



APN002 – IPsec Capabilities Package

APN002 - 17 February, 2009

1. SCOPE

Application Note APN002 is intended to be used by personnel with a working knowledge of IPsec set up procedures on the equipment to be used for a far end gateway. This is not an IPsec tutorial.

2. INTRODUCTION

Internet Protocol Security (IPsec) is a suite of protocols used to securely transmit and receive an Internet Protocol (IP) data stream. From a set up perspective the most visible component of IPsec is the Internet Key Exchange mechanism (IKE) which is used to establish a Security Association (SA) through protocols that authenticate a session and negotiate cryptographic keys. IPsec is specified by the IETF in RFC 4301 and RFC 4309.

3. CREDITS

Ctek's IPsec implementation is based on the Openswan implementation (<http://www.openswan.org/>) with adaptations to compensate for the specific behaviors of cellular networks.



APN002 – IPsec Capabilities Package

APN002 - 17 February, 2009

4 Set Up – Overview

To set up and administer an IPsec connection on a Ctek SkyRouter select the VPN button as shown in figure 1 below.

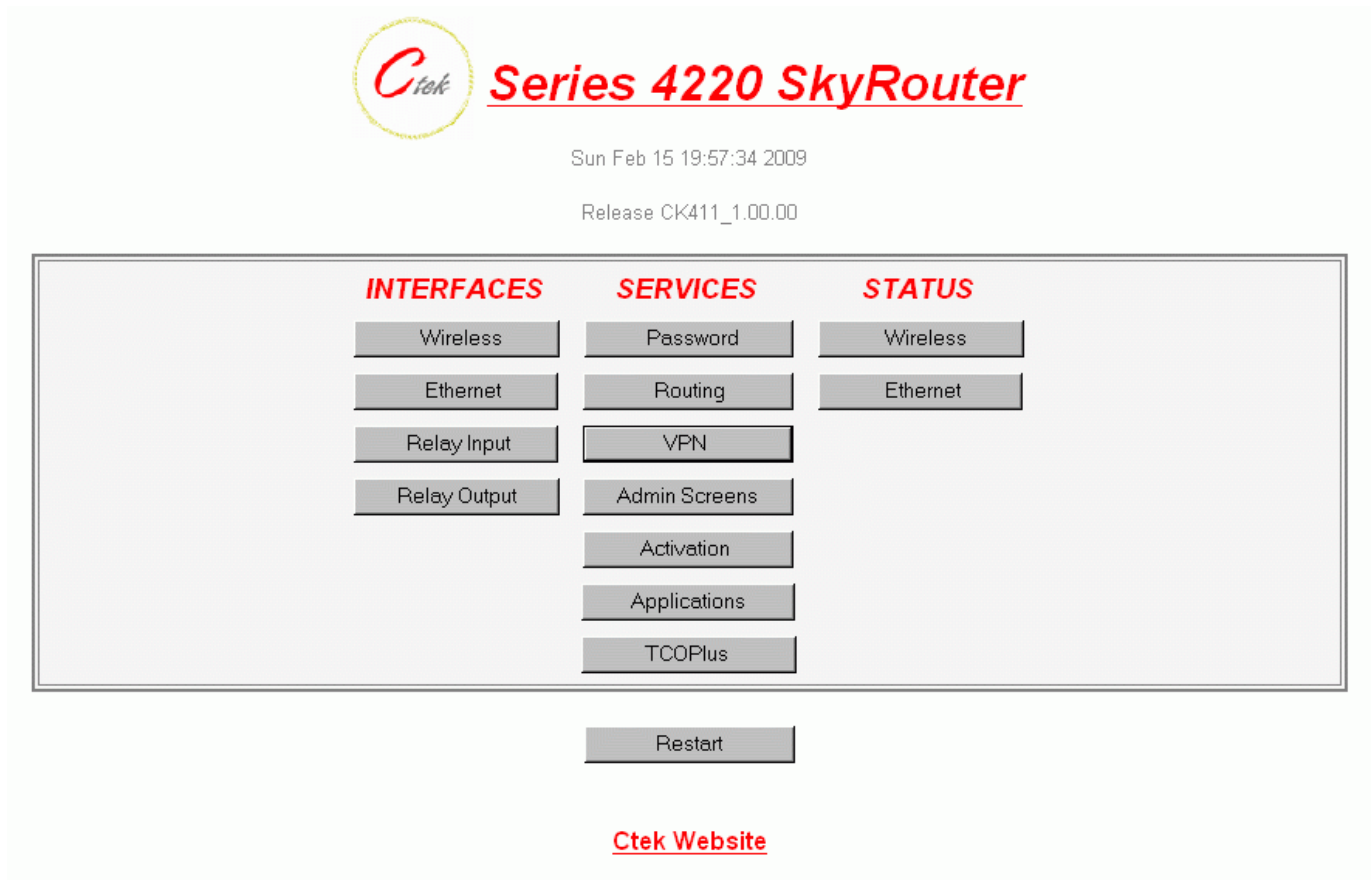


Figure 1

The VPN selection will take your browser to the top level IPsec administration screen where you are offered the three top level IPsec administrative functions available under this release. Figure 2 shows these choices.



