Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Koncepty v zabezpečení DMZ infrastruktury proti aktuálním kybernetickým útokům

Martin Koldovský

mkoldov@checkpoint.com

DMZ je o **segmentaci**

- 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)

Segmentace je o **řízení přístupu**

- 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

Prostředky řízení přístupu

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

Bez měření není řízení

- 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)

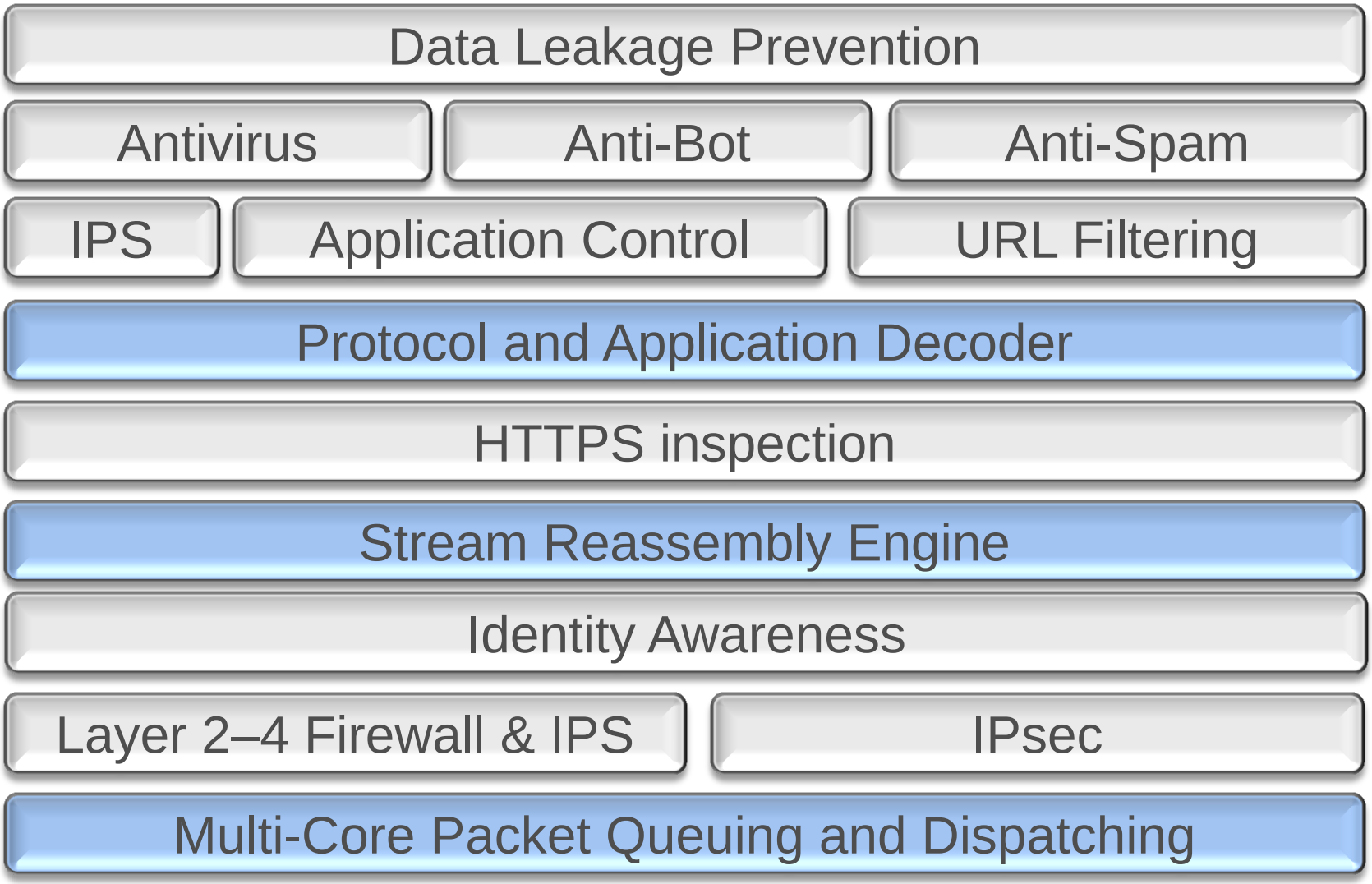
Infrastruktura

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

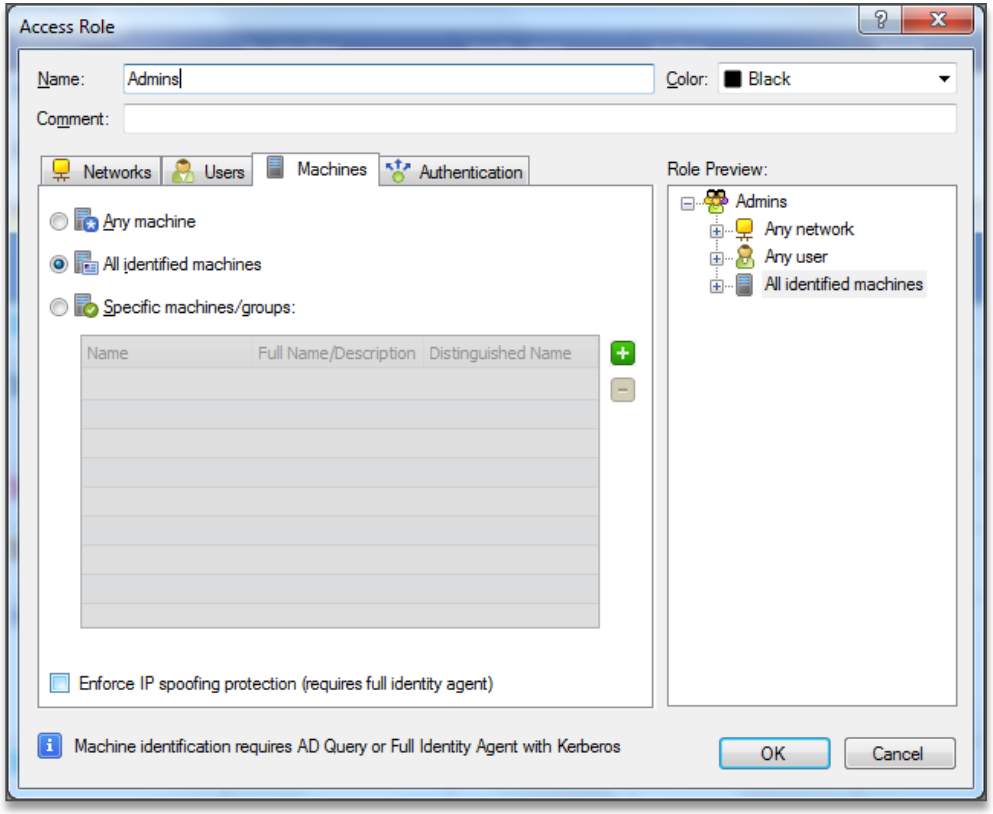
Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Řízení přístupu

