

Check Point®  
SOFTWARE TECHNOLOGIES LTD

# NEXT GENERATION POLICY MANAGEMENT

## R80.10 Training

**R80.10**

Technologies Training Material

楊松倫 Sung Yang | 資安工程師 Security Engineer, Taiwan

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

POWERED BY  CHECK POINT  
**INFINITY**

CLOUD • MOBILE • THREAT PREVENTION

# Agenda

- Check Point Security Management Architecture
- Unified Access Policy - Layers
  - Ordered Layers
  - Inline Layers
- Content Awareness
- Security Zones
- Domain Objects
- Threat Prevention





Check Point®  
SOFTWARE TECHNOLOGIES LTD

# CHECK POINT SECURITY MANAGEMENT ARCHITECTURE

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION

# Check Point Security Management Architecture

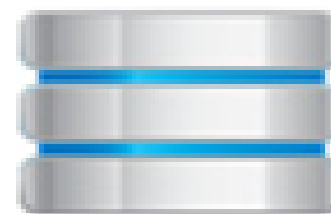
Three essential components of a secure network:



# Check Point Firewall Architecture

## Security Management Server

- security policy is defined using the policy editor on the Management client
- it is then saved to the Security Management Server
- SmartCenter Server maintains FW-1 NG databases including
  - network object definitions
  - user definitions
  - security policy
  - log files



**Security Management Server**

# Check Point Firewall Architecture

## Security Gateway

- Deployed on the Internet gateway
- An Inspection script written in INSPECT is generated from the security policy
- Inspection code is compiled from the script and downloaded to the enforcement module






Security Gateway

# Standalone

## Standalone Deployment

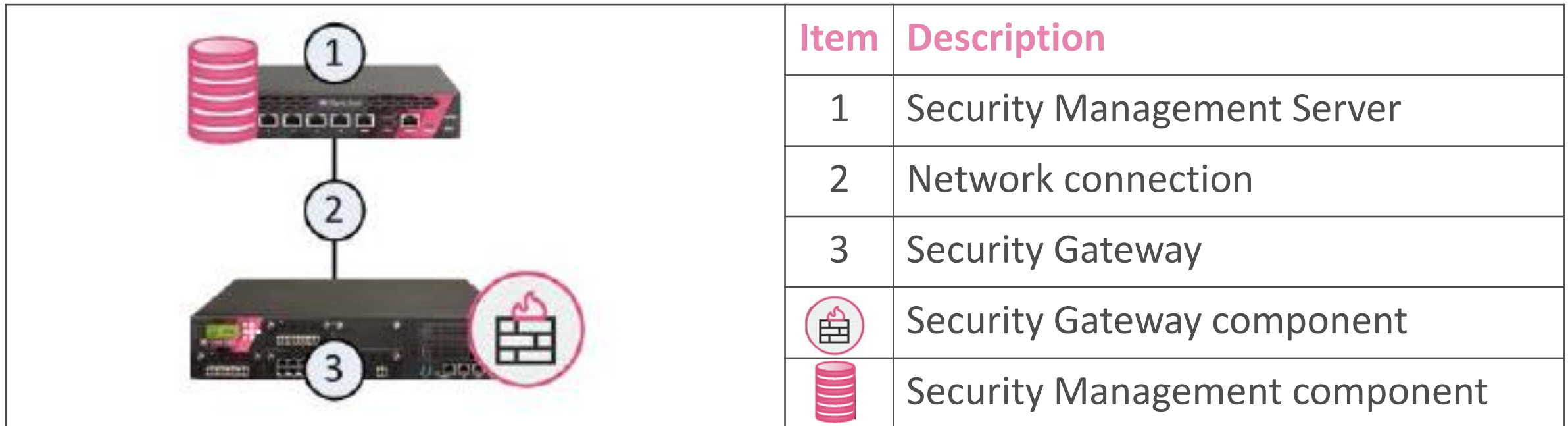
The Security Management Server (1) and the Security Gateway (3) are installed on the same computer or appliance (2).

	Item	Description
	1	Security Management Server
	2	All-in-one appliance
	3	Security Gateway
		Security Gateway component
		Security Management component

# Distributed Deployment

## Distributed Deployment

The Security Management Server (1) and the Security Gateway (3) are installed on different computers or appliances, with a network connection (2).

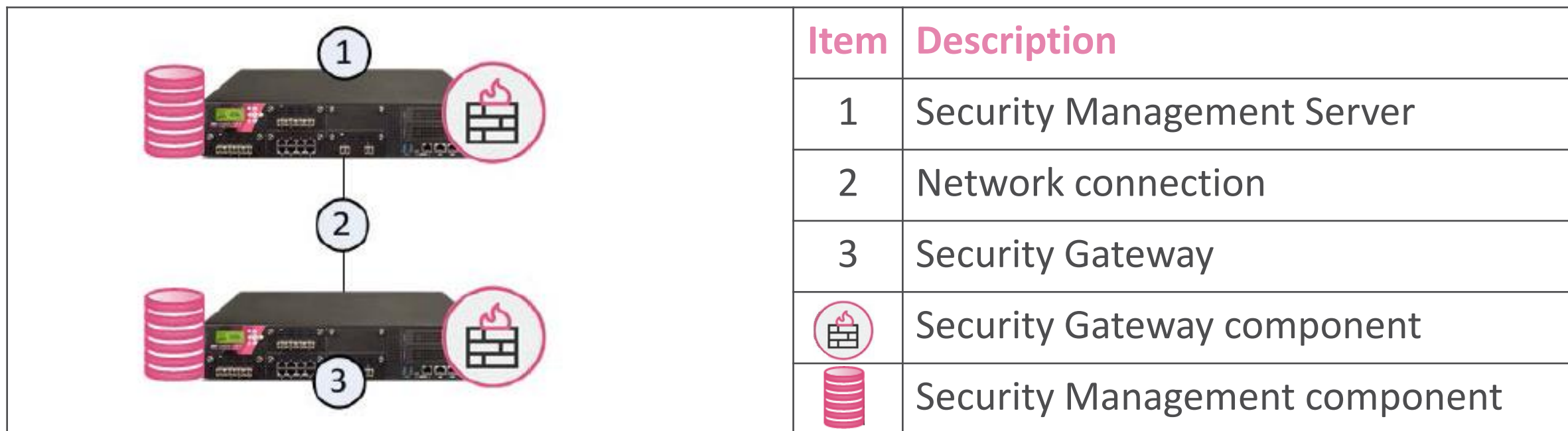




# Standalone Full HA Deployment

## Standalone Full HA

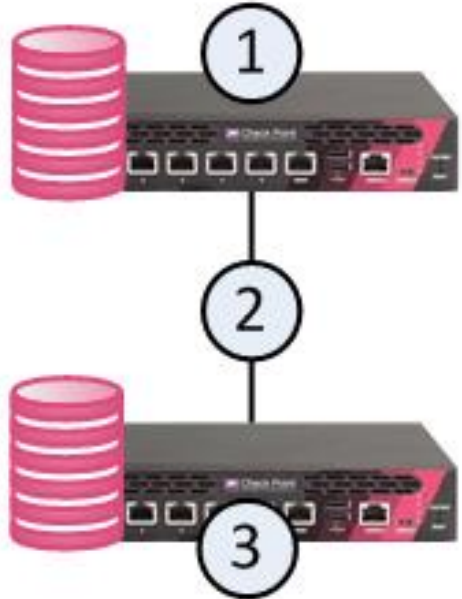

Security Management Server and Security Gateway are each installed on one appliance, in a standalone deployment. One standalone appliance is Primary (1), and one is Backup (3). The two appliances are connected with a direct connection (2) and work in High Availability mode.



# Management HA

## Management HA

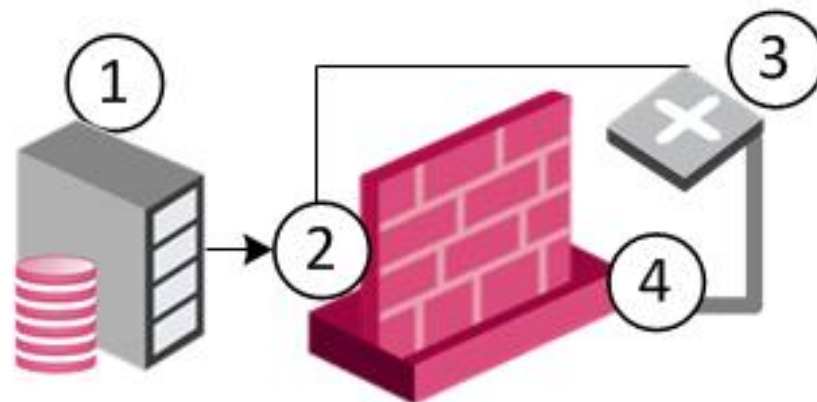
A Primary Security Management Server (1) has a direct or indirect connection (2) to one or more Secondary Security Management Servers (3).

	<b>Item</b>	<b>Description</b>
1	Primary Security Management Server	
2	Direct or indirect Security Management server to Security Management server connection	
3	Secondary Security Management server	
	Security Management component	



# Routing(NAT) Mode

- All externally accessible servers should be located in the DMZ.
- Clean up ARP cache on Broadcast Domain when replace gateway.



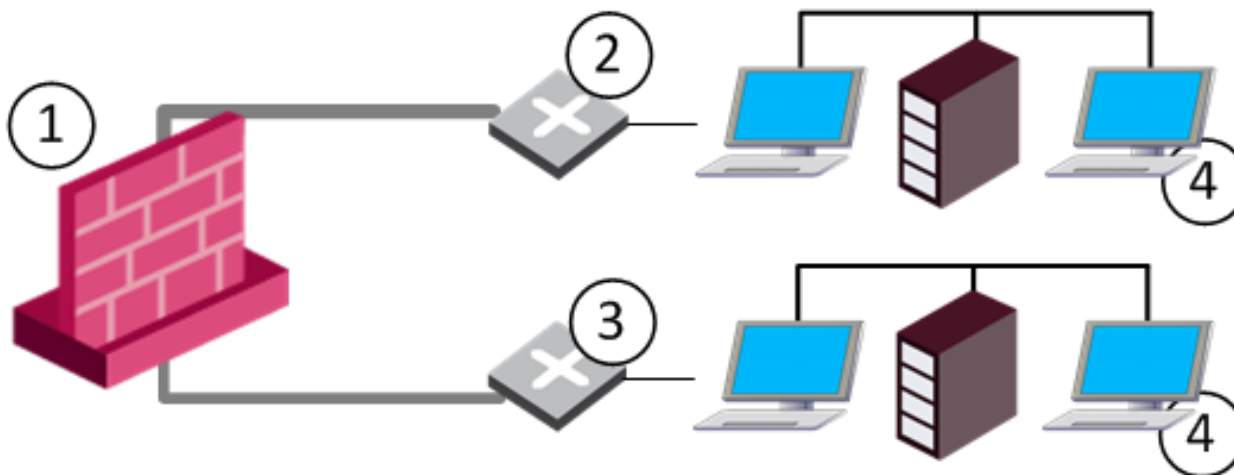
Item	Description
1	Security Management Server sends management packet to management interface
2	Management interface on Security Gateway Firewall bridging Layer-2 traffic inspects the packet and sends it to the router
3	Router sends the packet to the bridge interface
4	Bridge interface drops the packet as a retransmission

Configure the Security Gateway to handle management packets properly.



# Bridge Mode

- A bridge mode deployment adds a Security Gateway to an existing environment without changing IP Routing.



Item	Description
1	Security Gateway bridges Layer-2 traffic over one IP address, with a subnet on each side, using the same address
2	Switch from a bridged interface to a subnet
3	Switch from a second bridged interface to a second subnet
4	Internal network



# Important Note of Bridge Mode.(1)

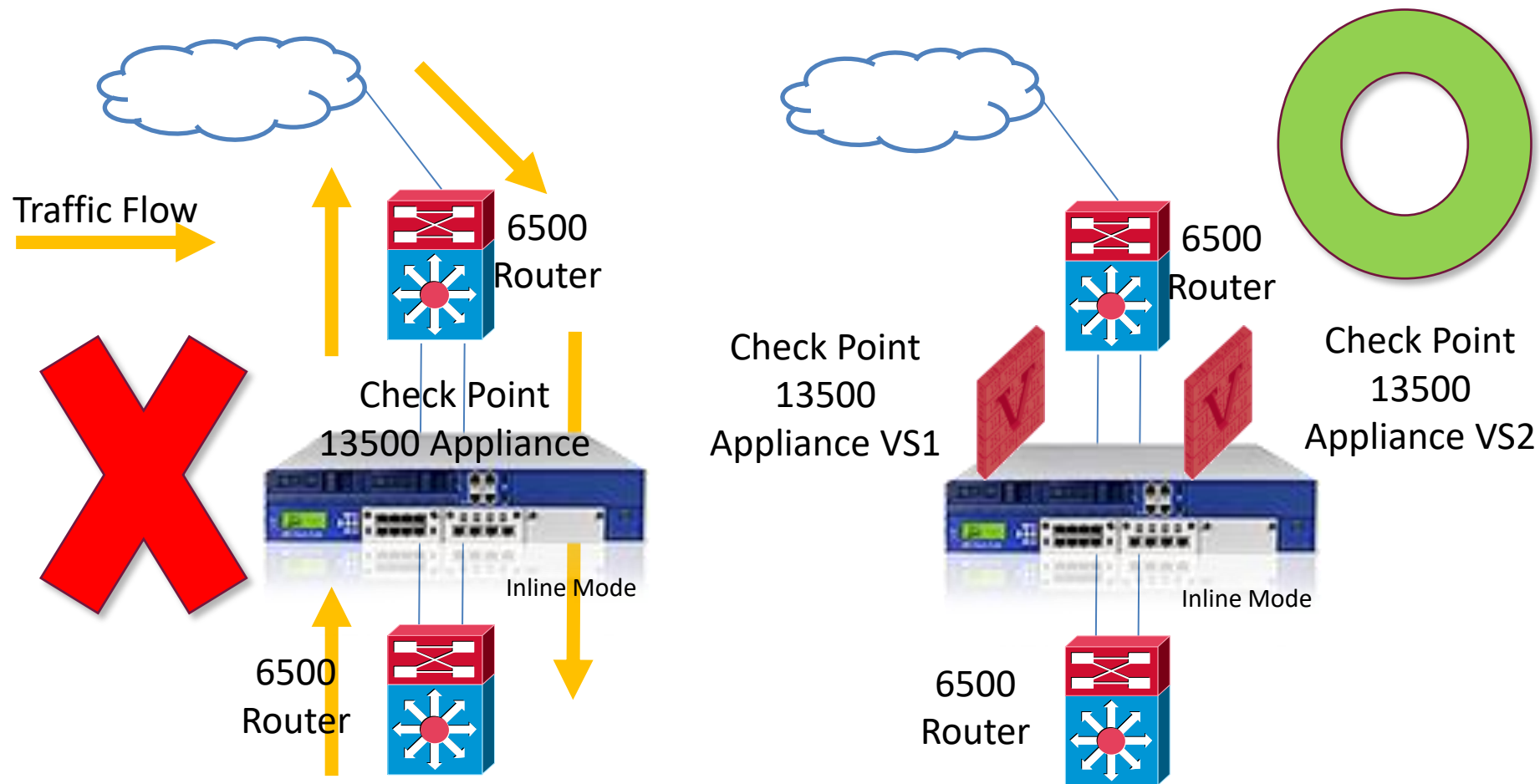
- Only two interfaces can be connected by a single Bridge interface. These two interfaces can then be thought of as a two-ports switch. Each port can be a **physical**, **VLAN**, or **bond device**.
- Only one IP address could be configuration on Bridge Interface.

These features, Software Blades and deployments are **not** supported in Bridge Mode:

- Mobile Access Software Blade
- IPSec VPN Software Blade
- Full High Availability deployment
- NAT on Security Gateways
- Access to Portals from bridged networks, if the bridge does not have an assigned IP address
- Assigning IP address on bridge in clusters is not supported
- Anti-Virus in Traditional Mode
- Identity Awareness authentication other than AD Query (AD Query is the only supported authentication)
- ClusterXL in R75.40 and lower / R75.45 / R75.46 / R75.47
- Asymmetric traffic inspection on Layer 2 Active/Active cluster deployment is not supported (asymmetric traffic inspection is any situation, where the Client-to-Server packet is inspected by one cluster member, while the Server-to-Client packet is inspected by the other member. In such scenarios several security features will not work)



# Important Note of Bridge Mode.(2)





# Important Note of Bridge Mode.(3)

To enable management over the bridge:

1. Edit `$FWDIR/boot/modules/fwkernel.conf`.  
If necessary, create this file.

2. Add the appropriate line to the file:

- For IPv4 traffic -

```
fwx_bridge_reroute_ipv4=<management>
```

- For IPv6 traffic -

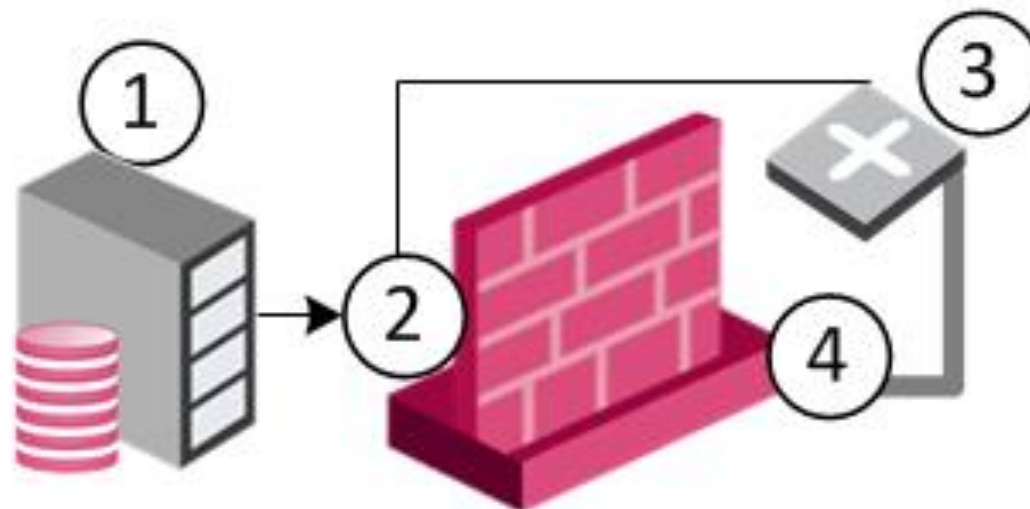
```
fwx_bridge_reroute_ipv6=<management>
```

<management> is the IP address of the management interface.

- Allow Ethernet frames with any protocol

```
fwaccept_unknown_protocol=1
```

3. Reboot the Security Gateway.



Item	Description
1	Security Management Server sends management packet to management interface
2	Management interface on Security Gateway Firewall bridging Layer-2 traffic inspects the packet and sends it to the router
3	Router sends the packet to the bridge interface
4	Bridge interface drops the packet as a retransmission

Configure the Security Gateway to handle management packets properly.

# Bridge Mode Support Blades List

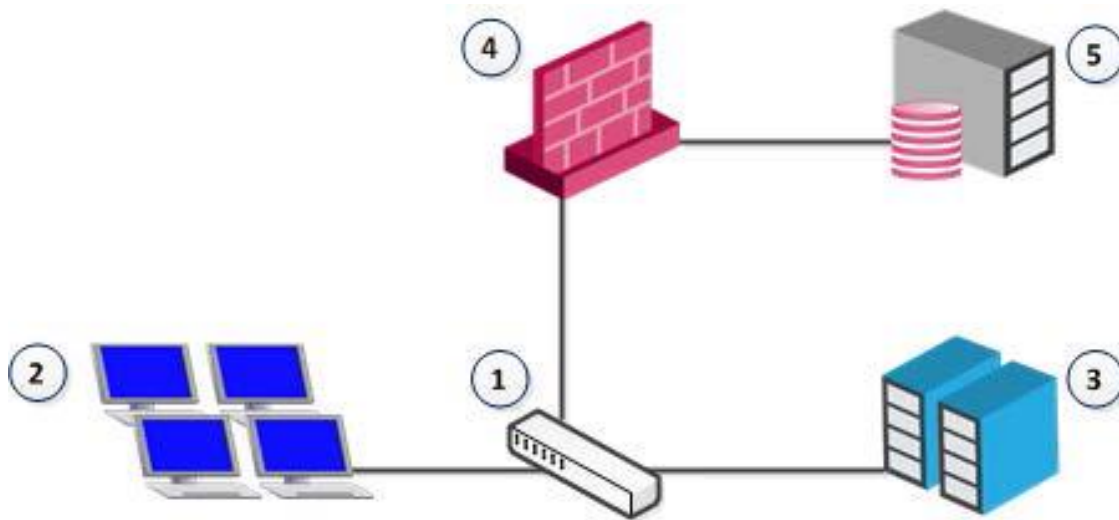
## Security Gateway blades

Bridge mode is **fully supported** (unless stated otherwise) on Gaia / SecurePlatform OS by the following blades for single Security Gateway deployment, for cluster with one switch in Active/Active and Active/Standby deployment, and for cluster with four switches:

Blade	Comments for Gateway mode	Comments for VSX mode
Firewall	Yes	Yes
IPS	Yes	Yes
URL Filtering	Yes	Yes
Data Loss Prevention	Yes	No
Anti-Bot	Yes	Yes
Anti-Virus	Yes	Yes
Application Control	Yes	Yes
HTTPS Inspection	Yes	No
Identity Awareness	Yes	No
Threat Emulation	Yes	Yes
UserCheck	Yes	No
QoS	Yes (see <a href="#">sk89581</a> )	No (see <a href="#">sk79700</a> )
HTTP / HTTPS proxy	Yes	No
SMTP / HTTP / FTP / POP3 Security Servers	Yes	No
Client Authentication	Yes	No
User Authentication	Yes	No



# Monitor(Sniffer) Mode



You can use mirror ports in these scenarios:

- To monitor the use of applications as a permanent part of your deployment
- To evaluate the capabilities of the Application Control and IPS blades before you buy them

Item	Description
1	Switch with mirror port
2	Computers
3	Servers
4	Security Gateway in monitor mode
5	Management for Security Gateway

# The SmartConsole

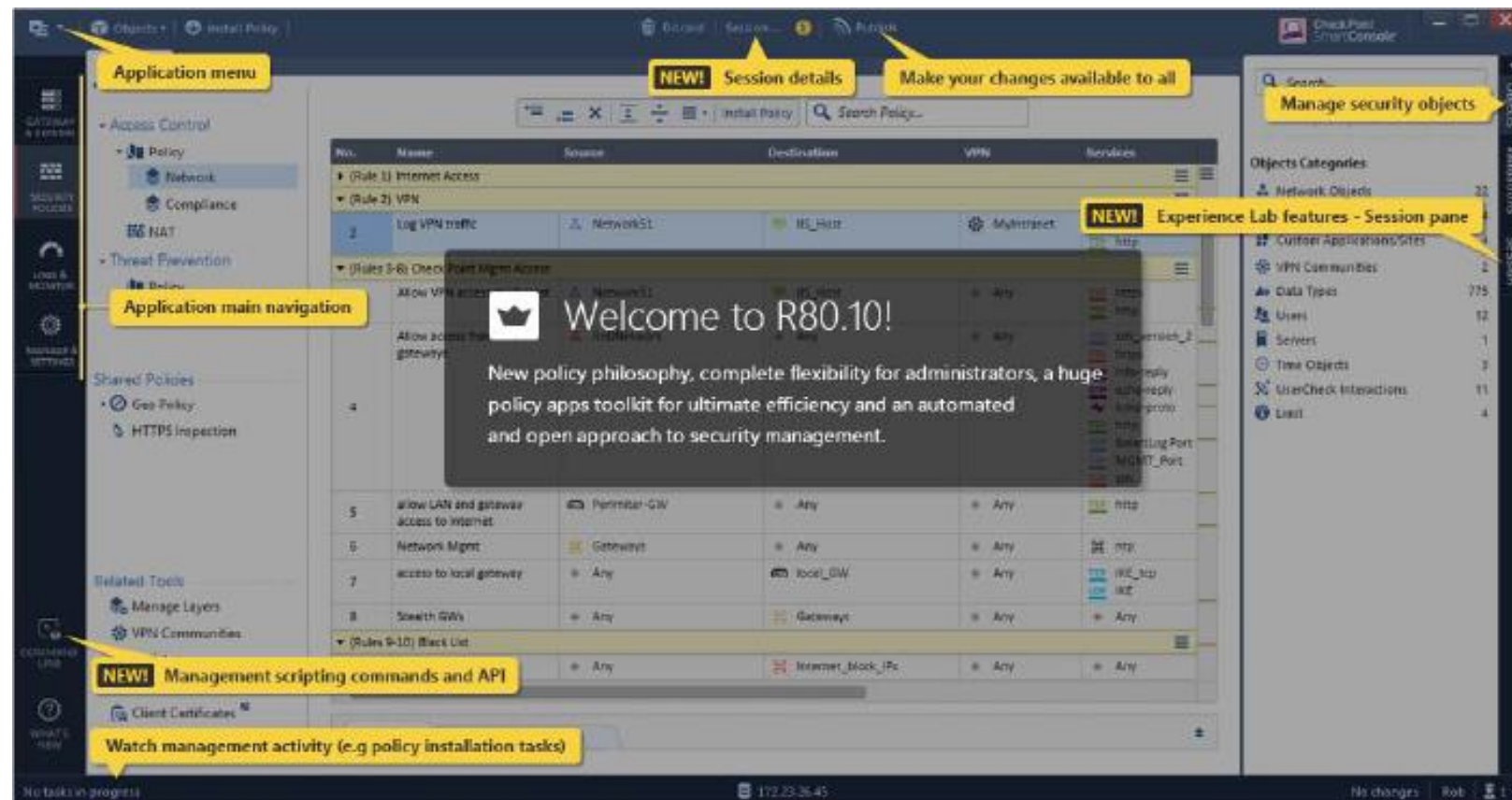


- Manage security policies
- Monitor events
- Install updates
- Add new devices and appliances
- Manage multi-domain environments



# Navigation Pane Overview

- Application Menu
- Application main Navigation
- Session details and action
- Objects management



# Gateways & Servers

- Server Status
- Module version
- Active software blades
- CPU usage
- Object summary



The screenshot shows the 'Gateway & Servers' management interface. At the top, there are three callouts: 'Create a new Gateway', 'Run scripts on selected gateways', and 'Filter the gateways list'. Below these is a table of gateways with columns for Name, Version, Active Blades, Hardware, CPU Usage, Available Up..., and Comments. A callout 'Select between predefined views' points to the 'Columns' dropdown. A large callout box titled 'Gateway & Servers' contains the text: 'Manage your Security Gateways. Configure blade activation, view gateway status and perform actions on gateways.' Below this, a callout 'More information on the selected gateway' points to the 'local\_GW' summary card. This card displays details for 'local\_GW' including IP Address (192.168.33.4), Policy Name (Standard Package), Last Install Date (06-01-2014 09:16:27), OS (Goia), and Version (Hero). It also shows 'Open server' status, CPU usage (2%), and Memory usage (40%). A callout 'Additional monitoring information' points to the CPU and Memory bars. On the right side of the summary card, there are sections for 'Access Blades' (Firewall, Site to Site VPN) and 'Threat Blades' (IPS). At the bottom, there are links for 'Device & Licenses Information...' and 'Activate Blades...'. The status bar at the bottom indicates 'No tasks in progress' and the IP address '172.23.36.45'.

Name	Version	Active Blades	Hardware	CPU Usage	Available Up...	Comments
local_GW	Hero	4	Open server		N/A	
Perimeter-GW	Hero	75	Open server		N/A	
Perimeter-rat-fake-21	Hero	1	Open server		N/A	

# Security Policies Tab



- Access Control Policy
- Threat Prevention Policy
- Shared Policy
- Install Policy Button



# Logs & Monitor Tab



- Gateway Statistics
- Infected hosts summary

**View and analyze system logs**

**Logs & Monitor**

**Your full visibility to your security:**

- View high level Graphs and pivots in a simple and intuitive dashboard
- Search through logs
- Schedule periodic customizable reports
- Monitor your Gateways

Blade	Reported by (Gateways)
148	12 Origins
179	5 Origins
302	6 Origins
63	12 Origin
89	5 Origins

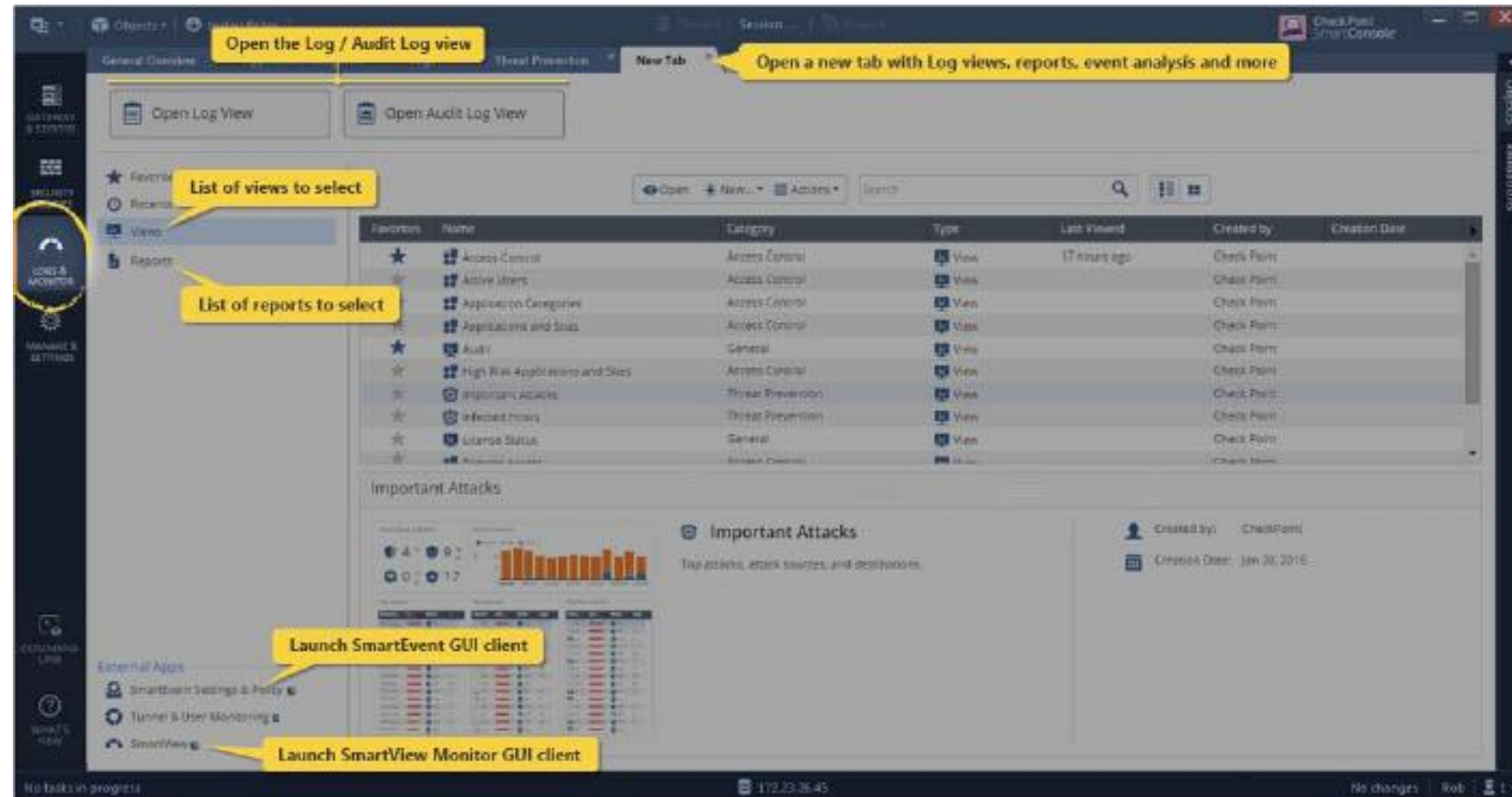
Timeline: Security Incidents (High, Critical)

Timeline Data: Tue 24 (213), Wed 25 (190), Thu 26 (96), Fri 27 (228), Sat 28 (261), Sun 29 (375), Mon 30 (12), Tue 1

# Logs & Monitor Tab



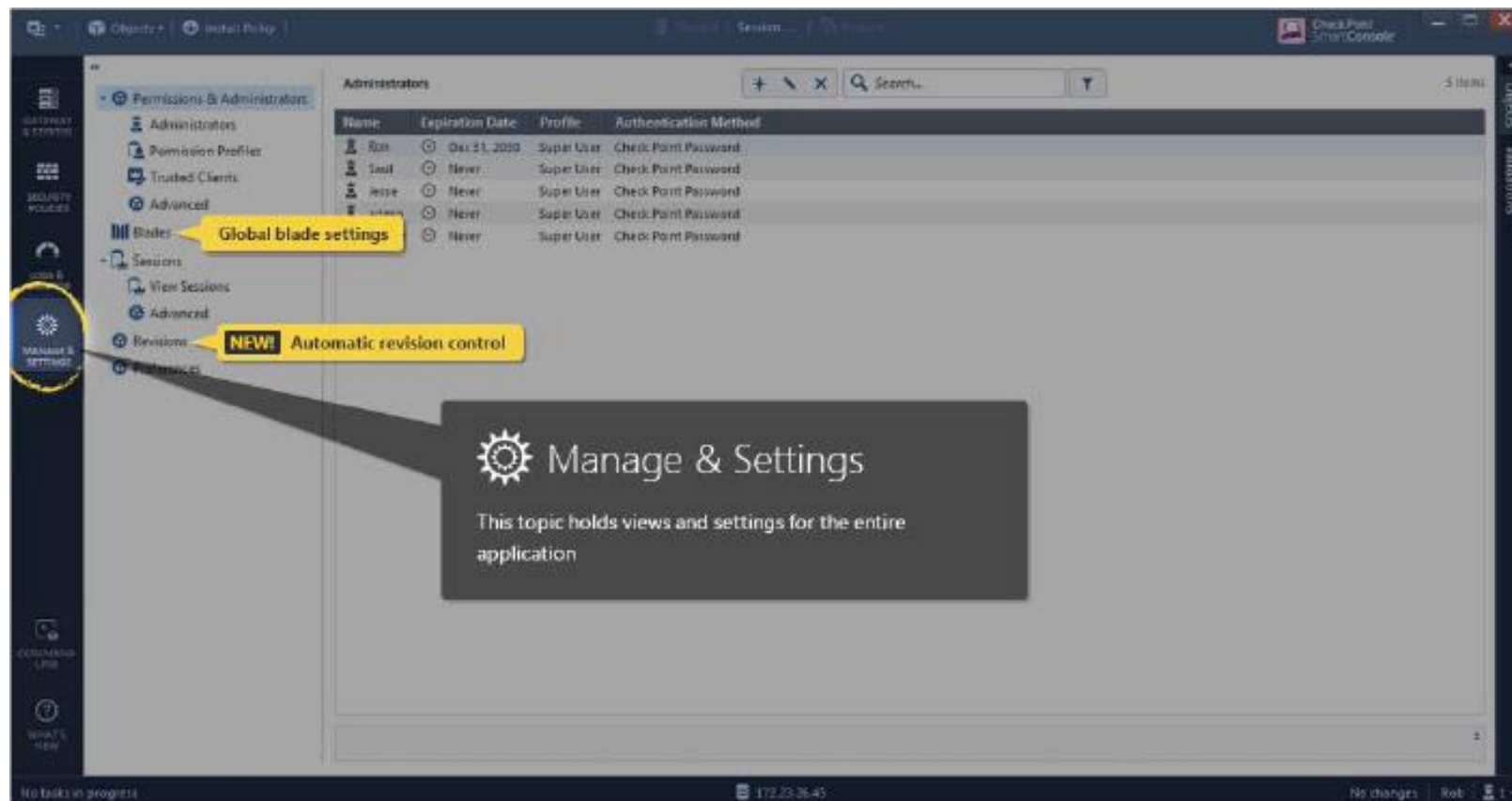
- Log views & reports
- Event Analysis
- Link to launch SmartEvent GUI Client
- Link to launch SmartView Monitor GUI Client





# Manage & Settings Tab

- Administrators
- Permission profiles
- Global software blades setting
- Automatic Security Policy revision control

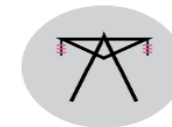




# Deployment Platforms

## Check Point Appliances

- Small Business and Branch Office
- Enterprise Network Security
- Data Center Security Systems
- Chassis Systems
- Rugged Appliances, and more



# Introduction to Gaia

- IPv4 and IPv6 network protocol
- High Connection and Virtual Systems Capacity (64 bits)
- Load Sharing
- High Availability
- Dynamic and Multicast Routing

**Check Point's operating system for all Check Point appliances and open servers.**



# Command Line Interface (CLI)

- Can be used via SmartConsole or Web browser.
- Default shell is called clish.
- Expert mode allows advanced system and Linux function access to the system.

```
Enter expert password:  
  
Warning! All configuration should be done through clish  
You are in expert mode now.  
  
[Expert@A-GW-01:0]# exit  
exit  
A-GW-01> _
```

# Gaia Commands

Commands have the following syntax: **operation feature parameter**

- To view all commands that the user has permissions to run:  
**show commands**
- To view a list of all features:  
**show commands feature <TAB>**
- To show all possible operations:  
**show commands op <SPACE> <TAB>**
- To show the full system version information:  
**show version all**



# Obtaining a Configuration Lock

- Only one user can have read/write access to Gaia configuration settings at a time.
- The database feature has two commands:
  - lock database override**
  - unlock database**
- Both commands obtain the configuration lock from another administrator.

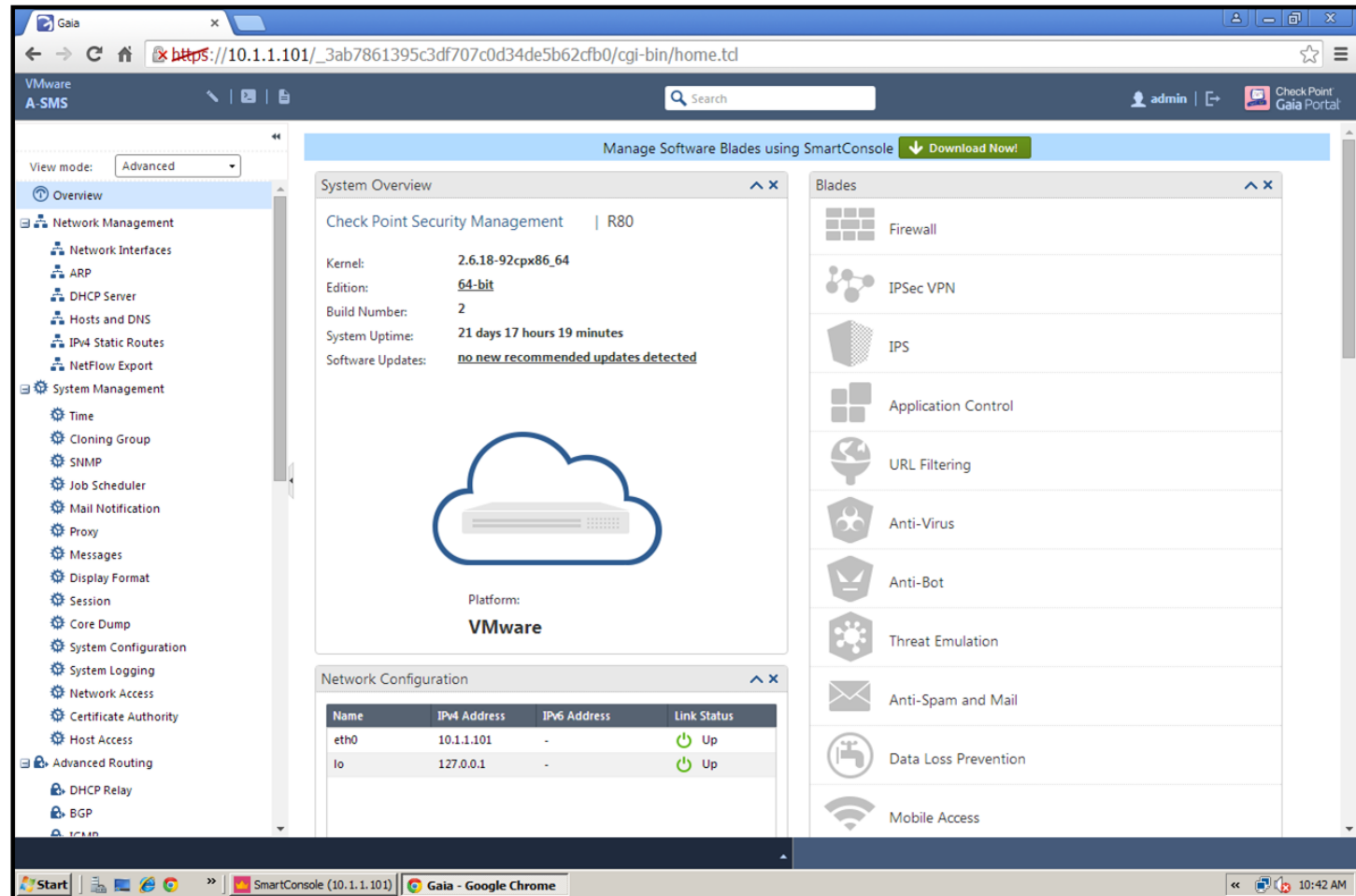


# WebUI

An advanced, web-based interface used to configure Gaia platforms.

