THE YANKEE GROUP

THE YANKEE GROUP REPORT

The Evolution of Virtual Private Networks

Executive Summary

For years enterprises have used Internet protocol virtual private networks (IP VPNs) to augment their corporate networks to connect remote users or branch offices. In the year 2000 only about 20% of corporate traffic was carried by IP VPNs, but we expect that number to increase to 46% by 2006 (Exhibit 1). Much of the future growth of IP VPNs will come from enterprises that extend the use of IP VPNs from augmenting their current network to replacing traditional access methods such as frame-relay and ATM services. There is currently a myriad of different types of equipment used to support customer premise based IP VPNs including routers, firewalls and VPN appliances and for companies that decide to build their own IP VPN infrastructure it is critical that they understand the strengths and weaknesses of each platform in order to make the right decision for their business. This report will provide an overview IP VPNs, describe the underlying business value behind a VPN infrastructure and provide a look into the infrastructure requirements needed to build a next generation network.

Exhibit 1.
Data Traffic Mix for North American Multinational Corporations
Source: the Yankee Group, 2002

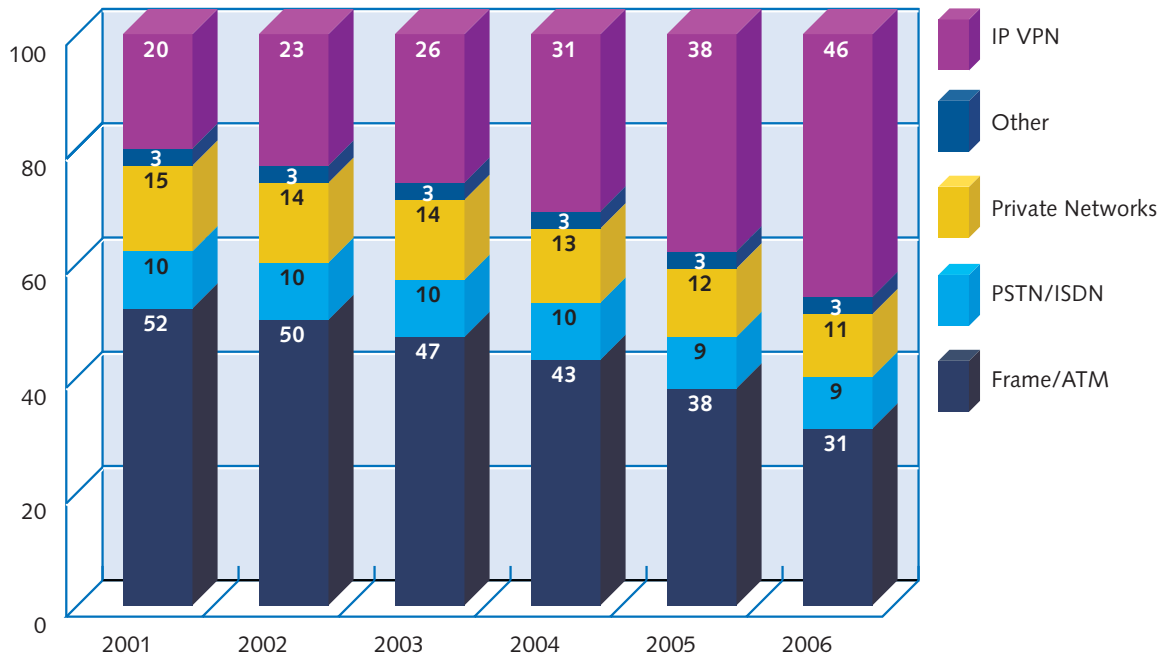
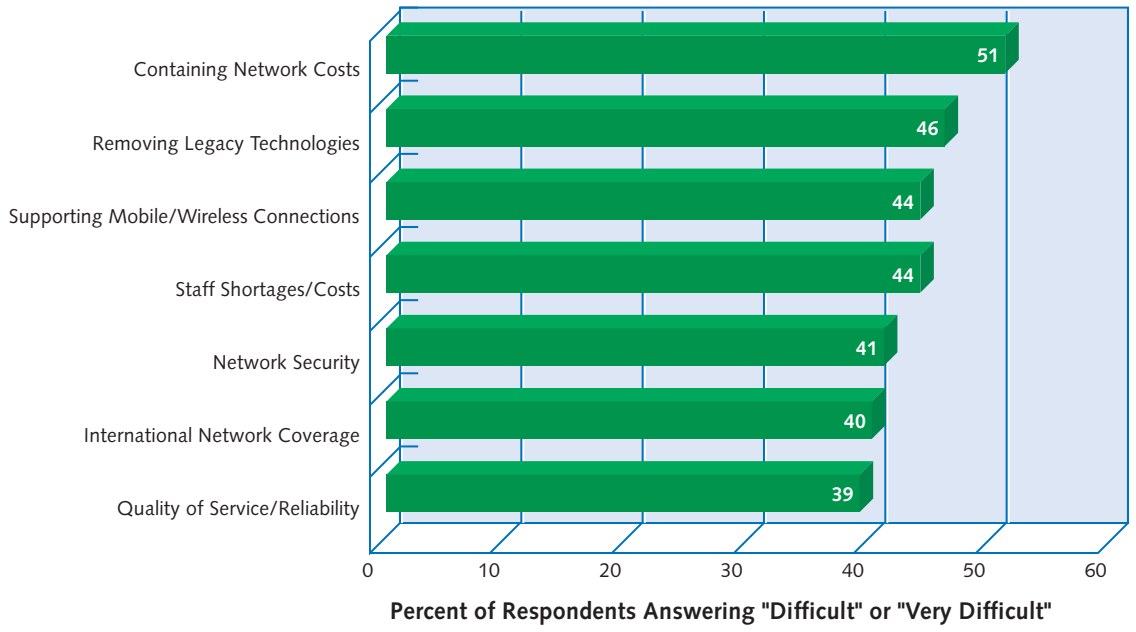


