White Paper

QVPN: Quality of Service in Virtual Private IP Networks

Using QoS to Build Corporate WANs on the Internet

Xedia Corporation

By its sheer utility and network simplicity, Virtual Private Networking (VPN) is shaping up to be the killer application for corporate communications on the Internet. Leveraging the ubiquity and low cost of Internet access, VPNs extend secure and private high-performance WAN connectivity to organizations, small offices and individual users anywhere.

Essentially a network outsourcing option, VPNs are logical private networks operating over a shared or public network infrastructure. Frame Relay is a familiar example of VPN services built upon carrier networks. The opportunity now emerging is to build VPNs on the vast network infrastructure of the Internet. Email and web-browsing have gotten the Internet where it is today, but business networking on the global scale of commerce is the prospect that Internet VPNs have in store. Ultimately, like the voice network of today, Internet VPNs will be the global channel of business communications.

With the advantage of easy access at lower cost, Internet VPNs that offer reliability, security, and performance are the evolutionary next-step beyond today's bandwidth-centric Frame Relay and Asynchronous Transfer Mode (ATM) services. The VPN challenge is to achieve a service infrastructure robust and scalable enough to sway business traffic onto the Internet.

Enterprise customers must be utterly convinced that the Internet can be made to perform as they require, and achieving this confidence is the crux of the Internet VPN challenge. This paper describes the network architecture that must come together in order to make VPNs thrive. As a pioneer of bandwidth management and QoS solutions for IP-based wide-area networking, Xedia Corporation has developed VPN technology that scales to meet the requirements of both business users and service providers. Xedia's Access Point QVPN architecture is a second-generation VPN solution that brings together all the elements for business-class networking over the Internet.

Market status

Internet VPNs are now at the early trial stage. Today's implementations mirror Frame Relay's early development back when organizations first deployed frame switching to reduce the cost of their leased-line networks. Then, the economics and improved reliability of public service offerings quickly spurred many users to move from private to public Frame Relay offerings.

Likewise, while customers today build their own VPN solutions on top of generic Internet access, real VPN growth will come as customers begin to outsource key Intranet, Extranet, and other IP service applications to VPN service providers. The major standards and technical requirements are in hand, and ISPs are pouring enormous capital into the Internet: buying hardware, building facilities, laying fiber in the ground and purchasing gigabits of bandwidth capacity on submarine and satellite links around the world.

Money is being spent to make the Internet indispensable to the corporate world. Service providers see IP being adopted and enhanced as *the* standard networking protocol for data, voice and video services. They see major promise in secure Internet communications with standards such as Internet Protocol Security (IPSec). And they see network performance gaining a quantum boost with the Differentiated Services (DiffServ) standard providing a model for end-to-end Quality of Service (QoS) across the Internet.

Key aspects are ready and the infrastructure is being deployed in anticipation of the Internet's business networking role. VPNs are the service offering that will make it happen.

Background: VPNs Before and After

The concept of virtual private networking has been proven in the voice and data worlds for many years. The model is well understood but faces a new challenge as corporations begin to see their network requirements extending beyond traditional branch office connectivity. The networking realm is becoming more dynamic, reaching a shifting audience of business partners, customers and end-users dispersed around the world.

Frame Relay and ATM services support VPNs in which the logical partitioning of network circuits ("virtual circuits") keeps each customer's bandwidth separate in an otherwise shared physical infrastructure. These services are a cost-effective alternative to the fixed private lines of branch office networks, but they lack the flexible connectivity, performance or scale required to build the next generation of global business services .

To the extent that automated, switched virtual circuits (SVCs) or "smart" permanent virtual circuits (PVCs) are not widely available and do not often interwork between different carrier networks, circuits have to be configured and maintained by the service provider. Reaching out to bring distant sites, customers and business partners on line requires multi-carrier coordination and substantial cost.

