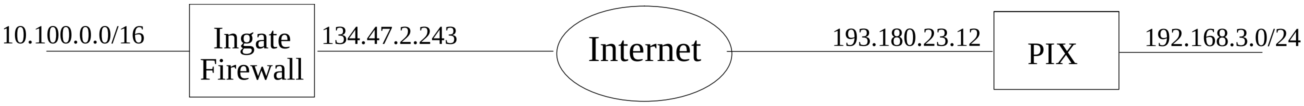
Configuration of VPN between Ingate Firewall and Cisco PIX

Tested versions: Ingate Firewall 2.6.0
Cisco PIX version 5.3(1), 3DES activated

1. Configuration

In this scenario, preshared secret is used.

The network is described in the picture below.



2. Configuration of Ingate Firewall

This is a quick guide to configuring VPN. For more information, read the chapter Virtual Private Networks in the User Manual..

- Press the Virtual Private Networks button in the web interface and create a new row for the PIX. Select 134.47.2.243 as the **Local side** and 193.180.23.12 as the **Remote side**. Select **Preshared secret** as the **Authentication type** and enter the shared secret after pressing the button in the **Authentication info** column. Make the connection **Active** under **On/Off** and set the **Lifetime of ISAKMP keys** to 3600 seconds.
- Go to the **Tunneled networks** page. Create a new row for the computers which will use the VPN tunnel and select the PIX under **Peer**. Enter the network number 10.100.0.0 with the netmask 16 under **Local side of network**. Enter the network number 192.168.3.0 with the netmask 24 under **Remote side of network** and set the **Lifetime of IPSec keys** to 28800 seconds.
- Press the **Firewall rules** button and go to the **Networks and Computers** page. Create a new network with 192.168.3.0 as the **Lower limit** and 192.168.3.255 as the **Upper limit**. Select '-' as the **Interface**. You should already have a network for your local computer network (10.100.0.0-10.100.255.255).
- Go to the **Rules** page and make new rules for the VPN traffic. If a rule is made for traffic from the PIX network to the local network, the PIX VPN peer should be selected under **From VPN**. If a rule is made for traffic from the local network to the PIX network, the PIX VPN peer should be selected under **To VPN**.. All other settings are made just as for normal firewall rules.
- Go to the **Save/Load configuration** page under **Administration** to apply all new settings.

3. Configuration of Cisco PIX

Below, some PIX configuration is extracted, with references to corresponding configuration in Ingate Firewall.

```
ip address outside 193.180.23.12 255.255.255.192
ip address inside 192.168.3.1 255.255.255.0
```

```
access-list 101 permit ip 192.168.3.0 255.255.255.0 10.100.0.0 255.255.0.0
```

*This corresponds to a row on the **Tunneled networks** page in Ingate Firewall*

```
crypto ipsec transform-set ingate esp-3des esp-sha-hmac
crypto map mymap 10 ipsec-isakmp
crypto map mymap 10 match address 101
```

Connects these settings to the access-list 101 which describes the tunneled networks.

```
crypto map mymap 10 set pfs group2
```

Select one of group2 and group5.

```
crypto map mymap 10 set peer 134.47.2.243
```

*This corresponds to **Local side** on the **VPN peers** page in Ingate Firewall.*

```
crypto map mymap interface outside
```

*The outside interface has the IP address chosen as **Remote side** on the **VPN peers** page in Ingate Firewall.*

```
isakmp enable outside
isakmp key S0DwILgKOxmD5D7hwsbP30H3uTImFmU33UphIkY30 address 134.47.2.243
```

The long string after key is the shared secret also entered in Ingate Firewall. 134.47.2.243 is the ***Local side*** *in Ingate Firewall.*

```
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash sha
isakmp policy 20 group2
```

group5 could also be used, but you have to use the same as was selected for crypto map above.

```
isakmp policy 20 lifetime 3600
```

3600 seconds is the same as for ***Lifetime for ISAKMP keys*** *on the* ***VPN peers*** *page.*