



Check Point®  
SOFTWARE TECHNOLOGIES LTD

Check Point  **Live!**  
**CHECKMATES**

# MIGRATE TO R80.20

CheckMates Live!  
Moscow 2018

Valeri (Val) Loukine | Cyber Security Evangelist

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

POWERED BY  CHECK POINT  
**INFINITY**

CLOUD • MOBILE • THREAT PREVENTION

Check Point   
**CHECKMATES** The Why:

To Build...



an online platform with **LARGE CROWD OF USERS** and give them the ability to share challenges, APIs, benefits, ideas, questions, discussions and connect through meetings and local User Groups.

And Encourage...



1. **Crowdsourcing**
2. Direct conversation
3. Information sharing
4. Excitement
5. Feedback
6. Ideas
7. Early adopters
8. Problem solving

# Introducing our User Community....

# Check Point CHECKMATES <https://community.checkpoint.com>

## FOLLOWING

 **Victor MR** in General Product Topics  
4 days ago

### My top 5 SecureKnowledge solutions

Usually during training events we talk about useful resources and tools, including several SecureKnowledge solutions. There are several of them that I could print and put in my nightstand. I will start with my top. sk97638: Check Point Processes and DaemonsList of the processes and daemons, what they do, where are their logs, how to

 4  1

## DEVELOPER NETWORK

 **Maarten Sjouw** in Developers (Code Hub)  
6 days ago

### Export of the VPN communities

Is there anyone who knows about the license information tool script? It is available on management and collects information from management and all gateways (if online) and exports all this information to a XML file. You can upload this to Check Point to update this info in the usercenter. We use this script for collecting info about the

 0  9

 0  0

## RECENT POSTS

 **Stuart Green** in Logging, Monitoring, & Event Analysis  
3 days ago

### Solution to an R80.10 problem with SmartEvent, an IP Address Change and a broken Correlation Unit

Thought I'd share a solution to a problem here as I couldn't find an sk on the exact error that was aimed at R80. We had to change the IP address on a customer's Smart-1 which broke the SmartEvent correlation unit and the only sk that seemed relevant was sk119072 but that hasn't been updated for R80 by the looks of things. I did,

 1  0

## CHECKMATES NEWS

 **Muhammad Nadeem Arif** in General Product Topics  
5 days ago

### i am planning to update license for my gateways and management servers. will this brake my cluster while updating license gateways, which are member of cluster



# We grow together

**CPX 2017**  
launched

**95K**  
**USERS**

From over  
**150+**  
Countries



Check Point  **CHECKMATES** Events



WELCOME TO THE FUTURE OF CYBER SECURITY

©2017 Check Point Software Technologies Ltd.

[Protected] Distribution or modification is subject to approval

# Grow, Share, and Inspire!

CheckMates activities



Getting Started on CheckMates

Check Point   
**CHECKMATES**

**TECHTALKS**  
LEARN.SHARE.INSPIRE.

 **CODE HUB**

**"HOW TO"  
VIDEOS**



Local User Group Meetings

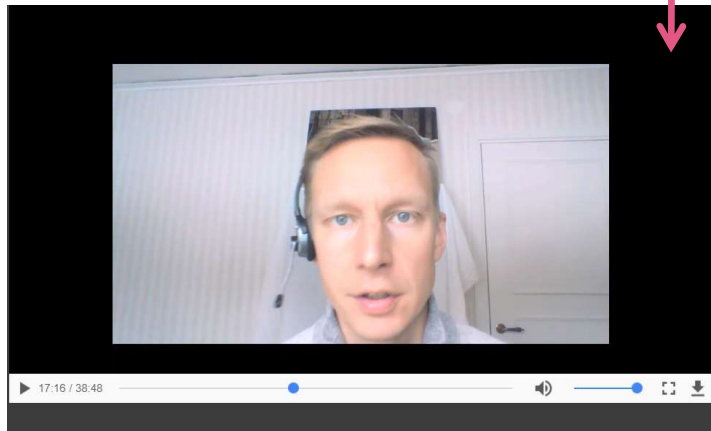


# Explore the Top 3 posts on CheckMates



Check Point  
SOFTWARE TECHNOLOGIES LTD

Content Leaderboard <span>?</span>		E-mail CSV	Download CSV
1	My Top 3 Check Point CLI commands Moti Sagey	Views: <b>135,657</b>	
2	I am Dorit Dor, VP of Products for Check Point, Ask Me Anything! Dorit Dor	Views: <b>73,070</b>	
3	R80.x Training Videos Dameon Welch Abernathy	Views: <b>72,211</b>	



R80 Management Training Lesson 1 - Big Picture

<http://tiny.cc/r80videos>

My Top 3 Check Point CLI commands  
Discussion created by **Moti Sagey** on Jul 19, 2017  
Latest reply on Oct 17, 2017 by Moti Sagey

Like • 40    Comment • 117

Just had a fun geeky conversation with [Dameon Welch Abernathy \(AKA Phoneboy\)](#), [Jony Fischbein](#), [Jeff Schwartz](#) and [Michael Poubion](#) (over 100 accumulated years of experience in Check Point products), on what are our favorite & most useful commands in a Check Point environment.  
Below are my 3, plz add yours in the comments (we will do a poll for the top 5 after getting your feedback ... 😊).

1) `fw ctl zdebug drop`  
used to quickly see all dropped connections and more importantly the reason (e.g. anti-spoofing, IPS, FW rule, ...)

<http://tiny.cc/top3cli>

---

I am Dorit Dor, VP of Products for Check Point, Ask Me Anything!  
Blog Post created by **Dorit Dor** on Sep 2, 2017

Liked • 19    Comment • 99

CheckMates members can **WATCH A VIDEO** of the event with special commentary here: [Ask Me Anything with Dr. Dorit Dor and Team](#)

I am Dr. Dorit Dor, Vice President of Products at Check Point. I lead the company's product management, business development, research and development (R&D) and quality assurance (QA). Together with the amazing product team at Check Point, we lead the initiatives from concept to delivery and oversee the roadmap.

<http://tiny.cc/amadorit>

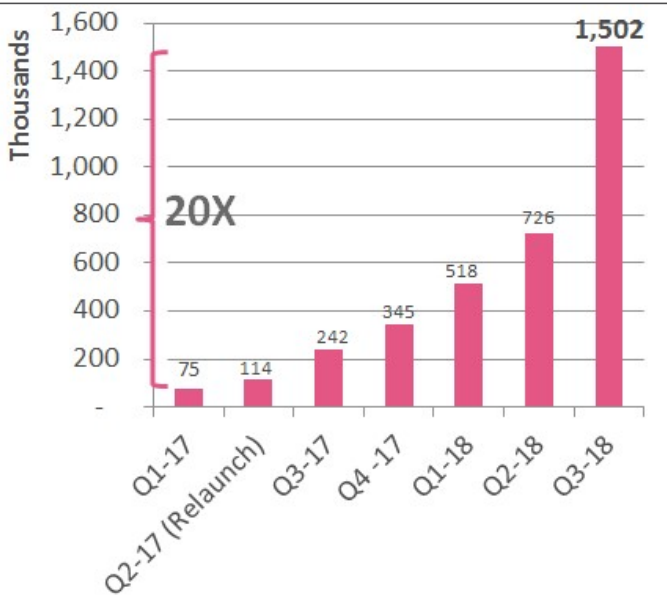
WELCOME TO THE FUTURE OF CYBER SECURITY

# CheckMates Community Growth Metrics

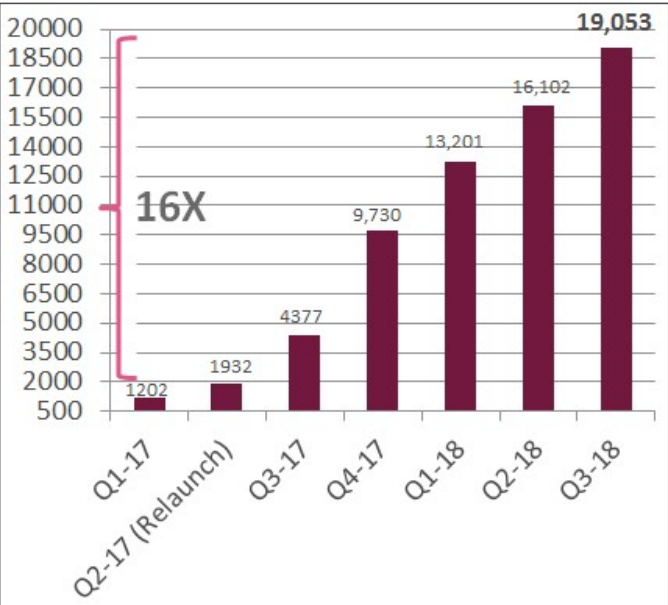
## Page views, New users, Active users



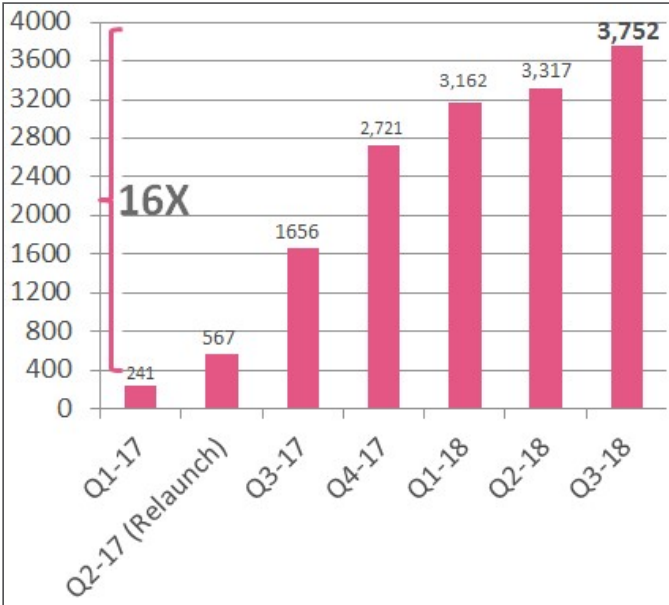
# of average monthly views (K)



# of registered users (non-employees)



# of active users (Monthly average)



**20X growth in views, 16X growth in new users, 16X growth in active users**

WELCOME TO THE FUTURE OF CYBER SECURITY

©2017 Check Point Software Technologies Ltd.

