

Moving Into the Cloud: The Case for Network-based VPNs

Table of Contents

Executive Summary	1
Virtual Private Networks Overview	1
CPE-based VPNs	2
Components of the current SP-managed VPN	2
Subscriber Premises Router	2
Application Proxy Firewall.....	3
General purpose, high-performance workstations	3
Encryption.....	3
Key Management	4
Bandwidth Management.....	4
Intrusion Detection	5
Tunnel termination.....	5
The Case for Network-based VPNs	5
The CoSine network-based VPN solution	6
Components of the CoSine solution.....	7
Benefits of the CoSine solution.....	8
Conclusion	8

Executive Summary

The landscape of the network Service Provider (SP) is rapidly changing. As competition increases, customer retention becomes more of a challenge and profitability can suffer. SPs need a cost-effective way to retain and grow their customer base, increase profitability and deliver differentiated services that customers want and are willing to pay for.

Virtual Private Networks (VPNs) give SPs the opportunity to attract subscribers with service offerings that the subscriber will need for years to come. This could be why Frost and Sullivan estimates that revenues from VPN products and services will reach \$18.7 billion by 2004. However, the limitations of first-generation VPN equipment make it difficult for SPs to deploy managed VPN services profitably and to scale delivery to meet increasing demand.

Early VPN implementations consist of multivendor "VPN solutions" that are little more than cobbled-together stand-alone hardware and software elements on the customer premises. This type of VPN becomes more expensive and difficult to manage over time, as new functionality is added to the mix. This Customer Premises Equipment (CPE)-based approach results in products and services that are expensive on a per user basis initially and on a per customer network on an on-going basis. And, because there is no natural synergy or cross-function support across these products, SPs who manage multivendor VPN solutions have little opportunity to reap future revenues from their investment.

As the VPN market begins to move from early adopter to broader acceptance, it has become apparent that a new model of delivering VPN services is required. The most effective way to deliver VPN services is from the SP's Point of Presence (POP) not the customer premises. A SP can effectively create, deploy and manage VPN services that originate from a network-based solution. A network-based VPN still enables the same services as a CPE-based VPN (application proxy firewall, encryption, intrusion detection, tunnel termination, etc) but it integrates them into a single SP-based platform. This enables SPs to support thousands of subscribers simultaneously with customized VPN services.

A network-based VPN platform can offer virtual services that are manageable as an integrated system from the access portion of the network to the very core. This enables SPs to guarantee high performance and Quality of Service (QoS) across the entire network. With a sophisticated customer care system as an integral part of a network-based VPN, SPs can offer their subscribers the ability to view and control their portion of the public IP network, relieving a major IT obstacle to outsourcing today. And, because a network-based VPN platform is designed specifically for a SP's network, it is compatible with existing SP-based equipment and has all the carrier-class features and functionality required for continuous, non-stop performance.

Virtual Private Networks Overview

The number and variety of Virtual Private Networks (VPN) "solutions" touted by vendors today has reached staggering proportions. There are more than 60 different VPN "solutions" on the market today offering products that either were "purpose-built" for VPN deployment or "modified" to accommodate some level of VPN functionality. It is clear that these vendors are simply filling a demand that grows as organizations learn more of the economic and performance benefits that are possible with a VPN.

However, there is still some confusion on what constitutes a VPN and how to implement one. Some VPNs consist solely of a managed application proxy firewall service while others include some combination of application proxy firewall, encryption, intrusion detection, tunneling and key management. Some are completely implemented by the subscriber while others are outsourced to a SP. Most VPN implementations, whether outsourced or "home grown", still require either the SP or the subscriber to string together various pieces of CPE in addition to the generally required router and Digital Service Unit (DSU).

The end result to this piecemeal approach is a VPN that is as costly and as difficult to manage as a private network. Subscribers expect a VPN to provide economic and performance benefits while providing guarantees on reliability, manageability, security and compatibility. SPs are looking for the means to deliver a VPN that is scalable, cost-effective to manage, allows them to guarantee QoS and increases their ROI. There is no way to ensure this mutually beneficial relationship with a piecemeal or CPE-based approach to VPNs. Each piece of equipment that is added to the premises results in a complexity that makes the VPN difficult to manage and maintain.

