Self-Defending Network

Visione & Strategia Cisco per la Sicurezza

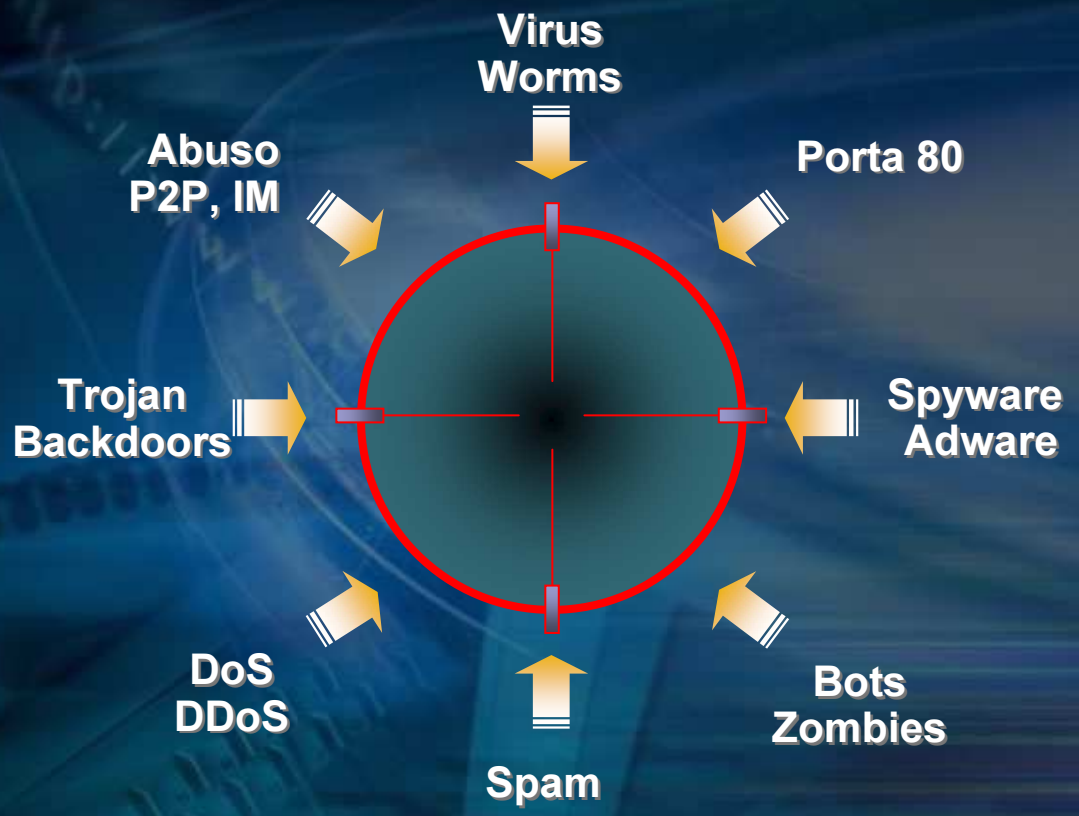
Luca Bertagnolio berta@cisco.com
Business Development Manager, Security

Agenda

- Evoluzioni
- Visione di Cisco
- Self-Defending Network
- Componenti

SICUREZZA: evoluzioni

Evoluzione delle Minacce



Il contenimento di minacce polimorfiche, sofisticate e repentine richiede oggi svariate tecnologie integrate, collaborative e adattative:

- *Vulnerability Signatures*
- *Exploit-specific*
- *Traffic Policy*
- *Traffic Anomaly*
- *Protocol Anomaly*
- *Heuristic - Statistic*

Evoluzione delle Dinamiche

Evoluzione dell'Approccio

PASSATO	PRESENTE
Reattivo	Proattivo/Adattativo
Firewalls/IDS	Sicurezza applicativa
Politiche statiche	Politiche granulari (time/location-based)
Desktop AV/Signatures	Analisi comportamentale
Gestione degli apparati	Correlazione e Mitigazione

Visione di Cisco per la Sicurezza

Fase I - Sicurezza Integrata

Reti Intrinsecamente Sicure

Cosa intendiamo!