Vícevrstvá architektura

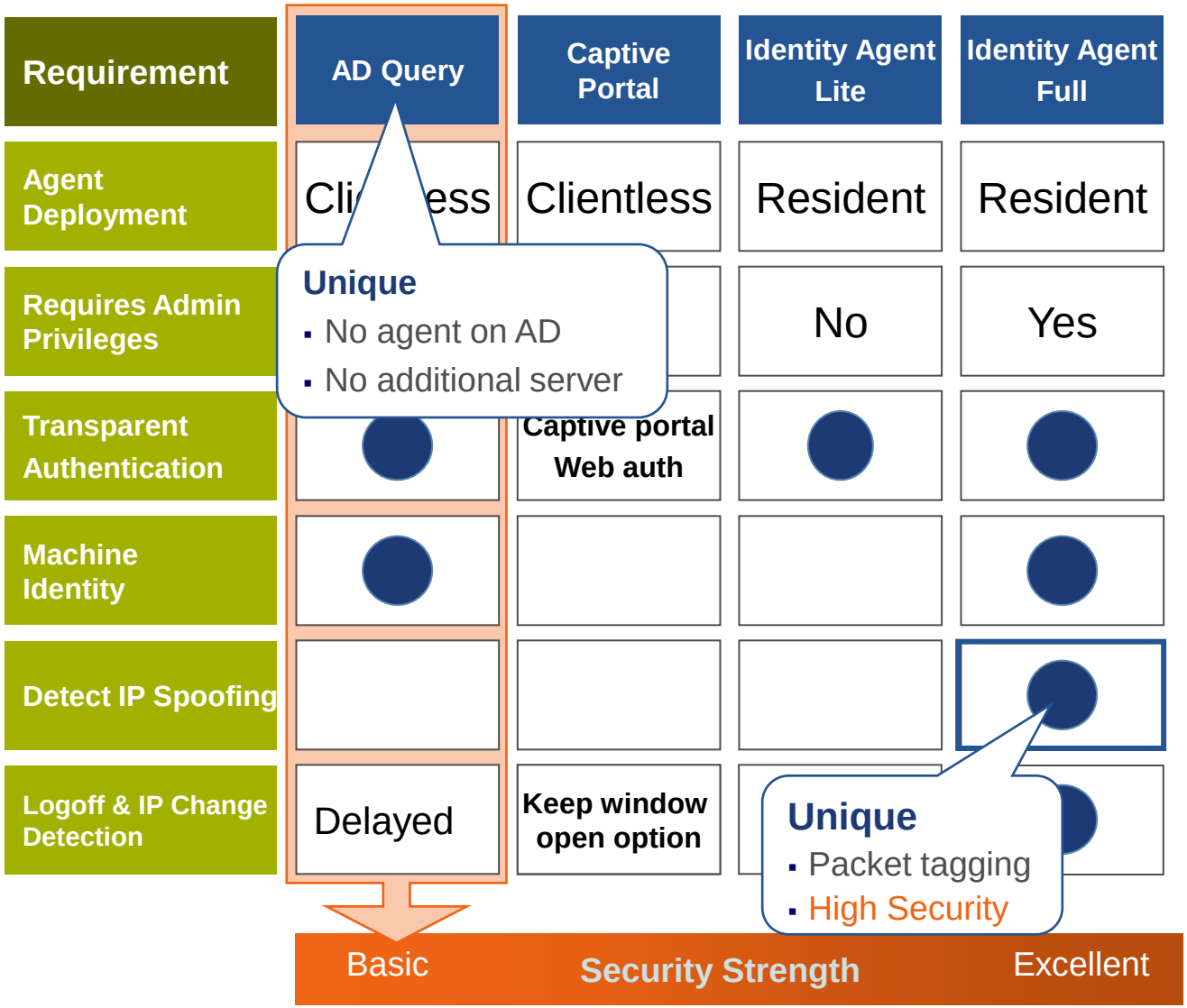


Identity Awareness

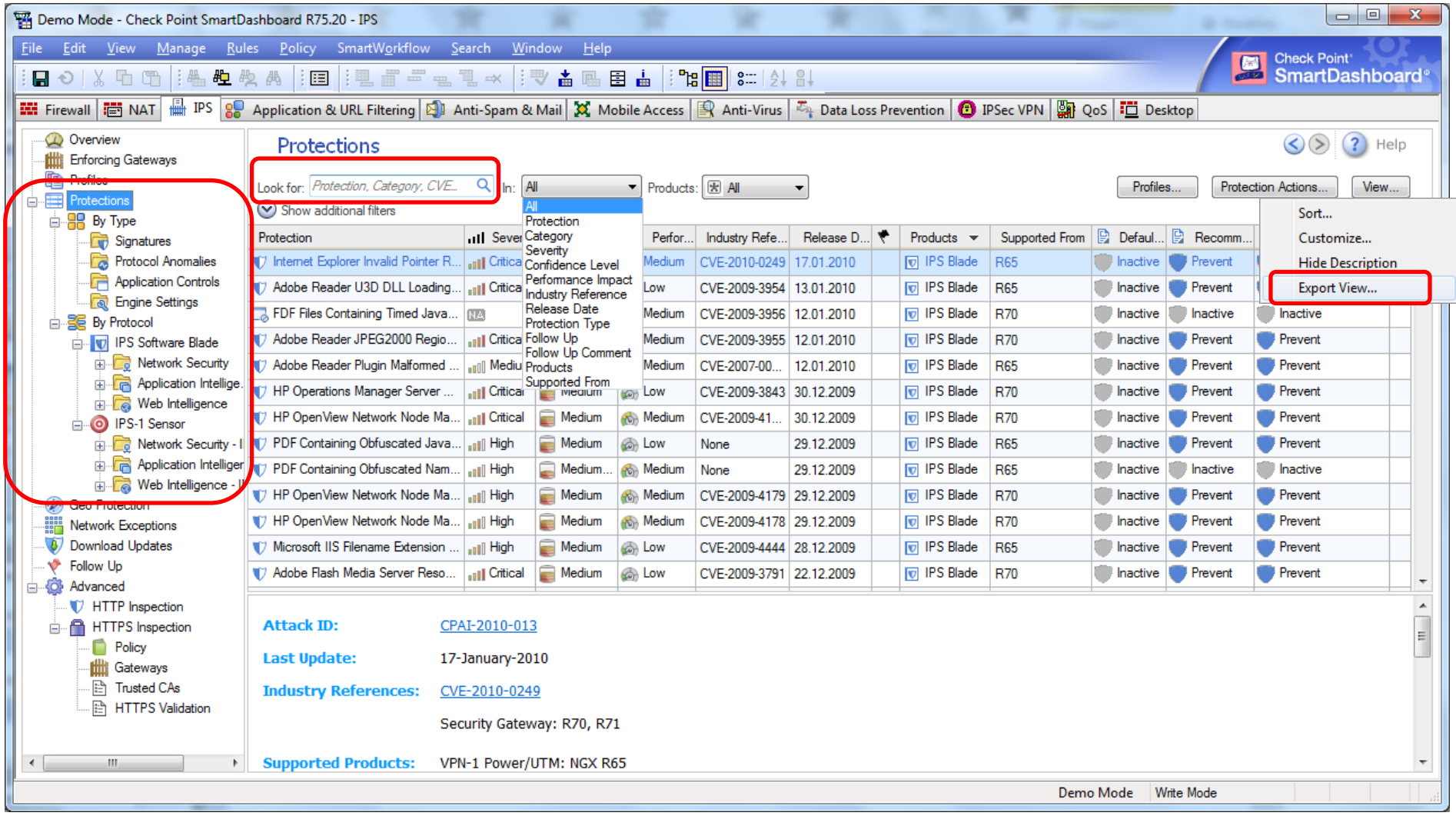


- Politiky založené na **rolích uživatelů**, ne pouze na IP adresách sítí a počítačů
- Uživatel, zařízení, lokalita

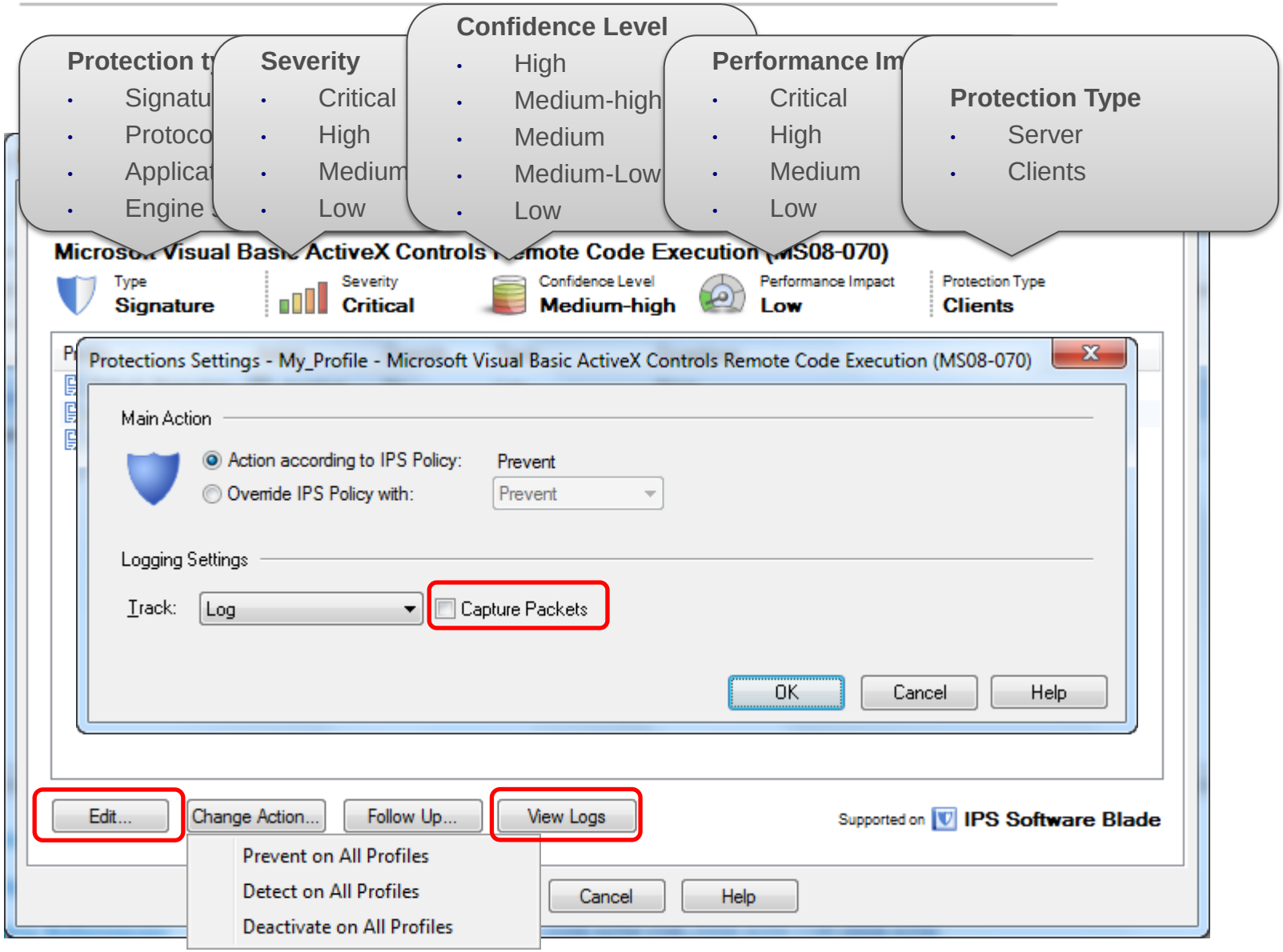
Srovnání některých zdrojů identity



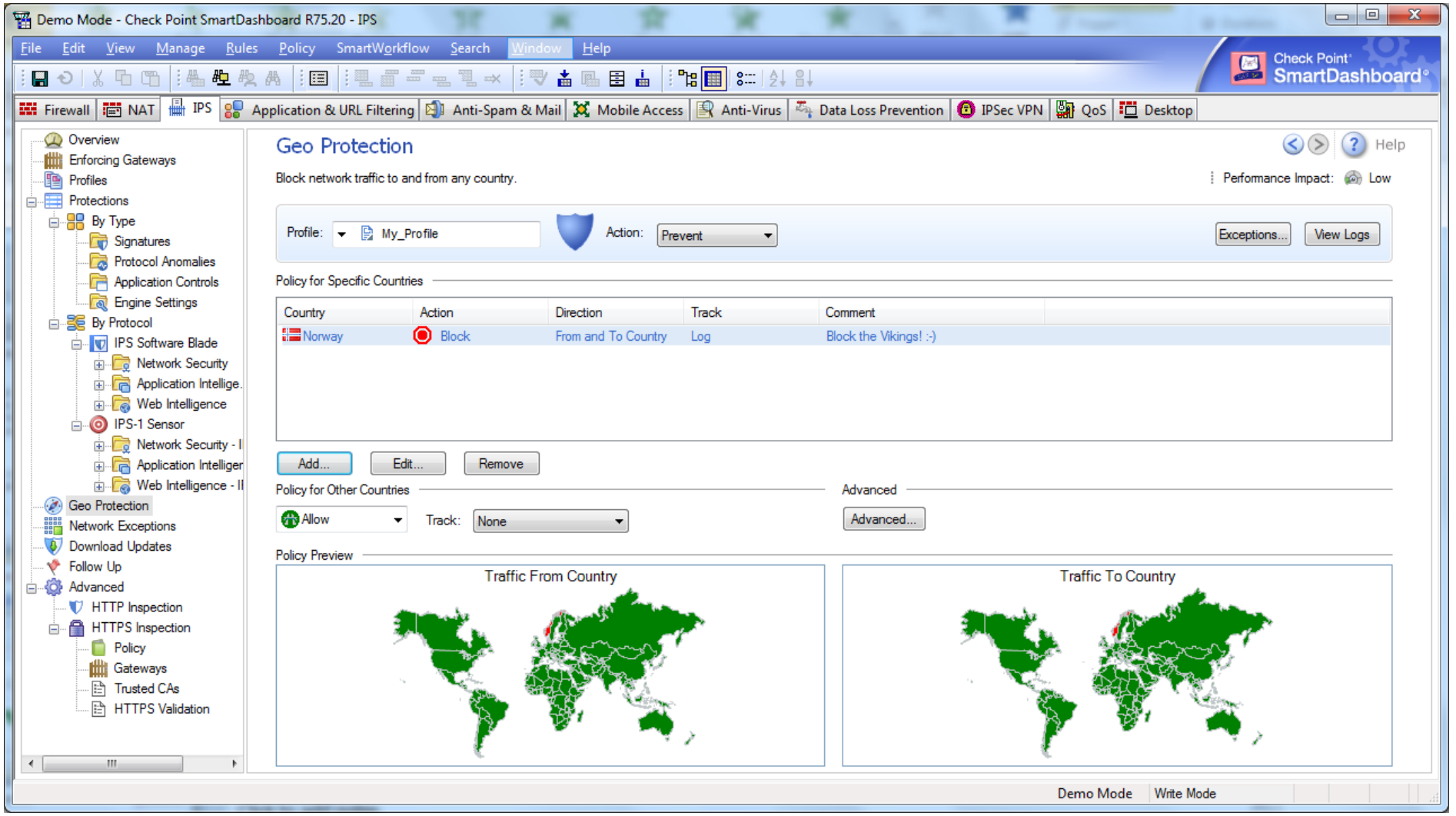
IPS: přehled ochran



IPS v detailu



Geo Protection



DDoS Attack Information

Network Flood	Server Flood	Application	Low & Slow Attacks
			
High volume of packets	High rate of new sessions	Web / DNS connection-based attacks	Advanced attack techniques

