2009

BizTechReports.Com

Editorial Director:
Lane F. Cooper

Managing Editor:
Steve Lee

The Role of IT Infrastructure Performance in the Federal Border, Transportation and Security Environment:

Optimizing Wide Area Network Infrastructures in Support of the Homeland Security Mission

The Role of IT Infrastructure Performance in the Federal Border, Transportation and Security Environment

By
Lane F. Cooper and Steve Lee
BizTechReports.Com

Executive Summary:

The community of federal, state and local agencies tasked with protecting people, property and institutions within the United States against natural disasters and man-made threats operates in an information- and communications-intense environment. It is not an exaggeration to state that, in this environment, getting the right information to the right people, at the right time, and at the right place can spell the difference between life and death. However, achieving the high levels of interconnectivity and interoperability necessary for effective collaboration across these agencies is complicated by a number of factors. Agencies tasked with the homeland security mission:

- Are dispersed throughout the country;
- Operate across jurisdictions and thus have multiple chains of command; and
- Have a complex array of legacy technologies and applications that must be linked in a meaningful manner to foster cross-agency cooperation.

These factors can inhibit the ability of agencies to effectively share vital information in real-time. Among the infrastructure elements that links first responders, key decision-makers and mission-critical applications across the federal border, transportation and security community are wide area networks (WANs). Consequently, the WAN is emerging as a strategic asset in the homeland security community that supports:

- Organizations that are looking for ways enable mobile and remote staff as well as field agents;
- Agencies seeking both operational and cost efficiencies by consolidating information processing infrastructures through virtualization; and
- Senior officials exploring ways to facilitate collaboration, increase security and accelerate the decision-making process.

In the federal border, transportation and security environment, specifically, there are a variety of dedicated and shared WANs that interconnect people, processes and technologies across the country. There is a growing consensus that the ability to ensure operational readiness, optimize response to threats, act on credible intelligence and implement policy effectively is now inextricably tied to the performance of the IT infrastructure in general – and the WAN infrastructure in particular.

To explore the key considerations that should be addressed by officials tasked with harnessing technology to meet the homeland security mission, the editors of ***BizTechReports.Com*** met with subject matter experts at San Francisco-based ***Riverbed Technology*** to gather key insights into emerging trends and best practices for WAN optimization within the homeland security community.

Introduction:

As broadband resources become more affordable and widespread, the architecture of core enterprise information technology infrastructures is rapidly shifting from dependence on local area networks (LANs) to WANs. This trend is further advanced because private and public sector enterprises are increasingly adopting new technology-enabled operational strategies that allow organizations to decentralize management structures.

While the private sector has in many ways led the way in embracing enterprise-wide "telework," mobility arrangements, and initiatives to connect distributed offices, public sector organizations are now developing a compelling case for deploying an IT infrastructure that leverages high-performance WAN architectures.

Nowhere in government is the need for flexible and distributed access to enterprise IT resources more critical than in the federal border, transportation and security arena.

Consider, for instance, the mission of the Department of Homeland Security (DHS) – which this year received $3 billion in stimulus funding in 2009 to support its critical objectives. DHS has consolidated and integrated dozens of federal agencies with varying missions and bureaucratic cultures. Not only must DHS:

- Coordinate its missions with a staggering number of state and local public safety organizations, such as county law enforcement and municipal fire departments;

It must also:

- Effectively interact with other federal agencies with overlapping mission responsibilities, such as agencies in the departments of Justice and Defense.

"The front lines of the homeland security mission are geographically dispersed, which means that homeland security IT infrastructure must be highly distributed," says Bill Hartwell, general manager and senior director of the federal markets division at San Francisco-based Riverbed Technology.

"Well over two-thirds of the homeland security workforce does its job outside of a headquarters building co-located with the enterprise LAN infrastructure. The homeland security frontline – border checkpoints, airport security checkpoints, immigration agents need a high-performance, distributed IT infrastructure," explains Hartwell.

In the years since the tragic events of 9/11 and the Katrina hurricane disaster in New Orleans, initiatives have been launched to strengthen DHS' ability to protect the American homeland. These initiatives include new technology deployments designed to improve communications and information access for DHS units and other agencies in the field.

In recent years, homeland security IT strategies have focused on ways to provide inspectors, agents and other personnel stationed across the country with access to the most current generation of applications for information reporting, access and retrieval. Increasingly, these systems are being built on WAN architectures.

Working through Legacy Systems to a WAN-Oriented Future

Getting to an end-to-end WAN environment, however, is a work in progress. DHS and local public safety IT professionals must contend with the evolutionary nature of government IT procurement. Many of the legacy applications that form the foundation of technology used by DHS were developed and deployed in an era dominated by LAN architectures.

"Legacy applications used in the homeland security space were designed to work on a LAN, where there is minimal distance between the client and server," explains Kari Gerster, director of product marketing for verticals at Riverbed.

"The longer distances over the WAN mean higher latency – in other words, it takes longer for information to travel across the network – and this can cripple application performance, thereby impacting mission performance," says Gerster.

