



Firewall UTM con Zero Day Protection

Maggio 2006

Fabrizio.Croce@watchguard.com
tel. +39-335-7030721
skype: fabrizio_croce
msn: fabrizio_croce@hotmail.com

Stronger Security, Simply Done™

WatchGuard®

WatchGuard (Nasdaq WGRD) e' stata fondata nel 1996, con uno scopo in mente, coprire le necessita' di sicurezza del business in crescita con soluzioni costruite intorno a soluzioni di protezione proattiva.

WatchGuard e' leader per la sicurezza per le aziende PMI con la sua linea di prodotti Firebox®, diffuso in piu' di 100 nazioni con piu' di 25.000 Firebox venduti mediamente all'anno.

Il Firebox ha introdotto la prima ed unica appliance pienamente aggiornabile ed integrabile nel mercato.

“

I nostri clienti parlano di noi:

I Prodotti WatchGuard sono eccellenti ed il servizio e' esemplare.

Garth Wertmer, Director of Technology, 9-11 Commission

”

STRONGER SECURITY, SIMPLY DONE

Condizione del Mercato

Le minacce di sicurezza sono in crescita sia in numero che in sofisticazione

- Virus
- Worm auto-propaganti
- Cavalli di troia
- Spyware
- Phishing
- Spam
- Nuove minacce

La complessità del network si sta incrementando

- Estensione del perimetro
- Incremento del Wireless
- Connettività a tempo pieno
- Pressione sui costi
- Gestire di più con le stesse risorse
- Rafforzamento delle politiche di sicurezza

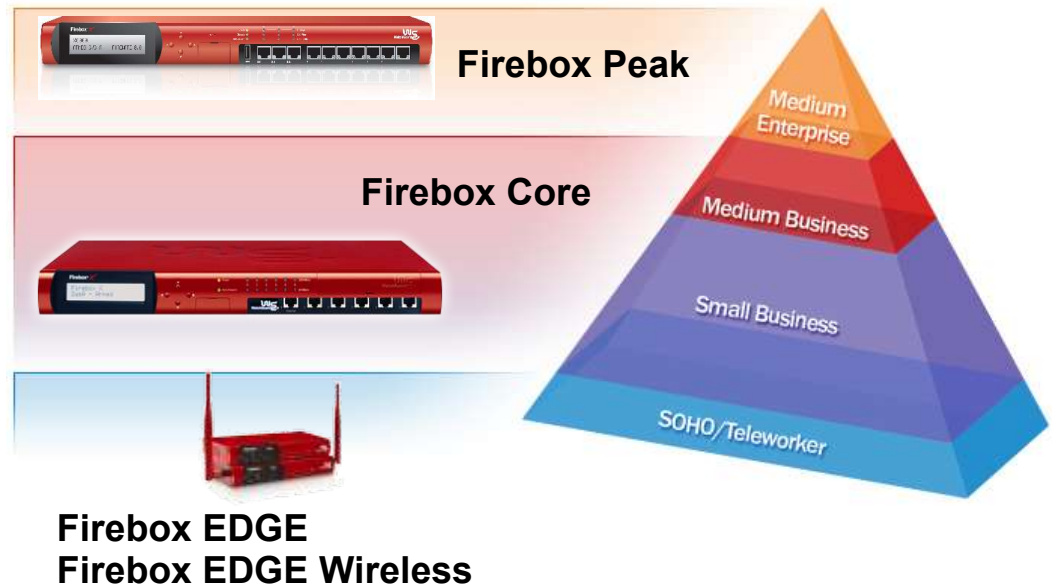
WatchGuard offre una soluzione 'all-in-one' che da maggiore sicurezza con minori sforzi

WatchGuard
Firebox[®] X



WatchGuard Firebox® X

- La famiglia di appliances di sicurezza integrate UTM (Unified Thread Management) **espandibili con chiavi software** per la massima scalarità'.
- Migrazione dei prodotti nella stessa famiglia per incrementarne le prestazioni con chiave software **senza sostituire hardware**.
- Nessuna licenza basata su numero di utenti ma per livello di apparato



Che cos'e' UTM?

Unified Threat Management

- Anti –spam, Anti – Virus, Intrusion Prevention, Web surfing control (integrato in una appliance firewall/VPN)
- Singola appliance (integrated security gateway)
- Facile da gestire (single user interface)
- Ridotti costi di proprieta'
- Servizi basati su Signatures (aggiornamenti basati su minacce conosciute)
- La competizione e' sulla velocita' di spedizione delle signatures

Che cosa NON e' quindi una UTM? Protezione Real Time!

Watchguard UTM: Signature based e Real time

Signature based



Real time

(Soluzione UTM)

- GAV/IPS (Instant messaging/P2P + Spyware)
- WebBlocker (Surfcontrol – Blocco IM/P2P, Categorie incrementate a 40)
- SpamBlocker (Commtouch, 97% spam bloccato 0.5% falsi positivi)
- Basato su Signatures che necessitano continui aggiornamenti lasciando finestre di vulnerabilita'

(Deep Application Layer Filters)

- I filtri Real Time di Watchguard bloccano il 90% delle minacce (senza bisogno di aggiornamenti) – SOBER, BAGEL, KAMASUTRA, SPYWARE (tutti bloccati senza signatures!)
- Filtra Web (HTTP), email (SMTP), file transfers (FTP) e (DNS)

SOLUZIONE COMBINATA PER LE MINACCE ODIERNE

Signature Based

Servizi di Sicurezza "Signature Based"

Attacchi basati sui contenuti

Troiani contenuti I file utilizzati per lavoro
Buffer overflow
Cross-site scripting attacks
Iniezioni SQL
Iniezioni HTML
Esecuzione di codice da remoto
Elevazione di privilegi
Protocol command decoding

Tentativi di login sospetti
Web messenger attivita'/traffico
P2P attivita'/traffico
Virus in file utilizzati per lavoro (i.e., .PDFs, .DOCs, etc.)
Iniezioni HTML da URL maligne
Spyware

Intelligent Layered Security

Protezione "Real Time"

Attacchi basati sui contenuti

Fingerprinting
Anomalie di protocollo
Pacchetti Malformati
Attacchamenti sospetti
Codici Active X maligni
Spyware/Adware

Attacchi sulla connessione

SynFlood
DoS, DDoS
Buffer overflows
Attacchi con la frammentazione

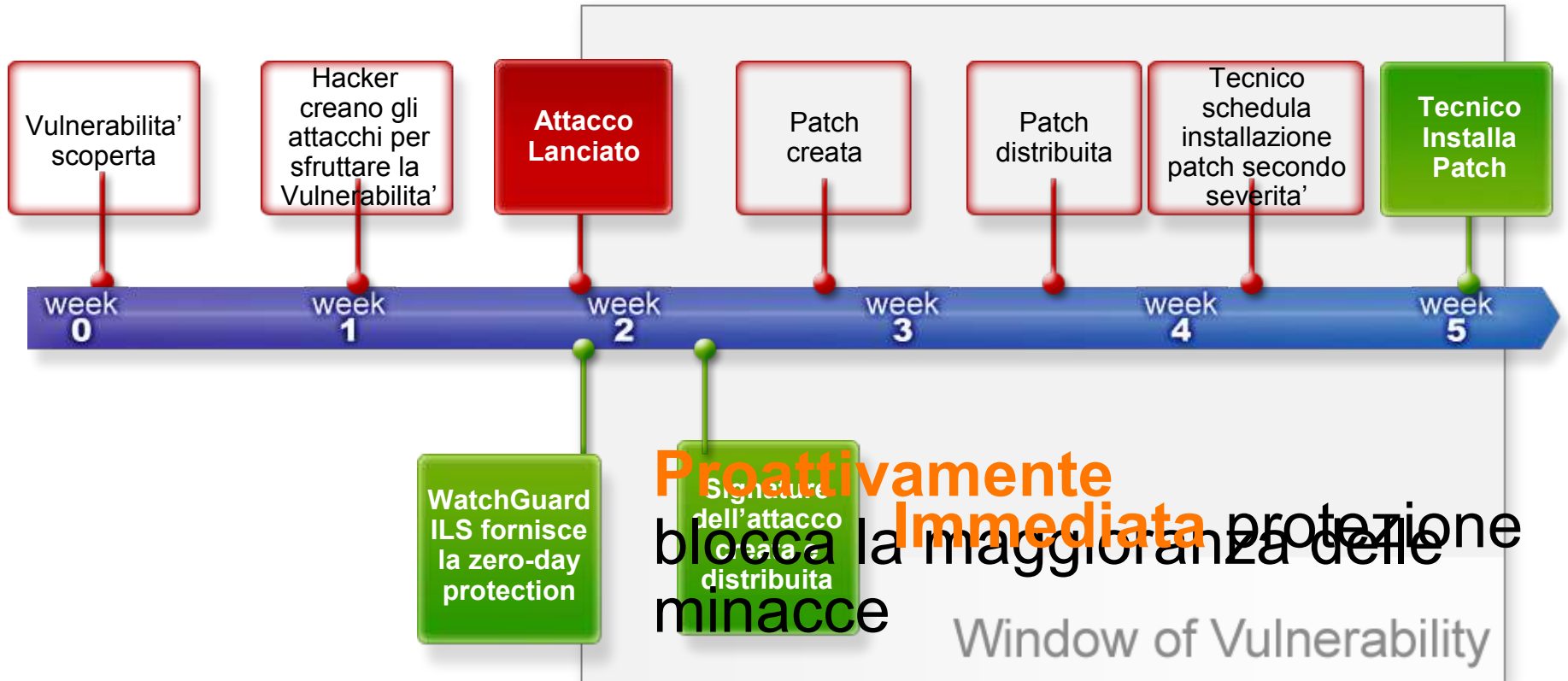
Attacchi su comportamenti (behaviour)

