Cisco ASA (8.4) to PIX (6.x) Site to Site VPN example

Cisco ASA (8.4) to PIX (6.x) Site to Site VPN example

April 13, 2012 13 Comments

Here is a basic example of a site to site VPN between a Cisco ASA firewall running version 8.3 or higher, and a Cisco PIX firewall running version 6.x

Configuration for the Cisco ASA side of the connection:

Define network objects for your internal subnets:

```
object network Main-Office
subnet 192.168.1.0 255.255.255.0
```

```
object network Branch-Office
subnet 192.168.2.0 255.255.255.0
```

Create an access list for the VPN traffic using the network objects that you have created:

```
access-list VPN-to-Branch-Office extended permit ip object Main-Office object Branch-Office
```

Use double NAT (efficitively no nat) to ensure the traffic travelling across the VPN tunnel will not have NAT applied to it:

```
nat (inside,outside) source static Main-Office Main-Office destination static Branch-Office Branch-Office
```

Create a transform set using the encryption of your choice, in this case AES 128:

```
crypto ipsec ikev1 transform-set myset-aes128 esp-aes esp-sha-hmac
```

Ensure IKE version 1 is enabled on the outside interface:

```
crypto ikev1 enable outside
```

Create a policy for phase 1 of the VPN connection:

```
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 5
lifetime 86400
```

Configure a tunnel group containing the Pre Shared Key:

```
tunnel-group 172.16.0.2 type ipsec-l2l
tunnel-group 172.16.0.2 ipsec-attributes
ikev1 pre-shared-key My53cr3tPSK
```

Create a crypto map for phase 2 of the VPN connection:

```
crypto map myvpnmap 10 match address VPN-to-Branch-Office
crypto map myvpnmap 10 set pfs group5
crypto map myvpnmap 10 set peer 172.16.0.2          (This should be set to the ip of the outside interface of the
PIX you are connecting to)
crypto map myvpnmap 10 set ikev1 transform-set myset-aes128
crypto map myvpnmap interface outside
```

Configuration for the Cisco PIX side of the connection:

Configure an access list for the VPN tunnel:

```
access-list 100 permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
```

Make sure NAT is not applied to traffic passing across the VPN tunnel:

```
nat (inside) 0 access-list 100
```

Configure the PIX to permit IPSEC:

```
sysopt connection permit-ipsec
```

Create a policy for phase 1 of the VPN connection:

```
isakmp enable outside
```

```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
```

Configure keepalives to match the default setting on the ASA of 10 seconds retry 2 seconds:

```
isakmp keepalive 10
```

Create a transform set to match the ASA end of the connection, in this case AES 128:

```
crypto ipsec transform-set myset-aes128 esp-aes esp-sha-hmac
```

Create a crypto map for phase 2 of the VPN connection:

```
crypto map myvpnmap 10 ipsec-isakmp
crypto map myvpnmap 10 match address 100
crypto map myvpnmap 10 set pfs group5
crypto map myvpnmap 10 set peer 172.168.0.1
```

(This should be set to the ip of the outside interface of the ASA you are connecting to)

```
crypto map myvpnmap 10 set transform-set myset-aes128
crypto map myvpnmap interface outside
```

Configure the Pre Shared Key to match the other end of the connection

```
isakmp key My53cr3tPSK address 172.16.0.1 netmask 255.255.255.255 no-xauth no-config-mode
```