

WHITE PAPER

Addressing the Challenges of Secure Branch Office Connectivity

Sponsored by: GoRemote

Keith Waryas

Mark Winther

May 2004

EXECUTIVE SUMMARY

In an age when "always available, always connected" has become the standard expectation in business, giving employees the ability to access applications and real-time information can be critical to a company's survival. Although some business applications are inevitably client based, many of the core business process applications, such as CRM, sales force automation, and email, are network-based utilities. Additionally, in business environments where collaboration and information sharing are critical, it often makes the most sense to leverage the corporate network as an electronic repository of information and resources. In both of these cases, providing real-time access to the most current information can be critical to employee productivity and, frequently, to the satisfaction of the enterprise's customers.

Over the past several years, we've witnessed a remarkable rise in the number of remote and mobile workers, which has made the modern enterprise an increasingly distributed work environment. This can present a tremendous challenge to IT administrators, who are faced with the often contradictory tasks of enabling remote employees to be as productive as non-remote workers, while keeping the company's network and information completely secure from the threats posed by hackers, data thieves, and viruses.

In an era when IT budgets and personal are being constantly squeezed, it is clear that distributed enterprises need remote solutions that can help them effectively manage the cost and support burdens associated with branch office connectivity. Although transport is an issue, it is only a single part of the equation. IT departments need complete solutions that include the remote security, policy and remediation engines, network and usage monitoring, and support services that can allow their company to keep branch office personnel as productive as possible, control the security exposure of the corporate network, and minimize the support demands on IT staff. They also need partners that can match their own geographic footprint to provide consistent network services across the entire distributed enterprise, which will allow them to fully leverage buying power, provide consistent levels of performance, and offer a single point of contact for problem resolution.

One such offering is the Branch Office Solution (BOS) provided by GoRemote. Since GoRemote operates under a network aggregation model, it is able to provide its customers with a single source for economical broadband services across all of their branch offices. But, unlike many carrier-provided offerings, GoRemote's solution integrates connectivity with robust, yet flexible security, powerful policy and

management capabilities, and centralized network and security monitoring to create a complete soup-to-nuts solution for branch office enablement. Additionally, since all components can be offered as a hosted service, enterprise customers can avoid much of the upfront and recurring costs associated with the infrastructure hardware, software, maintenance, and management, which allow these customers to realize attractive returns over traditional self-managed solutions.

INTRODUCTION

The Challenge of Branch Office Connectivity

When corporate users are inside the company firewall, the issues related to access (e.g., security, application access, and support) are easily understood and controllable. However, modern enterprises are becoming increasingly distributed. Since today's business climate creates the expectation that employees are always connected and always available, access issues can become a significant challenge for both the enterprise's technology professionals and its finance department.

As with employees at the corporate headquarters, employees seated in branch offices need the ability to connect to key applications that are central to business process. While some of these applications are inevitably client based, many core business process applications, such as CRM, sales force automation, and email, are network-based utilities. Additionally, in business environments where collaboration and information sharing are critical, it often makes the most sense to leverage the corporate network as an electronic repository of information and resources. In both of these cases, providing real-time access to the most current information can be critical to employee productivity and, frequently, the satisfaction of that enterprise's customers.

The distributed enterprise can also increase the burden of IT support and the costs associated with that support. In any branch office environment, users are far more likely to operate with less IT department supervision and regulation, meaning that technical and other user issues will occur at a greater rate and will increase per-user support costs to multiples of the costs found in headquarters/central offices. In unconnected or batch-connected branch office environments, this problem is exacerbated by the inability of a centrally located IT department to perform remote diagnostic and repair, establish and enforce security policies, and maintain the most up-to-date versions of critical software (e.g., antivirus) on client devices.

The Cost of Connectivity and the Performance Trade-Off

Historically, larger connected branch offices have been serviced by regulated telecom services, such as frame relay and ISDN, with small to mid-sized branch locations typically being relegated to dial-up service because the number of users did not justify the upgrade costs to frame relay or ISDN.

