



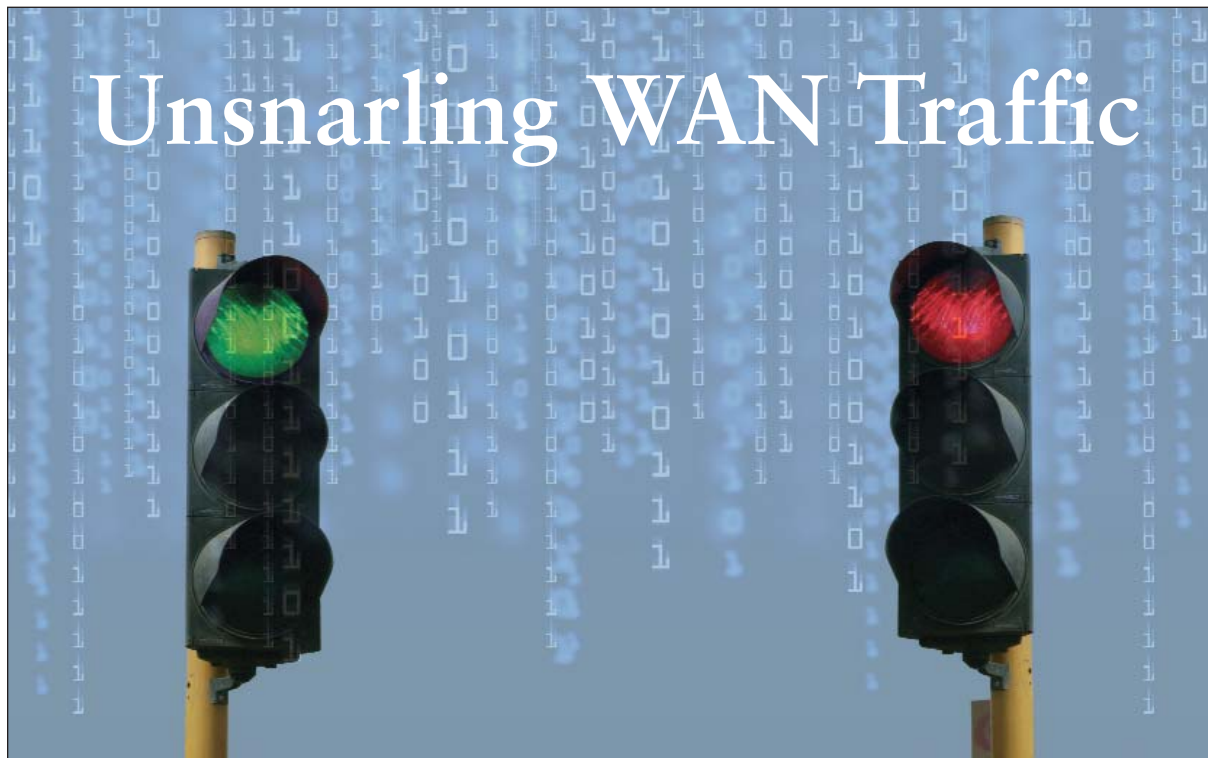
The Milestone Review

APRIL 2011

inside

Survey validates need for '3D security' ... page 4
Mobile transaction struggles hurt business ... page 6
'Spear fishing' on the rise ... page 8

Unsnarling WAN Traffic



Milestone partners with Riverbed
to deliver best-of-breed WAN
optimization solutions for remote
and mobile workers and the cloud.

Organizations continue to become more geographically dispersed due to acquisitions, entry into new markets and end-user demand for telework and mobility solutions. These distributed enterprises need their remote offices, mobile workers, regional facilities, manufacturing and distribution centers, and central headquarters to function as one integrated business unit.

This trend is placing a significant burden on the WANs that connect users, systems and applications across locations. Increasingly complex applications and growing file sizes have increased network congestion and caused serious performance issues — particularly on far-flung WAN links.

Historically, organizations relieved these bottlenecks by increasing bandwidth or deploying local storage at each location. However, these techniques add significantly to total cost of ownership in both operating and capital costs, while failing to address the underlying problems. Today, more organizations have begun to implement or evaluate technologies designed to significantly increase the effective data throughput on WANs.

