CISCO SYSTEMS

DATA SHEET

CISCO VPN CLIENT

Supports Easy VPN Remote

INTRODUCTION

The Cisco® VPN Client is software that enables customers to establish secure, end-to-end encrypted tunnels to any Cisco Easy VPN server. This thin-design, IP Security (IPSec)-compliant implementation is available from Cisco.com for customers with Cisco SMARTnet® support, and is included free of charge with Cisco VPN 3000 Series concentrators, Cisco ASA 5500 Series security appliances, and most Cisco PIX security appliances. The client can be preconfigured for mass deployments and initial logins require very little user intervention. VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, allowing simple deployment and management.

The Cisco VPN Client supports Windows 98, ME, NT 4.0, 2000, and XP; Linux (Intel); Solaris (UltraSparc 32- and 64-bit); and Mac OS X 10.2, 10.3, and 10.4.

The Cisco VPN Client is compatible with the following Cisco products (Cisco Easy VPN servers):

- Cisco VPN 3000 Concentrator Software Version 3.0 and later
- Cisco IOS® Software Release 12.2(8)T and later
- Cisco PIX® Security Appliance Software Version 6.0 and later
- Cisco ASA 5500 Series Software Version 7.0 and later

FEATURES AND BENEFITS

- Support for Windows 98, ME, NT 4.0, 2000, and XP; Linux (Intel); Solaris (UltraSparc 32- and 64-bit); and Mac OS X 10.2, 10.3, and 10.4.
- Automatic software updates (Windows 2000 & XP) makes deploying new client versions hassle free-new in v4.6
- VPN Virtual Interface Adapter present on Windows 2000 and XP
- Application Programming Interface (API) allows you to control operation of the VPN client from another application-new in v4.6
- System coexistence with Microsoft L2TP/IPsec client
- MSI (Windows Installer) package available for NT, 2000, and XP
- Intelligent peer availability detection (DPD)
- Simple Certificate Enrollment Protocol (SCEP)
- Data compression (LZS)
- Command-line options for connecting, disconnecting, and connection status
- Configuration file with option locking
- Support for Microsoft network login (all platforms)
- Domain Name System (DNS) including DDNS/DHCP computer name population, Split DNS,
- Windows Internet Name Service (WINS), and IP address assignment
- Load balancing and backup server support
- Centrally controlled policies (including backup server list)
- Integrated personal firewall (stateful firewall): Zone Labs technology-Windows only
- Personal firewall enforcement: Cisco Security Agent, Sygate, Zone Alarm-Windows only

- Integration with the iPass remote access client software, including: one-click (single sign-on), VPN auto-teardown, and Windows pre-login support-Windows only.
- Client connection auto initiation for wireless LAN environments

CISCO EASY VPN

Cisco Easy VPN, a software enhancement for existing Cisco routers and security appliances, greatly simplifies VPN deployment for remote offices and teleworkers. Based on the Cisco Unified Client Framework, Cisco Easy VPN centralizes VPN management across all Cisco VPN devices thus reducing the complexity of VPN deployments. Cisco Easy VPN enables an integration of VPN remotes-Cisco routers, Cisco PIX Security Appliances, Cisco VPN concentrators or software clients-within a single deployment with a consistent policy and key management method thus simplifying remote side administration.

Table 1. Product Specifications

Description	Specification
Operating Systems	Support for Windows 98, ME, NT 4.0, 2000, and XP; Linux (Intel); Solaris (UltraSparc 32- and 64-bit); and Mac OS X 10.2, 10.3, and 10.4.
Tunneling Protocols	IPSec Encapsulating Security Payload (ESP), PPTP, L2TP, L2TP/IPSec, Network Address Translation (NAT) Transparent IPsec, Ratified IPsec/UDP (with autodetection and fragmentation avoidance), IPsec/TCP
Encryption/Authentication	IPsec (ESP) using Data Encryption Standard (DES)/Triple DES (3DES) (56/168-bit) or AES (128/256-bit) with MD5 or SHA
Key Management	Internet Key Exchange (IKE)-Aggressive and Main Mode (Digital certificates) Diffie-Hellman (DH) Groups 1, 2, and 5 Perfect Forward Secrecy (PFS) Rekeying
Data Compression	Lempel-Ziv standard (LZS) compression
Digital Certificates	• The supported enrollment mechanisms are Simple Certificate Enrollment Protocol (SCEP) and Certificates enrolled with Microsoft Internet Explorer. • Supported certificate authorities (CAs) include: Entrust, Netscape, Baltimore, RSA Keon, Verisign, and Microsoft. • Entrust ESP and Entelligence Client support • Smartcards: Supported via MS CAPI (CRYPT_NOHASHOID) include: Activcard (Schlumberger cards), Aladdin, Gemplus and Datakey.
Authentication	• Extended Authentication (XAUTH) • Remote Authentication Dial-In User Service (RADIUS) with support for: State/Reply-Message attributes (token cards) Kerberos/Active Directory authentication Security Dynamics (RSA SecurID Ready) Microsoft NT Domain authentication MSCHAPv2-NT Password Expiration X.509v3 digital certificates • External user authorization information may be obtained via LDAP or RADIUS
Certifications	FIPS 140-2 Level 1 (v3.6)
Profile Management	Client can be easily distributed with preconfigured Profile Configuration Files (PCFs)
Policy Management	ISAKMP Configuration Method (Mode-Config) centrally controlled policies including DNS/Split DNS, WINS, IP Address, and Default Domain Name. Ability to save connection password, split tunneling/local LAN access control/networks, remote access load balancing, Centralized Protection Policy (firewall), personal firewall requirement (Are You There?), automatic software updates

