Check Point
SOFTWARE TECHNOLOGIES LTD.

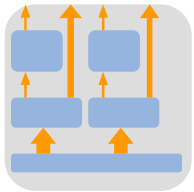
Check Point R70

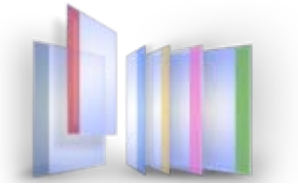
Patrick Hanel
CISSP, Technical Consultant

totalsecurity™

Agenda

- Check Point Software Blade Architecture
- Check Point R70 Technology
- Check Point Appliance

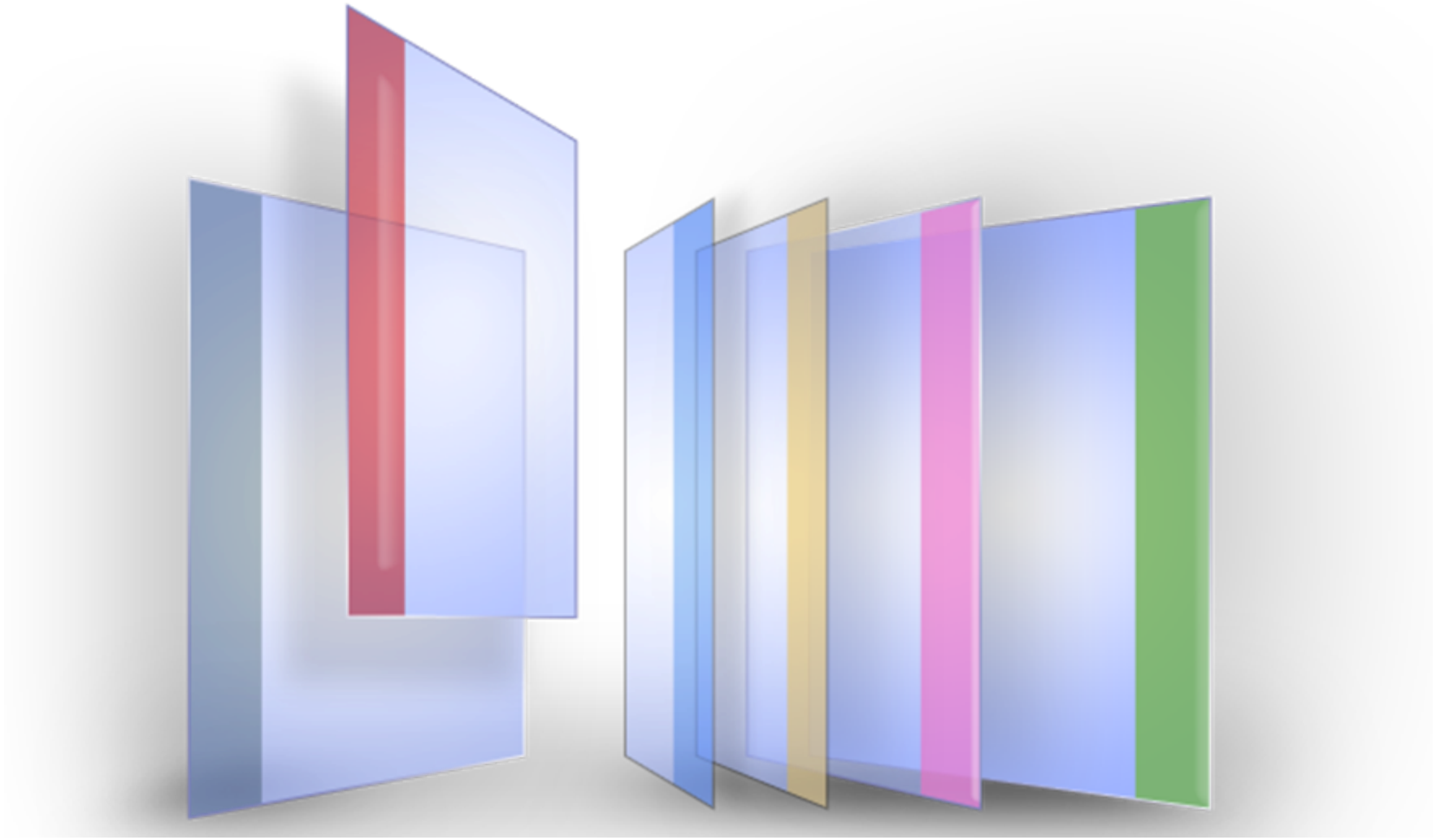




What organizations want

total security	Total security across all enforcement points
flexible security	The right protection at the right investment
simple security	Ease of deployment Ease of management

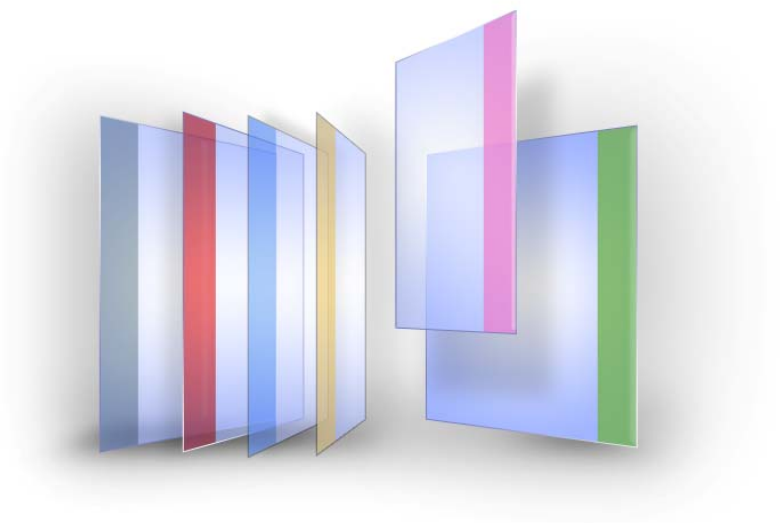
Introducing Check Point R70



with New Software Blade Architecture

totalsecurity™

What is a software blade?



A software blade is a security building block

- *Independent*
- *Modular*
- *Centrally managed*

How does it work?

Select blades

Configure system

Extend when necessary

Benefits

- Total security across all enforcement points
- Custom configuration for the right security at the right investment
- Simple planning, fast deployment

- Ease of consolidation
  - Add/activate blades easily into existing infrastructure
  - Segregation of duties in a single system
  - Dedicate system resources per software blade
- Simple migration and scaling

In 2009 customers have a choice

network security solutions

multiple projects
dedicated hardware
dedicated management

OR

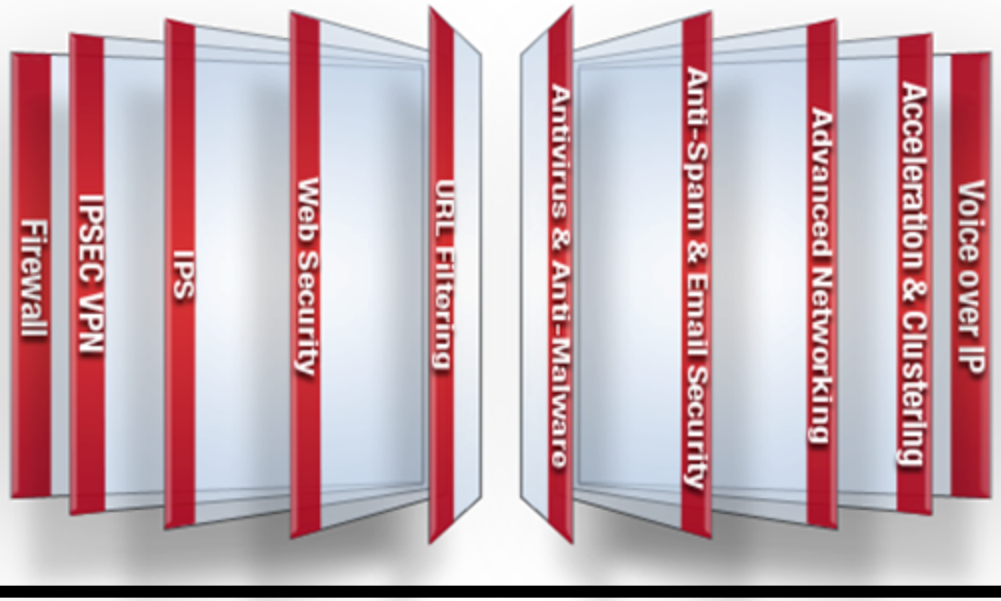
Check Point Software Blades

one project
multiple configurations
single management

Total Security
Complete Security & Management Portfolio

Check Point SOFTWARE TECHNOLOGIES LTD.