The alternative to a CPE-based VPN is a network-based solution. This type of VPN solution integrates VPN functionality and applications “into the cloud” for SPs, eliminating the need for premises-based VPN hardware and software. With a network-based solution, VPN functionality is not limited to what CPE vendors are offering today. A network-based implementation can evolve beyond this narrow definition to cater to changing requirements of today’s business subscriber. SPs can use this solution to deliver VPN and other IP services in a scalable, centrally manageable fashion with a high return on investment.

This paper explores the differences between CPE and network-based VPNs and establishes the benefits of a network-based VPN for SPs and subscribers alike.

CPE-based VPNs

CPE-based VPNs, even when outsourced to a SP, require an organization to piece together several pieces of hardware and software both at the headquarters and at the various remote locations. A typical enterprise may have six locations, each with as many as seven pieces of equipment dedicated to securing the network. This problem is compounded when a SP has multiple customers with multiple pieces of equipment. Each customer will have different configuration requirements, preventing SPs from amortizing the cost of a solution across multiple subscribers.

CPE-based VPNs often have many limitations for the SP including:

- High cost to install, implement, manage and maintain – especially on a per office basis
- Reliability: network interruptions when new users /functionalities are added; not non-stop or carrier-class
- No QoS across network components and thus no way to implement and support Service Level Agreements (SLAs)
- Manageability concerns: limited remote manageability, multiple management interfaces to support and a lack of visibility into the entire network
- Lack of scalability: Limited ability to add services or functionality; usually requires forklift upgrade or at least a truck roll to the subscriber’s premises
- Inconsistent monitoring and accounting due to limited visibility
- Compatibility issues: forced to buy vendor-specific routers to have a particular software-based VPN service that have a lack of interoperability

Components of the current SP-managed VPN

When you take a look at all of the pieces of standalone equipment and software that must interoperate, it is easy to see that SP-managed CPE-based VPNs offer limited functionality as well as profitability. Depending on subscriber requirements, a CPE-based VPN requires some combination of the following: subscriber premises router, application proxy firewall, general purpose, high-performance workstation, encryption, key management, bandwidth management, intrusion detection and tunnel termination. In addition, the SP will require some type of OSS/customer care system and access concentration equipment for handling VPN traffic in the cloud.

Subscriber Premises Router

The subscriber premises router continues to exist with any VPN solution, whether it is network-based or CPE-based. With a CPE-based VPN, this router is often the primary vehicle for deploying VPN services. When used as a VPN solution, most premises routers lack the processing power and scalability needed for adding other VPN services and functionality. Even the routers designed and marketed as “VPN solutions” offer limited scalability and become just another box to manage on the premises.

With a network-based VPN, the subscriber’s router does what it was designed to do- it routes packets. VPN services and functionality are deployed from the SP’s POP and can be added easily and cost-effectively without affecting the subscriber’s daily operations. Services can be turned up and billed for immediately without degrading network performance or waiting for a truck to roll. Most CPE access routers today are sold by Cisco Systems, although there are many players in the market offering basic routers at price points ranging from \$500 - \$250,000.

Application Proxy Firewall

An application proxy firewall is a key component of any VPN solution and is offered in many different formats by many different vendors. A firewall is a type of gateway that protects the resources of a private network from users from other networks. Application proxy firewalls typically reside on a general purpose, high-performance workstation that is located behind the router on the customer's premises. Firewalls should be evaluated on their ability to secure data reliably, the quality of the application proxy firewall management tools and performance as well as pricing. Recent *Data Communications* evaluations revealed vulnerabilities in these areas across many of the CPE-based application proxy firewall products. Although results vary depending on the product, researchers at *Data Communications* found that many application proxy firewalls deployed at customer sites were lacking in management capabilities and performance.¹ For example, if there were a problem encountered with the firewall or if an upgrade was required, the SP would be forced to "roll a truck", take down the firewall and disrupt their subscriber's daily operations.

