

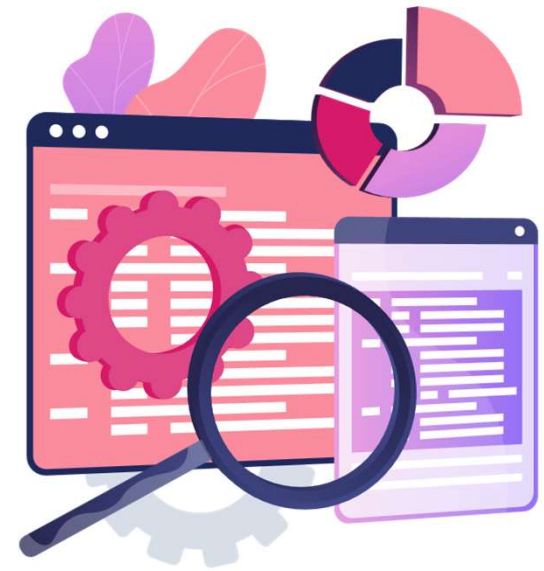
CHAPTER 5

SECURITY POLICY MANAGEMENT

YOU DESERVE THE BEST SECURITY

Learning Objectives

- Describe the essential elements of a Security Policy.
- Identify features and capabilities that enhance the configuration and management of the Security Policy.



Security Policy Overview

- A Security Policy is a collection of rules and settings that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.
- Policies are:
 - Created and managed using SmartConsole.
 - Stored on the System Management Server.
 - Enforced by Security Gateways.

Basic Policy Types

- Access Control Policy
- Desktop Security Policy
- QoS Policy
- Threat Prevention Policy



The Unified Policy

An innovative feature of SmartConsole is the concept of the Unified Policy, which lets an administrator control several security aspects from a single console. In addition, the information on connections from all Software Blades is collected in one log file.

Access Control Policy

- Lets you create a simple and granular rulebase that unifies these Access Control features:
 - Firewall
 - Application & URL Filtering
 - Content Awareness
 - IPsec VPN and Mobile Access
 - Identity Awareness

Desktop Security Policy

- Check Point clients that include Desktop Security, such as Endpoint Security VPN, enforce a Desktop Security Policy on the client to give it Firewall protection.
- Clients enforce the Desktop Policy to accept, encrypt, or drop connections based on the Source, Destination, and Service.

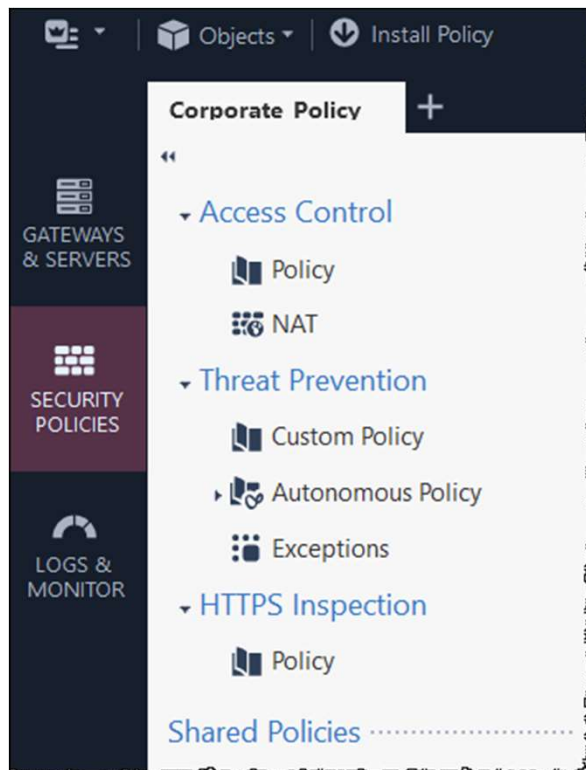
QoS Policy

- Policy-based bandwidth management solution.
- Prioritizes business-critical traffic over lower priority traffic.
- Guarantees bandwidth and control latency for streaming applications, such as Voice over IP (VoIP) and video conferencing.
- Gives guaranteed or priority access to specified employees, even if they are remotely accessing network resources.

Threat Prevention Policy

- Autonomous (out-of-the box) and Custom Threat Prevention.
- IPS - Comprehensive protection against malicious and unwanted network traffic.
- Anti-Bot - Post-infection detection of bots on hosts.
- Anti-Virus - Pre-infection detection and blocking of malware at the Security Gateway.
- SandBlast - Protection against infections from undiscovered exploits, zero-day, and targeted attacks.

Policy Management



- Policies are managed using SmartConsole from the Security Policies view.
- This view displays your available Software Blades (features).

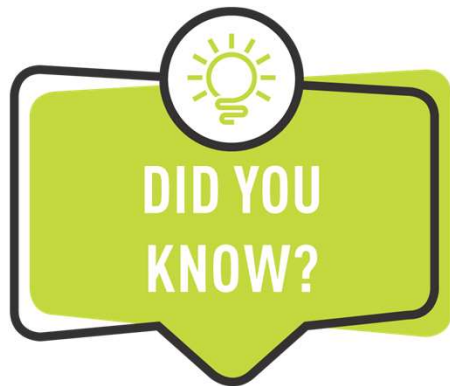
Shared Policies

The Shared Policies section in a policy package provides access to these granular Software Blades and features:

- Mobile Access
- Data Loss Prevention
- HTTPS Inspection

The Policy will be enforced only on gateways with HTTPS Inspection enabled. [Don't show this message](#)

No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Blade	Install On	Certificate	Comment
1	Bypass-rule	* Any	Internet	HTTPS default s...	Health Financial Services	Bypass	Log	* All	* Policy H...	Outbound Certi...	
2	Predefined Rule	* Any	Internet	HTTPS default s...	* Any	Inspect	Log	* All	* Policy H...	Outbound Certi...	

