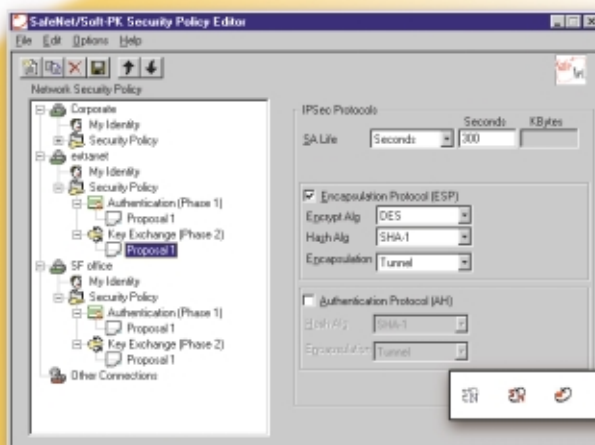


NetScreen-Remote 2.0

Product at a glance

NetScreen-Remote 2.0

- Windows 95, 98, NT VPN client
- Secure remote access
- IPSec compatible
- Policy-based



Powerful GUI provides familiar Windows Browsing method for creating and organizing multiple policy entries and associated configuration options.

NetScreen-Remote 2.0/ Safe-Net System Tray Icons

Seven multi-colored icons provide easy-to-read status indicator for NetScreen-Remote/Safe-Net's VPN connections. Icons appear conveniently in Windows Task Bar's System Tray.

Product overview

NetScreen-Remote 2.0 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 must be used in conjunction with an IPSec gateway, like the NetScreen family of Security Appliances, or another host running IPSec compatible software, like NetScreen-Remote 2.0. NetScreen-Remote 2.0 is designed for desktop and/or laptop computers connected to an IP network by either an Ethernet-LAN or remote access Dial-Up via modem.

NetScreen-Remote 2.0 represents a substantially different implementation architecture than previous NetScreen Remote products. Increased compatibility, ease of installation and use, in addition to a host of new VPN capabilities are among the important features of this NetScreen product release. A robust conversion mechanism also exists to ease users in updating configuration settings from previous NetScreen Remote products.

According to InternetWeek, Sept. 13th, 1999, Remote Access is the number one VPN application. NetScreen's-Remote 2.0 client is well positioned to address customer needs in this rapidly growing market.

Key product features of NetScreen-Remote 2.0:

- Fully IPSec compliant VPNs including
 - Algorithms: DES, 3-DES, MD-5, and SHA-1
 - IKE (Main, Quick and Aggressive* modes)
 - AH*
 - Tunnel and Transport* Modes
 - Authentication Extensions (X-Auth)*
 - ICSA Certified
- Certificates*
 - Separate Certificate Manager and utility
 - X.509 v3 digital certificates and request generation tools
 - Retrieves CA Public Key
- Powerful GUI allow users to build multiple layers of service-based policies
- Importing/Exporting of locked configuration files for easy deployment
- Compatible with PC Windows communications devices such as LAN adapters, modems, PC cards
- Operates as a Window's system service
- Seamless Windows 95/98/NT client access to NT Domains via VPN Tunnel
- Supports DHCP
- Complete policy enabling and disabling
- Logging/diagnostic log
- Complete and transparent ease of use
- Upgrade tool automatically converts and imports current settings



NETSCREEN™

Broadband Internet Security Solutions

Applications

"Road Warrior" - Secure Remote Access to Corp Network

The laptop toting "Road Warrior" can securely communicate back to the corporate network. NT Domain login, Intranet site browsing, FTP, Email, file browsing, even printing all transmit encrypted over public Internet lines. The user simply loads the software and imports the pre-created, locked configuration file given to them by their MIS staff. Once on the road, they dial-in to the local ISP POP, and any traffic bound for the corporate network is automatically encrypted and sent to the NetScreen Appliance acting as the Security Gateway. It's just that easy!

Home/Remote-Office User - Secure Remote Access Intranet

The 3 users in the remote sales office... the Contractor... the Employee at home with a sick child... The Executive at 1 a.m... all gaining secure, encrypted 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 NetScreen-Remote 2.0 software on their computer, regardless of the Internet connection mechanism. Once they import the configuration, a two-click process, they are ready to access your site securely. That's all it takes!