Table 2.   Remote Access Feature Comparison Chart

	Cisco VPN 3000	Cisco ASA 5500	Cisco PIX Security Appliance	Cisco IOS
Version used for Feature Chart	4.7	7.0	7.0	12.3(8)T or 12.2(18)SX
All Cisco Easy VPN Client OS Support	Y	Y	Y	Y
Apani (Mac OS 8/9) VPN Client Compatibility Tested	Y	N	N	N
Basic Client Functionality				
DES/3DES, MD5/SHA	Y	Y	Y	Y
AES (128, 256 bit)	Y	Y	Y	Y
PreShared Secret (Group)	Y	Y	Y	Y
DNS, WINS, Default Domain, IP	Y	Y	Y	Y
Split DNS Support	Y	Y	Y	Y
Dynamic DNS/DHCP (Computer name population)	Y	Y	Y	N
Connection Auto-Initiation	Y	Y	Y	Y
Authentication				
RADIUS	Y	Y	Y	Y
RADIUS with State+Reply Tokens	Y	Y	Y	Y
RADIUS with NT Password Expire	Y	Y	Y	Y
Native RSA SecurID (SDI)	Y	Y	Y	N
Native Kerberos/Active Directory	Y	Y	Y	N
Native NT Domain	Y	Y	Y	N
Certificate/Entelligence/Smartcard	Y	Y	Y	Y
Peer Detection (DPD)	Y	Y	Y	Y
Backup Server List (Client)	Y	Y	Y	Y
Backup Server List (Central Control)	Y	Y	Y	Y
Rekeying	Y	Y	Y	Y
Idle Timeout Support	Y	Y	Y	Y
Max Connection Limit	Y	Y	Y	Y
User IP Filters	Y (including Dynamic ACLs)	Y (including Dynamic ACLs)	Y (including Dynamic ACLs)	Y through ACLs
RADIUS Group Lock	Y	Y	Y	Y
Address Assignment				
Internal Address Pool	Y	Y	Y	Y
DHCP	Y	Y	Y	N
RADIUS	Y	Y	Y	Y
Advanced Functionality				
Data Compression	Y	Y	Y	Y
Concentrator Banner Message	Y	Y	Y	N
Automatic Software Updates	Y—Centrally Controlled	Y—Centrally Controlled	Y	Y
Software Update Notification	Y	Y	Y	N
Saved Password Control	Y	Y	Y	Y

	Cisco VPN 3000	Cisco ASA 5500	Cisco PIX Security Appliance	Cisco IOS
Tunnel Default Gateway	Y	Y	Y	Y
Clustering/Load Balancing	Y	Y	N	N
IPSec to MPLS, 802.1q or PVC Mapping	N	N	N	Y
Tunneling Methods				
All Tunneling/Split Tunneling	Y	Y	Y	Y
Local LAN Access Permission	Y	Y	Y	Y
Ratified IPSec/UDP NAT Transparency (including auto-detection and fragmentation avoidance)	Y	Y	Y	Y
Legacy NAT/PAT Transparency (UDP)	Y	Y	Y	N
TCP-Based IPsec (TCP)	Y	Y	Y	N
Client Personal Firewall Support				
User Controlled (Always On)	Y	Y	Y	Y
Cisco Security Agent/Sygate/Zone Alarm Enforcement (AYT)	Y	Y	Y	N
Centralized Protection Policy (CPP)	Y	Y	Y	N
Zone Labs Integrity	Y	N	N	N

ORDERING INFORMATION

Where to Buy Cisco Products

Visit http://www.cisco.com/public/ordering_info.shtml.

Product and Part Numbers

Available for customers with SMARTnet™ support at http://www.cisco.com/kobayashi/sw-center/vpn/client/.

Table 3.   Part Numbers for the Cisco VPN Client

Description	Part Number
Cisco VPN Client	CVPN-CLIENT-K9=

Documentation

For part numbers for product specific documentation, visit http://www.cisco.com/public/support/tac/tools.shtml#geninfo.

CISCO SYSTEMS

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on
the Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA