



Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point R70

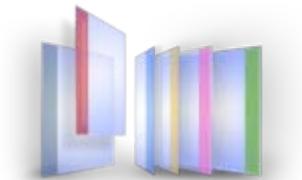
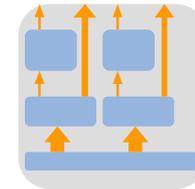
Patrick Hanel
CISSP, Technical Consultant

total**security**™



[Unrestricted]—For everyone

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



total security

Total security across all enforcement points

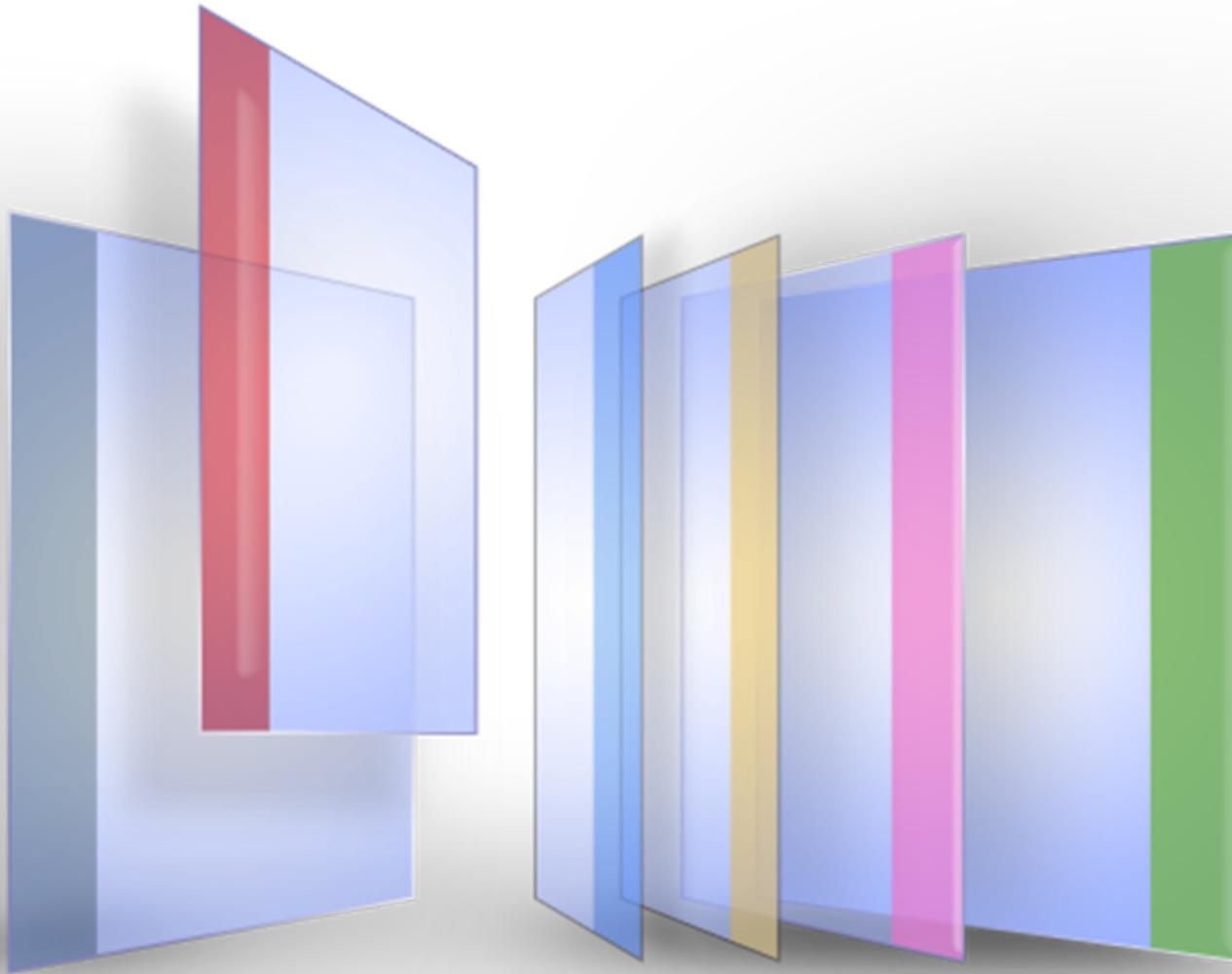
flexible security

The right protection at the right investment

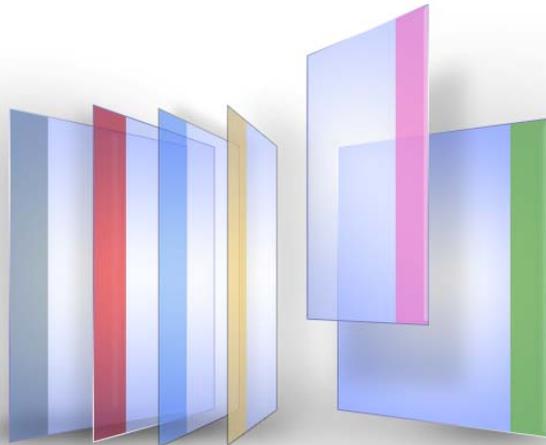
simple security

Ease of deployment
Ease of management

Introducing Check Point R70



with New Software Blade Architecture



A software blade is a security building block

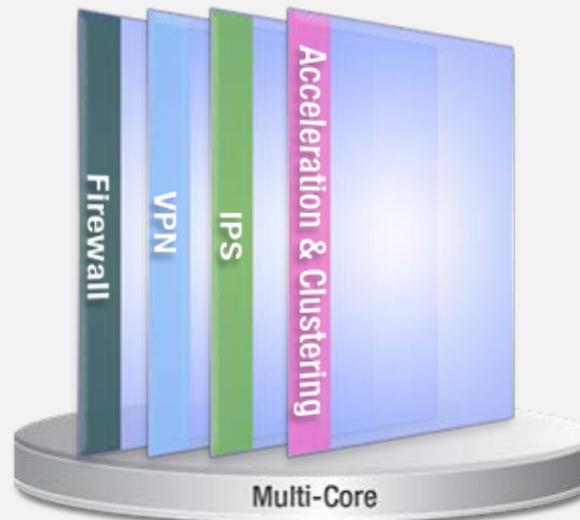
- *Independent*
- *Modular*
- *Centrally managed*

How does it work?

Select blades



Configure system



Extend when necessary



TOTAL
FLEXIBLE
SIMPLE
SECURITY

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

MIGRATION
CONSOLIDATION
LOWER
TCO

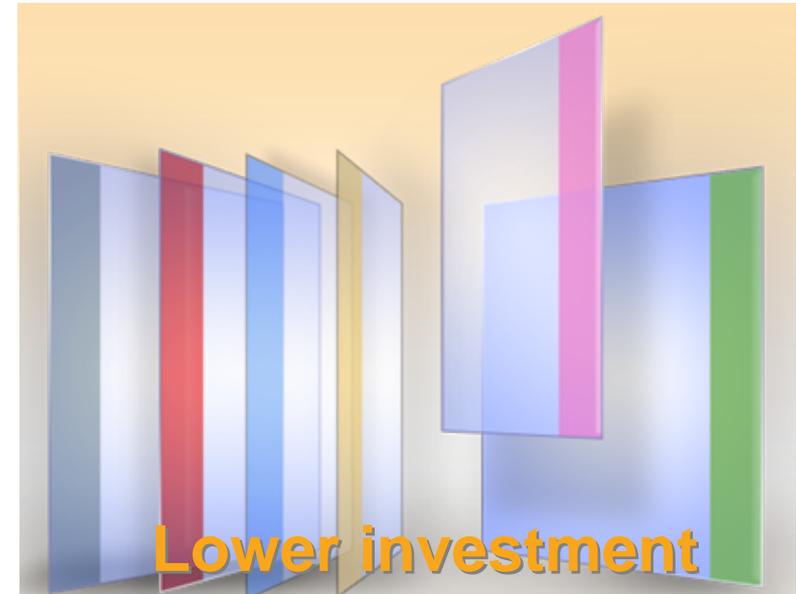
- Ease of consolidation
 - Add/activate blades easily into existing infrastructure
 - Segregation of duties in a single system
 - Dedicate system resources per software blade
- Simple migration and scaling