Table of Contents

I. Introduction

Every CIO is faced with the challenge of doing more with less. This means increasing user productivity, delivering new applications but also somehow, removing costs from the delivery of these applications and end user tools. Exhibit 2 shows that controlling network costs ranks #1 among current day challenges for today's IT executive. However, the entire mandate for the current day CIO differs from years past. The CIO today is much more part of the business team and is required to think about business first and technology second. This shift will continue over the next five years there are other business drivers that are driving the requirement for a new type of infrastructure. In addition to "doing more with less" the IT executive will be faced with the following trends:

Exhibit 2.
Problems Organizations Face Running Their Networks
Source: the Yankee Group, 2002



- **Globalization.** This is a concern for all companies, even local ones. As networks extend to extranet partners and remote workers, network managers need to start thinking of how to extend their network globally, but the cost cannot be cost prohibitive.

- **Increased use of remote access and telecommuting.** Telecommuting is at an all time high and corporations need to provide the infrastructure that can scale in size to accommodate the growing number of remote workers. This has typically been provided from a central location for ease of management.

- **Enhanced security.** By moving to a more open environment where extranet and remote access can be provisioned quickly, we also move to a less secure environment. The network architects need to ensure that security is not compromised for the sake of open access.

- **More efficient use of network resources.** The traditional hub and spoke environment that is currently used by most corporations is very inefficient since all corporate traffic is backhauled through a central location. Next generation networks need to be architected differently to make better use of network resources.

The above challenges clearly point to a different kind of infrastructure than the traditional wide area network choices available today. But what kind of infrastructure can deliver openness, security, and reliability and still be dynamic? The answer is IP VPNs.

II. Defining IP VPNs

There are currently a multitude of definitions to the term VPN. In its truest definition, VPNs provide for the access of information or network resources of a private network from a shared or public medium. This can include dial-up, broadband access with a PC-based VPN client, secure tunneling across the Internet and secure web access. Though the Yankee Group recognizes the value and popularity of each of these types of VPNs we will classify IP VPNs as virtual connections between dedicated sites over the public Internet or over a private network.

The Traditional Wide Area Network

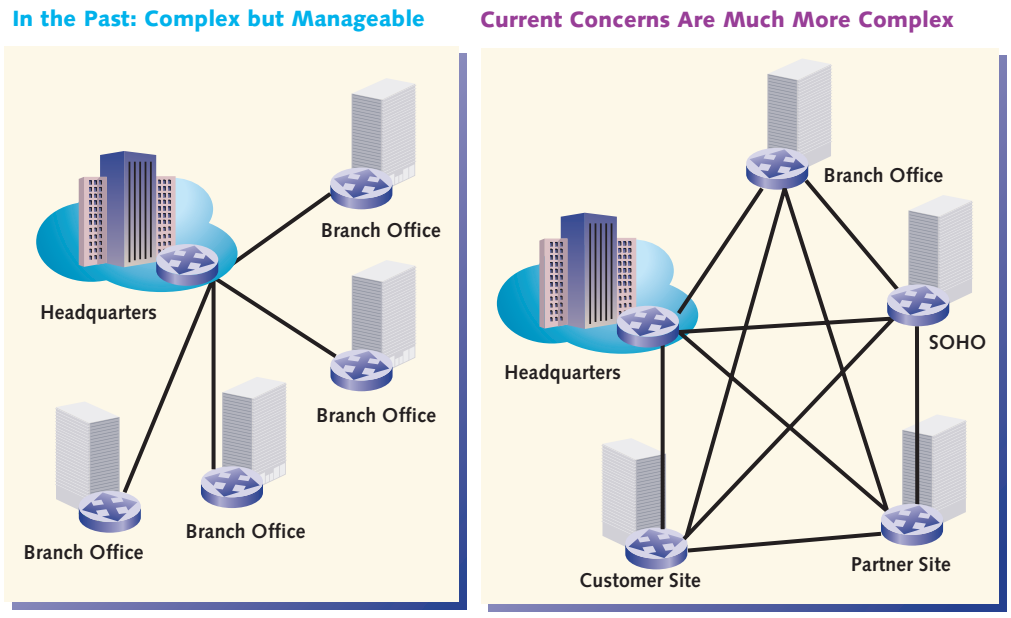
The majority of older WANs are complex but still simple enough to manage. Previously, networks did not have a high degree of meshing and were built on older technology platforms such as frame relay or ATM. This type of configuration is sufficient for yesterday's network needs but as our infrastructure becomes more complex, an advanced technology will be required (Exhibit 3).

