SearchEnterpriseWAN.com E-Guide

Security and WAN optimization: Getting the best of both worlds

As the number of people working outside primary office locations increases, the challenges surrounding security and optimization are becoming more prevalent. This E-Guide details how to maximize the potential of the Wide Area Network while keeping out security threats at all locations.

Sponsored By: Blue Coat®

TechTarget®
The Technology Media ROI Experts

SearchEnterpriseWAN.com E-Guide

Security and WAN optimization: Getting the best of both worlds

Table of Contents

Finding the right balance between WAN performance and security

The number of people working outside a primary office from remote locations like branch offices or even at home is increasing, creating security and optimization challenges for organizations.

Most organizations typically have some technology in place to secure IT and network resources at each branch office, but the bulk of these security solutions are being deployed in central network locations to control and manage data that is being sent to each remote location. Even though this type of approach reduces management costs, it can also reduce a company's ability to deal directly with security threats at each branch location.

Also, many organizations find it difficult to compress and accelerate Secure Sockets Layer (SSL) traffic without increasing the security risks and creating new management challenges. Accelerating this type of traffic creates an additional burden for Web servers because they must decrypt and re-encrypt SSL traffic, as well as process end-user requests.

Policy management and business-critical applications

Many organizations are still struggling with making educated decisions about defining network usage policies to ensure a proper balance between securing and optimizing performance of business-critical applications. It is important to ensure that the network usage policies in place protect a company's networks from malware, spyware and other security threats. At the same time, however, the security policies that are developed should not have a detrimental effect on the quality and consistency of the end-user experience.

End-user organizations often get into a position where they have to decide which is more important: protecting the data being delivered over the WAN or achieving the optimal level of end-user experience for applications being accessed by remote users. This should not be a dilemma, as both of these goals can be achieved if the right mix of technology and internal processes is in place.

The inability to effectively manage speed, availability and security of applications delivered over the WAN can have a significant impact on a company's business performance. Organizations struggling to execute effectively on these initiatives could experience lost revenue opportunities, declines in employee productivity, and increased IT management costs.

Likewise, the inability to prevent performance and security problems when delivering applications to end users that are "customer-facing" (sales, customer service, etc.) could lead to lost revenue opportunities. If these employees cannot access corporate data in a seamless way while communicating with customers and prospects, problems with customer satisfaction, longer sales cycles, and damage to the organization's brand image can result.

In addition, slow and not readily available applications can cause disruptions of business processes if business-critical data cannot be delivered to employees when they need it. This leads to increased idle time for employees and causes a decline in their productivity.

As well as benefits that organizations can derive from being able to address any security and performance risks in a timely manner, the use of integrated platforms for managing both security and performance can also be an advantage. In some cases, this may be a single product; in other cases, it may be a combination of different products that have a high degree of integration. These benefits predominantly include cost savings on implementation and management.

Deploying two or more different tool sets for managing application performance is associated with several management challenges for organizations' IT departments. In addition to time to implement and the management of each solution, organizations need to ensure that these products can work together in a seamless way. In other words, they need to ensure that the security solution(s) they have implemented are not causing problems with delivery of critical data to end users -- and vice versa. Organizations are expecting an optimal level of end-user experience for business users, and very often mistakes in defining security policies can negatively affect end users' ability to access their data. At the same time, as important as it is for organizations to improve and maintain an optimal level of end-user experience, they need to be aware of security and compliance issues and be able to keep their data protected.

It is apparent that using a single solution that can effectively address both security risks and performance management challenges would reduce the cost of implementation. Leveraging a single platform for managing WAN security and optimization also allows organizations to achieve significant savings in cost of maintenance, facility and labor.

Improving network visibility: Keeping an eye on applications, users

Effective management of wide-area network (WAN) security and performance starts with gaining full visibility into how network capacity is being used by both the applications and the users on the network.

Organizations not only need to understand what type of traffic is flowing through the network, they should also be able to measure bandwidth usage per application, location, and user (or group of users). The ability to identify types of traffic that are running on the network helps organizations to be more effective when defining network usage policies.

Not being able to view network traffic can reduce the effectiveness of WAN optimization initiatives, especially if optimization solutions accelerate malicious traffic along with data that is business critical. It can also increase the potential for security threats and undermine an organization's ability to better leverage its existing network capacity.