So what does this mean? Simply put, the CPE-based application proxy firewalls can pose many problems for the SP who deploys them to their subscribers. SPs have little control over these devices and some of the inefficiencies can result in constant maintenance issues. In addition, the SP only realizes revenue on the initial installation and on-going management of the application proxy firewall. Maintenance and performance issues can quickly eat away at those profits. In addition, the lack of scalability makes it difficult to quickly and easily deploy new application proxy firewall services.

Data Communications also evaluated the cost of application proxy firewall products from many of the top vendor including the hardware-based options from Cisco and Lucent as well as the software-based alternatives from CheckPoint, Axent/Raptor and Network Associates. *Data Communications* examined products from 20 vendors with prices that ranged from \$3,000 for 25 users to \$25,000 for up to 1,000 users. A SP who wanted to add users would have to pay for additional licenses and would be forced to allocate the personnel to potentially visit the site to install the new application proxy firewall. To ensure non-stop operation, dual systems would have to be deployed or an expensive, after-hours cutover would need to be scheduled.

General purpose, high-performance workstations

General purpose, high-performance workstations are used to run software-based applications like application proxy firewalls and intrusion detection. These workstations are required whether a SP elects to deploy stand-alone applications on the customer's premises or at the SP's POP. These workstations are typically provided by Sun, HP or IBM and range from \$5,000 to over a million dollars for the highly scalable, non-stop systems.

Encryption

IPSec is a recent standard for IP packet authentication as well as IP packet payload encryption. Encryption is the conversion of data into a format that cannot be easily deciphered by unauthorized people. IPSec encryption differs from tunneling in the sense that IPSec permits authentication every packet of data that is passed through the network while tunneling only authenticates the session. Encryption comes in many different formats: packaged with an application proxy firewall or bundled with some other piece of hardware or software that must be added to the network. This gives the SP yet another thing to worry about on the subscriber's network. CPE-based encryption hardware or software is often difficult to manage, maintain and upgrade. Every time a change is made to the software or hardware, a truck must be rolled and the entire network must be brought down to make even the simplest modification.

The major vendors offering encryption products include RedCreek, Checkpoint, VPNet, Cisco, Radguard, Onebox Networks, Shiva, 3Com, Timestep, Bay, Fortress and Indus River. Hardware-based solutions range from \$6550 to \$50,000 for the minimal configuration. There is often a separate charge for the certificate server and key management infrastructure. Software-based alternatives range from \$3995 to \$50,000 depending on the number of clients. Software-based encryption implementations solutions typically offer limited performance.

¹ "Firewalls: Don't Get Burned", *Data Communications Magazine*; March 21, 1997.

Key Management

A Public Key Infrastructure (PKI) is a combination of encryption algorithms, protocols and derived tools that enables secure communication across a variety of applications and platforms. The PKI resolves the fundamental problem of trust on the Internet by providing strong privacy, authentication and data integrity. Deployment and maintenance of a PKI on the subscriber's premises requires a large staff of technically trained experts to build and support the necessary infrastructure.

There are two leading vendors offering key management capabilities: Entrust and Verisign. A recent study by the Giga Information Group compared the two vendors to determine which solution made the most economic sense. Both Entrust and VeriSign were contacted for this report and were allowed to provide customer lists, pricing data, strengths and benefits, considerations, etc. In addition, both were given this report in advance of publication with the opportunity to review for inaccuracies.

The study contends that a PKI is the most critical security investment to make. The Giga Information group analyzed both the Total Economic Impact (TEI) and the Total Cost of Ownership (TCO). TEI measures effectiveness, taking into account the TCO while also evaluating the benefits, flexibility and risk. Table 1 summarizes the TCO of purchasing key management from either vendor.²

Table 1. Analysis of Entrust and VeriSign

Service	Entrust	VeriSign
Basic Certificates for Web Authentication (5,000 per year)	\$669,403	\$821,327
Basic Certificates for Web Authentication (20,000 per year)	\$1,062,538	\$1,729,725
Managing Certificates for Web Authentication (5,000 per year)	\$951,250	\$916,156
Managing Certificates for Web Authentication (20,000 per year)	\$1,953,180	\$1,846,525
Managing PKI Ids for Enterprise Applications (5,000 per year)	\$2,755,825	\$3,791,738
Managing PKI Ids for Enterprise Applications (20,000 per year)	\$7,915,680	\$12,389,110

The bottom line: key management is an important part of any encryption-oriented service but can be a costly investment when purchased as a separate item. A solution that has key management already built in would prevent both the subscriber and the SP from having to make a separate, costly investment. Additionally, If a SP had a solution with integrated key management, they could act as the mediator for third-party certificate authority and potentially generate additional revenue by offering services like cross certification.