“After carefully evaluating WAN optimization products, our engineers determined that Riverbed has the best solutions on the market,” said Mark Greer, COO, Milestone Systems. “Riverbed’s WAN optimization solution accelerates data and applications across the entire network and enhances visibility into applications over the WAN. Milestone has partnered with Riverbed to deliver solutions that will help our clients’ WANs run more efficiently, increasing productivity while reducing costs.”

Broad Range of Options

A number of technologies have been introduced to improve WAN throughput, including WAN optimization, wide-area file services (WAFS) and wide-area application services (WAAS) and applications acceleration. Each of these technologies attacks WAN limitations from different perspectives.

“Riverbed offers the broadest WAN optimization solution available, featuring data reduction, WAN optimization and application-level latency optimizations, along with remote office file and management functionality, in a single solution that scales across the broadest range of applications and network topologies,” Greer said. “Riverbed improves not only WAN throughput but application throughput, because applica-

tion performance problems are caused by more than just limited bandwidth.”

The award-winning Riverbed Steelhead product family offers organizations acceleration of applications and data regardless of location. Riverbed Steelhead appliances typically accelerate applications across the WAN by five to 50 times, and in some cases by up to 100 times. They also cut the use of WAN bandwidth by 65 percent to 95 percent, and deliver LAN-like performance to mobile workers and employees around the world. Relieving WAN congestion supports IT consolidation and virtualization initiatives, and optimizes business continuity and disaster recovery by enabling centralized data stores and efficient off-site replication.

Virtual World

Virtualization in the data center holds the promise of improved server utilization, more rapid deployments and lower power consumption. Riverbed recently released Virtual Steelhead, which enables customers to deploy Riverbed WAN optimization solutions in virtualized environments. The virtualized platform gives customers the ability to leverage existing virtual infrastructure and scale on demand.

“With the introduction of the Virtual Steelhead, built for the VMware vSphere Platform, organizations have the flexibility to provide anywhere access for employees from a comprehensive set of solutions that meets the needs of customers in any environment,” said Greer.

Virtual Steelhead offers customers greater flexibility to deploy Riverbed WAN optimization technology in a wider range of environments that have specialized needs and require resilience and customiza-

“Riverbed Steelhead Mobile allows organizations to provide remote workers with better access and performance, eliminating barriers to mobility. It enables organizations to take advantage of improved flexibility and simplified management functionality to provide mobile workers with accelerated performance no matter where they are working throughout the world.”

tion, while still offering simplified management. With Virtual Steelhead, a virtualized WAN optimization solution can now be deployed in virtualized data centers, as well as on hardened military or first responder equipment, news vans and construction trailers that are in rugged environments or where a Steelhead appliance won't fit due to physical space limitations.

Optimizing the Cloud

Riverbed has also introduced solutions for applications and storage in public cloud environments. These offerings will help IT organizations deliver anytime, anywhere IT performance to globally connected enterprises without requiring changes to their existing infrastructure.

"IT departments have traditionally deployed rich resources at the enterprise edge. To overcome the complexity of this model, organizations are consolidating their IT resources into private clouds, deploying WAN optimization and visibility solutions to improve performance as data moves farther from users. As organizations begin to incorporate public cloud into their IT strategies, however, they're finding that the same performance issues that impact private clouds challenge them in public cloud environments," Greer said.

Riverbed Cloud Steelhead is designed to accelerate public cloud migration and to speed access to data and applications hosted in the public cloud. Riverbed's Whitewater appliance extends its award-winning acceleration and de-duplication capabilities to cloud storage, providing organizations with a fast, secure and cost-efficient method to seamlessly integrate cloud storage into their existing backup infrastructure and disaster recovery strategies.

On the Road

Employees are becoming more mobile, even as the centralization of data and IT infrastructure makes remote access more of a challenge. Riverbed's Steelhead Mobile product allows organizations of all sizes to deploy a cost-effective mobile WAN optimization solution with increased scalability, speed and simplicity.

