

## NIR\_083: IPsec Error Messages and Troubleshooting in the Netopia

Written by: Patrick Karpinskas

Date: 06/16/03

This Technote refers to troubleshooting **IPsec** traffic failure through Netopia routers, and is relevant only for **IKE tunnels**. This document is NOT applicable to **IPsec Manual Key** tunnels. This troubleshooting is facilitated by the interpretation of certain error messages that are produced when anomalous behavior is present. Router to router IPsec VPN technotes can be found in [Netopia VPN Quick Guides](#).

---

**PLEASE NOTE:** VPN services to or from routers with **non-routable WAN addresses** are **not** supported by Netopia Technical Support. The National Internet Commission (**NIC**) unroutable address spaces are defined as the following:

- **10.x.x.x**
- **172.16.x.x-172.31.x.x**
- **192.168.x.x**

Even though it may be possible through experimentation to effect VPN functionality in the case of a non-routable WAN address, Netopia Technical Support cannot troubleshoot these configurations. To successfully use VPN Services with the Netopia and Cayman routers, please contact your Internet Service Provider to obtain an account which uses a real, routable IP address on the WAN interface of the router. In the example configurations outlined in this technote, the use of non-routable IP addresses is strictly for illustrative purposes only.

**Caution:** If you have a firewall device of any type, hardware or software, on the network, and the IPsec tunnel must pass through it, it will be necessary to open **port 500 (UDP)** and **protocol 50 and 51** in the configuration of the rules of the firewall to allow the IPsec encrypted data to pass.

**Please Note:** If you are using **Network Address Translation** on the LAN, you can disregard **protocol 51**, as the **AH protocol** does NOT work through NAT.

*Note: IPsec tunneling supports IP routing only. IPX, AppleTalk or any protocol other than IP will not be routed across an IPsec tunnel.*

---

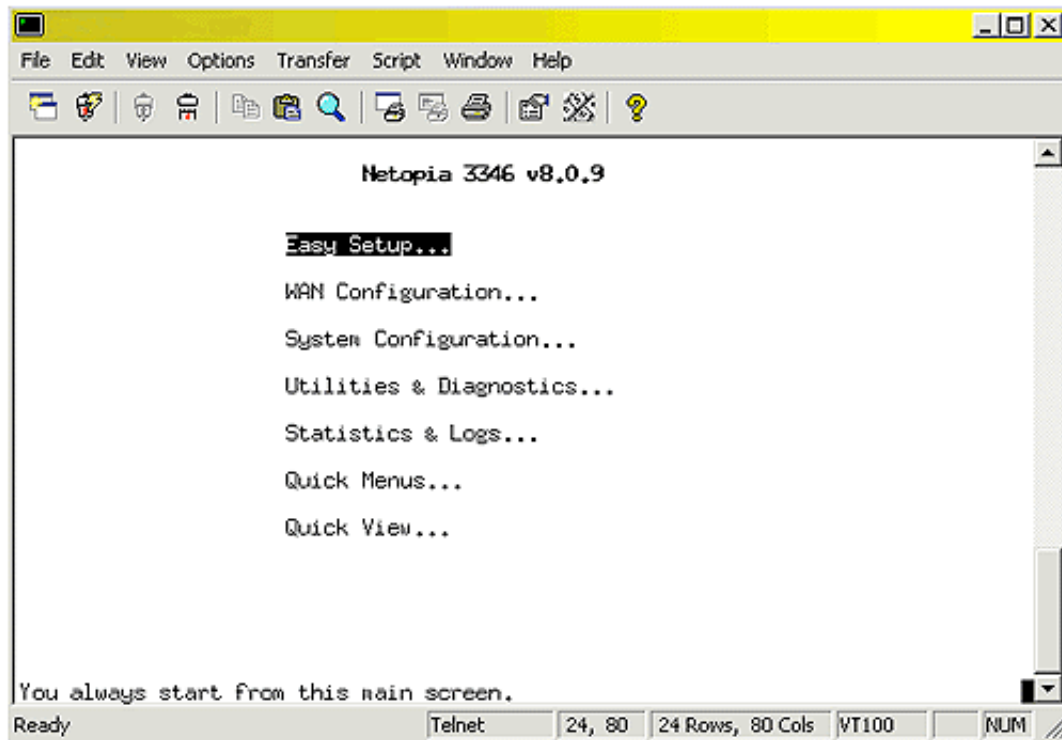
### Parameters:

Below is a list of hardware and firmware loads that this Technical Note is based upon:

Hardware	Firmware/Version	User Interface
4000 Series Routers	5.3.7 and later	Netopia "Menu"

3300 ENT Series Routers	8.0.9 and later	Netopia "Menu"
R-Series Routers	4.11 and later	Netopia "Menu"

To update your router firmware, go to our [firmware update page](#).