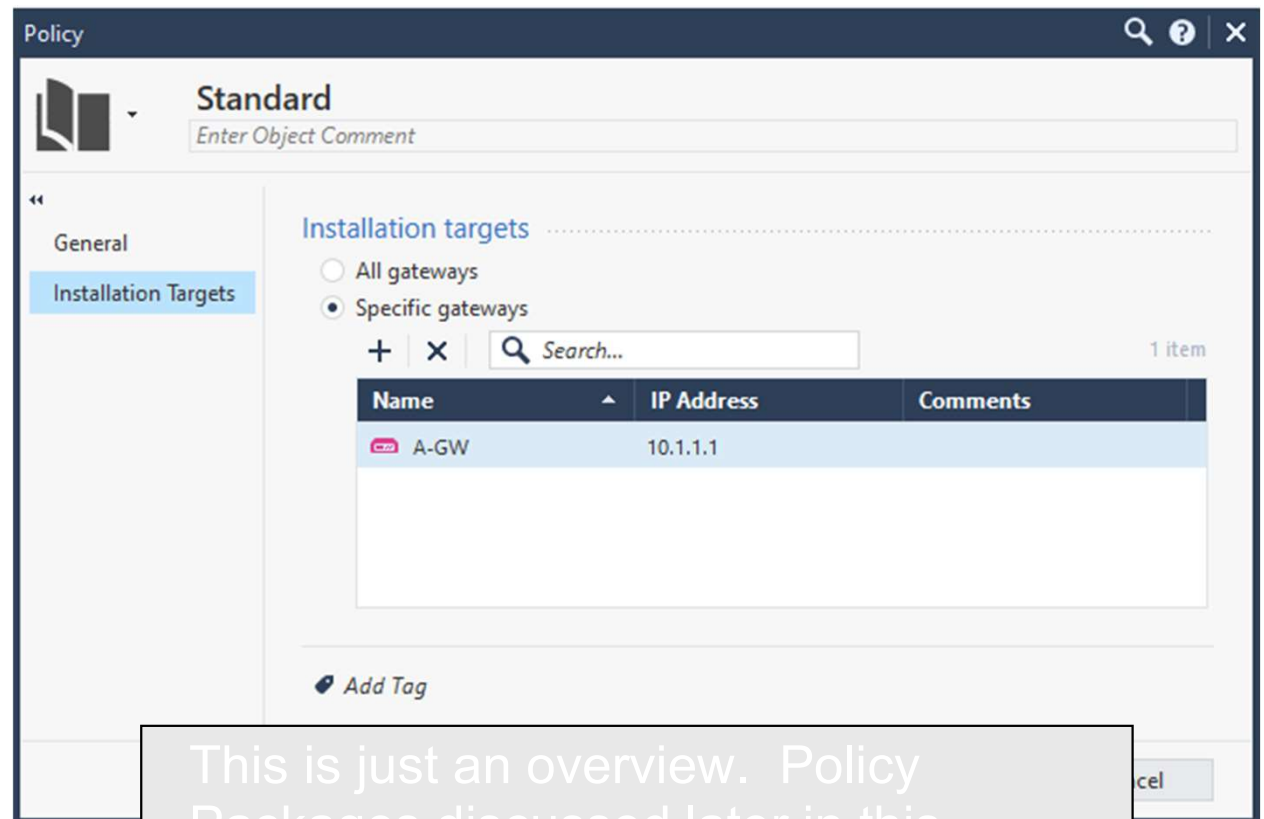


The Geo Policy is supported using Updateable Objects. Updateable Objects are discussed in the CCSE course.

For additional information, see the Quantum Security Management Administration Guide.

Policy Packages

- Group of different types of policies that are installed together on the same installation targets.
- The Security Gateway enforces all the policies in the package.



This is just an overview. Policy Packages discussed later in this chapter.

Default Rule

Add

Edit

No.	Name	Source	VPN	Destination	Services & Applicat...	Content	Action
		* Any	* Any	* Any	* Any	* Any	<ul style="list-style-type: none">AcceptDropAskInformMore ...Inline Layer

When you add a rule to the rulebase, a default configuration is applied. You then customize the rule using controls, such as pencil icon (edit), + (add), and down arrow (menu).

Select from menu



As discussed in Chapter 3, objects are used in rules to represent physical and virtual network components (such as Security Gateways, servers, and users), and logical components (such as applications, IP address ranges, and services).

When working with rules, you can select previously configured objects or create new ones.

Navigating a Default Rule

- Before creating a rule, it is important to understand a rule's default configuration. The figures on the following slides show a default rule.
- The following columns are not shown.
 - Hits - Accumulated hits a rule has received in the rulebase.
 - Time - Timeframe. The default is Any.
 - Comments - Notes about this rule. The default is a blank field.

Navigating a Default Rule - No (Number)



No.	Name	Source	Destination	VPN
1		* Any	* Any	* Any

- Automatically assigned.
- Indicates the rule's position in the rulebase.
- Changes if the rule's order is changed.

Navigating a Default Rule - Name



No.	Name	Source	Destination	VPN
1		* Any	* Any	* Any

- Meaningful name for the rule.
- Default is no entry.
- Appears in the logs for monitoring and troubleshooting.

Navigating a Default Rule - Source



No.	Name	Source	Destination	VPN
1		* Any	* Any	* Any

- Object that is traffic source.
- Default is **Any**.
- Can select from a list of network objects or create a new one.

Navigating a Default Rule - Destination



No.	Name	Source	Destination	VPN
1		* Any	* Any	* Any

- Object that is traffic destination.
- Default is **Any**.
- Can select from a list of network objects or create a new one.

Navigating a Default Rule - VPN




No.	Name	Source	Destination	VPN
1		* Any	* Any	* Any

- Displays the VPN Community, if applicable.
- Default is **Any**.

Navigating a Default Rule - Services & Applications




Services & Applicat...	Content	Action	Track	Install On
* Any	* Any	 Drop	— None	* Policy Targets

- Applicable services or applications. Default **Any**.
- Select from a list of service and application objects or create a new one.

Navigating a Default Rule - Content



Services & Applicat...	Content	Action	Track	Install On
* Any	* Any	 Drop	— None	* Policy Targets

- Content type. Default **Any**.
- Select from a list of content types (certificate, CSV file, key, media file, etc.) or create a new one.