This type of infrastructure has been widely deployed, is very popular today and has the following strengths:

- Predictable and dedicated bandwidth

- Secure

Exhibit 3.
Past Network Requirements
Source: the Yankee Group, 2002



- Known technology
- Reliable

However, the business environment has changed over the past five years and the traditional hub and spoke WAN design is facing the following challenges:

- **Adding new sites can be slow and difficult.** In a meshed environment when adding a site the network manager needs to call the service provider and request that the site be added to the network. The service provider then must configure a new permanent virtual circuit (PVC) at every location that needs a direct connection to this location. This process requires coordination between the enterprise and the service provider and can be very time consuming.
- **Meshing is costly.** In the above example, there is a charge for every PVC in the network. The higher the degree of meshing, the higher the overall cost of the network.
- **Off-net connectivity with remote users and extranet partners is expensive and difficult to manage.**
- **Adding IP services is costly.** Because each service is provisioned by adding another device, additional services are expensive. In addition, the multiple devices in the network are difficult to manage.
- **International connections can be very expensive.**

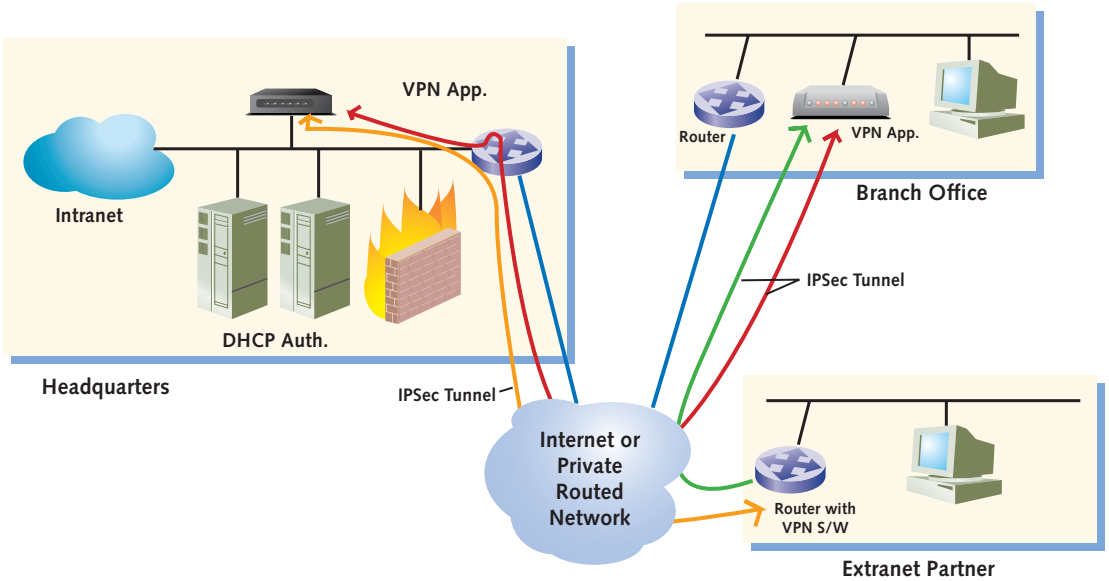
For enterprises that stay with traditional network methods, the problem becomes how to support new applications, extranet partners and network features in a way that is scalable and cost effective. Historically, this has not been a problem since most networks were closed to the corporation but companies need to start thinking more strategically about how their infrastructure affects their ability to do business. As networks evolve scalability, security and manageability will become much bigger concerns and traditional router centric networks will not meet these needs.

How CPE-Based IP VPNs Work

IP VPNs provisioned from the customer premise uses access devices (Exhibit 4) to initiate and maintain a 'tunnel' to the other end-point. The equipment used to support this type of connection can be a router with VPN capabilities, firewalls or VPN appliances. The devices can be configured with various tunneling protocols to create the virtual routes but the most common type of protocol is an IPSec encrypted GRE tunnel. GRE is needed in order to allow IPSec tunnels to dynamically route. This extra encapsulation does serve its purpose but adds extra overhead. GRE was an excellent work around in the early days of IP VPN deployments but as IP VPNs grow, GRE will have their scale and performance problems.

IP VPNs built from the customer premise have the advantage of having security applied from end-to-end, including the local loop. By having the traffic be based on IP, the corporation has the flexibility to add or remove tunnels dynamically, rather than needing the service provider to configure permanent virtual circuits (PVCs) within the network. This allows the enterprise to have the flexibility of a fully meshed network without having to pay for the numerous PVCs needed in frame-relay or ATM environments. This would allow the enterprise to bring up tunnels for video calls, overnight backups, file transfers, etc. and then take them down when not needed.

Exhibit 4.
CPE-Based IP VPN
Source: the Yankee Group, 2002



In addition to providing simple, cost effective meshing, IP VPNs also carry the following benefits:

- **Ubiquitous reach.** The growth of the Internet created a seamless network that can reach anywhere in the world. By using the Internet as the primary backbone, companies can create virtual connections as long as they have an Internet connection.

- **Secure connections.** This was mentioned earlier, but since the traffic is encrypted end to end, the communications are very secure. In fact, because the traffic is encrypted, it provides a higher level of security than traditional networking.

- **Quality of service.** If a common carrier is used for all the sites or a managed service is purchased, the service provider can provide SLAs around quality that is equal to or better than what may be offered over typical frame relay and ATM networks.

- **Lower cost.** This has been the main driver for IP VPNs. By using the Internet for transport, companies can save upwards of 50% on telecom charges for international connections. Domestically companies can still save money, depending on the degree of meshing.

- **Efficient use of bandwidth.** This is one of the big benefits of IP VPN. Each office can have a local connection to the Internet as well as a secure tunnel to the branch location. This significantly cuts down on wide area network traffic and enterprises can reduce or eliminate the need for dedicated Internet circuits at the headquarter location.

