

Introduction to Security Policy Management

Module 3: Introduction to Security Policy Management

Instructor: Kim Winfield

Objectives

- Create a security policy rule base and create network and service objects
- Design and use pre-defined network objects and services based on the best practices guidelines
- Apply security rule-base management best practices

Create a security policy rule base and create network and service objects

- Each rule should have a name that describes the intent of the rule
- Most rules will have logging of some level, or none if you choose not to log
- Source column will be a network, user or groups of users or networks

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Netbios_Drop	* Any	* Any	* Any	 NBT	 Drop	— None

User Access

- Internal User Database
- External User Database
- User Access

Network, Zone and Node Access

- Network objects and Groups of Networks
- Zone objects
- Host Node and Groups of Host Nodes
- Dynamic Object Access and Limitations

Design and use of pre-defined network objects and services based on the best practices guidelines

- Best Practices
 - Name and Comment on all rules
- Basic Rules
 - Cleanup
 - Stealth
- Hit Count
- Rule Expiration




Best Practices

- Refer to Knowledge Base Solution
- <https://supportcenter.checkpoint.com/supportcenter/>
 - Enter sk106597 in the search field
 - The article Best Practices – Rulebase Construction and Optimization
- Review this article

Basic Rules

- Clean Up

- Source: Any
- Destination: Any
- Service: Any
- Action: Drop
- Track: Log

Cleanup Logged Rule	* Any	* Any	* Any	* Any	 Drop	 Log	 A-GW-01
---------------------	-------	-------	-------	-------	--	---	---

- Stealth

- Source: Any
- Destination: GW's
- Service: Any
- Action: Drop
- Track: Log

Stealth	* Any	 A-GW-01	* Any	* Any	 Drop	 Log	 A-GW-01
---------	-------	---	-------	-------	--	---	---

Hit Count and Rule Expiration

- Hit Count

No.	Hits	Name	Source
1	<div><div></div></div> 0	Netbios_Drop	* Any
▼ 2	<div><div></div></div> 0	Internal_Net-Internet-Access	Internal_Net
2.1	<div><div></div></div> 0		Internal_Net

