Ctek
Industrial Control

IPSEC Tunnel Configuration

Tech Note – TN1002

December 2, 2020

1891 N. Gaffey St. Ste. E
San Pedro, CA 90731

p. 310.241.2973

support@ctekproducts.com
www.ctekproducts.com

Table of Contents

Introduction

Application Note AN002 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.

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.

Setup Overview

To set up and administer an IPsec connection on a Ctek SkyRouter select the IPSec Tunneling button on the Routers home screen. Shown below in Figure 1.

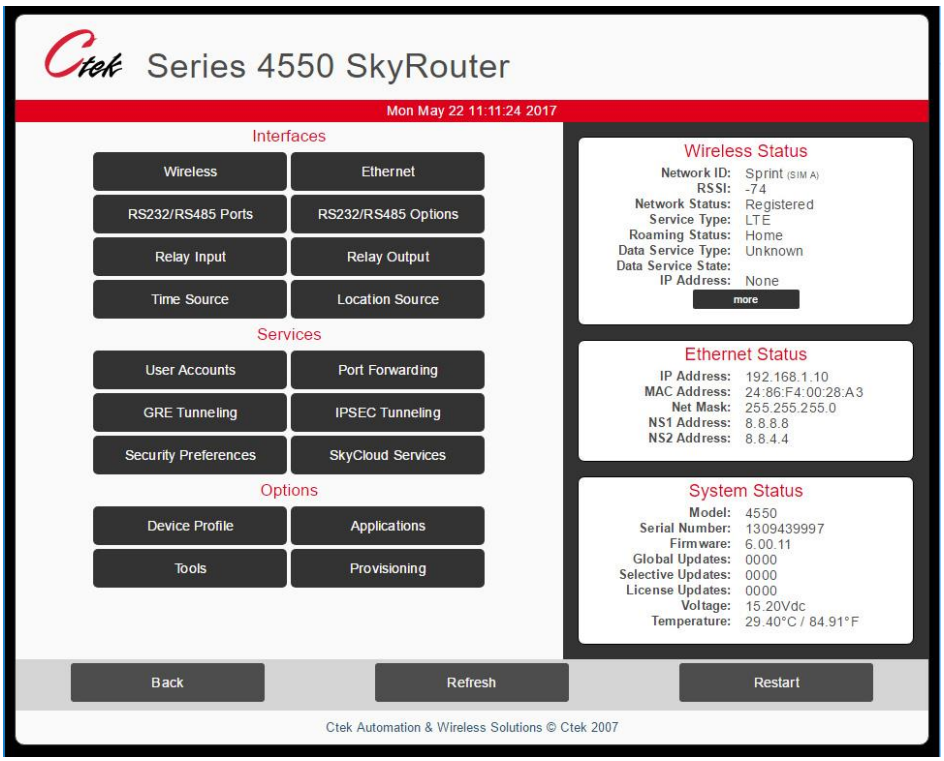

Figure 1

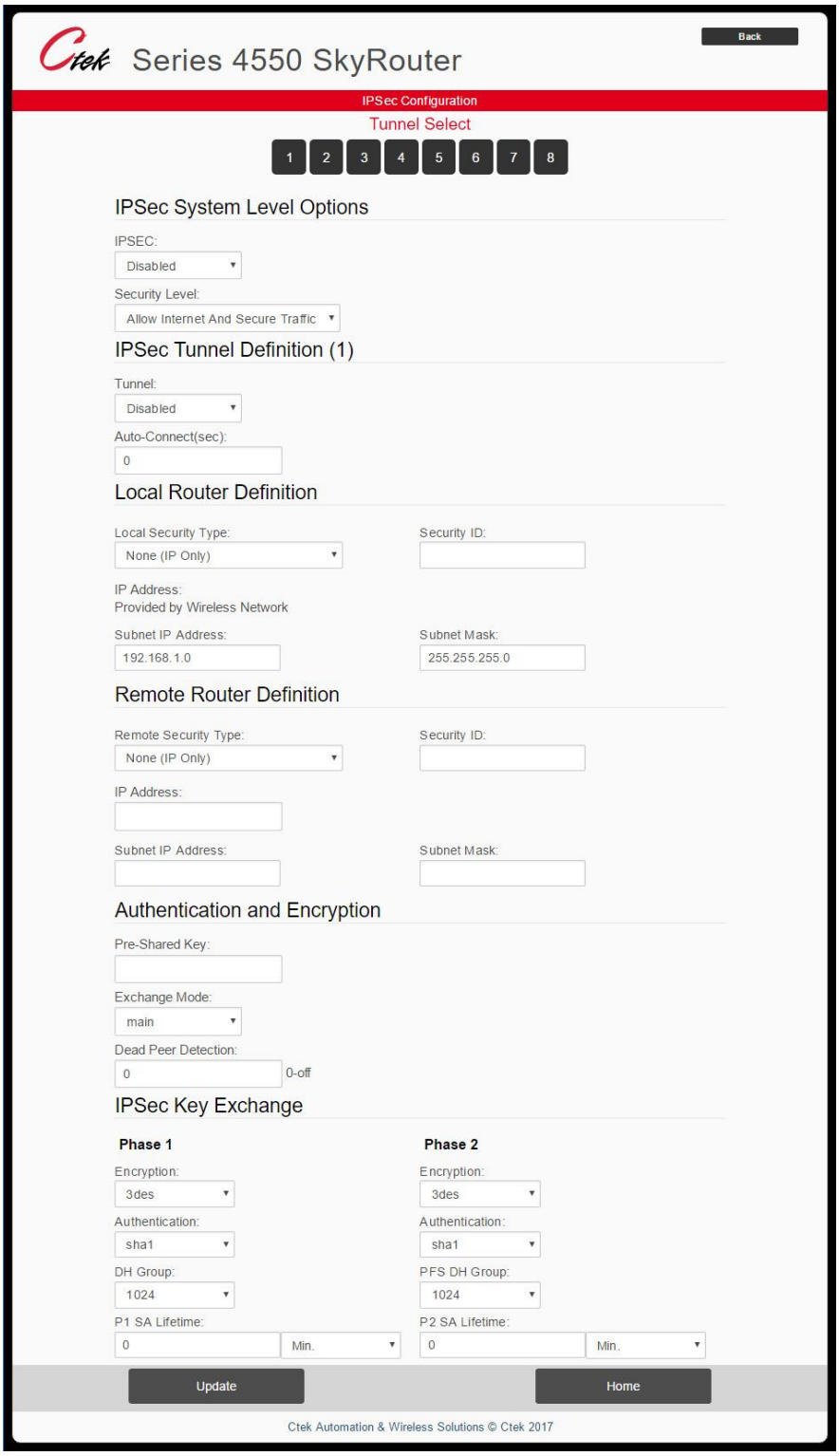
Series 4550 SkyRouter
Back
IPSec Configuration
Tunnel Select
1 2 3 4 5 6 7 8
IPSec System Level Options
IPSEC:
Disabled
Security Level:
Allow Internet And Secure Traffic
IPSec Tunnel Definition (1)
Tunnel:
Disabled
Auto-Connect(sec):
0
Local Router Definition
Local Security Type:
None (IP Only)
Security ID:
IP Address:
Provided by Wireless Network
Subnet IP Address:
192.168.1.0
Subnet Mask:
255.255.255.0
Remote Router Definition
Remote Security Type:
None (IP Only)
Security ID:
IP Address:
Subnet IP Address:
Subnet Mask:
Authentication and Encryption
Pre-Shared Key:
Exchange Mode:
main
Dead Peer Detection:
0
0-off
IPSec Key Exchange
Phase 1
Encryption:
3des
Authentication:
sha1
DH Group:
1024
P1 SA Lifetime:
0
Min.
Phase 2
Encryption:
3des
Authentication:
sha1
PFS DH Group:
1024
P2 SA Lifetime:
0
Min.
Update
Home
Ctek Automation & Wireless Solutions © Ctek 2017

Figure 2

Tunnel Select

Allows you to switch between up to eight different tunnels that you can configure.

IPSec System Level Options

- IPSec: Enable or disable IPSec on this tunnel.
- Security Level: Can use the drop down window to determine if you will allow only secure traffic or a mix of secure and Internet traffic going to the IP Address assigned by the wireless carrier. If set to Allow Only Secure Traffic it will only acknowledge connections coming through the tunnel. Allow Internet and Secure Traffic will acknowledge connections coming through the tunnel or the public Internet.

IPSec Tunnel Definition

- Tunnel: Can use the drop down window to Enable or Disable the defined Tunnel.
- Auto-Connect: allows you to specify how long to wait before automatically reestablishing the IPSec tunnel. Time defined in Seconds.

