



Check Point®

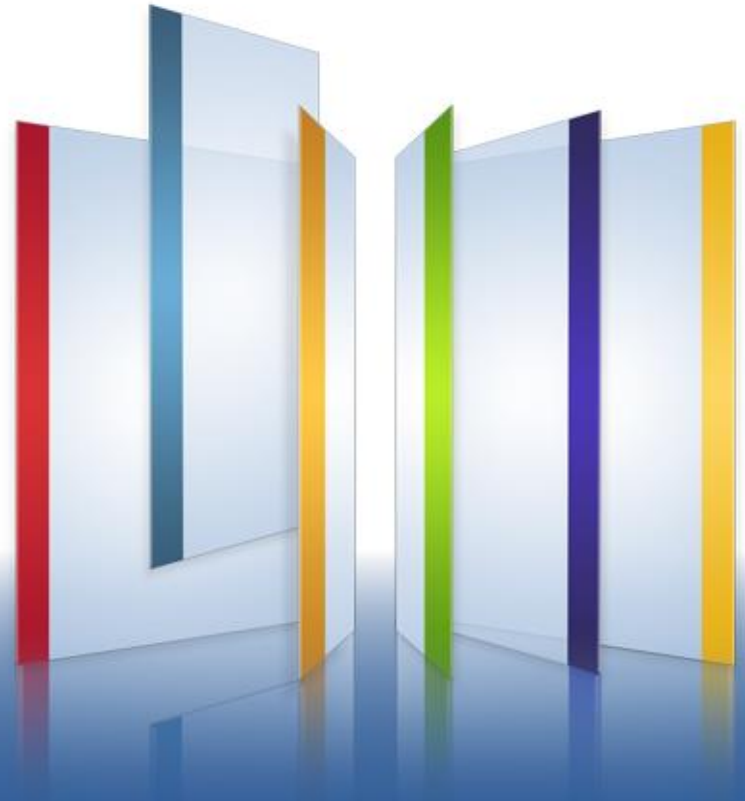
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Koncepty v zabezpečení DMZ infrastruktury proti aktuálním kybernetickým útokům

Martin Koldovský

mkoldov@checkpoint.com



- In computer security, a DMZ is a **physical or logical subnetwork** that **contains and exposes an organization's external-facing services** to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.
- The name is derived from the term "demilitarized zone", an area between nation states in which military action is not permitted.
- [http://en.wikipedia.org/wiki/DMZ_\(computing\)](http://en.wikipedia.org/wiki/DMZ_(computing))

- Vyčlenění služeb do **speciálně vytvořené zóny** pro flexibilnější **řízení přístupu**
 - přístup uživatelů na služby **z Internetu**
 - oddělení **klientských PC** a služeb
 - bezpečný vzdálený přístup poboček, partnerů a jednotlivých uživatelů **přes VPN**

3 oblasti

- Prostředky řízení přístupu
- Management
- Infrastruktura

- **Firewall**
- **Identity Awareness**
- **IPS – Intrusion Prevention**
- **Web Security**
- **Ochrana před DDoS útoky**

- Centrální sběr logů z mnoha bran a vrstev
- Prohledávání logů – Google pro logy
- Identifikace bezpečnostních incidentů
- Reporting
- Správa konzistentních a přehledných bezpečnostních politik
- Workflow změn politik a jejich audit
- Integrovaná kontrola splňování norem a best practices (Compliance Blade)

- Inspekce šifrovaného provozu – HTTPS
- Zabezpečení virtualizace – Virtual Edition
- Virtualizovaná bezpečnost – Virtual Systems

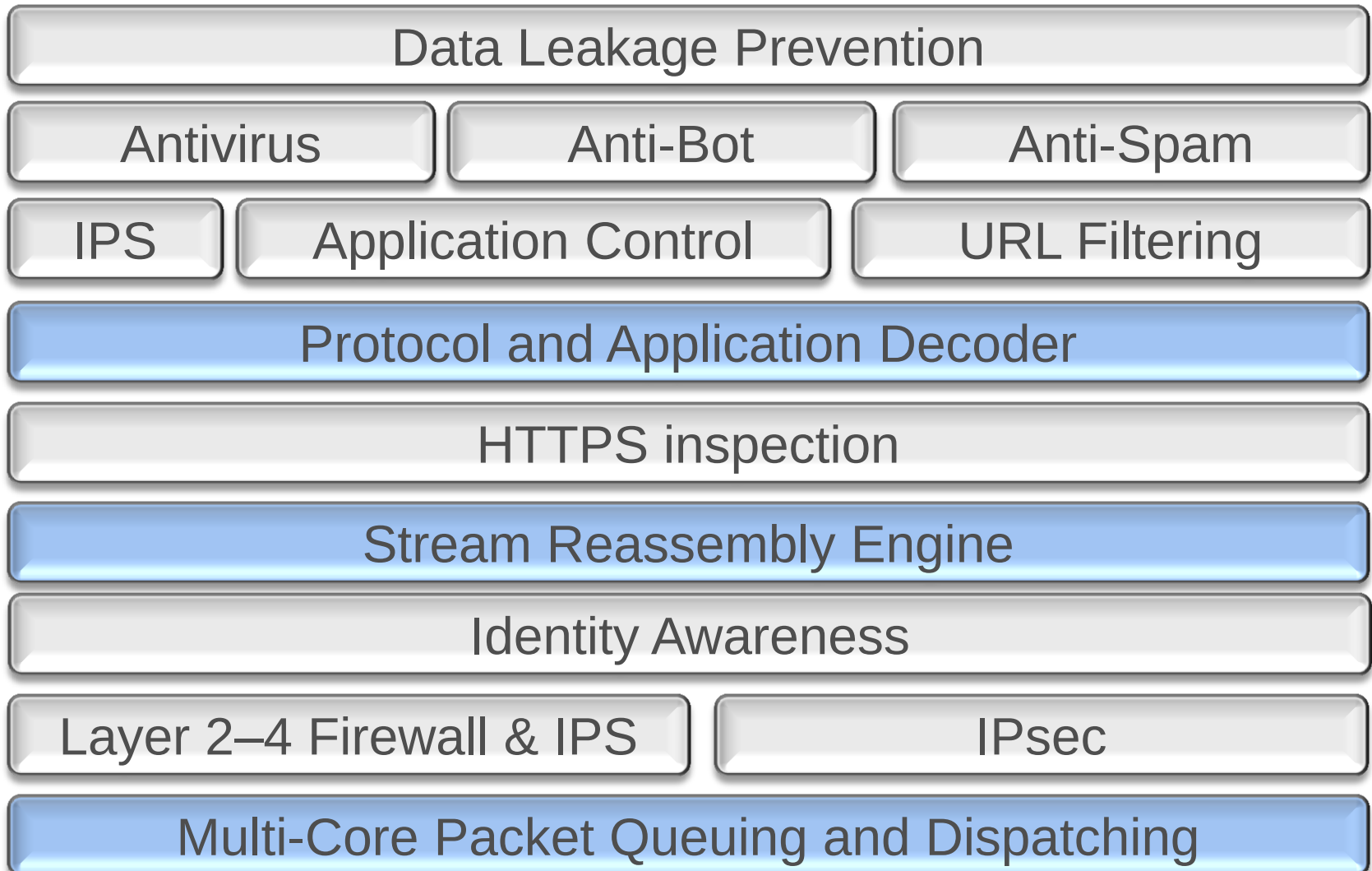


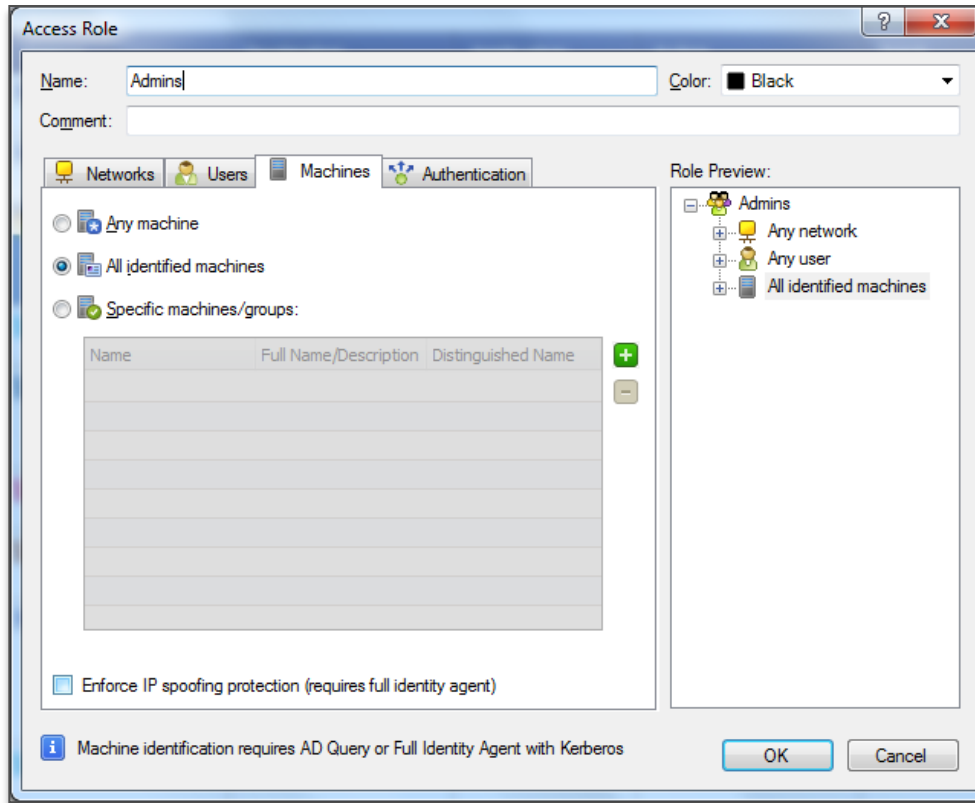
Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Řízení přístupu







