



Cisco VPN 3000 Series Concentrator

Introduction

The Cisco® VPN Series 3000 Concentrator allow corporations to take full advantage of the unprecedented cost savings, flexibility, performance, and reliability of remote access VPN connections. Corporations use VPNs to establish secure, end-to-end private network connections over a public networking infrastructure. VPNs have become the logical solution for remote-access connectivity for two main reasons:

- Deploying a remote-access VPN enables corporations to reduce communications expenses by using the local dialup infrastructures of Internet service providers.
- Remote Access VPNs allow mobile workers, telecommuters and day extenders to take advantage of broadband connectivity.

To fully realize the benefits of high-performance, remote-access VPNs, a corporation must deploy a robust, highly available VPN solution, and dedicated VPN devices are optimal for this purpose.

The Cisco VPN 3000 Series Concentrator is a best-in-class, remote-access VPN solution for enterprise-class deployment. A standards-based, asy-to-use VPN client and scalable VPN tunnel termination devices are included, as well as a management system that enables corporations to easily install, configure, and monitor their remote access VPNs. Incorporating the most advanced, high-availability capabilities with a unique purpose-built, remote-access architecture, the Cisco VPN 3000 Concentrator allows corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications.

Unique to the industry, it is the only scalable platform to offer components that are field-swappable and can be upgraded by the customer. These components, called Scalable Encryption Processing (SEP/SEP-E) modules, enable users to easily add capacity and throughput.

The Cisco VPN 3000 Concentrator supports the widest range of VPN client software implementations, including the Cisco VPN Client, the Microsoft Windows 2000/XP L2TP/IPsec Client, the Microsoft L2TP/IPSec VPN Client for Windows 98, Windows Millennium (ME), Windows NT Workstation 4.0, and Microsoft PPTP.



Five Models

The Cisco VPN 3000 Concentrator is available in five different models:

Cisco VPN 3005 Concentrator

The Cisco VPN 3005 Concentrator is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous sessions. Encryption processing is performed in software. The Cisco VPN 3005 does not have built-in upgrade capability.

Cisco VPN 3015 Concentrator

The Cisco VPN 3015 Concentrator is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous sessions. Like the Cisco VPN 3005, encryption processing is performed in software, but the Cisco VPN 3015 is also field-upgradeable to the Cisco VPN 3030 and 3060 models.

Cisco VPN 3030 Concentrator

The Cisco VPN 3030 Concentrator is a VPN platform designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3(50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. The Cisco VPN 3030 is field-upgradeable to the Cisco VPN 3060. Redundant and nonredundant configurations are available.

Cisco VPN 3060 Concentrator

The Cisco VPN 3060 is a VPN platform designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) and up to 5000 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and nonredundant configurations are available.

Cisco VPN 3080 Concentrator

The Cisco VPN 3080 Concentrator is optimized to support large enterprise organizations that demand the highest level of performance combined with support for up to 10,000 simultaneous remote access sessions. Specialized SEP modules perform hardware-based acceleration. The VPN 3080 is available in a fully redundant configuration only.



Models Comparison

Table 1 The Cisco VPN 3000 Series Supports the Entire Range of Enterprise Applications

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous Users¹	100	100	1,500	5,000	10,000
Maximum LAN-to-LAN Sessions	100	100	500	1000	1000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Available Expansion Slots	0	4	3	2	2
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	–	–	Option	Option	Yes
System Memory	32/64 MB (fixed)	128 MB	128/256 MB	256/512 MB	256/512 MB
Hardware Configuration	1U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

1. For planning purposes, a simultaneous user is considered to be a remote access VPN user connected in all tunneling mode—this includes one IKE Security Association and two unidirectional IPsec SAs (Security Associations). For environments with rekeying or split tunneling, we recommend using a VPN remote access load-balancing environment with spare capacity because these particular sessions will use additional system resources that otherwise would be used to support additional users. The Cisco VPN 3000 Series Concentrator supports the entire range of enterprise applications.