Bandwidth Management

Bandwidth management is a key requirement in a VPN as it determines how bandwidth is meted out for specific applications and/or subscribers. Bandwidth management is available as either a hardware-based or a software-based option for the subscriber's premises.

Xedia and Packeteer are some of the common hardware vendors while Checkpoint and Allot Communications offer software-based alternatives. Software-based alternatives require additional hardware that must be daisy-chained together. Neither hardware nor software-based solutions offer any type of SLA support.

² "A Total Economic Impact Analysis of Two PK Vendors: Entrust and VeriSign", the Giga Information Group; September 1998

CPE-based solutions fail to provide the SP with the big picture view of their network. Since these implementations are access-based, there is no idea of how bandwidth is managed on the edge and the core portions of the network. CPE-based bandwidth management solutions vary in cost from \$7,000 to 18,990, depending of the network configuration.

Intrusion Detection

Simply put, intrusion detection software is basically designed to “catch what the application proxy firewall misses”. With a CPE-based VPN, intrusion detection software usually resides on a general purpose, high-performance workstation that is located behind the premises router and firewall. CPE-based intrusion detection software is limited because it is processing-intensive and requires constant software updates. The end result is a solution that degrades performance and requires constant monitoring as well as maintenance.

Axent, Network Associates and ISS are some of the major vendors of intrusion detection software. This software varies in cost from \$1995 to \$245,000 depending on the number of users. For example, some vendors offer 50 licenses for \$3499 while other vendors charge \$49 for a minimum of 5,000 users. These costs are in addition to the cost of purchasing a general purpose, high-performance workstation.

Tunnel termination

IP tunneling is an easy and cost-effective way to provide secure point-to-point “tunnels” through the Internet. Most CPE-based remote access VPNs use PPTP, L2TP, L2F, ATMP or IPSec. The protocol that is used for tunneling largely depends on the vendor offering the tunnel termination service. Currently, there seems to be a convergence on IPSec and L2TP. PPTP is generally available since it ships with Microsoft Windows. L2F and ATMP are proprietary, vendor-specific protocols.

Tunneling protocols must deliver data without degrading performance and compromising security. Most vendors either offer tunnel termination capabilities in stand-alone access routers or they develop specialized tunnel servers or routers that act as servers to aggregate all tunnel connections at the central site to any other destination point in the subscriber’s network.

Vendors that are selling this type of solution include Indus River, Bay and Ascend. These implementations range from \$7,000 to \$75,000 depending on the number of users.

The Case for Network-based VPNs

Piecing together all of the components to implement a CPE-based VPN is costly proposition and a management nightmare. Figure 1 demonstrates how all of these pieces would reside on the subscriber’s premises. With CPE-based VPNs, there are new costs and scalability issues for every new piece of functionality. In addition, there are operational and management issues, no scalability across multiple platform and a lack of “always on” reliability. A SP’s revenue-generating opportunity is limited by the simple fact that purchasing, managing and having to constantly upgrade all of these individual components would limit profits.