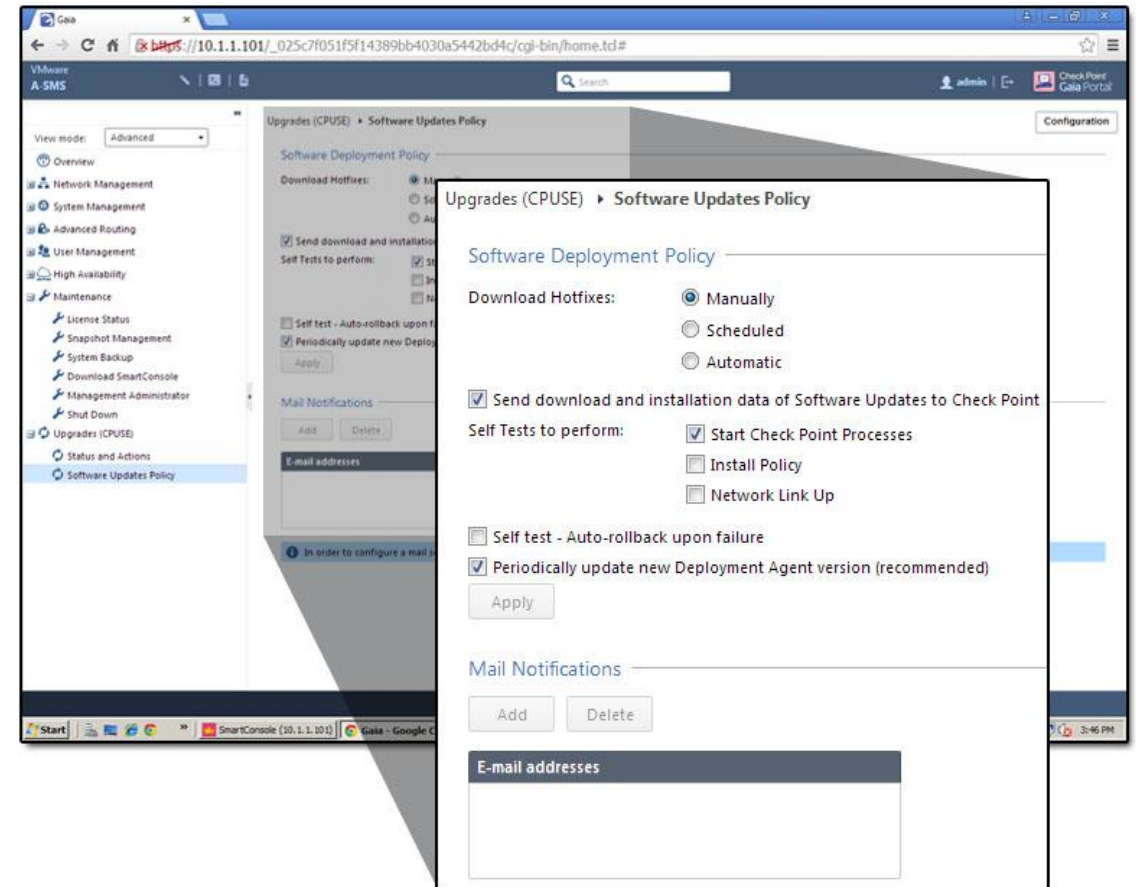
Two modes:

- Simplified
- Advanced



# Updates

- Automatically update Check Point Gaia and products using the Check Point Upgrade Service Engine (CPUSE)



# SECURITY POLICY MANAGEMENT



# Rules

No.	Name	Source	Destination	VPN	Services & Applications	Data	Action	Track
1	Enable open shell and open WebUI from management	mgmt	Gateways_Group	* Any	http	* Any	Accept	None
2	Stealth rule	* Any	mgmt Gateways_Group	* Any	* Any	* Any	Drop	None
<b>Internet Access (3-7)</b>								
3	Drop high risk applications	* Any	* Any	* Any	High Risk Critical Risk	* Any	Drop	None
4	Sales Operations Policy	Sales Operations	* Any	* Any	* Any	* Any	Sales Operations Pol	None
4.1	Allow Sales Operations to access Share Portal	* Any	Internet	* Any	Office 365	Any Direction Document...	Accept	None
4.2	Cleanup Rule	* Any	* Any	* Any	* Any	* Any	Drop	None
5	File Sharing - user check	* Any	Internet	* Any	File Storage and Sh...	* Any	Ask CompanyPolicy	None

Comprised of network objects such as Security Gateways, hosts, networks, routers and domains, and specifies the source, destination, service and action to be taken for each session.

# Default Rule



No.	Hits	Name	Source	Destination	VPN	Services & A...	Action	Track	Install On	Time
1	0	Stealth Rule	* Any	A-GW-0...	* Any	* Any	Drop	Log	* Policy...	* Any
2	0	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy...	* Any

Recommend to using for all rules.

# Objects



Objects are divided into the following categories:

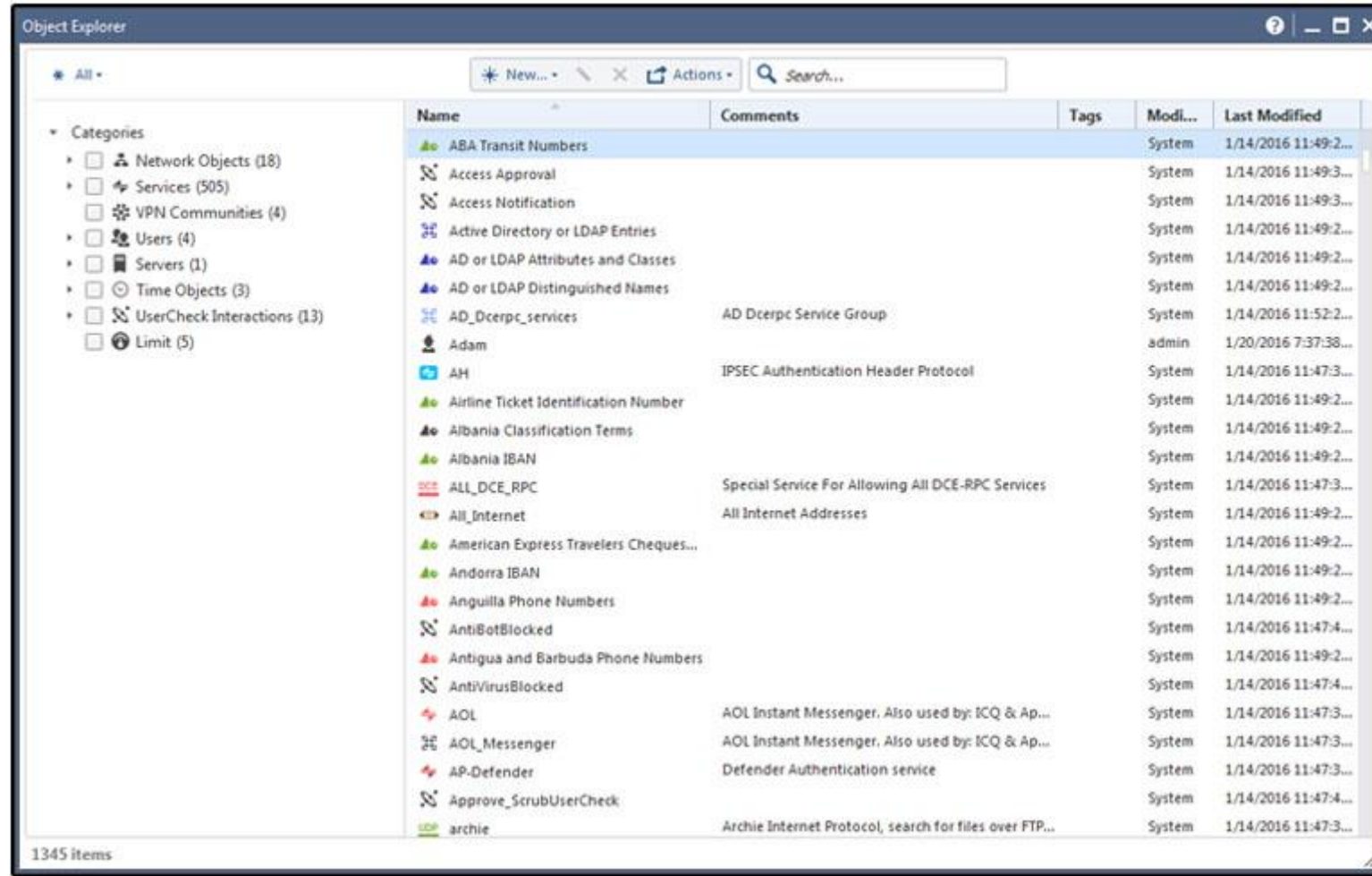
- Network Object
- Service
- Custom Application/Site
- VPN Community
- User
- Server
- Resource
- Time Object
- UserCheck Interactions
- Limit



When creating objects, consider organizational needs:

- What are the physical and logical components that make up the organization?
- What components will access the Firewall?
- Who are the users and how should they be grouped?
- Who are the Administrators and what are their roles?
- Will VPN be used? If so, will it allow remote users?

# Objects Management



The screenshot shows the 'Object Explorer' window with a tree view on the left and a table of objects on the right. The table has columns for Name, Comments, Tags, Modified, and Last Modified. The 'All' category is selected, showing 1345 items.

Name	Comments	Tags	Modi...	Last Modified
ABA Transit Numbers			System	1/14/2016 11:49:2...
Access Approval			System	1/14/2016 11:49:3...
Access Notification			System	1/14/2016 11:49:3...
Active Directory or LDAP Entries			System	1/14/2016 11:49:2...
AD or LDAP Attributes and Classes			System	1/14/2016 11:49:2...
AD or LDAP Distinguished Names			System	1/14/2016 11:49:2...
AD_Dcerpc_services	AD Dcerpc Service Group		System	1/14/2016 11:52:2...
Adam			admin	1/20/2016 7:37:38...
AH	IPSEC Authentication Header Protocol		System	1/14/2016 11:47:3...
Airline Ticket Identification Number			System	1/14/2016 11:49:2...
Albania Classification Terms			System	1/14/2016 11:49:2...
Albania IBAN			System	1/14/2016 11:49:2...
ALL_DCE_RPC	Special Service For Allowing All DCE-RPC Services		System	1/14/2016 11:47:3...
All_Internet	All Internet Addresses		System	1/14/2016 11:49:2...
American Express Travelers Cheques...			System	1/14/2016 11:49:2...
Andorra IBAN			System	1/14/2016 11:49:2...
Anguilla Phone Numbers			System	1/14/2016 11:49:2...
AntiBotBlocked			System	1/14/2016 11:47:4...
Antigua and Barbuda Phone Numbers			System	1/14/2016 11:49:2...
AntiVirusBlocked			System	1/14/2016 11:47:4...
AOL	AOL Instant Messenger. Also used by: ICQ & Ap...		System	1/14/2016 11:47:3...
AOL_Messenger	AOL Instant Messenger. Also used by: ICQ & Ap...		System	1/14/2016 11:47:3...
AP-Defender	Defender Authentication service		System	1/14/2016 11:47:3...
Approve_ScrubUserCheck			System	1/14/2016 11:47:4...
archie	Archie Internet Protocol, search for files over FTP...		System	1/14/2016 11:47:3...



# Security Zones

Topology Settings

**Leads To**

- This Network (Internal)
- Override
  - Internet (External)
  - This Network (Internal)  
IP Addresses behind this interface:
    - Not defined
    - Network defined by the interface IP and Net Mask
    - Specific:
    - Interface leads to DMZ

**Security Zone**

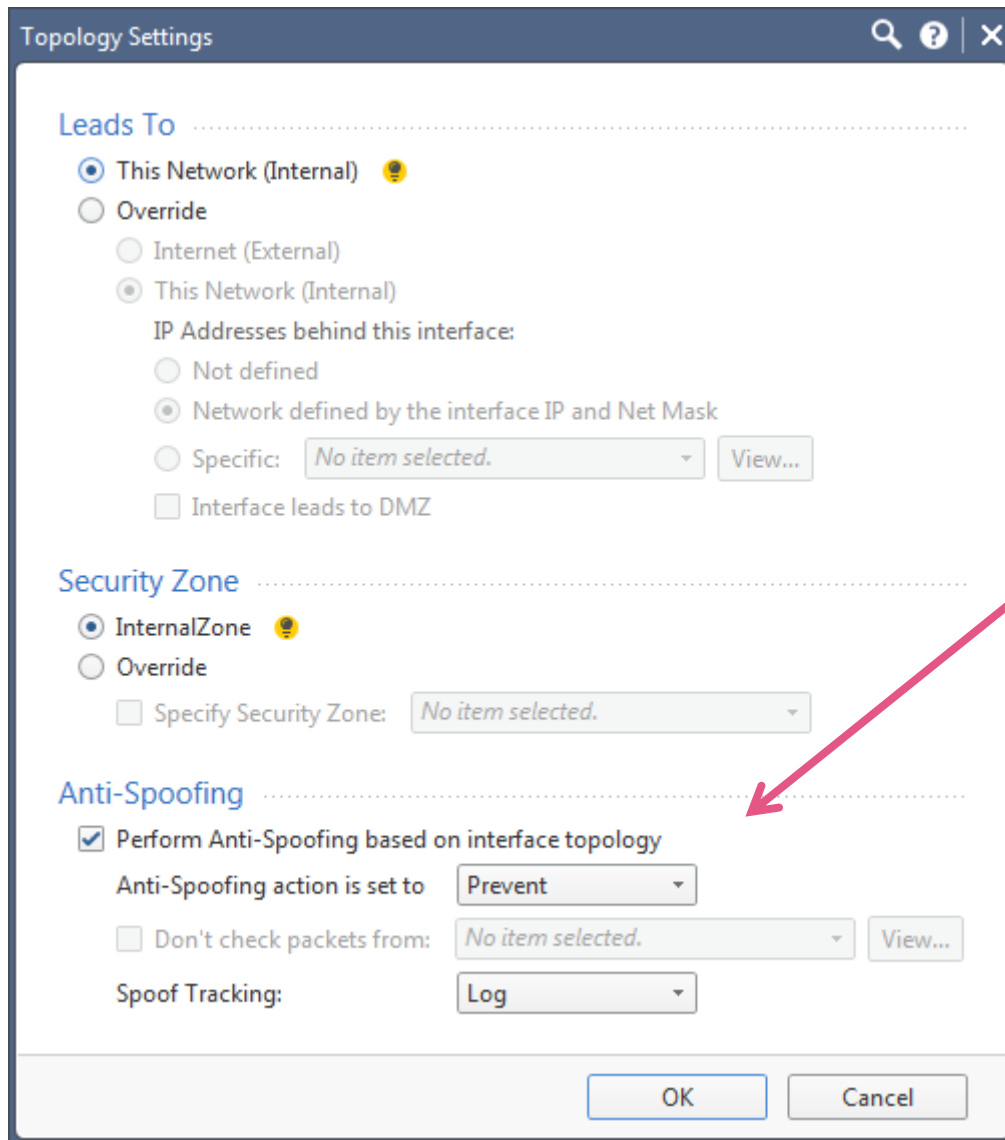
- InternalZone
- Override
  - Specify Security Zone:

**Anti-Spoofing**

- Perform Anti-Spoofing based on interface topology
  - Anti-Spoofing action is set to
  - Don't check packets from:
  - Spoof Tracking:

A group of one or more network interfaces bound together and used directly in the Rule Base.

# Anti-Spoofing



Topology Settings

Leads To

- This Network (Internal) ⚠
- Override
  - Internet (External)
  - This Network (Internal)
    - IP Addresses behind this interface:
      - Not defined
      - Network defined by the interface IP and Net Mask
      - Specific:
    - Interface leads to DMZ

Security Zone

- InternalZone ⚠
- Override
  - Specify Security Zone:

Anti-Spoofing

- Perform Anti-Spoofing based on interface topology
  - Anti-Spoofing action is set to
  - Don't check packets from:
  - Spoof Tracking:

Anti-Spoofing should be configured on all Gateway interfaces to be most effective.



# The Rule Base

No.	Hits	Name	Source	Destination	VPN	Services & A...	Action	Track	Install On	Time
1	0	Stealth Rule	* Any	A-GW-0...	* Any	* Any	Drop	Log	* Policy...	* Any
2	0	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy...	* Any

- The Rule Base is a collection of individual rules which builds the Security Policy.
- The Cleanup Rule determines how to handle unmatched connections.
- The Stealth Rule is to prevent any users from connecting directly to the Security Gateway.
- Explicit Rules are created by the administrator.
- Implicit Rules are defined by the Security Gateway and are not visible in the Rule Base.

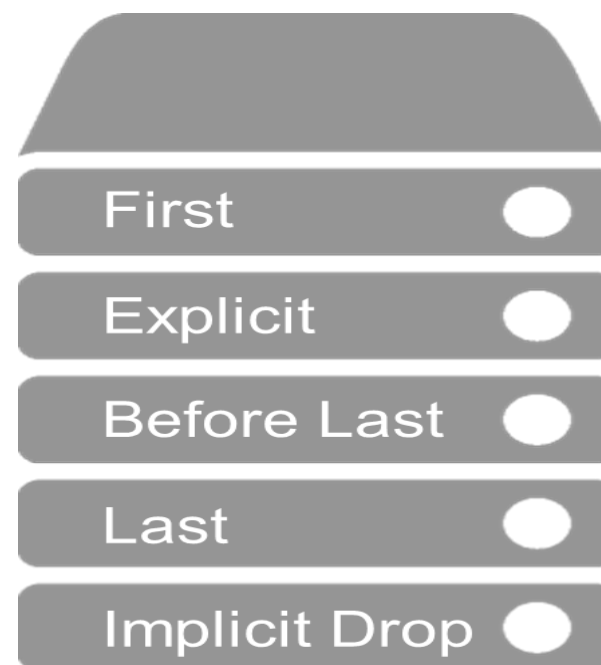


# Implied Rules

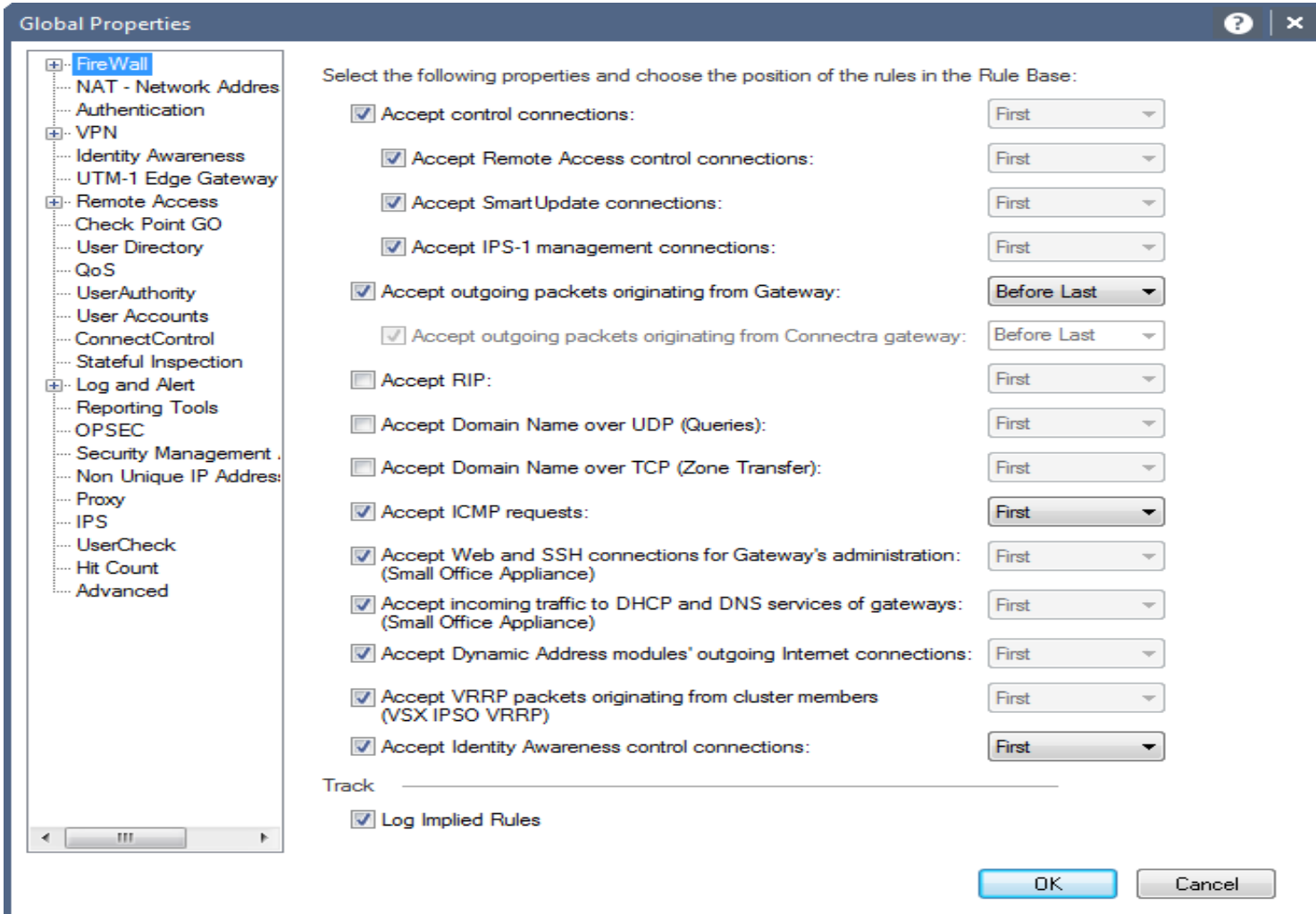
- Cannot be edited
- Configured to allow connections for different services used by the Security Gateway
- Some enabled by default

# Understanding Rule Base Order

- First
- Explicit
- Before Last
- Last
- Implicit Drop



# Global Properties



Settings configured as Global Properties are enforced by all Security Gateways managed by the Security Management Server.

# Sections

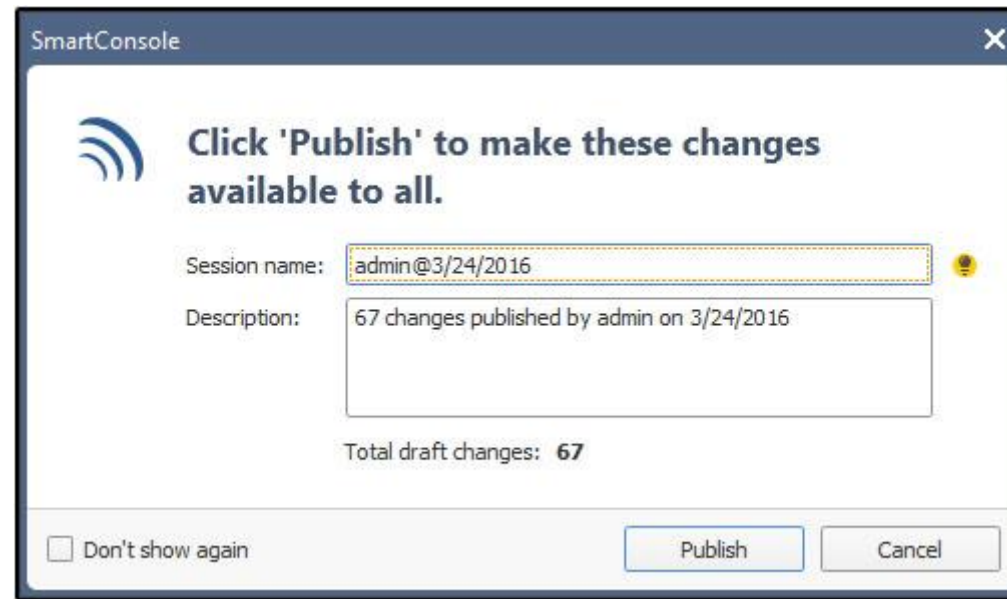


No.	Name	Source	Destination
1	Cleanup rule	* Any	* Any
▼ New Section (2-3)			
2	VPN rule	* Any	* Any
3	APPI rule	* Any	* Any

Sections are visual divisions of the rule base and do not hinder the order of rule enforcement.

# Publish Policy

New policies and changes to an existing Rule Base must be published on the Security Management Server before the policy can be installed and enforced on the Security Gateway.





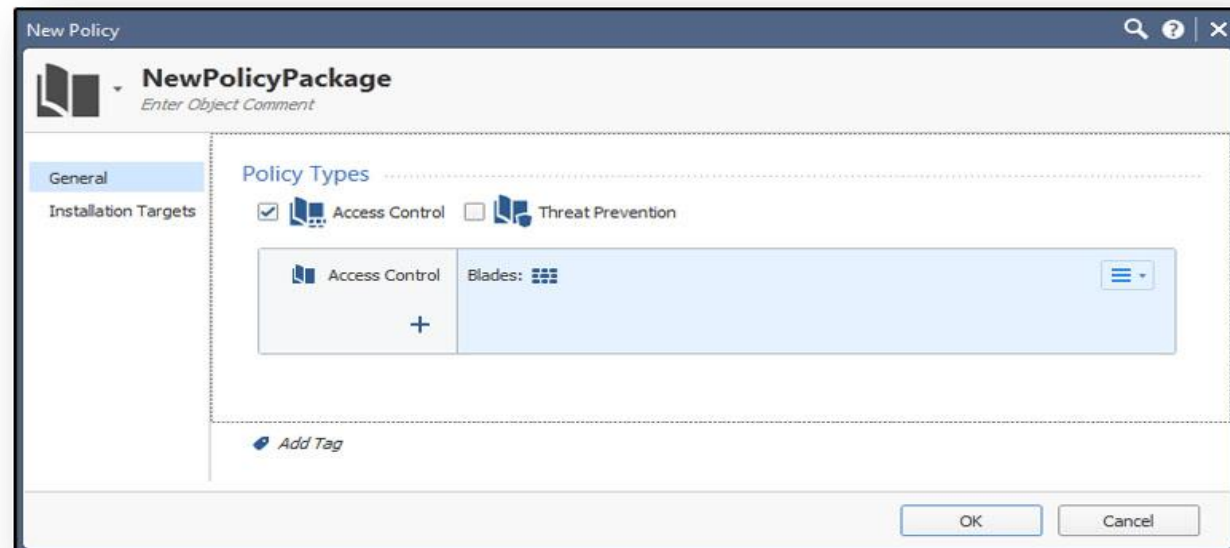
# Policy Packages

A group of different types of policies that are installed together on the same installation targets.



# Policy Types

- Access Control
- QoS
- Desktop Security
- Threat Prevention



# Policy Types

## Access Control

Consist of these types of rules:

- Firewall
- Application Control and URL Filtering
- NAT
- Data Awareness

## Desktop Security

The Firewall policy for endpoint computers that have an Endpoint Security VPN remote access client installed as a standalone client.

## QoS

Policy based bandwidth management solution which allows for prioritizing critical traffic

## Threat Prevention

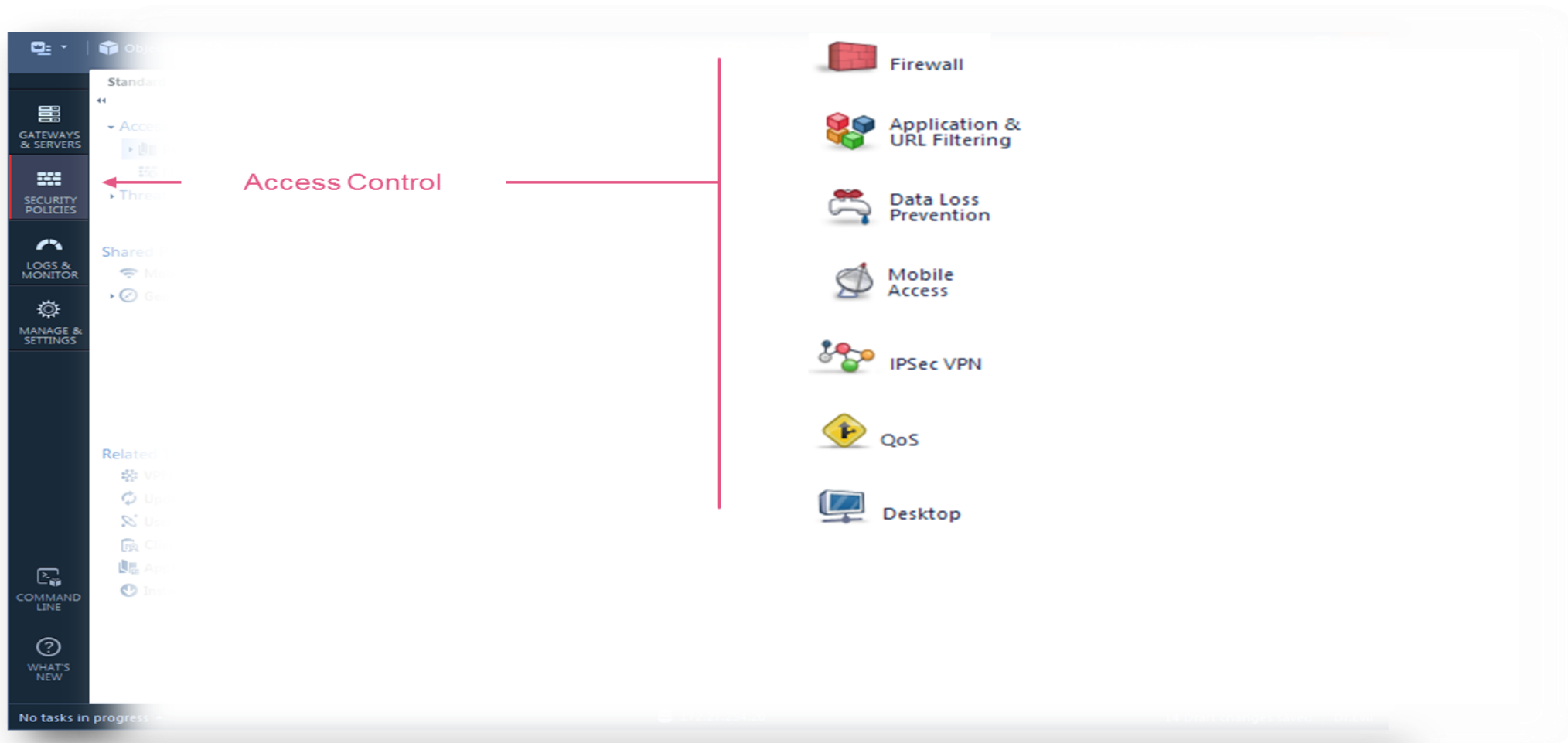
Consist of these types of rules:

- IPS
- Anti-Bot
- Antivirus
- Threat Emulation



# Unified Policies

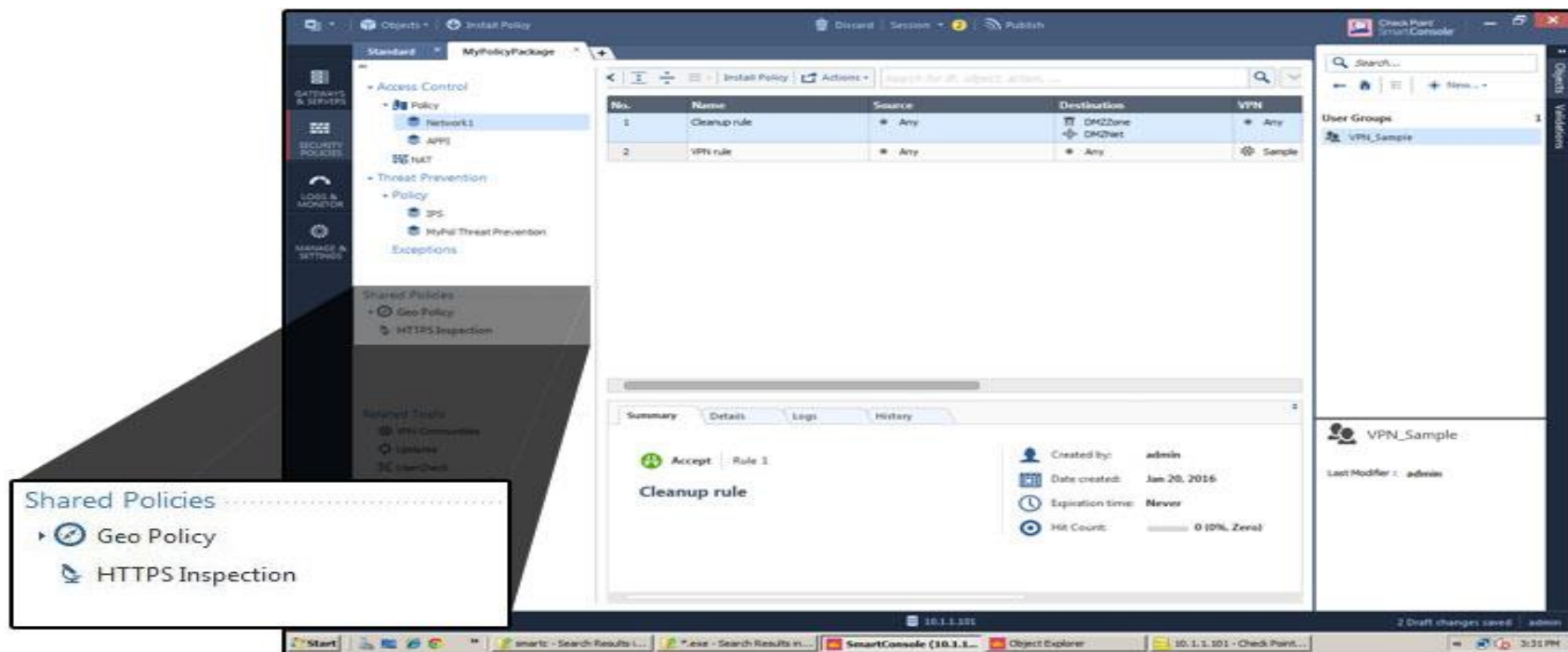
Control several security aspects from a single console.





# Shared Policies

- Mobile Access
- DLP
- HTTPS Inspection
- Geo Policy





# Additional Policy Management Tools

## Access Tools:

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

## Threat Tools:

- Profiles
- IPS Protections
- Protections
- Whitelist Files
- ThreatWiki
- Updates
- UserCheck



# Install Policy



SmartConsole

Publish



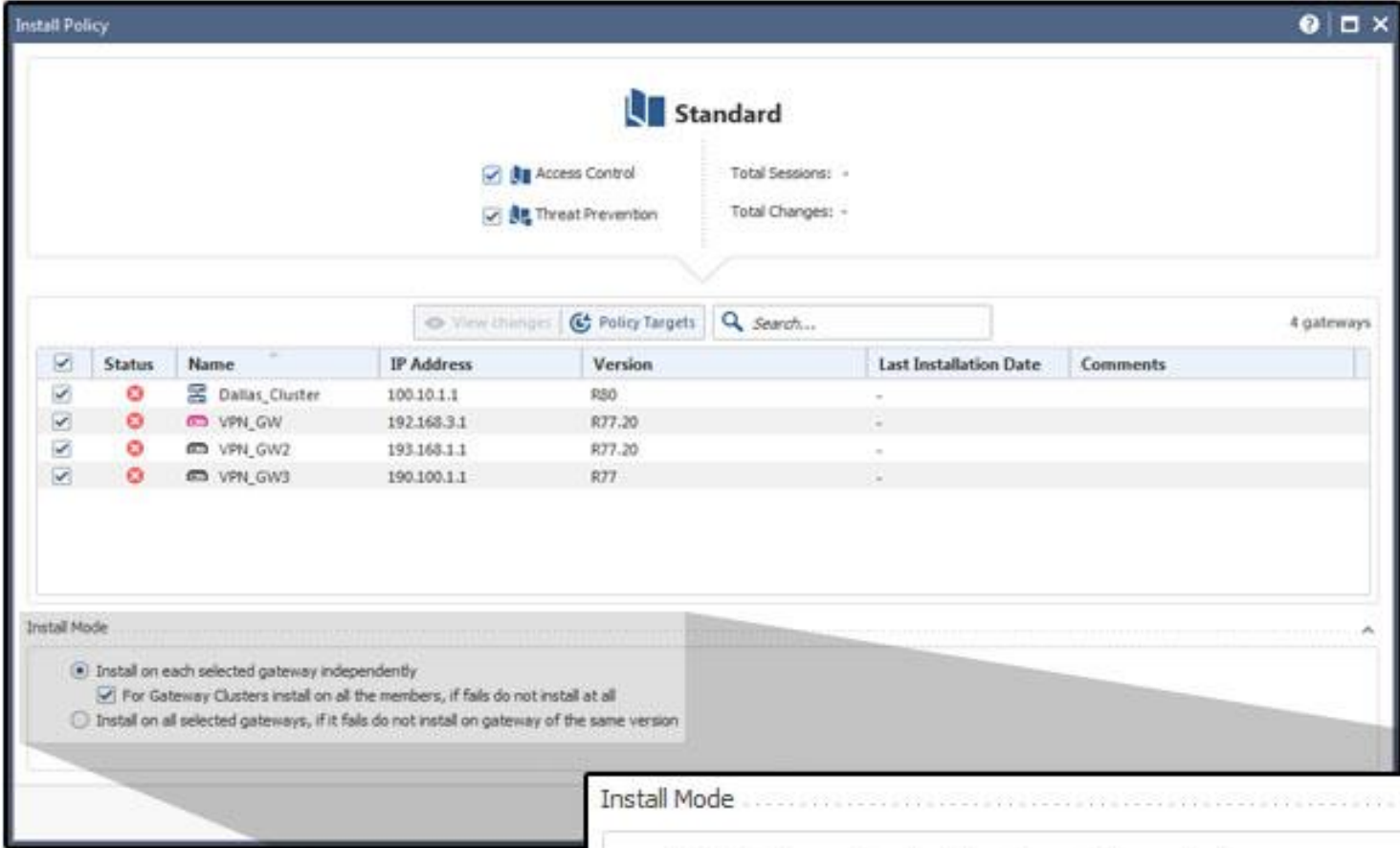
Security Management Server

Install



Security Gateway

# Install a Policy Package



**Standard**

Access Control  
 Threat Prevention

Total Sessions: -  
Total Changes: -

View Changes Policy Targets Search... 4 gateways

<input checked="" type="checkbox"/>	Status	Name	IP Address	Version	Last Installation Date	Comments
<input checked="" type="checkbox"/>	✘	Dallas_Cluster	100.10.1.1	R80	-	
<input checked="" type="checkbox"/>	✘	VPN_GW	192.168.3.1	R77.20	-	
<input checked="" type="checkbox"/>	✘	VPN_GW2	193.168.1.1	R77.20	-	
<input checked="" type="checkbox"/>	✘	VPN_GW3	190.100.1.1	R77	-	

**Install Mode**

- Install on each selected gateway independently
  - For Gateway Clusters install on all the members, if fails do not install at all
- Install on all selected gateways, if it fails do not install on gateway of the same version

**Install Mode**

- Install on each selected gateway independently
  - For Gateway Clusters install on all the members, if fails do not install at all
- Install on all selected gateways, if it fails do not install on gateway of the same version