- Politiky založené na **rolích uživatelů**, ne pouze na IP adresách sítí a počítačů
- Uživatel, zařízení, lokalita



Srovnání některých zdrojů identity

Requirement	AD Query	Captive Portal	Identity Agent Lite	Identity Agent Full
Agent Deployment	Clientless	Clientless	Resident	Resident
Requires Admin Privileges	Unique - No agent on AD - No additional server		No	Yes
Transparent Authentication	●	Captive portal Web auth	●	●
Machine Identity	●			●
Detect IP Spoofing				●
Logoff & IP Change Detection	Delayed	Keep window open option		●
Basic Security Strength Excellent				

IPS: přehled ochran

Demo Mode - Check Point SmartDashboard R75.20 - IPS

File Edit View Manage Rules Policy SmartWorkflow Search Window Help

Firewall NAT IPS Application & URL Filtering Anti-Spam & Mail Mobile Access Anti-Virus Data Loss Prevention IPSec VPN QoS Desktop

Overview
Enforcing Gateways
Profiles
Protections
By Type
Signatures
Protocol Anomalies
Application Controls
Engine Settings
By Protocol
IPS Software Blade
Network Security
Application Intelligence
Web Intelligence
IPS-1 Sensor
Network Security - I
Application Intelligence
Web Intelligence - I
Geo Protection
Network Exceptions
Download Updates
Follow Up
Advanced
HTTP Inspection
HTTPS Inspection
Policy
Gateways
Trusted CAs
HTTPS Validation

Protections

Look for: In: Products:

Show additional filters

Protection	Severity	Confidence Level	Performance Impact	Industry Reference	Release Date	Products	Supported From	Default	Recommend	Sort...
Internet Explorer Invalid Pointer R...	Critical	High	Low	CVE-2010-0249	17.01.2010	IPS Blade R65	R65	Inactive	Prevent	Customize...
Adobe Reader U3D DLL Loading...	Critical	High	Low	CVE-2009-3954	13.01.2010	IPS Blade R65	R65	Inactive	Prevent	Hide Description
PDF Files Containing Timed Java...	Medium	High	Medium	CVE-2009-3956	12.01.2010	IPS Blade R70	R70	Inactive	Inactive	Export View...
Adobe Reader JPEG2000 Regio...	Critical	High	Medium	CVE-2009-3955	12.01.2010	IPS Blade R70	R70	Inactive	Prevent	Inactive
Adobe Reader Plugin Malformed ...	Medium	High	Medium	CVE-2007-00...	12.01.2010	IPS Blade R65	R65	Inactive	Prevent	Prevent
HP Operations Manager Server ...	Critical	High	Low	CVE-2009-3843	30.12.2009	IPS Blade R70	R70	Inactive	Prevent	Prevent
HP OpenView Network Node Ma...	Critical	High	Medium	CVE-2009-41...	30.12.2009	IPS Blade R70	R70	Inactive	Prevent	Prevent
PDF Containing Obfuscated Java...	High	High	Low	None	29.12.2009	IPS Blade R65	R65	Inactive	Prevent	Prevent
PDF Containing Obfuscated Nam...	High	High	Medium	None	29.12.2009	IPS Blade R65	R65	Inactive	Inactive	Inactive
HP OpenView Network Node Ma...	High	High	Medium	CVE-2009-4179	29.12.2009	IPS Blade R70	R70	Inactive	Prevent	Prevent
HP OpenView Network Node Ma...	High	High	Medium	CVE-2009-4178	29.12.2009	IPS Blade R70	R70	Inactive	Prevent	Prevent
Microsoft IIS Filename Extension ...	High	High	Low	CVE-2009-4444	28.12.2009	IPS Blade R65	R65	Inactive	Prevent	Prevent
Adobe Flash Media Server Reso...	Critical	High	Low	CVE-2009-3791	22.12.2009	IPS Blade R70	R70	Inactive	Prevent	Prevent

Attack ID: [CPAI-2010-013](#)

Last Update: 17-January-2010

Industry References: [CVE-2010-0249](#)

Supported Products: VPN-1 Power/UTM: NGX R65

Security Gateway: R70, R71

Demo Mode Write Mode



IPS v detailu

Protection type

- Signature
- Protocol
- Application
- Engine

Severity

- Critical
- High
- Medium
- Low

Confidence Level

- High
- Medium-high
- Medium
- Medium-Low
- Low

Performance Impact

- Critical
- High
- Medium
- Low

Protection Type

- Server
- Clients

Microsoft Visual Basic ActiveX Controls Remote Code Execution (MS08-070)

Type: **Signature** Severity: **Critical** Confidence Level: **Medium-high** Performance Impact: **Low** Protection Type: **Clients**

Protections Settings - My_Profile - Microsoft Visual Basic ActiveX Controls Remote Code Execution (MS08-070)

Main Action

☒ Action according to IPS Policy: Prevent
☐ Override IPS Policy with: Prevent

Logging Settings

Track: Log ☐ Capture Packets

OK Cancel Help

Edit... Change Action... Follow Up... View Logs

Prevent on All Profiles
Detect on All Profiles
Deactivate on All Profiles

Cancel Help

Supported on  **IPS Software Blade**



Geo Protection

Demo Mode - Check Point SmartDashboard R75.20 - IPS

File Edit View Manage Rules Policy SmartWorkflow Search Window Help

Firewall NAT IPS Application & URL Filtering Anti-Spam & Mail Mobile Access Anti-Virus Data Loss Prevention IPSec VPN QoS Desktop

Overview
Enforcing Gateways
Profiles
Protections
By Type
Signatures
Protocol Anomalies
Application Controls
Engine Settings
By Protocol
IPS Software Blade
Network Security
Application Intelligence
Web Intelligence
IPS-1 Sensor
Network Security - I
Application Intelligence - I
Web Intelligence - I
Geo Protection
Network Exceptions
Download Updates
Follow Up
Advanced
HTTP Inspection
HTTPS Inspection
Policy
Gateways
Trusted CAs
HTTPS Validation

Geo Protection

Block network traffic to and from any country.

Profile: Action: Exceptions... View Logs

Policy for Specific Countries

Country	Action	Direction	Track	Comment
Norway	Block	From and To Country	Log	Block the Vikings! :-)

Add... Edit... Remove

Policy for Other Countries
 Allow Track: Advanced

Policy Preview

Traffic From Country



Traffic To Country



Demo Mode Write Mode

DDoS Attack Information

Network Flood



High volume of
packets

Server Flood



High rate of
new sessions

Application



Web / DNS
connection-
based attacks

Low & Slow Attacks



Advanced
attack
techniques

Multi-Layer DDoS Protection

Network Flood



**Behavioral
network
analysis**

Stateless and
behavioral
engines

Server Flood



**Automatic and
pre-defined
signatures**

Protections
against misuse
of resources

Application



**Behavioral
HTTP and
DNS**

Challenge /
response
mitigation
methods

**Low & Slow
Attacks**



**Granular
custom filters**

Create filters that
block attacks
and allow users

Layers Work Together

Protection Layers Flow

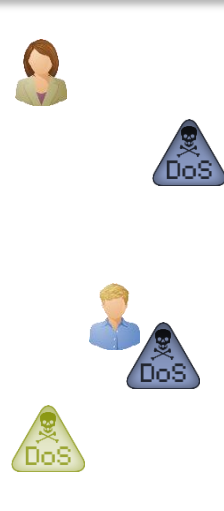
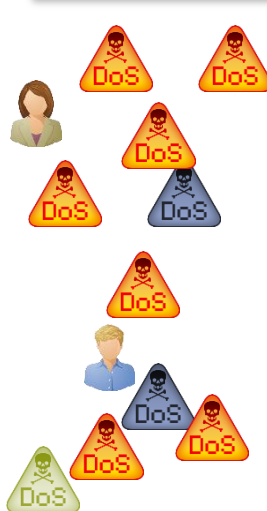
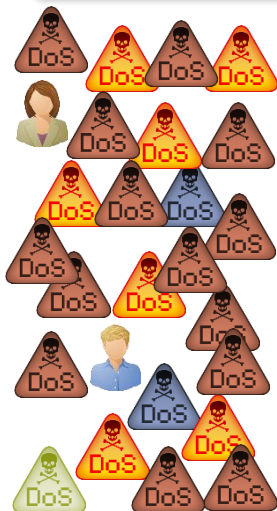
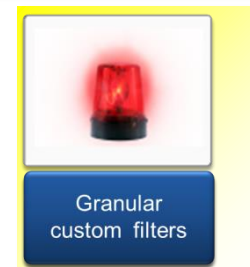
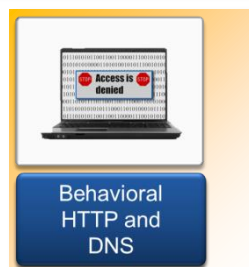
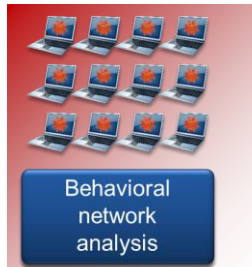
**Network
Flood**

