INFORMATION PRESSE

Cisco France
Véronique Jaffro – vejaffro@cisco.com
Tel : 01 58 04 31 90

Hill & Knowlton
Caroline Langlais – caroline.langlais@hillandknowlton.com
Tel : 01 41 05 44 48 / 23

Cisco élargit son architecture de sécurité Self-Defending Network, renforçant son expertise en gestion des risques informatiques

- A l'occasion du Cisco Partner Summit 2008, Cisco a présenté de nombreuses innovations apportées à son offre Self-Defending Network, solution globale de gestion des risques informatiques.

- Ces améliorations concernent les domaines suivants :

  - la sécurité du réseau, à travers la simplification de la gestion de sa gamme IPS (Intrusion Prevention Systems) et la version 4.0 du Firewall Service Module, firewall hautes performances intégré au Catalyst 6500
  - la sécurité des terminaux, avec le logiciel de sécurisation des postes de travail Cisco Security Agent version 6.0
  - la sécurité des applications, grâce au Web Application Firewall
  - la sécurité des contenus, par le biais d'une amélioration dans l'IOS de son filtrage web et d'une nouvelle protection SIP, assurant une sécurité des communications vocales
  - et la gestion de la sécurité, caractérisée par Cisco Security Monitoring Analysis Response System 6.0, solution assurant une gestion en temps réel des incidents de sécurité, et Cisco Security Manager 3.2, qui centralise le travail administratif afférent au déploiement des solutions de sécurité Cisco.

#####

Cisco Expands Self-Defending Network, Strengthens Its Role In IT Risk Management for Security and Compliance

Enhancements to Endpoint Defense, Firewalls, Intrusion Prevention, Router Security, And Security Management Bolster Network, Endpoint, Application, And Content Protection

SAN JOSE, Calif. – April 8, 2008 – With a focus aimed squarely on meeting customers' growing corporate IT risk management needs for security and compliance, Cisco today announced a number of enhancements across its portfolio that evolve the company's Self-Defending Network solution from network security offerings into a broader systems approach that strengthens the overall protection of networks as well as the increasingly diverse number of endpoints, applications, and content that utilize them.

Cisco's security enhancements strengthen the ability of businesses to protect their IT infrastructures against malware and address security requirements like data loss prevention, corporate policy compliance, and regulatory compliance. As networks become platforms for more and more devices, applications, and information, protecting the whole system becomes imperative. Today's announcement features endpoint protection, intrusion prevention, network- and application-based firewalls, security monitoring and analysis, centralized policy management, and other software and hardware enhancements that further that cause. These include Cisco Security Agent 6.0, Cisco Intrusion Prevention System 6.1, Cisco Security Monitoring Analysis Response System 6.0, Cisco Security Manager 3.2, incorporation of Web filtering into Cisco Integrated Services Routers, an upgrade to the Cisco Firewall Services Module for switches, and new features for Cisco's Web application firewall and voice-aware Cisco IOS® Firewall.

"Cisco security leads the industry because we are able to offer our customers solutions that include best-of-breed technologies that go beyond point products and work as a complete system," said Scott Weiss, vice president and general manager of the Security Technology Group at Cisco. "In keeping with this philosophy, today we are announcing a variety of products and capabilities that enhance our systems based security, as well as new innovations that push the boundaries of security visibility and manageability. Cisco is deeply committed to security and will continue to invest heavily to continue furthering our leadership position."

Details of Cisco's latest product enhancements include:

Network Security

- **Intrusion Prevention Systems:** Cisco is tailoring its IPS portfolio for businesses of all sizes by simplifying its management. Cisco IPS 6.1 provides deeper insight into

network health and features Cisco IPS Manager Express, a new, all-in-one application for IPS provisioning, monitoring, and reporting. In addition to the software enhancements, Cisco is delivering a new IPS module for Adaptive Security Appliance products that provides performance up to 650 megabits per second and services that help protect unified communications (data, voice and video), improve detection of peer-to-peer threats and enhance Microsoft vulnerability protection.

