

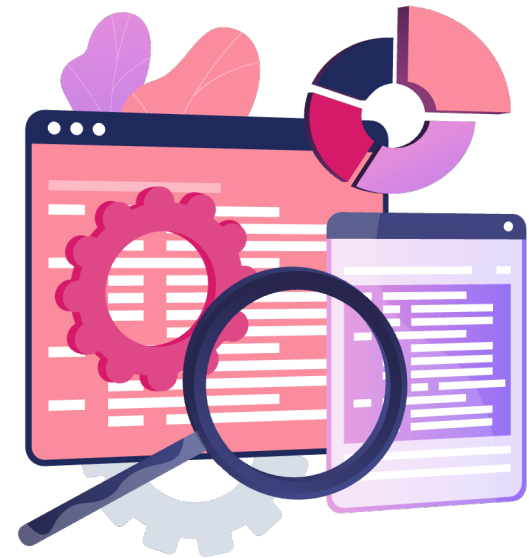
CHAPTER 6

POLICY LAYERS

YOU DESERVE THE BEST SECURITY

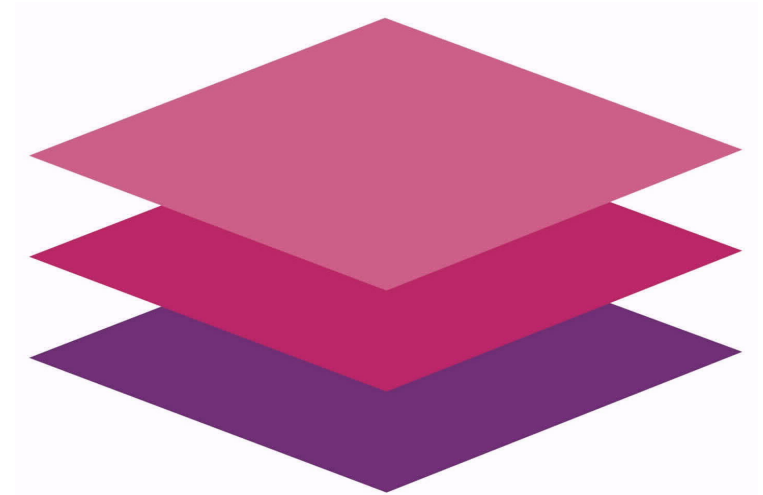
Learning Objectives

- Demonstrate understanding of the Check Point policy layer concept.
- Explain how policy layers affect traffic inspection.