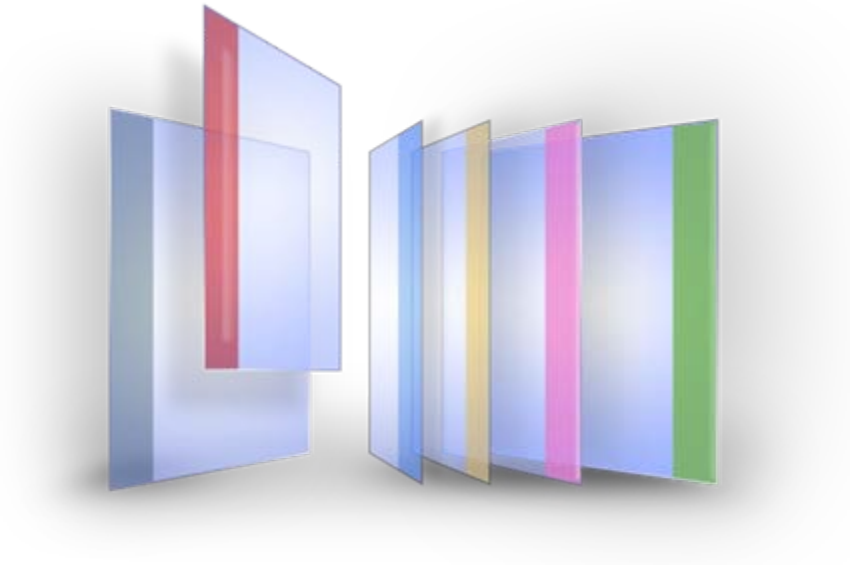
Security Gateway Blades



Security Management Blades

totalsecurity™

Check Point Software Blades



software**blades**

from Check Point

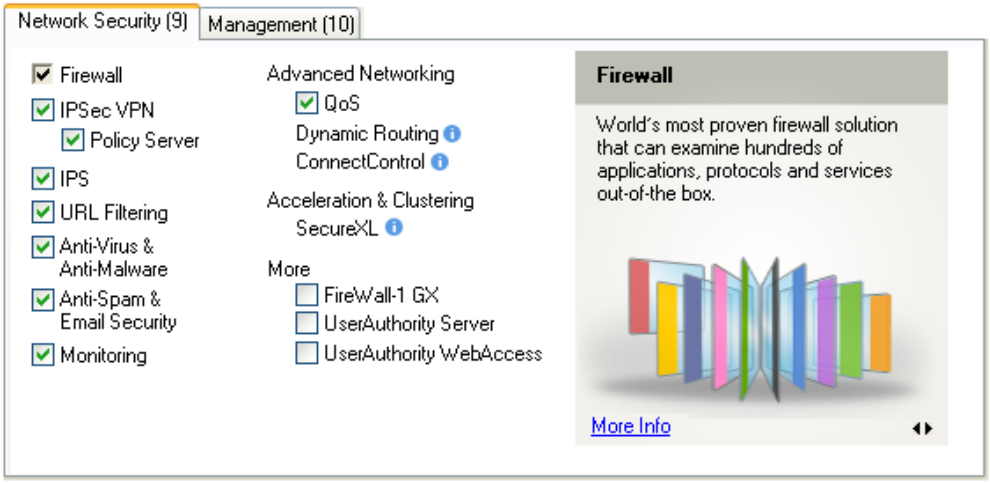
Secure | **Flexible** | **Simple**

Check Point R70 Technology

totalsecurity™

Check Point R70
- The Evolution Continues

- R70 release featuring Software Blade architecture



New **IPS Software Blade**

Improved **Core Firewall Performance**

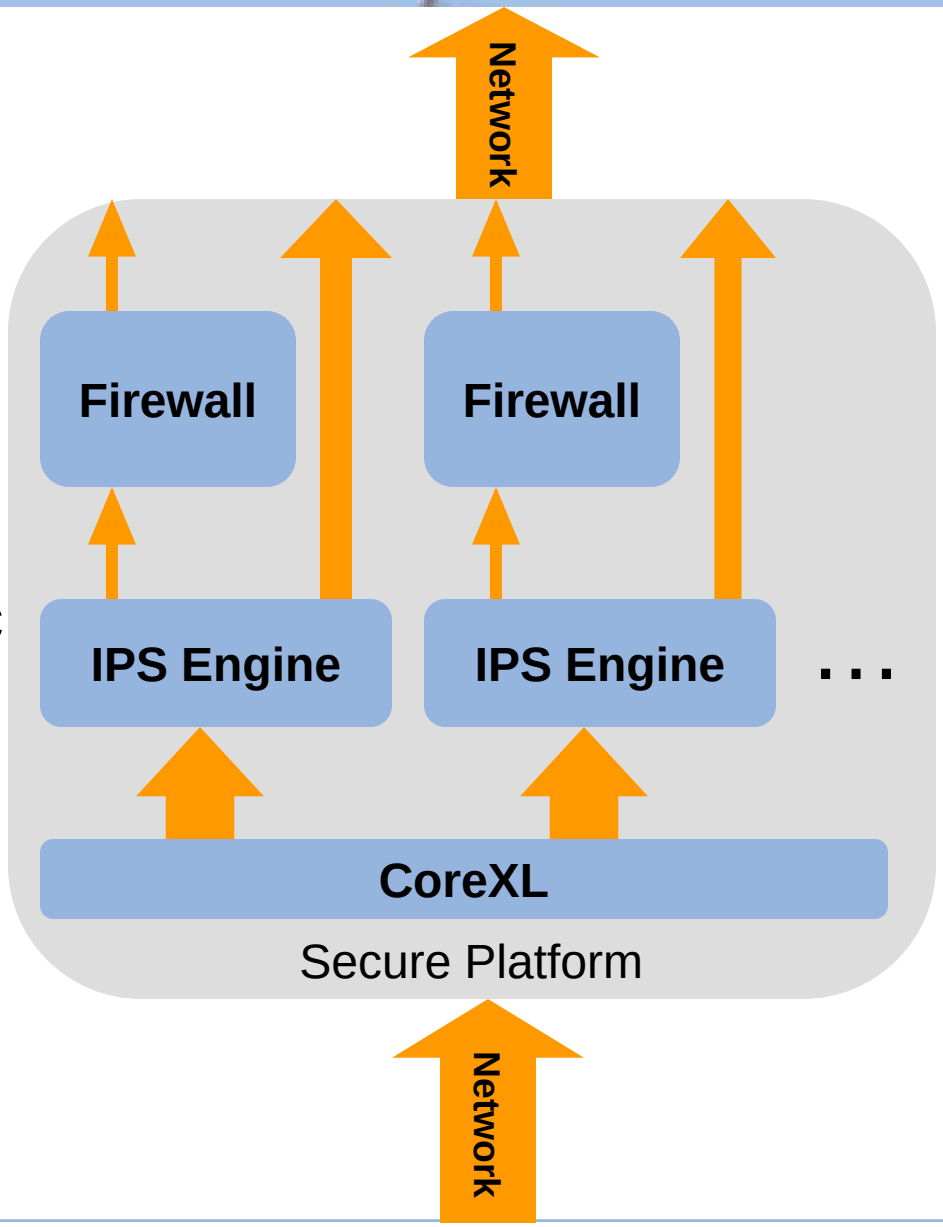
New **Provisioning Software Blade**

totalsecurity™

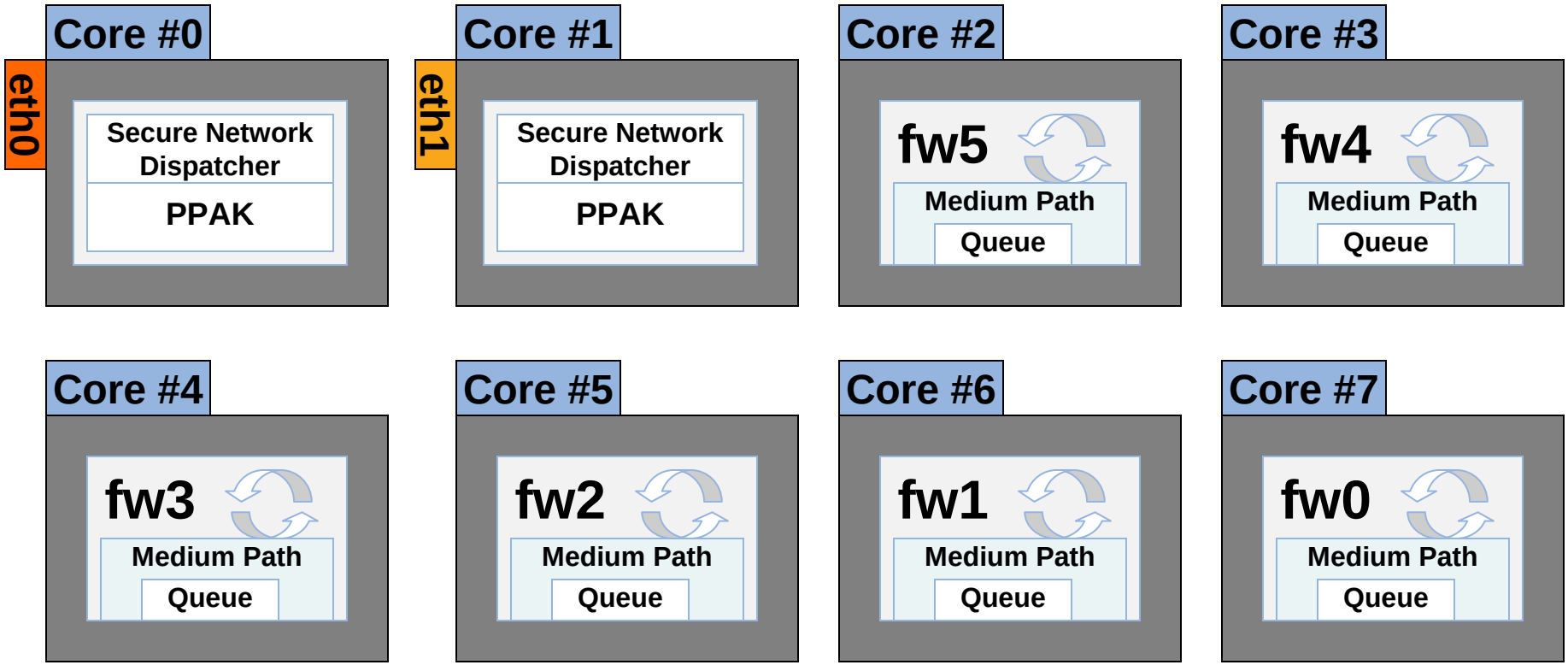
R70 architecture

R70 Architecture

- Deeper multi-core integration
- Multi-tier IPS filtering engine
  - quickly filters ~90% of traffic
- Filter attacks only on the relevant sections of the traffic
  - reduce overhead
  - Reduce false positives
- Performance Improvements in Secure Platform OS



