NetScreen-Remote
VPN and Security Client Software
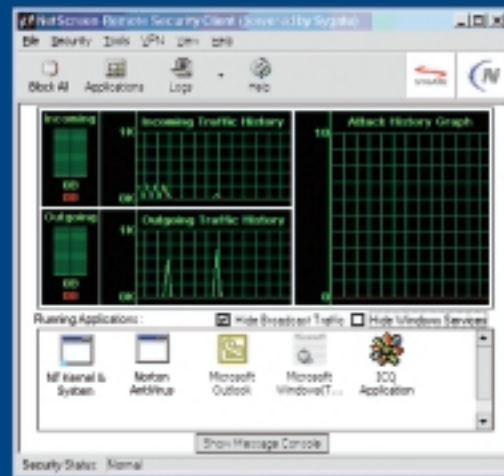

NetScreen-Remote VPN Client authenticates the user prior to retrieving VPN Policies

Seven multi-colored icons provide easy-to-read status indicator for Netscreen-Remote connections. Icons appear conveniently in the Windows taskbar

NetScreen-Remote Security Client includes Personal Firewall software which provides additional protection for mobile users

NETSCREEN®
Scalable Security Solutions

At a glance

- **Multi-platform security client**

  Enables client-initiated VPNs from Microsoft Windows® 95, 98, ME, NT, 2000, XP computers

- **Broad security support**

  Implements IPSec and L2TP security protocols, with optional certificates and/or smart-cards

- **NAT traversal support**

  Allows for VPN tunnel termination in environments where Network Address Translation (NAT) is used

- **Centralized VPN policy management**

  VPN policies are assigned to users, rather than machines, and retrieved automatically when used with NetScreen-Global PRO management products

- **Integrated personal firewall**

  Personal firewall software included with security client provides additional security to mobile users

- **Optional posture assessment**

  Prevents VPN from being established if personal firewall software has been disabled, compromised or is not installed on users machine

NetScreen-Remote Overview

The proliferation of remote access Virtual Private Networks (VPNs) as the industry standard for secure, mobile access to private networks has caused network security administrators to place additional requirements on client software. Remote access clients must now provide secure authentication and VPN policy retrieval while remaining easy to deploy and seamless to end users. The software must enable access from any network or medium the end-user will use including dial-up, broadband, and wireless without any additional configuration. Additionally, since most deployments provide remote users complete access to private enterprise networks, the client solution must protect the mobile users machine as well as the VPN connection against attacks initiated from the Internet or from within the VPN. NetScreen meets these requirements with the NetScreen-Remote line of VPN and personal firewall client software delivering centrally managed ICSA certified VPN software for all Windows desktop platforms and offering additional host-based security and firewall capabilities with the new NetScreen-Remote Security Client.

NetScreen-Remote VPN Client

NetScreen's VPN client enables client-initiated VPN communication. The VPN client is ideal for "road warriors" needing to securely access private networks across the public Internet as well as end-users within an enterprise environment that require secure connections across wireless networks or between departmental networks.

NetScreen-Remote VPN Client, based on SafeNet's industry-leading VPN software, runs on an end-user's Windows-based computer and facilitates secure remote access to remote networks, devices, or other hosts. Security is achieved by using the IPSec protocol and/or Layer 2 Tunneling Protocol (L2TP), with certificates or smart cards as an optional form of authentication.

In order to form a secure communications channel, this software must be used in conjunction with a VPN gateway, such as NetScreen's line of integrated security appliances and systems, or another host running compatible software, such as NetScreen-Remote VPN Client. With NetScreen-Remote VPN Client, encrypted communications can be initiated in any IP network environment, such as an Ethernet LAN, wireless LAN or dial-up. With NAT traversal capabilities, connections may now be initiated from behind a device performing NAT to any IPSec host or gateway supporting NAT traversal. NetScreen-Remote VPN Client supports a variety of configurations:

- Split-tunneling permits Internet traffic while the VPN is active
- Block-tunneling blocks Internet traffic while VPN is active
- Central tunneling forces all traffic (including Internet traffic) across the VPN tunnel for protection and filtering by the central NetScreen device

NetScreen-Remote Security Client

NetScreen-Remote Security Client includes all the features of NetScreen-Remote VPN, with the addition of an integrated personal firewall to provide additional security for mobile users. The NetScreen-Remote Security Client, which incorporates Sygate Technologies award-winning personal firewall software, brings together numerous host-based security features with NetScreen's VPN Client to protect mobile users systems from outside attacks as well as targeted attacks against the VPN by Trojan applications.