Fase I

Protezione dalle Minacce

Difendere la periferia:
- **Integrated Network FW+IPS**

Rilevare e prevenire attacchi dall'esterno

Protezione interna:
- **Switch Integrated Security**

Proteggere contro attacchi dall'interno

Presidiare i sistemi finali:
- **Endpoint Security**

Proteggere host e client dalle minacce

Trust & Identity

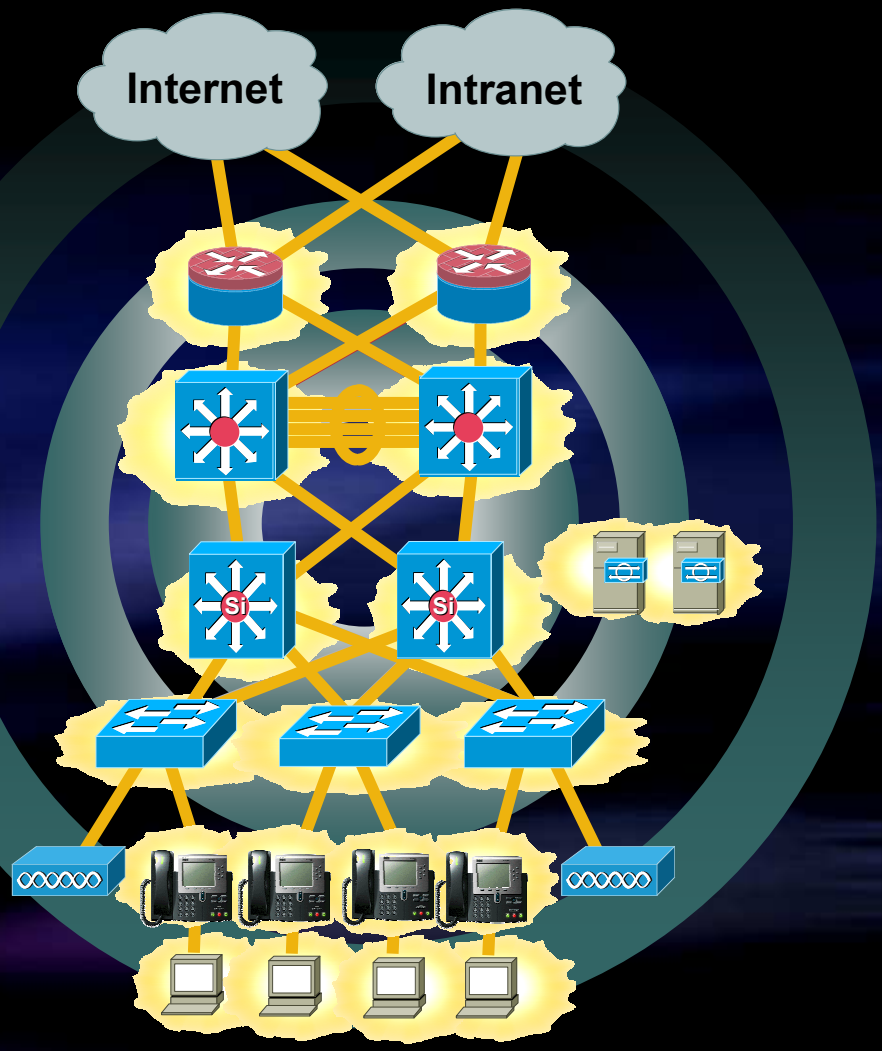
Verifica degli accessi:
- **Identity-Based Networking/NAC**

Controllo di chi/cosa ha accesso

Connett. Sicura

Trasporto Sicuro:
- **IPSec/SSL VPN**

Confidenzialità e integrità di Dati/Voce



Sicurezza Integrata NELLA Rete

Schede integrate

- Firewall
- IPSec VPN
- SSL Termination
- Intrusion Protection
- Network Analysis
- SSL Acceleration
- DDoS Mitigation
- Content Switching