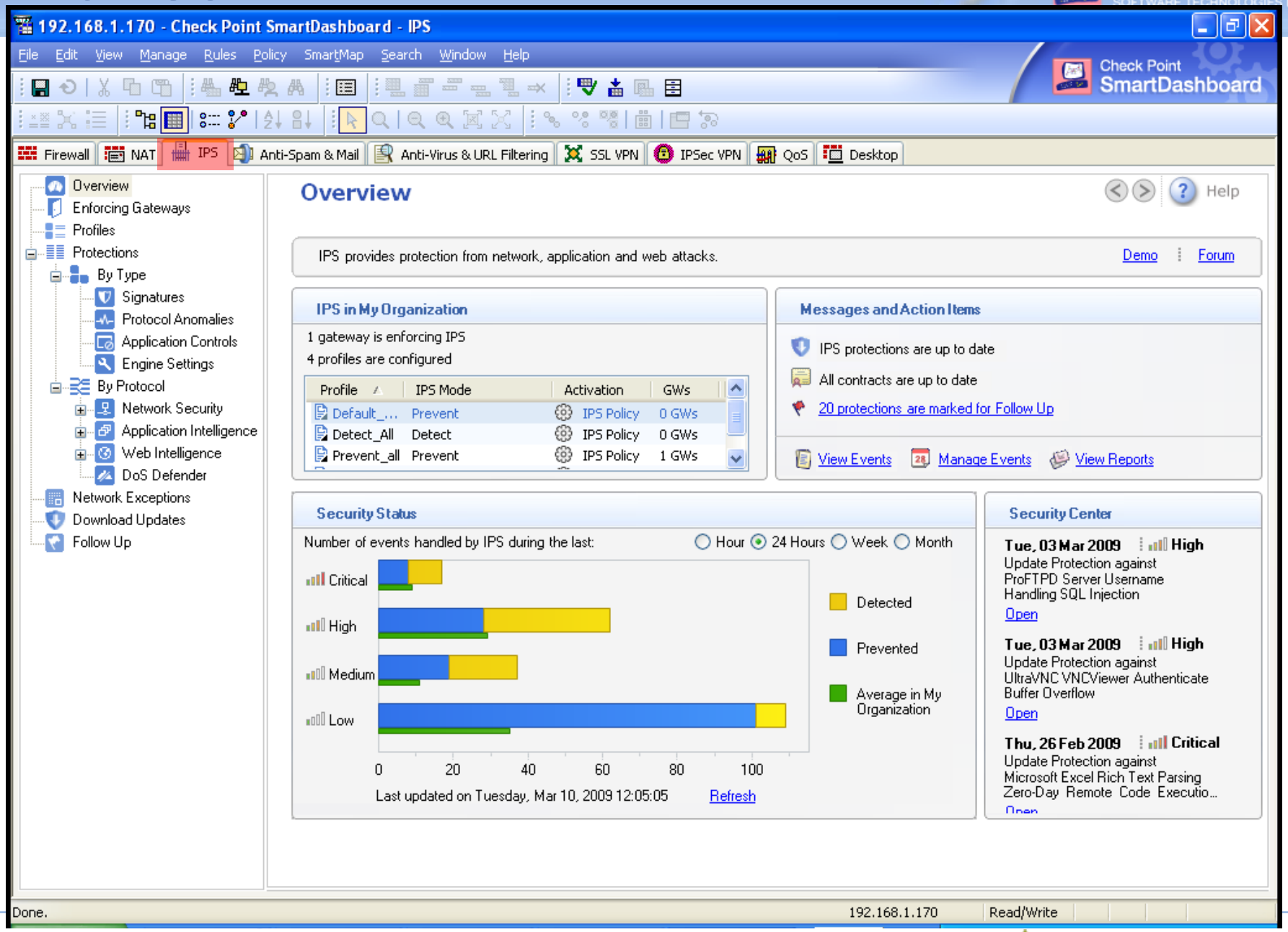
Integration with CoreXL



- Medium path – run PSL outside the firewall instance.
- IPS inspection scales with the cores, thanks to CoreXL.

R70 Technical

New GUI



Interface Changes - Tabs

NG & NGX	R70
Security	Firewall
SmartDefense	IPS
Messaging Security	Anti-Spam & Mail
Content Inspection	Anti-Virus & URL Filtering
Connectra	SSL VPN
VPN	IPSEC VPN