Cisco VPN Client

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator. This thin design, IPsec-compliant implementation is provided with the Cisco VPN 3000 Concentrator and is licensed for an unlimited number of users. The client can be pre-configured for mass deployments and the initial logons require very little user intervention. VPN access policies are created and stored centrally in the Cisco VPN 3000 Concentrator and pushed to the client when a connection is established.



Features and Benefits

Product Highlights

High-Performance, Distributed-Processing Architecture

- Cisco SEP modules provide hardware-based encryption, ensuring consistent performance throughout the rated capacity (Cisco VPN 3030–3080).
- Large-scale tunneling support provided for IPsec, PPTP and L2TP/IPsec connections.

Scalability (Cisco VPN 3015–3060)

- Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path.
- System architecture is designed to supply consistent, high-availability performance.
- All digital design provides the highest reliability and 24-hour continuous operation.
- Robust instrumentation package provides run-time monitoring and alerts.
- Microsoft compatibility offers large-scale client deployment and smooth integration with related systems.

Security

- Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products.
- Firewall capabilities through stateless packet filtering and address translation to ensure the required security of a corporate LAN.
- User and group level management offers maximum flexibility.

High Availability

- Redundant subsystems and multichassis failover capabilities ensure maximum system uptime.
- Extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early-warning alerts.

Robust Management

- The Cisco VPN 3000 Concentrator can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, SSHv1, and using a console port. Files can be accessed through HTTPS, FTP, and SSH Copy (SCP).
- Configuration and monitoring capability is provided for both the enterprise and the service provider.
- Access levels are configurable by user and groups, allowing easy configuration and maintenance of security policies. For larger scale deployments, the VPN 3000 Concentrators are supported in several Cisco network management applications. Those applications include:
 - *IP Solution Center (ISC)*—Provisions site-to-site and remote access VPN services
 - *VPN Monitor*—Monitors and reports on remote access and site-to-site VPN tunnel connections
 - *Resource Manager Essentials (RME)*—Provides operational management features such as software distribution, syslog reporting, inventory management
 - *CiscoView*—Provides real time system status monitoring



Technical Specifications

Hardware

Processor

- Motorola PowerPC Processor

Memory

- Redundant system images (Flash)
- Variable memory options (see chart)

Encryption

- *Cisco VPN 3005, 3015*—Software encryption
- *Cisco VPN 3030–3080*—Hardware encryption

Embedded LAN Interfaces

- *Cisco VPN 3005*—Two autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted)
- *Cisco VPN 3015–3080*—Three autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted and DMZ)

Instrumentation

- *Cisco VPN 3005 Front panel*—Unit status indicator
- *Cisco VPN 3005 Rear panel*—Status LEDs for Ethernet ports
- *Cisco VPN 3015–3080 Front panel*—Status LEDs for system, expansion modules, power supplies, Ethernet modules, fan
- *Cisco VPN 3015–3080 Rear panel*—Status LEDs for Ethernet modules, expansion modules, power supplies
- *Cisco VPN 3015–3080*—Activity monitor displays number of sessions, aggregate throughput, or CPU utilization; push-button selectable

Software

Client Software Compatibility

- Cisco VPN Client (IPsec) for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit), and Mac OS X 10.2 (Jaguar), including centralized split-tunneling control and data compression
- Microsoft PPTP/MPPE/MPPC, MSCHAPv1/v2, EAP/ RADIUS pass-through for EAP/TLS and EAP/GTC support
- Microsoft L2TP/IPsec for Windows 2000/XP (including XP DHCP option for route population)
- Microsoft L2TP/IPsec for Windows 98, Windows Millennium (ME), and Windows NT Workstation 4.0
- MovianVPN (Certicom) Handheld VPN Client with ECC
- Netlock (Mac OS 8 & 9) VPN Client

Tunneling Protocols

- IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec, Ratified IPsec/UDP (with auto-detection and fragmentation avoidance), IPsec/TCP
- Support for Easy VPN (client and network extension mode)



Encryption/Authentication

- IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) or AES (128, 192, 256-bit) with MD5 or SHA, MPPE using 40/128-bit RC4

Key Management

- Internet Key Exchange (IKE)
- Diffie-Hellman (DH) Groups 1, 2, 5, 7 (ECDH)