network security solutions



multiple projects
dedicated hardware
dedicated management

Check Point Software Blades



one project
multiple configurations
single management

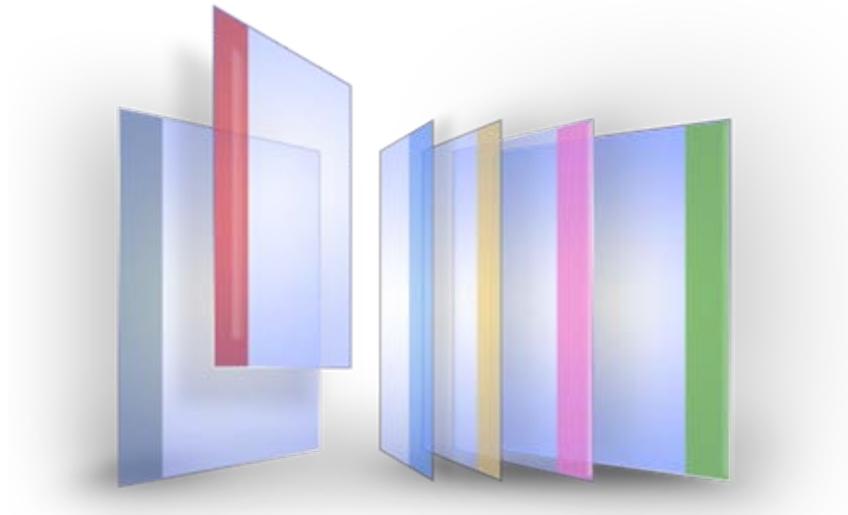
OR

Security Gateway Blades



Security Management Blades





softwareblades from Check Point

Secure

Flexible

Simple



Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point R70 Technology

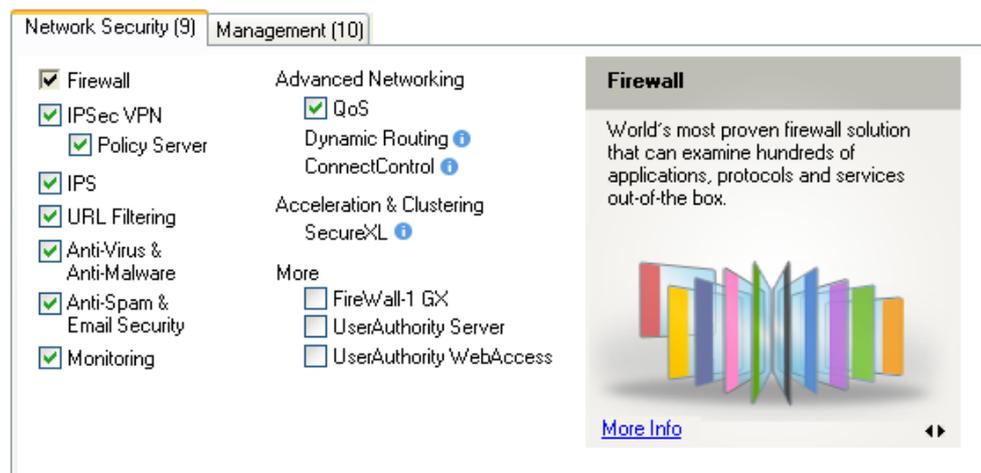


totalsecurity™



[Unrestricted]—For everyone

- R70 release featuring Software Blade architecture



New **IPS Software Blade**

Improved **Core Firewall Performance**

New **Provisioning Software Blade**



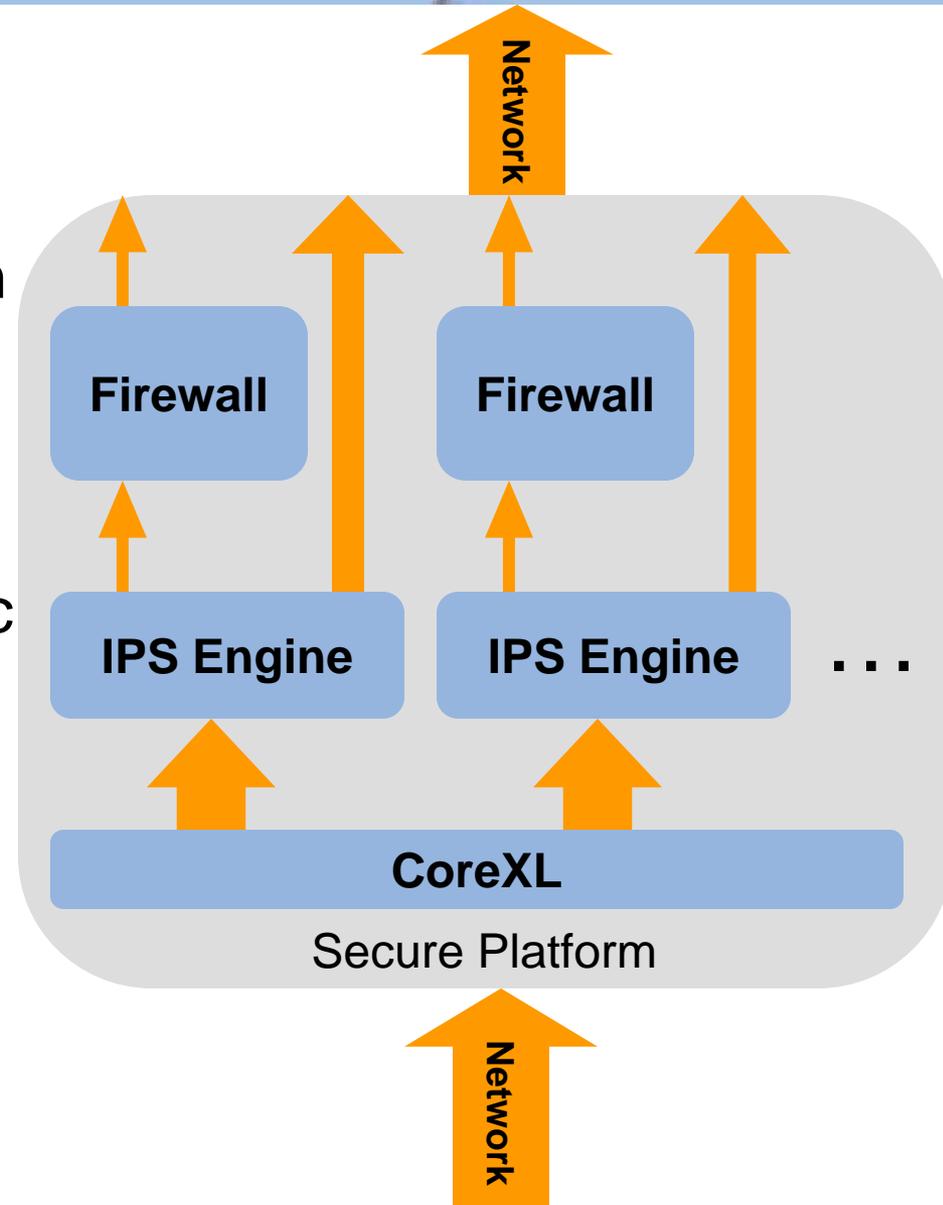
Check Point
SOFTWARE TECHNOLOGIES LTD.

