

Troubleshooting IPCOP IPSEC VPN Connections
By Todd Hampson Nov 2005

V1.02

The first place to look when trying to troubleshoot a IPSEC VPN connection is the IPSEC System Log. You can access this by selecting Logs then System Logs. From the Section pull down menu, select IPSEC then click update.



The log will provide finer details of what is going on with IPSEC. Based on the error messages or information in the log you can then try to resolve issues that may be keeping the vpn connection from establishing.

The following section outlines some of the common errors and things to try to resolve them

Firstly if you are getting something like this

```
22:49:46 pluto[585] "abc" #624: sent MR3, ISAKMP SA established
22:49:46 pluto[585] "abc" #624: transition from state STATE_MAIN_R2 to
state STATE_MAIN_R3
22:49:46 pluto[585] "abc" #624: Main mode peer ID is ID_IPV4_ADDR:
'202.45.115.18'
22:49:46 pluto[585] "abc" #624: transition from state STATE_MAIN_R1 to
state STATE_MAIN_R2
22:49:46 pluto[585] "abc" #624: NAT-Traversal: Result using draft-ietf-
ipsec-nat-t-ike-02/03: no NAT detected
22:49:46 pluto[585] "abc" #624: transition from state (null) to state
STATE_MAIN_R1
22:49:46 pluto[585] "abc" #624: responding to Main Mode
```

Then things should be fine and your connection should be up, this is what you should keep seeing every time a key exchange happens. This should happen about every 45 to 60

minutes. You should also see a green OPEN box in the status section of the VPN menu to illustrate that the vpn “abc” is up.

However if you are not seeing this then its time to analyse the IPSEC log to see whats going on and what needs to be fixed.

Common Error 1

```
23:58:40 pluto[14958] packet from X.X.X.X:500: initial Main Mode message
received on X.X.X.X:500 but no connection has been authorized with
policy=PSK
```

This is a very common error and will cause the vpn not to come up. This basically means that this end of the vpn (where the log is) has received a request to handshake an ipsec vpn connection, but as far as this end of the link is concerned its not expecting a vpn connection from the ip address x.x.x.x and so ignores it.

If the ip address is the one you are expecting it from then you should check the ipsec.conf file and the ipsec.secrets file.

```
/etc/ipsec.conf

config setup

interfaces=%defaultroute

klipsdebug=none

plutodebug=none

plutoload=%search

plutostart=%search

uniqueids=yes

nat_traversal=yes

virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,%v4:192.168.0.0/16,%v4:!1
92.168.2.0/255.255.255.0,%v4:!10.11.100.0/255.255.255.0,%v4:!192.168.4.0/2
55.255.255.0,%v4:!192.168.3.0/255.255.255.0,%v4:!192.168.0.0/255.255.255.0
```

```
conn %default

keyingtries=0

disablearrivalcheck=no

conn abc

left=1.2.3.4

leftnexthop=%defaultroute

leftsubnet=192.168.2.0/255.255.255.0

right=5.6.7.8

rightsubnet=192.168.3.0/255.255.255.0

rightnexthop=%defaultroute

dpddelay=30

dpdtimeout=120

dpdaction=hold

authby=secret

auto=start
```

```
/etc/ipsec.secrets
```

```
: RSA /var/ipcop/certs/hostkey.pem
```

```
1.2.3.4 5.6.7.8 : PSK "yoursecretpasswd"
```

make sure that the ip addresses of the left side (near end) and right side (far end) match in the ipsec.conf section as well as in the ipsec.secrets section. If they don't you will get this error. If you are using a FQDN such as firewall.yourcompany.com, make sure the firewall itself can resolve the name. Easiest way to do this is to ping it. See if the firewall resolves the FQDN to an ip address.

If it resolves and you are still getting the error, try to put in the actual ip addresses to reduce the problem of dns lookups from the problem solving equation, once you find out what the problem is you can always put it back.

Alternate Solution to Common Error 1 – submitted by Charles Trevor

The error discussed is can also be indicative of the remote end being natted.

This error most commonly occurs when the remote side of the connection is behind a NAT device such as a router. In this case the remote device

or IPCOP trying to connect will have a private ip address different than the public ip address that has been configured for it in the IPCop VPN

GUI.