### ***Example of the Main Menu in Netopia Firmware 8.x for Enterprise***

#### **Before you start:**

- Verify that your computer is connected via ethernet to the router's **Local Area Network**.
- Establish a serial connection to the Netopia router's console using a communications program such as HyperTerminal or Z-Term. The settings should be 9600 Baud, 8 Data Bits, and 1 Stop Bit. Disable flow control.
- Alternatively, you can use Telnet over your LAN to get to the console screens.
- For detailed instructions on using HyperTerminal, Z-Term, or Telnet, please see [Netopia Quick Guide NQG\\_100](#).

#### **Tips:**

In the Netopia "Menu" User Interface:

- Pressing Return takes you into a page; pressing Escape takes you out.
- Press Return after entering each setting to save it.

Remember to allow sufficient time for IPsec authentication to occur. If using ping to test the network-to-network connectivity, transmit **120 packets at 1 second intervals** to bring up the tunnel.

---

#### **Index of common Error Messages, trouble symptoms, their meanings, causes, and solutions:**

The best tool available when diagnosing problems with IKE and IPsec tunnels are the **error**

**messages** listed in the Netopia's **WAN Event History**, under the **Statistics & Logs** Screen. The error messages will give a basic indication of the problem, and more information can frequently be obtained by highlighting the error message with the cursor, and hitting *Enter*. The following table reproduces some information found in the 4.10 firmware addendum, but also adds some recommended troubleshooting steps to take upon encountering the error.