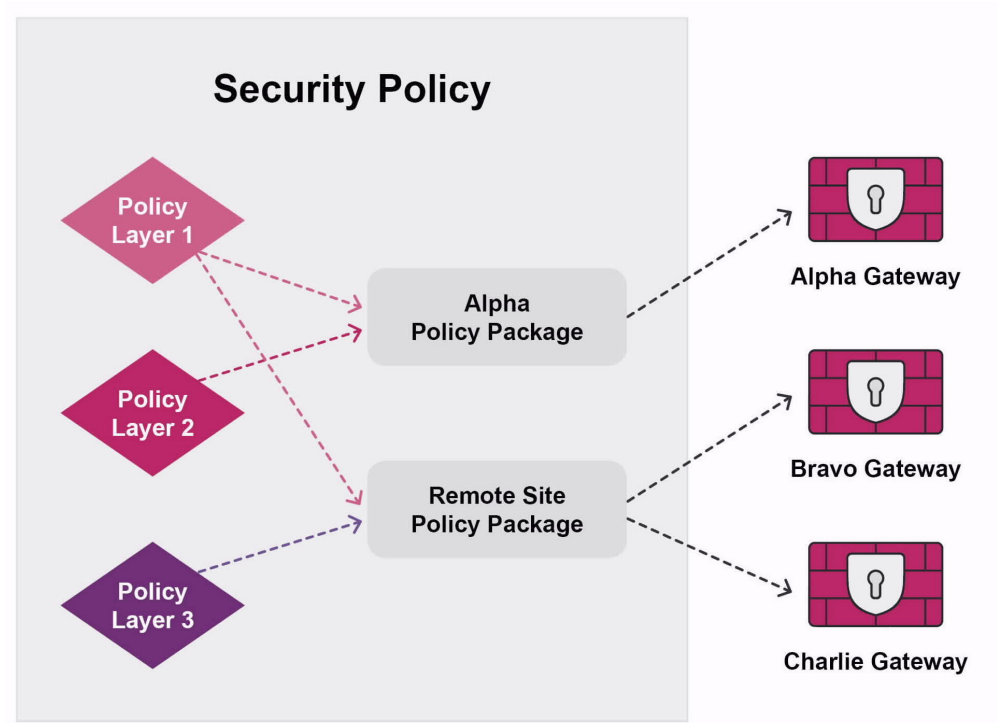
Policy Layer Concept

- Set of rules or rulebase in a policy.
- Lets you separate Security Policy into smaller, more manageable components.
- A layer can contain the following Blades:
 - Firewall (Network Access Control)
 - Application & URL Filtering
 - Content Awareness
 - Mobile Access



Benefits of Policy Layers

- Helps you visually organize the rulebase.
- Simplifies Policy management by allowing delegation of ownership of different layers.
- Improves performance by reducing the number of rules in a layer.



Ordered and Inline Layers

- Ordered layer:
 - Flat rulebase.
 - Each layer is processed sequentially for a match.
 - If an accept match is found, it is processed by the next layer until a final decision is made.
 - Can contain inline layers.
- Inline layer:
 - Sub-policy that is independent of rest of rulebase.
 - Attached to specific rules.
 - If rule is matched, inspection continues in attached sub-policy.
 - If rule is not matched, the sub-policy is bypassed.

Inspection of Policy Layers

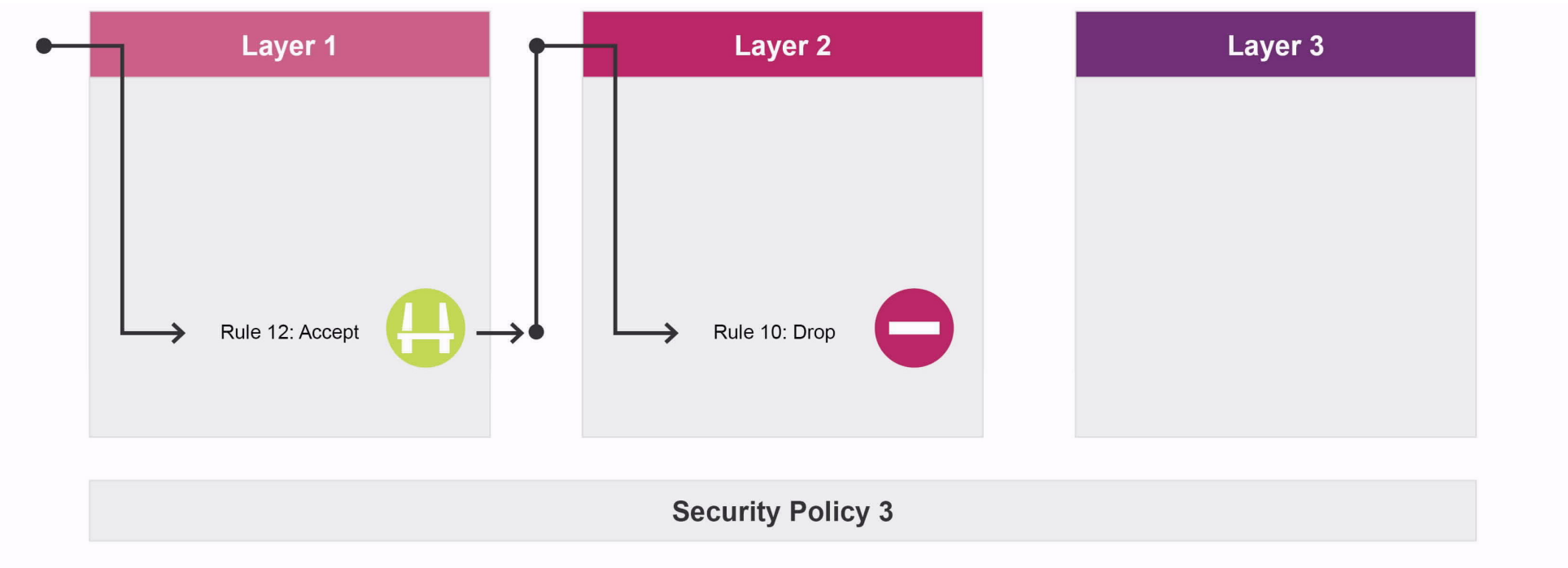
Layers

- Inspected in order they are defined.
- Exercise control over the rulebase flow and security functionality.
 - Accept action causes inspection to continue in the next layer.