**Server
Flood**

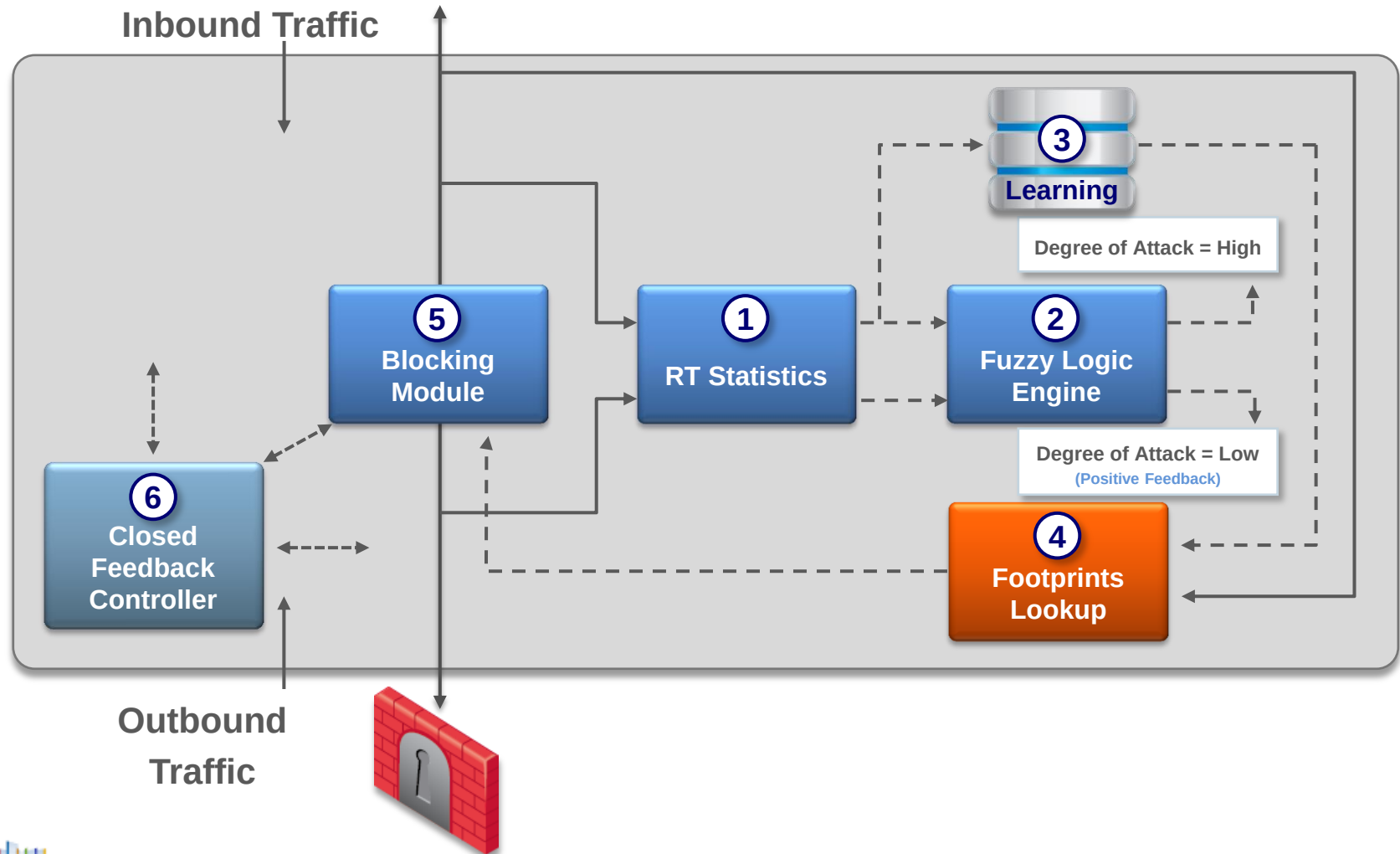
Application

**Low & Slow
Attacks**

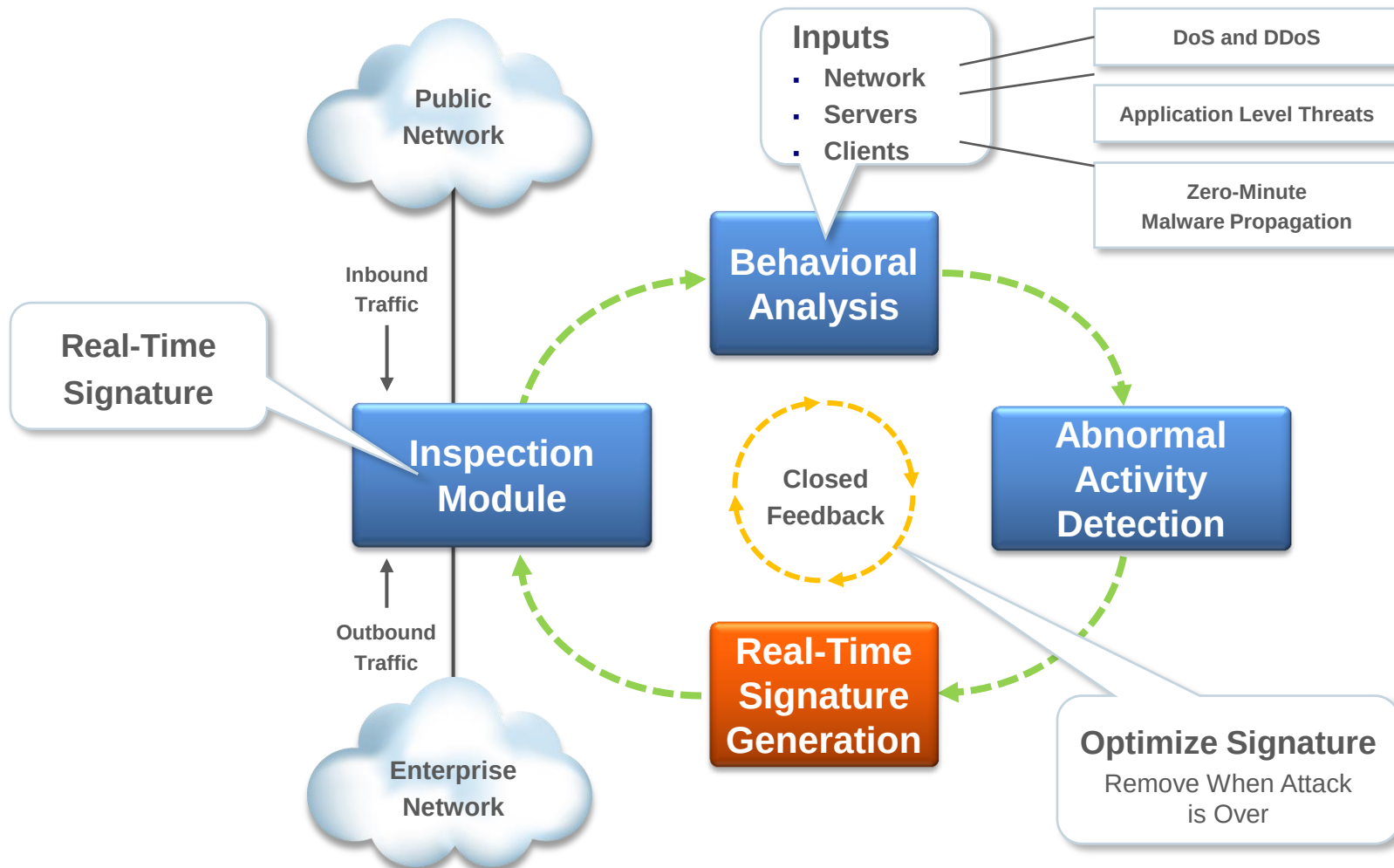
**Allowed
Traffic**



Automatically Block Abnormal Network Behavior



Protect Applications and Services Automatically



DDoS Protector



- DOS Shield (DOS signature)
- Behavioral DOS
- DNS Protection
- Syn Protection



- Out of state
- Connection Limit
- HTTP Mitigator
- White list/Black list

Block Denial of Service Attacks Within Seconds!

Where to Protect Against DDOS

Scenarios:

1

2

3

On-Premise Deployment



Off-Site Deployment



Appliance Specifications

							
Model	DP 506	DP 1006	DP 2006	DP 3006	DP 4412	DP 8412	DP 12412
Capacity	0.5Gbps	1Gbps	2Gbps	3Gbps	4GBps	8Gbps	12Gbps
Max Concurrent Sessions	2 Million				4 Million		
Max DDoS Flood Attack Protection Rate	1 Million packets per second				10 Million packets per second		
Latency	<60 micro seconds						
Real-Time Signatures	Detect and protect against attacks in less than 18 seconds						



