

Cisco VPN 3002 Hardware Client



Introduction

The Cisco VPN 3002 Hardware Client is a small hardware appliance that operates as a client in Virtual Private Networking (VPN) environments. It combines the best features of a software client, including scalability and easy deployment, with the stability and independence of a hardware platform.

One of the major advantages of the Cisco VPN 3002 is easy implementation. It has few local setup parameters and includes troubleshooting aids to ensure proper operation. Additional parameters and policy are “pushed” to the device from a central site after the unit has been set up.

In addition, the Cisco VPN 3002 scales easily to tens of thousands of devices. This is because as a client it can receive concentrator-assigned IP addresses from a pool, rather than end-to-end statically assigned addresses, which are required for LAN-to-LAN devices. The Cisco VPN 3002 can also coexist with, or work independently of, the software client typically used on MS-DOS or Windows, and NT-based PCs/workstations. This increases the number of operating system environments where VPN clients can be used.

In remote-office VPN environments customers now have three main choices for connectivity:

- Small router, VPN, or firewall devices for LAN-to-LAN connectivity
- Software clients that run on a PC or similar workstation
- The new Cisco VPN 3002 Hardware Client

Cisco VPN 3002 Hardware Client



Features and Benefits

- Provides fast and easy deployment and scalability to thousands of sites
- Includes Dynamic Host Control Protocol (DHCP) client and server compatibility for hundreds of stations behind the Cisco VPN 3002
- Supports Port Address Translation (PAT) for hiding stations behind the Cisco VPN 3002 from external view and attack
- Includes optional 8-port 10/100-Mbps auto-sensing switch
- Designed for wall mount or table top operation
- Supports Client and Network Extension modes for application flexibility
- Works with any operating system, such as Windows, MAC, Linux, Solaris, more
- Eliminates the need to add or support VPN applications on a PC or workstation
- Operates seamlessly with existing applications
- H.323 support in Client mode allows users to host and access NetMeeting sessions or access other H.323 applications



- Configurable Interface MTU, and Fragmentation Control Policy, including support for Path MTU Discovery (PMTUD)

Exploring Software Client and VPN Router Benefits

Small router, VPN, and firewall devices can be inexpensive and provide many features, including stateful firewall capabilities, but they lack true scalability beyond a few hundred devices. In addition, deployment and ongoing management can be inconvenient, time consuming, and expensive because of the numerous parameters and manual configurations required at both ends of the connection.

By contrast, software clients are typically provided for no charge with central site concentrators so they easily deploy and scale to large numbers. However, these clients have specific limited operating system support. Software clients may be impractical in extranet environments where the sponsor company does not own or control the PC (such as franchises), or does not want to incur the expense associated with maintaining non-company PCs and workstations.

Exploring Hardware Client Benefits

A hardware client combines the best features of a software client while maintaining the reliability and stability of a hardware platform. Because it uses push policy and is assigned an IP address from a pool of addresses in the concentrator, it has few parameters to manage and can be easily configured and deployed. However, unlike software clients, the hardware client operates across all operating systems and never interferes with the PC because it is an external piece of hardware. As a result, the hardware client is ideal for extranet applications or companies with a diverse set of operating system, or for companies with many remote offices or branches, such as franchise, bank, retail, and similar applications, that require simple, unattended operations or those applications where support is unavailable. A hardware client also appeals to companies that want to expand VPN solutions to home office users.

Why Use a Hardware Client?

Most large enterprises agree that the price of a hardware client is offset by the reduced or eliminated service calls typically associated with supporting software clients on the PC or the expense of supporting growing LAN-to-LAN networks with their complex configuration requirements at central and remote sites.

