Application Note

Configure VPN Tunnels on a Digi VC7400 using a Digi TransPort and Digi Connect

Patrick W Brannelly

June 29, 2009

VERSION 1.0

Contents

1 INTRODUCTION 4

1.1 Outline 4

1.2 Assumptions 4

1.3 Corrections 4

1.4 Version 5

2 DIGI VC7400 AND DIGI TRANSPORT VPN 6

2.1 Digi VC7400 Configuration 6

2.1.1 Configure port ETH5 as a WAN gateway 6

2.1.2 VPN Configuration 8

2.2 TransPort SR Configuration 14

2.2.1 VPN Configuration 14

3 DIGI VC7400 DIGI CONNECTPORT WAN VPN 20

3.1 Digi VC7400 VPN Configuration 20

3.1.1 Digi VC7400 Eroute Configuration 20

3.2 Digi ConnectPort WAN Configuration 21

3.2.1 Network Configuration: Ethernet IP Settings 21

3.2.2 Network Configuration: VPN Settings 22

4 TESTING 26

4.1 View the IPSec Peers 26

4.2 View the IKE Security Associations 27

4.3 View the IPSec Eroute 28

4.4 Digi ConnectPortWAN 30

4.5 Ping/Traffic test 30

Figures

Figure 2-1: Eth 5 Configuration 7
Figure 2-2: Default Route 0 Configuration 8
Figure 2-3: Ike Responder Configuration 9
Figure 2-4: Eroute 1 Configuration 12
Figure 2-5: User 11 Configuration 13
Figure 2-6: IKE Responder Configuration 15
Figure 2-7: Eroute 0 Configuration 18
Figure 2-8: User 10 Configuration 19
Figure 3-1: VC7400 Eroute 2 Configuration 21
Figure 3-2: Ethernet IP Settings 22
Figure 3-3: ConnectPort WAN VPN Global Settings 22
Figure 3-4: ConnectPort WAN VPN Settings 25
Figure 4-1: VC7400 IPSec Peers 26
Figure 4-2: Transport SR IPSec Peers 27
Figure 4-3: VC7400 IKE SAs 27
Figure 4-4: Transport SR IKE SAs 28
Figure 4-5: VC7400 IPSec Eroute 0 and Eroute 2 29
Figure 4-6: Transport SR IPSec Eroute 0 29
Figure 4-7: ConnectPortWAN Connections 30

1 INTRODUCTION

1.1 Outline

The Digi TransPort VC7400 is an enterprise class VPN concentrator that provides secure end-to-end connectivity for large numbers of remote devices and networks. It is fully compatible with all Digi VPN enabled cellular and wired routers and most IPsec and SSL compliant devices and clients. A centralized Digi VC7400 enables a fully integrated, single vendor solution with the highest level of reliability and security.

This application note details the configuration of a Digi VC7400 and two different VPN tunnels. One VPN is between a Digi TransPort, and the other between a Digi ConnectPort WAN, but could be any Digi Connect or ConnectPort router with IPsec VPN capability. The purpose of this document is to demonstrate a basic VPN configuration. The Digi VC7400 is capable of supporting 3000 VPN tunnels, with more complex configurations beyond the scope of this document.

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router and a Digi Connect router, and to configure them with basic routing functions.

This application note applies only to:

Model: Digi VC7400 VPN Concentrator, TransPort WR, SR or DR and a Digi Connect and/or ConnectPort WAN.

Firmware versions: TransPort firmware version 5064, ConnectPort WAN VPN version 2.8.4.13 EOS

Configuration: This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

For the purpose of this application note the following applies:

- The TransPort SR's IP address is dynamic
- IPSEC is to be used in "aggressive mode"

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: support@digi.com

Requests for new application notes can be sent to the same address.

1.4 Version

Version Number:	1.0
Status:	FINAL

2 DIGI VC7400 AND DIGI TRANSPORT VPN

2.1 Digi VC7400 Configuration

2.1.1 Configure port ETH5 as a WAN gateway

Any of the Ethernet ports on a Digi VC7400 can be used as a WAN port; however, port ETH 5 is designed to be the WAN port and supports Gigabit Ethernet (Gig-E). In this example, the VC7400 is configured with a cable modem as its WAN gateway. The steps for this are:

1. Configure ETH 5 to accept a DHCP IP address from the cable modem
2. Configure a default route for ETH 5

2.1.1.1 Configure ETH 5

ETH 5 is configured to accept DHCP addresses and to use Network Address Translation/Port Translation (NAPT). By default, these parameters are off and will need to be configured, and the default subnet mask needs to be replaced with "0". Ideally, the WAN gateway IP address would be static. If that were the case, the DHCP client setting would not be enabled and the IP address, subnet mask and gateway IP address would be configured. Also, because this will be the gateway for the VPN, IPSec must be enabled.

The Eth 5 configuration page is located at ***Configuration - Interfaces > Ethernet > ETH 5***.

The following figure shows this configuration. There are five items to configure:

- DHCP Client
- Change default subnet mask to zero
- Route Metric
- IPsec on this interface
- NAPT on this interface

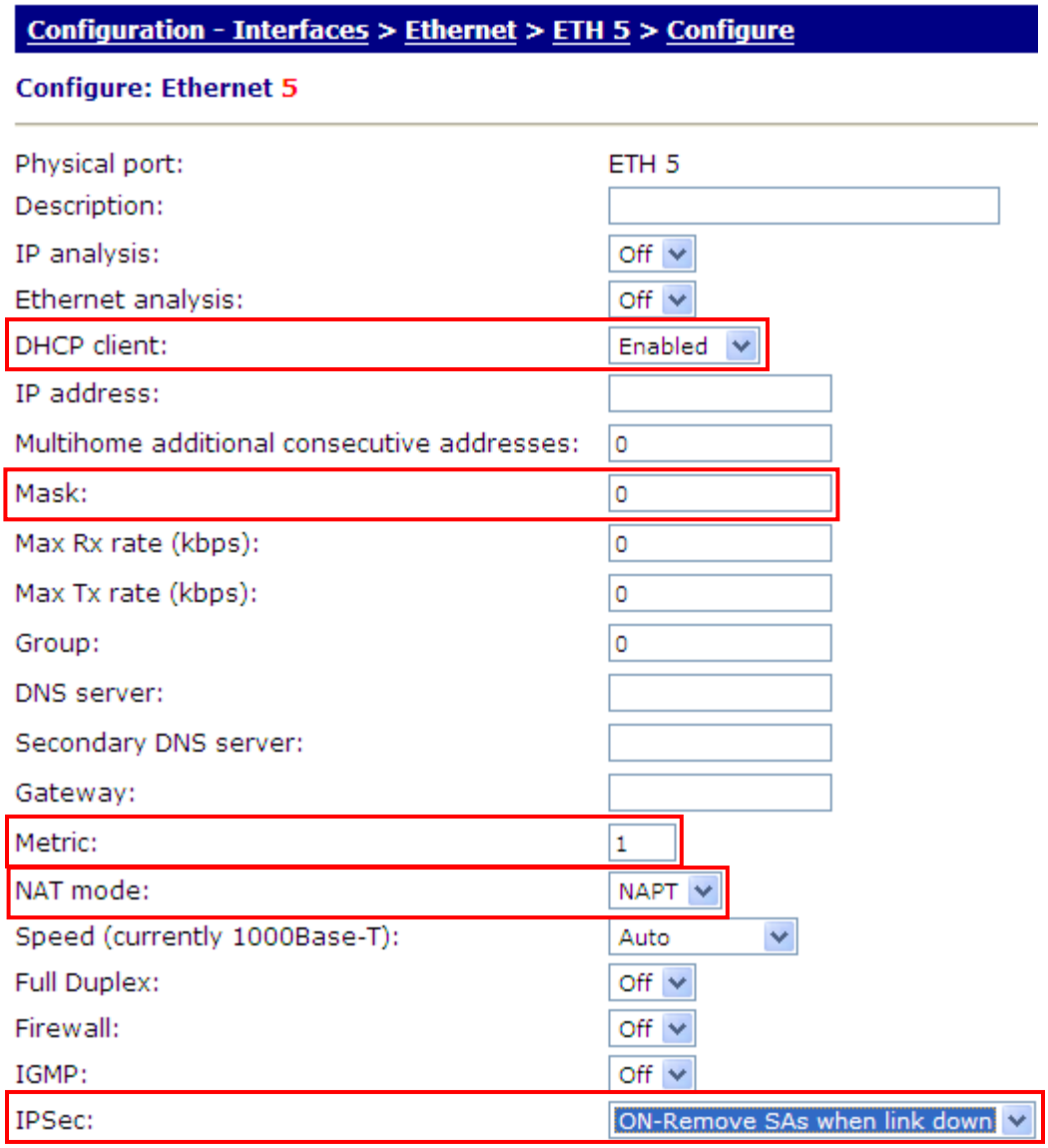


Figure 2-1: Eth 5 Configuration

2.1.1.2 Configure a Default Route for Eth 5

In order for the Digi VC7400 to recognize Eth 5 as a gateway, a default route must be configured to point to that port. In this example, default route 0 is tied to Eth 5. The steps are to set the Interface to "Ethernet" and the Interface # to "5".The configuration page is located at ***Configuration - Routing >Routing >Default Route 0***. Figure 2-2 demonstrates this.