[Protected] Distribution or modification is subject to approval





# Agenda

- Why Should You Upgrade
- Hardware Requirements
- Staging the Management Upgrade
- Doing the Upgrade

# What Is R80.x About?

- Presenting a new architecture for the security gateway
  - Improvements for existing customers
    - SecureXL template support for Domain, Time and Dynamic objects
    - VSX gateways can be upgraded in place and support more concurrent connections
- Providing visibility functionalities on the management server
  - Session based logging
  - Flexible event management and reporting
- Supporting delegation of duties
  - Assign administrative roles to security policy layers and dedicated security functions, for example creating a dedicated admin for IPS

# Security Policies Expressing Your Business Needs

- Unified Rule Base
  - Creating layered policies allowing delegation of duties, large complex rule bases without compromising performance
- Content Awareness
  - Achieve content control for applications
- Session Logging
  - Visualize the number of connections required and the amount of data being transferred



# Embracing The Critics

- I am a pure Firewall customer: why should I care about R80.10?
  - DNS Name objects and Time objects are now supporting SecureXL Templates
  - Multiple security administrators can work on the same policy at the same time
- I am a VSX customer and can't scale the amount of concurrent connections per VS
  - R80.X provides virtual systems running in 64bit mode supporting millions of concurrent connections
- I am using IPS and can't have a dedicated security admin
  - Delegation of duties through Layered Threat Prevention policies

---

The logo for R30.20, featuring the text 'R30.20' in a white, sans-serif font. The '30' is partially enclosed by a pink circular shape that overlaps the 'R' and the '0'.

R30.20



## Embracing The Critics

- I have tried DLP back in time and it was killing performance
  - Content Awareness runs in each CoreXL instance
- Check Point can only use a single core for IPSec VPN
  - With R80.X VPN connections are scaling across all CoreXL instances
- I can't create my own report
  - Use Logs & Monitor creating the reports and views as you need them
- Identity Awareness doesn't scale across my organization
  - Evaluate Identity Collector and ID Awareness API

---

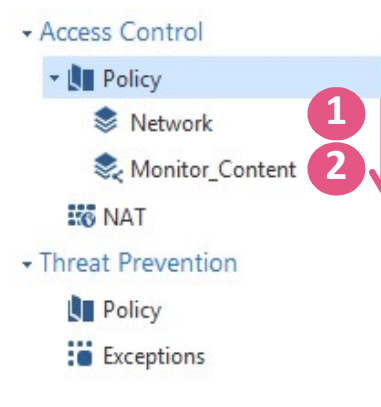
The logo for R30.20, featuring the text 'R30.20' in a white, sans-serif font. The '30' is stylized with a pink circular background behind the '0'.

R30.20

# Security Policies Expressing Your Needs

## Ordered Layers and Inline Layers

- Enforcing security using an **ordered** layered structure
  - The upper most policy layer will be matched first
  - In case a rule is matched, this traffic will be matched against subsequent layers
- Enforcing security using an **inline** layered structure
  - A rule (called “parent rule”) defers matching to a subsequent layer of specific rules
  - Only traffic that matches the “parent rule” will be matched against the rules of the Inline Layer



4	Parent rule for web server	* Any	web+mailserver	Web Browsing	* Any	WebServerPolicyLayer	N/A
4.1	Documents	* Any	web+mailserver	Web Browsing	Download Traffic Document File	Accept	Extended Log Accounting
4.2	Spreadsheets	* Any	web+mailserver	Web Browsing	Download Traffic Spreadsheet or CSV File	Accept	Extended Log Accounting

## Ordered Layers And Inline Layers Supported Policy Targets

- **R77.x** gateways support **only Ordered Layers**
  - **Only one Software Blade** can be active per layer
- **R80.10** gateways support **Ordered and Inline Layers**
  - Ordered Layered policies with **one Software Blade** active
  - Ordered Layered policies with **multiple Software Blades** active
  - Ordered Layered policies **including Inline Layers**

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action
▶ Management (1-2)							
▶ Network Services (3-5)							
▶ Identity Awareness (6-7)							
▼ Inbound (8)							
8	Email	net_192.168.169.0	web+mailserver	* Any	smtp	Any Direction Document File	Accept
▼ Outbound (9)							
9	Web Browsing	net_192.168.169.0 net_192.168.170.0	Internet	* Any	Search Engines / Por...	* Any	Accept
▶ Clean up (10-11)							

Example of an Ordered Layer Policy with APCL, URLF and Content Awareness Blades active



# Updatable Objects (R80.20+)

- Managing access rules to online services is now easier than ever
- Ready-to-use, automatically updated groups do the work for you!



The screenshot displays the Check Point SmartConsole interface. A policy rule titled "Internal network access to Office Online" is selected. The rule's configuration is as follows:

No.	Name	Source	Destination	VPN	Services & Applications	Action
18	Internal network access to Office Online	Internal Network	* Any	* Any	* Any	Deny

An "Online Services" dialog box is open, showing a list of services under the "Office365 (19)" group. "Office Online" is selected. The dialog provides the following information:

- Office Online**
- Office 365 is an online cloud-hosted software suite from Microsoft.
- Additional Info**: [Office 365 URLs and IP address ranges info page](#)
- Last Checked: 16-Jan-18 18:54
- Version: 160118160009 | Downloaded: 16-Jan-18 18:14

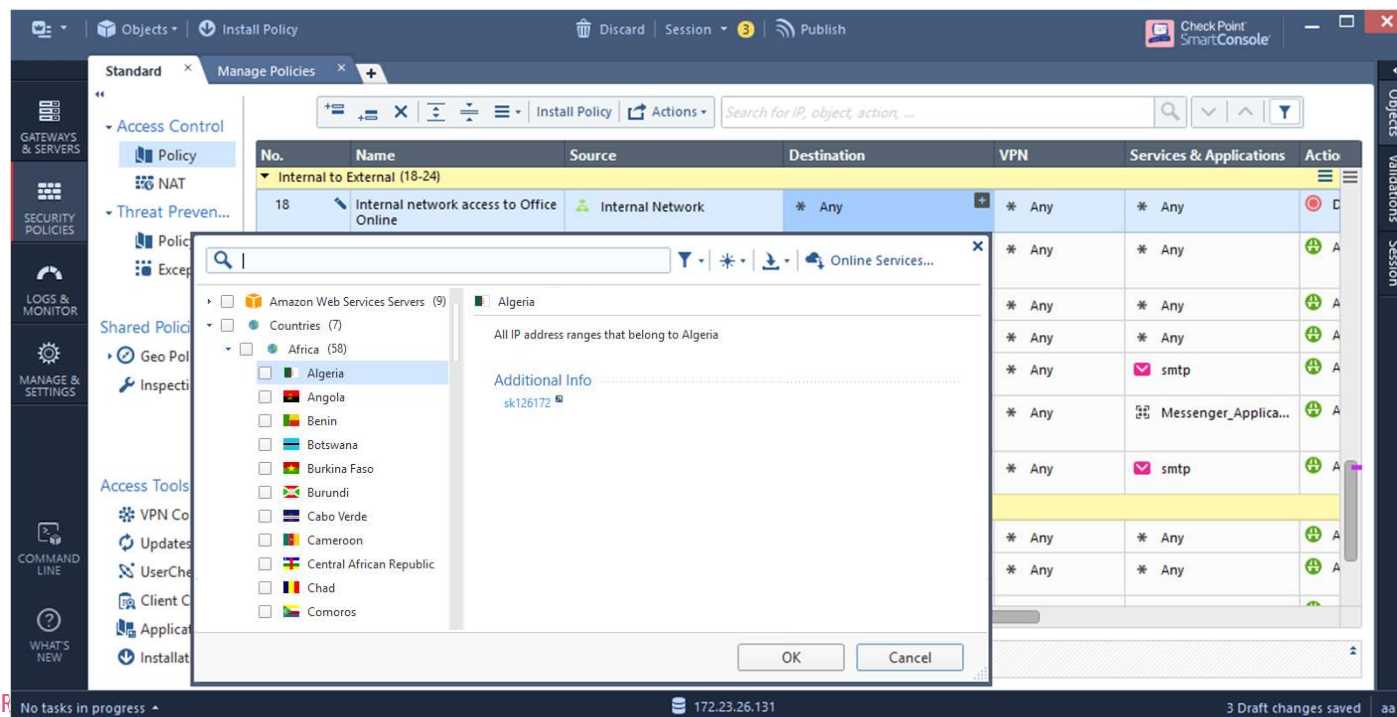
The background shows a policy table with columns for No., Name, Source, Destination, VPN, Services & Applications, and Action. The "Services & Applications" column for the selected rule lists "smtp" and "Messenger\_Applica...".





# Updatable Objects (R80.20)+

- New! Add countries to your Access Control Policy





# Schedule Install Policy (R80.20+ Multi-Domain)

- Schedule to push Policy Installation Presets automatically at a time window.

The screenshot displays the 'New Install Policy Settings' dialog box in the Check Point SmartConsole. The dialog is titled 'Edge schedule' and includes the following sections:

- Installation Targets:** Radio buttons for 'By Gateways' and 'By Policy Packages' (selected). A table lists the selected policy package:

Policy Name	Domain	Targets	Comments
Standard	Domain1	All	

- Scheduling:** 'Enable policy installation scheduling' is checked. 'Install policy at' is set to 12:42. 'One time' is selected with a date of 26-Mar-18. A tooltip indicates: 'Policy installation time will be according to your SmartConsole's local time zone (UTC+02:00) Jerusalem'.
- Install Mode:** 'Install on each selected gateway independently' is selected. A sub-option 'For gateway clusters, if installation on a cluster member fails, do not install on that cluster.' is also checked.

The background shows the SmartConsole interface with a table of policy installation results:

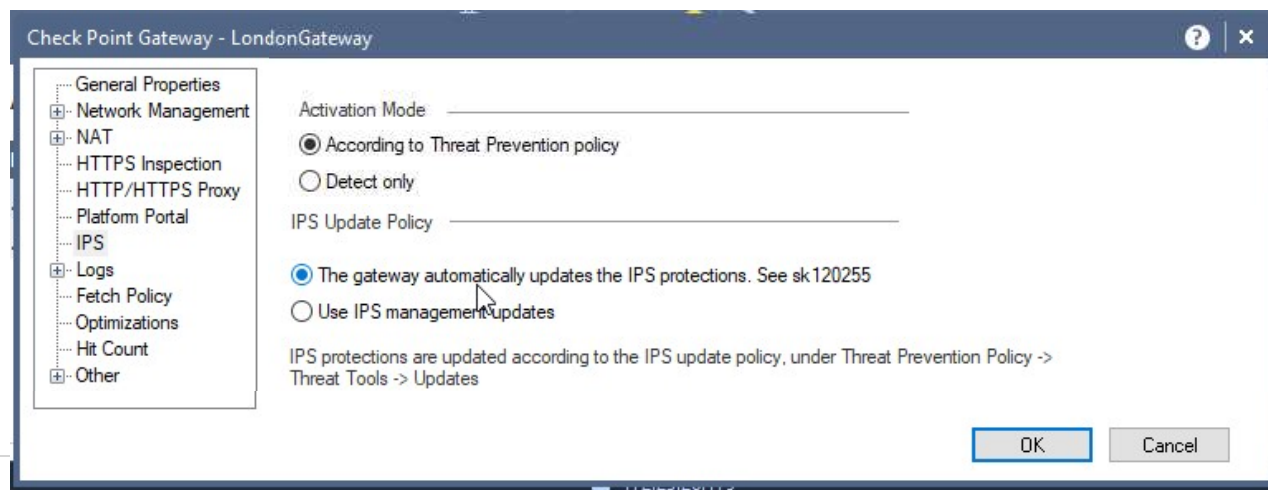
Total Gateways	Total Policies	Comments
	1	
	2	
	0	

# IPS Gateways fetch updates independently (R80.20+)



Check Point  
SOFTWARE TECHNOLOGIES LTD

- Configurable
- Similar to Application Control
- Will be the default option for users who used “scheduled IPS updates with automatic install policy” in R80.10 and upgraded to R80.20
- Action is set according to profile (including Detect-Staging if needed)



WELCOME TO THE FUTURE OF CYBER SECURITY

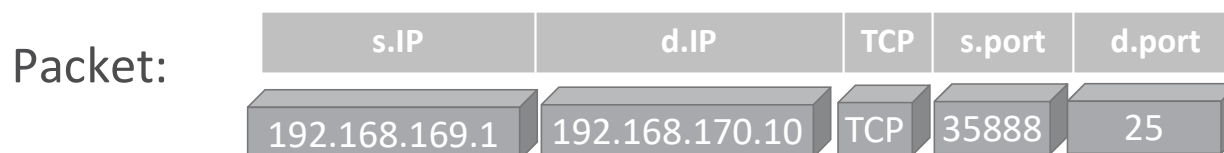
© 2017 Check Point Software Technologies Ltd.