In summary, the value proposition for a hardware client includes:

- Scales to very large networks without requiring expensive implementation support at the central site
- Enables easy and secure deployments because policy and configuration are pushed from the central site
- Supports any operating system, enabling the client to plug in easily across networks
- Improves application stability because the client is deployed independently of the PC
- Pays for itself if it saves even one service call per year versus a router or software client
- Enables VPNs to be easily implemented by enterprises that do not have control over the remote PCs

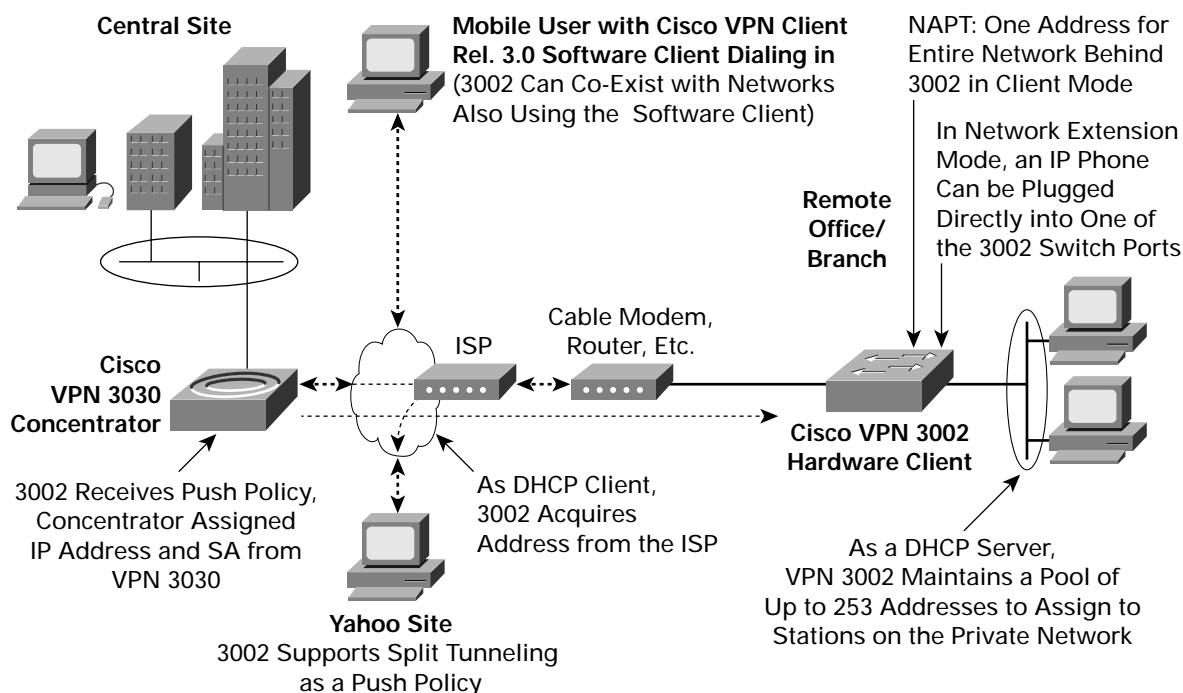
Cisco VPN 3002 Hardware Client Application

The Cisco VPN 3002 Hardware Client can also work alongside networks using the Cisco VPN (software) Client. It serves as a hardware client in applications where using a software client is impractical or undesirable. The Cisco VPN 3002 uses a DHCP client to acquire its IP address from the central site and a DHCP server to provide addresses to up to 253 stations in a single network behind it. The Cisco VPN 3002 uses PAT and can scale to tens of thousands of devices because as a client, it acquires a concentrator assigned IP address upon connection from a pool, eliminating manual route assignment.

The Cisco VPN 3002 supports the Cisco VPN Client Release 3.5 protocol using the Unified Client Framework. This enables it to connect to any Cisco central-site VPN Concentrator that supports the Unified Client Protocol Specification, including the Cisco PIX[®] Firewall, and Cisco IOS[®] central site concentrators, as well as to the Cisco VPN 3000 Concentrators.



Figure 1 Cisco VPN 3002 Hardware Client Application



Client and Network Extension Modes

For security and easy configuration, the Cisco VPN 3002 includes two modes: Client and Network Extension. In Client mode, the Cisco VPN 3002 emulates the operation of VPN client software. The stations behind the Cisco VPN 3002 are non-routable (invisible to the central site) and acquire their IP addresses from a built-in DHCP server. The VPN 3002 public port can acquire its IP address from an Internet service provider (ISP) by using its DHCP client capability.

