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

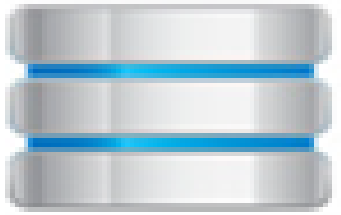
Three essential components of a secure network:

Check Point Firewall Architecture

Check Point
SOFTWARE TECHNOLOGIES LTD

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

Check Point
SOFTWARE TECHNOLOGIES LTD

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

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

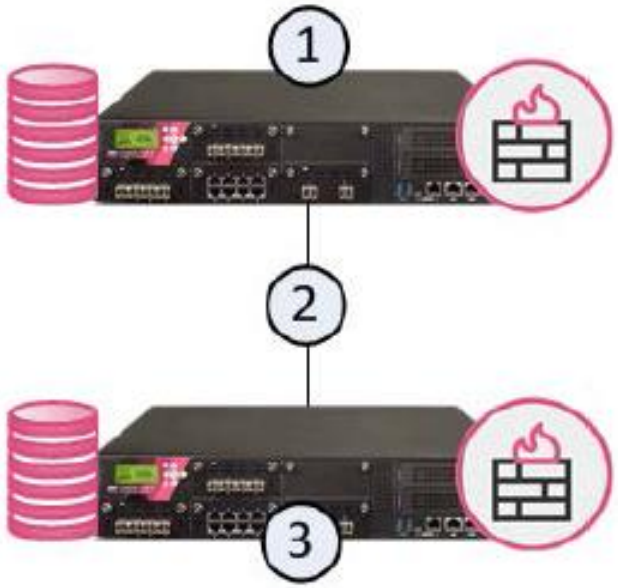
The Security Management Server (1) and the Security Gateway (3) are installed on different computers or appliances, with a network connection (2).

Item	Description
1	Security Management Server
2	Network connection
3	Security Gateway
	Security Gateway component
	Security Management component

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.

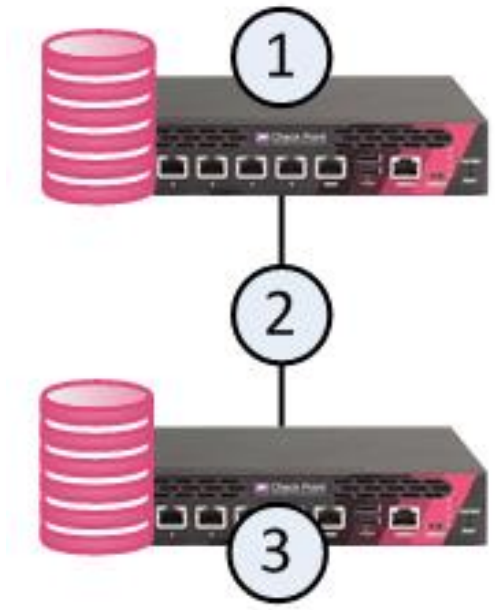


Item	Description
1	Security Management Server
2	Network connection
3	Security Gateway
	Security Gateway component
	Security Management component

Management HA

Management HA

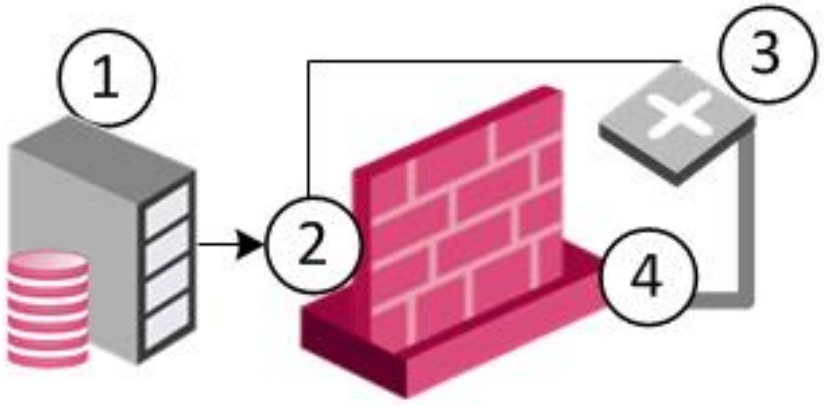
A Primary Security Management Server (1) has a direct or indirect connection (2) to one or more Secondary Security Management Servers (3).



Item	Description
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.

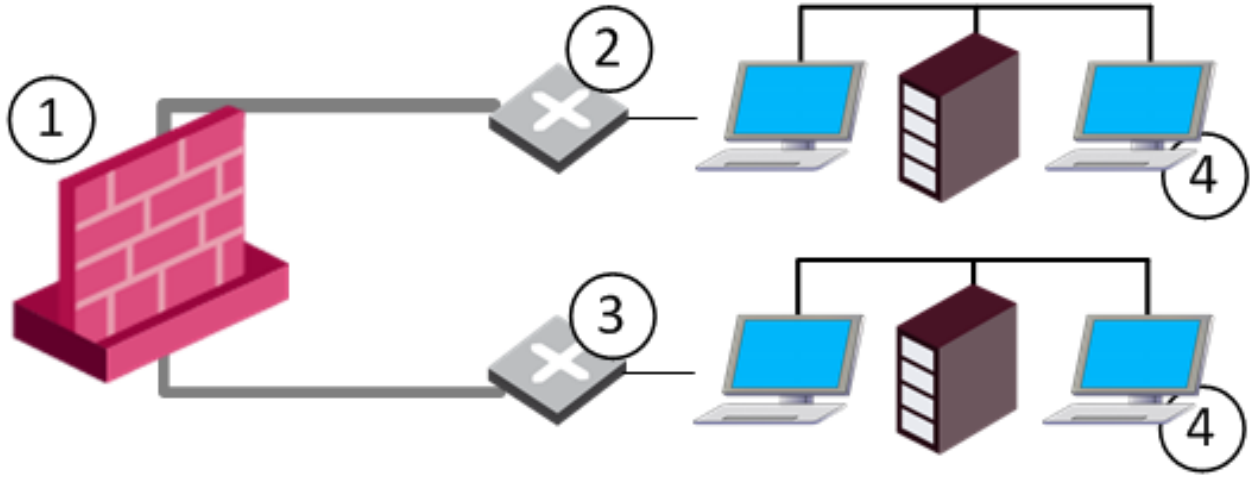


Item	Description
1	Security Management Server sends management packet to management interface
2	Management interface on Security Gateway Firewall bridging Layer-2 traffic inspects the packet and sends it to the router
3	Router sends the packet to the bridge interface
4	Bridge interface drops the packet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

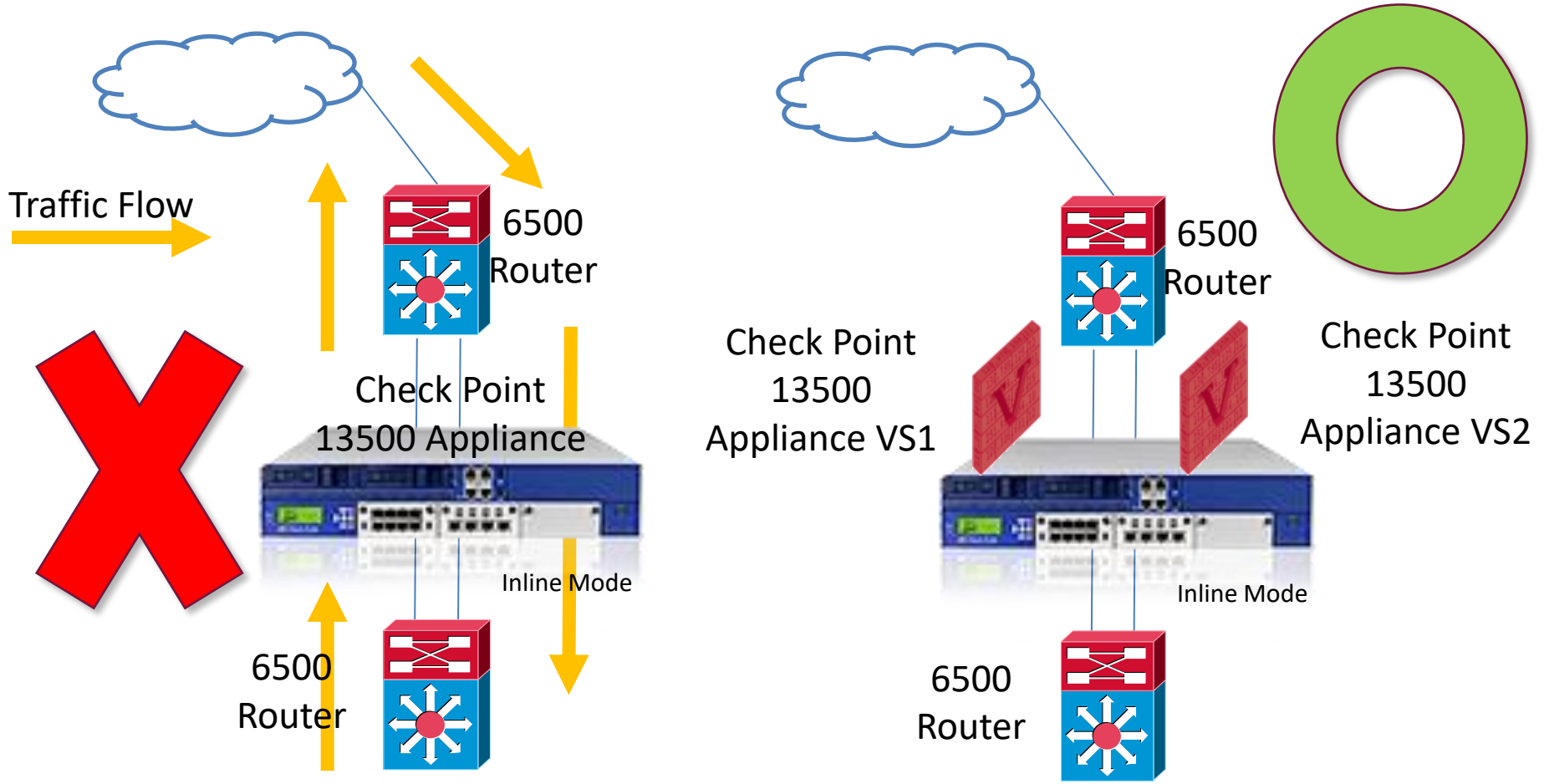
Important Note of Bridge Mode.(1)

- 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)



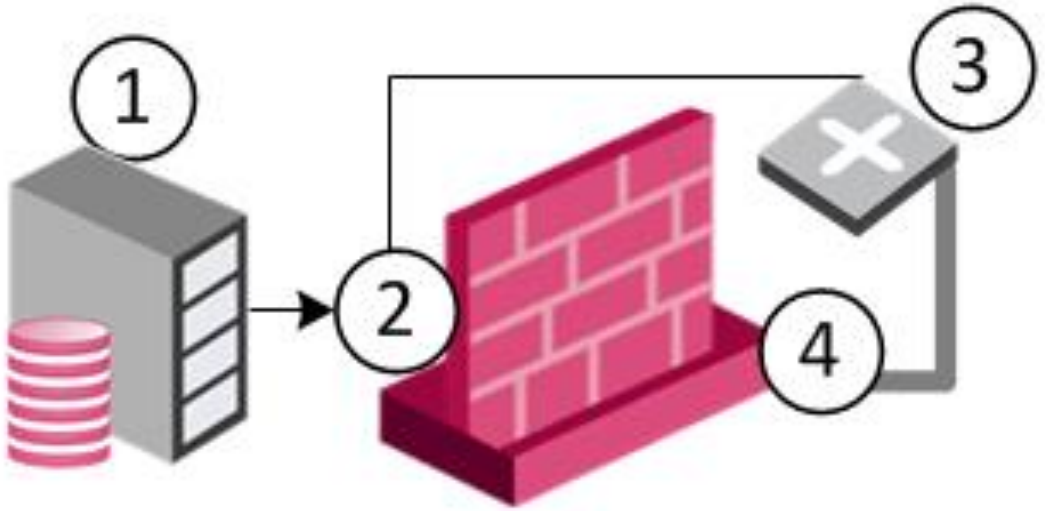
Important Note of Bridge Mode.(3)

To enable management over the bridge:

1. Edit `$FWDIR/boot/modules/fwkern.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

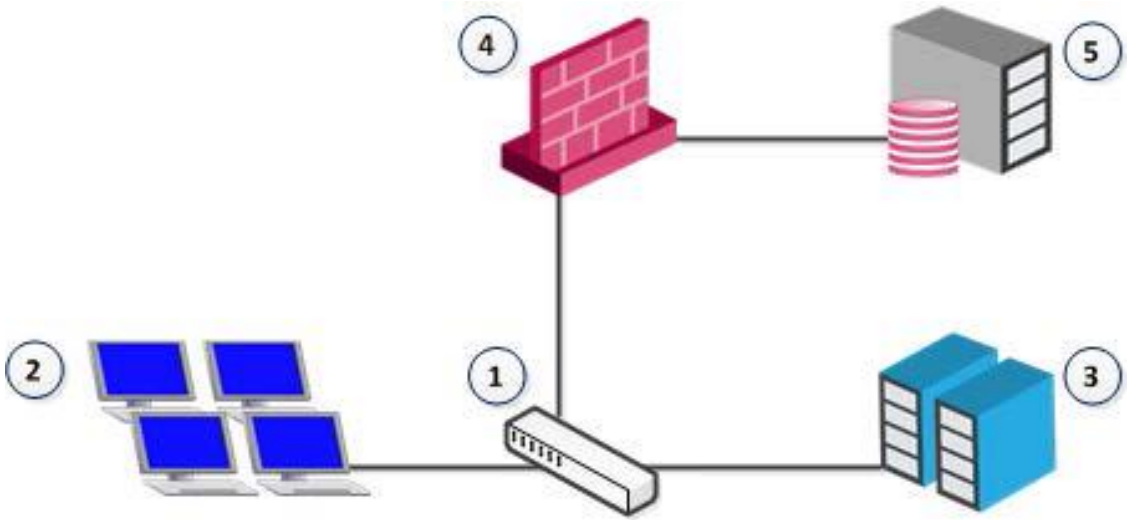
Check Point
SOFTWARE TECHNOLOGIES LTD

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 sk89581)	No (see sk79700)
HTTP / HTTPS proxy	Yes	No
SMTP / HTTP / FTP / POP3 Security Servers	Yes	No
Client Authentication	Yes	No
User Authentication	Yes	No

Monitor(Sniffer) Mode



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

You can use mirror ports in these scenarios:

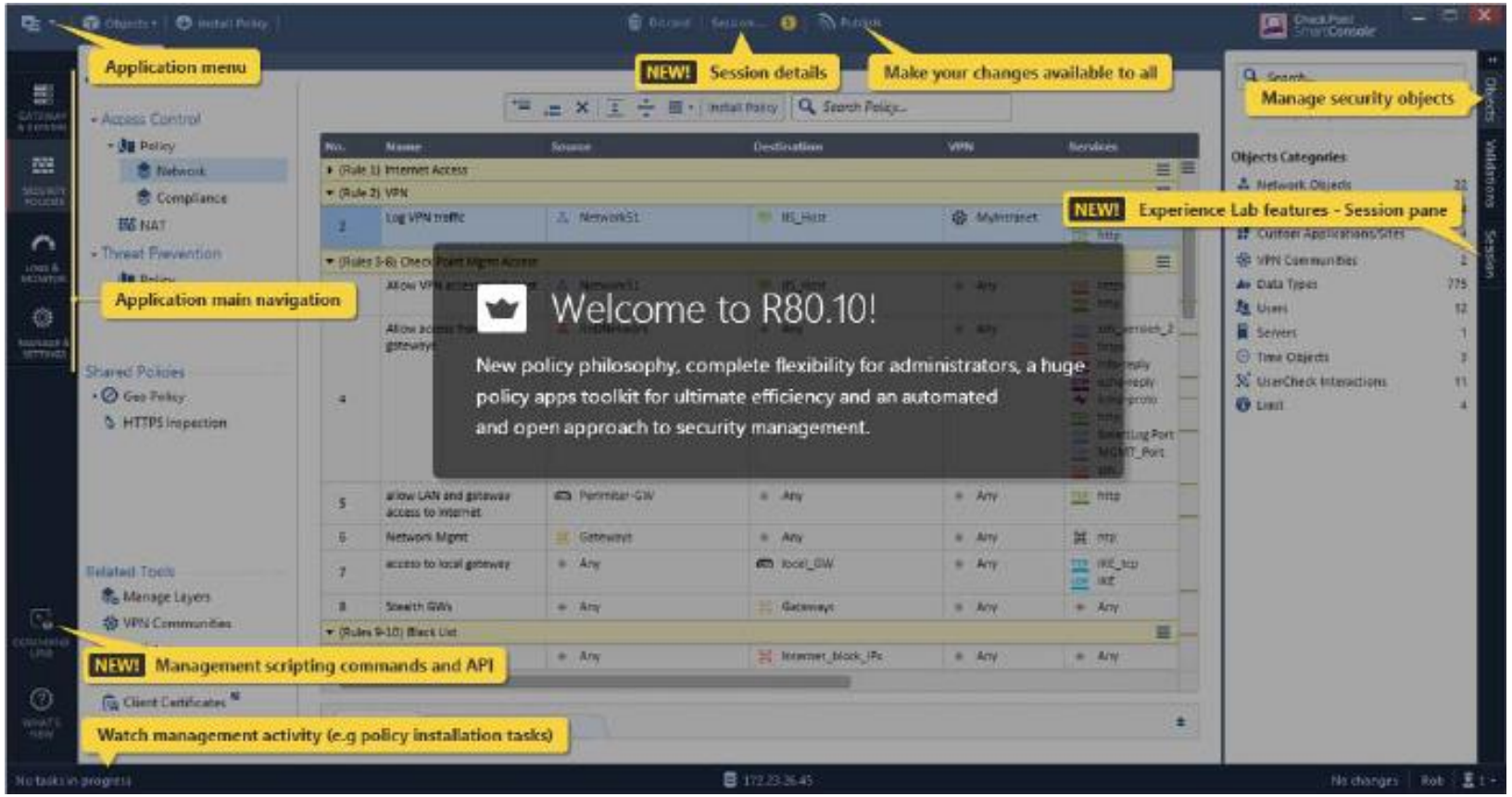
- To monitor the use of applications as a permanent part of your deployment
- To evaluate the capabilities of the Application Control and IPS blades before you buy them

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

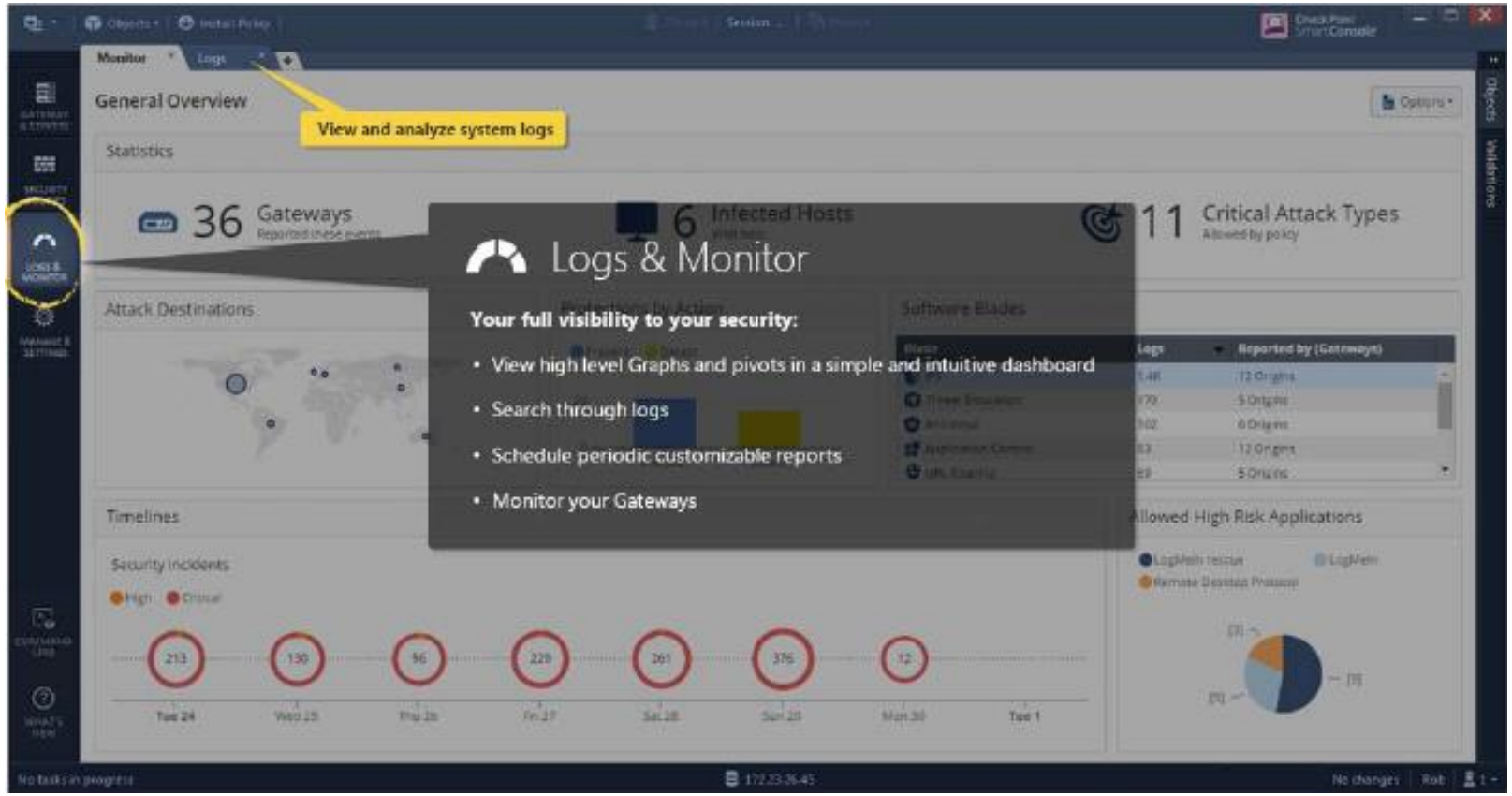
- Server Status
- Module version
- Active software blades
- CPU usage
- Object summary

Security Policies Tab

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

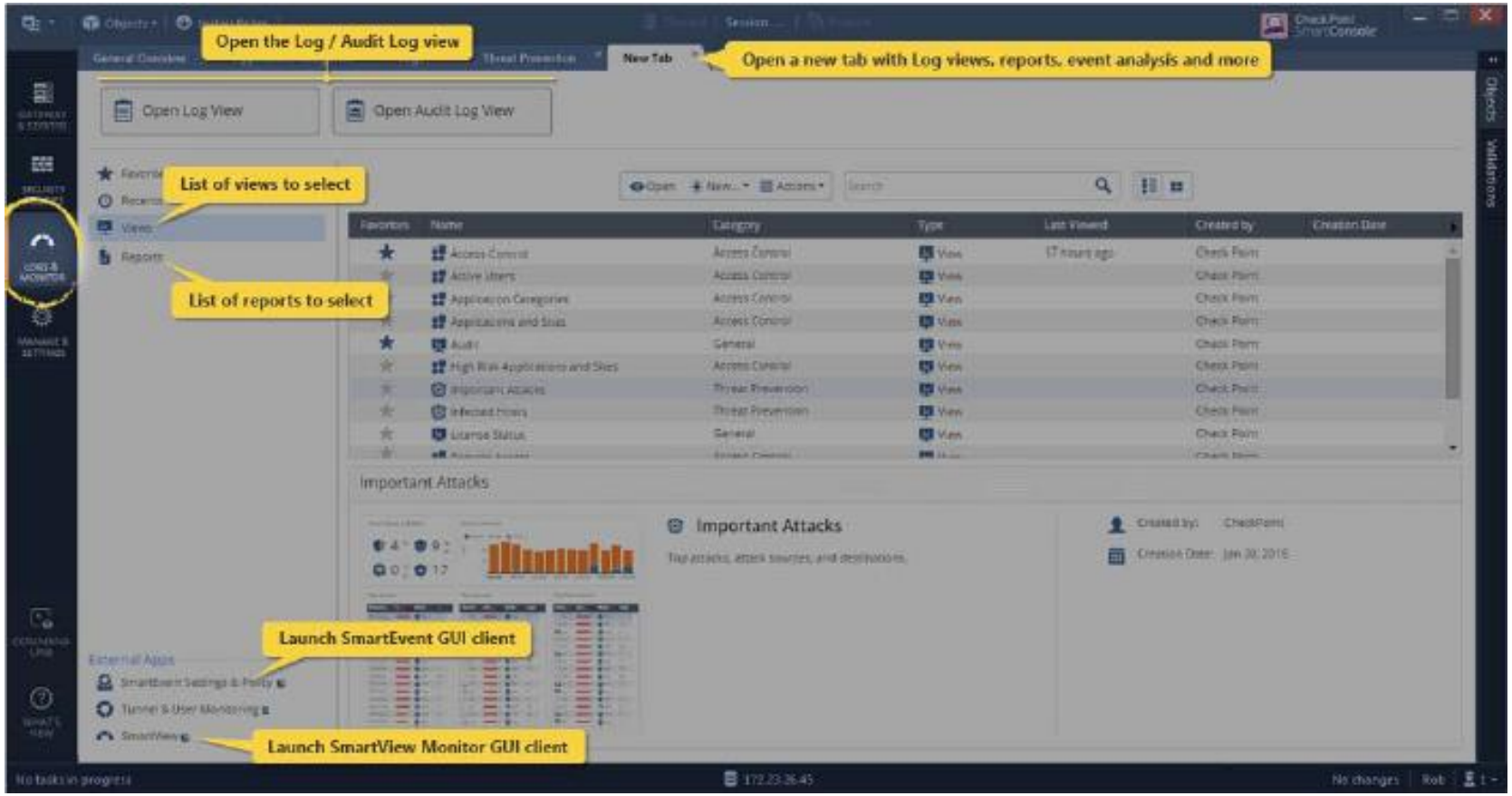
Logs & Monitor Tab

- Gateway Statistics
- Infected hosts summary



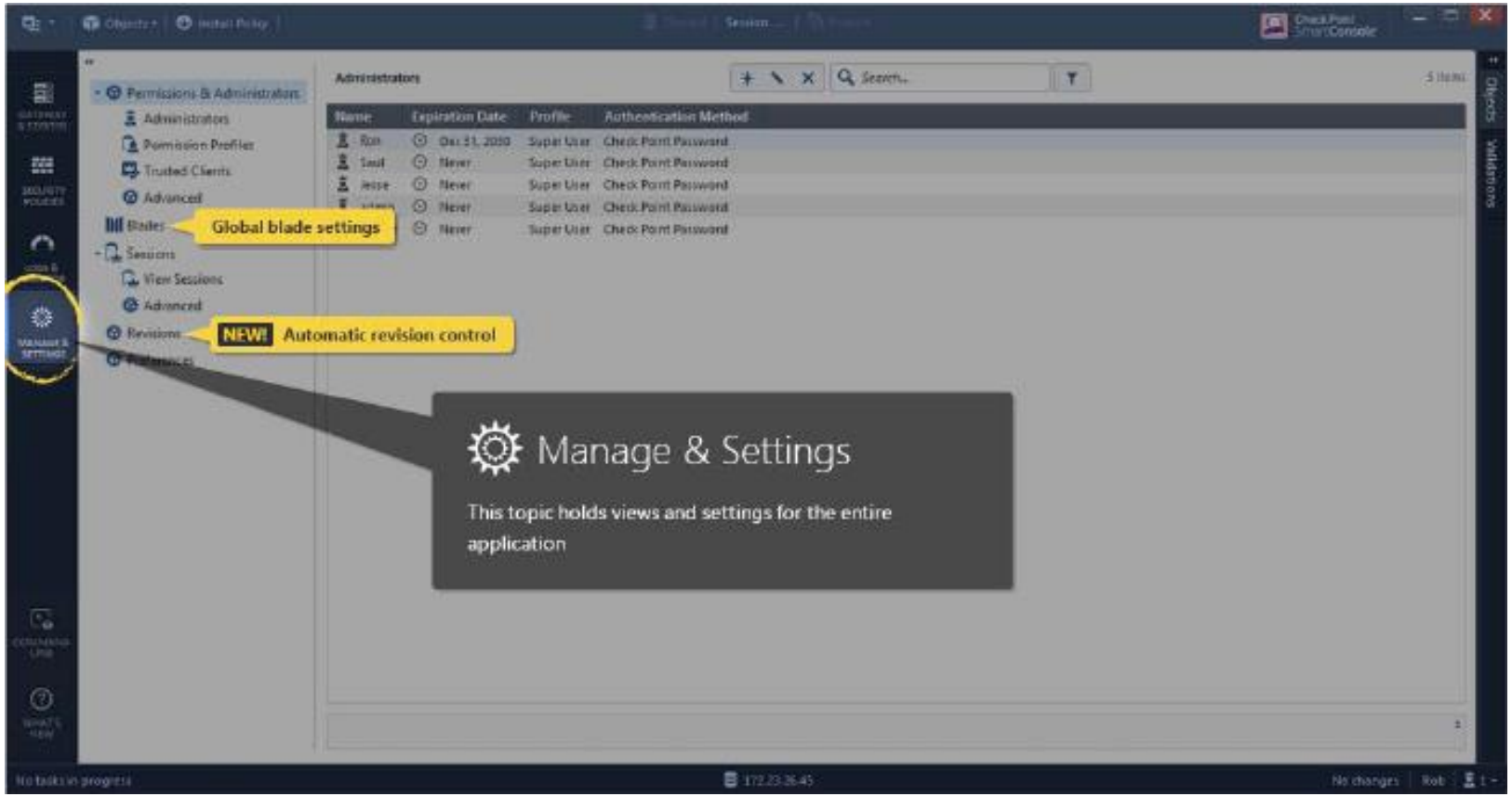
Logs & Monitor Tab

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



Manage & Settings Tab

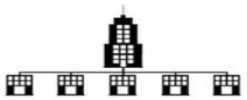
- Administrators
- Permission profiles
- Global software blades setting
- Automatic Security Policy revision control



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 command:

  lock database override

  unlock database

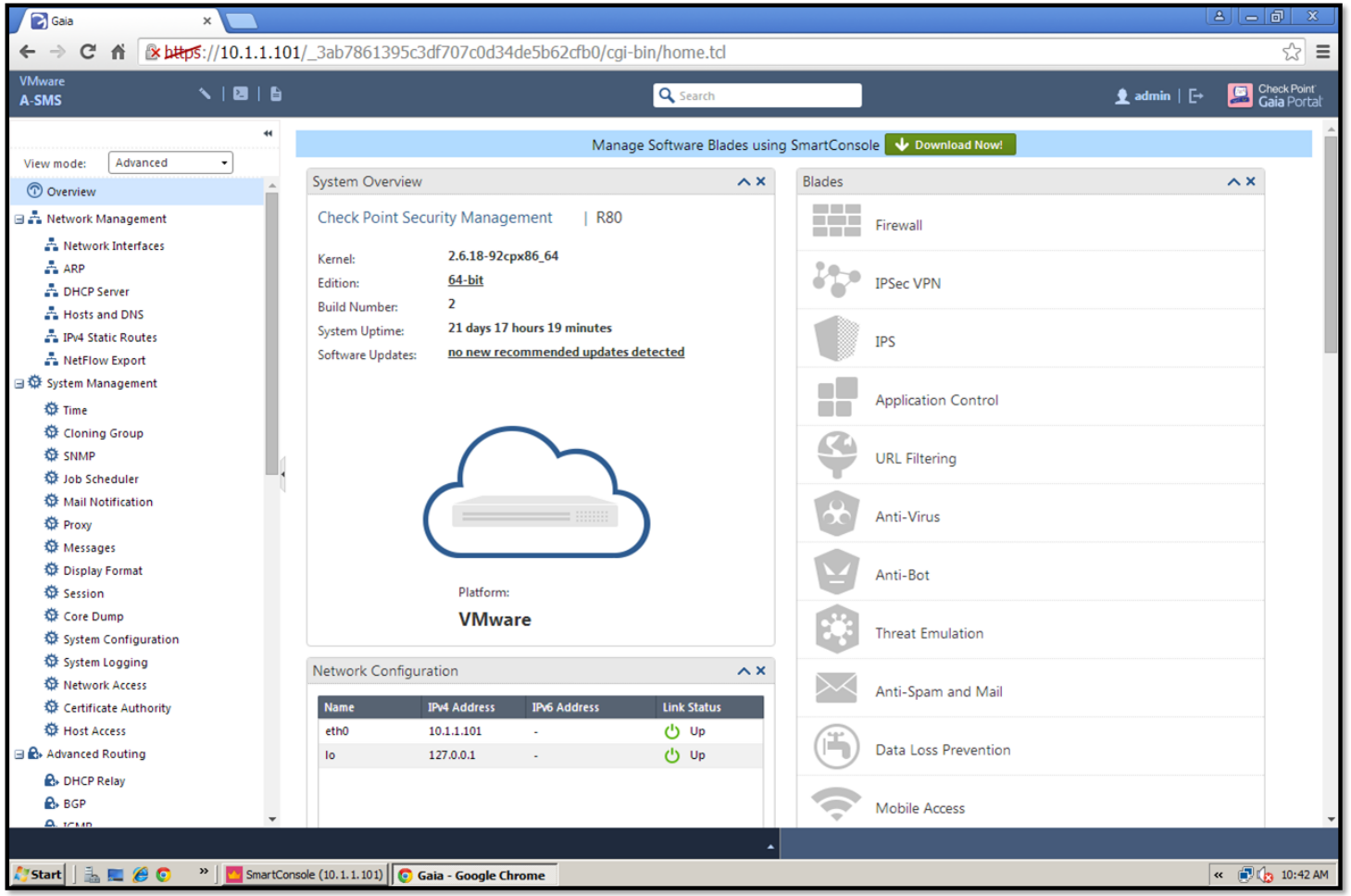
- Both commands obtain the configuration lock from another administrator.