Navigating a Default Rule - Action





Services & Applicat...	Content	Action	Track	Install On
* Any	* Any	<input checked="" type="radio"/> Drop	— None	* Policy Targets

- Action to apply to connection. Default **Drop**.
- Click the down arrow to select a different action; for example, Accept, Drop, Inform, or Reject.

Navigating a Default Rule - Track



Services & Applicat...	Content	Action	Track	Install On
* Any	* Any	 Drop	 None	* Policy Targets

- Tracking option for connection. Default **None**.
- Click the down arrow to select one or more options; for example, Log, Alert, and related settings.

Navigating a Default Rule – Install On



Services & Applicat...	Content	Action	Track	Install On
* Any	* Any	🎯 Drop	— None	* Policy Targets

- Firewall (Gateway) on which to enforce the rule.
- Default **Policy Targets** (all internal Firewall objects).
- Select a specific object or create a new one.






Cleanup and Stealth Rules

- For an effective Security Policy, Check Point recommends that rulebases contain Cleanup and Stealth rules.
- These rules are added first.

No.	Name	Source	Destination	VPN	Services & ...	Content	Action	Track
1	Stealth rule	* Any	 Corporate-GW	* Any	* Any	* Any	 Drop	 Log
2	Cleanup	* Any	* Any	* Any	* Any	* Any	 Drop	 Log

Cleanup Rule






- Recommended to determine how to handle connections not matched by the rules above it in the rulebase. It is also necessary for logging this traffic.
- Can be configured to allow or drop the connection.

No.	Name	Source	Destination	VPN	Services &...	Content	Action	Track
1	Stealth rule	* Any	 Corporate-GW	* Any	* Any	* Any	 Drop	 Log
2	Cleanup	* Any	* Any	* Any	* Any	* Any	 Drop	 Log

A Cleanup rule should always be placed at the bottom of the rulebase.

Stealth Rule

- A Stealth rule is recommended to drop any traffic destined for the Firewall that is not otherwise explicitly allowed.

No.	Name	Source	Destination	VPN	Services &...	Content	Action	Track
1	Stealth rule	* Any	 Corporate-GW	* Any	* Any	* Any	 Drop	 Log
2	Cleanup	* Any	* Any	* Any	* Any	* Any	 Drop	 Log

The Stealth rule should be located as early in your policy as possible, typically immediately after any management rules.

Connections that need to be made directly to the Security Gateway always go above the Stealth rule; for example: Client Authentication, Encryption, and Content Vectoring Protocol (CVP).

Explicit and Implied Rules

- **Explicit rules:**
 - Created by the administrator.
 - Configured to allow or block traffic based on specified criteria.
- **Implied rules:**
 - Created by the Security Gateway.
 - Placed first, last, or before the last in the explicitly defined rule.
 - Not visible in the rulebase.
- **Implicit Cleanup Action**
 - Often called the Implied Cleanup Rule.
 - Default function of the policy layer.
 - Options are drop or accept.



The Implicit Cleanup Action is often called the Implied Cleanup Rule; however, it is not a rule. It is a Gateway action or behavior. The options are Drop or Accept.

Control Connections Defined by Implied Rules

- Gateway-specific traffic that facilitates functionality, such as logging, management, and key exchange.
- Acceptance of Internet Key Exchange (IKE) and Reliable Datagram Protocol (RDP) traffic for communication and encryption purposes.
- Communication with various servers (such as RADIUS, CVP, UFP, TACACS, LDAP, and logical servers) even if these servers are not specifically defined resources in the Security Policy.

Rule Examples

- Critical Subnet
- Tech Support
- DNS Server
- Mail and Web Servers
- SMTP
- DMZ and Internet

Rulebase Management - Rulebase Order

- Within the rulebase, rules are arranged in top-down order for matching purposes.
- When the Security Gateway receives a packet for a connection, it examines the first rule in the rulebase to see if there is a match.
- If there is no match, the Security Gateway works its way down the list until it finds a match.
- After a rule is matched, the Security Gateway enforces the rule; for example: Accept, Drop, or Reject the connection.



- Rule order is a critical aspect of an effective rulebase. The rule order can affect the performance of the Security Gateway and the accuracy of the policy.
- Always place more specific rules at the top of the rulebase and place more general rules last to prevent a general rule from being applied before a more specific rule.

Order of Operations

- The rulebase is processed in a specific top-down order.
- However, other things happen in the Security Policy besides checking your defined rules.
- This is the order of operations.

0. Anti-spoofing Checks

1. First Implied Rule

2. Explicit Rules

3. Before Last Implied Rules

4. Last Explicit Rules

5. Last Implied Rule

6. Implicit Cleanup Action

Anti-Spoofing Checks

- Occurs before rules are processed.
- Detects such packets by requiring that the interface on which a packet enters a Security Gateway corresponds to its IP address.

0. Anti-Spoofing Checks

1. First Implied Rule

2. Explicit Rules

3. Before Last Implied Rules

4. Last Explicit Rules

5. Last Implied Rule

6. Implicit Cleanup Action

First Implied Rule

- Cannot be modified, moved or overwritten in the rulebase.
- No rules can be placed before it.
- Applied before all other rules, including explicitly-defined and Last Implied rules.

0. Anti-Spoofing Checks

1. First Implied Rule

2. Explicit Rules

3. Before Last Implied Rules

4. Last Explicit Rules

5. Last Implied Rule

6. Implicit Cleanup Action

Explicit Rules

- Located between First and Last Implied rules.
- Administrator-defined.

0. Anti-Spoofing Checks

1. First Implied Rule

2. Explicit Rules

3. Before Last Implied Rules

4. Last Explicit Rules

5. Last Implied Rule

6. Implicit Cleanup Action

Before Last Implied Rules

- More specific Implied rules.
- Enforced before the last rule is applied.

0. Anti-Spoofing Checks

1. First Implied Rule

2. Explicit Rules

3. Before Last Implied Rules

4. Last Explicit Rules

5. Last Implied Rule

6. Implicit Cleanup Action

Last Explicit Rules

- Should be Explicit Cleanup rule.

