IPCop v1.2.0 VPN Howto

Eric S. Johansson

Darren Critchley

IPCop v1.2.0 VPN Howto

by Eric S. Johansson and Darren Critchley

Published 2003

Revision History

Revision 1.0 04 Jan 2002 Revised by: esj
Original version.
Revision 1.1 30 Dec 2002 Revised by: dc
Add Windows to IPCop chapter
Revision 1.2 10 Jan 2003 Revised by: hg
Conversion to DocBook XML

Table of Contents

Introduction

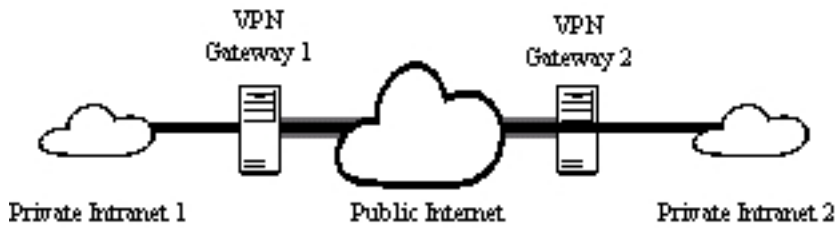
The VPN implementation used by IPCop is an IPSec standard VPN. It is also a very simple manually keyed system. This works reasonably well in small scale installations but does require an amount of discipline to manually change keys on a regular basis.

As it is currently implemented, the IPCop VPN environment is not suited for large-scale or road warrior use. It requires some changes in order to handle medium or large-scale VPN configurations as well as road warrior support.

However, these shortcomings do not stop the IPCop environment from being useful for small-scale VPN deployments between regional offices over DSL or leased lines.

Chapter 1. Basic Concepts

The concept of a VPN is very simple. It is a protected communication channel over an unprotected public thoroughfare. It is analogous to an armored vehicle traveling over public roads. At the top-level, a VPN consists of a small number of components, illustrated below:



In this diagram, there are two private Intranets connected via the VPN. The VPN is created by the two VPN Gateways over the public Internet.

A VPN works by encapsulating data for one network inside of an ordinary IP packet and transporting that packet to another network. When the packet arrives at the destination network, it is unwrapped and delivered to the appropriate host on the destination network. By encapsulating the data using cryptographic techniques, the data is protected from tampering and snooping while it is transported over the public network.

Unfortunately, this same protection against tampering makes it difficult to set up a VPN when the security perimeter is protected by an address translation firewall such as IPCop. The solution is to implement the VPN on the firewall and allow it to straddle both sides so that it can capture packets from the GREEN network and pass them, encapsulated, over the Internet without being tampered with by the address translation part of the firewall.

Chapter 2. Implementation Essential Details

When setting up the VPN, there are a few things that must be in place before the VPN can operate correctly. Those things are:

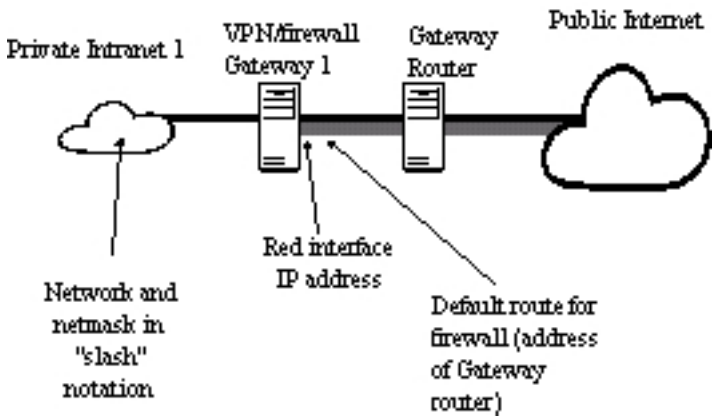
- Good connectivity between the two IPCop boxes (low packet loss).
- All VPN connected networks are in separate, non-overlapping IP address spaces.
- Routing must be properly set up to accommodate the VPN.
- Information has been collected accurately about each end of the VPN.

Good connectivity is extremely important because if there is high packet loss or latency, it will be reflected in the VPN's performance. The VPN is extremely persistent in trying to maintain a connection and re-establish any connections that may get broken but it can't work miracles when the network over which it travels is broken. One can test the connectivity by a combination of **ping** and **traceroute**. **Ping** should show low packet loss and **traceroute** should show reliable routing.