WebUI

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

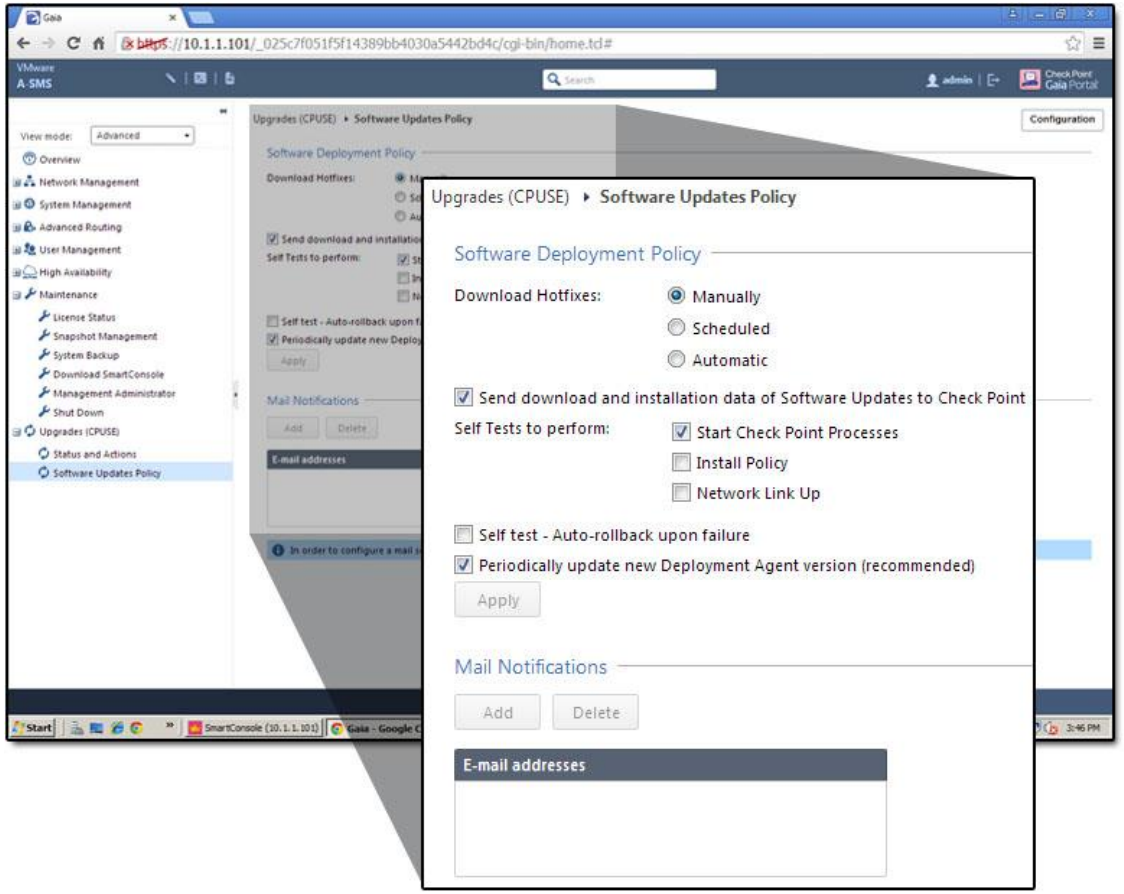
Two modes:

- Simplified
- Advanced



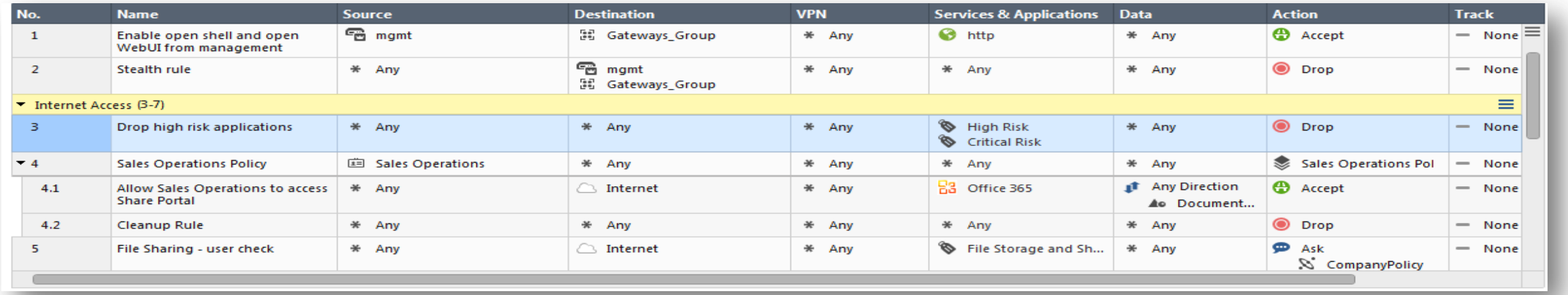
Updates

- 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
Internet Access (3-7)								
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.	Name	Source	Destination	VPN	Services & Applicat...	Action	Track	Install On	Time
1	NEW	* Any	* Any	* Any	* Any	Drop	— None	* Policy	* Any
2	Cleanup rule	* Any	DMZZone DMZNet	* Any	* Any	Accept	— None	* Policy	* Any

The Default Rule is added when you add a rule to the Rule Base.

Objects

Objects are divided into the following categories:

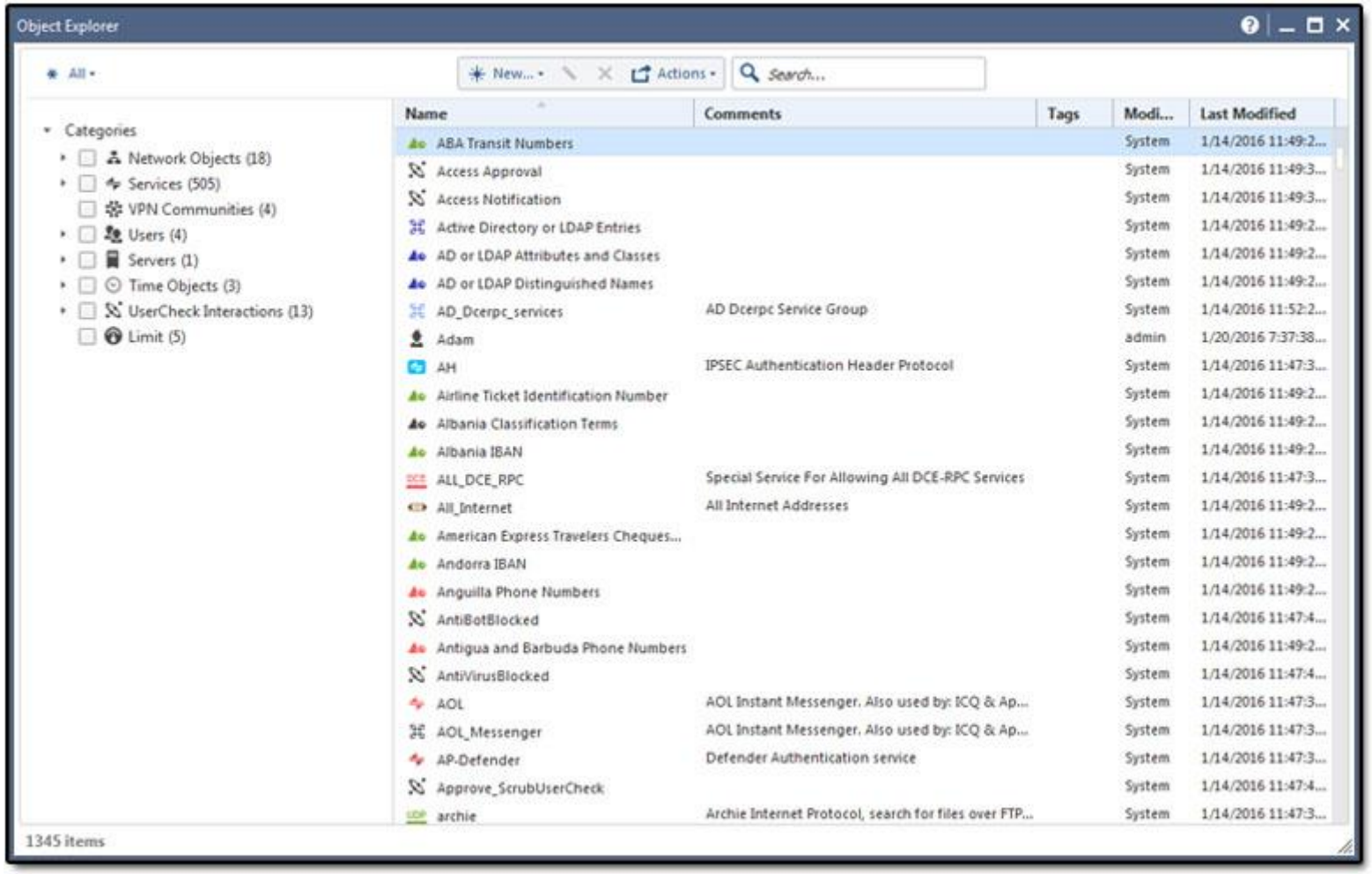
- Network Object
- Service
- Custom Application/Site
- VPN Community
- User
- Server
- Resource
- Time Object
- UserCheck Interactions
- Limit

Objects

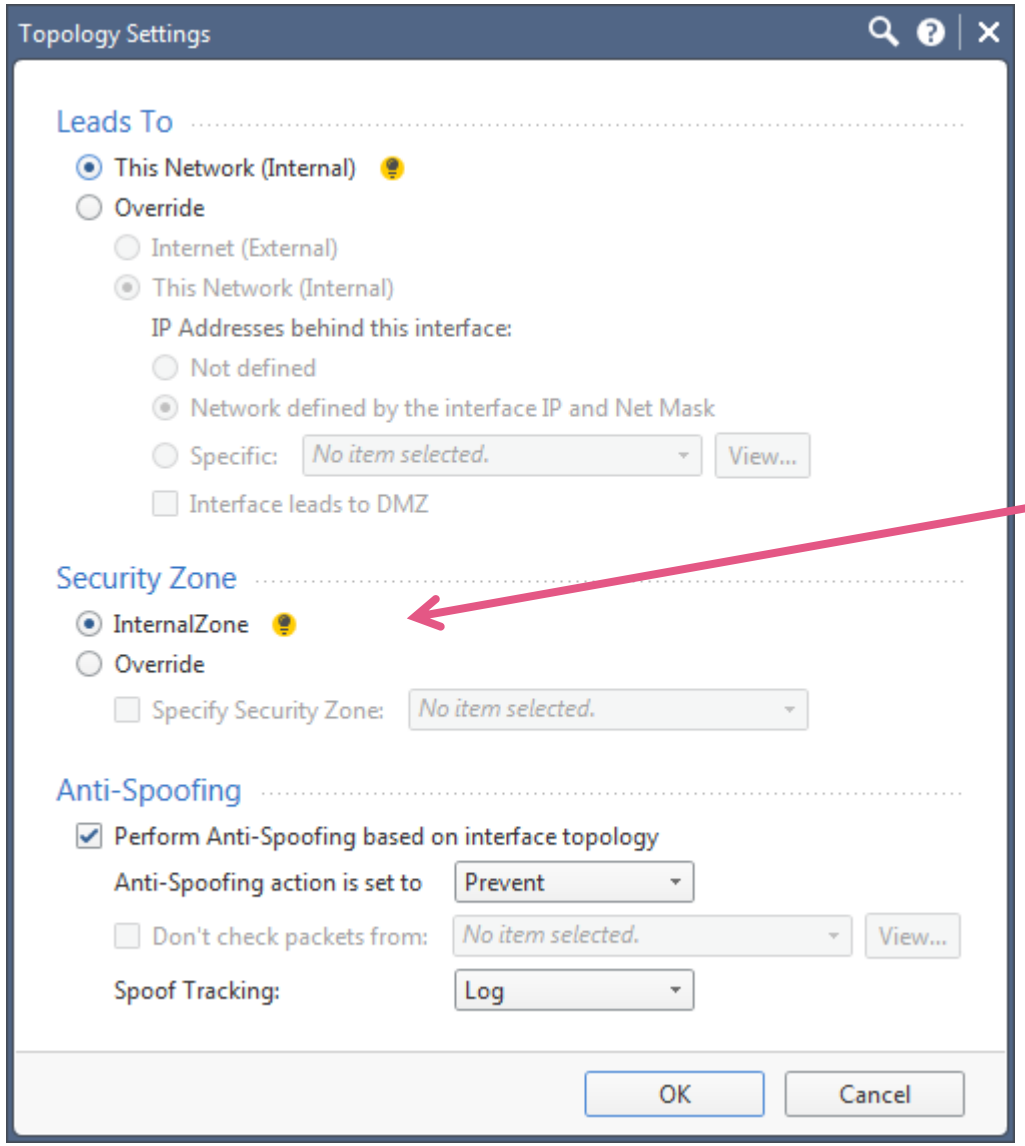
When creating objects, consider organizational needs:

- 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

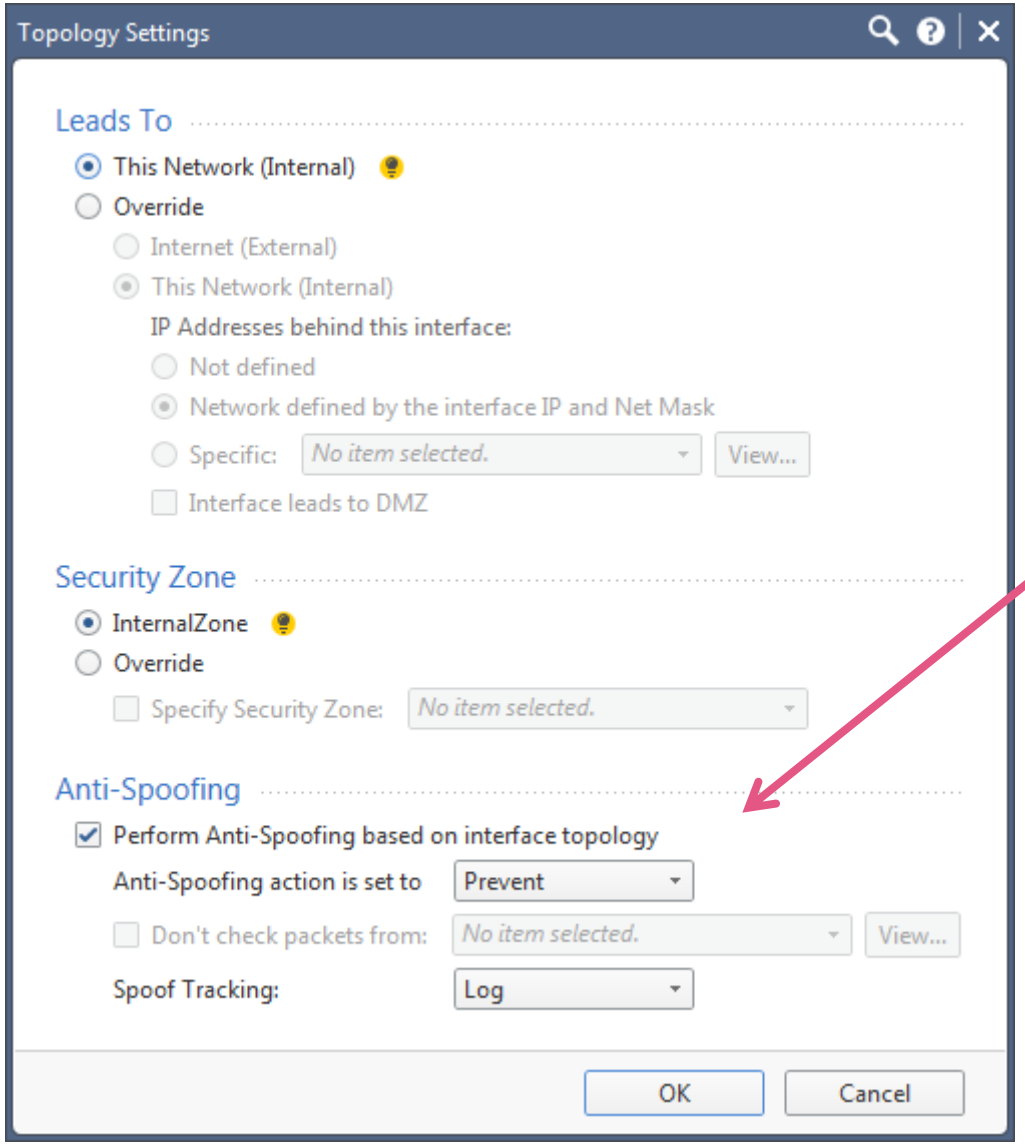


Security Zones



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

Anti-Spoofing



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.

Control Connections

- There are three types of Control Connections defined by default rules:
  - Gateway specific traffic
  - Acceptance of IKE and RDP traffic
  - Communication with various types of servers

Implied Rules

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

Additional Rule Types

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

Rule Base Management

Before creating a Rule Base:

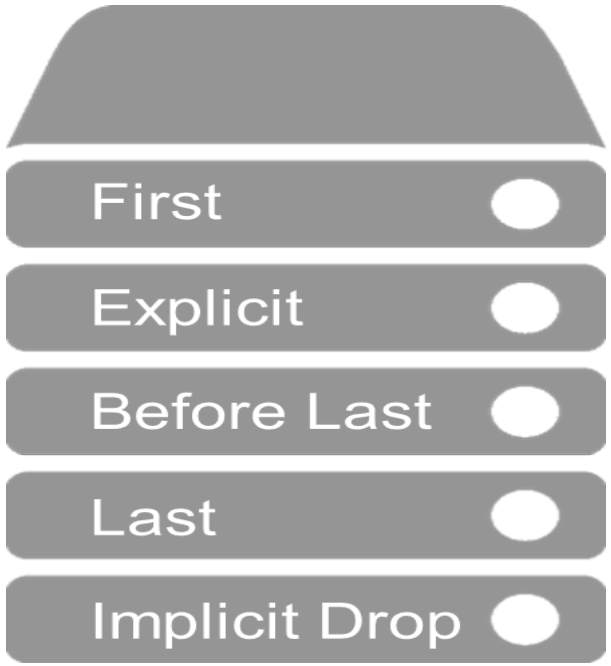
- Which objects are in the network?
- Which user permissions and authentication schemes are needed?
- Which services, including customized services and sessions, are allowed across the network?

Rule Base Management

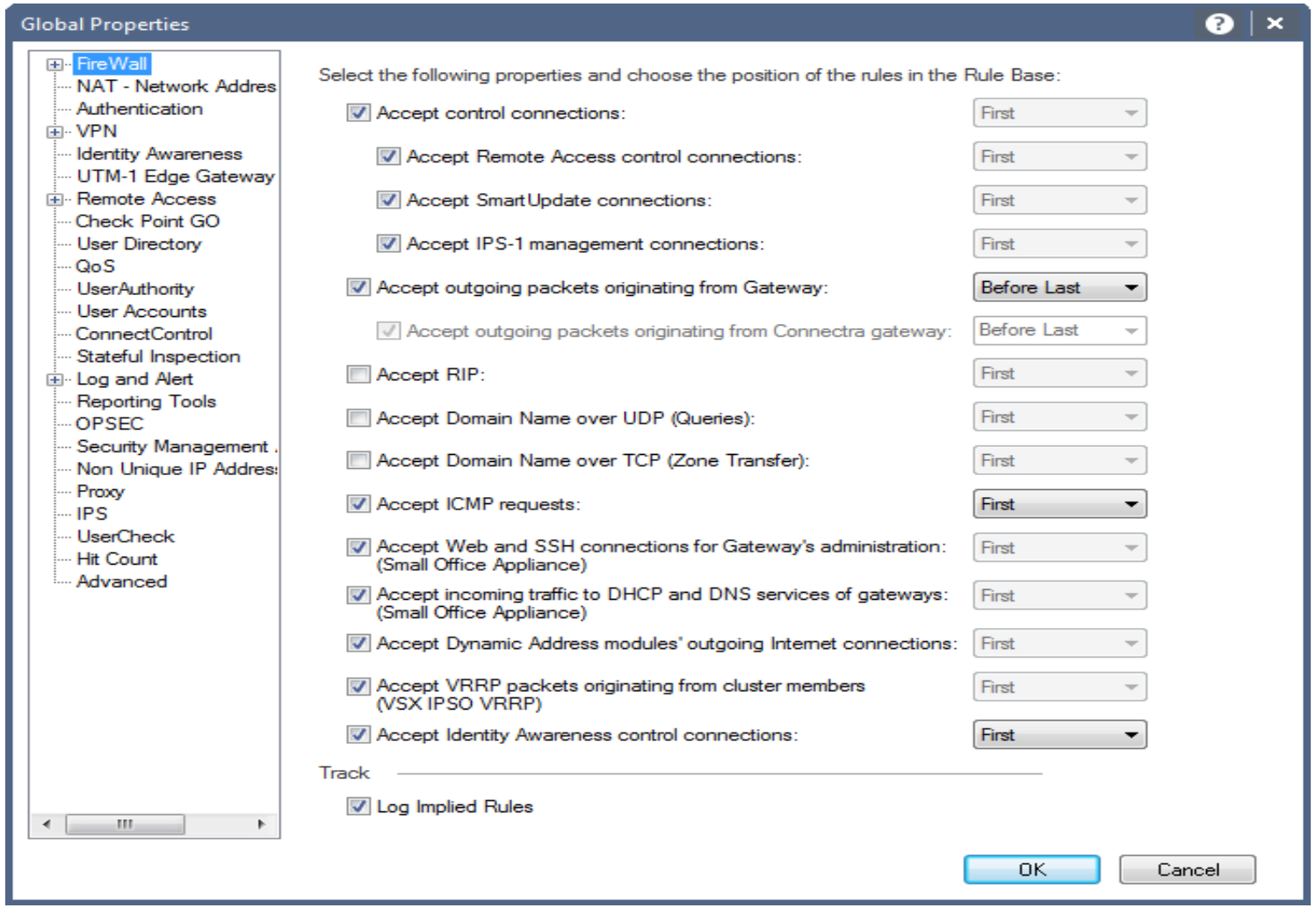
- The Policy is enforced from top to bottom.
- Place the most restrictive rules at the top.
- Keep it simple.
- Add Stealth and Cleanup rules first.
- Limit the use of the Reject action.
- Use section titles to group similar rules.
- Add comments to each rule.
- For efficiency, place most frequency used rules above less frequently used rules.

Understanding Rule Base Order

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

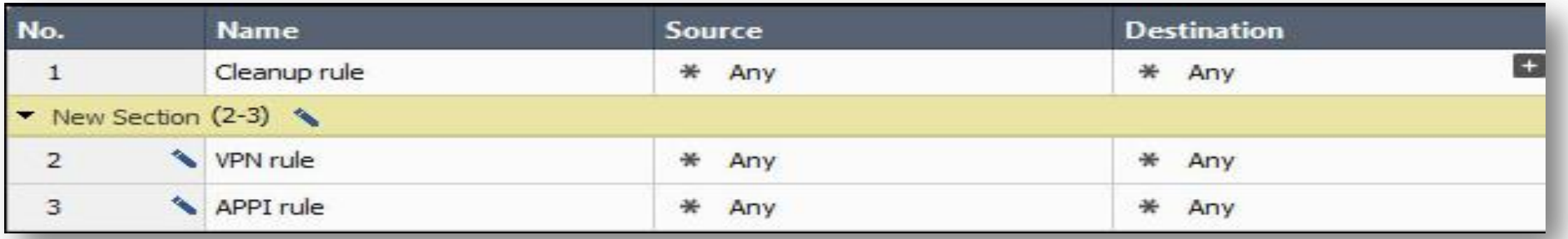


Global Properties



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

Sections

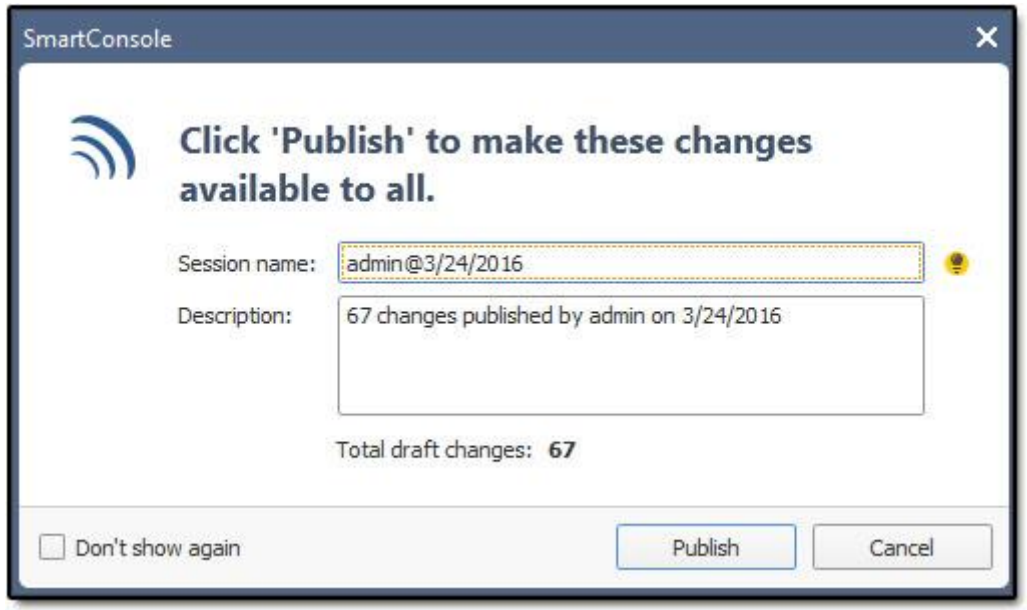


No.	Name	Source	Destination
1	Cleanup rule	* Any	* Any
New Section (2-3)			
2	VPN rule	* Any	* Any
3	APPI rule	* Any	* Any

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.

