Cisco lance la solution DDoS Protection

Grâce à de nouveaux perfectionnements, cette solution aide à la protection des fournisseurs de services et de leurs clients.

Issy les Moulineaux, le 10 juin 2005 – Cisco Systems annonce la disponibilité de la solution Distributed Denial of Service (DDoS) Protection. Conçue sur l’expertise de Cisco dans le développement de services managés, cette solution permet aux fournisseurs de services de fournir une protection DDoS contrôlée à leurs clients.

*****

Security features are an integral part of Cisco IP NGN architecture. At the Service Layer, the DDoS Protection solution enables service providers to deploy network-based security services for added revenue and fulfill the market demands for security with simplicity. At the Operational Layer, this solution also enables service providers to deploy hardening and protection measures to shield their own network infrastructure from DDoS attacks. This permits providers to deliver highly secure, resilient IP services, including VPN, IP voice communications, video and on-line gaming, to their customers, without disruption, in order to meet service-level agreement requirements.

A number of global and regional service providers have found measurable benefits in the Cisco DDoS Protection solution and many, including Sprint, are also finding great value in the managed network component of the solution.

"Cisco has provided leading products and solutions to meet requirements to help ensure reliable and highly secure data services," said Randy Ritter, vice president of product management at Sprint. "Our enterprise customers rely on the Internet to run their businesses. With Sprint's IP Defender service, based on those solutions, we can work to provide them the necessary security to deal with DDoS threats."

DDoS attacks are becoming more prevalent due to readily available attack creation tools, while motivations are becoming increasingly varied and malicious. While DDoS attacks were once primarily the work of hackers who wanted to temporarily take well-known sites offline to get media attention, they are more recently being used as the foundation of elaborate extortion schemes, costing companies millions of dollars.
DDoS attacks against host systems or network infrastructure result in the disruption of service to customers and users. These attacks may limit the ability to access servers and other critical network resources or completely block legitimate network traffic flows, saturating available bandwidth with excessive packet flooding.

The most effective way to mitigate DDoS attacks is to "scrub" the traffic before it reaches the customer premise, preventing malicious traffic from reaching customer networks. Combating these attacks requires a purpose-built, system-level architecture that detects and mitigates these increasingly sophisticated, complex and deceptive attacks.

Unlike other DDoS defense techniques, the Cisco DDoS protection solution is designed to deliver "clean pipes" capabilities that consist of several major functional elements working towards protecting a network from DDoS attacks, including detection, mitigation, and traffic diversion and injection. The Cisco solution's mitigation function aims to accurately distinguish legitimate traffic from malicious traffic destined for mission-critical hosts, filter out malicious traffic, and allow legitimate traffic to pass.

The Cisco DDoS Protection solution features three service deployment models:

- Managed Network DDoS Protection - Enables service providers to offer their customers protection against DDoS attacks on their last-mile connections and internal infrastructure
- Managed Hosting DDoS Protection - Enables hosting providers to help protect their web and other hosting services from DDoS attacks
- Peering Edge DDoS Protection - Works to enable service providers to provide DDoS-free wholesale connections to their ISP customers

Service provider benefits include:

- Ability to protect or "harden" IP service and network infrastructure to enable IP service delivery despite attempted DDoS attacks
- Ability to become a trusted partner that understands security implications to the business
- Enablement of a new revenue stream on top of existing IP VPN service delivery network
- Ability to take advantage of core assets for new service and differentiation
- Ability to build, then grow - providers do not need to make large CAPEX investments to start delivering protection services
Business customer benefits include:

- Proactive, real-time DDoS mitigation, through which the service provider detects attacks in real-time (day-zero) and mitigates the impact on the network rapidly, grounding the attack as it mounts and before network resources are overwhelmed
- Enhanced protection of critical assets in the data center, including web servers, DNS/DHCP servers and other mission-critical elements
- Business continuity assurance through upstream protection that keeps network resources active and usable

The Cisco DDoS protection solution portfolio incorporates new Cisco service modules that further integrate functionality into the infrastructure, along with interoperable, partner-developed products, including:

- The Cisco Traffic Anomaly Detector XT appliance and the new Cisco Traffic Anomaly Detector Service Module for the Cisco 7600 Series Router and Cisco Catalyst® 6500 Series Switch for anomaly detection
- The Cisco Guard XT 5650 appliance and the new Cisco Anomaly Guard Service Module for the Cisco 7600 Series Router and Cisco Catalyst 6500 Series Switch for anomaly mitigation
- Arbor Networks' Peakflow SP option for intelligent traffic and routing analysis and network-wide monitoring and detection

Arbor Networks, a Cisco Technology Developer Program Partner (CTDP), provides a solution that utilizes NetFlow data from Cisco devices for network-wide relational modeling, anomaly detection and intelligent mitigation management that alerts the Cisco Guard in the scrubbing centers.

**Enhancements to Cisco DDoS Protection Solution Elements**

New software for the Cisco Traffic Anomaly Detector XT appliance and the new Cisco Traffic Anomaly Detector Service Module for the Cisco 7600 Series Router and Cisco Catalyst 6500 Series Switch, integral components of the solution delivery, gives business customers added service control and simplifies service deployment for providers. The new release, Anomaly Guard and Detector Release 5.0, enhances the Detector as a customer-premise option for the managed service. While monitoring the network for attacks, the new software continuously "learns" and automatically adjusts the "normal behavior" baseline. It then automatically communicates these changes, along with changes in customer-defined policies to the provider.

This gives business users a level of service control and simplifies providers' operations. The software also eases deployment by independently rerouting traffic to the Guard and automatically activating the appropriate policies for mitigation. It further strengthens protection by automatically extracting content signatures that may be present in attacks for high-performance packet filtering, supplementing the core behavioral-based defenses.

"Security is top of mind for end customers today, and this DDoS Protection solution helps service providers address this critical need in a comprehensive, proven manner," said Mick Scully, vice president of product management for the security technology group at Cisco. "Security is also integral to a provider's ability to deliver all of its services reliably. To address this, Cisco is incorporating unique technologies and solutions throughout our IP Next-Generation Network architecture, helping to secure the very foundation of our service provider customers' businesses."
For more information about the Cisco Distributed Denial of Service (DDoS) Protection solution, please visit the Cisco web site at www.cisco.com/go/cleanpipes and www.cisco.com/go/nfp.

À propos de Cisco Systems

Cisco Systems, Inc. (NASDAQ : CSCO), premier fournisseur mondial de solutions réseaux pour Internet, célèbre cette année 20 ans d'innovation technologique, de position de leader sur son marché et d'engagement citoyen.