Benefici

- Prestazioni (multi-GB)
- Protezione dell'investimento
- Campus Security
- Gestione Integrata
- Convergenza dei servizi avanzati
- Scalabilità
- Alta affidabilità

Data Center ISR Appliance/Blade Desktop Router

Sicurezza

Firewall, IDS e VPN Appliances

Content & Video

Content Engine / Proxy

Servizi Voce

Connettività Geografica

Router d'Accesso di Filiale

Connettività Locale

LAN Switch & WLAN

Fase II - Sistemi Collaborativi

Dove si annidano le minacce?

Utenti & Sistemi

- Worm e virus *"Zero-day"*
- Spyware
- Utilizzo indebito di applicazioni
- Vulnerabilità delle applicazioni
- Terminali non protetti
- Utenti mobili/remoti
- Complessità oper e

Infrastruttura

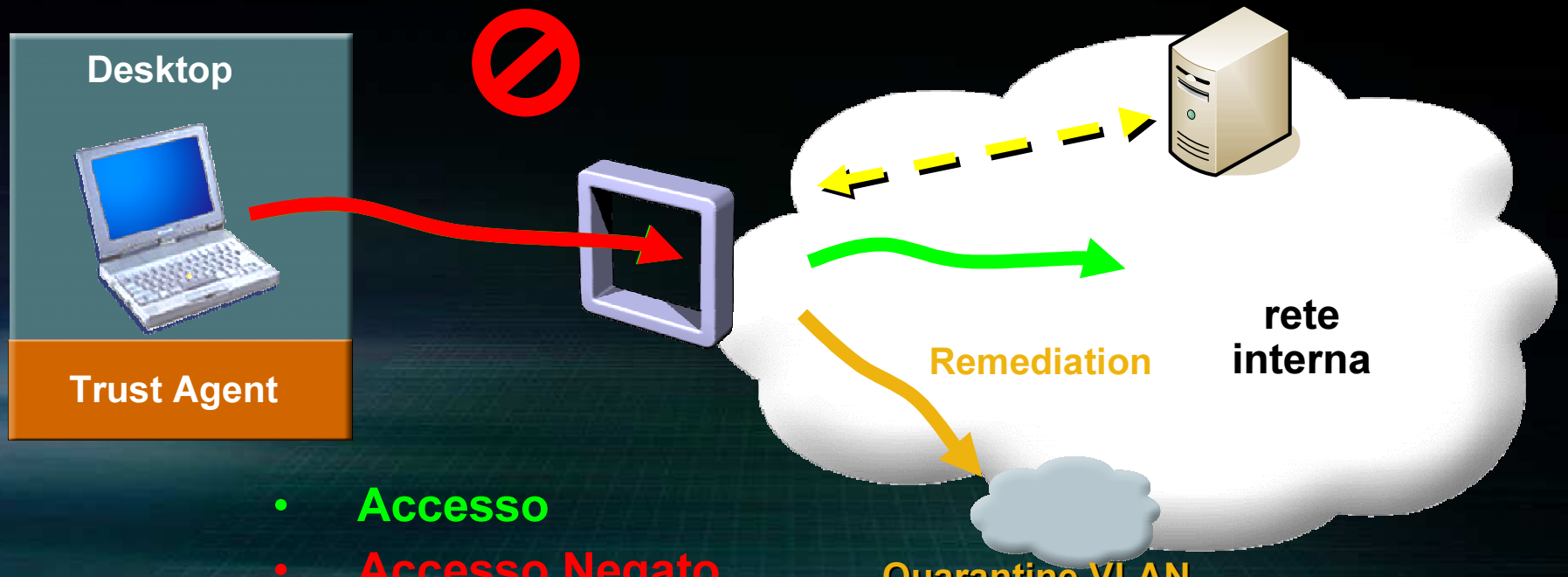
- Traffico di rete indesiderato
- Accesso di utenti non autorizzati
- Alterazione dei protocolli
- Attacchi di tipo *Denial of Service*
- Scanning, reconnaissance
- Abusi attraverso traffico autorizzato
- Propagazione di worm e attacchi distribuiti
- Complessità della Rete
- Minacce dall'interno (*insiders*)