Layers Concept Options

- Setting different view and edit permissions per layer.
- Reusing a layer in different places.

Ordered Layers



Inline Layers

Network Layer

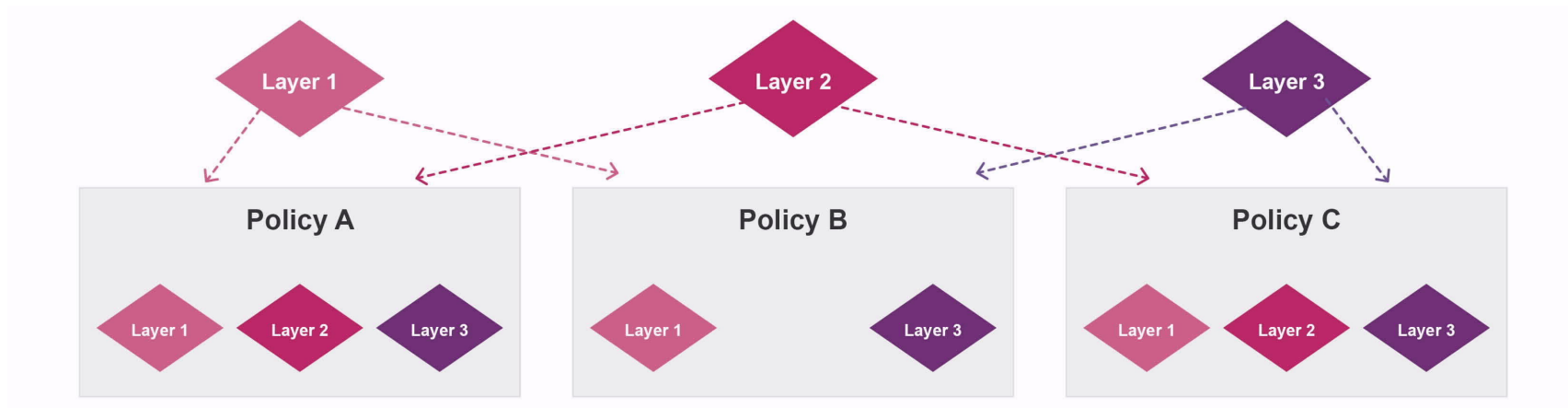
No.	Name	Action
Management Rules (1-5)		
1	Do Not Log	Drop
2	Management	URL_Filter
2.1	Corporate Standards	Drop Blocked Messa...
2.2	Log Everything	Accept
3	Remote Control	Accept
4	Stealth	Drop
5	VPN Traffic	Accept

Policy Layer Management

- Important factors to consider when creating policy layers:
 - Determine the number of layers.
 - Determine the Software Blades to enable in each layer.
 - Determine the order of rules in each layer.
 - Determine the order of layers in a policy.

Policy Layer Management (Continued)

- A policy can have one or more layers as its building blocks.
- You can move layers up/down the policy list based on security needs.
- You can also share layers in multiple policies.



Managing Policy Layers with SmartConsole

Name	Access Control	Threat Prevention	QoS	Desktop Security	Policy Targets
Bravo-Security-Zone-Policy	✓				B-GW
Standard	✓	✓			A-GW
Unified-Policy	✓				All gateways

Manage policies and layers page

Name	Number Of Rules	Comments
Branch_Office_Policy Network	8	
Customer Service Server Layer	2	
Data Center Layer	5	
Guest Exception Layer	4	
Network	15	
Public FTP Layer	2	

Managing Policy Layers with SmartConsole (Continued)

Manage policies and layers

«

Open * ✂ ✕ Actions Search...

