

Security Intelligence: tracking obfuscated and unrecognized attacks

Jarosław Prokop
jprokop@checkpoint.com
+48 507 010 447

Security Policy Rule Types:

1

Access

People, Applications, Services, Servers, Data

2

Threat Prevention

Cleanup actions for malware and attacks

Prevent downloading Credit Cards from corporate web server

- Standard services: HTTP and HTTPS
- Additional protection layer vs. injection attacks or server mis-configurations

Full data log, including:


















- URL
- HTTP resources accessed
- Methods
- File type
- File size
- Data types matched

No.	Name	Source	Destination	Services & Application...	Data	Action	Track
1	Allow employees to use facebook	📅 Employees	☁ Internet	📘 Facebook	* Any	🟢 Accept	📄 Full Data Log
2	Allow users to use Skype	📅 Employees	☁ Internet	💬 Skype	* Any	🟢 Accept	📄 Log
3	Prevent downloading credit card numbers from corporate web server	* Any	💻 Web Server	🌐 Web Services	⬇ Download Traffic 🔍 PCI - Credit Card...	🔴 Drop	📄 Full Data Log
4	Allow marketing and HR to upload documents to Facebook	📅 Marketing 📅 HR	☁ Internet	📘 Facebook	⬆ Upload Traffic 🔍 Document File	💬 Ask 🔍 Compan... 🕒 Once a d... 🔍 Per appli...	📄 Full Data Log
5	Cleanup rule	* Any	* Any	* Any	* Any	🟢 Accept	📄 Network Log



Control Network, Application & Data As well as User Check & Log level

Cleanup actions for protected networks

Protected Scope	Protection/Site/Fil...	Action	Track
 Corporate-rnd-net	— n/a	 Recommended_Profile ^  Anti-Bot  Detect  Anti-Virus  Detect  Threat Emulation  Detect	 Log
 Remote-3-internal	— n/a	 Branch-Profile ^  Anti-Bot  Prevent  Anti-Virus  Prevent	 Log  Packet Capture

Areas of ambiguity in defining and enforcing security policies:

- DoS / DDoS attacks
- Bots communicating with external Command&Control centers
- Industrial networks security policy (*SCADA / Critical Infrastructure*)
- Zero-day attacks and obfuscated (masked) malware



DDoS: Experiences collected during PoC installations: where to protect

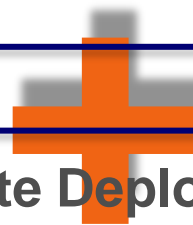
Scenarios:

1

2

3

On-Premise Deployment



Off-Site Deployment



DDoS: How to protect

(* Traffic used in DDoS attacks is accepted by standard security policy *)

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

 (* Traffic models, anomaly detection, filtering. Or: correlation of attack data based on logs *)

*Analysis of data collected by
DDoS protection appliance*

*Data collected and correlated in SmartEvent system
in May - July 2013*

(...)

*DDoS Protector deployed to identify problems related to
DNS servers*

(August / September 2014)

(...)

Zero-day attacks and targeted attacks

2012 Top Vulnerable Applications

 Adobe Reader 30 critical exploits	 Java 17 critical exploits	 Office Microsoft Office 16 critical exploits
 Adobe Flash 57 critical exploits	 FireFox 91 critical exploits	 Internet Explorer 14 critical exploits