0. Anti-Spoofing Checks

1. First Implied Rule

2. Explicit Rules

3. Before Last Implied Rules

4. Last Explicit Rules

5. Last Implied Rule

6. Implicit Cleanup Action

Last Implied Rule

- Applied after all other Explicit and Implied rules.
- In the rulebase, except the final Implied Cleanup rule.

0. Anti-Spoofing Checks

1. First Implied Rule

2. Explicit Rules

3. Before Last Implied Rules

4. Last Explicit Rules

5. Last Implied Rule

6. Implicit Cleanup Action

Implicit Cleanup Action

- Applied when no other rules are matched.
- Default behavior.

0. Anti-Spoofing Checks

1. First Implied Rule

2. Explicit Rules

3. Before Last Implied Rules

4. Last Explicit Rules

5. Last Implied Rule

6. Implicit Cleanup Action

Sections

No.	Name	Source	Destination
▼ Security Gateways Access (1-2)			
1	Administrator Access to Gateways	👤 Admins	🌐 Corporate-GW
2	Stealth rule	* Any	🌐 Corporate-GW
▼ VPN (3)			
3	VPN between Internal LANs and Branch office LAN	👤 Branch Office LAN 👤 Corporate LANs	👤 Branch Office LAN 👤 Corporate LANs
▼ Access To Internet (4-5)			
▶ 4	Access to Internet according to Web control policy	🏰 InternalZone	🏰 ExternalZone 🖨 Proxy Server
5	DNS outgoing access	🖨 DNS Server	🏰 ExternalZone
▶ DMZ (6-11)			
▶ Data Center Access (12-13)			
▶ Temporary Access Grant (14)			
▶ Cleanup (15)			

- Useful for managing large networks.
- Simple visual divisions.
- Do not hinder the order of rule enforcement.
- Are not sent to the Security Gateway side.

Security Zones and Topology Overview

- A Security Zone object represents a part of the network's topology; for example:
 - Internal network
 - External network
 - Demilitarized zone (DMZ)Do
- Security Zones simplify rulebase creation and policy management.
- Using zones, you can apply the same rule to many Security Gateways and add networks to Security Gateways interfaces without changing the rulebase.



Security Zone objects automatically enforce changes in the topology and let administrators efficiently add internal networks without updating the Security Policy.

However, Anti-Spoofing overrules security zones because it does not automatically trust all networks in a zone.

Predefined Security Zones

- **WirelessZone** - Networks that can be accessed by users and applications with a wireless connection.
- **ExternalZone** - Networks that are not secure, such as the Internet and other external networks.
- **DMZZone** - Demilitarized zone. Sometimes referred to as a perimeter network. It contains company servers that can be accessed from external sources.
- **InternalZone** - Company networks with sensitive data that must be protected and used only by authenticated users.

Optionally, you can also create custom zones to meet your needs.

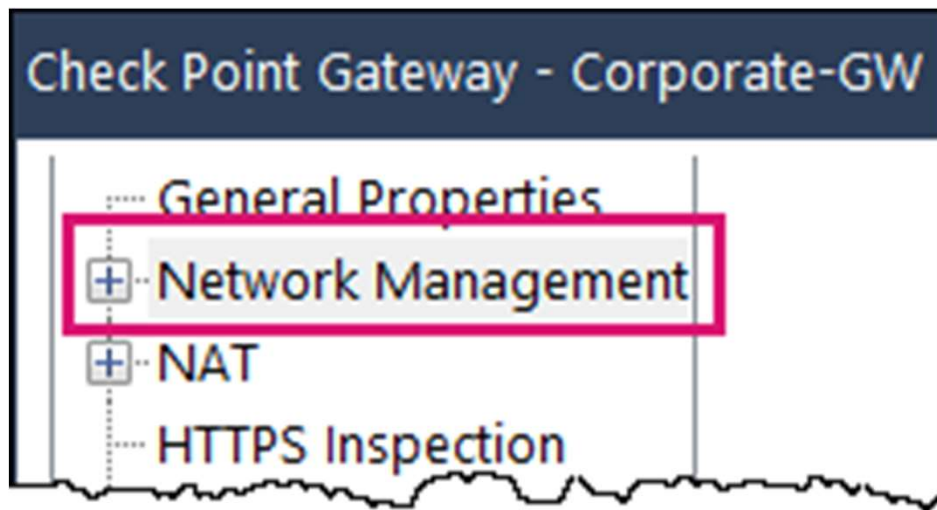


It is important to understand how security zones and related topology settings, such as Anti-Spoofing, settings work before making changes. Misconfiguring these can leave gaps in your network security.

For demonstration purposes, this section reviews the existing settings for a Security Gateway.

In the lab for this chapter, you learn how to modify the topology settings, such as security zones, for a Security Gateway.

Demonstration – Security Zones and Topology








- Open a **Security Gateway** object.
- In the left pane, click **Network Management**.

Detected Interfaces – Automatically Calculated

Check Point Gateway - Corporate-GW

General Properties
+ Network Management
+ NAT
... HTTPS Inspection
... HTTP/HTTPS Proxy
+ ICAP Server
... Anti-Bot and Anti-Virus
+ Threat Emulation
... Threat Extraction

Name	Topology	IP
 eth0	External	198.51.100.5/24
 eth1	This network	22.20.105.5/24
 eth2	This network	151.20.4.5/24

Detected Interfaces – Automatically Calculated

Check Point Gateway - Corporate-GW

General Properties
+ Network Management
+ NAT
HTTPS Inspection
HTTP/HTTPS Proxy
+ ICAP Server
Anti-Bot and Anti-Virus
+ Threat Emulation
Threat Extraction

Search...

Name	Topology	IP
eth0	External	198
eth1	This network	22.2
eth2	This network	151

External (leading to the Internet)
or
This Network (Internal)

Example – eth0

- **Leads to** - Internet (External)
- **Security Zone** - ExternalZone (predefined zone)
- **Anti Spoofing** - Prevent and Log (defaults.