"The challenge, as we move to a more distributed environment," continues Gerster, "is that LAN-based applications often produce a lot of redundant data and processes. While these applications worked well on the LAN-based infrastructure of a decade or so ago, performance really suffers when data makes the long journey across a WAN."

Department heads and IT professionals in the homeland security arena are consequently wrestling with how to optimize existing infrastructure and applications for the new WAN reality. Among the choices available to officials addressing this challenge:

- Agencies could procure all-new applications built specifically for the WAN operating environment. This is unrealistic because of the budget pressures and the high risks involved with replacing familiar, tried-and-true applications; or

- Officials can bridge the limitations of current LAN-oriented applications by making adjustments that allow applications to operate effectively over a geographically dispersed, highly connected network of agencies and units.

The key to filling the gap between legacy architecture and contemporary mission needs revolves around optimizing IT infrastructure performance.

Reevaluating Assumptions for Performance in a WAN Environment

When network performance degrades, most government IT professionals and managers instinctively believe that their maxed-out – or soon-to-be-maxed-out – networks need more bandwidth. It is a default position that seems to make sense. More bandwidth, however, only solves part of the WAN performance problem.

Pursuing bandwidth expansion as an exclusive infrastructure performance optimization strategy can get expensive. The time required to implement and deploy this option could also take between nine and 12 months. And as new capacity is created (by adding lines, switches, routers, etc.), more complexity and cost is added to the network topography.

Moreover, says Hartwell, simply throwing bandwidth at the issue does not address many aspects of the underlying challenge.

"Bandwidth is just one element of the IT infrastructure performance story. Adding more bandwidth, for instance, doesn't address latency – the lag time in data transmission that results from long distances and routing steps between network nodes – which is a persistent feature of the WAN environment."

"For users at the farthest edge of a network – like the crew of a satellite-connected Coast Guard cutter or agents in a Border Patrol vehicle – more bandwidth does not solve latency challenges that can leave these people out of the loop," explains Hartwell.

Legacy applications designed for a LAN environment were programmed for the client device to frequently "ping" the server side of the application. In addition, many of these applications run on TCP, which in itself requires many round trips to move information across the network.

On a LAN Ethernet, activity at both the TCP and the application protocol layers places an insignificant burden on the network.

But over long-distance WANs the story changes.

When data bounces off satellites 26,199 miles away in geosynchronous orbit, or sprints thousands of miles across the Pacific Ocean via fiber optic cable, latency will be an issue.

What is needed instead is a solution that revolves around:

- Reducing the **amount of data traffic** that needs to be sent via compression and the reduction of redundant data transmissions; and
- Limiting the **need to send "overhead" or "telemetry"** traffic that is needed to execute programs on both ends of the network (the client and the server). This can be done by optimizing applications to perform on a WAN environment.

Three Questions for Determining WAN Performance Requirements:

1. How much redundant data is on the WAN?
2. How much latency is there on the WAN?
3. How many round trips are applications making across the WAN?

"LAN-based applications and legacy infrastructures can be optimized to dramatically improve performance over a WAN," explains Gerster.

In other words, organizations must consider using what analysts at Gartner call WAN Optimization controllers, to enable a strategy that leverages the most performance out of existing bandwidth resources.[1]

By configuring and optimizing systems so that they send less data and transmit fewer TCP packets, and then reducing the number of steps in an application process, agencies with a homeland security mission can achieve between five- and 50-times faster WAN performance.

Riverbed, says Gerster, has been able to demonstrate that a combination of techniques – like data de-duplication and application-specific optimization – can streamline data transmission and accelerate application performance to yield significant improvements in IT infrastructure performance.

"WAN optimization can do far more for remote agents on a satellite or a poor quality terrestrial connection than simply adding more bandwidth capacity," points out Gerster.

Comprehensive WAN Optimization Reduces Cost Structure in FEA Context

Another aspect of WAN optimization that is capturing the interest of senior officials in the Homeland Security community is financial performance.

According to researchers at Chantilly, Va-based INPUT, a leading public sector IT market research firm, homeland security priorities have contributed as much as 8.5 percent to federal technology spending in recent years. Indeed, border and transportation security were called out in both versions of the American Recovery and Reinvestment Act (ARRA), with funding set-aside for detection and checkpoint technologies.

According to analysts, Homeland Security, Transportation, Energy and the Treasury Departments account for approximately 70 percent of a federal technology budget that will

[1] Gartner Magic Quadrant for WAN Optimization Controllers, 2009 (http://www.riverbed.com/lg/whitepaper-gartner-2009.php?CID=70170000000Iqlo)

© *BizTechReports.Com* 2009, All Rights Reserved

cross the $50 billion mark before the end of the decade.[2]

Nevertheless, even these managers and IT leaders are not exempt from growing scrutiny from oversight organizations like the Government Accountability Office (GAO) and the Office of Management and Budget (OMB).