# Network Address Translation

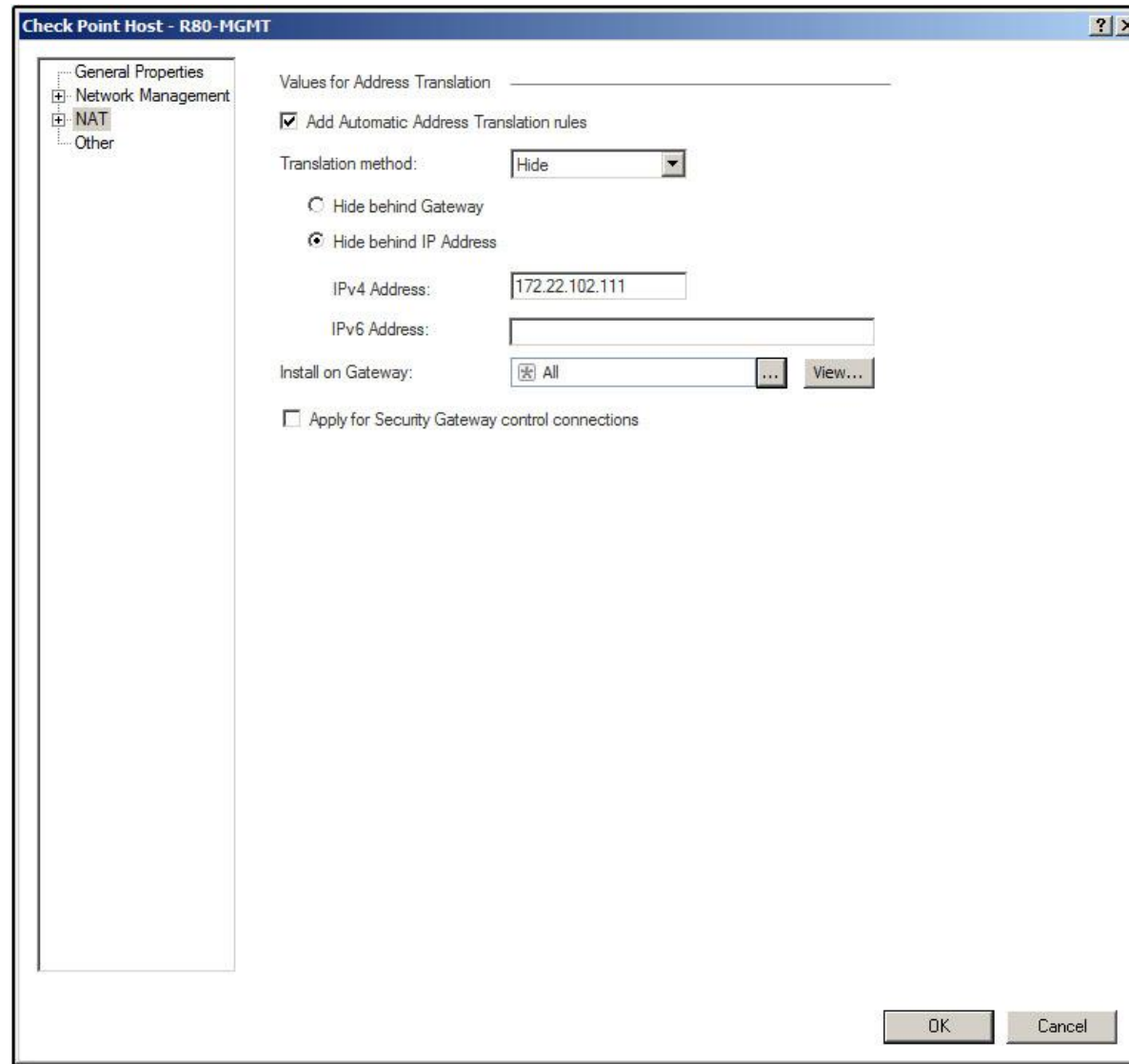
- Reasons for employing NAT:
  - Private IP addresses used in internal networks
  - Limiting external network access
  - Ease and flexibility of network administration
- Source NAT = IP of machine (client) initiating the connection
- Destination NAT = IP of machine receiving the connection



# Types of NAT

- Hide NAT (Dynamic NAT)
  - Many-to-one relationship
  - Multiple computers represented by one IP address
  - Only allows connections from protected side of Gateway
- Static NAT
  - One-to-one relationship
  - Each host translated to unique IP address
  - Connections initiated internally and externally

# Hide NAT Using Interface IP Address



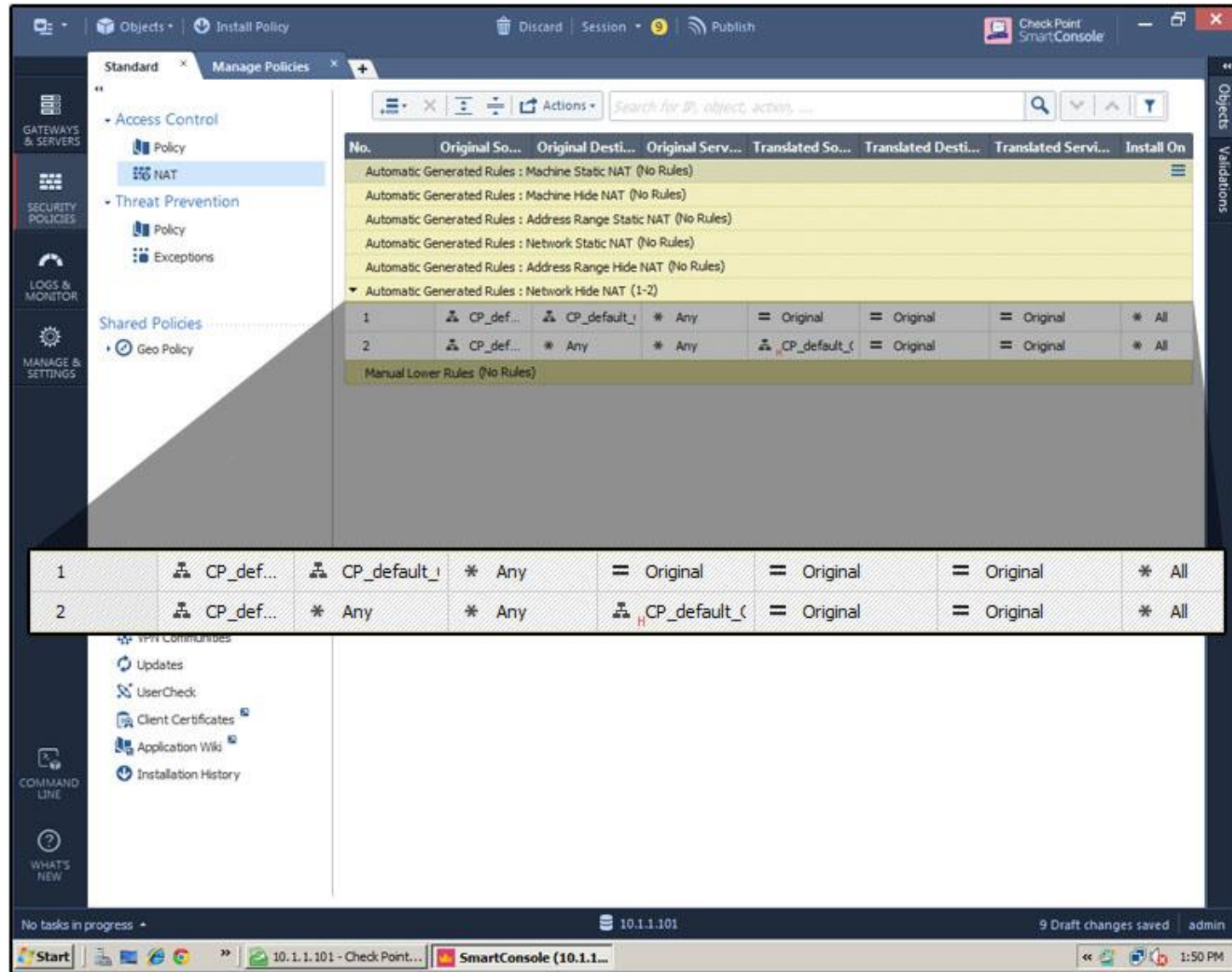
The screenshot shows the 'Check Point Host - R80-MGMT' configuration window. On the left, a tree view shows 'General Properties', 'Network Management', 'NAT', and 'Other'. The 'NAT' section is selected. The main area is titled 'Values for Address Translation' and contains the following settings:

- Add Automatic Address Translation rules
- Translation method: **Hide** (dropdown menu)
- Hide behind Gateway
- Hide behind IP Address
- IPv4 Address:
- IPv6 Address:
- Install on Gateway:  All (dropdown menu) [View...]
- Apply for Security Gateway control connections

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



# NAT Rules



No.	Original So...	Original Desti...	Original Serv...	Translated So...	Translated Desti...	Translated Servi...	Install On
1	CP_def...	CP_default_1	* Any	= Original	= Original	= Original	* All
2	CP_def...	* Any	* Any	CP_default_c	= Original	= Original	* All

# NAT Rules



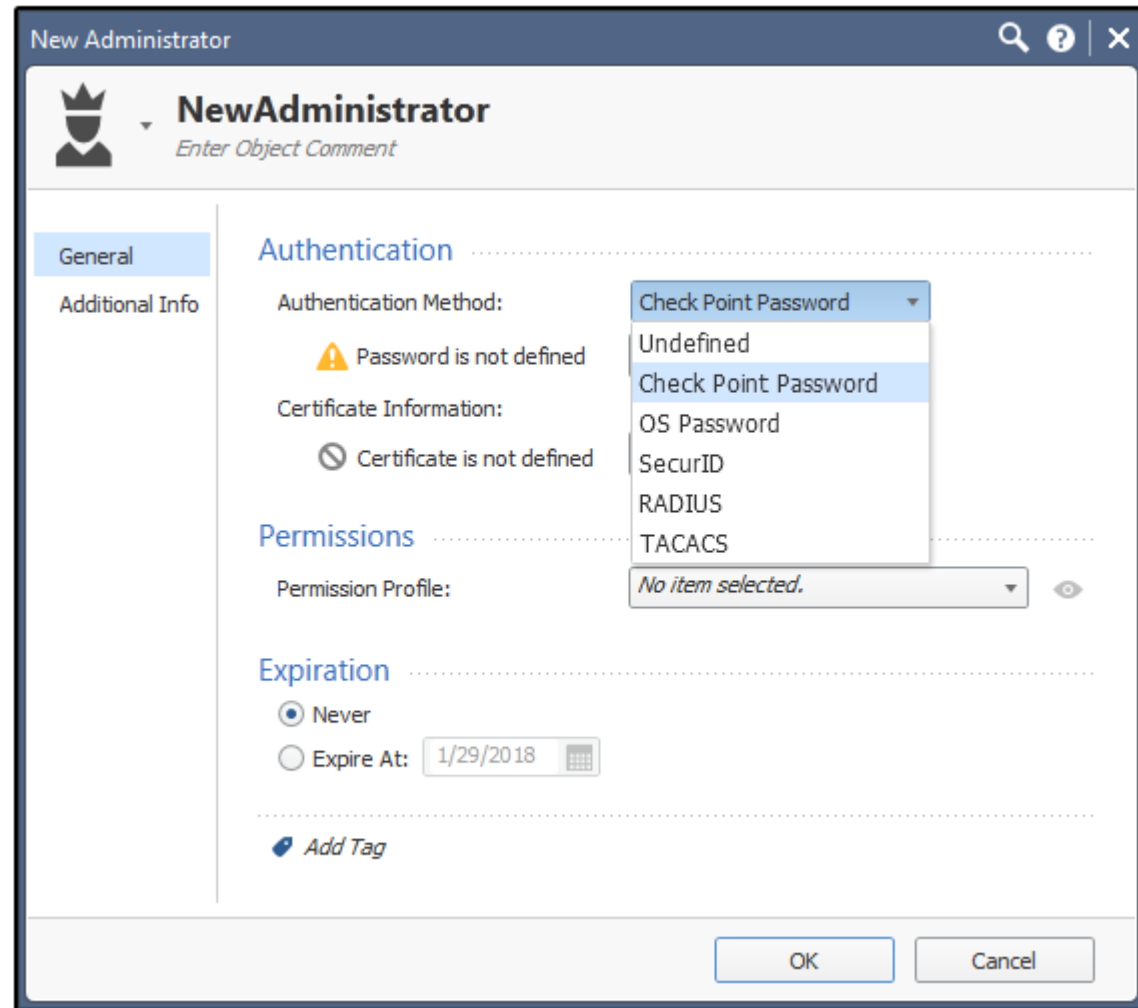
The screenshot shows the Check Point SmartConsole interface for configuring NAT rules. The left sidebar contains navigation options like 'GATEWAYS & SERVERS', 'SECURITY POLICIES', 'LOGS & MONITOR', and 'MANAGE & SETTINGS'. The main area displays a list of NAT rules. A zoomed-in view at the bottom highlights two rules:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Desti...	Translated Services
1	Alpha-Inter...	Alpha-Internal-I	* Any	= Original	= Original	= Original
2	Alpha-Internal...	* Any	* Any	Alpha-Internal-I	= Original	= Original

# Administration

## Authentication Methods:

- Check Point Password
- OS Password
- SecureID
- RADIUS
- TACACS



New Administrator

**NewAdministrator**  
Enter Object Comment

General  
Additional Info

**Authentication**

Authentication Method: Check Point Password

⚠ Password is not defined

Certificate Information:  
⚠ Certificate is not defined

**Permissions**

Permission Profile: No item selected.

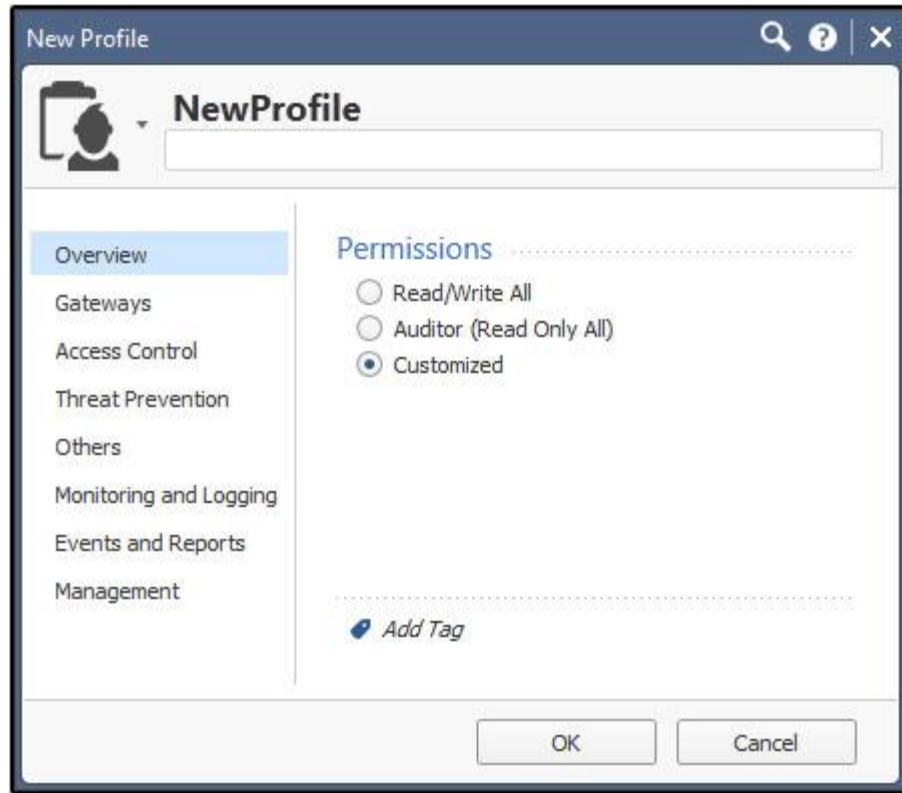
**Expiration**

Never  
 Expire At: 1/29/2018

[Add Tag](#)

OK Cancel


# Permission Profiles



Permission profiles allow for granular control over who can perform certain tasks and may be assigned to multiple administrators.

# Revoke a Certificate

Administrator

 **admin**  
*Enter Object Comment*



General  
Additional Info

**Authentication**


Authentication Method: OS Password


Certificate Information:  
 Certificate is defined

**Permissions**

Permission Profile:  Super User 

**Expiration**

Never  
 Expire At: 12/31/2030 

 Add Tag

OK Cancel

# Sessions



Session Details

Session name:

Description:

Name	Administrator	Connected From	Connection Mode	Application	Locks	Changes	Login
(Unnamed)	admin	N/A	Disconnected	SmartView...	0	0	1/22/2016 2:53 PM
(Unnamed)	admin	10.1.1.201	Read Write	SmartConsole	2 (Smar...	1	1/28/2016 4:48 PM
(Unnamed)	admin	N/A	Disconnected	SmartUpdate	0	0	1/29/2016 11:26...

# Database Revisions



The screenshot shows the 'Revisions' table in the Check Point SmartConsole. The table contains the following data:

Publish Time	Name	Publisher	Changes	Description
1/29/2016 11:10 AM	admin@1/29/2016	admin	1	1 change published by admin on 1/29/2016
1/25/2016 3:38 PM	admin@1/25/2016	admin	4	4 changes published by admin on 1/25/2016
1/22/2016 2:52 PM	admin@1/22/2016	admin	2	2 changes published by admin on 1/22/2016
1/22/2016 2:51 PM	admin@1/22/2016	admin	4	2 changes published by admin on 1/22/2016
1/22/2016 2:49 PM	admin@1/22/2016	admin	3	3 changes published by admin on 1/22/2016

The interface also shows a sidebar with navigation options like 'Permissions & Administrators', 'Blades', 'Sessions', 'View Sessions', 'Advanced', 'Revisions', 'Tags', and 'Preferences'. The bottom of the screenshot shows the Windows taskbar with the Start button and several open applications including 'SmartConsole (35.1.1.101)'.

# Concurrent Administration



Administrator Dan's  
View

Pencil icon

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	None	* Policy Targets
2	Management	Net_10.28.0.0	GW-R.7730	* Any	https, ssh	Accept	Log	* Policy Targets
3	Stealth	* Any	GW-R.7730	* Any	* Any	Drop	Log	* Policy Targets
4	DNS	Net_10.28.0.0	* Any	* Any	dns	Accept	Log	* Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http, https	Accept	Log	* Policy Targets
6	DMZ Rule	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp, AP-Defender	Accept	Log	* Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	None	* Policy Targets
2	Management	Net_10.28.0.0	GW-R.7730	* Any	https, ssh	Accept	Log	* Policy Targets
3	Stealth	* Any	GW-R.7730	* Any	* Any	Drop	Log	* Policy Targets
4	DNS	Net_10.28.0.0	* Any	* Any	dns	Accept	Log	* Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http, https	Accept	Log	* Policy Targets
6	DMZ Rule	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp, AP-Defender	Drop	None	* Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets



Administrator Mike's  
View

Lock icon



# Backups

- Snapshot
- System Backup (and System Restore)
- Migrate
- Save Configuration (and Load Configuration)

# Backups

	Snapshot	System Backup	Migrate	Save Configuration
Does it backup Gaia operating system configuration?	Yes	Yes	No	Yes
Does it backup Products configuration?	Yes	Yes	Yes	No
Does it backup Hotfixes?	Yes	No	No	No
Size of output file on Security Gateway	5 - 100 GB	Depends on configuration	Depends on configuration	Few KB
Size of output file on Security Management Server	5 - 100 GB	5 - 100 GB	Depends on configuration	Few KB
Does it support automatic scheduling?	No	Yes	No	No
Can you restore from different versions?	Yes	No	Upgrade is performed when importing to a newer version	With manual adjustments



# Performing Backups

## SmartConsole

System Backup

Backup 'the members of Dallas\_Cluster' to:

Backup server defined for this cluster   
Currently defined: None

The following backup server:

Server:

Protocol:

Username:

Password:

Path:

Comment:

OK Cancel

## WebUI

New Backup

Backup Type

This appliance

Management

SCP server

FTP server

TFTP server

The backup will be made to this appliance.

In order for the backup to be effective you should copy the file outside the machine

Backup Cancel

## CLI

Command Line

```
> add backup local
```



Check Point®  
SOFTWARE TECHNOLOGIES LTD

# UNIFIED ACCESS POLICY POLICY LAYERS

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION

# Agenda



- Check Point Security Management Architecture
- Unified Access Policy - Layers
  - Ordered Layers
  - Inline Layers
- Content Awareness
- Security Zones
- Domain Objects
- Threat Prevention

A policy layer is a **set of rules** describing the security enforcement applied by a gateway

Assign **one or more security functionalities** to a policy layer

Control administrative tasks (view/edit/install) of the policy layer using **administrative roles**



# Security policies expressing your needs

## Mapping the business needs into security policies

Business needs:

Finance: save costs

Marketing: be visible

HR: keep data secured

IT department trying to achieve:

Optimizing resources: delegation

Extending the network: cloud

Building fences: segmentation

# Security Policies Expressing Your Needs

## Ordered Layers and Inline Layers

### Values R80.10 Policy Layers are bringing to customers

#### Delegation

- Assign administrative roles to security policy layers
- Assign roles to administrative users or automated systems using the API

#### Cloud

- Use objects existing in private and public cloud environments
- Create automated process to scale up and down security instances according to your needs
- Use existing auto-scaling methods provided by the cloud infrastructure

#### Segmentation

- Create layers and active one or more security functionality (= Check Point Software Blade(s))
- Segment your rule base keeping it manageable
- Multiple administrators can work on the same policy layer at the same time (if allowed by admin role assigned to the layer)





# Security Policies Expressing Your Needs

## Ordered Layers and Inline Layers

Network Access Policy Layer

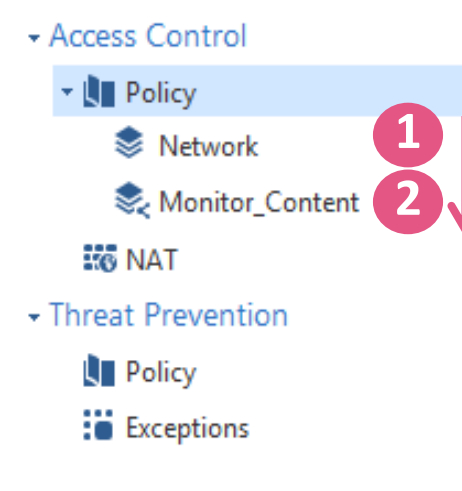
The screenshot shows the Security Policy configuration interface. The left sidebar contains navigation options: Access Control (Policy, NAT), Threat Prevention (Policy, Exceptions), Shared Policies (Mobile Access, Geo Policy, Inspection Settings), and Access Tools (VPN Communities, Updates). The main table lists 11 policies grouped into layers: Management (1-2), Network Services (3-5), Identity Awareness (6-8), Inbound (9-10), and Outbound (11). Annotations highlight various features: 'Services' (ssh, GaiaWebUI, http, https), 'Security Zones' (InternalZone, ExternalZone), 'Application Signature' (OCSP Protocol), 'Logging and Accounting' (Log, Accounting, Detailed Log, Extended Log), 'Content' (Any Direction, Document File, Spreadsheet File), 'Portal Applications' (IntranetPortal), and 'URL Category' (Business Applications, Search Engines / Portals).

No	Name	Source	Destination	Services & Applications	Content	Action	Track
<b>Management (1-2)</b>							
1	Management	net_192.168.169.0	gwR8010	ssh, GaiaWebUI	*	Accept	None
2	Update Services	mgnt	* Any	http, https	* Any	Accept	None
<b>Network Services (3-5)</b>							
3	Name Service	InternalZone	ExternalZone	dns	*	Accept	None
4	ICMP	InternalZone	ExternalZone	icmp-proto	*	Accept	None
5	OCSP	InternalZone	ExternalZone	OCSP Protocol	* Any	Accept	Log, Accounting
<b>Identity Awareness (6-8)</b>							
<b>Inbound (9-10)</b>							
9	Email	net_192.168.169.0	web+mailserver	SMTP	* Any	Accept	Log, Accounting
10	Intranet	Roaming Users	web+mailserver	IntranetPortal	Any Direction, Document File, Spreadsheet File	Accept	Detailed Log, Accounting
<b>Outbound (11)</b>							
11	Web Browsing	net_192.168.169.0, net_192.168.170.0	* Any	Business Applications, Search Engines / Portals	*	Accept	Extended Log, Accounting
<b>Clean up (12-13)</b>							

# 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

Extract of a larger rule base

Why do I need **Ordered** and **Inline** Layers?

# Security Policies Expressing Your Needs

## Ordered Layers and Inline Layers

### The need for Ordered Layers

- Managing gateways running R77.30 and earlier
  - When migrating a management server from R77.30 to R80.10 all policies will be represented as Ordered Layered Policies
  - Gateways running R77.30 and earlier support only Ordered Policy layers with just one Blade active on each layer
- Monitoring or temporary enforcement
  - Add a dedicated layer for a functionality such as Content Awareness to a policy monitoring the file and data types



# Security Policies Expressing Your Needs

## Ordered Layers and Inline Layers

### The need for **Inline Layers** supported by R80.10 Gateways

- Rule base matching performance
  - As long as traffic does not match the “parent rule” the Inline Layer is not used in the policy matching process
- Reoccurring needs combined with delegation of duties
  - Reuse an Inline Layer one or multiple times and assign a dedicated administrative role thus “outsourcing” the security management to a department or automated system

		Parent Rule				
4	Active Directory Central	Central_Client			* Any	Active_Directory_Layer Network
4.1	Active Directory Server	All_Client_networks	All_Domain_Controllers	NBT https ldap ldap-ssl kerberos_v5_TCP kerberos_v5_UDP dns	* Any	Accept
4.2	Identity Collector	All_Identity_Collectors	All_Gateways	https ssl_v3 DCE-RPC Protocol	* Any	Accept

# Ordered Layers

Use section titles structuring the policy



The screenshot shows the Check Point NGTPdemo interface for a policy named 'SimplePolicy'. The left sidebar shows the navigation menu with 'Policy' selected under 'Access Control'. The main area displays a table of policy rules, organized into sections. A pink callout box labeled 'Network Access Layer' points to the 'Policy' menu item. Another pink callout box labeled 'Structure a layer into sections' points to the 'Network Services (3-5)' section of the table.

	Destination	VPN	Services & Applications	Action	Track
▶ Management (1-2)					
▼ Network Services (3-5)					
3	Name Service net_192.168.169.0 net_192.168.170.0	* Any	* Any	dns	
4	ICMP net_192.168.169.0 net_192.168.170.0	* Any	* Any	icmp-proto	
5	OCSP net_192.168.169.0 net_192.168.170.0	* Any	* Any	OCSP Protocol	
▶ Identity Awareness (6-7)					
▼ Inbound (8)					
8	Email net_192.168.169.0	mailserver	* Any	smtp	Accept Log
▼ Outbound (9)					
9	Web Browsing net_192.168.169.0 net_192.168.170.0	* Any	* Any	http https	Accept Log
▶ Clean up (10-11)					



# Ordered Layers

## Software Blades and installation targets

The screenshot shows the Check Point management console interface. On the left, a navigation pane shows 'Policy' selected under 'Access Control'. A pink callout bubble labeled 'Edit' points to the 'Policy' item. The main area shows the 'Policy' configuration page for 'NGTPdemo'. The 'Installation Targets' tab is selected and highlighted with a pink callout bubble labeled 'Specify the gateway(s)'. Below this, there are radio buttons for 'All gateways' and 'Specific gateways', with 'Specific gateways' selected. A table lists the selected gateway:

Name	IP Address	Comments
gwR8010	172.27.254.254	

Buttons for '+', 'x', and 'Search...' are visible above the table. At the bottom of the configuration window are 'OK' and 'Cancel' buttons.



# Ordered Layers Summary

- You achieve an Access Control policy containing **Multiple Ordered Layers**
- Each layer performs one or more specific security actions
- The layers will be matched top-down

Access Control <input type="checkbox"/> VPN Traditional mode	1	Network	Blades:	
	2	Monitor_Content	Blades:	Shared

**Ordered Layers**

Access Control

- Policy
  - 1** Network
  - Monitor\_Content
- NAT
- Threat Prevention
  - Policy
  - Exceptions

Shared Policies .....

No.	Name	Source	Destination	VPN
Management (1-2)				
Network Services (3-5)				
3	Name Service	net_192.168.169.0 net_192.168.170.0	* Any	* Any
4	ICMP	net_192.168.169.0 net_192.168.170.0	* Any	* Any
5	OCSP	net_192.168.169.0 net_192.168.170.0	* Any	* Any

**Network Layer**

Access Control

- Policy
  - Network
  - 2** Monitor\_Content
- NAT
- Threat Prevention
  - Policy
  - Exceptions

Shared Policies .....

No.	Name	Source	Destination	VPN	Services & Applications	Content
1	Monitor documents	* Any	* Any	* Any	* Any	Any Direction Document...
2	Monitor spreadsheets	* Any	* Any	* Any	* Any	
3	Monitor large files	* Any	* Any	* Any	* Any	
4	Monitor credit card content	* Any	* Any	* Any	* Any	Any Direction PCI - Credit...

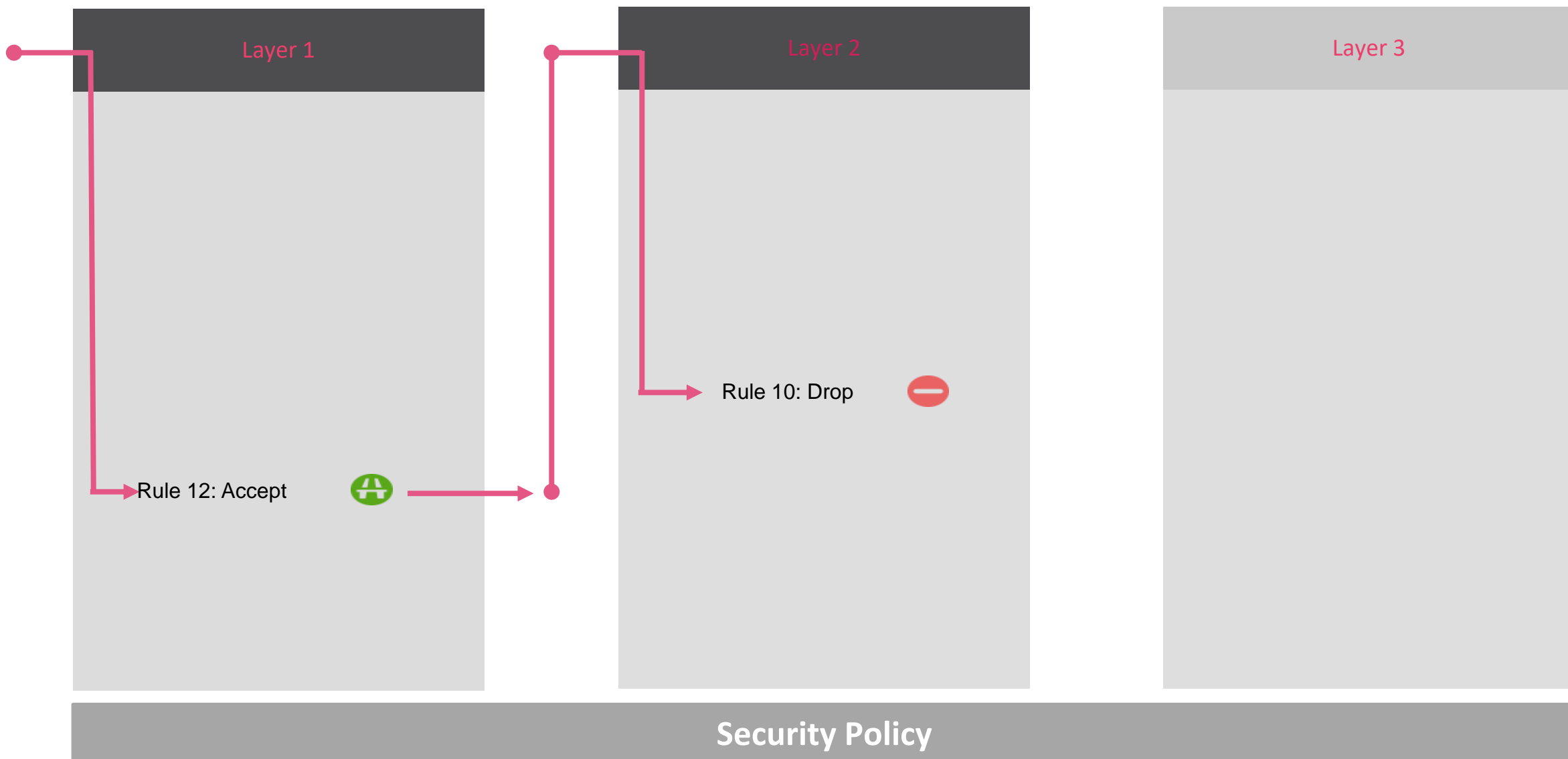
Missing cleanup rule - Unmatched traffic will be accepted and not logged.

**Content Layer**





# Traffic Inspection





# Inline Layers

## Optimizing matching process and reusing rules multiple times

- Only packets matching the **Parent Rule** will be checked against the rules of the **Inline Layer**
- **Reuse Layers** in multiple Policies or multiple times in the same policy

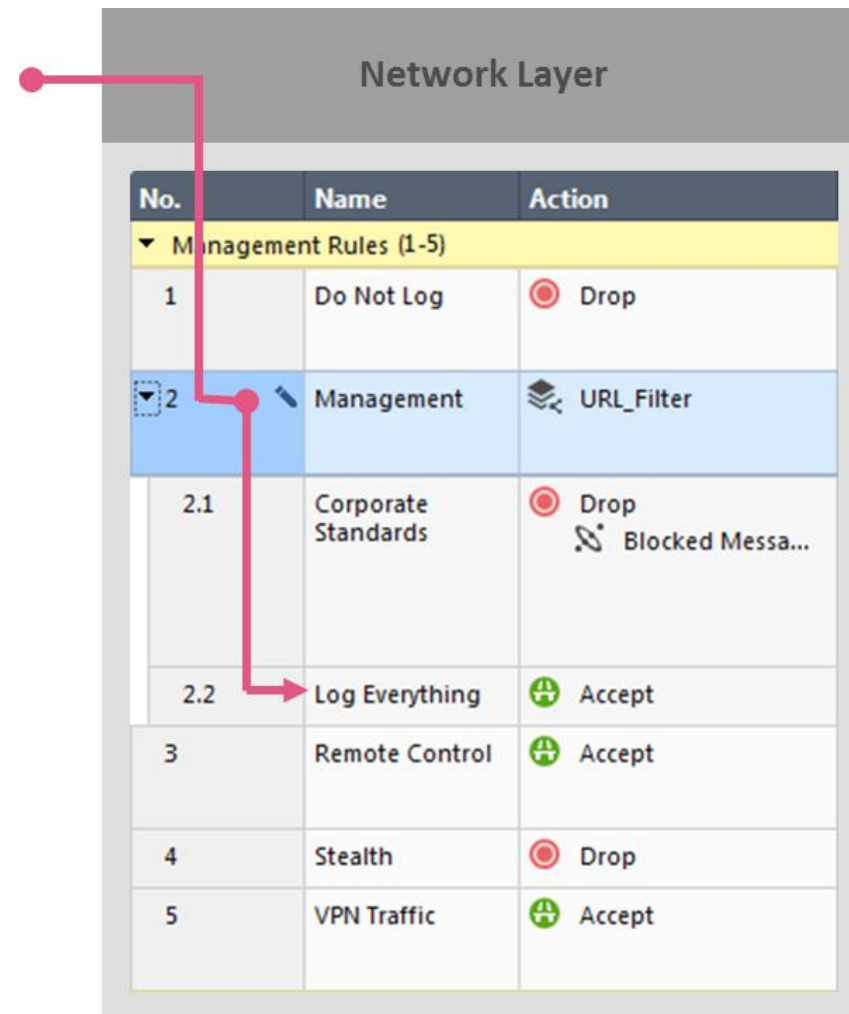
No.	Name	Source	Destination	Services & Applications	Content	Action
3	DNS	net_192.168.169.0 net_192.168.170.0	* Any	dns	* Any	Accept
4	Active Directory Central	Central_Client_Zone	Central_Services_Zone	* Any	* Any	Active_Directory_Layer Network
4.1	Active Directory Server	All_Client_networks	All_Domain_Controllers	NBT https ldap ldap-ssl Kerberos_v5_TCP Kerberos_v5_UDP dns	* Any	A
4.2	Identity Collector	All_Identity_Collectors	All_Gateways	https ssl_v3 DCE-RPC Protocol	* Any	A
4.3	Identity Collector	All_Identity_Collectors	All_Domain_Controllers	https	* Any	A
4.4	LDAP Group Query	All_Gateways	All_Domain_Controllers	ldap ldap-ssl	* Any	A
4.5	Cleanup rule	* Any	* Any	* Any	* Any	D
5	Active Directory Backup Site	Backup_Site_Zone	Backup_Site_Services_Zone	* Any	* Any	Active_Directory_Layer Network
6	SMTP	net_192.168.169.0	web+mailserver	smtp	* Any	Accept
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop

Ordered Layer

Example:  
Active Directory related rules

Inline Layers will only be checked for matching, if the parent rule is matching

# Traffic Flow Through an Inline Layer





# Inline Layers

## Assigning administrative privileges to dedicated roles

- Authorized administrators will be able to **modify only the rules inside the Inline Layer** but not the Parent Rule or any other rule of the Ordered Layer

No.	Name	Source	Destination	Track
2	Updates	mgmt	* Any	Log
3	DNS	net_192.168.169.0 net_192.168.170.0	* Any	None
4	Active Directory Central	Central_Client_Zone	Central_Ser...	N/A
4.1	Active Directory Server	All_Client_networks	All_Domai...	None
4.2				None
4.3				None
4.4	LDAP Group Query	All_Gateways	All_Domai...	None
4.5	Cleanup rule	* Any	* Any	None
5	Active Directory Backup Site	Backup_Site_Zone	Backup_Si...	N/A
6	SMTP	net_192.168.169.0	web+mail...	Log
7	Cleanup rule	* Any	* Any	Log

Layer Editor

### Active\_Directory\_Layer Network

Enter Object Comment

General  
Advanced  
Permissions

The following profiles can edit this layer as they have permissions to this layer blades:  
Firewall and Applications & URL Filtering

Name	Comments
Read Write All	Full Read/Write Permissions.
Super User	Full Read/Write Permissions including managing...

Select additional profiles that will be able to edit this layer: 🚫

+ | ×

Search...

Name	Comments
Active_Directory_adminRole	restricted to Active Directory Policy Layer

Add Tag

OK Cancel

Beneficial when collaborating  
or working with automation  
based on the API

Maintain rules in one place for  
all policies

Inline  
Layer



# Ordered Layers And Inline Layers

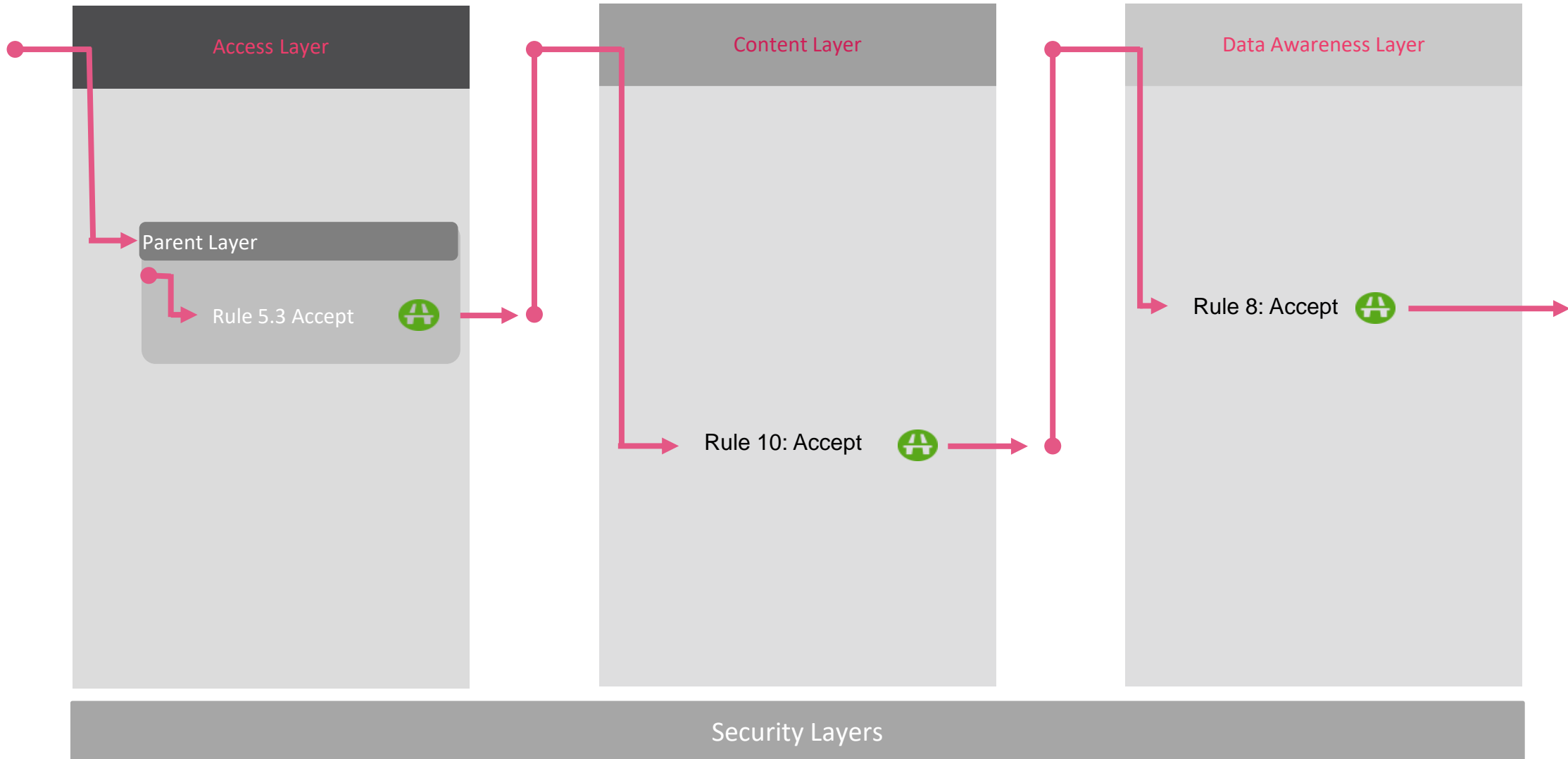
## Supported Policy Targets

- **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

# Traffic Inspection for Ordered Layers And Inline Layers





# Security Policies Expressing Your Needs

## Layer Options

- Editing the layer options allows enabling/disabling of Blades
- Specifying if this layer might be used in other policies

The screenshot shows the 'Layer Editor' window with the 'General' tab selected. The 'Blades' section is highlighted with a red box and contains the following options:

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

Below the Blades section is a 'Preview' table:

Destination	VPN	Services & Applications	Action	Track	Instal

The 'Sharing' section is also highlighted with a red box and contains the following option:

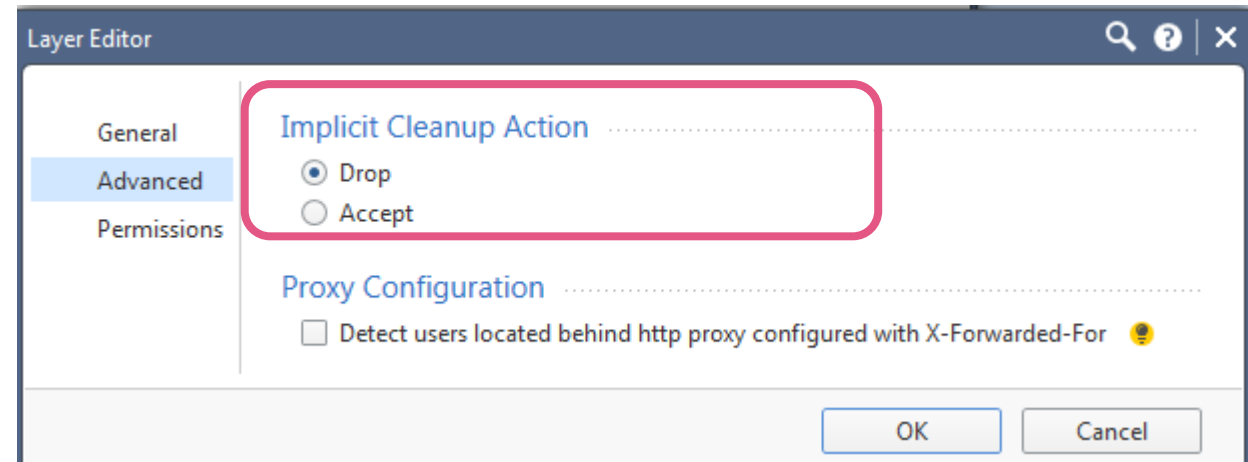
- Multiple policies and rules can use this layer

At the bottom right of the window are 'OK' and 'Cancel' buttons.