APN002 – IPsec Capabilities Package

APN002 - 17 February, 2009

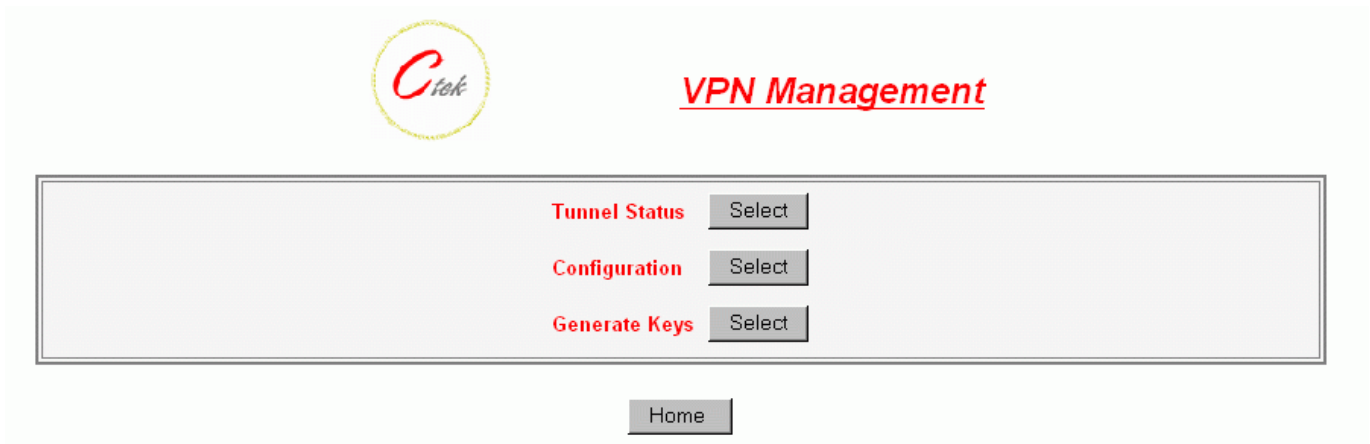


Figure 2

Tunnel Status

The tunnel status screen displays the current state of the IKE process and the current status of the tunnel as shown in figure 3 below.

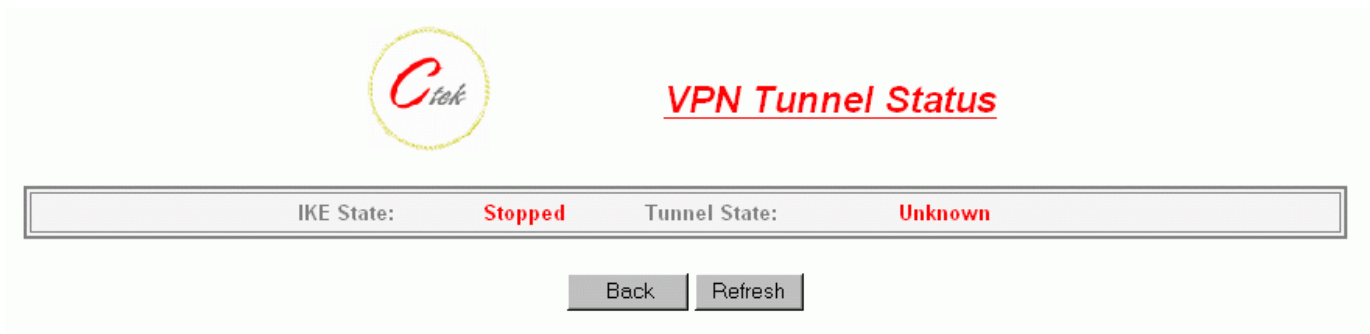


Figure 3



APN002 – IPsec Capabilities Package

APN002 - 17 February, 2009

VPN Tunnel Status Values Are:

Ike State – Unknown, Stopped, Running

Tunnel Status – Unknown, Up, Down

Generate Keys

The Generate Keys function will generate new cryptographic keys to be used between the SkyRouter and the Gateway or Firewall at the head end. Selecting this function brings up the screen shown in figure 4.