# Policy Rule Base Matching

## Column based matching

- Rule base matching process (there is a lab based on this example, mailserver ip: 192.168.170.10)



No.	Name	Source	Destination	Services & Applications	Action	Track
1					No match possible!	
2					No match possible!	
3					No match possible!	
4					No match possible!	
5	smtp	net_192.168.169.0	mailserver	smtp	Accept	Log
6	Cleanup rule	* Any	* Any	* Any	Drop	Log

- After the first matching round only three rules out of six remained for continued matching





# Introduction to Content Awareness

## File Types, Content Types and Direction used in multiple rules

- Controlling File Types, Content Types and Direction

Name	Source	Destination	Services & Applications	Content	Action	Track
Spreadsheets including credit card num	net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic Spreadsheets_incl_CreditCard...	Accept	Extended Log
Block credit card numbers	net_192.168.169.0	web+mailserver	Web Browsing	Any Direction PCI - Credit Card Numbers	Drop Blocked M...	
Documents	net_192.168.169.0	web+mailserver	Web Browsing	Upload Traffic Document File	Accept	
Spreadsheets	net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic Spreadsheet File	Accept	Extended Log Accounting

Direction  
up-/download/both

Data Type Group  
object

Content Type object

File Type objects

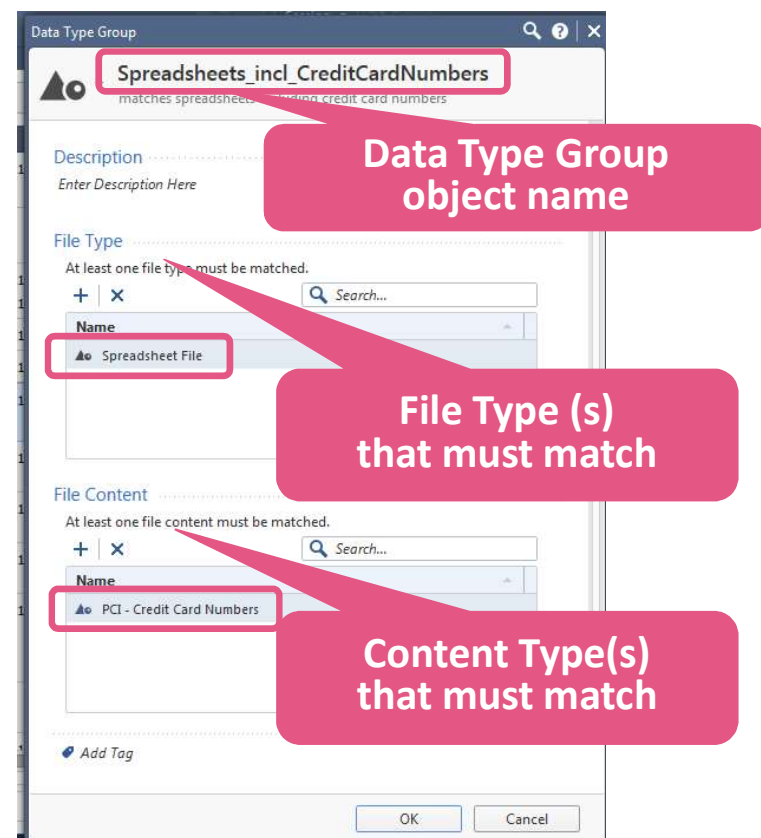
- In the above example extract of a larger rule base you see:
  - The download of spreadsheets that contain credit card numbers is allowed
  - The upload or download of credit card numbers is blocked
  - The upload of documents and the download of spreadsheets is allowed
- The order of the rules is important as the upper most rule will match first



# Introduction to Content Awareness

## Combining File Types and Content Types to a Data Type group object

- When using a **Data Type Group** object both **File Types** and **Content Types** need to match in order for the group object to match
- **Guideline:** you should use Data Type Group objects when the Content can be limited to specific File Types
- Using this group concept improves the efficiency of the Rule Base

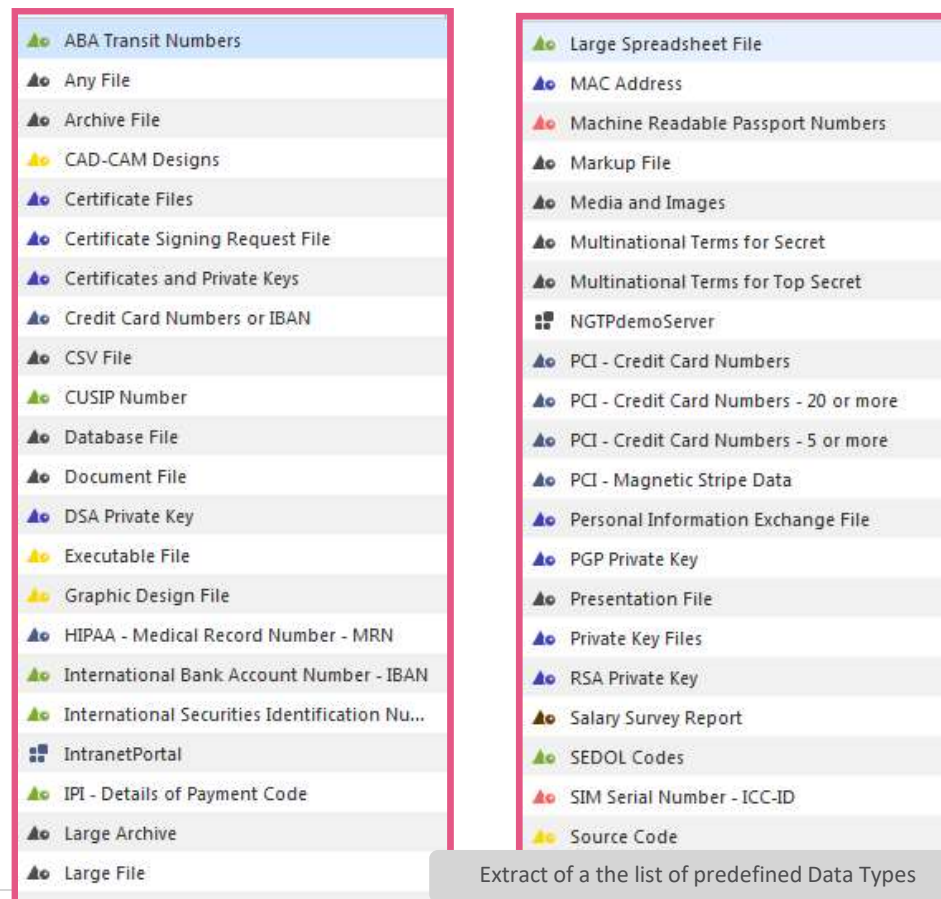
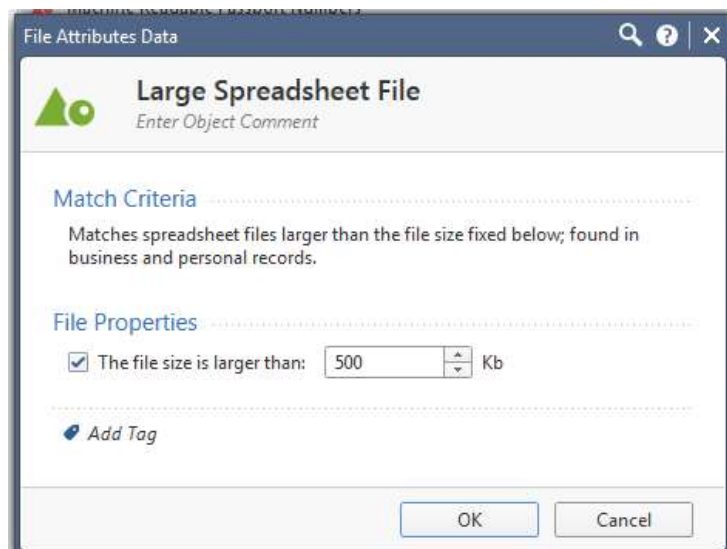




# Introduction to Content Awareness

## Predefined Data Types

- Using the Object Explorer you can browse the predefined Data Types
- You can edit properties



WELCOME TO THE FUTURE OF CYBER SECURITY

# Content Awareness & DLP – When To Use Which

**DLP** has more advanced engines and dedicated rule base but works only for HTTP POST, SMTP and FTP  
**Content Awareness** works for all directions and is integrated into the Unified Rule Base. Support of more advanced engines is on roadmap.

## Rule Base Independence

- DLP have a dedicated multi-match rulebase.
- Content Awareness is part of the first-match unified rulebase.
- Content Awareness can also be used as a dedicated layer

## Content Awareness

- Support VSX and IPV6.
- Part of unified rulebase with Application Control, URLF and other unified rulebase objects.
- Scan both incoming and outgoing traffic.
- Have direction granularity in each rule.

## DLP

- Support advanced Data Types, as templates and fingerprint for data-at-rest.
- Have full mail Quarantine support.
- Has an Exchange Agent to scan internal Exchange communication.



# Connections and Sessions

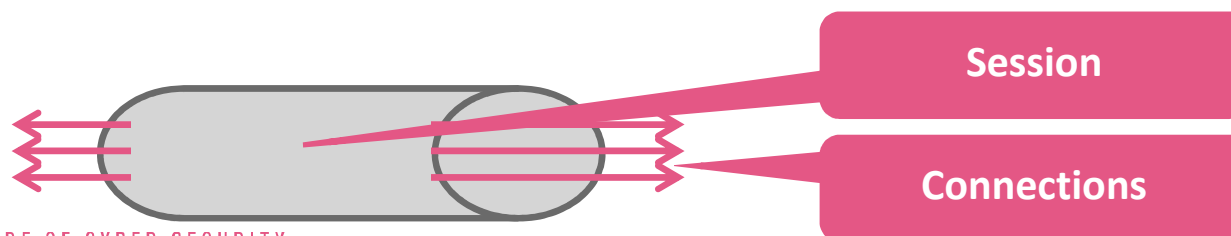
## Multiple connections are forming a session

- **Connection** log message

- Contains information related to the TCP connection or UDP pseudo connection
- Multiple **connections** form a **session**, if they are established within a given time window

- **Session** log message

- Contains information about the application or content
- Is created when APCL, URLF or Content Awareness are enabled or the track options are configured for “Detailed Log” or “Extended Log”







# Web Log Viewer

- [https://\[Management Server IP\]/smartview](https://[Management Server IP]/smartview)
- Improved log viewer with cards, profiles, statistics and filters.

