryption algorithm (we will use
3DES).
2.3 – Specifying the Diffie-Hellman group.
2.4 – Specifying the hash algorithm.
2.5 – Enable isakmp
2.6 – Selecting the pre-shared key (123mykey).

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
```

To verify your configuration you can use

```
show isakmp
show isakmp policy
```

Step 3:

The IPSec configuration will be completed in six steps:

3.1 - Creating an access-list (to define which traffic to encrypt).
3.2 - Configuring the transform set (the combination of encryption algorithms).
3.3 - Configuring IPSec SA Lifetime.
3.4 - Creating a crypto Map Entry.
3.5 - Apply the crypto map set to an interface.
3.6 - Exclude VPN traffic from 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

Step 4:

sysopt connection permit-ipsec

This command permit all packets that arrive via the IPSec tunnel to pass between the firewall.

To view your configuration, you can use the following commands:

show crypto ipsec sa

Or if you want to watch your IPSec negotiation, use the debug command:

debug crypto isakmp
debug crypto ipsec

Configuration resume:

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
```