Frame Relay and ATM will remain important elements of the public network infrastructure, providing the physical (Layer 2) connectivity of large-scale networks. But the accessibility of IP services are the driving force behind Internet VPNs. With Internet VPNs, any number of sites anywhere can be joined by connections across the Internet,

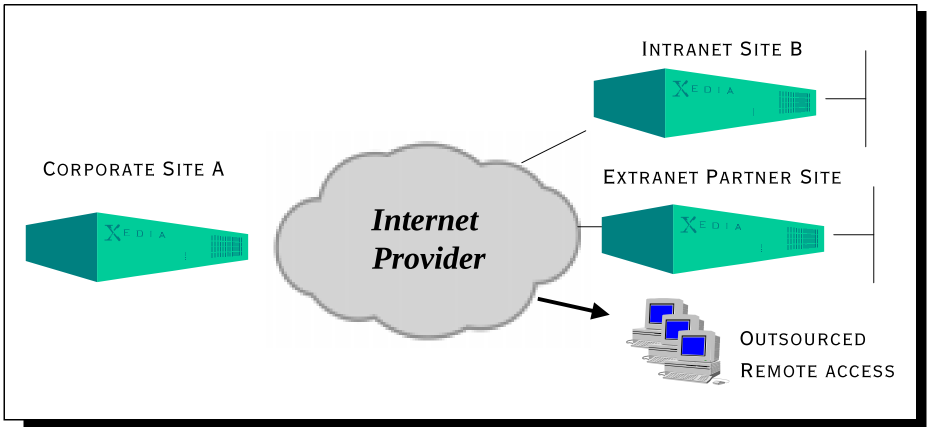


FIGURE 1.
Emerging Internet VPN Services

Internet VPNs allow enterprises to outsource rapidly growing IP services by providing high speed global connectivity at the lowest possible cost.

no matter which ISPs are used. Internet VPNs operate at the higher (IP) network layer and use “encrypted tunnels” to mimic connection-oriented circuits. In terms of service, the concept is the same - an organization can interconnect any of its locations or open the doors to business partners by carving a VPN out of the public network.

Internet VPNs will deliver high-speed, global connectivity at a very fair price. For the cost of Internet access at whatever speed, whether dial-up modem or fractional T-1, T-3 and beyond, Internet VPNs leverage the price advantage that new IP infrastructures have over traditional telecommunications services.

VPN Requirements

Performance. Security. Reliability. These are the fundamental requirements for business communications anywhere, and they are critical to the deployment, growth and success of Internet VPNs.

The Internet backbone has seen great improvement with respect to performance and reliability, as evidenced by the Service Level Agreements (SLAs) announced by major providers. More bandwidth, more advanced network provisioning capabilities, and IETF-driven standards such as DiffServ are enabling the higher, more predictable network performance that allows providers to meet explicit service level commitments to their business customers.

In addition, the IPSec security standards have emerged as an important counterpart to Internet improvements. IPSec is based on a set of protocols and procedures for establishing, managing and terminating secure communication channels (or tunnels) across public IP networks. The IPSec standards define strong authentication and encryption services at the IP network layer, or Layer 3, and will play a dominant role in implementing Internet VPNs.

At the network operations level, platform design and overall system architecture directly impact on the business case for VPN services. The early VPN gateway products are not what service providers look to as the model for large-scale implementation; they are point products that serve an immediate role, and they must grow to fulfill the larger requirements of a business-class networking service.

The following sections describe in more detail the capabilities needed for large-scale VPN deployment. Covering the technologies and specifications now in hand, Xedia’s Access Point QVPN solution is laid out as the model for an overall VPN architecture.

VPN Security

The “private” in virtual private networking is a matter of separating and insulating each customer’s traffic such that other parties can’t access or compromise the confidentiality of data. IPSec tunneling and data encryption achieves this feat by essentially carving private end-to-end pipes or “tunnels” out of the public bandwidth of the Internet and then encrypting the information within those tunnels to protect against someone else stealing the information.