The screenshot displays the Check Point SmartView Web Log Viewer interface. The top navigation bar includes the Check Point SmartView logo, a 'Logs' tab, and an 'Audit Logs' section. A search bar contains the text '(NOT product: "Compliance Blade")'. The main content area is divided into three sections:

- Statistics:** A 'Sessions Timeline' bar chart showing activity from Wednesday 25 to Tuesday 31. Below it, a 'Blade' list shows various security features and their percentages: Firewall (76.56%), IPS (8.89%), HTTPS Inspection (6.67%), Application Control (4.31%), URL Filtering (2.48%), Content Awareness (0.4%), DLP (0.24%), Identity Awareness (0.21%), Mobile Access (0.21%), and VPN (0.15%). An 'Action' section shows 'Accept' at 57.54%.
- Table:** A table of log entries with columns: Time, Blade, Action, Ty..., Interf..., Origin, and Severity. The entries show various actions like 'De...' and 'Pr...' from different blades (IPS, Anti-Bot) and interfaces (eth3, eth0, Remote-4-gw) originating from various IP addresses.
- Card:** A detailed view of a selected log entry. It includes 'Log Info' (Origin: 192.168.72.254, Time: Aug 1, 2018 5:05:09 AM, Blade: IPS, Product Family: Threat, Type: Log) and 'Protection Details' (Severity: Critical, Confidence Level: Medium-High, Attack Name: MSRPC Enforcement Violation, Attack Information: Microsoft Windows RASMAN service memory corruption (MS06-025), Performance Impact: Low, Protection Name: Microsoft Windows RASMAN Service Memory Corruption (MS06-025)).

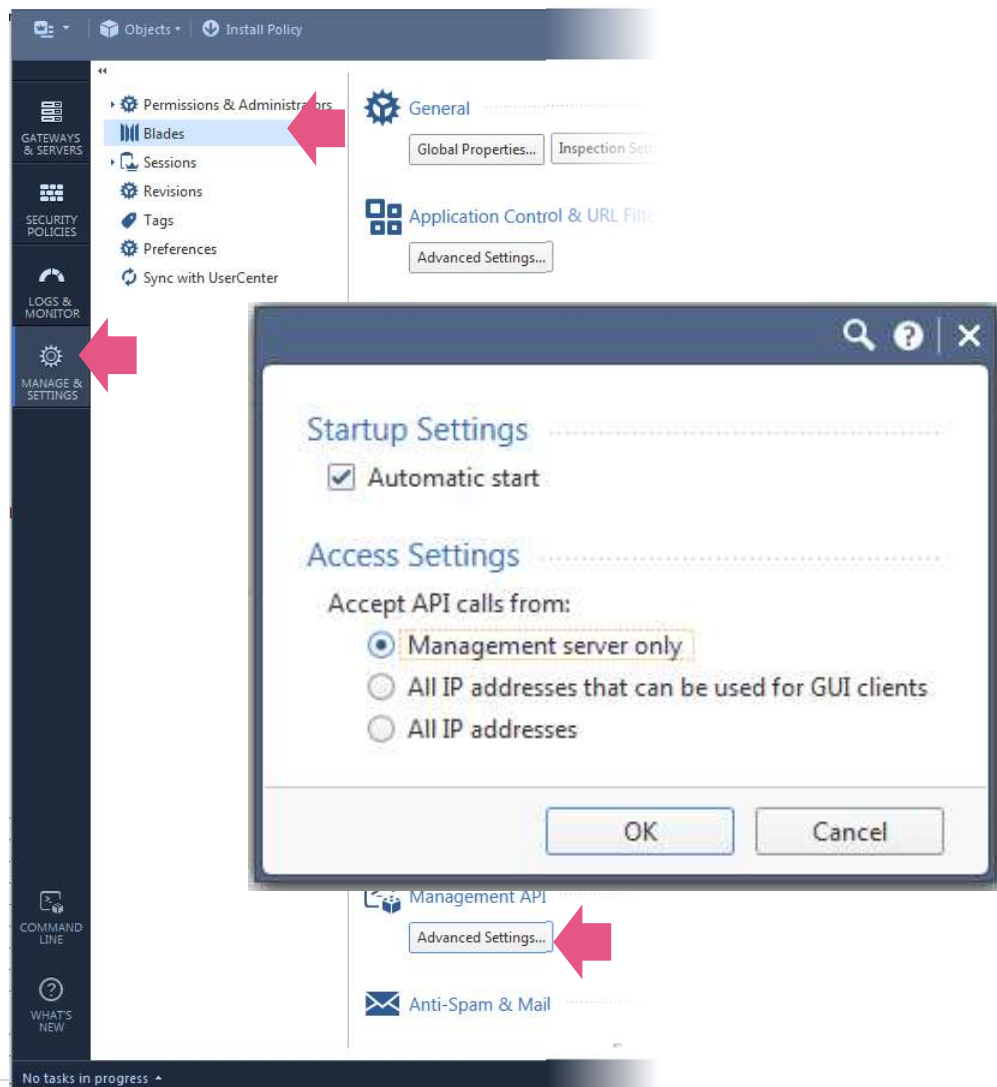
WELCOME TO THE FUTURE OF CYBER SECURITY



## Improvements to SmartView in R80.20

### Closes Gaps Compared to SmartConsole

- Statistics Pane
- More data in the log cards
- Choose Column Profiles
- Right-click log entry to filter the query
- Can select columns exported to Excel
- Auto-refresh views



# Efficient Operation and Automation with APIs

Efficiency



Improve productivity

Cost Savings




Increase Revenue

Agility



Deliver Services Faster

 Search ...

## API Overview:

[Introduction](#)

[SmartConsole CLI](#)

[The mgmt\\_cli tool](#)

[Management CLI in Gaia](#)

[Web Services](#)

▾ [Versioning](#)

[API Versions](#)

[Changelog](#)

API reference:

> [Session Management](#)

# Changelog

## What's New in v1.3

This release, API version 1.3, introduces several new features and several changes.

New features:

- Updatable Object.
- Show objects as ranges:
  - Show rules as ranges of IP addresses and ports instead of Check Point Objects.
  - Show a nested group, group-with-exclusion or service-group as the accumulative ranges of IP addresses and ports.

Show objects as ranges enables you to:

- Describe policies in a non-Check Point-language.
- Run custom validations easily.
- Find rules that are similar to your new rule request.

- EC2 Dashboard
- Events
- Tags
- Reports
- Limits
- INSTANCES
  - Instances**
  - Spot Requests
  - Reserved Instances
  - Dedicated Hosts
- IMAGES
  - AMIs
  - Bundle Tasks
- ELASTIC BLOCK STORE

**Launch Instance** **Connect** **Actions**

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
<input type="checkbox"/>	R8010Mgmt	i-0743f9832d4b6462a	m4.xlarge	us-west-1c	● running	✓ 2/2 checks ...
<input type="checkbox"/>	Ansible-Host	i-0e2a54ba42db1b3...	t2.micro	us-west-1c	● running	✓ 2/2 checks ...



Select an instance above



# Empty Security Management



Simple\_Policy x Manage Policies x +

Recent All

### Recent Policies

Manage policies and layers...

Name	Policies	Gateways
Simple_Policy		All gateways

Search...

← Home List New...

#### Network Objects

- Gateways and Servers 1
- Networks 2
- Hosts 2
- Groups 1
- Address Ranges 4
- Dynamic Objects 6
- Security Zones 4

Objects  
Validations  
Session

Simple\_Policy x Manage Policies x +

```
ubuntu@ip-172-31-18-40: ~/CheckMates_Aug15_Demos/Ansible-AWS-Demo
ubuntu@ip-172-31-18-40:~/CheckMates_Aug15_Demos/Ansible-AWS-Demo$ ansible-playbo
ok
autoprovision.json.txt
CheckMates_AWS_Ansible_AutoScale_Demo.pdf
CheckMates-aws-vpc-create.yml
CheckMates-aws-vpc-delete.yml
CheckMates_DEMO_Delete.yml
CheckMates_DEMO_Deploy.yml
CheckMates-r53-create.yml
CheckMates-r53-delete.yml
CheckMates-R80-Create.yml
CheckMates-R80-Delete.yml
fingerprints.txt
source_aws
vars_ohio.yml
ubuntu@ip-172-31-18-40:~/CheckMates_Aug15_Demos/Ansible-AWS-Demo$ ansible-playbo
ok CheckMates_DEMO_Deploy.yml
```

Search...

← Home List \* New...

**Network Objects**

Gateways and Servers	1
Networks	2
Hosts	2
Groups	1
Address Ranges	4
Dynamic Objects	6
Security Zones	4

- GATEWAYS & SERVERS
- SECURITY POLICIES
- LOGS & MONITOR
- MANAGE & SETTINGS
- COMMAND LINE
- WHAT'S NEW

# The AWS Infrastructure is Started...



Check Point  
TECHNOLOGIES LTD

The screenshot displays the AWS Management Console interface for the us-west-1 region. The main content area shows a table of EC2 instances, all of which are in a 'running' state. The table includes columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, and Public DNS (IPv4). A search bar at the top of the table allows filtering by tags and attributes. The left sidebar contains navigation options for various AWS services, including EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The bottom of the console shows the footer with copyright information and links to Privacy Policy and Terms of Use.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
CheckMates...	i-050d9e7195012912c	t2.micro	us-west-1d	running	2/2 checks ...	None	
R8010Mgmt	i-0743f9832d4b6462a	m4.xlarge	us-west-1c	running	2/2 checks ...	None	
CheckMates...	i-08dea45df5894bd77	t2.micro	us-west-1b	running	2/2 checks ...	None	
CHKP-AutoS...	i-0ace884f7b7275071	c4.large	us-west-1b	running	2/2 checks ...	None	ec2-54-67-14-61.us-west-1b.amazonaws.com
CHKP-GW-E...	i-0baf1e3051736fc9a	c4.large	us-west-1b	running	2/2 checks ...	None	ec2-13-57-126-06.us-west-1b.amazonaws.com
CHKP-AutoS...	i-0c05319296bde4d86	c4.large	us-west-1b	running	2/2 checks ...	None	ec2-54-183-208-22.us-west-1b.amazonaws.com
CheckMates...	i-0d2bce91bfe0dd7e5	t2.micro	us-west-1b	running	2/2 checks ...	None	
Ansible-Host	i-0e2a54ba42db1b3...	t2.micro	us-west-1c	running	2/2 checks ...	None	ec2-54-219-184-24.us-west-1c.amazonaws.com

# Rules and Objects Were Created Too

CheckMates\_Demo\_Policy +

Access Control

- Policy
- NAT

Shared Policies

- Geo Policy
- Inspection Settings

Install Policy Actions

Search for IP, object, action, ...