Network Admission Control
Conformità & Controllo

Fase II

Un Client tenta la connessione…

Autenticazione e controllo policy compliance



- Accesso
- Accesso Negato
- Quarantena

Benefici del *Network Admission Control*

Fase II

- **Visibilità e controllo** dei livelli di sicurezza dei client
- Regole di accesso alle risorse basate sulle **Politiche di Sicurezza**
- Politiche di Sicurezza attuate dai dispositivi di accesso alla Rete: **automatismo**, **granularità**, **flessibilità** e **scalabilità**
- **Valorizzazione degli investimenti** esistenti

Fase III - Protezione Adattativa

Cisco *Adaptive Threat Defense* (ATD)

Fase III

Adaptive Threat Defense **(ATD) minimizza i rischi di security indirizzandoli dinamicamente a multipli livelli, con approfondito controllo del *traffico* di rete, *applicazioni*, *utenti*, *sistemi***

- **Correlazione *on box* e identificazione di *meta-eventi* in IPS**
- **Policy che si adattano al luogo e metodo di accesso**
- **Policy basate sui flussi di dati**
- **Contenimento attivo di eventi pericolosi**
- **Mutua nozione tra le diverse funzionalità di Sicurezza e i servizi di Rete**

Protezione Adattativa in azione

Fase III

Controllo Accessi,
Ispezione del Traffico
Servizi Firewall

Ispez. Applicativa, Diritti di Utilizzo, Controllo del Web
Sicurezza Applicativa

Intelligenza Applicativa,
Ispezione dei Contenuti,
Mitigazione di Virus/Worm

Malware, Contenuti, Anomaly Detection
Difese *"Anti-X"*

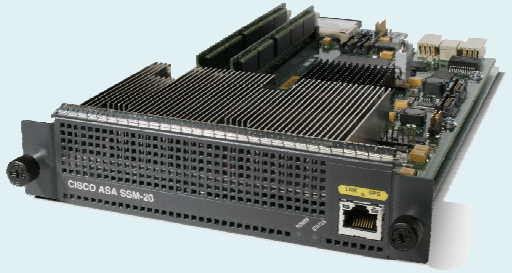
Identità, Virtualizzazione,
QoS, Segmentazione,
Visibilità sul Traffico

Traffic/Admission Control, Risposte Proattive
Contenim. & Controllo

Content Security and Control SSM
New "Anti-X" modules for Cisco ASA

New!

- Delivers industry-leading threat protection and content control at the Internet edge providing comprehensive antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering services
- Built on award-winning antivirus technology from Trend Micro's InterScan security suite
- Complete protection with a comprehensive database of viruses / malware; beyond the limited "in-the-wild" protection