- **Cisco Firewall Service Module 4.0 (for switches):** Cisco FWSM 4.0 accelerates the highly secure information delivery of high-volume traffic, such as large data backups or bulk data transfers. It features trusted flow acceleration, which enables trusted hosts to exchange information at as much as 20 to 50 gigabits per second.
- **Virtual Private Networking:** Cisco is incorporating its Group Encrypted Transport Virtual Private Network (GET VPN) technology into the Cisco 7200 VPN Services Adapter, generating performance improvements of as much as 300 percent. GET VPN represents a new category of VPNs designed to encrypt data transmitted across wide-area networks. It helps eliminate the need for point-to-point tunnels, allowing distributed branch networks to scale enterprise VPNs to several thousand sites while simultaneously supporting network intelligence needs that are critical to ensuring voice and video quality, such as quality of service, routing and multicasting. Because GET VPN's primary application runs over networks based on Multiprotocol Label Switching, GET VPN's inherent flexibility allows security-conscious businesses to manage their own network protection over a service provider's WAN service or offload encryption services to their providers.

Endpoint Security

- **Cisco Security Agent 6.0:** Cisco Security Agent is a software agent designed to secure endpoint devices such as servers and laptops. It helps identify threats and controls access to sensitive information. Version 6.0 marks the industry's first endpoint security offering that integrates day-zero attack defense, data-loss prevention, and signature-based antivirus detection into a single manageable agent. It incorporates automatic antivirus signature updates with no incremental licensing cost. The unique combination of these functions helps businesses protect themselves from persistent and emerging threats and enforce acceptable-use and compliance policies.

Application Security

- **Web Application Firewall:** This firewall addresses security challenges associated with Web 2.0 and social networking applications by protecting sensitive customer and corporate information within Web applications. Available as a standalone appliance or integrated into the Cisco Application Control Engine (ACE) XML Gateway, the full-proxy firewall controls access to applications, inspects HTML and XML Web traffic, identifies attack patterns, and strengthens a business's ability to address PCI compliance mandates for Web security.

Content Security

- **Content filtering:** Cisco is enriching security services offered via Cisco Integrated Services Routers, of which almost 4 million have been deployed, by adding content filtering from Trend Micro. This addition helps businesses protect users from accessing Web sites that are known sources of malware, control access to inappropriate content, and enforce acceptable Internet-use policies.
- **SIP Protection for Secure Unified Communications:** A useful addition to the security portfolio, the added Session Initiation Protocol protection enriches Cisco's IOS Firewall feature set with voice security. This protection helps businesses embrace a distributed enterprise by improving productivity while minimizing voice security concerns.

Security Management

- **Cisco Security Monitoring Analysis Response System 6.0:** Cisco Security MARS provides real-time visibility into security operations. It identifies threats by aggregating security information from Cisco and non-Cisco devices and determining the appropriate actions to mitigate attacks. Cisco Security MARS also provides reporting across the range of data collected to support regulatory compliance efforts. Version 6.0 adds a new device-support development framework that enables users or third parties to incorporate non-Cisco devices within a Cisco Security MARS deployment, accelerating IT's ability to manage security intelligence across a corporate network, even on devices that Cisco Security MARS does not natively support today. The new version of Cisco Security MARS makes it the first security

management appliance capable of accepting logs in syslog and Cisco NetFlow version 9 format from high-output devices like the Cisco ASA 5580 Adaptive Security Appliance and Cisco ASR 1000 Series Aggregation Services Routers.

- **Cisco Security Manager 3.2:** Cisco Security Manager manages enterprise-wide security in an efficient manner by centralizing the administrative task of configuring policies and controls for Cisco security deployments. Version 3.2 helps improve operational efficiency, significantly reduce troubleshooting times, and simplify IPS signature management. This is achieved through tighter integration and collaboration with security event data from Cisco Security MARS. Cisco Security Manager 3.2 further extends the value of the Self-Defending Network by broadening support of desktop and wiring-closet switches and the Cisco ASA 5580 Adaptive Security Appliance.

The Cisco systems-based approach is taking root at Coastal Federal Credit Union, a Raleigh, N.C., institution that manages nearly $2 billion in assets for more than 172,000 members. The Carolinas' second-largest credit union relies on Cisco products as pivotal parts of its security infrastructure. Together, the security products provide comprehensive network, application and content security for the credit union's communications infrastructure; in the process, they help address corporate security, risk management and compliance requirements.

"It's about protecting your company, its assets, and its employees," said Chris Whitesock, information security officer for Coastal Federal Credit Union. "Protecting our network is fundamental, but protecting all the data that is stored and transmitted across that network is just as important. We put a lot of time and effort into finding solutions that would fulfill our vision for comprehensive data security and believe in Cisco's Self-Defending Network solution strategy as a way to bring that vision to life."

For more information on Cisco security products and solutions, visit **www.cisco.com/go/security**.

About Cisco

Cisco, (NASDAQ: CSCO), is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at **http://www.cisco.com**. For ongoing news, please go to **http://newsroom.cisco.com**.

###