

# Introduction to Security Management

Module 2: Introduction to Security Management

Instructor: Kim Winfield

# Objectives

- Design and Manage a Security Policy
- Create a Security Rule-base with Network Objects and Services
- Apply the Rule-base policy to enforce a Security Policy, to and from Internal Networks, DMZ and External Networks

# Security Policy Rule Base

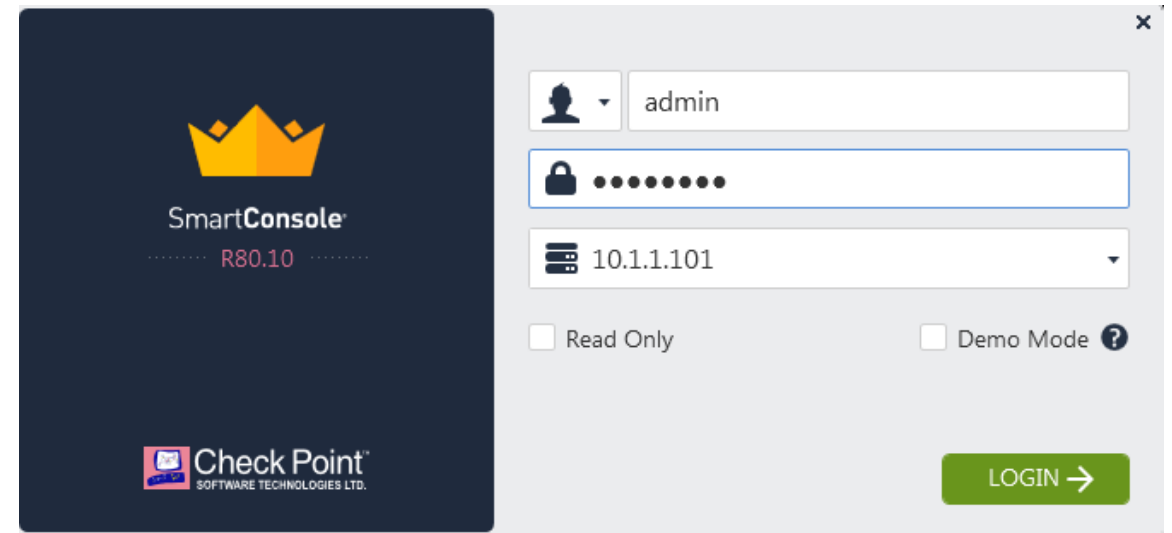
- IP Based Objects
- User Based Objects
- Dynamic Objects
- Zone Objects
- Service Objects
- Time Objects

# Network Objects

- Node Objects
- Network Objects
- Gateway Objects
- Check Point Host Objects

# SmartConsole Access

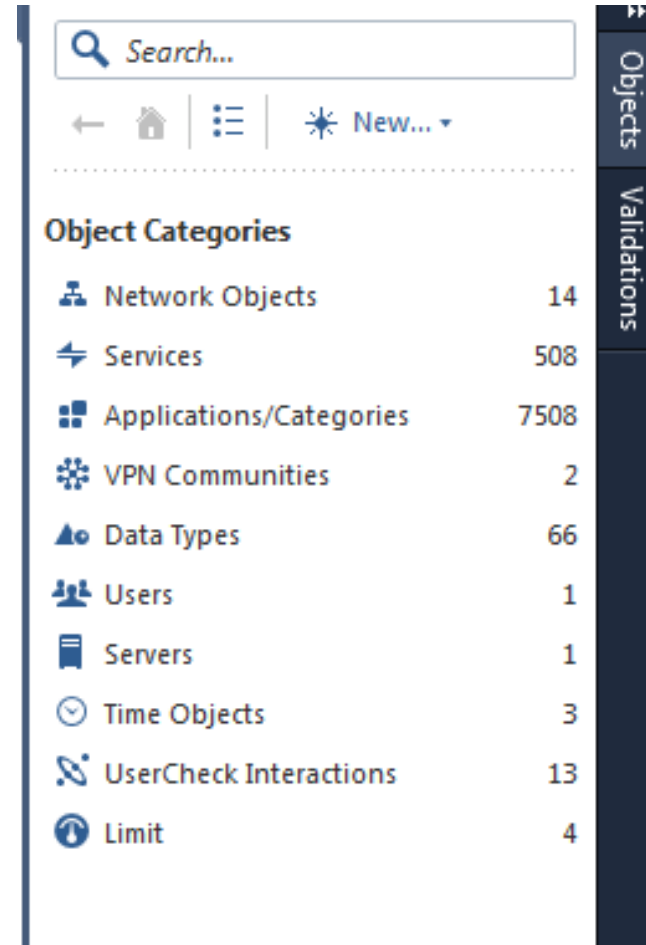
- Logging into the SmartConsole
- Multiple Administrator Access
- Permissions Profiles













