IT innovation is fueling change around the world. According to the 2013 Cisco Visual Networking Index (VNI) study, by the end of 2013, the number of mobile-connected devices will exceed the number of people on earth. One billion people use Facebook and Twitter. New tablets, smartphones, and other mobile devices are being introduced at a breakneck pace, enticing consumers with a never-ending supply of must-have devices, applications, and services.

Mobility has brought down the wall between business and personal, spiking corporate productivity and putting work/life balance within reach. The bring-your-own-device (BYOD) phenomenon is a way to be constantly connected for work, family, and play. Companies that do not adapt and allow people to work where, when, and how they want risk losing their highly skilled employees and may fail to attract the newest generation of workforce talent.

The cloud has quickly become an integral part of IT strategies among companies of all sizes, and public cloud services are seeing double-digit growth. Gartner forecasts the public cloud market to be $131 billion in 2013, with the market for infrastructure-as-a-service (IaaS) growing faster than software-as-a-service (SaaS).¹

Content and application models are also transforming as people flock to the convenience of the cloud. The demand for video, whether for entertainment or collaboration, is seemingly insatiable. Video is projected to quadruple all IP traffic by 2014, and 70 percent of the world’s mobile traffic is projected to be video by 2016.²

New Day for Security

With the tectonic cultural shifts caused by the consumerization of IT, it’s become clear that organizations’ carefully constructed security plans must be re-imagined. More than 1 million websites, including many sites used for legitimate, professional use, are compromised with some form of malware. In fact, workers are more likely to get malware from an ad on a trusted site than from visiting sites widely thought to be risky.

With four new pieces of malware created every second, information security is a high-speed race. Trying to keep pace with legacy security approaches and static policies is a steady drain on IT resources. But dedicated administrators continue to try: A typical firewall has more than five rules for every employee, and those rules change daily. Who can access which applications is a moving target for a security administrator, and that’s no small risk in a world of complex compliance and regulatory frameworks.

The challenge is formidable. IT is charged with protecting everything from the company’s intellectual property to a smartphone left in a cab. Despite the growth of mobility and BYOD, IT must ensure that acceptable use policies are enforced, no matter where workers are; whether they are using their personal or company-issued smartphone, laptop, or tablet; or whether the applications are for business or personal use.

A windfall of security resources is unlikely, and IT can’t continue to squander precious resources by constantly patching malware signatures and updating blacklists. Adding a second vendor’s firewall isn’t the answer, either. Rather, it only magnifies complexity and the risk of configuration errors. “There is a higher risk associated with configuring and managing firewalls from multiple vendors than from a single vendor,” according to Gartner.

IT needs a more efficient means to adapt security practices and protections to meet changes in work patterns, device usage, and applications. To meet that challenge, security must take into account users’ identities and the applications they use, as well as the context in which they use the applications.

“Context-aware and adaptive security will be the only way to securely support the dynamic business and IT infrastructures emerging in the next 10 years. The Future of Information Security Is Context Aware and Adaptive.”

Neil MacDonald, vice president and fellow at Gartner

---

3 1,159,000 compromised sites as of March, 2012. www.stopbadware.com
4 “One Brand of Firewall Is a Best Practice for Most Enterprises,” by Greg Young, Gartner Research, November 2012. ID G00217262
Next-Generation Firewall – Security in Context

Cisco ASA 5500-X Series Next-Generation Firewalls deliver the most comprehensive threat protection from targeted attacks and web-based malware, and can adapt to constantly evolving threats. Cisco next-generation firewalls apply the strengths of the world’s most widely deployed stateful inspection firewall (the ASA 5500 Series), class-leading Cisco AnyConnect® VPN, and network intrusion prevention, and build on that success with new application control and web security features that are backed by Cisco Security Intelligence Operations (SIO).

