



## **Cisco eleva ad un nuovo livello la Self-Defending Network**

*Nuovi rilasci estendono la sicurezza collaborativa e adattiva sull'intera rete per una protezione più efficiente ed intelligente*

Milano, 9 febbraio 2006 – Cisco ha recentemente annunciato nuove e significative funzionalità per una maggiore collaborazione tra i diversi prodotti e servizi della propria gamma di soluzioni per la sicurezza, rendendo più semplice alle organizzazioni il controllo e il blocco delle minacce alla sicurezza informatica in modo più coordinato e flessibile, razionalizzando la gestione e proteggendo la confidenzialità delle comunicazioni degli utenti remoti.

Tali ampliamenti riguardano i sistemi IPS (Intrusion Prevention Systems), CSA (Cisco Security Agent), CS-MARS (Cisco Security Mitigation Analysis and Response System), CSM (Cisco Security Manager) e SSL VPN (Secure Sockets Layer Virtual Private Network). nel loro complesso, tali ampliamenti danno vita all'evoluzione della Cisco Self-Defending Network – un framework completo che integra diversi prodotti per la sicurezza di rete e dei dispositivi finali all'interno di una soluzione per la sicurezza integrata, collaborativa e adattiva ideale per le organizzazioni di ogni dimensione.

Secondo Mick Scully, Vice President of Product Management della divisione sicurezza di Cisco, il pericolo sempre maggiore di minacce alla sicurezza informatica – sia dal punto di vista dei profitti che dell'impatto sulla produttività – fa sì che il controllo collaborativo delle minacce così come la protezione delle comunicazioni confidenziali sia qualcosa di più di un semplice requisito IT bensì un requisito aziendale mission-critical.

“Poiché le organizzazioni sono sempre più distribuite, gli approcci tradizionali alla sicurezza di rete devono dare la possibilità di adattarsi ai requisiti in evoluzione”, ha commentato Scully. “Le organizzazioni non si possono più affidare a singoli prodotti per la sicurezza. E' necessario unificare i singoli componenti per la sicurezza – dai dispositivi di rete a quelli finali per centralizzare gli strumenti di analisi e gestione – in un sistema integrato per la sicurezza. Tale sistema dovrebbe costantemente coordinare la protezione ovunque si estenda la minaccia. La sicurezza collaborativa permette alle organizzazioni di estendere la disponibilità dei servizi di rete, di condividere le informazioni e migliorare l'efficienza operativa”.

### **Il controllo collaborativo delle minacce: proteggere l'intera rete**

Il portafoglio di soluzioni per la sicurezza di Cisco include (ma non è limitato a) Cisco IPS 6.0, CSA 5.2, CS-MARS 4.3 e CSM 3.1 – quattro soluzioni che permettono di coordinare la visibilità, la protezione di tutta la rete, la gestione semplificata delle policy e la mitigazione dinamica delle minacce in modo da garantire la continuità del business. Queste nuove versioni potenziano l'approccio Cisco alla difesa coordinata, andando oltre la natura isolata di queste

classi di prodotto e stabilendo un legame vitale tra la rete e i propri sistemi finali. Ciò garantisce che tutti i potenziali punti di una rete possano essere protetti in modo coordinato.

Ad esempio, la condivisione delle informazioni tra l'IPS 6.0 e il CSA 5.2 riduce al minimo i falsi positivi e permette alle applicazioni IPS di bloccare le minacce prima che si proliferino. Inoltre, l'IPS 6.0 è caratterizzato dalla funzione di rilevamento adattivo delle anomalie "day zero" e da analisi dei comportamenti che identificano worm, codici maligni e altre attività indesiderate attraverso l'analisi dei profili del traffico di rete e a bordo dei sistemi finali, ed è integrabile con gli scanner di terze parti in modo da arricchire le analisi utilizzate per adottare azioni protettive proattive e mirate. Le altre funzioni adattative includono la capacità di regolare "la valutazione del rischio" in base alla rilevanza degli attacchi per i singoli potenziali bersagli e di implementare eventi e filtri automatizzati che corrispondono a specifici sistemi operativi.