Multi-Layer DDoS Protection

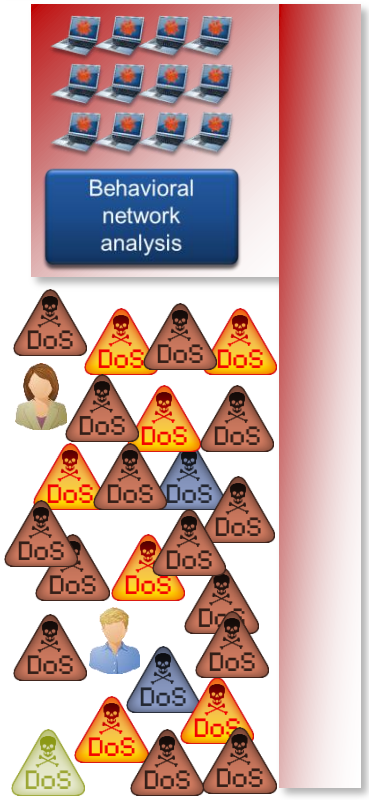
Network Flood	Server Flood	Application	Low & Slow Attacks
			
Behavioral network analysis	Automatic and pre-defined signatures	Behavioral HTTP and DNS	Granular custom filters
Stateless and behavioral engines	Protections against misuse of resources	Challenge / response mitigation methods	Create filters that block attacks and allow users

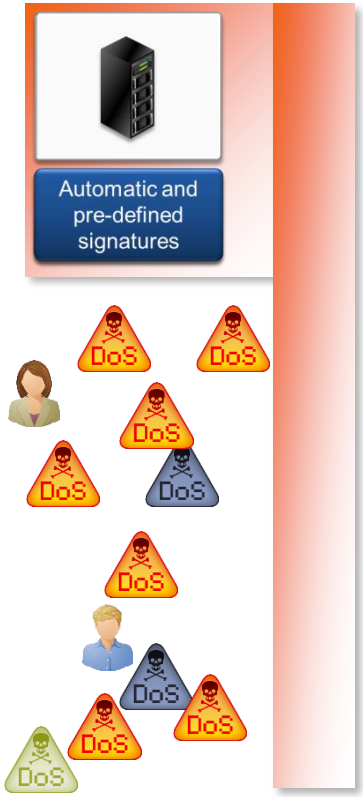
Layers Work Together

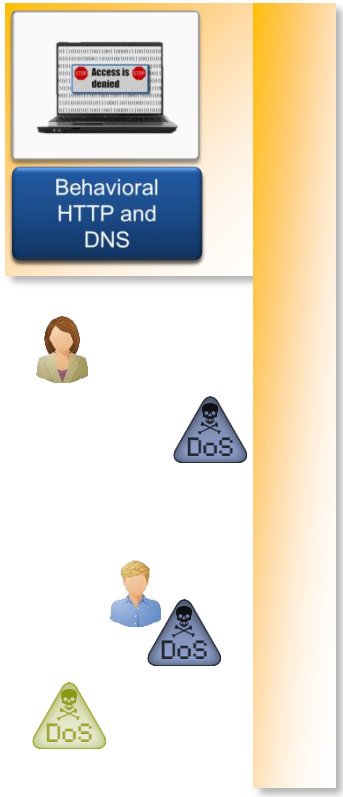
Check Point SOFTWARE TECHNOLOGIES LTD.

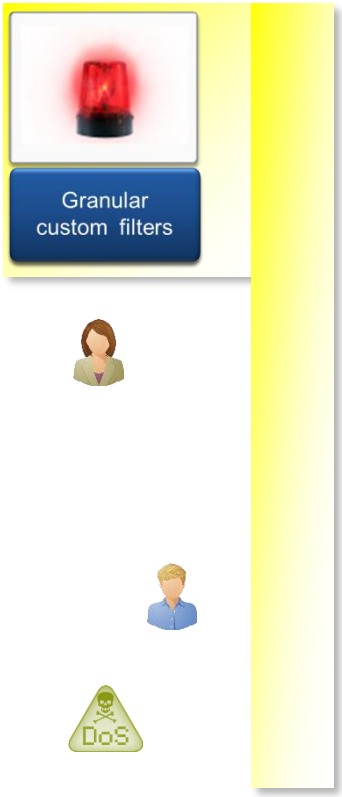
Protection Layers Flow

Network Flood	Server Flood	Application	Low & Slow Attacks	Allowed Traffic



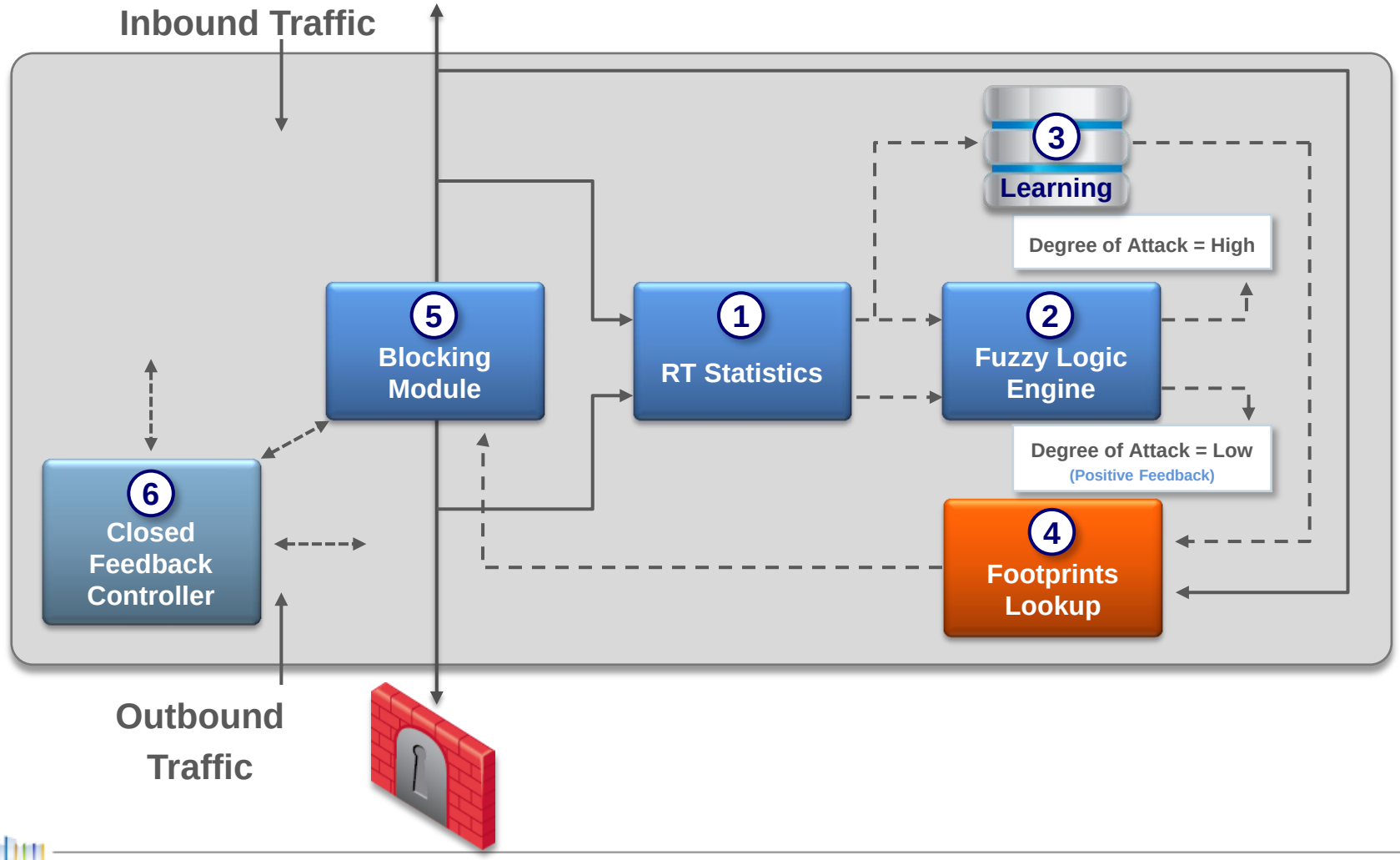






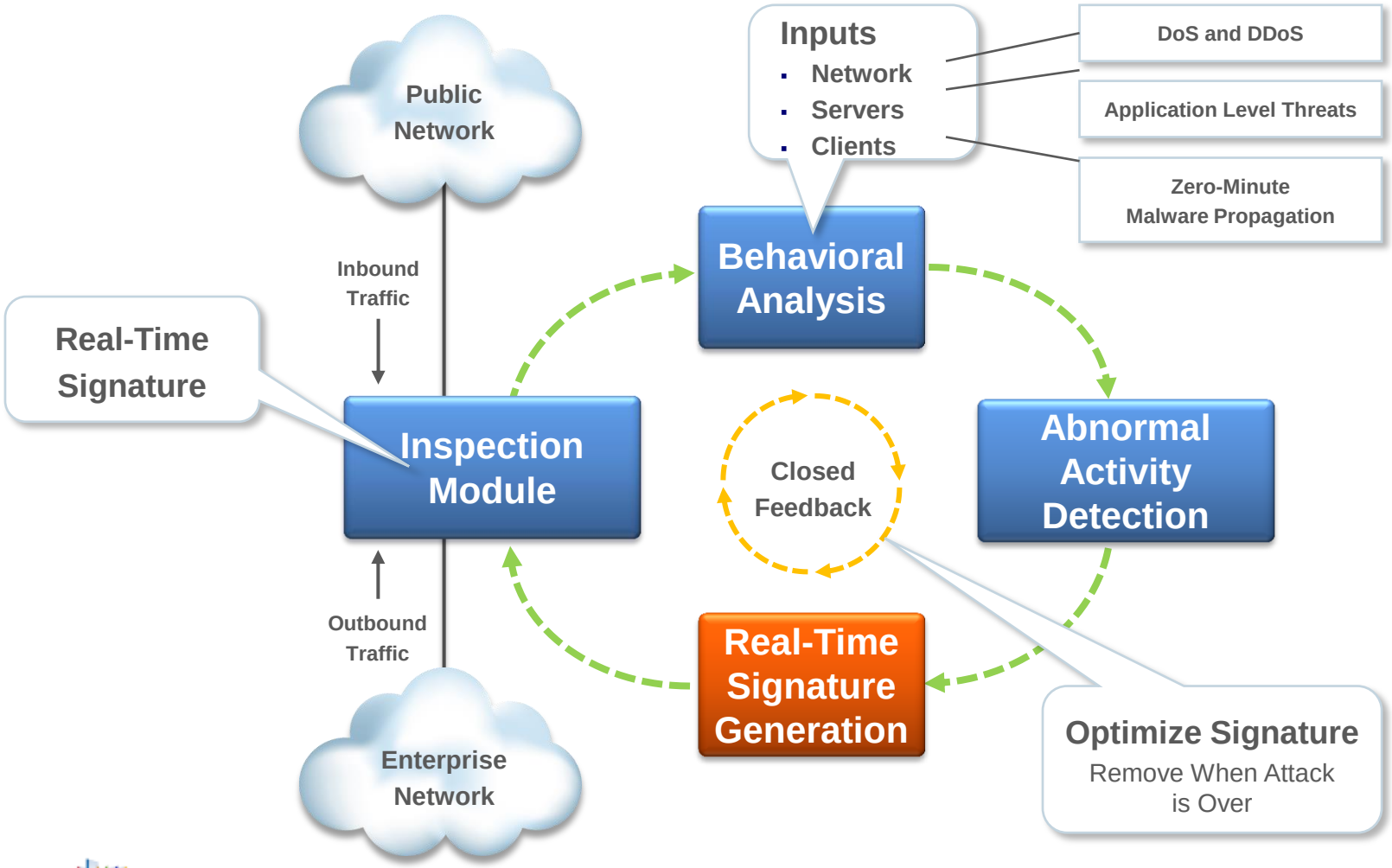
Behavioral DoS Protection System

Automatically Block Abnormal Network Behavior



DDoS: On-the-Fly Signature Creation

Protect Applications and Services Automatically



The Solution

Check Point SOFTWARE TECHNOLOGIES LTD.