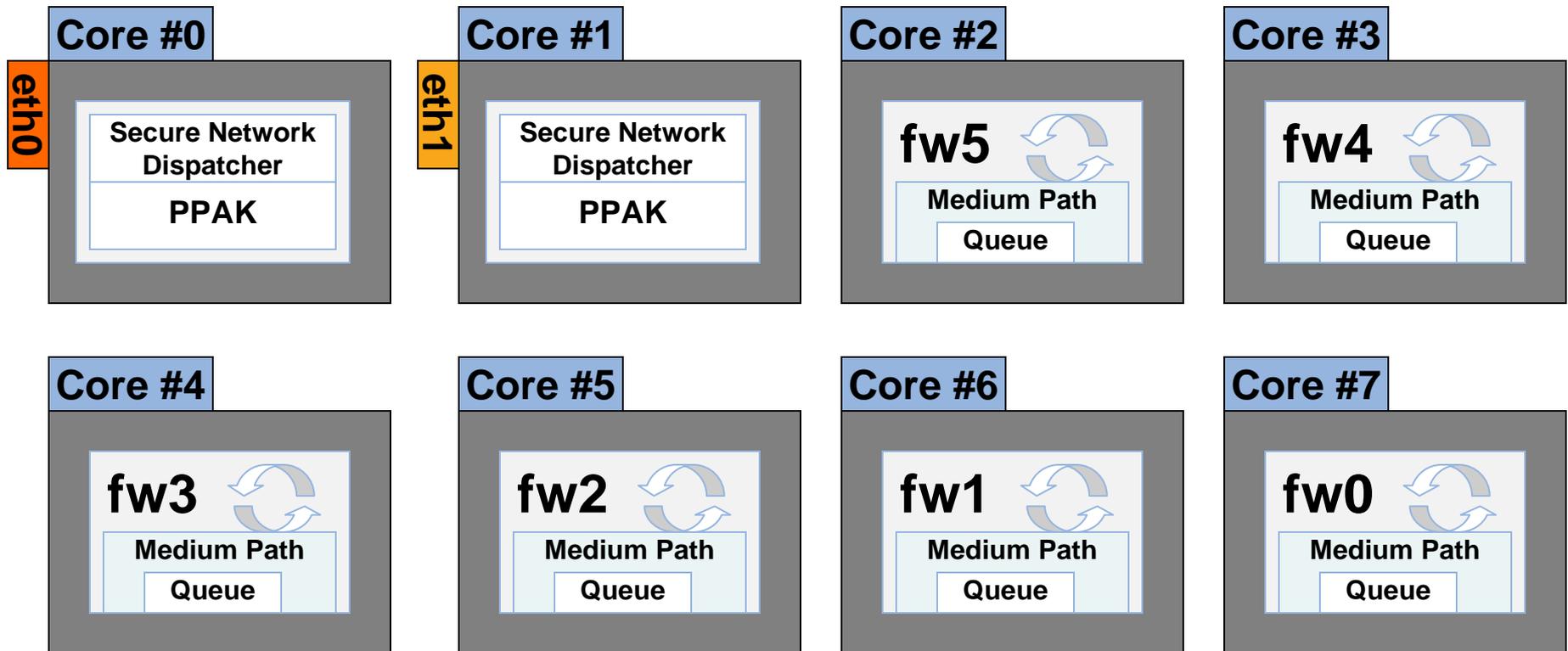
R70 architecture



totalsecurity™
[Unrestricted]—For everyone

- 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





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



Check Point
SOFTWARE TECHNOLOGIES LTD.

R70 Technical



totalsecurity™



[Unrestricted]—For everyone

192.168.1.170 - Check Point SmartDashboard - IPS

File Edit View Manage Rules Policy SmartMap Search Window Help

Check Point SmartDashboard

Firewall NAT **IPS** Anti-Spam & Mail Anti-Virus & URL Filtering SSL VPN IPsec VPN QoS Desktop

- Overview
- Enforcing Gateways
- Profiles
- Protections
 - By Type
 - Signatures
 - Protocol Anomalies
 - Application Controls
 - Engine Settings
 - By Protocol
 - Network Security
 - Application Intelligence
 - Web Intelligence
 - DoS Defender
- Network Exceptions
- Download Updates
- Follow Up

Overview

IPS provides protection from network, application and web attacks. [Demo](#) | [Forum](#)

IPS in My Organization

1 gateway is enforcing IPS
4 profiles are configured

Profile	IPS Mode	Activation	GWs
Default_...	Prevent	IPS Policy	0 GWs
Detect_All	Detect	IPS Policy	0 GWs
Prevent_all	Prevent	IPS Policy	1 GWs

Messages and Action Items

- IPS protections are up to date
- All contracts are up to date
- [20 protections are marked for Follow Up](#)

[View Events](#) | [Manage Events](#) | [View Reports](#)

Security Status

Number of events handled by IPS during the last: Hour 24 Hours Week Month

Last updated on Tuesday, Mar 10, 2009 12:05:05 [Refresh](#)

Security Center

- Tue, 03 Mar 2009** High
Update Protection against ProFTPD Server Username Handling SQL Injection
[Open](#)
- Tue, 03 Mar 2009** High
Update Protection against UltraVNC VNCViewer Authenticate Buffer Overflow
[Open](#)
- Thu, 26 Feb 2009** Critical
Update Protection against Microsoft Excel Rich Text Parsing Zero-Day Remote Code Executio...
[Open](#)

Done.

192.168.1.170

Read/Write

©2009 Check Point Software Technologies Ltd. All rights reserved.

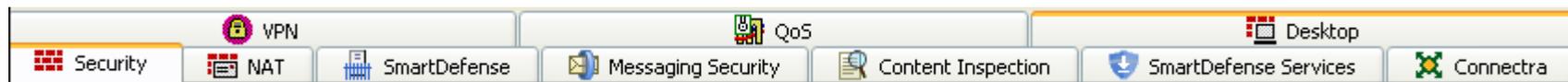
[Unrestricted]—For everyone

17

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

Check Point Gateway - R70

Check Point Gateway - General Properties

Machine

Name: R70 Color: [Black]

IP Address: 192.168.1.170 [Get address]

Comment: []

Secure Internal Communication

Communication... DN: cn=cp_mgmt,o=R70.vks5wv

Platform

Hardware: Open server Version: R70 OS: SecurePlatform [Get]

Software Blades

Network Security Blades: Package 7 Management Blades: Package 6

Network Security (7) Management (5)

Firewall
 IPSec VPN
 Policy Server
 IPS
 URL Filtering
 Anti-Virus & Anti-Malware
 Anti-Spam & Email Security
 Monitoring

Advanced Networking

QoS
Dynamic Routing [i]
ConnectControl [i]

Acceleration & Clustering

SecureXL [i]

More

FireWall-1 GX
 UserAuthority Server
 UserAuthority WebAccess

Firewall

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

[More Info](#)

OK Cancel Help

The screenshot shows the 'Protections' browser interface. On the left is a navigation tree with categories like Overview, Enforcing Gateways, Profiles, and Protections. The main area displays a table of security signatures. The table has columns for Signature, Severity, Confidence, Performance, Industry Reference, Release Date, Default Status, Recommendation, and Detection. A search bar at the top allows filtering by signature, category, or CVE. Buttons for 'Profiles...', 'Protection Actions...', and 'View...' are also present.