Figure 1. A CPE-based VPN

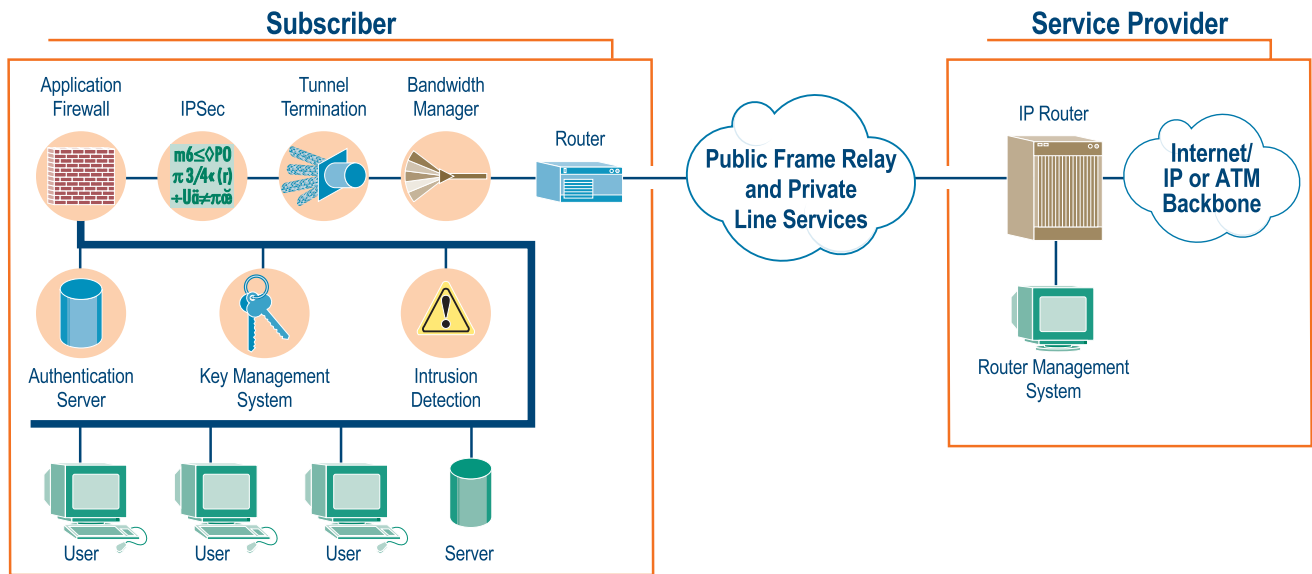


Figure 1. CPE-based VPNs require a SP to “cobble together” several pieces of hardware and software resulting in a VPN that is as costly and difficult to manage.

The time is right is for a new approach: to move VPN functionality “inside the cloud” to create a network-based VPN. A network-based VPN still enables the same services as a CPE-based VPN (application proxy firewall, encryption, intrusion detection, tunnel termination, etc) but it integrates them into a single service-provider based platform. Because all of these services are integrated into one solution, a SP can customize and deploy services immediately according to each subscriber’s requirements. And they can support thousands of subscribers with varying requirements simultaneously.

A network-based VPN platform can offer virtual services that are manageable as an integrated system from the access portion of the network to the very core. This gives the SP the ability to ensure QoS across the entire network. They can confidently deliver on their SLA commitments, monitor performance against these commitments and report on aggregate VPN performance.

With a sophisticated customer care system as an integral part of a network-based VPN, SPs can offer their subscribers the ability to view their portion of the public IP network. And it enables their subscribers to measure their network’s performance against the SP’s commitment.

And, because a network-based VPN platform is designed specifically for a SP’s network, it is compatible with existing POP-based equipment and has all the carrier-class features and functionality required for continuous, non-stop performance.

The CoSine network-based VPN solution

CoSine Communications develops and delivers a network-based IP services delivery platform that enables SPs to quickly and reliably turn up high-performance VPN services to their wholesale and retail subscriber. The CoSine platform consists of three elements:

- The IPSX 9000™: a non-stop high-performance IP services processing switch designed specifically to handle the heavy processing needs of comprehensive VPN functionality
- InVision™: a multi-tiered Services Management System (SMS) that allows SPs to easily deploy, manage and account for VPN services
- InGage™: a premises-based Customer Network Management (CNM) System that gives subscribers VPN visibility and control.

The CoSine solution replaces the multivendor, piecemeal approach of CPE-based VPNs with manageable, centralized support for VPN service delivery. With CPE-based solutions, there are new costs for every new piece of functionality. Each new piece adds operational and management issues as this type of “solution” does not scale across thousands of locations, especially when the system must provide “always on” reliability. CoSine’s solution provides manageable, centralized support for VPN service delivery. The subscriber can use any off-the-shelf CPE router to connect to the SP’s network. And, a SP can support thousands of subscribers VPNs with a single switch. Diagram 2 shows how CoSine Communications solution works in a SP’s network.