DDoS Protector

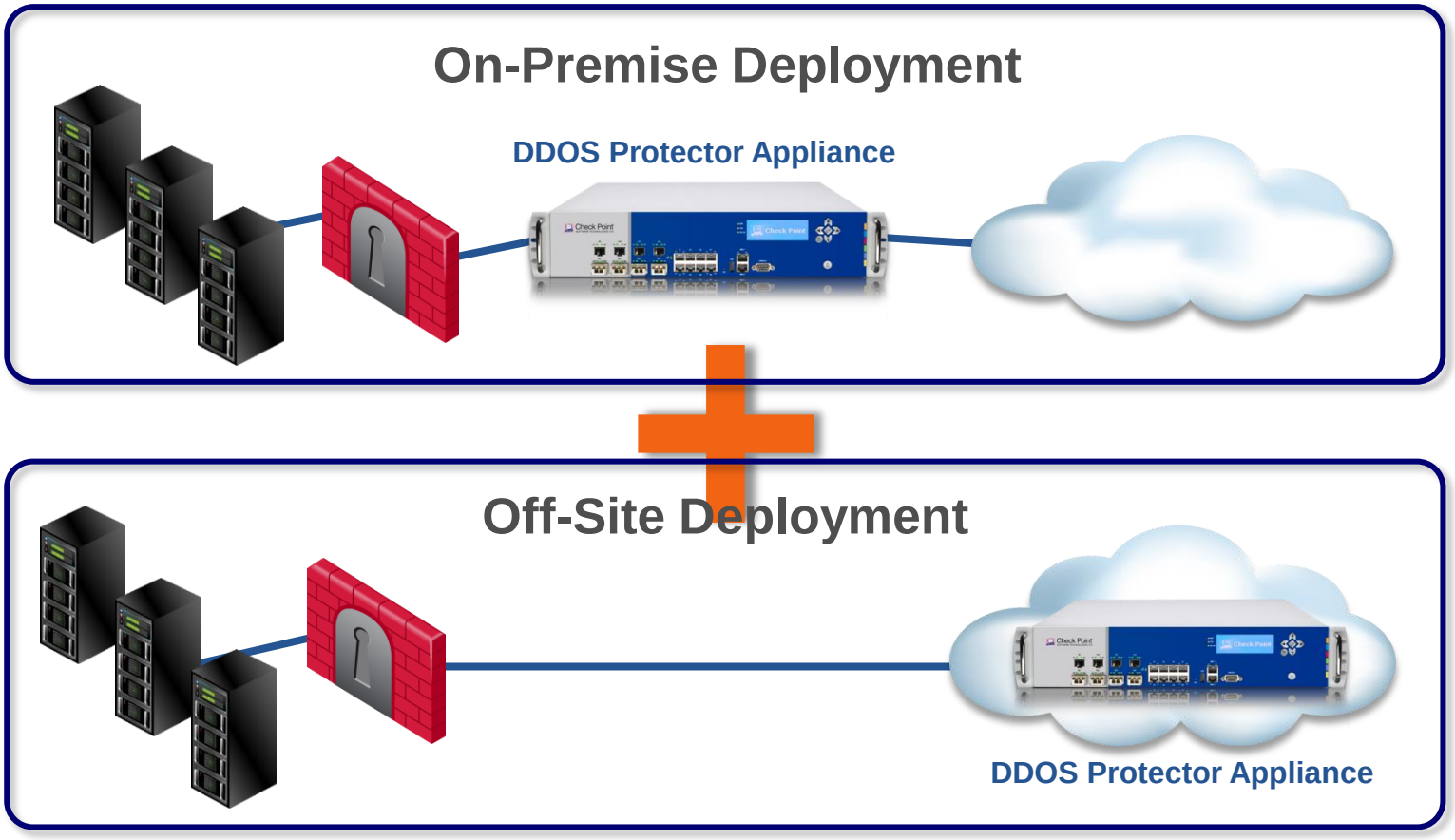
- DOS Shield (DOS signature)
- Behavioral DOS
- DNS Protection
- Syn Protection
- Out of state
- Connection Limit
- HTTP Mitigator
- White list/Black list

Block Denial of Service Attacks Within Seconds!

Where to Protect Against DDOS

Check Point SOFTWARE TECHNOLOGIES LTD.

Scenarios: 1 2 3



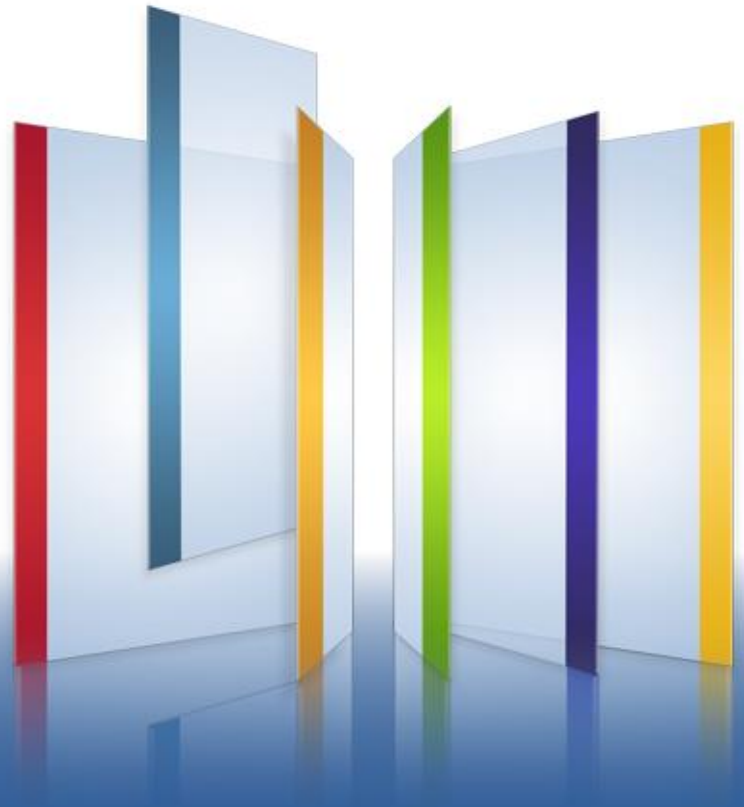
Appliance Specifications

Check Point SOFTWARE TECHNOLOGIES LTD.

