Using Omnisec 422 and 423 IP Encryptors Over BGAN

Version 02

29th 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, users want the assurance that their site-to-site communications via the Internet are entirely secure. In addition, a single satellite connection should allow any IP application on the client computer to communicate securely across the corporate network.

2 Benefits to BGAN Users

The Omnisec IP-based VPN 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
- 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 or Intranet applications (HTML, FTP, Java,…)
- Secure fleet management
- Secure company-wide information management
- Secure videoconferencing or voice-over-IP

4 Typical Users

- Government agencies, such as Military and defense personnel
- Police and security forces
- Oil, gas, and mining organizations
- Large banking, financial, and multinational corporations

5 Product Range

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

The Omnisec IP-based VPN establishes extremely secure site-to site communications for the exchange of e-mails, files, data, and voice over a corporate IP-based network or the Internet. Route-based VPN maximizes throughput by supporting redundant VPN communication paths with dynamic fallback mechanisms (VPN re-routing, relays) and load-sharing.

Omnisec's high-quality devices integrate easily into existing networks including third-party products (e.g. firewalls, virus checkers, intrusion detectors), and provide appropriate scalability to ensure the desired performance.

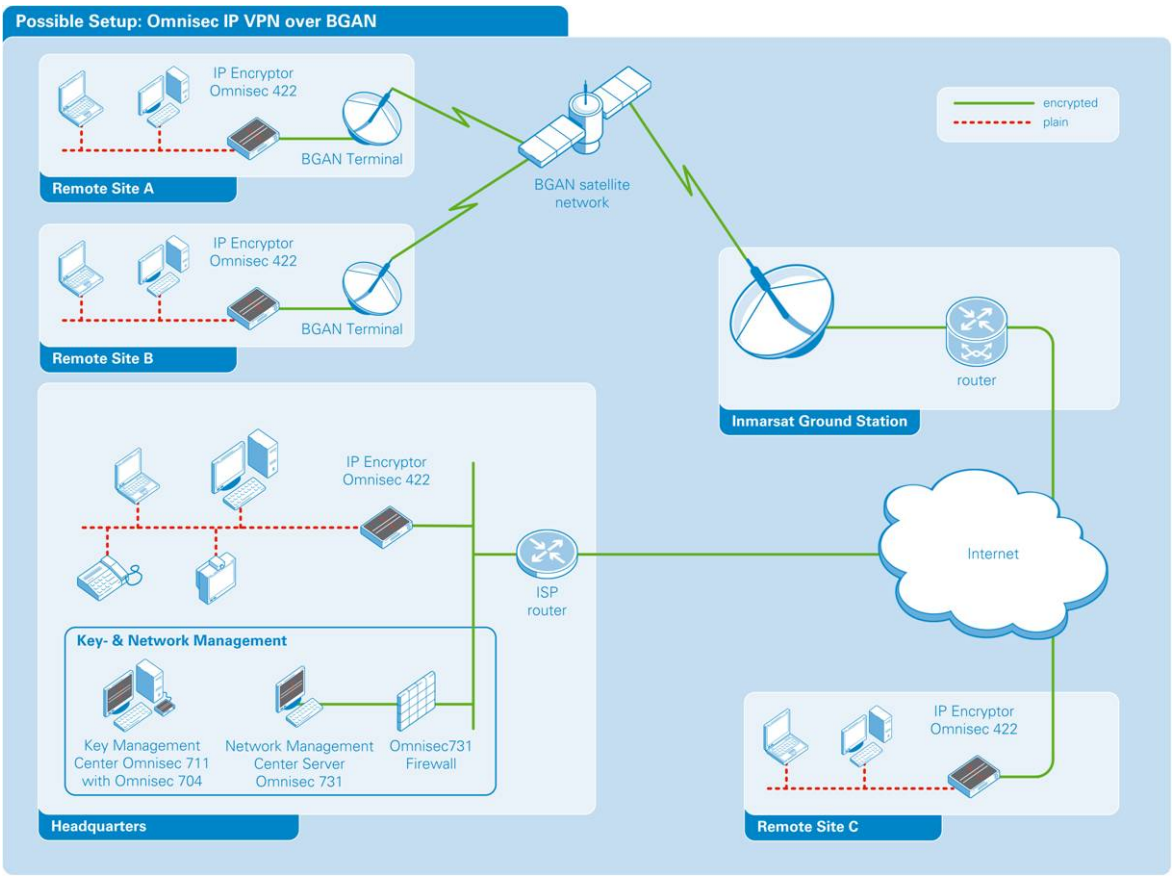
The IP Encryptor **Omnisec 423** is a 19" rack-mountable device. Its acceleration hardware provides the necessary performance for deployment in major sites such as a headquarters.

For lower-performance applications, the complementary **Omnisec 422** is the choice.

Single-system branches or mobile users can be securely connected using the IP Encryptor **Omnisec 421**. Please refer also to the solution sheet "Using Omnisec 421 IP VPN Clients Over BGAN".

6 Omnisec IP-based VPN over BGAN

Remote or mobile sites equipped with a BGAN terminal establish an encrypted satellite connection to an Inmarsat Ground Station. From there the secure communication continues via the Internet to other corporate sites, each equipped with a compatible IP Encryptor, Omnisec 422 or Omnisec 423. Any application within the headquarters network can thus be accessed remotely via satellite.



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).

7 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:

7.1 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.

7.2 Security Modules

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

7.3 Cryptography

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

8 Special BGAN Considerations

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.

9 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 422 for the remote site (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).
-

10 Setting up an Omnisec IP VPN Connection via BGAN

After initial programming of the Security Modules, proceed as follows to set up a BGAN connection with the IP Encryptors Omnisec 422 and 423.

- 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)
- Integrate the IP Encryptor in your network
- Use Ethernet cables to connect PORT 0 (Trusted) of your Omnisec 422 to the computer or in-house router and PORT 1 (Untrusted) via an Ethernet cable to the RJ-45 port of the BGAN terminal
- Insert the programmed E-SM into SM slot A (with help of the KESO key)
- Log in to the IP Encryptor as Configuration Manager with the appropriate PIN
- Work through the menu 'Connect to Management Center', setting the necessary IP parameters; the IP Encryptor is now ready to be finally configured from the Network Management Center Omnisec 731

Omnisec IP-VPN tunnels will be established from the remote LAN across the satellite link to the trusted corporate network, enabling the use of any IP-based application.

11 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