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	HTTP-8090_aws--i-0e3388b5bfc8333d2-___	net-group_HTTP-8090_aws...	internal-InternalELB-1612...	* Any	HTTP-8090_aws--i-0...	Accept
2	HTTP-8090_aws--i-03c396387824f3554-___	net-group_HTTP-8090_aws...	internal-InternalELB-1612...	* Any	HTTP-8090_aws--i-0...	Accept
AWS vSEC Controller Tagged Rules (3)						
3	Demo WebServers to Any using tags	Application=vSEC_Demo	* Any	* Any	* Any	Accept
AWS Rules (4-8)						
4	AWS external to Any	AWS-External	* Any	* Any	* Any	Accept
5	AWS internal to Any	AWS-Internal	* Any	* Any	* Any	Accept
6	AWS WebServer to DB	AWS-WebServers	AWS-DBServers	* Any	MySQL	Accept
7	AWS-LoadBalancers	* Any	AWS-LoadBalancer1 AWS-LoadBalancer2	* Any	http https	Accept
8	Allow ICMP	* Any	* Any	* Any	icmp-requests	Accept
default drop (9)						
9	Cleanup rule	* Any	* Any	* Any	* Any	Drop

WELCOME TO THE FUTURE OF CYBER SECURITY

# Auto-Provision Gateways



Check Point  
SOFTWARE TECHNOLOGIES LTD

The screenshot displays the Check Point SmartConsole interface for a gateway named R8010Mgmt. The main table lists the gateway with the following details:

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Comments
	R8010Mgmt	52.9.220.175	R80.10		Open server	6%	3 updates available	

The Summary section provides further details for R8010Mgmt:

- IPv4 Address: 52.9.220.175
- OS: Gaia
- Version: R80.10
- License Status: Warnings with 2 blades
- Hardware: Open server
- Management Blades: Network Policy Management, Logging & Status
- CPU Usage: 6%
- Memory Usage: 16%

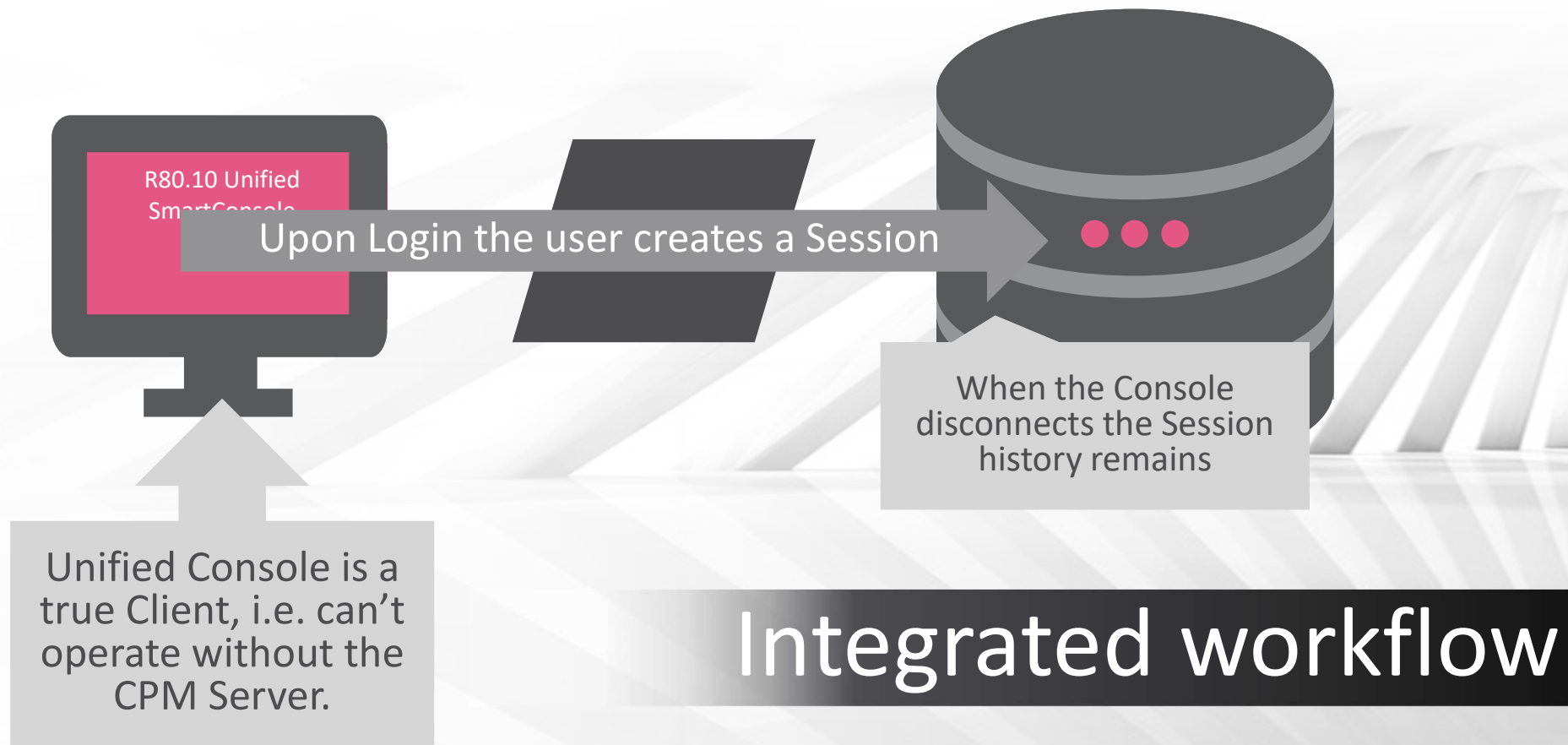
At the bottom of the summary, there are links for "Device & License Information..." and "Activate Blades...". The interface also shows a sidebar with navigation options like "GATEWAYS & SERVERS", "SECURITY POLICIES", "LOGS & MONITOR", and "MANAGE & SETTINGS". The Windows taskbar at the bottom shows the time as 6:53 AM on 10/31/2017.



# API 1.3 Changes

- Updatable Objects
  - Add/delete/show objects
  - Show/update objects repository
- Show Objects as Ranges
  - Show rules as a range of IP addresses and ports (instead of Check Point objects)
  - Enables policy to be described in non-Check Point language
  - Run custom validations, find similar rules to your new rule request
- Changes to the overrides parameter in set-threat-protection API

# Recap Architecture



# Threat Prevention APIs (API 1.2)

- Threat Prevention Indicators (IoC) API

- add threat-indicator
- show threat-indicator
- set threat-indicator
- delete threat-indicator
- show threat-indicator

- Example:

- set threat-indicator name "My\_Indicator" observables.add.1.name "My\_Other\_Observable" observables.add.1.mail-from "someone@somewhere.com" observables.add.1.confidence "low" observables.add.1.severity "high" action "prevent" profile-overrides.remove.1.profile "My\_Profile" ignore-warnings true

- Uses AV/AB Blades on R77.20+ Gateways

- Requires install of Threat Prevention policy for activation

[Protected] Distribution or modification is subject to approval

# Multi-Session Support (Starting R80.20.M1)



Check Point  
SOFTWARE TECHNOLOGIES LTD

The screenshot displays the Check Point SmartConsole interface. At the top, there is a navigation bar with icons for a menu, 'Objects', and 'Install Policy'. On the left, a vertical sidebar contains five main categories: 'GATEWAYS & SERVERS', 'SECURITY POLICIES', 'LOGS & MONITOR', and 'MANAGE & SETTINGS'. The 'MANAGE & SETTINGS' category is selected, and a sub-menu is open showing options like 'Permissions & Administrators', 'Blades', 'Sessions', 'View Sessions', 'Advanced' (highlighted), 'Revisions', 'Tags', 'Preferences', and 'Sync with UserCenter'. The main content area is titled 'Session Settings' and contains two sections: 'Session management' and 'Session name and description'. The 'Session management' section has two radio buttons: 'Each administrator can manage a single SmartConsole session at a time' (unselected) and 'Each administrator can manage multiple SmartConsole sessions at the same time' (selected). The 'Session name and description' section has a checkbox for 'Generate session name' (unselected) and a text input field with a placeholder '+ [administrator name] + @ + [date]'. Below this is another checkbox for 'All sessions must have a description' (unselected).

## Why You Shouldn't Upgrade (Yet)

- You're using a Smart-1 5/10/25/205/210
  - Trade-in hardware for Smart-1 405/410
- Standalone Gateway or Full HA Cluster
  - Gateways need a minimum of 8GB of RAM (more if possible)
  - R80.x Management requires more CPU / RAM
  - Consider separating management to a separate appliance/VM
- Managing Older End of Life Gateways
  - Pre-R75.20, UTM-1 EDGE/Safe@



## Why You Shouldn't Upgrade (Yet)

- Using Windows or IPSO Management
  - Only Gaia supported for R80 and above
- Traditional Mode VPNs
  - Simplified Mode VPNs added in NG FP3
  - Migrate to Simplified Mode VPNs prior to upgrade

## If You're Using Specific Features... (sk117237)

- Featured in R80.20:
  - Endpoint + Network Security Management on same system
  - SmartProvisioning and SmartLSM
  - Syslog From Gateway
    - Added in R80.20 but consider using Log Exporter instead (see sk122323)
  - Global VPN Communities
- SmartWorkflow
  - Many features in R80.20
    - Multiple sessions (which can be managed), Layers history, Revert Policy, Ticket #s
  - Additional feature to be integrated in future releases

## A Note About R80.20 Release Trains

### Management Release (Mx)

- Frequent releases (Every few months)
- For Security Management Products
- Jumbo Hotfixes only for current Mx release
- Can manage all GA gateways available at release time
  - Will require updating to newer Mx release when R80.20 GA ships

### General Availability

- Less frequent releases
- For Gateways and Management
- Regular Jumbo Hotfix Releases with major updates in next major release
- Can manage R80.20 gateways and earlier

# The

## Plan The Upgrade What do I

- Support R75.4
- Operate on GAIA or RHEL
- Hardware requirements  
For more information  
For any questions

## Pre-Upgrade

- Assures your system is ready for the upgrade
  - Tip! Verify system health
- Use R80 Upgrade Assistant
- You can do a manual upgrade



## Security Management Server Upgrade upgrading with Import/Export

## Security Management Server Upgrade upgrading with Export/Import

```
[Expert@smcr7730:0]#  
You are required to stop all Check Point services (cpstop) before  
or execute 'cpstop'.  
Do you want to continue? (y/n) [n]?  
Copying required files...  
Compressing files...  
The operation completed successfully.  
Location of archive: /var/tmp/upgrade_tools/
```

```
[Expert@smcr80:0]#  
[Expert@smcr80:0]# cd $FWDIR/bin/upgrade_tools  
[Expert@smcr80:0]# ./migrate import /migrate_to_r80/r7730_to_r80_export.tgz  
The import operation will eventually stop all Check Point services (cpstop).  
Do you want to continue? (y/n) [n]?  
Extracting the database...
```