# Security Policies Expressing Your Needs

## Layer Options

- Defining the **implicit cleanup** rule action
  - For a pure Network Layer: Drop
  - For a pure APP Control and URL Filtering Layer: Accept
  - For a pure Content Awareness Layer: Accept
  - For a Unified Policy Layer: Drop





# MATCHING OF APPLICATION, URLF CATEGORIES AND CONTENT OBJECTS



# Matching of Application, URLF and Content Objects

## Services associated with Applications, URLF Categories and Content Types

- The example shows a rule controlling access to all sites and applications that belong to the “Search Engines / Portals” category
  - The HTTP and HTTPS Services are implicitly allowed as they are listed as “matching services” for the category object

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		
▼ Outbound (9)							
9	Web Browsing	net_192.168.169.0 net_192.168.170.0	Internet	* Any	Search Engines / Portals		
▶ Clean up (10-11)							

### Search Engines / Portals

A search engine is a commonly used web application designed to let the user search for content based on the terms used.

Match By

- Site and application category
- Services:
  - http (tcp/80)
  - https (tcp/443)
  - HTTP\_proxy (tcp/8080)
  - HTTPS\_proxy (tcp/8080)

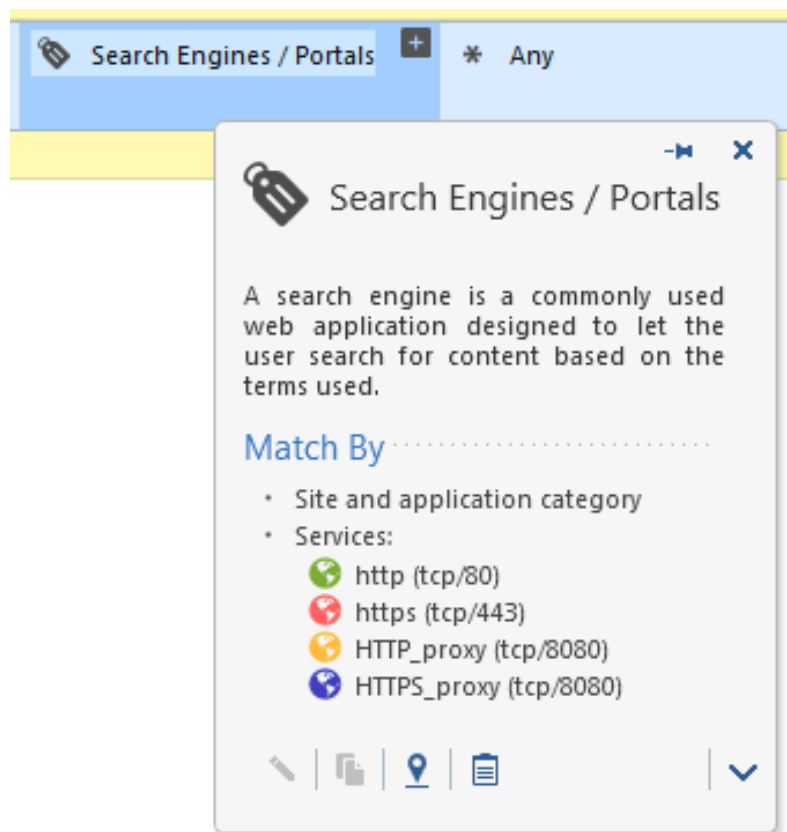
- You can see the services that are matching for this category using the “mouse over” functionality



# Matching of Application, URLF and Content Objects

## Services associated with Applications, URLF Categories and Content Types

- Application signatures and URL filtering category objects do have services associated
- These services must match together with the application signature or URL category

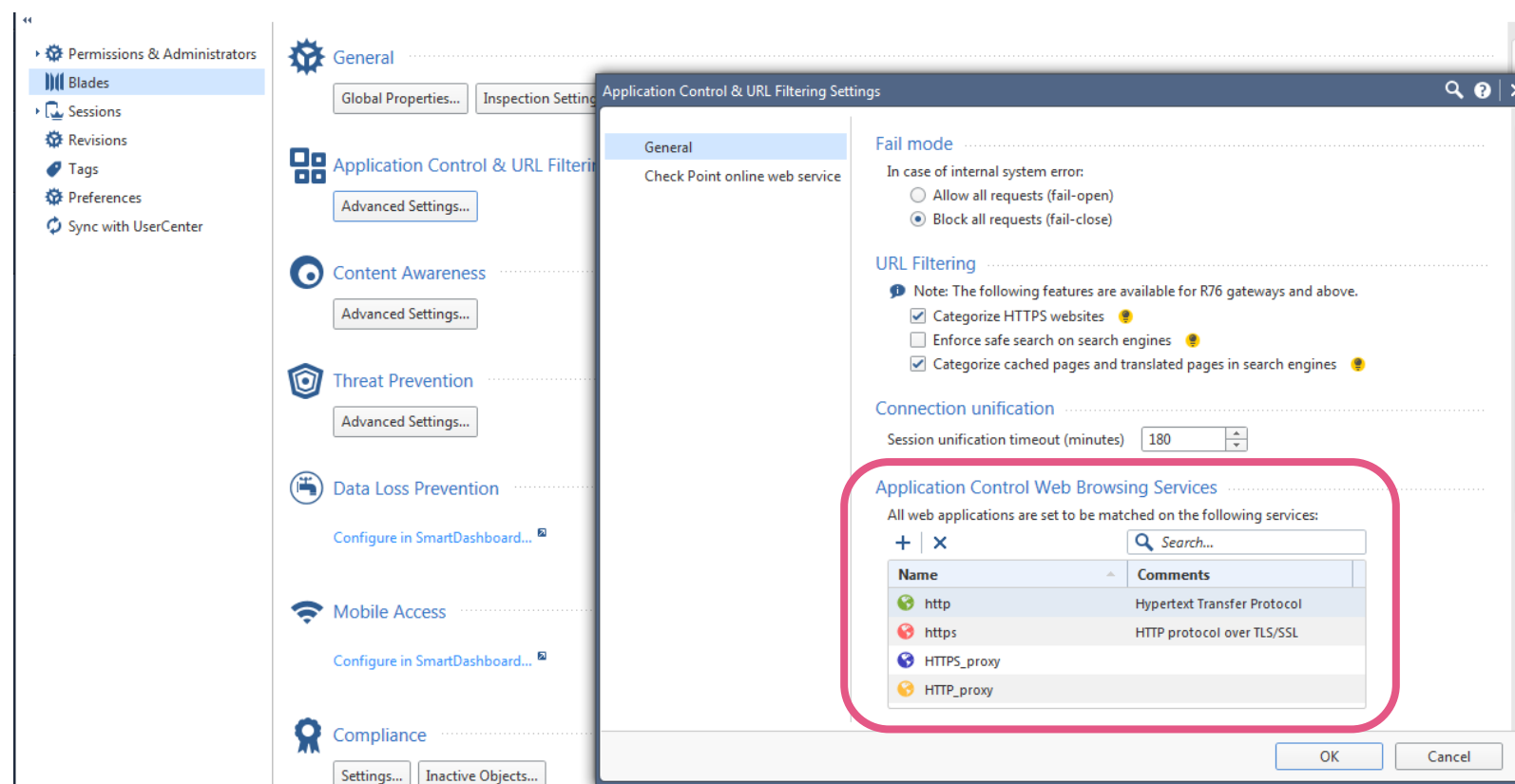


- When hovering with the mouse over the object, you see that this category will match for:
  - HTTP
  - HTTPS
  - HTTP\_proxy on port TCP 8080
  - HTTPS\_proxy on port TCP 8080

# Matching of Application, URLF and Content Objects

## Services associated with Applications, URL Categories and Content Types

- Application signatures and URL filtering categories will match for a predefined list of services configured as “Application Control Web Browsing Services”
  - Go to “Manage & Settings > Blades > Application Control > Advanced Settings”



The screenshot displays the 'Application Control & URL Filtering Settings' dialog box in the Check Point management console. The 'General' tab is selected, and the 'Application Control Web Browsing Services' section is highlighted with a red box. This section shows a list of services that are used for matching applications and URL filtering. The services listed are:

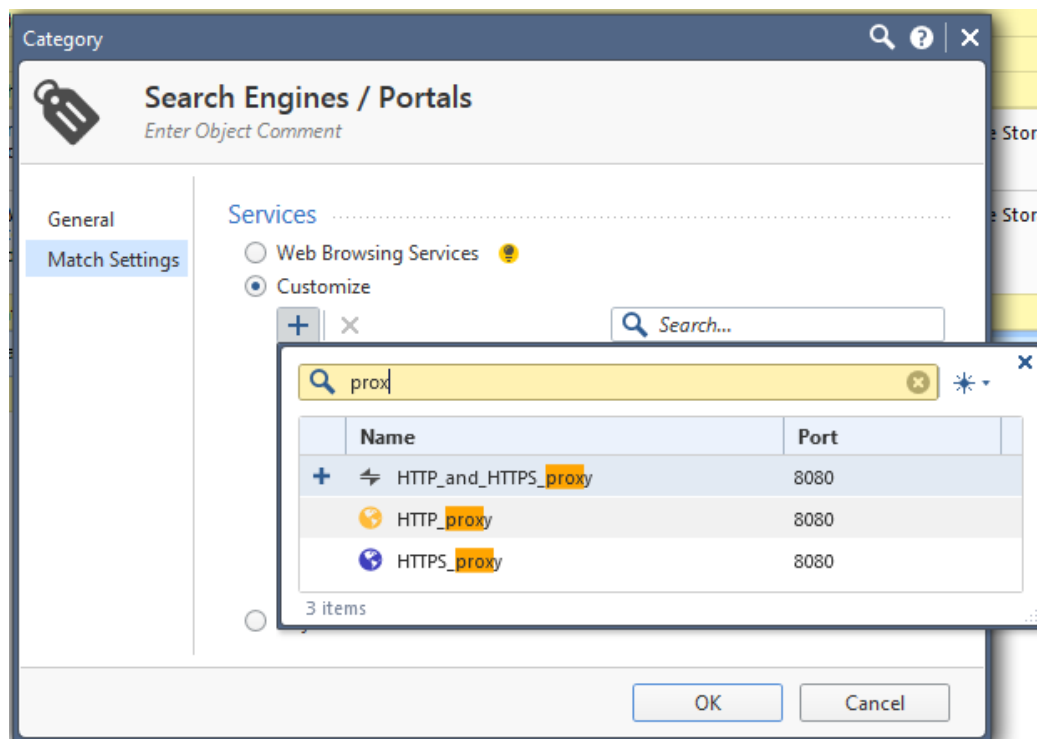
Name	Comments
http	Hypertext Transfer Protocol
https	HTTP protocol over TLS/SSL
HTTPS_proxy	
HTTP_proxy	



# Matching of Application, URLF and Content Objects

## Services associated with Applications, URLF Categories and Content Types

- You can configure the services a dedicated application signature and/or URLF category object is matching for
  - Doing so, you overwrite the “Application Control Web Browsing Services” associated with this object
  - You increase complexity in your environment and should consider carefully if there is a real need



- Double click on the object and select the “match settings” menu.
- Customize the services you want this object to “match for”.



# Matching of Application, URLF and Content Objects

## Services associated with Applications, URLF Categories and Content Types

- The same concept applies to objects of the **Content Awareness Blade**

Supported Services

Name	Comments
ftp	File Transfer Protocol
http	Hypertext Transfer Protocol
HTTPS_proxy	
HTTP_proxy	
smtp	Simple Mail Transfer Protocol

Application Control & URL Filtering

Content Awareness Settings

Fail Mode

In case of internal system error:

Allow all requests (fail-open)

Block all requests (fail-close)

Supported Services

Name	Comments
ftp	File Transfer Protocol
http	Hypertext Transfer Protocol
https	HTTP protocol over TLS/SSL
HTTPS_proxy	

Data Inspection

Inspect archives

HTTP Inspection

Enable HTTP inspection on non standard ports for Content Awareness

OK Cancel

# LOGGING

How can we achieve more visibility on the **connections** related to an application layer **session**?

How can we see in **one place** the **applications** used or the content accessed?

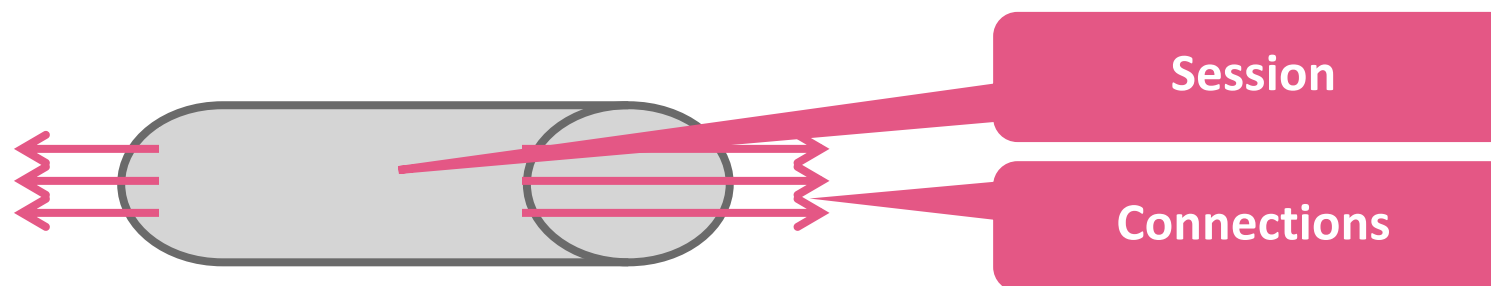




# Connections And Sessions

## 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”



# Logging

## Unified Logging Cards – see all in one place

Let's follow the logs for the highlighted rules

3	DNS	 net_192.168.169.0  net_192.168.170.0	* Any	 dns	* Any	 Accept	— None
4	ICMP	 net_192.168.169.0	 web+mail...	 icmp-proto	* Any	 Accept	— None
▼ 5	Intranet	 net_192.168.169.0	 web+mail...	 Web Browsing	* Any	 WebServerPolicyLaye	— N/A
5.1	Spreadsheets including credit card num	 net_192.168.169.0	 web+mail...	 Web Browsing	 Download Traffic  Spreadsheets_incl_CreditCardNumbers	 Drop  Blocked Messa...	 Extended Log  Accounting
5.2	Block credit card numbers	 net_192.168.169.0	 web+mail...	 Web Browsing	 Download Traffic  PCI - Credit Card Numbers	 Drop  Blocked Messa...	 Extended Log  Accounting
5.3	Documents	 net_192.168.169.0	 web+mail...	 Web Browsing	 Upload Traffic  Document File	 Accept	 Extended Log  Accounting
5.4	Spreadsheets	 net_192.168.169.0	 web+mail...	 Web Browsing	 Download Traffic  Spreadsheet File	 Accept	 Extended Log  Accounting



# Logging

## Unified Logging Cards – see all in one place

Log Details

**Accept**  
http Traffic Accepted from 192.168.169.1 to WebMailServer\_Site(192.168.170.10)

Details | Matched Rules | URLs | Files

**Log Info**

Origin: gwR8010  
Time: 07 May 17, 09:50:47  
Blade: Content Awareness, Application Control  
Product Family: Access  
Type: Session

**Application / Site**

Application Name: WebMailServer\_Site  
Primary Category: Custom Application/Site  
Additional Categor..: Custom Application/Site, Medium Risk  
Application Risk: Medium  
Server Type: Apache  
Client Type: Google Chrome

**Session**

Policy: Accept  
Policy Management: mgnt  
Policy Name: Simple\_Policy  
Policy Date: 07 May 17, 11:19:23  
Layer Name: WebServerPolicyLayer  
Access Rule Name: Documents  
Access Rule Numb...: 5.3

**Accounting**

**Web Traffic**

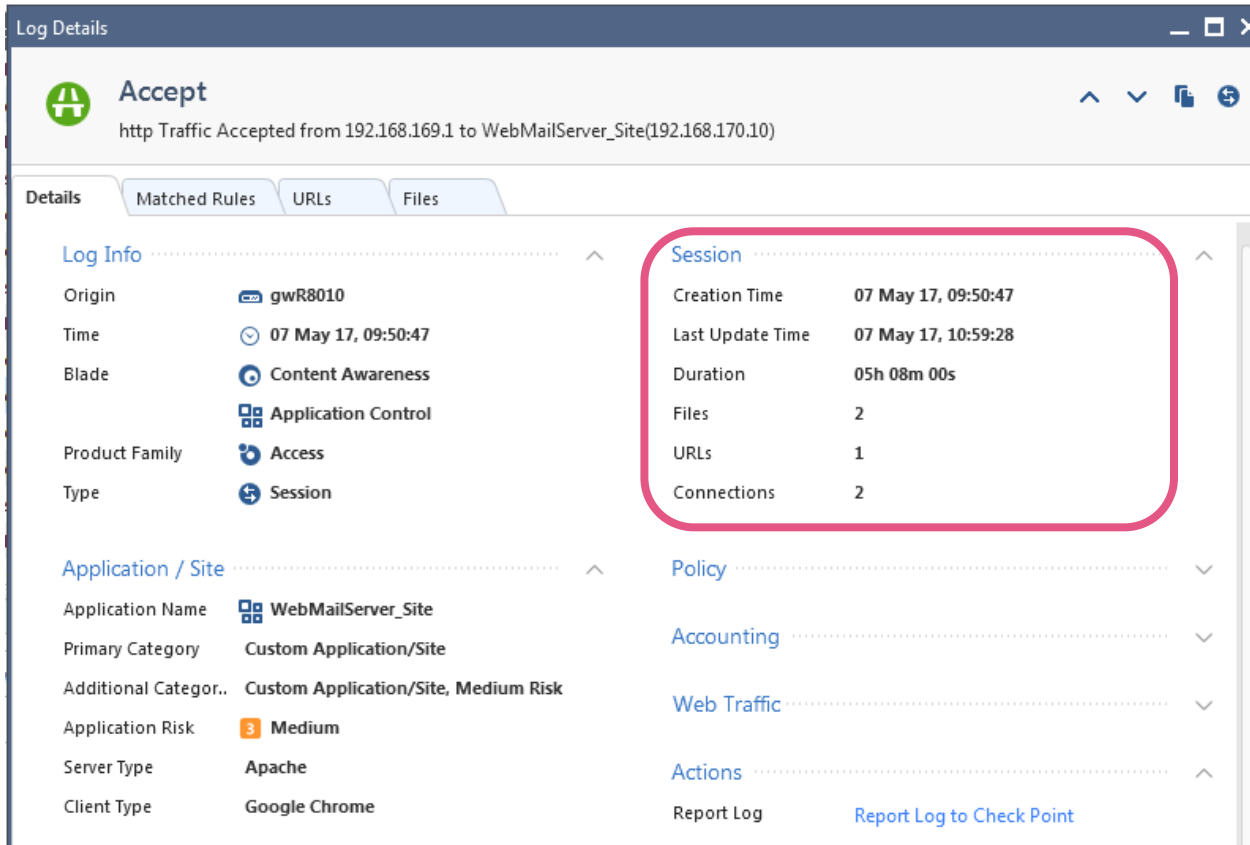
**Actions**

Report Log: Report Log to Check Point

- Software Blades
- Applications
- Policy triggered
- Policy Layer involved

# Logging

## Unified Logging Cards – see all in one place



Log Details

Accept  
http Traffic Accepted from 192.168.169.1 to WebMailServer\_Site(192.168.170.10)

Details Matched Rules URLs Files

Log Info

Origin gwr8010

Time 07 May 17, 09:50:47

Blade Content Awareness

Product Family Application Control

Product Family Access

Type Session

Application / Site

Application Name WebMailServer\_Site

Primary Category Custom Application/Site

Additional Categor.. Custom Application/Site, Medium Risk

Application Risk Medium

Server Type Apache

Client Type Google Chrome

Session

Creation Time 07 May 17, 09:50:47

Last Update Time 07 May 17, 10:59:28

Duration 05h 08m 00s

Files 2

URLs 1

Connections 2

Policy

Accounting

Web Traffic

Actions

Report Log [Report Log to Check Point](#)

- Session details
  - When it started
  - How long it has been established
  - How many files have been transmitted
  - Which URLs have been used
  - How many connections are related



# Logging

## Unified Logging Cards – see all in one place

The screenshot shows the 'Log Details' window for an 'Accept' event. The main title is 'http Traffic Accepted from 192.168.169.1 to WebMailServer\_Site(192.168.170.10)'. Below the title are tabs for 'Details', 'Matched Rules', 'URLs', and 'Files'. The 'Details' tab is active, displaying several expandable sections:

- File Operation**: Data Type: Document File
- Traffic**: Source: 192.168.169.1, Destination: web+mailserver (192.168.170.10), Service: http (TCP/80), Protocol: HTTP, Interface: eth1, Connection Direct...: Internal
- Web Traffic**: Resource: http://192.168.170.10/word2010\_unprotect..., Method: GET, User Agent: Chrome, Referrer: http://192.168.170.10/filedownload.html, Client Type Os: Windows 7/Server 2008 R2, Server Type: Apache
- Accounting**: Browse Time: 00h 00m 00s

Other sections include Log Info, Application / Site, Session, Policy, and Actions (Report Log, Report Log to Check Point).

- File Operation
- Source, destination and direction
- Time
- URL and resources



# Logging

## Unified Logging Cards – see all in one place

Log Details

**Accept**  
http Traffic Accepted from 192.168.169.1 to WebMailServer\_Site(192.168.170.10)

Details | **Matched Rules** | URLs | Files

Matched Rules

Rule	Layer	Rule Name	Action	Application	Category
5	Simple_Policy Netw...	Intranet	Inline	WebMailServer_...	Custom Application...
5.3	WebServerPolicyLayer	Documents	Accept	WebMailServer_...	Custom Application...

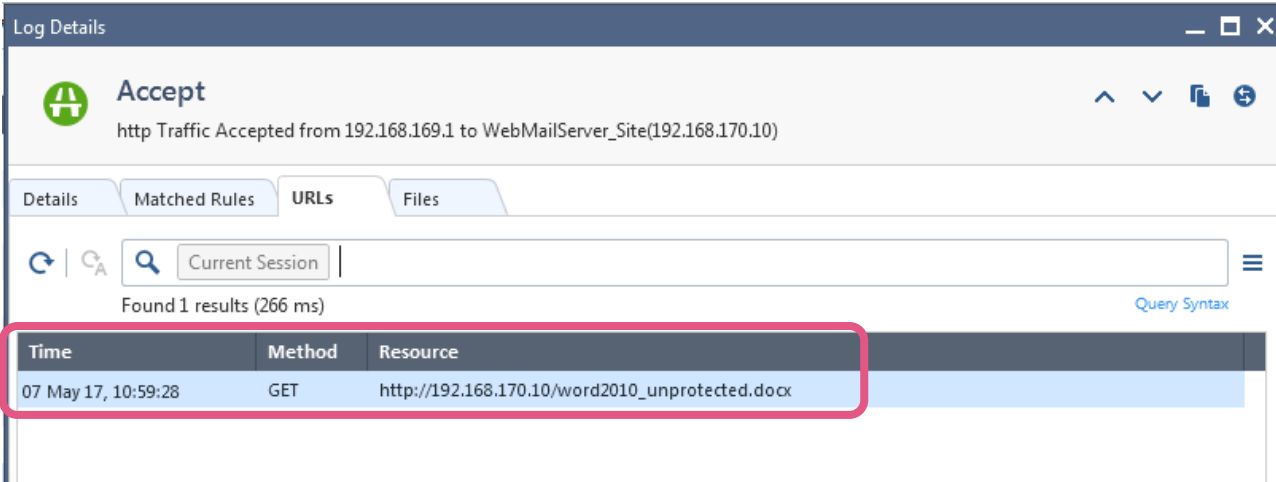
- Matched Rules and Layers
- Actions
- Application and category

3	DNS	net_192.168.169.0 net_192.168.170.0	* Any	dns	* Any	Accept	None
4	ICMP	net_192.168.169.0	web+mail...	icmp-proto	* Any	Accept	None
▼ 5	Intranet	net_192.168.169.0	web+mail...	Web Browsing	* Any	WebServerPolicyLaye	N/A
5.1	Spreadsheets including credit card num	net_192.168.169.0	web+mail...	Web Browsing	Download Traffic Spreadsheets_incl_CreditCardNumbers	Drop Blocked Messa...	Extended Log Accounting
5.2	Block credit card numbers	net_192.168.169.0	web+mail...	Web Browsing	Download Traffic PCI - Credit Card Numbers	Drop Blocked Messa...	Extended Log Accounting
5.3	Documents	net_192.168.169.0	web+mail...	Web Browsing	Upload Traffic Document File	Accept	Extended Log Accounting
5.4	Spreadsheets	net_192.168.169.0	web+mail...	Web Browsing	Download Traffic Spreadsheet File	Accept	Extended Log Accounting

Rule base

# Logging

## Unified Logging Cards – see all in one place



Log Details

Accept  
http Traffic Accepted from 192.168.169.1 to WebMailServer\_Site(192.168.170.10)

Details | Matched Rules | **URLs** | Files

Current Session

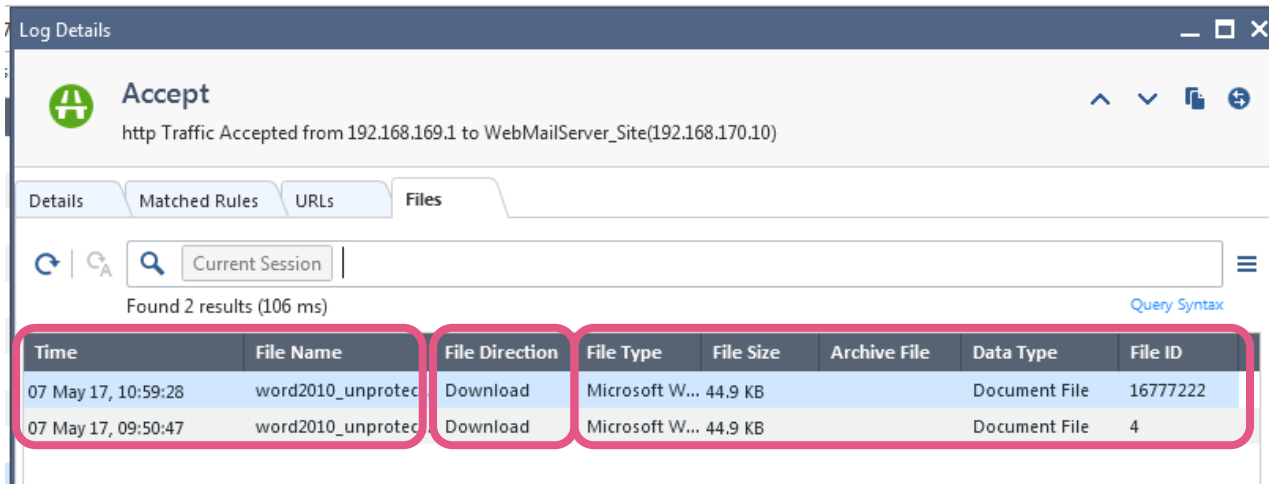
Found 1 results (266 ms) [Query Syntax](#)

Time	Method	Resource
07 May 17, 10:59:28	GET	http://192.168.170.10/word2010_unprotected.docx

- Complete URL

# Logging

## Unified Logging Cards – see all in one place



Log Details

Accept  
http Traffic Accepted from 192.168.169.1 to WebMailServer\_Site(192.168.170.10)

Details | Matched Rules | URLs | Files

Current Session

Found 2 results (106 ms)

Time	File Name	File Direction	File Type	File Size	Archive File	Data Type	File ID
07 May 17, 10:59:28	word2010_unprotect...	Download	Microsoft W...	44.9 KB		Document File	16777222
07 May 17, 09:50:47	word2010_unprotect...	Download	Microsoft W...	44.9 KB		Document File	4

- Content (here: file name)
- Direction
- Content details





# Connections And Sessions

## Connection log messages

- The Firewall Blade logging is telling us...
  - Who has performed a connection (or attempted to do so)
  - When this connection (or attempt) took place
- These logs are **Connection** log messages
  - Connection log messages will be created for TCP connections, UDP pseudo connections and other services like for example ICMP packets

Time	Blade	Action	Type	Interfa...	Origin	Source	Destination	Service	Access Rule...	Access Rule Name
21 Apr 17, 13:47:14	Firewall	Accept	Connection	eth0	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.4	Cleanup rule
21 Apr 17, 13:47:14	Firewall	Accept	Connection	eth0	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.4	Cleanup rule
21 Apr 17, 13:47:13	Firewall	Accept	Connection	eth0	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.4	Cleanup rule
18 Apr 17, 14:10:29	Firewall	Block	Connection	eth1	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.1	Credit Card Numbers
18 Apr 17, 14:10:29	Firewall	Accept	Connection	eth0	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.4	Cleanup rule



# Connections And Sessions

## Session log messages

- When enabling Application Control, URL Filtering or the Content Awareness Blade additional **Session** based logging is provided

Time	Blade	Action	Type	Interfa...	Origin	Source	Destination	Service	Access Rule...	Access Rule Name
21 Apr 17, 13:54:24	Multiple Blades	Drop	Session	eth1	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.4	Block Archive Files
21 Apr 17, 13:54:24	Firewall	Accept	Connection	eth0	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.5	Cleanup rule
21 Apr 17, 13:53:41	Multiple Blades	Accept	Session	eth1	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.2	Documents
21 Apr 17, 13:53:41	Firewall	Accept	Connection	eth0	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.2	Documents

- A **Session** log message contains information related to the application or content

Time	Blade	Action	Type	Interfa...	Origin	Source	Destination	Service	Access Rule...	Access Rule Name
21 Apr 17, 13:53:41	Multiple Blades	Accept	Session	eth1	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.2	Documents

Click on the "Connections" tab to see the Connections details related to this Session

For Content Awareness Sessions we see Connection details like file type, data type and direction

Time	File Name	File Direction	File Type	File Size	Access Rule	Access Rule ID
21 Apr 17, 13:54:24	word2010_unprotected.d...	Download	Microsoft Word		word2010_unprotected.zip	Document File 16777221
21 Apr 17, 13:53:41	word2010_unprotected.d...	Download	Microsoft Word	44.9 KB		Document File 3



# Connections And Sessions

## Configuration of the Logging options

No.	Name	Source	Destination	Services & Applicat...	Content	Action	Track
▼ 4	Parent rule for web server	* Any	web+mailserver	Web Browsing	* Any	WebServerPolicyLayer	N/A
4.1	Credit Card Numbers	* Any	web+mailserver	Web Browsing	Download Traffic PCI - Credit Card Numbers	Drop Content Management	Detailed Log
4.2	Documents	* Any	web+mailserver	Web Browsing	Download Traffic Document File	Accept	Detailed Log Accounting
4.3	Spreadsheets	* Any	web+mailserver	Web Browsing	Download Traffic Spreadsheet or CSV File	Accept	Extended Log Accounting
4.4	Cleanup rule	* Any	* Any	* Any	* Any	Accept	Log

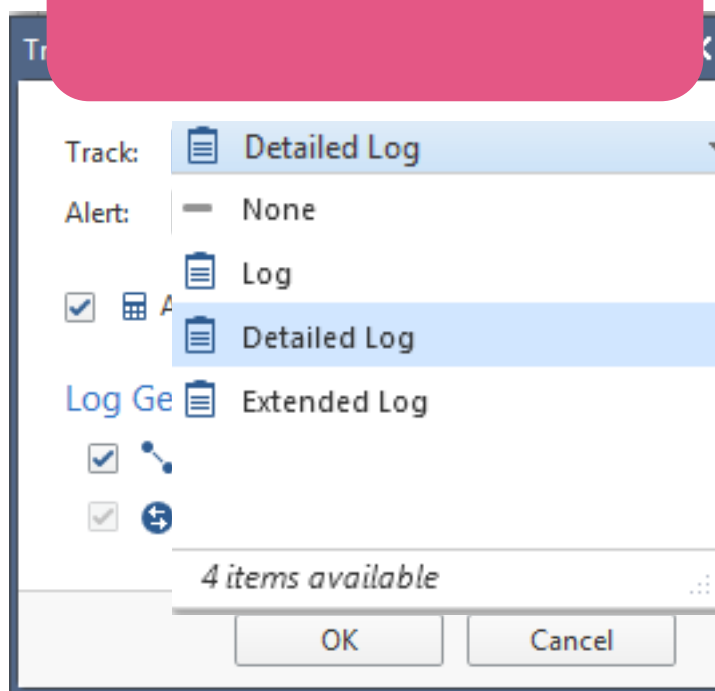
- **Log**: track source, destination, source port and destination port
- **Detailed Log**: in addition to “Log” the name of the application that has matched
  - Requires APCL, URLF or Content Awareness Blade being active
- **Extended Log**: in addition to “Log” the URLs and Files related to the session
- **Accounting**: the amount of data exchanged

# Connections And Sessions

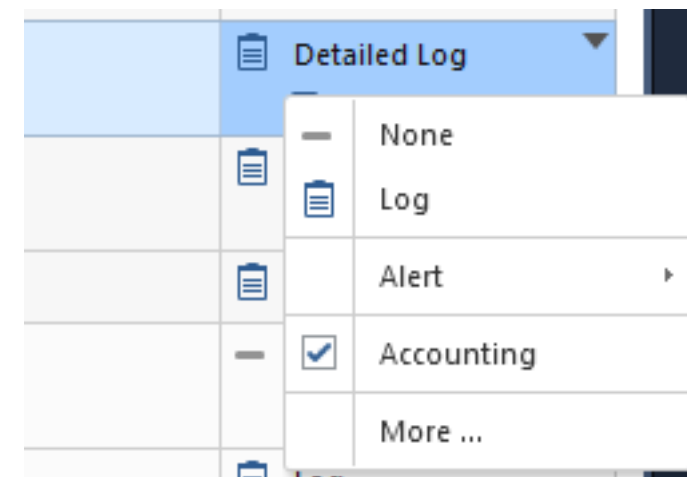
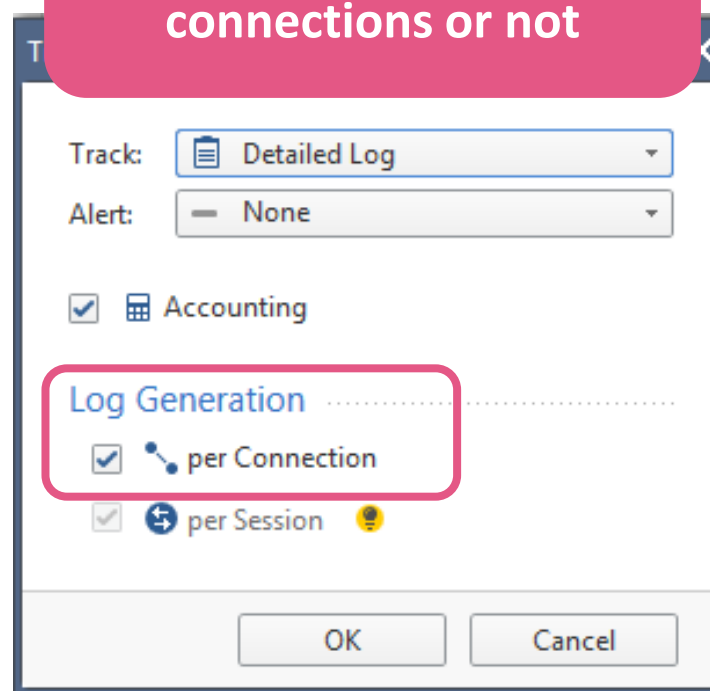
## Configuration of the Logging options

- Change the logging options using a right click on the track column

Select the track option



Select logs to be generated per connections or not



What is this good for?

You can provide **visibility** how many TCP connections are related to an application session.



Check Point®  
SOFTWARE TECHNOLOGIES LTD

# CONTENT AWARENESS

Obtaining visibility and control  
about files and data

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION

# INTRODUCTION

The **Content Awareness** Blade provides new capabilities controlling **File Types, Content Types** and the **direction of transport** (up-, download or both)

Matching for **content** is part of the **Unified Rule base** matching process

The Content Awareness logic engine is **running in the kernel**



What is Content Awareness good for?

You can use it to **learn** about content and the related traffic volume traversing your network, **educate** users in their behavior and **enforce** content related sharing policies.