Signature	Severity	Confide...	Perfor...	Industry Referen...	Relea...	Default...	Recom...	Detect...
Squid HTTP Version Number ...	High	Medium...	Low	CVE-2009-0478	23/02/2009	Inactive	Prevent	Detect
Oracle TimesTen In-Memory ...	High	Medium	Medium	CVE-2008-5440	23/02/2009	Inactive	Prevent	Detect
Oracle Secure Backup NDM...	Critical	Medium	Medium	CVE-2008-5444	23/02/2009	Inactive	Prevent	Detect
Oracle Secure Backup Multipl...	Critical	Medium	Medium	CVE-2008-5448; ...	23/02/2009	Inactive	Prevent	Detect
DNS TXT Record Parsing Bu...	High	Medium...	Medium	CVE-2008-2469	22/02/2009	Inactive	Prevent	Detect
Oracle Database SYS.OLAPL...	Critical	Medium	Medium	CVE-2008-3974	15/02/2009	Inactive	Prevent	Detect
Sun Solstice AdminSuite sad...	Critical	Medium...	Low	CVE-2008-4556	15/02/2009	Inactive	Prevent	Detect
Microsoft Exchange Server M...	Critical	Medium...	Low	CVE-2009-0098	10/02/2009	Inactive	Prevent	Detect
Microsoft Exchange Server E...	Critical	Medium	Medium	CVE-2009-0099	10/02/2009	Inactive	Prevent	Detect
Microsoft Visual Basic Kill Bits	High	Medium	Low	None	10/02/2009	Inactive	Prevent	Detect
Internet Explorer CSS Memory...	Critical	Low	Low	CVE-2009-0076	10/02/2009	Prevent	Prevent	Detect
Microsoft Internet Explorer Un...	Critical	Low	Low	CVE-2009-0075	02/02/2009	Prevent	Prevent	Detect
Microsoft Windows WRITE_...	Critical	Medium	Medium	CVE-2008-4114	29/01/2009	Inactive	Prevent	Detect
SMB TRANS2 Request Valid...	Critical	Medium...	Low	CVE-2008-4835	13/01/2009	Inactive	Prevent	Detect
SMB TRANS Request Buffer ...	Critical	Medium...	Low	CVE-2008-4834	13/01/2009	Inactive	Prevent	Detect
Comments Inside JPEG Files	Medium	Medium...	Medium	None	06/01/2009	Inactive	Inactive	Detect
SSL Certificate Forgery via M...	Critical	Medium...	High	None	05/01/2009	Inactive	Inactive	Detect
Thunder	NA	Medium	Medium	None	21/12/2008	Inactive	Inactive	Inactive
Microsoft Word RTF Object P...	Critical	Medium	High	CVE-2008-4027	17/12/2008	Inactive	Prevent	Detect
MS-SQL Server Sp_replwritet...	Critical	Medium	Medium	CVE-2008-5416	16/12/2008	Inactive	Prevent	Detect

- **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!**

SMARTDASHBOARD

File Edit View Manage Rules Policy SmartMap Search Window Help

Security NAT SmartDefense Messaging Security Content Inspection SmartDefense Services Connectra VPN QoS Desktop

- [-] Fingerprint Scrambling
- [-] Successive Events
- [-] DShield Storm Center
- [-] Port Scan
- [-] Dynamic Ports
- [-] Application Intelligence
 - [-] Mail
 - [-] FTP
 - [-] FTP Bounce
 - [-] FTP Security Server
 - [-] Oracle XDB Overflow*
 - [-] FTP Patterns*
 - [-] Microsoft Networks
 - [-] Peer to Peer
 - [-] Instant Messengers
 - [-] DNS
 - [-] VoIP
 - [-] SNMP
 - [-] Syslog*
 - [-] Syslog Relay Servers L...
 - [-] Block Message Length Vi
 - [-] Apply Malicious Code Pro
 - [-] Block Non-Standard Sour
 - [-] Block PRIORITY Field Vi
 - [-] Block TIMESTAMP Field
 - [-] Security Products*
 - [-] Block Alt-N Technologies
 - [-] LANDesk Management Su...

Download Updates

SmartDefense Services

Last updated: 10-Mar-09 17:19
Update version: 602090226

[View SmartDefense Services](#)

SmartDefense Logs

Last Update: 26-February-2009

References: [SmartDefense Service FAQ](#)

Recent updates:

Version	Contents	Date
618090223	Oracle Secure Backup Multiple Command Injections	23-February-2009
618090223	Oracle Secure Backup NDMP CONECT_CLIENT_AUTH Command Buffer Overflow	23-February-2009

*localdb Read/Write 100% 17:35

192.168.1.170 - Check Point SmartDashboard - IPS

File Edit View Manage Rules Policy SmartMap Search Window Help

Check Point SmartDashboard

Firewall NAT IPS Anti-Spam & Mail Anti-Virus & URL Filtering SSL VPN IPsec VPN QoS Desktop

Overview

Overview

IPS provides protection from network, application and web attacks. [Demo](#) [Forum](#)

IPS in My Organization

1 gateway is enforcing IPS
4 profiles are configured

Profile	IPS Mode	Activation	GWs
Default_...	Prevent	IPS Policy	0 GWs
Detect_All	Detect	IPS Policy	0 GWs
Prevent_all	Prevent	IPS Policy	1 GWs

Messages and Action Items

- IPS protections are up to date
- All contracts are up to date
- [20 protections are marked for Follow Up](#)

[View Events](#) [Manage Events](#) [View Reports](#)

Security Status

Number of events handled by IPS during the last: Hour 24 Hours Week Month

Legend:
■ Detected
■ Prevented
■ Average in My Organization

Last updated on Tuesday, Mar 10, 2009 17:37:14 [Refresh](#)

Security Center

Sun, 01 Mar 2009 High
 Update Protection against Squid HTTP Version Number Parsing Denial of Service Vulnerability
[Open](#)

Tue, 03 Mar 2009 High
 Update Protection against ProFTPD Server Username Handling SQL Injection
[Open](#)

Tue, 03 Mar 2009 High
 Update Protection against UltraVNC VNCViewer Authenticate Buffer Overflow
[Open](#)