In addition to IPSec, there are two standards for establishing tunnels at Layer 2. These are the Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP), neither of which includes the encryption capabilities of IPSec. The value of IPSec beyond these solutions is that it operates at IP’s Layer 3. It allows for native, end-to-end secure tunneling and, as an IP-layer service, it is also promises to be more scalable than the connection-oriented Layer 2 mechanisms.

IPSec provides a robust architecture for secure wide-area VPN and remote dial-in services. It is fully complementary to any underlying Layer 2 network architecture, and with its addition of security services that can protect a company’s virtual private network, IPSec marks the transition from early tunneling to fully fledged Internet VPN services.

At issue is the fact that different implementations of IPSec will confer varying degrees of security services. Products must be compliant with the latest IPSec drafts, must support high performance encryption, and must scale to VPNs of industrial size. The Access Point QVPN architecture meets these criteria with encrypted throughput up to 90 Mbps for wire speed T3 rate services, and scalability to 4,000 L2TP tunnels.

Rather than handing off to a standalone security server, Access Point QVPN integrates this functionality in its unified IP services architecture. It supports both site-to-site

WAN and remote user dial-up VPN services. Security integration includes support of Internet Key Exchange (IKE), which automatically negotiates security associations among gateway endpoints, and Access Point QVPN is also melded into the Public Key Infrastructure via support for X.509 formatted certifications and interoperability with emerging Certificate Authorities.

Performance - Bringing QoS to VPNs

Security is only one component of the VPN solution. Customers will also demand predictable performance with service levels matching what they've come to expect on their existing networks.

There are two different aspects to the VPN performance requirement. First, users need guaranteed service levels that apply to VPN trunks across the backbone. These bandwidth guarantees mimic private leased lines and must offer performance akin to Frame Relay's Committed Information Rate (CIR) service, for example. The goal is to achieve IP services that can deliver on the same parameters as today's established technologies.

Secondly, customers need control over how their VPN bandwidth is shared and partitioned among their own users and applications. This Quality of Service (QoS) requirement is a bandwidth management and backbone traffic concern that plays out at every network access point.

Xedia's QVPN solution is unique in its ability to manage bandwidth at both VPN performance levels. It ensures bandwidth for the virtual trunks connecting Internet VPN sites, and at the network edge it allocates bandwidth and manages QoS according to business user and application priorities.

Differentiated Services (DiffServ) is the IP backbone specification for establishing QoS from end to end across the public wide area. Access Point QVPN uses DiffServ but further leverages Xedia's industry-leading IP bandwidth management to guarantee service level agreements across an Internet VPN.

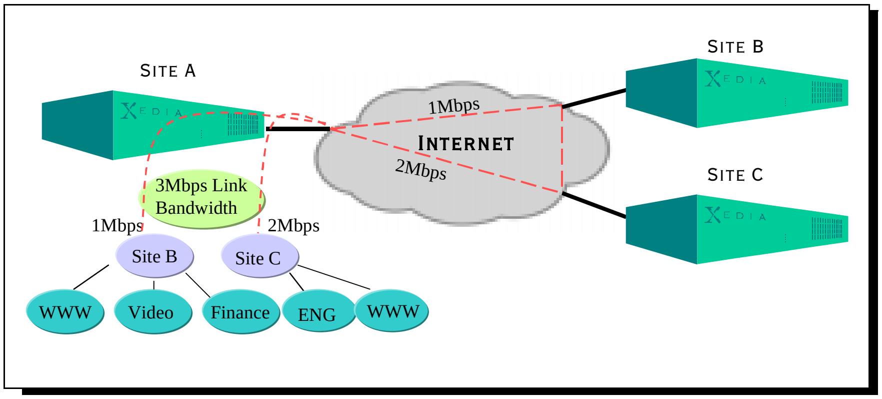
For example, Xedia's QVPN features a bandwidth borrowing capability that allows customer trunks to burst at traffic rates beyond their CIR when idle bandwidth is available on the network. Likewise, different traffic classes within a customer's VPN link may borrow bandwidth from each other as needed. The result is a Layer 3 VPN that achieves the bandwidth efficiencies of statistical multiplexing at Layer 2.