Interface: eth0

eth0
Enter Object Comment

General

QoS

Advanced

General

IPv4: 198.51.100.5 / 24

IPv6: /

Topology

Leads To: **Internet (External)**

Security Zone: **ExternalZone** ⓘ

Anti Spoofing: **Prevent and Log**

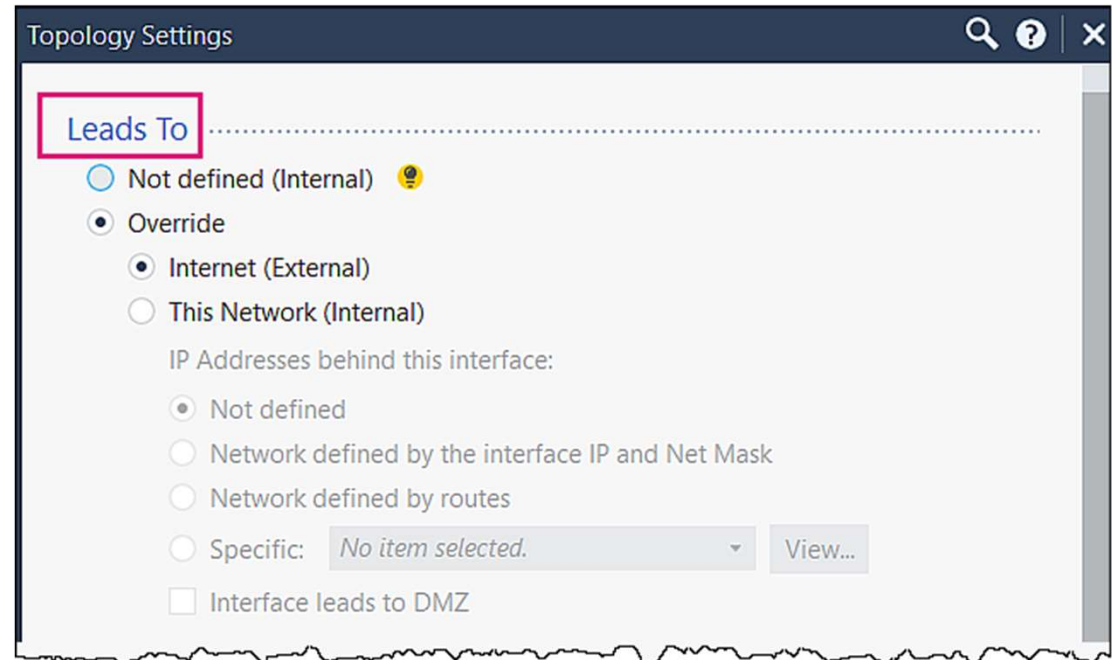
Modify...

Add Tag

OK Cancel

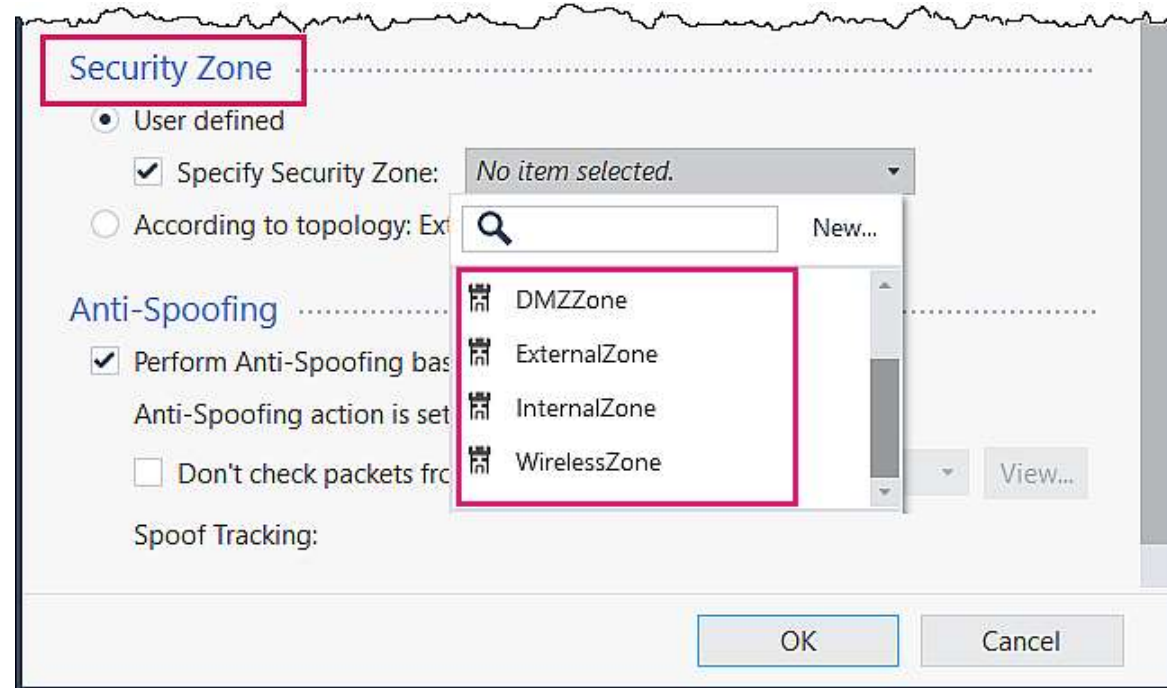
Leads To

- Defines the type of network.
- Optionally, you can override this setting; for example, define a specific network object.