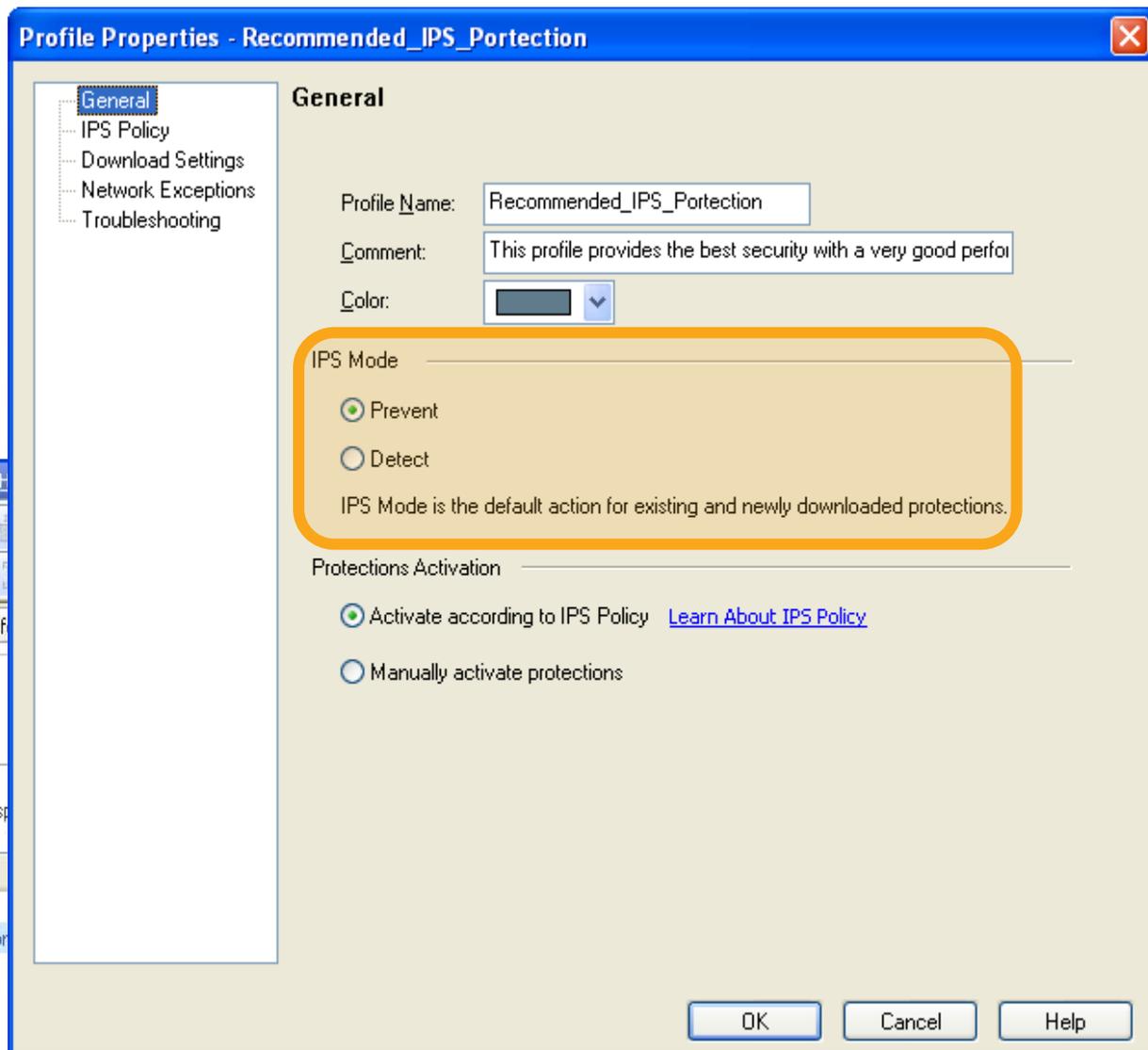
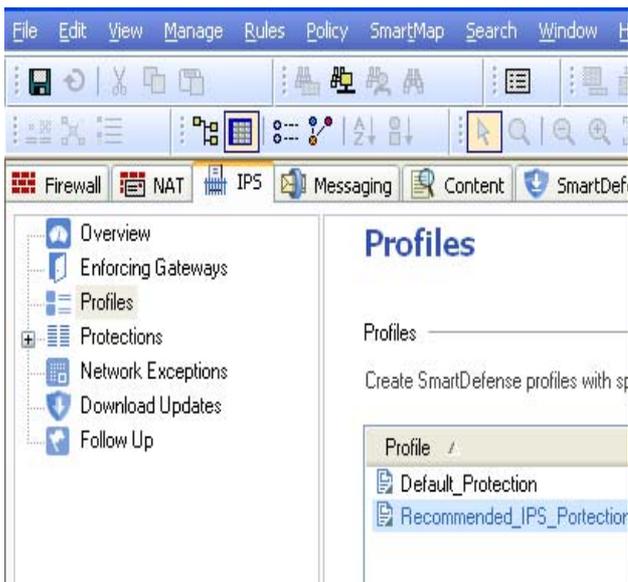
Done. 192.168.1.170 Read/Write

start | Inbox... | 3 Wi... | Micros... | Free ... | 192.1... | *local ... | 192.1... | 100% | 17:37

- 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**



Follow Up



Mark newly downloaded protections for Follow Up

Trial Mode

2 profiles are using Trial Mode to detect-only protections while in Follow Up

Manage...

Protections marked for follow up

Look for:

Search In:

All

Clear

Mark...

Unmark

Protection Actions...

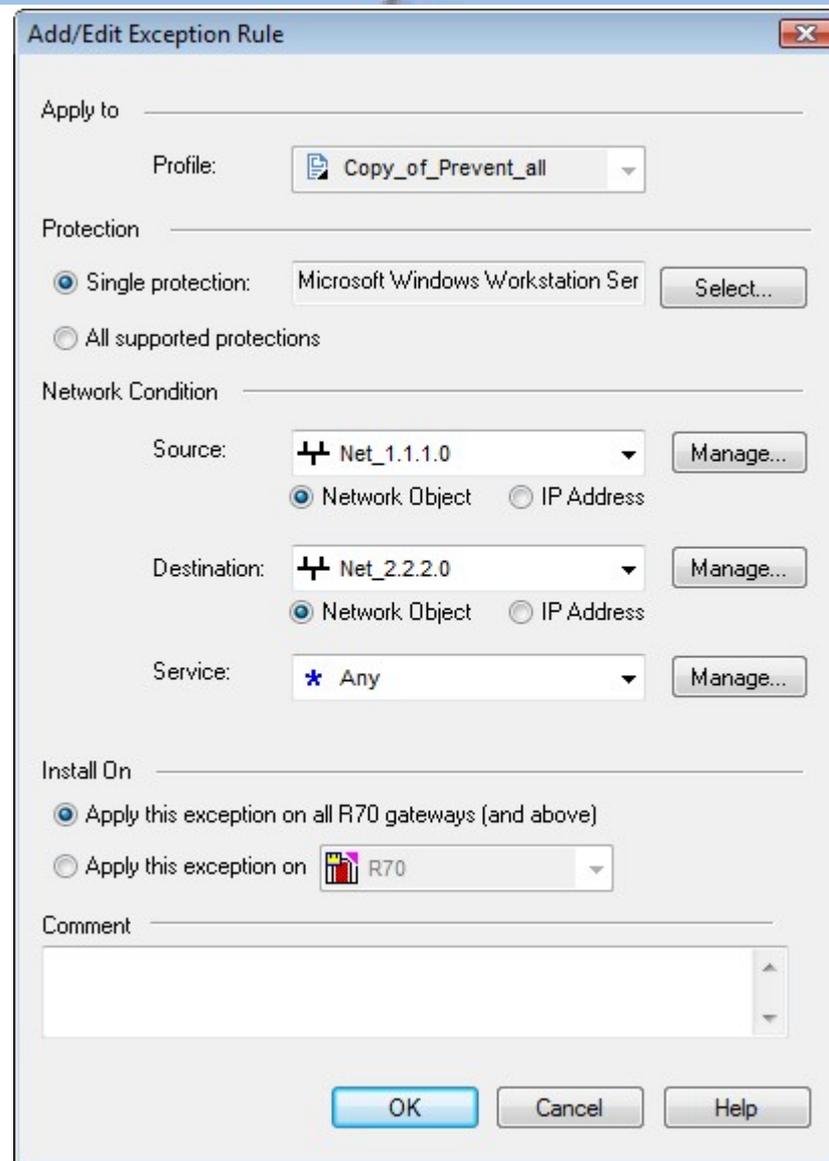
View...