Today, with the increased availability of DSL and cable access, businesses have more choices in enabling branch offices to connect at high speed with lower price points. This means that there isn't nearly as much of a trade off between price and

performance as in the past. In fact, since these access technologies can offer higher throughput speeds than frame relay, companies might even find better performance for less money. However, DSL and cable are not available from all providers to all locations, so enterprises with a large number of branch offices still face the challenge of trying to create consistency with and realizing the price benefits of volume purchasing across geographies.

Security

Security is always at the top of mind for IT administrators. They face the daunting task of insulating the corporate network, which often contains information that is the lifeblood of the organization, from the myriad of threats posed by viruses, hackers, and data thieves. At the same time, they must keep the network fully accessible to outside-the-firewall employees, who need to remain as productive as possible. In an era when technology budgets seem to be tightening almost as fast as security threats are expanding, it is clear that IT administrators require solutions that can help consolidate their outside-the-firewall access tools and create management efficiencies that control capital and overhead costs, without sacrificing performance or accessibility.

Manageability in a Distributed Enterprise Environment

With any IT initiative, manageability is key. Put simply, to maximize network performance and return, the IT department must be able to fully manage the end points, the traffic, and the manner in which corporate IT resources are accessed and utilized. In a distributed enterprise environment, where a branch office may be 500 or 5,000 miles away, this can be an extremely difficult task. IT managers must have the resources to make certain that rogue elements are minimized or eliminated and the tools to ensure that problems and issues that arise don't threaten the integrity of the network, its data, or the overall IT cost structures.

Consistency and Predictability Across Geographies

Consistency can be a major factor in network planning, design, and build because the boundaries of utilization and performance will often dictate the specific elements needed to make electronic resources available. In a closed or single provider environment, this is relatively easy because the variables are fairly predictable. However, in an enterprise that is distributed across a large area, this can be quite difficult.

In connecting branches, businesses will often find that the technology they used to connect an office in one area is not available for a different branch. They may find that a provider selected in one region doesn't offer service in the other regions where branch offices are located. These companies are also likely to find that the security, guaranteed levels of service, and general capabilities of these fragmented providers just don't match up.

The GoRemote Branch Office Solution

GoRemote, a company which specializes in providing managed remote access solutions to distributed enterprises, is able to address many of the branch office

connectivity challenges through its Branch Office Solution (BOS). BOS represents only a portion of GoRemote's total distributed enterprise solution offering. However, the branch office offering shares many of the best-of-breed solution components that have made its other components (e.g., Mobile Office) successful.

A Network Aggregation Model

One of the core strengths shared across offerings is the GoRemote network aggregation business model, which gives the company the ability to offer services at much lower costs than direct suppliers. Using more than 150 broadband suppliers in the United States and Canada, GoRemote is able to aggregate these supplier networks to offer its customers a virtually unified footprint that includes DSL and cable services. The company is also expanding its broadband coverage in Europe, offering additional opportunities for multinational companies looking to unify their branch office connections across continents.

The value of this network aggregation manifests itself in two important ways. First, since GoRemote manages the offering, it provides the customer with a consistency and predictability of access across the geography, which customers simply would not be able to match using multiple suppliers and buying directly from the carrier. Second, for companies that are looking to connect more than 100 branch offices using cable or DSL access, it is extremely difficult, if not impossible, to interconnect these branches using only a few suppliers. Put simply, using multiple suppliers has a very negative impact on a company's buying power and its ability to drive down costs. This loss of buying power is only amplified as the number of branch offices increases across geography.

Security, Policy, and Service Management

Another common set of threads that runs across the GoRemote offerings is its security capabilities, including policy selection and enforcement, and service management. With any IT solution, and with distributed connectivity solutions in particular, security is always top of mind. While securing the network and clients can be very expensive, especially if approached in a disjointed fashion, the cost implications of shortcomings in this area can be staggering, from both an IT and a business operations perspective. However, GoRemote's unique approach to this issue offers customer companies some compelling opportunities that can help to control expense while offering a high level of security using best-of-breed components.

