IP VPNs
COME OF AGE

USERS DRIVE NETWORK TRANSFORMATION

The global transition to new-generation Internet Protocol (IP) networks is the latest step in the evolution of corporate networking. These networks eliminate the bandwidth limitations and service impediments of older technologies that restricted business expansion. Telecommunications carriers and their customers are realising the benefits of these new capabilities in the deployment of IP Virtual Private Networks (VPNs).

THE EVOLUTION OF REMOTE NETWORKING

The last two decades have seen a rapid evolution in the technologies businesses use to connect sites and allow remote access from outside the network. But until recently, the products available left many business users unsatisfied.

In the early 1990s, many businesses started using modems and ISDN tie lines to share data and applications across multiple sites. While this allowed basic connectivity, information usually resided in several silos across the business, meaning staff often made decisions based on outdated or incorrect data.

By the late 1990s, these connections had mostly been replaced with technologies such as Frame Relay and Asynchronous Transfer Mode (ATM), which enabled data and applications to be shared between offices and with key partners. However, these links were complicated and slow to provision and required considerable technical expertise to install and maintain.

Early in the new millennium, the growth of email and internet use greatly increased the demand for bandwidth and made IP networks the norm. However, telecommunications carriers still relied on legacy technologies such as ATM for backhaul links.

Sending IP traffic over these hybrid networks was technically demanding, which reduced the flexibility of services carriers could provide. It was also difficult to ensure that the bandwidth necessary to service demanding applications such as Voice over IP (VoIP) and videoconferencing was available.

THE MOVE TO IP VPNS

Over the past five years, many Australian businesses have deployed IP VPNs; in fact, IP VPN has become the standard for Wide Area Network (WAN) deployment. Australian businesses now entrust IP VPNs with sensitive financial and client data as well as new-generation applications such as teleconferencing, videoconferencing and unified messaging, which makes voice, email, video and fax messages available from a single inbox.

But while a VPN can improve overall staff productivity and provide flexibility, managing this infrastructure is still time consuming and distracts information technology staff from more strategic tasks.

The complexity of most telecommunications providers' VPN offerings, including a wide range of features and multiple speed options across access and IP ports, makes it harder for network managers to support business growth and flexibility. VPN technologies such as IP Security (IPSec) require complicated firewalls that are difficult and time consuming to configure, troubleshoot and maintain, and require a high level of expertise. .

With business growth fuelling demand and CFOs increasingly concerned about rising bandwidth costs, IT and network managers are anxious to deploy application awareness across the network rather than just access 'tails'. Real-time applications such as voice and video require strong, reliable service.

IT and network managers are demanding IP VPN solutions that allow them to:

- Obtain comprehensive reporting for network utilisation and application performance and predict network utilisation trends
- Reduce the complexity of provisioning and managing WAN and remote site connections
- Deliver business continuity and disaster recovery capabilities
- Access greater bandwidth at lower cost
- Implement flexible converged solutions that improve productivity
- Prioritise the performance of bandwidth-hungry applications while ensuring the delivery of less critical traffic
- Enable staff to work from home and access corporate IT resources while on the road.

Service providers globally have responded to these demands by building end-to-end IP networks that better serve customers' business needs.

OPTUS EVOLVE™ NETWORK: VPNs MADE EASY

End-to-end IP networks are eradicating many of the problems that plagued hybrid IP networks and predecessors such as Frame Relay and ATM. Telecommunications carriers worldwide are investing heavily in these networks in response to customer demand and Optus is at the forefront of this movement.

Optus has built it's new Optus Evolve™ network and a suite of communications products tailored to the way customers want to do buisness. The Optus Evolve IP VPN service is designed to minimise confusion and maximise ease of management. It is delivered over Ethernet, a technology network administrators are familiar and comfortable with. Customers can choose a variety of access speeds and a range of value-added services. Optus' redesigned cost structures delivers simply, easy-to-understand quotes, bills and service level agreements.

MPLS DELIVERS ADVANCED CAPABILITIES

The enabling technology of the Optus Evolve IP VPN service is multi-protocol label switching (MPLS), which delivers vastly improved class of service (CoS) and quality of service (QoS) capabilities compared to standard IP packet routing.

This moves the complexity away from customers' networks to the service provider's network. MPLS makes it much easier to provision and remove IP VPN connections or change the connection speed. A customer can simply connect its router to a provider edge (PE) router over Ethernet. There is no need for complex and time-consuming WAN routing or high-maintenance IPSec firewall routers.

This is as close as it gets to plug-and-play networking. By reducing complexity and using commodity Ethernet technology, Optus IP VPN delivers a cost-effective wide-area network and remote access solution that frees up IT resources to focus on more important business needs.

WANT MORE?

Optus Evolve IP VPN offers advanced connection capabilities that are easy to deploy and manage. Where required, customers can also use value-added services such as:

- **Secure Socket Layer (SSL)** remote access. Staff can securely access data from inside the network – including email, files and core business systems – from any internet-connected computer using VPN over SSL technology.
- **Managed router service (MRS)** for remote sites where skilled technology staff may not be available, Optus can remotely manage routers and remove the hassles of network administration. Optus' expert staff will proactively monitor the network and provide reports on network traffic and trends to ensure quality for vital applications.