Choices, Choices: the Equipment Behind IP VPNs

By architecting the network to provide localized Internet access, it does require local security to be installed into every branch and there are various ways of solving this problem. Each solution is listed below:

- Branch router running encryption and firewall software features. Since the router terminates the T1 connection, it seems logical to have it perform VPN functions as well as firewall functionality. This is sufficient for small sites but as the number of VPN tunnels grows and firewall features are added, router performance degrades. Also, traditional routers are designed for clear text routing making security more of an add on or afterthought rather than be integrated into it.

- Firewalls with VPN software can also be used, but these can be very expensive and will still require a separate router to handle all of the routing functionality. Many security professionals do not like to use firewalls for VPN functionality as it compromises the firewall. In addition, firewalls generally do not make very good routers and many of them require routes to be configured statically limiting their effectiveness as a router to very small companies.

- Dedicated VPN appliances can be used to provide the IP VPN functionality. By best practices this is typically the most scalable way to deploy a large scale VPN infrastructure. The only downside is that there needs to be a router for the routing functions and a firewall for the perimeter security. Having this many devices in every branch location creates a management problem.

The lack of a true multi-service platform has forced most enterprises into deploying separate devices for each function. This is very expensive from an operational standpoint as well as capital expenditure perspective (Exhibit 5).

The best solution would be a product that is purpose built to be a security product, VPN appliance and router all in one. The requirements for such a product would be:

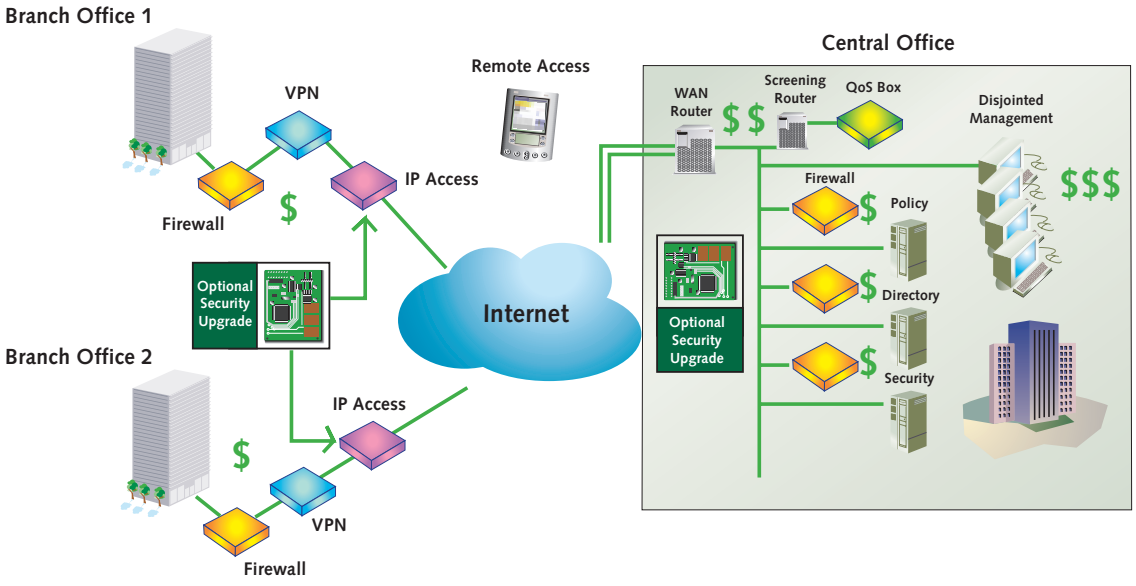
- **Provide full featured routing functionality.** This includes the ability to not only provide advanced routing functionality such as support for network addressing, NAT services, RIP and OSPF as well as being able to terminate the physical WAN interfaces such as T1, frame-relay and dial services within an IPSec branch office VPN tunneling construct.

- **Stateful firewall functionality.** The product needs to offer full firewall functionality including robust rule support, authentication and management support beyond simple packet (ACL) based filtering.

- **High performance and scale.** The product needs to be able to apply all these critical IP services simultaneously without any impact to performance while also allowing the network to scale.

Exhibit 5.
TCO Concerns of Current Deployments

Source: the Yankee Group, 2002



Multiple Platforms, Vendors and Service Costs

- **Cost conscious.** Router based platforms can provide additional functionality but costly add on hardware accelerators are required. This cost of any next generation product must help control capital and operational expenses for any enterprise looking to deploy IP VPNs for the corporate backbone.

As more and more enterprise move to deploy Virtual Private Networks, it becomes critical to address the performance, scalability and dynamic requirements of these networks in the same dynamic manner that traditional "clear text" IP routed networks have benefited from in the past.

Most of the recently deployed enterprise branch VPN networks have been constrained by static branch configurations along with complex overlay protocols and administration that have limited the size and scale of these networks. These early designs have been typified by bolted on IPSec encryption to existing multi-protocol routers or access control (firewall devices) with no real integration between dynamic routing and VPN/security.

III. The Evolution of VPN Solutions

The technology that VPNs are built on has not changed much in the past 10 years. It is true that the hardware platforms have been improved and scale better than products built just a few years ago, but the underlying technical framework is still the same.

The flexibility that IP and the ubiquitous Internet provide is a result of the openness and standardization of IP. This has allowed enterprise customers to share information with anyone, anywhere across the public Internet; however, it does require security beyond the levels currently being offered with current technology.

Current enterprise routers cannot provide security with routing without complex configuration and performance overhead. Because IPSec does not explicitly define how to dynamically route within an IPSec tunnel, some vendors have implemented generic routing encapsulation (GRE) as a work around to a deliver dynamic IP routing of VPNs.