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



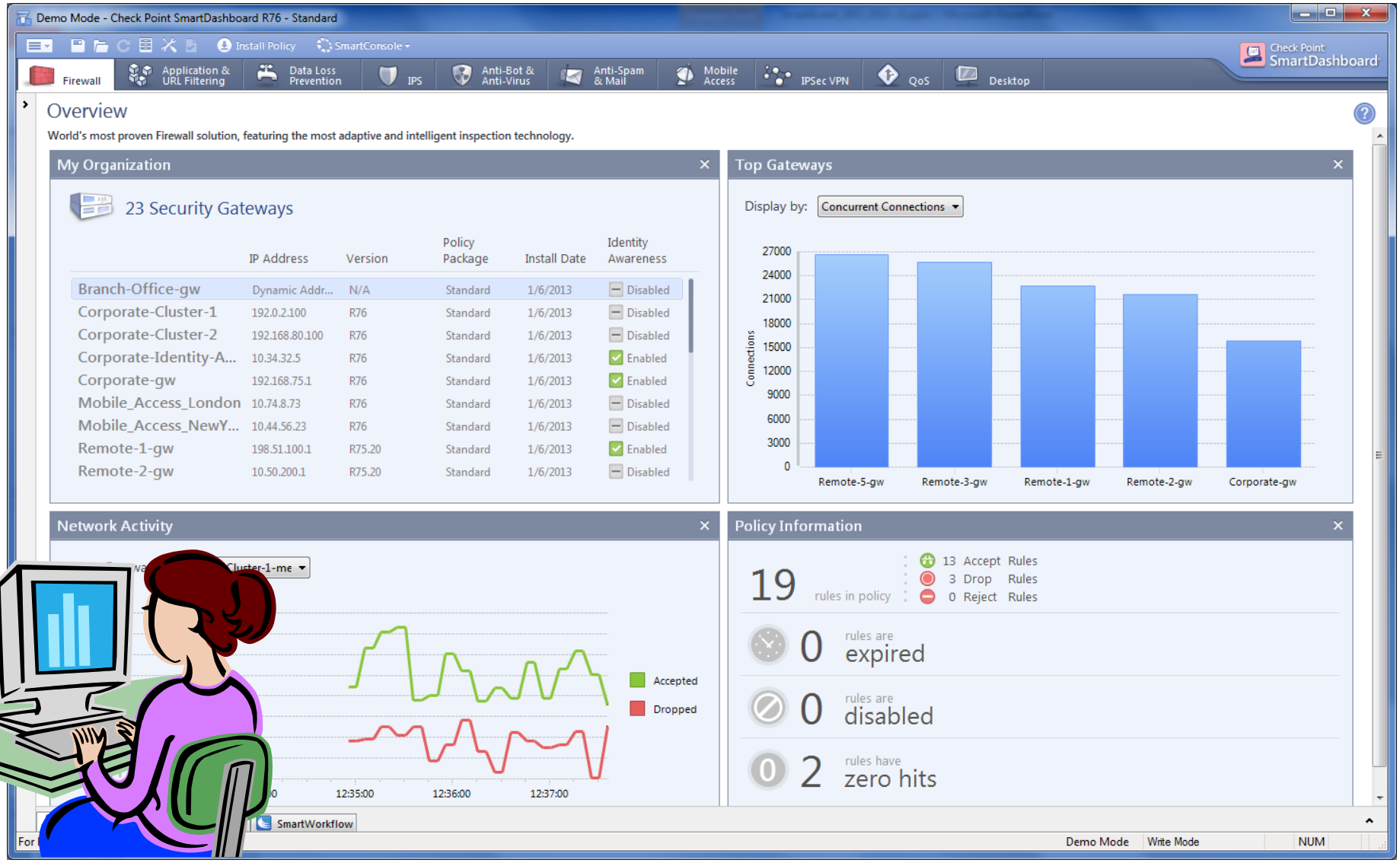
Seznamte se s Májou

Systémová administrátorka ve velké firmě na léky

Seznamte se s Alexendrem

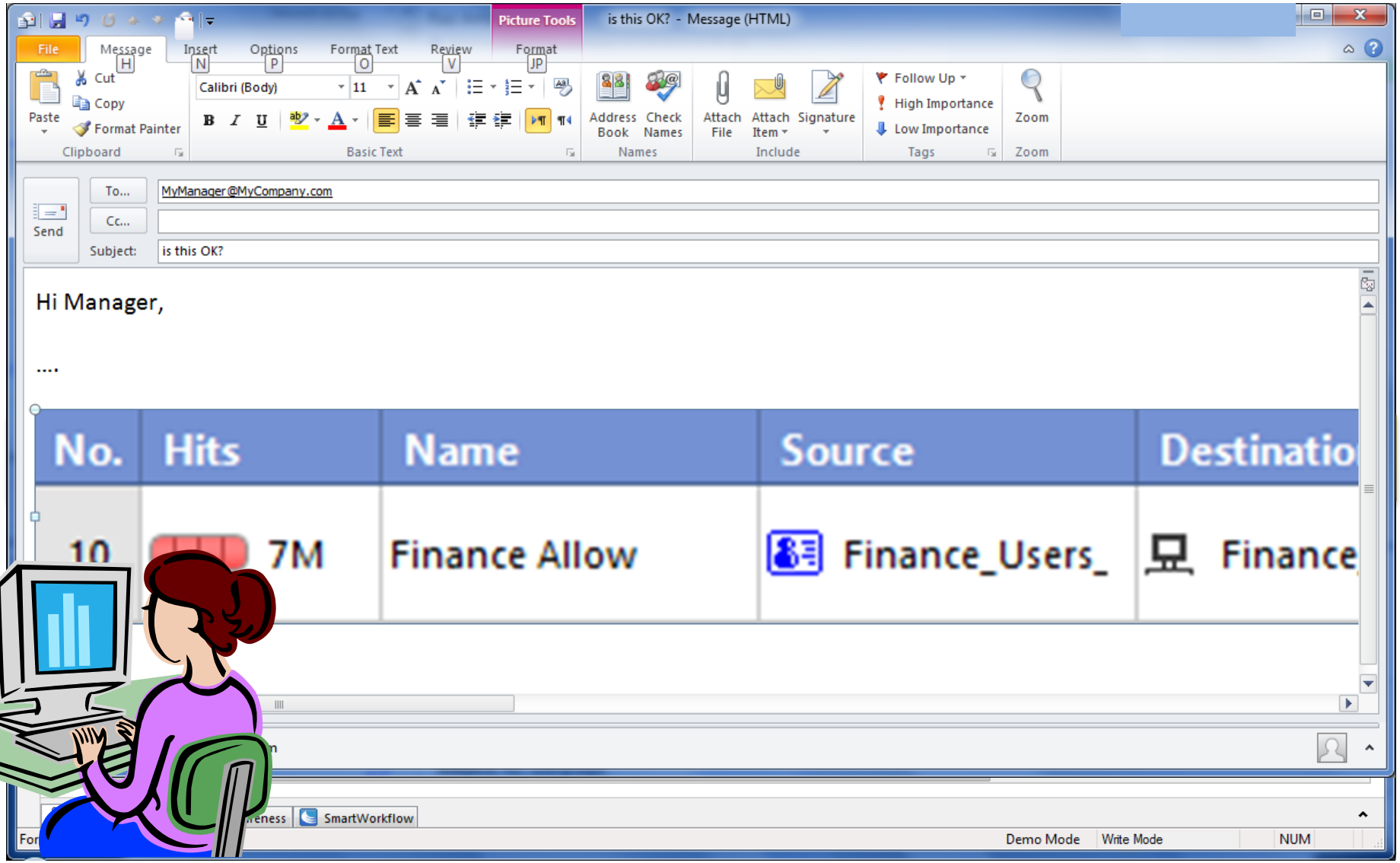
Finanční ředitel
ve velké firmě na léky

Přehledný management

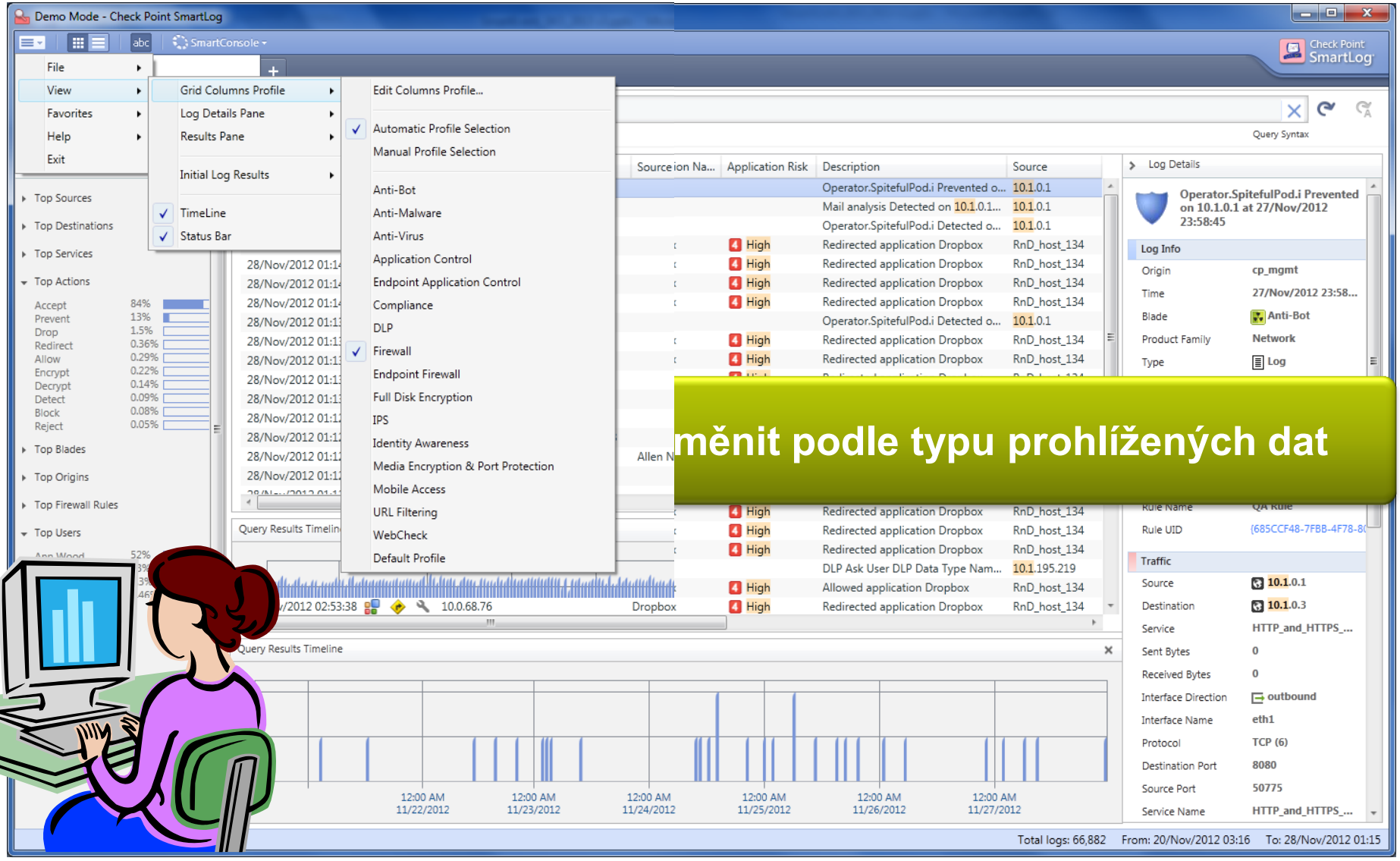


Viditelnost

Bezpečnostní politika - firewall