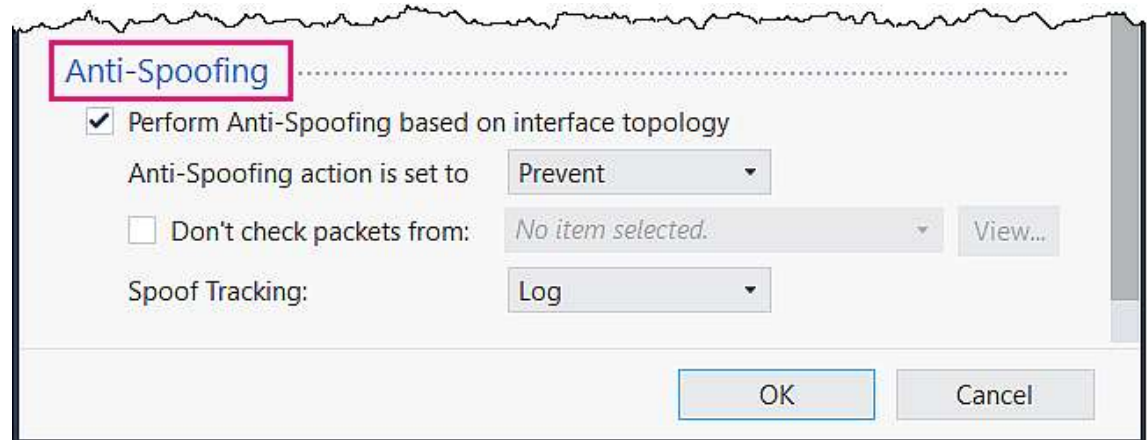
Security Zone

- Preefined:
 - DMZZone
 - ExternalZone
 - Internal Zone
 - WirelessZone
- Custom



Anti-Spoofing

- Spoofing Action – Prevent
 - Drop spoofed packets.
 - Best practice
- Spoof Tracking - Log.
 - Create a log entry,
 - Optionally, set to Alert.



The screenshot shows a configuration window titled "Anti-Spoofing". The title bar is highlighted with a red box. The window contains the following settings:

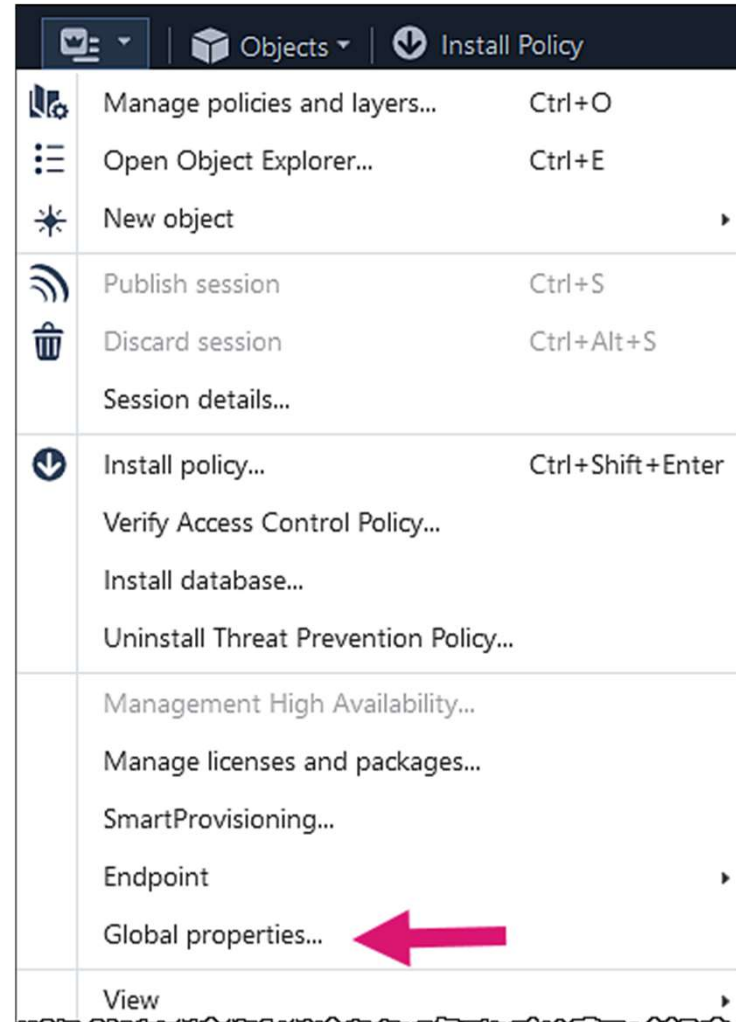
- Perform Anti-Spoofing based on interface topology
- Anti-Spoofing action is set to: Prevent (dropdown menu)
- Don't check packets from: No item selected. (dropdown menu) View... (button)
- Spoof Tracking: Log (dropdown menu)

At the bottom right, there are "OK" and "Cancel" buttons.

For Anti-Spoofing to be most effective, it should be configured on all Security Gateway interfaces.

Global Properties

- Enforced by all Security Gateways managed by the Security Management Server.
- Configured from the Global Properties window, which is accessed from the SmartConsole applications menu.



Global Properties Window

- Settings apply to a variety of Check Point products, services and functions, such as Firewall, NAT, VPN, and Logging and Alerts.
- Click ? (question mark icon) for Help for each setting.

Global Properties

Select the following properties and choose the position of the rules in the Rule Base:

Property	Position
<input checked="" type="checkbox"/> Accept control connections:	First
<input checked="" type="checkbox"/> Accept Remote Access control connections:	First
<input checked="" type="checkbox"/> Accept SmartUpdate connections:	First
<input checked="" type="checkbox"/> Accept IPS-1 management connections:	First
<input checked="" type="checkbox"/> Accept outgoing packets originating from Gateway:	Before Last
<input checked="" type="checkbox"/> Accept outgoing packets originating from Connectra gateway:	Before Last
<input checked="" type="checkbox"/> Accept outgoing packets to Check Point online services: (Supported for R80.10 Gateway and higher)	Before Last
<input type="checkbox"/> Accept RIP:	First
<input type="checkbox"/> Accept Domain Name over UDP (Queries):	First
<input type="checkbox"/> Accept Domain Name over TCP (Zone Transfer):	First
<input type="checkbox"/> Accept ICMP requests:	Before Last
<input checked="" type="checkbox"/> Accept Web and SSH connections for Gateway's administration: (Small Office Appliance)	First
<input checked="" type="checkbox"/> Accept incoming traffic to DHCP and DNS services of gateways: (Small Office Appliance)	First
<input checked="" type="checkbox"/> Accept Dynamic Address modules' outgoing Internet connections:	First
<input checked="" type="checkbox"/> Accept VRRP packets originating from cluster members (VSX IPSO VRRP)	First
<input checked="" type="checkbox"/> Accept Identity Awareness control connections:	First