With this depth and breadth of policy enforcement, the ASA 5500-X Series delivers network wide security without compromise. Organizations can ensure that Web 2.0 and collaborative applications commonly used for business and personal reasons can be monitored and controlled based on context-aware policies. Organizations can be confident that their security policies will be enforced across physical and virtual domains to ensure complete protection and simplify administration.

The ASA 5500-X Series brings the context of user identity, device type, device location, application type, web reputation, and threat information into the policy. With complete visibility into which users and devices are accessing the network, administrators can enforce policies by both device and user, rather than one or the other. Policies are enforced consistently and within context across the network—without any penalties in network performance.

Unmatched Global Threat Intelligence

Next-generation, context-aware protection is predicated on the latest threat intelligence across the world. Operating around the clock, Cisco SIO pushes real-time threat intelligence from the cloud to your firewalls and other security infrastructure so you can make decisions based on up-to-the-minute threat information as well as the reputation of the domain, IP, URL, and sender. The combination of cloud-based intelligence and a context-aware firewall provides an unmatched advantage: Cisco can protect your organization months ahead of the threat.

For example, in September 2012, when security researchers warned of a zero-day vulnerability in Internet Explorer (IE) that would allow an attacker to attain full administrator access to a vulnerable machine running IE version 6, 7, or 9, security providers rushed to develop and publish traditional signatures to protect against a potential attack. However, more than two weeks earlier, Cisco SIO had already automatically blocked the malicious site hosting the exploit. In addition, Cisco quickly moved to block access to domains that were subsequently used to spread the malware and identified more than 40 parked domains registered by the same attacker. With cloud-based intelligence and reputation analysis, Cisco stopped the attack at the source—and disarmed the attacker weeks before competitive solutions could take any action.

Gartner predicts that by 2015, 90% of enterprise security solutions will be context-aware.³

Stop Threats Everywhere

The comprehensive threat protection provided by Cisco next-generation firewalls gives companies the power to stop threats everywhere. The ASA 5500-X Series provides best-in-class threat protection against malware, targeted attacks, botnets, and web-based threats. With built-in reputation-based protection, your organization is protected far in advance of published exploits, and threats are blocked well before they can take hold.

Web-based anti-malware protection ensures that any of more than 1 million compromised websites don’t spread malware to an unsuspecting victim. All web traffic is inspected in the cloud for optimal efficiency and deployment simplicity.

The ASA 5500-X Series also integrates the world’s only reputation-based intrusion prevention system to ensure that attackers cannot penetrate the firewall and your critical systems. Using telemetry feeds from nearly 2 million Cisco security devices and 150 million endpoint devices located throughout the world, Cisco SIO analyzes and correlates that data to assess the reputation of websites and delivers near-real-time protection against zero-day threats. Cisco SIO updates this information and pushes it to all Cisco security devices globally every three to five minutes – 24 hours a day, seven days per week.

Similarly, Cisco IPS is the only context-aware IPS that uses device awareness, network reputation of the source, target value, and user identity to drive mitigation decisions – so administrators can enforce proactive policies to act more aggressively on threats that present a more serious or immediate risk to network resources.

The ASA 5500-X Series also identifies botnets, so if a device in your organization is compromised, such as via an infected USB, it can be rapidly identified and quarantined, limiting the damage.

Your next-generation firewall investment is protected, even as business requirements change. Cisco ASA 5500-X Series Next-Generation Firewalls combine the industry’s most deployed stateful inspection firewall with comprehensive next-generation network security services, so organizations can start with the protection they need now and layer in additional security services as needed. But even as you add threat definitions, application control, and threat management, comprehensive security will not compromise performance.

Granular Application Visibility and Control

As the line between business and personal applications has blurred, IT can no longer unilaterally declare Facebook, Twitter, and LinkedIn “bad” and block their use. When the use of social media applications becomes essential for business, IT needs more flexible, granular controls over applications and their components.
The Cisco Application Visibility and Control (AVC) software module provides the greatest levels of visibility and control over mobile, collaborative, and Web 2.0 applications—and even micro-applications, such as Facebook games. AVC identifies more than 1000 applications and 150,000 micro-applications, so administrators can easily allow or deny entire categories of applications, or allow access to some micro-applications while denying others.

