Cisco Expands Security Services Into the Cloud

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[[](http://itmanagersinbox.com/wp-content/uploads/2009/04/cisco.jpg)](http://itmanagersinbox.com/wp-content/uploads/2009/04/cisco.jpg)Cisco today announced new additions to its portfolio that bolster the network security infrastructure and the delivery of cloud[security](http://www.cisco.com/en/US/products/hw/vpndevc/index.html) services, thereby enabling businesses to collaborate with greater confidence even as their workforce and partners become increasingly mobile and interactive.

Today’s announcement, being made at the RSA Conference in San Francisco, comes at a time when [collaboration](http://www.cisco.com/en/US/netsol/ns870/index.html) and mobility technologies are redefining how, when and where business gets done. As companies continue to extend connectivity outside their office walls, businesses must focus on new ways to protect its data and communications.

While today’s business applications, social media, software-as-a-service and wireless technologies gain widespread adoption and lead to new interactive business models, those same technologies and business models are jeopardized by threats that are just as novel and agile.

Tom Gillis, vice president and general manager, Security Technology business unit, Cisco said “In today’s changing world, businesses require a security strategy that accounts for the physical, virtual, mobile and global aspects of their business.

Our vision for security is based on a balance of protection and enablement, which integrates security from the network through to the endpoint and the user. Security needs to capture the latest threat intelligence to mitigate shifting threats. This combination enables businesses to collaborate with greater confidence when engaging employees, partners and customers.”

[[](http://itmanagersinbox.com/wp-content/uploads/2009/04/cips.jpg)](http://itmanagersinbox.com/wp-content/uploads/2009/04/cips.jpg)

**Cisco Intrusion Prevention System (Cisco IPS)**

Current network security developments and security trends will be highlighted tomorrow at the 2009 RSA Conference, where Cisco Chairman and CEO John Chambers will deliver a keynote address titled “Collaborate with Confidence.” Chambers will describe security trends and discuss his perspective on the heightened importance of network security in a collaborative world. To attend a live webcast of Chambers’ keynote address, please visit:<http://www.cisco.com/offer/rsakeynote>.

The Cisco security offerings announced today incorporate new threat defense products and services that will help customers protect against attacks, malware and botnets, no matter where they connect and communicate.

New Product Offerings:

* **Cisco Security Cloud Services:** This unique approach for delivering security as a service ties together services from multiple networks and applications, bringing together the cloud and the enterprise network for highly secure collaborative communications. The Cisco Security Cloud supports the recently announced Cisco IronPort® [Hosted Email Security Services](http://newsroom.cisco.com/dlls/2009/prod_030309.html) as well as Global Correlation, a powerful new technique that powers security services integrated into Cisco’s broad range of security offerings.
* **Cisco IPS Sensor Software Version 7.0:** Global Correlation for intrusion prevention system (IPS) harnesses the power of Cisco Security Intelligence Operations, a powerful threat-defense ecosystem, to achieve unprecedented threat-protection efficacy. Cisco turns global threat data captured from a massive footprint of security devices into dynamic updates and actionable intelligence, such as “reputation” scores, and pushes that intelligence out to a business’s network security infrastructure for protective action. By incorporating Global Correlation, Cisco IPS 7.0 is up to two times as effective in stopping malicious attacks, in a shorter amount of time, than traditional signature-only IPS technologies.
* **Cisco ASA 5500 Series 8.2 Software:** This offering in the Cisco Adaptive Security Appliances family is designed to enhance end-to-end security for offices of all sizes, improving threat mitigation and enabling companies to more securely connect, communicate and conduct business. With a new Botnet Traffic Filter for identifying infected clients, IPS availability for small offices, and increased clientless remote-access capabilities, Cisco now offers support for the widest range of platforms, operating systems and endpoints in the industry.
* **Cisco ASA Botnet Traffic Filter:** The new Botnet Traffic Filter enables Cisco ASA 5500 Series appliances to more accurately identify infected clients using information from Cisco Security Intelligence Operations: – more than 1,000 threat-collection servers that receive information from more than 700,000 sensors and 500 third-party feeds. With improved threat intelligence, customers can more accurately identify infected clients and streamline their operations so that security administrators can focus on the most challenging threats.
* **Cisco Remote Access and VPN Enhancements:** Cisco ASA Software Release 8.2 expands remote access capabilities with next-generation tunneling and session persistence through Cisco AnyConnect Essentials for corporate and mobile users, thus covering the widest range of platforms, operating systems, and endpoints in the industry. Support for the Cisco Virtual Office solution has also been added to the Cisco ASR 1000, allowing this wide-area network aggregation platform to also act as the head-end device for Cisco Virtual Office deployments capable of supporting several thousand remote clients. The Cisco ASR 1000 also now supports GET VPN, allowing instant provisioning of security services and delivering high-performance, highly secure any-to-any connectivity for up to 10,000 Internet Protocol Security (IPsec) tunnels at up to 7 gigabits per second of throughput, enabling customers to prioritize and deliver data flows efficiently to multiple network addresses.
* [**Cisco SAFE**](http://www.cisco.com/go/safe)**:** A security reference architecture that provides prescriptive validated design guides to help organizations plan, design and deploy security solutions across the network, such as campus offices, the Internet edge, branches and data centers. These blueprints provide defense-in-depth guidance and best practices for securing data and transactions as they traverse the network.
* [**Cisco Information Technology Governance, Risk Management, and Compliance (IT GRC) Security Assessment Services**](http://www.cisco.com/go/services/security): These services help organizations establish a single program for reducing information security risk and the cost of compliance, by aligning business and technology strategies. Businesses are better able to balance the need for collaboration and information sharing with privacy and information control and to manage disparate security and compliance programs that often lead to inefficiency, duplicated effort, coverage gaps and higher costs. With the Cisco IT GRC Security Assessment Services, organizations can establish a common control framework: a single, unified set of security controls that efficiently meet compliance obligations and protect organizations from threats. The services provide a comprehensive assessment of a business’s security policies and security architecture and map them against the requirements of the common control framework to identify gaps and make prioritized recommendations for resolving those gaps.