The second, or user-level of QoS is achieved with Xedia's QVPN implementation of Class Based Queuing (CBQ). CBQ is an IP feature that classifies traffic according to very granular network policies. It allows individual applications, subnets, or different groups of users to each receive bandwidth tailored to meet their specific QoS requirements. Bandwidth guarantees and borrowing privileges can be applied to each traffic class in real time, dynamically, by using CBQ.

The combination of DiffServ and CBQ is Xedia's unique approach to delivering bandwidth that will serve Internet VPNs in the most demanding business environments.

FIGURE 2.
Two Points of QoS Control

User applications and flows have the distinct level of service they need as they pass over the virtual private "trunks" connecting different sites.



Reliability and Ease of Management - Routing Integration versus Multibox Complexity

Because VPNs will operate over the Internet, robust and reliable Internet-scaled routing services must be integrated at the access point. The solution must be easily deployed and managed by the provider, and it must scale to meet the needs of a growing base of corporate users and business services.

More than a VPN gateway device, Access Point QVPN is an integrated access router supporting the major IP routing protocols. It provides multi-homing access to the Internet with a robust BGP4 implementation, plus added reliability via support for the Virtual Router Redundancy Protocol (VRRP). These dual protocols allow inherent redundancy across network access links, making Access Point QVPN a mission-critical, scalable router for VPN service.

Such integration is the key to a robust VPN architecture. With the early focus on IPSec encryption alone, first-generation VPN platforms are point-products that address only one piece of the VPN challenge, requiring a host of other platforms to handle routing, security, bandwidth management and other aspects of a business-class service. The multi-box alternative increases management complexity and also reduces reliability by introducing many single points of failure.

The result is that each VPN access point often requires four or more separate networking platforms - a router, VPN gateway, bandwidth manager and security firewall. Each device is a potential point of failure that could bring the entire link down, so for mission-critical WAN deployments, users have to double the hardware count at each site - eight boxes, total - in order to provide backup redundancy.

This multiplicity of platforms is what early adopters have had to deal with, cobbling together a VPN solution from the various parts available. So many separate, discrete boxes not only increase management and reliability concerns, but they also introduce added latency with performance mismatches that typically compromise the performance and scalability of the entire solution.

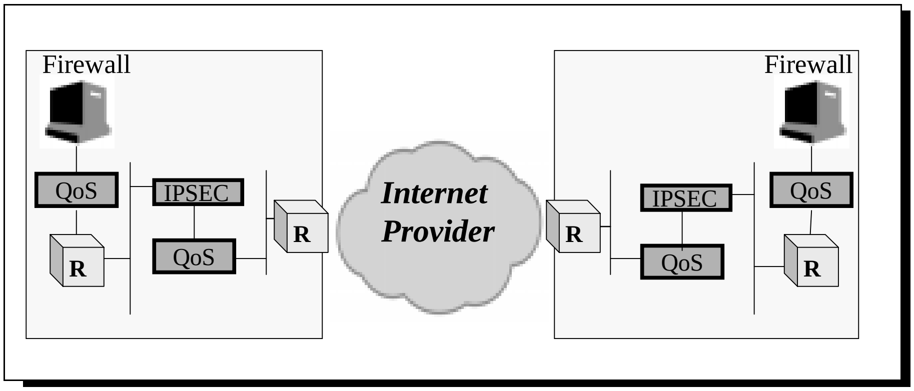


FIGURE 3.
Multiple Boxes are Complex to Configure, Provision and Manage

Many services, such as routing and bandwidth management, are required twice.