Port-Scans
Scan di Indirizzi
Attacchi di Spoofing

Attacchi basati su policy

TCP hijacking
State-based attacks
ICMP (Ping of Death)

ZERO DAY PROTECTION



Definizione protezione agli attacchi “ZERO-DAY”

“ Zero-day protection semplicemente significa che si e' protetti da una nuova minaccia nel momento in cui esiste. Non 15 minuti dopo ma istantaneamente. Contrasta quindi con i dispositivi che utilizzano solamente le signatures.

- Joel Snyder, *Definition of Zero Day Protection*

“ Per ‘vera’ zero day protection, si intende una soluzione di sicurezza in grado di scoprire e bloccare comportamenti anormali....senza aver bisogno di un database di signatures.

- Juergen, *Esphion Network Disaster Protection*

INTELLIGENT LAYERED SECURITY

Capacita' chiave per la Zero-Day Protection

- **Protocol Anomaly Detection (PAD) – fa osservare gli standard di protocollo**
- **Pattern Matching**
 - Controlla i file ed i tipi mime utilizzati per trasportare malware (i.e. .wmf .exe .pif .scr)
 - Controllo granulare degli attachment per tipo di file o URL
 - Permette download di .exe solo da sorgenti sicure come update Microsoft.com o device drivers da HP
 - Le minacce sono bloccate mentre le operazioni chiave sono permesse
- **Limitazione dei comandi (es FTP SITE)**
- **Cloaking – nasconde le informazioni dei server dagli scan degli hackers**
- **Filtra/Blocca headers**
- **Protegge i Web server dagli attacchi**
 - Inbound HTTP protection

WATCHGUARD®

INTELLIGENT LAYERED SECURITY

Sicurezza a livello applicativo: SICUREZZA PIU' FORTE

WatchGuard ILS proattivamente blocca:

Virus via E-mail al gateway– nella configurazione di default:

- Beagle, Nimda, Sober, My Doom, Bable, Netsky.x, Fizzer, Kamasutra e varianti

Senza Signatures

Top 10 spyware*:

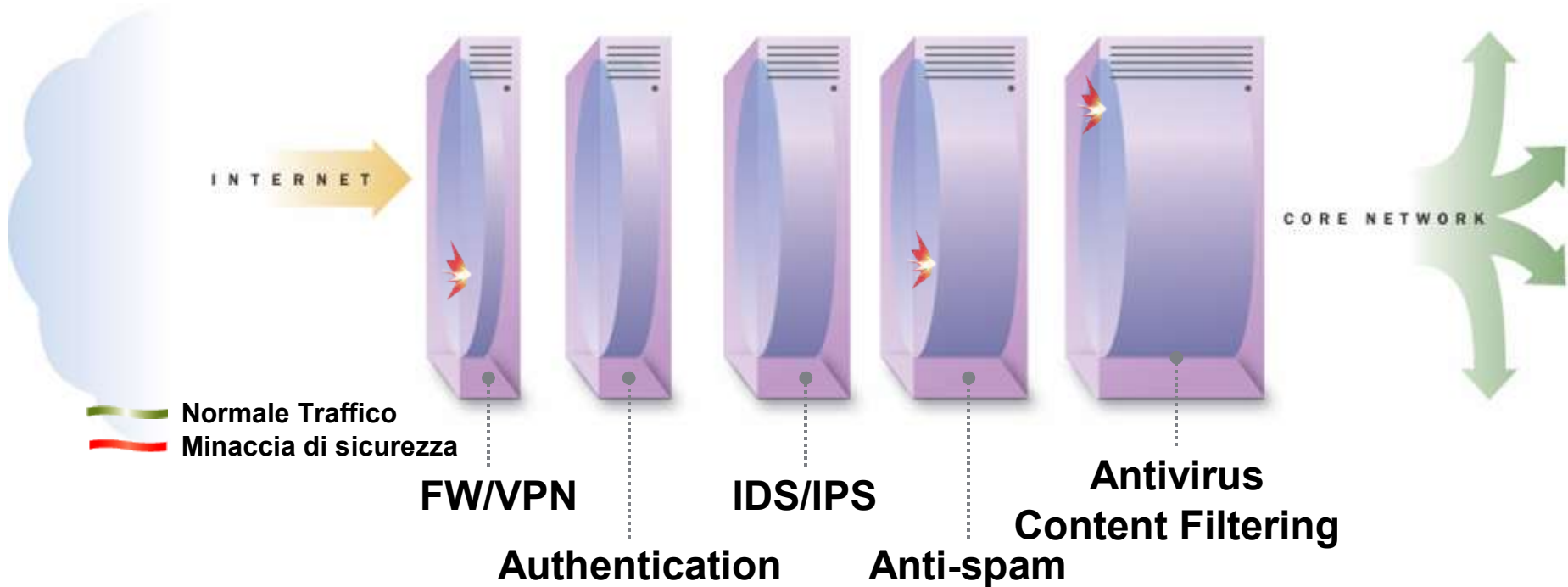
- PurityScan, N-Case, Gator, CoolWebSearch, Transponder, ISTbar, KeenValue, Internet Optimizer, Perfect Keylogger, TIBS Dialer