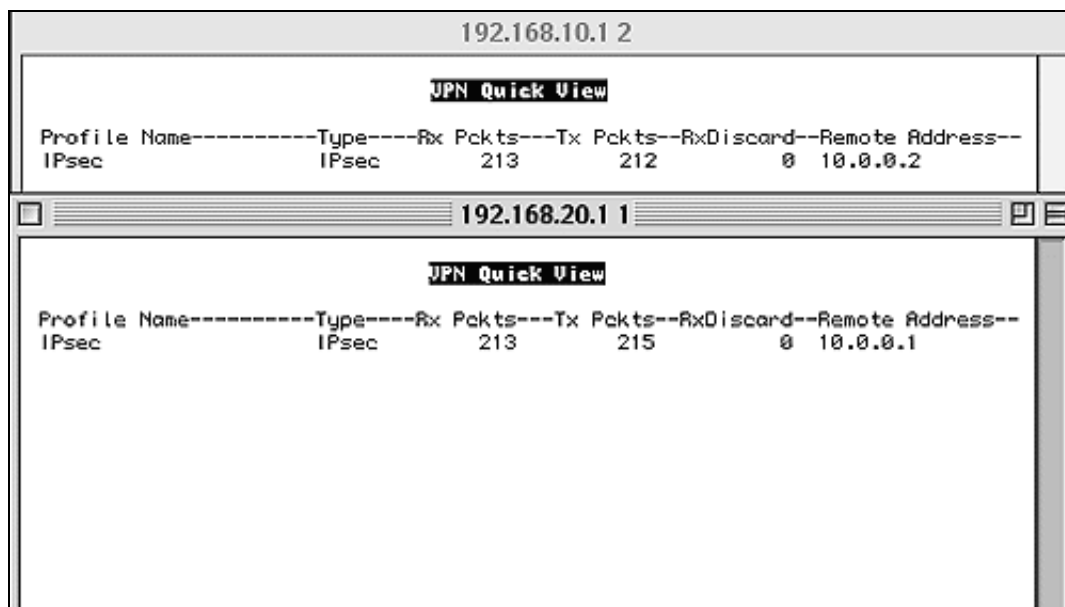
<b>ERROR MESSAGE</b>	<b>PROBLEM</b>	<b>SOLUTION</b>
no ph1 preferences assigned	An attempt was made to send traffic through an IPsec profile where IKE is the selected authentication method, but no IKE profile is assigned to the IPsec profile	Assign an IKE profile to the IPsec profile. Go into <b>Quick Menu -&gt; Change Connection Profile</b> . Select the IPsec profile and go into the <b>Encapsulation Options</b> . Make sure an IKE profile is associated with the connection profile.
DNS Lookup Failure	<p>1. If the Netopia is using a RTE of all zeros it cannot initiate an IPsec tunnel but only act as a responder.</p> <p>2. The router tried to look up the hostname associated with the IP Address of the Remote Tunnel Endpoint, but was not able to.</p>	<p>1. A Remote Tunnel Endpoint (RTE) of all zeros is used and the router initiates traffic to an address in the local member IP range. Change the <b>Negotiation...</b> to <b>Initiate Only</b> in the <b>Advanced IKE Phase 1 Options</b></p> <p>2. This is not in itself a problem, unless the Remote Tunnel Endpoint was specified as a hostname and not an IP address. If the RTE was specified as a hostname, try using an IP address instead. Also, make sure that the router has DNS server information configured under <b>Quick Menu -&gt; IP Setup</b>.</p>
no matching phase1 profile	The Netopia router that is logging this message is receiving an IKE request however no tunnel matches this remote tunnel endpoint.	Check the remote tunnel endpoint in the IPsec profile. Make sure the RTE matches the device which is sending the IKE request.
no matching proposal	An IKE request was sent or received, but the cryptographic parameters were not identical	This will be a mismatch of one of the cryptographic parameters in the IKE profile: DES vs. 3DES, or SHA1 vs. MD5. Confirm that the proposals on both sides are in agreement
phase1 auth failure	The authentication (i.e., the Shared Secret) failed.	The shared secret is incorrect. Try retyping the shared secret, and bear in mind that the shared secret is case sensitive.
phase1 resend timeout	Phase1 Negotiation was initiated, but no response was received from the remote tunnel endpoint, and the attempt timed out	<p>1. Verify that the remote tunnel endpoint in the IPsec profile is correct, and see if the IP address can be pinged. The remote peer may be offline or traffic between the two may be blocked by NAT or a filter set.</p> <p>2. If you have a filter set applied to the WAN of the Netopia make sure UDP 500 and protocol 50 and 51 are allowed.</p>
phase1 complete	All phase1 negotiations completed successfully.	This means that phase 1 has been established and the router will proceed with phase2 negotiations.
phase2 hash failed	The phase2 data received is out of date or has been tampered with	Tear down the tunnel by enabling and disabling the IPsec profile, and re-establish the vpn.
ph2 resend timeout	Phase 2 Negotiation was initiated but the tunnel was not completed.	Phase 2 negotiations failed. Check all of the Phase 2 IPsec profile parameters. Phase 1 is complete and does not need troubleshooting. * (Cisco products)
phase2 complete	Phase2 negotiations all completed successfully.	At this point, the tunnel is established.

\*Please Note on Cisco devices this may be a **Perfect Forward Secrecy (PFS)** mismatch. The Netopia has PFS **enabled** by default; however Cisco IOS and 3000 Series concentrators have PFS **off** by default. A mismatch of this option with Cisco devices will cause a failure of

Phase 2 negotiation with the Netopia logging a Phase 2 resend timeout. Try disabling PFS on the Netopia and attempting the connection again.

### Trouble Shooting with VPN Quick View

Another tool that can be used when trouble shooting Netopia VPNs is the **VPN Quick View**. This menu item can be found, from the Main Menu, go to **Quick View** ---> **VPN Quick View** and hit *Enter*. This is a screen shot of the VPN Quick View screen.



### VPN Quick View Page

The VPN Quick View can tell you if the Netopia Router has installed the VPN profile and whether the profile is sending and receiving packets. In this screen shot you see the simultaneous telnet views of each router sending and receiving packets over the tunnel.

You should see your IPsec tunnel show up in this location after the profile has been created and committed when creating a connection Profile. You should always see the profile in this area if the profile has been created and committed. If you do not see the profile here then the router is not recognizing the profile so you may want to recreate it.