It's essential that every network joined by the VPN has independent, non-overlapping IP address spaces. For example, if one network is 192.168.0.0/24 and the other network is 192.168.0.128/25, the VPN connection will not work. However, if the other network was 192.1 68.1.0/25, the VPN would work because the address ranges do not overlap.

Routing is another source of errors when setting up a VPN. It's important for all hosts that must communicate across the VPN to be configured so that the VPN specific routes are known and handled properly. A common way to deal with this is to use a router as the default gateway and reroute traffic as appropriate from that router. The primary advantage of this technique is that routes are controlled in one place. The disadvantage is that in a non-switched network, there can be some additional network congestion and that the router is a single point of failure. If there is no internal router pre-existing, the IPCop machine will usually be the network's default route and can be used as a general router.

In order to turn on the VPN on an IPCop firewall, there are three essential bits of information that must be collected from each side of the VPN (shown below).



The three bits of information are the: firewall's RED interface IP address, the default route for the firewall, and the network and net mask of the VPN connected network (usually GREEN network). This information can be extracted from a running firewall using two commands. One can extract the network and net mask information using the **ifconfig**. For example, on the Internet Guide Service firewall, eth1 is the RED interface:

```
root@ipcop:~ # ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:48:54:8F:3C:66
```

```
          inet addr:68.5.12.246(1)  Bcast:68.5.15.255  Mask:255.255.252.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:4715621 errors:0 dropped:0 overruns:0 frame:0
          TX packets:397580 errors:0 dropped:0 overruns:0 carrier:0
          collisions:34857 txqueuelen:100
          RX bytes:814964446 (777.2 Mb)  TX bytes:59306224 (56.5 Mb)
          Interrupt:11 Base address:0xc000

root@ipcop:~ #
```

(1) The IP address of the RED interface.

To get the rest of the information, we use the **netstat -rn** command as shown in the box below.

```
root@ipcop:~ # netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.0(1)   0.0.0.0         255.255.255.0(2) U         0 0          0 eth0
68.5.12.0       0.0.0.0         255.255.252.0   U         0 0          0 eth1
0.0.0.0         68.5.12.1(3)     0.0.0.0         UG        0 0          0 eth1

root@ipcop:~ #
```

(1) Network for the GREEN interface.

(2) Net mask for the GREEN network.

(3) Default gateway for the firewall.

Unfortunately, the net mask, above, is in the wrong form. Instead of dotted notation, the netmask must be in “slash notation”. In this case, slash notation would be “/24”. The table below provides a conversion between slash notation and dotted notation netmask.

Table 2-1. Network Masks

bitlength	netmasks	IPs usable
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2
/31	255.255.255.254	0 (point-to-point)
/32	255.255.255.255	0 (single-host netmask)

Once this information has been gathered for both sides of the VPN, then one can configure the firewall and activate the VPN. A VPN data worksheet is provided as part of this document to help organize the information collection process.

The IPCop VPN is a manually keyed system. This means that you must use a single shared secret for all VPN nodes, which becomes the key for encrypting all traffic. Keys must be changed regularly and hidden from view so that it would be difficult

if not impossible for someone to tap the VPN. Future versions will replace manual keying with automatic keying and RSA based authentication.

Manually keyed systems should use relatively long random bit strings. A simple technique for generating keys would be to take the output of **ps -aux** passed through **md5sum**. This is still a very weak method of generating a manual key but it's far stronger than usual human generated passwords. Generate the key, record it somewhere safe and don't lose it until you've replaced it.

Chapter 3. IPCop VPN Details

Before activating the VPN:

Start with a 1.2.0 IPCop firewall. This procedure may not work with any other revision.

Verify you can **ping** and **traceroute** from the GREEN network host to the remote firewall. *Do not* proceed any further if you cannot reach the other the firewall by **ping** and **traceroute**.

Setting up the VPN:

- Point your Web browser to your IPCop firewall.
- Click on the left hand margin menu button labeled *VPN*
- Login using the user ID "admin" and your administrator password. At this point, you should be looking at the VPN administration web page. In most circumstances, the global settings should be left blank and unchecked. If you have not created any VPNs, the manual control and status section should be empty as well.
- Click on the tab labeled *connections* at the top of the VPN administration page.
- Fill in the values for the *connection name* and the *left* and *right* hand networks.
- Fill in the *secret* field from the generated secret pass phrase.
- Click **add**

At this point, all the data you entered should be visible in the *current connections* section of the page. Verify that you entered all data correctly and then repeat the above steps on the other end of the VPN. Once both ends of the VPN have been filled with identical data, activate the connections:

- Click the tab labeled *control* at the top of the VPN administration page.
- Click the **restart** button.