Protection				Industry Referen...	Release D...	Follow Up Comment ^		Recommended_Profile
Microsoft Word RTF styleshe...				CVE-2008-4031	12/09/2008	Newly downloaded protection; automatically marked for follo...		Detect
Sun Solaris rpc.yppupdated Co...				CVE-1999-0208	11/18/2008	Newly downloaded protection; automatically marked for follo...		Detect
Microsoft Internet Explorer HT...				CVE-2008-4261	12/09/2008	Newly downloaded protection; automatically marked for follo...		Detect
Microsoft Internet Explorer U...				CVE-2008-4260	12/09/2008	Newly downloaded protection; automatically marked for follo...		Detect
Microsoft Internet Explorer W...				CVE-2008-4259	12/09/2008	Newly downloaded protection; automatically marked for follo...		Detect
Microsoft Internet Explorer X...				CVE-2008-4844	12/11/2008	Newly downloaded protection; automatically marked for follo...		Detect
Microsoft Internet Explorer Cr...				CVE-2008-3474	10/14/2008	Newly downloaded protection; automatically marked for follo...		Inactive

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

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

Host Port Scan		R70
Non-MDS Authenticated B...	Go to Advisory	R70
Null payload ICMP packet	Open Protection...	R70
DCE-RPC interface scanni...	Add Exception...	R70
Invalid TCP packet - source / destina...	eth2	R70
Version Information Leak Detected o...	eth2	R70
RIP Protocol Version Is Not 2	eth2	R70



Add/Edit Exception Rule

Apply to _____

Profile:  Copy_of_Prevent_all ▾

Protection _____

Single protection: Microsoft Windows Workstation Ser 

All supported protections

Network Condition _____

Source:  Net_1.1.1.0 ▾ 

Network Object IP Address

Destination:  Net_2.2.2.0 ▾ 

Network Object IP Address

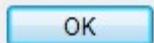
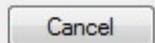
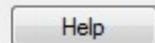
Service: * Any ▾ 

Install On _____

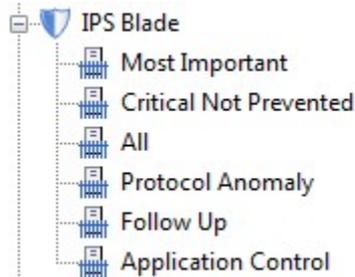
Apply this exception on all R70 gateways (and above)

Apply this exception on  R70 ▾

Comment _____

■ New IPS Blade Section



■ New Details view

Record Details

Previous Next Copy Switch Colors

MS-RPC over CIFS Inspection Properties
DCE-RPC Enforcement Violation

Severity: High
Confidence Level: Medium

Product	SmartDefense
Date	8Mar2009
Time	16:36:57
Number	1536
Type	Log
Origin	R70

Source	Ubuntu (2.2.2)
Destination	XP (1.1.1.1)
Service	microsoft-ds (445)
Protocol	TCP tcp
Interface	eth2
Source Port	34671

Policy Name	Standard
Policy Date	Sun Mar 08 16:34:47 2009
Policy Management	R70
SmartDefense Profile	Recommended_Protection

Action	Reject
Protection Name	MS-RPC over CIFS Inspection Properties
Attack	DCE-RPC Enforcement Violation
Attack Information	Unallowed number of context items in Bind/Alter context request
CVE	CVE-2005-0533
Severity	High
Confidence Level	Medium
Performance Impact	Medium
Protection Type	Signature
Follow Up	Not Followed

Resource	...
Packet Capture	...
Reject ID	...

Information	...
--------------------	-----

Attack ID: [CPAI-2005-136](#)

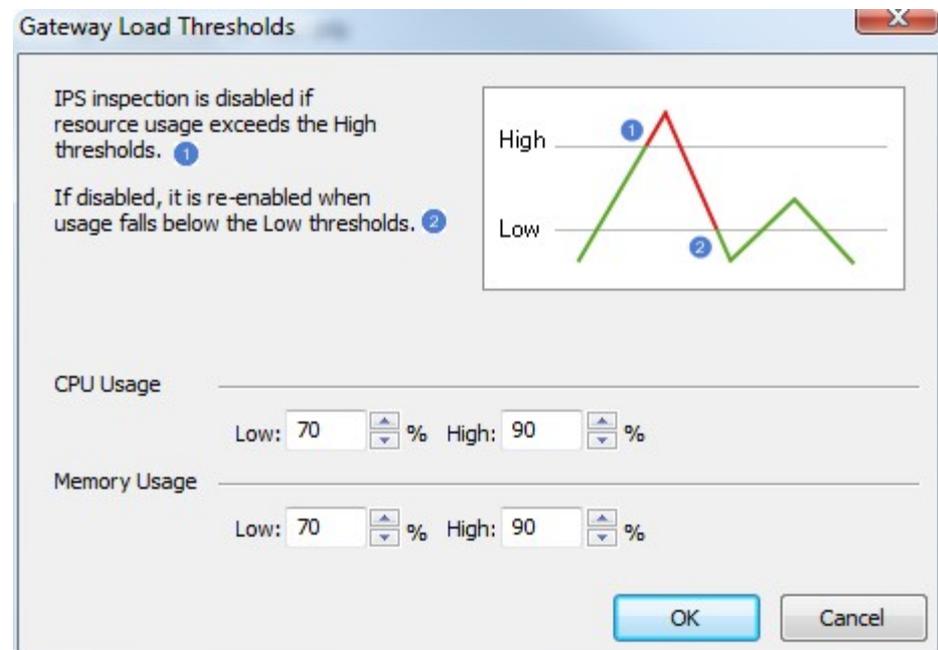
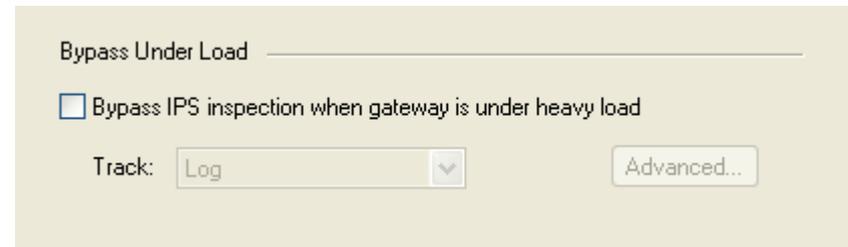
Last Update: 09-October-2005

Industry References: [CVE-2005-0533](#)