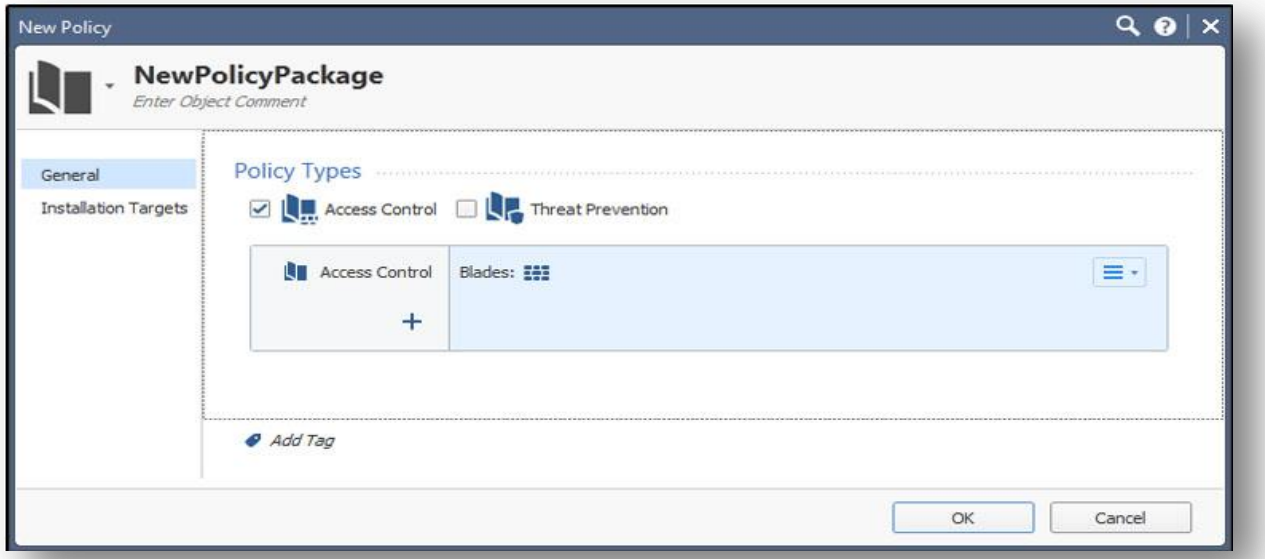


Policy Packages

A group of different types of policies that ar
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

QoS

Policy based bandwidth management solution which allows for prioritizing critical traffic

Desktop Security

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

Threat Prevention

Consist of these types of rules:

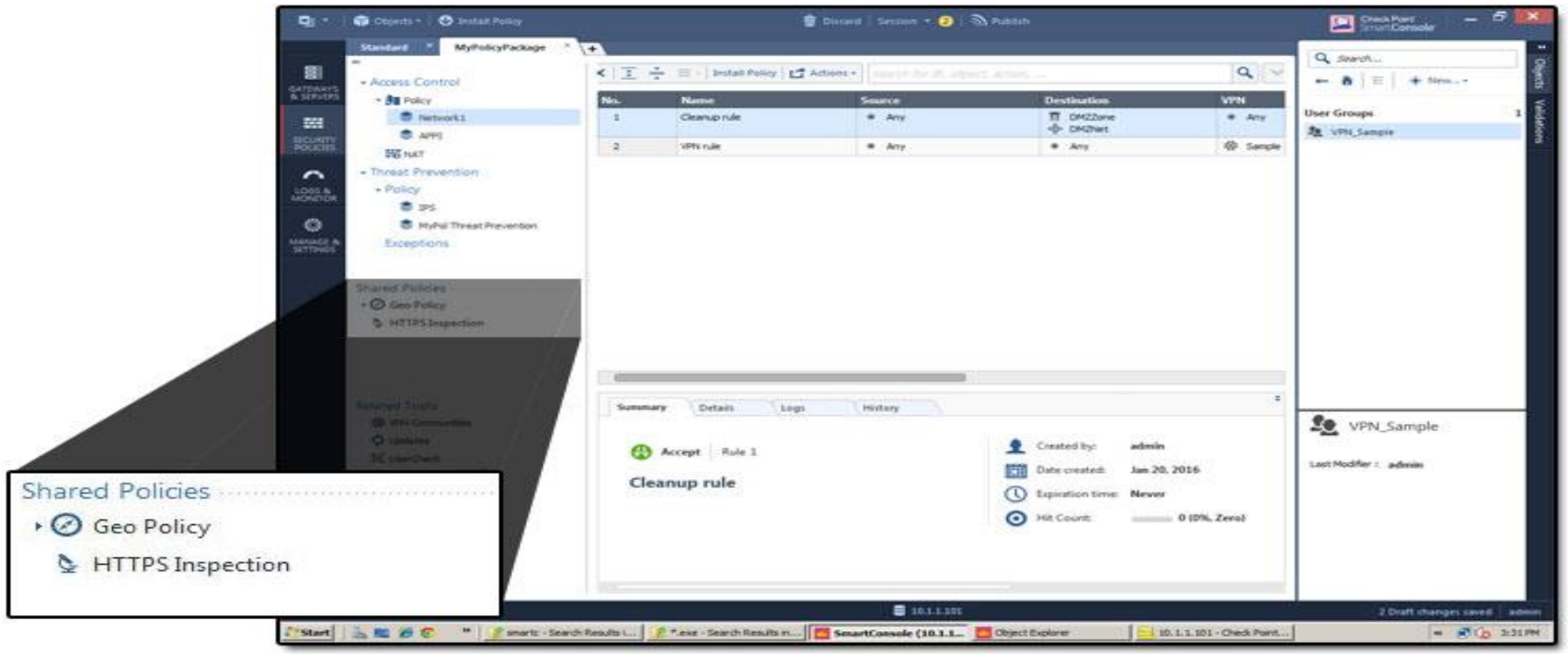
- IPS
- Anti-Bot
- Antivirus
- Threat Emulation

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:

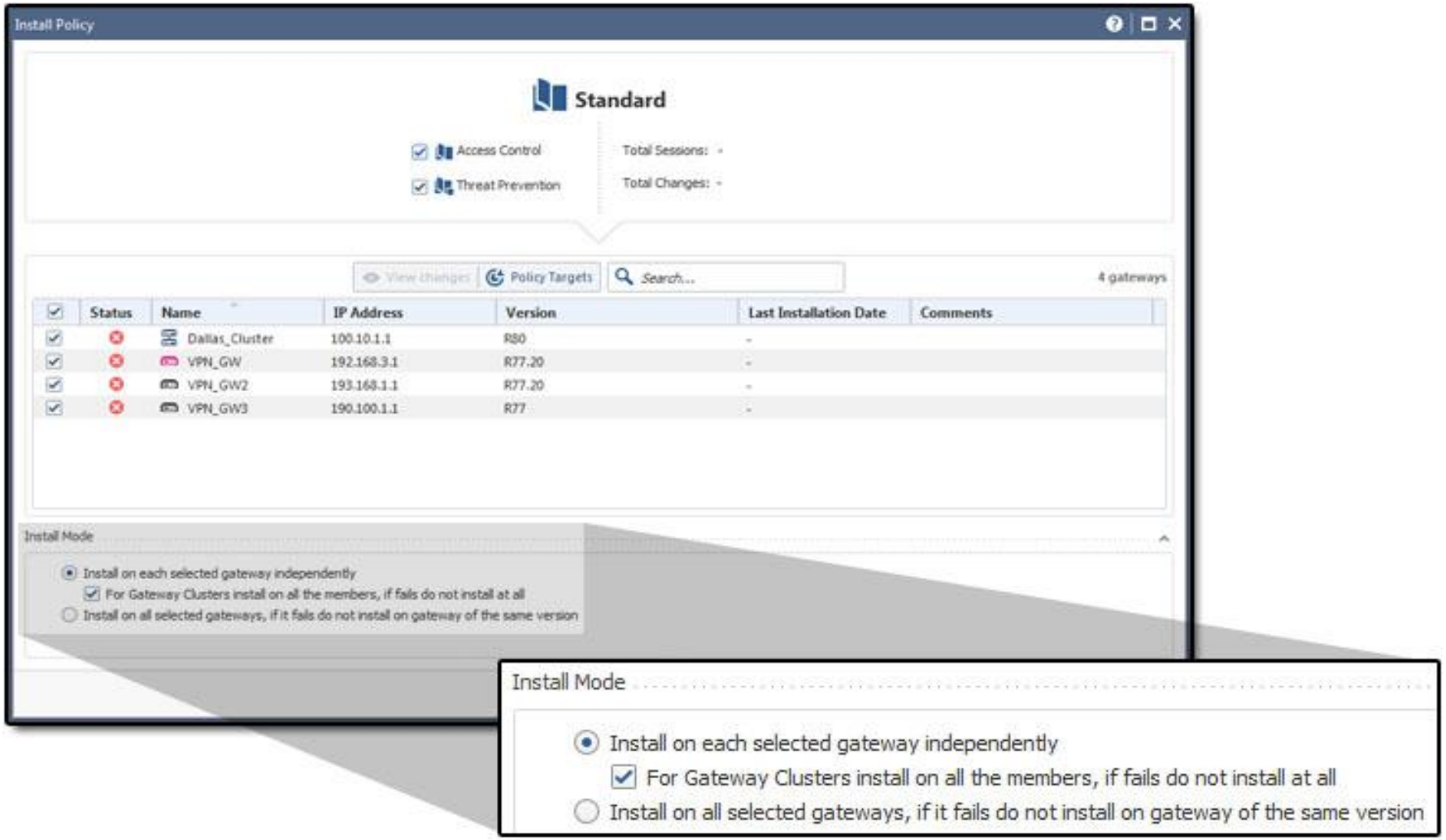
- VPN Communities
- Client Certificates
- Application Wiki
- Installation History
- Updates
- UserCheck

Threat Tools:

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

Install Policy

Install a Policy Package



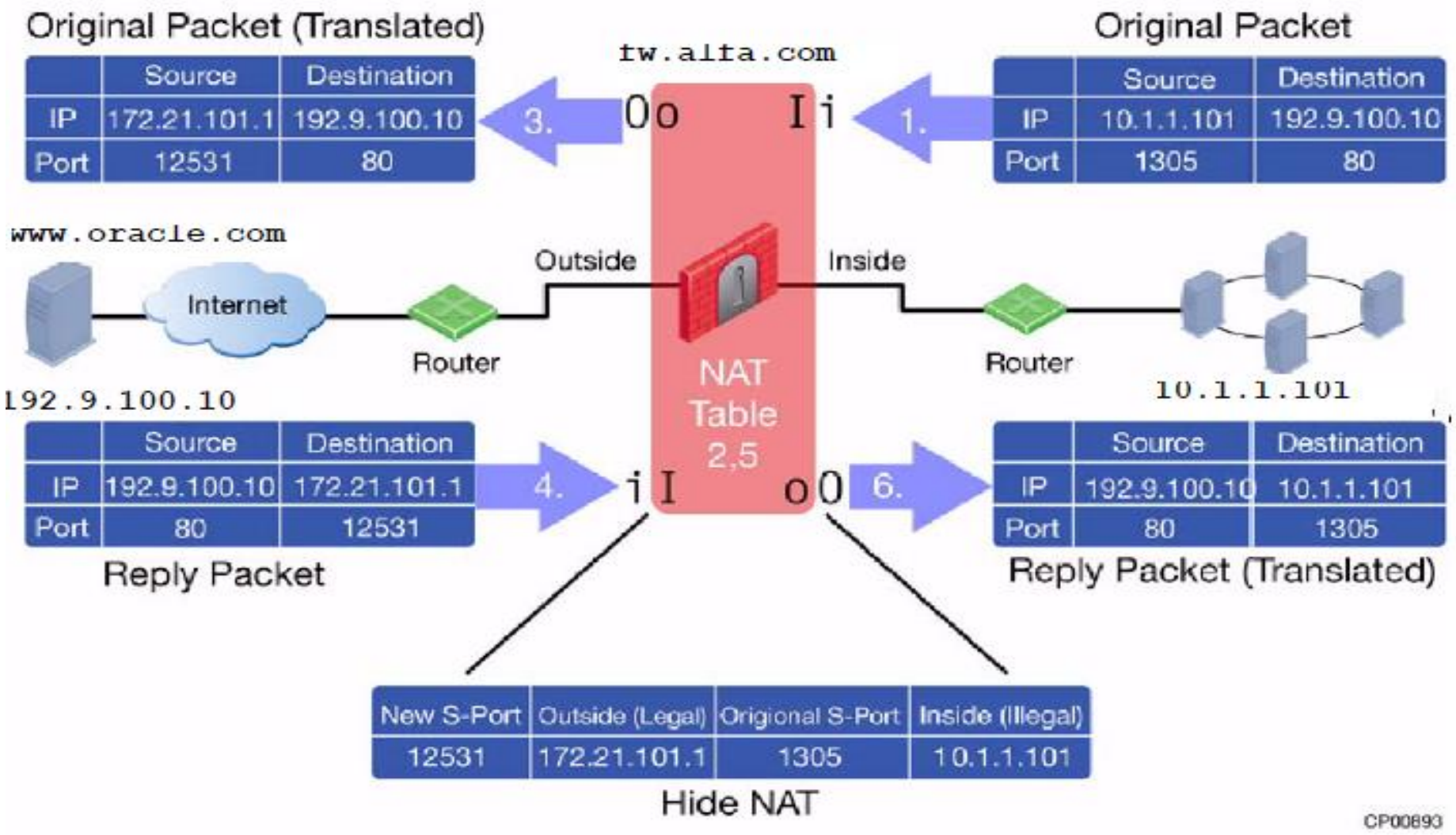
Network Address Translation

- 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

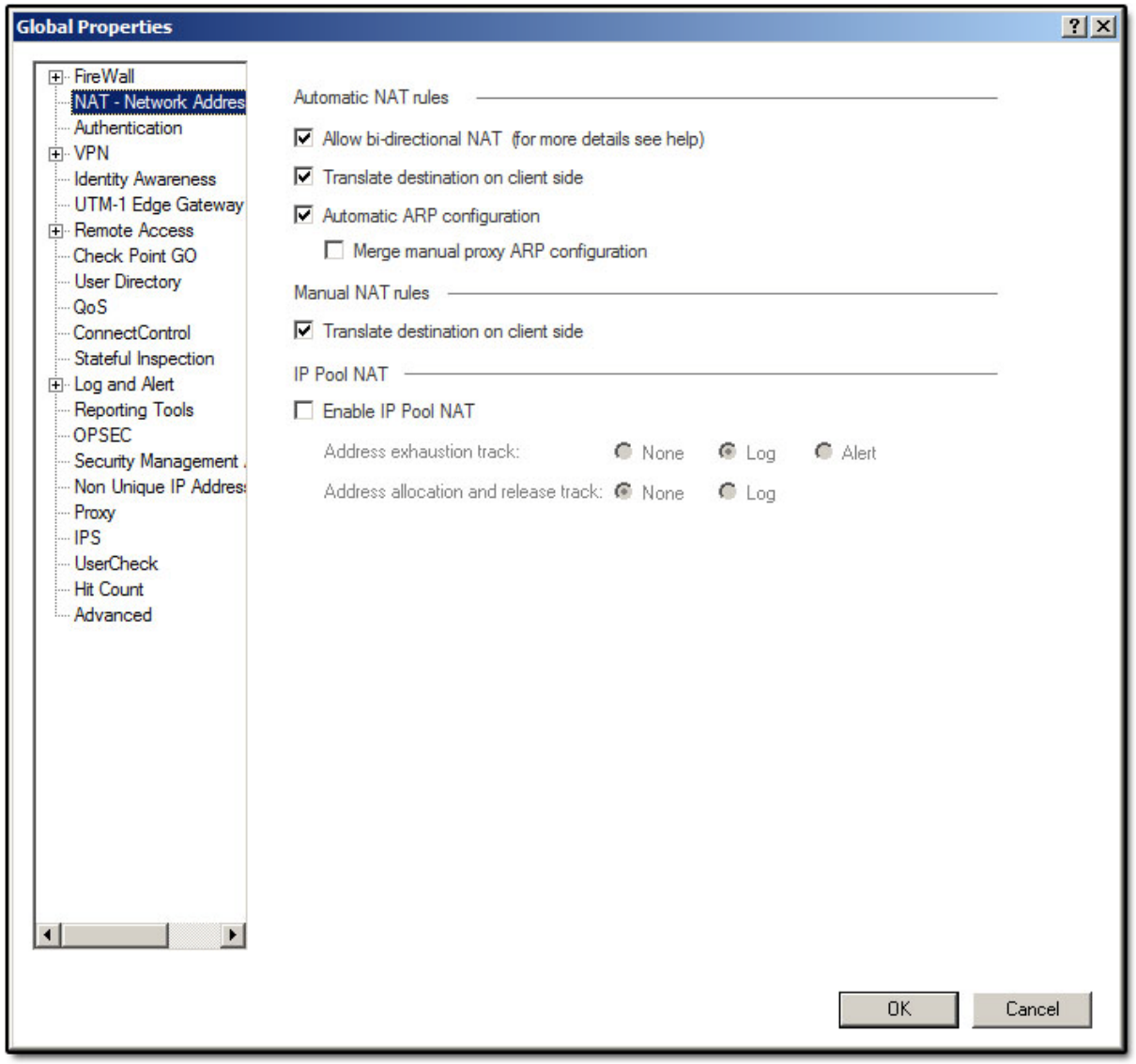
Types of NAT

- 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

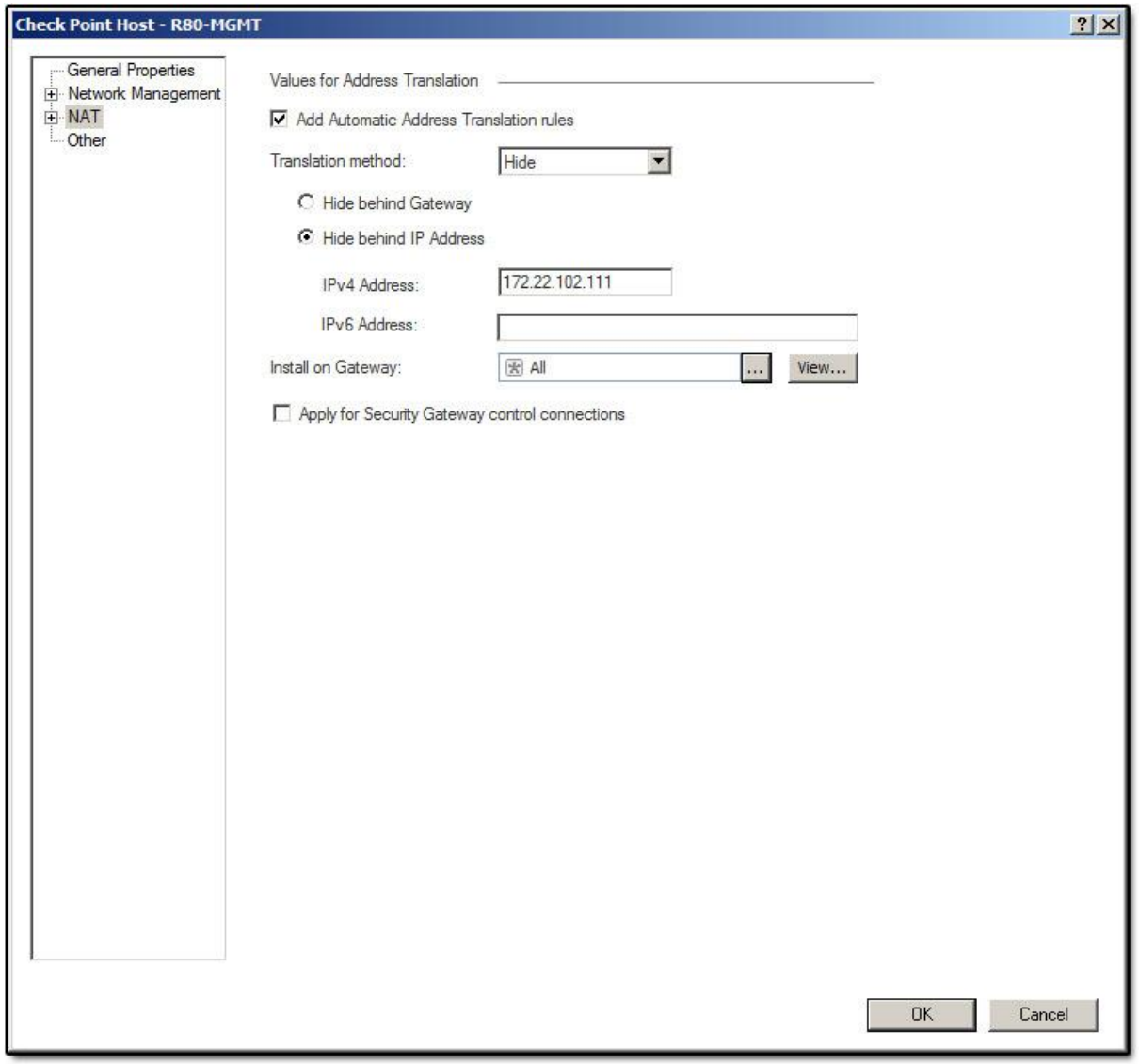
Hide NAT



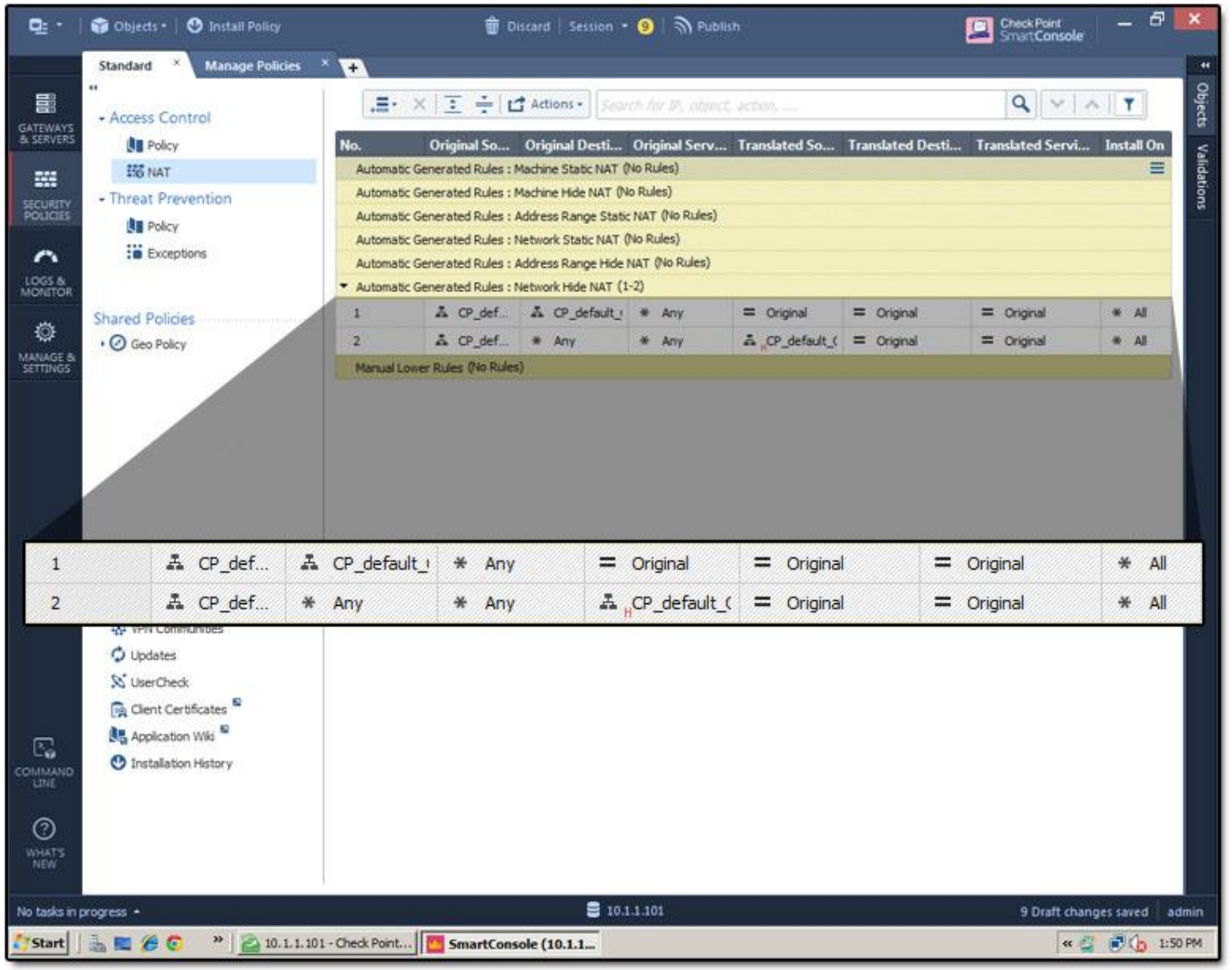
NAT – Global Properties



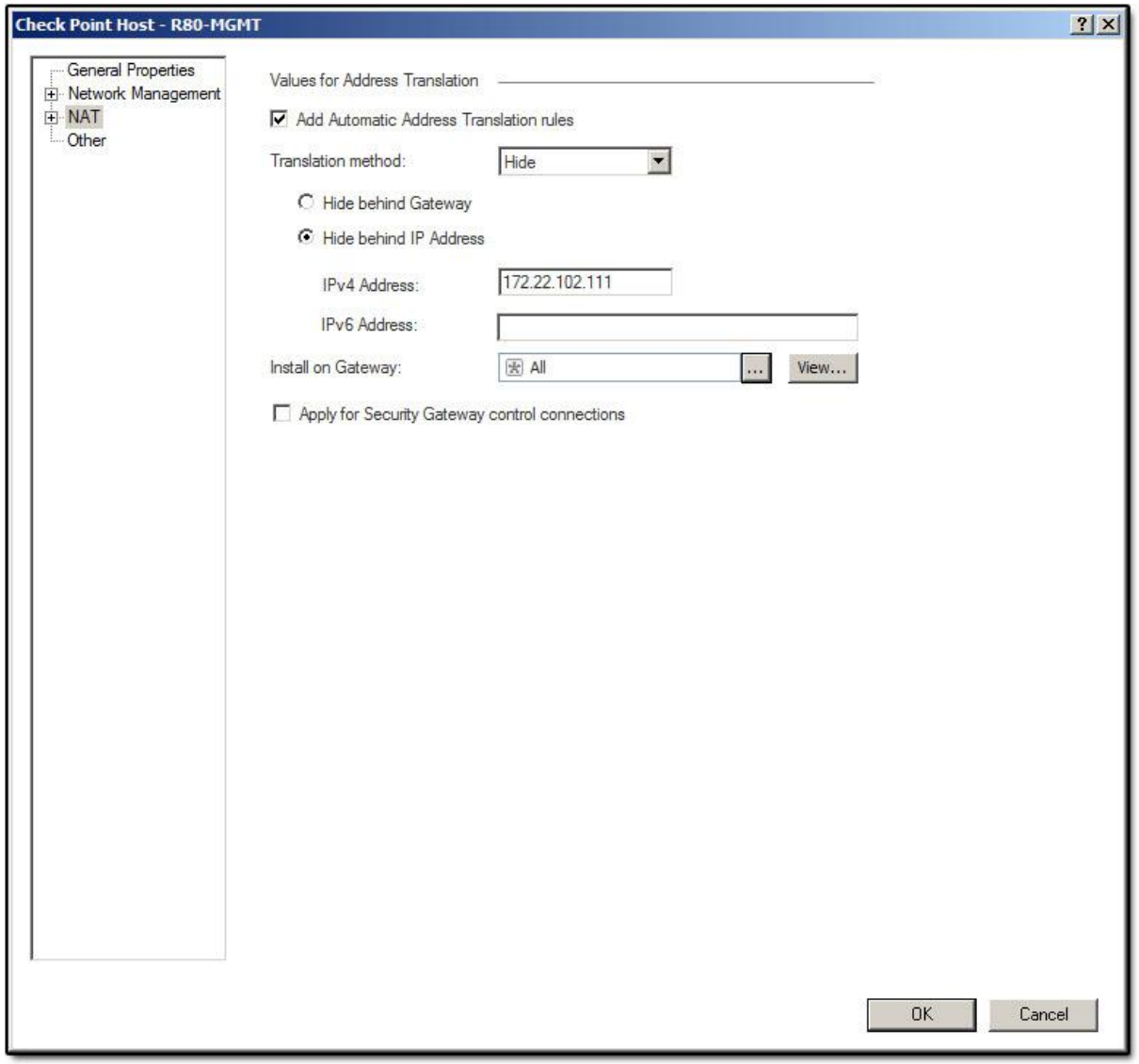
Object Configuration – Hide NAT



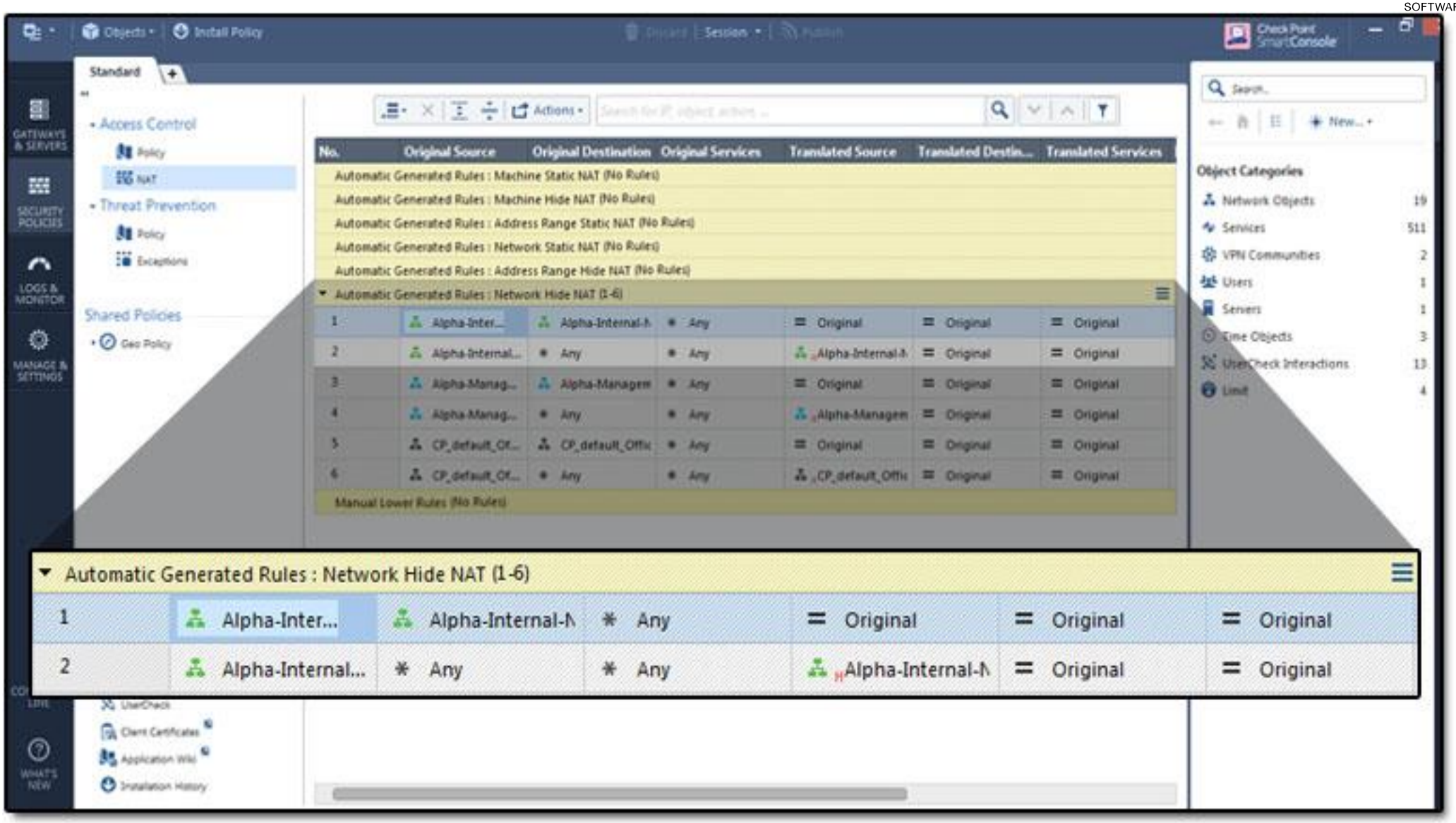
NAT Rules



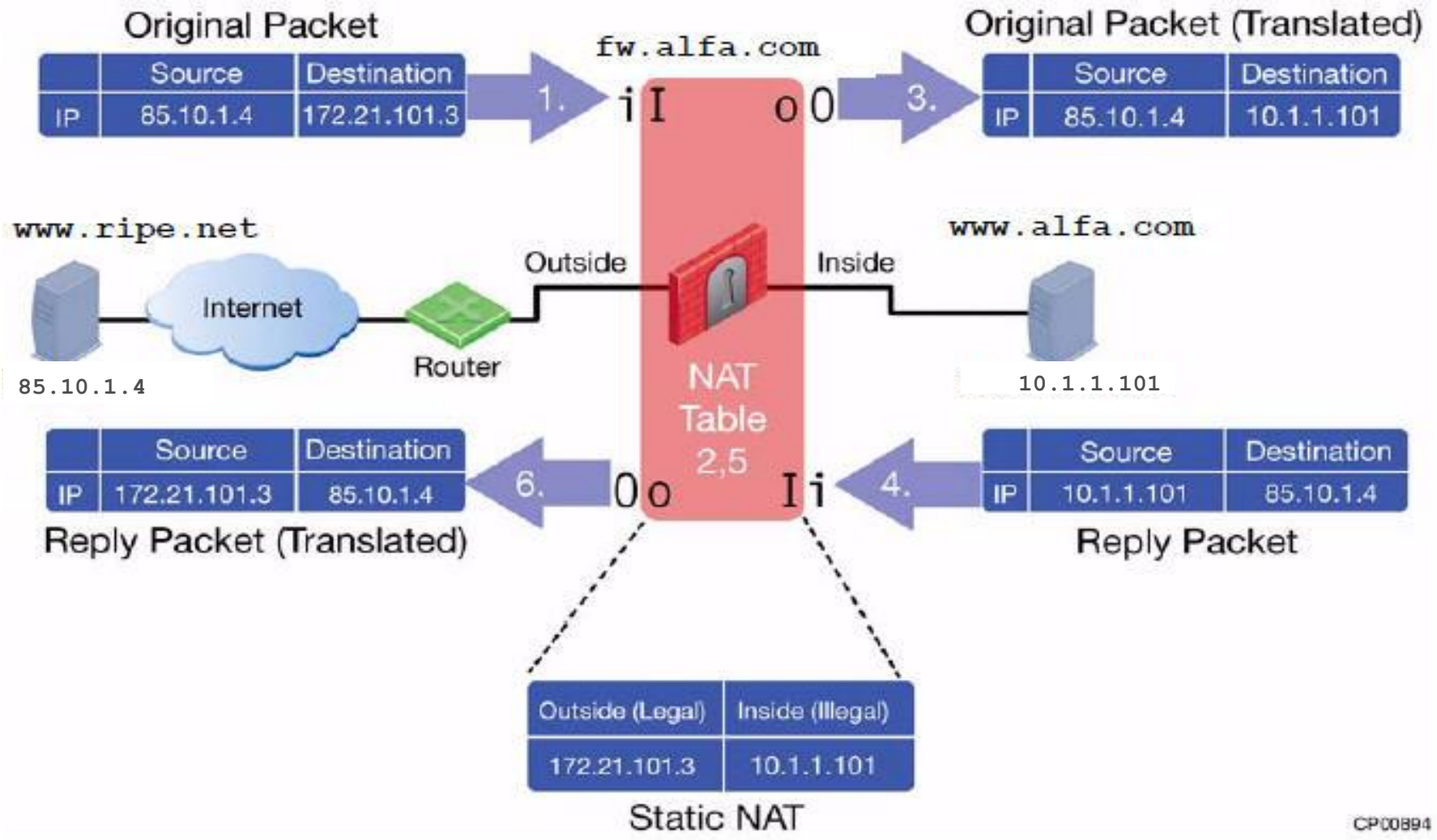
Hide NAT Using Interface IP Address



NAT Rules


Automatic Generated Rules : Network Hide NAT (1-6)
1 Alpha-Inter... Alpha-Internal-N * Any = Original = Original = Original
2 Alpha-Internal... * Any * Any Alpha-Internal-N = Original = Original