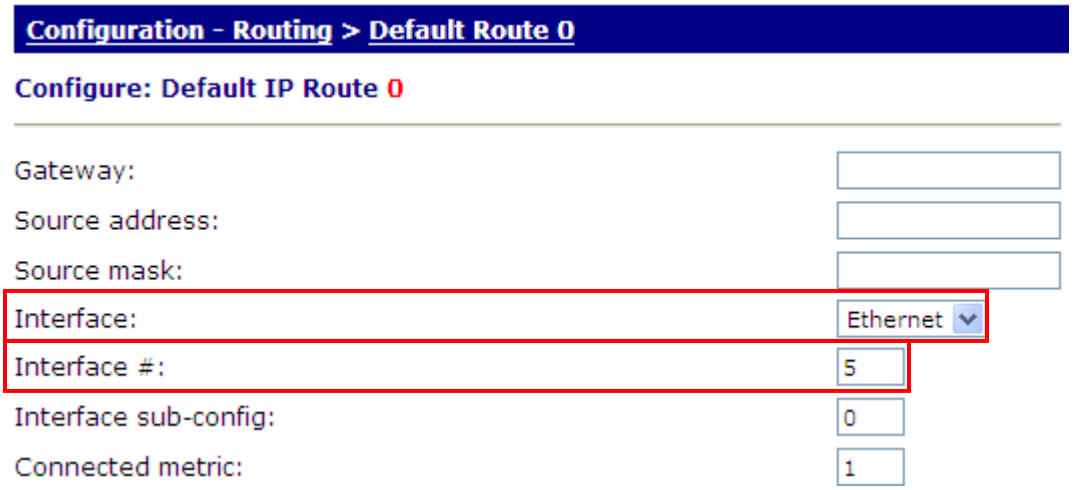


Figure 2-2: Default Route 0 Configuration

2.1.2 VPN Configuration

The Digi VC7400 is usually configured as the VPN Responder, and as such is configured differently.

The steps for this configuration are:

1. Configure the IKE Responder
2. Configure the Eroute (i.e., the VPN tunnel)
3. Configure the User, which acts as the pre-shared key

2.1.2.1 Configure the IKE Responder

The IKE Responder is set to a range of IPSec parameters. In order for the Initiator to connect, its parameters must fall within these ranges. The majority of the settings will be the default settings. For this reason they are not highlighted in the following graphic.

For troubleshooting purposes, it is a good idea to enable debugging at level “Very High”.

This page is located at ***Configuration - VPN>IPSec >IKE>Responder.*** Figure 2-3 shows the IKE Responder settings.

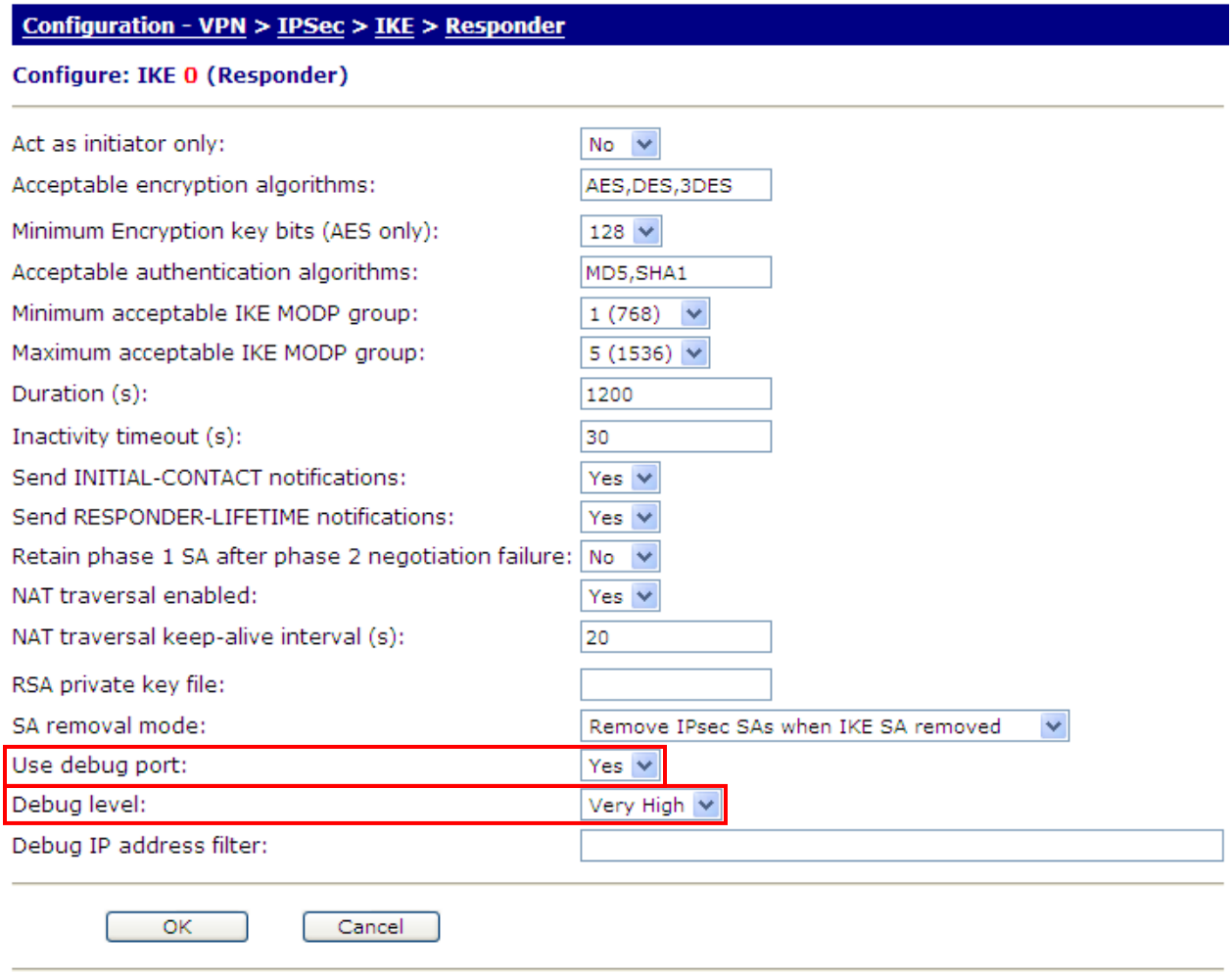


Figure 2-3: Ike Responder Configuration

2.1.2.2 Configure Eroute 1

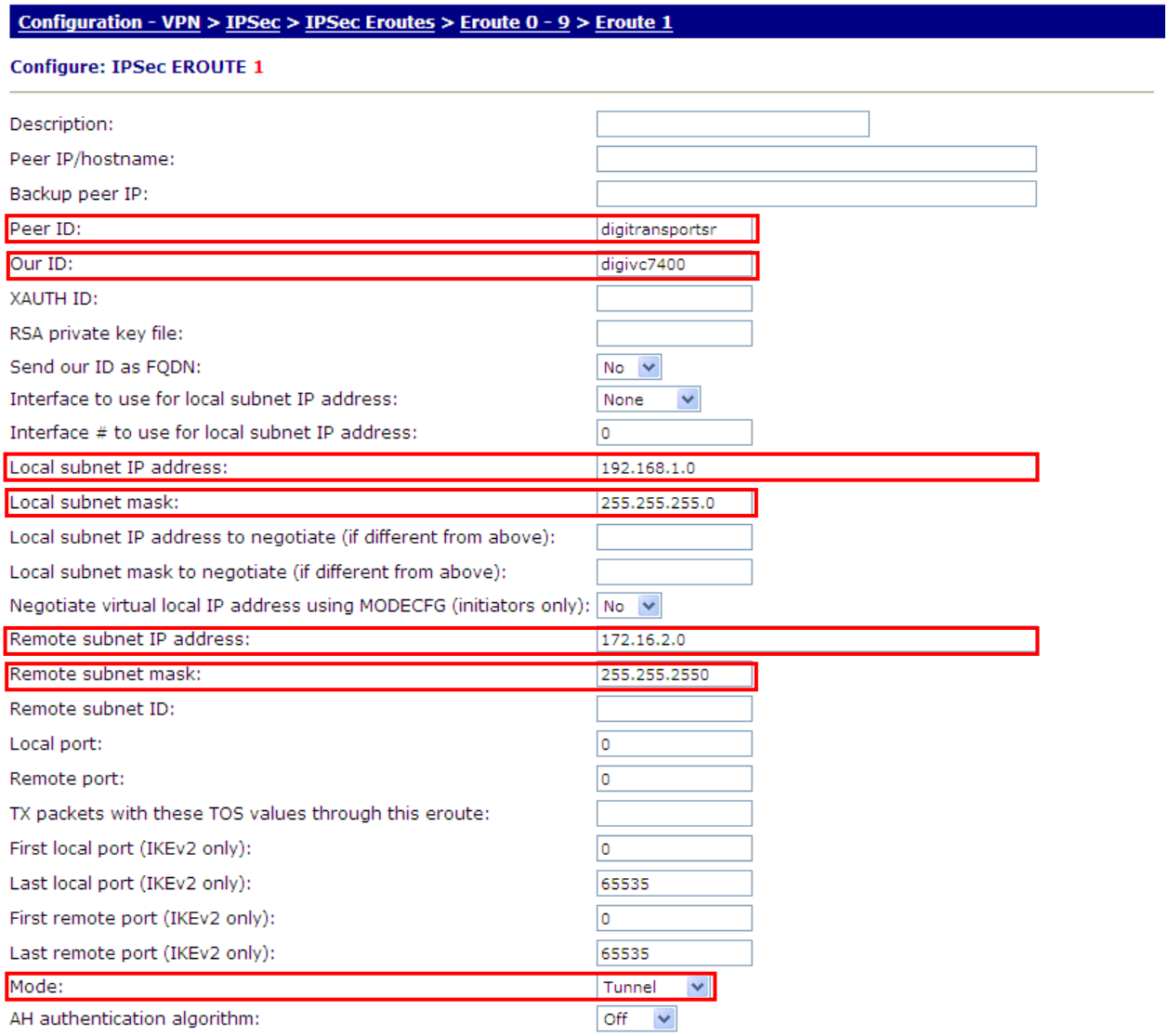
The Eroute can be thought of as the VPN tunnel. The Eroute is where the Peer IP, Peer ID, local and remote subnets, etc. are configured. As the responder, the TransPort DR doesn't require the Peer IP of the responder, but the peer ID and our ID parameters must be set. In addition, as the responder, the VC7400 does not require the creation of SA's or an SA Action parameter. Finally, the duration parameters should be configured so they don't too much load on the VPN concentrator when there are multiple sites connected. The duration (s) should be to 28800 and duration (kb) to 0.