"Il livello di sofisticazione e di coordinamento del Cisco IPS 6.0 fornisce una soluzione intelligente per il controllo delle minacce lungo l'intera azienda e che permette di migliorare la produttività", ha commentato Tami Martin, Intrusion Detection System Engineer di Argonne Labs. "I sistemi collaborativi per la sicurezza permettono alle attività di procedere in modo fluido, indipendentemente dalle minacce esterne. E questo è un pensiero che ci rincuora. In definitiva, Cisco ci fornisce qualcosa che va oltre ai vantaggi produttivi. Cisco ci fornisce vantaggio competitivo, ovvero attività aziendali protette".

Inoltre, la maggiore collaborazione estende il controllo della QoS (qualità of service) e wireless al CSA 5.2. Ad esempio, il CSA 5.2 abilita policy per i dispositivi mobili, come ad esempio i computer portatili, per limitare i metodi e i sistemi mirati ad indentificare i meccanismi di cifratura e le caratteristiche dei sistemi, e per richiedere connessioni VPN protette da postazioni esterne all'ufficio. Insieme, queste nuove policy permettono all'azienda di proteggere maggiormente i lavoratori mobili.

Grazie al forte coordinamento tra l'IPS 6.0 e il CSA 5.2, l'attività relativa alle minacce viene indirizzata al CS-MARS, il quale aggrega le informazioni all'interno di una singola appliance. Essa conduce analisi sofisticata dei comportamenti di rete e, dopo aver identificato il raggio d'azione della minaccia, si coordina con il CSM 3.1, il quale applica i cambiamenti necessari alle policy aziendali.

"Ciò che si ha disposizione è un'eccezionale intelligenza ottenuta dai sistemi e dai dispositivi che parlano tra loro e coordinano la protezione end-to-end", ha continuato Scully. "Ciò permette ai clienti di identificare diverse tipologie di minacce – violazioni alle policy, vulnerabilità, strumentalizzazioni e comportamenti anomali – e semplifica la gestione dei propri sistemi di controllo delle minacce. L'intelligenza collaborativa abilita un controllo semplificato ed efficiente, risultando in risposte immediate alle minacce".

"La collaborazione è il requisito principale della nostra strategia di sicurezza, e l'approccio a livello di sistema perseguito da Cisco alla sicurezza collaborativa è senza precedenti", ha dichiarato Carl Goodman, Information Services Manager di Premier Valley Bank basata in California. "Ci affidiamo alle soluzioni di sicurezza collaborativa di Cisco per coordinare la

protezione in tutta l'azienda. Ci affidiamo al service provider HEIT Consulting quale partner strategico per l'implementazione. Insieme con Cisco e HEIT, siamo in grado di proteggere le nostre attività interne, i nostri clienti ed essere conformi alle normative. In pratica, Cisco e HEIT alleviano lo stress che quotidianamente accumuliamo in termini di sicurezza aziendale”.

### **Gli ampliamenti VPN SSL apportati a Cisco ASA potenziamo la sicurezza degli accessi remoti**

Oltre agli ampliamenti apportati al controllo collaborativo delle minacce, Cisco ha annunciato miglioramenti VPN SSL per il software della famiglia di appliance ASA (Adaptive Security Appliance), la quale offre funzionalità firewall, IPS, anti-malware e VPN integrate. L'ultima versione del software ASA 8.0 è all'avanguardia tra le soluzioni VPN SSL, andando a complementare le soluzioni IPsec di Cisco con funzioni che riducono il TCO legato all'IT anche nel caso in cui l'azienda diventi maggiormente distribuita e i propri utenti più mobile e remoti. Gli aggiornamenti VPN SSL degli ASA includono:

- VPN senza client (SSL) con migliore progettazione del portale d'accesso per un'esperienza utente maggiormente personalizzata, inclusi bookmarks personalizzati, feed RSS e supporto nella localizzazione.
- Client VPN “Any Connect” di nuova generazione, con ampio supporto per i sistemi operativi Microsoft Vista e Windows, MAC OS X e Linux.
- Supporto Cisco AnyConnect Mobile VPN per Windos Mobile 5.0 Pocket PC Edition.
- Accesso di rete ottimizzato per il VoIP (voice over IP) e altri traffici sensibili alla latenza.
- Capacità di creare “smart tunnels” che forniscono accessi alle applicazioni policy-driven senza dover richiedere diritti amministrativi.
- La Certificate Authority (CA) e altre opzioni relative alle credenziali dell'utente semplificano l'autenticazione.
- La mappatura diretta dei membri Windows Active Directory all'accesso VPN semplifica la gestione della sicurezza da parte degli amministratori IT concedendo agli utenti i privilegi VPN appropriati.
- L'estensione della valutazione dei comportamenti regola i permessi VPN degli utenti in modo più efficiente.
- Gestione intuitiva attraverso il CSM 3.1, l'Adaptive Security Device Manager dell'ASA.

“Capgemini mette a disposizione di tutti gli impiegati la conoscenza sviluppata dall'azienda e l'offerta VPN SSL di Cisco ci permette di fornire accesso sicuro alle nostre applicazioni mission-critical a centinaia di consulenti dislocati presso i clienti”, ha commentato Alex Zuiderwijk, Network and Security Manager di Capgemini Olanda. “Anche sui PC gestiti dai clienti dove gli accessi privilegiati sono limitati, siamo in grado di offrire ai consulenti accessi personalizzati alle risorse di rete indispensabili, il tutto in modo sicuro”.

### **Gli ampliamenti ai servizi per la sicurezza del ciclo di vita potenziano le attività di controllo delle minacce**

Cisco Lyfecycle Services ottimizzano i benefici di tali ampliamenti collaborativi supportando i clienti nell'implementazione più efficiente delle soluzioni. Cisco ha introdotto ulteriori

funzionalità alla propria gamma di servizi di sicurezza, incluso il nuovo portale Security Center, Cisco Security IntelliShield Alert Manager Service e Cisco IPS Signature Management Service.

Il portale Security Center offre una fonte di informazione centrale sulle attività attuali legate alla sicurezza così come guide dei prodotti e servizi Cisco per mitigare le minacce. Gli abbonamenti a Cisco IPS Signature forniscono accesso al database Cisco Security IntelliShield Alert Manager per offrire intelligenza agli eventi IPS. Tali ampliamenti, combinati alle funzioni che permettono ai clienti di correlare le firme IPS alle informazioni relative agli alert IntelliShield, permettono di velocizzare la risoluzione di potenziali attacchi. Inoltre, Cisco IPS Signature Management Service semplifica le attività quotidiane dei dispositivi IPS implementando e sintonizzando gli aggiornamenti delle firme nel momento in cui diventano disponibili.

### **Cisco**

*Cisco (NASDAQ:CSCO) è leader mondiale nella fornitura di soluzioni di rete che trasformano il modo con cui le persone comunicano e collaborano. Notizie e informazioni relative alla società ed ai prodotti sono disponibili all'indirizzo <http://www.cisco.com/> Le apparecchiature di Cisco Systems sono fornite in Europa da Cisco Systems International BV, una consociata interamente controllata da Cisco Systems, Inc.*

###

### **Ufficio Stampa**

**Cisco Systems**

Tel: 039/62951

email: [pressit@external.cisco.com](mailto:pressit@external.cisco.com)

Cristina Marcolin

Susanna Ferretti

### **Prima Pagina Comunicazione**

Tel: 02/76.11.83.01

email: [ciscotech@primapagina.it](mailto:ciscotech@primapagina.it)

Marzia Acerbi

Roberta Natalicchio