This, of course, affects performance and adds configuration complexity. The performance issues can be addressed with additional hardware encryption cards but this adds additional cost to the overall solution.

Enter Nortel Secure Routing Technology (SRT)

Secure Routing Technology (SRT) is a Nortel Networks secure architectural framework that addresses the dynamic routing and scaling requirements of deploying large scale secure Virtual Private Networks.

SRT on Contivity is an example of this "security in the DNA" design philosophy, applied to a purpose-built Secure IP Services Gateway. SRT provides a highly secure platform that truly integrates dynamic IP routing, VPN services along with critical access control, policy and authentication security services to provide enterprises with extreme levels of scalability and performance, and overall security integrity when building large scale IP Virtual Private Networks.

SRT is comprised of four integrated secure pillars: secure policy, secure access, secure routing, and secure management framework which are described below.

Secure Policy

Secure Policy is a design construct where tightly integrated services share and apply a common security policy. This policy follows the user (or branch locations) from service to service, as opposed to each service maintaining a separate policy for each connection. In this sense, firewall rules can be set against VPN tunnels, encryption strengths can be set based on source/destination, QoS can be applied based on port of entry, and all the above is configured and monitored from one interface. The security administrator can then begin to treat end-users or partners or locations as whole entities, establishing all their rights, levels of access and related security requirements all at once.

Secure Access

Contivity offers access agnostic flexibility in applying any of the above secure policies to virtually any access type into the platform.

Individual users and branch locations can connect to Contivity over a routed VPN tunnel and/or non-tunneled (clear text) connection, through a physical connection (Ethernet, V.35 PPP/Frame or dial interface), a wireless connection (802.11 or WWAN PDA) or over virtual IP interface connection.

Any of the centrally provisioned IP services can be applied in any combination to any of the access connection methods that an enterprise customer may need to leverage.

Secure Routing

SRT enables dynamic routing over IPSec tunnels without the need for GRE. Many of the current VPN enabled platforms either require a separate encrypted tunnel for route updates or only allow static routes over tunnels forcing manual configuration. Conforming to the IPSec standard, SRT on Contivity defines a "virtual IP interface" that is mapped to the IPSec tunnel making the tunnel appear simply as another routing path to RIP or OSPF. This approach avoids manual configuration and additional tunnel processing and packet overhead offering much higher levels of scalability than traditional router centric solutions.

Secure Management Framework

SRT provides a secure management framework on which all the IP services are based. Nortel has tried to secure all interfaces to eliminate any "back doors" that might compromise the device. Contivity provides inherent Denial of Service (DOS) protection and remote management is only possible via strong encryption (IPSec), with no SNMP access over the public interface, which is a common security flaw of other products. Full Stateful Firewall inspection and strong user authentication (PKI) services are provided, with integrated security logging.

SRT on Contivity Product Challenges

Nortel Networks has developed a product with security in mind to support an era when IP VPNs will be used as the dominant network connectivity method. However, the product will need to overcome the following challenges:

- **Slow IP VPN deployments.** Despite its promise, IP VPN deployments have been slow to move past the state where it is anything more than an augmentation to the current network. Part of the problem is that in order for an IP VPN to be most effective, the network must be architected differently. Many companies have not had the time or desire to go through this redesign but the need to "do more with less" will help stimulate adoption.

- **Limited support.** While Nortel has followed industry standards when designing the platform, Nortel is the only vendor currently supporting SRT. An all SRT network can provide advanced services with a low TCO, but in a mixed environment its features are limited.

- **Single point of failure.** By combining all the functions into one platform the product is a single point of failure. If the product is unavailable for any reason, there is no product at the edge that can act as a backup. This is one of the tradeoffs for the lower TCO.

- **Security concerns.** In general, security best practices rarely advocate combining security functions into a single platform. By having each feature located in a separate platform it is very simple to design an infrastructure with security layers so if one device is compromised the internal network is not. This, of course, has management and TCO concerns but will be an issue for security conscious professionals.

SRT Summary

Contivity Secure IP Services Gateways with SRT are a new class of products designed to implement security features and dynamic routing in a single platform. Security is integrated into the network and a cap is put on traditional routers that treat security more as an overlay rather than part of the fabric of the network. SRT on Contivity will allow companies to take that next step toward building reliable and scalable IP VPN networks.

The Business Case Behind Contivity with SRT

The business case for Contivity with SRT is multi-faceted. The business case addresses operational and capital concerns as well as the security concerns that face all CIOs today. Enterprises considering the build out of next generation IP VPN branch networks can benefit from SRT on Contivity in the following ways:

- **Lower total cost of ownership.** Contivity is a purpose built IP services appliance that offers VPN features, stateful firewalling, wide area networking and routing as well as quality of service (QoS) and LDAP features. These services are fully integrated into the platform and can be "turned on" with license activation. This means that all of the enterprise edge features can be delivered in one scalable platform versus individual products for each feature or expensive add-on cards that create downtime when they are installed.

- **Lower operation costs.** Since all of the features are consolidated into a single platform operational costs are significantly reduced. Multiple devices require much more operational support since each one must be administered independently. This can be very time consuming when applying new policies, making configuration changes or applying new versions of software.

- **Investment protection.** Contivity can be deployed behind an existing IP access device. The routing functionality can remain on the existing router until such a time when the legacy router needs to be replaced. The (routing/WAN/security) functionality can then be transitioned to the Contivity platform.