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Management



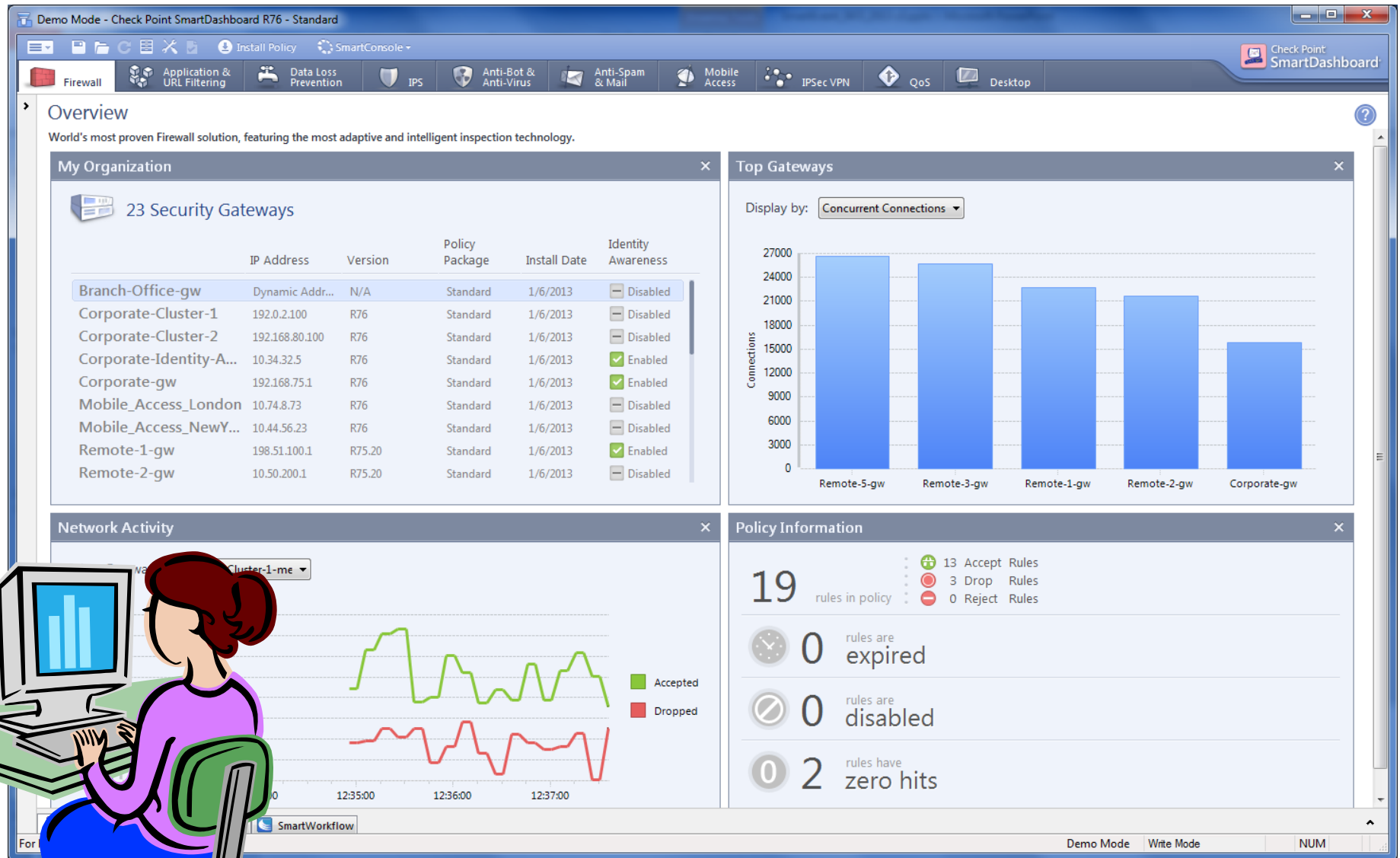
Systémová administrátorka ve velké firmě na léky



Finanční ředitel ve velké firmě na léky



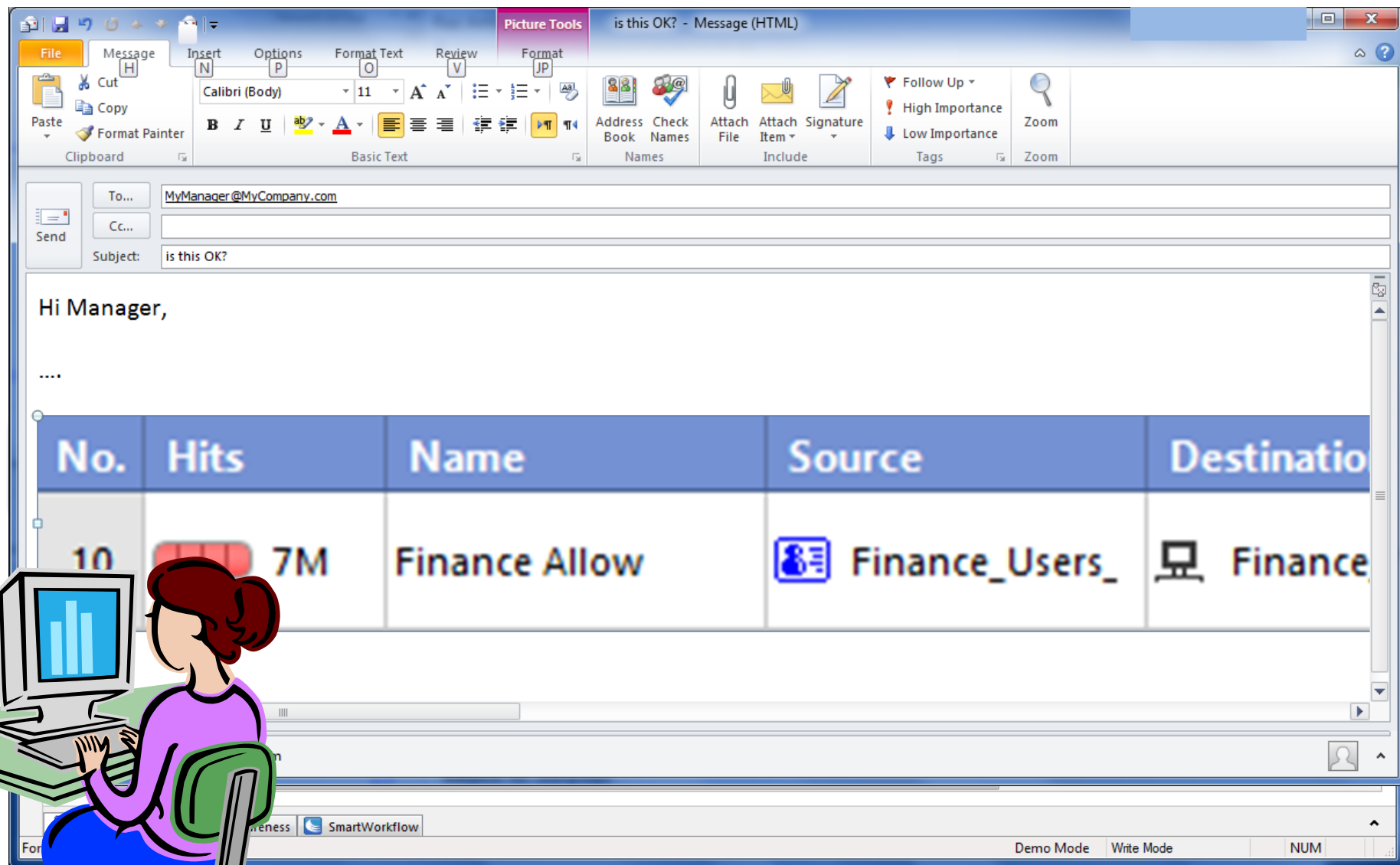
Přehledný management



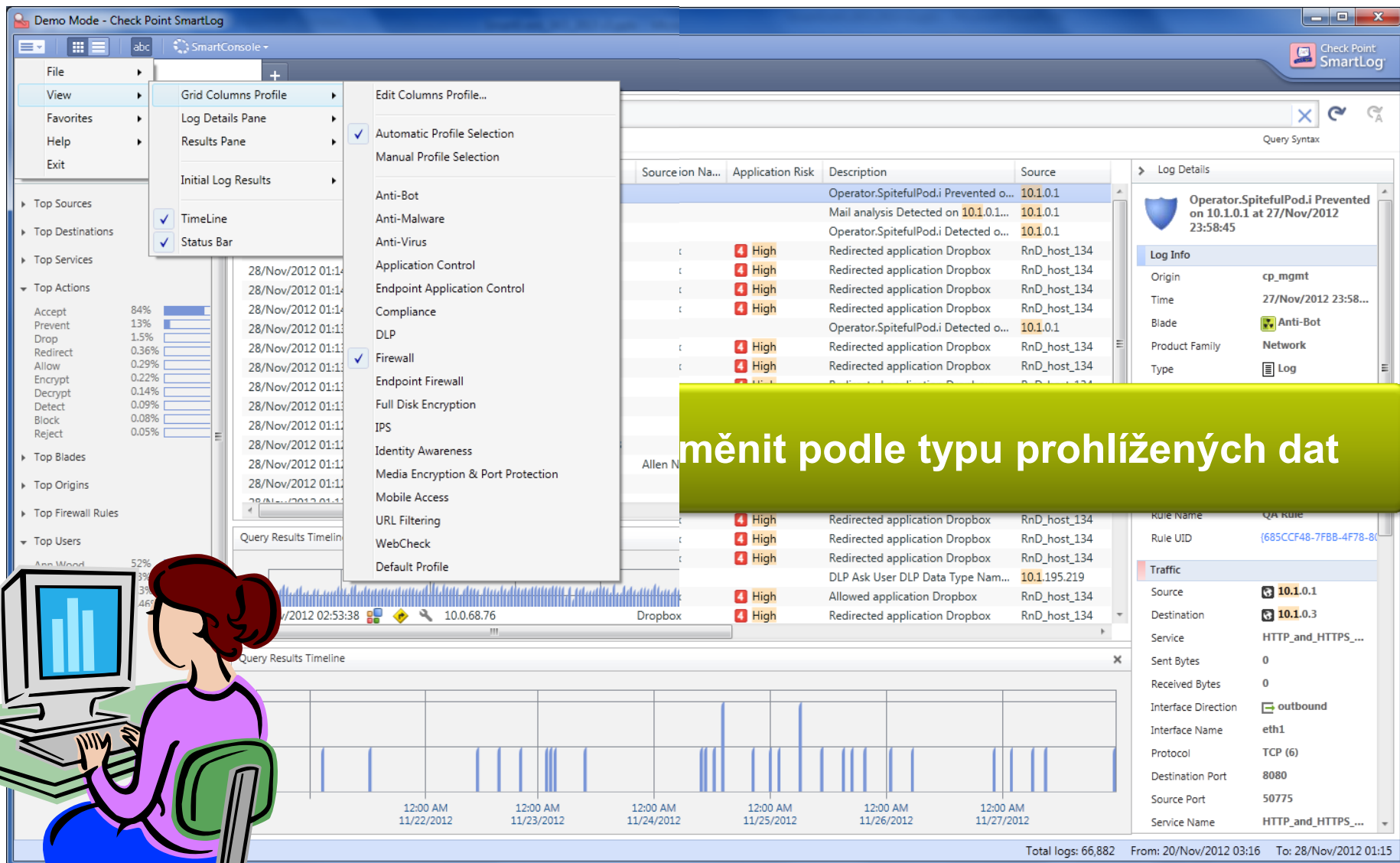
Chci vědět, jak jsme na tom
s bezpečností a co se děje
na síti našeho oddělení