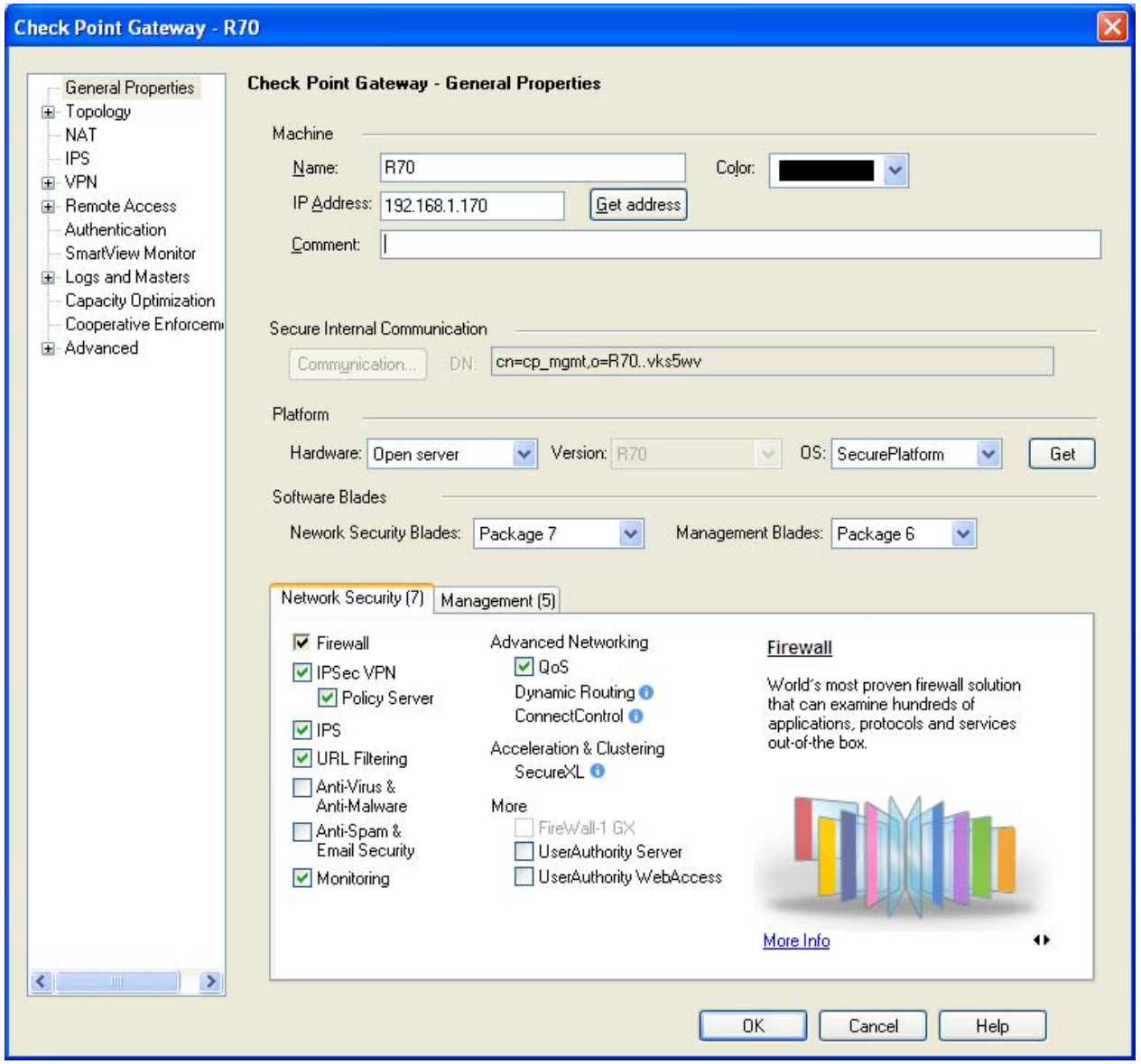
R65

R70

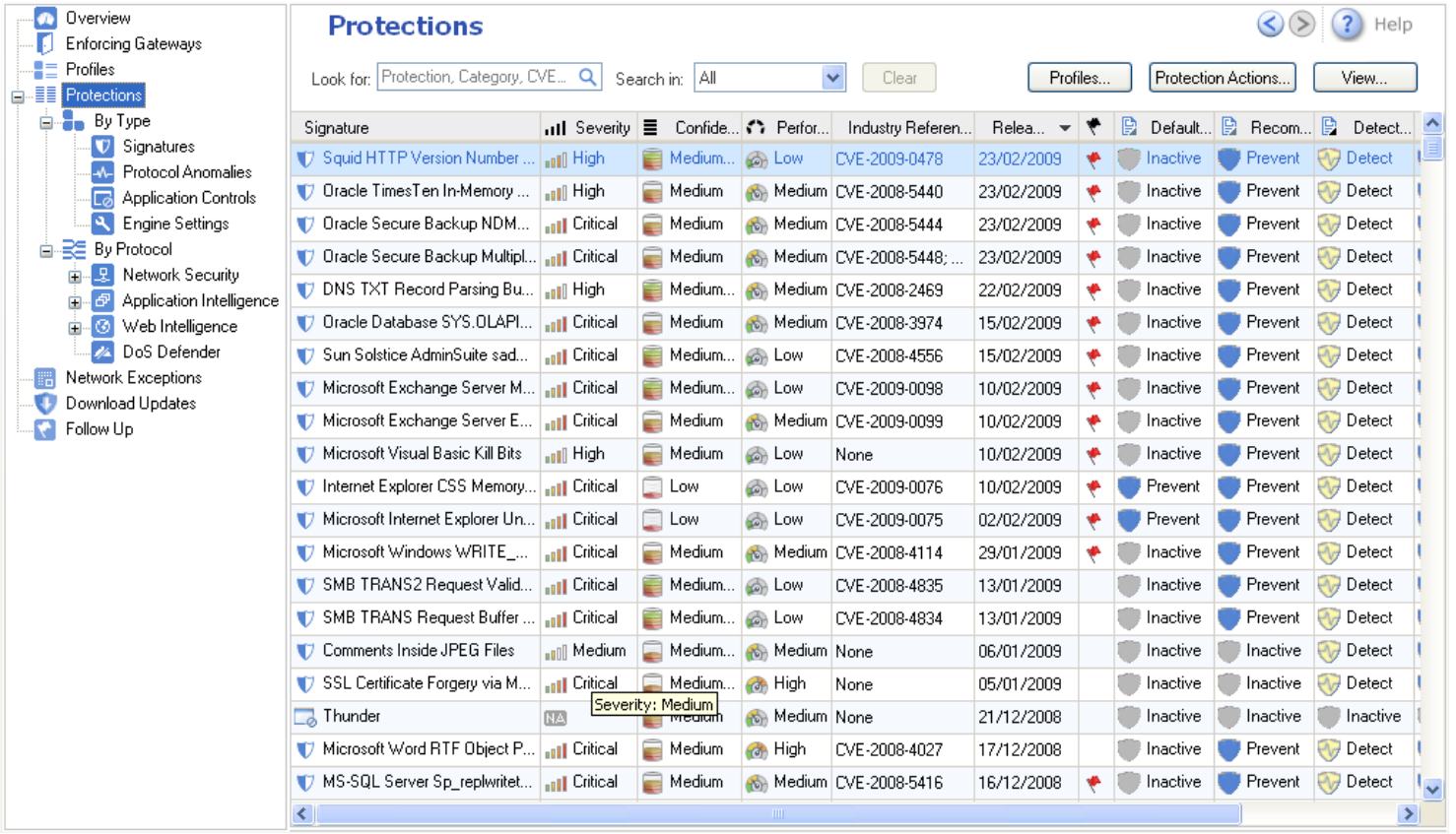
- "SmartDefense Services" tab replaced by new IPS Overview screen

New gateway / host properties

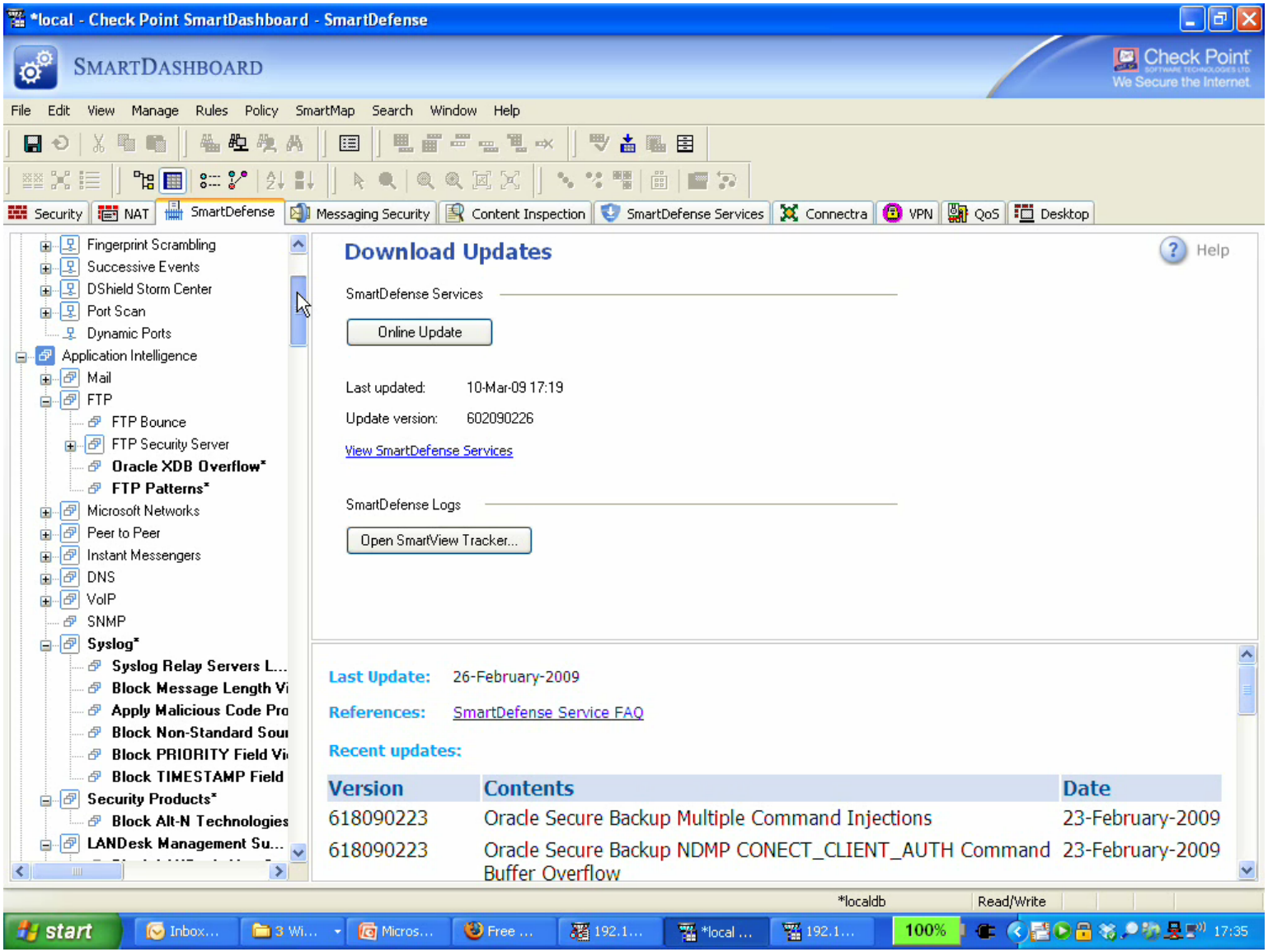
- Reflects new Software Blades Architecture



Protection Browser

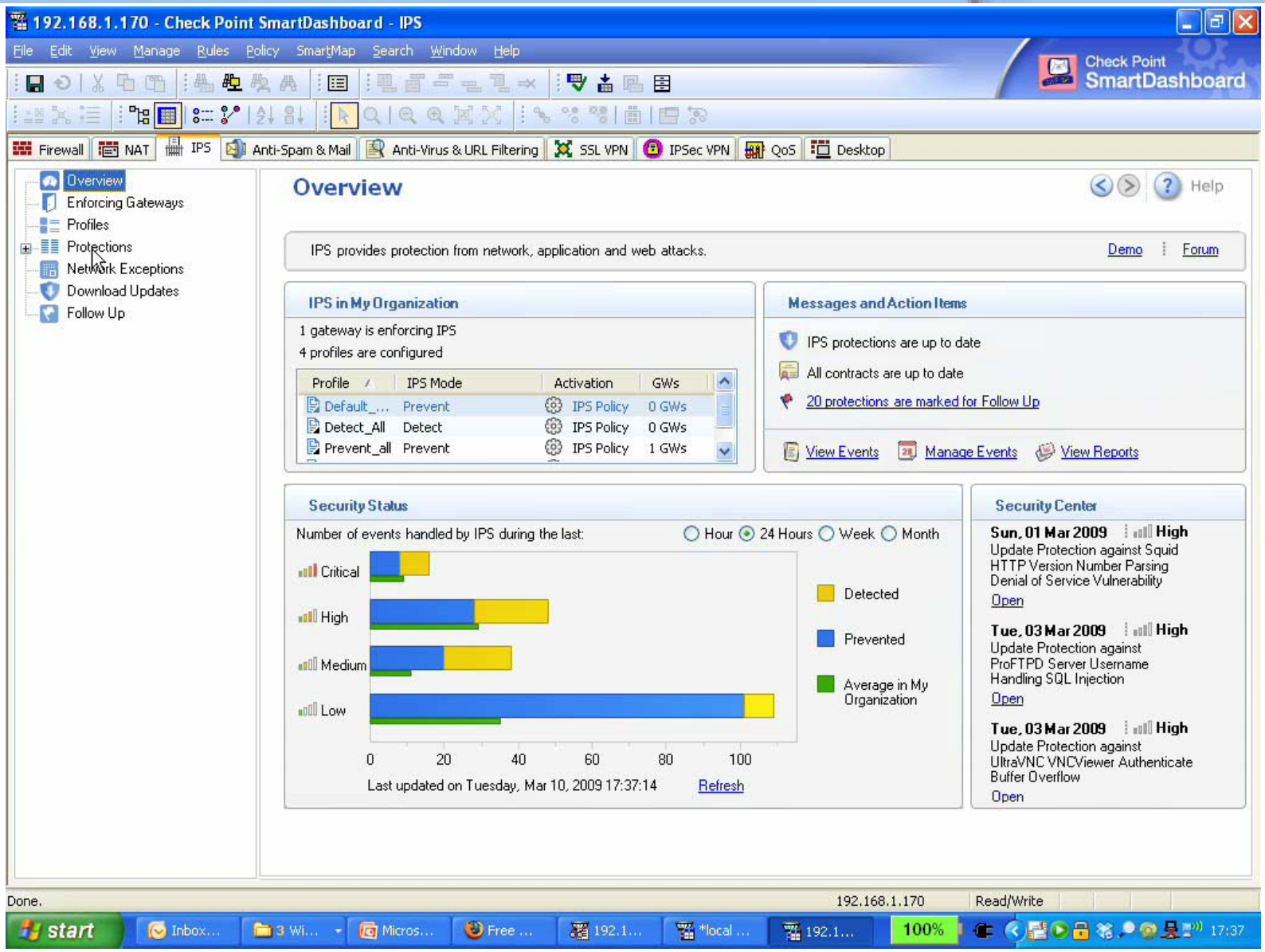


- **The Protection Browser allows easy and simple navigation through the entire list of protections.** You can search, sort, filter, export and take action directly from the grid!