In Network Extension mode the private address must be set manually but the stations behind the VPN 3002 are routable. This is important in applications where reaching a server, printer, POS terminal or other device is critical to the business. Push policy is still implemented and security is maintained at the central site.

Securing the Network in Client Mode

To secure the network in Client mode, the Cisco VPN 3002 uses Port Address Translation (PAT). The Cisco VPN 3002 can only make outbound connections;

therefore, no outside source can connect with the Cisco VPN 3002 or the stations behind it. Split tunneling, which is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet, can also be prohibited by creating a policy that is pushed from the central site. The Cisco VPN 3002 uses PAT to protect the stations it serves during split tunneling operations to the Internet.

Securing the Network in Network Extension Mode

In Network Extension mode, the stations behind the Cisco VPN 3002 are fully routable because the Cisco VPN 3002 now uses a secure site-to-site connection with the central site. However, when split tunneling is used to the Internet, the stations behind the Cisco VPN 3002 are still PAT protected. Outbound PAT on the Cisco VPN 3002 provides centralized security control because there are no configuration parameters for local users to adjust which might otherwise cause the central site to be compromised. All policies are pushed from a concentrator at the central site, eliminating the need or ability of local users to affect company security policies.



Auto Upgrade

The Cisco VPN 3002 also supports auto update to assist in upgrades. If an upgrade is needed, the unit upgrades automatically from an internal Trivial File Transfer Protocol (TFTP) server defined on the central site VPN Concentrator without end-user interaction.

Authentication Features

The VPN 3002 provides a unique client authentication mechanism that supplies a high level of security for both the VPN 3002 and the users behind the VPN 3002. With Interactive Unit Authentication the VPN 3002 can be set to use Saved or One Time Passwords. If Saved passwords are used, the device will not need to reauthenticate if the tunnel cycles. If One Time passwords are used, the device will need to be reauthenticated each time the tunnel cycles. The VPN 3002 supports preshared secrets, digital certificates and tokens for this mechanism.

In addition, the VPN 3002 can be set to require that each user behind the VPN 3002 authenticate before traversing the tunnel. This Individual User Authentication feature can be used alone or in conjunction with Interactive Unit Authentication to maximize security. Users behind the 3002 can be required to use preshared secrets or tokens with this method.

A unique capability of this technique is that the user is automatically intercepted when attempting to traverse the tunnel and redirected to a browser page to authenticate. Users do not need to initiate the security transaction since it happens automatically. This vastly improves ease of use. Users attempting to access the internet are not prompted for credentials unless Split Tunneling is disabled.

Load Balancing and Failover

The VPN 3002 supports the VPN 3000 load balancing mechanism in conjunction with the Cisco VPN Client. In this environment VPN 3002 will be transparently redirected to the least utilized concentrator in the central site network. This spreads the load evenly among all VPN Concentrators. In addition the VPN 3002 supports up to five back-up concentrators in the event the primary location is unavailable. It cycles through each back up IP address until it makes a successful connection thus

maximizing availability. The VPN 3002 can also be configured using the authentication techniques listed above to auto-reconnect and re-authenticate if desired.

PPPoE Support

Many ISPs now require PPPoE authentication for DSL or other access to their networks. VPN 3002 supports PPPoE Client mode for access to these networks. Users need only to authenticate to the PPPoE server the first time and VPN 3002 will authenticate for the user all subsequent attempts.

NAT Transparent IPSEC

The VPN 3002 supports three methods of NAT Transparent IPSEC including the UDP method implemented in the original release of the product, IPsec/TCP method, and the Ratified IPsec/UDP NAT-T specification, which includes Auto-detection and Fragmentation avoidance.

Specifications

Operating Environment

Temperature: 29° to 104°F (-5° to 0°C)

Storage: -4° to 176°F (-40° to 70°C)

Relative humidity: 0 to 95% noncondensing

Hardware Processor

Motorola 8260 processor: dual flash image architecture

Network Interfaces

On all models, all Ethernet ports are auto-sensing, which eliminates the need for crossover cables.