"Riverbed Steelhead Mobile allows organizations to provide remote workers with better access and performance, eliminating barriers to mobility," Greer said. "It enables organizations to take advantage of improved flexibility and simplified management functionality to provide mobile workers with accelerated performance no matter where they are working throughout the world."

"Riverbed's leadership in the WAN optimization market can be attributed to product innovation and focus on creating a comprehensive WAN optimization solution. The company has maintained a focus on customer priorities and ever-changing IT requirements," said Cindy Borovick, research vice president at IDC. "Enterprise IT departments are being pressed to improve IT efficiency and employee productivity with a reduced IT budget. As more companies move forward with IT consolidation projects to cut costs, performance for end-users is a concern. Mobile WAN optimization can help overcome this challenge by improving the performance of critical enterprise applications for remote and mobile workers."

To discuss the benefits of Riverbed's technology, contact Milestone Systems at 866-646-9211 or email ask@milestonesystems.com.

milestone
systems, inc.

Ensuring High Availability and Network Security
for Mission-Critical Applications, Since 2000.

BlueCoat



JUNIPER
NETWORKS



info@milestonesystems.com

866-646-9211

www.milestonesystems.com

Survey Validates Need for ‘3D Security’

Emerging technologies and limited user awareness creates greater security complexity, according to Check Point and the Ponemon Institute.

Managing complex security environments is the most significant challenge facing organizations today, according to a February 2011 survey of more than 2,400 IT security administrators in organizations of all sizes around the world. The research, conducted by the Ponemon Institute and sponsored by Check Point, found that more than 55 percent of companies are using products from seven or more different vendors to secure their networks. Organizations can benefit from approaching security with a holistic view of their environment in order to understand where risks can reside

The survey, *Understanding Security Complexity in 21st Century IT Environments*, also shows that organizations struggle with a growing set of security priorities and limited employee awareness about corporate policies. Key findings from the report validate the importance of Check Point 3D Security, a new approach to security that goes beyond technology and combines policy, people and enforcement to help organizations align their IT policies with their business needs

“To improve security in this day and age, organizations need a better understanding of their current environments and prioritize their short- and long-term initiatives,” said Juliette Sultan, head of global marketing at Check Point Software Technologies. “Check Point’s approach with 3D Security goes beyond technologies — it also rais-



es awareness on today’s security challenges, while providing better visibility and control to organizations.

“By educating end-users and enforcing security policies with a holistic view of the organization, companies can minimize the complexities associated with security and compliance in modern-day business environments.”

Emerging Technologies Cause Concern

According to the survey, more than 700 respondents believe the primary concern with emerging technology

adoption is compliance. With the proliferation of cloud computing, mobility, Web 2.0 and file-sharing applications, organizations often struggle to apply the appropriate levels of security across all layers of the network, while also adhering to stringent compliance requirements. Security and compliance in modern-day environments begin with a well-defined policy that aligns with an organization’s business needs and industry regulations.

While emerging technologies have created new methods of communication and collaboration for enterprises, organizations struggle with managing multifaceted IT environments. This often contributes to greater security complexity and the risk of data loss by employees or other insiders.

In fact, 48.8 percent of respondents believe their organizations’ employees have little or no awareness about their data protection or corporate policies. As a result, more education and awareness is needed to help people realize their important role in maintaining the organization’s security profile. In addition, survey respondents believe the ability to manage policies by user is a key functionality to enforce better security overall, with 58 percent citing identity awareness as a priority today and in the future.

“Companies are constantly facing new and costly security risks from both internal and external sources that

can jeopardize the business. Our research has shown that one cyber-attack can range anywhere from \$237,000 to \$52 million,” said Dr. Larry Ponemon, chairman and founder, Ponemon Institute. “However, employees can play a big role in being a first line of defense, helping their company enforce stronger security measures and promoting more user awareness within the organization.”

The Importance of 3D Security

Check Point’s 3D Security redefines security as a three-dimensional business process for stronger protection across all layers of security. With 3D Security, corporations can now implement a blueprint for security that goes beyond technology to ensure the integrity of all information security.