IV. SRT Case Study: Criminal History Information Network (CHIN) IP VPN Deployment

The following case study is based on an actual state government law enforcement network transitioning from frame relay to an IP VPN network built on Contivity. The case study illustrates the business value that SRT delivered to the customer.

The Criminal History Information Network (CHIN) currently operates a 50 site frame relay network connecting large state law enforcement branch locations. Although the current network is operationally adequate for the limited number of branch locations it currently connects together, several new state and federal informational access and security mandates have been put in place that will require a drastic change to the current size, scope and overall capability of the network.

The first major requirement that CHIN needs to address is tremendous growth in the size and reach of its network. New legislation requires that CHIN allow ubiquitous "open access" to extend wide reaching access to the information in its criminal history database beyond its primary 50 branch sites locations to over 500 plus new state & local law enforcement, municipal, port authority, State DMVs and newly established Home Land security offices.

Several new (graphic intensive) applications (criminal and licensing imaging) are also coming online that will require a substantial WAN bandwidth speed increase (currently frame PVC's at 56K) in the 384K–512K range and up to T-1 speeds.

In addition to the new physical branch locations that need access, the CHIN will also need to provide remote access for 400 plus gun dealers for access to new applications that document and streamline the mandatory weapon registration and associated individual background checks.

Finally, in accordance with the newly established FBI data communications regulations, the network itself must provide security in the form of data confidentiality, data integrity, strong user authentication and access control in adherence to federal security best practices.

Extend the Frame Relay Network or Move to an Internet (IP)-Based Model?

The first decision that CHIN needed to make was whether to continue with its current frame relay network or move to an IP based alternative. For some sites it clearly made sense to continue with the current service based on marginal price/performance gains in moving to IP. For many other sites, however, it was decided that scaling the frame network to the higher WAN speeds that where required (384K–Full T1) would prove to be far too cost prohibitive (Exhibit 6). The IP based alternative provided on average 40% less cost per site while exceeding the higher WAN speed requirement.

The IP based alternative also provided a nice fit for supporting both the remote access requirement as well as many of the new applications. Furthermore, 70% of the new locations that needed to access the CHIN already had Internet access. Rather than waiting weeks or months to get a frame PVC provisioned to a new site, the new location could be up and running within days by leveraging the Internet access connection.

Based on these compelling circumstances it was decided that the network would be based on IP moving forward and any frame sites would begin the transitions to IP as it made sense.

Security Requirements

Throughout its decision-making process, a primary concern for CHIN was the ability to meet the new federal security mandate. After consulting with both internal and external security experts, it was decided that the network would use IPSec as the primary method of ensuring data confidentiality, integrity, and non-repudiation, by leveraging IPSec data encryption, authentication, and secure hashing functions.

CHIN would build a "closed" encrypted VPN tunnel network on top of an "open" IP-access network. They would deploy IP-access gateways with integrated IPSec/routing.

Exhibit 6
Frame Relay vs. IP Access Pricing (Business Class DSL)
Source: the Yankee Group, 2002

Frame Relay vs. Internet Access (Business DSL) Pricing

Location/Site	Frame Site	IP Network	IP Advantage
Site A (small) bandwidth	56-64 Kbps	56-64 Kbps	No Speed Advantage
Monthly cost	$150 per month	$75 per month	$75 in savings
Site B (medium) bandwidth	128 Kbps	384 Kbps	+256 Kbps in speed
Monthly cost	$280 per month	$190 per month	$90 in savings
Site C (large) bandwidth	384 Kbps	512 Kbps	+128 Kbps in speed
Monthly cost	$875 per month	$350 per month	$525 in savings

To address the network access-control requirement, CHIN decided that stateful packet inspection firewalling would need to be deployed at all branch locations. This would strictly limit access to the network to authorized personnel and prevent "backdoor" access through any site with an ISP (Internet) connection for which CHIN didn't have control. For the 400-plus remote users who required access to the network (via dialup, DSL, ISDN), CHIN would need to provide a secure IPSec client to allow these users to be authenticated and gain secure access to the network.

Retrofit the Legacy or Deploy Next Generation?

After a close examination of their existing installed base of legacy IP routers, the CHIN quickly realized that many of their older legacy routers couldn't be upgraded to support IPSec 3DES at all. Some of the newly deployed routers that could be upgraded to support 3DES in software could not scale to the new security requirements at speeds of 256K and beyond. These routers would need hardware encryption cards or be replaced.

In examining if they should retrofit their current installed base of IP routers to provide security, the CHIN was faced with two very costly options, neither of which seemed attractive: Upgrade their existing legacy router infrastructure to support VPN functions or deploy a very costly new VPN + router bundle. Exhibit 7 details the hardware costs for both of these options. *(Service calls and network downtime not included in upgrade costs.)*

The CHIN determined that upgrading and/or replacing the legacy branch routers would prove to be far too costly. Also, since the legacy routers do not support any meaningful firewall, a second and third device would need to be deployed at the branch level, driving the costs of this solution up further.

After some initial VPN branch office testing at the central location there was also additional concern that the router centric device would be challenged to meet the VPN performance and scaling requirements. The router-based solution would need at least 5 large VPN class boxes to terminate the required 500 plus sites ultimately adding even more cost and complexity to the overall VPN network design.