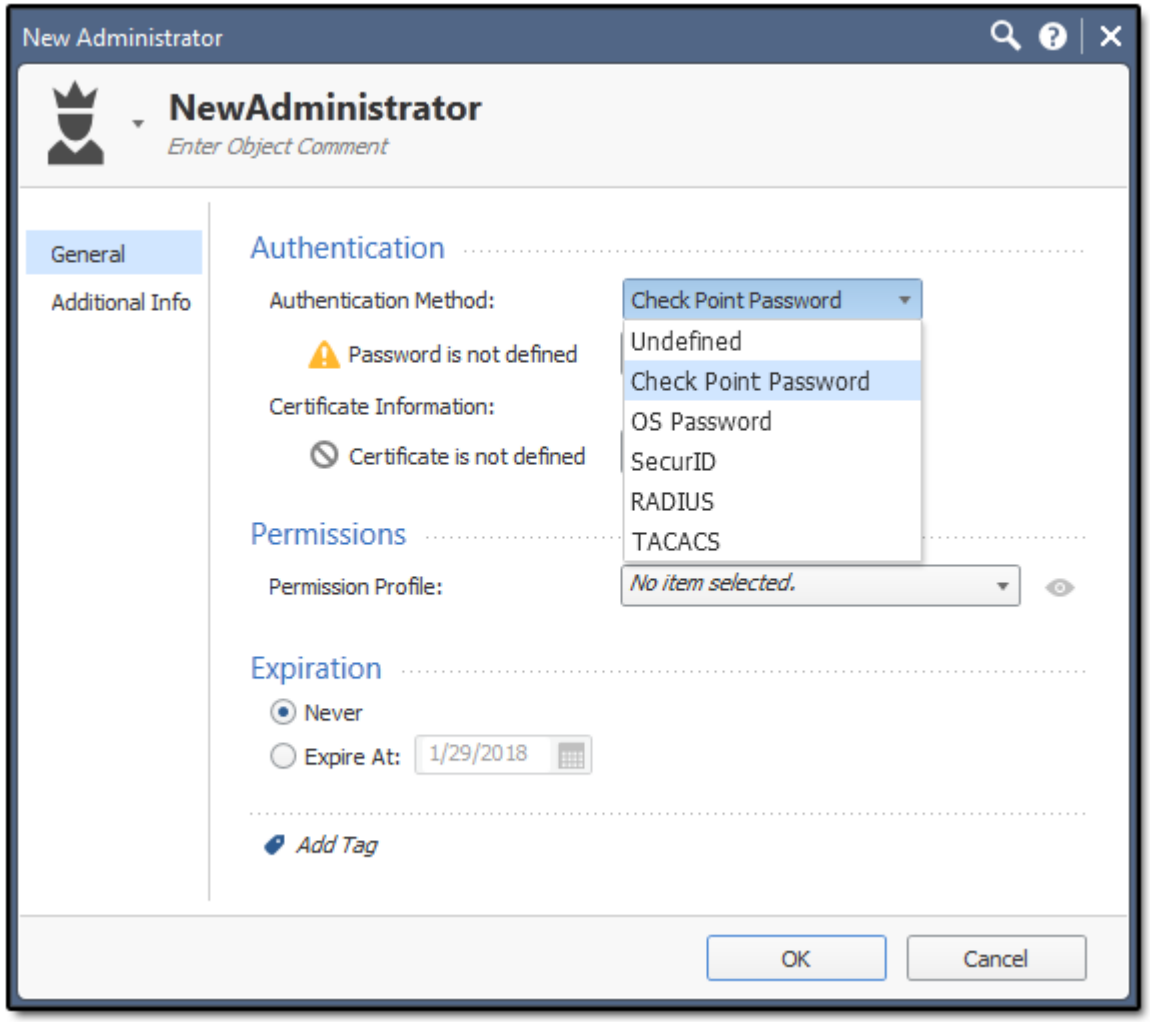
Static NAT



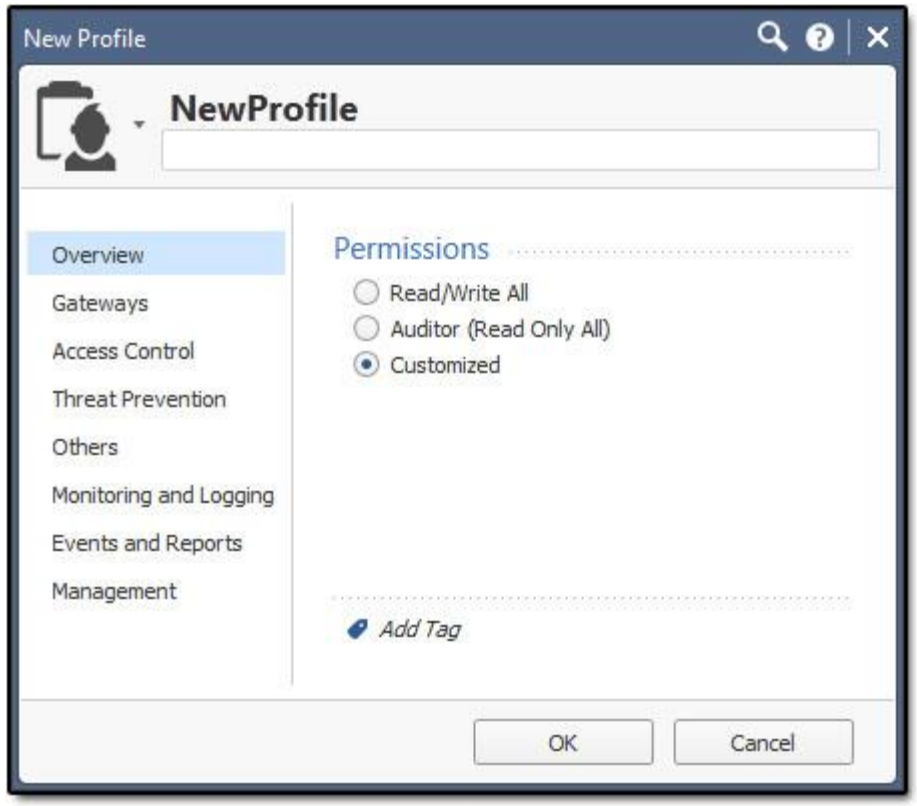
Administration

Authentication Methods:

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

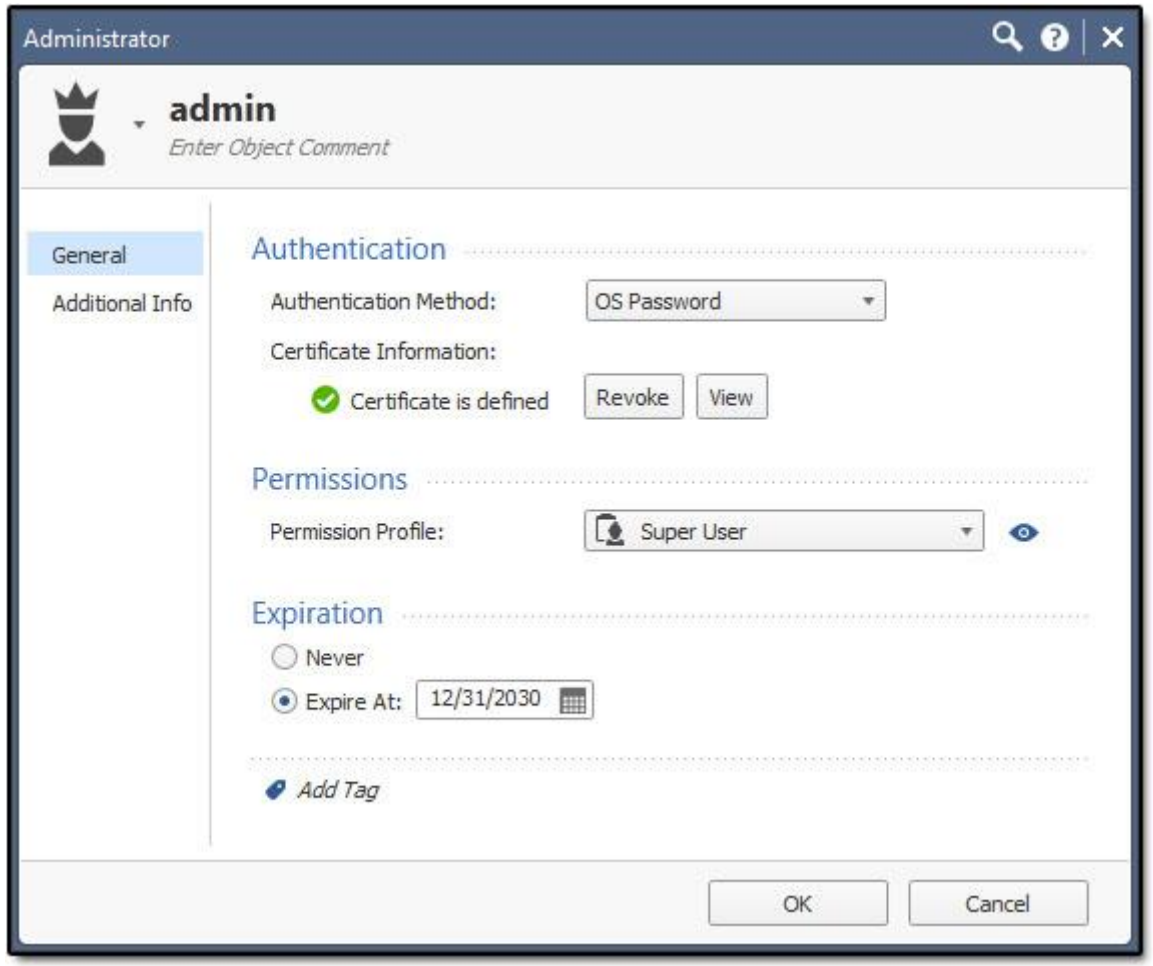


Permission Profiles

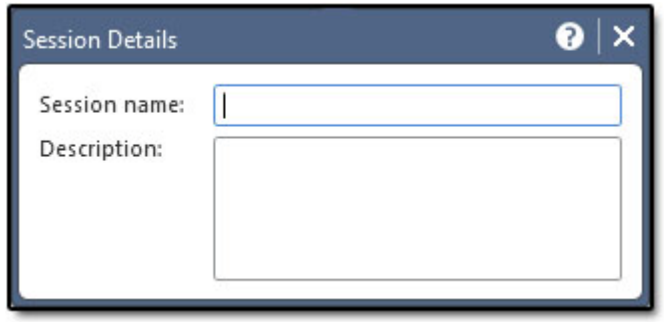


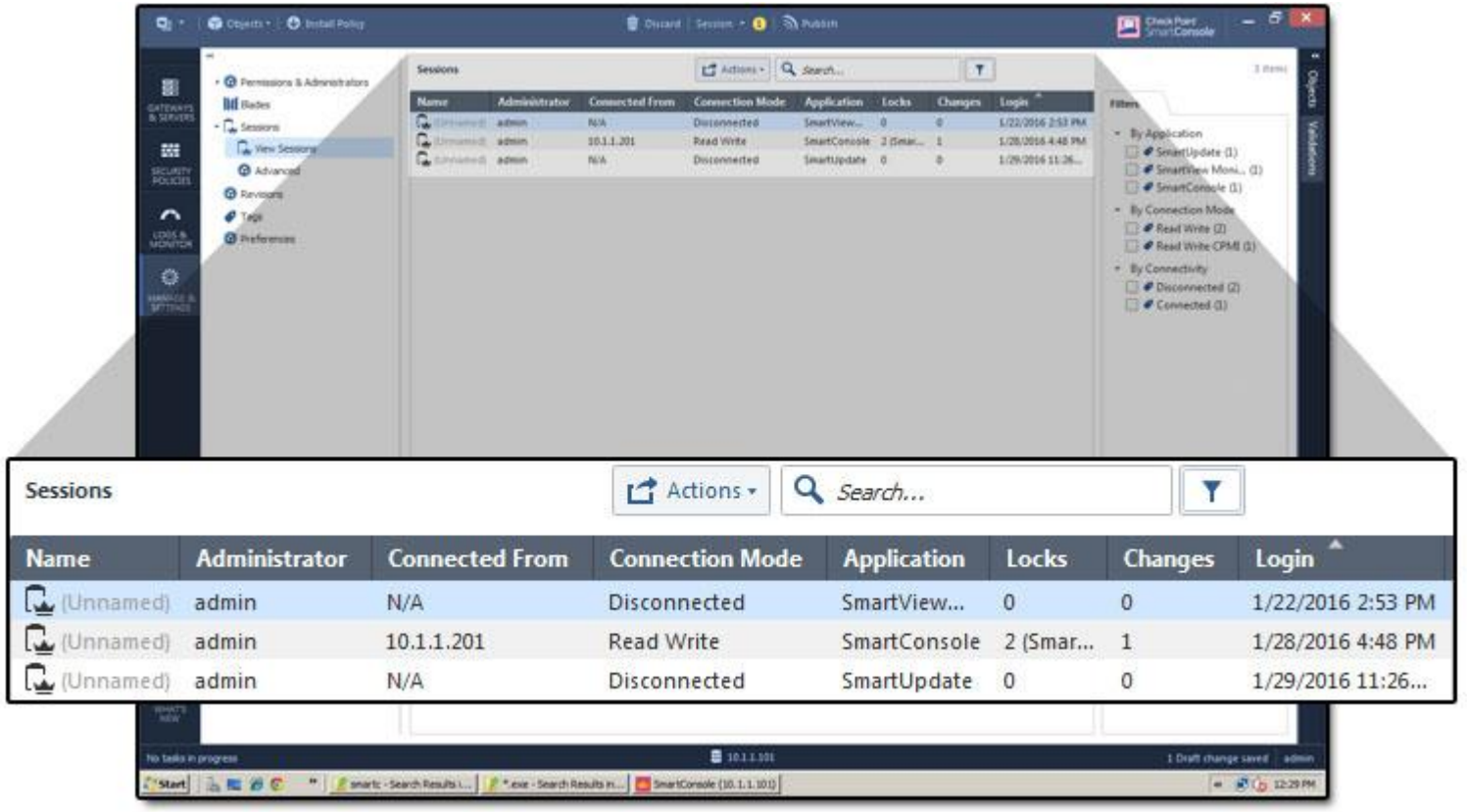
Permission profiles allow for granular control over who can perform certain tasks and may be assigned to multiple administrators.

Revoke a Certificate

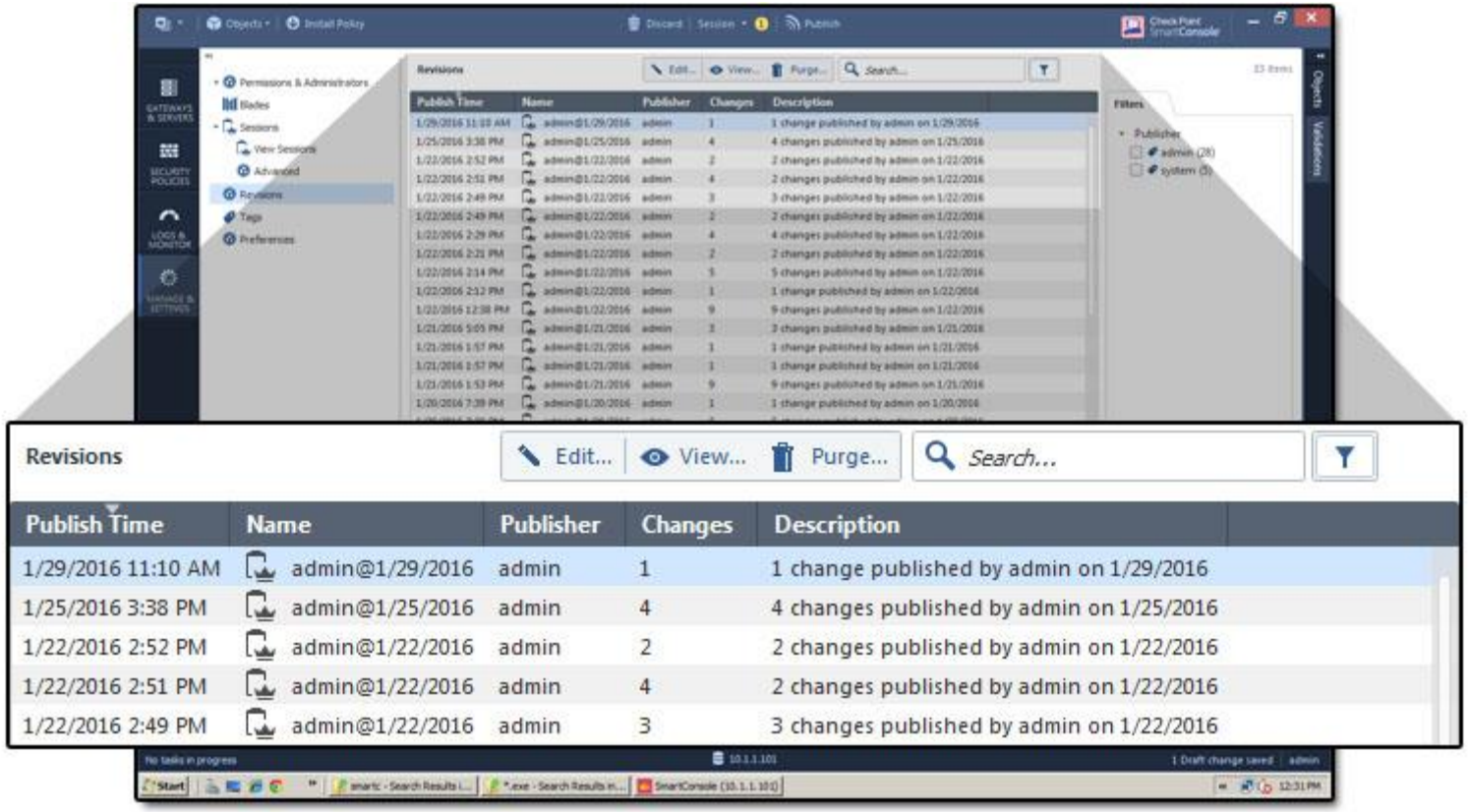


Sessions





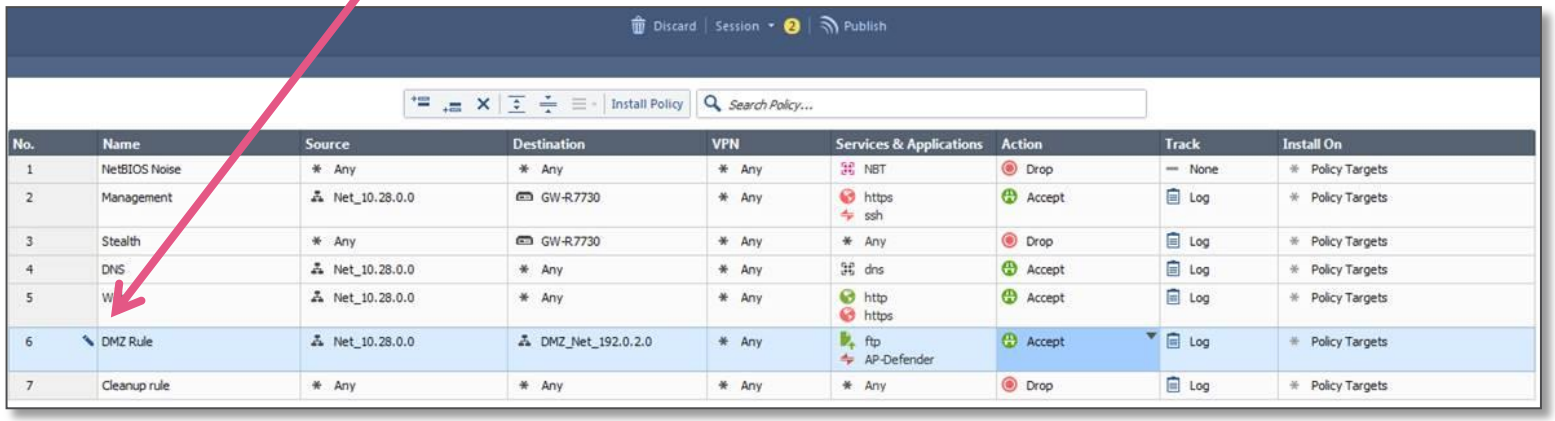
Database Revisions



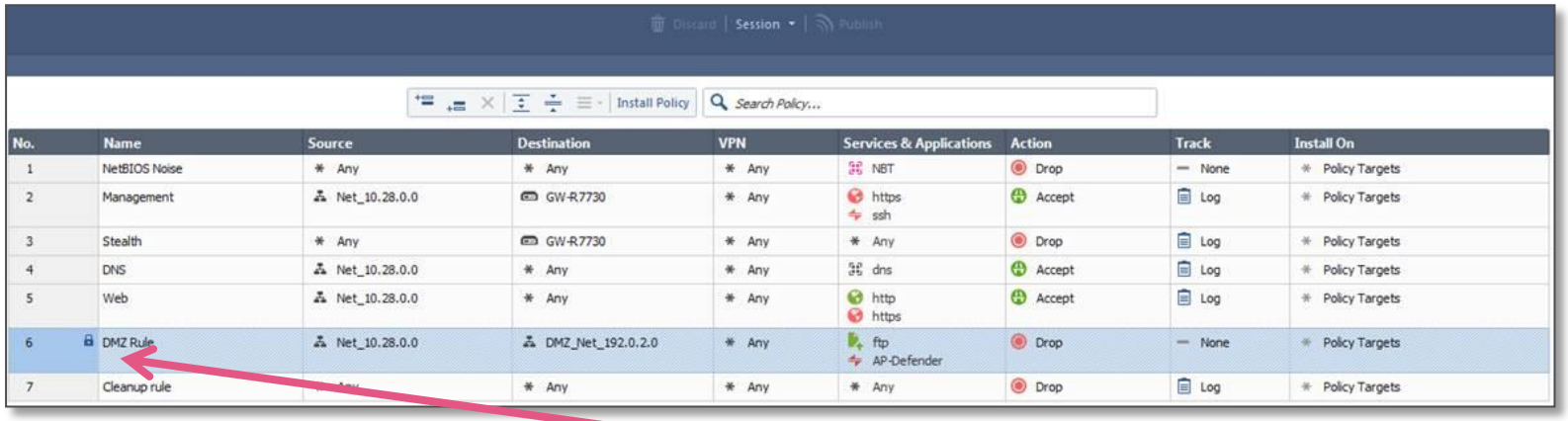
Concurrent Administration

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-R7730	Any	https ssh	Accept	Log	Policy Targets
3	Stealth	Any	GW-R7730	Any	Any	Drop	Log	Policy Targets
4	DNS	Net_10.28.0.0	Any	Any	dns	Accept	Log	Policy Targets
5	W	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-R7730	Any	https ssh	Accept	Log	Policy Targets
3	Stealth	Any	GW-R7730	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

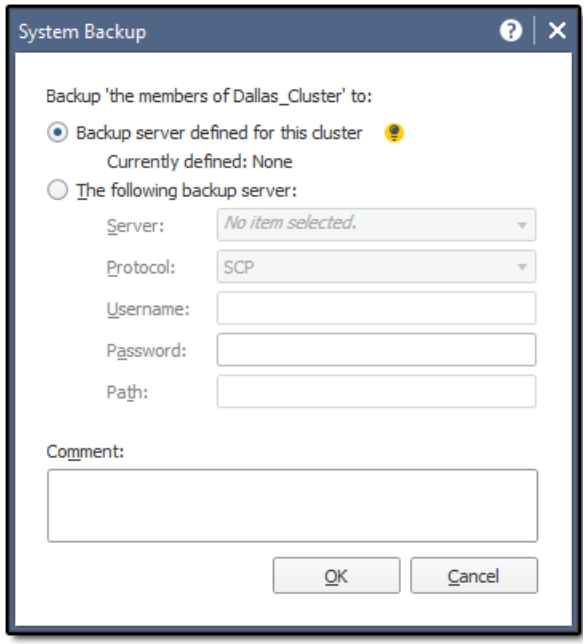
- Snapshot
- System Backup (and System Restore)
- Migrate
- Save Configuration (and Load Configuration)

Backups

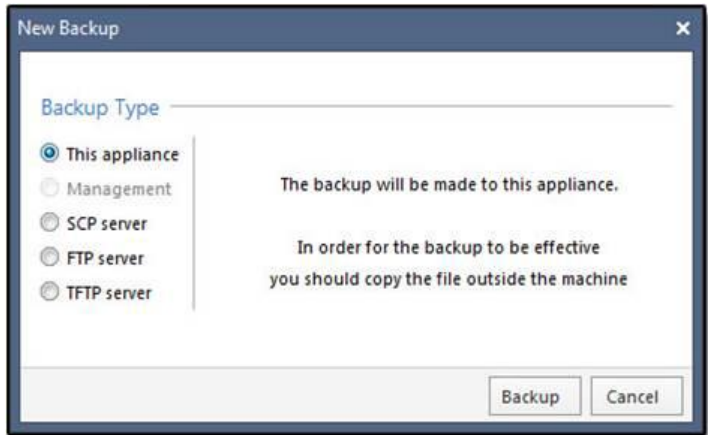
	Snapshot	System Backup	Migrate	Save Configuration
Does it backup Gaia operating system configuration?	Yes	Yes	No	Yes
Does it backup Products configuration?	Yes	Yes	Yes	No
Does it backup Hotfixes?	Yes	No	No	No
Size of output file on Security Gateway	5 - 100 GB	Depends on configuration	Depends on configuration	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

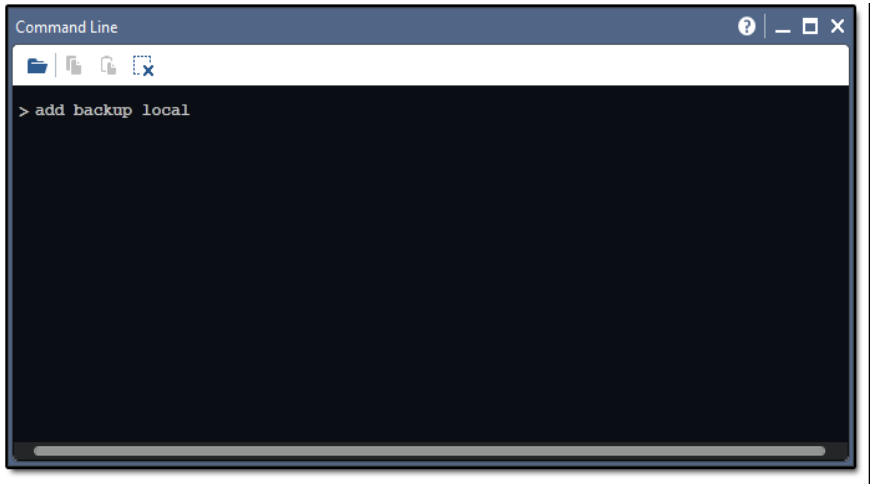
SmartConsole



WebUI



CLI



Check Point
SOFTWARE TECHNOLOGIES LTD

UNIFIED ACCESS POLICY
POLICY LAYERS

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

Check Point
SOFTWARE TECHNOLOGIES LTD

Mapping the business needs into security policies

Business needs:	IT department trying to achieve:
Finance: save costs	Optimizing resources: delegation
Marketing: be visible	Extending the network: cloud
HR: keep data secured	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

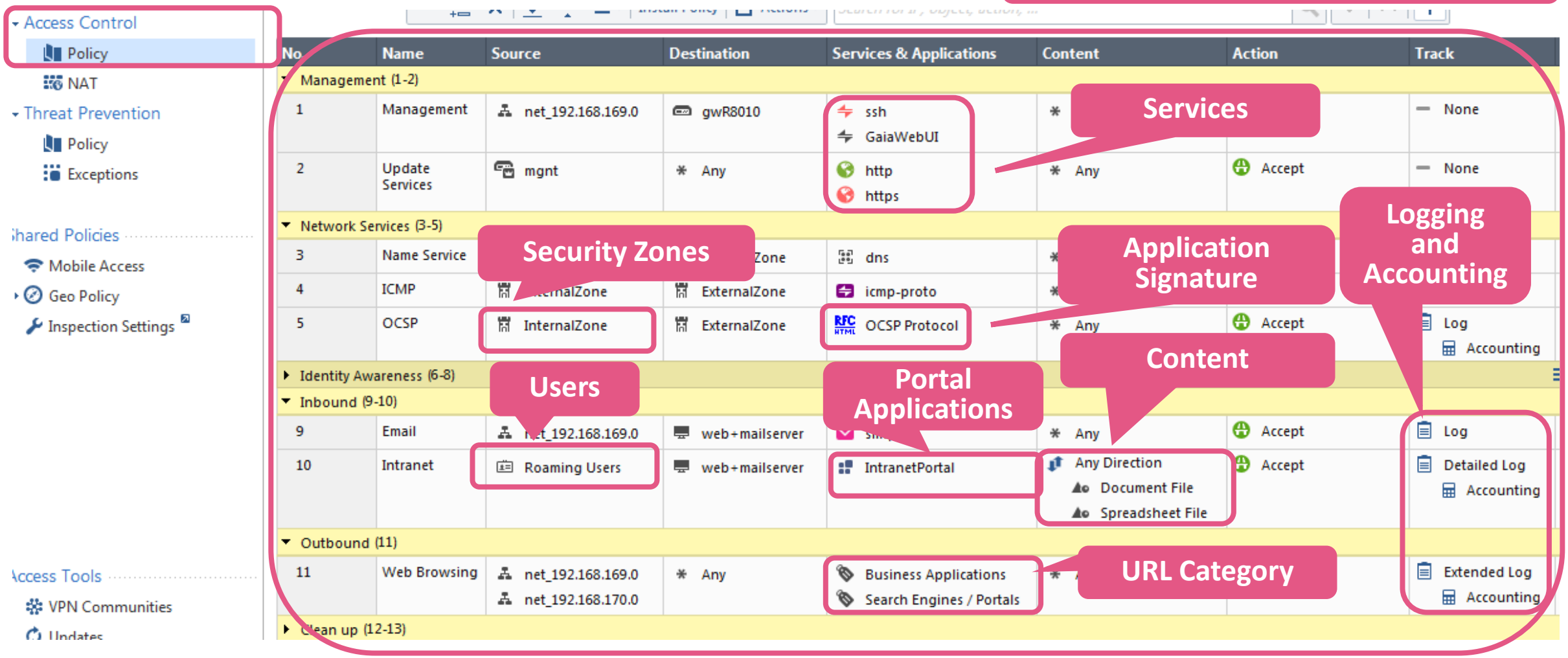
- Create layers and active one or more security functionality (= Check Point Software Blade(s))
- Segment your rule base keeping it manageable
- Multiple administrators can work on the same policy layer at the same time (if allowed by admin role assigned to the layer)

Security Policies Expressing Your Needs

Ordered Layers and Inline Layers

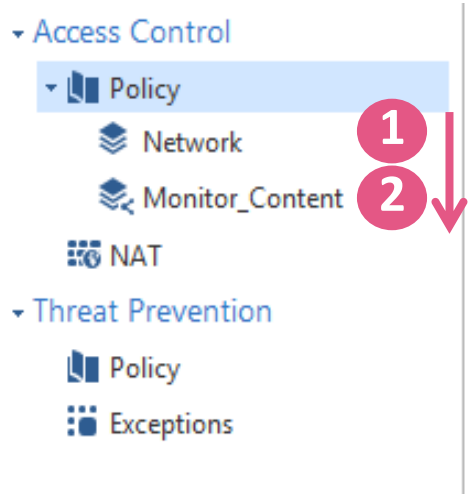
Check Point
SOFTWARE TECHNOLOGIES LTD

Network Access Policy Layer



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	Parrent 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

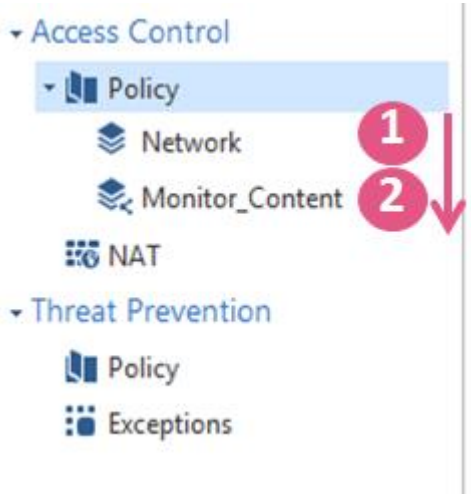
Extract of a larger rule base

Why do I need Ordered and Inline Layers?

