Using Omnisec 421 IP VPN Clients Over BGAN

Secure VPN

Version 01

27th December 2009

Contents

1 Overview

Satellite communications can be intercepted from almost anywhere. For this reason, protecting one's information against eavesdropping and intrusion is of paramount importance in such scenarios. In particular, mobile users want the assurance that their communications with their headquarters via the Internet are entirely secure. In addition, a single satellite connection should allow any IP application on the client computer to communicate securely with the corporate network.

2 Benefits to BGAN Users

The Omnisec 421 offers the following benefits to BGAN users:

- A security solution built on Swiss-made IP Encryptors and convenient-to-use portable Security Modules, which provides maximum protection for all kinds of IP-based traffic over Inmarsat BGAN and the Internet
- Mobile users – wherever in the world they may be – are able to connect easily to common services normally accessed through a direct Internet connection
- Strong user authentication and proprietary 256-bit symmetric key encryption assures total confidentiality and guaranteed integrity of all data traffic from any IP-based application.

3 Possible Application Scenarios

- Secure e-mail applications
- Secure Intranet applications (HTML, FTP, Java,…)
- Secure fleet management
- Secure company-wide information management
- Secure videoconferencing
- Secure voice-over-IP.

4 Typical Users

- Traveling government agents
- Mobile military and defense personnel
- Police and security forces
- Oil, gas, and mining organizations
- Traveling private decision-makers of banking, financial, and multinational corporations.

5 Technical Details

5.1 Omnisec 421 – Overview

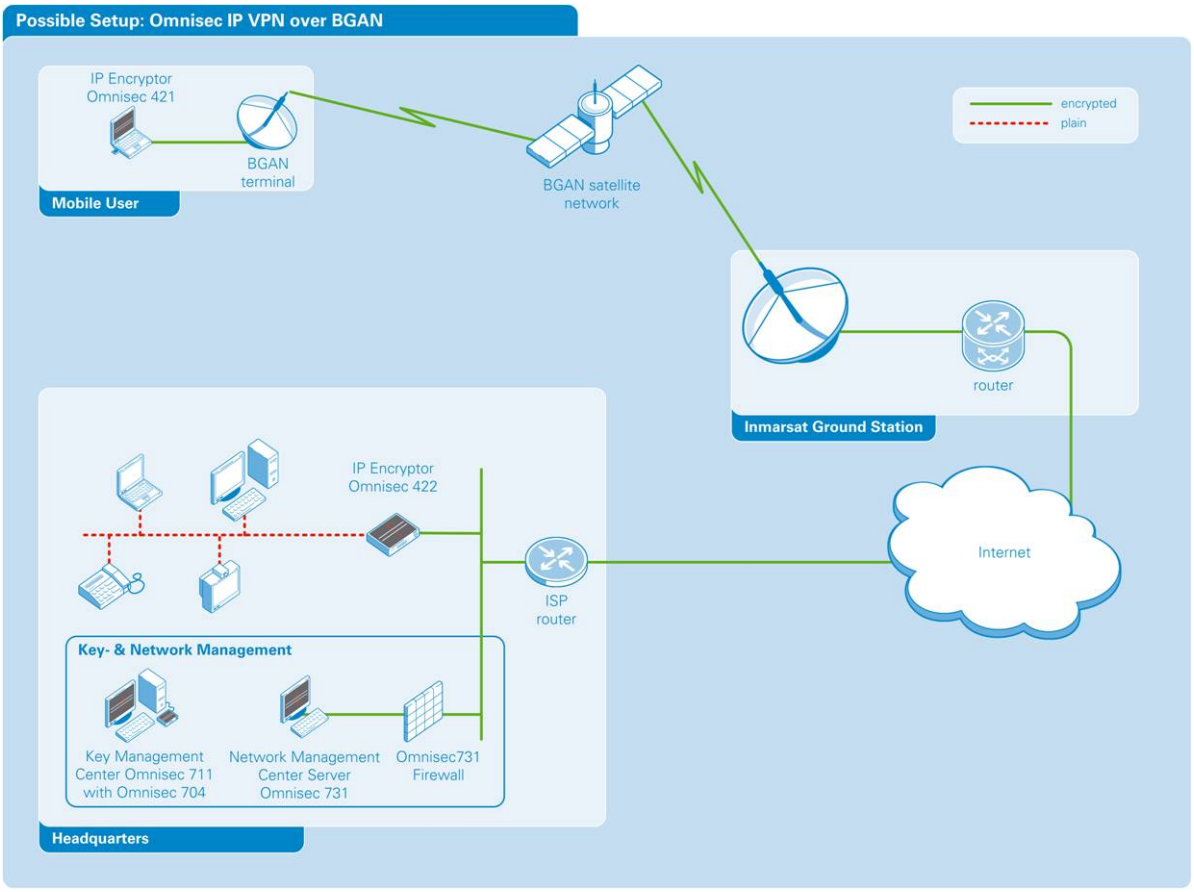
The Omnisec 421 is a member of Omnisec's family of IP Encryptors, which together constitute the Omnisec IP-based VPN – a reliable Virtual Private Network solution offering the highest level of security.

The Omnisec 421 is a Windows application allowing mobile users or single-system branches to communicate securely with their headquarters. All IP-bound traffic is encrypted by the Omnisec 421 Virtual Adapter (NDIS Driver) using secret keys stored in the Security Module.