After the tunnel has phase 1 and phase 2 complete you may use the Rx and Tx counters to troubleshoot traffic across the IPsec tunnel. The VPN Quick View screen has counters for Rx Packets, Tx Packets, and Rx Discards. The usefulness of these counters is to attempt a ping to an ip address in the Remote Member Network and watch to see the Tx and Rx packets on the profile. If you send a ping containing five packets and you see five packets sent and five packets received you know that the traffic was sent and received across the tunnel. On the other hand if you transmit five packets and received zero packets back from the ping you know that traffic you sent was not received.

What would cause an IPsec VPN to be able to transmit (TX) traffic but not receive (Rx) a response?

The most common reasons would be:

1. The machine you are attempting to ping is not gatewayed properly to the VPN gateway on the other side. In this case the workstation is actually receiving the traffic but not replying to a gateway which is routing back over the VPN.
2. A filter set is applied on either side of the connection that is interfering with the ICMP response. Make sure there is not a firewall device behind the VPN gateway that the Netopia IPsec tunnel is connected to.

3. The workstation that is the target ip of your test ping does not respond to ICMP echo requests. The machine may have a personal PC firewall like ZoneAlarm , McAfee, Norton Firewall . You could also run a packet sniffer program on the lan and see if you see the incoming traffic to the workstation from the remote IPsec VPN.

What does the Rx Discard field mean?

The Rx Discard for an IPsec profile means that the Netopia is receiving traffic that does not match the IPsec profile parameters. The router will drop traffic that does not match the IPsec profile.

### Rx discards for IPsec:

1. Unknown protocol (known ones are: ESP, AH, IP compression mismatch in profile)
2. Unknown SPI (no match to existing SA bundles)
3. ESP/AH error
4. SA mismatch (protocol doesn't match in packet/SA)
5. Source address didn't match any VPN network remote members ranges
6. Destination address didn't match any VPN network local member ranges

### How to use the *show ip nat translations* CLI command

One of the most useful items in the Netopia CLI is the ability to see the NAT translation being performed by the router. After issuing a Cltr-N at the main menu of the Netopia , type *show ip nat translation* and hit <Enter>. At first you will see something like the following:

Troubleshooting a Phase 1 resend timeout with *show ip nat translation* command

Let us use the example of two Netopia routers connecting WAN-to-WAN with an IPsec tunnel as the diagram shows.



**Local WAN 10.0.0.1 < ----- > Local WAN 10.0.0.2**

The R9100 router at 10.0.0.1 attempts to connect an IPsec tunnel to the 3386 router at 10.0.0.2 The R9100 is constantly logging a Phase 1 resend timeout. You have checked the IPsec error message logs in this guide above and know the possible reasons for this message. The NAT Translation table may be used to see if the IKE request is making it to the 3386. You can show ip nat translation on the 3386 at 10.0.0.2. Is there a UDP 500 incoming translation from the R9100 at 10.0.0.1 ? If no NAT translation is shown the IKE traffic is not even making it to the 3386 router. What you would see in this instance is the following:

### R9100 10.0.0.1 initiating IPsec tunnel

*#show ip nat trans*

```
LAN IP Address-- Port-- WAN IP Address-- Port-- Rem IP Address-- Port-- Dir-- Prot
10.0.0.1:      500    10.0.0.1:      500    10.0.0.2:      500    out UDP
```

Total entries in NAT cache: 1

Since Phase 1 and Phase 2 has not completed note that no ESP is seen since no data transfer can take place. After the completion of Phase 2, IPsec Security Associations will have been negotiated and Protocol 50 ESP will be logged when data is sent across the tunnel.

### 3386 10.0.0.2 waiting for incoming tunnel

*#show ip nat trans*

```
LAN IP Address-- Port-- WAN IP Address-- Port-- Rem IP Address-- Port-- Dir-- Prot
 10.0.0.2      55663    10.0.0.2      55663 204.152.184.72 123  out  UDP
```

Total entries in NAT cache: 3

You can see that there is no UDP 500 incoming from the R9100 10.0.0.1 router. There are some NAT translations but they do not apply to the incoming tunnel. ( NOTE: the one translations here applies to NTP Network Time Protocol). What would be causing this?