- Rule Expiration

New #CpmiTime..ClassName

🕒

Rule 2 Expiration

Enter Object Comment

Time Period

Start

☒ Immediately
 ☐ At: 5/2/2017 14:22

End

☐ Never
 ☒ At: 8/1/2017 14:22

Recurring

Hour Ranges

☒ From: 09:00 To: 17:00
 ☐ From: 00:00 To: 00:00
 ☐ From: 00:00 To: 00:00

Day Recurrence

☒ Daily Every day
 ☐ Days in week
 ☐ Days in month

Add Tag

OK

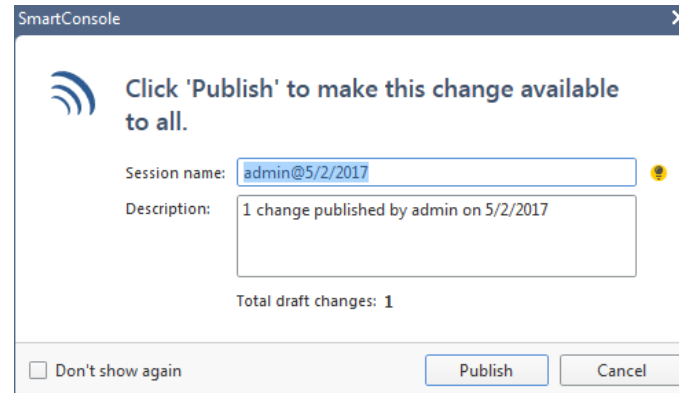
Cancel

Apply security rule-base management

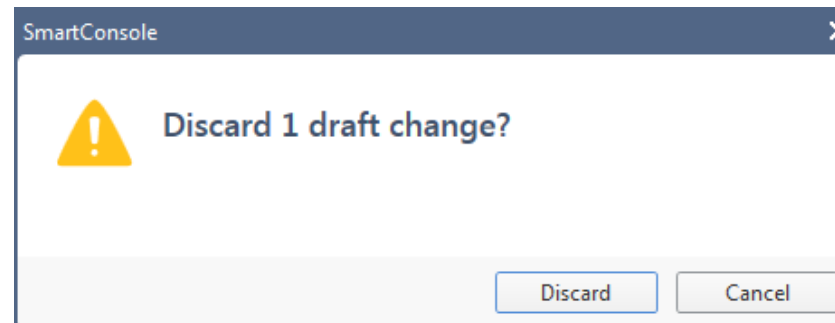
- Publish
- Install Database
- Install Policy