Figure 4

WARNING – Key generation will take at least thirty (30) minutes to complete.

Start - Initiates the creation of new keys.

Status – Displays the progress of key generation



APN002 – IPsec Capabilities Package

APN002 - 17 February, 2009

Configuration

The Configuration selection is used to select the parameters that will be used to negotiate and operate an IPsec tunnel between the SkyRouter and the host gateway or firewall. Selection choices are shown in figure 5.

The screenshot displays the 'VPN Configuration' interface. At the top left is the Ctek logo. The title 'VPN Configuration' is centered in red. Below the title are three controls: 'VPN: Disabled' (dropdown), 'Tunnel Restart Events: None' (dropdown), and 'Test Log: Off' (checkbox). The interface is divided into three main panels:

- Remote VPN Gateway:** Gateway IP: 72.215.211.110, Subnet IP: 192.168.0.0, Subnet Mask: 255.255.255.0
- Authentication And Encryption:** Pre-shared key: a secret key, PFS: Enabled, Mode: Main, Re-key: Enabled, Key life: 60 (min)
- Phase 1 and Phase 2:** Phase 1: Encryption: AES, Authentication: SHA1, Group: 1024; Phase 2: Encryption: AES, Authentication: MD5, Group: 1536

At the bottom are 'Update' and 'Back' buttons.

Figure 5

The IPsec configuration screen is divided into a control header and two discrete panels. Each panel and its associated attributes is discussed below.



APN002 – IPsec Capabilities Package

APN002 - 17 February, 2009

Control Header:

VPN – Selections are Enabled or Disabled. When Enabled inbound traffic is blocked at the router's firewall, NAT is turned off, and remote administration is turned off. When Disabled all settings are returned to their original state. Once a connection is established Remote Administration may be re-enabled for diagnostic purposes but should not be left on in a production environment.

Tunnel Restart Events – Selects the conditions under which the SkyRouter will restart the tunnel.

Choices are:

None – rely on gateway for restarts

Loss of IP Address – Wireless network invalidated the SkyRouter's IP address

Change of IP Address – Wireless network assigned new IP address

Loss/Change of IP Address – Covers both conditions above

Test Log – Selections are ON or OFF. When ON is selected debug information concerning tunnel creation is output on the unit's serial application port (green connector) at 115.2 kbs. Lap top programs like Hyperterm or Minicom can be used to view it. **Caution** – Logging should be turned off for production. Consult the specific User Manual for your model to configure the serial application port.

Remote VPN Gateway Panel:

Gateway IP – The public IP address of the Gateway or Firewall with which the SkyRouter will establish a tunnel.

Subnet IP – The subnet address range upon which the router will operate for communications through the tunnel.

Subnet Mask - The mask that defines the range of subnet addresses available for tunnel operation.



APN002 – IPsec Capabilities Package

APN002 - 17 February, 2009

Authentication and Encryption Panel:

PFS – Perfect Forward Secrecy. Available settings are Enabled or Disabled

Re-Key – Available settings are Enabled or Disabled. When Enabled will re-key at a rate established by Key Life. When Disabled the re-key operation can still be forced by the far end gateway.

Mode – Available settings are Main or Aggressive. Defines the number of exchanges used to complete IKE Phase 1. Main is the more robust setting while aggressive mode uses few exchanges and is therefore somewhat more risky.

Key life – Key Life specifies the interval (in minutes) that a key will be valid.

Note – Phase 1 and Phase 2 on this panel refer to IKE Phase 1 and IKE phase 2.

During IKE phase 1 IKE authenticates IPsec peers and negotiates IKE Security Associations (SAs), setting up a secure channel for negotiating IPsec SAs in phase 2.

During IKE phase 2 IKE negotiates IPsec SA parameters and sets up matching IPsec SAs in the peers.

The selection choices with this panel for Phase 1 and Phase 2 are identical but repeated so that different choices can be applied to Phase 1 and Phase 2.



APN002 – IPsec Capabilities Package

APN002 - 17 February, 2009

Pull Down Selections For Phase 1 and Phase 2:

Encryption – Choices are Auto, NONE, 3DES, or AES. In Auto mode the actual mode will be negotiated with the other end. The NONE setting is used for un-encrypted tunnels such as L2TP.

Authentication – Choices are Auto, SHA1, or MD5. In Auto mode the actual mode will be negotiated with the other end.

Group – Defines what size modulus to use for Diffie-Hellman calculation. Choices are Auto, 1024, or 1536. In Auto mode the actual mode will be negotiated with the other end. Group 768 is not offered as it is viewed as being too weak for commercial implementations.