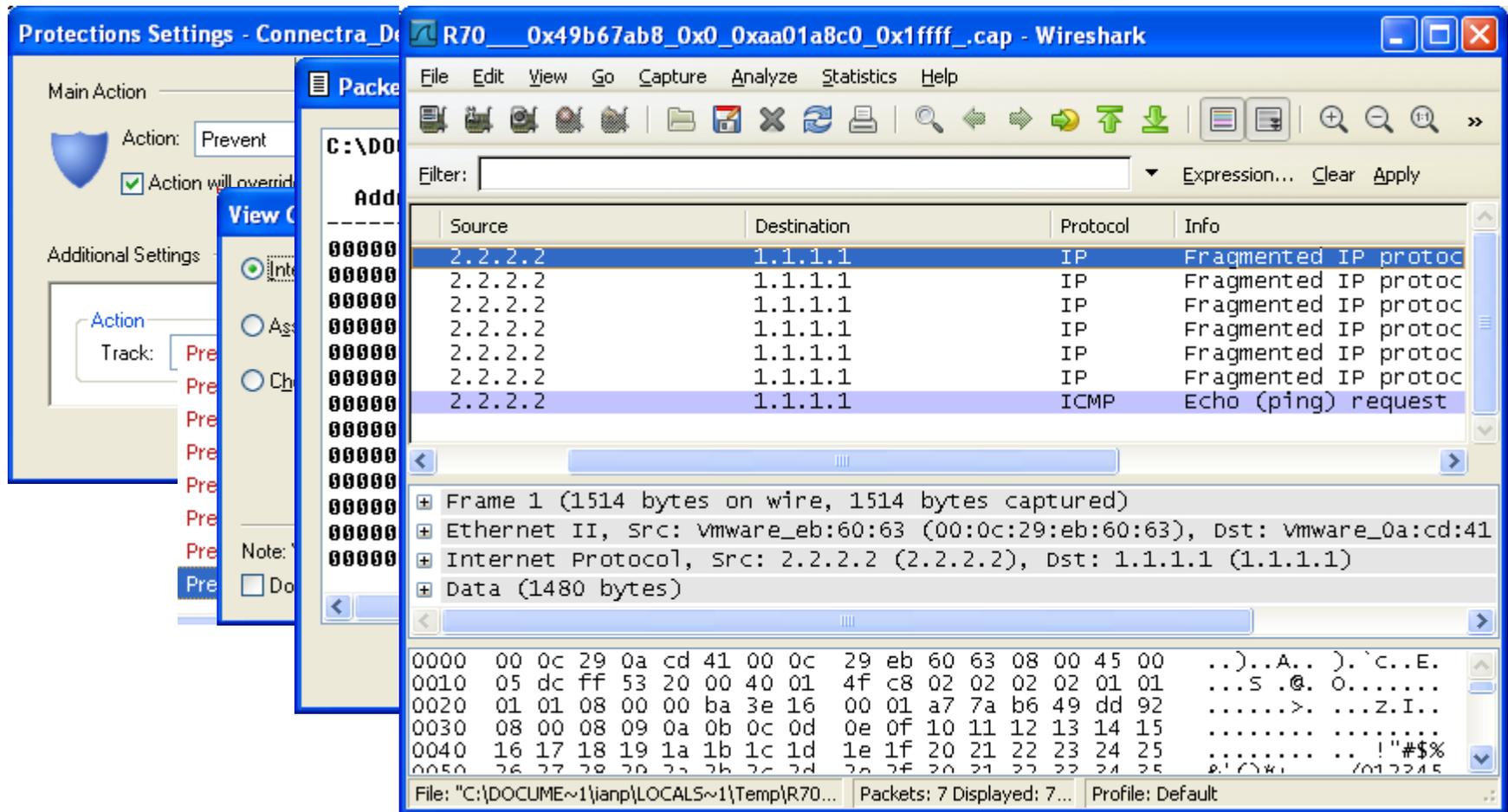
Security Category: R70

Abort Close

- **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.



- Integrated Packet Capture



The screenshot shows two overlapping windows. The background window is 'Protections Settings - Connectra_D...'. The foreground window is 'R70__0x49b67ab8_0x0_0xaa01a8c0_0x1ffff_.cap - Wireshark'. The Wireshark window displays a list of captured packets with the following table:

Source	Destination	Protocol	Info
2.2.2.2	1.1.1.1	IP	Fragmented IP protoc
2.2.2.2	1.1.1.1	IP	Fragmented IP protoc
2.2.2.2	1.1.1.1	IP	Fragmented IP protoc
2.2.2.2	1.1.1.1	IP	Fragmented IP protoc
2.2.2.2	1.1.1.1	IP	Fragmented IP protoc
2.2.2.2	1.1.1.1	IP	Fragmented IP protoc
2.2.2.2	1.1.1.1	ICMP	Echo (ping) request

The selected packet (Frame 1) details are shown below:

- Frame 1 (1514 bytes on wire, 1514 bytes captured)
- Ethernet II, Src: vmware_eb:60:63 (00:0c:29:eb:60:63), Dst: vmware_0a:cd:41
- Internet Protocol, Src: 2.2.2.2 (2.2.2.2), Dst: 1.1.1.1 (1.1.1.1)
- Data (1480 bytes)

The packet bytes pane shows the following hex and ASCII data:

```
0000 00 0c 29 0a cd 41 00 0c 29 eb 60 63 08 00 45 00  ..)..A.. ).`c..E.
0010 05 dc ff 53 20 00 40 01 4f c8 02 02 02 01 01  ...S .@. O.....
0020 01 01 08 00 00 ba 3e 16 00 01 a7 7a b6 49 dd 92  .....>. ...Z.I..
0030 08 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#$$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  8'()@k /012345
```

- **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 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



total**security**[™]



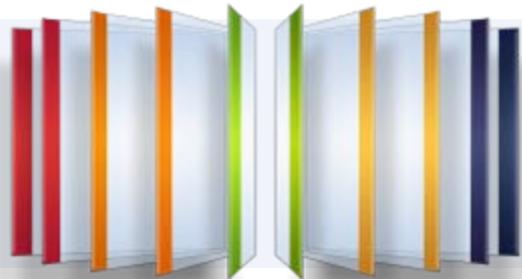
[Unrestricted]—For everyone



Expanded **Power-1** Appliances!



New **IP** Appliance Line!



Software Blade Architecture!

- Enables tailored solutions for every business need

- Centrally Managed

- Expands without additional hardware or management complexity

- Delivers low-cost ownership and cost-efficient protection



NEW!



Power-1 11000 Series



Power-1 9075



Power-1 5075



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 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:** Solution for enterprises and data centers



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

Key Differentiators



Simple field performance upgrades

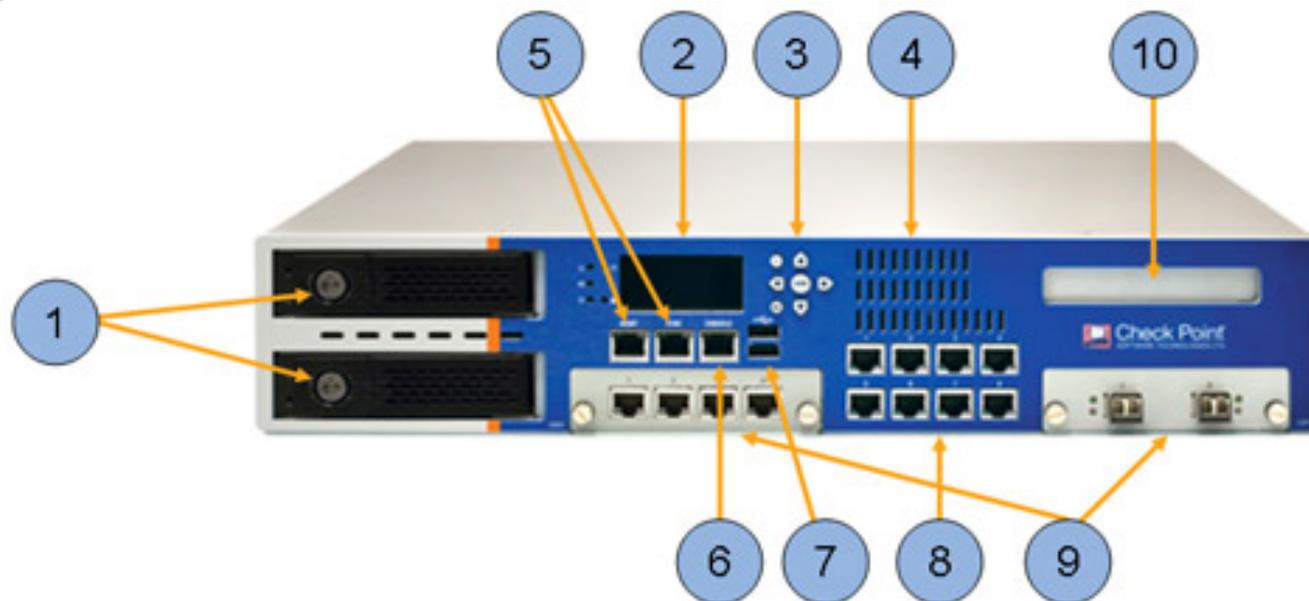
Up to 25 Gbps firewall performance in a 2U form factor