Total Security Protection

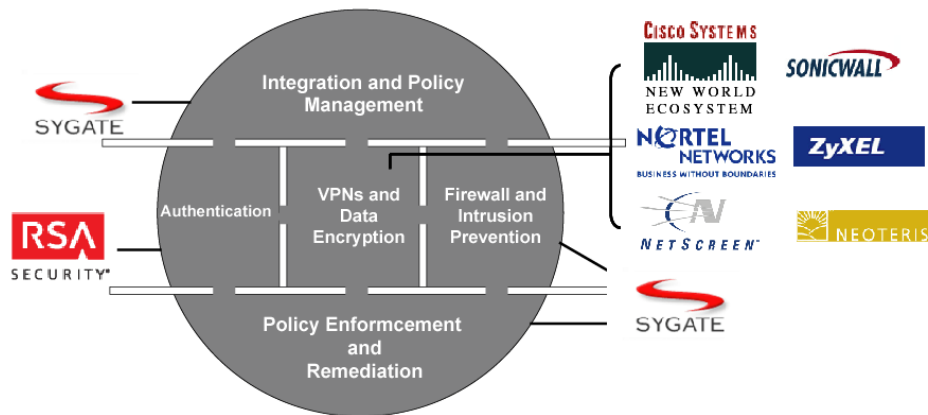
The GoRemote Total Security Protection (TSP) service is designed to meet businesses' complete end-to-end security needs for remote access (e.g., mobile worker/mobile office connectivity, branch/remote office access, and remote telecommuter connectivity) while providing a maximum level of flexibility and control with regards to policy selection, policy enforcement and remediation, and security components (e.g., legacy components and equipment). Because network and client-side point components, policy, and management features are fully integrated with one another and act/react in real time, IT professionals are able to proactively define, enforce, change, and monitor security practices and policies. This allows them to

maintain the integrity of the network and its security far more effectively than with individually deployed, nonintegrated point products. Additionally, because the solution can be deployed as a "security overlay," occupying little or no space on the enterprise IT infrastructure, companies may realize savings in capital expense, as well as maintenance costs, especially in an environment that includes remote offices and mobile users.

Rather than developing the individual point products that make up the solution, GoRemote's Total Security Protection service maintains flexibility by leveraging best-of-breed security components provided by leading component vendors. Added value comes from GoRemote's ability to fully integrate each of these point products to create a unified, seamless security solution that can address security needs, eliminate security gaps, and minimize upfront and recurring investments. This approach has the additional benefit of allowing customers to leverage existing or legacy security point products they may already have deployed on the network, without losing any of the functionality, integrity, or ease-of-use associated with the completely outsourced solution (see Figure 1).

FIGURE 1

Components of GoRemote's Total Security Protection Service



Source: IDC, 2004

TSP also includes managed VPN service as part of the branch office solution. Often considered a "must have" for any remote connection, a VPN offers full end-to-end data encryption between the client (branch office) and the corporate datacenter to ensure that even if traffic is intercepted, the contents remain secure. GoRemote's VPN service has the benefit of being fully managed, and it is monitored on a 24 x 7 basis by the GoRemote Security Operations Center (SOC). This monitoring helps to ensure optimal configuration to minimize network vulnerability and the threat of attack.

Universal Remote Control

As mentioned previously, one of the most important aspects of any IT initiative is manageability. But, when dealing with remote access, it is important to understand that real-time management and control can be an extremely strong contributor to the

overall security, value, integrity, and cost of the remote access security solution. This is where the GoRemote Universal Remote Control fits into the equation.

