BLUE COAT

Security Empowers Business

THE NEED FOR INCREASED SECURITY CAPACITY

WHITEPAPER

PREPARING YOUR NETWORK TO MANAGE TODAY'S WEB THREATS AND LEVERAGE KEY WEB TRENDS

Today's complex web environment is driving the need for a web security infrastructure with greater levels of performance and capacity. In the course of a few short years, the World Wide Web has demonstrated its ability to add tremendous value to the operations of all kinds of organizations. The web has become a critical communications tool, enabling commercial transactions to take place quickly and effectively, regardless of barriers imposed by time and distance. The Internet has secured a vital niche as a medium that businesses can leverage to promote products and services to millions of people. The web has also established itself as an indispensable source of information and intelligence which can improve the decision-making process and outcomes.

However, as with other communication media, the web brings risks as well as benefits. Risks in the form of malware, viruses, and data loss have the potential to devastate organizations that do not have adequate protection in place. In addition, these risks are compounded by the sheer volume of traffic, and the demands for higher performance and security capacity necessary to ensure that critical business operations are not impacted.

In the past, web security was about implementing corporate policy and reducing productivity loss on well-known websites. Today those same websites offer fully encrypted sessions for security and embedded photo and video sharing. Employees now access the internet with multiple devices, including tablets, smartphones and notebooks which may not necessarily be controlled by the enterprise IT organization. Many websites pose a threat as a base for stealthy cyber-attacks which are designed to obtain sensitive corporate and personal information. While existing secure web gateways may have met the security capacity requirements of yesterday's web, they require a significant boost in performance to address the security needs of a dynamic and rapidly evolving web environment.

Web Threat Trends

Websites have become the preferred delivery mechanism for damaging malware such as viruses, spyware, and adware. In some cases, simply visiting an infected website is enough to download unwanted programs onto a computer. This malware can surreptitiously leak sensitive financial or client data to a criminal third party, and recovering from security breaches is time consuming and costly.

Web-based malware and threats continue to grow at a phenomenal rate. Traditional URL filtering has evolved to address some of these issues, but the increase in volume and complexity of threats ensures the need for continually evolving security technologies. As these new technologies are rolled into secure web gateways, there is a need for additional security capacity and processing performance in the web gateway.

Survey - Web Use on the Job

64% of respondents say they visit non-work related websites during work hours. 41% of those regularly visit Facebook and other social networking sites.

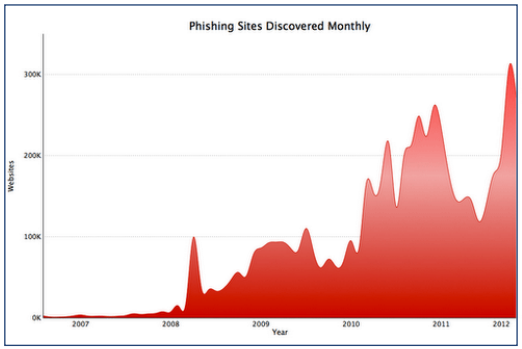
– Salary.com, 2012

Recreational web use continues to be a major issue facing businesses today. Efficiency, productivity, bandwidth, and corporate reputation are compromised when employees squander office time on inappropriate surfing activities. The web offers more potential distractions than ever before, including social media, chat rooms, streaming media, and online games. Visits to adult and illegal websites expose businesses to legal risks, and can result in loss of client trust and embarrassing media coverage.

In the face of this alarming and continually evolving threat landscape, businesses face a challenge in establishing the right balance in their approach to web usage. It is critical that the organization and individual employees are properly protected, but also that the speed and efficiency of business operations are not compromised by overly restrictive policies.