Verifying

Verifying that the VPN is up is fairly easy. The first test is to try and **ping** a system on the remote end using its real IP address. If that doesn't work, you'll need to run the **netstat** command and verify that the VPN has been activated and entered routes to the other end of the VPN. You should see something like the following:

```
root@ipcop:~ # netstat -nr
Kernel IP routing table
Destination     Gateway     Genmask         Flags   MSS Window  irtt Iface
192.168.2.0     68.5.12.1   255.255.255.0   UG        0 0          0 ipsec0(1)
192.168.0.0     0.0.0.0     255.255.255.0   U         0 0          0 eth0
68.5.12.0       0.0.0.0     255.255.252.0   U         0 0          0 eth1
68.5.12.0       0.0.0.0     255.255.252.0   U         0 0          0 ipsec0(2)
0.0.0.0         68.5.12.1   0.0.0.0         UG        0 0          0 eth1

root@ipcop:~ #
```

(1)(2) Routes on ipsec0.

Notice the two routes on interface ipsec0. Both of them will be there if the VPN is up and running. If they are not there, then something is wrong with the parameters entered into the VPN configuration or the network between the two firewalls.

Worksheet

Note: it does not matter which system is considered left or right. Pick a convention for which system is left and which system is right and stick to that convention. You pick to be the left or right side system must be that system on both ends of the VPN.

Note: Don't guess! Verify parameters on each firewall using the techniques described earlier. Incorrect values can cause hours of debugging fun.

Connection Name _____

Left-hand VPN parameters:

RED Network IP address: _____(left)

Firewall Gateway Address: _____(left next hop)

VPN connected network/netmask: _____(left subnet)

Right-hand VPN parameters:

RED Network IP address: _____(right)

Firewall Gateway Address: _____(right next hop)

VPN connected network/netmask: _____(right subnet)

Chapter 4. Connecting With Win2k or XP Using Their Built In IPSec

> **Note:** if your RED IP address changes like the weather, you will have to register your IPCop with one of the dynamic DNS services such as dyndns.org. Also note that this cannot be done through the IPCop Web interface, it must be done from a command line, and if you use the connections page of the web interface, it will wipe out all your settings.

Connecting a Win2K/XP box to an IPCop using the built in IPSec of Win2k Pro/XP is accomplished in about ten minutes. While not tested, the same should work for a Windows XP box.

> **Note:** You will have to edit the `ipsec.conf` and `ipsec.secrets` which are both placed in the `/var/ipcop/vpn` directory on your IPCop machine.

In my situation, I have a Win2K box behind an Assante Cable/DSL router connected to a cable modem. The IPCop box protects a private network with a subnet of 192.168.1.x and I am running a subnet of 192.168.10.x at my end. You need different subnets at each end otherwise the routing will not behave properly. By this I mean that you could not setup the network behind the IPCop to be 192.168.1.x and then have your road warrior be 192.168.1.x, it would have to be 192.168.2.x or some other private IP address. In the logging examples, you will see 255.255.255.255 as an IP address. This is a fictional address for this example. My particular machine is 192.168.10.159 and you will see that entered in the conf files, etc. And the IPCop box is 192.168.1.254. Again you will see this in the logs, etc.

> **Note:** My Win2K machine is a different subnet to the IPCop machine.

Now on to the good stuff! First, make sure your Win2K box is ready to do the job, Service Pack 2 must be installed or at least the high encryption pack, it installs 3DES which is needed by IPCop. This is not necessary for XP as it contains 3DES already.

For Windows 2000, get the IPSec policy editor[1].

For Windows XP you will need the **Ipseccmd** program: You have to install the Win XP Support tools. They reside on your Win XP CD in the directory `\SUPPORT\TOOLS`. Just start **setup.exe** in this directory. You have to select a "Complete installation" to get **ipseccmd**.

Next download this utility:[2] and extract the contents to the same place that the `IPSECPOL.EXE` for Win2k was installed to (typically `c:\Program Files\Resource Kit\`) or where **Ipseccmd.exe** was installed to for Windows XP.

Also to make sure you know what is going on with the IPCop box. Download and install **PuTTY** or some other Secure Shell. **PuTTY** is free and can be downloaded from here[3].

Make sure you turn on SSH on your IPCop box so that **Putty** or another Secure Shell can access the command line.