Bezpečnostní politika - firewall



SmartLog – Google pro logy



SmartLog – Google pro logy

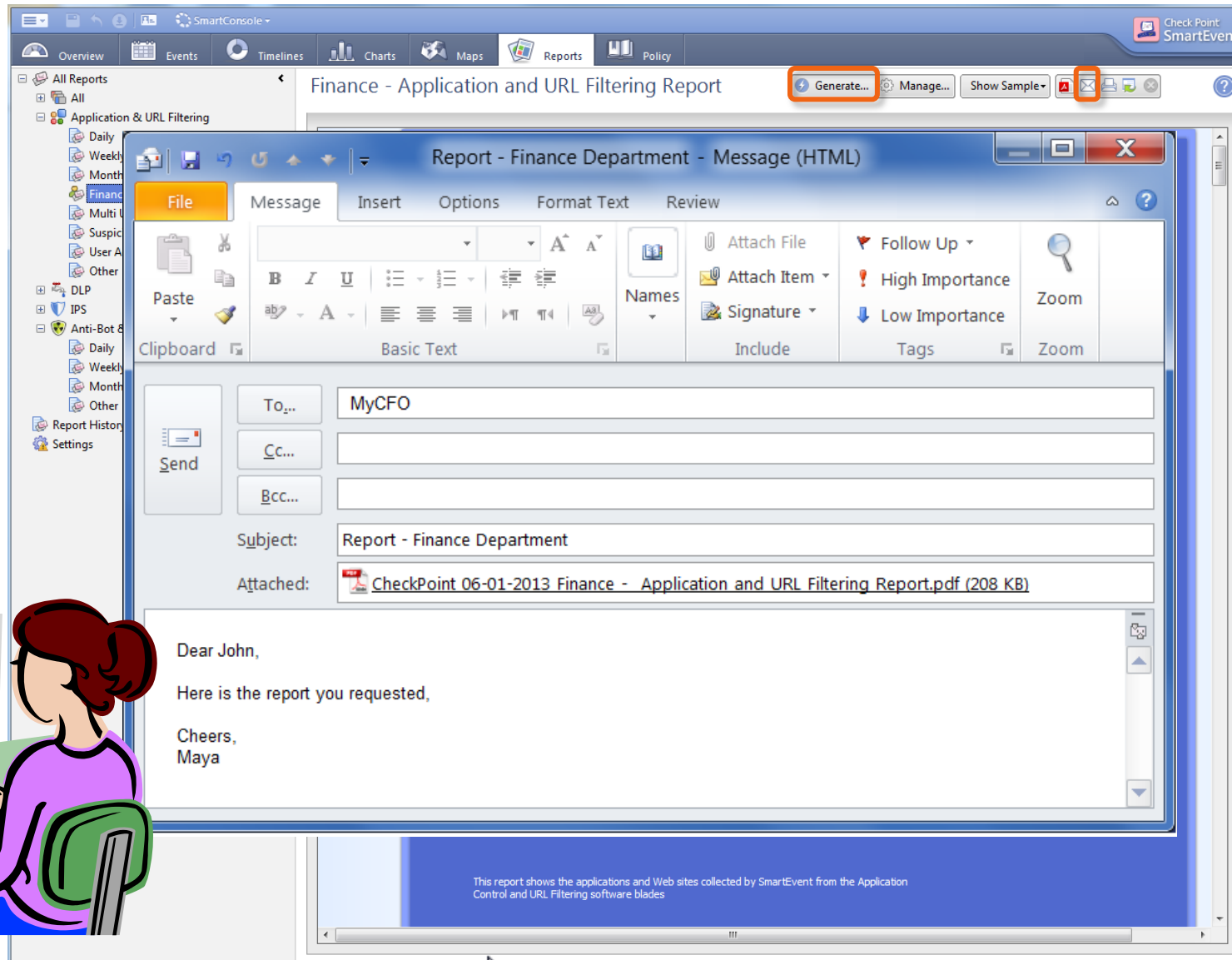
The screenshot displays the Check Point SmartLog interface in Demo Mode. The interface is divided into several sections:

- Left Panel:** Contains a menu (File, View, Favorites, Help, Exit) and a list of sources, destinations, services, actions, blades, origins, firewall rules, and users. A bar chart shows the distribution of actions: Accept (84%), Prevent (13%), Drop (1.5%), Redirect (0.36%), Allow (0.29%), Encrypt (0.22%), Decrypt (0.14%), Detect (0.09%), Block (0.08%), and Reject (0.05%).
- Central Panel:** Displays a table of log entries. The table has columns for Sourceion Na..., Application Risk, Description, and Source. The log entries show various events, including "Operator.SpitefulPod.i Prevented o...", "Mail analysis Detected on 10.1.0.1...", and "Redirected application Dropbox".
- Right Panel:** Shows the "Log Details" pane, which provides information about the selected log entry, including the Origin (cp_mgmt), Time (27/Nov/2012 23:58...), Blade (Anti-Bot), Product Family (Network), and Type (Log).

A yellow banner is overlaid on the central panel, containing the text:

měnit podle typu prohlížených dat

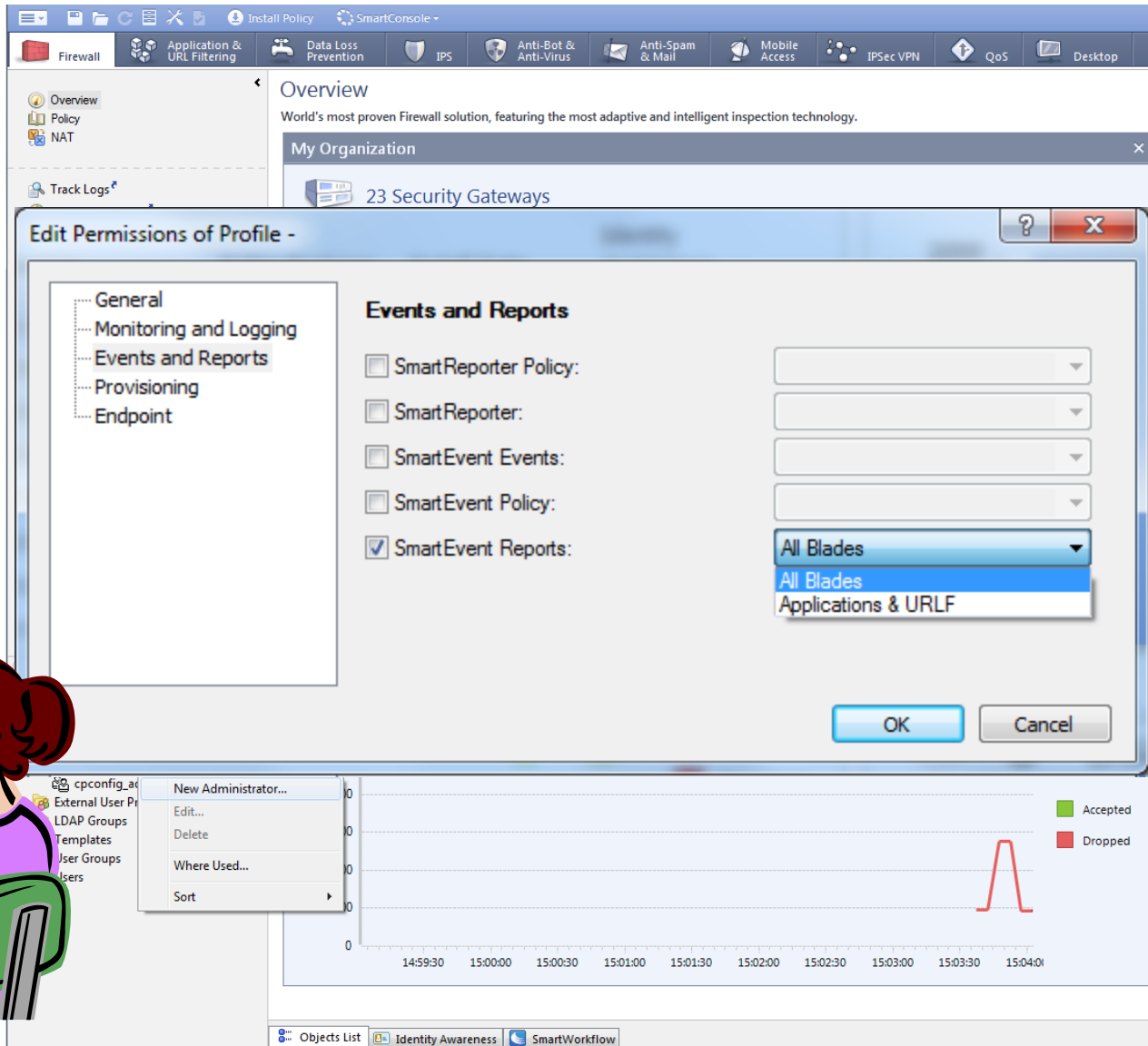
SmartEvent – reporty za oddělení



The screenshot displays the SmartEvent console interface. The main window shows a report titled "Finance - Application and URL Filtering Report". A "Generate..." button is highlighted with an orange box. Below the report title, a "Report - Finance Department - Message (HTML)" window is open, showing a message template for email distribution. The message includes a "To:" field with "MyCFO", a "Subject:" field with "Report - Finance Department", and an "Attached:" field with a PDF file named "CheckPoint 06-01-2013 Finance - Application and URL Filtering Report.pdf (208 KB)". The message body contains the text: "Dear John, Here is the report you requested, Cheers, Maya". The console's left sidebar shows a tree view of reports, including "All Reports", "Application & URL Filtering", and "Daily". The bottom of the console displays a footer message: "This report shows the applications and Web sites collected by SmartEvent from the Application Control and URL Filtering software blades".



