

TCC

NS-2

Network Security

VPN
Security
for
Mission-Critical
Networks



TCC's Network Security
Family of Products

Product Overview

The TCC NS-2, powered by NetScreen™, is a software package that runs on a user's host computer (desktop or laptop) and is used to facilitate secure remote access to networks, devices, or other hosts located across a public or untrusted network.

Security is achieved by using the IPSec protocol with certificates as an additional option. In order to form a secure communications channel, this software can be used in conjunction with the TCC NS-5, TCC NS-10 or TCC NS-100 network security devices, or another host running IPSec compatible software similar to the TCC NS-2.

The TCC NS-2 is designed for desktop and/or laptop computers connected to an IP network by either an Ethernet LAN or remote access via modem.

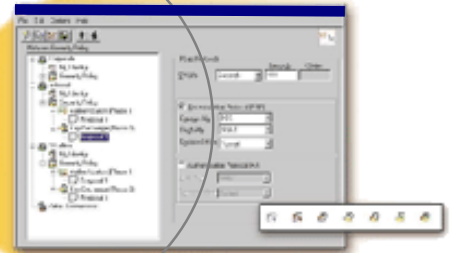
The TCC NS-2 addresses customer needs in a rapidly growing VPN application market.

The TCC NS-2 supports, and is interoperable with, IPSec communication devices from most major equipment manufacturers. It is also compatible with IPSec-compliant gateways, VPN encryptors i.e., TCC NS-5, TCC NS-10 and TCC NS-100, encrypting routers and firewall systems.

Ease in configuration of security policy and the ability to manage certificates, e.g., Verisign, Cybertrust, Entrust, and Netscape is provided through industry-standard, user-friendly icons in the tray portion of the Windows TaskBar.

Security capabilities of the TCC NS-2 are ensured through either 'Tunnel' or 'Transport' Mode IPSec connections.

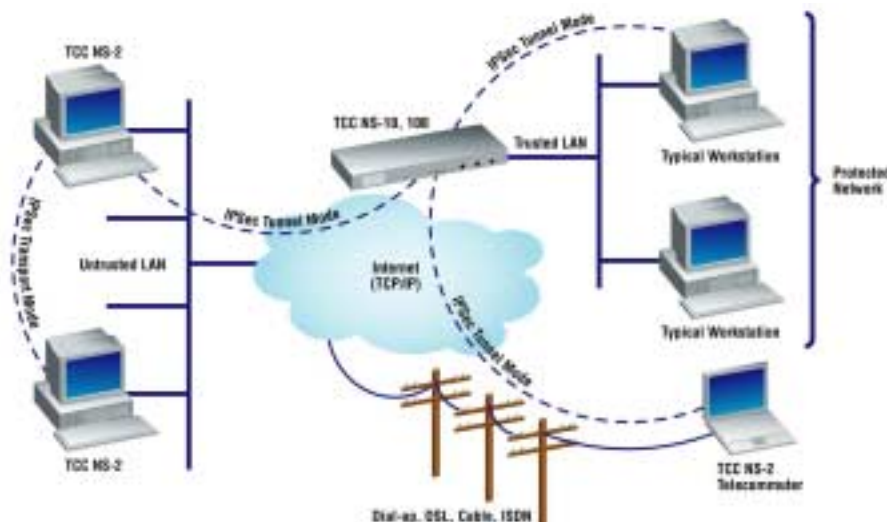
Security configuration is allowed on a connection-by-connection basis via the Security Policy Editor.



key benefits

- > Fully IPSec compliant VPN including
 - Algorithms: DES, Triple-DES, MD5 and SHA-1
 - IKE (Main, Quick and Aggressive modes)
 - Authentication Header
 - Tunnel and Transport Modes
 - Authentication Extensions (X-Auth)
 - ICSA Certified
- > Certificates
 - Separate Certificate Manager and utility
 - X.509 v3 digital certificates
 - Retrieves CA Public Key
- > Importing/Exporting of locked configuration files for easy deployment.
- > Compatible with PC Windows communications devices, i.e., LAN adapters, modems, PC cards.
- > Seamless Windows 95/98/NT client access to NT Domains via VPN Tunnel.
- > Supports DHCP.
- > Complete policy enabling and disabling.
- > Logging / diagnostic log.
- > Upgrade tool automatically converts and imports current settings.

Virtual Private Network



global network security system

TCC NS-2

specifications

network
security
solution
for mission-critical
virtual private networks

Applications:

Road Warrior

Secure Remote Access to Corporate Network
The laptop toting 'Road Warrior' can securely communicate back to the corporate network. NT Domain login, intranet site browsing, FTP, e-mail, file browsing and printing can all be transmitted encrypted over public Internet lines. The user simply loads the software and imports the pre-created, locked configuration file given by their MIS department. Once off-site, they dial-in to the local ISP POP and any traffic bound for the corporate network is automatically encrypted and sent to the TCC NS-X network security device acting as the security gateway. It's just that easy! For example, a remote sales office with several users, contract workers, and employees at home are all able to have access to the corporate network via a local ISP dial-up, DSL, cable modem or ISDN connection.

Extranet User Access

Simply create policy sets, export a locked copy of them and place them on a diskette. Extranet users then install the TCC NS-2 Software Package on their computer, regardless of the Internet connection mechanism. Once the configuration is imported, they are ready to access the site securely.

That's all it takes!

Client-to-client Encryption

The TCC NS-2 can also be used to secure communication between two end-hosts. Both hosts must have the software package installed and configured to encrypt traffic between them.

Systems and Security Standards:

PC compatible computer with a Pentium (or like) processor.

Microsoft Windows 95/98, Windows NT 4.0 Operating System.

Compatible with AOL (4.x or 5.0).

18 MB hard disk space.

16 MB RAM for Windows 95/98, 32 MB RAM for Windows NT.

CD-ROM Drive or 3.5 inch high-density floppy drives to install software.

Internal or external modem (no encryption) or direct network connection.

IPSec standards and RFCs.

Encapsulating Security Payload (ESP)

IKE key management (ISAKMP/Oakley)

X.509 v3 certificates

FIPS Pub 46-1: Data Encryption Standard

FIPS Pub 180-1: Secure Hash Standard

PKCS #7: Cryptographic Message Syntax Standard

PKCS #10: Certification Request Syntax Standard



Quality

As an ISO 9001 certified company, TCC designs, manufactures and supports high-grade secure communications systems that protect highly sensitive information transmitted over a wide range of data, voice and fax networks. Over 2,000 government/military agencies, financial institutions, telecom carriers and other multinational corporations worldwide rely on TCC to protect their communications networks.

TCC secures mission critical networks for governments, corporations and financial institutions around the world. With over 39 years of experience, TCC is the trusted supplier for organizations that place a high value on the confidentiality of their data and voice communications.

CipherONE is a trademark of TCC. NetScreen is a trademark of NetScreen Technologies, Inc. Other brand and product names may be trademarks or registered trademarks of their respective owners.

Technical Communications Corporation
100 Domino Drive Concord, MA 01742-2892 USA
Tel: 978/ 287-5100 Fax: 978/ 371-1280
E-mail: info@tccsecure.com
Web Site: www.tccsecure.com