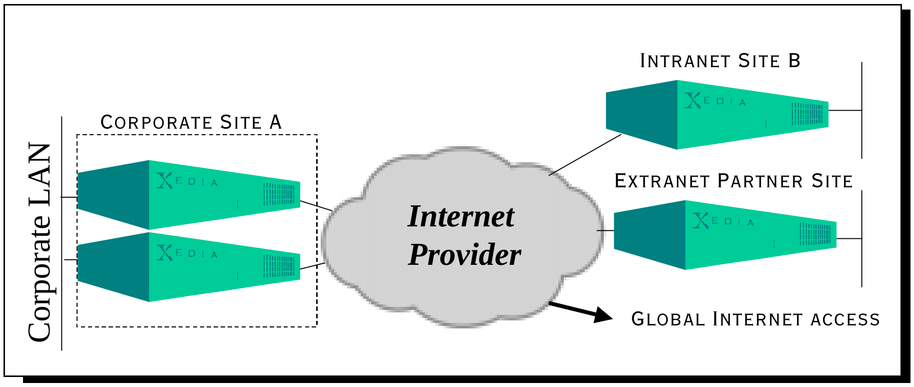


FIGURE 4.
Access Point QVPN -- Simplicity, Scale, High Availability

Xedia's integrated solution simplifies management while providing high availability from any user to any user with secure or clear Internet access.

Access Point QVPN instead integrates these separate platform functions in its design. It is a true second-generation solution that brings the key elements together in an architecture built for large-scale VPNs. The following table illustrates the integrated capabilities of this all-in-one approach:

Access Point QVPN in action

Deployed on an enterprise network or as a service provider's VPN gateway, the Access Point QVPN sits between the LAN and the WAN. It acts as a router and as a VPN gateway establishing tunnels across any wide area backbone: either IP, Frame Relay or ATM. Remote dial-up users can also be supported through tunneling via Internet access - Access Point QVPN applies the same security, CBQ and bandwidth management capabilities to remote user traffic.

Traffic is first classified according to QoS and bandwidth requirements, then encrypted using any of the available industry specifications: DES (data encryption standard), Triple DES, IPSec or L2TP. Access point QVPN also provides local password authentication, and supports RADIUS authentication services.

Network access is controlled by an integrated firewall that filters packets according to their source and destination IP address. This state informed firewall remembers which ports numbers are being used by each network connection and will terminate access to those ports when the connection shuts down.

Network Address Translation (NAT) is supported to ease IP address management and increase network security. NAT substitutes a tunneling address for IP traffic across the WAN; outsiders can't see the topology of a customer's network, and internal users need only one IP address for calls across the VPN.

The integration of dynamic IP routing, QoS, and bandwidth management with the security mechanisms just described is what sets Access Point QVPN apart from other VPN gateway designs. Its scalability to T3/E3 bandwidth and over 4,000 simultaneous network tunnels is an equally key differentiator in the realm of large-scale VPN service requirements.

Conclusion: Fulfilling the VPN wish-list

Access Point QVPN is the industry's most thoroughly integrated Internet VPN solution. It brings together all the necessary components of a scalable, broadband VPN architecture that allows service providers and large enterprise customers to build private backbones on the Internet.

The next evolution of public networking is underway and will give business users the leverage of IP's global reach. A model for what VPN services can achieve, Access Point QVPN delivers the QoS and bandwidth management to match IP's performance against guaranteed services such as Frame Relay. As business traffic on the Internet will demand nothing less, Access Point QVPN is an ideal answer to IP's new service architecture.

TABLE 1. A Carrier Class VPN Services Platform

Access Point QVPN		
Bandwidth QoS	yes	cbq; diff-serv
standards-based security	yes	ipsec (des, 3des), firewall
internet quality ip routing	yes	ospf, bgp4, nat
router redundancy	yes	vrrp
wide area access	yes	frame relay, ppp, atm
management	yes	cli, snmp, web, radius
scalability	yes	10's to 1000's of tunnels
performance	yes	100 mbps; t1, t3, oc3

Xedia Corporation
119 Russell Street
Littleton, MA USA
Tel: 978-952-6000
Fax: 978-952-6066
www.xedia.com