Delegace práv pro reporty



Edit Permissions of Profile -

Events and Reports

- ☐ SmartReporter Policy:
- ☐ SmartReporter:
- ☐ SmartEvent Events:
- ☐ SmartEvent Policy:
- ☒ SmartEvent Reports:

OK Cancel

Accepted
Dropped

Přehled uživatelské aktivity

SmartConsole - User Activity Report

Generate... Manage... Show Sample

User Activity Report
May 01, 2012 12:00 AM - May 14, 2012 11:59 PM
User: Jared Josh(jaredjosh@myBiz.com)

(1 out of 2)

Start Time	Application / Site	Risk	Category	Action	Traffic	Browse Time (hh:mm:ss)
14-May-2012 04:31:10 PM	Facebook	2 Low	Social Networking	Allow	12.3MB	00:23:47
14-May-2012 04:33:15 PM	bettingsitesreview.com	Unknown	Gambling	Allow	3.6KB	00:19:47
14-May-2012 04:41:12 PM	espn.com	Unknown	News / Media	Allow	3.6KB	00:19:47
14-May-2012 04:55:00 PM	YouTube	2 Low	Video Streaming	Allow	207.5MB	00:19:27
14-May-2012 05:01:12 PM	Gmail	3 Medium	Webmail	Allow	4KB	00:13:44
14-May-2012 05:02:28 PM	LinkedIn	2 Low	Social Networking	Allow	3KB	00:13:58
14-May-2012 05:05:10 PM	Twitter	2 Low	Social Networking	Allow	136MB	01:18:44
14-May-2012 05:22:33 PM	mIRC	4 High	Instant Messaging	Block	0B	00:00:00
14-May-2012 05:23:12 PM	Time.com	Unknown	News / Media	Allow	39.5KB	00:03:44
14-May-2012 05:29:05 PM	PayPal	1 Very Low	Business Applications	Allow	9.7MB	00:00:54
14-May-2012 05:31:10 PM	Windows Live Writer	2 Low	Multimedia	Allow	50.7MB	00:53:44
14-May-2012 05:32:00 PM	adobe.com	Unknown	Business Applications	Allow	2.5KB	00:35:55
14-May-2012 05:41:20 PM	Telnet Protocol	4 High	Network Protocols	Block	0B	00:00:00
14-May-2012 05:44:10 PM	Adobe Update	1 Very Low	Business Applications	Allow	1000B	00:00:00
14-May-2012 05:44:20 PM	Windows Update	1 Very Low	Business Applications	Allow	1.9KB	00:13:44
14-May-2012 05:47:25 PM	Odnoklassniki	2 Low	Social Networking	Allow	3.6KB	00:13:44
14-May-2012 05:49:10 PM	eMule	4 High	P2P File Sharing	Block	0B	00:00:00
14-May-2012 05:52:10 PM	iTunes	3 Medium	Multimedia	Allow	69.2KB	00:00:00
14-May-2012 05:53:29 PM	DNS Protocol	1 Very Low	Network Protocols	Allow	4.9KB	00:00:00
14-May-2012 05:55:32 PM	Photobucket	2 Low	File Storage and Sharing	Allow	65KB	00:00:00
14-May-2012 06:05:13 PM	Flickr	2 Low	File Storage and Sharing	Allow	1.9KB	00:00:00
14-May-2012 07:05:02 PM	google.com	Unknown	Search Engines / Portals	Allow	1.9KB	00:00:00
14-May-2012 07:20:12 PM	Google Toolbar	2 Low	Browser Plugin	Allow	4.9KB	00:00:00
14-May-2012 07:20:12 PM	yahoo.com	Unknown	Search Engines / Portals	Allow	9.7MB	00:00:00
15-May-2012 05:49:10 PM	OpenFT	4 High	P2P File Sharing	Block	0B	00:00:00
15-May-2012 05:52:10 PM	Google Earth	2 Low	Virtual Worlds	Allow	7.0MB	00:04:00

Server Time: 1/17/2013 15:26 Demo Mode



Vyšetřování možných incidentů

All Events

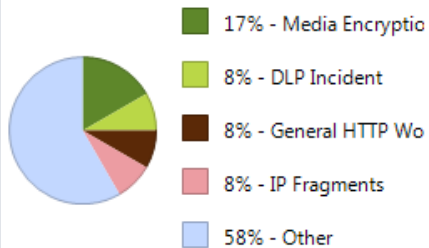
Last 30 Days # 30000

Type to Search



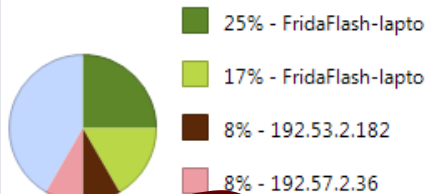
Group by Product

Top Events



No filter applied

Top Sources



C..	Product Name	User	Event Name	S...	Source
5	Check Point IPS Software Blade	Frida Flash	5 Event Names	4...	5 Sources
	Check Point IPS Software Blade	Frida Flash	Non Compliant DNS		FridaFlash-laptop...
	Check Point IPS Software Blade	Frida Flash	SSH over Non Standard Ports		192.53.2.182
	Check Point IPS Software Blade	Frida Flash	General HTTP Worm Catcher		192.62.2.26
	Check Point IPS Software Blade	Frida Flash	Non Compliant HTTP		FridaFlash-laptop...
	Check Point IPS Software Blade	Frida Flash	IP Fragments		192.53.2.177
2	Media Encryption and Port Protection	Frida Flash	Media Encryption File Operation		2... 2 Sources
	Media Encryption and Port Protection	Frida Flash	Media Encryption File Operation		192.80.2.209
	Media Encryption and Port Protection	Frida Flash	Media Encryption File Operation		192.57.2.36
1	Check Point URL Filtering Software Blade	Frida Flash	Web Browsing		192.123.2.51
1	Check Point DDoS Protector	Frida Flash	Invalid TCP Flags		192.116.2.81
1	Check Point Anti-Bot	Frida Flash	Bot Incident		FridaFlash-laptop...
1	Check Point Application Control Software Blade	Frida Flash	Application Activity		FridaFlash-laptop...
1	Check Point DLP	Frida Flash	DLP Incident		FridaFlash-laptop...
	Check Point Security Gateway	Chloe Cash	Port scan from external network		192.62.2.153
2	Check Point SmartEvent Client	2 Users	Check Point administrator login ...		2... 2 Sources

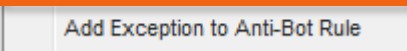
Translate Security Information into **Action!**

Count		Source	User		Protection Type	Protection Name	Malware Activity		
3		3 Sources	3 Users		URL Reputation	REP.ggds	Malicious file/exploit download	3...	3 De
		BlancaBash-laptop (125.0....	Blanca Bash		URL Reputation	REP.ggds	Malicious file/exploit download		204.
		HerbieHash-laptop (125.0....	Herbie Hash		URL Reputation	REP.ggds	Malicious file/exploit download		91.0
		LeeLash-laptop (125.0.0.3)	Lee Lash		URL Reputation	REP.ggds	Malicious file/exploit download		87.0
3		2 ... 3 Sources	3 Users		2 Protection Types	2 Protection Names	2 Malware Activities	2...	3 De
		BrianBash-laptop (86.0.0.12)	Brian Bash		Suspicious Mail	Mail Analysis	Spam		81.0
		DiedreDash-desktop (125....	Diedre Dash		IP Reputation	REP48034	Communication with C&C		88.0
		IanWhitewash-laptop (86....	Ian Whitewash		Suspicious Mail	Mail Analysis	Spam		116.

Mar 23
2012


Bot Incident:  Detect

[Copy Details](#)
[Actions](#)
[Anti-Bot](#)
[Summary](#)
[Details](#)



 Diedre Dash

 REP48034 (IP Reputation)

 Detected

 Communication with C&C

 High Severity

 High Confidence

 Today at 09:45:51

Event Description:

A Malware on machine  125.0.0.63 attempted to locate and download a malicious file from  88.0.0.22 at 09:45:51 04 Apr 2012.