Track _____

Log Implied Rules

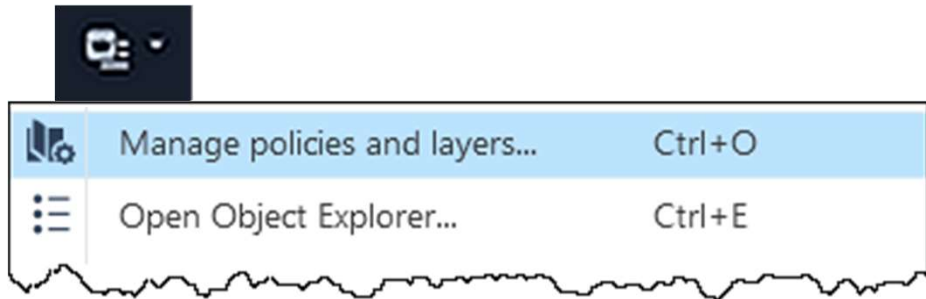
Policy Packages Overview

- After policy configuration, it is useful to create policy packages.
- Policy packages are logical grouping of one or more of these policy types:
 - Access Control
 - QoS
 - Desktop Security
 - Threat Prevention

Policy packages let you install different combinations of policies on an organization's Security Gateways.

Working with Policy Packages

- Policy packages are configured using SmartConsole:



Applications menu →
Manage policies and layers

Workflow



Create (or add to existing package).



Publish session changes.



Install policy on targets.



Publishing changes is not the same as saving changes.

Changes made during a session in SmartConsole creates a draft of the edited policy on the Security Management Server.

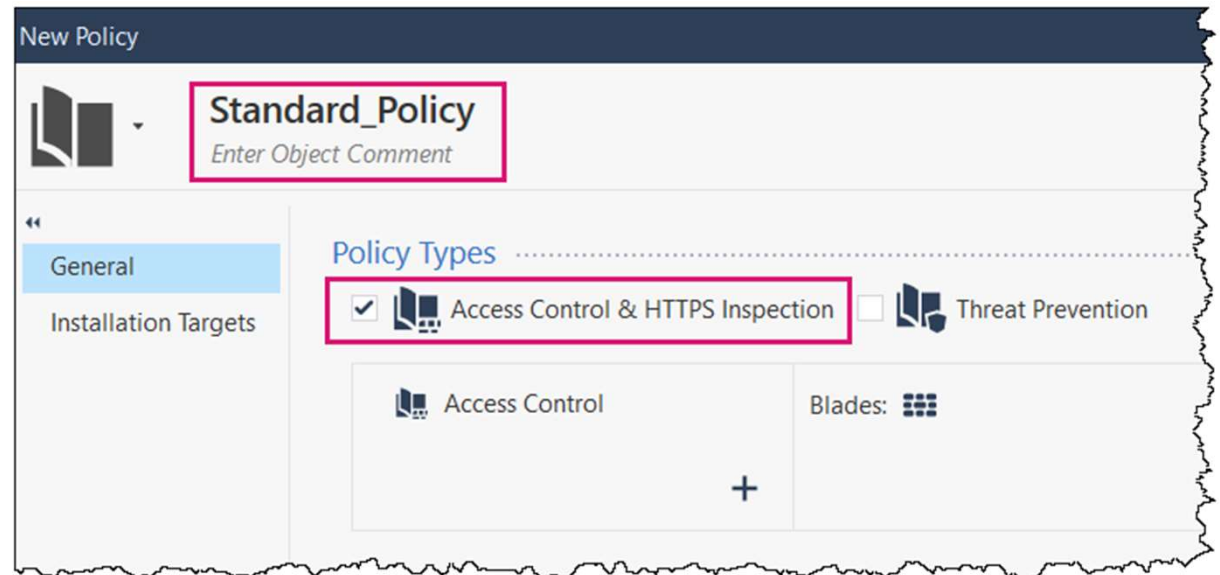
Publishing updates the policy on the Security Management Server and/or Log Server and makes the changes visible in SmartConsole.

Many organizations amend policy regularly but only publish policy during a change window.

Creating a Policy Package

General:

- Name
- Description (optional)
- Policy Types to include/exclude



New Policy window → * (new) → General

Creating a Policy Package (Continued)

Installation Targets:

- All gateways or specific gateways
- OK
- Close

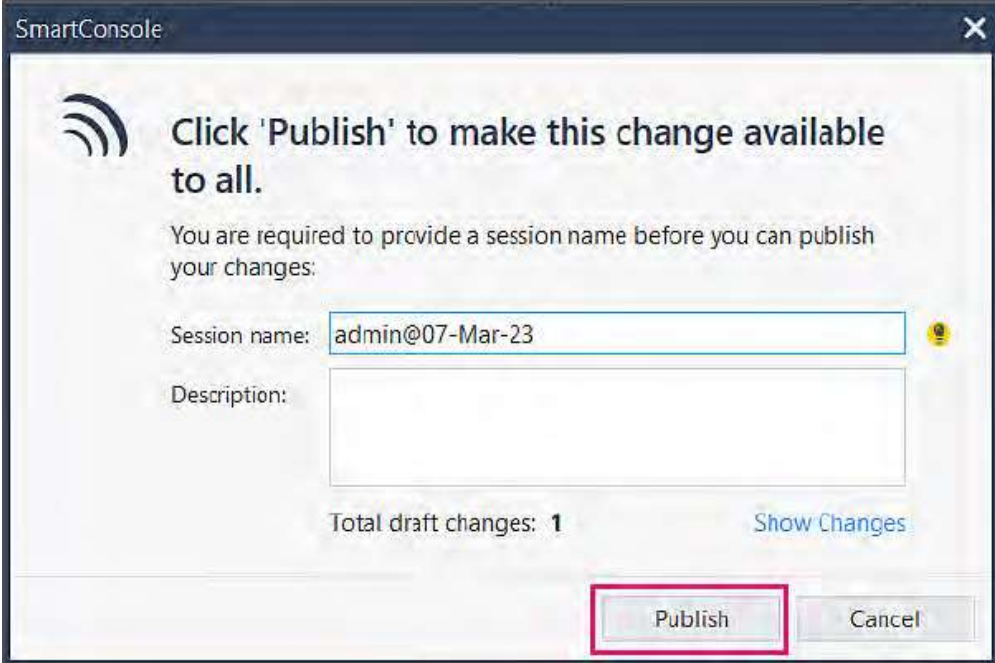


New Policy window → Installation Targets

Publishing a Policy Package

From the Global Toolbar:


- Click **Publish**.
- Type a name.
- Provide an optional description.
- Click **Publish**.