Flexible, extensible, investment protection



Field Performance Upgradability

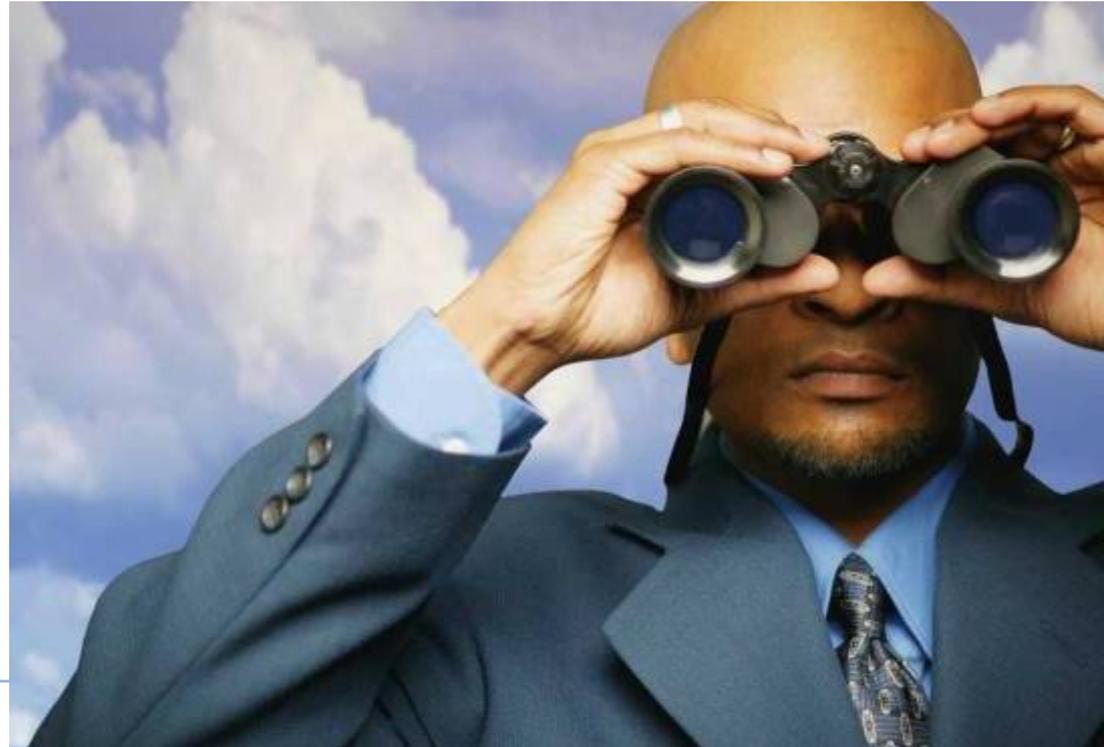




1. Redundant hot-swappable hard drives
2. LCD display
3. LCD control buttons
4. Air intake
5. Management & Sync ports
6. Console port
7. USB ports

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

- 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



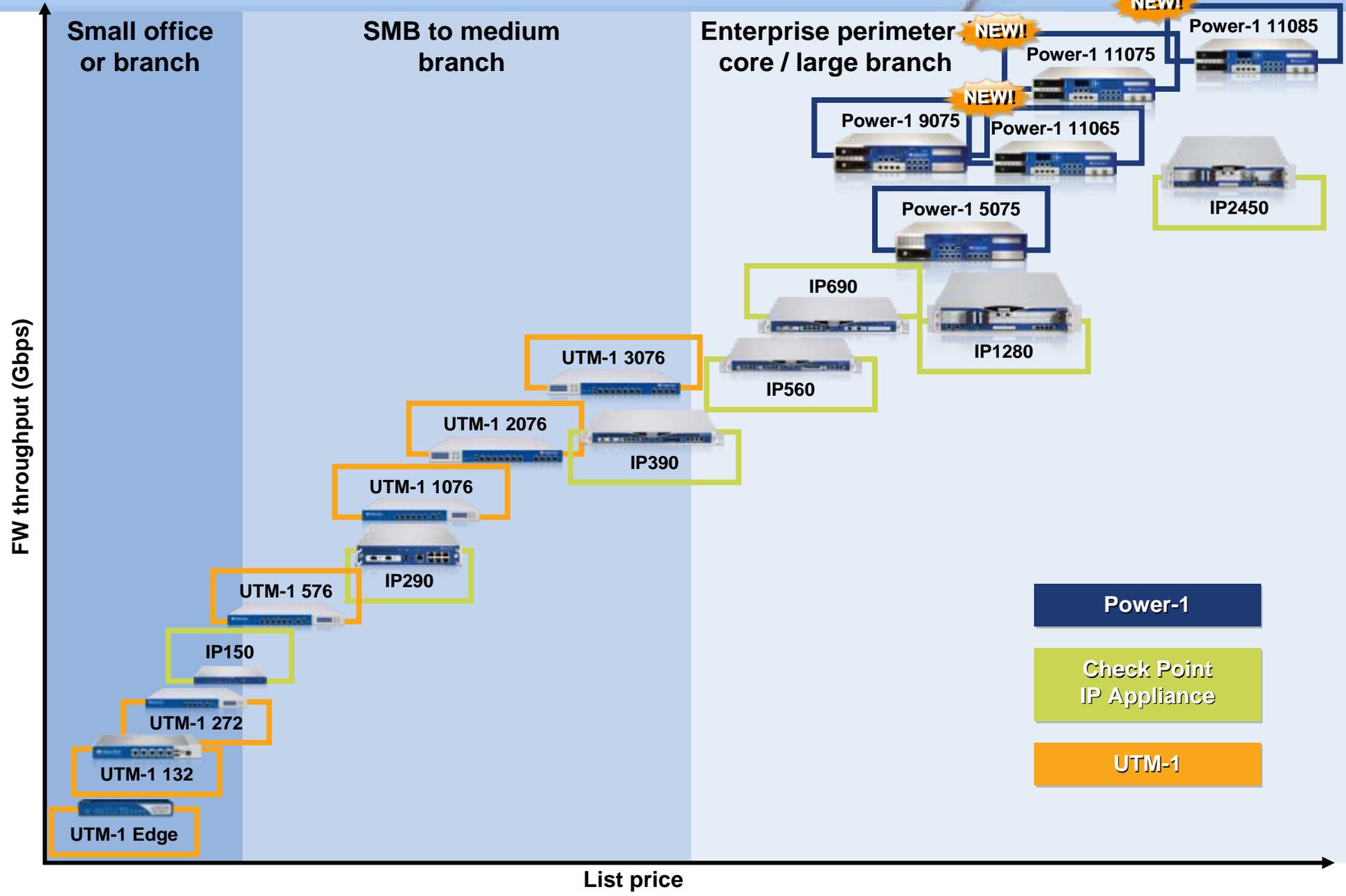
gatewayblade 	firewall
gatewayblade 	IPsec VPN
gatewayblade 	IPS
gatewayblade 	acceleration & clustering
gatewayblade 	advanced networking
gatewayblade 	web security
gatewayblade 	voice over IP
gatewayblade 	URL filtering
gatewayblade 	anti-virus & anti-malware
gatewayblade 	anti-spam & email security

 Security perpetual blade

 Security service blade

totalsecurity™

Check Point Appliance Line



Check Point Appliances + R70

Maximum security and performance

Streamlined deployment and maximum flexibility

Manageability, modularity and field upgradability