SC Magazine Global Awards 2004 Finalist

Technology & Business Editors Choice

SSPA star award best practices

SCP Support Center Practices Certified

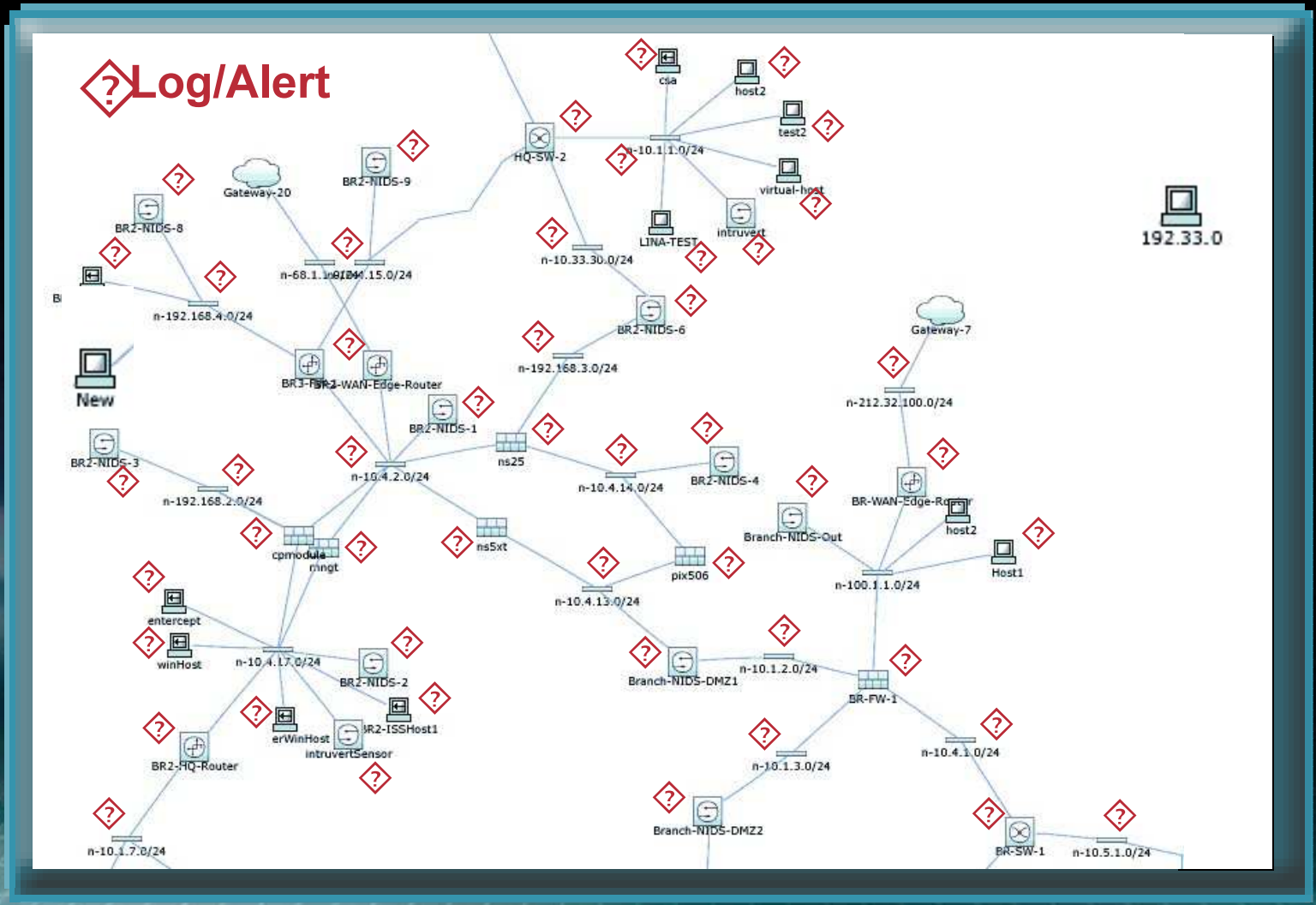
Trend Micro Awards

ICSA labs Certified Antivirus

West Coast Labs Check Mark Spyware

Trend Micro Certifications

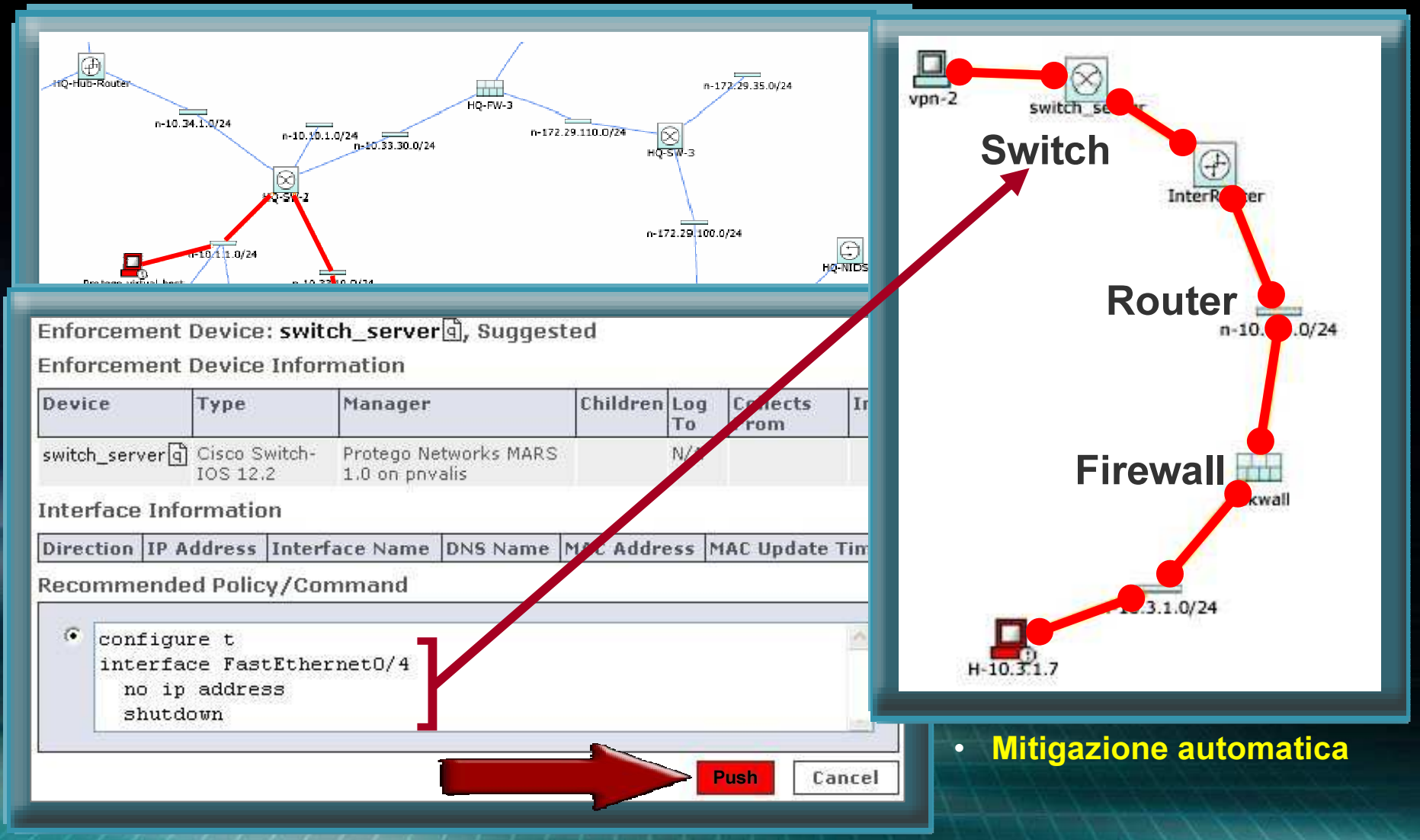
Il Problema: la Complessità



Scoprire l’attacco…

CS-MARS
Protezione Adattativa in azione

Fase III



- **Mitigazione automatica**

Slide 22

BH2 IS SureVector OK? SHOULD IT BE Cisco SureVector? IF SO, NEED TO ADD REGISTERED TM SIGN TO THE WORD Cisco
Admin; 12/02/2005

Cisco Security MARS 4.2

"Multi-Vendor Monitoring and Mitigation"

New!

