

AVAYA



Avaya VPNet Solutions: VSU™ Series Gateways

Making VPNs Easier to Deploy, Manage, and Scale



Converged Voice and
Data Networks
Customer Relationship
Management
Unified Communication
Supported by:
Avaya Labs and Services

Communication without boundaries



Now, organizations of all sizes can take full advantage of the cost-saving, productivity, and customer relationship-building benefits of replacing existing communications systems with Virtual Private Networks (VPNs).

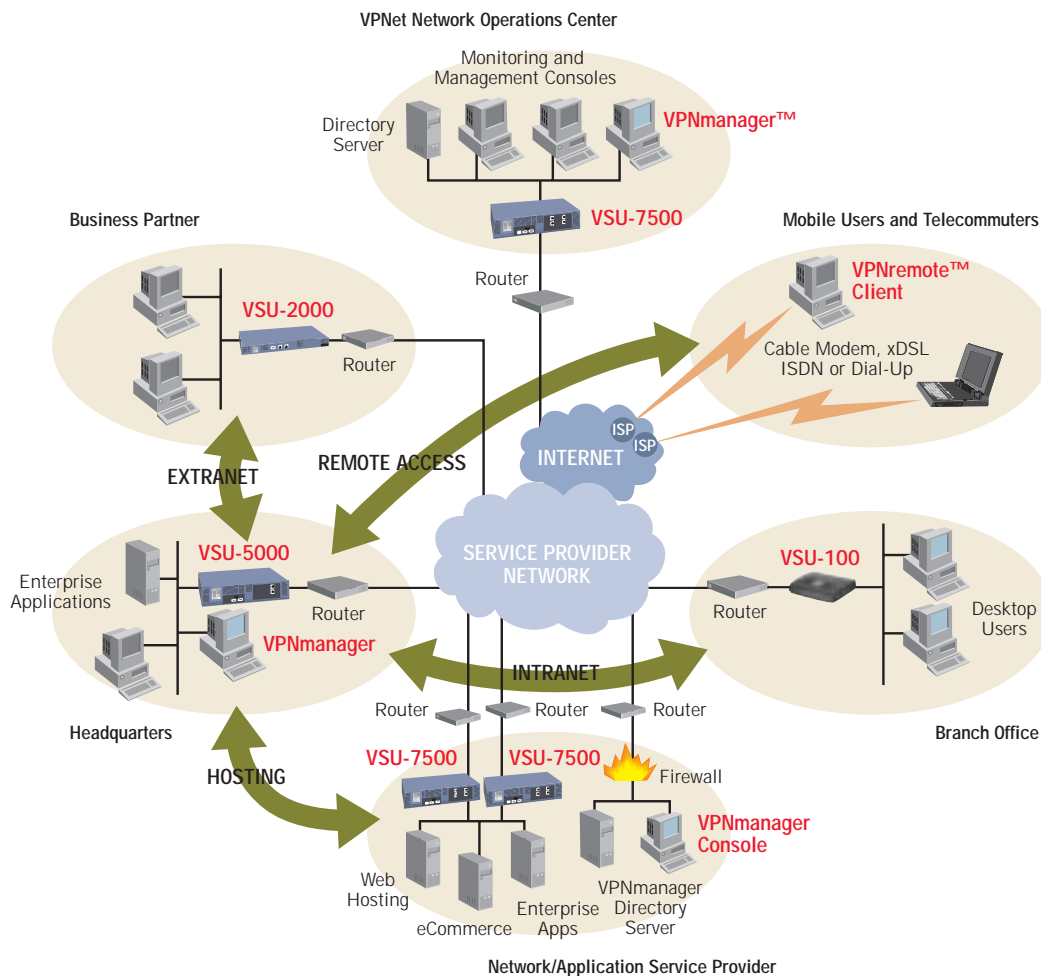
Avaya VPN Service Units (VSUs) are dedicated hardware-based VPN gateways that enable data communications over shared public IP networks (such as the Internet) with unmatched levels of price/performance, manageability, and security. So you can focus on your core business, rather than on the network infrastructure that supports it.

Your Gateway to Private Data Communications over Public IP Networks

Powered by integrated Avaya VPNos operating software, Avaya VSU™ Series Gateways provide standards-based IPSec services that enable organizations to securely connect remote users, branch offices, partners, and customers to enterprise networks. Avaya VSUs provide an overlay VPN solution that integrates transparently

and non-intrusively into your existing network. This provides authentication, encryption, tunneling, and firewall security services — protecting both private networks and data as it traverses public networks.