Senza Signatures

Attacchi al Network non sono conformi allo standard dei protocolli

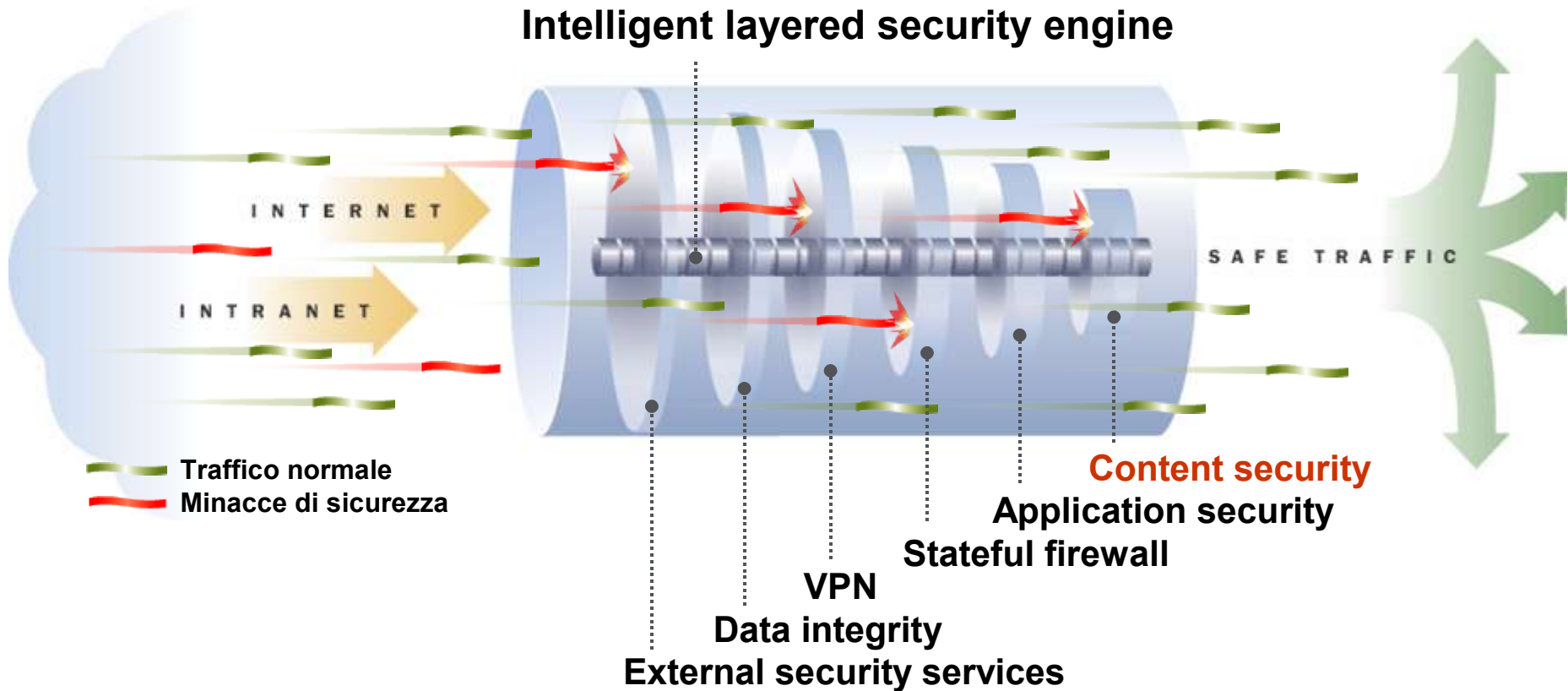
Senza signatures

Architettura Tradizionale



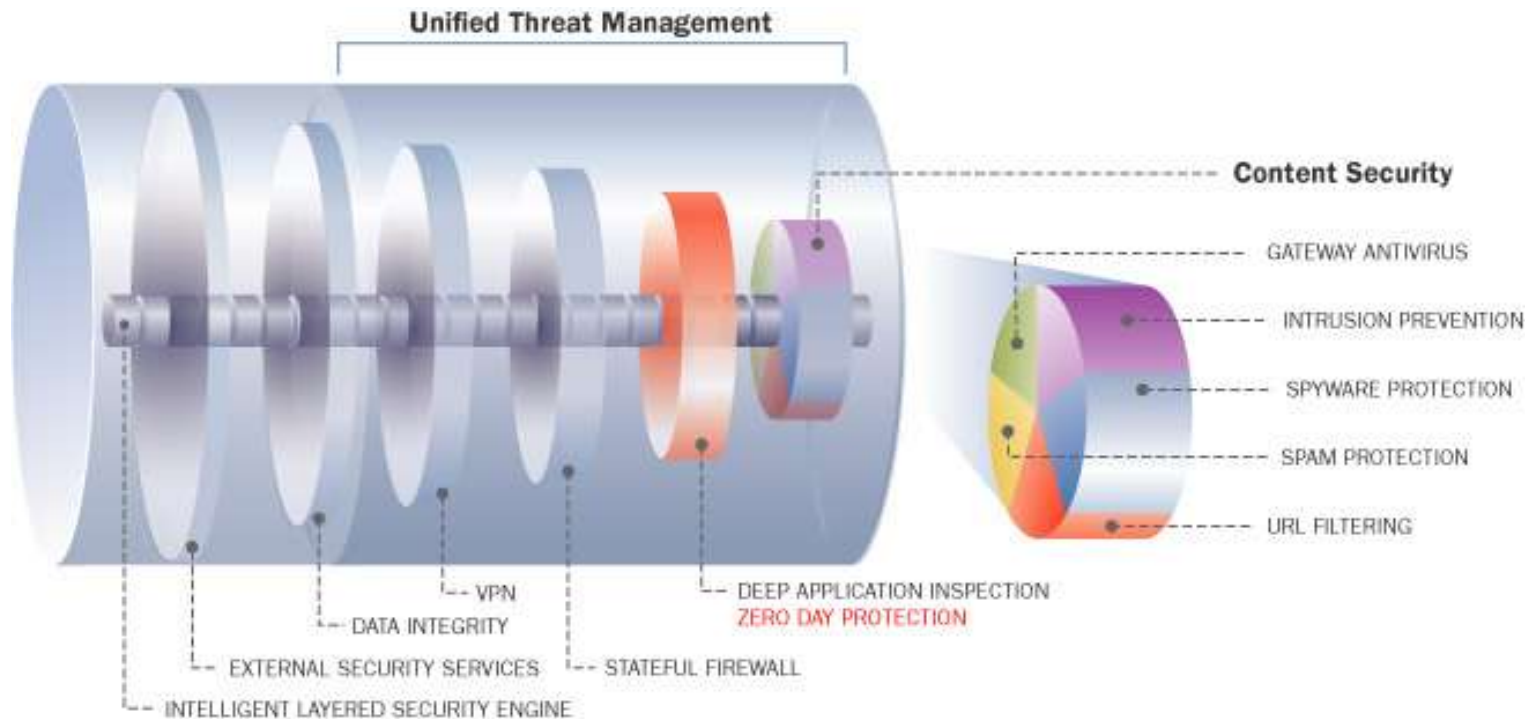
Alto costo/complessità, Limitate performance/protezione

Architettura Intelligent Layered Security™ (ILS)



Costo Inferiore, Alte Prestazioni, Migliore Protezione

SOLUZIONE COMBINATA : ZERO-DAY + ISPEZIONE DEL TRAFFICO



INTELLIGENT LAYERED SECURITY

WatchGuard

Signature-based GAV/IPS

Zero Day Protection

Stateful Packet Inspection
Firewall



Competitor

Signature-based GAV & IPS

Stateful Packet Inspection
Firewall



REAZIONE AGLI ULTIMI ATTACCHI

Data	OS	Attacco	Soluzione WatchGuard	Utenti non protetti
20/4/05	Windows, Mac, Linux	RealPlayer Buffer Overflow – root access	Configure HTTP and SMTP proxies to block all .ram files immediately	SonicWALL, Fortinet NetScreen, Cisco Pix, Zyxel
12/04/05	Windows	Xlsasink.dll Buffer Overflow – critical Exchange vulnerability	Default with Zero-Day Configure policy if needed.	SonicWALL, Fortinet NetScreen, Cisco Pix, Zyxel
22/2/05	Windows	Sober.k and variants	Default with Zero-Day – SMTP proxy blocking .pif files Configure policy if needed. Signature made available within 9 hours	SonicWALL, Fortinet NetScreen, Cisco Pix, Zyxel
14/12/04	Windows	Zafi.d and Variants – worm to gain access for zombie network	Default with Zero-Day – SMTP proxy blocking .pif, .com, .cmd, .bat Configure policy if needed.	SonicWALL, Fortinet NetScreen, Cisco Pix, Zyxel

REAZIONE AGLI ULTIMI ATTACCHI

Data	OS	Attacco	Soluzione WatchGuard	Utenti non protetti
10/1/06	Windows	.tnef vulnerability	Default with Zero-Day – blocking .tnef files in SMTP proxy Configure policy if needed.	SonicWALL, Fortinet NetScreen, Cisco Pix, Zyxel
6/1/06	Windows	.wmf attack – root access	Configure HTTP and SMTP to block .wmf files immediately. Signature made available within 7 days.	SonicWALL, Fortinet NetScreen, Cisco Pix, Zyxel
17/08/05	Windows	Zotob and variants – infectious worm	Default with Zero-Day Configure policy if needed. Signature made available within 9 hours.	SonicWALL, Fortinet NetScreen, Cisco Pix, Zyxel
9/05/05	Window, Mac	iTunes Buffer Overflow – root access	Configure HTTP & SMTP proxies to block .mp4 files immediately Signature made available within 5 days	SonicWALL, Fortinet NetScreen, Cisco Pix, Zyxel



Stronger Security, Simply Done™

Firebox Fireware

FIREBOX Fireware: Il sistema operativo

Funzionalità di Networking e Sicurezza:

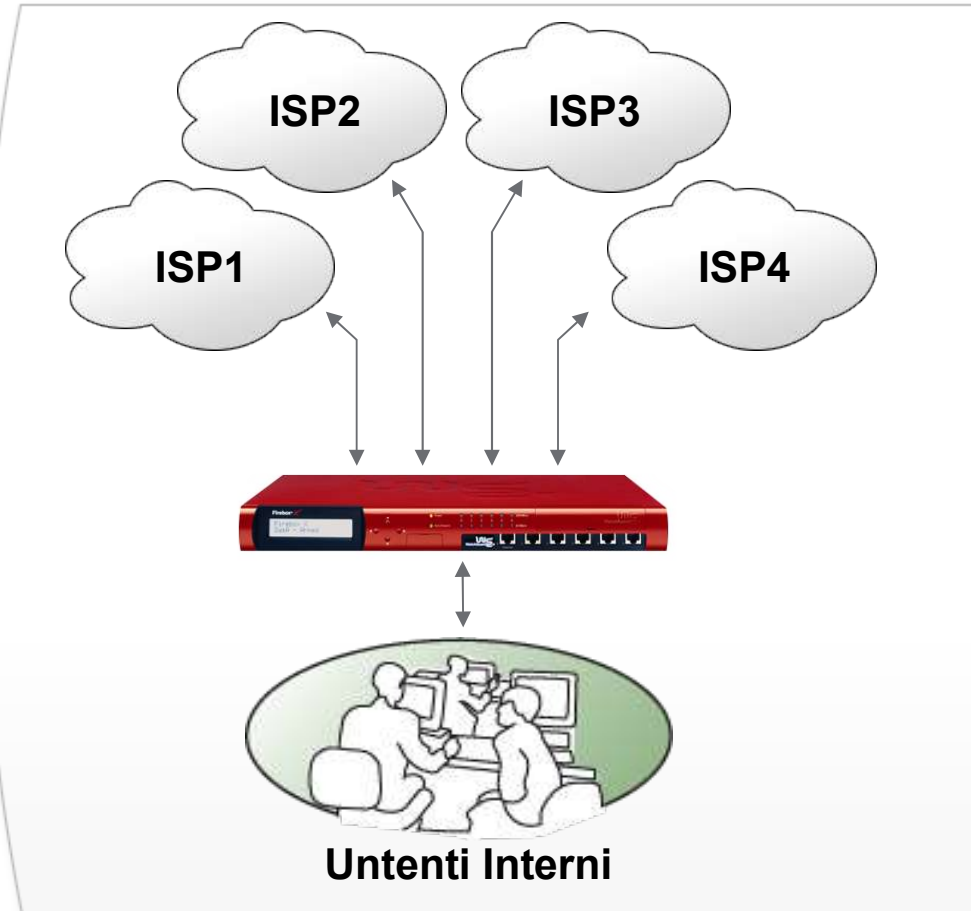
- Firewall/VPN
- Intelligent Layer Security: Sicurezza a livello applicativo
- Multi-WAN Load Sharing / Failover
- Port Independence
- Traffic Management e Quality of Service (QoS)
- High Availability
- Dynamic Routing
- SNMP Support
- Upgradabilità con chiavi software
- Gestione Centralizzata

Servizi di sicurezza opzionali:

- Gateway Antivirus perimetrale
- Web Filtering – Surfcontrol Cybernot
- Spamfiltering

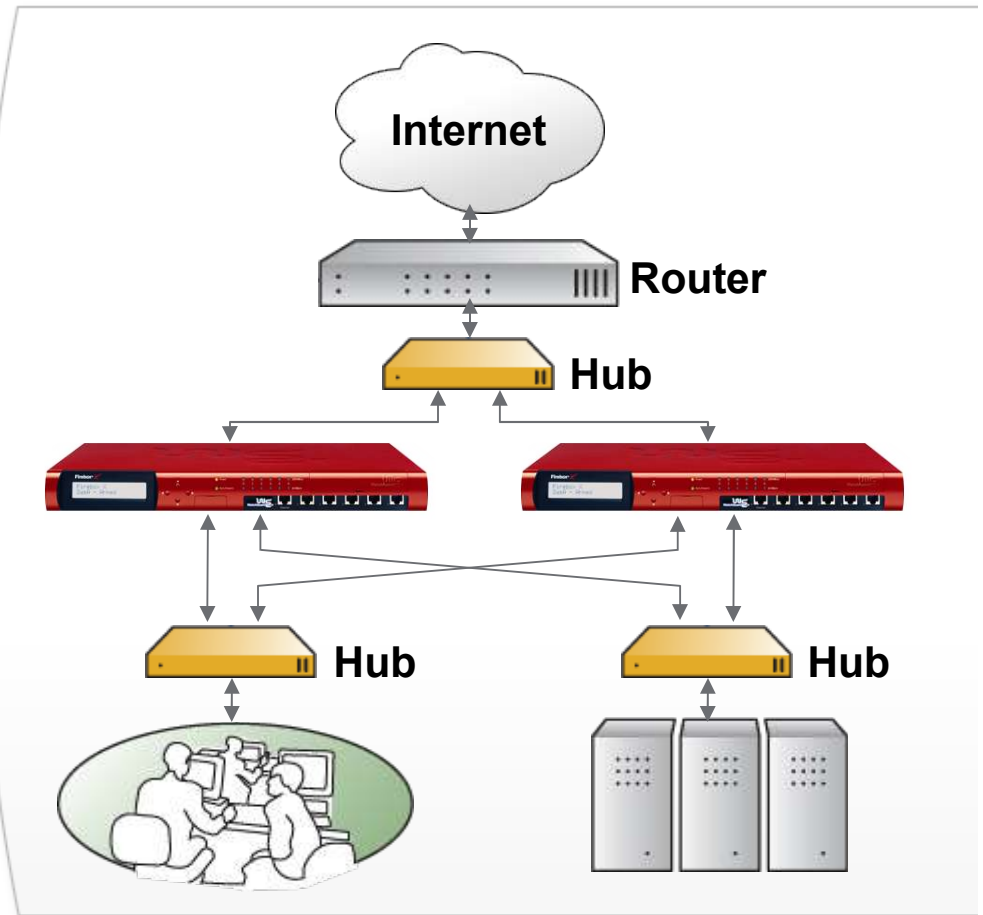
FIREWARE: Multi-WAN Load Sharing / Failover

- Il failover protegge contro l'interruzione di una connessione ISP
- Fino a 4 connessioni ISP "Multi-WAN"
- Round robin load sharing per condividere il traffico su piu' connessioni



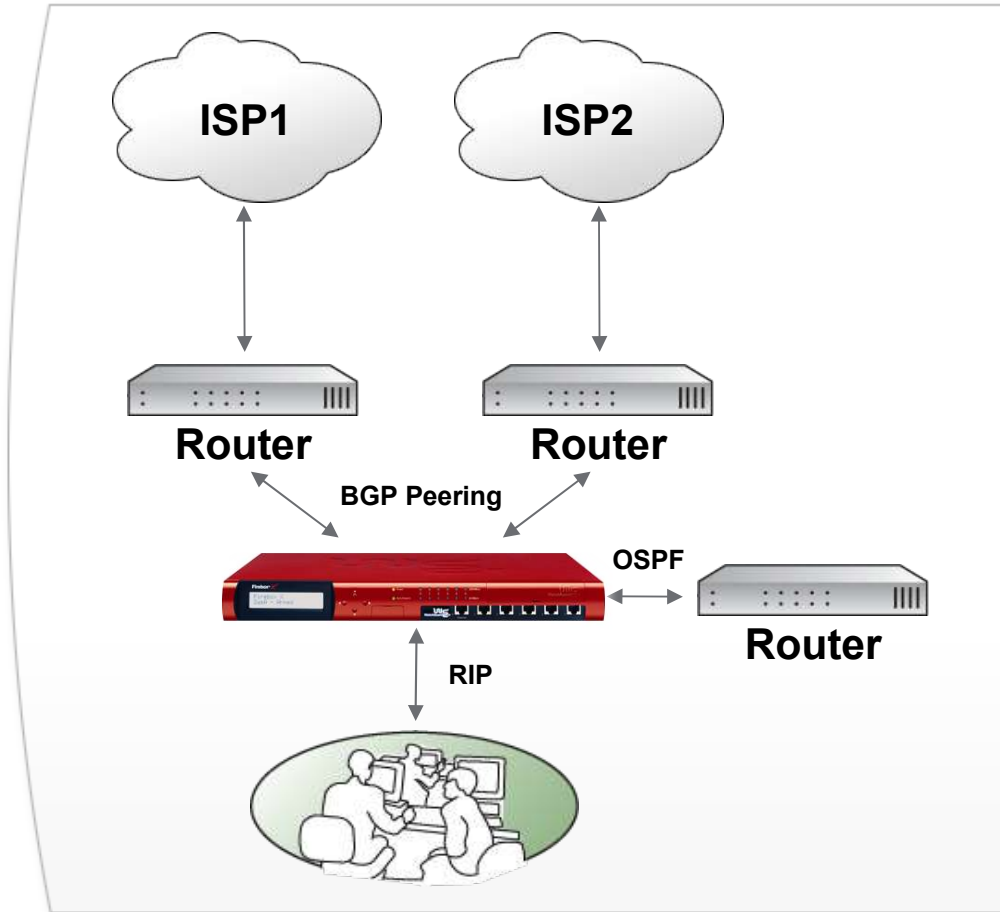
FIREWARE: High Availability (Attiva/Passiva)

- Consente la rindondanza delle appliances per incrementare l'affidabilita'
- Completa sincronizzazione e failover
- Sincronizzazione della configurazione semplifica l'installazione