# Introduction to Content Awareness

## Visibility and enforcement

- The Content Awareness Blade provides **visibility and enforcement** based on the **content transmitted** in the data streams through the security gateway
  - You can activate the Blade in conjunction with Application Control, URL Filtering and HTTPS inspection, Mobile Access, IPsec VPN and Identity Awareness
- Content Awareness is working with **File Types, Content Types** and **Direction**
  - You can control File Types and Content Types independent from each other in a rule or use group objects as a combination of both

No.	Name	Source	Destination	Services & Applicat...	Content	Action	Track
▼ Content Awareness (11-14)							
11	Spreadsheets including credit card details	net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic ▲ Spreadsheets including credit card details	Accept	Extended Log Accounting
12	Block credit card numbers in any other file or as text	net_192.168.169.0	web+mailserver	Web Browsing	Any Direction ▲ PCI - Credit Card Numbers	Drop Blocked Message -...	Extended Log
13	Documents	net_192.168.169.0	web+mailserver	Web Browsing	Upload Traffic ▲ Document File	Accept	Extended Log Accounting
14	Spreadsheets	net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic ▲ Spreadsheet File	Accept	Extended Log Accounting
▶ Outbound (15)							



# Introduction to Content Awareness

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

- Controlling File Types, Content Types and Direction

Spreadsheets including credit card details	net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic Spreadsheets including credit card details	Accept
Block credit card numbers in any other file or as text	net_192.168.169.0	web+mailserver	Web Browsing	Any Direction PCI - Credit Card Numbers	
Documents	net_192.168.169.0	web+mailserver	Web Browsing	Upload Traffic Document File	
Spreadsheets	net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic Spreadsheet File	

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

**Remember this example!**

**Data Type Group object name**

**File Type (s) that must match**

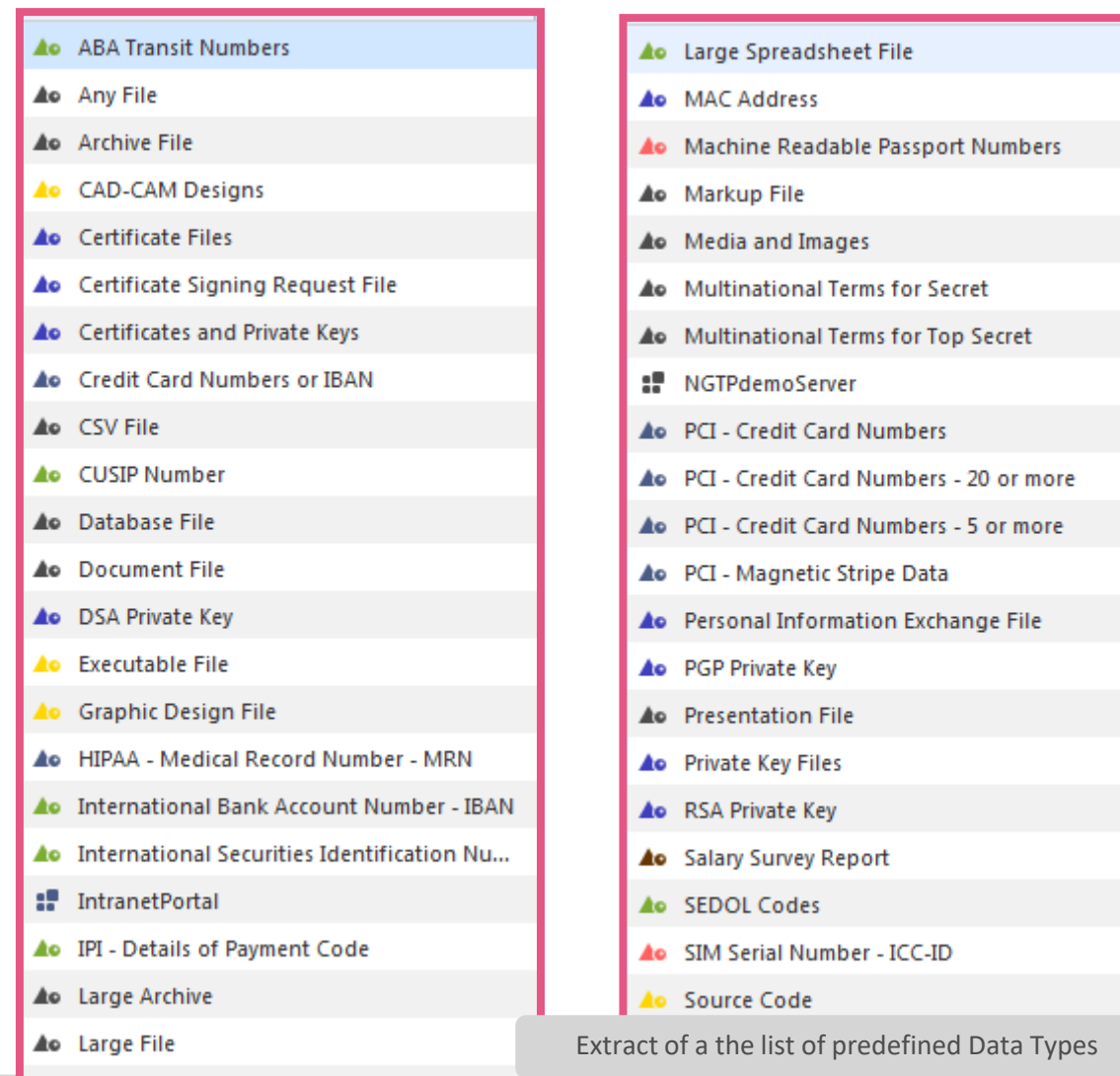
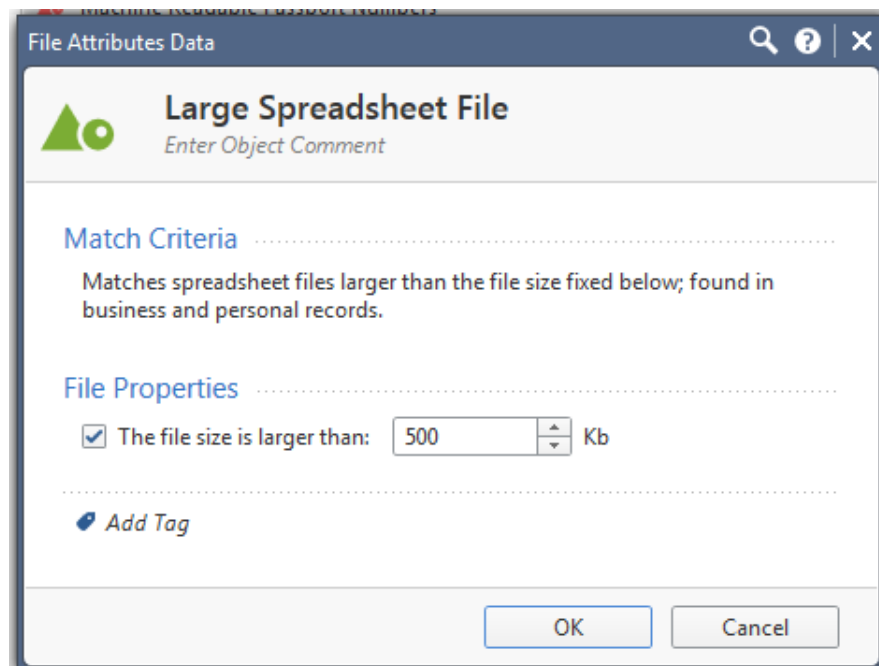
**Content Type(s) that must match**



# Introduction to Content Awareness

## Predefined Data Types

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





# Introduction to Content Awareness

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

- Which of the rules below would **only** block **Spreadsheets** that have **Credit Card Numbers** as content? Only 1), only 2) or would both rules work?

1)

Source	Destination	Services & Applications	Content	Action
net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic Spreadsheets_incl_CreditCard...	Drop

2)

Source	Destination	Services & Applications	Content	Action
net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic PCI - Credit Card Numbers Spreadsheet File	Drop







Multiple objects in one rule are OR related

- Only rule 1 would achieve your objective
- Rule 2 would match for **Credit Card Numbers** content **OR** files of type **Spreadsheet**

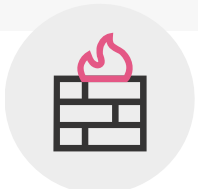


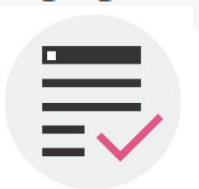


# Introduction to Content Awareness

- **Matching** for content **is part of the Unified Policy** matching process
- All elements (columns) of a rule are considered for matching

Source	Destination	Services & Applications	Content	Action
 net_192.168.169.0	 web+mailserver	 Web Browsing	 Download Traffic  Spreadsheets_incl_CreditCard...	 Drop

 Firewall	 Firewall	 Application Control	 Content Awareness
---	---	--	--

Look at competitive products:\*

**Some match a rule only based on the application signature. After the match is done, content is verified. With these solutions your content control is limited to application signatures matching!**

# Introduction to Content Awareness

## A quick look on the competition

- PAN does handle content using the construction of **Security Profiles**
  - **Security Profiles are checked after the rule has matched** for application signature or URL category

## Security Profiles

While security policies enable you to allow or block traffic on your network, security profiles help you define an *allow but scan* rule, which scan allowed applications for threats, such as viruses, malware, spyware, and DDOS attacks. When traffic matches the allow rule defined in the security policy, the security profile(s) that are attached to the rule are applied for further content inspection rules such as antivirus checks and data filtering.



Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy.

**Source:** <https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/policy/security-profiles>



# USE CASES

# Content Awareness

## Planning and implementation considerations

- **Planning** Content Awareness

- Requires a detailed planning phase and a **dialog with business process managers** and not only with technical and security administrators
- Consider **UserCheck** functionalities for educating employees



### Benefit of Policy Layers

- Create a **dedicated Ordered Layer**
- Create rules for **monitoring**
- **Unified Logging** will provide visibility

### Benefit of Delegation

- Create a **dedicated administrative Role**

# 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.

WHAT YOU WANT TO  
KEEP IN MIND



# Content Awareness – Monitoring Content

## What you want to keep in mind

- You can now filter for “type:Session” and look at the log messages

The screenshot displays the Check Point management console interface. On the left, a log table is filtered for 'type:Session', showing 8 results. A red arrow points to the log entry at 'Today, 13:51:38' with 'Multiple Blades' as the blade and 'Accept' as the action. Below this, a search for 'Current Session' shows 1 result for 'excel\_formated\_2010.xlsx'. On the right, the 'Log Details' window for the selected entry is shown, with a red box highlighting the 'Log Info' section. A pink callout box points to the 'Log Info' section with the text: 'You see the Blades involved in the matching process'.

Time	Blade	Action	Type
Today, 13:51:45	Multiple Blades	Accept	Session
Today, 13:51:40	Multiple Blades	Accept	Session
Today, 13:51:38	Multiple Blades	Accept	Session
Today, 13:25:31	Multiple Blades	Accept	Session
Today, 13:25:31	Application Control	Accept	Session
Today, 13:15:18	Firewall	Accept	Session
Today, 13:14:54	Multiple Blades	Accept	Session
Today, 13:14:22	Firewall	Accept	Session

Time	File Name	File Direction
Today, 13:51:38	excel_formated_2010.xlsx	Download

Log Info	Value
Origin	gwR8010
Time	Today, 13:51:38
Blade	Application Control
	Content Awareness
Product Family	Access
Type	Session

Application / Site	Policy
Application Name	ContentDemo
Primary Category	Custom Application/Site
Additional Categor..	Custom Application/Site, Medium Risk
Application Risk	Medium
Server Type	Apache
Client Type	Google Chrome
Action	Accept
Policy Management	mgnt
Policy Name	SimplePolicy
Policy Date	Today, 13:41:39
Layer Name	SimplePolicy Network
Access Rule Name	Parent rule for web server
Access Rule Numb...	4



# Content Awareness – Monitoring Content

## What you want to keep in mind

- You can see the type of content that was matched (here: File Operations)

The screenshot shows a log entry for an 'Accept' action. The 'Files' tab is selected, showing a table with file details:

Time	File Name	File Direction
Today, 13:51:38	excel_formated_2010.xlsx	Download

The detailed view also shows the following information:

- Log Info:** Origin: gwR8010, Time: Today, 13:51:38, Blade: Application Control, Product Family: Access, Type: Session.
- Session:** Creation Time: Today, 13:51:38, Last Update Time: Today, 13:51:40, Duration: 00h 01m 00s, Files: 1, URLs: 1, Connections: 1.
- Application / Site:** Application Name: ContentDemo, Primary Category: Custom Application/Site, Additional Categor.: Custom Application/Site, Medium Risk, Application Risk: Medium, Server Type: Apache, Client Type: Google Chrome.
- Policy:** Action: Accept, Policy Management: mgnt, Policy Name: SimplePolicy, Policy Date: Today, 13:41:39, Layer Name: SimplePolicy Network, Access Rule Name: Parent rule for web server.
- File Operation:** Data Type: Spreadsheet File.

You see the file name

File Operation  
Data Type: Spreadsheet File

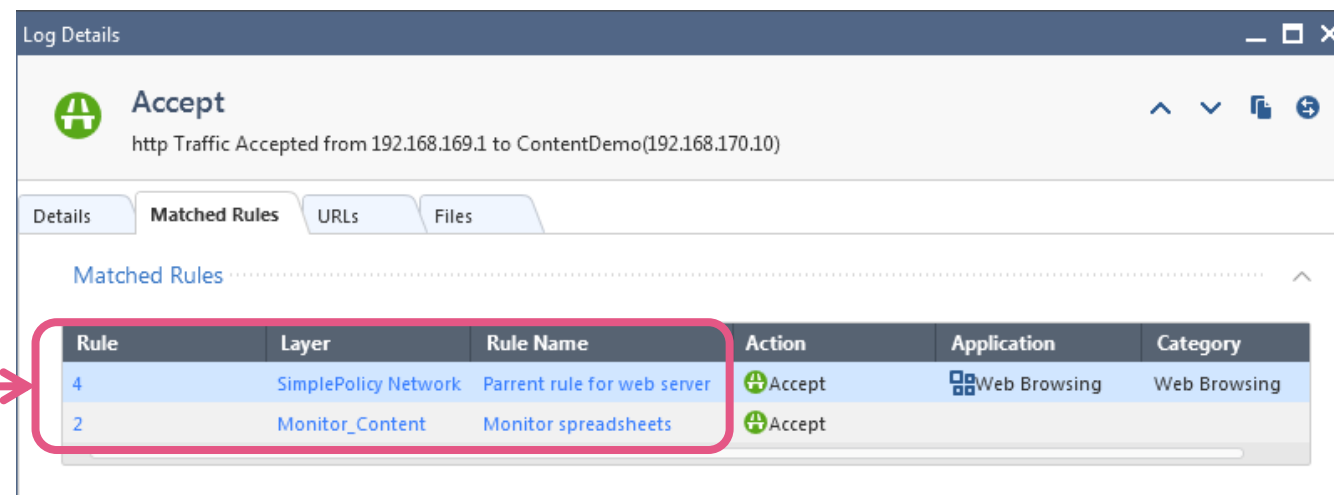
You see the Data Type

# Content Awareness – Monitoring Content

## What you want to keep in mind

- You can see the rules that have matched


Rule number and Policy Layer



The screenshot shows the 'Log Details' window with the 'Matched Rules' tab selected. A table lists the rules that matched the traffic. A red box highlights the first two rows, and a red arrow points from the text 'Rule number and Policy Layer' to the 'Rule' and 'Layer' columns of the first row.

Rule	Layer	Rule Name	Action	Application	Category
4	SimplePolicy Network	Parent rule for web server	Accept	Web Browsing	Web Browsing
2	Monitor_Content	Monitor spreadsheets	Accept		

- You can see the URLs that have been accessed



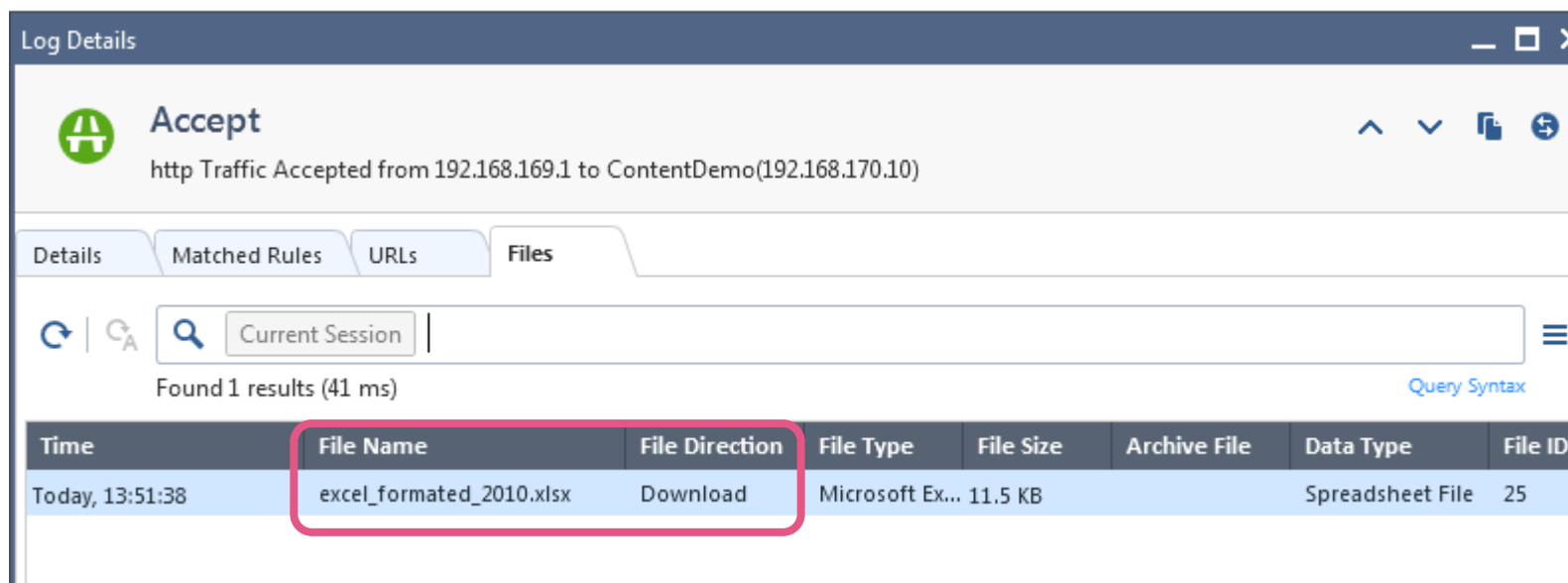
The screenshot shows the 'Log Details' window with the 'URLs' tab selected. A search bar is visible with the text 'Current Session' and a magnifying glass icon. Below the search bar, it says 'Found 1 results (114 ms)'. A table lists the accessed URLs.

Time	Method	Resource
Today, 13:51:40	GET	http://192.168.170.10/creditcard.txt

# Content Awareness – Monitoring Content

## What you want to keep in mind

- You can see the name of the file and the direction (upload or download)



The screenshot shows the 'Log Details' window in Check Point. The main event is 'Accept' with the description 'http Traffic Accepted from 192.168.169.1 to ContentDemo(192.168.170.10)'. The 'Files' tab is selected, showing a search for 'Current Session' with 1 result found. A table below lists the file details:

Time	File Name	File Direction	File Type	File Size	Archive File	Data Type	File ID
Today, 13:51:38	excel_formated_2010.xlsx	Download	Microsoft Ex...	11.5 KB		Spreadsheet File	25



# DETAILS ABOUT CONTENT TYPES



# Content Awareness – File and Content Types

- Supported File and Content Types – [sk114640](#)
  - Detection is done locking at the beginning of the file
  - Some file types can be extracted from archives (check sk114640 for details)

File Type	FILE ID	File Group	Common Extensions	Text / Archive Extraction
Zip	1	Archive	zip	Yes (compressed with deflate algorithm)
Microsoft Word	2	Word	docx	Yes
Microsoft Excel	3	Spreadsheet	xlsx	Yes
Microsoft PowerPoint	4	Presentation	pptx	Yes
PDF	101	Viewer	pdf	Yes
JPEG	103	Image	jpg, jpeg	
Executable	105	Executable	exe, com, dll, drv, pif, qts, qtx, sys, scr, vbx, vxd	

- Content types
  - Some examples: Credit card (PCI), Medical data (HIPA), Design (CAD)
  - Detecting Data Types requires inspecting the file until the end
- You want to have Content Type rules below File Type rules in order to achieve a high performance



# Content Awareness – File and Content Types

- Use the Object Explorer for getting an overview about file types and data types

The screenshot shows the 'Object Explorer' interface. On the left, under 'Categories', 'Data Types (4)' is selected. The main table lists the following items:

Name	Comments	Tags	Modifier	Last Modified
PCI - Magnetic Stripe Data			System	
PCI - Credit Card Numbers			System	
PCI - Credit Card Numbers...				
PCI - Credit Card Numbers...				

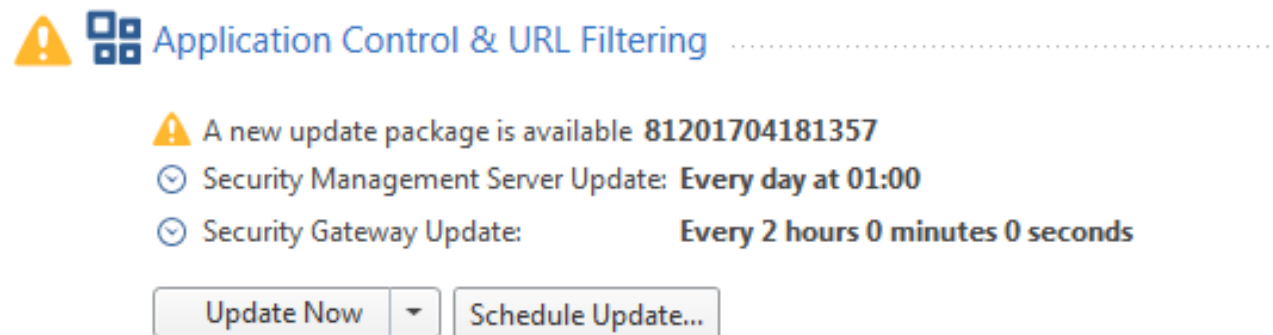
A detail window titled 'Compound Data' is open for 'PCI - Credit Card Numbers - 5 or more'. It contains the following information:



- Match Criteria**: Related to Payment Card Industry (PCI); matches data containing credit card numbers such as MasterCard, Visa, JCB and more.
- Example**: 4580-0000-0000-0000.
- Add Tag**: A button to add a tag.


- Use the right click and edit to see details


# Content Awareness – File and Content Types


- Data types are updated from the cloud using the same process like Application Control
- Access Policy > Updates



  Application Control & URL Filtering .....

 A new update package is available **81201704181357**

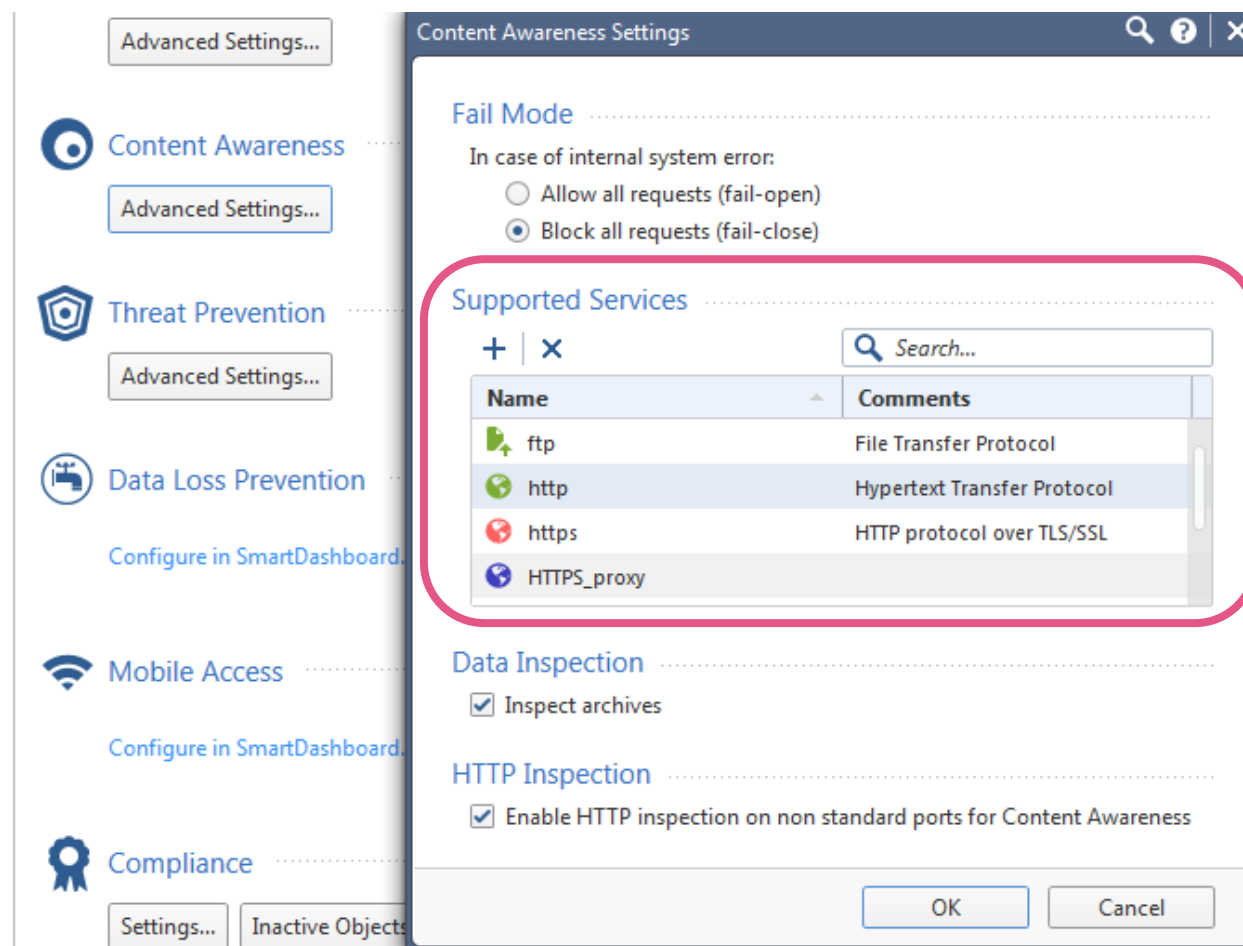
 Security Management Server Update: **Every day at 01:00**

 Security Gateway Update: **Every 2 hours 0 minutes 0 seconds**

- This process may change in the future

# Content Awareness – Supported Services

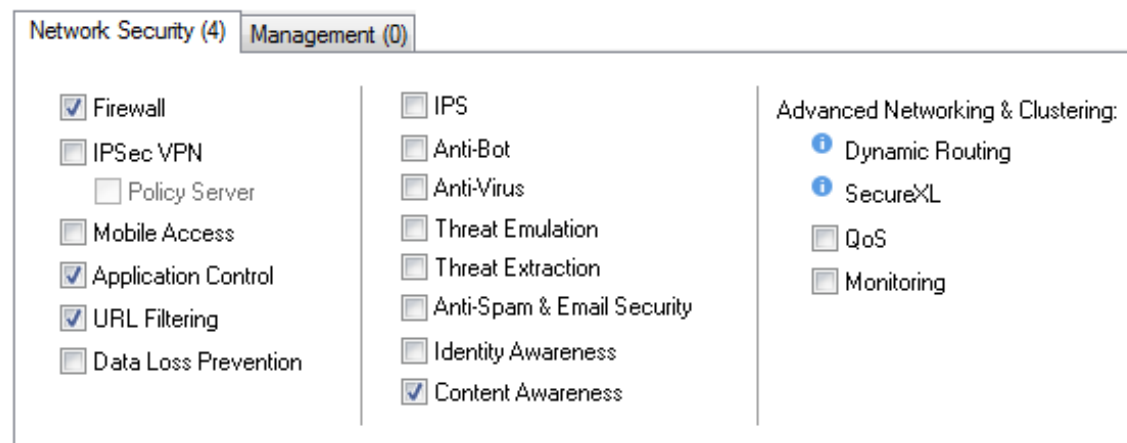
- You can see the services associated with the Content Awareness Blade in Manage & Settings > Blades > Content Awareness > Advanced Settings
  - Services are http, https, http\_proxy, https\_proxy, ftp and smtp.
  - You can add services that are based on http, https, ftp or smtp protocols
  - Currently zip archives are supported up to six levels.
    - You can configure this default level
    - When exceeding this value the “Fail Mode” operation will be executed



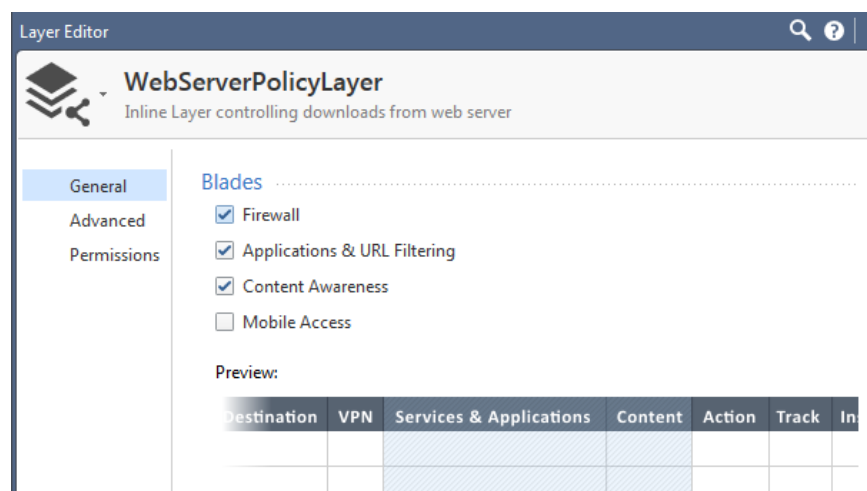
**R80.10 includes a new protocol parser for ftp and security servers are not used for Content Awareness.**

# Content Awareness – Enabling the Blade

- Enable the Blade on the gateway and on the policy
- Gateway properties
  - VSX Gateways are supported



- Policy Layer properties



# Licensing

- Information provided by Product Management 8<sup>th</sup> May 2017

“Content Awareness blade is part of R80.10.

We’re **providing it free-of charge** to all customers/products.

All new products (and renewals) will receive by default the license of the new blade.

Existing **customers upgrading to R80.10 can use the eval-license** when activating the blade.

The eval-license has no expiration date and no warnings.”



Check Point®  
SOFTWARE TECHNOLOGIES LTD

# SECURITY ZONES

A method describing the topology

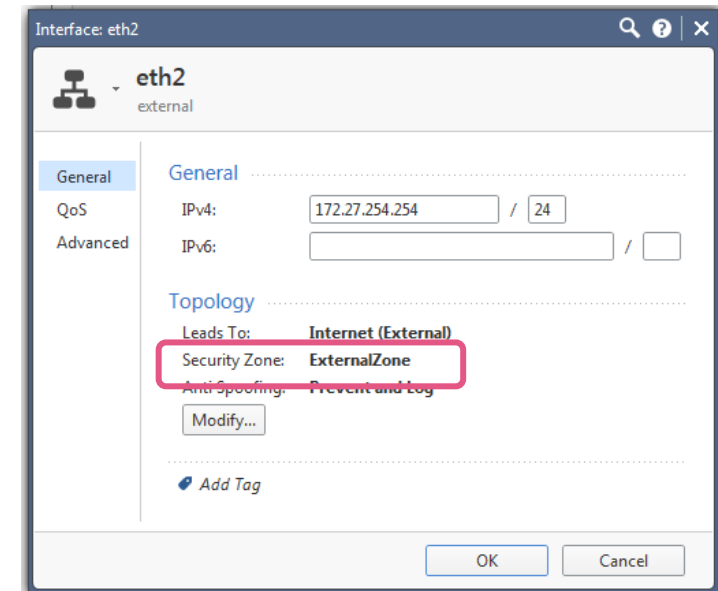
WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION



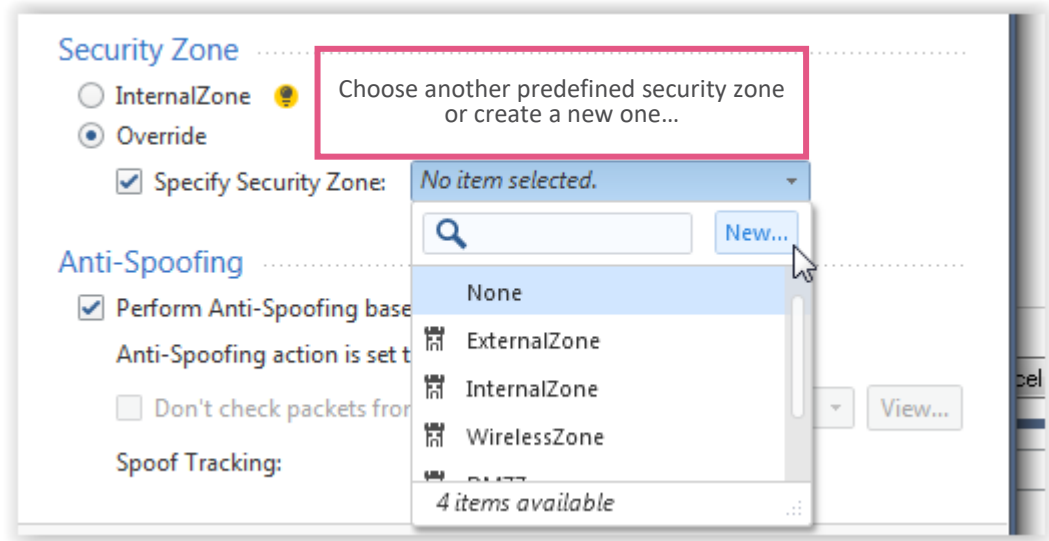
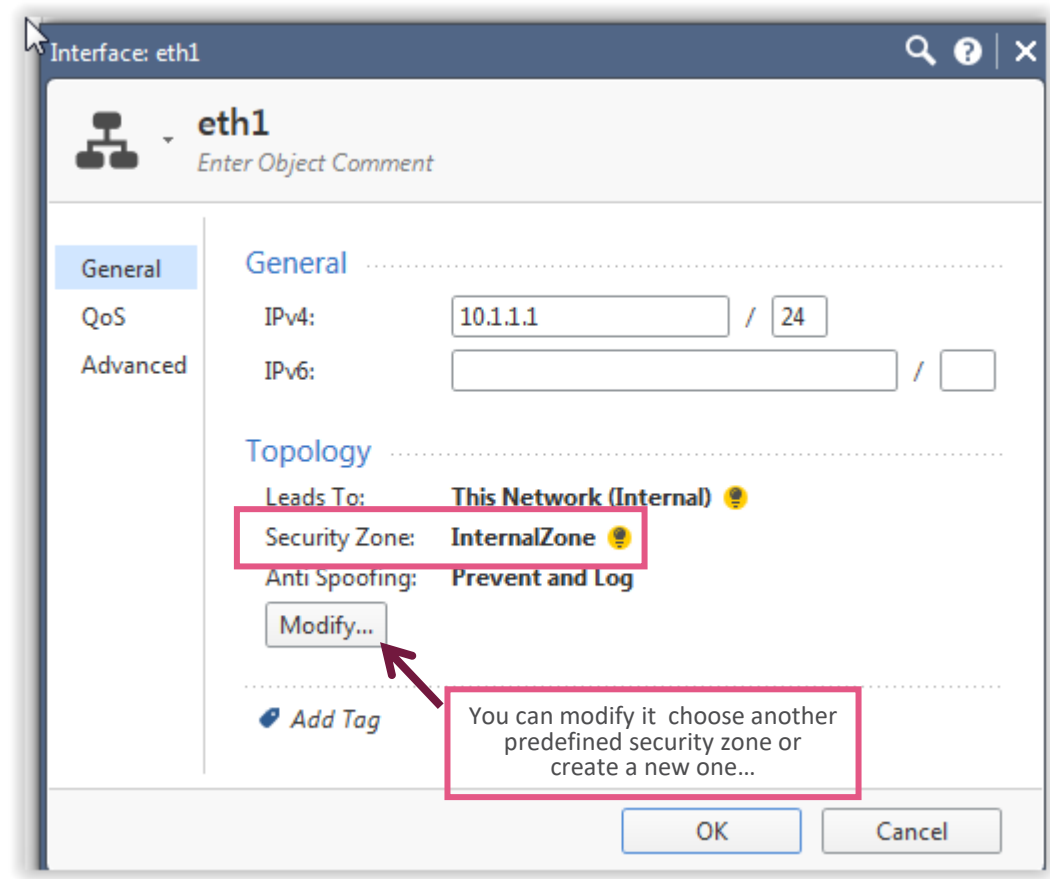
# Security Zones – What they are

- Security zones are logical objects to which one or more network interfaces are associated used to define the network topology
- Benefits:
  - Simplified security policy where the same granular rule can be applied on many gateways
  - Allows the administrators to add internal networks without updating the security policy
  - Security zones objects are supporting acceleration



# Security Zones – How you can use them

- Set the security zone on the interface



















# Security Zones – How you can use them

- The current implementation works independent of the Anti-Spoofing functionality
- As a result you need defining Anti-Spoofing reflecting the IP network topology of your network






The screenshot displays the configuration interface for interface 'eth2' (external) and the 'Topology Settings' dialog box. The interface shows the 'General' tab with fields for IPv4 and IPv6 addresses. The 'Topology' section shows 'Leads To' set to 'Internet (External)', 'Security Zone' set to 'ExternalZone', and 'Anti Spoofing' set to 'Prevent'. The 'Topology Settings' dialog box is open, showing the 'Leads To' section with 'Override' selected and 'Internet (External)' chosen. The 'Security Zone' section has 'User defined' selected, with 'Specify Security Zone' checked and 'ExternalZone' selected. The 'Anti-Spoofing' section has 'Perform Anti-Spoofing based on interface topology' checked, with 'Anti-Spoofing action is set to' 'Prevent'.

# Security Zones – How you can use them

- Use Security Zone in an Access Control rule
  - You can use Security Zone objects just like any other source or destination object

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action
1	Management	 net_192.168.169.0	 gwR8010	* Any	 ssh	* Any	 Accept
2	ICMP	 net_192.168.169.0	 net_192.168.170.0	* Any	 icmp-proto	* Any	 Accept
3	DNS	 ManagementZone  PublishedZone	 dnserver  OpenDNS	* Any	 dns	* Any	 Accept

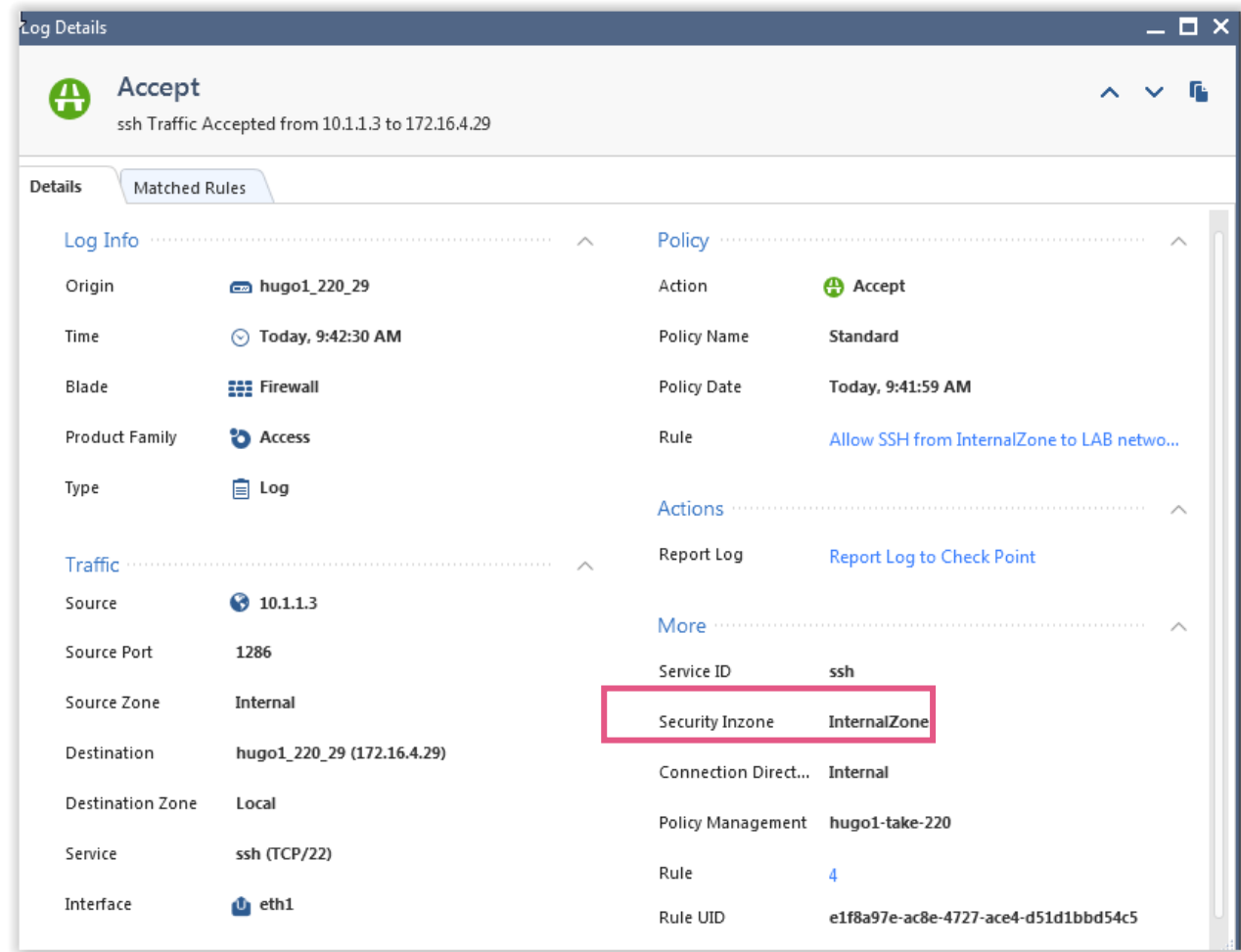
- You can use Security Zone objects as well in Threat Prevention rules

No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track
▶ 1	Protecting Email Servers	 PublishedZone	– N/A	 Strict 	 Log  Packet Capture

- Security Zones are **not supported in NAT rules**

# Security Zones – How can you use them

- SSH traffic from InternalZone to my LAB networks will be matched on the rule and allowed:



The screenshot shows the 'Log Details' window for an 'Accept' action. The traffic is identified as 'ssh Traffic Accepted from 10.1.1.3 to 172.16.4.29'. The 'Matched Rules' tab is active, showing a rule named 'Allow SSH from InternalZone to LAB netwo...'. The 'Traffic' section shows the source as 10.1.1.3 and the source zone as 'Internal'. The 'Policy' section shows the action as 'Accept' and the security zone as 'InternalZone', which is highlighted with a red box.