totalsecurity™

R70



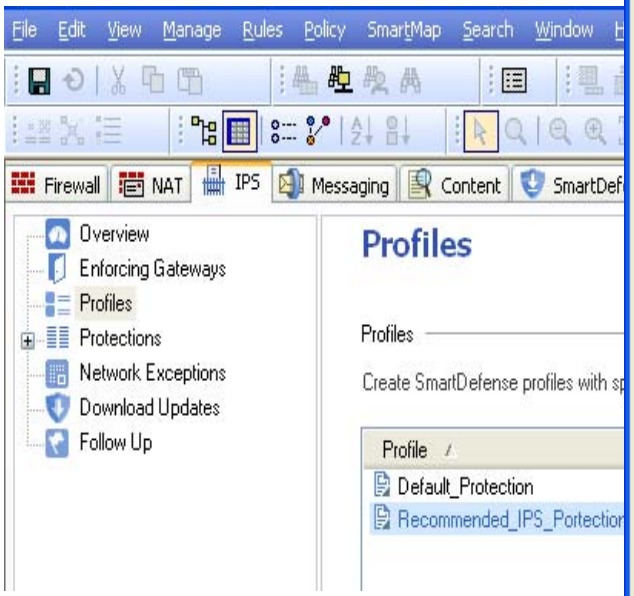
totalsecurity™

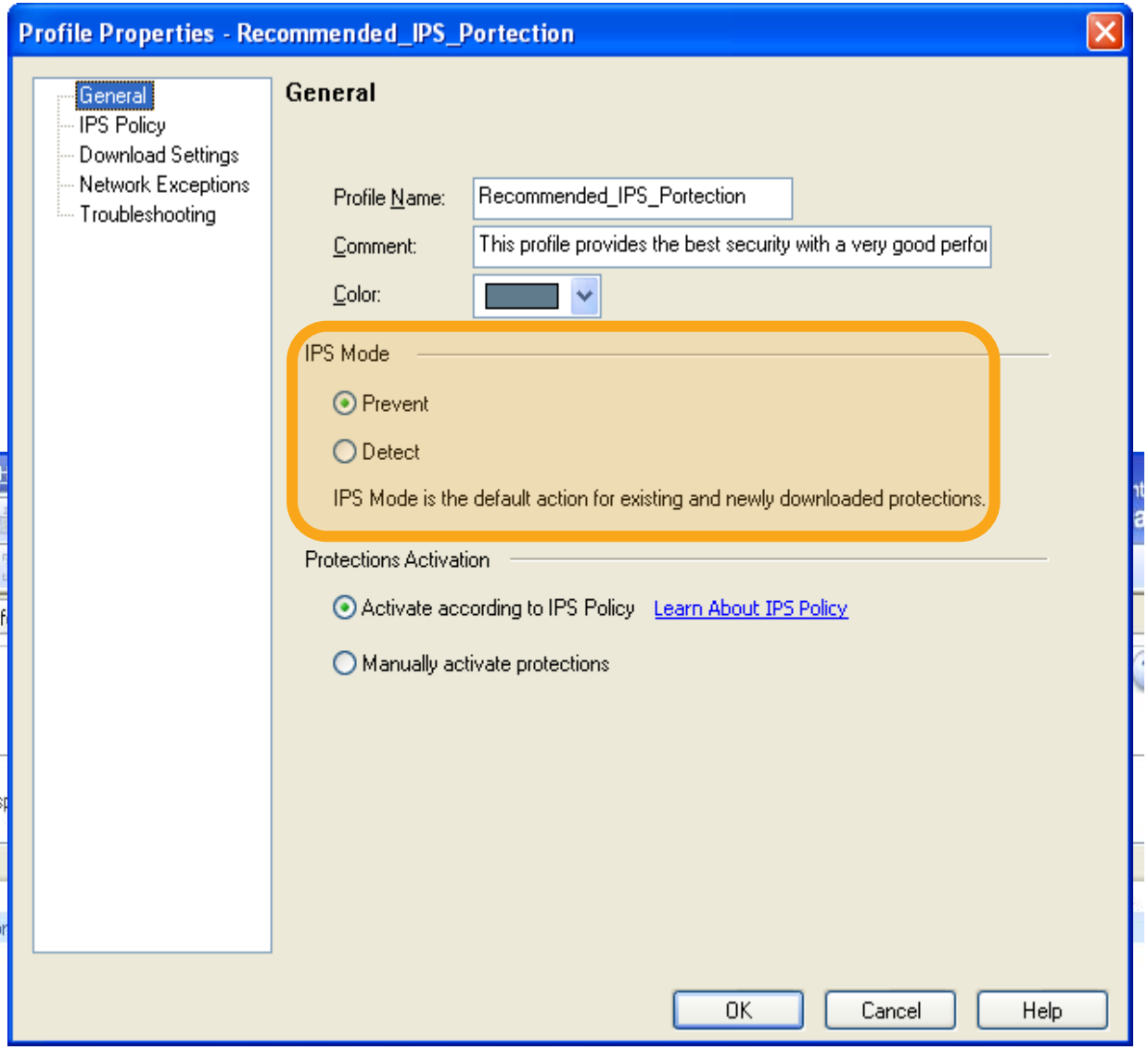
Profile vs IPS Policy

- Profile
  - Allows IPS settings to be managed across numerous GWs
  - Protect/Detect, Automatic / Manual
  - Multiple Profiles allow for different types of GW (e.g. Internal & perimeter GWs).
  - Profile includes IPS policy
- IPS Policy
  - IPS Policy determines which general protections will be activated (e.g. Client / Server protections)
  - Default action for new protections (prevent / detect)
  - Selectively Activate individual protections based on factors such as Severity, Confidence Level, Performance impact, or specific categories.
- Profiles Are Assigned to GWs, Policies are included in profiles.

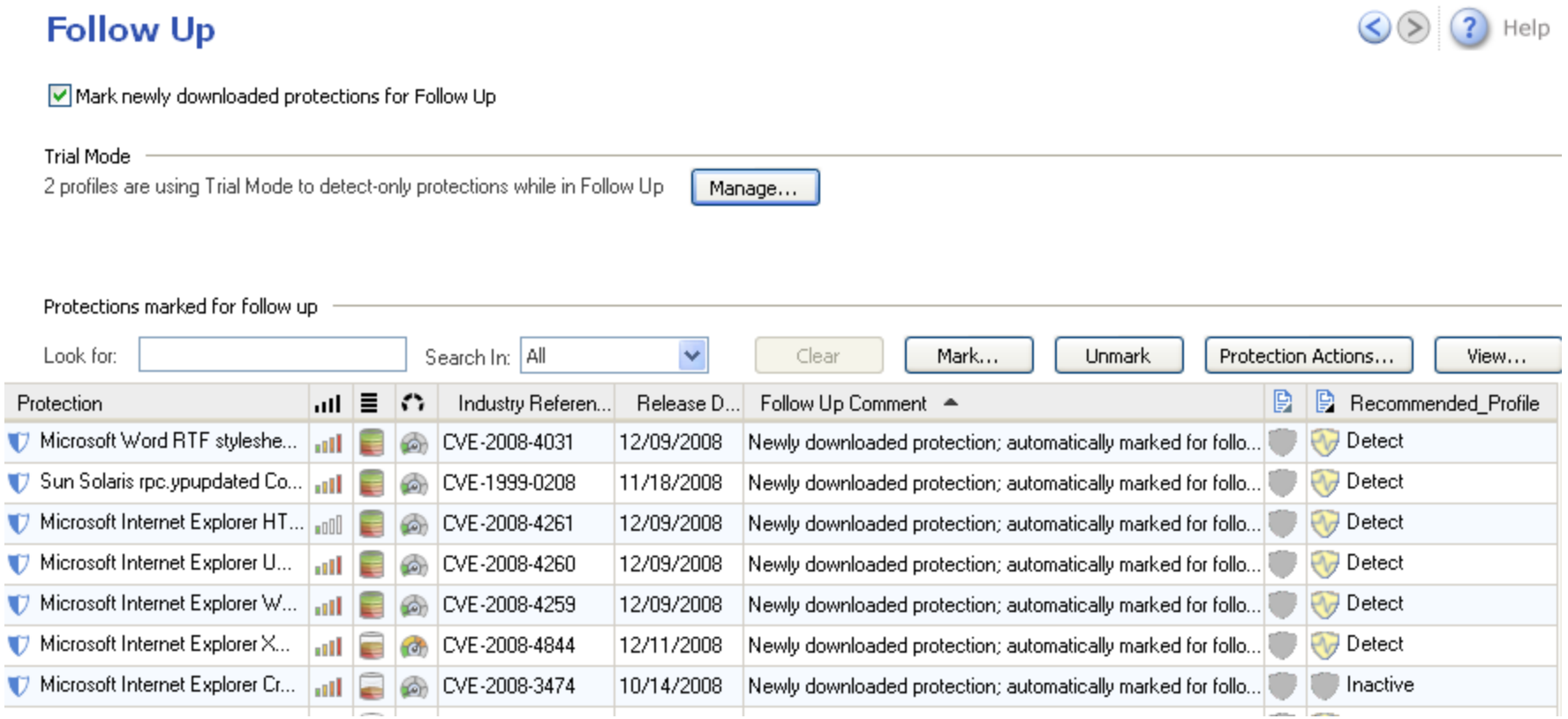
Define Your Own IPS Policy

1. **Start with the Recommended IPS profile. Optimized for Security, Performance and confidence**