5.2 Omnisec 421 over BGAN

A mobile user with a BGAN terminal makes an encrypted satellite connection to an Inmarsat Ground Station. From there the secure communication continues via the Internet to the corporate headquarters site, which is equipped with one of the other members of the IP Encryptor family, Omnisec 422 or Omnisec 423. Any application within the headquarters network can thus be accessed by the remote user.

The headquarters typically also houses the Key Management Center (for generating the secret Master Keys and programming the Security Modules), and the firewall-protected Network Management Center (for configuring and monitoring all IP Encryptors in the network).



6 Omnicrypt™ Security Architecture

The multi-barrier Omnicrypt™ Security Architecture, OSA, raises IP encryption to the highest level of security. The strength of OSA is based among other things on the following fundamental security building blocks:

6.1 Key and Network Management

Secret bilateral Master Keys are generated either by means of the Built-in Key Equipment (BIKE) utility within the IP Encryptor Omnisec 422 or Omnisec 423 (for small networks), or by the Key Management Center application, Omnisec 711, in conjunction with the Security Module Programmer Omnisec 704 (for networks of any size). Efficient and flexible Network Management is assured by the Network Management Center, Omnisec 731; a decentralized client-server application.

All network traffic is encrypted using short-lived symmetric 256-bit Session Keys, derived from the secret Master Keys.

6.2 Security Modules

All the secret information required for encryption and decryption is safely contained in a convenient, portable Security Module (SM). The integrated microprocessor within the SM controls an electronic data store, which is protected both against read-out and tampering.

6.3 Cryptography

The 256-bit symmetric encryption algorithms developed by Omnisec offer unsurpassed levels of security.

7 Setup and Configuration

7.1 BGAN Considerations

MTU Setting

It is recommended to change the client computer's MTU size to a maximum of 1300 bytes in order to avoid network congestion within the satellite network. The reason to do so lies in the IP overhead added by the encryption process (up to 86 bytes per packet). Best performance is achieved when this setting is not only applied on the client end but also at the HQ site.

Note: The MTU Size is set on the Omnisec Virtual Adapter Property Dialog under Ethernet Settings.

When the MTU Size is set, any Path MTU Discovery features in the network devices can be turned off. This will stop the devices from checking the network for the best MTU size.

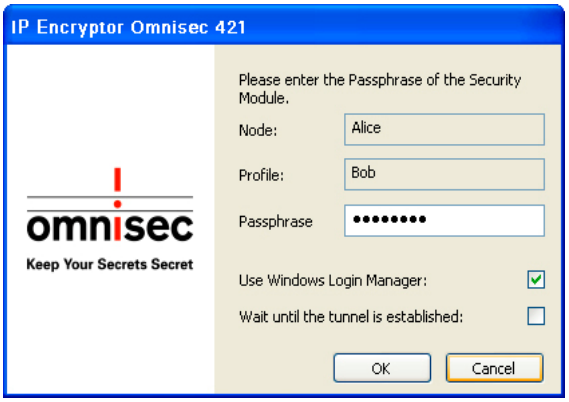
Note: In Windows, the Path MTU Discovery is turned off (0 = false) by altering the value of the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery.

7.2 Omnisec 421 System Requirements

Windows XP or Vista with the latest Service Pack installed, min. 512 MB RAM, min. 20 MB disk space, USB interface to connect the Security Module.

7.3 Handling of the Security Module

As soon as the Security Module is inserted into your computer's USB port, all IP connectivity is cut off. You first have to authenticate yourself to the Security Module by entering your PIN or passphrase at this prompt.



7.4 Required Equipment

Typical example:

- At least one IP Encryptor, Omnisec 422 or Omnisec 423, at the headquarters site (including one programmed Security Module per unit)
- At least one Omnisec 421 for the mobile client computer (including a programmed Security Module)
- Key Management Center Omnisec 711 with SM Programmer Omnisec 704 (or BIKE utility for small networks) and two Network Security Modules (N-SMs)
- Network Management Center Omnisec 731, Omnisec 731 Firewall, two programmed Configuration Security Modules (C-SMs), and one programmed Personal Security Module (P-SM)
- BGAN terminal: Thrane & Thrane Explorer™ 500, or Explorer™ 700, or Hughes HNS 9201 with terminal adapter
- BGAN SIM card from the local Inmarsat service provider
- Videoconferencing system (if required).

7.5 Setting up an Omnisec 421 Connection

After initial programming of the Security Modules, proceed as follows to set up BGAN for use with the IP Encryptor Omnisec 421.

- Install the Omnisec 421 software and the USB driver for the Security Module on the client computer
- Connect your computer via an Ethernet cable to the RJ-45 port of the BGAN terminal
- Start up Inmarsat LaunchPad to configure the BGAN terminal to register with the satellite network (for further assistance please consult the terminal's user guide)
- Check IP connectivity over the BGAN terminals by browsing a known website (e.g. www.omnisec.ch)
- Insert the pre-programmed Equipment Security Module (E-SM) into a USB port of the client computer and log in with your PIN or passphrase

An Omnisec IP-VPN tunnel will be established to the trusted headquarters network, enabling the use of any IP-based application from your client computer.

8 Further Details and Support

Inmarsat Contact:

E-mail: customer_care@inmarsat.com

Omnisec AG Contact:

E-mail: bgan@omnisec.ch

Web: www.omnisec.ch/421

Postal address: Rietstrasse 14
CH-8108 Dällikon
Switzerland

Phone: +41 44 847 67 11