Security Policies Expressing Your Needs
Ordered Layers and Inline Layers

The need for Ordered Layers

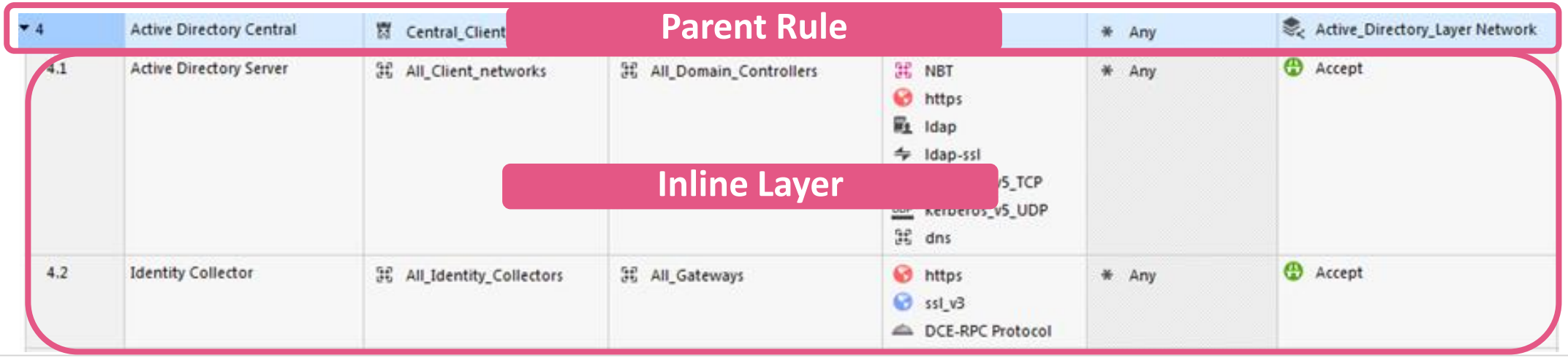
- Managing gateways running R77.30 and earlier
  - When migrating a management server from R77.30 to R80.10 all policies will be represented as Ordered Layered Policies
  - Gateways running R77.30 and earlier support only Ordered Policy layers with just one Blade active on each layer
- Monitoring or 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

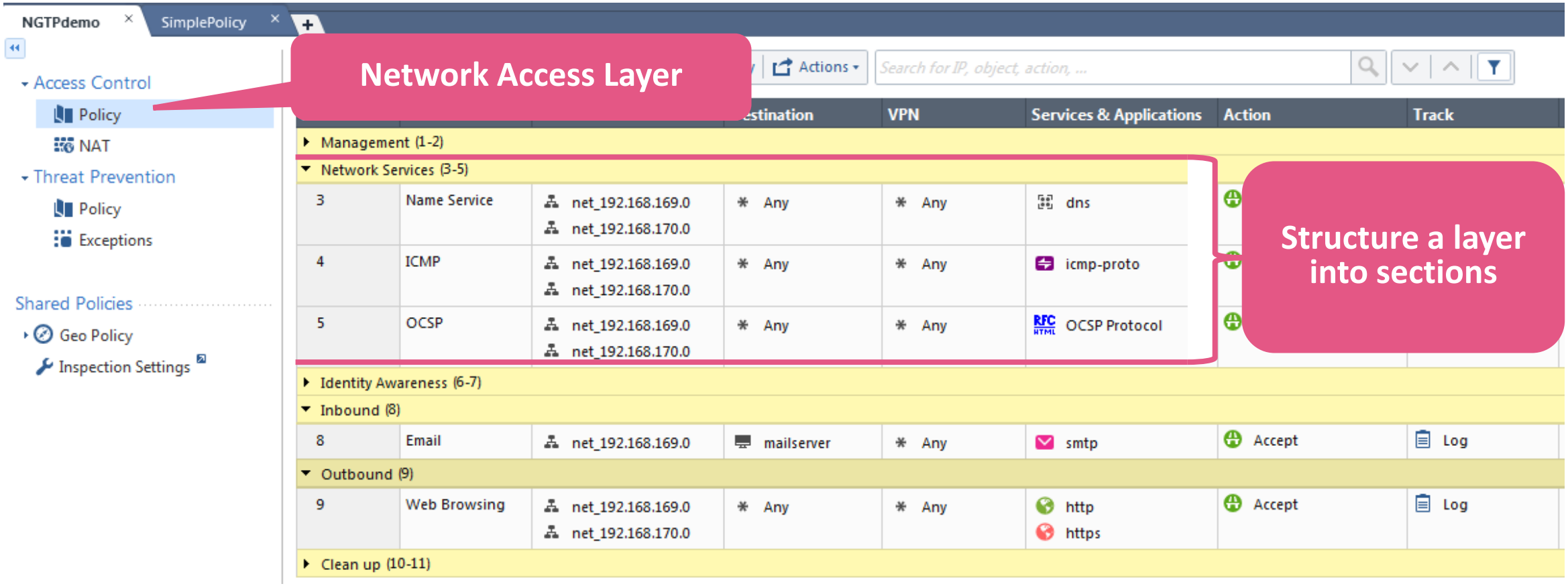
The need for Inline Layers supported by R80.10 Gateways

- 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



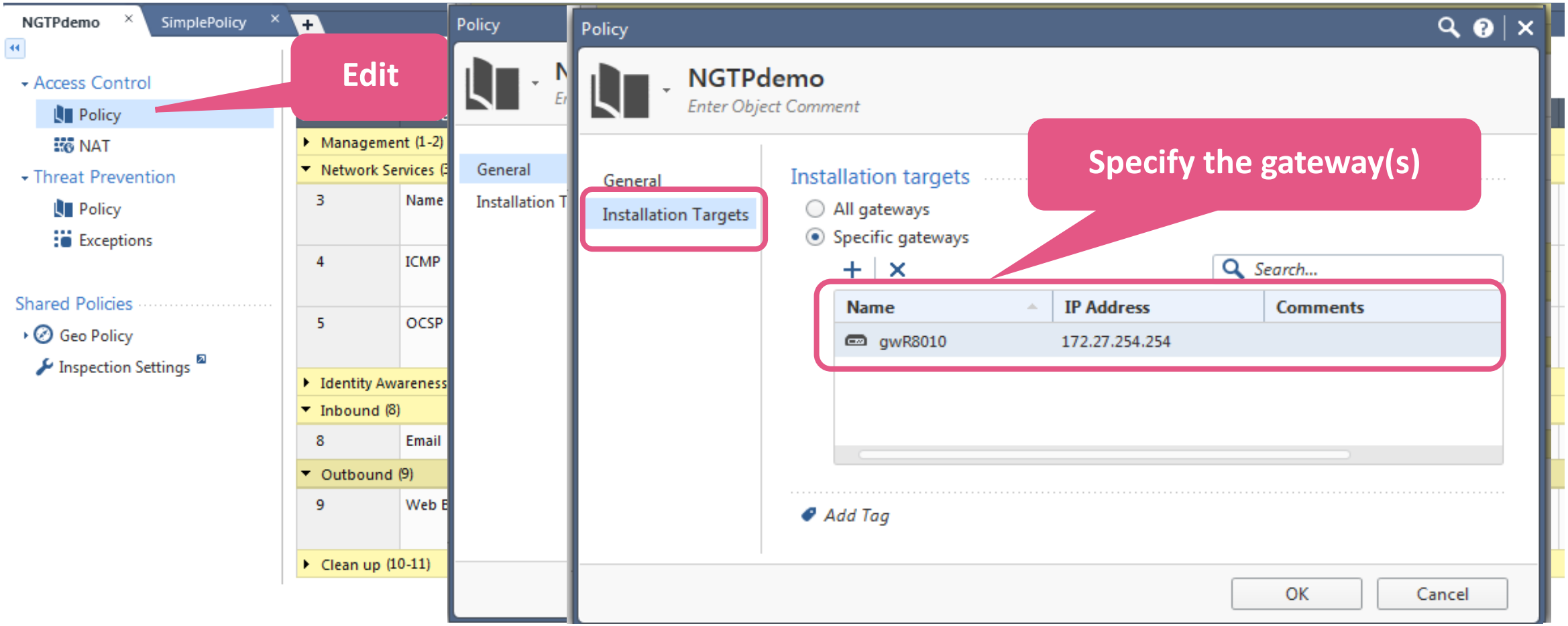
Ordered Layers

Use section titles structuring the policy



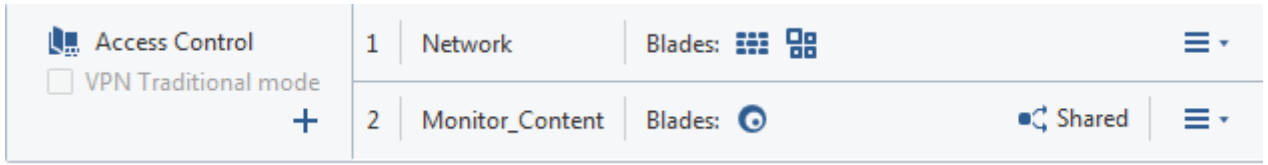
Ordered Layers

Software Blades and installation targets

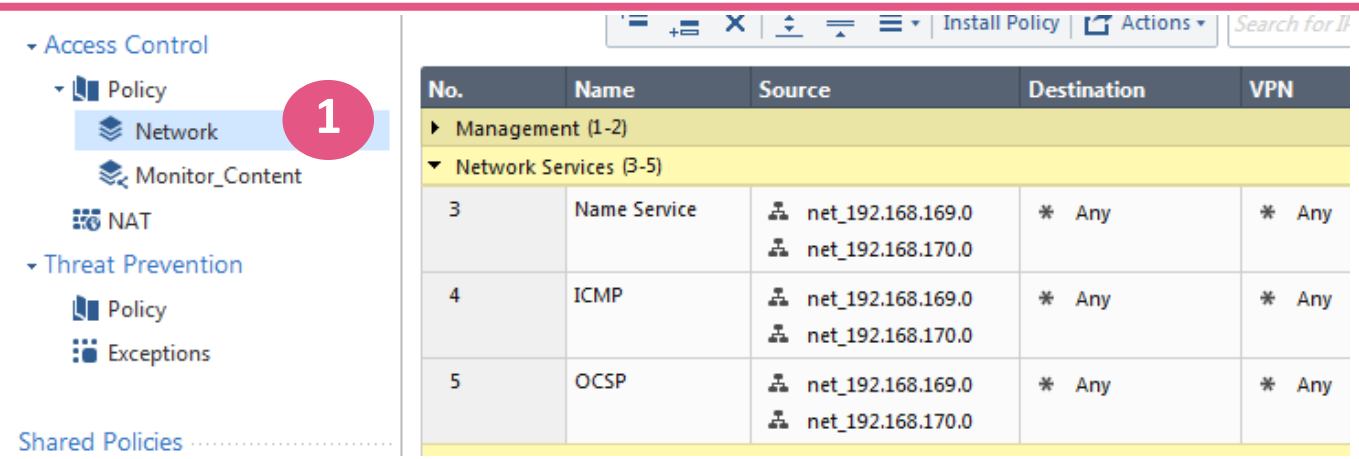


Ordered Layers
Summary

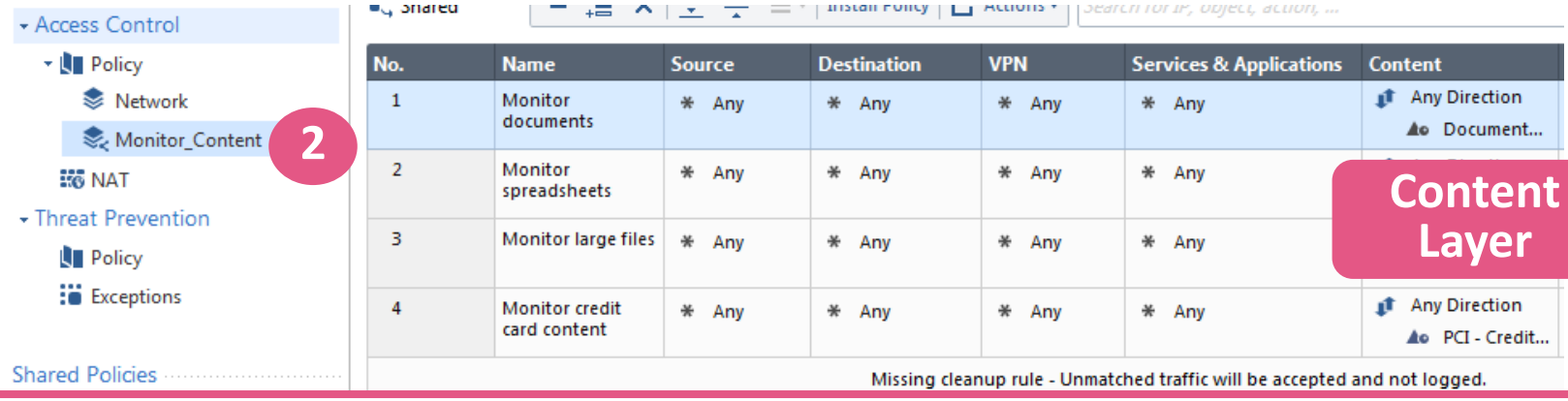
- You achieve an Access Control policy containing **Multiple Ordered Layers**
- Each layer performs one or more specific security actions
- The layers will be matched top-down



Ordered Layers

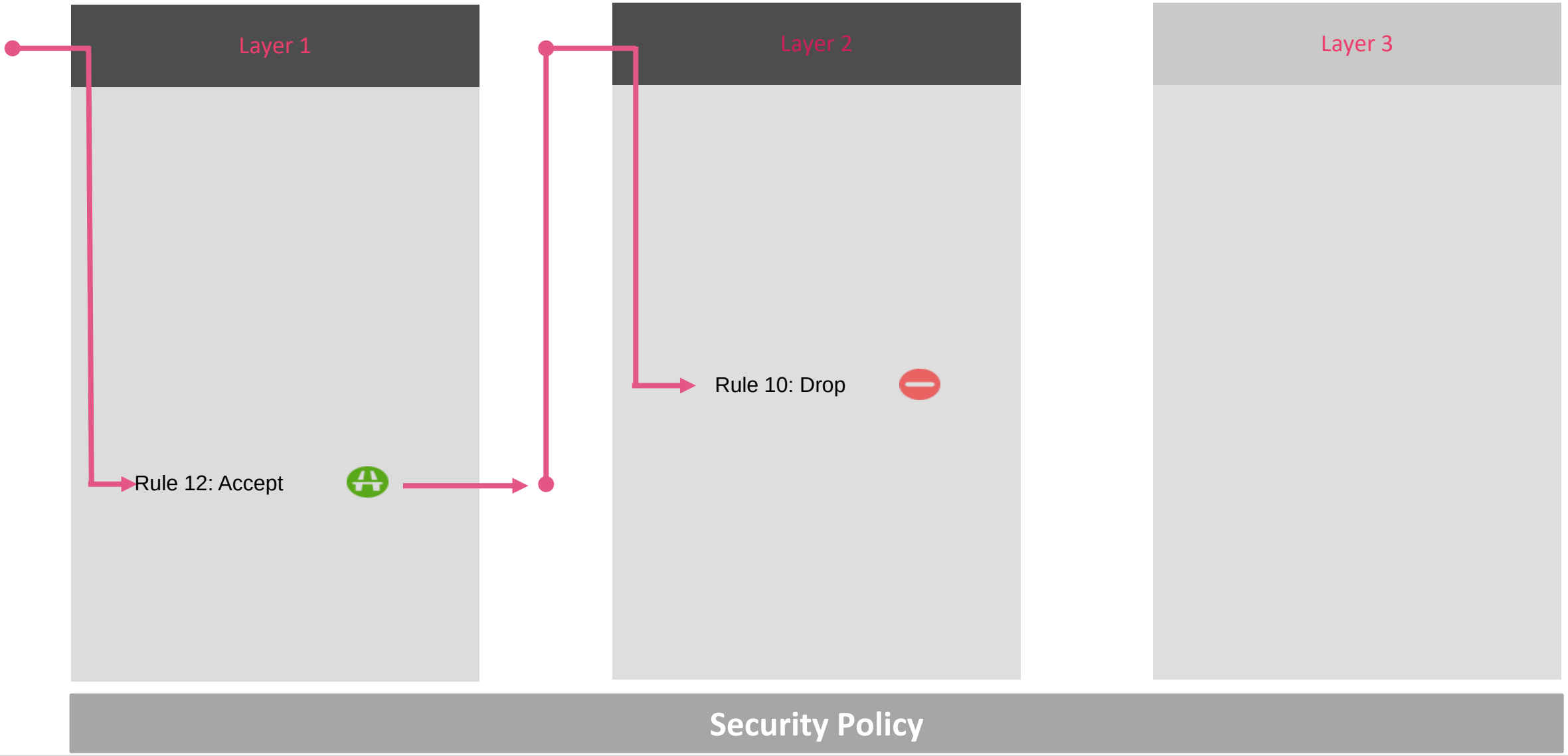


Network Layer



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

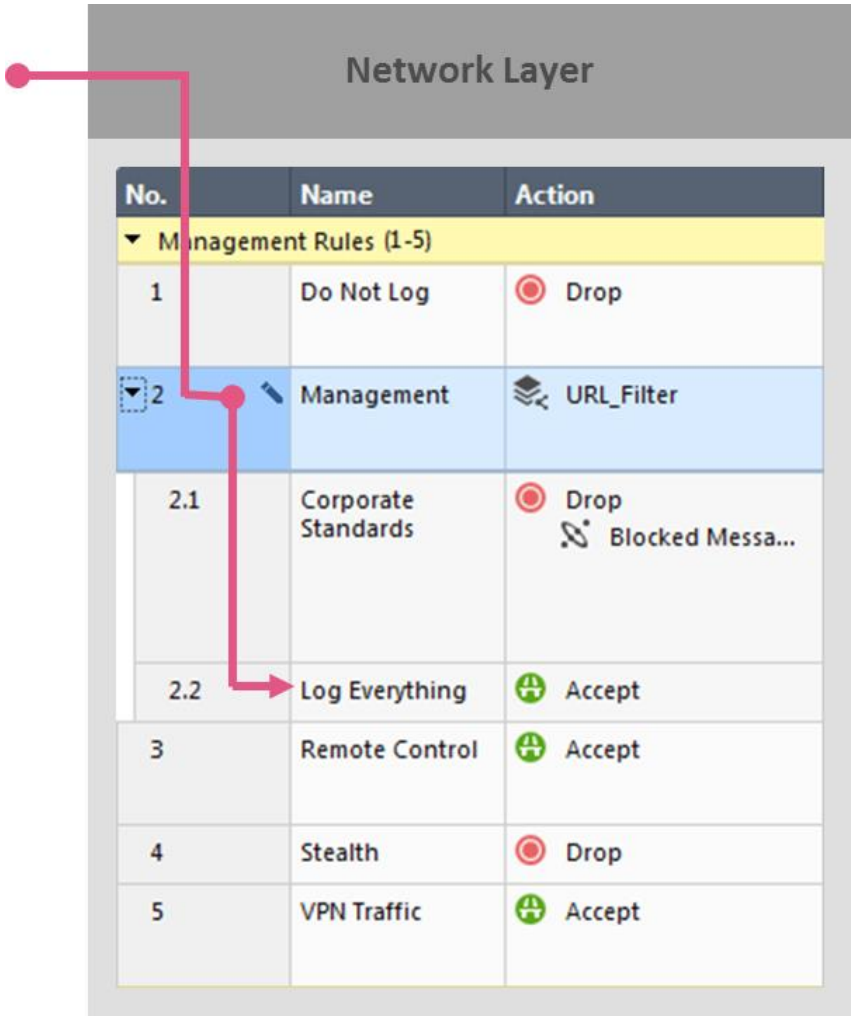
No.	Name	Source	Destination	Services & Applications	Content	Action	
				https			
3	DNS	net_192.168.169.0 net_192.168.170.0	Any	dns	Any	Accept	
4	Active Directory Central	Central_Client_Zone	Central_Services_Zone	Any	Any	Active_Directory_Layer Networ	
4.1	Active Directory Server	All_Client_networks	All_Domain_Controllers	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	None
5	Active Directory Backup Site	Backup_Site_Zone	Backup_Site_Services_Zone	Any	Any	Active_Directory_Layer Network	N/A
6	SMTP	net_192.168.169.0	web+mailserver	smtp	Any	Accept	Log
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

Ordered Layer

Example:
Active Directory related rules

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

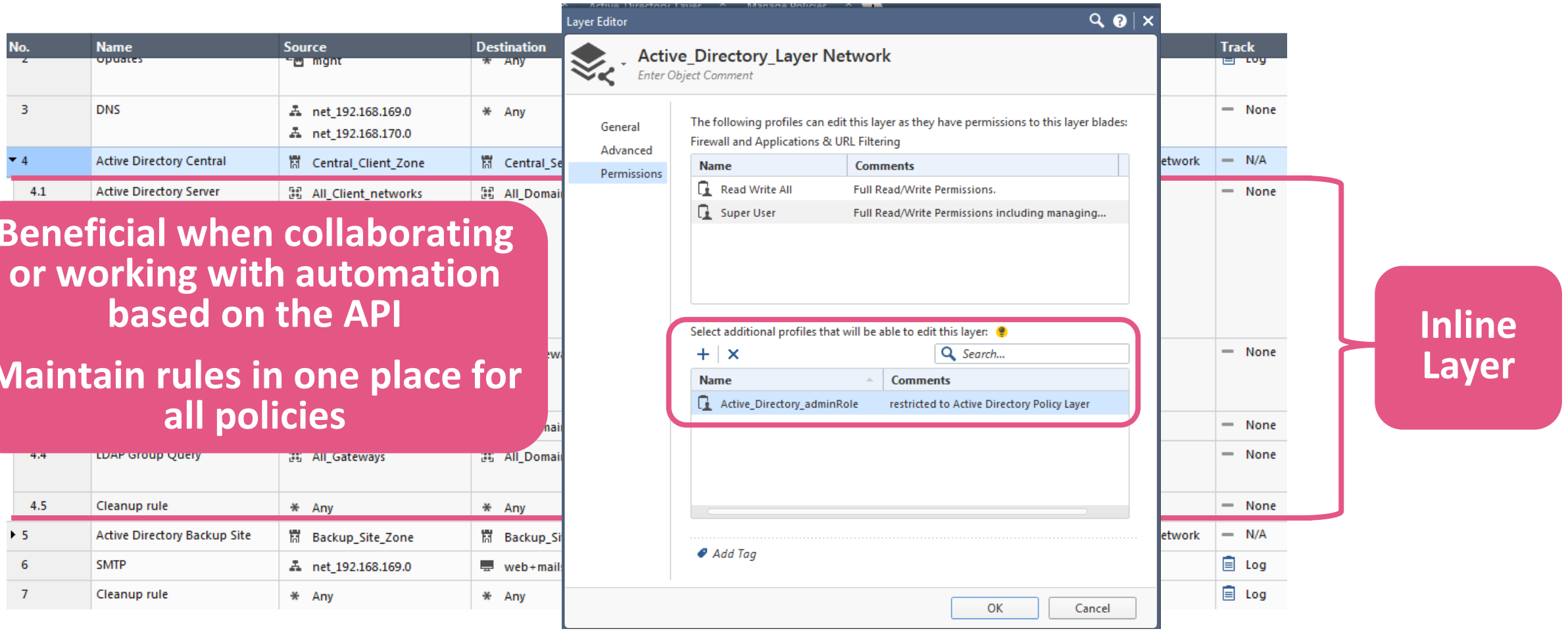
Traffic Flow Through an Inline Layer



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



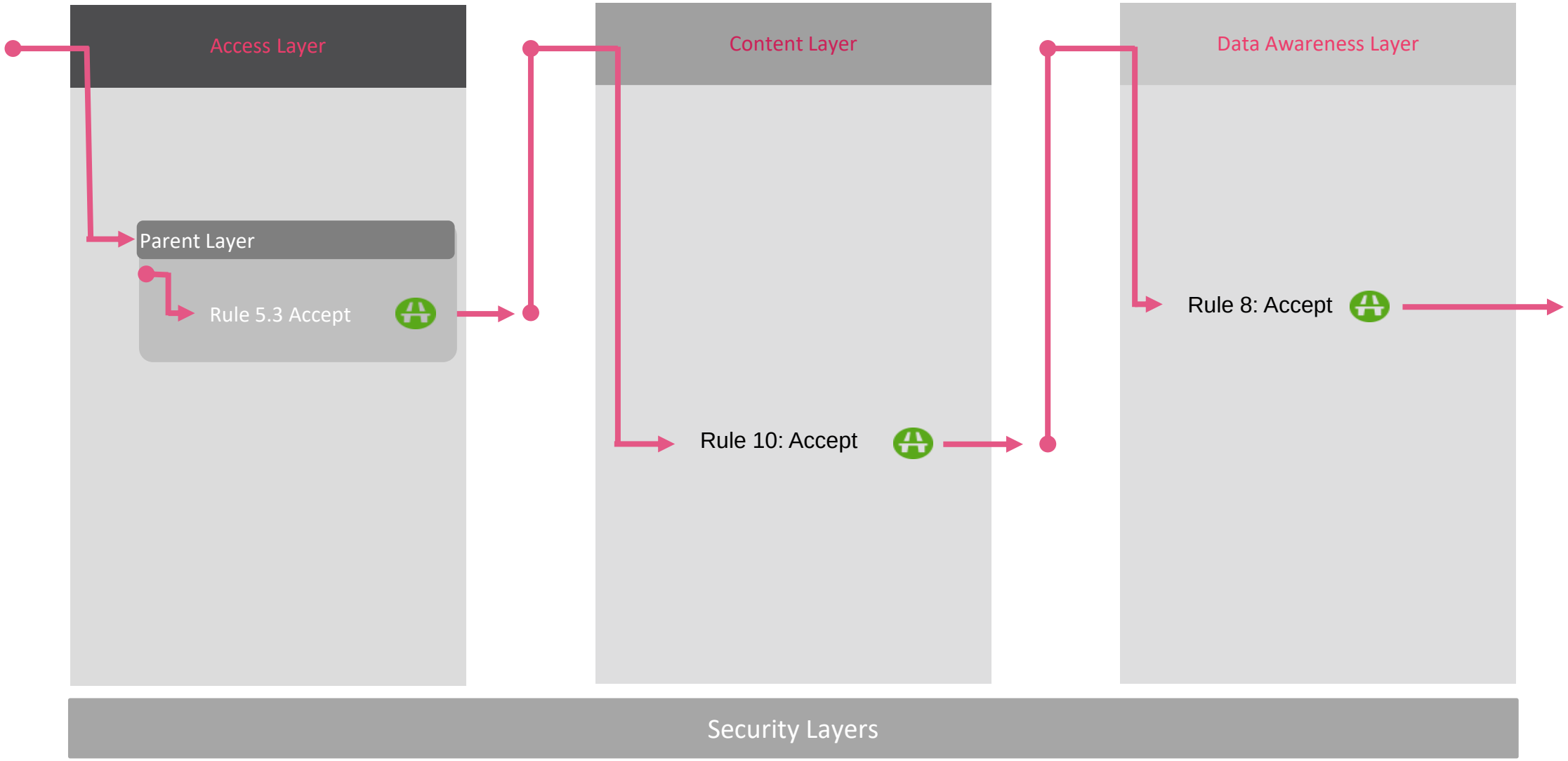
Ordered Layers And Inline Layers
Supported Policy Targets

- **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)							

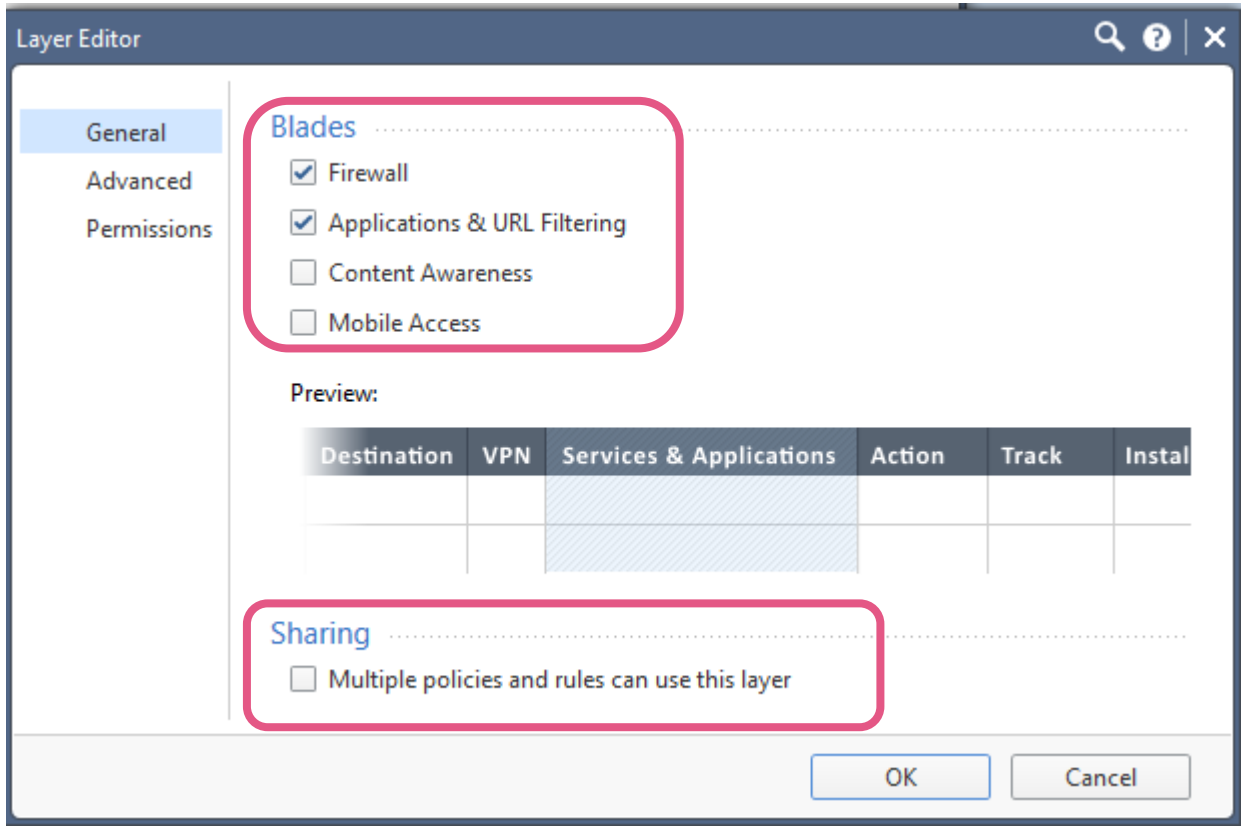
Example of an Ordered Layer Policy with APCL, URLF and Content Awareness Blades active

Traffic Inspection for Ordered Layers And Inline Layers



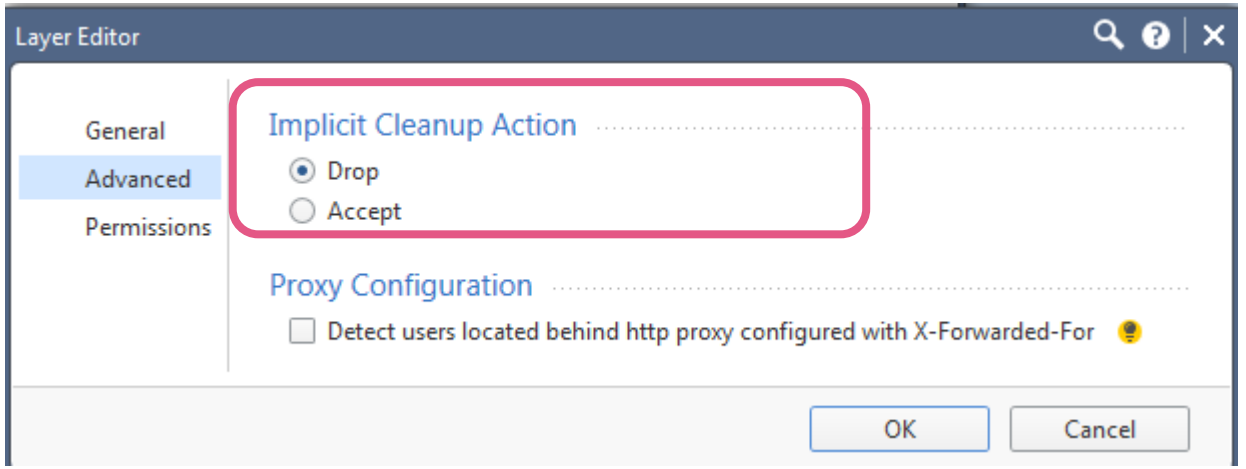
Security Policies Expressing Your Needs
Layer Options