The image shows the SmartConsole login interface. On the left is a dark blue panel with a yellow crown icon, the text "SmartConsole", "R80.10", and the Check Point logo. On the right is a light gray login form with a close button (X) in the top right corner. The form contains a user selection dropdown with a person icon, a text field with "admin", a password field with a lock icon and ten dots, a server icon dropdown with "10.1.1.101", and two checkboxes: "Read Only" and "Demo Mode" with a help icon. A green "LOGIN" button with a right arrow is at the bottom right.

# Object Creation

- Creating New Objects and Services
- Create a Network Object
- Create a Node Object
- Create a Group of Objects













The screenshot shows the 'Object Creation' interface. At the top, there is a search bar labeled 'Search...'. Below it, a navigation bar contains a back arrow, a home icon, a list icon, and a 'New...' button with a dropdown arrow. The main content area is titled 'Object Categories' and lists various object types with their respective counts. On the right side, there is a vertical sidebar with two tabs: 'Objects' (selected) and 'Validations'.

Object Categories	
 Network Objects	14
 Services	508
 Applications/Categories	7508
 VPN Communities	2
 Data Types	66
 Users	1
 Servers	1
 Time Objects	3
 UserCheck Interactions	13
 Limit	4

# Service Creation

- Creating Services
- Creating Custom Services
- Creating Service Groups

<input type="text" value="Search..."/>			Objects
<span>←</span> <span>🏠</span> <span>☰</span> <span>✳️ New... ▾</span>			Validations
<b>Services</b>			
	TCP	217	
	UDP	93	
	RPC	18	
	DCE-RPC	41	
	ICMP Services	37	
	GTP	4	
	Compound TCP	4	
	Citrix TCP	1	
	Other Services	42	
	Services Groups	51	

# Rule Base Creation

- Rulebase Essentials
  - Stealth Rule
  - Clean-up Rule
- Rule Base Columns
- Rule Base Rows



# Layers

- Ordered Layers
- In-line Layers
  - Implicit Cleanup – Drop or Accept?
- Best Practices
  - White List
  - Black List

1	Netbios_Drop	* Any	* Any	* Any	NBT	Drop	None
▼ 2	Internal_Net-Internet-Access	Internal_Net	* Any	* Any	* Any	Internal_net_web-ac	Log
2.1		Internal_Net	* Any	* Any	Facebook LinkedIn Twitter	Accept	Log ▼
	Cleanup	* Any	* Any	* Any	* Any	Accept	None
3	Logged_Cleanup	* Any	* Any	* Any	* Any	Drop	Log
	Cleanup	* Any	* Any	* Any	* Any	Drop	None

# In-Line Layer

- Rule 2.1 is an example of an Inline layer. Rule 2 allows traffic from the internal-net to any destination, and any service. Rule 2.1 allows Facebook, LinkedIn and Twitter applications from the internal network to anywhere (Internet)

1	Netbios_Drop	* Any	* Any	* Any	NBT	Drop	None
▼ 2	Internal_Net-Internet-Access	Internal_Net	* Any	* Any	* Any	Internal_net_web-ac	Log
2.1		Internal_Net	* Any	* Any	Facebook LinkedIn Twitter	Accept	Log ▼
Cleanup		* Any	* Any	* Any	* Any	Accept	None
3	Logged_Cleanup	* Any	* Any	* Any	* Any	Drop	Log
Cleanup		* Any	* Any	* Any	* Any	Drop	None

# Summary

- Designed and Managed a Security Policy
- Created a Security Rule-base with Network Objects and Services
- Applied the Rule-base policy to enforce a Security Policy, to and from Internal Networks, DMZ and External Networks

# Bibliography

*Best Practices Rulebase Construction and Optimization* California: USA

*Check Point Security Management* California: USA

*Introduction to Security Management SmartConsole*

[https://youtu.be/LN\\_PdBZONqU](https://youtu.be/LN_PdBZONqU)

*Security Gateway Creation*

<https://youtu.be/sHaCr251QM0>

*Network Object Creation*

[https://youtu.be/DyNlcSY\\_rnE](https://youtu.be/DyNlcSY_rnE)

*Host Object Creation*

<https://youtu.be/QpQA8CYkvX8>