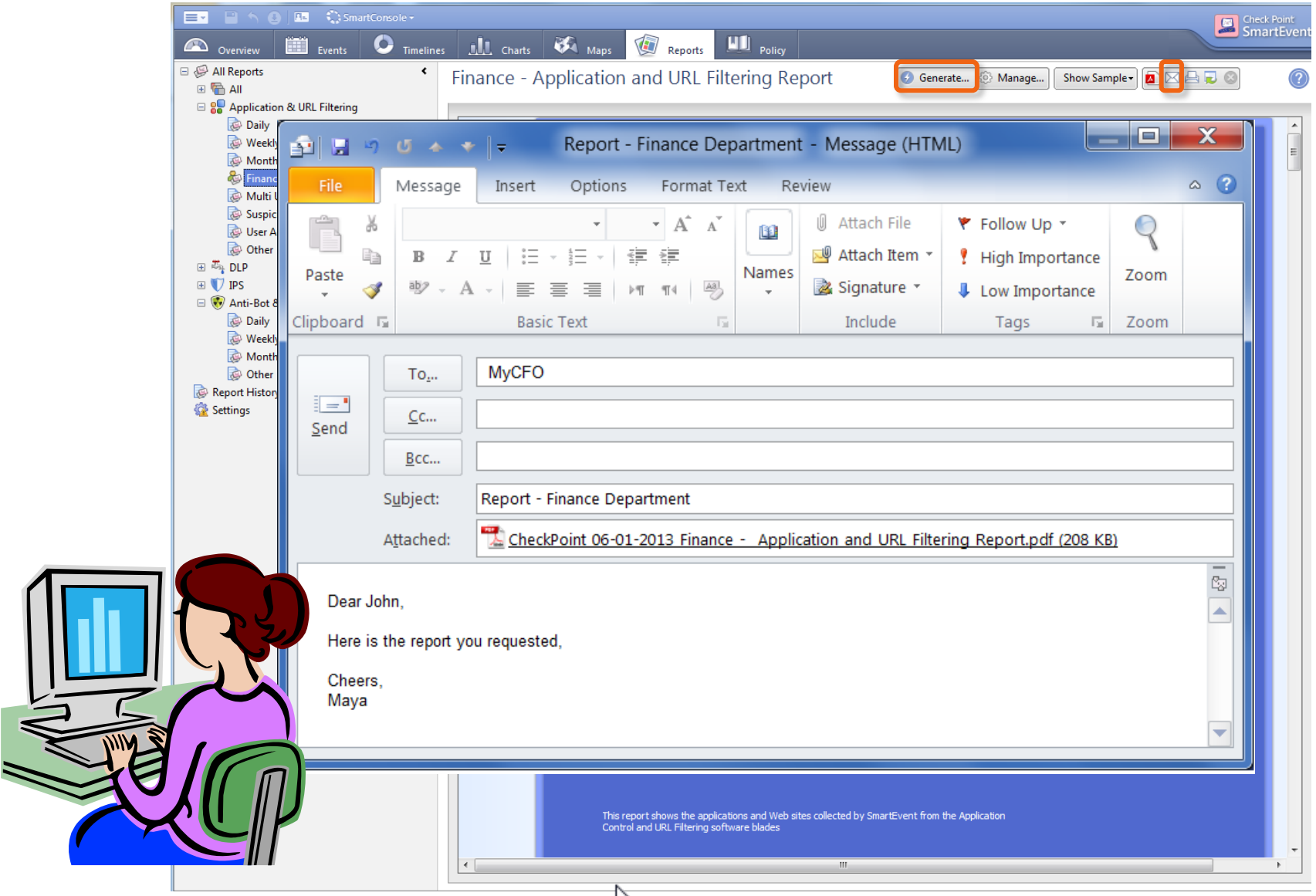


SmartLog – Google pro logy

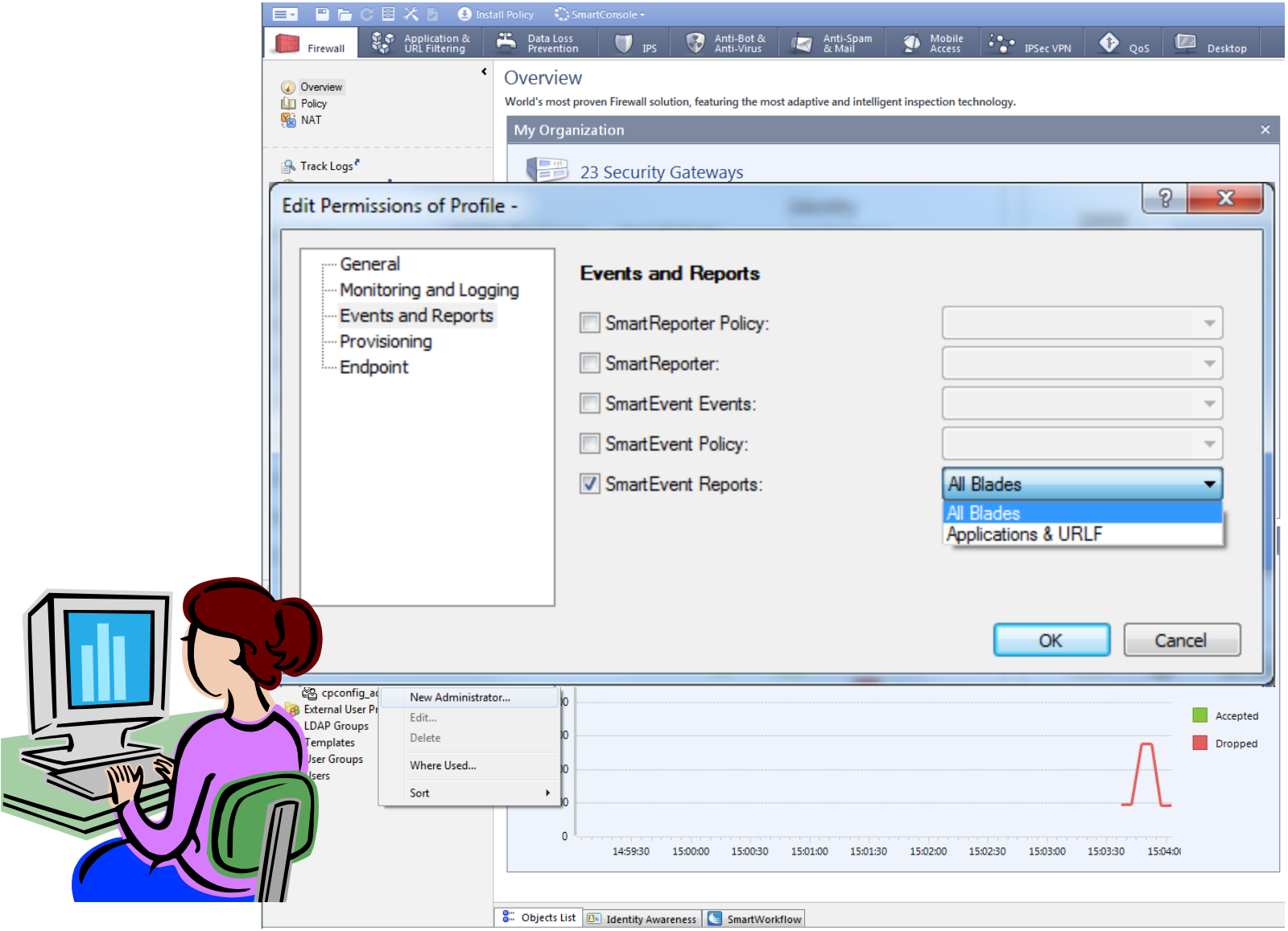


měnit podle typu prohlížených dat

SmartEvent – reporty za oddělení

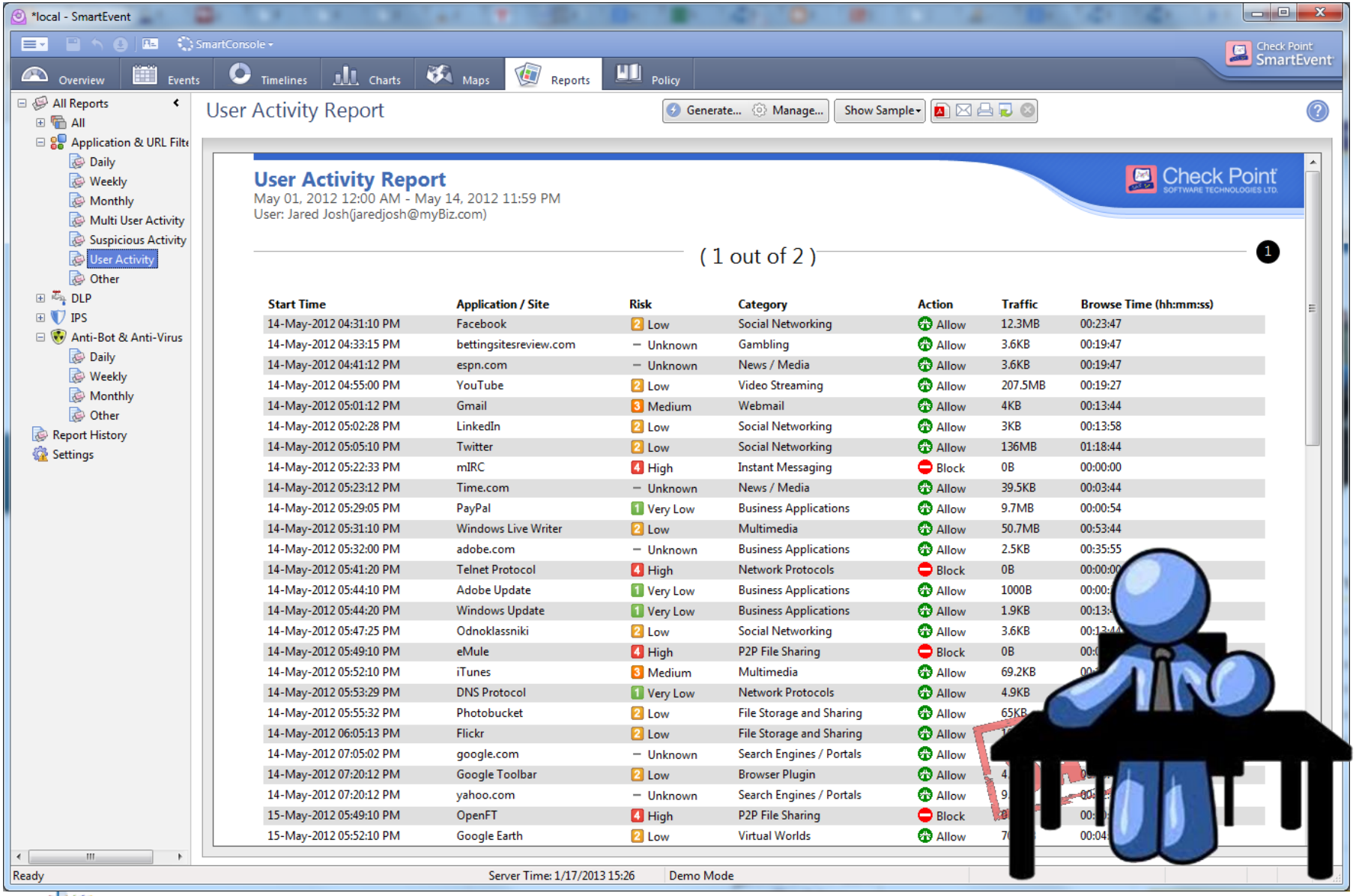


Delegace práv pro reporty

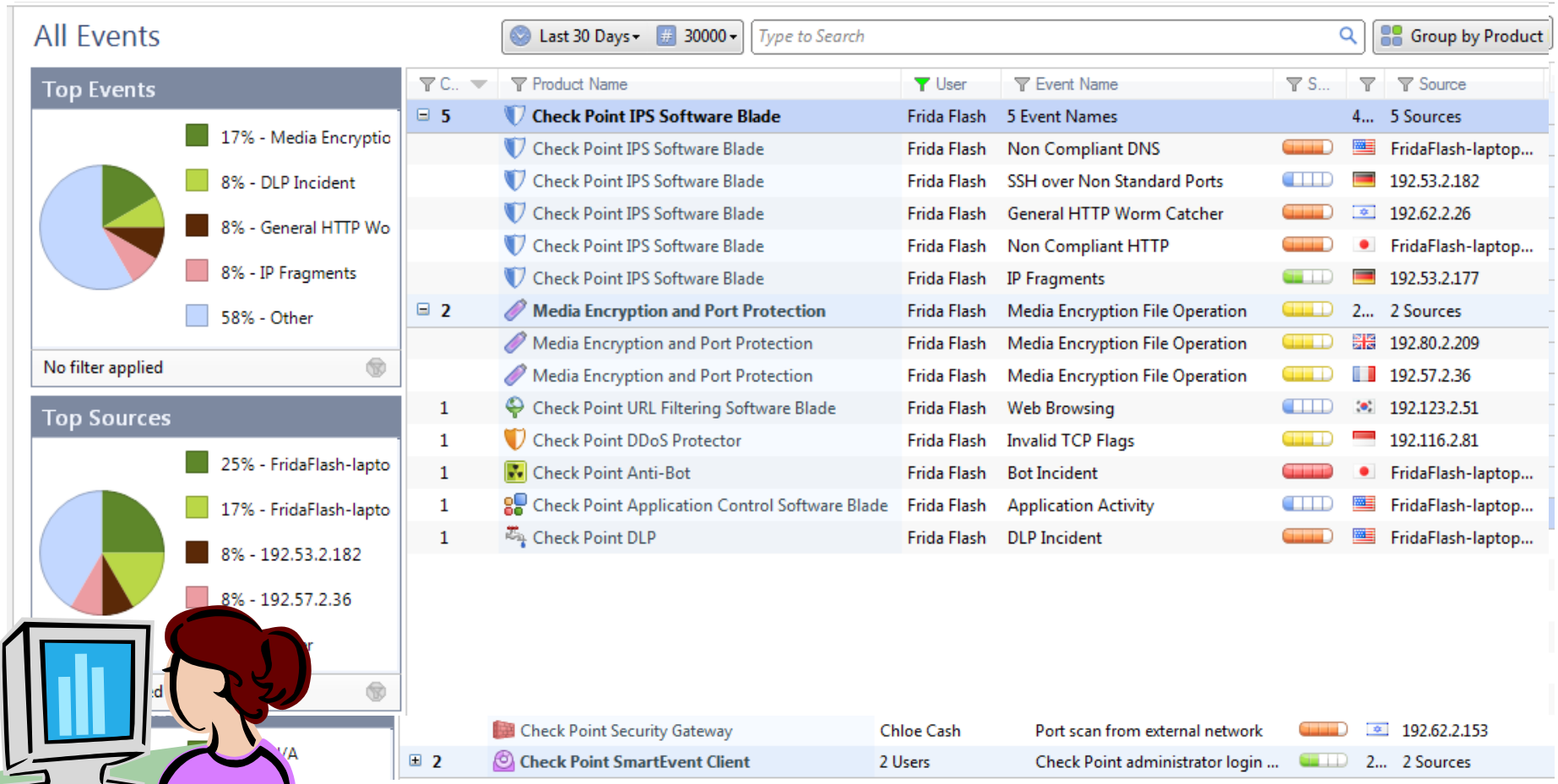


Přehled uživatelské aktivity

Check Point SOFTWARE TECHNOLOGIES LTD.



