NetScreen-Remote

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

Product at a glance
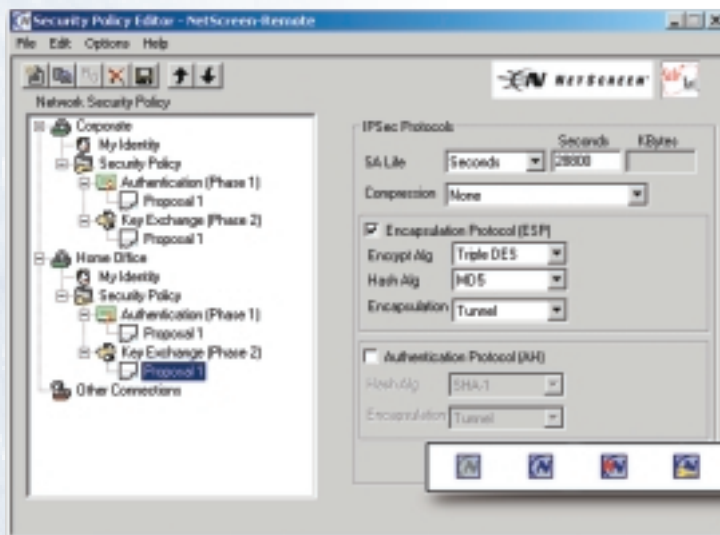
- **Multi-platform client**

  Allows for client-initiated VPNs from Microsoft Windows® 95, 98, ME, NT®, 2000 computers

- **Broad security support**

  Implements IPSec and L2TP security protocols, with optional certificates

- **Flexible**

  Provides for multiple layers of security policy

NetScreen-Remote Tray Icons

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

NetScreen-Remote overview

The NetScreen-Remote VPN client provides the critical ability for client-initiated Virtual Private Network (VPN) communication. NetScreen-Remote is ideal for "road warriors" needing to access mission-critical networks across an untrusted or public network as well as end-users within a enterprise environment that require a secure end-user-to-host connection.

NetScreen-Remote, based on SafeNet's industry-leading VPN client software, runs on an end-user's computer and facilitates secure remote access to networks, devices, or other hosts. Security is achieved by using the IPSec protocol and Layer 2 Tunneling Protocol (L2TP), 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, such as NetScreen's line of integrated security systems and appliances, or another host running IPSec compatible software, including other computers running NetScreen-Remote. NetScreen-Remote encrypted communications can be initiated in any IP network environment, be it an Ethernet LAN or dial-up modem connection.

Extensive compatibility

NetScreen-Remote 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, supporting multiple encryption and authentication algorithms—including DES, 3DES, MD-5, and SHA-1. Support for both IKE (main, quick and aggressive modes) and a wide assortment of certificate authorities (eg. VeriSign, Cybertrust, Entrust, and Netscape) is provided. In addition, support is available for Windows 95/98, Windows Millenium Edition (ME), Windows NT, and Windows 2000 operating systems.

Ease of use

Netscreen-Remote provides various features that make the software very easy to install, configure, and maintain. First, a powerful policy GUI allows the administrator to build multiple layers of service-based policies. Next, these policies can be easily imported into client machines and locked down so no changes can be made. Finally, a diagnostic log and connection monitor provide valuable feedback to the administrator.