Above all, Avaya VSU Series Gateways make it easy for your authorized users to securely perform everyday network tasks — regardless of where they work in your enterprise. This makes life easier for both users and system administrators.





Highlights

- Simple Installation and Configuration
 - Reduces complexity for branch offices and partner sites
- Centralized Security Management
 - Policy and configuration information centrally configured and transparently delivered
- Simple integration into networks of all sizes and complexity
 - Transparent and non-intrusive gateway integration
- Easy integration with existing network devices leverages investment in authentication servers or firewalls
- Robust IPSec, Authentication, and Firewall Security Services
- Standards-Based and Interoperable
 - ICSA IPSec, NIST FIPS 140-1 Level 2 Certified
 - ICSA Firewall Certification
 - Support all major PKI vendors

Avaya VPNet Solutions: Part of an End-to-End MSNI Solution

The broad line of Avaya VPN products and services are easy to use, manage, and deploy on a small or large scale. These solutions serve enterprises of all sizes (as well as managed data service providers who have enterprise customers) that demand performance, scalability, rapid VPN deployment, and lower capital and administrative costs.

Avaya offers industry-leading integrated management of VPN, firewall, networking policies, and device configurations. This integration allows remote access, site-to-site, and Extranet VPNs to be delivered on a single platform.

The Avaya VPNet portfolio is part of the high-quality Avaya MultiService Networking Infrastructure (MSNI) solutions. Working together, MSNI components leverage your existing network investment to support IP-enabled voice, data, and video convergence applications.

Along with the Avaya VPN Solutions Portfolio, Avaya's proven MSNI components include:

- Avaya Cajun™ Network Switch Solutions
- CajunView™ Network Management and CajunRules™ Policy Management
- SYSTIMAX® Structured Connectivity Solutions
- Avaya Wireless LAN Solutions

VSU-7500



The Right VPN Gateway Solution for Your Networking Needs

By delivering IPsec 3DES encryption, data integrity and authentication, and key management, Avaya VSUs give you the confidence to run your business-critical data and applications across public IP networks. You'll always know who's accessing your VPN because Avaya VSUs support a range of two-factor user authentication methods — including RADIUS servers, RSA SecurID® tokens, smartcards, and digital certificates.

Avaya offers a full line of VSU Series Gateways to meet the price/performance requirements of all segments of the enterprise and service provider markets:

- The VSU-100 for small and medium-size businesses;
- The VSU-2000 for branch offices; and
- The VSU-5000 and VSU-7500 for larger-scale enterprises.

All Avaya VSU Series Gateways offer resilient VPN tunneling. In the event of a data link failure, the gateways continually sense endpoint availability and transition VPN connectivity to a secondary VSU.

Plus, the VSU-7500 offers an additional level of fault tolerance by providing high-availability hardware features such as redundant Ethernet interfaces, IPsec processors, power supplies, and cooling fans.

Fast Wire Speeds Keep Pace with Networks and Users

Whether you're managing thousands of remote access users or connecting multiple sites of a globally-distributed enterprise organization, your network will continue to perform optimally with the Avaya VSU series of VPN gateways. That's because they deliver all the benefits of VPNs without creating the performance bottlenecks that slow your network to a crawl.

Unlike firewall- or router-based VPN solutions, each Avaya VSU gateway offers dedicated IPsec packet-processing engines and real-time data compression.



VSU-5000



Scalable Architecture for Flexible Networking

Ease of Use:
The Avaya VPNet Difference

- Delivers VPN policy transparently to end user desktops
- Simplifies VPN networking for end users and remote administrators
- Lowers your overall cost of network ownership

Is your network enabling the growth of your business — or inhibiting it? Avaya VSU Series Gateways provide a secure solution that can easily adapt to your changing networking needs.

This scalability starts with industry-leading IPSec performance and ICSA-certified interoperability. It also means removing the bottlenecks associated with managing large remote user groups. Because the building and re-keying of IPSec tunnels is data-intensive, VSUs feature a dedicated engine to process IPSec security associations.

Making VPNs scalable means more than just ensuring compatibility, tunnel processing power, and optimum throughput. You also need to be able to quickly and easily update remote site and user configurations for large or complex VPNs.

Avaya VSUs accomplish this by leveraging the scalable client/server architecture of Avaya VPNmanager™, which is built on an LDAP directory server backbone. Using VPNmanager, policy changes are made centrally at the directory server rather than locally at each VSU gateway. Then, VPN policy information is securely delivered via a fast and efficient communication protocol — transparently and efficiently updating multiple devices simultaneously. This eliminates the need to provide costly IT resources to support the deployment and management of VPNs.