Although many remote solutions provide reports on past activity, the GoRemote Universal Remote Control allows the monitoring of network activity in real time. This provides administrators with a number of benefits, including:

- ☒ The ability to view traffic trends and generate traffic reports in real time
- ☒ The capability to review bills online and to monitor bandwidth utilization, giving the administrator the opportunity to upgrade to a higher bandwidth service, if needed
- ☒ The ability to initiate and monitor customer care requests online, including opening tickets, viewing ticket status, and gauging completion rates and response times

On the administration side, the Universal Remote Control also gives IT professionals the ability to submit orders for new branches, view the status of existing orders, view existing case status, and submit new cases for action. IT professionals can also review real-time and historical network reports, check performance against monthly SLAs, and view their invoices. These features can be a major productivity benefit for administrators because they ensure that the administrators get the most value and service from their branch office spending.

Service Level Agreements

From a customer's perspective, service level agreements (SLAs) can be critical to ensure the consistency and quality of any network-based service offering. These agreements form the contractual bounds under which the service provider is expected to perform and detail the penalties and remediation should the service provider fail to meet those guidelines. Essentially, the SLA acts as a measurable guarantee to the customer that the service it is purchasing will be delivered in a manner consistent with what was promised.

The GoRemote Branch Office solution measures and reports the provider's performance across nine areas that are key to the performance and quality of branch office services:

- ☒ **End-to-end availability:** This is a measure of the network uptime (the percentage of time the connection between the branch office and headquarters is available). Availability is managed around the clock and reported on a monthly basis. GoRemote promises 98.9% and 99.9% availability, depending on the site pairs, including broadband and VPN.
- ☒ **End-to-end latency:** This is a measure of application response time over the GoRemote managed network, where the roundtrip (HQ to branch office) transmission latency (delay) is managed around the clock and reported on a monthly basis. The GoRemote SLA offers less than 135ms latency for each site pair.

- ☒ **End-to-end delivery:** This measures the number/percentage of packets that are successfully delivered between the branch office and headquarters. These statistics are measured around the clock and reported on a monthly basis. Greater than 99.5% delivery is promised for each site pair covered under the GoRemote SLA.
- ☒ **Firewall vulnerabilities:** To maintain network security, branch office firewalls are tested weekly for open TCP or UDP ports. Vulnerabilities and trouble cases are reported immediately as found.
- ☒ **Tunnel usage:** This measures the VPN tunnel utilization and performance between the branch office and headquarters. These statistics are measured around the clock and reported on a monthly basis.
- ☒ **Call summary:** Dealing with a provider's customer service system can often be a major time burden for an IT administrator and can have important consequences for service uptime. To minimize this, GoRemote includes a number of guarantees on the performance of its customer service in the call summary section of the SLA. First, it guarantees that the average hold time will be less than two minutes and that the average time to call the customer back will be less than 30 minutes. Additionally, GoRemote also guarantees that its 24 x 7 customer care center will maintain the mean time to problem resolution to less than four hours.
- ☒ **Portal uptime:** Defined as the percentage of total hours in a month that the branch office portal is available to the customer. Greater than 95% availability is guaranteed by GoRemote.
- ☒ **Days to install service:** When initiating service at multiple branches, the time-to-install can be critical, especially if a delay means branch office downtime and lost productivity. GoRemote reports to its customer both the time to completion of installation, as well as the status and expected completion of installations in progress. The GoRemote SLA provides that installation and changes to standard broadband will be completed in less than 33 business days; DS1 will be completed in less than 60 business days, while DS3 will be completed in less than 75 business days.
- ☒ **Percentage of proactive cases:** This measures the number of trouble tickets and time to resolution for network/customer issues — such as excessive packet latency, VPN tunnel failures, low packet delivery, and dial backup conditions — detected proactively by GoRemote. This is an essential metric since, according to GoRemote, only about 2% of the total tickets are opened by the customer, while the remaining tickets are generated proactively by the GoRemote network monitoring center. In the SLA, more than 90% of all trouble cases detected are guaranteed to be initiated by GoRemote.

Although a very small portion of the total trouble tickets generated by branch office solution customers are actually user generated, GoRemote maintains a 24 x 7 technical support service that handles both the network issues discovered proactively, as well as any issues discovered by customers.