Additional Data:

Destination: [88.0.0.22](#)

Sent Bytes: 84 Bytes

Received Bytes: 224 Bytes

Origin:  Japan-gateway (125.0.1.245)

SmartWorkflow: Automated Policy Change Management



Visual change tracking

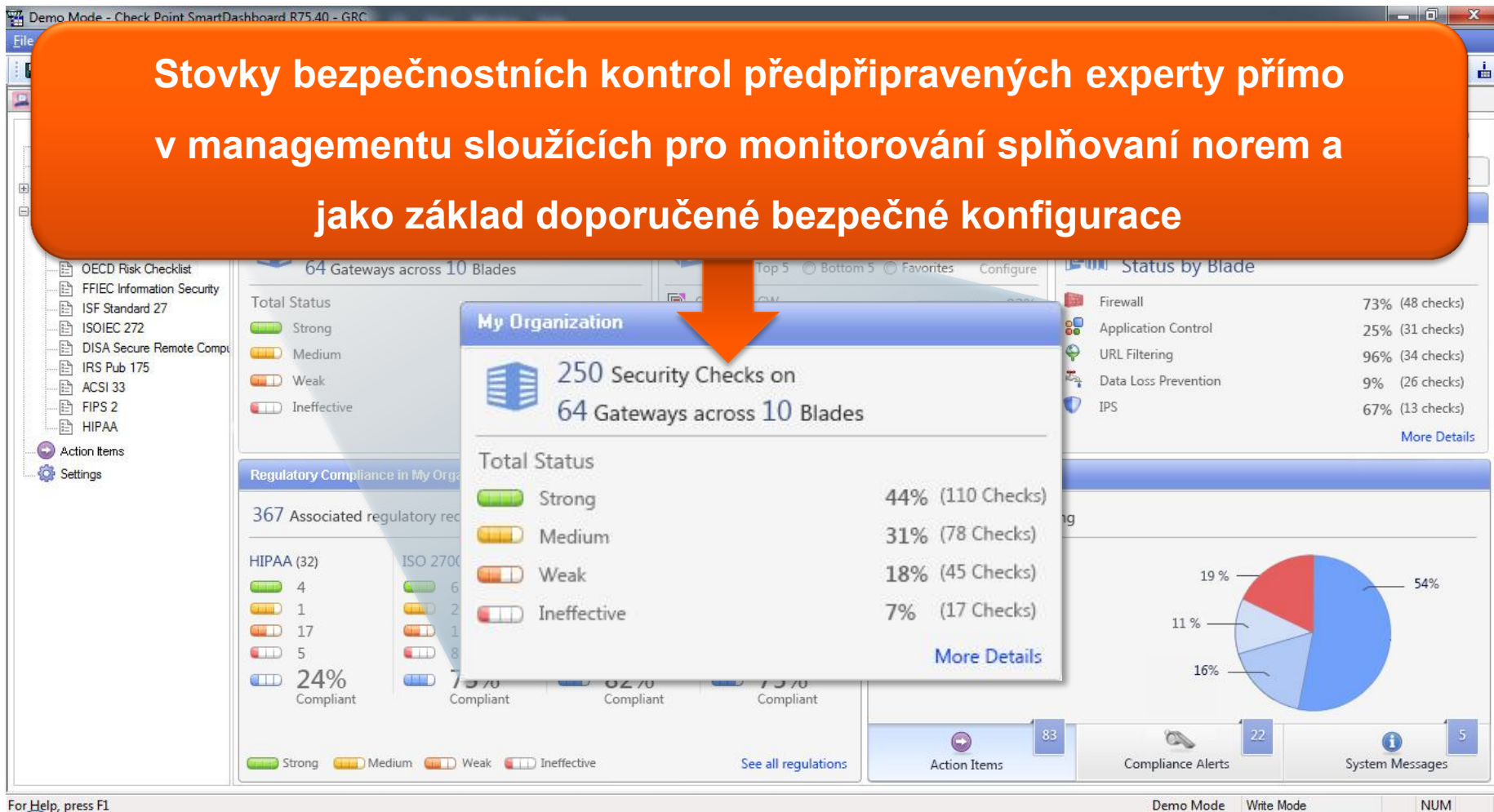
Flexible authorization

Audit trails

Single Console Integration

Compliance, best practices

**Stovky bezpečnostních kontrol předpřipravených experty přímo
v managementu sloužících pro monitorování splňování norem a
jako základ doporučené bezpečné konfigurace**



Compliance: Bezpečnostní kontroly politik

Demo Mode - Check Point SmartDashboard R75.40 - GRC

File Edit View Manage Rules Policy SmartWorkflow Search Window Help

Welcome Firewall NAT Application & URL Filtering Data Loss Prevention IPS Anti-Bot & Anti-Virus Anti-Spam & Mail Mobile Access IPsec VPN QoS Desktop Compliance

Overview Security Checks Gateways

Security Checks

Type to Search --No Grouping--

Doporučení

Stav plnění

Související předpisy

Security Check #FW107: Check that there is additional log server defined for each Gateway and Cluster for the storage of Firewall logs

Relevant Gateways: 0 of 17 items are effective

Active	Object	Profile	Result
☒	Remote-5-gw	Default_Protection	Ineffective
☐	Mobile_Access_NewYork	Default_Protection	Ineffective
☐	Remote-1-gw	Recommended_Protection	Ineffective
☒	V4V6_cluster	Default_Protection	Ineffective
☒	GX	Default_Protection	Ineffective
☒	Remote-4-gw	Default_Protection	Ineffective
☒	Remote-5-gw	Default_Protection	Ineffective

Relevant Regulatory Requirements

Regulation	Id	Result
ISO 27001	010053	Medium
ISO 27001	010067	Medium
ISO 27001	010069	Medium
ISO 27001	010131	Medium
ISO 27001	010133	Medium
HIPAA Security	020002	Medium
HIPAA Security	020004	Medium

For Help, press F1

Demo Mode Write Mode NUM

EN 100% 11:50 AM



Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Infrastruktura





Application Control Blade can block/allow important HTTPS based applications even without enabling HTTPS inspection!

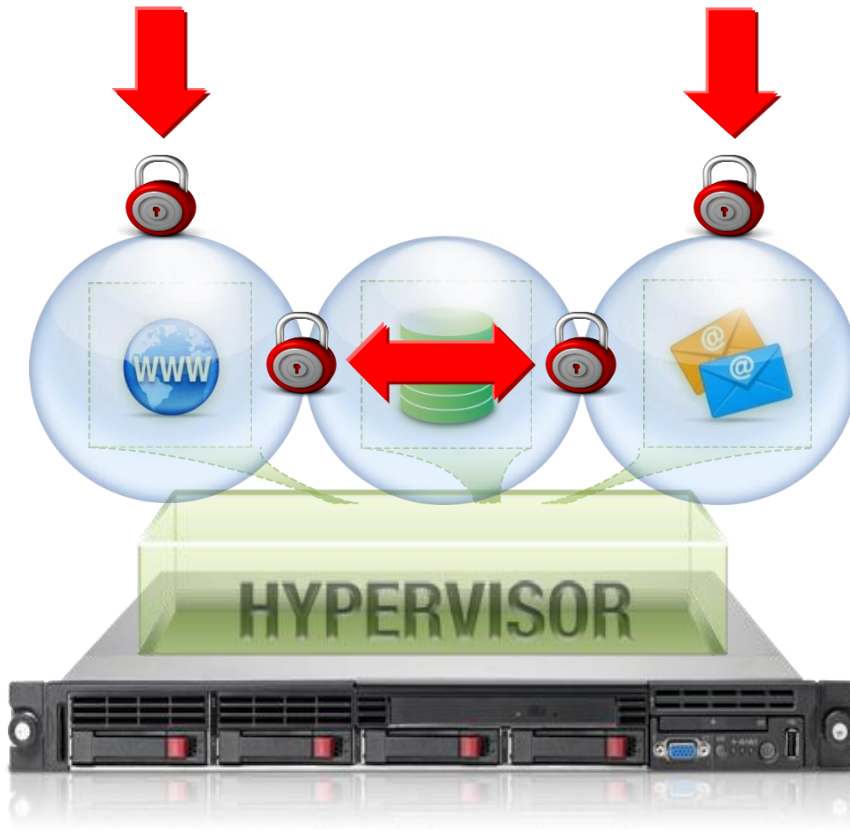
Source	Destination	Application	Action
 Any	 Internet	 Facebook	 Block

- The above rule would block all access to the following examples (and more)
 - <http://www.facebook.com>
 - <http://www.facebook.com/FarmVille>
 - <https://www.facebook.com>
 - <https://www.facebook.com/FarmVille>

HTTPS inspection

- Granular policy
- Active Directory objects
- URL Filtering groups
- All or per Software Blade
- Supports Inbound and outbound
- CA list and certification verification

No.	Name	Source	Destination	Services	Site Category	Action	Track	Blade
1		 CEO_office	 Internet	<u>TCP</u> https <u>TCP</u> HTTP_and_H...	 Any	 Bypass	- None	 All
2		 Any	 Internet	<u>TCP</u> https <u>TCP</u> HTTP_and_H...	 Email  Financial Services  Health	 Bypass	- None	 All
3		 Any	 Internet	<u>TCP</u> https <u>TCP</u> HTTP_and_H...	 Any	 Inspect	 Log	 All