For this example, Eroute 1 was used. The full list of parameters is as follows:

1. Peer ID: "digitransportsr"
2. Our ID: "digivc7400"
3. Local Subnet IP address
4. Local Subnet mask

5. Remote Subnet IP address
6. Remote Subnet mask
7. Mode: Tunnel
8. ESP authentication algorithm: SHA1
9. ESP encryption algorithm: AES
10. Duration (s): 28800
11. Duration (kb): 0
12. No SA Action: Drop Packet
13. Create SA's automatically: No
14. Authentication method: Preshared Keys
15. Display IKE lookup debug info: Yes (This step is not necessary, but a good idea for troubleshooting purposes)

The configuration page is located at ***Configuration - VPN > IPSec > IPSec Eroutes > Eroute 0 - 9 > Eroute 0*** and Figure 2-4 shows these settings:


Configuration - VPN > IPSec > IPSec Eroutes > Eroute 0 - 9 > Eroute 1
Configure: IPSec EROUTE 1
Description:
Peer IP/hostname:
Backup peer IP:
Peer ID: digitransportsr
Our ID: digivc7400
XAUTH ID:
RSA private key file:
Send our ID as FQDN: No
Interface to use for local subnet IP address: None
Interface # to use for local subnet IP address: 0
Local subnet IP address: 192.168.1.0
Local subnet mask: 255.255.255.0
Local subnet IP address to negotiate (if different from above):
Local subnet mask to negotiate (if different from above):
Negotiate virtual local IP address using MODECFG (initiators only): No
Remote subnet IP address: 172.16.2.0
Remote subnet mask: 255.255.2550
Remote subnet ID:
Local port: 0
Remote port: 0
TX packets with these TOS values through this eroute:
First local port (IKEv2 only): 0
Last local port (IKEv2 only): 65535
First remote port (IKEv2 only): 0
Last remote port (IKEv2 only): 65535
Mode: Tunnel
AH authentication algorithm: Off

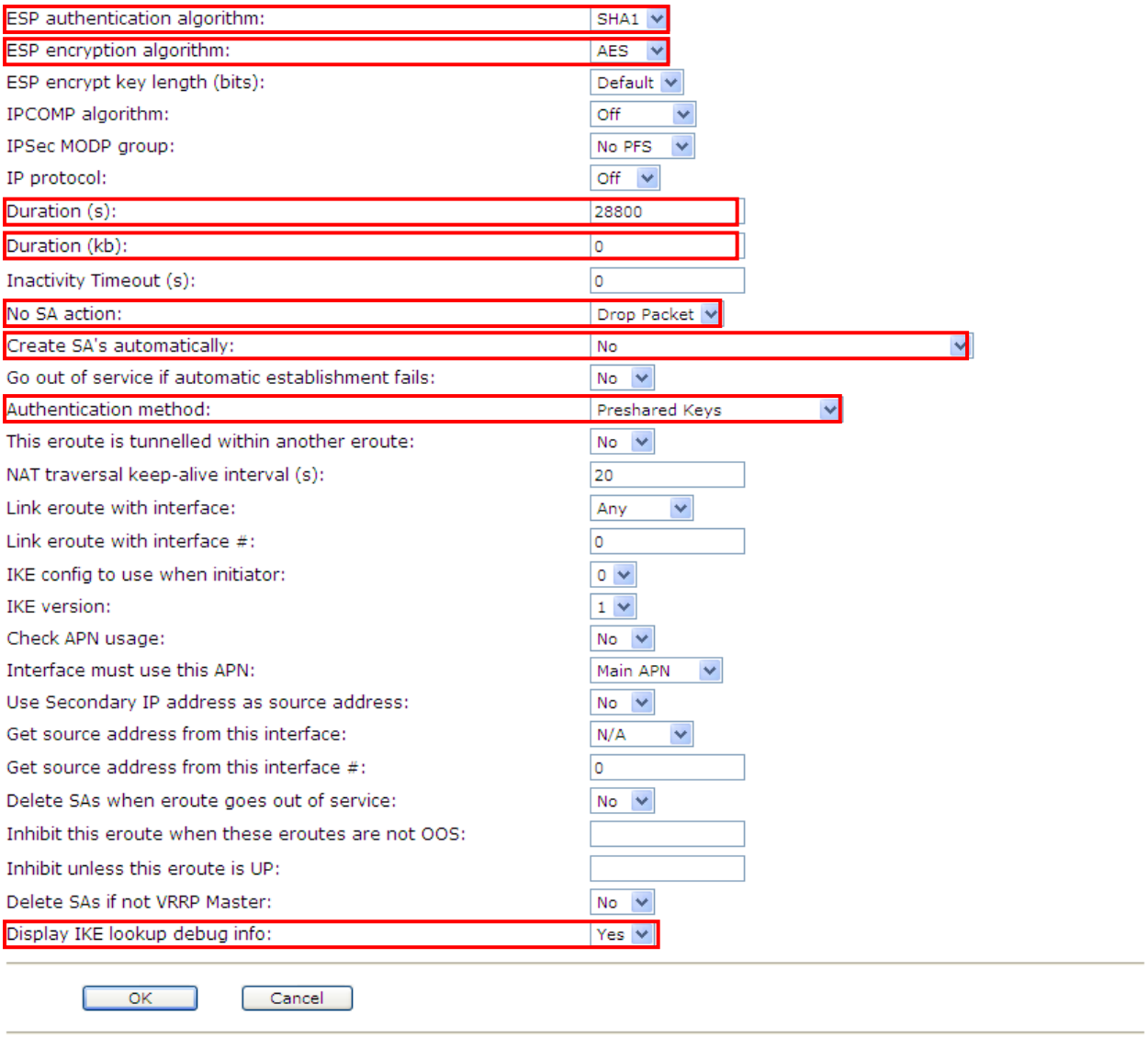


Figure 2-4: Eroute 1 Configuration

2.1.2.3 Configure the User/Pre-shared Key

The Digi TransPort uses a user account for the pre-shared key. In this example, User 11 was used. This is because the default user accounts occur between 0 through 9. Digi recommends using user 10 and higher to avoid inadvertently changing important user settings. The page is located at ***Configuration - Security > Users > User 10 - 19 > User 11***. The steps are to configure the name, password and access level. The name is the peer ID and the password is the pre-shared key. The access level was set to "None" for security purposes. For this application note, the name is "digitransportsr" and the password is "transport". Figure 2-5 demonstrates this:

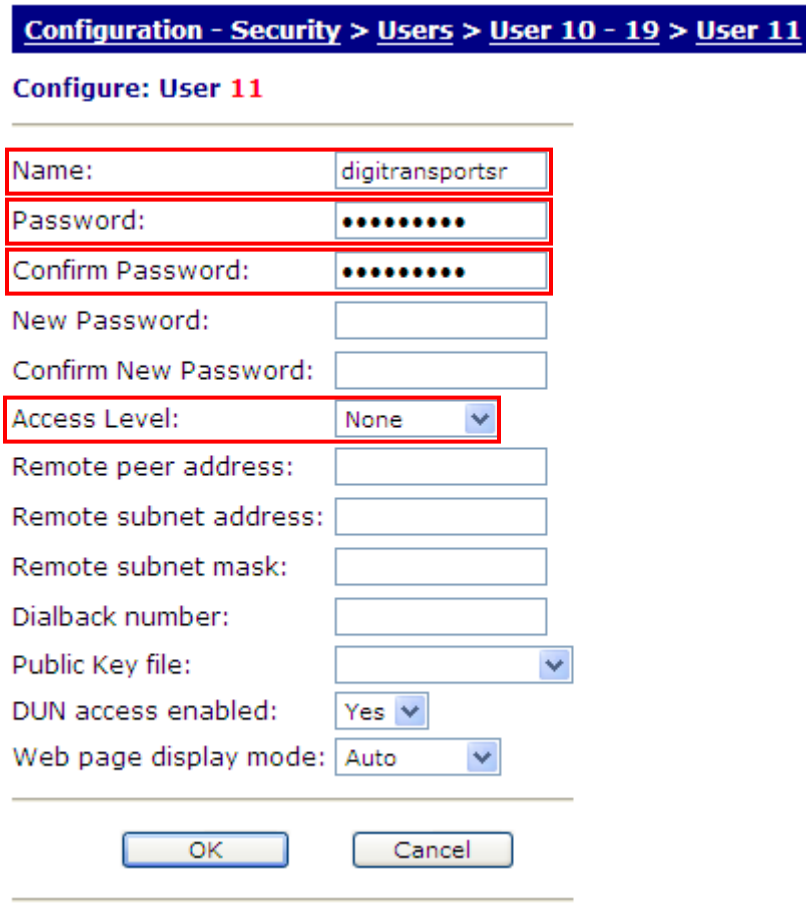


Figure 2-5: User 11 Configuration

2.2 TransPort SR Configuration

The Digi TransPort SR in this application note acts as the initiator, using the cellular W-WAN interface, associated with PPP 1. . This application note assumes the wireless module has been properly provisioned. If this were a GSM module, there would be parameters to set that vary on the provider's account settings. Instructions for configuring the W-WAN interfaces are located in the Digi TransPort User Guide and other application notes.

2.2.1 VPN Configuration

The Digi TransPort SR is the VPN Initiator in this example, and as such is configured to match the parameter ranges of the Responder.

The steps for this configuration are:

1. Configure the IKE 0 (Initiator)
2. Configure the Eroute
3. Configure the User, which acts as the pre-shared key

2.2.1.1 Configure IKE

The IKE instance is set with the parameters of the VPN tunnel. It is important to note that Aggressive Mode is on. In this test, the IP address for the W-WAN connection is dynamic and for this reason aggressive mode is required. It is not necessary when using static IP addresses.

Also, the duration should be set at a higher level. In this case, it is 28800.

For troubleshooting purposes, it is a good idea to enable debugging at level "Very High". This page is located at ***Configuration - VPN>IPSec >IKE>IKE 0.*** Figure 3-3 shows the IKE 0 settings.