OMB in particular has been exerting pressure on agencies to justify spending initiatives by requiring agencies to present detailed "Business Case" documents that describe the costs and benefits of new technology investments. In many cases, Business Case requirements are tied to alignment with the Federal Enterprise Architecture (FEA).

The FEA framework equips OMB and federal agencies with a common language and framework to describe and analyze investments, enhance collaboration and ultimately transform the federal government.

The FEA consists of a set of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps and opportunities for collaboration within and across agencies. The WAN is included within the Technical Reference Model (TRM) under "Service Platform and Infrastructure."

"The TRM provides a framework to describe how standards and technologies support the secure delivery, exchange and construction of Service components. In this context, WAN optimization has been shown – on average – to generate a return on investment within seven months," explains Hartwell.

Best Practices in Infrastructure and WAN Management

So, what specific steps can department heads and IT leaders in the federal border, transportation and security environments take to design, launch/deploy and manage a WAN-based infrastructure modernization initiative?

According to Riverbed's Hartwell, there are no shortcuts to achieving mission-critical objectives while maintaining high levels of operational readiness along the way. To that end, he advises organizations to:

- ***Do the necessary homework:*** IT managers should understand their WANs, before making any moves to modernize or optimize the enterprise network. A detailed study and analysis of all applications, protocols, storage, and services is an excellent start. The good news is that there are several commercial-off-the-shelf (COTS) tools that can enable this analysis and provide the supporting reporting to accelerate this analytical process.

  Officials should also analyze the way network elements interact with specific operations and processes. Public sector IT managers should also go outside of their organizations – and beyond their usual stable of vendors and contractors – to find examples of how WANs in other agencies have deployed and managed an optimization controller installation.

  The key is to ensure that an apples-to-apples analysis takes place. To that end, time and scale are important considerations in comparing current WAN optimization activities.

  Hartwell recommends comparing technologies that have been deployed within the last six-to-twelve months, and that represents a network topology that is similar to the planned deployment.

[2] "Federal Border and Transportation Security Market Forecast, 2008-2013." (http://www.input.com/corp/library/detail.cfm?ItemID=7960)

- ***Focus on proven, compliant products and services:*** In the public sector environment, compliance with standards and a high degree of reliability and integrity are vital. Technologies that already address compliance requirements – such as those called for by Joint Interoperability Test Command (JITC) and Federal Information Processing Standards (FIPS) – offer public sector IT managers assurances that can save time and anguish.

- ***Test under field conditions:*** Public sector IT managers can further mitigate risk while proving that a WAN optimization controller installation enhances performance for end-users by setting up 'proof of concept' environments in discreet enterprise-wide applications or specific processes.

Lab or bench testing can prove inadequate for a WAN optimization test or proof of concept. This is because an overly controlled environment does not account for the multitude of variables that are far more prevalent in WAN vs. LAN environments. It is therefore necessary to take the proof of concept project into the field to test how both real use, distance, and network topography effect performance.

Conclusion

The WAN will play an increasingly vital role in meeting the mission-critical objectives of the homeland security community. This is especially true as agencies:

- Continue the now decades-old effort to break down silos of operation without impacting the mission;

- Improve interoperability across agencies; and

- Empower key personnel in the field.

Optimizing this strategic asset is therefore a rising priority for both operational and technology leaders in this sector. Advances in WAN optimization technology provide opportunities to significantly improve the WAN performance without adding actual bandwidth, which is both expensive and complex.

New best practices in WAN optimization offer an opportunity to improve performance, reduce costs and better support the homeland security mission.

About Riverbed Technology

Riverbed Technology is the IT infrastructure performance company. The Riverbed family of wide area network (WAN) optimization solutions liberates businesses from common IT constraints by increasing application performance, enabling consolidation, and providing enterprise-wide network and application visibility – all while eliminating the need to increase bandwidth, storage or servers.

Riverbed works with many government organizations, ranging from one of the world's largest navies – which achieved "near-terrestrial" performance of its key Web applications on all of its ships – to the Defense Contract Management Agency's (DCMA) efforts to consolidate its data centers.

Dozens of government organizations have deployed Riverbed Steelhead products, ranging from small deployments to multi-site deployments with hundreds of appliances. These organizations have chosen Riverbed products to enable consolidation of global IT assets, speed data transfer for mobile field operations units, decrease backup and data replication times by up to 90 percent, and reduce bandwidth costs and utilization.

Thousands of companies with distributed operations use Riverbed to make their IT infrastructure faster, less expensive and more responsive. Additional information about Riverbed (NASDAQ: RVBD) is available at www.riverbed.com.

About BizTechReports.Com

BizTechReports.Com is an independent reporting agency with offices in Washington, DC and the San Francisco Bay Area that analyzes user trends in business technology. *BizTechReports.Com* explores the role that technology products and services play in the overall economy and/or in specific vertical industries. For more *BizTechReports.Com* white papers, case studies and research reports, visit www.biztechreports.com.

© ***BizTechReports.Com*** 2009, All Rights Reserved