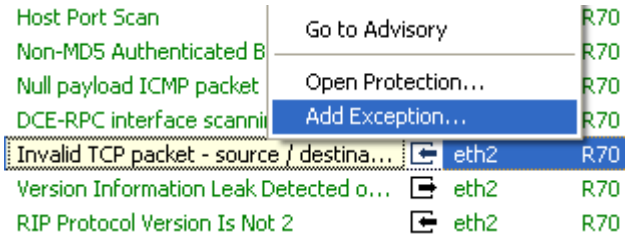
Safely Integrate New Protections

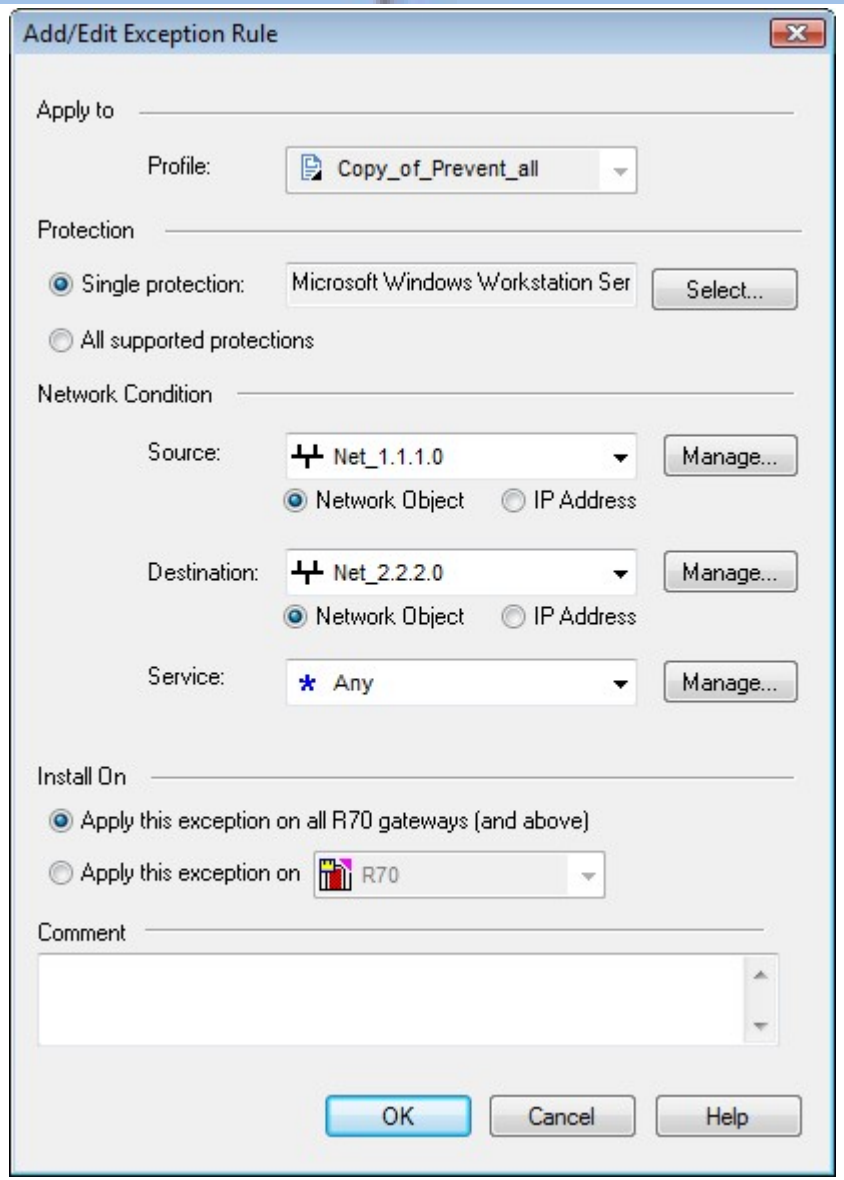


- **Follow up on newly downloaded protections.**
- **Manage the integration of each new protection individually.** The user has complete control.

Exceptions

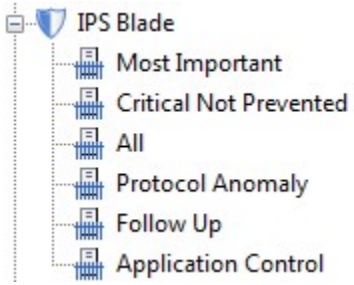
- Define exceptions per profile
  - Based on:
    - » Protection
    - » Source
    - » Destination
    - » Service
    - » Gateway
- Can also be defined from a log entry in tracker



