AT&T Virtual Private Network tunneling services

Description

AT&T VPN Tunneling Service is an IP-based service that sends encrypted confidential business data over the Internet or other public networks.

With AT&T VPN Tunneling Service, use broadband, wireless, dial-up, or dedicated access services to connect to the network. Once connected, you can access your corporate Local Area Network (LAN) and intranet applications.

Your VPN is created by adding intelligent devices at your locations and using private and public networks to transport data between them. Transporting data over public networks has an inherent security risk. IPSec is today's most widely used encryption technology, and AT&T VPN Tunneling Service uses IPSec to create paths that carry your data encrypted over public networks creating a highly secure pathway.

Encryption helps prevent others from copying or reading transmitted information, integrity checks help ensure that no one tampers with data in transit and authentication is designed to verify that the user sending or viewing the data is authorized to do so. These three security measures allow your sensitive data to reliably transit the public network to its destination.

Flexible

AT&T VPN Tunneling Service can be used as a remote access service or as an inter-office service. Remote or mobile users can access your corporate network over AT&T's wireless, Wi-Fi, Wired Ethernet, Broadband, AT&T dial-up, or any other existing Internet connections. Connect small, medium, or large office locations over broadband or dedicated connections. This is a fully-managed premises-based service with all required hardware and software located at your business or employee locations.
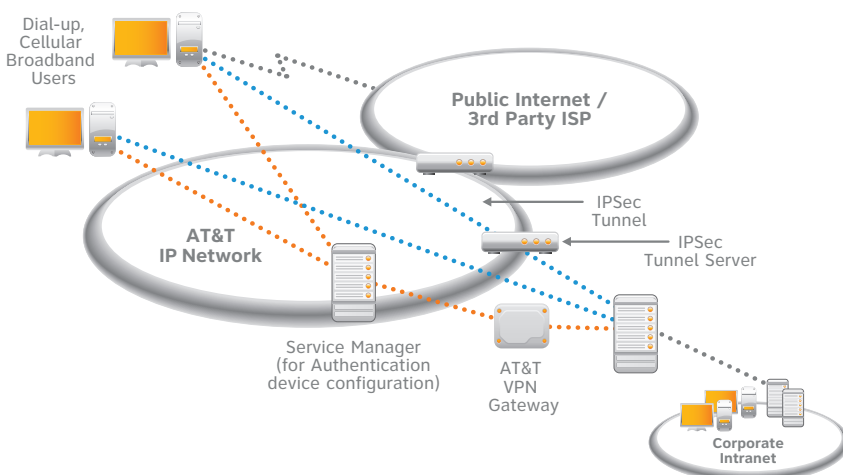
Potential Benefits

- Extensive availability, both domestically and globally
- Security through encryption, firewalls, and customized security policy
- Flexible access permits virtually from 'any' to 'any' connectivity
- Affordable and easy to use, including all hardware and software
- Reliable, built in disaster recovery and end-to-end managed services

Features

- Management of all customer onsite devices 24x7 provides proactive heads-up and initiation of trouble resolution activities. We watch the network, so you don't have to
- Service Level Agreements provide reports on network performance
- Coordinated management of CPE requirements, design and installation activities with vendors helps ensure the highest quality service available
- Managed design and installation assures the integration into the overall corporate network infrastructure, both on customer site and AT&T access facilities

AT&T IP Network

Dial-up, Cellular Broadband Users

Public Internet / 3rd Party ISP

AT&T IP Network

IPSec Tunnel

IPSec Tunnel Server

Service Manager (for Authentication device configuration)

AT&T VPN Gateway

Corporate Intranet

Share this with your peers

AT&T VPN Tunneling Services Advantage

Performance – Seamless integration of applications with your core infrastructure from multiple types of connections, broadband, wireless, Wi-Fi or dial

Agile – With our integrated, agile networking platform, you can quickly add or change applications as your business needs dictate

Control – Visibility and control with web-based tools. user authentication and encrypted transport of data, from users in the office or working remotely

Security Services – Built-in robust security measures at every network layer to minimize the risk of outages and intrusions

Options with AT&T VPN Tunneling Services

IPSec – Provides network layer security such as authentication, encryption and data integrity checks. IPSec supports both remote access and site-to-site connections

Secure Socket Layer (SSL) – Designed to help secures two end-points of an application that are communicating (e.g., client-server). SSL provides transport layer security feature for remote access connections for applications that use a web-browser interface

Layer 2 Tunneling Protocol (L2TP) – Provides tunneling capability through Point-to-Point Protocol (PPP) processes. L2TP allows you to choose RADIUS

support, RSA Security's SecurID™ token based authentication, or AT&T authentication for remote access for your employees

Point-to-Point Tunneling Technology – Provides tunneling between Windows remote users with AT&T remote access service and AT&T's LAN-based connectivity server. Point-to- Point Transfer Protocol (PPTP) provides security services such as authentication, and encryption at the data link layer

Site-to-Site Access – provides three site to-site Intranet options and one extranet option: SOHO (small office/home office), using, High-End, using dedicated 56k – DS3 Internet access and Integrated VPN Tunneling Service which supports all remote access or site-to-site access options

Share this with your peers

For more information contact your AT&T Solution Provider.

Scan this code to learn more.

at&t Solution Provider