1. First thing would be to verify connectivity between the two WAN IP addresses. In our example this would be a ping from the 10.0.0.1 router to the 10.0.0.2. Can you get a successful ping reply?
2. Are both profiles enabled and do you have the correct Remote Tunnel Endpoints in each router?
3. Make sure there is not a firewall device in front of your VPN router.
4. Lastly make sure the ISP is not doing any UDP port 500 filtering.

A successful incoming IKE UDP 500 attempt looks like the following on the receiving router:

*#show ip nat trans*

```
LAN IP Address-- Port-- WAN IP Address-- Port-- Rem IP Address-- Port-- Dir-- Prot h:mm
 10.0.0.2      55663    10.0.0.2      55663 204.152.184.72 123  out  UDP 0:02
 10.0.0.2       500     10.0.0.2       500   10.0.0.1       500  in   UDP 0:02
```

If a filter set is applied to the WAN of the 3386 blocking UDP 500 you would see the same translation below. The reason you still see the UDP 500 translation is that this traffic is NOT blocked until after NAT has translated it. This looks the same as a successful incoming negotiation as above. Netopia firmware behavior is that NAT processing comes before the firewall . A packet hitting the router is processed by NAT first then the firewall. The transmitting router would show a transmitting UDP 500 in the NAT translation and the receiving router would show the translation below however Phase 1 would never complete. So you can see in this instance a successful negotiation and a filter set problem will look the same. The only difference is that when a filter set is applied you will never complete IKE Phase 1.

*#show ip nat trans*

```
LAN IP Address-- Port-- WAN IP Address-- Port-- Rem IP Address-- Port-- Dir-- Prot h:mm
 10.0.0.2      55663    10.0.0.2      55663 204.152.184.72 123  out  UDP 0:02
 10.0.0.2       500     10.0.0.2       500   10.0.0.1       500  in   UDP 0:02
```

### Proper IPsec translation Behavior after the tunnel is connected.

IPsec NAT Trans #1 ESP and UDP 500

This screenshot is from the 10.0.0.1 Router after Phase 1 and Phase 2 has completed in the Wan Event History.

**WAN Event History**

Current Date -- 6/17/03 05:57:31 PM

```
-Date---Time---Event-----
-----SCROLL UP-----
06/17/03 15:47:51   IKE: phase 2 complete sg 10.0.0.2
06/17/03 15:47:36   IKE: phase 1 complete sg 10.0.0.2
06/17/03 15:46:27 >>WAN: Ethernet WAN1 activated at 10000 Kbps

-----SCROLL DOWN-----
Clear History...
```

A ping was used to test connectivity from a workstation behind the R9100 to a workstation behind the 3386.

The following shows the IKE UDP 500 translation and the eventual ESP translation for the data transfer taking place over IPsec.

*#show ip nat trans*

LAN IP Address	Port	WAN IP Address	Port	Rem IP Address	Port	Dir	Prot	h:mm
10.0.0.1		10.0.0.1		10.0.0.2		out	ESP	0:02
10.0.0.1	500	10.0.0.1	500	10.0.0.2	500	out	UDP	0:02

Total entries in NAT cache: 2

You can see the UDP 500 IKE traffic outbound from the Netopia R9100 WAN. You can also see the ESP traffic which is the ICMP ping data traveling over. ESP will be seen after traffic passes across the IPsec tunnel. Until traffic is passed you will only see the UDP 500.

### **NAT Translation Lifetime Values**

These values are in seconds:

ESP\_LIFE = 180

IKE\_LIFE = 600

### **IPsec NAT Trans #2 ESP Only**

This is from the 3386 10.0.0.2 router ten minutes after the tunnel was established. The ping was performed purposely after ten minutes so the UDP 500 session which originally set up IKE would not be seen. This demonstrates that the IKE UDP 500 translation may not be seen after a period of time. ESP also may not be seen if the ESP sessions times out. However once traffic is sent over the tunnel the ESP session map should reappear.

*#show ip nat trans*

LAN IP Address	Port	WAN IP Address	Port	Rem IP Address	Port	Dir	Prot
10.0.0.2		10.0.0.2		10.0.0.1		out	ESP