To resolve this the private IP address used needs to be added to both ipsec.conf and ipsec.secrets. In the example below the private IP used

is 192.168.0.2 and has been added in the form rightid=192.168.0.2 to the con abc section of ipsec.conf and directly into ipsec.secrets.

```
/etc/ipsec.conf
```

```
config setup
```

```
    interfaces=%defaultroute
```

```
    klipsdebug=none
```

```
    plutodebug=none
```

```
    plutoload=%search
```

```
    plutostart=%search
```

```
    uniqueids=yes
```

```
    nat_traversal=yes
```

```
virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,%v4:192.168.0.0/16,%
```

```
v4:!192.168.2.0/255.255.255.0,%v4:!10.11.100.0/255.255.255.0,%v4:!
```

```
192.168.4.0/255.255.255.0,%v4:!192.168.3.0/255.255.255.0,%v4:!
```

192.168.0.0/255.255.255.0

conn %default

keyingtries=0

disablearrivalcheck=no

conn abc

left=1.2.3.4

leftnexthop=%defaultroute

leftsubnet=192.168.2.0/255.255.255.0

right=5.6.7.8

rightid=192.168.0.2 #####Change to the private IP of your Natted device!!

rightsubnet=192.168.3.0/255.255.255.0

rightnexthop=%defaultroute

dpddelay=30

dpdtimeout=120

dpdaction=hold

authby=secret

auto=start

/etc/ipsec.secrets

: RSA /var/ipcop/certs/hostkey.pem

1.2.3.4 5.6.7.8 192.168.0.2 : PSK "yoursecretpasswd"

Common Error 2

```
23:58:40 "abc" #1: initiating Main Mode
23:58:40 "abc" #1: STATE_MAIN_I1: initiate
23:58:40 "abc" #1: STATE_MAIN_I1: retransmission; will wait 20s for
response
23:59:00 "abc" #1: STATE_MAIN_I1: retransmission; will wait 40s for
response
23:59:20 "abc" #1: max number of retransmissions (2) reached
STATE_MAIN_I1.
23:59:20 No acceptable response to our first IKE message
```

What is happening here is that this end of the link is trying to establish a connection but the other end is not accepting or seeing the request and its timing out. This could be a number of things.

First ensure the simple things are working. Make sure the routing is correct between both firewalls. You can try pinging each firewall from the other firewall, ie: ssh to the first firewall and ping the RED interface of then other. Then ssh to the other firewall and ping the RED interface of the first one. If the external routing is correct then you should be able to ping each RED interface from either end successfully.

Next is check that the firewall is actually receiving the request. ie: if 1.2.3.4 is sending the request (the one that has this error), then ssh to the other firewall and issue the command

```
tcpdump -i eth1
```

This assumes that eth1 is your RED interface. IF your not sure check the STATUS the NETWORK STATUS from the web interface. This will list your interfaces and the one that is in red text will be your RED interface, if its eth1 then use this above in the tcpdump command, if its eth0 or any other Ethernet interface use that.

When tcpdump is running it will display each of the packets leaving or entering the red interface of that firewall. If there is a lot of traffic you can filter this out and only get packets from the other firewall. Use

```
tcpdump host 5.6.7.8
```

Also as IKE uses UDP port 500 you can just filter on that if you wish

```
tcpdump host 5.6.7.8 and udp port 500
```

doesn't matter which tcpdump command you use, set it running in a ssh window then go back to the web interface of the firewall with this error message and hit the restart button. It's the one that looks like a circle with an arrow on it



As soon as you click that restart you should start to see packets on the other firewall as the first one try's to start the connection. If you don't see anything, and you continue to get this message (and your pings worked successfully before) then there is something blocking the IKE requests.

If you are getting packets then at least you know the requests are getting to the other firewall. Time to look at what could be blocking it

You need to make sure the far end firewall (not the one with the message) is not blocking IKE. IKE uses UDP port 500. You can issue the iptables list command to see all the iptables rules

```
/sbin/iptables -L
```

will list all your active rules. If they flash through too fast (and they will there are a lot of them) use the

```
/sbin/iptables -L | more
```

command and it will pause every full screen. If you want to save this dump to a file you can do so and look through it at your leisure

```
/sbin/iptables -L > /root/myiptablesrules.txt
```

If you see something like this

```
DROP upd -- anywhere 5.6.7.8 upd dpt:500
```

Then that your problem, go into `/etc/rc.d/firewall.local` and check that this rule has not been put in there. You can also check `/etc/rc.d/rc.firewall`, but it won't be there by default, someone would have had to put it there.