BLUE COAT

Security Empowers Business



Reference:
Blog.sucuri.net, 2012

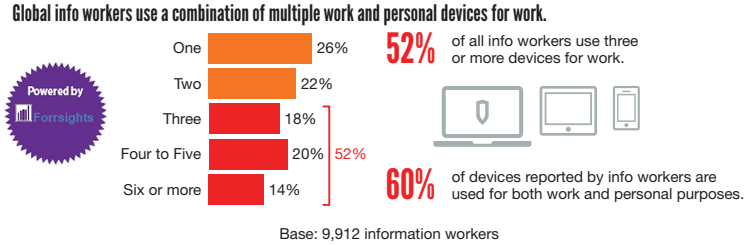
BYOD and the Consumerization of IT

The list of information technologies that end users are adopting directly, without the involvement of their company's IT department, is getting longer every day. Personal smartphones and tablets are increasingly used in the workplace, contributing to a trend that some companies embrace as advantageous and others reject as risky. Google Apps, Salesforce.com, Skype, Twitter, Facebook, and countless other cloud-based services and applications are readily available, easy to use, and can be provisioned with the motion of a fingertip. IT organizations are only beginning to deal with managing their presence.

The consumerization of IT goes far beyond personal technology choices and the bring your own device (BYOD) phenomenon. Individuals, managers, and entire business units are making their own technology decisions, presenting a challenge to traditional IT organizations that are accustomed to provisioning and controlling access to all information assets. As information technology continues to play a more prominent role, information workers and technology staff must establish a new balance. Workers must have the freedom and flexibility to meet business needs. Concurrently, IT must ensure that important considerations like security and compliance are not compromised.

Forrester estimates that 52 percent of all information workers use three (3) or more devices for work, a combination of laptops, smartphones, and tablets. 60 percent of these devices are used for both work and personal purposes.[1] With each employee having multiple devices on the corporate network, the need for increased performance and security capacity will grow significantly.

[1] Forrester Research; Forrsights Employee Workforce Survey, Q4 2011



Forrsights Workforce Employee Survey, Q4, 2011. Forrester Research, Inc.

Social Networking

Web applications such as social networking are now widely used by enterprises worldwide. These cloud-based applications lower costs, increase productivity, and contribute to work/life balance for employees. They also place stress on the security, control, and performance of legacy web infrastructure. As web applications like social networking have become part of legitimate business operations, they have become integral to Internet-based criminal operations.

Attackers leverage social media sites to target spam. Spear-phishing and targeted social networking emails link to sites with unpatched vulnerabilities. The ability to send a message on a social networking service is similar to sending an email, but with far less spam or phishing protection.

Facebook is a social networking website that allows users to interact with other users in a multimedia environment on the web. Facebook users can install and use applications to enhance their experience. Businesses want to enable Facebook access to maintain employee satisfaction, but at the same time they also want to control access to it. IT organizations seek more granular ways to enable certain groups such as Marketing and HR with read and write access, while restricting other organizations to read-only.

The increased traffic to social networking sites, which are now multimedia rich, is driving bandwidth requirements as well as new approaches to security. Many enterprises still depend on aging web and messaging security solutions that simply do not provide the performance, web content filtering and security capacity that is needed for the dynamic environment of the web.

Rich Media

Video continues to dominate bandwidth usage on global networks. The Cisco Visual Networking Index forecasts that video will exceed 50% of worldwide bandwidth usage in 2012. By 2016, the amount of Video-on-demand traffic will triple and will be equivalent to 4 billion DVDs per month.[2] Other forms of rich media are also significant drivers of traffic, including music, high-resolution images, and video games. Organizations routinely use video in-house for telepresence meetings, sometimes involving thousands of participants company-wide, as well as to facilitate training. Specialty cable channels featuring popular sporting events sometimes supplement their cablecasts by streaming media over the Internet, further increasing bandwidth consumption.

All of this traffic is placing higher performance and security capacity demands on enterprise networks and service provider networks. While some organizations may be able to limit and control the amount of video crossing their networks, others may find that their business needs will require them to allow different tiers of service on their networks. Caching and stream-splitting can provide some temporary relief, but even with these bandwidth management techniques in place, increased capacity to support rich media is a must-have.