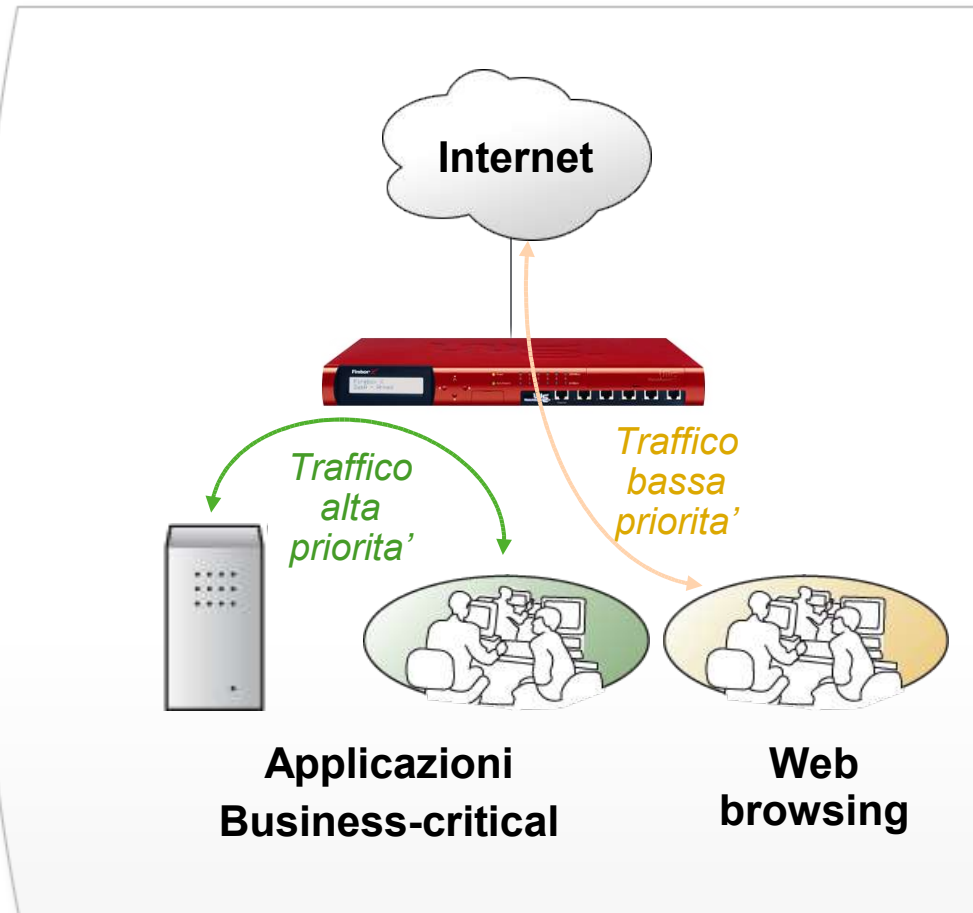
FIREWARE: Dynamic routing

- Supporto per i protocolli di routing BGP4, OSPF, RIPv1,v2
- Dinamicamente aggiorna le routing table
- Incrementa l'affidabilità del network



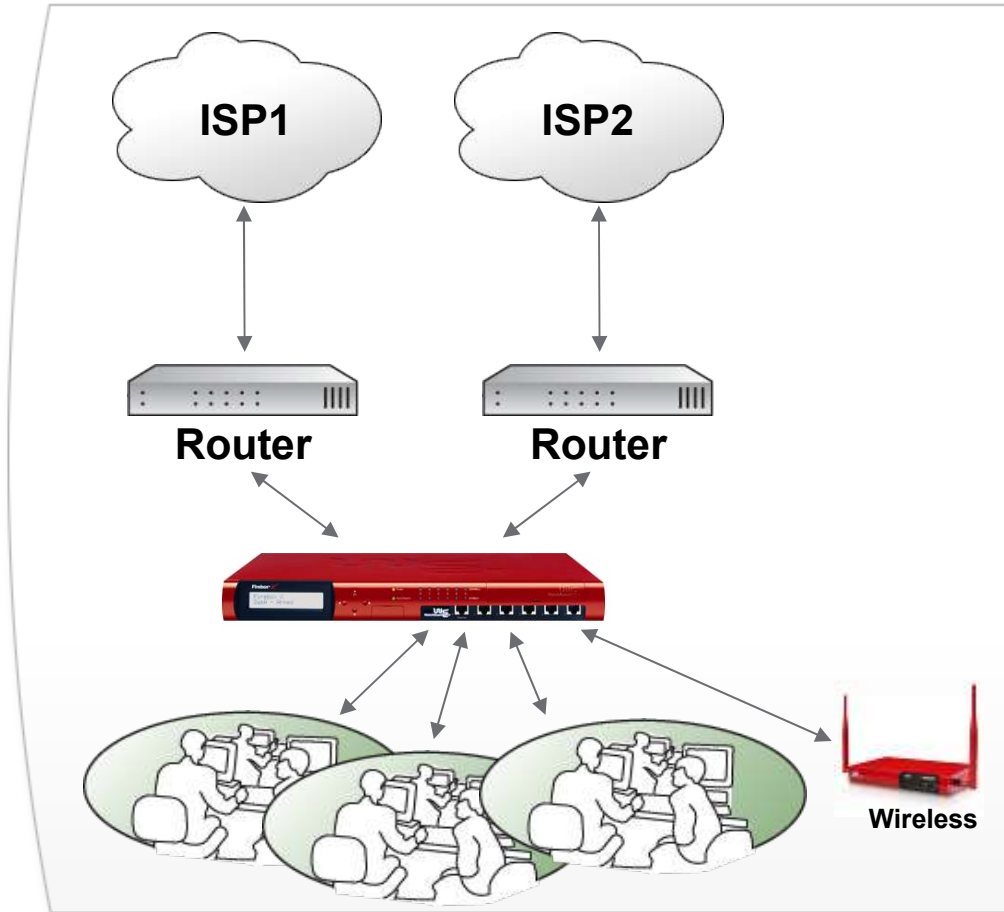
FIREWARE: Traffic Management e QoS

- Assicura la banda necessaria alle applicazioni necessarie
- Permette la prioritá', banda massima e connessioni massime per secondo



FIREWARE: Port Indipendence

- Ognuna delle 6 porte (xcore) o 10 porte (xpeak) puo' essere configurata come DMZ, TRUSTED o EXTERNAL
- Limite 4 porte EXTERNAL
- Incrementa la flessibilita' e la sicurezza



FIREWARE: Gateway Antivirus/IPS

Blocca allegati pericolosi

- Previene l'esecuzione automatica o accidentale di codice pericoloso sui desktop

Piena protezione delle e-mail

- Inbound and outbound SMTP scanning

Protezione Non-stop

- Le nuove signatures automaticamente aggiornate senza interruzioni

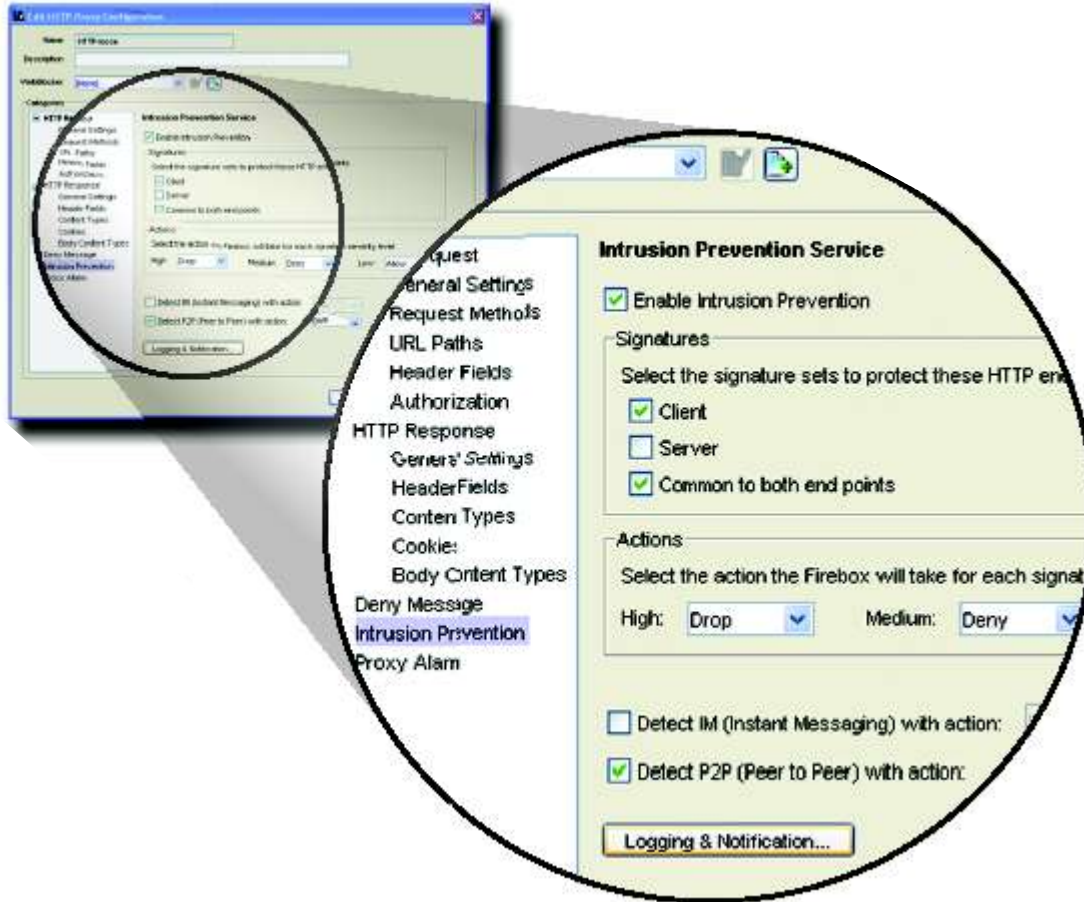
Database robusto ed efficiente

- Signature per piu' di 23,000 virus, spyware, worm e trojan, incluse WildList e zoo virus