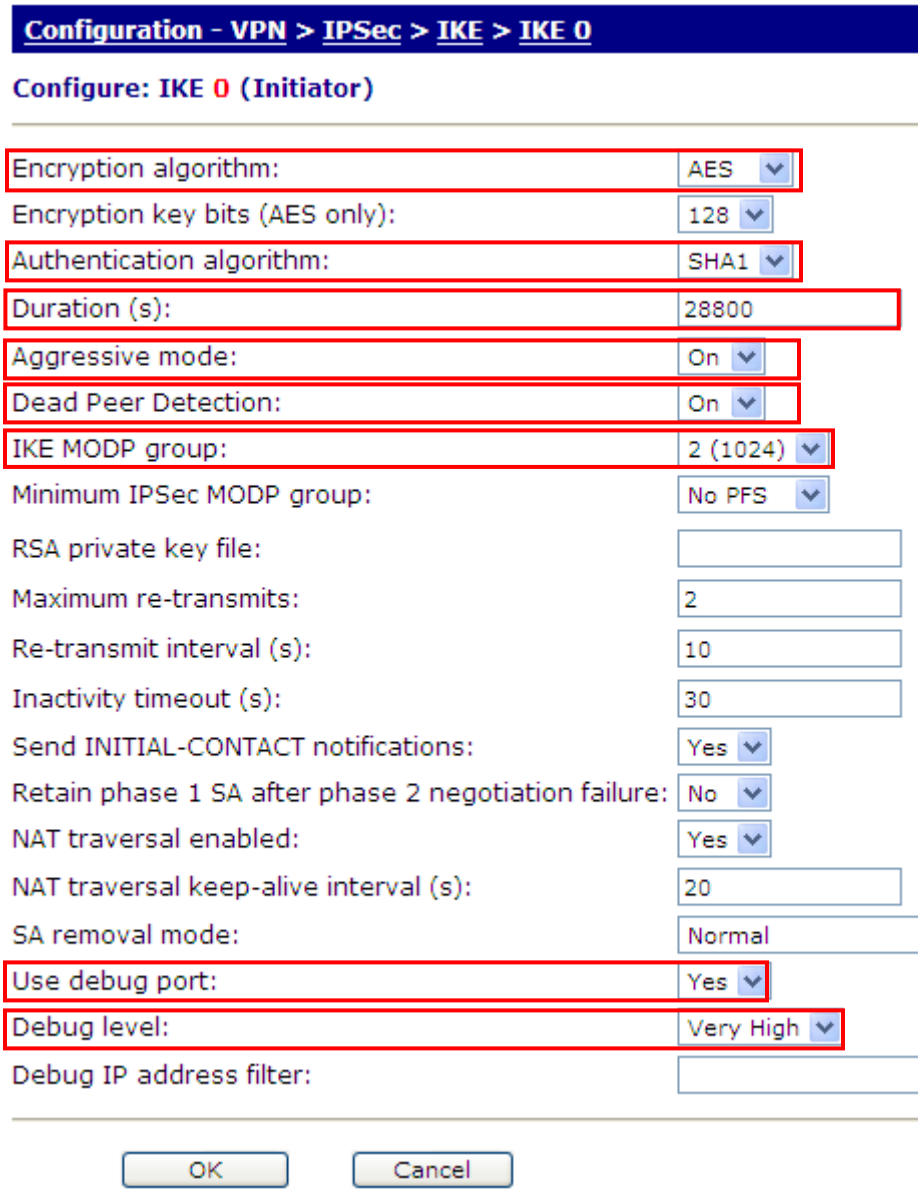


Figure 2-6: IKE Responder Configuration

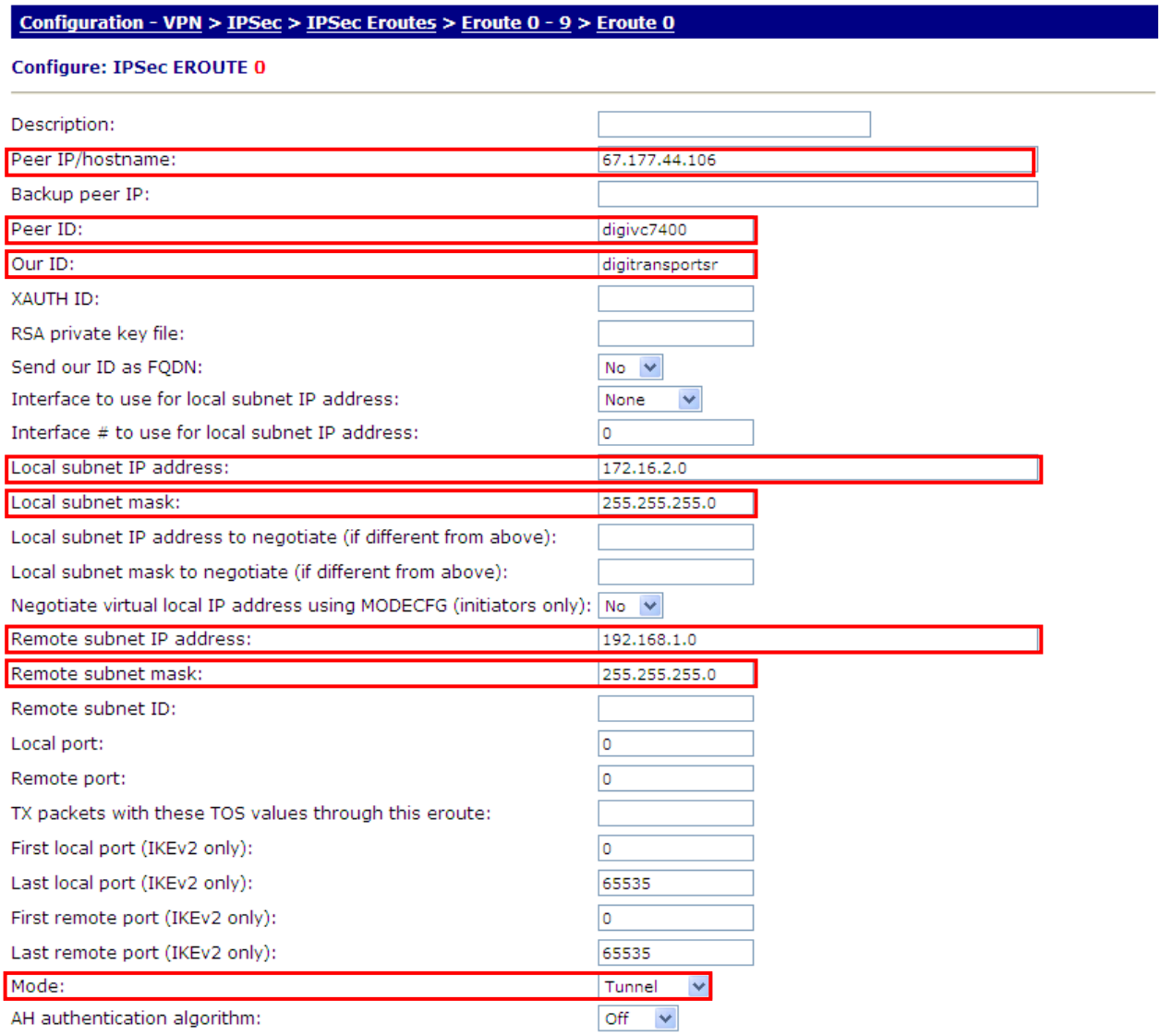
2.2.1.2 Configure Eroute 0

The Eroute is the same as a VPN tunnel. The Eroute is where the Peer IP, Peer ID, local and remote subnets, etc. are configured. As the initiator, the TransPort SR needs a public IP address with which to initiate the tunnel. The full list of parameters is as follows:

1. Peer IP: “70.57.159.140”
2. Peer ID: “digivc7400”
3. Our ID: “digitransportsr”
4. Local Subnet IP address

5. Local Subnet mask
6. Remote Subnet IP address
7. Remote Subnet mask
8. Mode: Tunnel
9. ESP authentication algorithm: SHA1
10. ESP encryption algorithm: AES
11. Duration (s): 28800
12. Duration (kb): 0
13. No SA Action: Use IKE
14. Create SA's automatically: Yes. Route with matching interface required (for Always-on settings)
15. Authentication method: Preshared Keys

The configuration page is located at ***Configuration - VPN > IPSec > IPSec Eroutes > Eroute 0 - 9 > Eroute 0*** and Figure 3-4 shows these settings:


Configuration - VPN > IPSec > IPSec Eroutes > Eroute 0 - 9 > Eroute 0
Configure: IPSec EROUTE 0
Description:
Peer IP/hostname: 67.177.44.106
Backup peer IP:
Peer ID: digivc7400
Our ID: digitransportsr
XAUTH ID:
RSA private key file:
Send our ID as FQDN: No
Interface to use for local subnet IP address: None
Interface # to use for local subnet IP address: 0
Local subnet IP address: 172.16.2.0
Local subnet mask: 255.255.255.0
Local subnet IP address to negotiate (if different from above):
Local subnet mask to negotiate (if different from above):
Negotiate virtual local IP address using MODECFG (initiators only): No
Remote subnet IP address: 192.168.1.0
Remote subnet mask: 255.255.255.0
Remote subnet ID:
Local port: 0
Remote port: 0
TX packets with these TOS values through this eroute:
First local port (IKEv2 only): 0
Last local port (IKEv2 only): 65535
First remote port (IKEv2 only): 0
Last remote port (IKEv2 only): 65535
Mode: Tunnel
AH authentication algorithm: Off