IPv6

The current Internet standard communications protocol IPv4 (Internet Protocol Version 4) was conceived three decades ago, at a time when the expansion of the Internet to its current state was inconceivable. The most apparent limitation of IPv4 is its lack of address space. Designed for a limited number of research campuses, IPv4 provides up to 4 billion addresses: Not enough to meet current demand. IPv4 was also not designed to be secure. Features such as virtual private networks with encryption, secure routing, and authentication were bolted on later and never properly integrated. IPv6 (Internet Protocol Version 6) does however integrate these later additions properly, and even provides for future expansion in an organized way.

Today, the current over-use of addresses causes delays and difficulties in routing Internet traffic and limits the growth of the Internet in emerging markets. Mobile technologies are constrained because network providers cannot assign routable addresses to every mobile device.

IPv6 not only substantially increases the number of addresses, but also enables more efficient routing and greater support for mobile devices.

IPv6 is also inherently more secure than IPv4. For example, IPSec (encrypted VPNs) are now a mandatory component. To begin the transition to IPv6, many IT organizations are deciding to run dual-stack networks which allow for the operation of both IPv4 and IPv6 environments across the same hardware, ensuring no disruption to service delivery. During this process, it is paramount that organizations deploy network solutions that have sufficient performance and security capacity available to simultaneously process IPv4 and IPv6 traffic.

Cloud Computing

Cloud computing has emerged as a top priority on CIO agendas, and one of the most significant IT developments over the past decade, offering new and flexible ways to manage IT costs, scale IT operations and streamline related processes. But cloud also presents new dimensions of complexity relating to information security and privacy, with risks varying significantly with the type of cloud, the architecture, and the application.

Cloud computing also changes the way organizations approach security in the network. When physical infrastructure is virtualized, new strategies are required to create and maintain security boundaries in the absence of physical partitions. As companies adopt more cloud-based applications and services, they are seeking effective ways to control which users have access to specific services, as well as their access rights within each service. However, the increasing number of users moving outside the traditional enterprise security boundary complicates this already difficult challenge.

More remote and mobile workers are accessing the network and cloud-based applications, from wherever they are working, and through different devices...From smartphones to laptops to netbooks. In addition, they are passing sensitive data, such as sales or customer information, through these devices, which may not be supported by the enterprise, and often, are used for both professional and personal computing.

Data centers have increasingly high-density server environments that require high switching and routing capacity. Organizations face difficult

[2] Cisco Visual Networking Index, May 2012

choices when it comes to performance and security, sometimes even limiting security in order to meet performance demands. In the current threat environment, organizations can no longer afford to sacrifice security for performance.

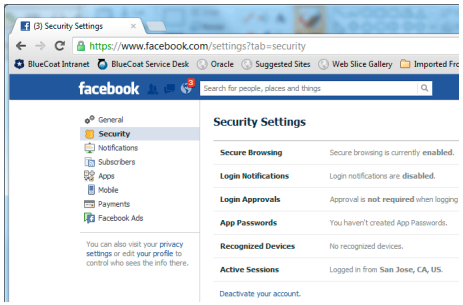
As if these issues were not enough, cloud computing environments must meet the compliance expectations that are imposed on physical systems. For example, regulations specify regular maintenance of anti-malware. All of these problems represent practical concerns about day-to-day security operations for cloud networks within a dynamic threat landscape. Traditional models of security from the physical world must be extended in favor of higher capacity security that is optimized for cloud-based environments.

Increased Website Security and Encrypted Content

When web security was in its infancy, it was not unusual to bypass scanning and filtering of secure websites encrypted with SSL. SSL proxies were not common, and those that did exist generally had high overhead and resource requirements to operate. Outside of financial services and e-commerce transaction websites, SSL encryption was rarely found.

Today many websites use SSL encryption, and it is not uncommon for entire web sessions to remain encrypted while the user is accessing the website. Examples of common websites that have full-time encryption include Gmail and Facebook, both of which pose risks for data loss, productivity loss, and inbound malware. Without SSL inspection and proxy, SSL encrypted websites represent a significant security risk for most organizations.

To maintain regulatory compliance and web security, IT administrators should incorporate SSL inspection in their web security plans. Because of the significant resources that SSL inspection requires, IT administrators must consider security performance and capacity upgrades as part of their web security strategy.