Grande supporto di decompressione

- ZIP, RAR 2.0, TAR, GZIP, ARC, e CAB files

FIREWARE: Gateway Antivirus/IPS



- **Signature database ottimizzato:** Riduce i falsi positivi ed aumenta il numero di attacchi rilevati
- **Blocca IM:** Yahoo, IRC e MSN Messenger
- **Blocco P2P:** Napster, Gnutella, Kazaa, Morpheus, BitTorrent, eDonkey2000 e Phatbot
- **Whitelist configurabili**
- **Flessibilità** per applicazioni e destinazioni che richiedono accesso continuativo
- **Modalità** Block, Deny e Allow

FIREWARE: SpamBlocking

Che cos'è:

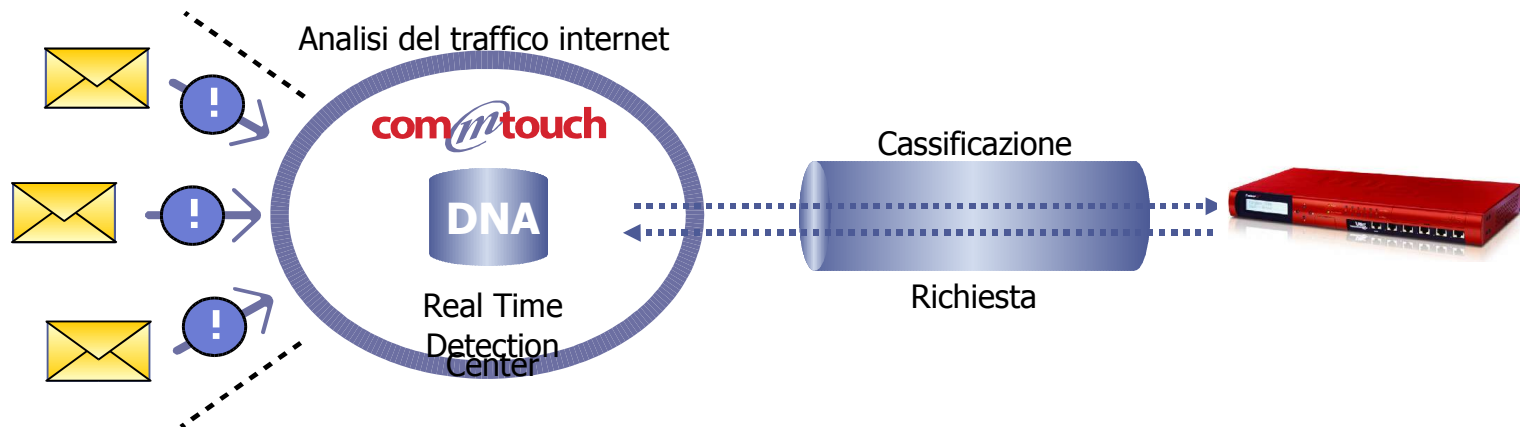
- Spam blocking service per le appliances Firebox con Fireware, In Partnership con Commtouch, un leader per la prevenzione dello spam

Valore:

- E' il migliore servizio di blocco degli attacchi spam in grado di fermare il **97%** delle email non sollecitate con lo 0,5% di falsi positivi
- Il processo avviene al di fuori della appliance quindi l'impatto sulla velocità del dispositivo è minimo

Come funziona:

- Rileva i componenti ripetitivi di ogni epidemia ed identifica in modo univoco il DNA di ogni epidemia
- Paragona i messaggi in arrivo con lo spam DNA in tempo reale



FIREWARE: Webblocker

Partner con SurfControl

PERSONE REALI NEL MONDO

Cercano i siti internet pericolosi, spyware, etc.

+

INTELIGENZA ARTIFICIALE

Traccia cambiamenti URL/IP, NUOVO contenuto e siti ritirati

+

AGGIORNAMENTI INCREMENTALI GIORNALIERI

Veloce e schedulato, utilizza minima banda

=

BLOCCA MINACCE E TRUFFE

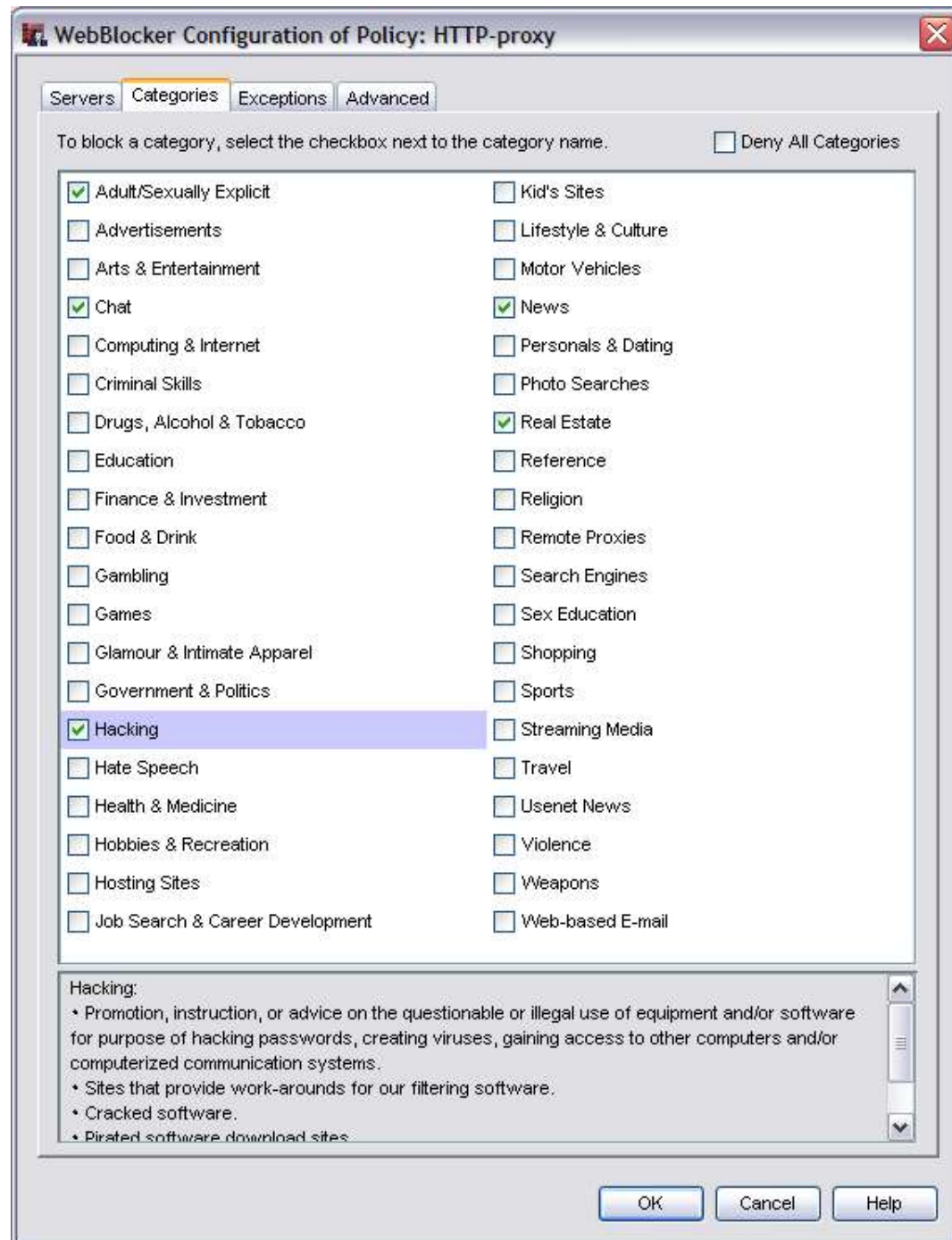
Quasi in tempo reale

Che cosa è?