Local Router Definition

- Local Security Type: Can use the drop down window to choose between
    - None (IP only)
    - IP + Domain Name (FQDN)
    - IP + Email Address (user FQDN)
    - IP + Key ID (Key ID)
- Security ID: Relates to the local security type. (ie. If you chose IP + Email the Security ID would be email@domain.com)
- IP Address: Will automatically be assigned by the wireless provider and cannot be changed.
- Subnet IP Address: 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.

Remote Router Definition

- Remote Security Type: Can use the drop down window to choose between
    - None (IP only)
    - IP + Domain Name (FQDN)
    - IP + Email Address (user FQDN)
    - IP + Key ID (Key ID)
- Security ID: Relates to the local security type. (ie. If you chose IP + Email the Security ID would be email@domain.com)
- IP Address: The public IP address of the Gateway or Firewall with which the SkyRouter will establish a tunnel.
- Subnet IP Address: 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.

Authentication and Encryption

- Pre-Shared Key: A key value defined and distributed outside of this network.
- Exchange Mode: Can use the drop down window to choose between Main and Aggressive modes. This 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.
- Dead Peer Detection: Allows you to define how much time the router will wait without receiving any transition before sending a detection packet to confirm that the other end is still connected. Time measured in seconds.

IPSec Key Exchange

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.

- Encryption: Can use the drop down window to choose between 3DES and AES encryption.
- Authentication: Can use the drop down window to choose between SHA1 and MD5 hashes.
- Diffie Hellman (DH) Group: Can use the drop down window to choose between 768, 1024, 1536, and 2048 bit keys.
- Perfect Forward Secrecy (PFS) DH Group: Can use the drop down window to choose between No PFS, 768, 1024, 1536, and 2048 bit keys.
- Security Association (SA) Lifetime: Allows you to set the specific amount of time before a new key is generated and used for the connection. Can use the drop down window to choose between minutes and seconds.