Run migrate import

```
# /migrate_tools
```

```
# cd $FWDIR/bin/upgrade_tools  
# migrate import /migrate_to_r80/r77_to_r80.10_export.tgz
```

New HTML interface  
better readability

Management



# Management Servers

## *supported migrate & upgrade methods table*

Type	From	To: R80.20
SMS MDSM <sup>1</sup> LS <sup>2</sup> SE	R7x.xx R80.x	<ul style="list-style-type: none"><li>In-place with CPUSE</li><li>Export/Import (“Advanced”)<ul style="list-style-type: none"><li><sup>1</sup>Index the logs by following <a href="#">“Importing Offline Log Files”</a></li><li><sup>2</sup>Upgrade the events database following <a href="#">sk110173</a></li></ul></li></ul>
MDSM	R7x.xx	<ul style="list-style-type: none"><li><b>Gradual</b></li></ul>

SMS - Security Management Server  
MDSM - Multi-Domain Security Management  
LS – Log Server  
SE – SmartEvent





# Hardware Requirements

## Supported Smart-1 Appliance

- Smart-1 50, 150, 225, 405, 410, 3050, 3150
  - Consider adding more RAM
- Smart-1 25, 205, 210 supported with limitations
  - Cannot run Management + SmartEvent

## Open Server / VM

- Security Management: 2 Cores, 6GB RAM
  - Recommendation is at least 4 cores and 16GB of RAM, more if available
- Multi-Domain: 8 Cores, 32GB RAM
  - The more domains you have, the more cores and RAM you should have



## Migration Tools

- Download appropriate tool based on:
  - Source Management OS
  - Target upgrade version
  
- Links for upgrading to R80.10 from:
  - [Gaia \(pre-R80\)](#)
  - [SecurePlatform/Linux](#)
  - [Windows](#)
  - [Solaris](#)

# MIGRATE EXPORT AND IMPORT

VMware bunsen admin Sign Out

Search

View mode: Advanced

Overview

Network Management

- Network Interfaces
- ARP
- DHCP Server
- Hosts and DNS
- IPv4 Static Routes
- NetFlow Export

System Management

- Time
- Cloning Group
- SNMP
- Job Scheduler
- Mail Notification
- Proxy
- Messages
- Display Format
- Session
- Core Dump
- System Configuration
- System Logging
- Network Access
- Certificate Authority
- Host Access

Advanced Routing

- DHCP Relay

Manage Software Blades using SmartConsole [Download Now!](#)

**System Overview**

**Check Point Security Management | R77.30**

Kernel: 2.6.18-92cpx86\_64  
Edition: 64-bit  
Build Number: 3  
System Uptime: 1 day 13 hours 39 minutes

Platform: VMware

**Blades**

- Firewall

**Network Configuration**

Name	IPv4 Address	IPv6 Address	Lin
eth0	10.3.2.230	-	
lo	127.0.0.1	-	

phoneboy — admin@bunsen:~ — ssh admin@10.3.2.230 — 80x24

```
[[Expert@bunsen:0]# migrate/migrate export bunsen7730.tgz

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

Do you want to continue? (y/n) [n]?
```

# Migrate Export



Check Point  
SOFTWARE TECHNOLOGIES LTD

```
phoneboy — admin@bunsen:~ — ssh admin@10.3.2.230 — 80x24
[[Expert@bunsen:0]# migrate/migrate export bunsen7730.tgz ]

You are required to close all clients to Security Management Server
or execute 'cpstop' before the Export operation begins.

[Do you want to continue? (y/n) [n]? y ]

Copying required files...
Compressing files...

The operation completed successfully.

Location of archive with exported database: /home/admin/bunsen7730.tgz

[Expert@bunsen:0]#
```



# Migrate Import



```
phoneboy — admin@eightyten:~ — ssh admin@10.3.2.220 — 80x24
[[Expert@eightyten:0]# migrate/migrate import bunsen7730.tgz
The import operation will eventually stop all Check Point services (cpstop).
Do you want to continue? (y/n) [n]
```



# Migrate Import Continues



```
phoneboy — admin@eightytyn:~ — ssh admin@10.3.2.220 — 80x24
Management Portal: CPHTTPD failed to stop
Stop Search Infrastructure...
Stopping RFL ...
cpwd_admin:
successful Detach operation
Stopping Solr ...
cpwd_admin:
successful Detach operation
Stop SmartView ...
Stopping SmartView ...
cpwd_admin:
successful Detach operation
Stop Log Indexer...
cpwd_admin:
Process INDEXER (pid=15005) stopped with command "kill 15005". Exit code 0.
Stop SmartLog Server...
cpwd_admin:
Process SMARTLOG_SERVER terminated
dbsync is not running
evstop: Stopping product - SmartEvent Server
evstop: Stopping product - SmartEvent Correlation Unit
Check Point SmartEvent Correlation Unit is not running
SmartView Monitor: Management stopped
```

WELCOME TO THE WORLD OF CHECK POINT

## Migrate Import Still Going...



Check Point  
SOFTWARE TECHNOLOGIES LTD

```
phoneboy — admin@eightyten:~ — ssh admin@10.3.2.220 — 80x24
Stopping SmartView ...
cpwd_admin:
successful Detach operation
Stop Log Indexer...
cpwd_admin:
Process INDEXER (pid=15005) stopped with command "kill 15005". Exit code 0.
Stop SmartLog Server...
cpwd_admin:
Process SMARTLOG_SERVER terminated
dbsync is not running
evstop: Stopping product - SmartEvent Server
evstop: Stopping product - SmartEvent Correlation Unit
Check Point SmartEvent Correlation Unit is not running
SmartView Monitor: Management stopped
FireWall-1: cpm stopped
FireWall-1: fwm stopped
VPN-1/FW-1 stopped
Stopping Critical Alerts Sensor
SVN Foundation: cpd stopped
Stopping cpview
SVN Foundation: cpWatchDog stopped
SVN Foundation stopped
Importing files...
```

## And... It's Done!



```
phoneboy — admin@eightytyn:~ — ssh admin@10.3.2.220 — 80x24
successful Detach operation
Stop Log Indexer...
cpwd_admin:
Process INDEXER (pid=15005) stopped with command "kill 15005". Exit code 0.
Stop SmartLog Server...
cpwd_admin:
Process SMARTLOG_SERVER terminated
dbsync is not running
evstop: Stopping product - SmartEvent Server
evstop: Stopping product - SmartEvent Correlation Unit
Check Point SmartEvent Correlation Unit is not running
SmartView Monitor: Management stopped
FireWall-1: cpm stopped
FireWall-1: fwm stopped
VPN-1/FW-1 stopped
Stopping Critical Alerts Sensor
SVN Foundation: cpd stopped
Stopping cpviewd
SVN Foundation: cpWatchDog stopped
SVN Foundation stopped
Importing files...

The import operation completed successfully.
Do you wish to start Check Point services? (y/n) [y]? 
```

# Remember To Get A New License!



The image shows a terminal window with a dark background and white text. The terminal output includes the following lines:

```
cpwd_admin:
Process INDEXER (pid=4368) stopped with command "kill 4368". Exit code 0.
Stop SmartLog Server...
cpwd_admin:
Process SMARTLOG_SERVER terminated
dbsync is not running
evstop: Stopping produ
evstop: Stopping produ
Check Point SmartEvent
SmartView Monitor: Mar
FireWall-1: cpm stoppe
FireWall-1: fwm stoppe
VPN-1/FW-1 stopped
Stopping Critical Alert
SVN Foundation: cpd st
Stopping cpviewd
SVN Foundation: cpWatc
SVN Foundation stopped
Importing files...

The import operation completed successfully.
Do you wish to start Check Point services? (y/n) [y]? y

[Expert@eightyten:0]#
```

Overlaid on the terminal is a dialog box with a dark blue header and a light gray body. The header contains a yellow crown icon, the text "SmartConsole", and "R80.10". The body contains a red circle with a white 'X' icon and the text "The license on the Security Management Server has expired. Add a new license and try again." At the bottom right of the dialog is a "BACK" button. The Check Point logo is visible in the bottom left corner of the dialog.



**And now...**  
**IT'S UPGRADE TIME!**

# R77.30 Overview



Check Point  
SOFTWARE TECHNOLOGIES LTD

World's most proven Firewall solution, featuring the most adaptive and intelligent inspection technology

### My Organization

2 Security Gateways

	IP Address	Version	Policy Package	Instal
animal	10.3.2.222	R77.30	AnimalPolicy	10/27
ArrSixFive	10.3.2.165	NGX R65	NGX	10/27

WE

# R77.30 Firewall Policy



Check Point  
SOFTWARE TECHNOLOGIES LTD

## Policy



Search for IP, object, action, ...

Query Syntax



No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	0	TrafficToBlockedIPs	net-internal	block-ips	Any Traffic	Any	accept	Log	Policy Targets	Any
2	185K	InternalOut	net-internal	Any	Any Traffic	Any	accept	None	Policy Targets	Any
3	32K	DMZOut	net-dmz	net-internal	Any Traffic	Any	accept	None	Policy Targets	Any
4	0	DrTeethMgmt	drteeth-int	bunsen	Any Traffic	TCP FW1_ica_pull TCP FW1_log TCP CPD TCP FW1_ica_servic UDP syslog	accept	None	Policy Targets	Any
5	0	InboundGWMgmt	Any	animal	Any Traffic	TCP ssh_version_2 TCP https-4434	accept	Log	Policy Targets	Any
6	0	DMZ-Syslog	edgew wrt54gs	bunsen	Any Traffic	UDP syslog	accept	None	Policy Targets	Any
7	0	InboundNarfSSH	Any	narf	Any Traffic	TCP ssh-54269	accept	Log	Policy Targets	Any
8	0	InboundNarfBT	Any	narf	Any Traffic	narf-bt-fwd	accept	None	Policy Targets	Any
9	0	InboundXbox	Any	xbox360	Any Traffic	xbox	accept	None	Policy Targets	Any
10	7K	DHCP	Any	broadcast	Any Traffic	dhcp-request	accept	None	Policy Targets	Any
11	557	Cleanup	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any

# R77.30 App Control



Check Point  
SOFTWARE TECHNOLOGIES LTD

Application & URL Filtering | Data Loss Prevention | IPS | Threat Prevention | Anti-Spam & Mail | Mobile Access | IPsec VPN | Compliance | QoS | More

Policy Type to Search Hit Count

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time	Co
1	0	Block Child Abuse sites	Any	Internet	Child Abuse	Block	Log	All	Any	
2	0		minime-3ds minime-gtab minime-gtab-dmz	Internet	DNS Protocol DHCP Protocol	Allow	None	All	Any	
3	0		minime-3ds minime-gtab minime-gtab-dmz	Internet	Any Recognized	Block	Log	All	Bedtme Bedtime_WE	
4	0		adult-machines	Internet	Any Recognized	Allow	Extended Log	All	Any	
5	0		Any	Internet	Google Talk pro... Skype Amazon S3 cizgifilmerizle Google Talk talk.google.com youtube-mp3.org	Allow	Extended Log	All	Any	
6	0		zoe fozzy fozzyw minime-gtab minime-gtab-dmz	Internet	Facebook	Allow	Log	All	Any	
7	0		zoe	Internet	YouTube-safety ...	Allow	Extended Log	All	Any	

# R77.30 IPS



Check Point  
SOFTWARE TECHNOLOGIES LTD

The screenshot shows the Check Point SmartDashboard interface for the R77.30 IPS. The main navigation bar includes Firewall, Application & URL Filtering, Data Loss Prevention, IPS (selected), Threat Prevention, Anti-Spam & Mail, Mobile Access, and IPsec VPN. The left sidebar contains a tree view with categories like Overview, Gateways, Profiles, Protections, Geo Protection, Network Exceptions, Download Updates, Follow Up, Additional Settings, Track Logs, and Analyze & Report. Below this is a 'Network Objects' section with a tree view including Check Point, animal, arrsixfive, bunsen, Nodes, Networks, Groups, Address Ranges, and Dynamic Objects.