NetScreen-Remote Security client blocks unapproved applications, such as Trojan's, from accessing the network.
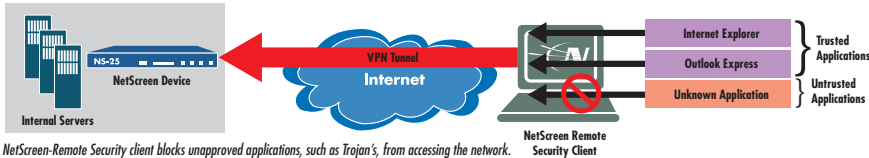
The personal firewall included with NetScreen-Remote Security Client performs traditional stateful-inspection on TCP/IP packets, virtually eliminating the possibility of hijacked or unwanted connections. Denial of Service (DoS) attack protection is performed on each interface, blocking known attacks. Finally, application control limits network-access to trusted applications, such as Microsoft Internet Explorer. Applications attempting to access the network must first be approved by the administrator or end-user. Any unapproved applications will be blocked, helping to stop Trojan applications.

Extensive logging is available, including attack, session and packet logs that can be easily exported or forwarded to an e-mail system automatically. Alerts and open connections are displayed in real-time on the main window of the product along with network traffic and attack history graphs. Attack's can be traced to locate the attacker source address while AutoBlock prevents subsequent attacks from that address. Since updates to the software are checked automatically over the web, users remain up-to-date and protected against newly discovered attacks.

Automated VPN Policy Updates

Both NetScreen-Remote VPN Client and NetScreen-Remote Security Client provide a mechanism for secure, automated VPN policy retrieval from the NetScreen-Global PRO line of security management systems, supporting thousands of users. VPN policies for mobile users are centrally defined within NetScreen-Global PRO and propagated to NetScreen-Remote client users after successful authentication. Users may authenticate directly to NetScreen-Global PRO or via NT domain or Active Directory through
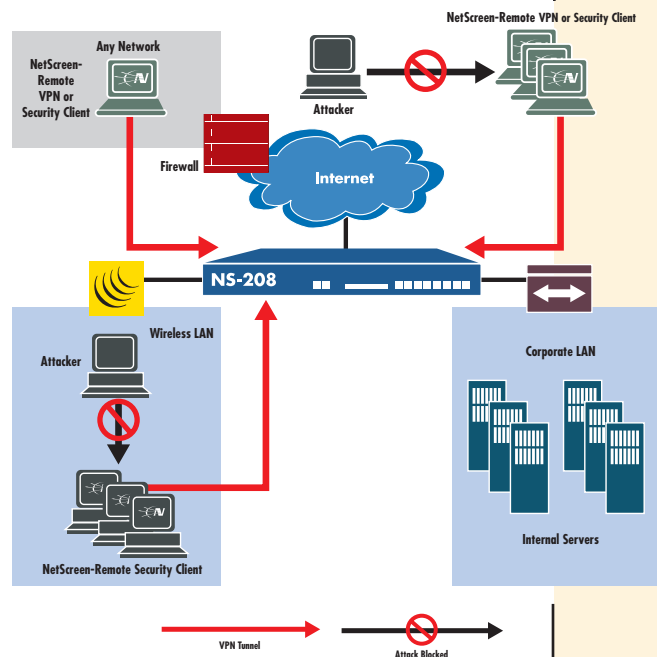
NetScreen-Global PRO's RADIUS interface. User authentication occurs over SSL prior to retrieving the VPN policies, ensuring only valid users can retrieve their VPN policies. Since VPN policies are linked to users as opposed to machines, users can move between multiple PCs running NetScreen-Remote clients and receive their VPN policy. As an added security measure, when the user logs out of the VPN, all of their confidential VPN policys and keys may be optionally cleared, resulting in a more secure, more controllable remote access solution.

If the NetScreen-Global PRO administrator enables posture assessment, NetScreen-Remote Security Clients will not retrieve any VPN policies unless the personal firewall software is installed and operational. This ensures that mobile users are protected before allowing mobile users to establish VPN sessions.

Extensive compatibility

Both the NetScreen-Remote VPN Client and NetScreen-Remote Security Client support and are interoperable with IPSec-compliant communication devices from most major equipment manufacturers. They also support the highest levels of encryption and authentication algorithms—including DES, 3DES, MD-5, and SHA-1. Support for IKE (main, quick and aggressive modes) and a wide assortment of smart cards and certificate authorities (eg. VeriSign, RSA, Entrust, and Microsoft) are provided. NetScreen-Remote clients support all Microsoft Windows desktop platforms.

The NetScreen-Remote line of products allow client-initiated VPN communication from any environment using standards-based technology.

NetScreen-Remote Security Client also blocks attacks initiated from the Internet or from within VPN networks.