- URL filtering a 40 categorie (oltre 12 milioni di URL) in partnership con SurfControl
- Configurazione razionalizzata nel Policy Manager
- Database URL globali - Inglese, Tedesco, Spagnolo, Francese, Italiano, Olandese, Giapponese, Cinese tradizionale e semplificato. 24x7x365 www scanning con persone e mezzi automatici
- Riduce il contenuto pericoloso di siti WEB pesa entrare nel network con oltre 12+ milioni di siti bloccati e riduce la navigazione improduttiva
- Blocca l'accesso ai siti di download IM/P2P, WebMail ed oltre 9000+ siti di spyware

WEBBLOCKER

- **40 categorie – WebMail ha la sua propria categoria**
- **Help on line di spiegazione per ogni categoria**
- **Cache locale configurabile per aumentarne le performances**
- **Utilizzo web configurabile per utenti/grupp/dominio e ora del giorno**





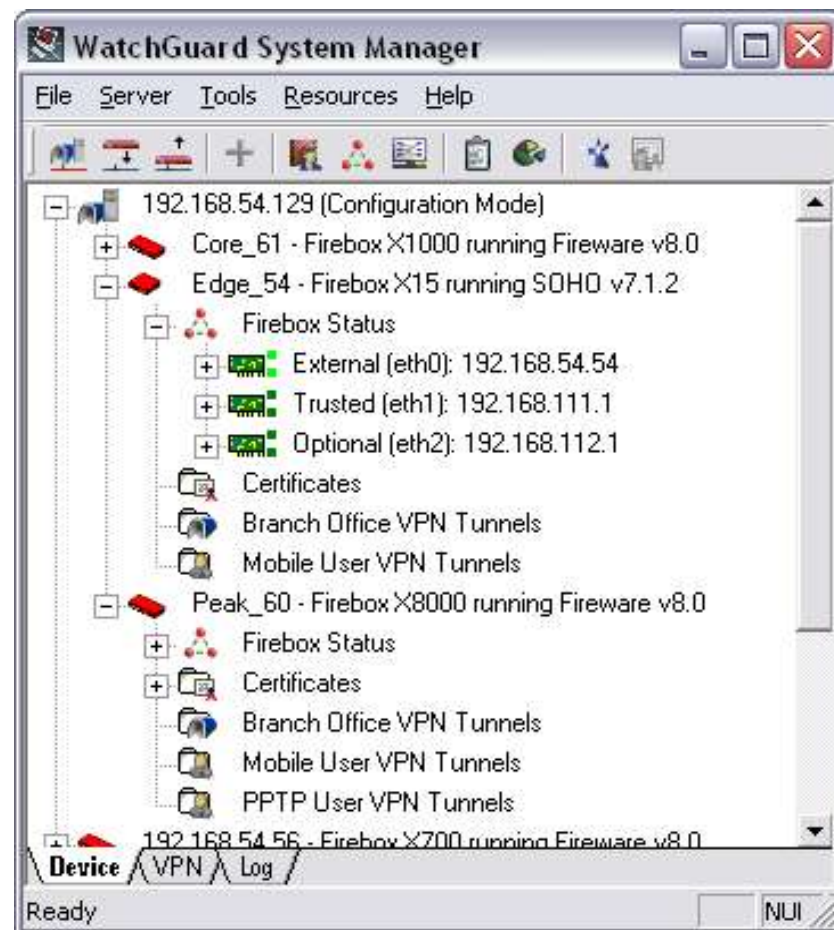
Stronger Security, Simply Done™

Watchguard System Manager

WATCHGUARD SYSTEM MANAGER 8.x

Management software per la famiglia Firebox X e opzioni di sicurezza

- Semplifica la sicurezza delle reti per gli esperti IT
- Facilita' di utilizzo per I neofiti



Interfaccia grafica intuitiva

- Facile da imparare; Facile da usare

Console di gestione unificata

- Nessuna necessita' di mantenere separati software di gestione per soluzioni multiple point

Real-time monitor interattivo

- Guarda, analizza e prendi azioni correttive – tutto in tempo reale.

Drag-and-drop VPN

- Un modo veloce e facile per creare Branch Office VPN

Logging e Reporting. Sicuro, flessibile, comprensibile

- Un completo insieme di utilita' per l'analisi della sicurezza e dell'analisi dell'attivita' del network

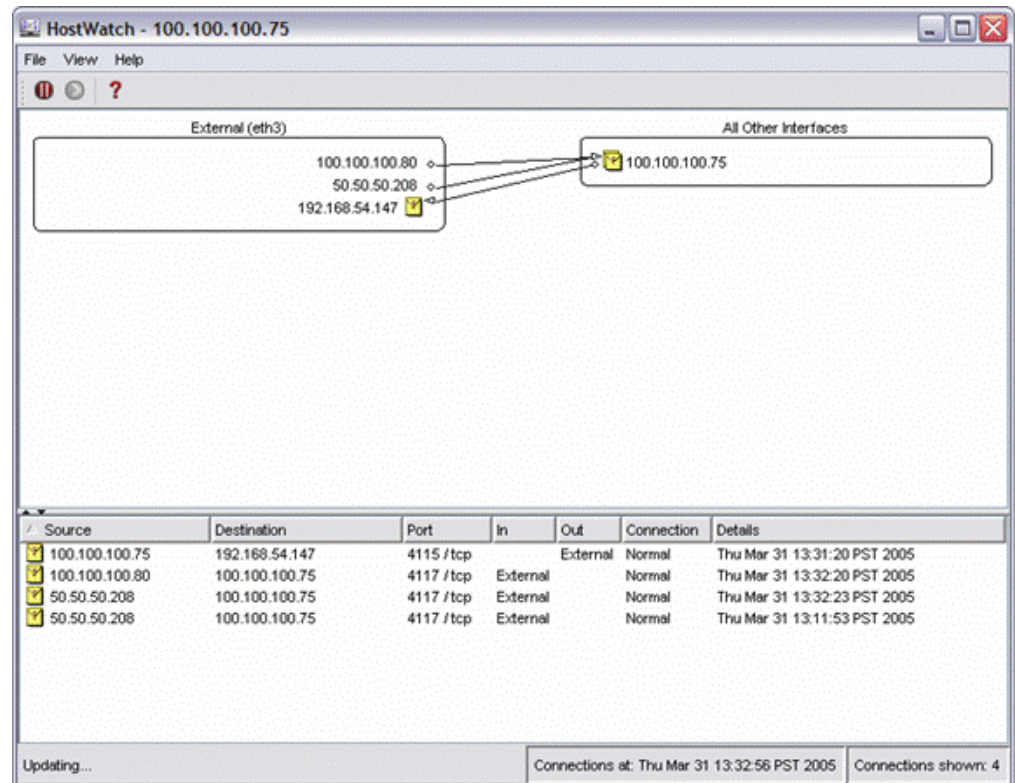
Reportistica integrata

- Report grafici granulari, chi ha fatto cosa da esterno verso interno e da interno verso esterno



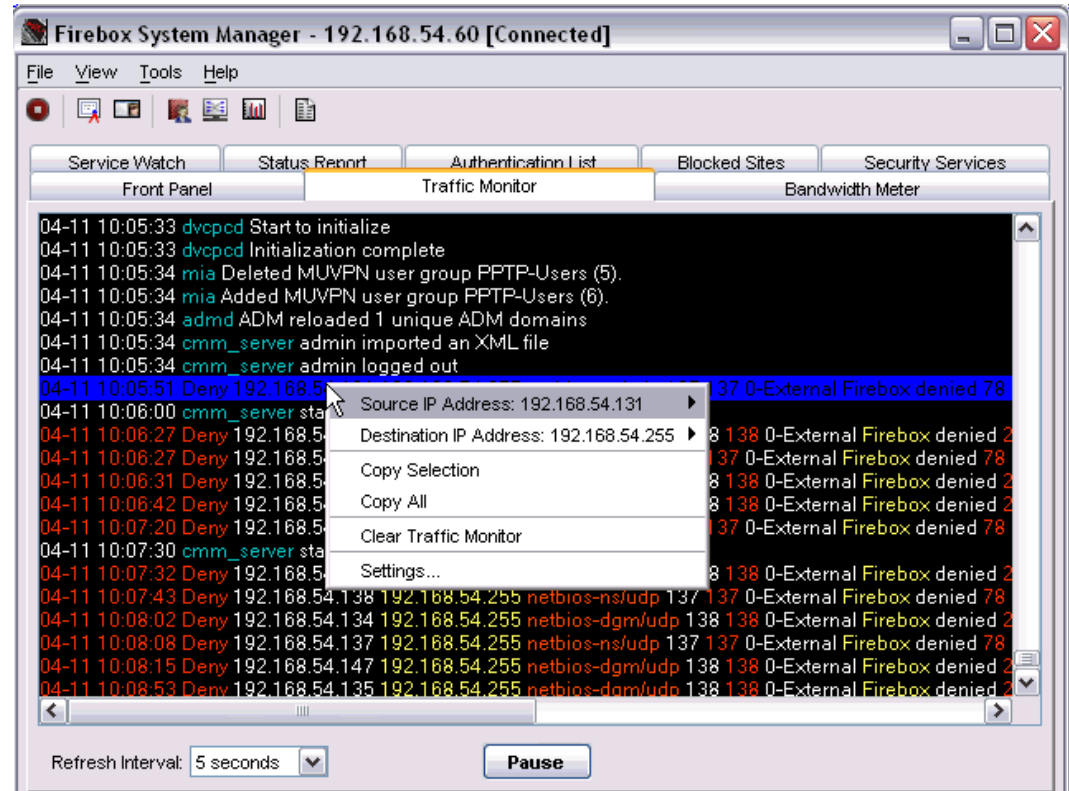
MONITOR IN TEMPO REALE ED INTERATTIVO: HOSTWATCH