“To achieve the level of protection needed in the 21st century, security needs to grow from a mere collection of technologies to a business process that incorporates three major dimensions — policies, people and enforcement,” said Gil Shwed, founder, CEO and chairman of Check Point. “Check Point’s 3D Security vision redefines security as a business process that will enable companies to achieve the required level of security while streamlining operations.”

Check Point 3D Security enables organizations to transform security into a business process by integrating the three following dimensions:

* Policy: Security starts with a well-defined and widely understood policy that outlines the organization’s needs and strategies. Few organizations today have such a policy; instead most companies rely on lists of system-level checks and a collection of disparate technologies that do not always deliver the desired level of security.

* People: Users of IT systems are a critical part of the security process. It is often users who make mistakes that result in malware infections and information leakage. Few organizations pay much attention to the involvement of users in the security process, when in fact, employees need to be informed and educated on security policy and their expected behavior. At the same time, security should be as seamless and transparent as possible and should not change the way users work.

* Enforcement: Security is about gaining better control over the many layers of protection. Unfortunately, corporations often find themselves losing control over the disparate policies from various point products. In many cases security systems generate violation reports but do not enforce the policy. Companies should and can achieve a higher level of visibility and control by consolidating their security infrastructure, and using systems that prevent security incidents rather than just detecting them.

“To improve security, businesses should rely on a combination of technology, policy and people. Recognizing this need for defense in depth, Check Point’s vision for 3D Security aligns with a lot of the security needs and business priorities we hear from customers,” said John Grady, senior analyst, Security Products research at IDC. “By adding an educational element and giving employees the opportunity to participate in the security process, businesses can significantly reduce their risks.”

To discuss how you can implement 3D Security, contact Milestone Systems at 866-646-9211 or email ask@milestonesystems.com.



Technical Training



BlueCoat



IronPort Email and Web Security

JUNIPER
NETWORKS

training@milestonesystems.com
866-646-9211

See current schedule:
www.milestonesystems.com/training/

milestone
systems, inc.



Mobile Transaction Struggles Hurt Business

Four out of five consumers experience problems conducting mobile transactions.

Businesses have a great deal to gain by attracting mobile consumers. They also have a great deal to lose if the mobile experience does not meet or exceed the in-store or online experience. Do your mobile transactions measure up?

That's the question asked by Harris Interactive in a survey commissioned by Tealeaf. The survey found that 84 percent of online adults in the U.S. who have conducted a mobile transaction via smartphone or other mobile device in the past year have experienced problems with those transactions. Despite the hyper growth of the mobile Internet, one fundamental truth remains: regardless of whether the platform is a mobile device, tablet or computer, online customer experience is still fraught with issues. The success of mobile channels will depend largely on customers' ability to complete transactions and their willingness to return.

"If your revenue comes from mobile or online customers, you need to pay close attention to the activity on your website," said Tom Olson, Senior Network Engineer, Milestone Systems. "Milestone has partnered with Tealeaf to offers tools that can

provide detailed reports on both customer experience and application performance.

"They key to Tealeaf's benefits is the proactive nature of the tool. Instead of waiting for a customer complaint, by which time you might have already lost customers, Tealeaf can inform you of a single customer experience that is below acceptable levels of performance, and even take action to help retain that customer. Having real-time information on the experiences of customers also drives action plans, site improvement projects, and other tasks that can now be measured for success in a timely manner."

We've Got Trouble

Mobile devices are set to become the medium for digital commerce. According to ABI Research, U.S. mobile commerce sales will reach \$4.9 billion this year and will account for \$163 billion in sales worldwide by 2015. Mobile consumers are trying to conduct transactions — from shopping and travel to banking and insurance — and time after time they are frustrated by poor website experiences, leading to site abandonment and brand damage. Beyond basic connectivity, the mobile experience is fraught

with issues that prevent users from accomplishing their goals struggle-free.