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



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

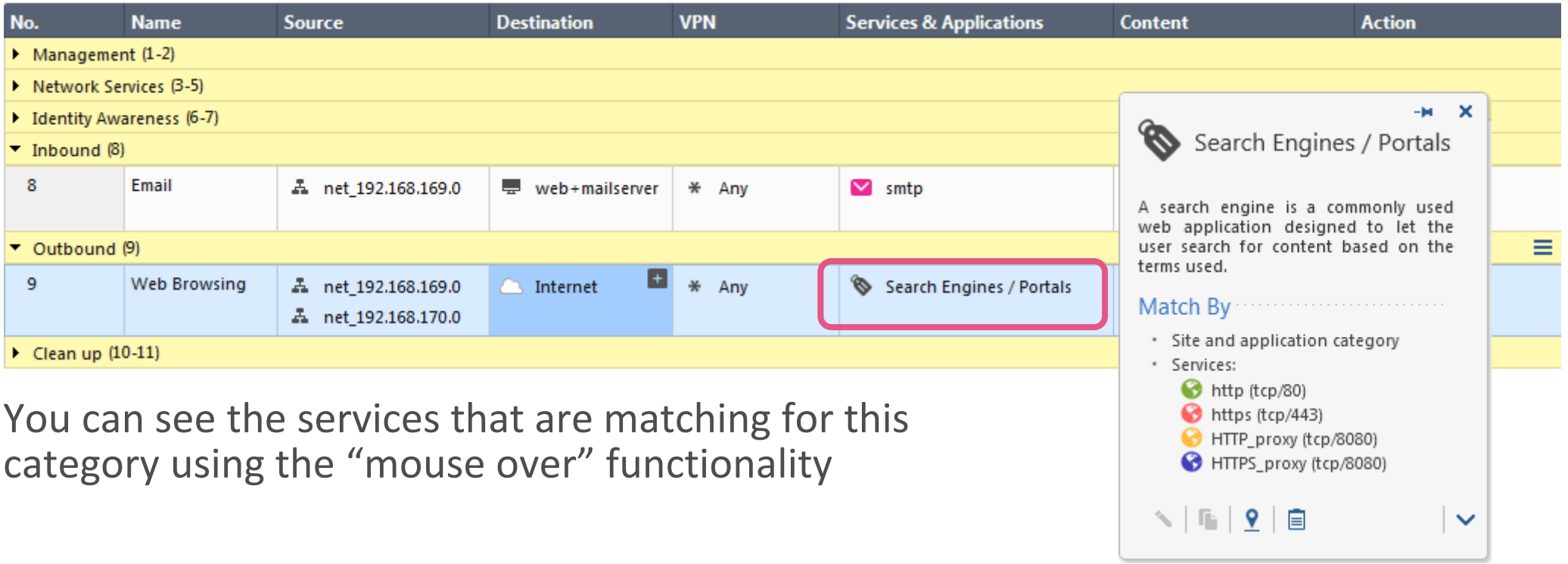


MATCHING OF APPLICATION, URLF CATEGORIES AND CONTENT OBJECTS

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

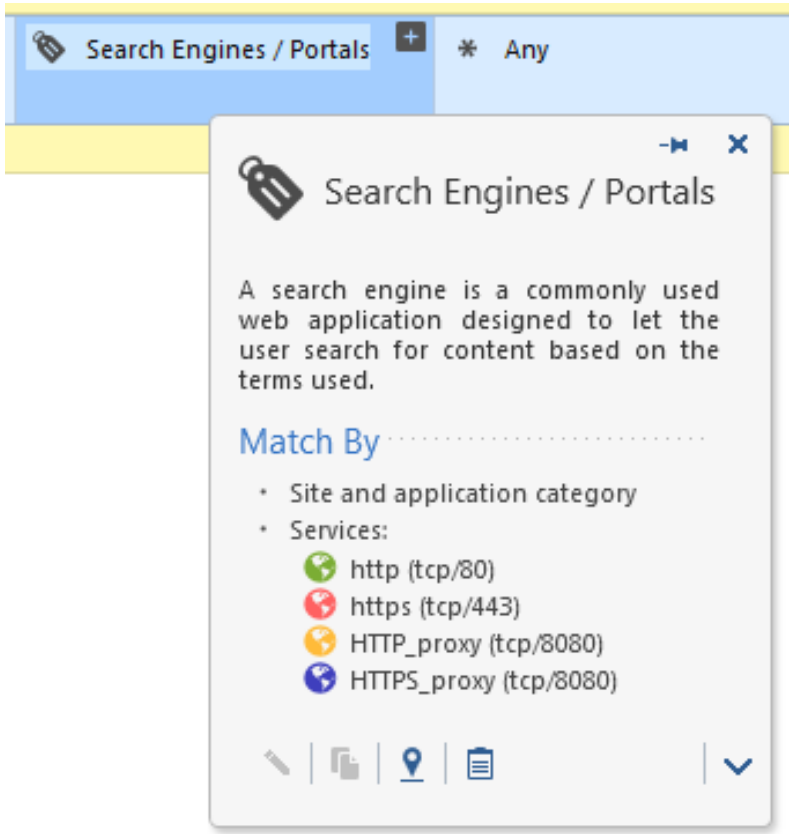


- You can see the services that are matching for this category using the “mouse over” functionality

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

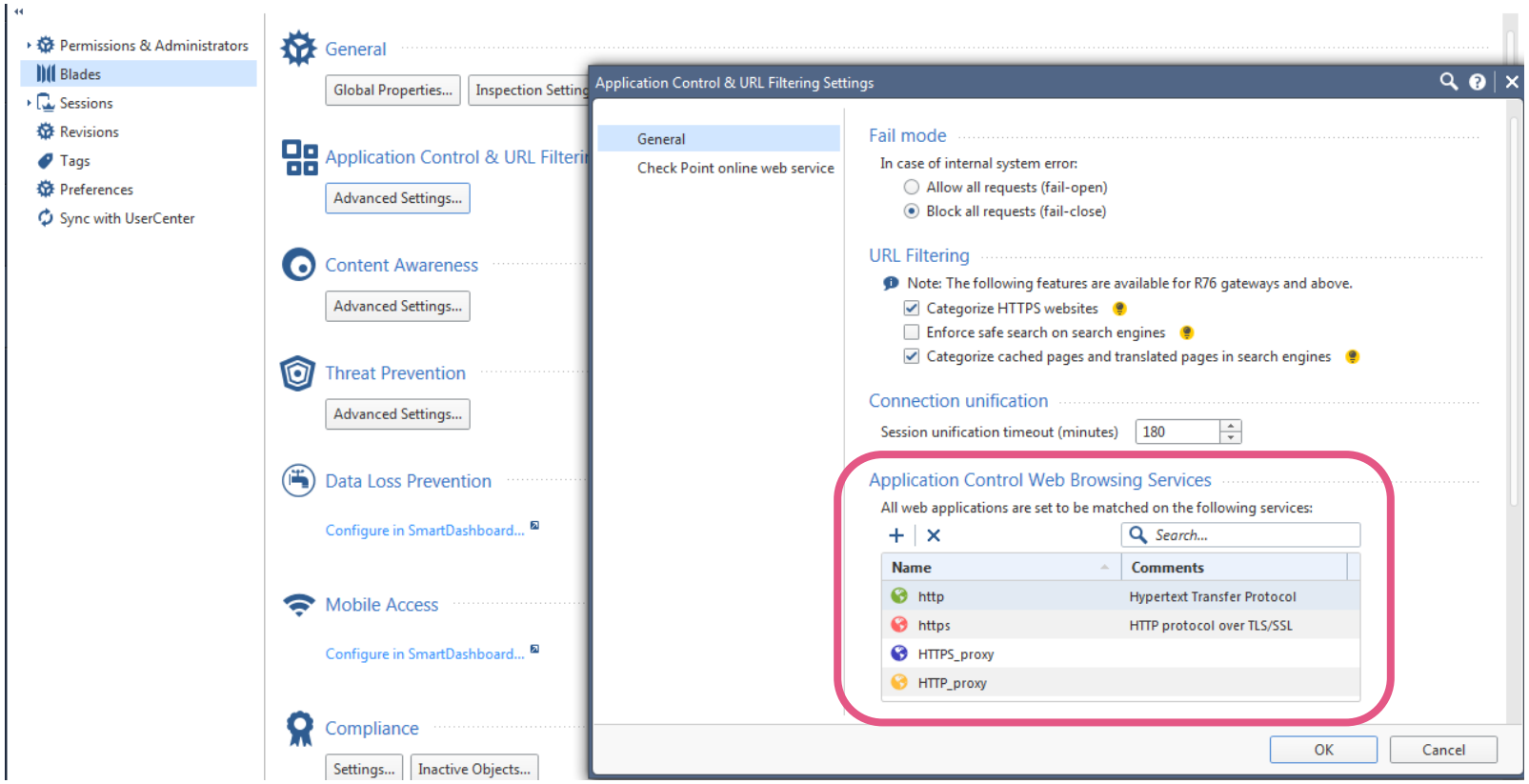


- When hovering with the mouse over the object, you see that this category will match for:
  - HTTP
  - HTTPS
  - HTTP_proxy on port TCP 8080
  - HTTPS_proxy on port TCP 8080

Matching of Application, URLF and Content Objects

Services associated with Applications, URL Categories and Content Types

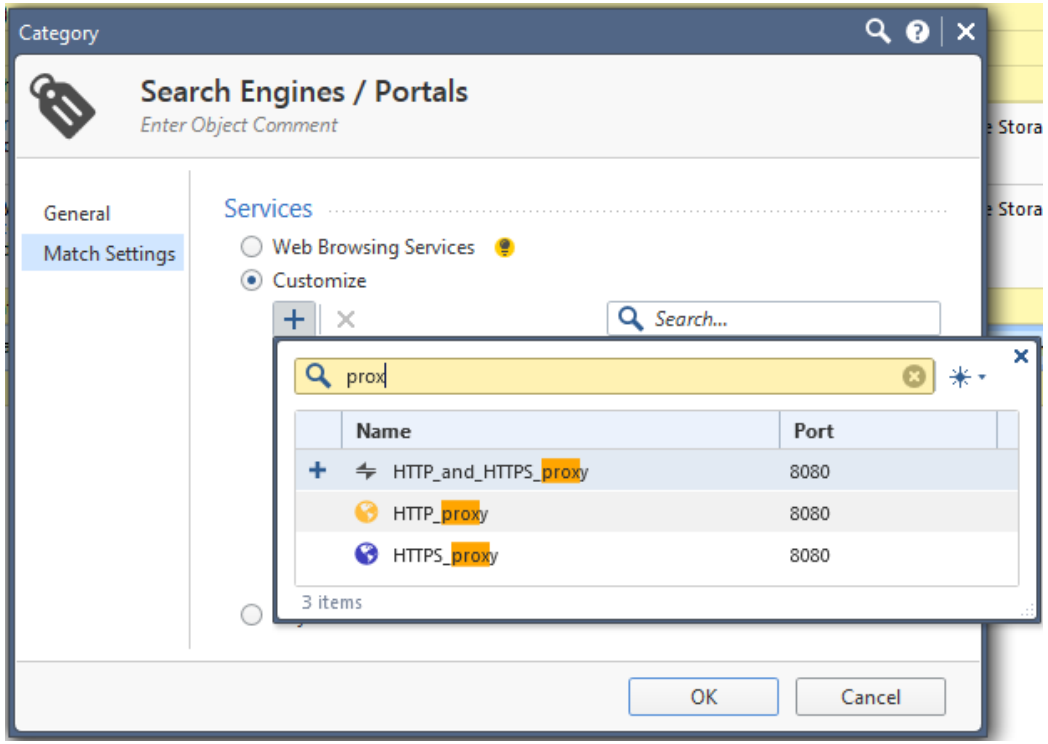
- Application signatures and URL filtering categories will match for a predefined list of services configured as “Application Control Web Browsing Services”
  - Go to “Manage & Settings > Blades > Application Control > Advanced Settings”



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

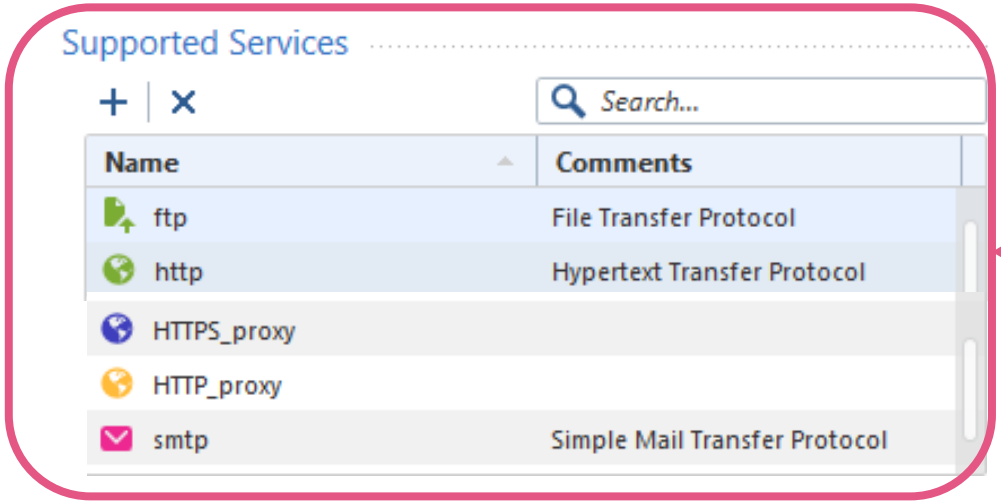


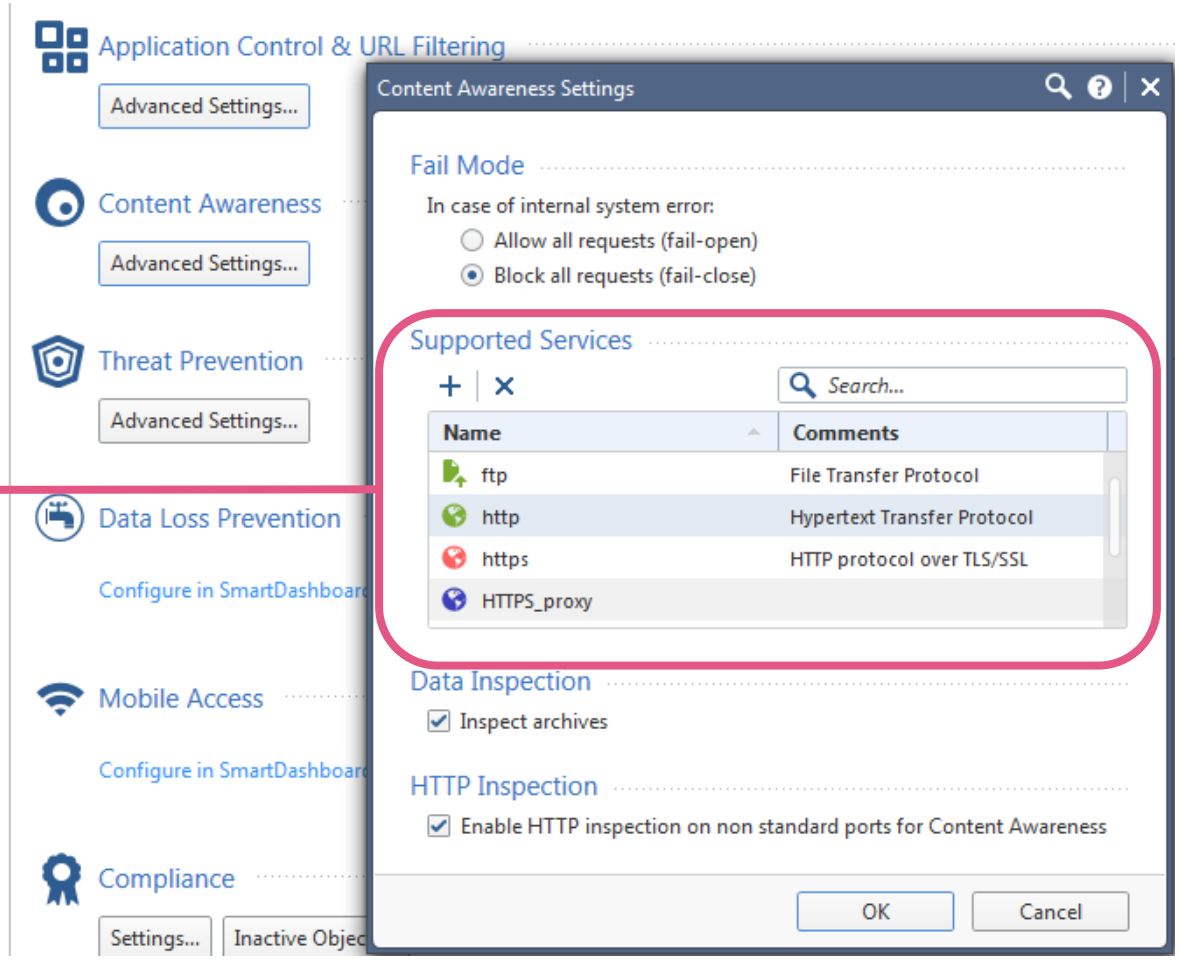
- Double click on the object and select the “match settings” menu.
- Customize the services you want this object to “match for”.

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





POLICY RULE BASE MATCHING

Policy Rule Base Matching
Introduction

Objective for the Unified Rule Base:

Matching must be performed based on all objects forming a rule

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 / Portals	* Any	Accept
▸ Clean up (10-11)							

- Match on source, destination, user access role (identity), service, application signature, content, VPN community and Mobile Access resource

Policy Rule Base Matching
Introduction

Check Point
SOFTWARE TECHNOLOGIES LTD

Solution

- A new methodology was introduced based on database matching algorithms
- A matching state was introduced to either “continue the matching process” or “achieve a final match state”

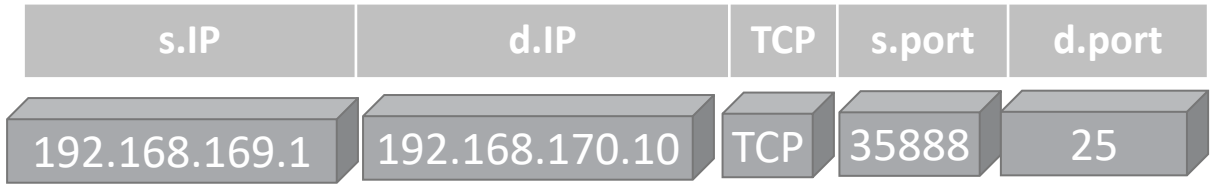
R80.10 can enforce
a complex rule base without
compromising performance

No.	Name	Source	Destination	Services & Applicat...	Content	Action
1	Management	net_192.168.169.0	gwR8010	ssh	Any	Accept
2	ICMP	net_192.168.169.0	net_192.168.170.0	icmp-proto	Any	Accept
3	DNS	Any	dnsserver OpenDNS	dns	Any	Accept
4	Parrent rule for web server	Any	web+mailserver	Web Browsing	Any	WebServerPolicyLayer
4.1	Credit Card Numbers	Any	web+mailserver	Web Browsing	Download Traffic PCI - Credit Card Numbers	Drop Content Management
4.2	Documents	Any	web+mailserver	Web Browsing	Download Traffic Document File	Accept
4.3	Spreadsheets	Any	web+mailserver	Web Browsing	Download Traffic Spreadsheet or CSV File	Accept
4.4	Cleanup rule	Any	Any	Any	Any	Accept
5	outbound	web+mailserver	Any	http https	Any	Accept
6	SMTP	net_192.168.169.0	web+mailserver	smtp	Any	Accept
7	Cleanup rule	Any	Any	Any	Any	Drop

Policy Rule Base Matching
Column based matching

- Rule base matching process (mailserver IP address 192.168.170.10)

Packet:



No.	Name	Source	Destination	Services & Applications	Action	Track
1	No match possible!					
2	No match possible!					
3	No match possible!					
4 →	No match possible!					
5 →	smtp	net_192.168.169.0	mailserver	smtp	Accept	Log
6	Cleanup rule	* Any	* Any	* Any	Drop	Log

- After the first matching round only three rules out of six remained for continued matching

This is an animated slide. Click once, then wait until this element is blinking.

Policy Rule Base Matching
Column based matching

- Look at the Inline Layers Policy

No.	Name	Source	Destination	Services & Applications	Content	Action	Track
2	Updates	mgmt	Any	http https	Any	Accept	Log
3	DNS	net_192.168.169.0 net_192.168.170.0	Any	dns	Any	Accept	None
4	Active Directory Central	Central_Client_Zone	Central_Services_Zone	Any	Any	Active_Directory_Layer Network	N/A
4.1	Active Directory Server	All_Client_networks	All_Domain_Controllers	NBT https ldap ldap-ssl Kerberos_v5_TCP	Any	Accept	None
4.2	Iden			DCE-RPC Protocol		Accept	None
4.3	Identity Collector	All_Identity_Collectors	All_Domain_Controllers	https	Any	Accept	None
4.4	LDAP Group Query	All_Gateways	All_Domain_Controllers	ldap ldap-ssl	Any	Accept	None
4.5	Cleanup rule	Any	Any	Any	Any	Drop	None
5	Active Directory Backup Site	Backup_Site_Zone	Backup_Site_Services_Zone	Any	Any	Active_Directory_Layer Network	N/A
6	SMTP	net_192.168.169.0	web+mailserver	smtp	Any	Accept	Log
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

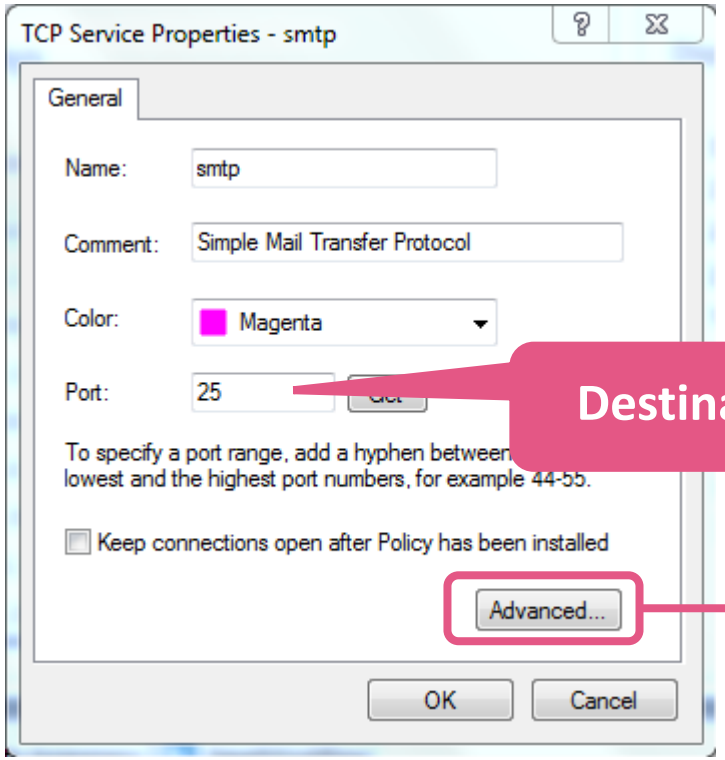
Only traffic matching the "Parent Rule" will be matched against the "Inline Layer" rules

04
PROTOCOL SIGNATURES

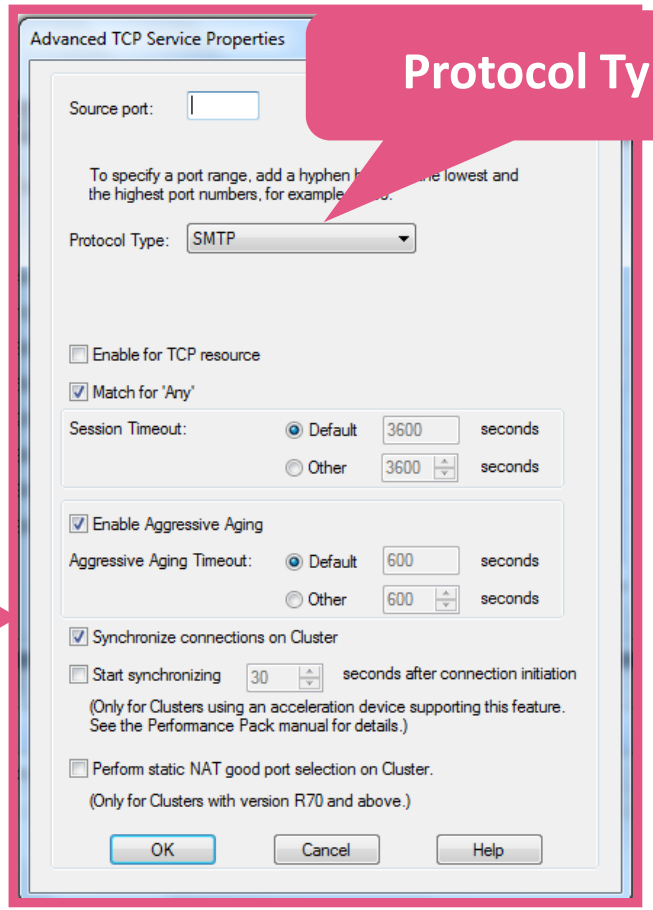
Reviewing R77.30 Service Objects – Firewall Blade

R77.30 (and older releases) Service Objects - Protocol Type

- Example: the service object for SMTP includes a **Protocol Type** definition



Destination Port



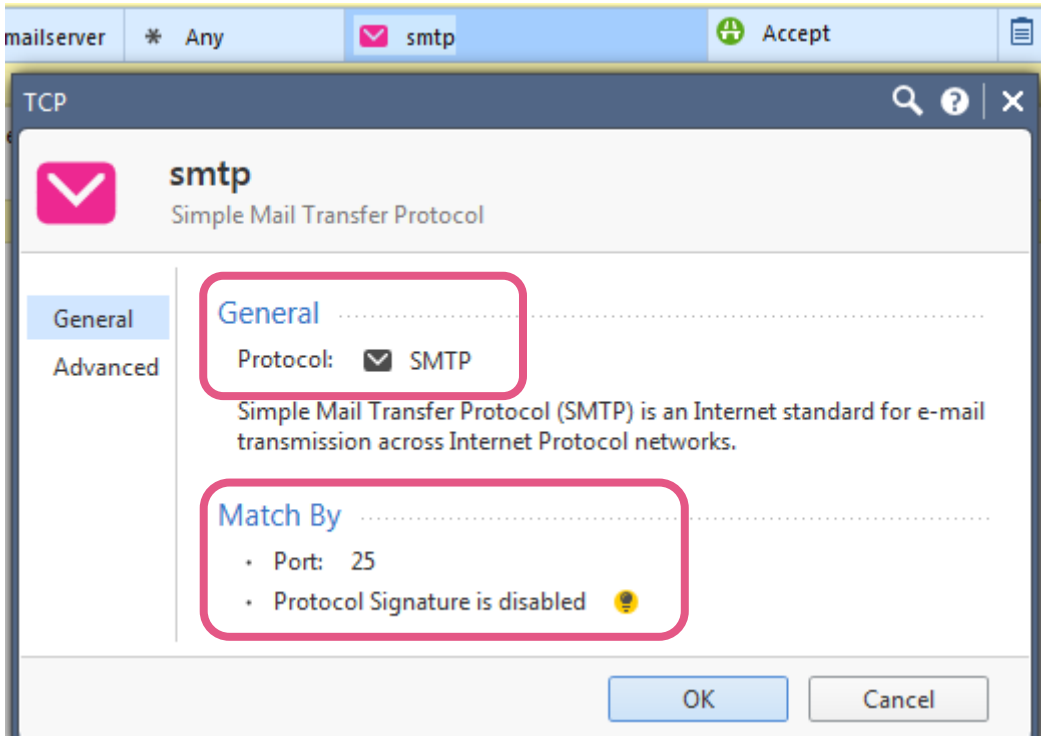
Protocol Type

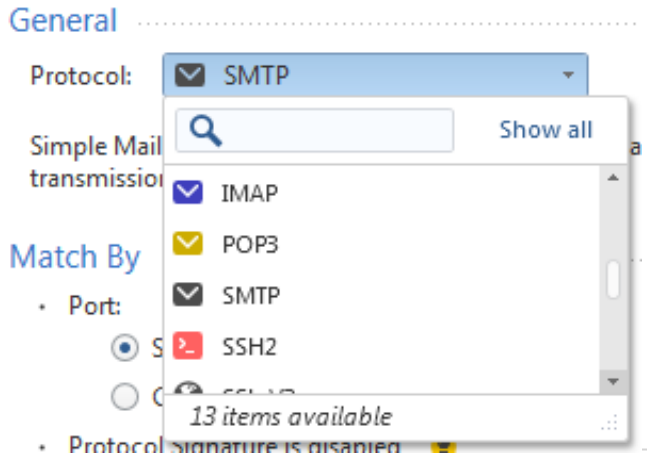
The Protocol Type includes INSPECT Code used when enforcing the protocol

While working on R80.10 all Protocol Type definitions have been reviewed

R80.10 Service Objects - Protocol Signatures

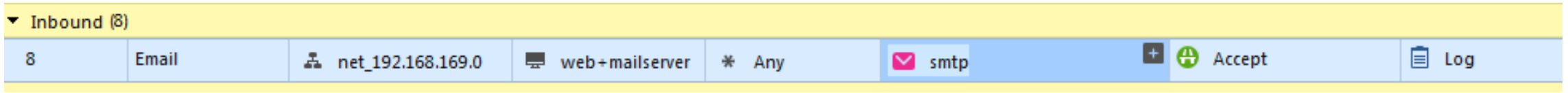
- In R80.10 service objects can be used in a more flexible way enforcing the protocol
- By default a service object like SMTP refers to a Protocol Type can't be edited or changed
- The "Match By" definition tells:
  - By default the object is matching by the destination port
- You can change the Protocol Type on a cloned object

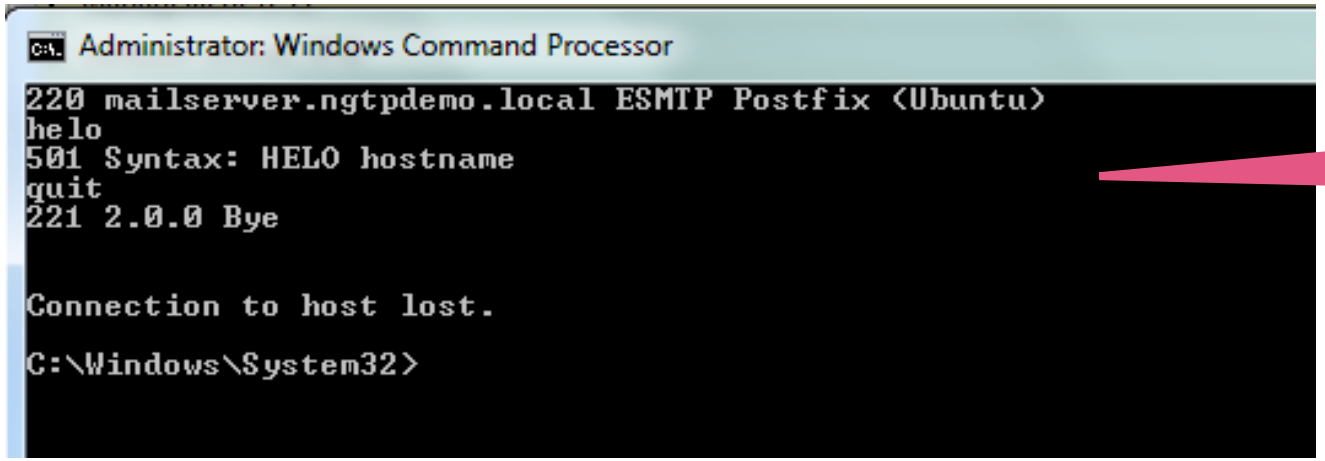




R80.10 Service Objects - Protocol Signatures

- When using Service objects with default settings a gateway running only the Firewall Blade works like it used to work with R77.30 (and older) releases
- Example: even if the firewall rule states “allow SMTP to the mail server” you can do a telnet session with destination port 25 and you’ll have a successful connection



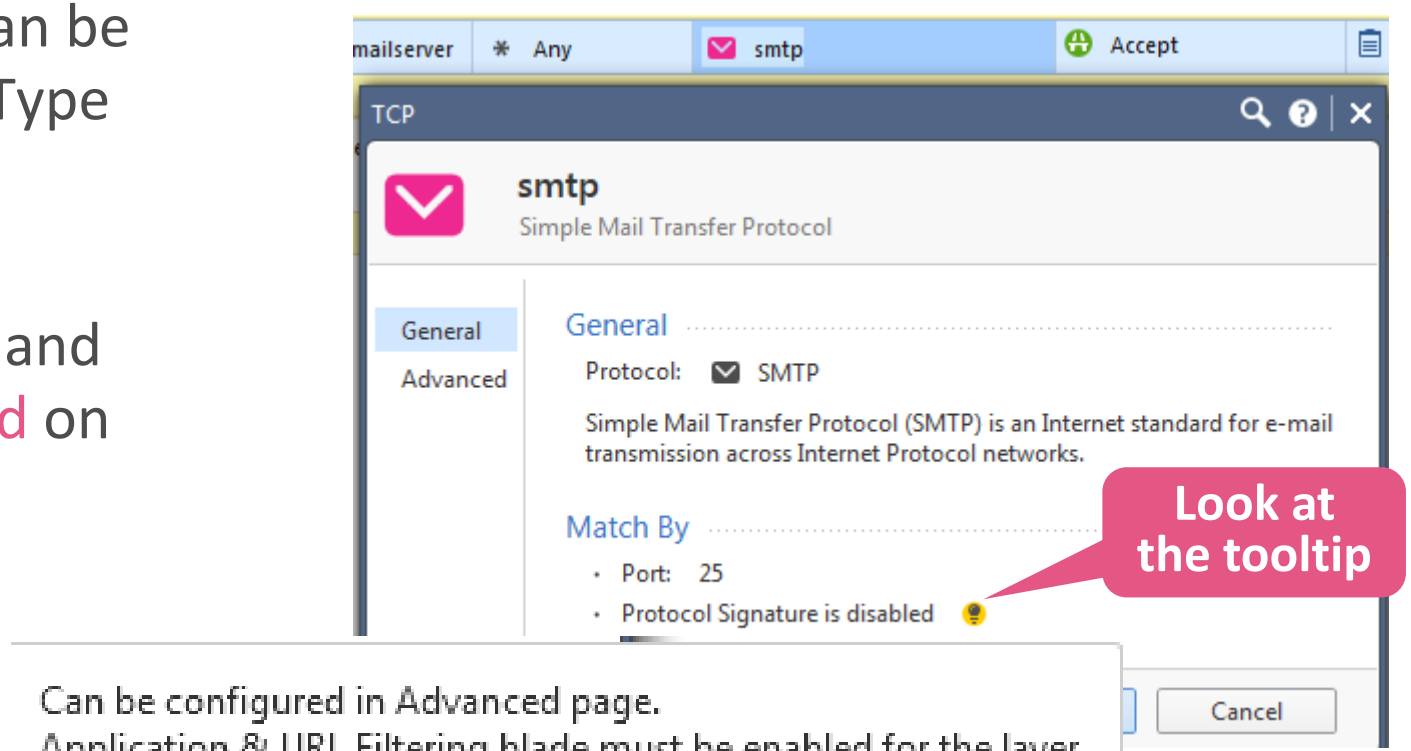


The telnet connection will stay open until you close it.