### Overview

IPS provides protection from network, application and web attacks.

#### IPS in My Organization

1 Security Gateway is enforcing IPS  
3 profiles are configured

Profile	IPS Mode	Activation	Gateways
Default_Protection	Prevent	IPS Poli...	0 GWs
HomeProfile	Prevent	IPS Poli...	1 GWs
Recommended_Pr...	Prevent	IPS Poli...	0 GWs

#### Security Status

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

Legend:   
■ Detected (Yellow)   
■ Prevented (Blue)   
■ Average in My Organization (Green)

Graph: No recorded attacks

# R77.30 IPS Profile



Profile Properties - HomeProfile

General  
IPS Policy  
Updates Policy  
Network Exceptions  
Troubleshooting

### IPS Policy

Protections to Activate

Automatically activate protections of the following types:

- Client Protections
- Server Protections

Protections to Deactivate

- Do not activate protections with severity Low or below
- Do not activate protections with confidence-level Medium-low or below
- Do not activate protections with performance impact High or above
- Do not activate Protocol Anomalies
- Do not activate protections in the following categories Configure... (0 Selected)

Notices

- Application Control enforcements will not be activated automatically. You can activate these controls manually.





The screenshot shows the Gaia web interface in a browser window. The address bar displays a URL starting with https://10.3.2.230. The interface includes a navigation menu on the left with categories like Network Management and System Management. The main content area is divided into several sections:

- System Overview:** Displays system information for 'Check Point Security Management | R77.30'.
  - Kernel: 2.6.18-92cpx86\_64
  - Edition: [64-bit](#)
  - Build Number: 3
  - System Uptime: 4 days 58 minutes
  - Platform: VMware
- Network Configuration:** A table showing network interfaces and their status.
 

Name	IPv4 Address	IPv6 Address	Link Status
eth0	10.3.2.230	-	Up
lo	127.0.0.1	-	Up
- Blades:** A vertical list of system components including Firewall, IPS, IPSec VPN, URL Filtering, Anti-Spam and Mail, and Mobile Access.

# Verifier



Check Point  
SOFTWARE TECHNOLOGIES LTD

The screenshot shows the Gaia web interface for a VMware bunsen environment. The browser address bar shows a URL starting with https://10.3.2.230/. The interface includes a navigation menu on the left with categories like 'Static and Dynamic Routes' and 'User Management'. The main content area is titled 'Upgrades (CPUSE) Status and Actions' and contains a table of upgrade items:

Category	Item Name	Status	Date
Hotfixes	Jumbo Hotfix Accumulator General Availability for R77.30 Take 216	Installed, self-test passed	16-Feb-2017
Minor Versions (HFAs)	Check Point CPinfo build 176 for R77, R77.10, R77.20, R77.30	Downloaded Successfully	22-Mar-2017
Major Versions	R80.10 Fresh Install and Upgrade from R7X	Available for Download	17-May-2017

A context menu is open over the 'R80.10 Fresh Install and Upgrade from R7X' item, showing two options: 'Verifier' and 'Download'.

WELCOME TO THE FUTURE OF CYBER SECURITY

©2017 Check Point Software Technologies Ltd.

[Protected] Distribution or modification is subject to approval

# Verifier Result



The screenshot shows the Check Point GUI for a VMware environment. The main window displays the 'Upgrades (CPUSE) > Status and Actions' page for 'Check Point Upgrade Service Engine (CPUSE) | R77.30 take'. A dialog box titled 'Verifier results' is open, showing a green checkmark and the following text:

**Verifier results**  
**Package: R80.10 Fresh Install and Upgrade from R7X**  
Clean Install:  
Installation is allowed.  
Upgrade:  
Upgrade is allowed. Before upgrading, please note the following log:  
`/var/log/DA_puv_Check_Point_R80.10_T421_Fresh_Install_and_Upgrade_from_R7X_METADATA.tgz.log`

The background page shows a table of 'Major Versions' with one item: 'R80.10 Fresh Install and Upgrade from R7X' with a status of 'Downloaded Successfully' and a date of '17-May-2017'. The left sidebar contains navigation options like 'Policy Based Routing', 'Routing Monitor', 'User Management', 'High Availability', and 'Maintenance'.



## Verifier: Obsolete Check Point Objects

\* Description: Some legacy Check Point network objects are obsolete in the current Security Management Server version. These objects are no longer supported.

Please upgrade or remove the following Check Point network objects before proceeding with an upgrade procedure. Leaving those unsupported objects in the database may cause error messages and policy installation problems:

ArrSixFive (Version: NGX R65, Minimal supported version: R75.20)



## Service Name Conflicts with New Default Objects

\* Description: Check Point has added 36 protocols and 33 services to the default database. A number of these new default objects conflict with existing user objects.

To resolve the issue, rename these objects:

Services:

RDP

snmp-trap

Comment: if you choose to leave objects as is, during upgrade process "\_" will be added as suffix to each object name which conflicts default database.



## IPS Protections by Type Changes in R80

\* Description: Deactivating IPS protections by type (Client/Server) will be supported for pre R80 gateways only.

When deactivating Client or Server protections, it will not be supported for R80.10 gateway.

We recommend you to move to the new tag based activation for Client/Server protections.

Profiles name:

HomeProfile



# Deprecated Application Control Categories in R80



\* Description: Rulebase contains Application Control categories or group of categories that were deprecated.

For deprecated categories list and recommended substitutes please refer to sk106783.

The following categories are deprecated:

The category: "Google Talk protocol" in rule Num. 5 of "AnimalPolicy" policy is deprecated

The category: "Oscar protocol" in rule Num. 9 of "AnimalPolicy" policy is deprecated

The category: "Torrent Trackers" in rule Num. 9 of "AnimalPolicy" policy is deprecated, it will be replaced with "P2P File Sharing"

# LTE Services



Check Point  
SOFTWARE TECHNOLOGIES LTD

```
* Description: Database contains LTE services that are not  
yet supported in R80.10
```

```
These LTE services will be deleted during the upgrade to  
R80.10:
```

```
Unsupported LTE services are:
```

```
gtp_v2_default
```

```
gtp_mm_v2_default
```

```
gtp_additional_v2_default
```

# Now for the Upgrade



Check Point

← → ↻ **Not Secure** | [https://10.3.2.230/\\_c7a4d09bbdcd824fc056937da81012fc/cgi-bin/home.tcl](https://10.3.2.230/_c7a4d09bbdcd824fc056937da81012fc/cgi-bin/home.tcl) ☆

VMware **bunsen** admin Sign Out Search

Upgrades (CPUSE) ▶ Status and Actions Configure

View mode: **Advanced** ▼

- Create Multiple Profiles
- RIP
- OSPF
- Route Aggregation
- Inbound Route Filters
- Route Redistribution
- Routing Options
- Router Discovery
- Policy Based Routing
- Routing Monitor
- User Management
  - Change My Password
  - Users
  - Roles
  - Password Policy
  - Authentication Servers
  - System Groups
  - GUI Clients
- High Availability
  - VRRP
  - Advanced VRRP
- Maintenance
  - Licenses

Check Point Upgrade Service Engine (CPUSE) | R77.30 take 3 [Hotfixes](#) Last updated on: Sat Aug 26 22:11 2017 Check For Updates Import Package Add Hotfixes From The Cloud

Clean Install Upgrade More ▼ Showing All packages ?

Package	Status	Release date
Hotfixes	✔ Aligned with the latest version	
Minor Versions (HFAs)		2 items
Major Versions		1 item
R80.10 Fresh Install and Upgrade from R7X	Downloaded Successfully	17-May-2017

- Clean Install
- Verifier
- Upgrade
- Export Package
- Delete From Disk

**Package Details**

**File Name:** Check\_Point\_R80.10\_T421\_Fresh\_Install\_and\_Upgrade\_from\_R7X.

**Image Size:** 2739.4 MB

**Package Type:** Major Version

**Release Date:** 17-May-2017

**Status:**  
The package downloaded successfully

**Important Messages:**

- While the package is installing, the cpstop and cpstart commands are run
- After the package is installed, the gateway reboots

**Description:**  
R80.10 creates a breakthrough in Check Point Security Gateway, matching the R80 security management innovations. R80.10 is part of Check Point Infinity, a consolidated cyber security architecture that spans networks, cloud, and mobile. It provides the highest level of threat prevention against both known and unknown targeted attacks to keep you protected now and in the future.

**Hotfixes** are Check Point's lightest software updates, for security fixes and feature improvement.

Hotfixes are released after issue fixes are developed and tested. For more information, refer to [sk95746](#)

# Are You Sure?



Check Point  
SOFTWARE TECHNOLOGIES LTD

The screenshot shows the Check Point Upgrade Service Engine (CPUSE) interface. The main window displays a table of packages with columns for Package, Status, and Release date. The table shows a package named "R80.10 Fresh Install and Upgrade from R7X" with a status of "Downloaded Successfully" and a release date of "17-May-2017". A warning dialog box titled "Image Upgrade" is overlaid on the interface, containing a yellow warning icon and the text: "After this upgrade, there will be an automatic reboot. (Existing OS settings and the Check Point Database are preserved.)". The dialog has "OK" and "Cancel" buttons.