Feature	NetScreen-Remote VPN	NetScreen-Remote Security
VPN		
Manual key	Yes	Yes
AutoKey (IKE) preshared	Yes	Yes
AuthKey (IKE) certificate	Yes	Yes
ESP and AH	Yes	Yes
L2TP protocol support	Yes	Yes
NAT traversal	Yes	Yes
Main and aggressive mode IKE	Yes	Yes
Redundant gateway support	Yes	Yes
Cryptography		
3DES and DES	Yes	Yes
SHA-1 and MD5	Yes	Yes
AES and SHA-256	Yes (1)	Yes (1)
FIPS140-1 certified libraries	Yes	Yes
PKI		
PKCS7 certificate chains	Yes	Yes
PKCS10 certificate requests	Yes	Yes
PKCS12 certificate import	Yes	Yes
MSCAPI support	Yes	Yes
Smart Card support	Yes (2)	Yes (2)
X.509 certificate authority	Yes (3)	Yes (3)
User Authentication		
RADIUS integration	Yes	Yes
LDAP integration	Yes	Yes
NT domain integration	Yes	Yes
Extended authentication (XAUTH)	Yes	Yes
Authenticated VPN policies	Yes	Yes
Security Features		
Split tunneling	Yes	Yes
Block tunneling	Yes	Yes
Central tunneling	Yes	Yes
Packet filtering	Yes	Yes
Statefull inspection firewall	No	Yes
DoS attack protection	No	Yes
Application control	No	Yes
NetBIOS protection	No	Yes
Posture assessment	No	Yes
Driver-level protection	No	Yes
AutoBlock	No	Yes
Management, Logging and Monitoring		
Central management of VPN	Yes (4)	Yes (4)
Optional VPN policy purge	Yes	Yes
VPN diagnostics logs	Yes	Yes
VPN connection monitor	Yes	Yes
Attack logs	No	Yes
Evidence logs	No	Yes
Packet logs	No	Yes
E-mail alerts and logs	No	Yes
Attacker tracing system	No	Yes

(1) Available in NetScreen-Remote VPN Client and NetScreen-Remote Security Client 8.1 release, scheduled Q4 2002
(2) Official support for Schlumberger, Rainbow IKey and DataKey drivers
(3) X.509 Certificate Authorities supported include: VeriSign OnSite, Entrust VPN Connector, Microsoft CA, RSA KeyOn CA, iPlanet (Netscape) CA, Baltimore UniCert and DODPKI CA
(4) Requires NetScreen-Global PRO or NetScreen-Global PRO Express (sold separately)

NetScreen-Remote VPN and Security Client Software

Specifications:

System Requirements:

IBM compatible computer with a Pentium (or equivalent) processor

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

35 MB hard disk space, 40 MB for NetScreen-Remote Security Client

16 MB RAM for Windows 95/98

32 MB RAM for Windows 98/NT

64 MB for Windows ME/2000/XP

Ethernet or Wireless Ethernet interface with NDIS compliant driver and/or dial-up networking using an internal or external modem, ISDN adapter or PPPOE adapter

Standards and RFCs Supported

L2TP: Layer 2 Tunneling Protocol (RFC2661)

ESP and AH: Encapsulating Security Payload and Authentication Header (RFC2406, 2402)

IKE (ISAKMP/Oakley): Internet Key Exchange (RFC2407-2409)

PPPoE: PPP over Ethernet (RFC2516)

NAT traversal (draft-ietf-ipsec-nat-t-ike, draft-ietf-ipsec-udp-encaps-main)

X.509 v3 certificates: (RFC2459)

CEP: Certificate Enrollment Protocol

PKCS #7: Cryptographic Message Syntax Standard (RFC2315)

PKCS #10: Certification Request Syntax Standard (RFC2986)

PKCS #12: Personal Information Exchange Syntax Standard

MSCAPI: Microsoft Certificate API

Certifications

ICSA IPSec
ICSA PC Firewall (NetScreen-Remote Security Client)
FIPS PUB 46-1: Data Encryption Standard
FIPS PUB 180-1: Secure Hash Standard
FIPS 140-1: Cryptographic Modules

Ordering information:

Product	Part Number
NetScreen-Remote Security Client – 10 User License	NS-R8P-010
NetScreen-Remote Security Client – 100 User License	NS-R8P-100
NetScreen-Remote Security Client – 1,000 User License	NS-R8P-110
NetScreen-Remote VPN Client –10 User License	NS-R8A-010
NetScreen-Remote VPN Client –100 User License	NS-R8A-100
NetScreen-Remote VPN Client –1,000 User License	NS-R8A-110

Site license available upon request.

NetScreen product warranty and services

NetScreen-Remote's standard software warranty is for a period of one year. Optional services are also available such as extended software subscription. 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 services or products, please call toll-free 1-800-638-8296 in the US, +44 8700 750000 in Europe, or 852-2519-3988 in Hong Kong, or visit us at www.netscreen.com.

NETSCREEN®

350 Oakmead Parkway
Sunnyvale, CA 94085
Phone: 408.730.6000
Fax: 408.730.6200

www.netscreen.com