VSU-100

Easy to Deploy and Integrate with Your Network

Avaya VSU Series Gateways are deployed behind an access router to provide site-to-site and remote access VPN solutions. They support remote access, Intranet and Extranet site-to-site, and service provider VPN deployments.

As a layered network security solution, Avaya VSUs integrate easily with existing firewalls, routers, and servers on enterprise networks. They also provide an integrated interface to service provider managed IP backbones. Avaya VSUs support full-featured network firewall, dynamic routing, and Quality of Service (QoS)-enabled networking capabilities and Network Address Translation (NAT). This makes them easy to install, configure, and maintain in networks of all sizes and complexity.

In fact, the only installation information required locally at the gateway is the IP address, mask, and



VSU-2000

setting the console password. All additional configuration and policy information is pushed out to the VSUs from Avaya VPNmanager — without the need for local intervention. To monitor network activity and gather system management information from Avaya VSUs, VPNmanager uses SSL-secured SNMP traffic. This reduces the skill set required to provision and manage branch offices. For easy remote network access, the Avaya VSU Series Gateways are supported by Avaya VPNremote™ Client software.

Dedicated VPN Gateway Advantages

- Superior encryption performance
- Simplified network integration
- More network configuration flexibility
- Simplified network troubleshooting
- No single point of failure



Integrated Firewall Protection

All Avaya VSU Series Gateways provide a comprehensive set of network firewall features based on stateful inspection and packet filtering technologies. Avaya VSUs offer a built-in firewall that allows firewall and VPN policies to be managed in a unified environment. This firewall can be applied to either VPN or non-VPN traffic.

This advanced firewall functionality further enhances the protection of private networks by providing a high level of security policy granularity and a rich set of attack prevention mechanisms. Avaya VPNmanager integrates both firewall and VPN policy management within a simple-to-use, graphical user interface (GUI)-based Java™ console — making Avaya VSUs a complete perimeter security appliance without sacrificing ease of use.

	VSU-100 VSU-100R	VSU-2000	VSU-5000	VSU-7500
Description	Low-cost, entry-level VPN gateway; Available with optional remote access services	Mid-range VPN gateway	High-capacity VPN gateway	High-availability VPN gateway with hardware redundancy
Simultaneous Tunnels	Up to 100	Up to 1,000	Up to 5,000	Up to 7,500
Typical Users	Small enterprise, branch/partner office, or home office	Mid-sized enterprise, branch/partner office	Large enterprise	Large enterprise, managed VPN data service provider
Bandwidth	T1/E1, xDSL, cable modem, ISDN	Up to T3/DS3	Up to Full Duplex T3/DS3	Up to Line Speed Fast Ethernet
Applications	Intranets and extranets up to 100 IPsec site-to-site sessions; VSU-100R additionally supports remote access services	Remote access up to 1,000 users, intranets, extranets	Remote access up to 5,000 users, high bandwidth intranets and extranets	Remote access up to 7,500 users, high bandwidth intranets and extranets, application hosting, managed VPN services requiring hardware redundancy

Avaya VSU Series Gateway Features

Data Encryption

- DES encryption (56-bit key)
- Triple DES (EDE-CBC) encryption* (168-bit key)

Data Authentication

- Keyed MD5™ AH Message Digest Algorithm (RFC 1321)
- HMAC-MD5 and HMAC SHA-1 (RFC 2104)

User Authentication

- LDAP
- RADIUS
- RSA SecurID tokens (including New Pin/Next Token Modes)
- X.509v3 digital certificates (IKE key management)

Compression

- Stac™ Lempel-Ziv hardware data compression IPsec Security Services
- AH — Authentication Header (RFC 2402)
- ESP — Encapsulating Security Payload (RFC 2406)
- Tunnel and Transport Modes
- Full IPsec compliance (RFC 1825-1829, 1851, 2401-2410, 2412, 2451)

Key Management

- IKE key management: key updates configurable starting from 60 seconds (RFC 2409)
- SKIP key exchange: keys updated every 30 seconds

Firewall

- Stateful inspection-based firewall providing strong attack prevention against DOS (denial of service attack), Syn flood, ICMP flood, port scan, and many more.

Network Address Translation (NAT)

- Supports static, dynamic, and port mapping
- Client IP address pool for remote access clients
- QoS
- DiffServ packet classification (RFC 2474)

Routing Support

- Default router auto-discovery using ICMP packets
- RIPv1 and RIPv2 routing for VPN traffic
- Static routes

Digital Certificates

- X.509v3 for management and IPsec communication
- PKCS#7/10/11/12
- Compatible with Entrust, RSA, Baltimore, VeriSign, IBM, Microsoft, and Netscape



* U.S. export regulations restrict the use of strong cryptography for certain applications and in certain countries. Contact Avaya VPNet or your Avaya VPNet representative for a current list of controlled and uncontrolled applications and territories. Specifications subject to change without notice.