Figure 2. The CoSine Network-based VPN

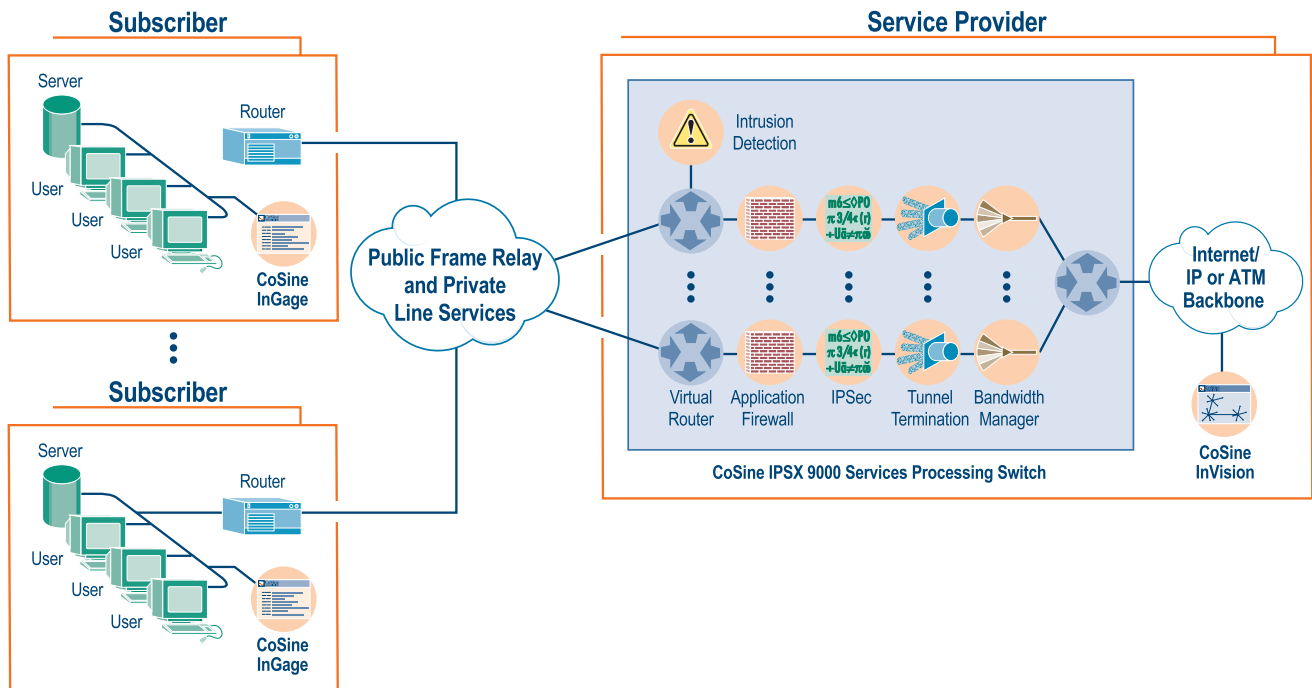


Figure 2. CoSine’s solution integrates all the functionality into a single, SP-based solution, enabling SPs to customize and deploy VPN services according to each subscriber’s requirements.

Components of the CoSine solution

CoSine’s IPSX 9000 is a carrier-class, non-stop services processing switch that integrates a patent-pending Nested Flow Queuing architecture. Nested, prioritized IP flows are enforced for each VPN in the network, for each Virtual Network Connection (VNC) within each VPN and for each VNC Queue within each VNC. The IPSX 9000 IP services suite includes IPSec, L2TP, PPTP, application proxy firewall, key management, tunnel termination, intrusion detection, MPLS, packet filtering, NAT and virtual routing capabilities. These and other IP services may be easily combined to create sophisticated VPNs, each composed of many VNCs. SPs can establish VPNs that are associated with each other in “peering” or hierarchical relationships, providing the freedom to create secure, manageable services which offer high value to the subscriber and high margins to the SP. SPs may confidently offer dynamic Service Level Agreements that are tailored specifically to the end users requirements.