According to the mobile consumer behavior survey commissioned by Tealeaf, of those who struggled while conducting a transaction via their mobile devices:

- * 34 percent received an error message
- * 29 percent said the app/website was difficult to navigate
- * 25 percent were unable to complete a transaction due to an endless loop
- * 23 percent had trouble logging in
- * 16 percent said they encountered insufficient, incorrect or confusing information

Previous online consumer behavior surveys conducted by Harris Interactive show similar customer struggles. Between 2005 and 2009, Harris Interactive conducted five online consumer transaction surveys on behalf of Tealeaf. On average, 86 percent of online consumers surveyed during that period experienced similar problems when conducting online transactions from traditional desktop or laptop computers. The new mobile survey highlights that, while the platform for conducting transactions is shifting, consumer struggles continue.

Almost half (47 percent) of consumers who have conducted a mobile transaction in the past year expect the experience on their phones to be better than the in-store experience. Eighty percent expect the mobile experience to be better than or equal to the in-store experience, and 85 percent expect the mobile experience to be better than or equal to using a laptop or desktop computer.

Just how frustrating are customer struggles on a mobile device? The survey found that more adults would be extremely or very frustrated by experiencing a transaction problem on a mobile device (58 percent) than by going to the DMV (50 percent) or being stuck in traffic (56 percent).

Abandon Ship

If they experienced problems attempting to conduct mobile transactions, many consumers would abandon their transactions and take their business elsewhere:

- * 43 percent would abandon the mobile transaction and try later on a computer
- * 16 percent would become more likely to buy from a competitor
- * 14 percent would email or log a complaint with customer service
- * 12 percent would abandon the transaction at the app/site and try a competitor's app/site

Most important, customer struggles on a mobile device can drive consumers away from doing business with a company entirely. More than 60 percent of all online adults said they would be less likely to buy from the same company via other channels if they experienced a problem conducting a transaction on their mobile phones.

“Everyone talks about the momentum in the mobile channel and customers continue to show an increasing appetite for moving transactions to these devices,” said Rebecca Ward, CEO of Tealeaf. “However, mobile consumers find the convenience of transacting anywhere is often offset by unsatisfying and unproductive experiences. Just because we can pay our bills from our smart phones while riding the subway doesn’t mean our expectations are reduced. Mobile consumers are no more willing to tolerate poor experiences than customers accessing websites from their desktops.”

Are you providing customers with a high-quality web application experience? Milestone and Tealeaf can help you find out. Call 866-646-9211 or email ask@milestonesystems.com.

When You Need

High Availability & Network Security

Call Milestone Systems



A value-added integrator focused on enhancing networks and serving IT teams in 4 main ways:

- Network Appliances
- Consulting
- Training Classes
- Managed Services

Serving Minnesota, Iowa, Wisconsin, SoDak, NoDak, Omaha, Florida, Georgia, NoCarolina, SoCarolina, Alabama, Mississippi, and Tennessee

952-543-6999 // 866-646-9211

info@milestonesystems.com
www.milestonesystems.com

milestone
systems, inc.

‘Spear Phishing’ on the Rise

In response, FireEye introduces next-generation email security appliances that use a real-time, signature-less malware protection engine.



Experts say that phishing attacks declined in 2010 but a more targeted technique known as “spear phishing” increased dramatically. FireEye is helping to combat this threat with new technology that accurately identifies spear phishing attacks — even those utilizing zero-day exploits — to prevent costly data security breaches and time-consuming post-incident investigation.

While phishing attacks cast a wide net hoping that a few victims will bite, spear phishing targets select groups with meticulously crafted emails containing malicious attachments or links. Generally, the targets work for the same company, are members of the same organizations or otherwise have something in common, and the emails are ostensibly sent from organizations or individuals from which the victims would normally receive email.

According to the FBI, spear phishers start by gaining access to inside information on their targeted victims by hacking into an organization’s computer network or by combing through other websites, blogs, and social networking sites. They then send legitimate-looking emails explaining why they urgently need the victim’s personal data. The victims are lured into clicking on a link inside the e-mail that takes them to an authentic-looking website

where they are asked to provide user IDs and passwords, PINs, access codes, etc. They may also be tricked into downloading malware that can be used to access sensitive internal information.

“Spear phishing emails are extremely deceptive thanks to social engineering,” said Terry Shidla, CISSP, Milestone Systems. “Instead of sending out official-looking emails from organizations the victim may or may not be associated with, spear phishers launch sophisticated attacks against specific users. In many cases, the goal is to not only get personal information but information that can be used to attack the enterprise network, steal trade secrets or engage in economic espionage. Cyber criminals are becoming focused on the quality of attacks rather than sheer numbers.”