Name	Number Of Rules	Comments	Modifier
Branch_Office_Policy Network	8		admin
Customer Service Server Layer	2		admin
Data Center Layer	5		admin
Guest Exception Layer	4		admin
Network	15		admin
Public FTP Layer	2		admin

Layer Details

Network

Blades

Used in policies

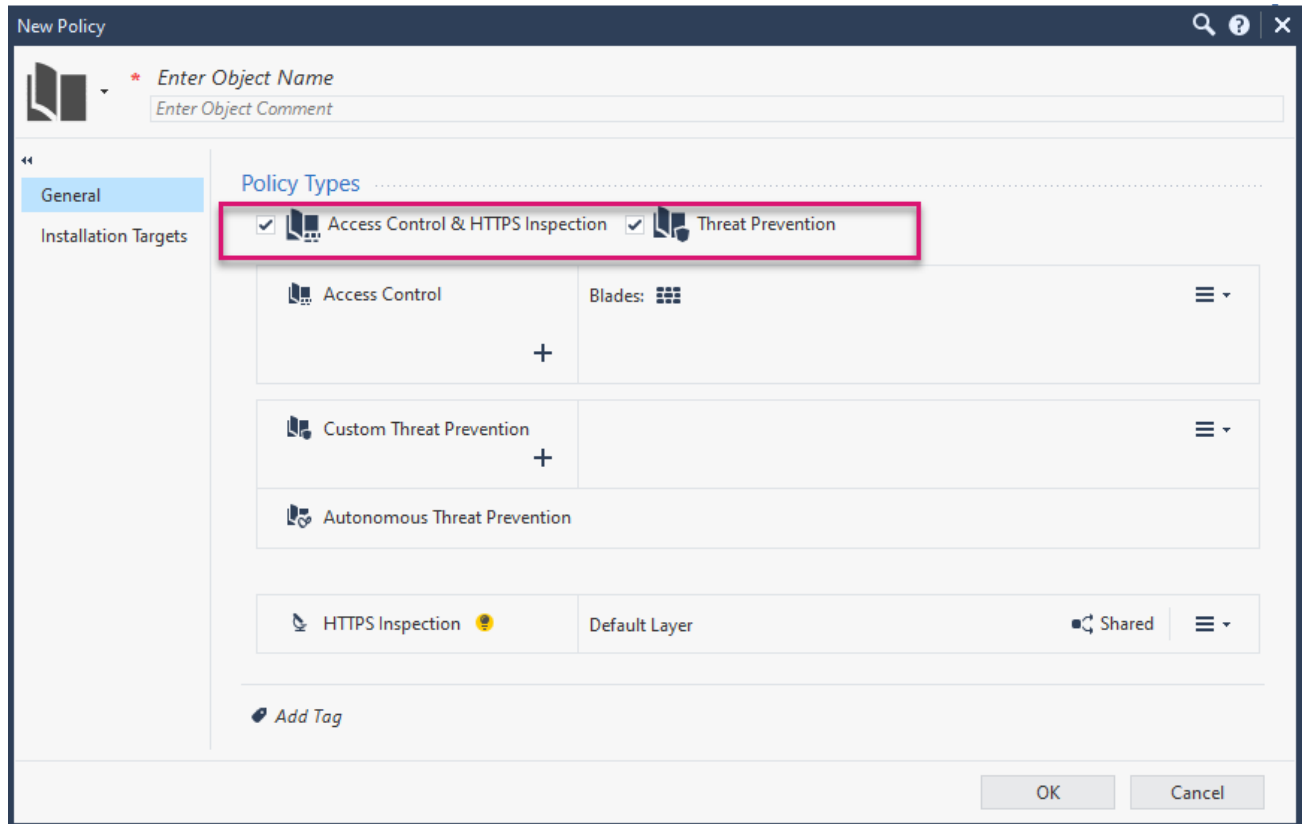
Name	Mode
Corporate_Policy	Ordered

Select a layer to view its details

Creating a New Policy Layer

From the **Application** menu:

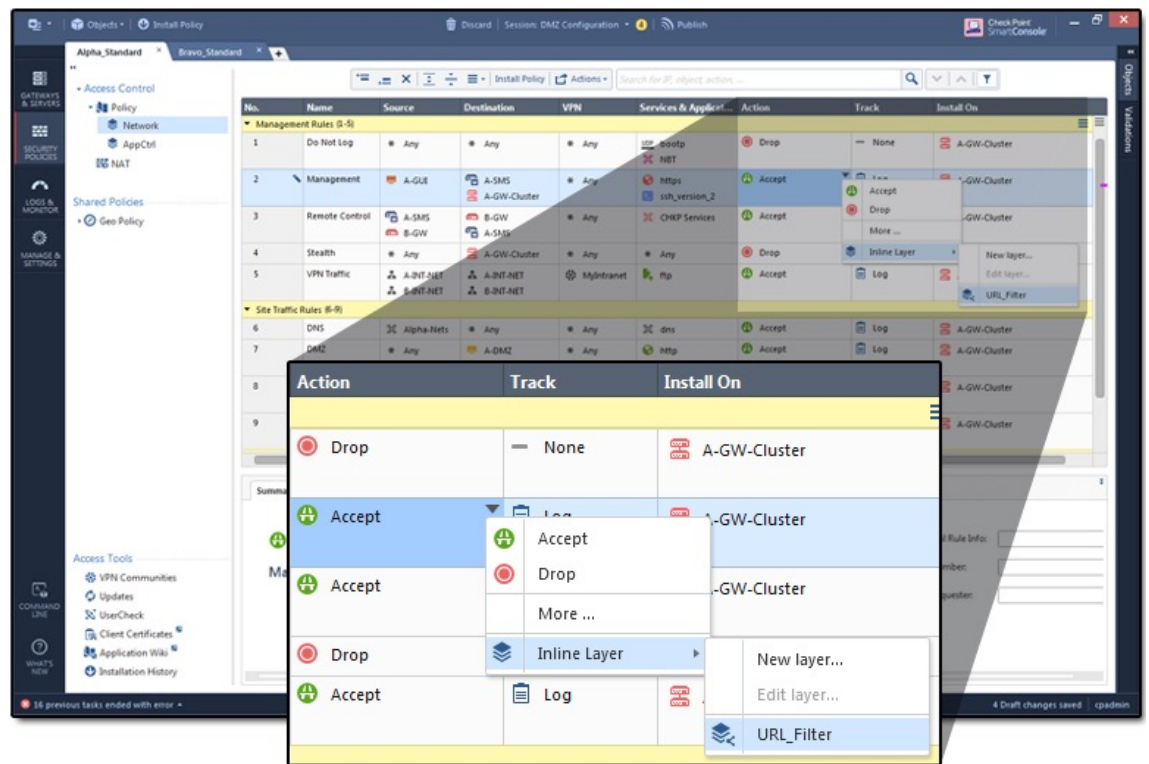
1. Select Manage policies and layers.
2. Click the **New** icon.
3. Configure policy details.



Adding an Inline Policy Layer

- Select parent rule.
- Under Action column of parent, select Inline Layer.
- Select or create new layer to be added.

Note: It is possible for a layer to function as an ordered layer in one policy package and as an inline layer in another policy package.



Modifying an Existing Policy Layer

From the **Manage policies and layers** window:

1. Select **Access Control**.
2. Open the layer and edit settings.



When possible, it is a best practice to share policy layers with other policy packages. To enable this, check the **Multiple policies and rules can use this layer** checkbox.

The screenshot shows the 'Layer Editor' window for 'Customer Service Server Layer'. The 'General' tab is selected in the left sidebar. Under the 'Blades' section, the following options are visible:

- Firewall
- Applications & URL Filtering
- Content Awareness
- Mobile Access

Below the blades is a 'Preview' table:

Destination	VPN	Services & Applications	Action

At the bottom, the 'Sharing' section has the checkbox Multiple policies and rules can use this layer, which is highlighted by a red arrow.

Exporting Layer Rules

To export to a CSV file:

1. Select **Menu** → **Manage policies and layers**.
2. Select a layer and then select **Actions** → **Export**.
3. Type a path and file name.



Review Questions

1. What is the purpose of Policy layers?
2. What type of Policy layer is independent of the rest of the rulebase?

Lab 6A

Configuring Ordered Layers



Lab 6B

Configuring a Shared Inline Layer