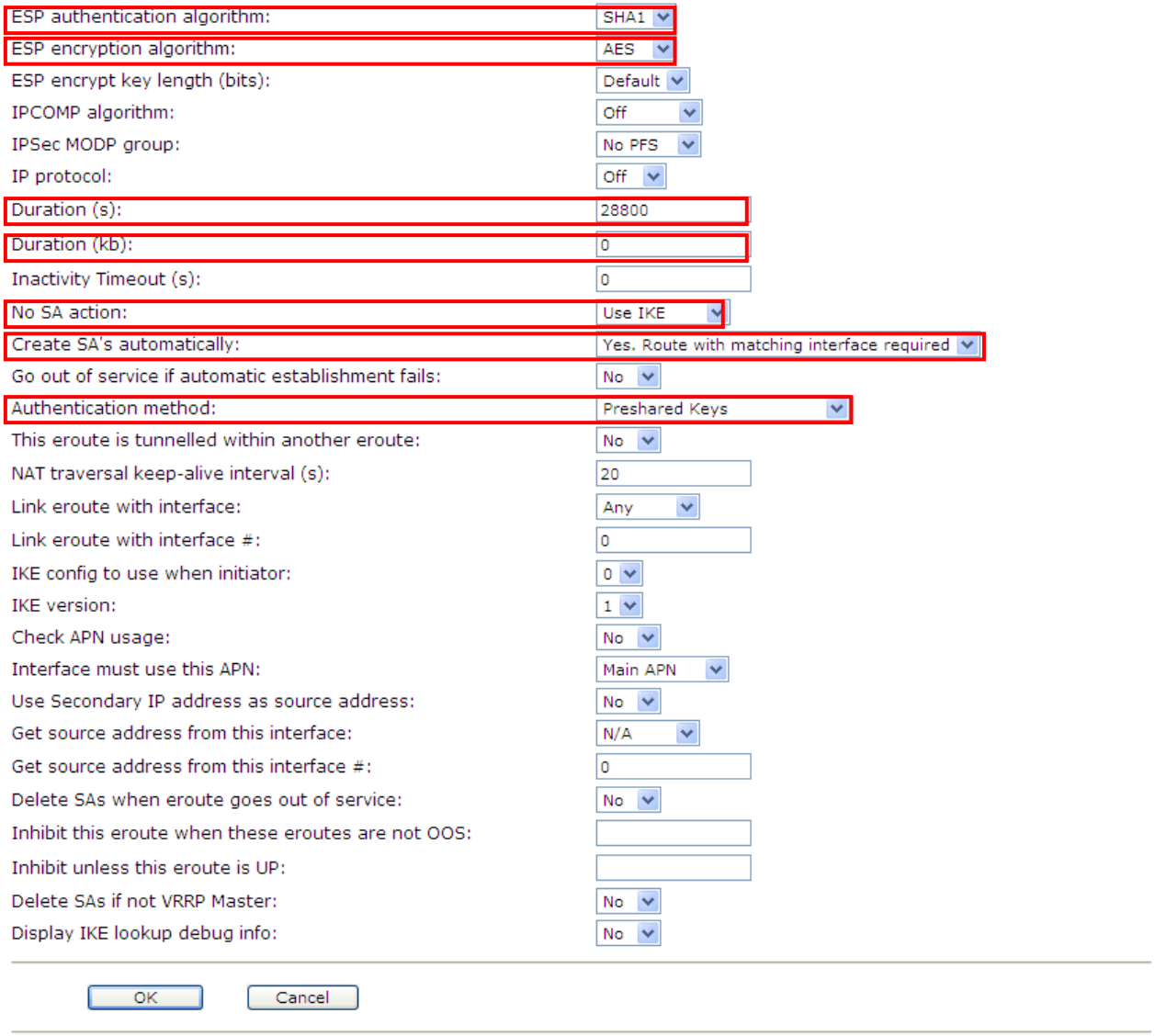


Figure 2-7: Eroute 0 Configuration

2.2.1.3 Configure the User/Pre-shared Key

The Digi TransPort uses a user account for the pre-shared key. In this example, User 10 was used. The page is located at ***Configuration - Security > Users > User 10 - 19 > User 10***. The steps are to configure the name, password and access level. The name is the peer ID and the password is the pre-shared key and the access level is "None".

In a normal setting, it is advisable to use a pre-shared key of at least 10 characters, ideally with random upper and lower case characters. Use of a dictionary word could potentially be cracked in a matter of seconds. The password in this example is for simplicity, and is not recommended in a production environment.

For this application note, the name is “digivc7400” and the password is “transport”. Figure 3-5 demonstrates this:

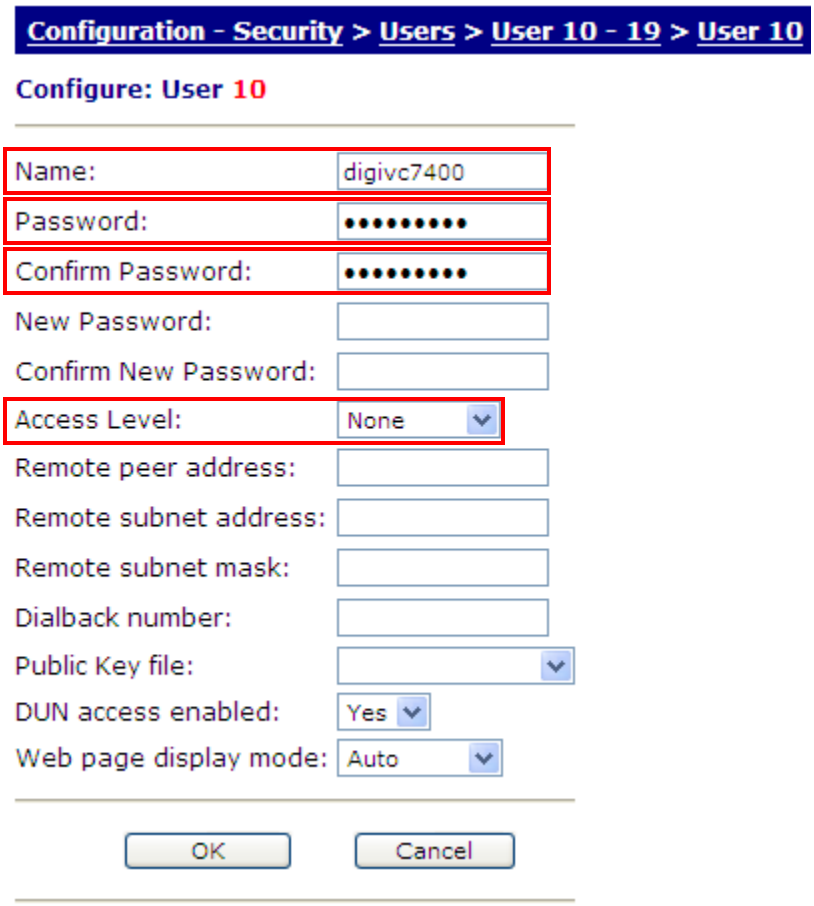


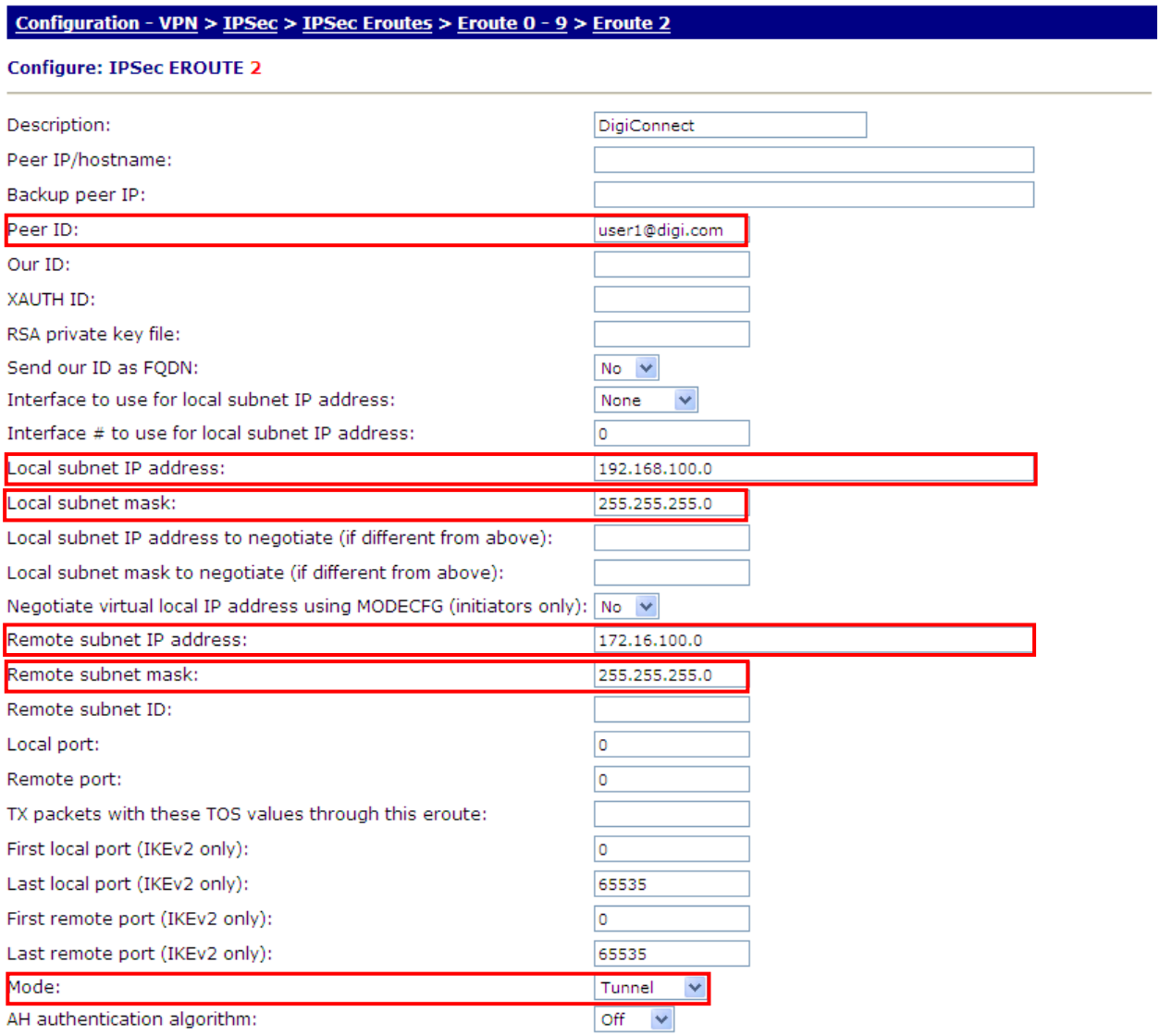
Figure 2-8: User 10 Configuration

3 DIGI VC7400 DIGI CONNECTPORT WAN VPN

3.1 Digi VC7400 VPN Configuration

3.1.1 Digi VC7400 Eroute Configuration

For this example, Eroute 2 was configured for the ConnectPort WAN VPN. Much of the settings are the same as the configuration for the TransPort VPN, with a few exceptions. The Peer ID can be regular text or in a Fully Qualified Domain Name (FQDN) format. In this example, the ID is "user1@digi.com". The IPSec MODP Group must match the Diffie-Hellman Group in the Eroute settings, which in this case is Group 2. Figure 3-1 demonstrates this configuration.