Section	Field	Value
Log Info	Origin	hugo1_220_29
	Time	Today, 9:42:30 AM
	Blade	Firewall
	Product Family	Access
	Type	Log
Traffic	Source	10.1.1.3
	Source Port	1286
	Source Zone	Internal
	Destination	hugo1_220_29 (172.16.4.29)
	Destination Zone	Local
	Service	ssh (TCP/22)
	Interface	eth1
	Policy	Action
Policy Name		Standard
Policy Date		Today, 9:41:59 AM
Rule		Allow SSH from InternalZone to LAB netwo...
Actions		Report Log to Check Point
Service ID		ssh
Security Inzone		InternalZone
More	Connection Direct...	Internal
	Policy Management	hugo1-take-220
	Rule	4
Rule UID	e1f8a97e-ac8e-4727-ace4-d51d1bbd54c5	



# Summary

- We learned what Security Zones are
- What they can be used for



Check Point®  
SOFTWARE TECHNOLOGIES LTD

# DOMAIN OBJECTS

Using Objects adhering to  
changing IP Addresses

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION

# REGULAR MODE

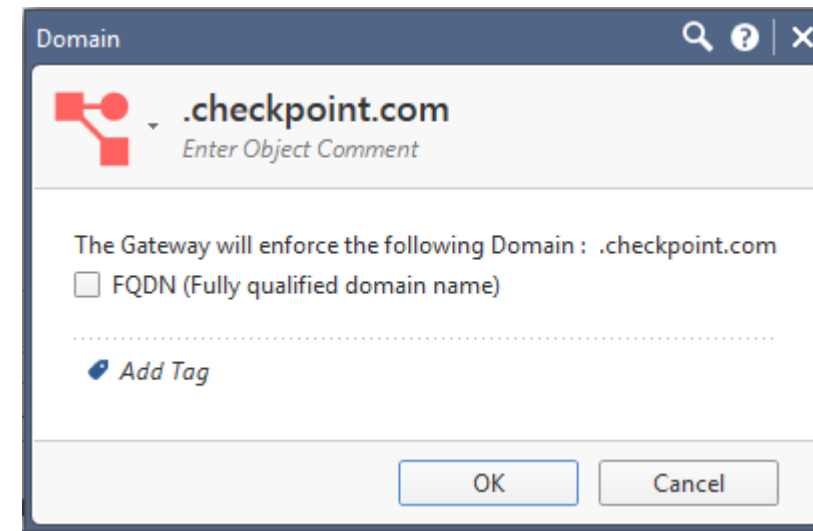


# How to describe a Domain as an object?

Working with R77.30 based security gateways.

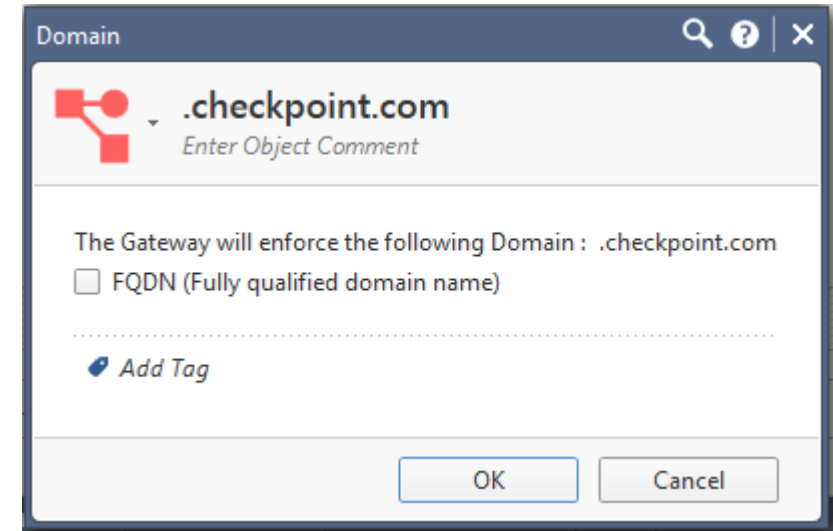
# Domain Object – Regular mode

- Regular mode (supported in older gateway versions)
  - Will match [checkpoint.com](https://www.checkpoint.com) and all of its sub-domains (for example: support.checkpoint.com)
  - Requires reverse DNS lookup (DNS server that is configured on the gateway should support reverse DNS queries)
  - For each connection reverse DNS query is sent to DNS server. The domain returned from the DNS query is being matched against the domain in the rule
  - The result is being cached on the gateway



# Domain Object – Regular mode

- This mode might be inaccurate because of:
  - Not all IP addresses have a reverse entry in the DNS server
  - Canonical Name record (CNAME record)
- In case the IP is not in the cache, the connection is being held till the reverse query returns.

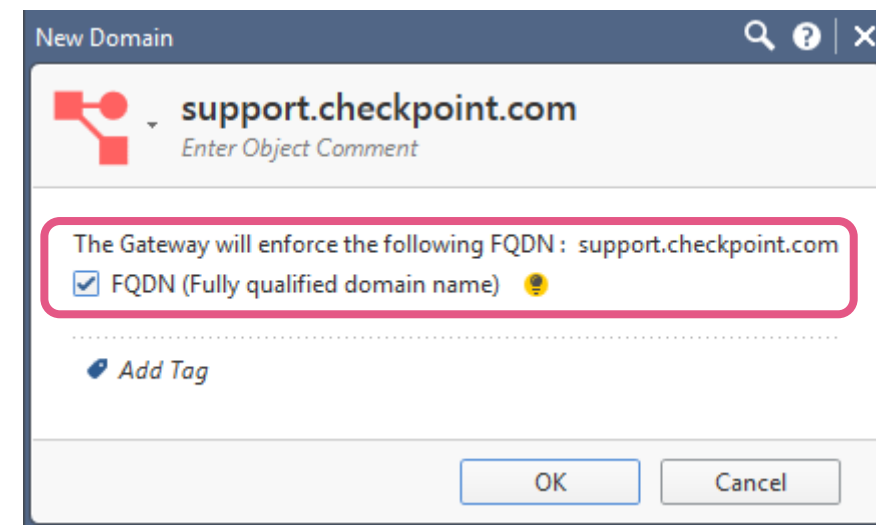


# FQDN MODE

The new Domain Object based on “FQDN mode”  
Overcoming incumbent challenges with Dynamic Objects and  
performance obstacles.

# Domain Object - FQDN mode (recommended)

- FQDN mode (supported only from R80.10)
  - Will match exactly the domain configured.  
In this example: support.checkpoint.com will match, but qa.support.checkpoint.com will NOT match
  - The gateway performs direct DNS query upon policy installation and caches the result
  - An additional DNS query is being sent every 30 seconds. The result will be accumulated to the existing IPs
  - Entry in cache expires after 1 hour
  - For each connection, the IP is looked up in the cache. If found, the domain in the cache is being matched against the domain in the rule





# Time Objects

- A Time Object is adding the time dimension to the matching process of a rule

## Example

A rule allowing access to dedicated resources can be active only during “working hours”

- In R80.10 Time are supported by SecureXL Connection Acceleration templates
  - In earlier versions all rules below a rule including a Time Object did no longer benefit from SecureXL Connection Acceleration

The screenshot shows the 'New Time' configuration window. The title bar reads 'New Time'. Below the title bar, there is a clock icon and the text 'Working hours' with a sub-label 'Enter Object Comment'. The window is divided into two main sections: 'Time Period' and 'Recurring'.  
**Time Period:** This section has two columns: 'Start' and 'End'. Under 'Start', there is a radio button for 'Immediately' (which is selected) and another for 'At: 5/7/2017 18:46'. Under 'End', there is a radio button for 'Never' (which is selected) and another for 'At: 5/7/2017 18:46'.  
**Recurring:** This section has a sub-section 'Hour Ranges' with three rows. The first row is checked and shows 'From: 08:00 To: 18:00'. The other two rows are unchecked and show 'From: 00:00 To: 00:00'. Below this is 'Day Recurrence' with three radio buttons: 'Daily', 'Days in week' (which is selected), and 'Days in month'. To the right of these are buttons for the days of the week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. At the bottom left of the window is an 'Add Tag' button, and at the bottom right are 'OK' and 'Cancel' buttons.



# Summary

- Gateways prior to R80.10 support Domain Objects – regular mode
- Gateways R80.10 support Domain Objects – FQDN mode
- FQDN mode is accelerated by SecureXL
- Dynamic and Time objects are now supported by SecureXL





Check Point®  
SOFTWARE TECHNOLOGIES LTD

# THREAT PREVENTION

Architecting the defense

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION

# SECURITY ARCHITECTURE

# Preventing Threats By Architecture

## Overview of the NGTP Threat Prevention Software Blades

- **IPS Software Blade**

- Blocking the attempt of **utilizing known vulnerabilities**
- Providing a large spectrum of signatures and configuration settings



- **Antivirus**

- Blocking **known malware** using signatures and heuristics
- Presenting flexible configuration options



- **Anti-Bot**

- Blocking **connections** to **Command & Control servers**
- Helping you to identify infected systems

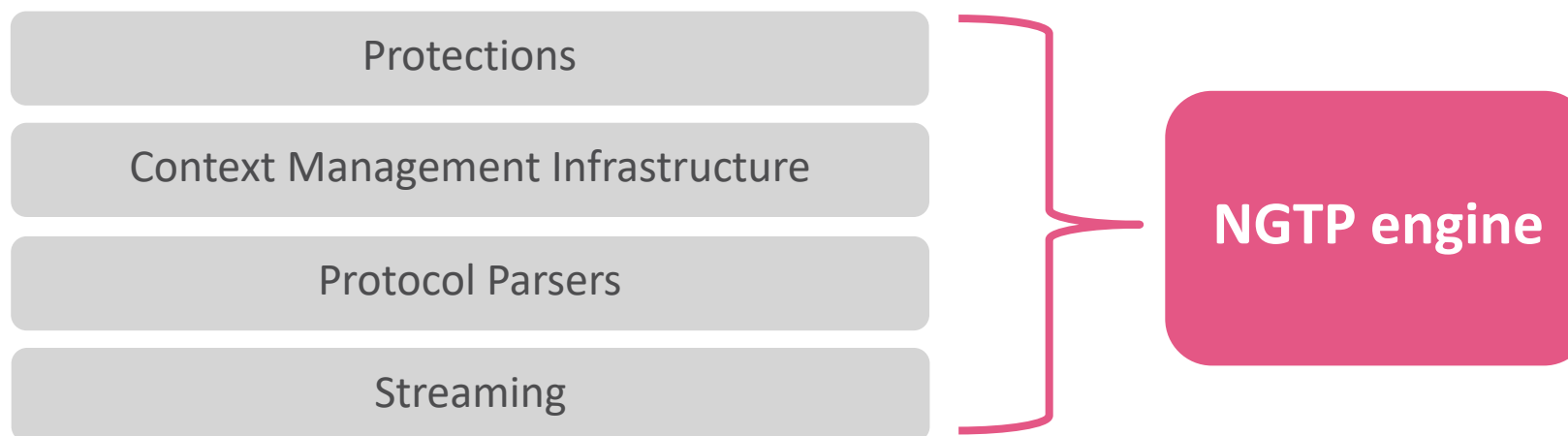


**Threat Extraction and Threat Emulation** Software Blades are part of the SandBlast portfolio and are not covered in this presentation

# Preventing Threats By Architecture

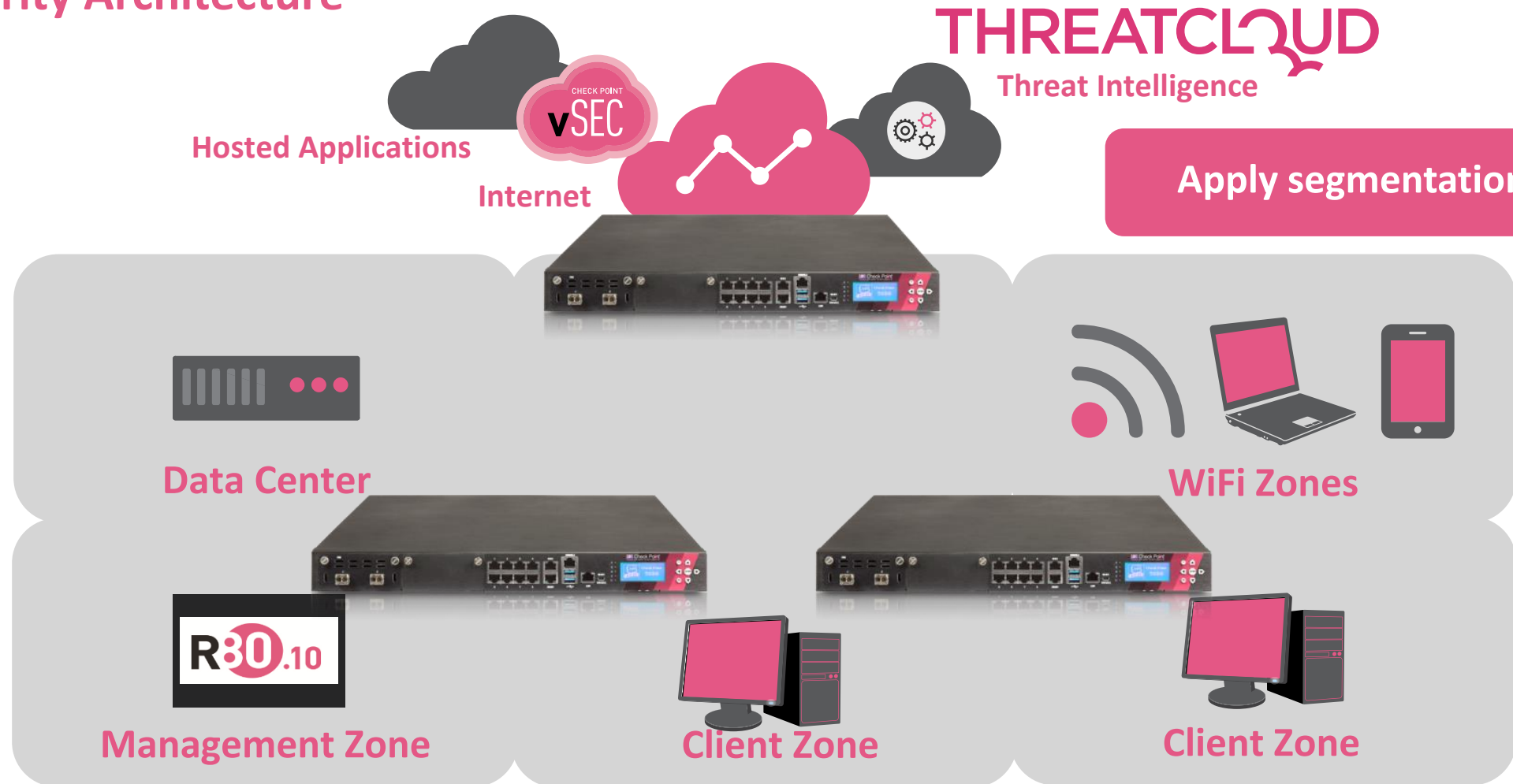
## Overview of the NGTP Software Blades

- All NGTP Software Blades are using the NGTP packet processing infrastructure
  - This architecture is documented in the [sk95193](#)
  - A dedicated presales training presentation is available
- Before enabling Threat Prevention Blades get familiar with the health status of your Security Gateway
  - Optimize the system before you enable Threat Prevention Software Blades
  - Refer to [sk98348](#) Best Practices – Security Gateway Performance



Where do we need Threat Prevention?

# Integrating Threat Prevention Security Architecture

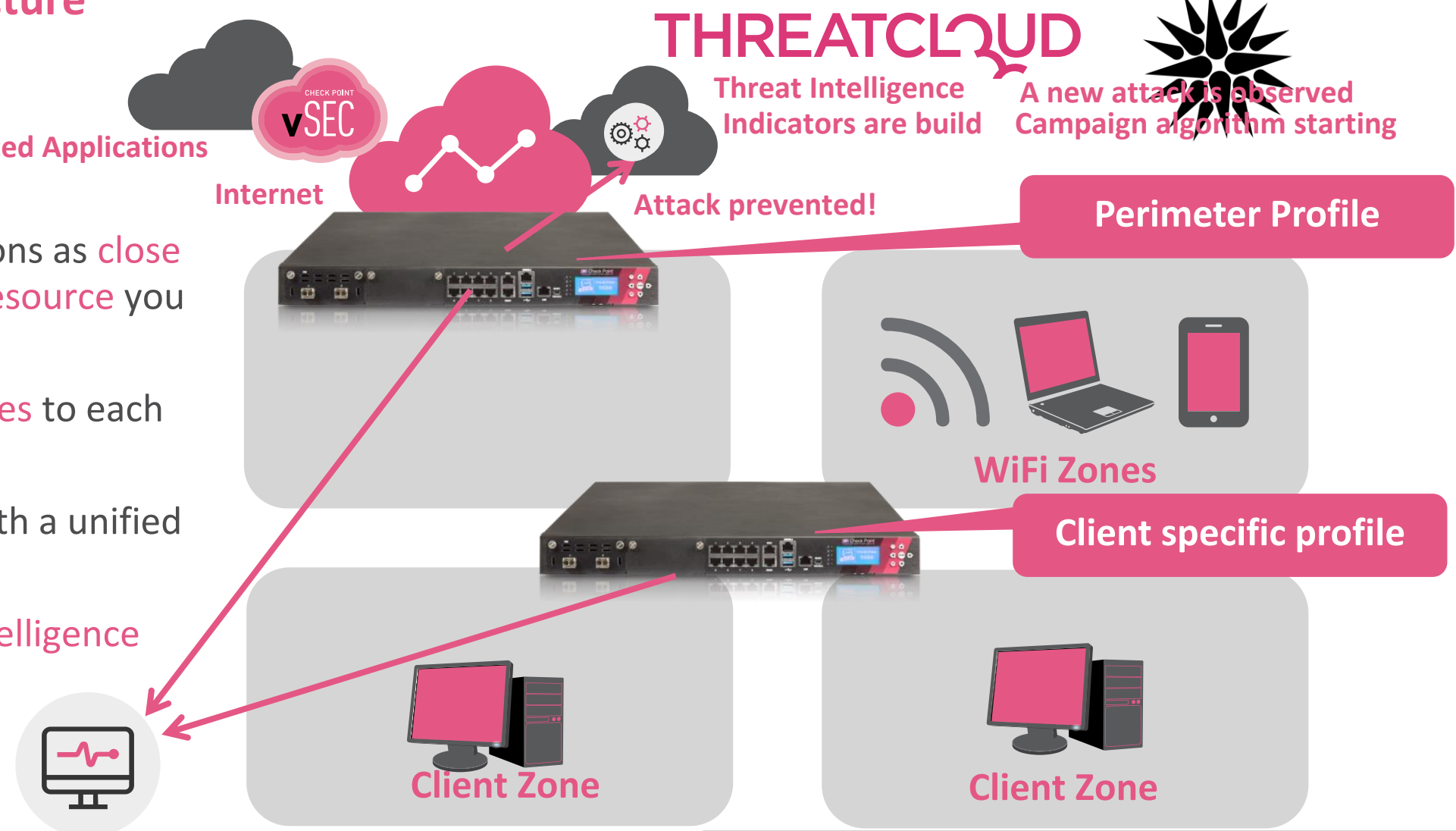


Animation has started – wait for next click until this is blinking

# Integrating Threat Prevention Security Architecture



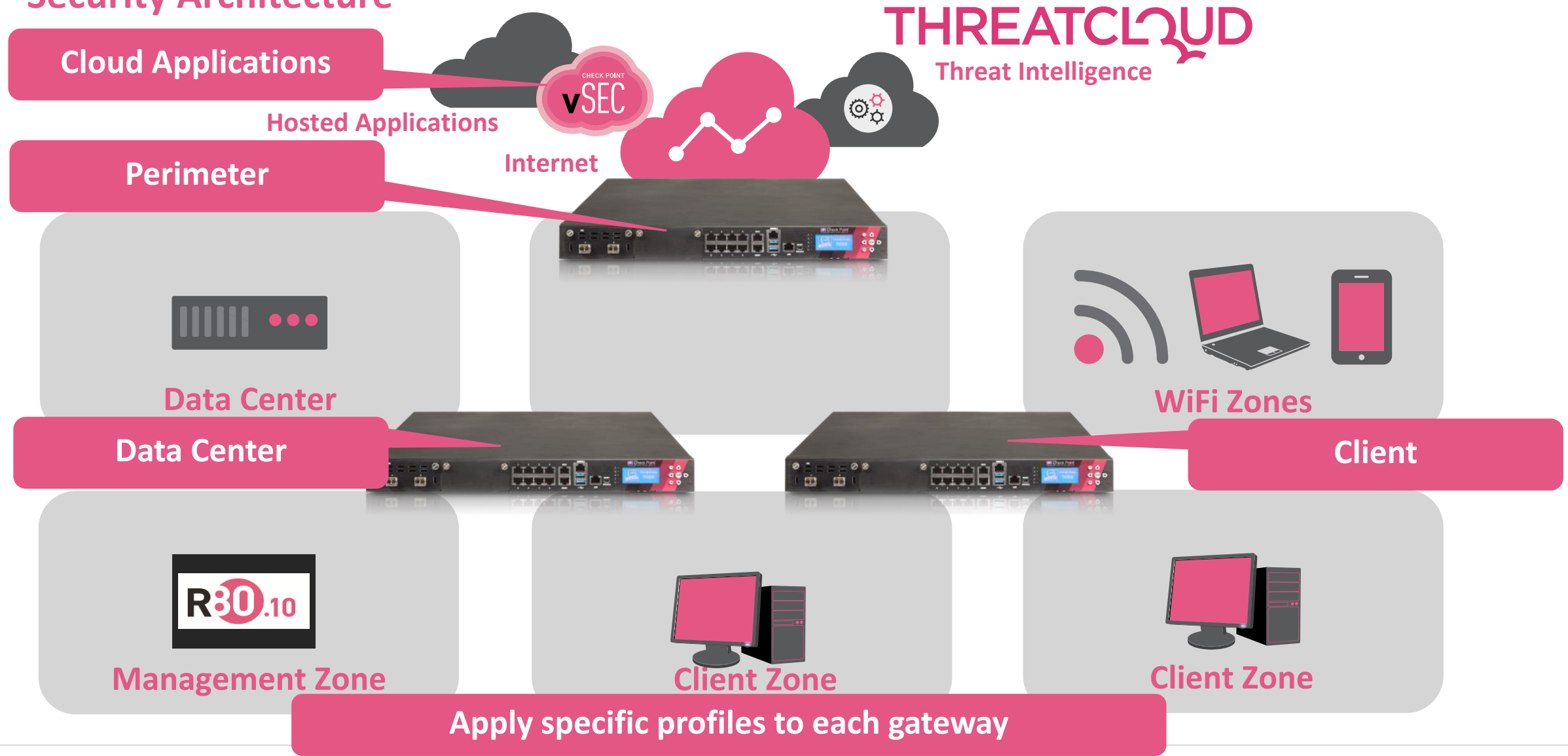
Check Point  
SOFTWARE TECHNOLOGIES LTD



- Place your protections as **close** as possible **to the resource** you want to protect
- Apply **specific profiles** to each enforcement point
- Achieve **visibility** with a unified management
- Leverage **Threat Intelligence**

Animation has started – wait for next click until this is blinking

# Integrating Threat Prevention Security Architecture





And now the training turns into a Sales Event.

This is annoying! Stop it!

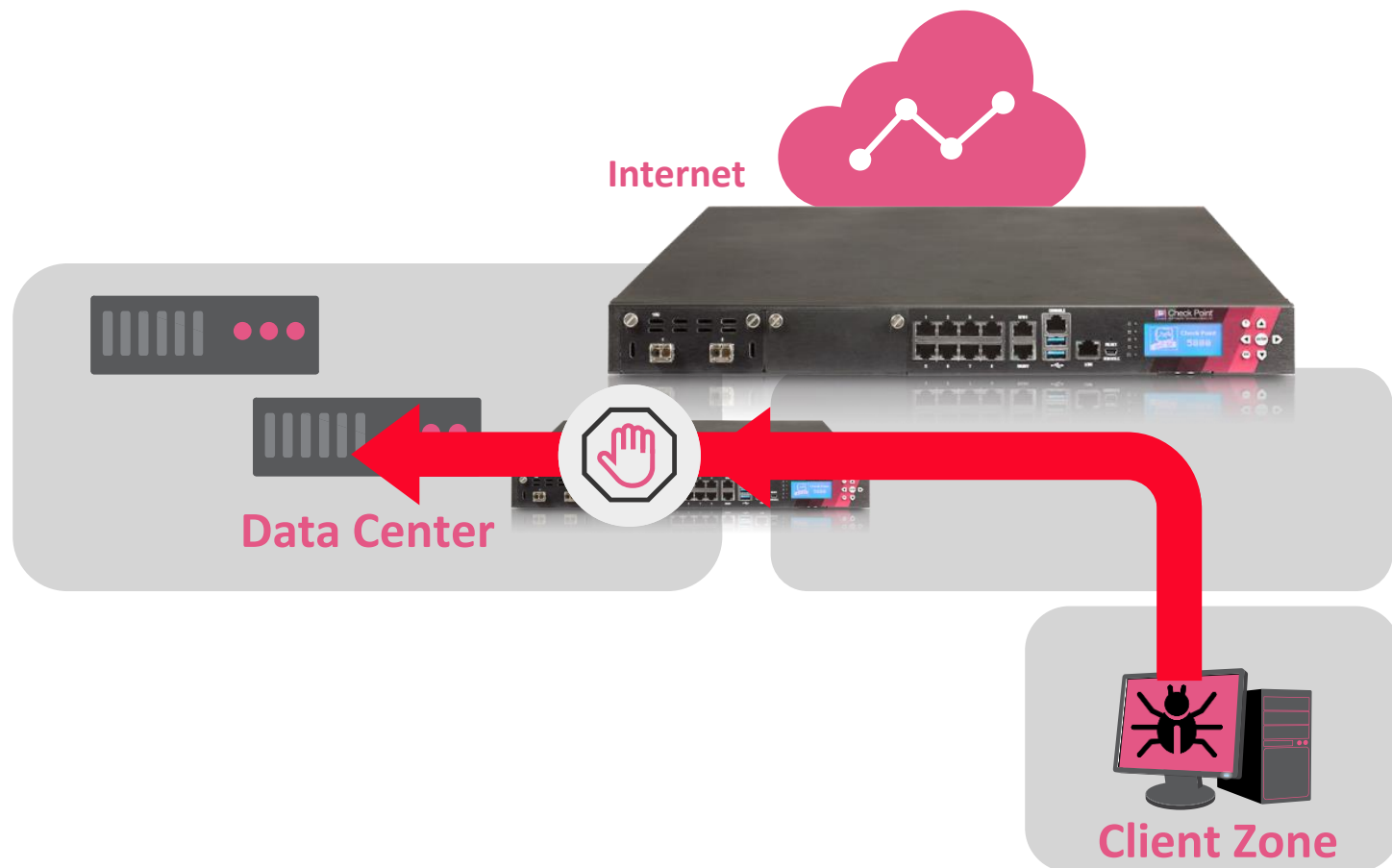
Remember that a recent Ransomware attack  
was more than annoying!

Would have architecture and IPS been helpful?



# Integrating Threat Prevention

## Security Architecture – Blocking Ransomware Shared Folder Attacks



- IPS signature blocking Ransomware Shared Folder Access
- Released: 30-Aug-2016



# Integrating Threat Prevention Security Architecture – Blocking Ransomware Shared Folder Attacks

Show selected profiles (1 out of 5)

View Actions Ransom

3 items

Protection	Industry Reference	Release Date	Update Date	Severity	Confidence...	Strict (Clone)*
Suspected Ransomware Dropzone	None	20/02/2017	15/03/2017	High	Medium	Shield
Ransomware Shared Folder Access	None	30/08/2016	14/05/2017	High	Medium	Shield
PDF File Containing Ransomware Downloader	None	21/05/2017	28/05/2017	High	Medium	Shield

Protection	Industry Reference	Release Date	Update Date
Suspected Ransomware Dropzone	None	20/02/2017	15/03/2017
Ransomware Shared Folder Access	None	30/08/2016	14/05/2017
PDF File Containing Ransomware Downloader	None	21/05/2017	28/05/2017

No Industry Reference – Released 30<sup>th</sup> Aug 2016 – Updated 14<sup>th</sup> May 2017

We are innovative – we started early – we don't stop improving


\* Stay tuned learning why a cloned profile is used in this example

Confidence: Common, Threat Prevalence: Common, Protection Tuning: Non-Configurable.

# IPS Protections Update Service

## Keep yourself and customers informed

When using IPS **subscribe to the Update Advisories** email service



Urgent Update

The following protections detect attacks seen in the wild; we advise to install the latest IPS online update

May

### New IPS Protections

Severity	Protection Name	R7x Profile		R80 Profiles	
		Recommended	Basic	Optimized	Strict
CRITICAL	Microsoft Malware Protection Engine Denial of Service (CVE-2017-8535)	✓	○	✓	✓
	Microsoft Malware Protection Engine Denial of Service (CVE-2017-8536)	✓	○	✓	✓
	Microsoft Malware Protection Engine Denial of Service (CVE-2017-8537)	✓	○	✓	✓
	Microsoft Malware Protection Engine Denial of Service (CVE-2017-8539)	✓	○	✓	✓

**Subscribe** to: <https://www.checkpoint.com/advisories/>



# Maintain the IPS Policy

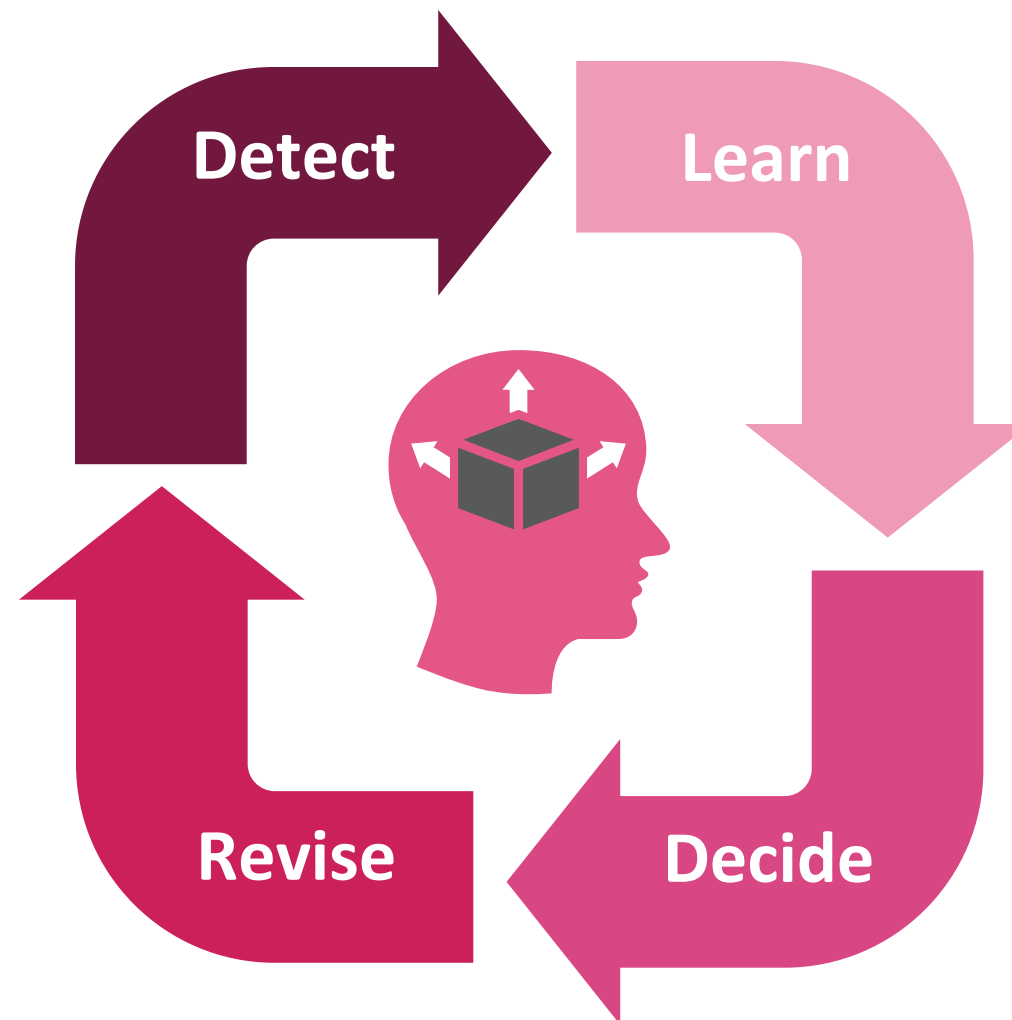
Never stop being attentive

- **Detect** and monitor
- **Learn** what is happening
- **Decide** setting protections **to prevent**
- **Revise** your policy

Let professionals help you

# THREATCLOUD

MANAGED SECURITY SERVICES



<https://www.checkpoint.com/support-services/threatcloud-managed-security-service/>

So now we know:

The most important element in the  
protection scenario is our brain 😊

# UNDERSTANDING THE COMPONENTS



# Understanding The Components

## Turning Threat Intelligence into actions

- Threat Intelligence
  - Gateways must reach the ThreatCloud providing signatures and indicators
    - Alternative: Private ThreatCloud or offline updates
- Protected scope
  - Network(s)/ zone(s) being protected
- Threat Prevention Policy
  - Installed on the gateway
  - Defining the actions per protected scope
- Threat Prevention Profile
  - Containing the protections (signatures)





# Understanding The Components Threat Prevention Policy Layers

- Enable Threat Prevention policy to creating the first Threat Prevention Policy Layer

The screenshot shows the Check Point NGTPdemo interface. On the left, a navigation pane shows 'Threat Prevention' expanded to 'Policy'. A red callout bubble labeled 'Right click' points to this 'Policy' item. The main window displays the 'Policy' configuration for 'NGTPdemo'. Under 'Policy Types', both 'Access Control' and 'Threat Prevention' are checked. A red callout bubble labeled 'First Threat Prevention Policy Layer' points to the 'Threat Prevention' entry in the list below. The 'Blades' section shows 'Access Control' and 'Threat Prevention' entries. At the bottom, there are 'OK' and 'Cancel' buttons.

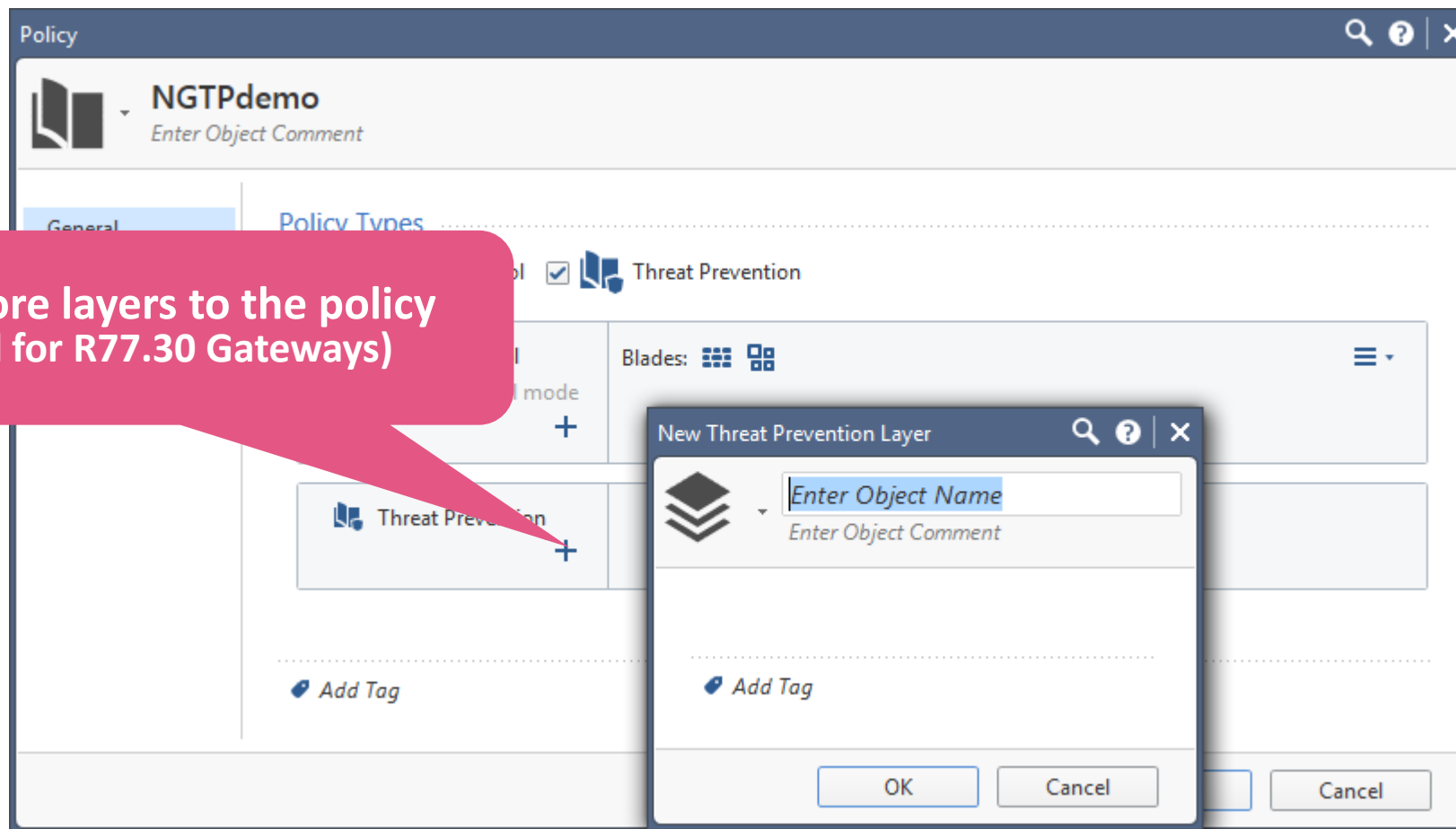


# Understanding The Components

## Threat Prevention Policy Layers for R77.30 Gateways

- Each layer will have it's own rule base

Adding more layers to the policy  
(required for R77.30 Gateways)





# Understanding The Components

## Threat Prevention Policy Rule Base using Protected Scope structure

- Threat Prevention policy rule using Protected Scope object

No.	Name	Protected Scope	Protection Profile / File/Blade	Action	Track
▶ 1	Protecting Email Servers	net_192.168.170.0	N/A	Strict	Log Packet Capture

Callout boxes: "What to protect" points to the Name column; "How to protect" points to the Protected Scope column; "What to see" points to the Track column.