There is a lab about this example

R80.10 Service Objects - Protocol Signatures

- A new functionality called “Protocol Signature” can be enabled
- The **Protocol Signature** option can be enabled, replacing the Protocol Type based enforcement
- The Protocol Signature function requires the Application Control and URL Filtering Blade being enabled on the gateway and on the policy

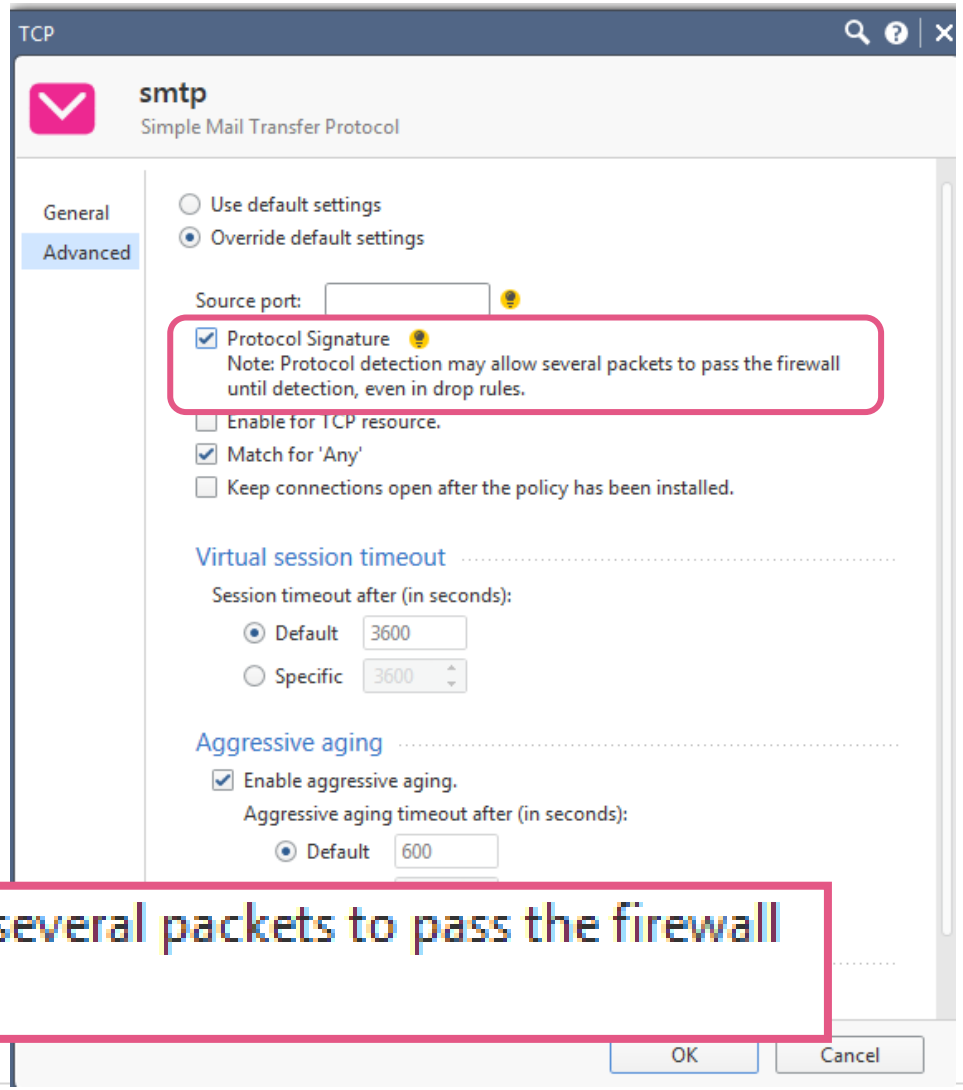


Can be configured in Advanced page.
Application & URL Filtering blade must be enabled for the layer.
Application Control must be enabled on the gateway.

There is a lab about this example

R80.10 Service Objects - Protocol Signatures

- Under “Advanced” the enforcement of the **Protocol Signature** can be enabled
  - It is a best practice to clone a default object and to change the settings on the cloned object
- Enabling the Protocol Signature enforcement the gateway enforces the TCP protocol SMTP using elements of the Application Control Blade (like the pattern matcher)
- As a consequence several packets may pass the firewall until detection

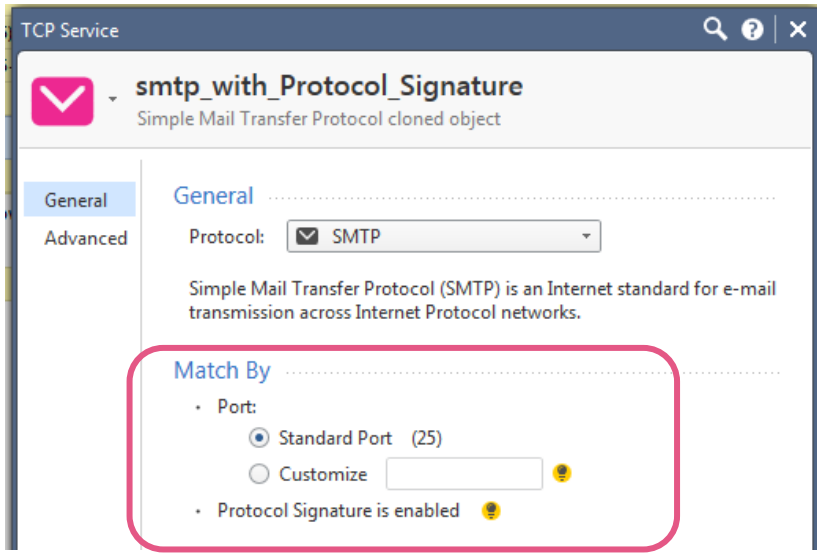


Note: Protocol detection may allow several packets to pass the firewall until detection, even in drop rules.

R80.10 Service Objects - Protocol Signatures

- When using an object with Protocol Signature enforcement the telnet session to port 25 will be dropped, once the violation is detected

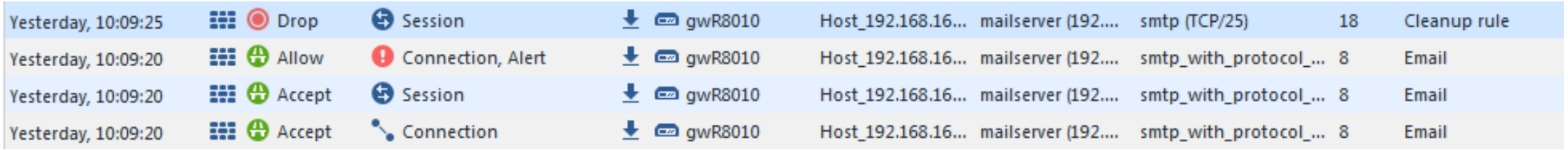
Inbound (8)							
8	Email	net_192.168.169.0	web+mailserver	Any	smtp_with_Protocol_Signa...	Accept	Log
Outbound (9)							



There is a lab about this example

R80.10 Service Objects - Protocol Signatures

- Example: what are the consequences when using the service object “SMTP with Protocol Signature” for controlling the access to a mail server?
- Logging will show
  - A successful “Connection”
  - A successful “Session”
  - In sequence a “Connection, Alert” log message
  - A final “Drop” Session log message

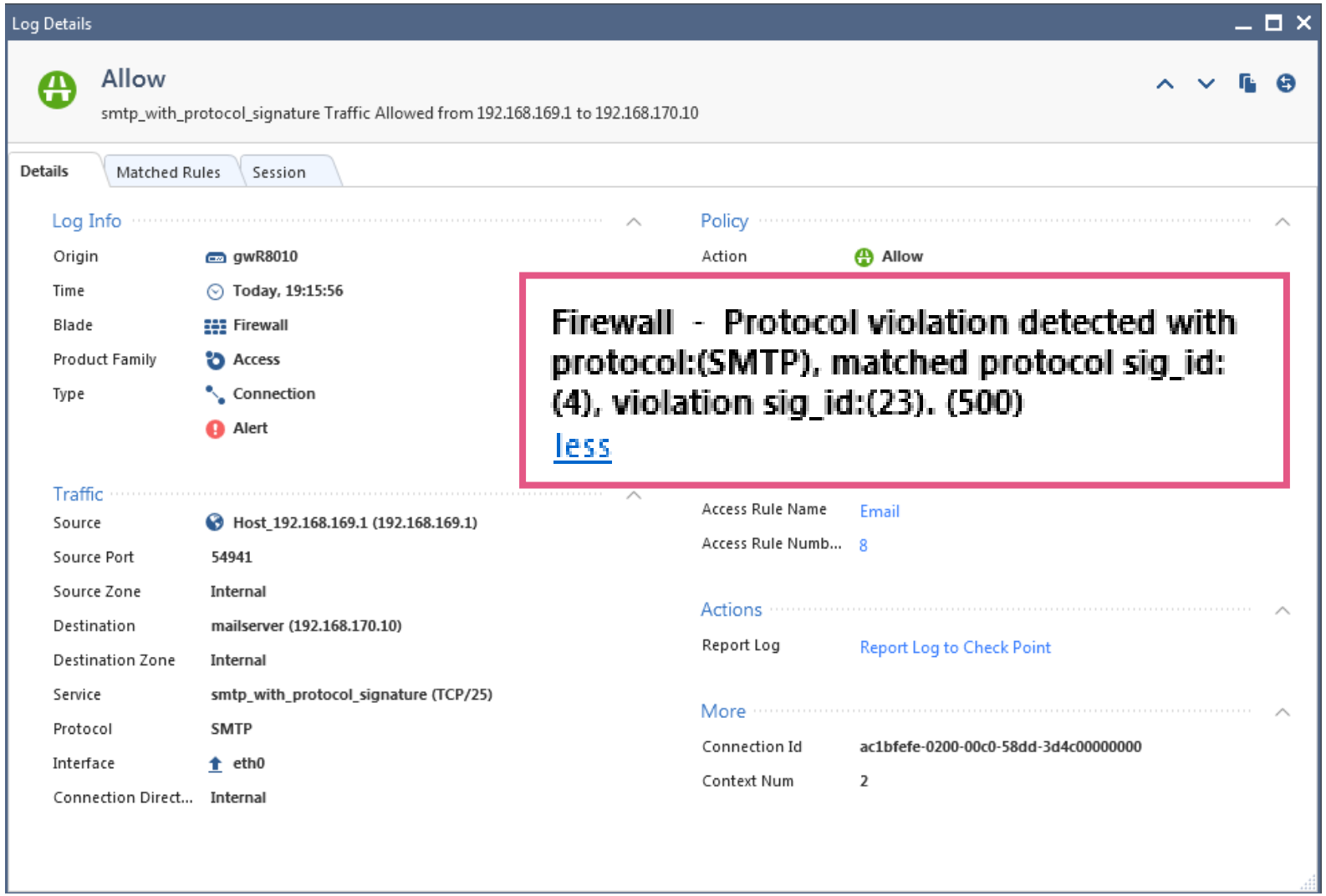


Yesterday, 10:09:25	Drop	Session	gwR8010	Host_192.168.16...	mailserver (192....	smtp (TCP/25)	18	Cleanup rule
Yesterday, 10:09:20	Allow	Connection, Alert	gwR8010	Host_192.168.16...	mailserver (192....	smtp_with_protocol_...	8	Email
Yesterday, 10:09:20	Accept	Session	gwR8010	Host_192.168.16...	mailserver (192....	smtp_with_protocol_...	8	Email
Yesterday, 10:09:20	Accept	Connection	gwR8010	Host_192.168.16...	mailserver (192....	smtp_with_protocol_...	8	Email

There is a lab about this example

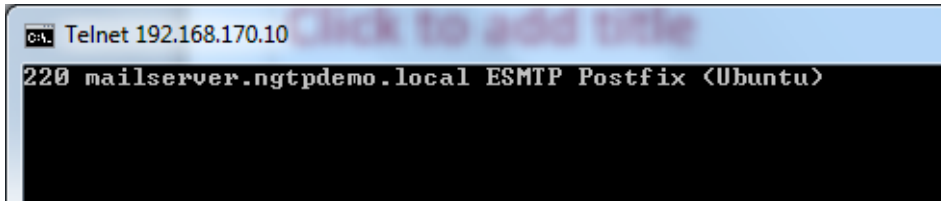
R80.10 Service Objects - Protocol Signatures

- Details of the “Connection, Alert” log message



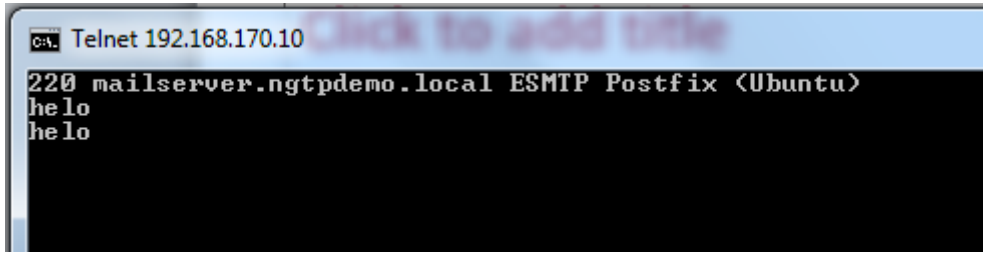
R80.10 Service Objects - Protocol Signatures

- If you just open the connection and leave it idle you will see the connection still allowed



Time	..	..	Type	..	Origin	Source	Destination	Service	Access Rule...	Access Rule N...	Policy...	..
Today, 19:30:07			Connection		gwR8010	Host_192.168.169.1 (192.168.169.1)	mailserver (192.168....	smtp_with_protocol_signature (TCP/25)	8	Email	NGTPde...	s..

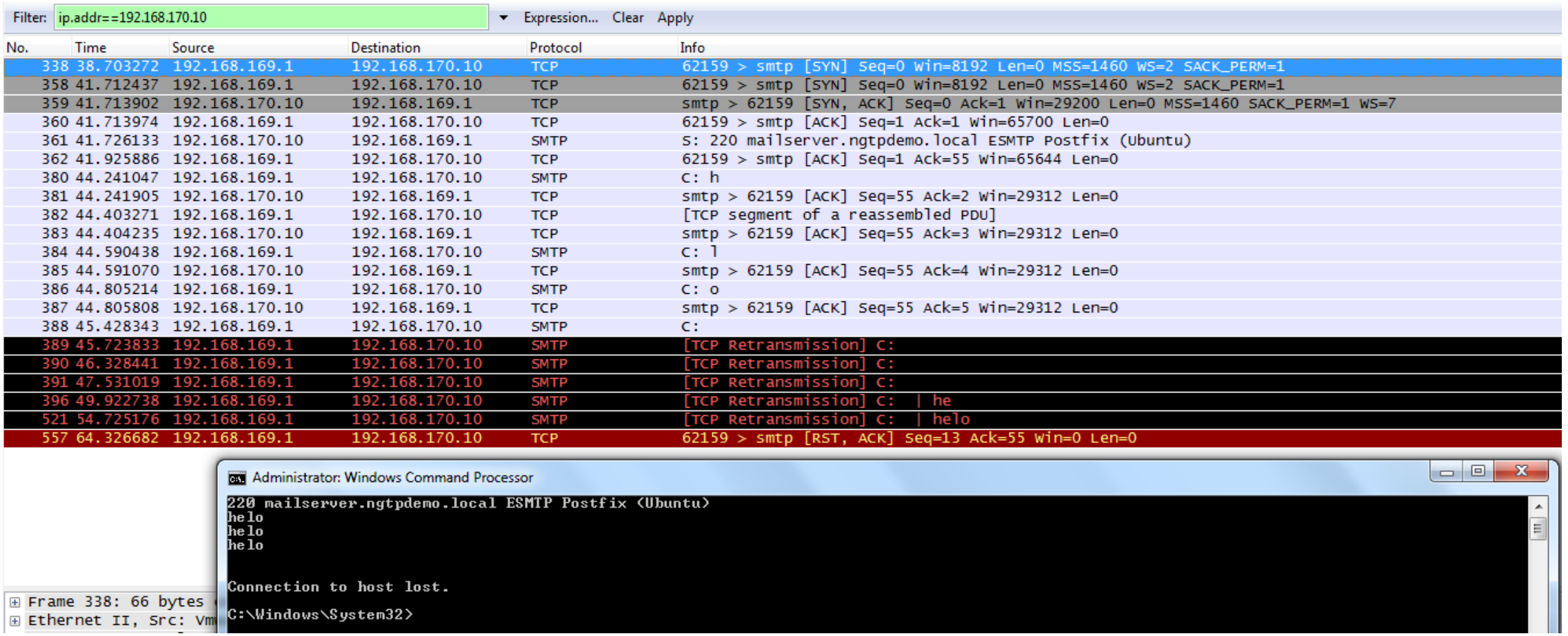
- Sending packets the gateway will drop the connection



Time	..	..	Type	..	Origin	Source	Destination	Service	Access Rule...
Today, 19:32:52			Session		gwR8010	Host_192.168.169.1 (192.168.169.1)	mailserver (192.168....	smtp (TCP/25)	18
Today, 19:31:34			Connection		gwR8010	mailserver (192.168.170.10)	94.245.88.28	https (TCP/443)	11
Today, 19:30:07			Connection, Alert		gwR8010	Host_192.168.169.1 (192.168.169.1)	mailserver (192.168....	smtp_with_protocol_signature (TCP/25)	8
Today, 19:30:07			Connection		gwR8010	Host_192.168.169.1 (192.168.169.1)	mailserver (192.168....	smtp_with_protocol_signature (TCP/25)	8

R80.10 Service Objects - Protocol Signatures

- Running a TCPDUMP on the client computer you will see a packet flow like this:



R80.10 Service Objects - Protocol Signatures

Summary

- By default Service Objects use the matching methods by Protocol Type and port
- Customers may decide enabling Protocol Signatures using cloned service objects
- The Protocol Signature enforcement may allow passing of packets even the service object is used in a drop rule
- The Protocol Signatures are stored on the gateway in a database
- This database can get updated in the future

What is this good for?

You have a granular control on how services are enforced.

LOGGING

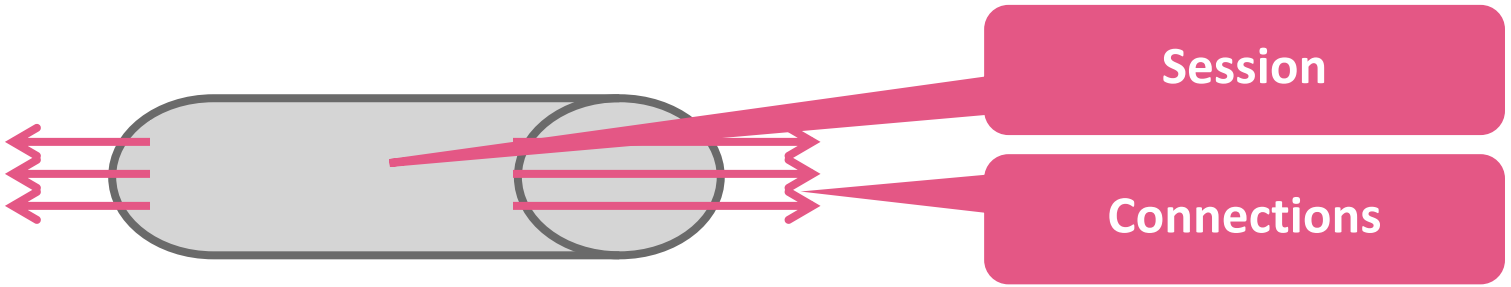
How can we achieve more visibility on the connections related to an application layer session?

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”

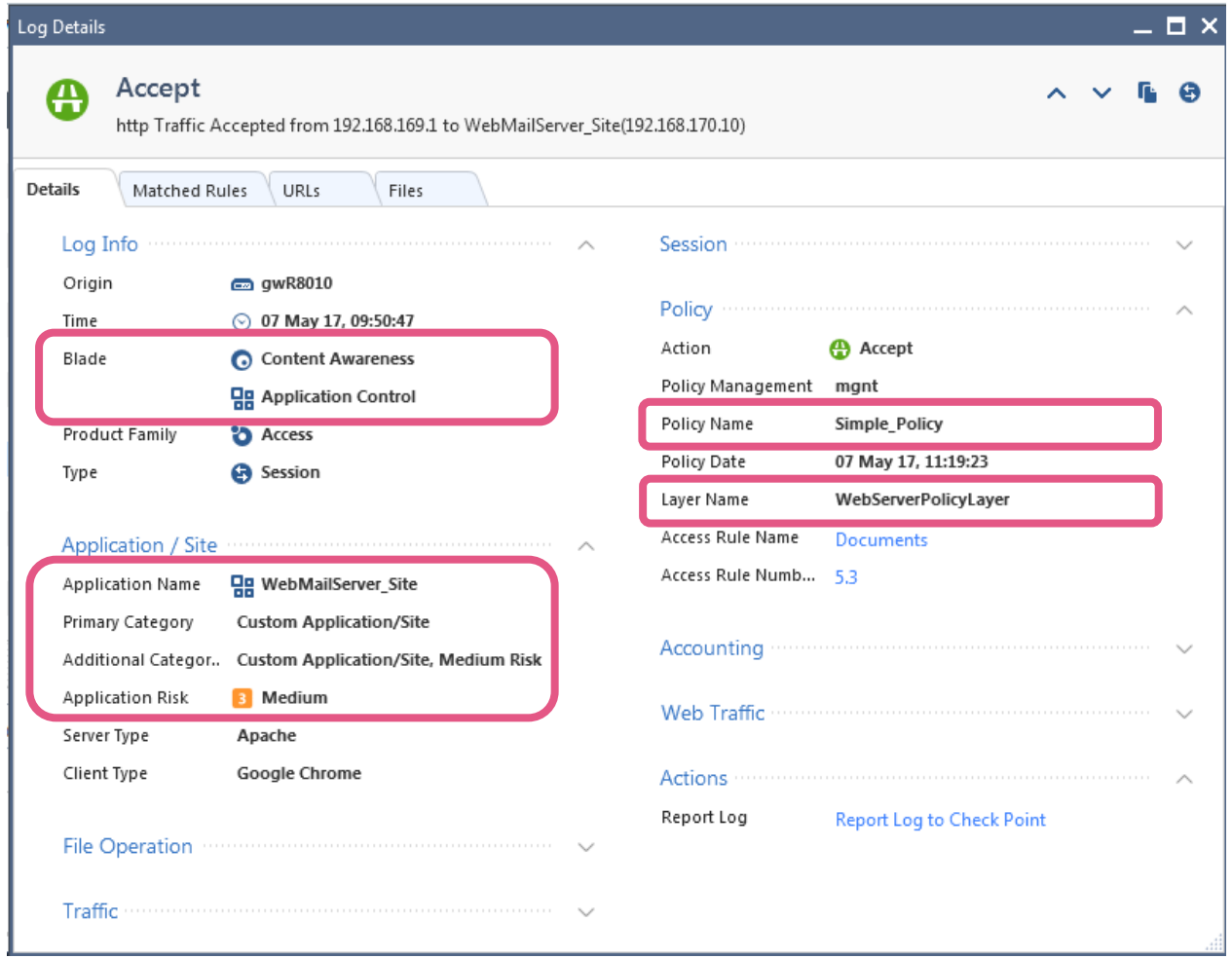


Logging
Unified Logging Cards – see all in one place

Let's follow the logs for the highlighted rules

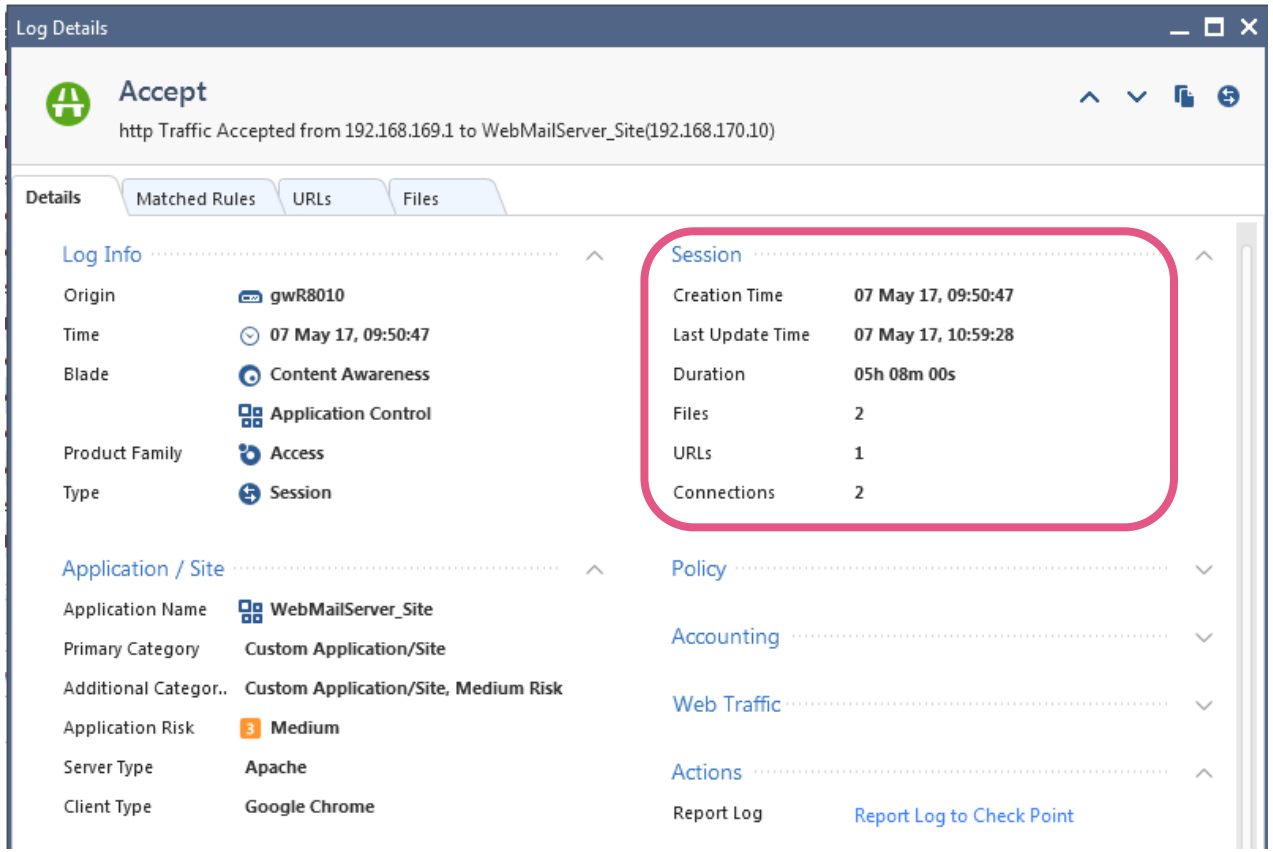
3	DNS	net_192.168.169.0 net_192.168.170.0	Any	dns	Any	Accept	None
4	ICMP	net_192.168.169.0	web+mail...	icmp-proto	Any	Accept	None
5	Intranet	net_192.168.169.0	web+mail...	Web Browsing	Any	WebServerPolicyLaye	N/A
5.1	Spreasheets including credit card num	net_192.168.169.0	web+mail...	Web Browsing	Download 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