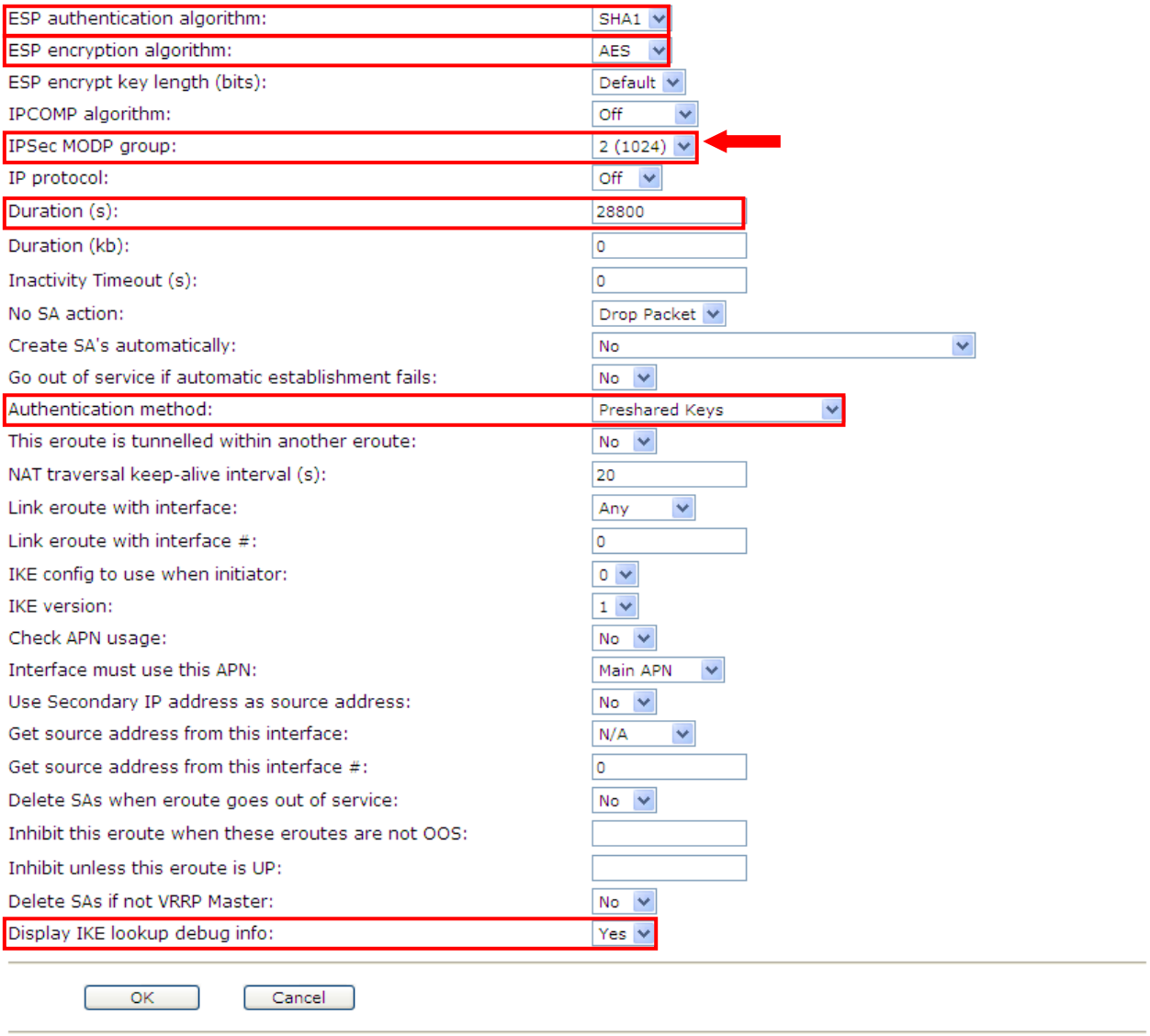


Figure 3-1: VC7400 Eroute 2 Configuration

3.2 Digi ConnectPort WAN Configuration

3.2.1 Network Configuration: Ethernet IP Settings

The default settings for Ethernet include a subnet of 192.168.1.0/24. For the purposes of this application note, the subnet is 172.16.100.0/24 so as not to conflict with the VC7400's local subnet. The default gateway is the mobile interface. Figure 3-1 shows this configuration.

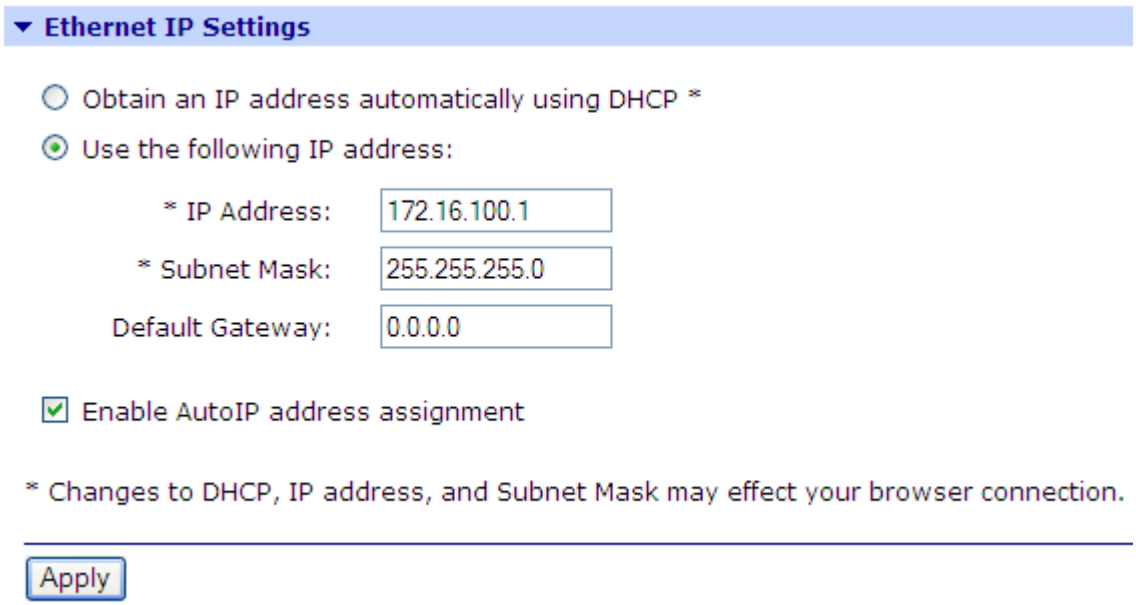


Figure 3-2: Ethernet IP Settings

3.2.2 Network Configuration: VPN Settings

The global VPN settings are left to default, with the exception of one of the miscellaneous settings, "Suppress Delete Phase 1 SA Message for PFS", which is checked, as shown in figure 3-3.

