Maximize your WAN

AT&T Private Mobile Connection

Introduction

In today's competitive landscape, connecting remote workers and branch locations to the enterprise Wide Area Network (WAN) has become a necessity. However, flexibility in the connections to that WAN has become ever more important given the fast pace of today's enterprise environment. Mobile access technology enables enterprises to support remote worker and branch office access to the enterprise WAN, while also providing true access diversity in backup applications.

To learn more about AT&T Private Mobile Connection, visit www.att.com/privatemobileconnection or have us contact you.

Share this with your peers

Overview

AT&T Private Mobile Connection can extend an enterprise's existing WAN infrastructure into the mobility network. This extension of the enterprise WAN enables business and government entities to pursue application deployments that include mobile workers, hard to reach locations, and temporary locations. In addition, this service also supports backup application scenarios that ensure true path diversity when a customer's primary wireline application goes down. AT&T Private Mobile Connection offers the reliability, protection, and flexibility that wireless enterprise applications require.

Key features of this solution include:

- Network extension with the ability to leverage an enterprise's existing WAN infrastructure
- Variety of network connectivity options with AT&T VPN services – MPLS or IPSec
- ProxyMobile IP (PMIP) capability that advertises IP addresses behind the wireless router
- Flexible IP addressing options (public, private, dynamic, static, customer or AT&T provided)
- Customizable standards – based security enhancements (private IP, firewall options, access control, traffic isolation)
- Diversity options for enterprise connections and redundancy in AT&T radio and core network elements

Potential Benefits

- No additional costs utilizing existing WAN infrastructure
- Easy to use with flexible connection options
- User satisfaction through support

Supporting Applications in a Wireless Environment

A wide variety of applications, supporting different lines of business, can be supported in the network. Support of enterprise applications are subject to the speeds supported by the air link segment of the AT&T wireless network. Currently, our network supports three airlink network technologies: EDGE, HSPA and LTE

- EDGE – Effectively supports lower bandwidth telemetry applications and provides an alternative to ISDN for backup applications
- HSPA (HSUPA+HSDPA) – Provides even higher uplink speeds, which increases the available bandwidth for traffic sent from a remote site to the host site
- LTE – Provides highest (4G) bandwidth via an industry standard format where available

Applications Currently Supported by AT&T Private Mobile Connection

Given the air link network technologies currently available, a wide variety of enterprise applications can be supported in the network. Examples of the applications currently supported by this service today include:

- Government/Public Safety – Support of first responder applications, such as remote government database access, computer aided dispatch, automated vehicle location (AVL)
- Financial – Support of wireless ATM machines, backup of applications with wireline connectivity
- Utilities – Telemetry applications, remote meter reading
- Transportation/Logistics – Vehicle location and vehicle performance monitoring, package tracking applications
- Manufacturing – Support of Supervisory Control and Data Acquisition (SCADA) applications
- Healthcare – Remote monitoring of patient vital signs, support of patient monitors through maintenance metrics reporting
- Retail – Point of sale and energy management applications

Devices Supported

Wireless access to an enterprise's network can be accomplished via a variety of wireless devices. These include handsets, laptops, tablets (via embedded radio antennas, PC-card, or USB wireless interfaces), wireless routers, embedded devices, and specialty devices.

Although AT&T Private Mobile Connection does not specify which devices an enterprise must use to support their application, the selected device used must be certified to work with the AT&T network. When implementing this solution, we may team with a device manufacturer to provide the required devices. Alternatively, the customer may work with a third-party supplier to obtain the devices.

Architecture

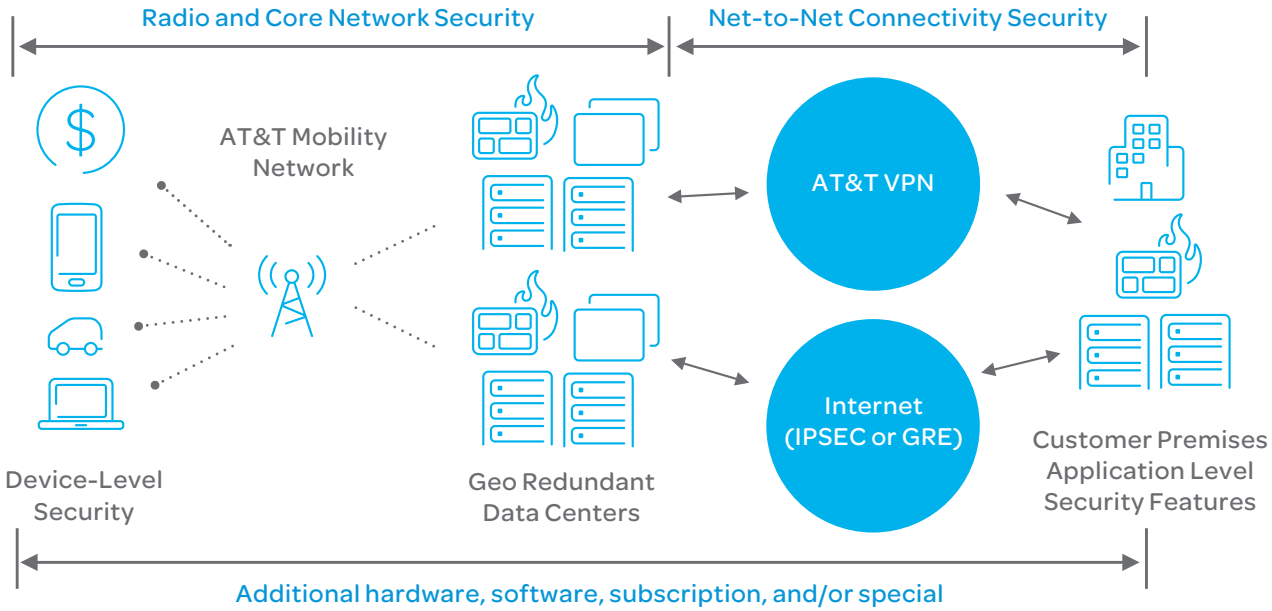
AT&T Private Mobile Connection enables our enterprise customers to connect their Wide Area Network to our wireless network. Network-to-network connectivity options including MPLS-based VPN services, Internet VPN IPSec or GRE tunneling provide enterprises with a private and reliable link between the wired and wireless environments which encompass the enterprise's entire network. The enterprise's wireless traffic is segmented and isolated within the network, aggregated at our National Data Centers (NDCs), and handed off to the enterprise's WAN via a private connection. Figure 1 shows the high level elements associated with implementation, including security features associated with each element.