Spotting Fake Attachments and URLs

FireEye has introduced the FireEye Email Malware Protection System (MPS), which uses real-time analysis of embedded URLs and attachments to stop spear phishing attacks. The Real-time Attachment and URL Analysis engine evaluates emails for zero-hour malware using virtual machines that run a cross-matrix of operating systems and applications, such as various web

browsers and plug-ins. This dynamic analysis enables FireEye to detect and stop spear phishing email attacks aimed at known and truly unknown OS and application vulnerabilities. With global data from the FireEye MAX Cloud Intelligence network, customers get the latest security content about malicious attachments targeting zero-day vulnerabilities, malware callback channels and URL blacklist updates.

The incorporation of real-time, dynamic analysis coupled with global security content enables customers to stop the email-borne modern malware infection cycle. With blended attacks using email and the Web on the increase, it is critical to have a zero-hour, signature-less malware protection engine to analyze links in email as well as file attachments, such as PDF documents, Microsoft Office files, multimedia content, and other file formats.

“Using the FireEye Email MPS, we’ve been able to stop over three dozen separate spear phishing attacks over the course of two weeks,” said an IT administrator who asked to remain anonymous. “In our case, we’ve seen no false quarantines, and by integrating with our FireEye Web MPS, we can quickly trace a zero-day web exploit back to its spear phishing email, preventing a breach and saving at least 320 hours of forensic analysis for just one of the incidents.”

Targeting Targeted Attacks

The FireEye Email MPS is an easy-to-deploy appliance that requires no tuning. It deploys as an MTA (Message Transfer Agent), SPAN (Switched Port Analyzer) device, or BCC destination, and sits behind existing email control points like anti-spam gateways. The new Email MPS family includes the Email MPS 8000 Series for high-volume email environ-

ments and the Email MPS 5000 Series for midsize to large email volumes.

FireEye Email MPS complements FireEye MPS, which enables organizations to secure their networks against inbound zero-hour malware and outbound data theft callbacks, and to dynamically inoculate their networks from future attacks. FireEye MPS blocks targeted attacks, zero-day exploits and advanced persistent threats, and provides accurate, actionable forensics that detail the exact nature of an inbound attack or outbound callback, such as keylogging and other data theft or fraudulent transaction activities.

FireEye network security appliances protect against zero-day attacks through advanced malware analysis across multiple protocols, including but not limited to HTTP, IRC, FTP and SMTP. Conducting deep packet inspection via highly instrumented virtual machines, the FireEye technology engine is able to identify both previously infected machines as well as systems under attack with pinpoint accuracy that virtually eliminates the problem of false positives.

“FireEye customers benefit from the combination of next-generation malware protection and an extensive malware intelligence network to enhance their overall cyber security infrastructure. FireEye’s network security appliances deploy quickly, filling the security gaps in traditional antivirus, intrusion detection and secure web gateways to protect against targeted exploits,” said Shidla. “Now FireEye Email MPS extends this protection to email to prevent targeted spear phishing attacks.”

Milestone and FireEye can help protect against these emerging threats. To find out more, call 866-646-9211 or email ask@milestonesystems.com.

JUNIPER
NETWORKS

NOW!

Juniper Training for Network Architects & Engineers



Learn the full capabilities of your Juniper equipment from highly experienced, “been there” instructors at Milestone Technical Training Classes. Multi-day courses such as:

- ◆ JUNOS software (intro, troubleshooting, or advanced)
- ◆ Advanced Juniper Routing in the Enterprise
- ◆ Configuring Security Threat Management
- ◆ Integrating Juniper Firewalls & VPN’s into High Performance Networks
- ◆ And more! Call us for the topic you need.

See current schedule of classes at www.milestonesystems.com/training or call Paul Eck, Milestone Training Manager, to discuss your Juniper training requirements. Class can be at our facility or yours.

milestone
systems, inc.

866.646.9211 or 952-767-5142
training@milestonesystems.com