Planning For Capacity Growth

Increasing malware and threats, the need for improved web site security, and the exponential the growth in rich media traffic, social networking use, and BYOD are all forcing IT administrators to recognize the need to plan for capacity growth in their secure web gateways. While existing web gateway technology may meet current capacity requirements, the trends in web security point to a need for headroom to accommodate new features, new functionality, and expanded bandwidth requirements.

How can IT administrators scale their web security infrastructure to keep pace with security capacity requirements and deliver high levels of WAN performance, while still complying with internal expense mandates?

Blue Coat is aggressively developing new web security technologies for both on-premises and cloud deployments. Current trends in malware, along with rapid growth in the use of web-based video are driving Blue Coat innovation in secure web content delivery, even to mobile users. With Blue Coat's wide range of appliances and cloud offering, IT organizations will never have to compromise between performance and the industry's most comprehensive web security.

The Blue Coat ProxySG appliance family, part of Blue Coat's web security solutions, provides complete web security and acceleration, enabling flexible, granular policy controls over content, users, applications, web applications, and protocols. The web Application Policy Engine provides visibility and comprehensive control over web and mobile applications such as social networking and chat sites. For example, it can control specific operations such as posting, chatting, uploading, downloading, and playing games to meet internal user compliance guidelines for web content read and write access.

Proxy SG defenses include strong user authentication, web filtering, deep inspection of content for threats or data loss, security checks to the Blue Coat WebPulse™ collaborative defense, and inspection and validation of SSL traffic. To support the performance demands of rich media content, ProxySG provides content caching, stream splitting, traffic optimization, and bandwidth management.

The ProxySG security solutions also deliver high performance web security in the cloud as well as with on-premise appliances. Blue Coat Cloud Service deployed for branch offices and remote workers, in

BLUE COAT

Security Empowers Business

conjunction with ProxySG on-premises appliances, creates a hybrid design providing the best of on-premise control with always-on protection for the roaming and remote user.

The Blue Coat ProxySG security framework has proven scalability with deployments in over 86 percent of the FORTUNE® Global 500. ProxySG performance innovations require less hardware, rack space and energy than alternative solutions. They are greener, more efficient to install, power, and cool, thus enabling lower TCO. And ProxySG is ready for the inevitable migration to IPv6 with a full IPv6 implementation, IPv6 advanced policy management, and an IPv4 to IPv6 proxy for seamless transition.

Summary - Providing the Right Balance of Security and Performance

In today's dynamic web environment, the need for a web security infrastructure with greater levels of performance and capacity has never been greater. Exponential growth in web traffic, the migration to cloud-based architectures, the consumerization of IT, and the steady evolution of malware and security risks continues to challenge IT organizations everywhere.

With the rise in social media and other web-based distractions, IT must also deal with inappropriate and irresponsible use of the web, the impact on worker productivity, and potential harm to the corporate brand. In the face of this alarming and continually evolving threat landscape, businesses face a challenge in establishing the right balance in their approach to web usage. The key is to ensure that the organization and individual employees are properly protected, but also that the speed and efficiency of business operations are not compromised by overly restrictive policies.

The ProxySG appliance family and Blue Coat Cloud Service deliver the increased performance and security capacity to meet the needs of the most demanding IT environment, whether on-premises or cloud-based. The Blue Coat security solution provides comprehensive protection and control over web traffic, including strong user authentication, web filtering, and deep inspection of content for data loss or threats. Blue Coat enables granular visibility and control over applications, content, users, and protocols, providing the ultimate foundation for a secure web gateway.

About Blue Coat

Blue Coat empowers enterprises to safely and securely choose the best applications, services, devices, data sources, and content the world has to offer, so they can create, communicate, collaborate, innovate, execute, compete and win in their markets. Blue Coat is the trusted by 86 percent of the FORTUNE Global 500.

Visit us at bluecoat.com for more information.

BLUE COAT

Security Empowers Business

v.WP-NEED-FOR-SECURITY-CAPACITY-EN-v2a-1013

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000