Just having some type of tool for monitoring the network and applications does not ensure successful improvements in managing WAN security and performance. Recent research has revealed that even though 85% of organizations improved their ability to collect network and application performance data over the last two years, only 54% of these organizations improved their ability to resolve issues with network and application performance in a timely manner over the same period.

There is a wide range of monitoring solutions available in the market today. In order to achieve full WAN performance visibility, it is important to choose solutions that can collect not only generic performance data but also that data which is truly actionable and can be turned into information needed to prevent performance problems.

The goal is to be more proactive when managing WAN security and performance. To do this, you need tools in place that will alert the IT staff to potential problems before end users are affected. Tools for network anomaly detection, for example, can analyze historic performance data to define dynamic thresholds for acceptable levels of performance and issue alerts every time the performance falls below these thresholds. Also, the majority of these tools can define baselines based on capabilities for ongoing learning, which enable organizations to adjust to changes in network traffic, which in turn automates the process for proactive WAN management.

Automating processes for identifying performance anomalies improves the success rate in preventing problems while enabling organizations to manage more with less. The effectiveness of these capabilities also improves if they are coupled with tools for ensuring that the policies are enforced. This gives organizations the ability to have full control over their WAN traffic, and it also allows them to measure the effectiveness of their initiatives.

Matching security techniques to application needs

Less than three years ago, the top performance metric that end-user organizations were using to evaluate performance of their networks was the amount of unplanned network downtime. Since then, organizations have started to understand that managing only network performance does not ensure an optimal level of security and experience for each user. Companies have become more concerned about security and performance of applications that are running on the network, as opposed to the network itself. As a result, there is more of an emphasis on such metrics as application availability and response times when evaluating the management initiatives.

In order to effectively execute on these initiatives, organizations started looking beyond basic connectivity levels and started deploying solutions that will help them understand not only which Internet Protocol (IP) addresses and ports are being affected but, more importantly, which applications and/or users are suffering from performance issues.

Organizations need to be aware that there are different types of security risks associated with the different applications deployed and then take specific actions to address each of these threats. As organizations roll out more applications, the complexity of managing the security and performance of each of these applications is increasing, and so are the business risks that can come from an inability to effectively execute on key management strategies.

Applications such as instant messaging (IM) or peer-to-peer (P2P) sharing pose new security and performance management challenges, calling for a new set of capabilities to control this type of traffic. Organizations need to have capabilities in place that will allow them to identify this type of traffic and to take actions to filter these applications and ensure that they don’t have a negative impact on their networks. Underlying technologies for these applications are significantly different from those of traditional enterprise applications, so organizations need to adjust their security techniques to the specific functionalities of each of these applications.

In order to achieve this goal, organizations must not only deploy new technologies but develop new strategies that will allow them to take a more coordinated approach when managing security and performance of data delivered over the network. This means, of course, that organizations should be focusing on the overall application delivery infrastructure (storage, networks, end-user devices, etc.) as opposed to just monitoring the network.

Virtualized solutions, cloud computing drive demand for proactive Net monitoring

Organizations are increasingly deploying Virtual Desktop Infrastructure (VDI) solutions to simplify IT management and improve flexibility of delivering applications to end users.

However, even though this type of technology can deliver measurable business benefits for end-user organizations, VDI deployments are increasing the amount of data that is being accessed remotely and therefore pose new challenges for managing WAN performance and security.

The top four challenges that organizations report when managing performance in VDI environments are:

1. Reduced visibility into application performance.
2. Increased bandwidth consumption.
3. Increased network latency.
4. Inability to deal effectively with an increased amount of interactive traffic over the WAN.

Effective traffic management policies and tools that are taking an application-centric approach (as opposed to network-centric) can help address these challenges.

As deployments of VDI technologies shift operating systems from end-user devices to a centralized data center, desktop/laptop-based security solutions are becoming redundant, which puts even more emphasis on securing the network. In addition, as VDI technologies enable organizations to access any business-critical data from any device that is connected to the network, it becomes harder to ensure an optimal level of security, especially since IT has to manage a wider range and number of devices.

Traditional network visibility tools are not as effective when monitoring interactions between virtual machines. In order to address this challenge, organizations need advanced network monitoring capabilities that will be able to detect why these interactions are occurring and whether they are caused by any malicious attacks. Obviously, it makes more strategic sense not to wait until these problems affect key business processes and create problems with regulatory compliance. The solution is to have advanced alerting capabilities that enable IT teams to resolve these issues in a timely manner, before they compromise the network and become even bigger problems.