- **Visualizzazione grafica in tempo reale delle connessioni**
- **Controlla il traffico del network in tempo reale**
- **Accesso ai dettagli di ogni connessione con un click**
- **Previene accessi non autorizzati bloccandoli istantaneamente**



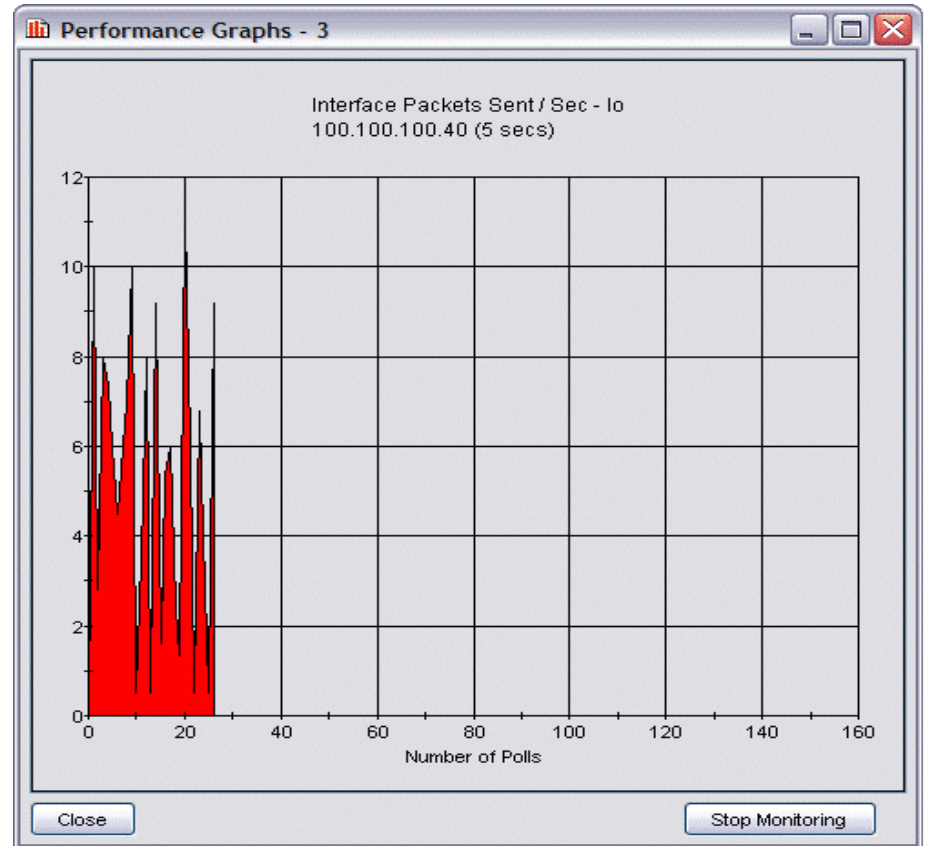
MONITOR IN TEMPO REALE ED INTERATTIVO: TRAFFIC MONITOR

- Visualizza il Firebox logs in una interfaccia a scorrimento intuitiva
- Elimina la necessita' di caricare ed analizzare i file di log
- Nuovo: ti permette di fare ping, traceroute, o bloccare un sito *istantaneamente*



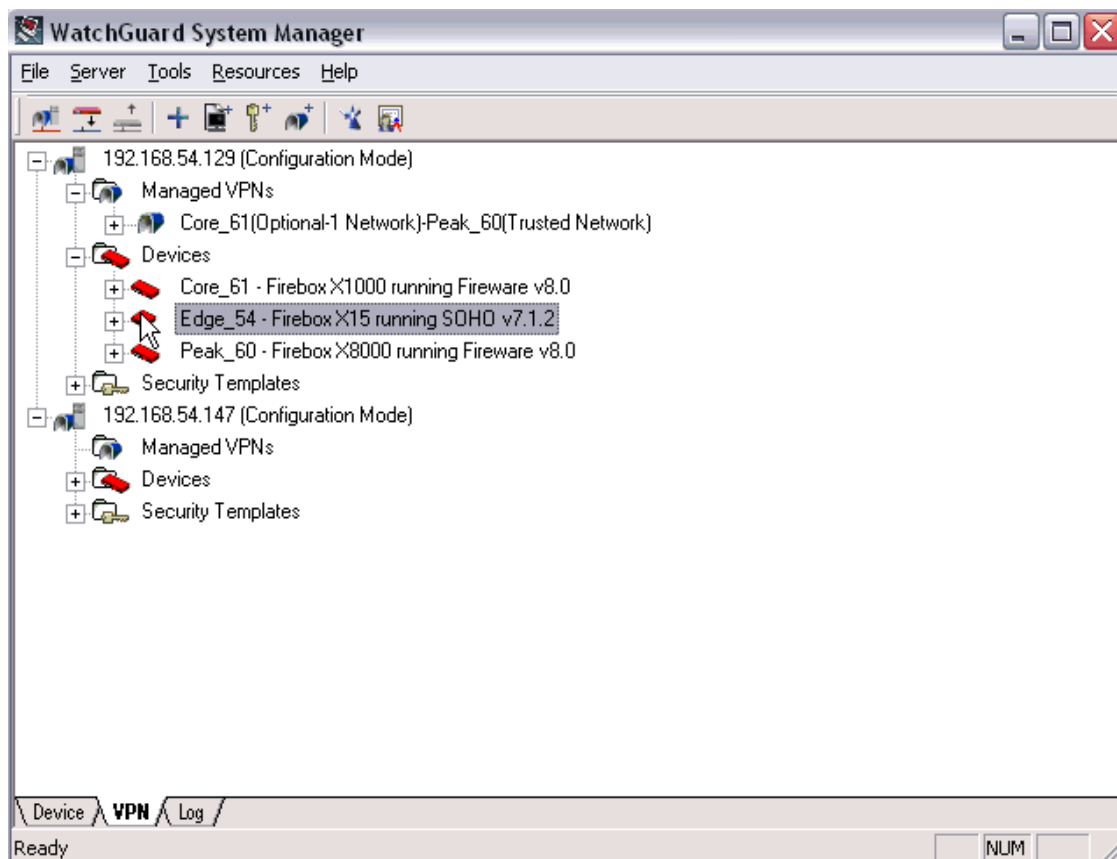
MONITOR IN TEMPO REALE : PERFORMANCE CONSOLE

- Display grafico delle performances del sistema
- Monitor performance di dozzine di parametri del sistema
- Pieno controllo in tempo reale di come il firebox sta funzionando
- Valida le policies attraverso la visualizzazione delle policy-based statistics



DRAG-AND-DROP VPN MANAGEMENT

- **Sposta un dispositivo su un altro per creare un tunnel VPN tra due sedi**
- **Supporto per piattaforme multiple WG**
- **Riduce I costi di amministrazione**
- **La configurazione delle VPN sono distribuite automaticamente**



LA NOSTRA MISSIONE...

A close-up portrait of a woman with dark hair, smiling warmly. She is wearing a light blue collared shirt. The portrait is framed with a thin red border.

Stronger Security

“ Fornire la più completa soluzione di sicurezza Unified Threat Management disponibile nel mercato oggi ”

Simply Done

“ Con la più facile console di security management per tutte le appliances Firebox X e servizi di sicurezza ”



Grazie!

Fabrizio.Croce@watchguard.com
tel. +39-335-7030721
skype: fabrizio_croce
msn: fabrizio_croce@hotmail.com

Stronger Security, Simply Done™