Vyšetřování možných incidentů



Vazba incidentů na správu politik

Check Point SOFTWARE TECHNOLOGIES LTD.

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
	BlancaBash-laptop (125.0....	Blanca Bash	URL Reputation	REP.ggds	Malicious file/exploit download
	HerbieHash-laptop (125.0....	Herbie Hash	URL Reputation	REP.ggds	Malicious file/exploit download
	LeeLash-laptop (125.0.0.3)	Lee Lash	URL Reputation	REP.ggds	Malicious file/exploit download
3	3 Sources	3 Users	2 Protection Types	2 Protection Names	2 Malware Activities
	BrianBash-laptop (86.0.0.12)	Brian Bash	Suspicious Mail	Mail Analysis	Spam
	DiedreDash-desktop (125....	Diedre Dash	IP Reputation	REP48034	Communication wtih C&C
	IanWhitewash-laptop (86....	Ian Whitewash	Suspicious Mail	Mail Analysis	Spam
13					

Mar 23 2012

19

Bot Incident: Detect

Copy Details | Actions | Anti-Bot | Summary | Details

- Go to Rule
- Add Exception to Anti-Bot Rule

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)

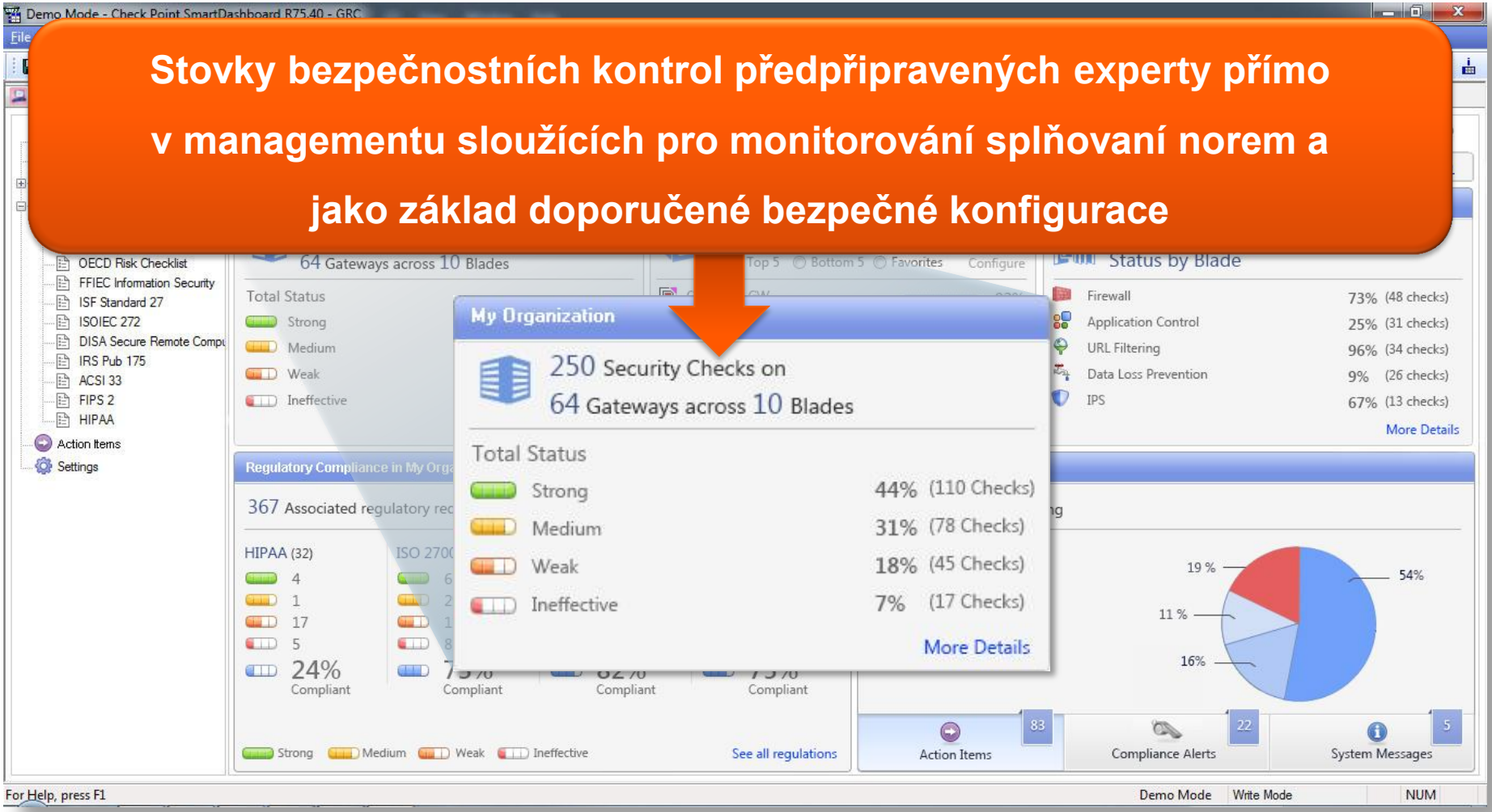
Workflow: přehled, autorizace, revize

SmartWorkflow: Automated Policy Change Management

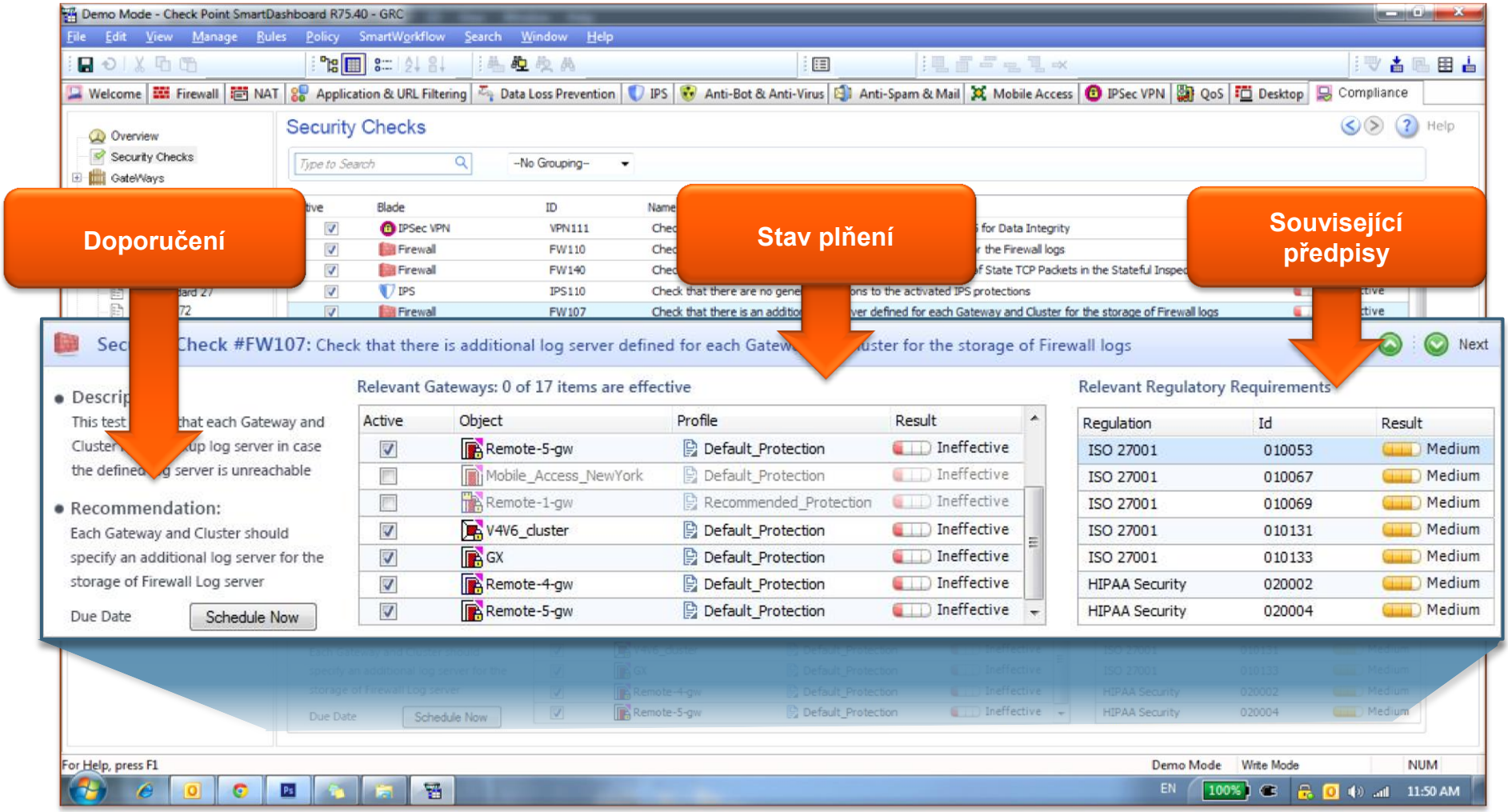
- Visual change tracking
- Flexible authorization
- Audit trails
- Single Console Integration