Package	Status	Release date
Hotfixes	Aligned with the latest version	
Minor Versions (HFAs)		2 items
Major Versions		1 item
R80.10 Fresh Install and Upgrade from R7X	Downloaded Successfully	17-May-2017

# During the Upgrade...



Check Point  
SOFTWARE TECHNOLOGIES LTD

Log in - VMware ESXi x Gaia x

← → ↻ Not secure | https://10.3.2.230/\_93a7e1113e4214400cacb90fa586dd0e/cgi-bin/home.tcl

VMware  
bunsen

View mode: Advanced

- Routing Monitor
- User Management
  - Change My Password
  - Users
  - Roles
  - Password Policy
  - Authentication Servers
  - System Groups
  - GUI Clients
- High Availability
  - VRRP
  - Advanced VRRP
- Maintenance
  - License Status
  - Snapshot Management
  - System Backup
  - Download SmartConsole
  - Shut Down
- Upgrades (CPUSE)
  - Status and Actions

Upgrades (CPUSE) ▶ Status and Actions

Check Point Upgrade Service Engine (CPUSE) | R80.10 Hotfixes updated on: Wed Oct 18 4:53 2017

Install Update | More | Showing Recommended packages

Package	Status	Release date
Hotfixes	✓ Aligned with the latest version	
Minor Versions (HFAs)	✓ Aligned with the latest version	
Major Versions	✓ Aligned with the latest version	
R80.10 Fresh Install and Upgrade from R7X	Importing Database: 45 %	17-May-2017

WELCOME TO THE FUTURE OF CYBER SECURITY

©2017 Check Point Software Technologies Ltd.

[Protected] Distribution or modification is subject to approval

# THE FINISHED PRODUCT



# Firewall Policy Layer



Check Point  
SOFTWARE TECHNOLOGIES LTD

AnimalPolicy x Manage Policies x +

Access Control

- Policy
  - Security
  - Application
  - NAT
  - Desktop
  - QoS
- Threat Prevention
  - Policy
  - Exceptions

Shared Policies

- Geo Policy
- Inspection Settings

Access Tools

- VPN Communities
- Updates
- UserCheck
- Client Certificates

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	TrafficToBlockedIPs	net-internal	block-ips	* Any	* Any	Accept	Log
2	InternalOut	net-internal	* Any	* Any	* Any	Accept	None
3	DMZOut	net-dmz	<b>Negated</b> net-internal	* Any	* Any	Accept	None
4	DrTeethMgmt	drteeth-int	bunsen	* Any	FW1_ica_pull FW1_log CPD FW1_ica_services syslog	Accept	None
5	InboundGWMgmt	* Any	animal	* Any	ssh_version_2 https-4434	Accept	Log
6	DMZ-Syslog	edgew wrt54gs	bunsen	* Any	syslog	Accept	None
7	InboundNarfSSH	* Any	narf	* Any	ssh-54269	Accept	Log
8	InboundNarfBT	* Any	narf	* Any	narf-bt-fwd	Accept	None
9	InboundXbox	* Any	xbox360	* Any	xbox	Accept	None
10	DHCP	* Any	broadcast	* Any	dhcp-request_	Accept	None
11	Cleanup	* Any	* Any	* Any	* Any	Drop	Log

WELCOME TO THE FUTURE OF CYBER SECURITY



AnimalPolicy x Manage Policies x +

Access Control

- Policy
  - Security
  - Application
- NAT
- Desktop
- QoS

Threat Prevention

- Policy
- Exceptions

Shared Policies

- Geo Policy
- Inspection Settings

Access Tools

- VPN Communities
- Updates
- UserCheck
- Client Certificates
- Application Mibi

Install Policy Actions Search for IP, object, action, ...

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Block Child Abuse sites	* Any	Internet	* Any	Child Abuse	Drop	Log Acco
2		minime-3ds minime-gtab minime-gtab-dmz	Internet	* Any	domain-udp-Protoc... domain-tcp-Protoc... dhcp-Protocol-Sign...	Accept	None
3		minime-3ds minime-gtab minime-gtab-dmz	Internet	* Any	* Any	Drop	Detailed Acco
4		adult-machines	Internet	* Any	* Any	Accept	Extended Acco
5		* Any	Internet	* Any	Skype Amazon S3 cizgifilmerizle Google Talk talk.google.com youtube-mp3.org Google Talk protocol	Accept	Extended Acco
6		zoe fozy fozyw minime-gtab	Internet	* Any	Facebook	Accept	Log Acco



Access Control

- Policy
  - Security
  - Application
  - NAT
  - Desktop
  - QoS
- Threat Prevention
  - Policy
    - IPS
    - Threat Prevention
  - Exceptions

Shared Policies

- Geo Policy
- Inspection Settings

Access Tools

- VPN Communities
- Updates
- UserCheck
- Client Certificates
- Application Wiki

Install Policy Actions

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	TrafficToBlockedIPs	net-internal	block-ips	* Any	* Any	Accept
2	InternalOut	net-internal	* Any	* Any	* Any	Inter
2.1	Block Child Abuse sites	* Any	Internet	* Any	Child Abuse	Drop
2.2		jaden-gtab jaden-gtab-dmz jaden-3ds	Internet	* Any	domain-udp-Protoc... domain-tcp-Protoc... dhcp-Protocol-Sign...	Accept
2.3		jaden-gtab jaden-gtab-dmz jaden-3ds	Internet	* Any	* Any	Drop
2.4		adult-machines	Internet	* Any	* Any	Accept
2.5		* Any	Internet	* Any	Skype Amazon S3 cizgifilmerize Google Talk talk.google.com youtube-mp3.org Google Talk protocol	Accept
2.6		zoe	Internet	* Any	Facebook	Accept



AnimalPolicy +

Access Control

- Policy
  - Security
  - Application
- NAT
- Desktop
- QoS

Threat Prevention

- Policy
  - IPS
  - Threat Prevention
- Exceptions

Shared Policies

- Geo Policy
- Inspection Settings

Install Policy Actions Search for IP, object, action, ...

No.	Name	Source	Destination	VPN	Services & Applications
2.10		* Any	Internet	* Any	ssl_v3-Protocol-Sig...
2.11		* Any	Internet	* Any	* Any
2.12		* Any	Internet	* Any	Unknown Traffic Unknown Traffic
Missing cleanup rule - Unmatched traffic will be dropped and not logged.					
3	DMZOut	net-dmz	<del>net-internal</del> net-internal net-ext	*	
4	DrTeethMgmt	drteeth-int	bunsen	* Any	FW1_ica_pull FW1_log CPD FW1_ica_services syslog

Add Cleanup Rule  
Learn More...



Access Control

- Policy
  - Security
  - Application
  - NAT
  - Desktop
  - QoS
- Threat Prevention
  - Policy
  - Exceptions

Shared Policies

- Geo Policy
- Inspection Settings

Access Tools

- VPN Communities
- Updates
- UserCheck
- Client Certificates
- Application MGR

Install Policy Actions

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	TrafficToBlockedIPs	net-internal	block-ips	* Any	* Any	Accept
2	InternalOut	net-internal	* Any	* Any	* Any	Accept
3	DMZOut	net-dmz	<div style="background-color: #800000; color: white; padding: 2px; display: inline-block;">Negated</div> net-internal net-ext	* Any	* Any	Accept
4	DrTeethMgmt	drteeth-int	bunsen	* Any	FW1_ica_pull FW1_log CPD FW1_ica_services syslog	Accept
5	InboundGWMgmt	* Any	animal	* Any	ssh_version_2 https	Accept
6	DMZ-Syslog	edgew wrt54gs	bunsen	* Any	syslog	Accept
7	InboundNarfSSH	* Any	narf	* Any	ssh-54269	Accept
8	InboundNarfBT	* Any	narf	* Any	narf-bt-fw	Accept
9	InboundXbox	* Any	xbox360	* Any	xbox	Accept
10	DHCP	* Any	broadcast	* Any	dhcp-request_	Accept

# A Word About IPS Profiles



Check Point  
SOFTWARE TECHNOLOGIES LTD

Note: IPS layer is shared among all...

Search for IP, object, action, ...

No.	Destination	Protection/Site/File/Blade	Services	Action
1	* Any	- N/A	* Any	Hor...

- HomeProfile
- AV\_Only
- Recommended\_Protection
- Recommended\_Profile
- Default\_Protection
- Strict
- Optimized
- Basic
- View...
- Edit...

WELCOME TO THE FUTURE OF CYBER SECURITY

©2017 Check Point Software Technologies Ltd.

[Protected] Distribution or modification is subject to approval



Profiles

**HomeProfile**  
Enter Object Comment

General Policy

- Mail
- IPS
  - Additional Activation**
  - Updates
  - Pre R80 Settings
  - Indicators
  - Malware DNS Trap

Activate IPS protections according to the following additional properties:

Protections to activate:

+ | ×

Category	Name
Protocol	SSH
Vendor	Microsoft
Vendor	Adobe

Protections to deactivate:

+ | ×

Category	Name
<i>No items found</i>	

OK Cancel



Objects | Install Policy | Inspection Settings

General

Profiles

Gateways

Exceptions

ⓘ The following settings are set according to [gateways settings](#) and installed via Access policy installation.

Show profiles used by one of the gateways (1 out of 2) View  146 items

Settings	Performance Impact	Default Inspection
Aggressive Aging		Drop
ASCII Only Request		Inactive
ASCII Only Response Headers		Inactive
Block H.245 Tunneling		Inactive
Block H.323 Messages with Illegal ASN.1 Encoding		Inactive
Block H.323 Multicast Connections		Drop
Block H.323 Sessions that Do Not Start with Setup...		Inactive
Block MGCP Fax		Inactive
Block MGCP Messages with Binary Characters		Inactive
Block MGCP Multicast Connections		Drop
Block SCCP Multicast Connections		Drop
Block SIP Audio		Inactive
Block SIP Basic Authentication		Drop
Block SIP Calls from Unregistered Users		Inactive
Block SIP Early Media		Inactive
Block SIP Instant Messaging		Inactive
Block SIP Keep Alive Messages		Inactive
Block SIP Messages with Binary Characters		Inactive
Block SIP Messages with Invalid Format in CSeq Hea...		Inactive
Block SIP Messages with Invalid Format in Start Line		Inactive
Block SIP Messages with Invalid Format in Via Header		Inactive
Block SIP Messages with Invalid Formats in Headers...		Inactive

Access Control

- Policy
- NAT

Threat Prevention

- Policy
- Exceptions

Shared Policies

- Geo Policy
- Inspection Settings

Access Tools

- VPN Communities
- Updates
- UserCheck
- Client Certificates
- Application Wiki
- Installation History



Check Point®  
SOFTWARE TECHNOLOGIES LTD

# THANK YOU!

COMMUNITY: [HTTPS://COMMUNITY.CHECKPOINT.COM](https://community.checkpoint.com)

TWITTER: [@CPCHECKMATES](https://twitter.com/cpccheckmates)

FACEBOOK: [HTTPS://FACEBOOK.COM/CPCHECKMATES](https://facebook.com/cpccheckmates)

LINKEDIN: [HTTPS://WWW.LINKEDIN.COM/COMPANY/CPCHECKMATES](https://www.linkedin.com/company/cpccheckmates)

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

POWERED BY  CHECK POINT  
**INFINITY**

CLOUD • MOBILE • THREAT PREVENTION



Check Point®  
SOFTWARE TECHNOLOGIES LTD

Check Point  **Live!**  
**CHECKMATES**

# MIGRATE TO R80.20

CheckMates Live!  
Paris 2018

Valeri (Val) Loukine | Cyber Security Evangelist

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

POWERED BY  CHECK POINT  
**INFINITY**

CLOUD • MOBILE • THREAT PREVENTION