Security Features

As Figure 1 indicates, AT&T Private Mobile Connection handles security using a layered approach. There is no one silver bullet that will address all security concerns, so it builds on best network management practices that include security features at each segment of the network.

- Device segment – A wide variety of vendors offer device security solutions, and AT&T partners with these vendors to provide the device security solution that best works with the enterprise's application and network deployment
- Radio Access Network – Provides encryption of the enterprise's data traffic that that is exchanged between the device and our mobility network (64 bit encryption on the EDGE network, and 128 bit encryption on the 3G and 4G (LTE) network)

High-Level Architecture



AT&T Private Mobile Connection provides end-to-end security elements for extending your network.

- Core Network segment – Segments the enterprise's mobile data traffic in the core network by using individual Layer 2 tunnels to route the traffic to AT&T's National Data Centers. The traffic is aggregated and further isolated per enterprise at these data centers via the use of individual Layer 2 Virtual LANs (VLANs) and virtual routing and forwarding instances
- Network Data Center segment – Employs fully geo-redundant data centers that will divert wireless traffic to other data centers in the case of a link or data center outage
- Connectivity segment – Supports a variety of private network connection protocols that connect our network to the customer's WAN. AT&T Private Mobile Connection supports AT&T MPLS based VPN services[1], and IPSec and GRE protocols for Public VPN connections, all of which are tailored to keep customer's traffic private and to reduce the risk that exists on unprotected public networks and public gateways
- Customer premises segment – Once the aggregated mobile traffic is handed off to the enterprise's WAN, additional application level security features can be implemented. Please contact your sales representative for our WAN security features and additional security offers

WAN Connectivity Options

- Given that AT&T Private Mobile Connection extends an enterprise's existing Wide Area Network, it can connect the mobility network to the most widely deployed WAN technologies: MPLS, and a variety of network connectivity options (MPLS with AT&T VPN service, Internet VPNs [IPsec or GRE tunnels], or direct Internet access)
- MPLS Based VPN Services – Multi-Protocol Label Switching (MPLS) is currently one of the fastest growing data networking technologies. Its appeal stems from its ability to provide customers a fully meshed network without having to deploy individual virtual connections to each end location. By using distributed IP routers and Virtual Routing and Forwarding (VRF) tables, MPLS enables customers to economically reach all of their locations. AT&T Private Mobile Connection can connect the mobility network to a customer's existing MPLS based VPN network with AT&T VPN service.
- Internet VPN – The increased popularity of Virtual Private Network (VPN) technologies has led to a number of different VPN deployment architectures. However, the unifying theme of VPN deployments is that they can accept IPSec or GRE tunnel connections over the Public Internet. In order to support the variety of IP VPN deployments enterprises have today, AT&T Private Mobile Connection can support a range of standard IPSec or GRE tunnel configurations. IPSec tunneling is a widely used and standards based method of connecting to Internet VPN networks

IP Address Management

AT&T Private Mobile Connection provides for a range of capabilities in the IP address stage. Enterprise applications dictate the type of IP addressing required, and this service has the ability to support all the existing types of IP addressing.

- Static IP Addressing – Allows the enterprise to specify the IP address that will consistently be assigned to each mobile device
- Dynamic IP Addressing – Allows AT&T to assign a different IP address to each individual mobile device each time the device makes a connection to the network

To learn more about AT&T Private Mobile Connection, visit www.att.com/privatemobileconnection or have us contact you.

Share this with your peers

- Private IP Addressing – Per RFC1918, IP addresses not routable on the public internet because they can be used by multiple enterprises; they are used due to limited availability of registered, public IP addresses
- Public IP Addressing – Registered IP addresses routable over the public internet

Professional Services Support

Coordinating logistics to deploy and support wireless communications equipment is highly complex. AT&T makes this process effortless by combining premier equipment solutions and a selection of comprehensive professional services, which include:

- Site Qualification
- Integration Design & Equipment Selection
- Equipment Deployment & Installation
- Network Management & Maintenance Dispatch
- Device Buy-back/Recycling

Customer Care & Technical Support

Enterprise customers risk significant consequences if their applications experience service interruptions. In order to support customers, we have experienced customer care organizations available on a 7 day per week, 24 hour a day basis to provide assistance. Customers with their own help desk can obtain help desk to help desk support, while customers without their own help desk can obtain direct end user support.

Additional Information

For additional, detailed information on AT&T Private Mobile Connection, please contact your AT&T account team.

Notes

1. The AT&T mobility network can interface to AT&T VPN service via standard IP routing 10 Gigabit Ethernet infrastructure connection. The MPLS protocol and its features are supported within those VPN services; the customer will not interface directly with the mobility network using MPLS.

Share this with your peers

For more information contact your AT&T Representative or visit www.att.com/privatemobileconnection.

Scan this code to learn more.

To learn more about AT&T Private Mobile Connection, visit www.att.com/privatemobileconnection or have us contact you.

11/15/16 AB-2725-03