SmartConsole

Click 'Publish' to make this change available to all.

You are required to provide a session name before you can publish your changes:

Session name: 

Description:

Total draft changes: 1 [Show Changes](#)

Installing a Policy Package

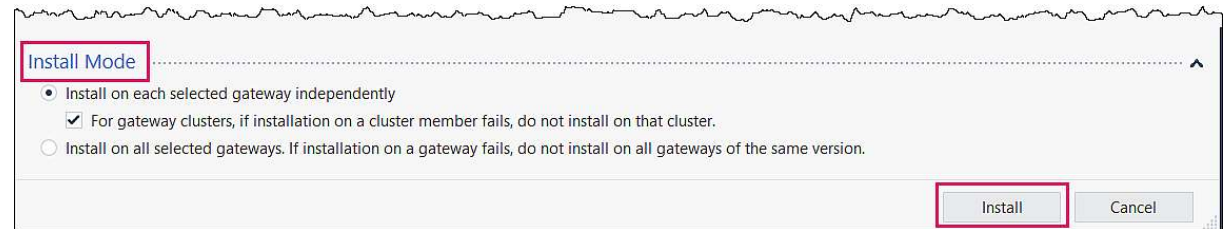
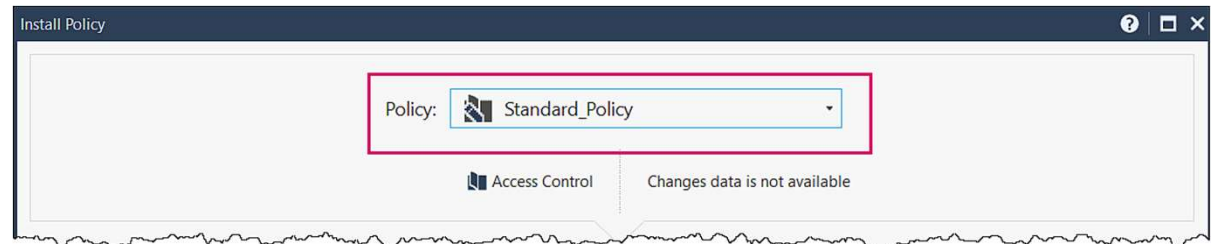
Global toolbar:

- Install Policy

Install Policy window:

- Policy package
- Install Mode

Install



Global toolbar → Install Policy

Install Modes

- Install on each Gateway independently (default):
 - If the installation fails on one target Gateway, it does not affect the installation on the rest of the target Gateways.
- Install on all selected Gateways:
 - If the policy fails to install on one of the Gateways, the policy is not installed on any of the other target Gateways.

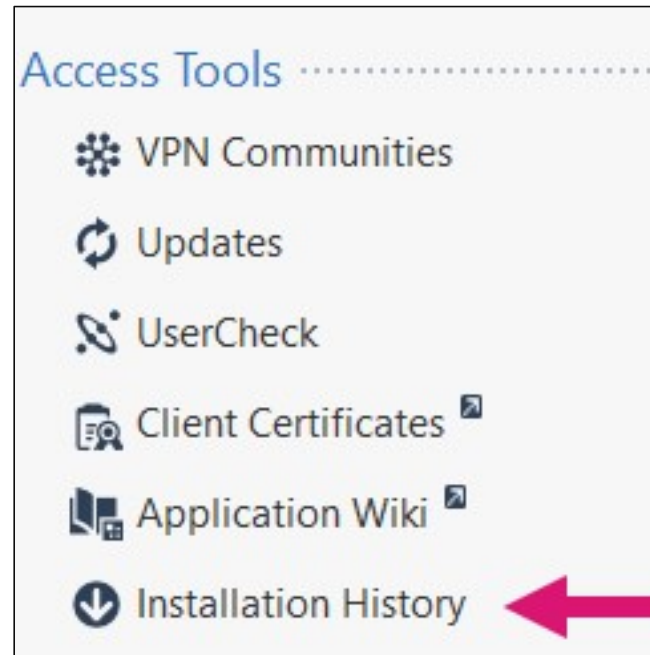
Policy Installation - A Closer Look



- Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.
- Makes sure each Security Gateways enforce at least one of the rules. If no rules are enforced, the default drop rule is enforced.
- Distributes the user database and object database to the selected installation targets.

Installation History

- Shows history of all the policy installations so that the administrators can revert to a previous version.
- Can view as Audit Logs or they can be viewed in a Read Only instance.



SmartConsole Security Policies view:
Access Tools → Installation History

Accelerated Policy Installation

- Decreases Access Control policy installation (R81 and higher).
- Example Access Control operations that trigger Accelerated Install Policy:
 - Access Control Rule
 - Creating a rule (without editing it)
 - Editing selected columns, such as Name, Source, Destination, VPN, Services & Applications, Content, Action, Track, and Time
 - Deleting, enabling, or disabling rule
 - Access Control Layer:
 - Creating a layer or editing layer properties

Review Questions

1. What type of rules are created by the Security Gateway?
2. What type of rules are created by the administrator?
3. Where should the Cleanup rule be placed?

Lab 5A

Creating a Security Policy



Lab 5B

Creating Bravo Security Policy