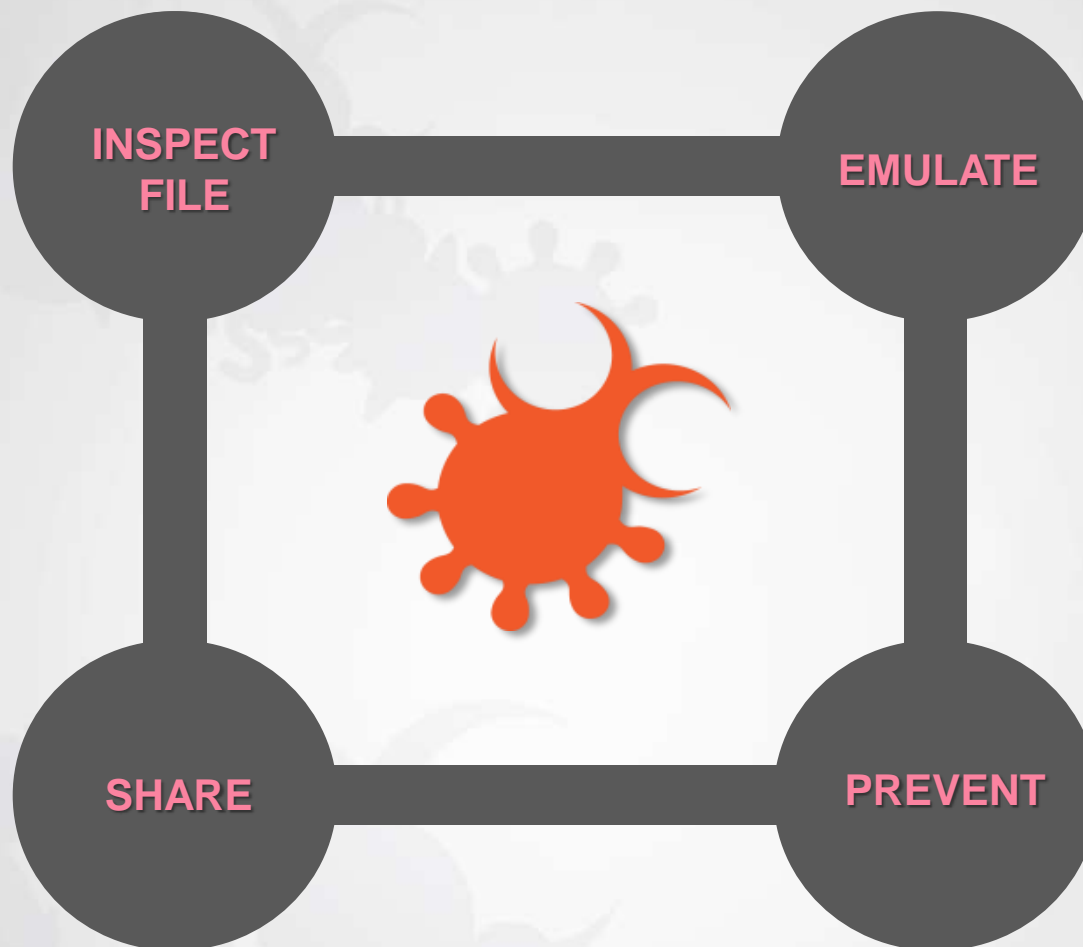
New vulnerabilities



Variants of old exploits

“nearly 200,000 new malware samples appear around the world each day”

- net-security.org, June 2013



Stop undiscovered attacks with
Check Point Threat Emulation

System otwarty i udostępniony w Internecie
Wyślij plik – otrzymasz raport Threat Emulation:



threats@checkpoint.com



threatemulation.checkpoint.com



Data collected in search of obfuscated
and/or zero-day attacks and high-risk
applications
(sandboxing in public cloud)

(May 2014)

(...)



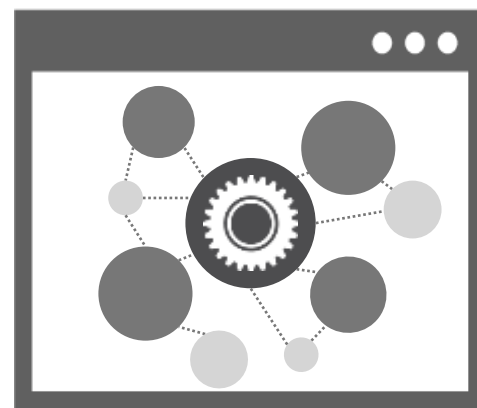
Security **best practices** built right into your workflow



Policy Apps



Trusted
Automation



Orchestration

Standard +

Access Policy

NAT

Shared Policies

- Desktop
- QoS
- Mobile Access

Install Policy Search Policy...