3.2.2.1 VPN Global Settings

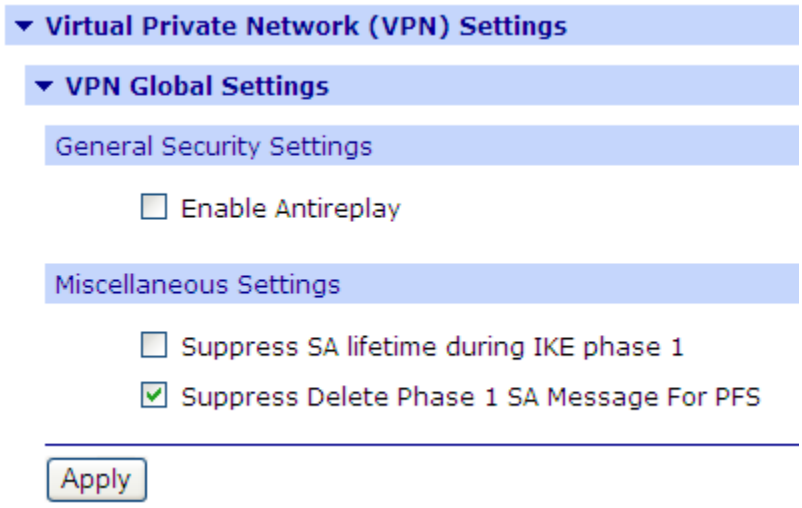


Figure 3-3: ConnectPort WAN VPN Global Settings

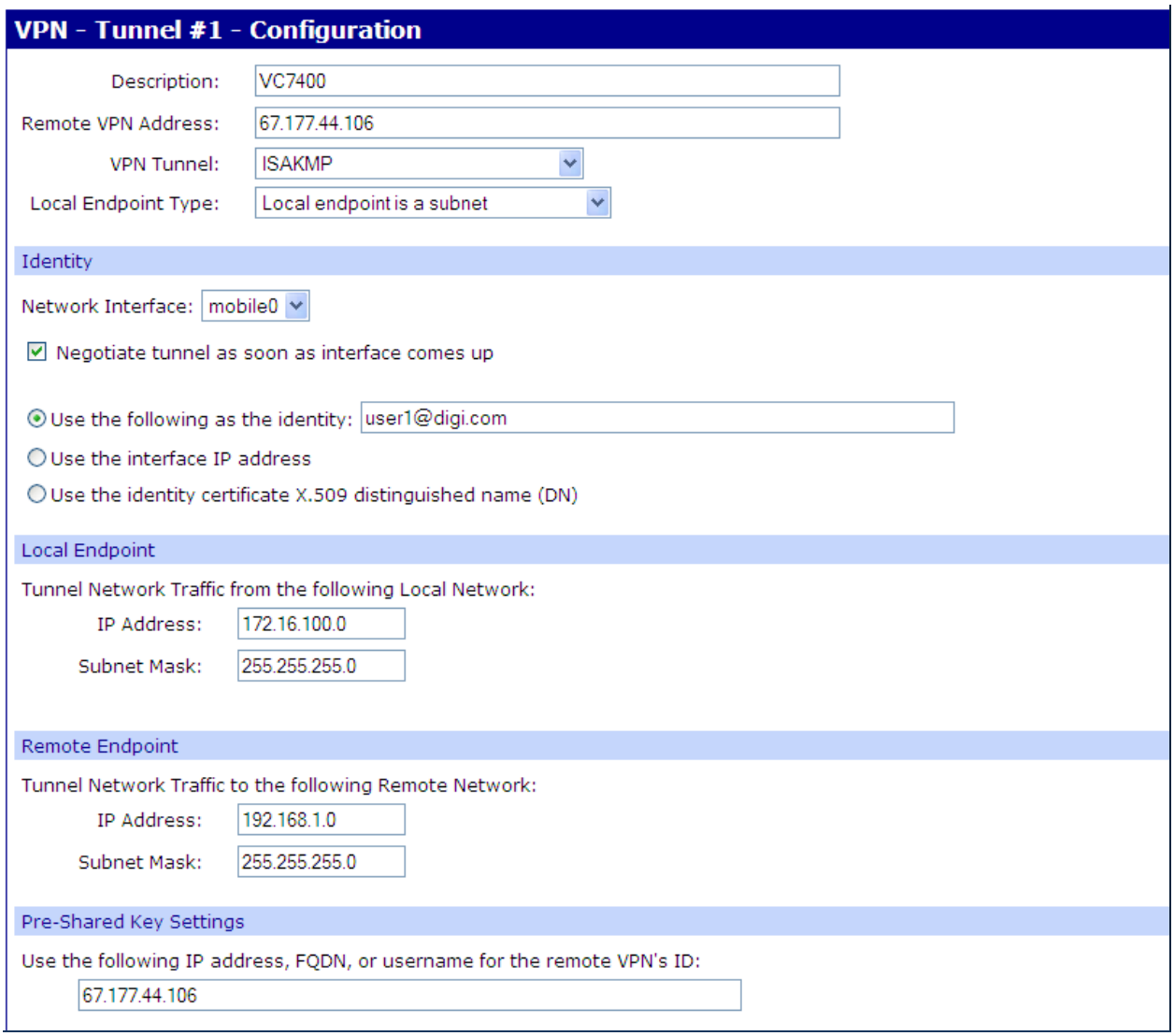
3.2.2.2 VPN Settings

The following VPN settings need to be configured:

1. Remote VPN Address: The public IP address of the Digi VC7400.

2. VPN Tunnel: “ISAKMP”
3. Local Endpoint Type: “Local endpoint is a subnet”
4. Identity: Set the network interface to “Mobile0”, and the identity as a FQDN.
5. The local and endpoint subnets
6. The pre-shared key settings, which are the above-mentioned IP address of the VC7400 and the key itself. In this example, the key is “transport”.
7. ISAKMP Phase 1 settings:
    a. Connection Mode: Aggressive
    b. Enable Perfect Forward Secrecy (PFS)
8. ISAKMP Phase 1 policies: Match the Eroute settings: Pre-shared key, AES-128, SHA-1 and Group 2.
9. ISAKMP Phase 2 Settings:
    a. Diffie-Hellman: Group 2
10. ISAKMP Phase 2 Policies: AES-128, SHA-1.

Figure 3-4 shows these settings.


VPN - Tunnel #1 - Configuration
Description:
VC7400
Remote VPN Address:
67.177.44.106
VPN Tunnel:
ISAKMP
Local Endpoint Type:
Local endpoint is a subnet
Identity
Network Interface:
mobile0
Negotiate tunnel as soon as interface comes up
Use the following as the identity:
user1@digi.com
Use the interface IP address
Use the identity certificate X.509 distinguished name (DN)
Local Endpoint
Tunnel Network Traffic from the following Local Network:
IP Address:
172.16.100.0
Subnet Mask:
255.255.255.0
Remote Endpoint
Tunnel Network Traffic to the following Remote Network:
IP Address:
192.168.1.0
Subnet Mask:
255.255.255.0
Pre-Shared Key Settings
Use the following IP address, FQDN, or username for the remote VPN's ID:
67.177.44.106

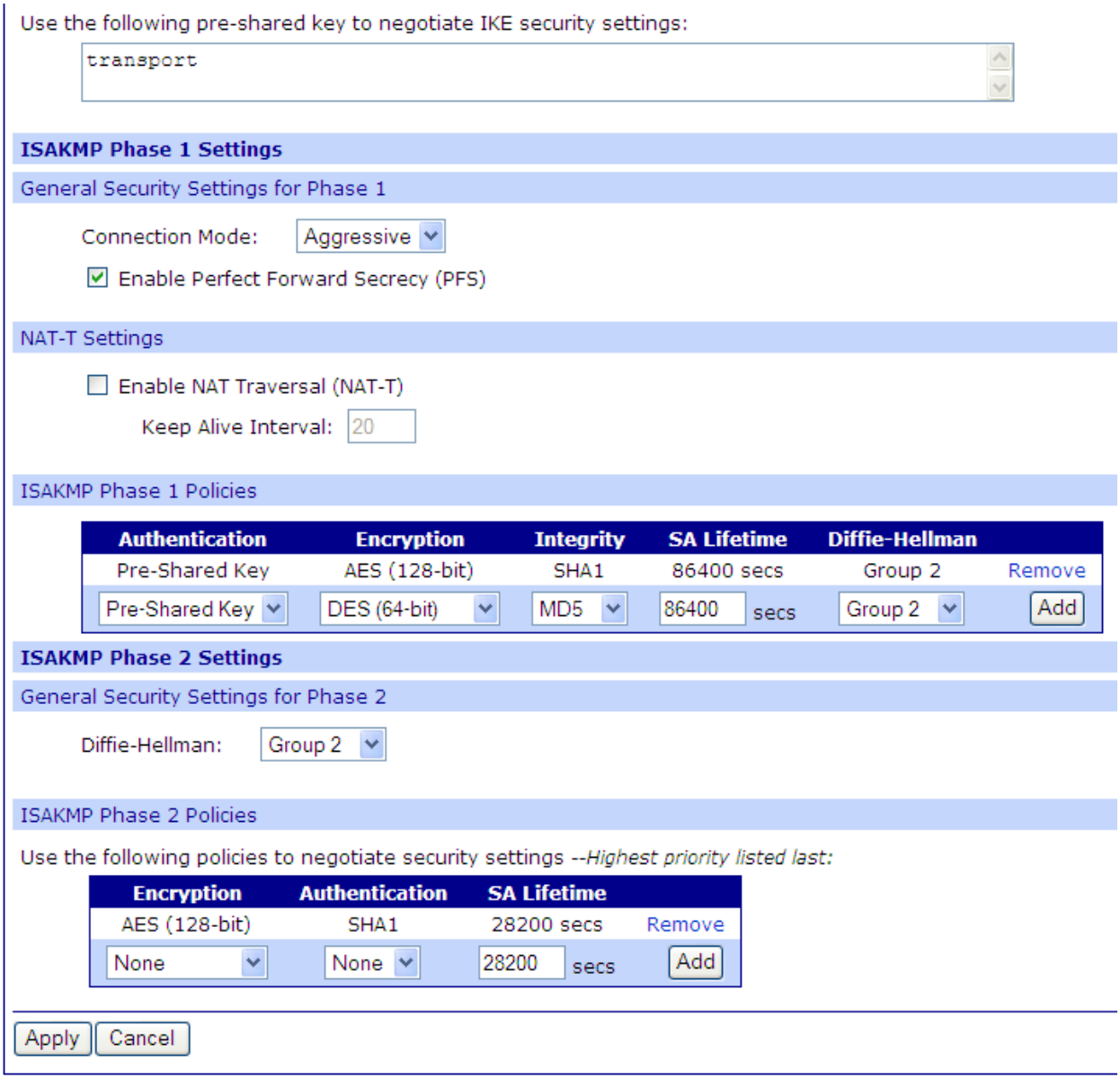


Figure 3-4: ConnectPort WAN VPN Settings

4 TESTING

The VPN tunnels can be tested by viewing the IPSec peers, the IKE and IPSec security associations and the Eroute under **Diagnostics - Status > IPsec > IPSec SAs** on the TransPort, and by pinging the end device from the other end device. The following figures/screen captures were taken at different times, so there is some duplication.

4.1 View the IPSec Peers

Figure 4-1 shows the peers of the VC7400, which shows the Peer IP, which is the dynamic public IP address of the TransPort SR's W-WAN interface, the Peer ID of "digitransportsr" and Our ID "digivc7400". Figure 4-2 shows the IPSec peer of the SR, which shows the Peer IP of the VC7400 and the Peer ID and Our ID settings.