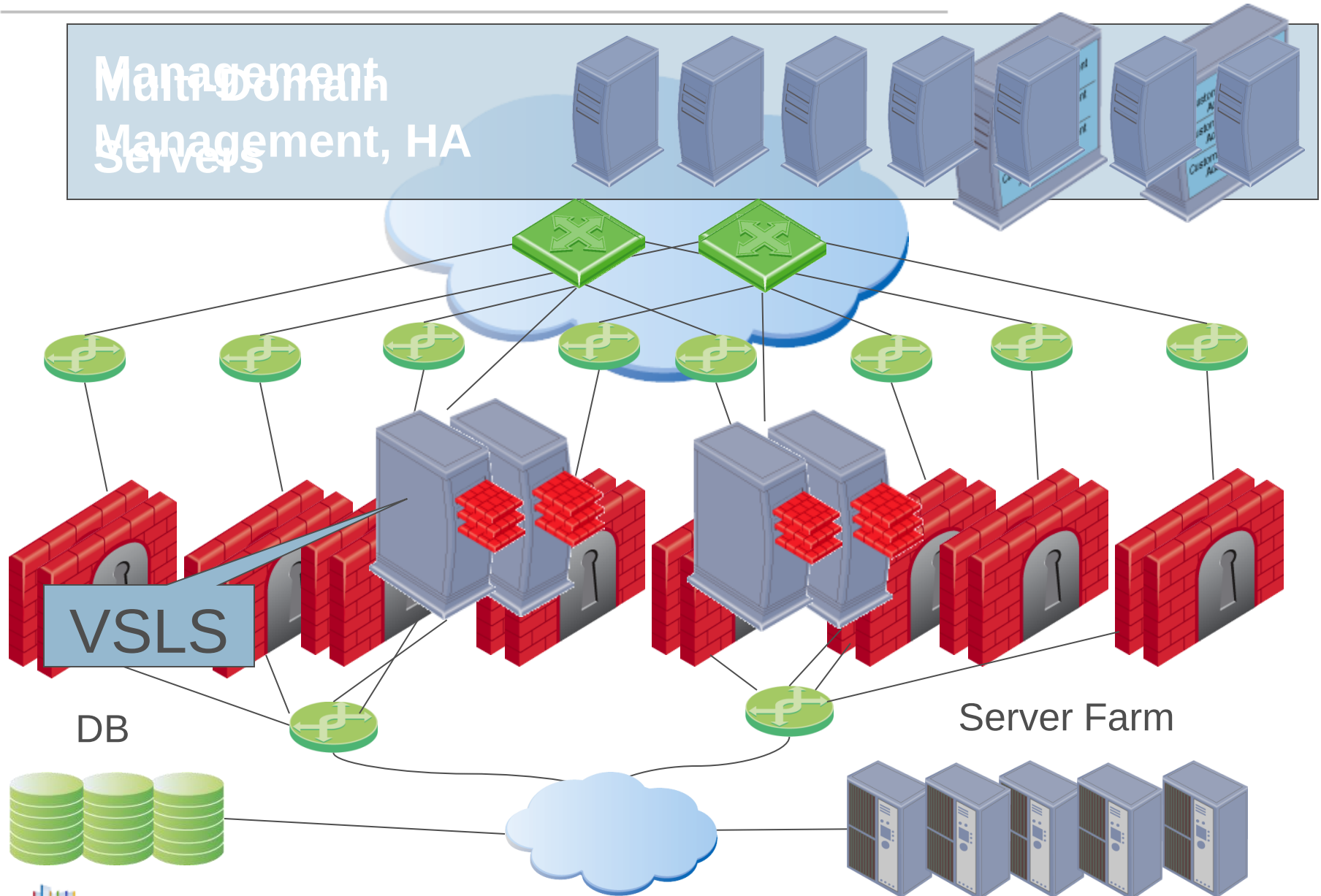
Security Challenges in Virtual Environments

Protection from external
threats

Inspect traffic between
Virtual Machines (VMs)

Secure new Virtual Machines
automatically

Virtualized Security – Virtual Systems





Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Shrnutí



- Prostředky řízení přístupu – vícevrstvá ochrana
- Management – pokročilé nástroje použitelné snadno i ve velkých prostředích, viditelnost
- Infrastruktura – flexibilní podpora vykonávání bezpečnosti v nejrůznějších podmínkách (platformy, výkon)

- Přístup uživatelů do Internetu – **Secure Web Gateway**
 - **Application Control** – identifikace a řízení aplikací bez ohledu na protokol
 - **URL Filtering** – předchůdce, první generace App. Ctrl.
- Ochrana uživatelů před hrozbami a malware – **Threat Prevention**
 - multi-layer **Antivirus**
 - slabiny klientských aplikací – **IPS**
 - neznámé hrozby – **Threat Emulation**
 - post-infekční ochrana – **Antibot**

CHECK POINT 2013 SECURITY REPORT

What's Hiding on Your Network?

63% infected with bots • 54% experienced data loss • 47% used anonymizers

Based on research of nearly 900 companies and 120,000 hours of monitored traffic, the 2013 Check Point Security Report reveals major security risks organizations are exposed to on a daily basis. Most importantly, the report provides security recommendations on how to protect against these threats.

DOWNLOAD

A sample of what your custom
Security Report Analysis could look like

Take a Look Inside

CHECK POINT 2013 SECURITY REPORT

01

Introduction & Methodology

004

02

Threats to Your Organization

006

03

Applications in The Enterprise Workspace

020

04

Data Loss Incidents in Your Network

030

05

Summary and Security Strategy

036

06

01 INTRODUCTION AND METHODOLOGY

**"JUST AS WATER RETAINS NO
CONSTANT SHAPE, SO IN WARFARE
THERE ARE NO CONSTANT
CONDITIONS."**

ALTHOUGH THIS SENTENCE IS 2,600
YEARS OLD, SURPRISINGLY IT IS STILL
MORE THAN RELEVANT, REFLECTING
TODAY'S MODERN WARFARE -
CYBER WARFARE.

Hackers' motives are constantly changing, using more
advanced and sophisticated attack methods, raising
the security challenge to new levels. Data centers,
employees' computers and mobile phones are prime
targets for hackers who deploy an endless variety of
tools such as bots, malware and drive-by downloads.
Hackers use real-time engineering to manipulate
incoming data to give access to corporate information
such as internal documents, financial records, trade
and customer data and more, all in an effort to steal
data and disrupt the flow of service. This

is why we expect to see just how many of the
questions that kept Check Point's security research team
busy in the past few months. While gathering answers to
these questions, Check Point has conducted an intensive
security analysis.

This report provides a quick look at 2013 network security
events that occurred in organizations worldwide.
The report presents the security events based on these
organizations, with examples of incidents published
publicly, explanations on how some of the attacks
were conducted, followed by recommendations on
how to protect against such security threats. The report is
divided into three parts. Each part is dedicated to a
different aspect of security. The first part focuses on
security changes such as bots, viruses, security breaches
and attacks. The second part discusses today's web
applications that compromise organizational network
security. The last part is dedicated to how data is stolen
by unauthorized employee actions.

Methodology

Check Point's 2013 Security Report is based on a
collaborative research and analysis of security events
gathered from four main sources: Check Point Security

First Name

Last Name

Company Name

Company Size

Please select...



Country

Please select...



State / Province

Please select...





Check Point Achieves Top Scores for **Firewall, Next-Gen Firewall** and **IPS** Tests by NSS Labs

HIGHEST SCORE FOR SECURITY EFFECTIVENESS AND MANAGEMENT

Check Point NGFW Achieves the highest score for security effectiveness and management in the latest NSS Labs test



Firewall
100%
Security Effectiveness



Next Generation Firewall
98.5%
Security Effectiveness



Intrusion Prevention System
99%
Overall Protection

Check Point extends its record of exceptional security effectiveness and management by receiving three "Recommend" ratings from NSS Labs in their most recent round of Next Generation Firewall (NGFW), Intrusion Prevention System (IPS), and Firewall testing.

- Firewall: 100% Security Effectiveness and Management and Recommend Rating
- NGFW: The top score in Security Effectiveness and Management and Recommend Rating
- IPS: The best overall protection at 99% and Recommend Rating

With the outstanding results in the latest NSS Labs tests, Check Point continues its history of excellence in both security management and leadership.

Learn how you can leverage Check Point's industry-leading firewall, NGFW and IPS solutions to protect your business' critical network infrastructure.

Register Now to Schedule Your Onsite Security Analysis

Additional Information

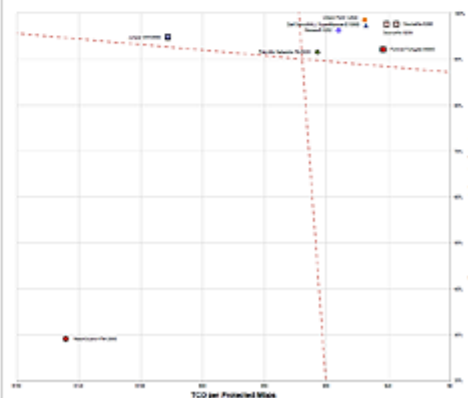
Download a summary of the 2013 NSS Labs Firewall, NGFW, and IPS Tests



Download Now



NSS Value Map



[Click to enlarge](#)

Check Point: Leader in Enterprise Network Firewall Magic Quadrant for 16 Years

Check Point Recognized As Leader in Enterprise Network Firewall Magic Quadrant for the Sixteenth Consecutive Year

Check Point was positioned as a leader in the latest Gartner 2013 Enterprise Network Firewall Magic Quadrant. This is the sixteenth year Check Point has been positioned as a leader in the Enterprise Network Firewall Magic Quadrant. Check Point is the industry leader in providing robust firewall technology. As the firewall market has evolved to include integrated IPS and other next generation firewall capabilities, Check Point continuously expand its firewall capabilities to maintain that leadership. Check Point not only has the vision for next generation firewall security technologies but also leads in the ability to execute and deliver the most advanced firewall. Download a complimentary copy of the report and see why Check Point has been positioned as a leader in Gartner's Enterprise Network Firewall Magic Quadrant.



We'd Like to Help!



Contact Us

Download the **FULL REPORT** "Magic Quadrant for Enterprise Network Firewalls"

* = required

First Name *

Last Name *

Company Name *

Company Size *

[Register Now to Schedule an Onsite Security Analysis](#)



Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Vaše dotazy