- **Gain Network Intelligence**

  Topology, Traffic Flow, Netflow Analysis

- **Event Correlation**

  Correlates, reduces and categorizes events

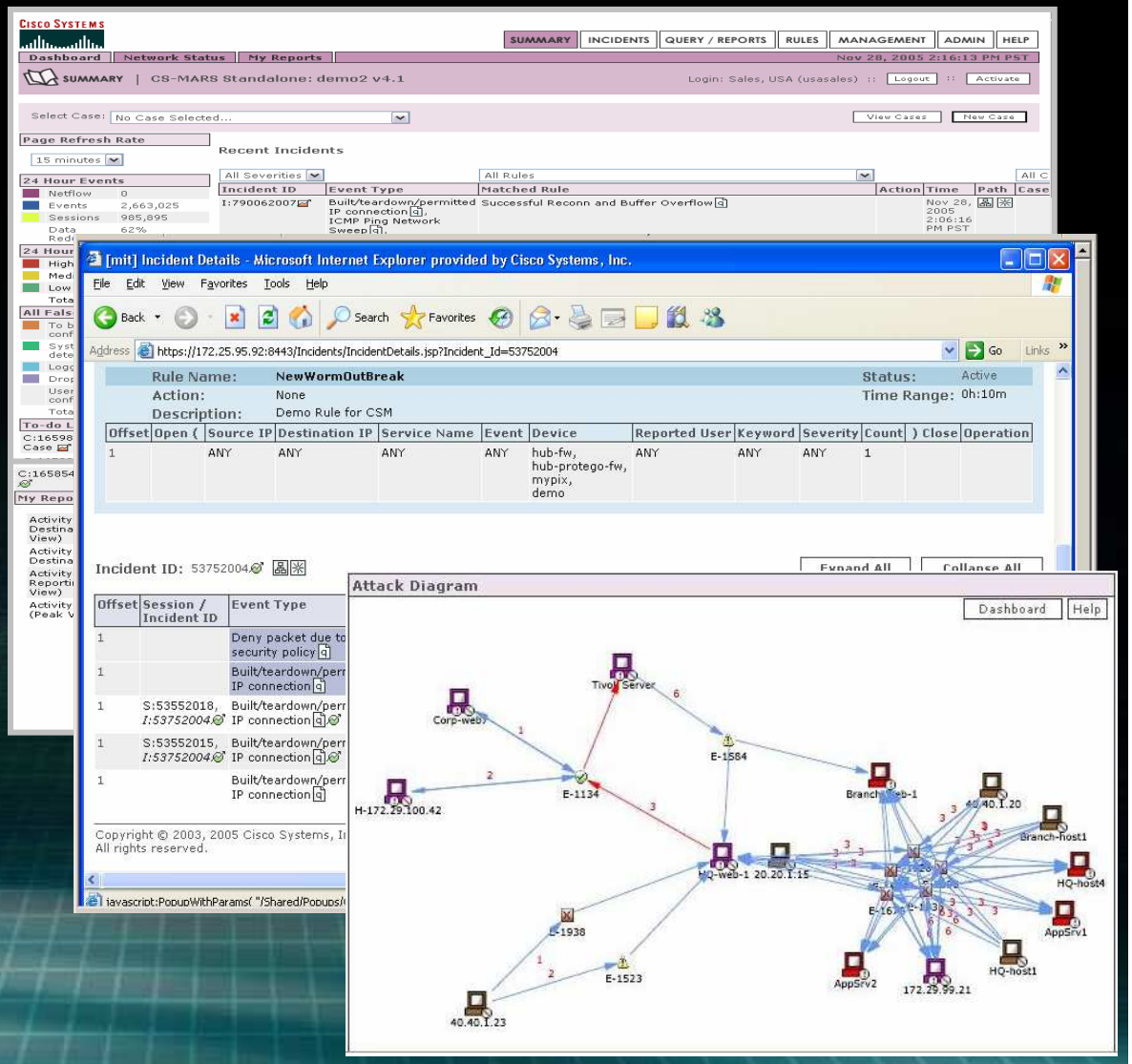
  Validates incidents

  Propose mitigation action

- **Extensive Reporting**
- **Multi-vendor**

Release 4.2 highlights

- Log data to policy lookup
- Low latency, real-time event viewer
- Ticketing system integration via XML Incident Notification



Conclusioni

Sicurezza Cisco

Approccio Globale, Integrato e Sistemico

Servizi IP e Sicurezza nativamente integrati

Protezione degli Investimenti

Luca Bertagnolio
berta@cisco.com

www.cisco.com/go/security