

Juniper Networks NetScreen-Remote



NetScreen-Remote VPNClient 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

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 user's machine as well as the VPN connection against attacks initiated from the Internet or from within the VPN. Juniper meets these requirements with the Juniper Networks 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 Juniper Networks NetScreen-Remote Security Client.

	Juniper Networks NetScreen-Remote VPN Client	Juniper Networks NetScreen-Remote Security Client
--	--	---

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 (128, 192, 256-bit)	Yes	Yes
FIPS 140-1 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 ⁽¹⁾	Yes ⁽¹⁾
X.509 certificate authority	Yes ⁽²⁾	Yes ⁽²⁾

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

	Juniper Networks NetScreen-Remote VPN Client	Juniper Networks NetScreen-Remote Security Client
--	--	---

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 ⁽⁴⁾
Application control	No	Yes
NetBIOS protection	No	Yes
Posture assessment	No	Yes ⁽⁵⁾
Driver-level protection	No	Yes
AutoBlock	No	No

Management, Logging and Monitoring

Central management of VPN	Yes ⁽³⁾	Yes ⁽³⁾
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) Official support for Schlumberger, Rainbow iKey and DataKey drivers

(2) X.509 Certificate Authorities supported include: VeriSign OnSite, Entrust VPN Connector, Microsoft, RSA KeyOn, iPlanet (Netscape), Baltimore UniCert and DODPKI

(3) Requires Juniper Networks NetScreen-Global PRO or Juniper Networks NetScreen-Global PRO Express (sold separately)

(4) Only in firewall policy

(5) When using ANG (Authenticate and Go)

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)
 Extended Authentication (XAUTH)
 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 1.1
 ICSA PC Firewall (NetScreen-Remote Security Client)
 FIPS PUB 46-1: Data Encryption Standard
 FIPS PUB 180-1: Secure Hash Standard

Ordering Information

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



1194 North Mathilda Avenue Sunnyvale, CA 94089 USA
 Phone: 888-JUNIPER (888-586-4737) or 408-745-2000
 Fax: 408-745-2100

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Part Number: 110012-001 Apr 2004