Exhibit 7
Hardware Costs for the New CHIN Network
Source: the Yankee Group, 2002

Legacy Router VPN Upgrade/Replacement Costs

Installed Router	Software Upgrade	Hardware Upgrade	Total VPN Upgrade Price	New VPN Router Bundle
50%+ of the existing installed base	None	None	Swap-out for new router required for 3DES	Not available, must replace with an option listed below:
Small router	$1,495	$1,000	$1,295-$2,495	$2,895
Small/mid range	$2,000	$2,250	$4,250	$6,000+
Mid/large range	$3,700	$2,500-$3,500	$6,200-$7,200	$8,500+

Lastly, security consultants were concerned over the inherent insecurity of an open IP router based solution that from a design perspective was not architected to address security in a holistic manner. “Bolting on” this type of security solution was not in line with the agency’s “best practices” security policy.

After careful examination of the requirements the CHIN determined that it needed a multi-service device that could provide IP access in addition to IP security services, such as VPN and firewall, in a cost effective, integrated platform.

Evaluating the Contivity SRT Solution

The CHIN was introduced to the Contivity solution by another state agency that had similar requirements and success with its deployment. Since the Contivity platform met or exceeded all of the VPN, security and routing requirements, the CHIN decided to evaluate the Contivity solution.

Because CHIN wanted to run the firewall, VPN and routing services on the same platform, extensive testing was done to validate the capabilities of the Contivity platform. The results showed that the purpose-built Contivity maintained its performance while running all the services where the traditional router’s performance was degraded while running multiple services simultaneously. The other test that the CHIN performed was at the central location. The results showed that the Contivity platform could maintain its high level of performance while terminating all 500 of the branch VPN connections under real world VPN branch office stress testing. The alternate solution would have required at least five legacy routers to meet the same scaling requirements, adding to overall complexity and capital costs.

Comparing Costs at the Branches

CHIN compared the overall costs of either upgrading or deploying a new VPN router bundle to that of deploying a Contivity Secure IP Services Gateway. This comparison was done across the CHIN sites, from small sites that only needed DSL type access to the medium and large sites that needed support for V.35, PPP and Frame Relay along with support for OSPF and high performance VPN and stateful firewall.

Exhibit 8 shows that the Contivity solution was 15% to 37% less expensive than upgrading or deploying new routers and VPN devices. The Contivity capital savings increased to 21%–53% when stateful firewall was added to the branch requirement by simply enabling the firewall feature on the Contivity gateway versus having to deploy a second low-end stand alone firewall at each branch location along with the legacy router.

Summary

After careful evaluation, the CHIN ultimately determined that the Contivity solution exceeded all of their strict network requirements and was ultimately less expensive than retro-fitting their installed legacy routers from both a CAPEX and ongoing OPEX perspective.

After extensive testing of multiple solutions, the CHIN chose the Contivity platform since it met their large scale and high performance VPN branch routing, firewall, and remote access requirements as well as exceeding their strict security mandate.

Exhibit 8
Legacy Router Upgrade/Replacement vs. Contivity
Source: the Yankee Group, 2002

Legacy Router (Upgrade or New VPN Bundle) vs. Contivity Cost Comparison

Installed Legacy Branch Routers	VPN Upgrade Cost	New VPN Bundle Cost	Contivity Solution	Contivity Savings
Small Branch Site *Behind a DSL Modem*	N/A	$1,295	$999	**22%**
Small Branch Site *Including V.35 I/O Card*	$2,495	$2,895	$1,795	**28% to 37%**
Medium Branch Site *Including V.35 I/O Card*	$4,250	$5,395	$3,595	**15% to 33%**
Medium/Large Branch Site *Including V.35 I/O Card*	$6,500	$8,500	$5,300	**18% to 37%**

V. Conclusion

As enterprises continue to open up their networks and deploy peer-to-peer applications such as IP telephony, video conferencing and other productivity enhancing applications, the requirements for the network infrastructure will change.

Current day network technologies such as frame relay and ATM will not be sufficient to deliver future requirements such as the ubiquitous reach, dynamic capabilities for scalability and real time addition of new locations, enhanced security and quality of service. IP VPNs can provide all of these features and will be the preferred network of the future. However, most corporations will find it risky to quickly migrate to an all IP VPN network so transition and migration strategies will be key aspects to the deployment of future networks.

For corporations looking to deploy an IP VPN we make the following recommendations:

- **Understand what you are buying.** There are many products on the market that offer VPN support but they differ in scalability and features. Make sure the products purchased meet the corporate security and scalability standards.

- **Security should not be an afterthought.** Weave security into the fabric of the infrastructure rather than have it bolted on. This will ensure the same maturity levels of security are in effect in all parts of the network.

- **Avoid complexity.** Complexity of the infrastructure will quickly drive up operational and capital costs. Companies should look to reduce the complexity of their infrastructure wherever possible. The edge of the network is typically one of the areas with the most complexity. Products that can combine multiple functions, but still provide the needed scalability and reliability can help reduce the complexity.

- **Leverage what you have.** Do not replace technology or infrastructure components unless it makes sense. As an example, it may make more sense to not remove the legacy access router if it means disrupting the business. Look for solutions that can be deployed with the legacy platform but can also be transitioned into a bigger role when needed.

- **Calculate your ROI.** In order to fully understand the value that IP VPN can deliver to the business, it will be important to calculate the return on investment. This should include metrics such as capital costs, operation savings and improvements to productivity.

- **Architect the network differently.** For corporations who deploy an IP VPN network but architect it the same way as their frame relay or ATM networks, full value will not be realized. Companies should look for ways to deliver better efficiencies to the network by changing the architecture of the network. An example of this would be to deliver Internet access locally to each branch rather than backhauling Internet traffic through a centralized hub. Ensure the platforms deployed can support the high degree of meshing that may be required to support the new architectures.