Diagnostics - Status > IPsec > IPsec Peers

IPSec Peers

Peer IP	Our ID	Peer ID	DPD	NATT local port	NATT remote port
70.57.159.140	0.0.0.0	70.57.159.140	Inactive. Next REQ in 113 secs	N/A	N/A
75.216.93.39	digivc7400	digitransportsr	Active (60). Next REQ in 124 secs	N/A	N/A

Remove all unused

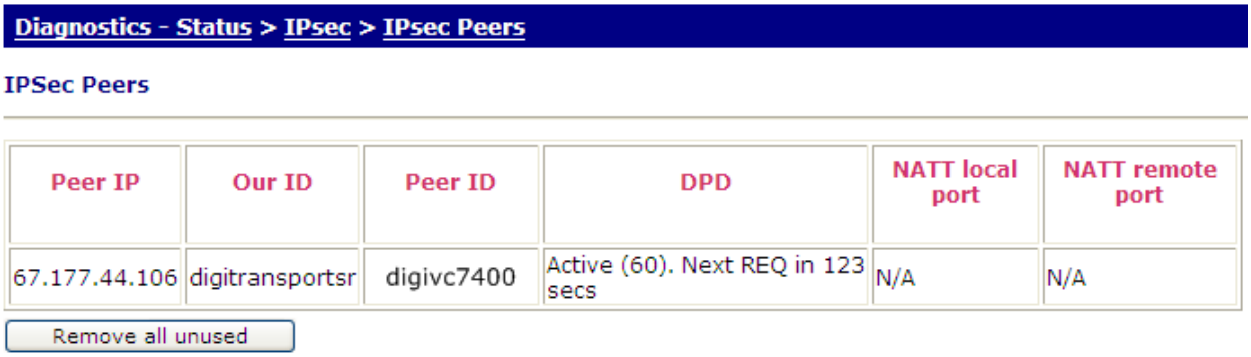
Diagnostics - Status > IPsec > IPsec Peers

IPSec Peers

Peer IP	Our ID	Peer ID	DPD	NATT local port	NATT remote port
70.193.194.217		user1@digi.com	N/A	N/A	N/A
70.57.159.140	0.0.0.0	70.57.159.140	Active (2). Next REQ in 118 secs	N/A	N/A

Remove all unused

Figure 4-1: VC7400 IPSec Peers



Diagnostics - Status > IPsec > IPsec Peers

IPSec Peers

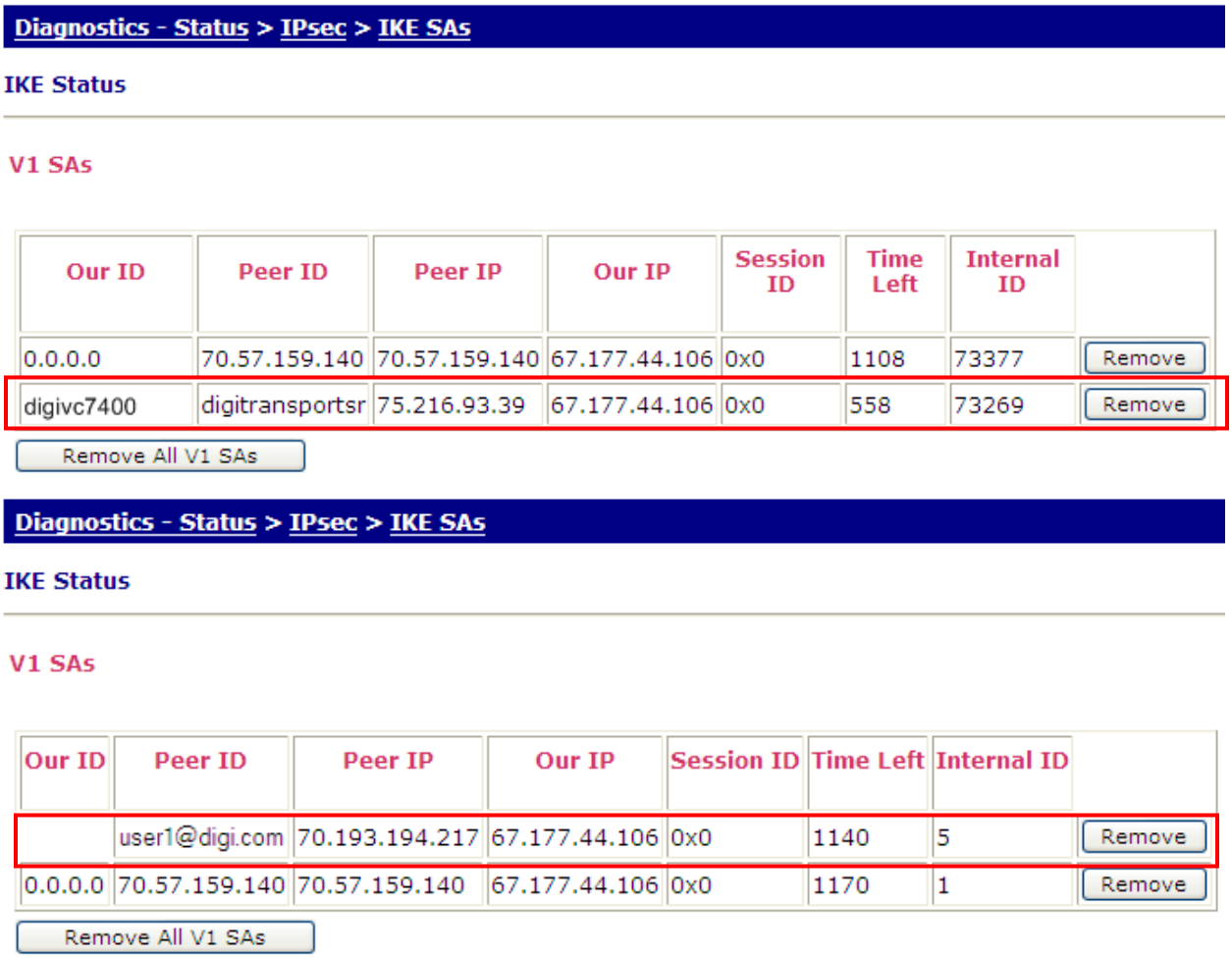
Peer IP	Our ID	Peer ID	DPD	NATT local port	NATT remote port
67.177.44.106	digitransportsr	digivc7400	Active (60). Next REQ in 123 secs	N/A	N/A

Remove all unused

Figure 4-2: TransPort SR IPSec Peers

4.2 View the IKE Security Associations

Figures 4-3 and 4-4 show the IKE version 1 security associations of the VC7400 and TransPort SR router respectively, consisting of the DR's and SR's IDs and IP addresses.



Diagnostics - Status > IPsec > IKE SAs

IKE Status

V1 SAs

Our ID	Peer ID	Peer IP	Our IP	Session ID	Time Left	Internal ID	
0.0.0.0	70.57.159.140	70.57.159.140	67.177.44.106	0x0	1108	73377	Remove
digivc7400	digitransportsr	75.216.93.39	67.177.44.106	0x0	558	73269	Remove

Remove All V1 SAs

Diagnostics - Status > IPsec > IKE SAs

IKE Status

V1 SAs

Our ID	Peer ID	Peer IP	Our IP	Session ID	Time Left	Internal ID	
	user1@digi.com	70.193.194.217	67.177.44.106	0x0	1140	5	Remove
0.0.0.0	70.57.159.140	70.57.159.140	67.177.44.106	0x0	1170	1	Remove

Remove All V1 SAs

Figure 4-3: VC7400 IKE SAs

Figure 4-4: TransPort SR IKE SAs

4.3 View the IPSec Eroute

Figures 4-5 and 4-6 show the IPSec Eroutes which display the peer IP address, the remote and local selectors (the local subnets for each device), the ESP authentication and encryption, and the outbound interface.

Diagnostics - Status > IPsec > IPSec SAs > Eroute 0 - 9 > Eroute 1

IPSec Status: Eroutes 1 -> 1

Outbound V1 SAs

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
725b9ac3	1	75.216.93.39	172.16.2.0/24	192.168.1.0/24	N/A	SHA1	AES (128)	N/A	20	980	1120	ETH 5	Remove

Remove All

Inbound V1 SAs

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
32402c26	1	75.216.93.39	172.16.2.0/24	192.168.1.0/24	N/A	SHA1	AES (128)	N/A	52	948	1120	ETH 5	Remove

Remove All

Outbound V2 SAs

Diagnostics - Status > IPsec > IPSec SAs > Eroute 0 - 9 > Eroute 2

IPSec Status: Eroutes 2 -> 2

Outbound V1 SAs

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
c316ef7d	2	70.193.194.217	172.16.100.0/24	192.168.1.0/24	N/A	SHA1	AES(128)	N/A	0	1000	1116	ETH5	Remove

Remove All

Inbound V1 SAs

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
b8f3d36e	2	70.193.194.217	172.16.100.0/24	192.168.1.0/24	N/A	SHA1	AES(128)	N/A	0	1000	1116	ETH5	Remove

Remove All

Figure 4-5: VC7400 IPSec Eroute 0 and Eroute 2

Diagnostics - Status > IPsec > IPSec SAs

IPSec Status: Eroutes 0 -> 4

Outbound V1 SAs

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
32402c26	0	67.177.44.106	192.168.1.0/24	172.16.2.0/24	N/A	SHA1	AES (128)	N/A	208	792	912	PPP 1	Remove

Remove All

Inbound V1 SAs

SPI	Eroute	Peer IP	Rem. selector	Loc. selector	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
725b9ac3	0	67.177.44.106	192.168.1.0/24	172.16.2.0/24	N/A	SHA1	AES (128)	N/A	75	925	912	PPP 1	Remove

Remove All

Outbound V2 SAs

Figure 4-6: TransPort SR IPSec Eroute 0

4.4 Digi ConnectPortWAN

On the Digi ConnectPort WAN, the VPN tunnels can be viewed under Management ->Connections. The status will be “Connected”. If it says “enabled” the policy is in place but the VPN tunnel is not up.

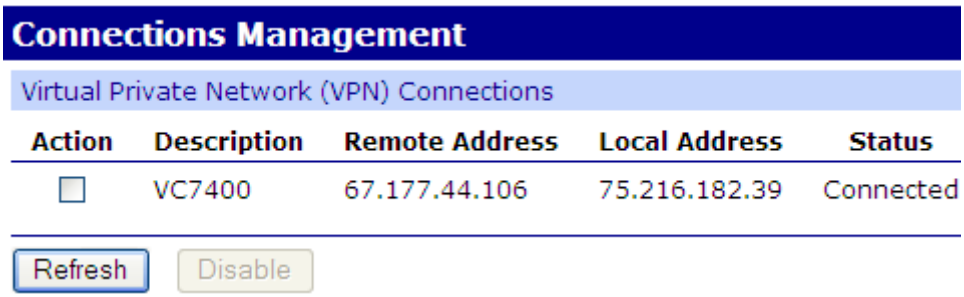


Figure 4-7: ConnectPortWAN Connections

4.5 Ping/Traffic test

If in the above sections the SA’s can be seen then the tunnel is up, the next step is to confirm the connectivity by sending a ping or passing some kind of network traffic (e.g., HTTP, Telnet, FTP, etc.) through the tunnel from one endpoint to the other.