Secure Remote Management/Monitoring

Your "Trusted" network is no longer as trusted as it once was. So managing your NetScreen Security Appliance over the company network must occur on an encrypted transmission. Or you may need to check an alarm from home or change a NetScreen Security Appliance's policy while on the road. Either way NetScreen-Remote ensures that your management session is not visible by any other parties, even when you are on the "Untrusted" side of the world.

Client-to-client Encryption

NetScreen-Remote 2.0 can also be used to secure communication between two end hosts. As long as both hosts have the NetScreen-Remote 2.0 installed, they can be configured to encrypt traffic between them.

NetScreen-Remote 2.0 supports and is interoperable with IPSec communication devices from most major equipment manufacturers.

It is also compatible with IPSec-complaint gateways, gateway encryptors, VPN routers and firewall systems.

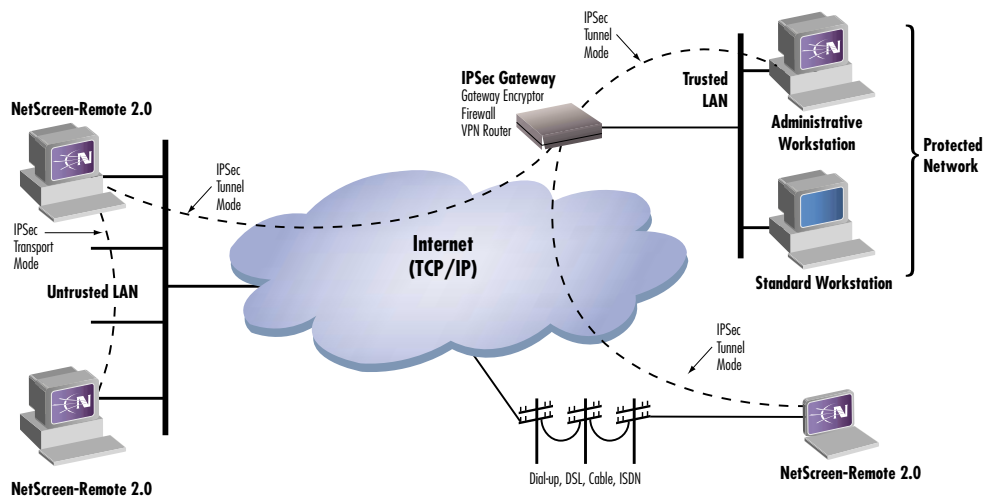
Easy configuration of security policy and ability to manage certificates*, e.g., Verisign, Cybertrust, Entrust, and Netscape is provided

through industry-standard, familiar, and easy-to-access icons in the tray portion of the Windows TaskBar.

Security capabilities of NetScreen-Remote 2.0 are ensured through either "Tunnel" or "Transport"* mode IPSec connections.

Configuration of security is allowed on a connection-by-connection basis via the Security Policy Editor.

* For use with future versions of NetScreen Appliances



Specifications:

Systems and Security Standards:

- PC compatible computer with a Pentium (or like) processor
- Microsoft Windows 95/98 Windows NT 4.0 Operating System (SP 3, 4, 5)
- 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
- Authentication Header (AH)
- 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

Ordering information:

Product	Part Number
Strong Encryption (export controlled):	
NS-Remote 2.0-1 User License	NS-R2A-001
NS-Remote 2.0-10 User License	NS-R2A-010
NS-Remote 2.0-25 User License	NS-R2A-025
NS-Remote 2.0-100 User License	NS-R2A-100
NS-Remote 2.0-1,000 User License	NS-R2A-110
Export version:	
NS-Remote 2.0-1 User License	NS-R2E-001
NS-Remote 2.0-10 User License	NS-R2E-010
NS-Remote 2.0-25 User License	NS-R2E-025
NS-Remote 2.0-100 User License	NS-R2E-100
NS-Remote 2.0-1,000 User License	NS-R2E-110

For more information on NetScreen products, call toll-free 1-800-638-8296

NetScreen, the NetScreen logo, and NetScreen-Remote 2.0 are trademarks of NetScreen Technologies, Inc. All other trademarks are the property of their respective holders.
 ©1999 NetScreen Technologies, Inc. All rights reserved. Information in this document is subject to change without notice. NetScreen Technologies, Inc. assumes no responsibility for errors that appear in this document.
 Literature Part Number: 1999.12.10.2.R2.0



2860 San Tomas Expressway
 Santa Clara, CA 95051
 Phone: 408-330-7800
 Fax: 408-330-7850

www.netscreen.com