- Protected Scope
  - The network or zone we want to protect
- Action
  - The profile that will be applied to traffic directed to the Protected Scope
- Track
  - Packet capture will be performed for the first match of a signature but not for suppressed logs



# Understanding The Components

## Threat Prevention Policy Rule Base using Source and Destination structure

- Threat Prevention policy rule using **source** and **destination** objects

No.	Name	Source	Destination	Protection/Site/File/Blade	Action	Track
▶ 1		net_192.168.169.0	net_192.168.170.0	N/A	Strict (Clone)	Log Packet Capture

**Traffic Direction** (points to Source and Destination columns)

**How to protect** (points to Protection/Site/File/Blade column)

**What to see** (points to Track column)

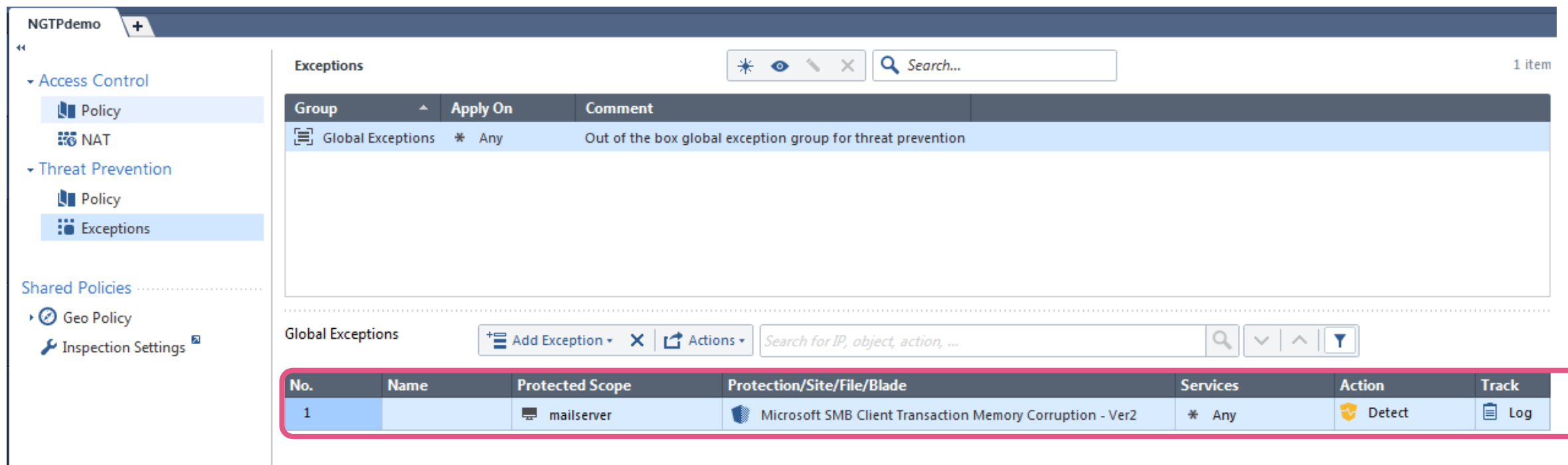
- Right click on the top bar of the policy
- Select “Protected Scope” or “Source and Destination”

No.	Track
▶ 1	<input checked="" type="checkbox"/> Name <input type="checkbox"/> Protected Scope <input checked="" type="checkbox"/> Source <input checked="" type="checkbox"/> Destination <input checked="" type="checkbox"/> Protection/Site/File/Blade <input type="checkbox"/> Services <input checked="" type="checkbox"/> Action <input checked="" type="checkbox"/> Track <input checked="" type="checkbox"/> Install On <input checked="" type="checkbox"/> Comments

# Understanding The Components

## Threat Prevention Policy Rule Base – Global Exceptions

- Global Exceptions apply to all Threat Prevention policies



The screenshot shows the 'Global Exceptions' configuration page in the Check Point GUI. The page is titled 'NGTPdemo' and has a navigation menu on the left. The main area displays a table of exceptions with one entry highlighted:

Group	Apply On	Comment
Global Exceptions	* Any	Out of the box global exception group for threat prevention

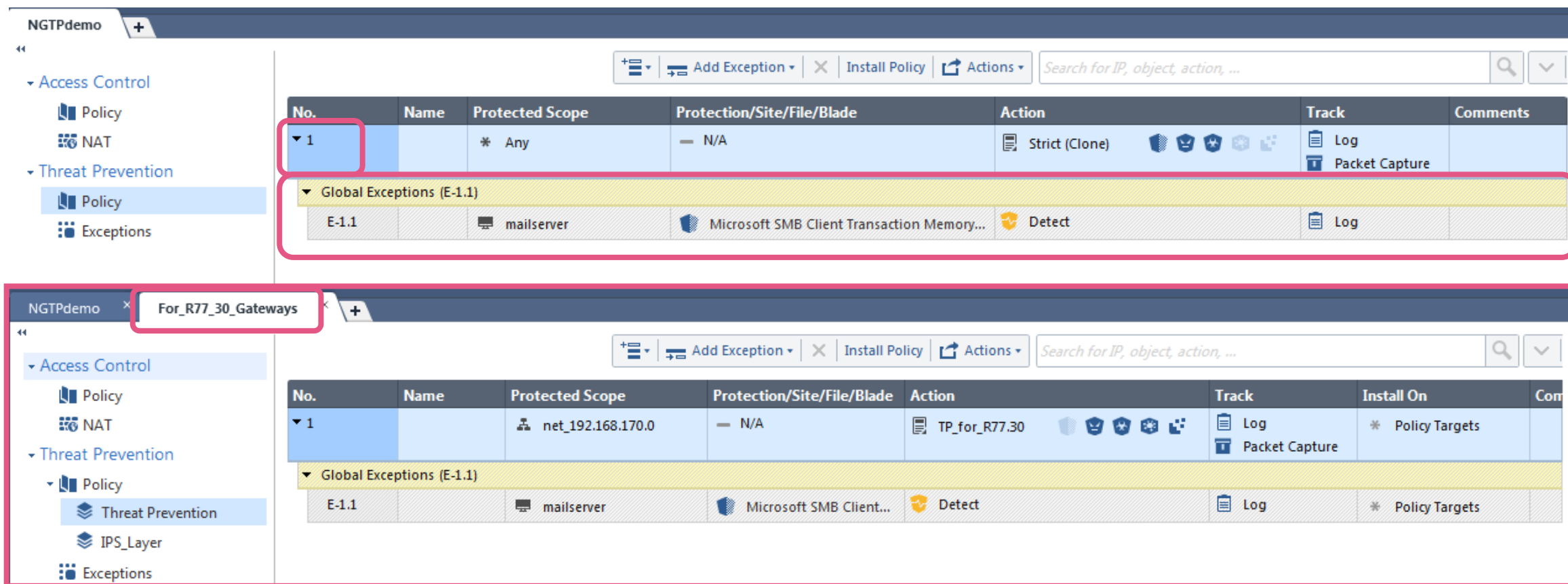
Below this, a section titled 'Global Exceptions' contains a table with one entry:

No.	Name	Protected Scope	Protection/Site/File/Blade	Services	Action	Track
1		mailserver	Microsoft SMB Client Transaction Memory Corruption - Ver2	* Any	Detect	Log

# Understanding The Components

## Threat Prevention Policy Rule Base – Global Exceptions

- Global Exceptions are visible in all the Threat Prevention policies



The image displays two screenshots of the Check Point GUI, illustrating the configuration of Threat Prevention policies and their associated Global Exceptions.

**Top Screenshot: NGTpdemo Policy**

No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Comments
1		* Any	- N/A	Strict (Clone)	Log Packet Capture	
Global Exceptions (E-1.1)						
E-1.1		mailserver	Microsoft SMB Client Transaction Memory...	Detect	Log	

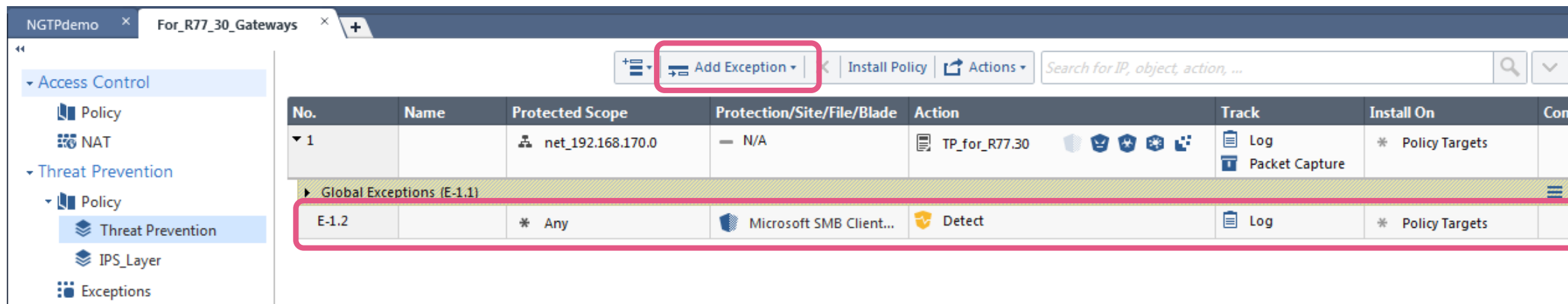
**Bottom Screenshot: For\_R77\_30\_Gateways Policy**

No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Install On	Comments
1		net_192.168.170.0	- N/A	TP_for_R77.30	Log Packet Capture	* Policy Targets	
Global Exceptions (E-1.1)							
E-1.1		mailserver	Microsoft SMB Client...	Detect	Log	* Policy Targets	

# Understanding The Components

## Threat Prevention Policy Rule Base – Exceptions

- Define Exceptions per policy and see them listed
- Click the arrow for the Global Exceptions to see all Exceptions that apply



No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Install On	Com
▼ 1		net_192.168.170.0	N/A	TP_for_R77.30	Log Packet Capture	* Policy Targets	
▶ Global Exceptions (E-1.1)							
E-1.2		* Any	Microsoft SMB Client...	Detect	Log	* Policy Targets	

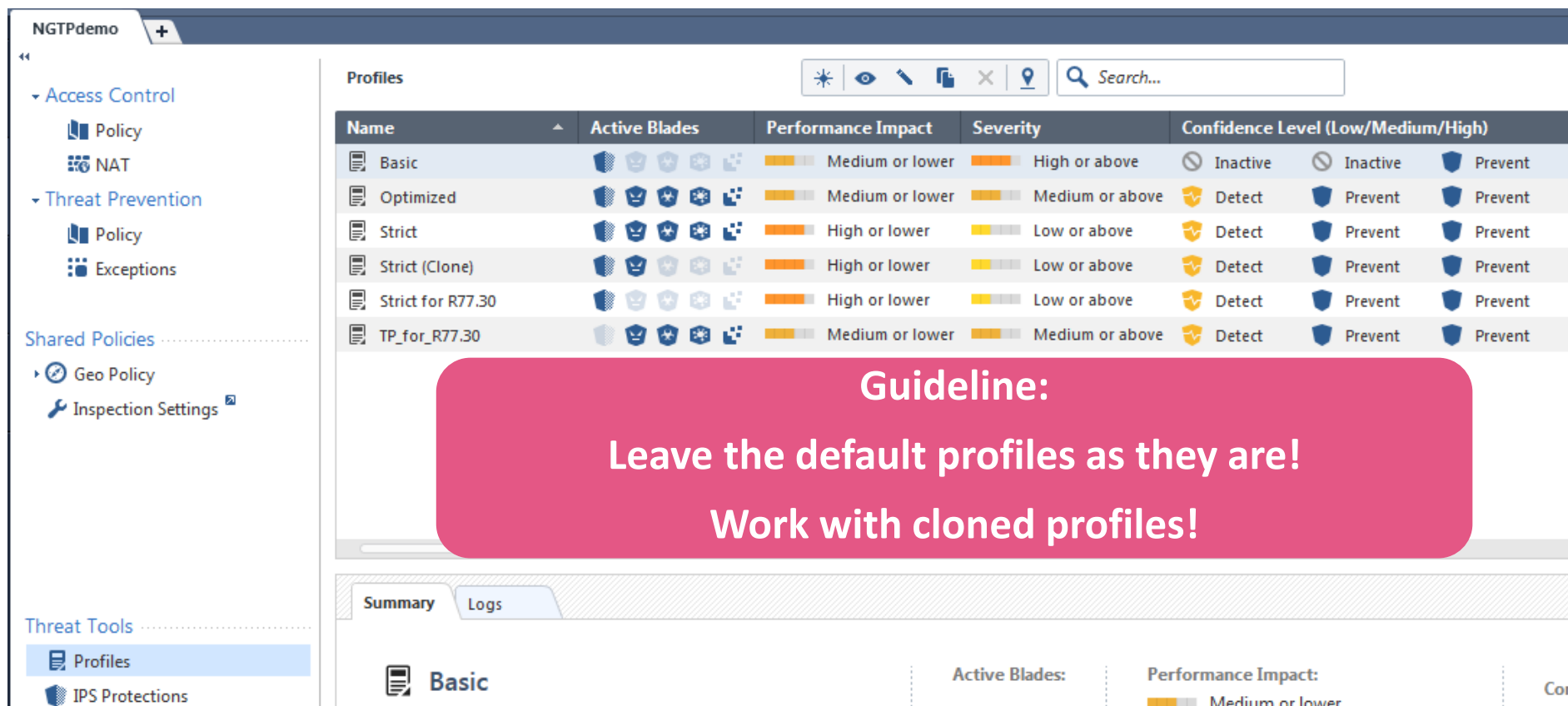
No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Install On	Com
▼ 1		net_192.168.170.0	N/A	TP_for_R77.30	Log Packet Capture	* Policy Targets	
▼ Global Exceptions (E-1.1)							
E-1.1		mailserver	Microsoft SMB Client...	Detect	Log	* Policy Targets	
E-1.2		* Any	Microsoft SMB Client...	Detect	Log	* Policy Targets	



# Understanding The Components

## Threat Prevention Profile

- Threat Prevention Profiles contain protections
- Profiles are assigned in rules as actions executed on the traffic defined



The screenshot displays the 'Profiles' section in the Check Point NGTPdemo interface. The table below lists the available profiles and their configurations.

Name	Active Blades	Performance Impact	Severity	Confidence Level (Low/Medium/High)
Basic	[Icons]	Medium or lower	High or above	Inactive, Inactive, Prevent
Optimized	[Icons]	Medium or lower	Medium or above	Detect, Prevent, Prevent
Strict	[Icons]	High or lower	Low or above	Detect, Prevent, Prevent
Strict (Clone)	[Icons]	High or lower	Low or above	Detect, Prevent, Prevent
Strict for R77.30	[Icons]	High or lower	Low or above	Detect, Prevent, Prevent
TP_for_R77.30	[Icons]	Medium or lower	Medium or above	Detect, Prevent, Prevent

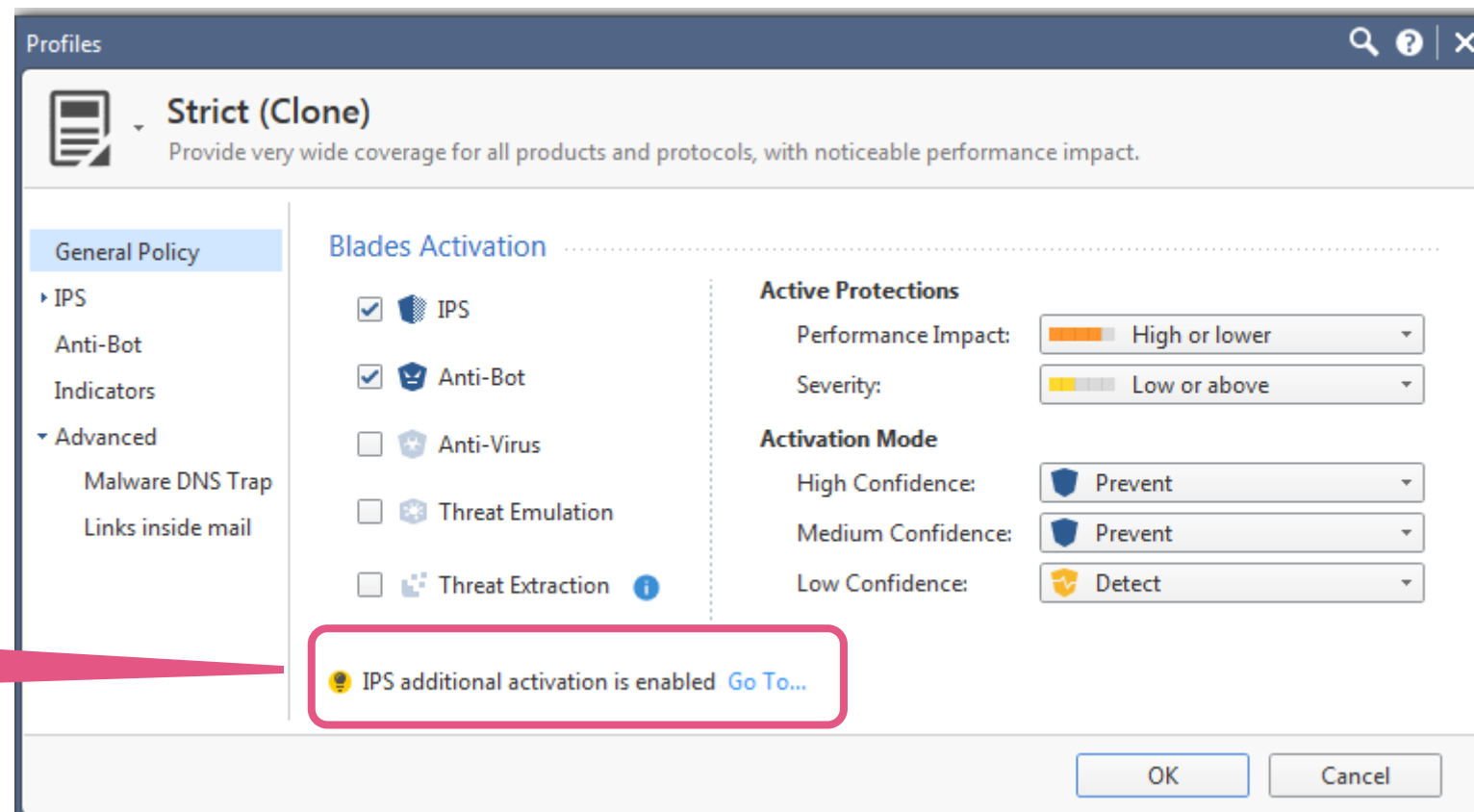
**Guideline:**  
Leave the default profiles as they are!  
Work with cloned profiles!

# Understanding The Components Threat Prevention Profile

## Editing a profile

- Enable desired Software Blades
- Activate Protections according to your needs
- Import indicators from 3<sup>rd</sup> parties

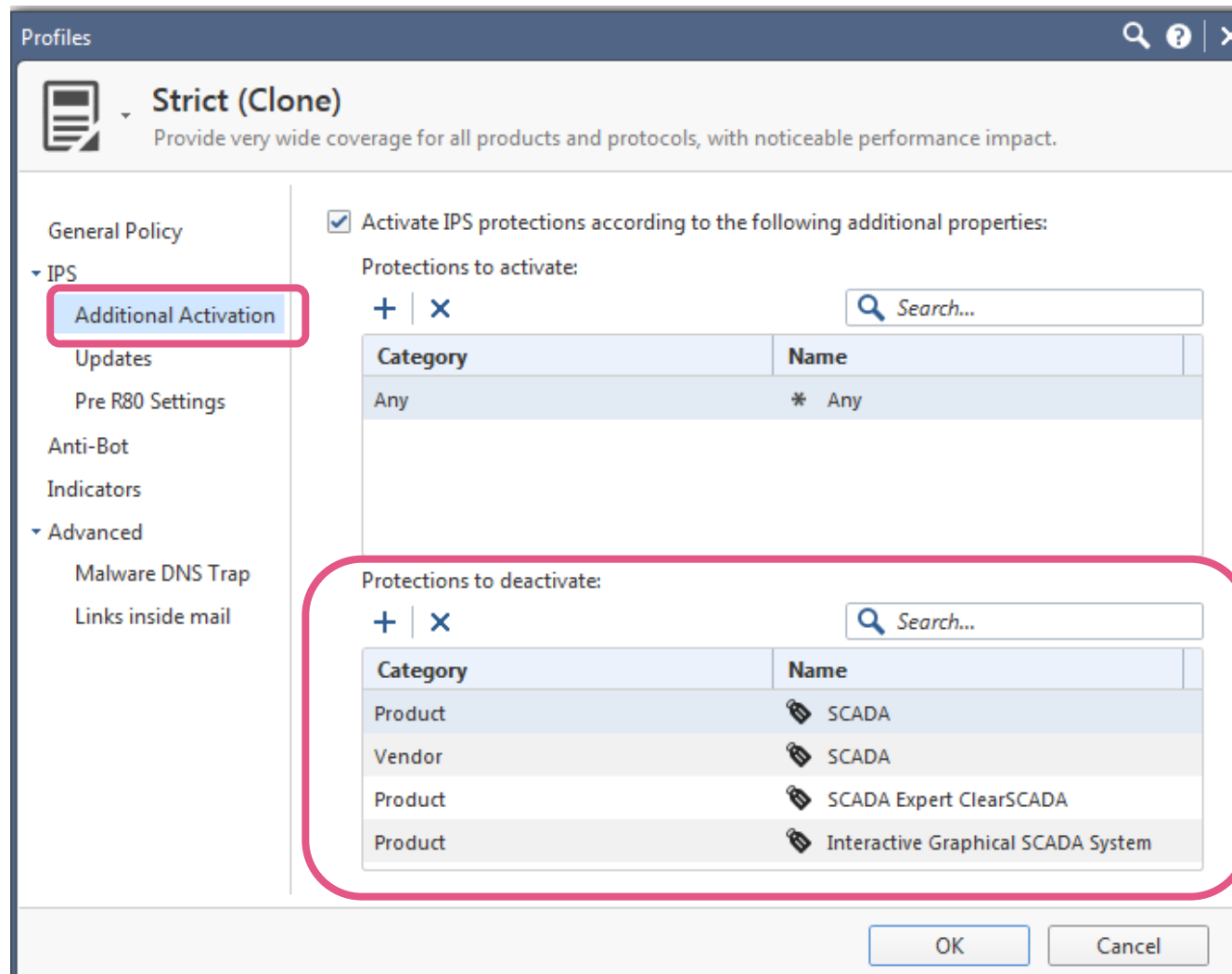
See IPS Profile is modified



# Understanding The Components Threat Prevention Profile

## Editing IPS specific settings

- Activate or deactivate dedicated protections



The screenshot shows the 'Profiles' configuration window for a profile named 'Strict (Clone)'. The profile description is 'Provide very wide coverage for all products and protocols, with noticeable performance impact.' The left sidebar shows the 'IPS' section expanded, with 'Additional Activation' highlighted. The main area shows the 'Activate IPS protections according to the following additional properties:' checkbox checked. Below this, there are two tables: 'Protections to activate' and 'Protections to deactivate'. The 'Protections to deactivate' table is highlighted with a red box.

**Protections to activate:**

Category	Name
Any	* Any

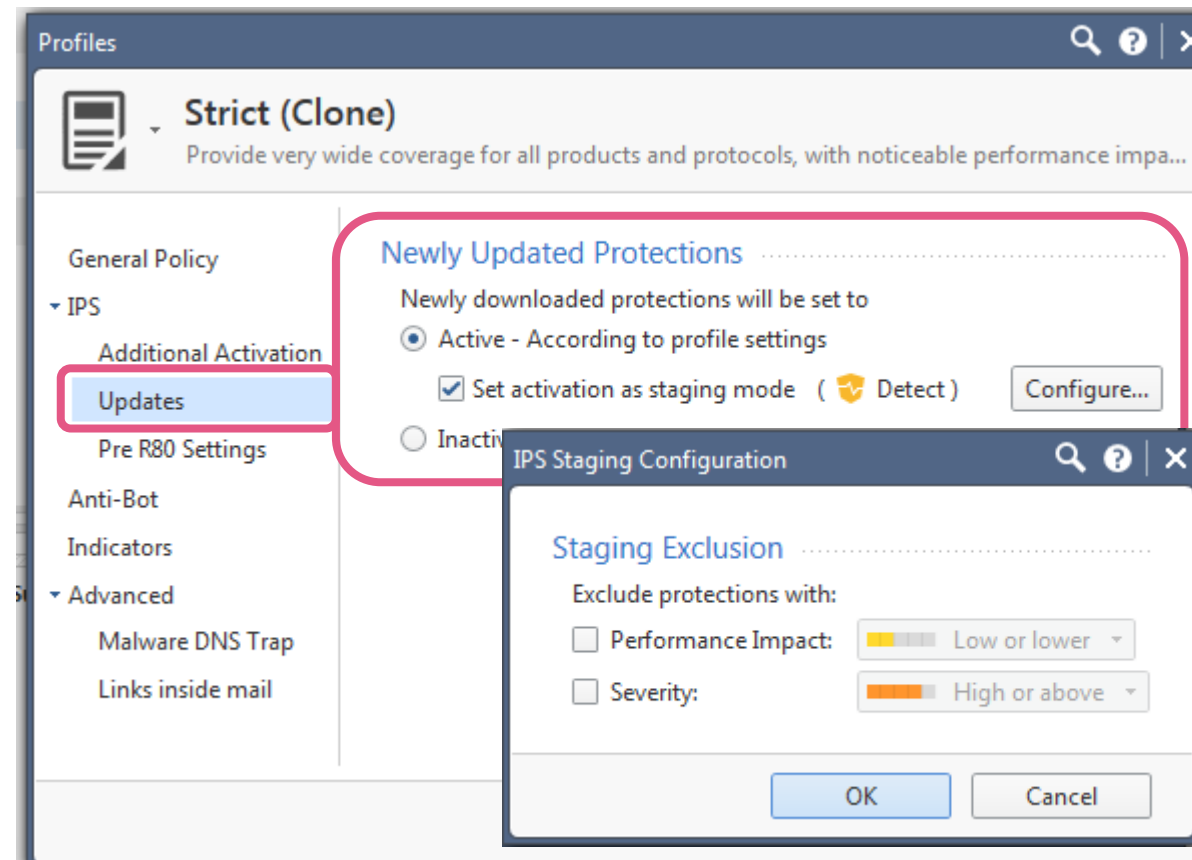
**Protections to deactivate:**

Category	Name
Product	SCADA
Vendor	SCADA
Product	SCADA Expert ClearSCADA
Product	Interactive Graphical SCADA System



# Understanding The Components Threat Prevention Profile

- **Staging** allows tracking newly downloaded protections
- Specify protections regarding performance impact of severity if needed





# Understanding The Components

## Threat Prevention Profile

- You can export and import profiles using the `mgmt_cli` command
- See [sk65627](#) and Threat Prevention Administration Guide for details

A. Connect to the Management CLI:

```
[Expert@HostName:0]# mgmt_cli login user <UserName> password <Password> >  
/var/tmp/id.txt
```

B. Retrieve existing objects:

```
[Expert@HostName:0]# mgmt_cli show threat-profiles details-level full --  
session-file /var/tmp/id.txt > /var/log/export_profiles_information.txt
```

This operation might take some time.

C. Refer to the output file `/var/log/export_profiles_information.txt`.

Now we learned about Policies and Profiles.

What about Protections?

# Understanding The Components Threat Prevention Profile

- Select the profiles you want to see in the protections overview table

Show selected profiles (1 out of 5)

View ▾
Actions ▾
Search...

Protection	Industry Referenc...	Update Date	Severity	Con
3Com Network Supervisor Directory Traversal	CVE-2005-2020	24/11/2009	<div style="width: 100%; height: 10px; background-color: #f00;"></div>	
3Com TFTP Server Transporting Mode Remote Buffer Overflow	CVE-2006-6183	15/11/2011	<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
3CX Phone System VAD_Deploy.aspx Arbitrary File Upload	None	29/12/2016	<div style="width: 100%; height: 10px; background-color: #f00;"></div>	
3ivx MPEG-4 MP4 File Handling Stack Overflow	CVE-2007-6401	20/10/2013	<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
3ivx MPEG-4 MP4 File H			<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
3S Smart Software Solu			<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
3S Smart Software Solu			<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
3S Smart Software Solu			<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
3S Smart Software Solu			<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
3S Smart Software Solu			<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
7-Zip ARJ Archive Hand			<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	
7T Interactive Graphica			<div style="width: 100%; height: 10px; background-color: #f00;"></div>	
7T Interactive Graphica			<div style="width: 100%; height: 10px; background-color: #f00;"></div>	
7T Interactive Graphica			<div style="width: 100%; height: 10px; background-color: #f00;"></div>	
7T Interactive Graphica			<div style="width: 100%; height: 10px; background-color: #f00;"></div>	
7T Interactive Graphica			<div style="width: 100%; height: 10px; background-color: #f00;"></div>	
7T Interactive Graphica			<div style="width: 100%; height: 10px; background-color: #f00;"></div>	
ABB MicroSCADA Wser			<div style="width: 100%; height: 10px; background-color: #ffc000;"></div>	

Show Profiles

All IPS enabled profiles used in the Threat Prevention Policy  
 Specific IPS enabled profiles

	Name
<input checked="" type="checkbox"/>	Strict (Clone)
<input type="checkbox"/>	Strict for R77.30
<input type="checkbox"/>	Optimized
<input type="checkbox"/>	Strict
<input type="checkbox"/>	Basic

# IPS LOGGING



# Packet Capture And Suppressed Logs

## ThreatCloud protections and Core protections logging

- Logs related to the IPS Blade

Filter: "Time Period"

Filter: "Blade: IPS"

Logs | General Overview

Queries | Last 7 Days | blade:IPS

Found 17 results (173 ms)

Time	Blade	Action	Ty...	Inte...	Origin	Sever...	Source User...	Source	Destination	Protection Type	Protection Name	IPS Profile
Today, 09:29:30	IPS	Prevent	L...	eth0	gwR8010			192.168.169.1	mailserver (192...	Signature		N/A
Today, 09:29:05	IPS	Prevent	L...	eth0	gwR8010			192.168.169.1	mailserver (192...	Signature		N/A
Today, 09:29:05	IPS	Prevent	L...	eth0	gwR8010			192.168.169.1	mailserver (192...	Signature		N/A
Today, 09:29:05	IPS	Prevent	L...	eth0	gwR8010			192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A
Today, 09:29:05	IPS							2...		Signature		N/A
Today, 09:29:05	IPS							2...		Signature		N/A
Today, 09:29:05	IPS							2...		Signature		N/A
Today, 09:22:37	IPS	Prevent	L...	eth0	gwR8010			192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A
Today, 09:22:32	IPS	Prevent	L...	eth0	gwR8010			192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A
Today, 09:22:32	IPS	Prevent	L...	eth0	gwR8010			192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A
Today, 09:19:48	IPS	Prevent	L...	eth0	gwR8010			192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A
Yesterday, 19:48:31	IPS							2...		IPS		Strict (Clone)
Yesterday, 18:17:11	IPS							2...		IPS		Strict (Clone)

Profile

Many logs of the same type in a short timeframe

Type: Signature

Just two logs of the same type after about 90min

Profile

Let's **understand** what we just have seen here:  
Some IPS logs include an **indication to a profile** and  
others don't.

Some IPS logs occur **one after the other**  
others occur with a delta of a certain time.

Don't panic:

You just have seen **log suppression** 😊

# Packet Capture And Suppressed Logs

## ThreatCloud protections (signatures) matching

How can we avoid flooding the management server with IPS related logs?

- By default the **first signature match** will be **logged and** a **packet capture** will be taken
- If the same **signature** will **match again in the period of less than two minutes**, no additional packet capture will be taken and no new log message will be sent
- The “**suppressed logs**” **counter** of the previous log message **will be updated**, reflecting the number of times the signature has been matched

**Don't panic – keep on breathing normally 😊**

- If the **same signature will match again after a period of more than two minutes** a **new packet capture** will be taken and a **new log message** will be generated
- These packet captures will be taken **independent of the setting in the signature** 😊



# Packet Capture And Suppressed Logs

## ThreatCloud protections logging

The screenshot displays the Check Point Threat Prevention interface. On the left, a navigation pane shows 'Access Control' > 'Policy' > 'Threat Prevention' > 'Policy' selected. The main area shows a table of policy rules. A red callout bubble points to the first rule, labeled 'Policy Rule'. Below the table, the 'Logs' tab is active, showing a search query and a table of log entries. A second red callout bubble points to the log entries, stating 'See the logs in the lower window of the Threat Prevention Policy view when selecting the rule'.

No.	Name	Source	Destination	Protection/Site/File/Blade	Action	Track	Ins
1		net_192.168.169.0	net_192.168.170.0	N/A	Strict (Clone)	Log Packet Capture	*

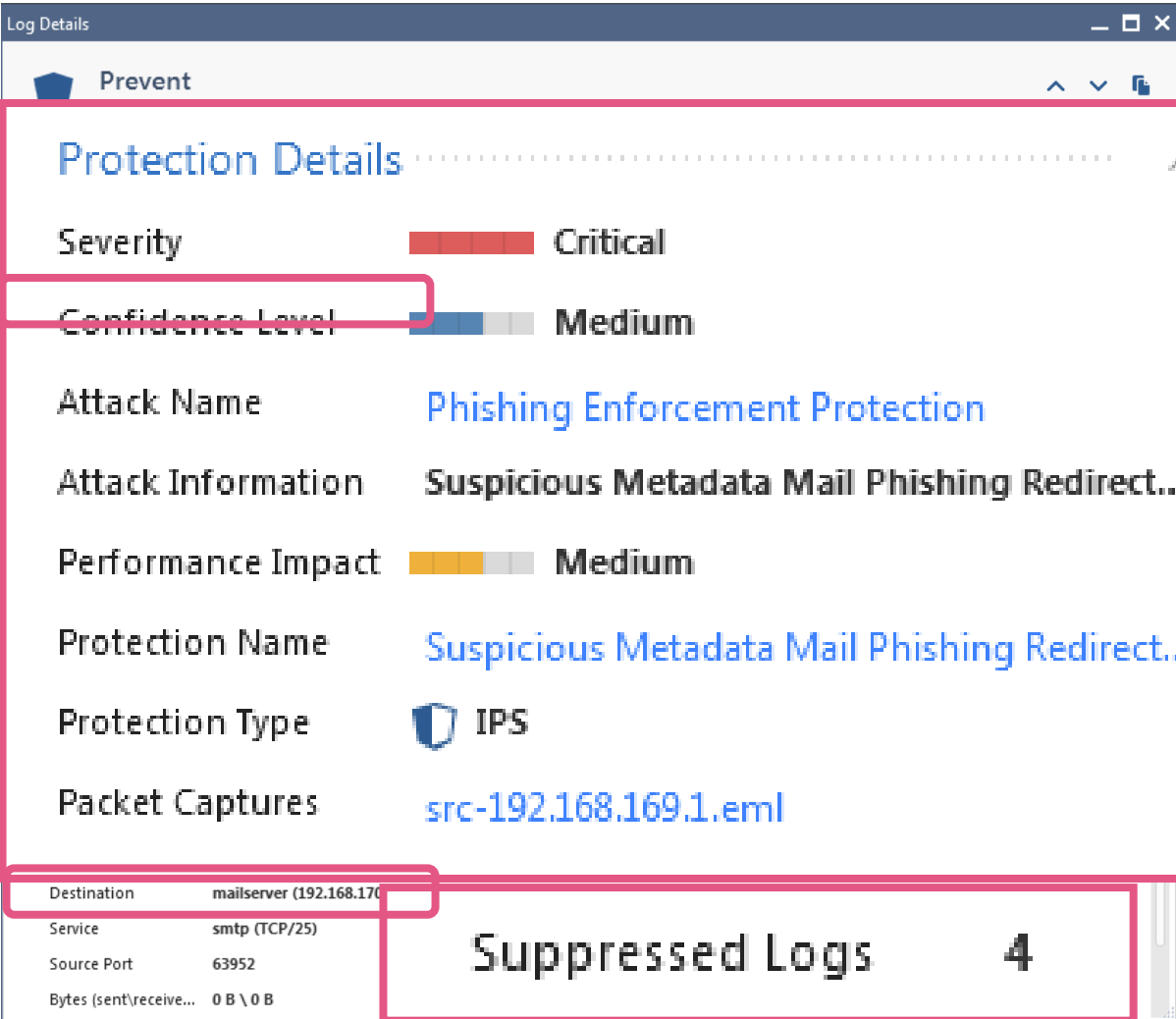
  

Time	Origin	Sever...	Source User...	Source	Destination	Protection Type	Protection Name	IPS Profil
30 May 17, 19:48:31	gwR8010			192.168.169.1	mailserver (192....	IPS	Suspicious Metadata Mail...	Strict (Clo
30 May 17, 18:17:11	gwR8010			192.168.169.1	mailserver (192....	IPS	Suspicious Metadata Mail...	Strict (Clo

# Packet Capture And Suppressed Logs

## ThreatCloud protections logging

- Time
- Target
- Attack type
- Packet captures
- Has the attack been repeated?



Log Details

Prevent

### Protection Details

Severity ■ Critical


Confidence Level ■ Medium

Attack Name [Phishing Enforcement Protection](#)

Attack Information **Suspicious Metadata Mail Phishing Redirect...**

Performance Impact ■ Medium

Protection Name [Suspicious Metadata Mail Phishing Redirect...](#)

Protection Type  IPS

Packet Captures [src-192.168.169.1.eml](#)

Destination	mailserver (192.168.170...
Service	smtp (TCP/25)
Source Port	63952
Bytes (sent\receive...	0 B \ 0 B

**Suppressed Logs 4**



# Packet Capture And Suppressed Logs

## Configuring packet capture for ThreatCloud protections (signatures)

The screenshot shows the Check Point management console interface. On the left, the navigation pane includes 'Access Control', 'Threat Prevention', 'Shared Policies', and 'Threat Tools'. 'Threat Tools' is expanded to show 'IPs Protections', which is highlighted with a red box. The main area displays a table of protection profiles. The profile 'Repetitive SMB Rename Command Attempts' is selected and highlighted in blue. A modal window titled 'Protection Details - Repetitive SMB Rename Command Attempts' is open, showing configuration options. The 'Main Action' is set to 'Prevent'. Under the 'Logging' section, the 'Track' dropdown is set to 'Log', and the 'Capture Packets' checkbox is checked. A red box highlights the 'Capture Packets' checkbox and the 'Track' dropdown. A red callout bubble points to the 'Capture Packets' checkbox with the text: 'Enabling packet capture here will lead to have a packet capture for every match'. Another red callout bubble points to the 'Track' dropdown with the text: 'Packet capture can take up to 1MByte in size'. The table below shows the configuration for this protection profile.

Protection	Industry Refere...	Update Da...	Sev...	Confidence Level	Strict (Clone)
Repetitive SMTP Login Failures	None	04/12/2013	Red	Blue	Shield
Repetitive POP3 Login Failures	None	28/10/2015	Red	Blue	Shield
Repetitive SMB Login Attempts	None	10/01/2006	Yellow	Blue	Shield
Repetitive SMB Rename Command Attempts	None	09/11/2016	Red	Blue	Shield

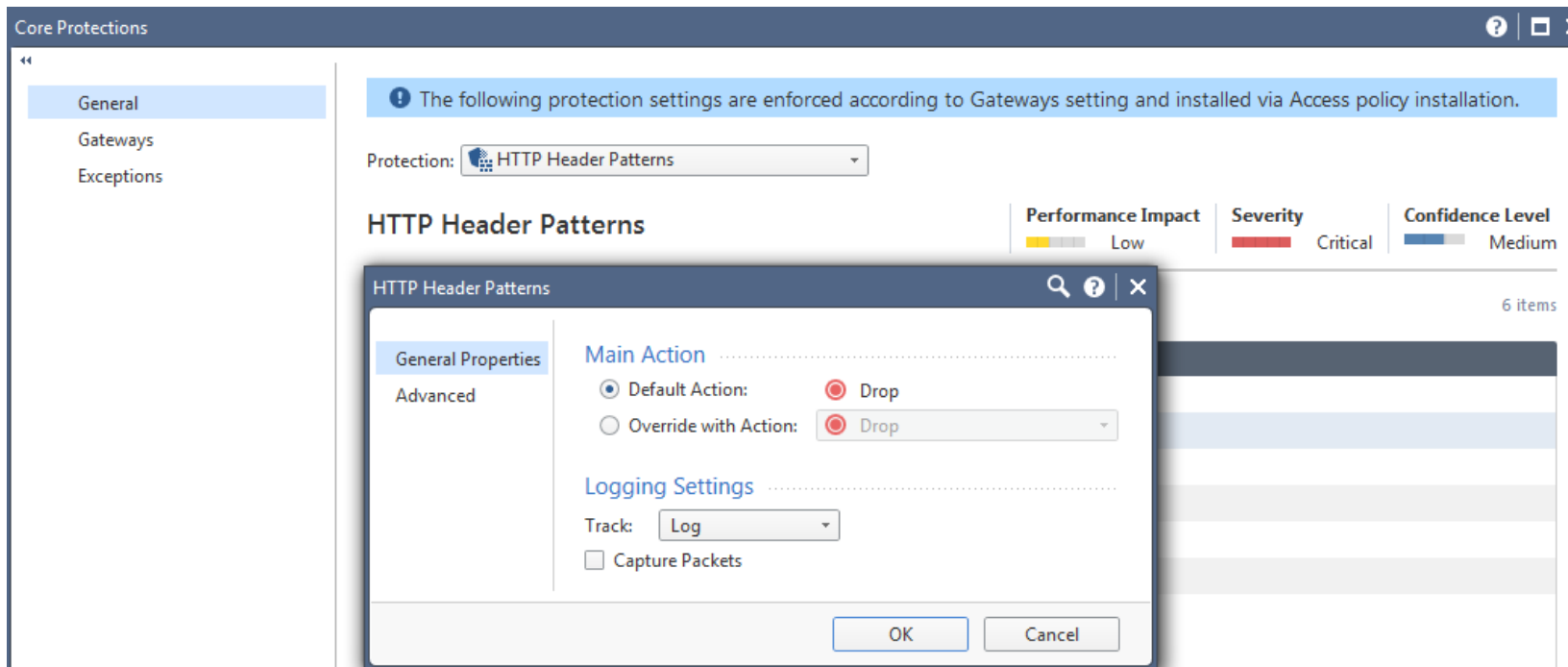
Profile	Action	Override	Track
Strict (Clone)	Prevent	No	Log
Optimized	In...	No	Log
Strict	De...	No	Log
Basic	Ina...	No	Log

# Packet Capture And Suppressed Logs

## Core protections and Inspection settings matching

When Core protections or Inspection settings are matching

- **No log suppression** is performed
- **No packet capture** is performed **unless** the respective setting is enabled



The screenshot displays the 'Core Protections' configuration window. On the left, a sidebar lists 'General', 'Gateways', and 'Exceptions'. The main area shows a notification: 'The following protection settings are enforced according to Gateways setting and installed via Access policy installation.' Below this, the 'Protection' is set to 'HTTP Header Patterns'. The configuration for 'HTTP Header Patterns' is shown with 'Performance Impact' at 'Low', 'Severity' at 'Critical', and 'Confidence Level' at 'Medium'. A modal dialog titled 'HTTP Header Patterns' is open, showing 'General Properties' and 'Advanced' tabs. Under 'Main Action', 'Default Action' is 'Drop' and 'Override with Action' is also 'Drop'. Under 'Logging Settings', 'Track' is set to 'Log' and 'Capture Packets' is unchecked. 'OK' and 'Cancel' buttons are at the bottom of the dialog.