Routing

- RIP, RIP2, OSPF, RRI (Reverse Route Injection), static, automatic endpoint discovery, Network Address Translation (NAT), Classless Interdomain Routing (CIDR)
- IPsec fragmentation policy control, including support for Path MTU Discovery (PMTUD)
- Interface MTU control

Third-Party Compatibility

- Certicom, iPass Ready, Funk Steel Belted RADIUS certified, NTS TunnelBuilder VPN Client (Macintosh and Windows), Microsoft Internet Explorer, Netscape Communicator, Entrust, Baltimore, SA Keon

High Availability

- VRRP protocol for multi-chassis redundancy and fail-over
- Remote Access Load Balancing clusters
- Destination pooling for client-based fail-over and connection re-establishment
- Redundant SEP modules (optional), power supplies, and fans (Cisco VPN 3015–3080)

Management

Configuration

- Embedded management interface is accessible through console port, Telnet, SSHv1, and Secure HTTP (HTTPS)
- Administrator access is configurable for five levels of authorization. Authentication can be performed externally through TACACS+
- Role-based management policy separates functions for service provider and end-user management

Monitoring

- Event logging and notification through e-mail (SMTP)
- Automatic FTP backup of event logs
- SNMP MIB-II support
- Configurable SNMP traps
- Syslog output
- System status
- Session data (including client assign IP, encryption type connection duration, client OS, version, etc)
- General statistics



Security

Authentication and Accounting Servers

- Support for redundant external authentication servers:
 - RADIUS
 - Kerberos/Active Directory authentication
 - Microsoft NT Domain authentication
 - Microsoft NT Domain authentication with Password Expiration (MSCHAPv2)

RSA Security Dynamics (SecurID Ready), including native support for RSA 5 (Load Balancing, Resiliency)

- User authorization through LDAP or RADIUS
- Internal Authentication server for up to 100 users
- X.509v3 digital certificates (including CRL/LDAP and CRL/HTTP, CRL Caching and Backup CRL Distribution Point support)
- RADIUS accounting
- TACACS+ Administrative user authentication

Internet-Based Packet Filtering

- Source and destination IP address
- Port and protocol type
- Fragment protection
- FTP session filtering
- Site-to-Site Filters and NAT (for overlapping address space)

Policy Management

- By individual user or group
 - Filter profiles (defined internally or externally)
 - Idle and maximum session timeouts
 - Time and day access control
 - Tunneling protocol and security authorization profiles
 - IP Pool
 - Authentication Servers

Certification

- FIPS 140-2 Level 2 (3.6) in process, FIPS 140-1 Level 2 (3.1), VPNC

Ports

- Console port-Asynchronous serial (DB-9)



Table 2 Physical Characteristics

Concentrator	Cisco VPN 3005	CiscoVPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Height	1.75" (4.45cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)
Width	17.5" (44.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)
Depth	11.5" (29.21cm)	-	-	-	-
Unit without front bezel or SEPS/PS	-	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)
Unit with front bezel, no SEPS/PS	-	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)
Unit with front bezel and SEPS/PS	-	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)
Weight	8.5 lbs(3.9kg)	27 lbs(12.3kg)	28 lbs(12.7kg)	33 lbs(15kg)	33 lbs(15kg)

Table 3 Power Type and Requirements

Concentrator	Cisco VPN 3005	CiscoVPN 3015-3080
Nominal	15 watts (51.22BTU/hr)	35 watts (119.50BTU/hr)
Maximum	25 watts (85.36BTU/hr)	50 watts (170.72BTU/hr)
Input Voltage	100-240VAC	100-240VAC
Frequency	50/60 Hz	50/60 Hz
Power Factor Correction	Universal	Universal

Environmental

- Temperature: 32 to 131 F (0 to 55 C) operating; -4 to 176 F (-40 to 70 C) nonoperating
- Humidity: 0 to 95 percent noncondensing

Regulatory Compliance

- CE Marking

Safety

- UL 1950, CSA

EMC

- FCC Part 15 (CFR 47) Class A, EN 55022 Class A, EN50082-1, AS/NZS 3548 Class A, VCCI Class A



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 • 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