Yankee Group Planning Services

Application Infrastructure & Software Platforms
Australasian Market Strategies
Billing & Payment Application Strategies
Brazil Market Strategies
Broadband Access Technologies
Business Applications & Commerce
Canadian Market Strategies
Communications Network Infrastructure
Consumer Technologies & Services
Convergent Communications Asia-Pacific
Convergent Communications Europe
Convergent Communications Latin America
Customer Relationship Management Strategies
Enterprise Computing & Networking
Global Regulatory Strategies
Internet Business Strategies
Japan Market Strategies
Media & Entertainment Strategies
Networked Business Strategies Asia-Pacific
Networked Business Strategies Europe
Networked Business Strategies Latin America
Security Solutions & Services
Small & Medium Business Technologies
Technology Management Strategies
Telecom Software Strategies
Telecommunications Strategies
Wholesale Communications Services
Wireless/Mobile Asia-Pacific
Wireless/Mobile Enterprise & Commerce
Wireless/Mobile Europe
Wireless/Mobile Latin America
Wireless/Mobile Services
Wireless/Mobile Technologies

CORPORATE HEADQUARTERS
31 St. James Avenue, **BOSTON, MASSACHUSETTS** 02116-4114
T 617-956-5000 F 617-956-5005
info@yankeegroup.com

NORTH AMERICA
28030 Dorothy Drive, Suite 203, **AGOURA HILLS, CALIFORNIA** 91301-2682
T 818-706-8318 F 818-706-8505

951 Mariner's Island Boulevard, Suite 260, **SAN MATEO, CALIFORNIA** 94404 T 650-356-1960 F 650-356-1966

1111 Brickell Avenue, 11th Floor, Office 1109, **MIAMI, FLORIDA** 33131-3101 T 305-913-2372 F 617-303-3733

400 Galleria Parkway, Suite 1500, **ATLANTA, GEORGIA** 30339
T 678-385-5990 F 617-368-9524

9 Barrow Street, **NEW YORK, NEW YORK** 10014
T 646-414-7816 F 617-303-3769

5455 Rings Road, Suite 100, **DUBLIN, OHIO** 43017
T 614-789-1642 F 617-368-9511

5700 West Plano Parkway, Suite 1000, **PLANO, TEXAS** 75093
T 972-381-2765 F 617-210-0083

2804 South Ives Street, Suite 100, **ARLINGTON, VIRGINIA** 22202
T 703-683-5444 F 617-368-9518

6135 Seaview Avenue NW, #2F, **SEATTLE, WASHINGTON** 98107
T 206-706-6586 F 617-303-3723

320 March Road, Suite 400B, **KANATA, ONTARIO, CANADA** K2K 2E3 T 613-591-0087 F 613-591-0035
canadainfo@yankeegroup.com

ASIA-PACIFIC
Regional Headquarters
10/F City Plaza Three, Taikoo Shing, **HONG KONG**
T 852 2843 6483 F 852 2568 3340
asiainfo@yankeegroup.com

Level 14, 309 Kent Street, **SYDNEY** NSW 2001, **AUSTRALIA**
T 61 2 9279 0990 F 61 2 9279 0995

Itochu Enex Bldg., 6F 1-24-12 Meguro, Meguro-Ku, **TOKYO** 153-8655 **JAPAN** T 81 3 5740 8081 F 81 3 5436 5057

EUROPE, MIDDLE EAST, AFRICA
Regional Headquarters
55 Russell Square, **LONDON** WC1B 4HP, **UNITED KINGDOM**
T 44 20 7307 1050 F 44 20 7323 3747
euroinfo@yankeegroup.com

c/o ORT, 12, Villa de Lourcine, 1624, rue Cabanis, 75014, **PARIS, FRANCE**
T 00 33 14589 2871 F 00 33 14589 1597

c/o Reuters AG, Hanauer Landstrasse 207, D-60314, **FRANKFURT, GERMANY** T 49 69 7565 3268 F 49 69 7565 3283

Levinstein Tower, 19th Floor, 23 Begin Road, **TEL AVIV** 66182, **ISRAEL** T 972 3 566 6686 F 972 3 566 6630

P.O. Box 7360, 2701 AJ Zoetermeer, **THE NETHERLANDS**
T 31 79 368 1000 F 31 79 368 1001

ul. Zolnierska 25, 40-697, **KATOWICE, POLAND**
T 48 32 202 2778 F 48 32 202 2778

c/o Reuters, Juan Bravo, 3C, Plt. 7, 28006, **MADRID, SPAIN**
T 34 91 585 82 96 F 34 91 435 38 08

LATIN AMERICA
Regional Headquarters
Alameda Santos, 234, 7º andar, 01418-000, **SÃO PAULO, SP, BRASIL** T 55 11 3145 3855 F 55 11 3145 3892
info@yankeegroup.com.br

Carrera 7, No. 71-21, Torre B, Oficina 1003, **BOGOTA, COLOMBIA** T 571 317 4880 F 571 317 4858

Blvd. Manuel Avila Camacho 36, Piso No. 19, Torre Esmeralda II, **MEXICO DF, MEXICO** 11000
T 52 55 5282 7086 F 52 55 5282 7171

For More Information . . .

Phone: (617) 956-5000, Fax: (617) 956-5005. E-mail: *info@yankeegroup.com.* Web site: *www.yankeegroup.com.*

ACCURATE • RELIABLE • TRUSTED