# Packet Capture And Suppressed Logs

## Core protections logging

- Time
- Target
- Attack type

The screenshot displays the 'Log Details' window for a 'Prevent' action. The log entry is for an 'HTTP Header Patterns' attack. Key details include:

- Origin:** gwR8010
- Source:** 192.168.169.1
- Time:** Today, 09:29:05
- Destination:** mailserver (192.168.170.10)
- Severity:** Critical
- Confidence Level:** High
- Attack Name:** HTTP Header Patterns
- Attack Information:** HTTP Header Pattern Found
- Performance Impact:** Low
- Protection Name:** HTTP Header Patterns
- Protection Type:** Signature
- Industry Reference:** CVE-2000-0032, CAN-2003-0237, CAN-2002-0254, CVE-2002-0155, CAN-2003-0397, CAN-2002-0314

The 'Protection Details' section is highlighted with a red box. The 'Log Info' and 'Traffic' sections are also partially highlighted with red boxes.



# Packet Capture And Suppressed Logs

## Core protections and Inspection settings matching

The screenshot displays the 'Log Details' window for a 'Prevent' log message. The log entry is for 'HTTP Header Patterns' with a severity of 'Critical' and a confidence level of 'High'. The source is '192.168.169.1' and the destination is 'mailserver (192.168.170...)'. The service is 'http (TCP/80)' and the interface is 'eth0'. The action is 'Prevent' and the threat profile is 'Go to profile'. The industry reference includes CVE-2000-0032, CAN-2003-0237, CAN-2002-0254, CVE-2002-0155, CAN-2003-0397, and CAN-2002-0314. The protection ID is 'HttpHeaderRejection' and the policy management is 'mgnt'.

Time	Severity	Blade	Type
31 May 17, 16:44:36	Critical	gwr8010	Log
31 May 17, 16:44:36	Critical	gwr8010	Log
31 May 17, 09:29:45	Critical	IPS	Log
31 May 17, 09:29:30	Critical	IPS	Log
31 May 17, 09:29:05	Critical	IPS	Log
31 May 17, 09:29:05	Critical	IPS	Log
31 May 17, 09:29:05	Critical	IPS	Log
31 May 17, 09:29:05	Critical	IPS	Log
31 May 17, 09:29:05	Critical	IPS	Log
31 May 17, 09:29:05	Critical	IPS	Log
31 May 17, 09:29:05	Critical	IPS	Log
31 May 17, 09:29:05	Critical	IPS	Log
31 May 17, 09:22:37	Critical	IPS	Log
31 May 17, 09:22:32	Critical	IPS	Log
31 May 17, 09:22:32	Critical	IPS	Log

Example of a log message generated by a Core protecting matching

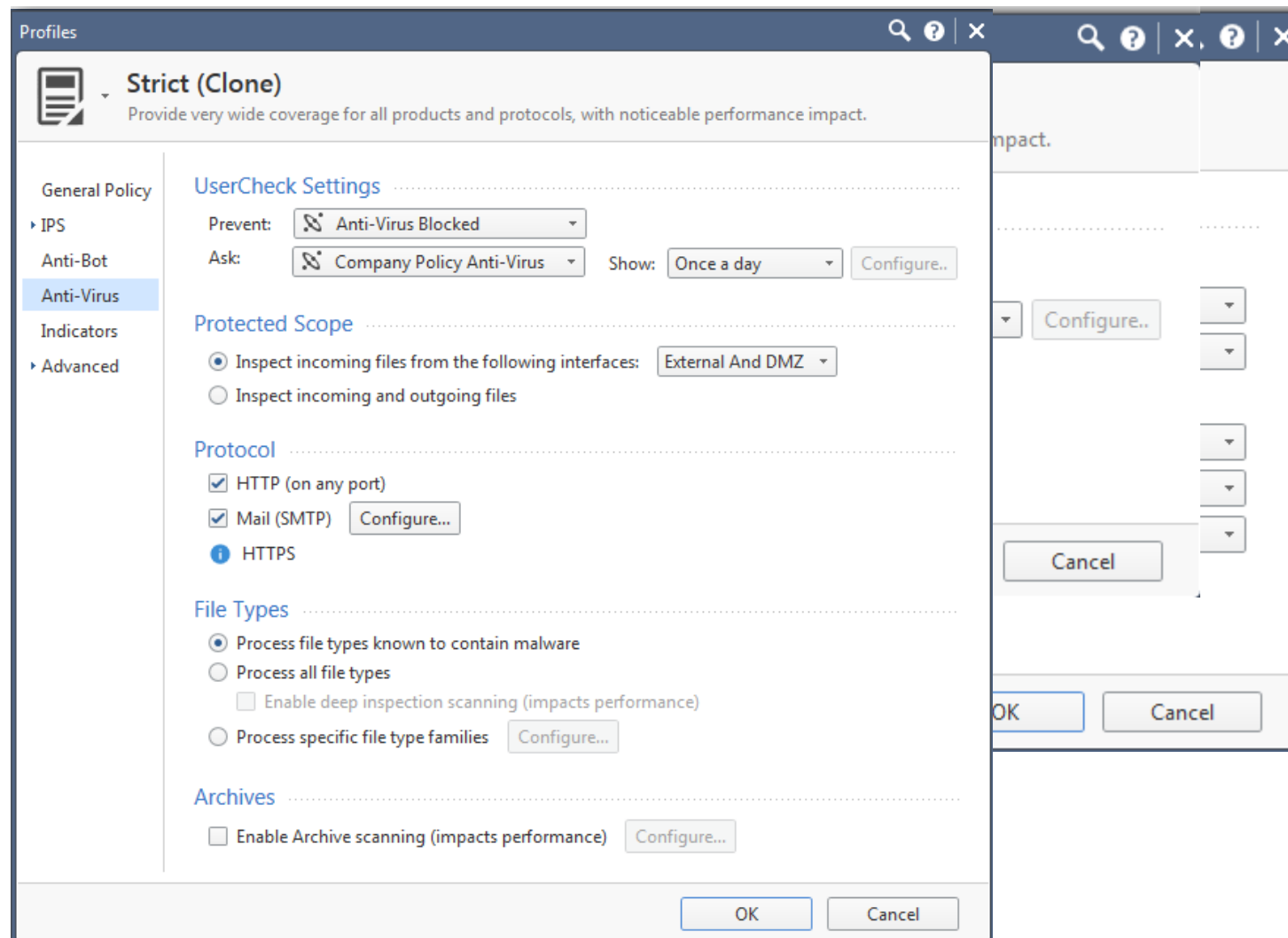
# ANTI-VIRUS ANTI-BOT



# Anti-Virus and Anti-Bot

## Manage their settings in the profile

- Protections will get activated according to the configuration
- Define UserCheck settings for Anti-Bot
- Configure Anti-Virus Blade





# Anti-Virus and Anti-Bot

## Manage their settings in the profile

- Configured UserCheck for Anti-Virus
- Configure MIME nesting
- Enabling deep inspection will cause the gateway loading additional software from the update service
- Configure file type specific inspection
- Configure archive scanning

The screenshot displays three overlapping configuration windows from the Check Point management console:

- Profiles:** Shows the 'Strict (Clone)' profile with a description: 'Provide very wide coverage for all products and protocols, with noticeable performance impact.' The 'UserCheck Settings' tab is active.
- File Types Configuration:** Shows 'Specific file types families actions:' with a search filter 'exe'. A table lists file types and their actions:

Extension	Type Description	Action
exe,scr	MS-DOS executable (including self-ext...	Drop
exe	MS-DOS executable (built-in)	Bypass
exe,dll	Windows PE	Inspect

- Archive Scanning Configuration:** Shows options for processing archives. The 'Stop processing archive after (seconds):' is set to 30. The 'When maximum time is exceeded (action on file):' is set to 'Allow'. There are 'OK' and 'Cancel' buttons.

At the bottom, the 'Archives' section has a checked option 'Enable Archive scanning (impacts performance)' with a 'Configure...' button.



# Anti-Virus and Anti-Bot

## Manage their settings in the profile

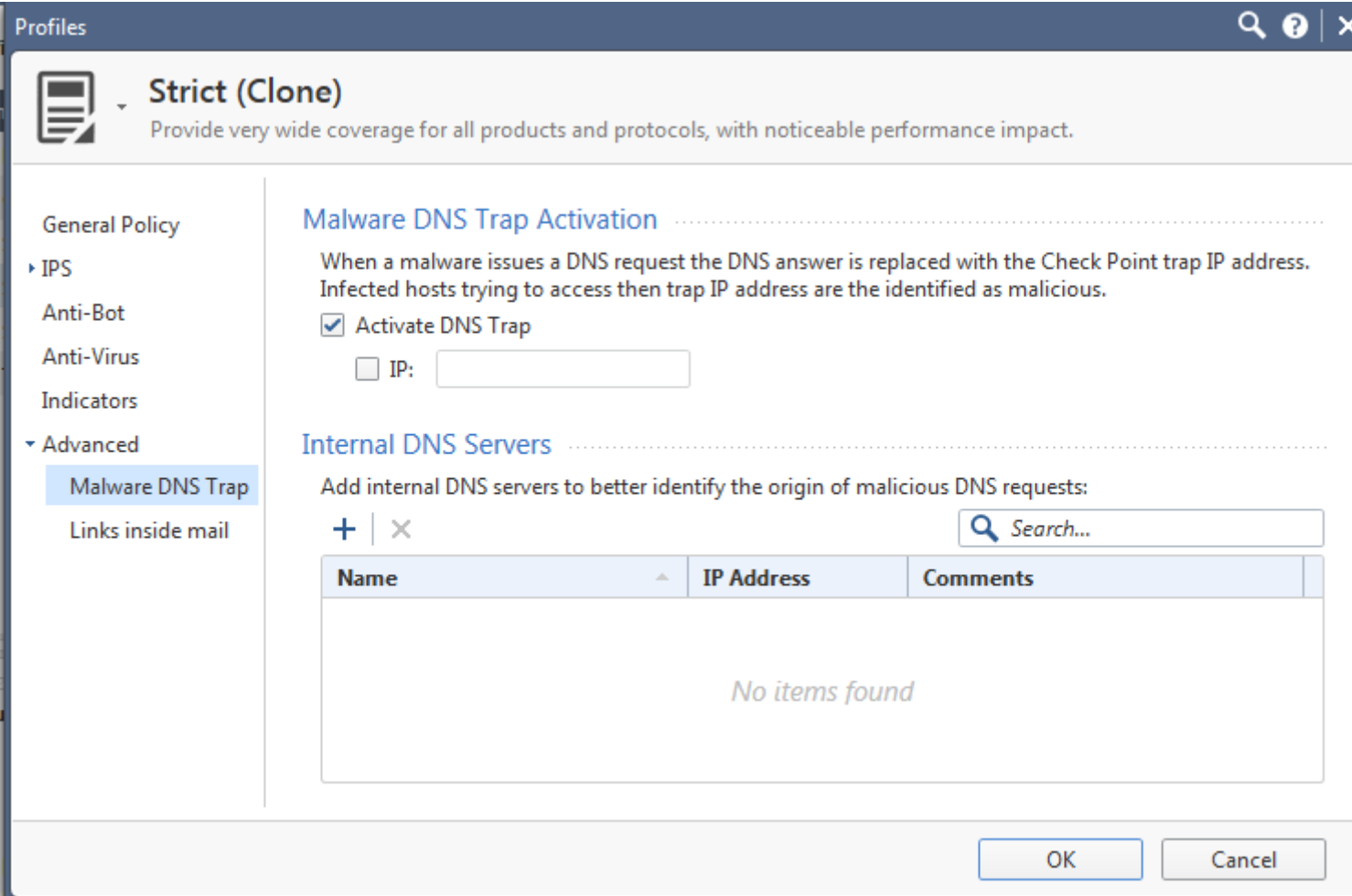
- Manage indicators
- Import indicators using the “Indicators” menu under the Threat Tools section

The screenshot displays the Check Point NGTPdemo web interface. On the left is a navigation sidebar with sections: Access Control (Policy, NAT), Threat Prevention (Policy, Exceptions), Shared Policies (Geo Policy, Inspection Settings), and Threat Tools (Profiles, IPS Protections, Protections, Whitelist Files, Indicators). The 'Indicators' menu item is highlighted. The main content area shows the 'Indicators' management page with a table header: Name, Actions, File Name, Description, Comments. A search bar is present at the top right. An 'Indicator' dialog box is open in the foreground, containing fields for 'Enter Object Name' and 'Enter Object Comment', an 'Indicator file' field with an 'Import...' button, an 'Action' dropdown menu set to 'Prevent', and an 'Add Tag' button. At the bottom of the dialog are 'OK' and 'Cancel' buttons. The text 'No preview available' is visible at the bottom right of the main interface.

# Anti-Virus and Anti-Bot

## Manage their settings in the profile

- By default a DNS query for a known Botnet is answered with the IP Address of the Check Point sinkhole
- Botnet communication can be analyzed by Check Point sinkhole
- Define corporate DNS Server IP Addresses

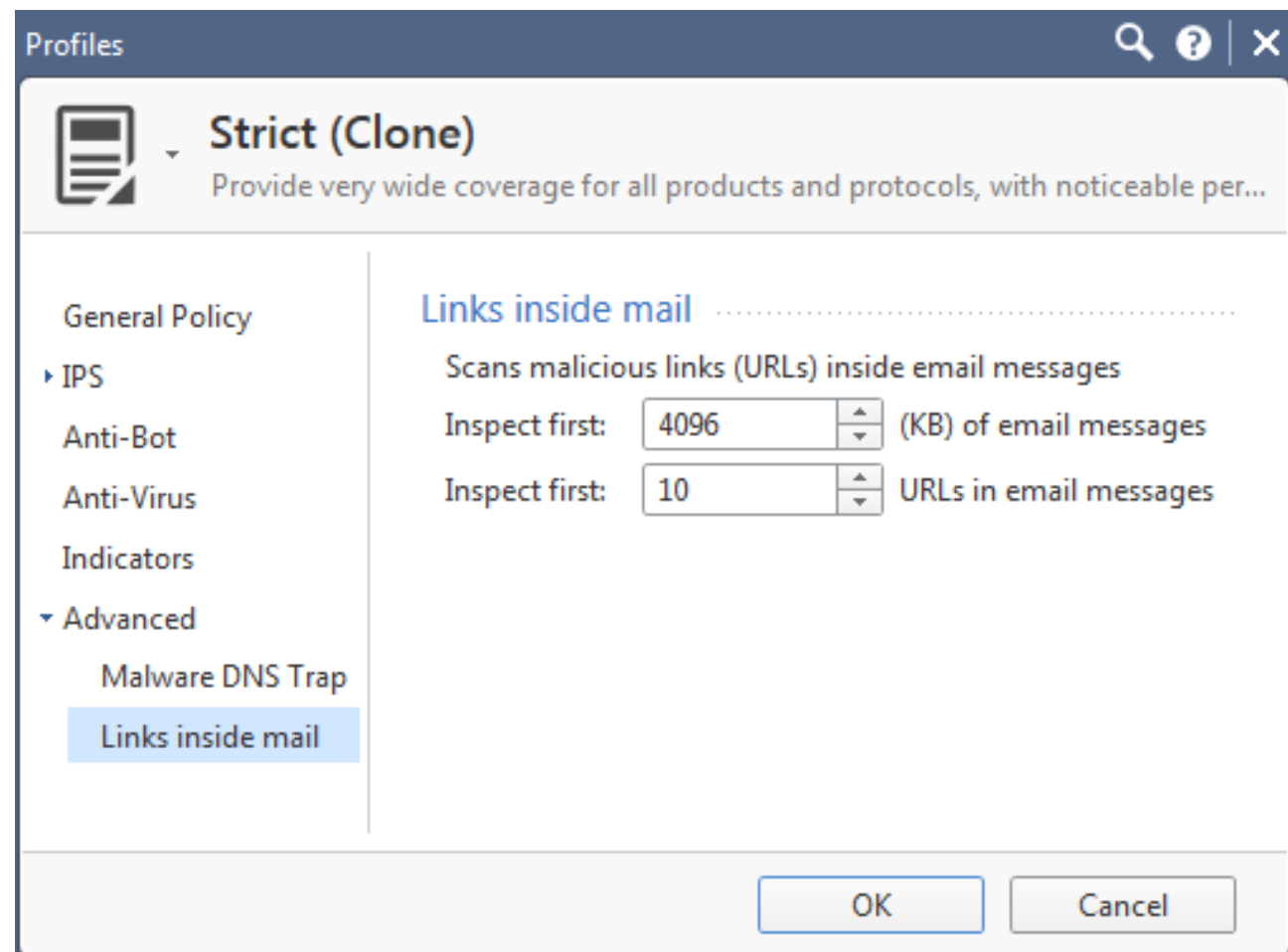


The screenshot shows the 'Profiles' configuration window for a profile named 'Strict (Clone)'. The window title is 'Profiles' and the profile name is 'Strict (Clone)'. Below the profile name, there is a description: 'Provide very wide coverage for all products and protocols, with noticeable performance impact.' The left sidebar contains a navigation menu with the following items: 'General Policy', 'IPS', 'Anti-Bot', 'Anti-Virus', 'Indicators', 'Advanced', 'Malware DNS Trap' (highlighted), and 'Links inside mail'. The main content area is divided into two sections: 'Malware DNS Trap Activation' and 'Internal DNS Servers'. The 'Malware DNS Trap Activation' section has a description: 'When a malware issues a DNS request the DNS answer is replaced with the Check Point trap IP address. Infected hosts trying to access then trap IP address are the identified as malicious.' It includes a checked checkbox for 'Activate DNS Trap' and an unchecked checkbox for 'IP:' followed by an empty text input field. The 'Internal DNS Servers' section has a description: 'Add internal DNS servers to better identify the origin of malicious DNS requests:'. It features a search bar with a magnifying glass icon and the text 'Search...'. Below the search bar is a table with three columns: 'Name', 'IP Address', and 'Comments'. The table is currently empty, displaying the text 'No items found' in the center. At the bottom right of the window, there are 'OK' and 'Cancel' buttons.

# Anti-Virus and Anti-Bot

## Manage their settings in the profile

- Links inside emails can be verified for being referrals for malware distribution sites
- Incoming emails will be scanned by Anti-Virus Blade
- Outgoing emails will be scanned by Anti-Bot Blade
- Deactivate this function using the Protections settings menu





# Anti-Virus and Anti-Bot Manage Protections

NGTPTdemo

- Access Control
  - Policy
  - NAT
- Threat Prevention
  - Policy
  - Exceptions
- Shared Policies
  - Geo Policy
  - Inspection Settings
- Threat Tools
  - Profiles
  - IPS Protections
  - Protections
  - Whitelist Files
  - Indicators
  - Updates
  - UserCheck
  - Threat Wiki
  - Installation History

**Protections**

Actions Search Protection

Protection	Blade	Engine	Known Today	Last Update
IPS	IPS	Signatures	7,951	5/30/2017
Reputation IPs	Anti-Bot	Reputation	61,966,065	6/4/2017
Reputation URLs	Anti-Bot	Reputation	242,991,538	6/4/2017
Reputation Domains	Anti-Bot	Reputation	242,326,235	6/4/2017
Mail Activity	Anti-Bot	Suspicious Mail Outbreaks	1,493,363	6/4/2017
Unusual Activity	Anti-Bot	Behavioral Patterns	30	6/4/2017
Malicious Activity	Anti-Bot	Signatures	10,972	6/4/2017
Viruses	Anti-Virus	Signatures	16,973,115	6/4/2017
URLs with Malware	Anti-Virus	Reputation	8,332,371	6/4/2017
File Types	Anti-Virus	File Type	89	6/4/2017
Exploit Detection	Threat Emulation	Exploit Detection	N/A	6/4/2017
Malicious Activity	Anti-Virus	Signatures	N/A	6/4/2017
Unusual Activity	Anti-Virus	Behavioral Patterns	24	6/4/2017
Links Inside Mail	Anti-Virus	Reputation	243,575,096	6/4/2017
Links Inside Mail	Anti-Bot	Reputation	235,638,354	6/4/2017

**Summary** Activations

**IPS** | 7,951

General	Confidene Level	Performance Impact	Description
Blade: IPS	Low 0.00%	Low 0.00%	Intrusion Prevention System (IPS) Software Blade combine industry-leading IPS protection with breakthrough perform

Protections

Details of selected



# Anti-Virus and Anti-Bot Manage Protections

Protection	Blade	Engine	Known Today	Last Update
IPS	IPS	Signatures	7,951	5/30/2017
Reputation IPs	Anti-Bot	Reputation	61,966,065	6/4/2017
Reputation URLs	Anti-Bot	Reputation	242,991,538	6/4/2017
Reputation Domains	Anti-Bot	Reputation	242,326,235	6/4/2017
Mail Activity	Anti-Bot	Suspicious Mail Outbreaks	1,493,363	6/4/2017
Unusual Activity	Anti-Bot	Behavioral Patterns	30	6/4/2017
Malicious Activity	Anti-Bot	Signatures	10,972	6/4/2017
Viruses	Anti-Virus	Signatures	16,973,115	6/4/2017
URLs with Malware	Anti-Virus	Reputation	8,332,371	6/4/2017
File Types	Anti-Virus	File Type	89	6/4/2017
Exploit Detection	Threat Emulation	Exploit Detection	N/A	6/4/2017
Malicious Activity	Anti-Virus	Signatures	N/A	6/4/2017
Unusual Activity	Anti-Virus	Behavioral Patterns	24	6/4/2017
Links Inside Mail	Anti-Virus	Reputation	243,575,096	6/4/2017
Links Inside Mail	Anti-Bot	Reputation	235,638,354	6/4/2017

Protections

Details of selected

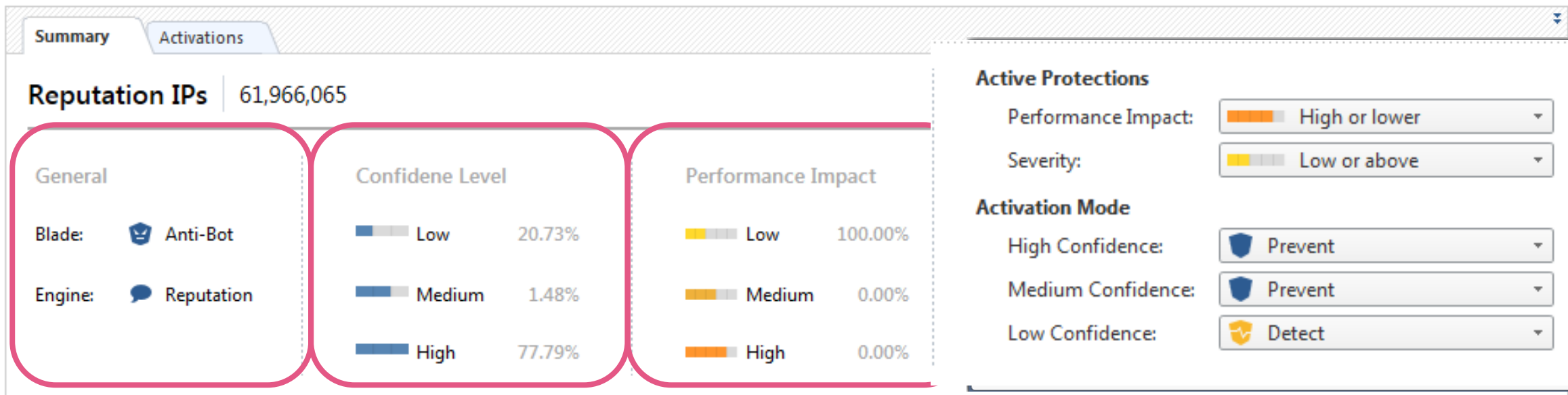
Summary | Activations

**Reputation IPs** | 61,966,065

General	Confidene Level	Performance Impact	Description
Blade:  Anti-Bot	Low 20.73%	Low 100.00%	For Reputation IPs protections, the Reputation layer of the ThreatSpect engine prevents "call home" connections to

# Anti-Virus and Anti-Bot Manage Protections


- Enlarge the details view
- Understand “Blade and Engine”, “Confidence Level” and “Performance Impact”
- Now remember the profile settings




**Summary** | Activations



**Reputation IPs** | 61,966,065

**General**




Blade:  Anti-Bot

Engine:  Reputation


**Confidence Level**


	Low	20.73%
	Medium	1.48%
	High	77.79%

**Performance Impact**


	Low	100.00%
	Medium	0.00%
	High	0.00%


**Active Protections**


Performance Impact:  High or lower

Severity:  Low or above

**Activation Mode**

High Confidence:  Prevent

Medium Confidence:  Prevent

Low Confidence:  Detect

# Anti-Virus and Anti-Bot Manage Protections

Protections Actions  15 items

Protection	Blade	Engine	Known Today	Last Update
IPS	IPS	Signatures	7,951	5/30/2017
Reputation IPs	Anti-Bot	Reputation	61,966,065	6/4/2017
Reputation URLs	Anti-Bot	Reputation	242,991,538	6/4/2017
Reputation Domains	Anti-Bot	Reputation	242,326,235	6/4/2017
Mail Activity	Anti-Bot	Suspicious Mail Outbreaks	1,493,363	6/4/2017
Unusual Activity	Anti-Bot	Behavioral Patterns	30	6/4/2017
Malicious Activity	Anti-Bot	Signatures	10,972	6/4/2017
Viruses	Anti-Virus	Signatures	16,973,115	6/4/2017

Summary **Activations**

Profile	Action
Strict for R77.30	Prevent
TP_for_R77.30	Prevent
Strict (Clone)	Prevent
Optimized	Prevent
Strict	Prevent
Basic	Prevent

**Understand in which profile the protections are active**



# Anti-Virus and Anti-Bot Manage Protections

The screenshot displays the Check Point management console interface. On the left, a list of protection objects is shown under the 'Blade' category, including 'IPS', 'Reputation IPs', 'Reputation URLs', 'Reputation Domains', 'Mail Activity', and 'Unusual Activity'. The 'Unusual Activity' blade is selected, showing a table of protection objects:

Protection	Category	Blade
Bot lookup IP location.C	Unusual Activity	Anti-Bot
Communication to a known malware sinkhole.A	Unusual Activity	Anti-Bot
Communication to a known malware sinkhole.B	Unusual Activity	Anti-Bot
Communication to a known malware sinkhole.D	Unusual Activity	Anti-Bot
Communication to a known malware sinkhole.E	Unusual Activity	Anti-Bot
Possible bot DNS cache poisoning.A	Unusual Activity	Anti-Bot
Possible bot DNS cache poisoning.B	Unusual Activity	Anti-Bot

Below the table, the configuration for 'Bot lookup IP location.C' is shown. The 'Summary' tab is active, displaying the 'Blade' as 'Anti-Bot' and the 'Engine' as 'Behavioral Patterns'. A 'Confidene Level' slider is also visible.

An 'Add Exception' dialog box is open in the foreground. It shows the following configuration:

- Protection: Bot lookup IP location.C
- Scope: A table with one entry: \* Any
- Source: (Dropdown menu)
- Destination: (Dropdown menu)
- Service: (Dropdown menu)
- Install On: (Dropdown menu)
- Apply On: Global exception group (apply on all rules)

Buttons for 'OK' and 'Cancel' are at the bottom of the dialog. A pink callout box labeled 'Actions menu' points to the right side of the interface.

# Anti-Virus and Anti-Bot Initiate Update Process sk117852

## For Anti-Bot file:

- `# cd $FWDIR/amw/update/`
- Edit the file `next_update`:  
Change the first row from *any number* to `1`
- Run: `# watch -n 1 ls -lh`
- Wait for the size of the `next_update` file to increase. This should take up to two minutes.

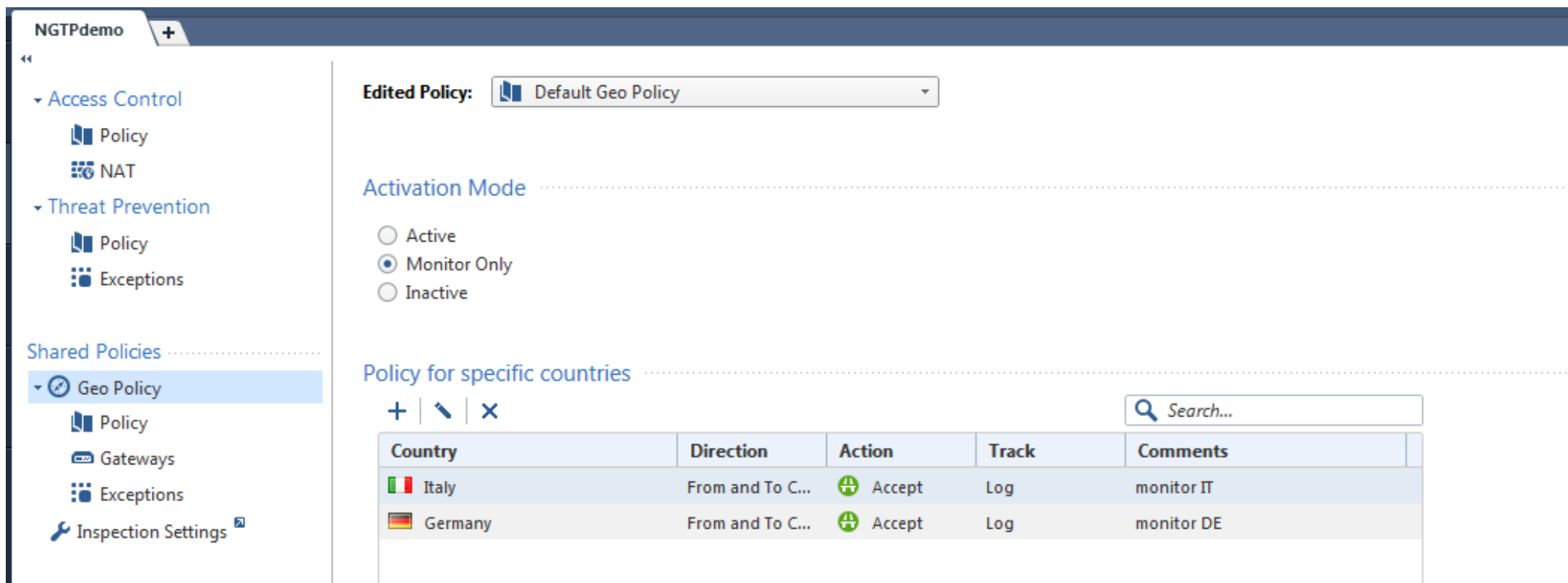
## For Anti-Virus file:

- `# cd $FWDIR/amw_kss/update/`
- Edit the file `next_update`:  
Change the first row from *any number* to `1`
- Run: `# watch -n 1 ls -lh`
- Wait for the size of the `next_update` file to increase. This should take up to two minutes.

# Two slides about Geo Protections

# Geo Protections

- Enforced using a profile
- Installed with the Access Policy







The screenshot shows the NGTPdemo web interface. On the left is a navigation menu with sections for Access Control, Threat Prevention, and Shared Policies. The 'Geo Policy' option under Shared Policies is selected. The main content area shows the configuration for the 'Default Geo Policy'. The 'Activation Mode' is set to 'Monitor Only'. Below this, there is a table titled 'Policy for specific countries' with columns for Country, Direction, Action, Track, and Comments. Two entries are visible: Italy and Germany, both with 'Accept' actions and 'Log' tracking.

**Edited Policy:** Default Geo Policy

**Activation Mode**

Active  
 Monitor Only  
 Inactive

**Policy for specific countries**

Country	Direction	Action	Track	Comments
 Italy	From and To C...	 Accept	Log	monitor IT
 Germany	From and To C...	 Accept	Log	monitor DE



# Geo Protections

- Geo location information will be added to the logs
- SecureXL connection rate acceleration remains active

```
Log Details
Accept
http Traffic Accepted from 192.168.170.10 to 90.147.160.69

gwR8010> fwaccel stat
Accelerator Status : on
Accept Templates : enabled
Drop Templates : disabled
NAT Templates : disabled by user
NMR Templates : enabled
NMT Templates : enabled

Accelerator Features : Accounting, NAT, Cryptography, Routing,
                      HasClock, Templates, Synchronous, IdleDetection,
                      Sequencing, TcpStateDetect, AutoExpire,
                      DelayedNotif, TcpStateDetectV2, CPLS, McastRouting,
                      WireMode, DropTemplates, NatTemplates,
                      Streaming, MultiFW, AntiSpoofing, Nac,
                      ViolationStats, AsynchronousNotif, ERDOS,
                      McastRoutingV2, NMR, NMT, NAT64, GTPAcceleration,
                      SCTPAcceleration

Cryptography Features : Tunnel, UDPEncapsulation, MD5, SHA1, NULL,
                      3DES, DES, CAST, CAST-40, AES-128, AES-256,
                      ESP, LinkSelection, DynamicVPN, NatTraversal,
                      EncRouting, AES-XCBC, SHA256

gwR8010>
```

# UPDATING MONITORING



# CPVIEW

## Observe rad\_admin stats for Software Blades

- The resource advisor is the instance communicating with ThreatCloud

```
CPVIEW.Advanced.RAD
-----
Overview SysInfo Network CPU Software-blades Advanced
-----
CPU-Profiler Memory Network SecureXL ClusterXL CoreXL PrioQ Streaming RAD UP HTTP-Parser
-----

To activate RAD statistics, run 'rad_admin stats'
-----

RAD General Information:

RAD Statistics Up Time      13 days, 19:28:15

Name                APPI      AB      AV      URLF
Found in LDB        N/A      N/A      N/A      5
Sent to Site        0         12      0        99
Round Trip (ms)     0        1,427   0       45,378
Hit Count           0         514     0       1,071
Miss Count          0         29      0        104
Error Count         0         0        0         0
Cache Size (bytes)  0         0        0       3,788
Max Cache Size (bytes) 0         0        0       3,788
Cache Total Host Records 0         0        0        55
Max Cache Total Host Records 0         0        0        55
Avg Family Size     0         0        0         0
Max Family Size     0         0        0         71
Expired Requests    0         0        0         9
```

# Updating Threat Prevention Protections

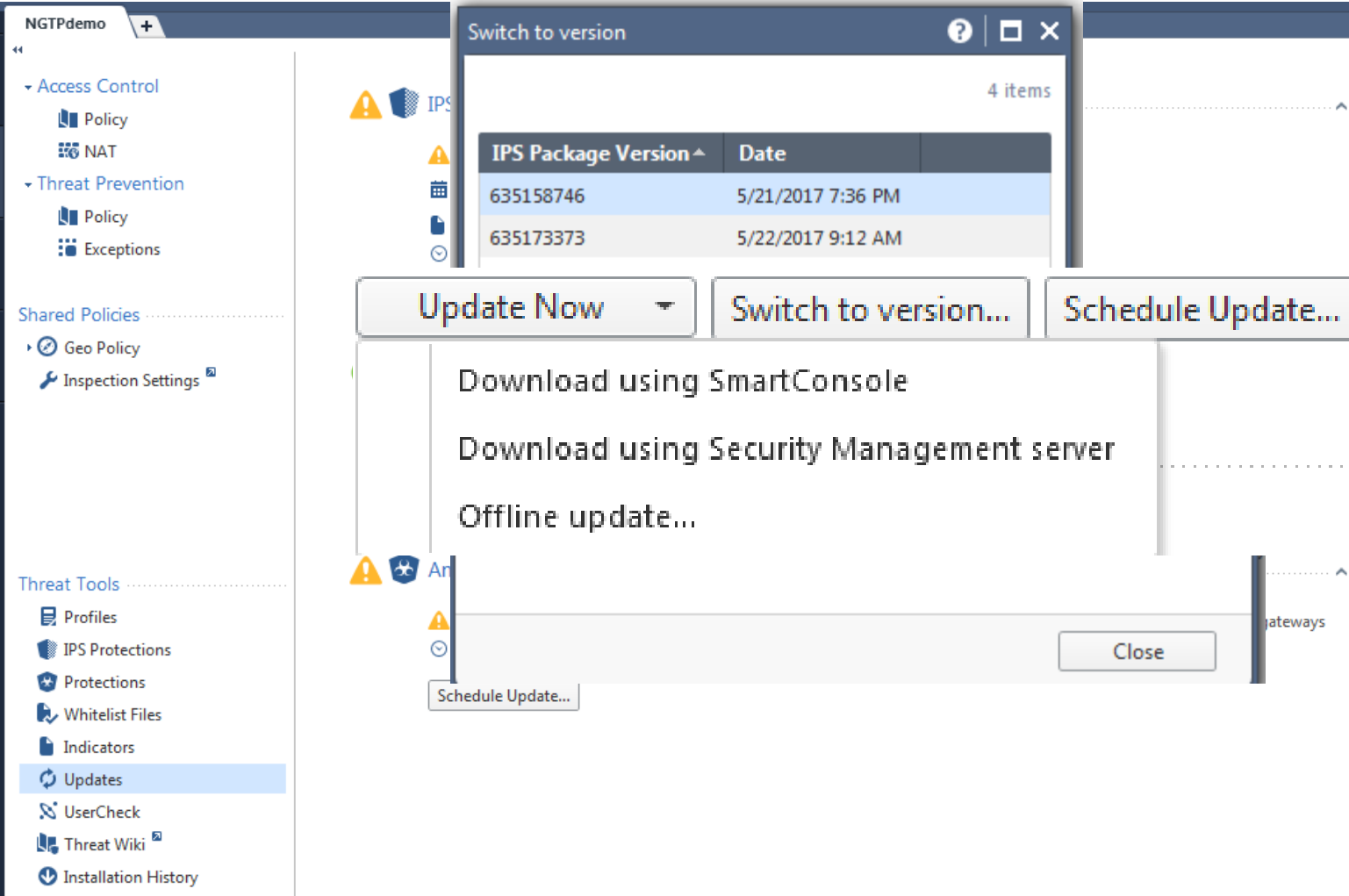
## Challenges of the past

- R77.30 and earlier
- Protections have been stored on a per domain level
- A Multi-Domain Server has stored the same protection per each domain
- The guideline performing Database Revision Control before updating the IPS Protections was not applicable when managing VSX Gateways ([sk65420](#))

# Updating Threat Prevention Protections

## Managing Protection Updates

- Centralized view
- Download via SmartConsole or Management Server
- “Switch to version” support for IPS protections
- Shared Antivirus and Anti-Bot update configuration



The screenshot displays the SmartConsole interface for managing updates. On the left, a navigation pane shows 'Updates' selected under 'Threat Tools'. The main area shows a list of updates with a 'Switch to version' dialog box open. The dialog box contains a table with the following data:

IPS Package Version	Date
635158746	5/21/2017 7:36 PM
635173373	5/22/2017 9:12 AM

Below the table, there are three buttons: 'Update Now', 'Switch to version...', and 'Schedule Update...'. A dropdown menu is open under 'Schedule Update...', showing options: 'Download using SmartConsole', 'Download using Security Management server', and 'Offline update...'. A 'Close' button is visible at the bottom right of the dialog box.

# Monitoring

- Check Point Support [sk43733](#) documents a tool to measure the CPU resources
  - Learn which IPS Protections are causing High CPU Load
  - The script collects information to csv files
- The following script collects and analyzes the required data - *`$FWDIR/scripts/get_ips_statistics.sh`*
- To see the complete usage instructions, run:  
  
*`[Expert@HostName]# $FWDIR/scripts/get_ips_statistics.sh -h`*
- The *`$FWDIR/scripts/get_ips_statistics.sh`* script generates a report, which includes **both** IPS and Pattern Matcher statistics.
- In addition statistics about the Pattern Matcher can be collected.
  - These information can be analyzed by Check Point R&D

# Monitoring

- Use SNMP to monitor the CPU and memory usage
- Extract from “IPS Best Practices Guide”
  - Average load of the CPUs should be lower than 30%
  - Peak load of the CPUs should not exceed 50%
  - At least 20% of RAM should be free
- Consider if you need IPS Protections with Performance Impact “Critical”

**Detect and Prevent Action have almost the same performance impact  
Logging and Packet Capture are impacting the performance!**

# Monitoring

- Best Practices for Performance Tuning are documented in [sk98348](#)

Table of Contents (click on section titles to see sub-sections):

- **(1) Background**
- **(2) Introduction and Limitations**
- **(3) Best practices**
  - [3-1] Network interface cards
  - [3-2] Throughput
  - [3-3] SecureXL
  - [3-4] CoreXL
  - [3-5] SecureXL with CoreXL
  - [3-6] SMT (HyperThreading)
  - [3-7] Multi-Queue
  - [3-8] Rulebase optimization
  - [3-9] IPS optimization
  - [3-10] Application Control & URL Filtering optimization
  - [3-11] Anti-Virus & Anti-Bot optimization
- **(4) Initial diagnostics**
- **(5) Advanced diagnostics**
- **(6) Command Line syntax**
- **(7) Examples**
- **(8) Related documentation**
- **(9) Related solutions**
- **(10) Revision history**





# Summary

- The Value Of Architecture
- Understand The Components
- Optimize Your Policy



Check Point®  
SOFTWARE TECHNOLOGIES LTD

THANK YOU

WELCOME TO THE FUTURE OF  
**CYBER SECURITY**

CLOUD • MOBILE • THREAT PREVENTION