Visibility challenges in virtualized environments

One of the key issues in managing application performance in virtual environments is the loss of visibility into network application performance through the use of monitoring tools that are designed to deal with traditional physical environments. Most of these tools were built for either network or server monitoring and are not as effective when deployed in virtualized environments. As a result, visibility into the entire transaction flow has emerged as one of the top challenges when managing delivery of applications over the network in virtualized environments.

Over the next two years, 16% of the traffic currently being transferred across corporate WANs will be delivered to end users through the public Internet, according to surveys of top organizations. As these companies become increasingly dependent on Web-based applications and use cloud computing techniques to deliver business services, new management challenges arise.

To keep pace with demand, IT and network managers are increasingly requesting that their service providers offer service-level agreements (SLAs) that go beyond application uptime and guarantee speed of applications and optimal levels of security. As cloud computing gains more traction in the enterprise market, this issue will become more prevalent, since organizations will be dealing with the challenge of pulling data from multiple resources, making it more challenging to distinguish between business-critical data and security threats.

While a company can achieve significant operational and business benefits from leveraging cloud computing, these benefits can diminish if it does not have capabilities in place to ensure proper levels of services being delivered by its cloud providers.

Finding a balance between TCO and performance

Reducing total cost of ownership (TCO) has emerged as one of the top objectives this year for companies looking to improve network performance management. In order to achieve this, however, organizations are increasingly planning to deploy solutions that will allow them to achieve multiple management and technology targets, such as security, WAN acceleration, network monitoring, and so on -- all by using a single platform. This allows companies to do more with less while avoiding interoperability issues and reducing the cost of management and maintenance.

These solutions include the following:

- Network routers with integrated WAN optimization capabilities. Several vendors are offering networking equipment that not only offers advanced security capabilities but also has built-in application acceleration capabilities. Deploying these solutions significantly reduces management cost and mitigates any interoperability risks that come from deploying different WAN security and optimization hardware.

- Tools for analyzing packet flow data for security and performance management purposes. Most organizations already have capabilities for collecting packet flow data (NetFlow, sFlow, etc.) from their networking equipment. But many of them are struggling with turning this data into actionable information. Using tools that can leverage existing packet flow data for both security and performance can help organizations reduce their TCO while enabling them to make more educated decisions when defining network usage policies.

- Hardware solutions that include multiple application delivery functionalities on a single device. Companies often deploy solutions for accelerating WAN traffic that include some capabilities that are not used on a regular basis (or ever). Since some of these solutions come with predefined management interfaces, organizations do not have a choice about the capabilities they want to turn on or off, based on their needs. In order to avoid that situation, organizations will often deploy multiple solutions to manage different aspects of their WAN traffic, which consequently increases TCO and overall management cost.

Deploying hardware solutions that include multiple application delivery functionalities (such as caching, compression, SSL acceleration, etc.) on a single device, and provide flexible management capabilities so organizations will use only the features that they really need, can result in a significant saving in TCO and make for a better and more effective WAN architecture.

About the author:

Bojan Simic is a proven expert in areas of application performance management (APM), WAN optimization, network management, application delivery, and network management. Over the last three years, Simic interviewed more than 2,000 IT and business professionals. He published more than 50 research reports that were downloaded by more than 15,000 IT and business decision makers worldwide.

His domain knowledge includes insights into end-user experiences, best practices in deploying solutions for network and application performance management, and strategies of related solution providers.

Simic holds a B.A. in economics from Belgrade University in Belgrade, Serbia, and an M.B.A. from McCallum Graduate School of Business at Bentley College.

Resources from Blue Coat

[Accelerating Delivery of Critical Applications Worldwide](#)

[Stopping Malware Attacks Before They Impact User Desktops](#)

[5 Reasons Why You Need Better Visibility of Your Network](#)

About Blue Coat

Blue Coat Systems is the technology leader in application delivery networking. Blue Coat offers an Application Delivery Network infrastructure that provides the visibility, acceleration and security required to optimize and secure the flow of information to any user, on any network, anywhere. This provides the comprehensive application and user control required to contain costs, enhance productivity and respond quickly to changing business requirements, fueling a long-term competitive advantage for the distributed enterprise. Blue Coat has an aggressive strategy and solution roadmap for advancing the integration of the visibility, acceleration and security technologies at the heart of the application delivery network. Additional information is available at www.bluecoat.com.