Robust reliability

Remote users' access to secure resources is mission critical, and Netscreen-Remote helps ensure successful business transactions through extensive reliability elements. Multiple gateways can be configured on the client to provide redundancy in case a primary gateway fails. Meanwhile, exchange [IKE] "keepalives" help maintain the persistence of the VPN connection.
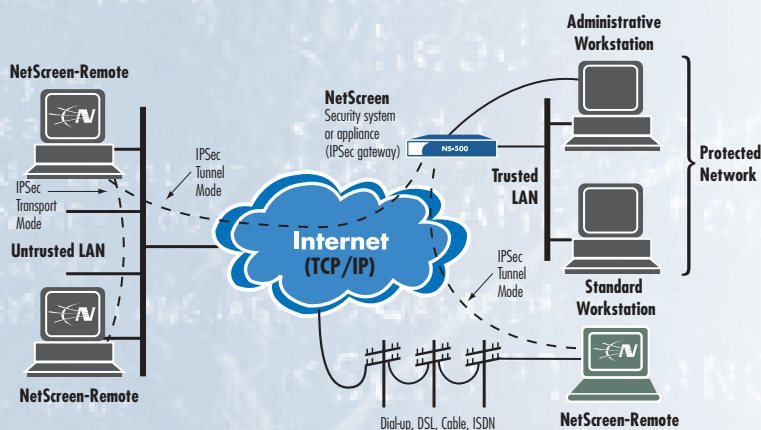
Specifications and Ordering

Feature		NetScreen-Remote
VPN	Manual Key, IKE, PKI (X.509)	Yes
	DES (56-bit) and 3DES (168-bit) encryption algorithms	Yes
	AH	Yes
	Tunnel or transport mode	Yes
	Layer 2 Tunnel Protocol [L2TP]	Yes
IPSec	Key management	
	Manual	Yes
	IKE/ISAKMP [Main,Quick, Aggressive Modes]	Yes
	MD5	Yes
	SHA-1	Yes
	Certificate requests/standards	
	PKCS 7	Yes
	PKCS 10	Yes
	PKCS 12	Yes
	Certificate manager utility	Yes
	X.509 v3 digital certificates and request generation tool	Yes
	Certificate servers supported	
	Verisign On Site CA	Yes
	Entrust CA with VPN Connector	Yes
	Microsoft CA	Yes
	RSA Keon CA	Yes
	iPlanet (Netscape) CMS CA	Yes
	Baltimore Unicert CA	Yes
High Availability (HA)	Redundant gateways	Yes
	Exchange [IKE] keepalives	Yes
User Authentication	Extended authentication protocol [Xauth] Version 6	Yes
Administration	Administration GUI	Yes
	Import/export of security configuration files	Yes
	Lock down of client configurations	Yes
	Certificate manager utility	Yes
Logging/Monitoring	Diagnostic log/connection monitor	Yes

Ordering information:

Product	Part Number
Strong Encryption — 3DES version (export controlled):	
NetScreen-Remote -10 User License	NS-R5A-010
NetScreen-Remote -100 User License	NS-R5A-100
NetScreen-Remote -1,000 User License	NS-R5A-110
NetScreen-Remote - Unlimited User License	NS-R5A-UNL
DES version:	
NetScreen-Remote -10 User License	NS-R5E-010
NetScreen-Remote -100 User License	NS-R5E-100
NetScreen-Remote -1,000 User License	NS-R5E-110
NetScreen-Remote - Unlimited User License	NS-R5E-UNL

NetScreen product warranty and services

NetScreen-Remote's standard software warranty is for a period of 90 days. Optional services are also available such as extended software subscription products. These are recommended to keep the system updated with the latest software enhancements and to ensure high availability for end-users. Phone support services and training courses are also available from NetScreen.

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

Part Number: 2001.7.20.2.nsr

Specifications:

Options:

Licenses available for 10, 100 or 1,000, and unlimited users

System Requirements:

IBM compatible computer with a Pentium (or equivalent) processor

Microsoft Windows 95/98, ME, Windows NT 4.0, Windows 2000 operating system

18 MB hard disk space

16 MB RAM for Windows 95/98, 32 MB RAM for Windows 98/NT, 64 MB for Windows ME/2000

CD-ROM drive to install software

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

Ethernet network interface card with NDIS compliant driver and/or dialup adapter (modem or ISDN)

Standards Supported

IPSec standards and RFCs

Layer 2 Tunneling Protocol (L2TP)

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

PKCS #12: Personal Information Exchange Syntax Standard

PPPoE

Certifications

ICSA

NETSCREEN™

350 Oakmead Parkway
Sunnyvale, CA 94085
Phone: 408.730.6000
Fax: 408.730.6200
www.netscreen.com