If you don't have that rule, check if the kernel is dropping packets on your RED interface (eth1) by going to the network STATUS then NETWORK STATUS of the remote firewall and check under the section where the RED interface is, look at the statistics errors, dropped, overruns and frame.

The screenshot shows the Mikrotik WinBox interface with the 'NETWORK STATUS' tab selected. The top navigation bar includes 'SYSTEM', 'STATUS', 'NETWORK', 'SERVICES', 'FIREWALL', 'VPNS', and 'LOGS'. Below the navigation bar, there are links for 'Interfaces:', 'Routing Table Entries:', and 'ARP Table Entries:'. The main content area displays the configuration and statistics for two interfaces: eth0 and eth1.

```

eth0      Link encap:Ethernet  HWaddr 00:50:BF:13:C2:2B
            inet addr:          Bcast:          Mask:
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:4158510 errors:43 dropped:0 overruns:0 frame:43
            TX packets:4324111 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1465435314 (1397.5 Mb)  TX bytes:1987686133 (1895.6 Mb)
            Interrupt:9 Base address:0xf400

eth1      Link encap:Ethernet  HWaddr 00:50:BF:13:BB:D1
            inet addr:          Bcast:          Mask:
            UP BROADCAST RUNNING  MTU:1500  Metric:1
            RX packets:4418419 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4092810 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:2102180419 (2004.7 Mb)  TX bytes:1542885959 (1471.4 Mb)
            Interrupt:3 Base address:0xf800
  
```

(Note my personal ip address information has been deleted for my own security)

They should be 0 or a very small number, if they are large (ie anywhere near 1% of the total or above) then there may be the problem, also, see if they increment after you try another restart of the vpn. You can use the

`ifconfig eth1`

command from the command line to get this same information

If your machine is dropping packets it could be a faulty network card. If there is a lot of them consider replacing it.

Common Error 3:

```
23:09:48 pluto[585] packet from X.X.X.X:500: ignoring Vendor ID payload  
[draft-ietf-ipsec-nat-t-ike-00]
```

This error is the other end of the vpn connection trying to do a main mode rekey behind a NAT-ed connection. The problem will seem to occur in NAT-ed setups when the VPN gateway which is usually the responder during IKE main mode,

suddenly takes the initiative and starts actively renegotiating Phase1 of the tunnel.

You may also see this in roadwarrior connections where the roadwarrior is NATed but the source port is still 500. This is often due to IPSec-Passthrough functionality and the NAT device drops every packet it can't understand (especially ESPinUDP packet). For roadwarriors Disable IPSec passthru support on their NAT box and this error should stop.

Some users have reported success by dropping the MTU size on the roadwarrior to 1432.

I have seen this message whilst the vpn stays up and stable as long as 1 end is controlling the rekeying.

Other Useful Tools to help diagnose a problem

This is a list of tools you can run from the command line to help you diagnose a problem

ping a.b.c.d

this will let you check connectivity to another device with ip a.b.c.d

traceroute a.b.c.d

this command will let you see the routers that your packets traverse and the response times to get to your destination

/sbin/iptables -L

this command lists your firewall active rules

tcpdump -i eth0

this command will let you see all packets coming into or out of a network interface, work on ipsec interfaces as well. Many filter options available

tail -n x /var/log/messages

will display the last x lines of the system log.

ipsec auto --status

This command to get status report from running system. Displays Pluto's state. It Includes the list of connections which are currently "added" to Pluto's internal database; lists state objects reflecting ISAKMP and IPsec SAs being negotiated or installed.

ipsec look

This command provides brief ipsec status information

ipsec barf

This command provides copious amounts of debugging info for ipsec.

netstat -rn

This command displays your current routing table (in memory)

netstat -an

This command displays your current active ports and their state. Ie: If your firewall is listening on a certain port or connected on a certain port