Publish and Discard

- Publish Changes

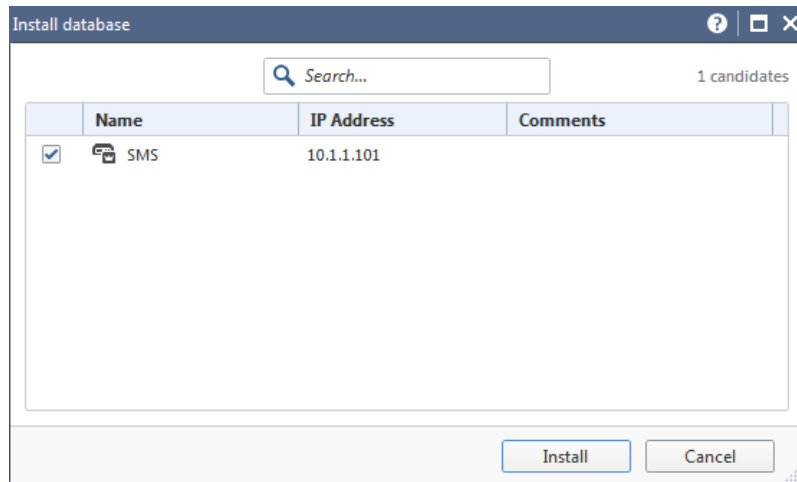


- Discard Changes



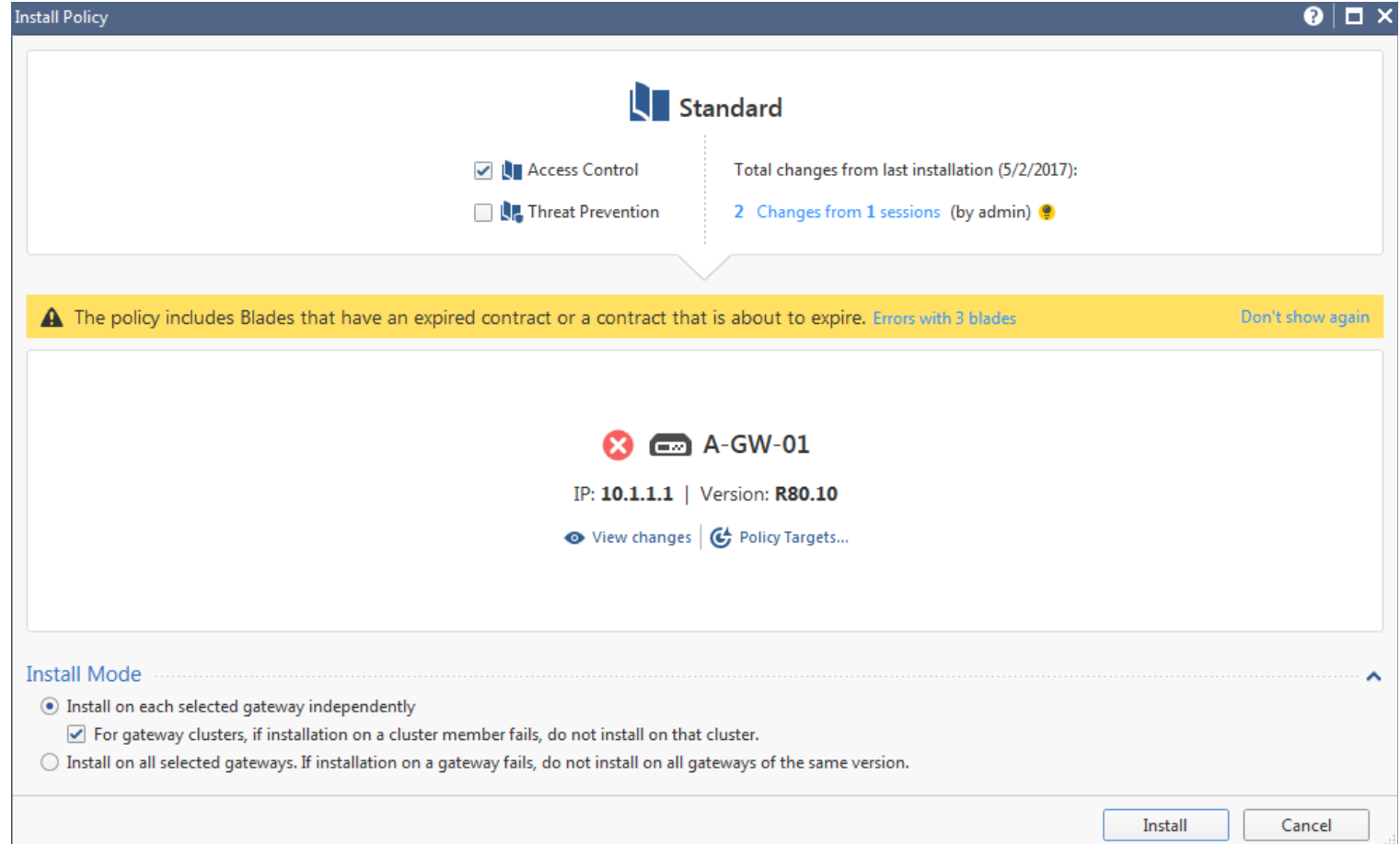
Install Database

- Installs all changes of publish actions to management database
- Installs database changes to Management Server and Log Servers
- Does not install the policy to the gateway



Install Policy

- Access Control
- Threat Prevention



The screenshot shows a web-based 'Install Policy' window. At the top, the title bar reads 'Install Policy'. The main content area is divided into sections. The first section, titled 'Standard', contains two checkboxes: 'Access Control' (checked) and 'Threat Prevention' (unchecked). To the right of these checkboxes, it states 'Total changes from last installation (5/2/2017): 2 Changes from 1 sessions (by admin)'. Below this, a yellow warning banner reads: 'The policy includes Blades that have an expired contract or a contract that is about to expire. Errors with 3 blades' with a 'Don't show again' link. The next section displays a gateway named 'A-GW-01' with a red 'X' icon, IP '10.1.1.1', and Version 'R80.10'. Below the gateway name are links for 'View changes' and 'Policy Targets...'. The 'Install Mode' section at the bottom has three radio buttons: 'Install on each selected gateway independently' (selected), 'For gateway clusters, if installation on a cluster member fails, do not install on that cluster.' (checked), and 'Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.' At the bottom right are 'Install' and 'Cancel' buttons.

Install Policy

Standard

☒ Access Control

☐ Threat Prevention

Total changes from last installation (5/2/2017):
2 Changes from 1 sessions (by admin)

Warning: The policy includes Blades that have an expired contract or a contract that is about to expire. [Errors with 3 blades](#) [Don't show again](#)

A-GW-01

IP: 10.1.1.1 | Version: R80.10

[View changes](#) | [Policy Targets...](#)

Install Mode

☒ Install on each selected gateway independently

☒ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

☐ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

[Install](#) [Cancel](#)

Summary

- Created a security policy rule base and create network and service objects
- Designed and use pre-defined network objects and services based on the best practices guidelines
- Applied security rule-base management Best Practices

Bibliography

R80.10 Security Management California: USA

Best Practices Rulebase Construction California: USA

Video's