System Management

- Configuration and monitoring via VPNmanager
- Monitoring from any application with SNMPv1
- Configuration traffic secured through SSL
- Syslog event and usage logging

Remote Client Support

- VPNremote Client (Windows® 95/98, Windows NT®, Windows 2000, Windows ME)
- Simultaneous VPN and Internet access (split tunneling)
- Compatible with major Windows dialers

Physical Security

- Tamper-evident enclosure (FIPS 140-1 Level 2)

Open a New Gateway to VPN Profitability

Make the most of the profit potential of VPNs — and leverage your existing network investment — with the Avaya VPNet portfolio.

The industry-leading ease-of-use, manageability, scalability, and price/performance of Avaya VSU Series Gateways make them superior to any other gateway solution. And since the VSU Series is backed by the global presence and leadership of Avaya, you know you'll be getting a complete end-to-end network solution that will help your enterprise excel in the new Customer Economy for years to come. Plus, Avaya Services and Avaya Labs offer your enterprise world-class support for your multi-vendor data networks.

To find out more about selecting the right Avaya VSU Series solution for your enterprise and networking applications — and the other Avaya MSNI solution components — please contact your Avaya representative or Authorized BusinessPartner — or visit our Web site at: avaya.com/solutions.



	VSU-100	VSU-2000	VSU-5000	VSU-7500
Dimensions	7.75" × 6.5" × 1.9" (19.7 cm × 16.5 cm × 4.8 cm) Wall mountable	17.5" × 11.5" × 1.75" (44.5 cm × 29.2 cm × 4.45 cm) 1U high 19" rank mountable	17.0" × 13.5" × 3.5" (43.2 cm × 34.3 cm × 8.9 cm) 2U high 19" rank mountable	17.0" × 14.9" × 3.5" (43.2 cm × 38.0 cm × 8.9 cm) 2U high 19" rank mountable
Weight	2.75 lbs. (1.24 Kg)	8 lbs. (3.6 Kg)	17 lbs. (7.7 Kg)	20 lbs. (9 Kg)
LAN Interface	Two 10/100BaseT Ethernet ports	Two 10/100BaseT Ethernet ports	Two 10/100BaseT Ethernet ports	Four 10/100BaseT Ethernet ports
Management Interfaces	RS-232 and 100BaseT Ethernet	RS-232 and 100BaseT Ethernet	RS-232 and 100BaseT Ethernet	RS-232 and 100BaseT Ethernet
High Availability Features				Redundant hardware features: Ethernet interfaces Encryption processors Power supplies (hot-swappable) Cooling fans (hot-swappable)
Power Requirements	120/240 VAC Input frequency: 60/50 Hz AC current input: 1.0–0.5 Amps	120/240 VAC Input frequency: 60/50 Hz AC current input: 1.0–0.5 Amps	120/240 VAC Input frequency: 60/50 Hz AC current input: 2.5 Amps	115/230 VAC Input frequency: 60/50 Hz AC current input: 6.0–3.0 Amps
Operating Environment	Temperature: 32° to 104°F, 0 to 40°C Relative Humidity: 5 to 90% (non-condensing) Altitude: 0–12,000 feet, 3660 meters			
Safety Certification	UL, US/C, CSA US/C, CE,CB	CSA US/C, CE,CB	CSA US/C, CE,CB	CSA US/C, CE,CB
EMI/RFI	FCC Part 15, Class B CISPR 22/85A VCCI, BSMI	FCC Part 15, Class A CISPR 22/85A VCCI, BSMI	FCC Part 15, Class A CISPR 22/85A VCCI, BSMI	FCC Part 15, Class A CISPR 22/85A VCCI, BSMI
Warranty	12-month warranty. Extended support contracts available.			

Ordering Information

Product	PEC Code	COM Code
VSU-100	4570-001	700057078
VSU-100R	4570-003	700057102
VSU-2000	4571-001	700057151
VSU-5000	4572-001	700057177
VSU-7500	4573-001	700057201

AVAYA

© 2001 Avaya Inc.

All rights reserved. All trademarks identified by ®, SM and TM are registered trademarks, servicemarks or trademarks respectively. All other trademarks are properties of their respective owners.

Printed in the U.S.A. 09/01 • VPN1416