No.	Name	Source	Destination	VPN	Services	Action	Applications / Sites	Data
▼ (Rules 1-2) Management & Gateways								
1	Enable open shell and open WebUI from management	Management Server	Gateways	* Any	Management...	Accept	Any Recognized	*
2	Stealth rule	* Any	Gateways	* Any	* Any	Drop	Any Recognized	*
▼ (Rules 3-7) Internet Access								
3	Drop high risk applications	* Any	* Any	* Any	* Any	Drop BlockedM...	High Risk Critical Risk	*
4	Sales Operations Policy	Sales Opeartions	* Any	* Any	* Any	Sales Operatio...	Any Recognized	*
5	File Sharing - User Check	* Any	* Any	* Any	* Any	Ask FileSharing Once a day Per applic...	File Storage and Shar...	*
6	Finance Access	Finance	DMZ Servers	* Any	TCP http	Accept	Any Recognized	*
7	Enable Internet access	InternalZone	Internet	* Any	Internet Prot...	Accept	Any Recognized	*

Summary Details Logs History

Summary Details Logs History

Timeline

- Today | 1:20PM
Rule edited by Jack Snow
- 13 Aug 2015 | 12:34PM
Rule edited by Mike Sun
- 12 Aug 2015 | 10:01AM
Rule created by Jack Snow

Name	Source	Destination	Services	Action
Finance Access	Finance_net_A Finance_net_B DELETED	Corporate_Server1 Corporate_Server2	TCP http	Accept
Finance Access	Finance_net_A Finance_net_B	Corporate_Server1 Corporate_Server2 ADDED	TCP http	Accept
Finance Access	Finance_net_A Finance_net_B	Corporate_Server1	TCP http	Accept

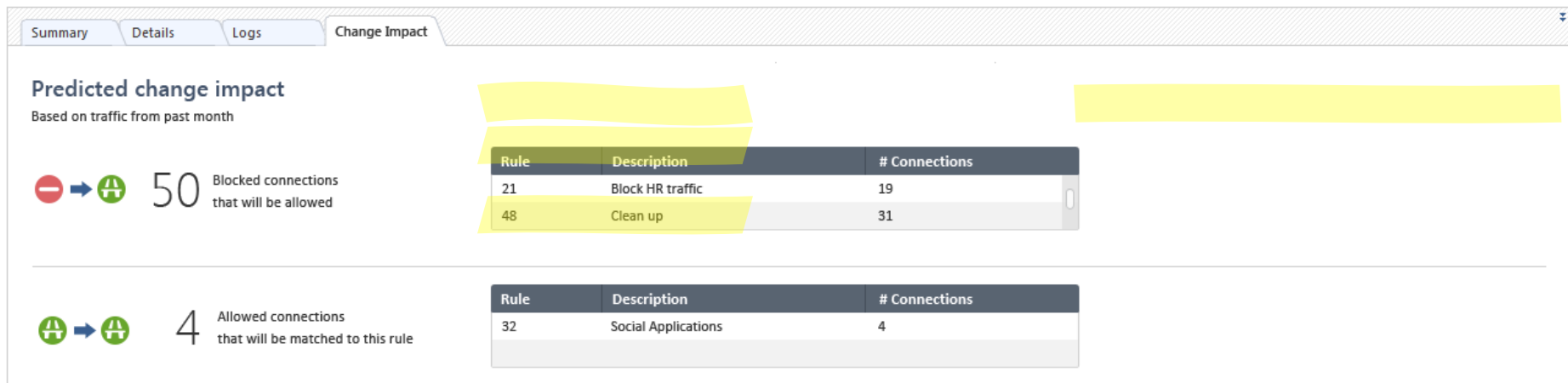


POLICY APPS – RULE'S HISTORY

Track historic changes of rules and objects

Items to consider before changing a rule

- When was it created? By who? Why? Is this rule being hit and how much?
- What sources / users / destinations / applications are using it?
- How this change is going to affect traffic going through lower rules?



Thank you!

Jarosław Prokop

jprokop@checkpoint.com

+48 507 010 447