CPVN3002-K9: one public 10/100-Mbps RJ-45 Ethernet interface and one private 10/100-Mbps RJ-45 Ethernet interface

CVPN3002-8E-K9: one public 10/100-Mbps RJ-45 Ethernet interface and 8 private ports 10/100-Mbps RJ-45 Ethernet interfaces via auto-sensing switch, which eliminates the need for crossover cables

Physical Dimensions

Height: 1.967 x 8.6 x 6.5 in (5 x 22.5 x 16.51) (HxWxD)

Power Supply

External AC operation: 100-240V at 50/60 Hz with universal power factor correction; 4-ft cord included and international pigtail power cord selection



Instrumentation and Physical Ports

Front panel: status LEDs for Power, Tunnel Status and VPN establishment

Rear panel: status LEDs for Ethernet ports (amber/green)

Rear connectors for CVPN 3002-K9: three (3) RJ-45 ports including (1) public port, (1) private port and (1) console port with full signals

Rear connectors for CVPN 3002-8EK9: ten (10) RJ-45 ports including (1) public port, (8) private port switch and (1) console port with full signals

Reset switch: resets unit to factory defaults

Power cord connector

Approvals

Product bears CE Marking indicating compliance with the 89/336/EEC and 72/23/EEC Directives: UL 60950, CSA C22.2 No.60950, IEC 60950, EN 60950, AS/NZS 3260, FCC (CFR47) Part 15 Class B, ICES-003 Class B, EN55022 Class B, CISPR22 Class B, AS/NZS 3548 Class B, VCCI Class B, EN55024, EN50082-1

Tunneling Protocol Support

IP Security (IPSec) with Internet Key Encryption (IKE) key management

Cisco Unified Client Framework Compatibility

Connects in Client mode with Cisco VPN 3000 Concentrators, Cisco PIX Firewalls, and many Cisco IOS (Central Site Concentrators. Works with devices that comply with the Cisco Unified Client Protocol Specification..

Monitoring and Configuration

Event logging; SNMP MIB-II support

Embedded management interface: accessible via console port or local Web browser; Secure Shell (SSH)/Secure Socket Layer (SSL)

Encryption Algorithms, Key Management, and Authentication Algorithms

56-bit Data Encryption Standard (DES) (IPSec); 168-bit Triple DES (3DES) (IPSec); AES (128/256-bit); MD5; SHA-1; HMAC with MD5; HMAC with SHA-1

Authentication

- Unit User Name and Password preshared secret or Digital Certificates and/or Tokens
- Browser intercepted Interactive Unit Authentication with One Time or Saved Passwords
- Browser intercepted Individual User Authentication for up to 253 users behind the 3002; security information maintained at the central site
- SDI Tokens supported: Digital Certificates supported for Unit Authentication only (not for Individual User Authentication)
- Patent Pending on VPN 3002 Interactive Unit Authentication only (not for Individual User Authentication with HTTP Redirect)

Configuration Modes

Client mode: Cisco VPN 3002 acts as client, receives IP address from a concentrator pool; uses PAT to hide stations behind the Cisco VPN 3002; network behind the Cisco VPN 3002 is unroutable (invisible to central site and the world); provides few configuration parameters

Network Extension mode: Cisco VPN 3002 acts as site-to-site device; uses PAT to hide stations only to Internet (stations visible or routable to central site); network behind the Cisco VPN 3002 is routable; provides additional configuration parameters

Authentication, Authorization, and Accounting (AAA)

Supports Remote Authentication Dial-In User Service (RADIUS) accounting and security from the central site

Part Numbers

Part Number	Description
CVPN3002-K9	Basic unit without switch; software and power cord ordered separately
CVPN3002-8E-K9	Unit with 8-port switch; software and power cord ordered separately
CVPN3002-BUN-K9	Includes hardware, latest software, and US power cord
CVPN3002-8E-BUN-K9	Includes 8-port switch, hardware, latest software, and US power cord

Part Number	Description
CVPN3002-SW-36-K9	Release 3.6 software for Cisco VPN 3002



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site 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

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratim, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0402R) DB/KC/LW5853 3/04