CoSine InVision SMS provides all the tools for provisioning, maintaining and accounting for new VPN services. InVision gives SPs the ability to control service level guarantees in a hierarchical manner to maximize network utilization for both SPs and their subscribers. InVision also has an intuitive graphic user interface for provisioning and maintaining complex IP services. The SP may easily customize VPN configurations and SLA commitments for each subscriber or “cookie-cut” from well-known templates across a number of subscribers and locations.

The SMS provides the SP with comprehensive network management functionality, including fault, performance and security monitoring, Common Object Request Broker Architecture (CORBA) and Telecommunication Management Network (TMN) compliance, as well as detailed accounting statistics for each VNC Queue.

CoSine InGage is a Customer Network Management (CNM) system that enables the SP to reach out and connect to both wholesale and retail subscribers. InGage gives the subscriber a unique view of their VPN, regular updates on network performance compared to SLA commitments and tools to adjust services to meet the rapidly changing needs of the business.

Benefits of the CoSine solution

CoSine's network-based VPN solution provides both the SP and the subscriber with a win-win scenario. For the SP, it shortens their time to market. The IP Service Delivery Platform enables SPs to immediately develop, market and deliver their own custom suite of high-value VPN services. It also allows them to increase ROI. CoSine's solution reduces operational and maintenance costs, enables quicker turn up for immediate billing and reduces the number of technical personnel required to manage each individual component. Additionally, CoSine's modular platform architecture allows SPs to add third-party and CoSine-originated features, technologies and services as subscriber business requirements evolve. This builds customer loyalty and reduces churn.

The subscriber also benefits when a SP chooses a CoSine network-based VPN solution. The subscriber maintain on-site control and visibility of their portion of the public IP network, eliminating the trust issues many have with outsourcing to SPs today. Subscribers also receive non-stop network availability for all mission-critical operations. The IP Service Delivery system is "purpose built" for handling traffic in the most demanding network in the world – the public IP network. It also enables Enterprise IT managers to confidently and securely outsource IP service delivery to Service Providers which enables them to reduce on-site equipment and focus their overburdened network staff on strategic business issues.

Conclusion

Fundamentally, there are significant economies of scale in centralized, managed services. These economies will drive an increasing amount of business towards SP-based solutions over CPE equipment. CPE-based VPNs require expensive, difficult-to-manage devices that must reside on the subscriber's premises. This results in products and services that are expensive on a per user basis initially and on a per customer network on an on-going basis. And, these products offer little opportunity for on-going, value-added services for the SP. Most SPs are only able to derive revenue on the initial sale of the equipment and on the bandwidth used by each service. Since these services typically run over a SP's standard network, the rate of billing does not change appreciably based on the type of traffic. A CoSine, network-based VPN provides:

- Complete flexibility and scalability of managed network service offerings with modular applications and processing resources to support a broad combination of high-performance and managed services.
- Cost-effective managed service support for very high densities of dedicated IP services
- Cost-effective scalability of CPU and memory to support managed services with processing requirements that scale asymmetrically with the amount of access bandwidth.
- Single-point integration of a range of managed service offerings – VPN, application proxy firewall, virtual routing, etc. – that can be easily managed and supported by an SP.

In short, CoSine Communications solution provides a revolutionary approach to VPN deployment that will change the way IP services are delivered today. CoSine will continue to leverage the scalable, open architecture of the network-based IP Service Delivery Platform to enable SPs build out profitable, IP services that will evolve in real time with enterprise business requirements.



The Next Wave in Carrier Services

1200 Bridge Parkway
Redwood City, CA 94065
Phone: 650.637.4777
Toll Free: 877.426.7463
Fax: 650.637.4778
www.cosinecom.com

©1999 CoSine Communications

About CoSine Communications

CoSine Communications, founded in 1997, develops and delivers a new class of managed, network-based IP Service Delivery Platforms "purpose built" for the deployment of high-value IP services such as Virtual Private Networks (VPNs). CoSine's platform provides Business IP Service Providers with the services processing, service management, and customer care capabilities required for offering highly differentiated IP services to subscribers with a high return on investment.

For more information, please find CoSine at www.cosinecom.com or call us at 1-877-4COSINE.

CoSine and the CoSine logo are registered trademarks and all CoSine product names are trademarks of CoSine Communications, Inc. Other brand and product names are trademarks of their respective holders.

051-00001
05/99