Consolidated Billing

As mentioned previously, working with multiple providers to enable branch offices across a geography can have a negative impact on a company's ability to leverage scale to drive down costs. However, the multiple provider approach can also generate "soft costs," which, while not as easy to measure, still exist. One example is the administrative costs and issues associated with multiple service bills and payment.

Since GoRemote aggregates networks to provide single-source, uniform service, these soft costs can be easily avoided. Customers receive one bill for service, regardless of how many branches are in operation, and have a single company to work with in the event of discrepancies or problems.

Total Remote Solution Opportunities

With the growth in mobile workers, as well as the always on, always connected expectations that are driving teleworkers and day extenders, the distributed enterprise connectivity concerns clearly extend well beyond the branch office. However, many of the tools and capabilities that address the concerns, sensitivities, and issues of branch office enablement can also be fully leveraged if a company wishes to extend its distributed enterprise tools to include mobile and teleworkers.

As mentioned previously, GoRemote leverages many core components of its business across distributed enterprise service offerings. This means that businesses that use GoRemote Branch Office solutions can leverage the same aggregated networks, TSP, and universal remote control tools to extend connectivity across all types of users in their distributed enterprise environment.

CHALLENGES/OPPORTUNITIES

The challenges companies face in connecting branches of their distributed enterprise are numerous. Operationally, companies face the headaches of having to deal with the fragmented footprints that are inherent when dealing directly with a plethora of broadband providers and technologies, most of whom offer little in the way of SLAs to ensure consistent network performance. However, dealing with multiple providers can also have measurable impact on the cost of provisioning and the bottom line of the company.

With IT budgets that have tightened considerably over the last four years, many IT departments have little in the way of resources to deal with solution design, increased end-user support, and support and maintenance of individually deployed security-point products. Add to this the resources necessary to manage deployment installations, VPN and remote site firewall, as well as proactive network monitoring and problem identification, and the task goes from difficult to daunting.

However, these companies also face an important opportunity if they are able to view their branch office, and indeed their total remote needs, holistically. By leveraging products, such as GoRemote's Branch Office solution to connect distributed offices using DSL and cable, these businesses have the opportunity to realize up to a 60% cost savings over traditional frame relay solutions, with up to a 5x increase in throughput. They can also leverage site-to-site managed VPNs that can help secure

their enterprise data. But, perhaps most important, they can enhance their distributed network performance to support more applications and improve the overall productivity of remote sites, having a positive impact on the organization's bottom line.

CONCLUSION

IT administration in a distributed enterprise can be difficult and expensive. The classic model of contracting with multiple local broadband providers/carriers to connect each branch office to the corporate network and then building out and maintaining the appropriate authentication, security, and management capabilities behind the company's own firewall often results in substantial capital expenditures, a large, inconsistent and difficult-to-manage base of suppliers, and high recurring costs associated with support and management. Additionally, when something goes wrong, the complex environment makes it difficult and time consuming to find and correct problems. This can increase downtime, and hurt branch office employee productivity.

One answer to this problem is the GoRemote Branch Office Solution, which operates under a network aggregation business model, so customer companies can use a single source to enable high-speed access for all of its branch offices. Additionally, because BOS can be configured as a completely hosted service, most if not all of the behind-the-firewall infrastructure costs can be eliminated, reducing upfront expenditures. Security features, including VPN, can also be completely hosted, which can improve the overall cost structure, and, because GoRemote employs dedicated security experts to manage, maintain, and monitor these features, improve performance as well.

Nevertheless, the biggest potential benefit of the Branch Office Solution is likely in its business case. The solution is fully supported on a 24 x 7 basis and guaranteed by service level agreements. It takes much of the expense and worry out of distributed enterprise enablement, and gives administrators a single point of contact for any problem. This effectively frees up the IT department's time and budget, as well as allows the department to put more focus on accomplishing other tasks that can help drive the business.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2004 IDC. Reproduction without written permission is completely forbidden.