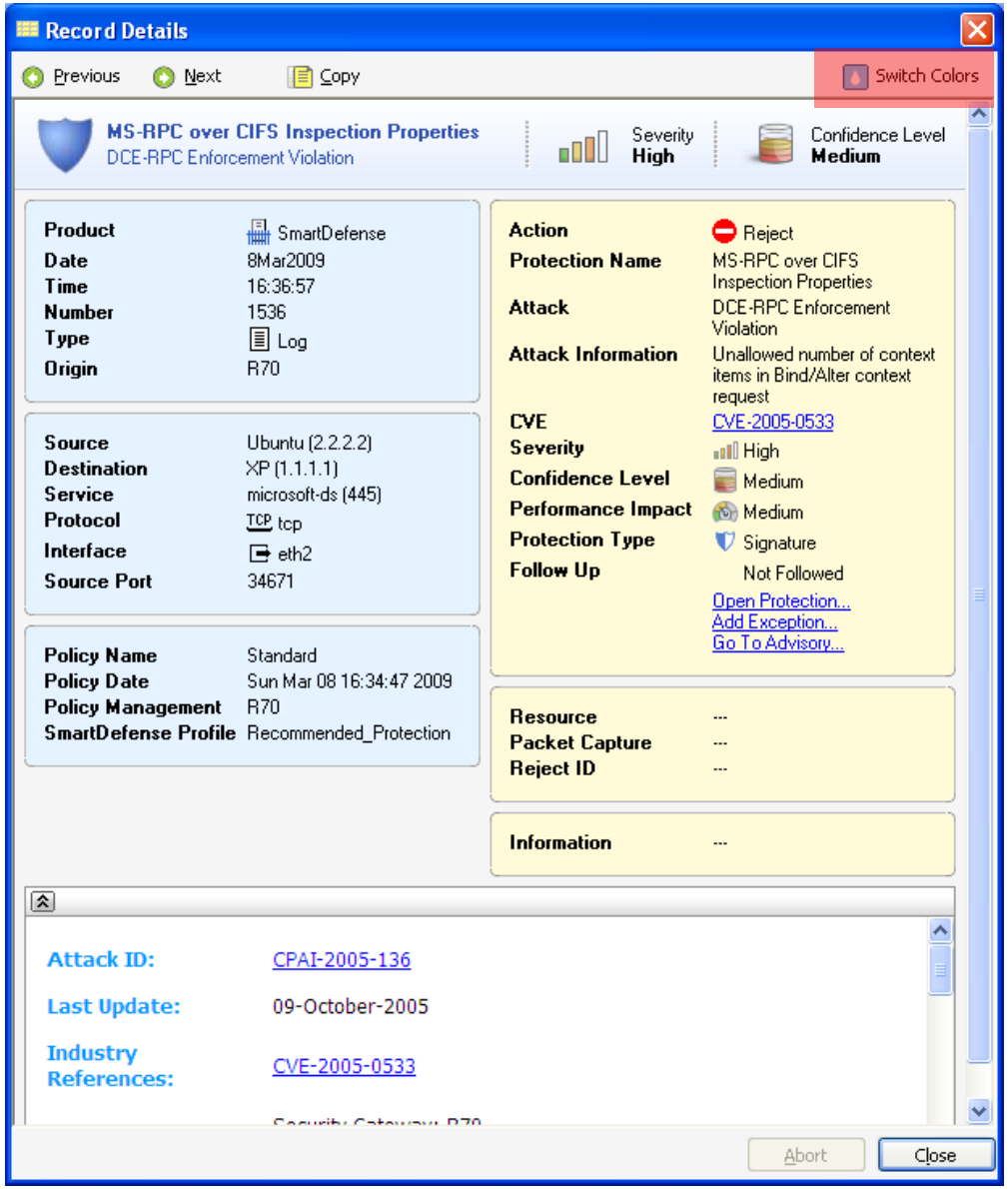


SmartView Tracker

- New IPS Blade Section

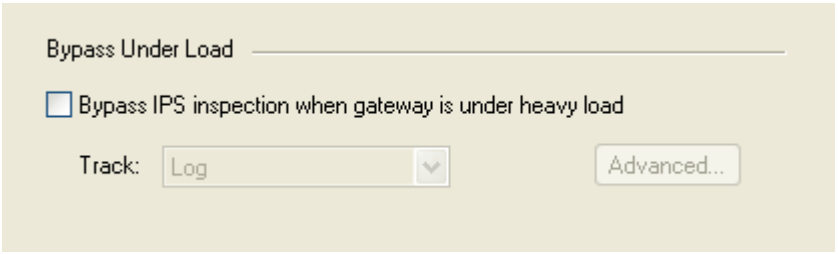


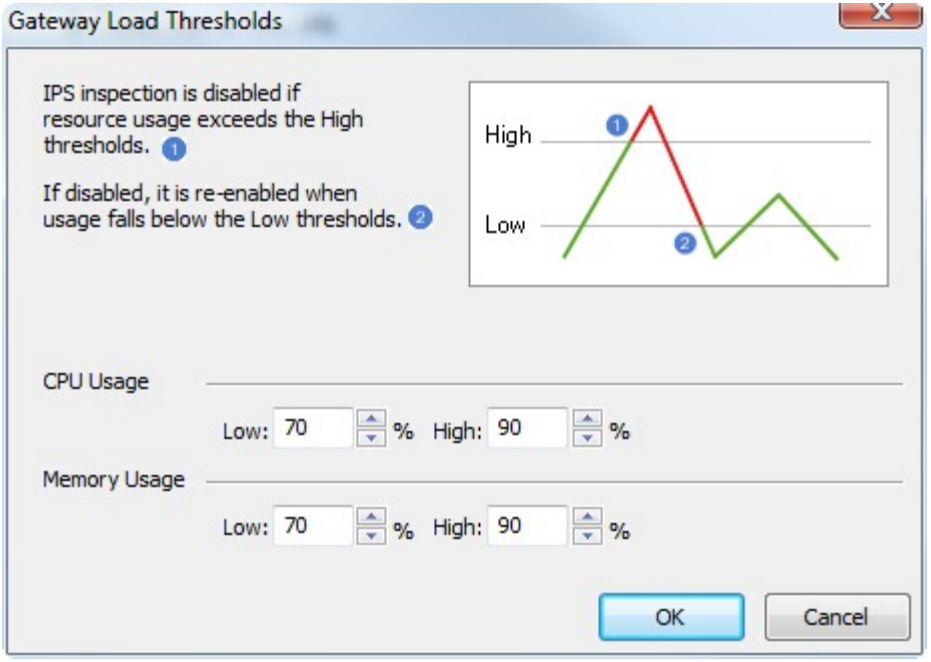
- New Details view



Software Fail-Open

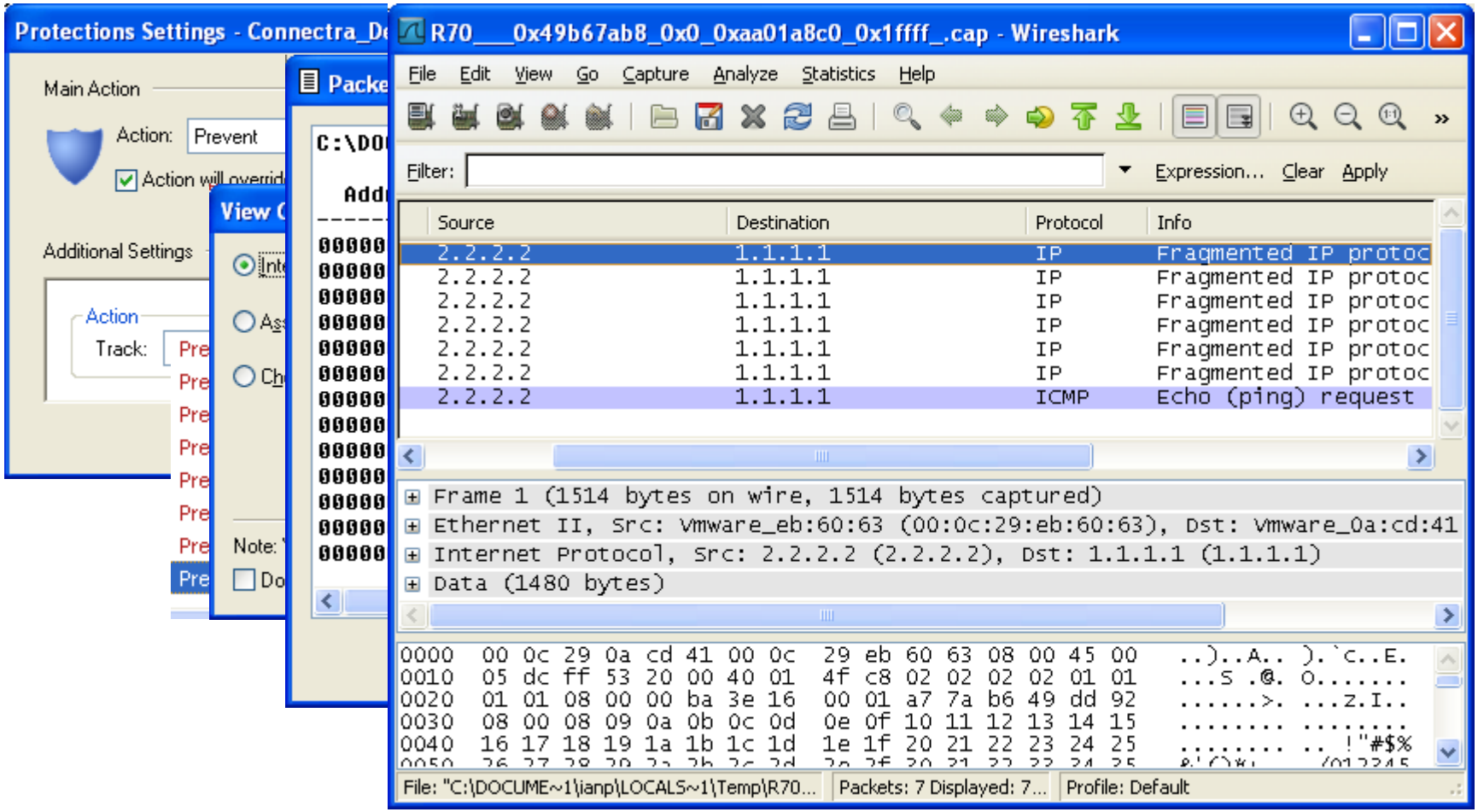
- **Software fail-open for IPS capabilities**
  As an extra safety measure, use the "Bypass Under Load" mechanism to automatically disable the IPS in the unlikely event of high load.
- When the CPU or memory usage exceeds a certain threshold, IPS inspection will be disabled until the low thresholds are reached.





Troubleshooting

- Integrated Packet Capture



Platform support in R70

- **SecurePlatform is now based on 2.6 kernel**
  - Installation on new hardware platforms. E.g. -
    - » HP 580G5, Dell R900, IBM x3850 M2
    - » Dell R300/R200
    - » HP Blades 460C/480C
  - Setting new performance records (about 25% increase in packet rate)
- **Support for IPSO 6.x allows extending CoreXL to leverage the new multi-core platforms from Nokia**
  - IP690, IP1280 and IP2450 are supported
  - IP560 supported only for SmartCenter
  - IP260, IP390, IP560 ...
- **Added support for Windows Server 2008**

CoreXL enhancements

- CoreXL was introduced in R65 with CoreXL release (a special release)
- Starting R70, CoreXL is included in the main-train product, and is enabled by default when installing on multi-core box
- New functionality supported in this release with CoreXL
  - UTM functionality : AV, URL filtering
  - Dynamic routing
  - VoIP
  - Bridge mode
  - SSL network extender

Check Point
SOFTWARE TECHNOLOGIES LTD.

Appliances

Scalable Security Performance

totalsecurity™

Expanded and Flexible Appliance Portfolio

Expanded **Power-1** Appliances!

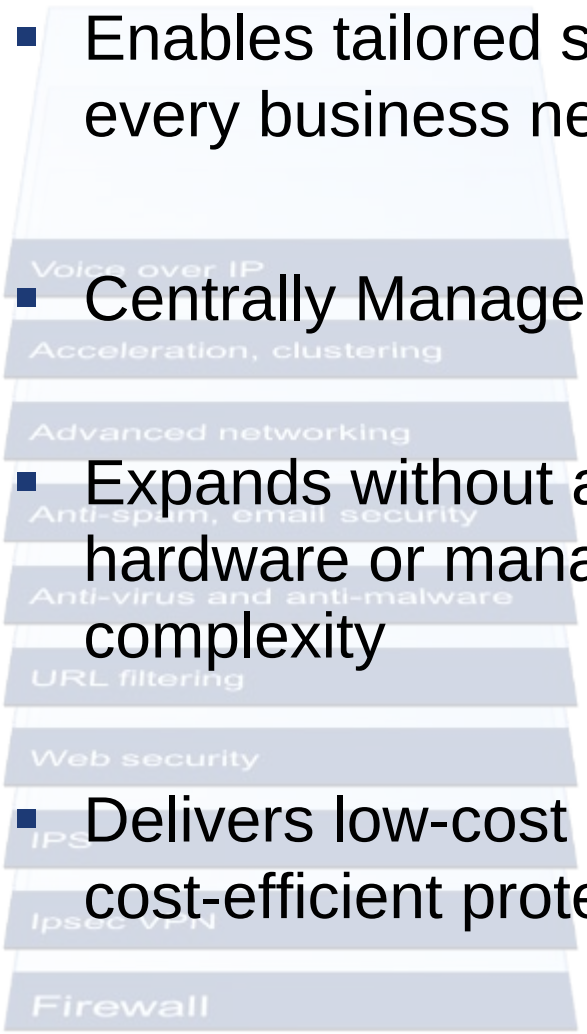
New **IP** Appliance Line!