AVC can also identify application behaviors and can even identify individual actions a user takes within an application. For example, workers may be allowed to view but not post to Facebook. Or workers on a 3G cellular connection may be unable to stream music and movies or make purchases. AVC also ensures the security of applications, such as Skype and BitTorrent, which hop across different TCP ports, rendering useless the practice of using port numbers as a proxy for applications. This gives administrators new levels of control over social media, streaming media, and other applications.

Reputation-Based Web Protection

Cisco Web Security Essentials (WSE) delivers reputation-based protection against web-borne threats, often months before they are detected by antivirus engines. Using Cisco SIO’s global threat correlation, WSE delivers reputation protection for URL, domain, and IP addresses. This helps protect organizations from zero-day attacks from compromised sites without requiring emergency signature updates or system patches. Web reputation feeds from Cisco SIO enable more granular policies based on reputation of the host site, as well as the most effective, timely coverage available.

Cisco WSE also enables robust content-based URL filtering with differentiated access policies based on user, group, device, and role. It includes 65 URL categories and a comprehensive URL database that encompasses sites in more than 200 countries and over 60 languages.
Assured Identity and Device Access

With mobility and BYOD making great strides, IT needs a way to easily differentiate access based on mobile devices and location. For example, workers may be allowed more limited access when using their personal tablets than when using company-owned laptops or virtual desktops. And access may be even more restricted when using a personal laptop. That access may change, depending on whether a user is in the corporate headquarters, at a branch office, or using Wi-Fi from home or cellular on the road.

Together, the Cisco ASA 5500-X Series and Cisco AnyConnect Secure Mobility Client make it easy to provide flexible access that can be differentiated by the user’s identity, network location, and specific device used. This way, when the vice president of manufacturing logs on with a new Android tablet or remotely via the VPN, IT can be confident that access policies will be enforced within the changing context.

In addition to passive authentication methods using Active Directory agent and Lightweight Directory Access Protocol (LDAP), Kerberos and NT LAN Manager can provide active authentication for differentiated access control based on user, group and role.

The Cisco ASA 5500-X Series integrates with Cisco TrustSec®, allowing administrators to use the device and user identity already available in the network. This information can be used to identify and tag traffic from employees, contractors, and guests and then control access. For example, guest traffic can be limited to a guest network, and the Cisco ASA 5500-X Series firewall can limit the applications or websites that guests may use. No other next-generation firewall is able to provide such diverse access control mechanisms.
Security Without Compromise: Context-Aware and Adaptive Next-Generation Firewalls

Built on a Strong Foundation

Context-aware security provides protection against advanced threats in the new world of mobility, cloud, and collaboration. Organizations can depend on the comprehensive suite of Cisco ASA Next-Generation Firewall Services that can be added without sacrificing the proven protection of the industry’s most trusted—and most widely deployed—stateful inspection firewall, unlike other “next generation” vendors. Administrators can use their network know-how to maximize their effectiveness while creating flexible, context-aware policies. Cisco ASA 5500-X Series Next-Generation Firewalls are designed to scale to meet the needs of small businesses to global enterprises, and simplify the maintenance and auditing of policies, even across thousands of sites.

Security Without Compromise

Corporate networks are encountering unprecedented change as work becomes an activity, rather than a physical place. As more workers need anywhere, anytime access to enterprise and cloud-based resources, IT needs a fresh approach to ensure that the organization remains protected without impeding business innovation. Cisco ASA 5500-X Series Next-Generation Firewalls provide security capabilities at scale while delivering superior levels of application visibility and control, web security, intrusion prevention, remote access, and cloud-based threat protection – for flexible enterprise-class security today and tomorrow.

Learn More

Cisco ASA 5500-X Series Next-Generation Firewalls
Cisco Next-Generation Firewall Services