Compliance, best practices

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

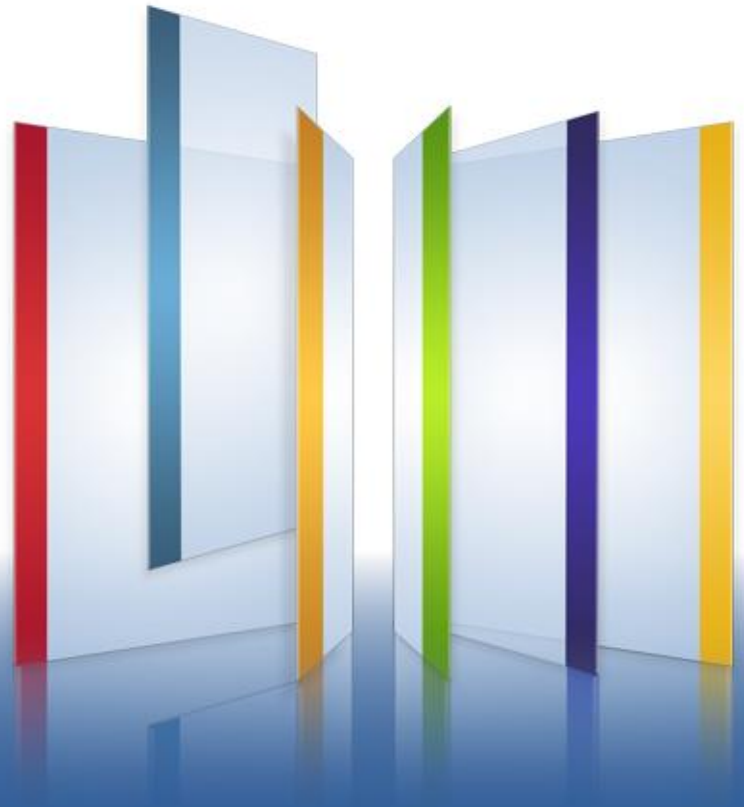


Compliance: Bezpečnostní kontroly politik



Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Infrastruktura



Check Point and HTTPS Inspection

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

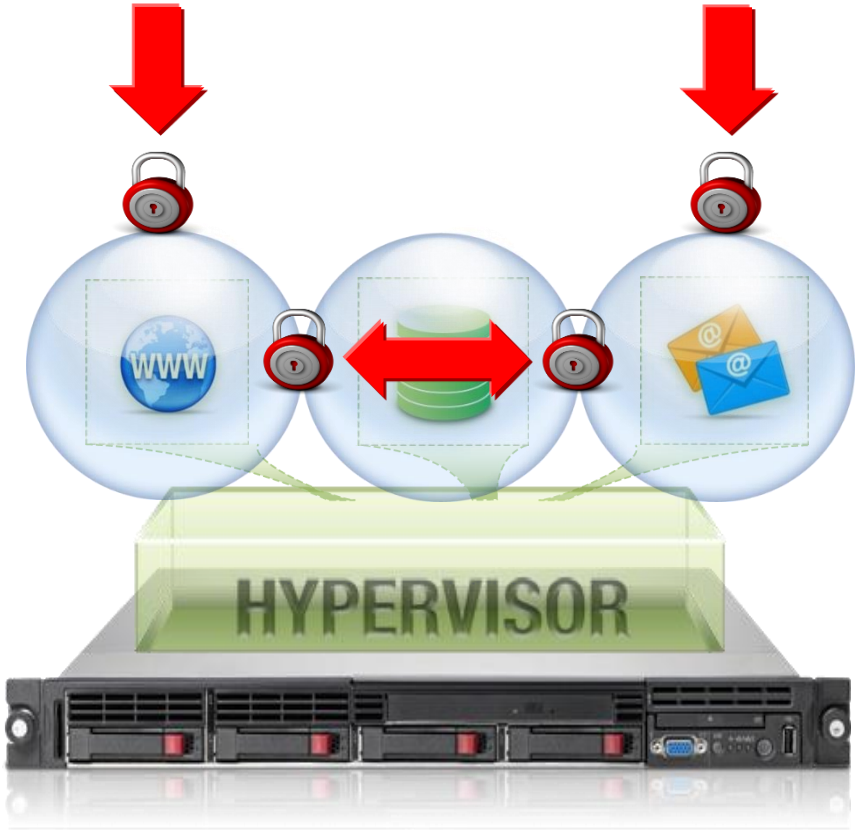
Check Point HTTPS inspection

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	TCP https TCP HTTP_and_H...	Any	Bypass	None	All
2		Any	Internet	TCP https TCP HTTP_and_H...	Email Financial Services Health	Bypass	None	All
3		Any	Internet	TCP https TCP HTTP_and_H...	Any	Inspect	Log	All

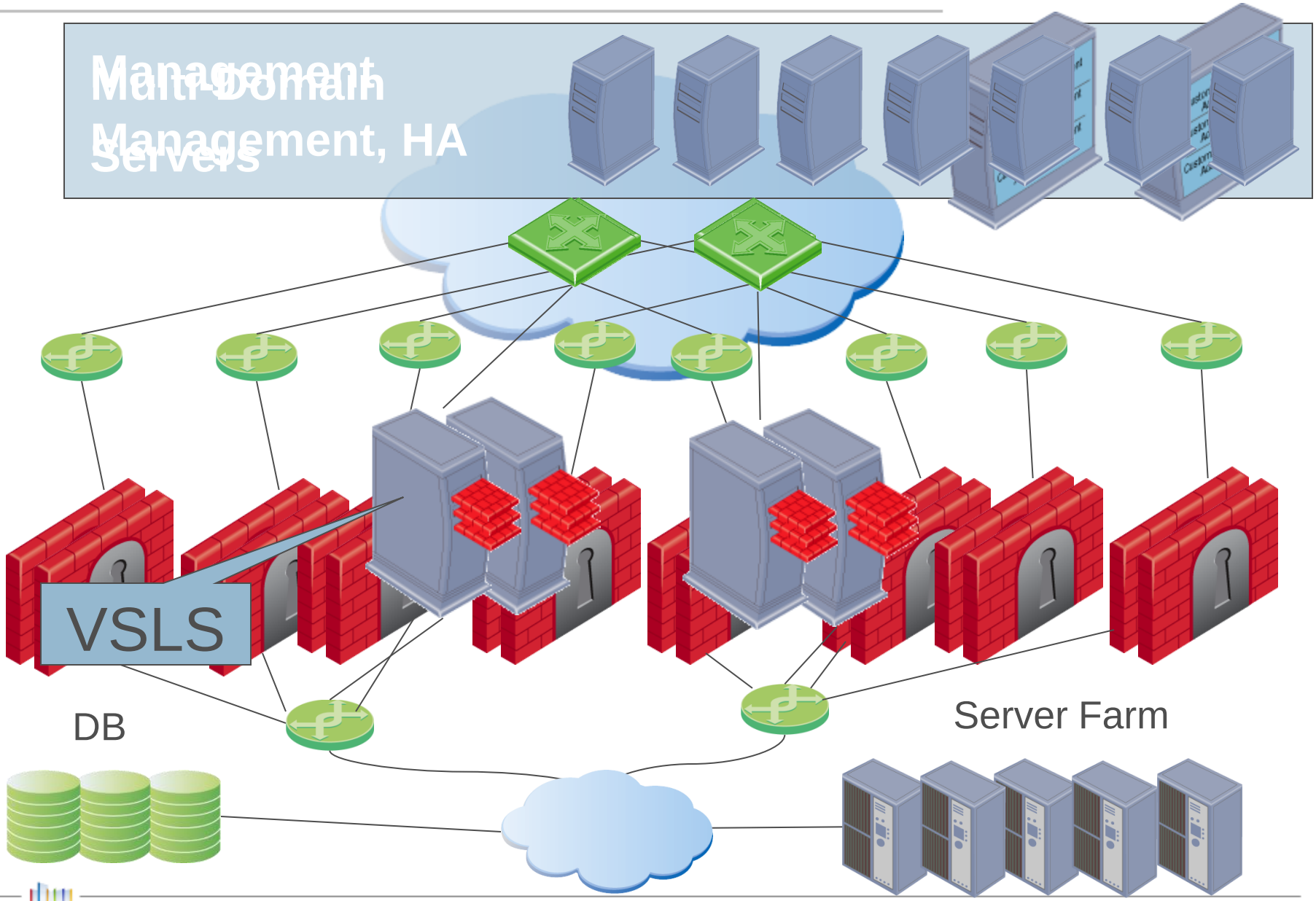
Virtual Edition: zabezp. VMware ESX



Security Challenges in Virtual Environments

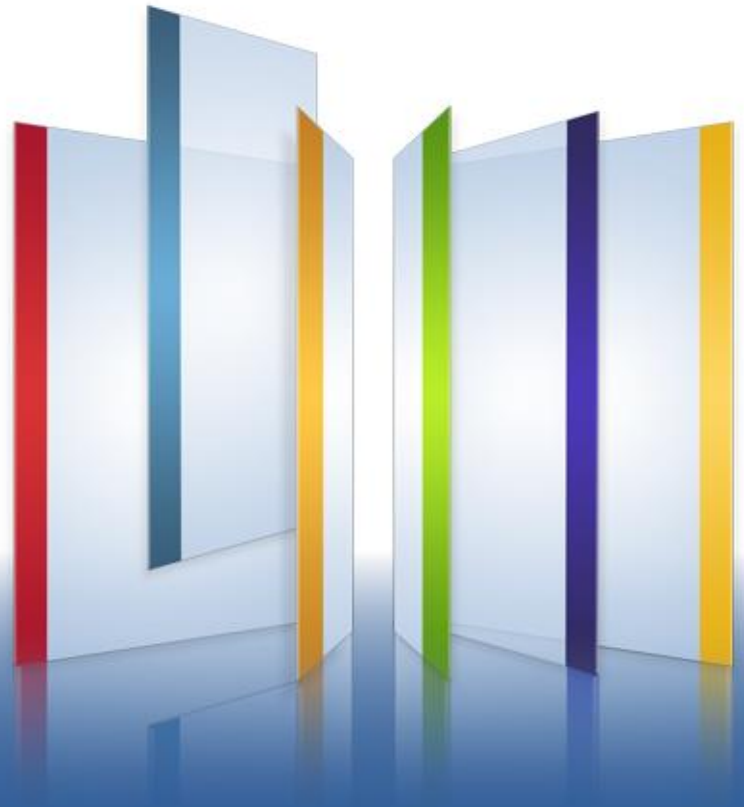
- Protection from external threats
- Inspect traffic between Virtual Machines (VMs)
- Secure new Virtual Machines automatically

Virtualized Security – Virtual Systems



Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Shrnutí



DMZ – koncepty zabezpečení

- 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)

Nad rámec prezentace

- 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

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.

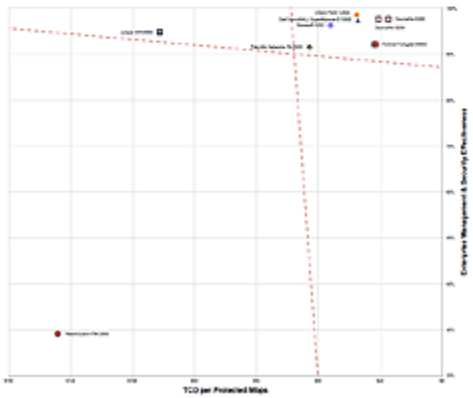
Register Now to Schedule Your Onsite Security Analysis

Additional Information

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

Download Now

NSS Value Map



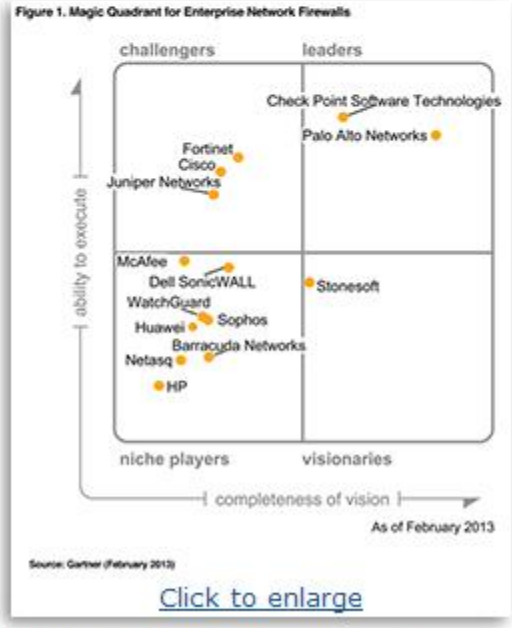
Click to enlarge

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

Gartner

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.



Click to enlarge

Register Now to Schedule an Onsite Security Analysis

We'd Like to Help!

CHATLIVE Start Chat Now

Contact Us

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

* = required

First Name*

Last Name*

Company Name*

Company Size*

Please select...

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Vaše dotazy