Now, you need to setup the `ipsec.conf` on both IPCop and the Win2k/XP machine. Here's a sample one for IPCop:

```
conn roadwarrior
    compress=no
    left=(RED address or dynamic dns name)
```

```
    leftsubnet=192.168.1.0/24                          (1)
    leftnexthop=%defaultroute
    type=tunnel
    authby=secret
    pfs=yes
    right=%any
    rightsubnet=192.168.10.159/32                      (2)
    rightnexthop=%defaultroute
    auto=add
```

(1) Subnet behind IPCop

(2) If you are behind a firewall or other router put private address here otherwise leave blank

In the ipsec.secrets on the IPCop file make sure you have:

```
(RED address or dynamic dns) 0.0.0.0 : PSK “PreShared secret here”
(RED address or dynamic dns) %any : PSK “PreShared secret here”
```

Now for the Win2k setup.

> **Warning**
>
> The `ipsec.conf` file that was downloaded, above, needs to be edited now. You will find that it already comes with sample connections inside of it. Erase all of these and replace them with a modified copy of the example, below. Change the connection name and IP addresses.

Here is a sample of a Win2K or XP ipsec.conf file:

```
conn KDI
    left=(RED address of ipcop or dynamic dns name of ipcop)
    leftsubnet=192.168.1.0/24                          (1)
    right=%any
    presharedkey=PreShared secret here
    network=auto
    auto=start
    pfs=yes
```

(1) Subnet behind IPCop

Now, from a DOS box, change directories to where the `IPSECPOL.EXE` was installed to (typically `c:\Program Files\Resource Kit\`) and then type **IPSEC.EXE** and that will initiate the IPSec connection. It took me two attempts to get this working, but it works and works well if all is configured properly. You should see this from Windows 2K:

```
    C:\Program Files\Resource Kit>ipsec.exe
IPSec Version 2.1.4 (c) 2001,2002 Marcus Mueller
Getting running Config ...
Microsoft’s Windows 2000 identified
Host name is: darrenc
No RAS connections found.
LAN IP address: 192.168.10.159
Setting up IPSec ...

        Deactivating old policy...
        Removing old policy...

Connection KDI:
```

```
        MyTunnel     : 192.168.10.159
        MyNet        : 192.168.10.159/255.255.255.255
        PartnerTunnel: (RED IPCOP address or Dyn DNS Name)
        PartnerNet   : 192.168.1.0/255.255.255.0
        CA (ID)      : Preshared Key ******************
        PFS          : y
        Auto         : start
        Auth.Mode    : MD5
        Rekeying     : 3600S/50000K
        Activating policy...

C:\Program Files\Resource Kit>
```

Next from the Win2K box **ping** the GREEN IP Address of the IPCop box, after a couple of pings, it should get a reply. (Takes two tries with my setup, I have heard of it taking four or five) To ping type the following:

```
C:\>ping 192.168.1.254                          (1)


Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=51ms TTL=255
Reply from 192.168.1.254: bytes=32 time=60ms TTL=255
Reply from 192.168.1.254: bytes=32 time=50ms TTL=255
Reply from 192.168.1.254: bytes=32 time=50ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum =  60ms, Average =  52ms
```

(1) GREEN address of IPCop

Ideally to make sure things are going as planned, have a putty (SSH - Secure Shell) session running to your IPCop box so you can examine `/var/log/secure`. For more information on SSH and how to set it up, look in the IPCopFAQ for How do I turn on SSH[4].

As for the IPCop log it should show something like the following:

```
root@ipcop:~ # cat /var/log/secure
...#5: responding to Main Mode from unknown peer 255.255.255.255
...#3: Peer ID is ID_IPV4_ADDR: '192.168.10.159'
...#3: sent MR3, ISAKMP SA established
...#6: responding to Quick Mode
...#6: IPsec SA established

root@ipcop:~ #
```

The above log can also show you what went wrong, or at least the vital information to post to the list to show us what went wrong so we can help you correct it.

If you fail to connect on the first attempt or try to reconnect after the connection goes idle, I have found that I have to restart the VPN on both ends, on the win2k box type

```
C:\>ipsec -off
```

Then on the IPCop, use the web interface to restart the VPN. Now start the Win2K IPSec again.

Now you know how to connect a Win2K box to an IPCop using the built in IPSec of Win2K.

Notes

1. http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp
2. http://vpn.ebootis.de/package.zip
3. http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
4. http://ipcop.sourceforge.net/cgi-bin/twiki/view/IPCop/IPCopFAQ#How_do_I_turn_on_SSH_