Software Blade Architecture!

totalsecurity™

Check Point Appliances—Software Blades

- Enables tailored solutions for every business need
- Centrally Managed
- Expands without additional hardware or management complexity
- Delivers low-cost ownership and cost-efficient protection



Power-1 11000 Series


Power-1 9075


Power-1 5075

totalsecurity™

Power-1 11000 Appliances
Scalable Security Performance

Scalable Security Performance

Power-1 11065, 11075, 11085

- Maximum security and performance for data centers and large sites
  - Firewall, IPSec VPN, and intrusion prevention (IPS)
  - Field upgradable for maximum performance flexibility
  - Advanced acceleration and networking technologies assure application availability
- Streamlined deployment and maximum flexibility
  - Single vendor hardware/software solution
  - Software blade architecture for expandability with no extra hardware
- Manageability, modularity and serviceability
  - LOM Card (Lights-Out Management) for out-of-band management
  - Centrally managed
  - Hot swappable, replaceable power supply and hard drive

Power-1 11000 Appliances

Power-1 11000 Series

- **Power-1 11000 Series:** Solutions for large enterprises and data centers. Includes 3 models:
  - **Power-1 11085:** Firewall throughput up to 25 Gbps and IPS up to 15 Gbps
  - **Power-1 11075:** Firewall throughput up to 20 Gbps and IPS up to 12 Gbps. Field upgradable to Power-1 11085
  - **Power-1 11065:** Firewall throughput up to 15 Gbps and IPS up to 10 Gbps. Field upgradable to Power-1 11075 or Power-1 11085


Power-1 9075

- **Power-1 9075:** Solution for enterprises and data centers


Power-1 5075

- **Power-1 5075:** Solution for enterprises and large branch offices

totalsecurity™

Key Differentiators

Simple field performance upgrades

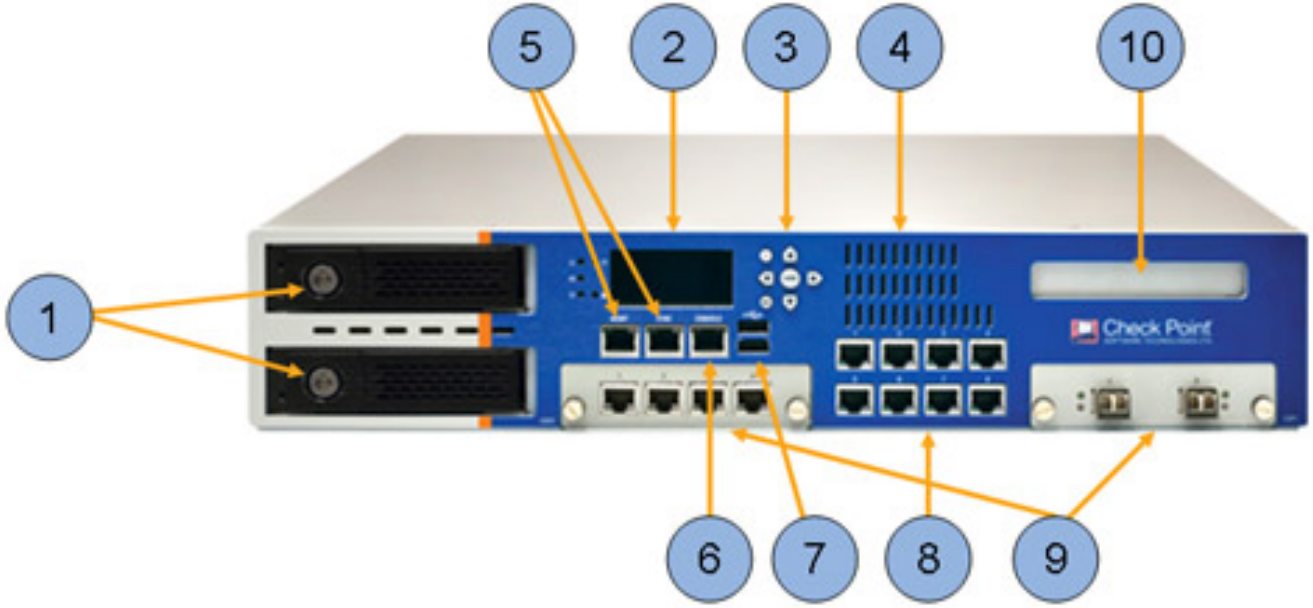
Up to 25 Gbps firewall performance in a 2U form factor

Flexible, extensible, investment protection

totalsecurity™

Field Performance Upgradability

Manageable, Modular, and Serviceable



1. Redundant hot-swappable hard drives
2. LCD display
3. LCD control buttons
4. Air intake
5. Management & Sync ports
6. Console port
7. USB ports
8. Eight 1 GbE ports
9. Field swappable expansion modules
   - 1 GbE Copper (4 ports)
   - 1 GbE LX Fiber (single mode) (4 ports)
   - 1 GbE SX Fiber (multi mode) (4 ports)
   - 10 GbE LR Fiber (single mode) (2 ports)
   - 10 GbE SR Fiber (multi mode) (2 ports)
10. LOM (Out-of-Band Management) card

Lights-Out Management—Out of Band

- The ability to monitor and manage the appliance remotely and out-of-band whether device is on or off
- Implemented via a hardware solution—LOM card
- Dedicated power source

Customize with Additional Software Blades

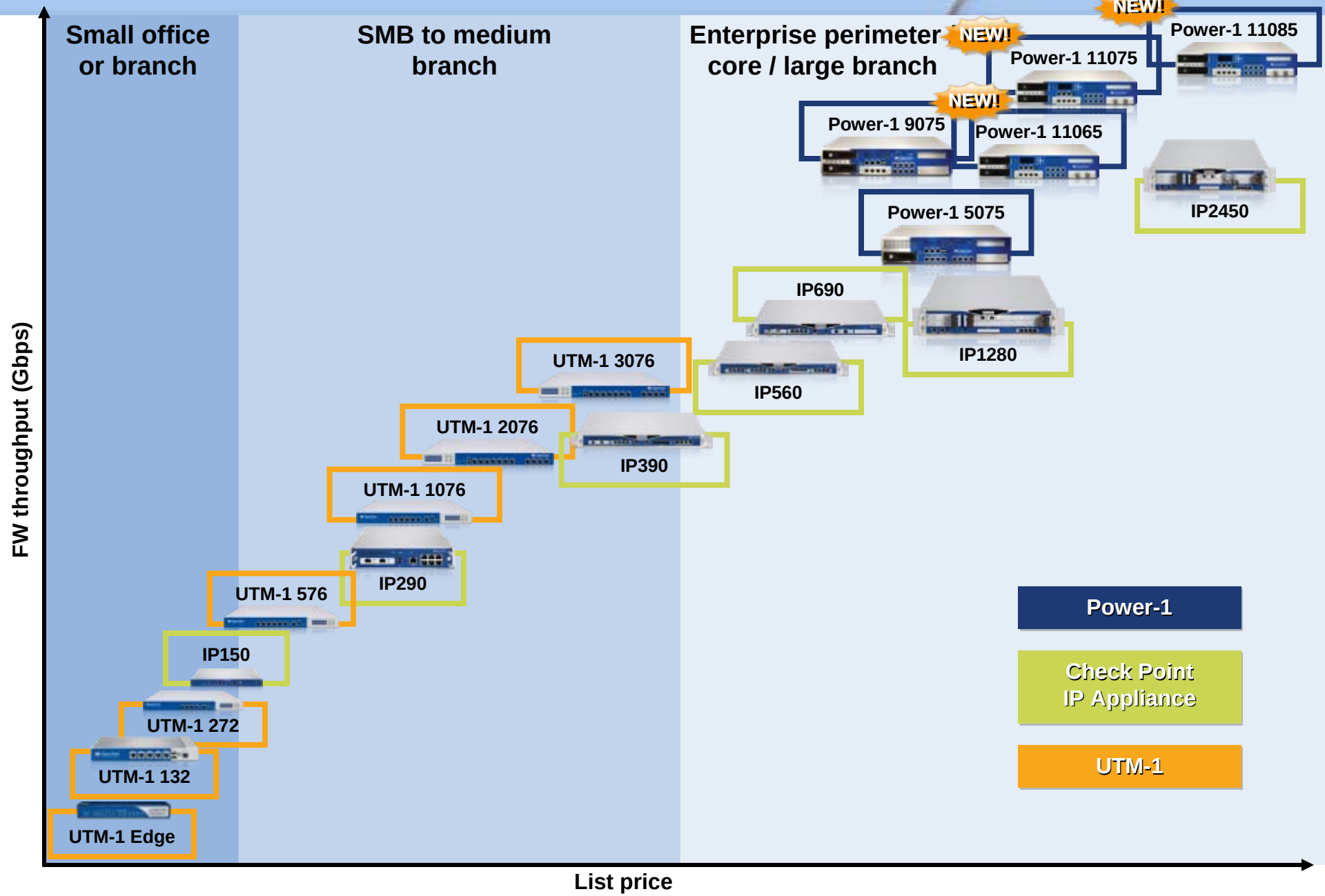
gatewayblade	**firewall**
gatewayblade	**IPsec VPN**
gatewayblade	**IPS**
gatewayblade	**acceleration & clustering**
gatewayblade	**advanced networking**
gatewayblade	**web security**
gatewayblade	**voice over IP**
gatewayblade	**URL filtering**
gatewayblade	**anti-virus & anti-malware**
gatewayblade	**anti-spam & email security**

Security perpetual blade

Security service blade

totalsecurity™

Check Point Appliance Line



Summary

Check Point Appliances + R70

Maximum security and performance

Streamlined deployment and maximum flexibility

Manageability, modularity and field upgradability

totalsecurity™