

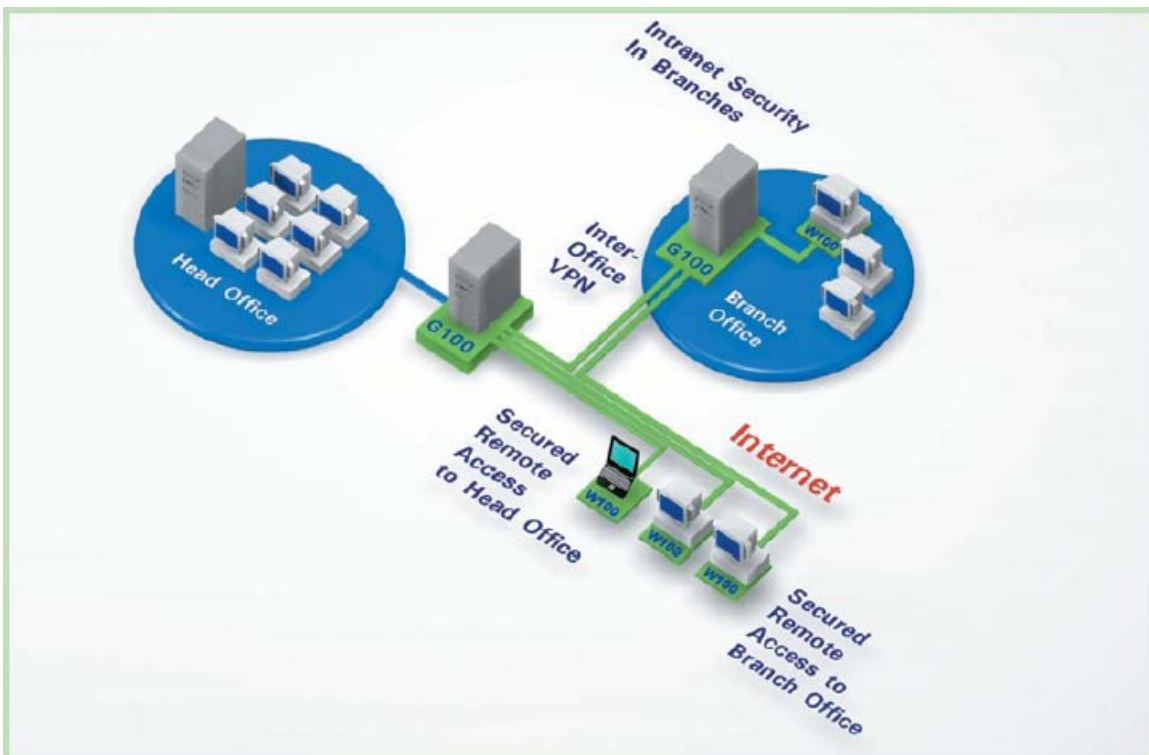


## Gateway Software

The Rock VPN Gateway Software is a part of the Rock VPN suite of products. Used in conjunction with other Rock VPN product models or with third party IPSec compliant products, the Gateway Software allows you to set up secure communications to other Rock VPN gateways, Server Protectors or user workstations running the Rock VPN Workstation software.

## Product Description

Rock VPN Gateway Software is an easily installed software package that allows you to communicate securely with other Rock VPN and other IPSec-compliant VPN products. The Rock VPN Gateway Software package extends the network stack of the operating system to provide full-featured communication security. It is a standards-based product using the IETF IPSec and IKE protocols. With the Gateway software you can selectively enable privacy, integrity and authenticity of information sent between the Rock VPN Gateway and other participants in Virtual Private Networks (VPNs). The secure traffic can safely be sent across the Internet and other untrustworthy networks, allowing networks to participate securely in user communities, corporate or dial-up VPNs, as well as Intranet VPNs.





## Benefits

The Gateway Software's multi-platform support allows you to choose which operating system you want to use. You can select the hardware platform based on your performance requirements. The Gateway's full implementation of IPsec makes it versatile to use in any situation.

## Features and Specifications

### ***IPSec features supported:***

- AH/ESP tunnel and transport mode
- Main, Quick and Aggressive modes
- Expiration of Security Associations (SAs) using time and/or kilobytes
- NAT Traversal
- Path MTU discovery

### ***Platforms supported:***

- Windows 2000
- Windows NT 4.0 (Service Pack 3 and above)

### ***Network support:***

- Ethernet
- Dial-up

### ***Encryption algorithms supported:***

- DES (56 bit), 3DES (168 bit)
- IDEA (128 bit)
- Blowfish (40 - 446 bit)
- AES / Rijndael (128, 192 & 256 bit)

### ***Authentication and Key Exchange support:***

- IKE (formerly known as ISAKMP/Oakley)
- Diffie-Hellman (768, 1024 bit)
- RSA (1024, 2048 bit)
- Signatures: RSA, DSS, X.509
- Pre-shared secrets
- Perfect forward secrecy (PFS) support for Diffie-Hellman in Quick Mode

### ***Hash functions supported:***

- MD5
- SHA1



**Standards supported:**

- IETF IPsec
- ISO X.509 v3
- PKCS #1, #10, #12
- SCEP / CMP

**Certification Authorities supported:**

- VeriSign
- RSA Data Security Certificate Server (Keon)
- Baltimore
- Entrust

**Certificate Management:**

- Automatic retrieval and processing of certificates and Certificate Revocation Lists (CRLs)
- X.509v3 certificates supported
- Automatic certificate enrolment using SCEP / CMP

**Management:**

- Policy + rule based configuration with a user-friendly Graphical User Interface
- Live configuration
- Granular control based on IP address, subnet address, address range, port and protocol.
- Use of wizards for installation and configuration
- Access control based on X.509 certificate contents.
- Event log viewer
- Quick policy selection
- Password protection for policy
- Management software included with Gateway Software
  - Remote management
  - Local management
- Remotely manageable using Workstation Software
- Centrally manageable using Central Manager
- Security Association (SA) monitor (both phase I and phase II)

## Contact Details

Tel: +603-6203 5303  
Fax: +603-6203 5302  
URL: [www.rockvpn.com](http://www.rockvpn.com)

For more information or support requests, please visit [www.rockvpn.com](http://www.rockvpn.com) or [www.mynetsec.com](http://www.mynetsec.com).

*Performance figures and data quoted in this document are typical and must be confirmed before they become applicable to any order or contract. Network Security Solutions reserves the right to make alterations or amendments to Specifications. Rock VPN is a registered trade mark of Network Security Solutions. All other trademarks are the property of their respective owners.*