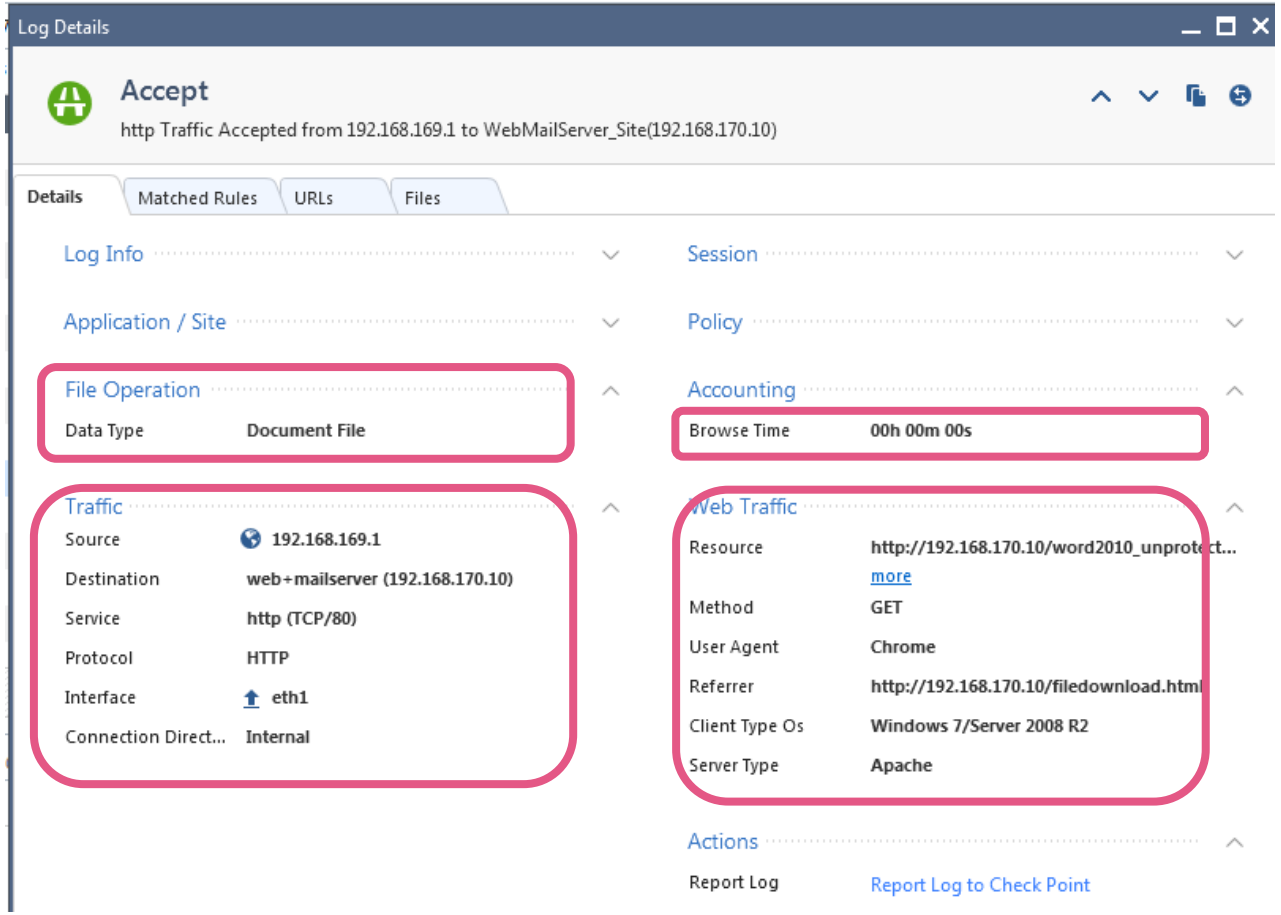
- Software Blades
- Applications
- Policy triggered
- Policy Layer involved

Logging
Unified Logging Cards – see all in one place



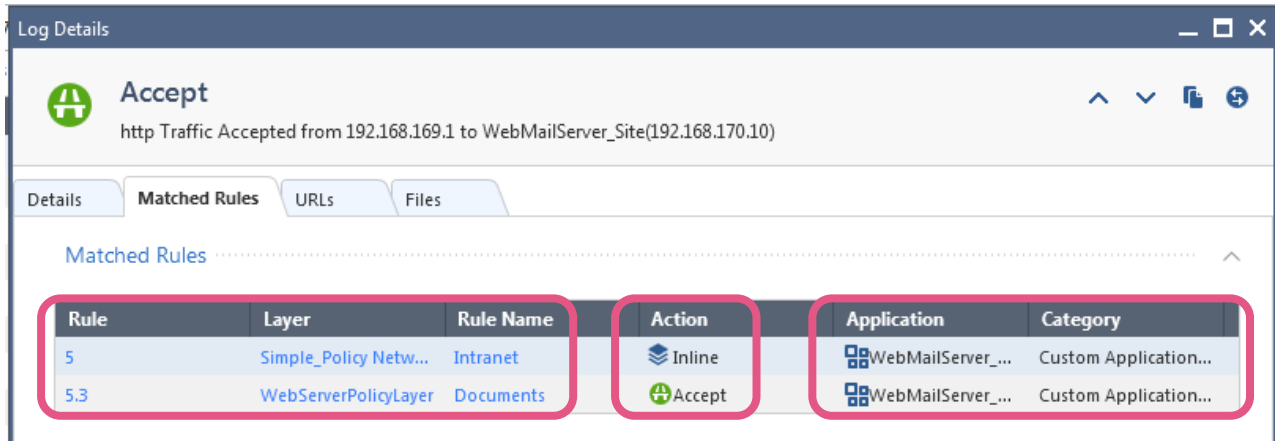
- Session details
  - When it started
  - How long it has been established
  - How many files have been transmitted
  - Which URLs have been used
  - How many connections are related

Logging
Unified Logging Cards – see all in one place



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

Logging
Unified Logging Cards – see all in one place

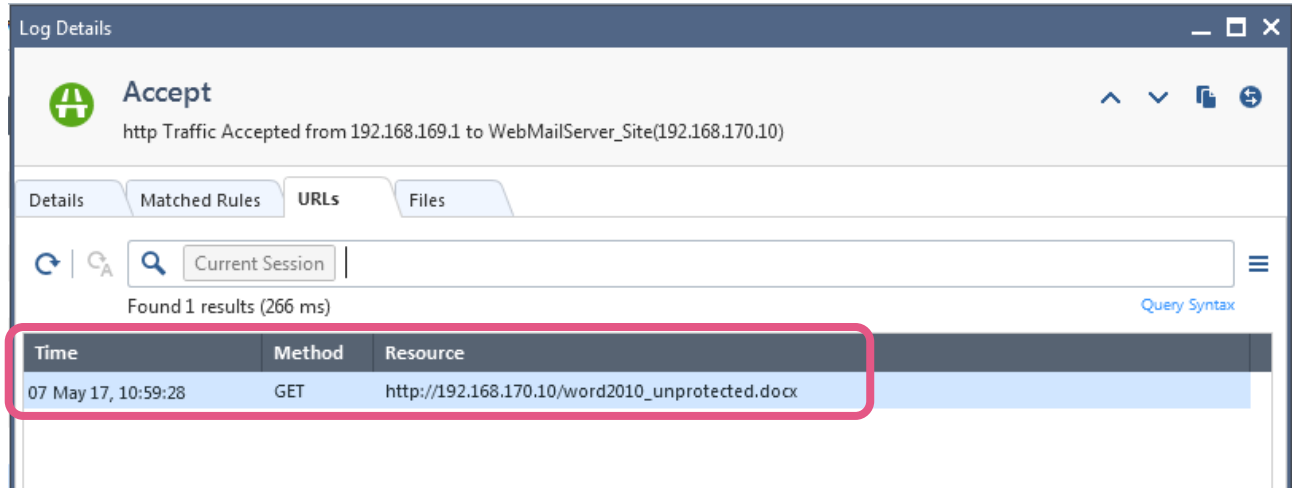


- Matched Rules and Layers
- Actions
- Application and category

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	Spreasheets 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

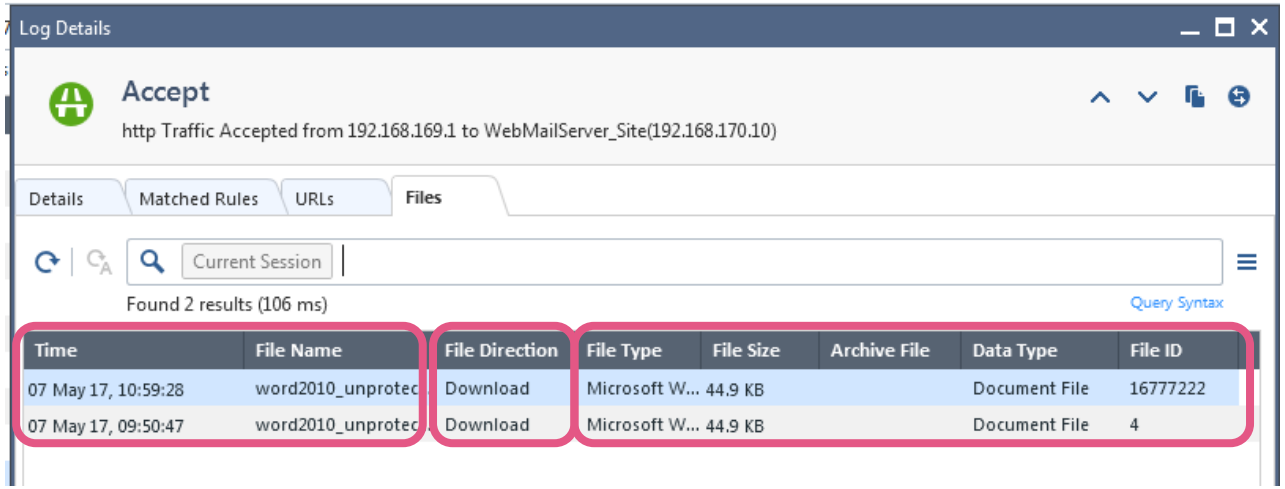
Rule base

Logging
Unified Logging Cards – see all in one place



- Complete URL

Logging
Unified Logging Cards – see all in one place



- 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

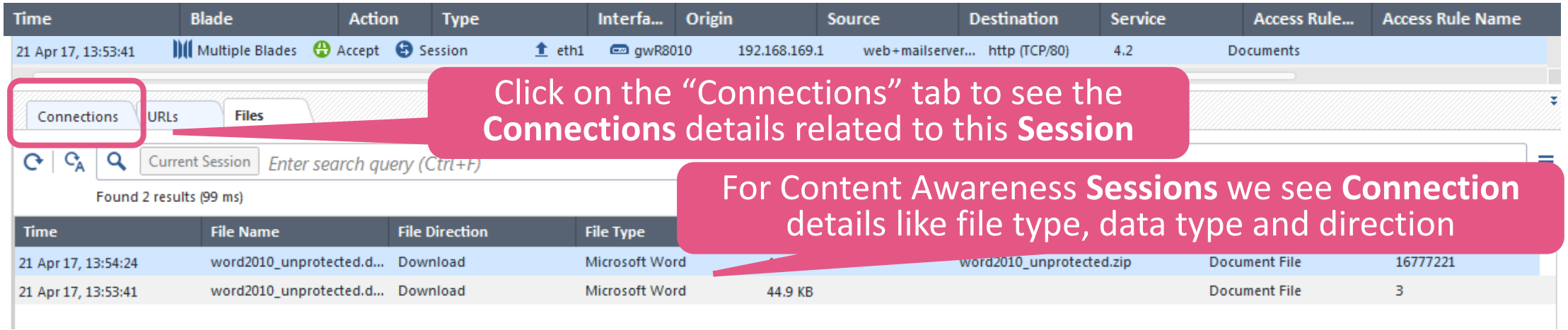
Time	Blade	Action	Type	Interfa...	Origin	Source	Destination	Service	Access Rule...	Access Rule Name
21 Apr 17, 13:47:14	Firewall	Accept	Connection	eth0	gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	4.4	Cleanup rule
21 Apr 17, 13:47:14	Firewall	Accept	Connection	eth0	gwR8010	192.168.169.1	web+mailserver...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



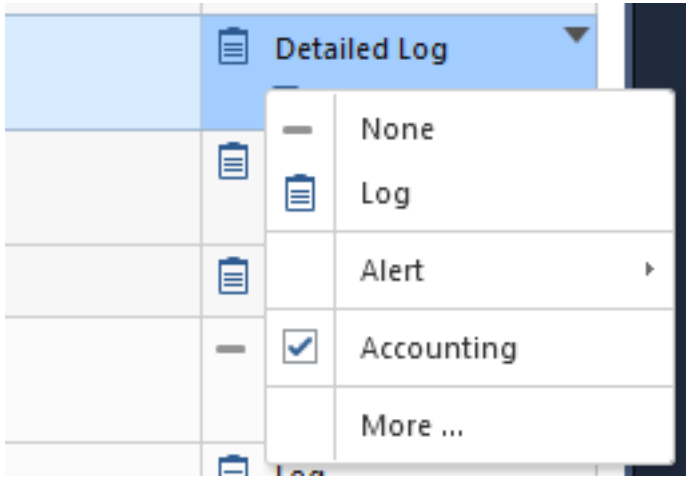
Connections And Sessions
Configuration of the Logging options

No.	Name	Source	Destination	Services & Applicat...	Content	Action	Track
4	Parrent 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

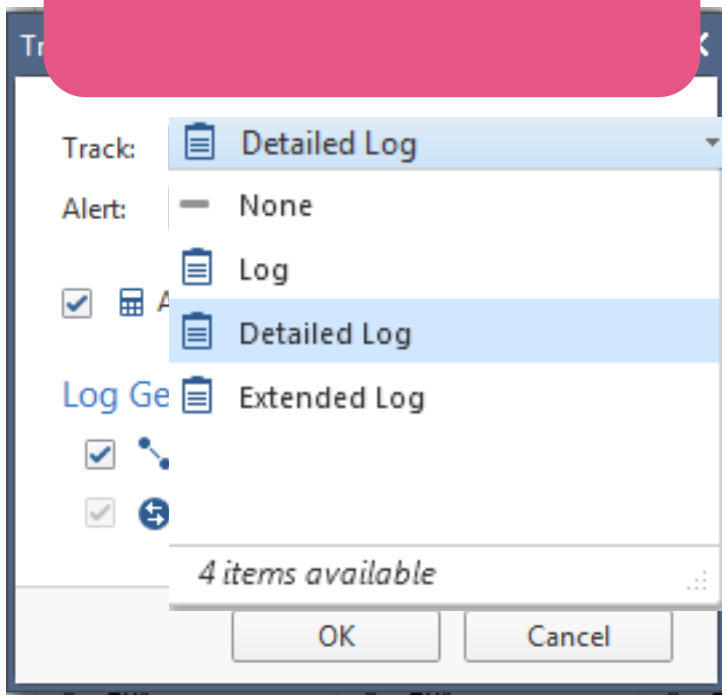
- Log: track source, destination, source port and destination port
- Detailed Log: in addition to “Log” the name of the application that has matched
  - Requires APCL, URLF or Content Awareness Blade being active
- Extended Log: in addition to “Log” the URLs and Files related to the session
- Accounting: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

Connections And Sessions
Configuration of the Logging options

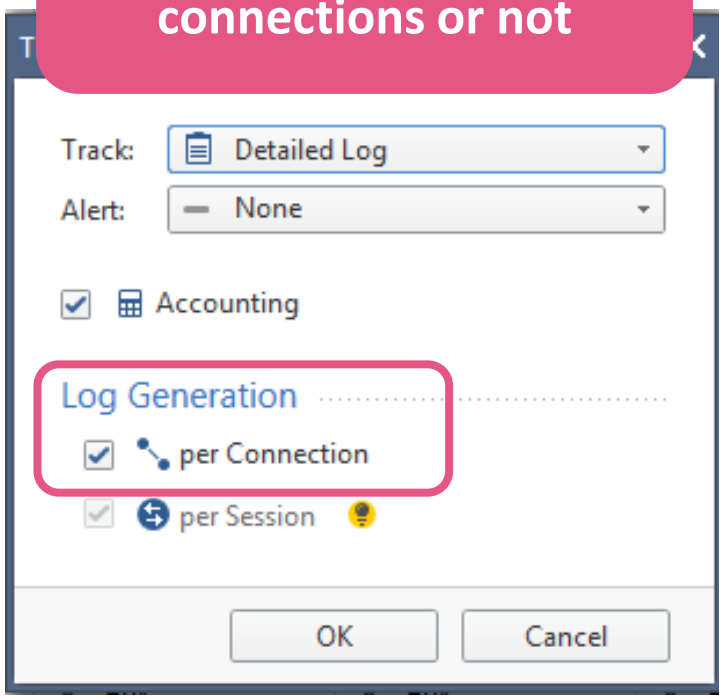
- Change the logging options using a right click on the track column



Select the track option



Select logs to be generated per connections or not



What is this good for?

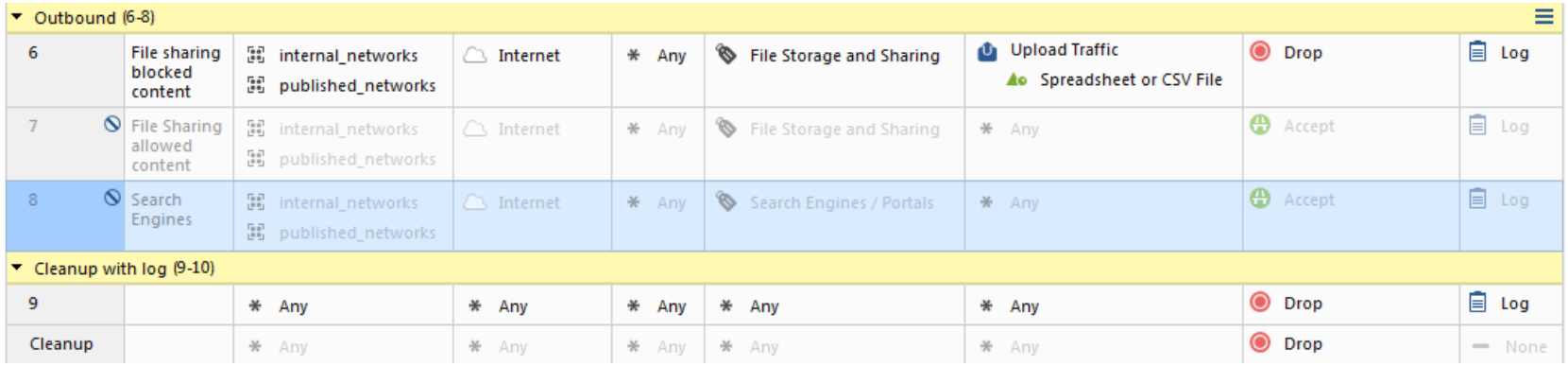
You can provide visibility how many TCP connections are related to an application session.

THE “EARLY DROP” FUNCTIONALITY

Early Drop

Dropping connections before a final rule match is achieved - sk111643

- Filter criteria such as Application or Content can’t be resolved on first packets
- The security policy may decide to **block the connection** at an early stage without a final rule decision, **if all potential rules** of a layer for a specific connection **have a Drop** or Reject action
- This drop will issue a log with rule name "CP_Early_Drop" and hits will be counted for all the potential rule like shown in this
  - Example: rule #7 and #8 are disabled, rule #6 prevents uploading content, so any access to “File Storage and Sharing” sites will be blocked by “Early Drop”

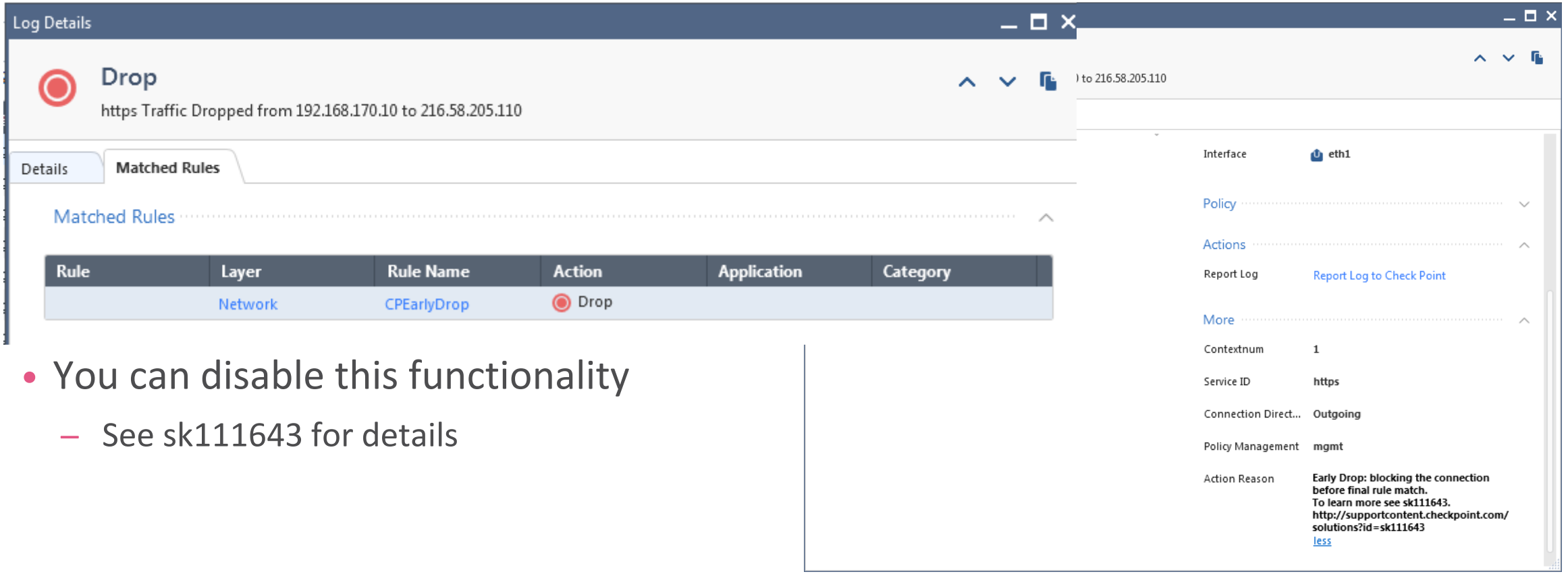


Outbound (6-8)								
6	File sharing blocked content	internal_networks published_networks	Internet	Any	File Storage and Sharing	Upload Traffic Spreadsheet or CSV File	Drop	Log
7	File Sharing allowed content	internal_networks published_networks	Internet	Any	File Storage and Sharing	Any	Accept	Log
8	Search Engines	internal_networks published_networks	Internet	Any	Search Engines / Portals	Any	Accept	Log
Cleanup with log (9-10)								
9		Any	Any	Any	Any	Any	Drop	Log
Cleanup		Any	Any	Any	Any	Any	Drop	None

Early Drop

Dropping connections before final rule match sk111643

- A log example for a packet that has been dropped by the “Early Drop” functionality



- You can disable this functionality
  - See sk111643 for details

CoreXL News
Dynamic Dispatcher and Priority Queuing

Both functions are now configured using dedicated commands

Sk105261 CoreXL Dynamic Dispatcher is **enabled by default**

Sk105762 Priority Queues

- **disabled by default**
- you can enable a mode to monitor heavy data connections using cpview
- you can enable the functionality completely

Summary

- Policies can be organized using Inline or Ordered Layers
- Policy matching for APCL, URLF and Content Awareness objects
- Policy rule base matching
- Protocol Signatures
- Logging
- Early Drop functionality

Check Point
SOFTWARE TECHNOLOGIES LTD

CONTENT AWARENESS

Obtaining visibility and control about files and data

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

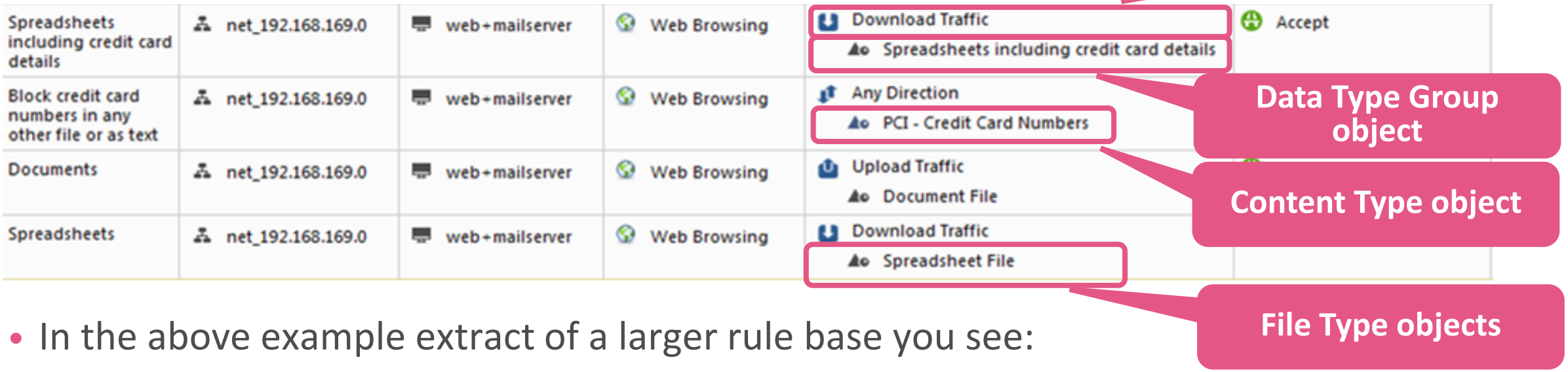
- The Content Awareness Blade provides visibility and enforcement based on the content transmitted in the data streams through the security gateway
  - You can activate the Blade in conjunction with Application Control, URL Filtering and HTTPS inspection, Mobile Access, IPSec VPN and Identity Awareness
- 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	

- 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

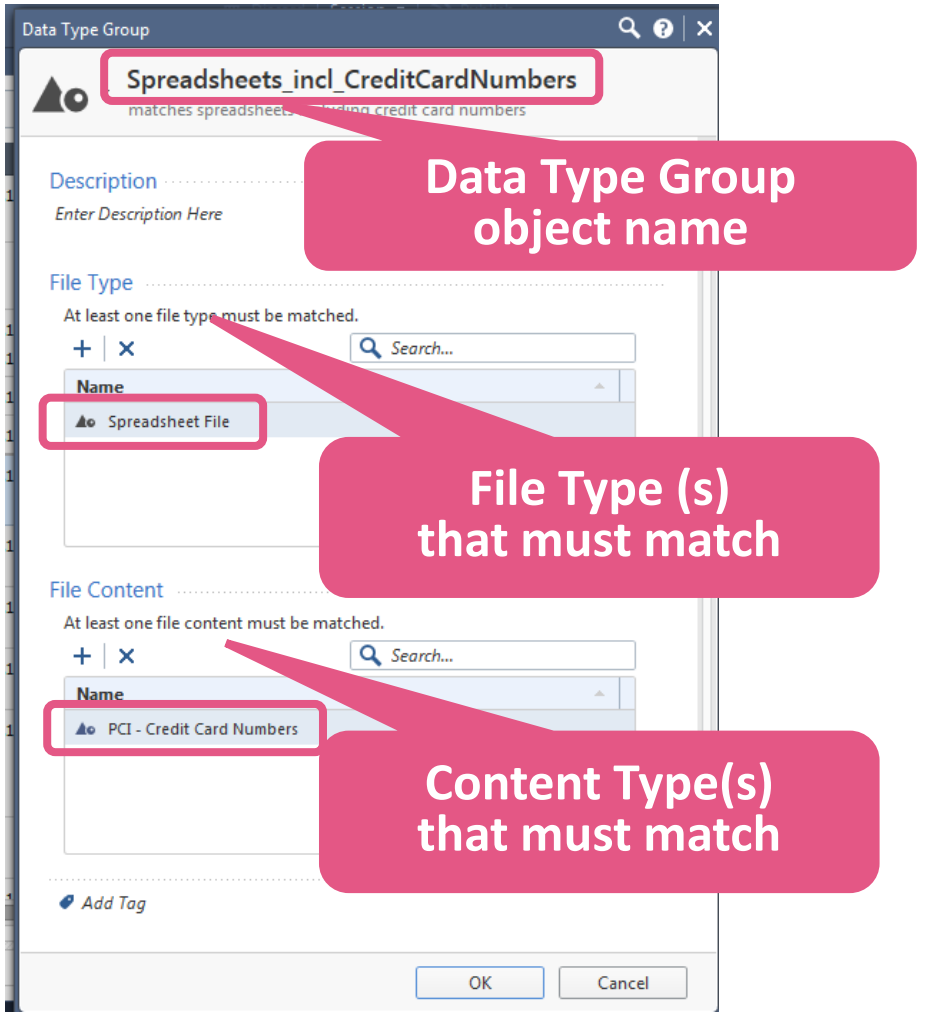
Combining File Types and Content Types to a Data Type group object

- 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

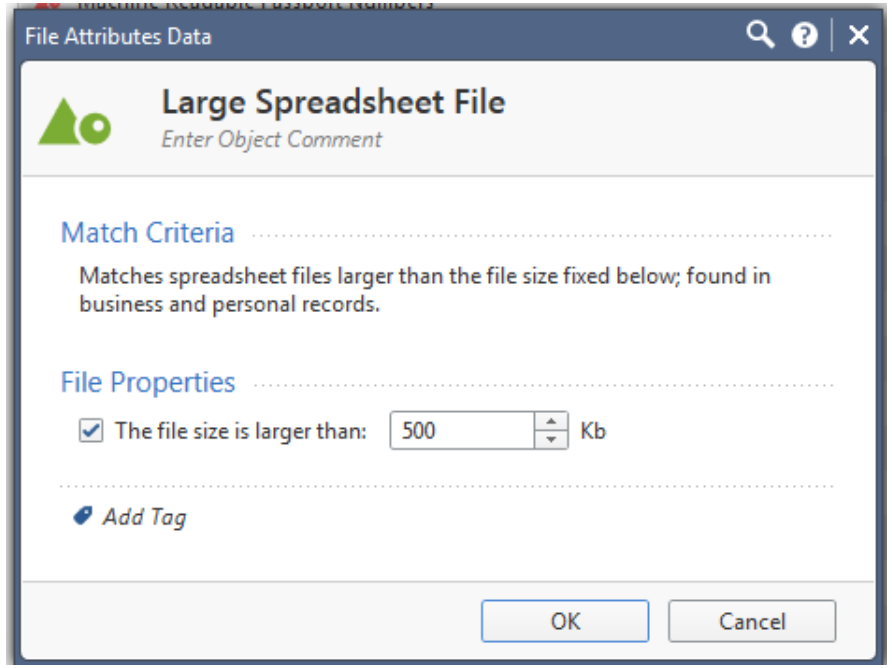
Remember this example!

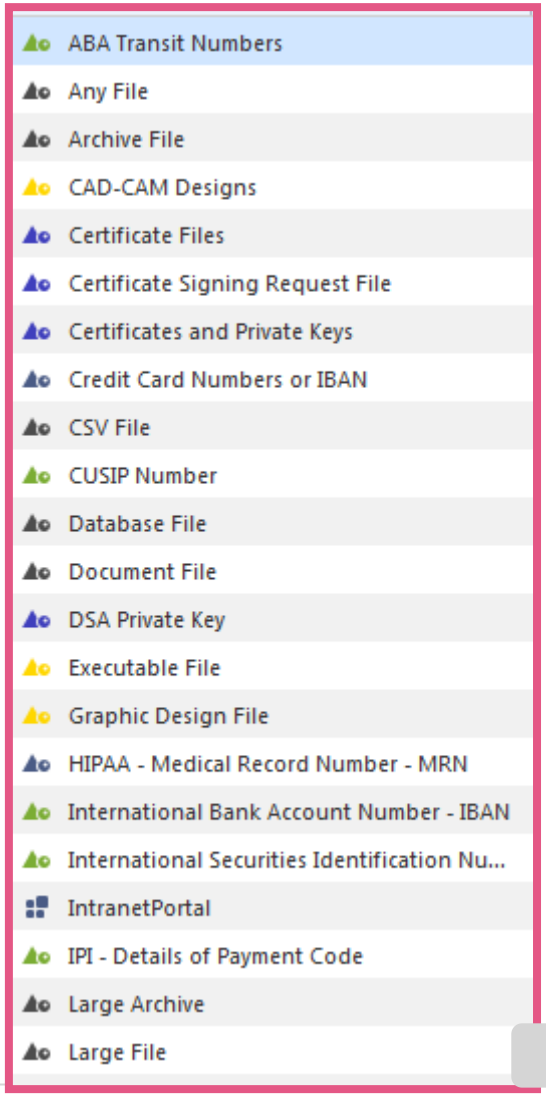


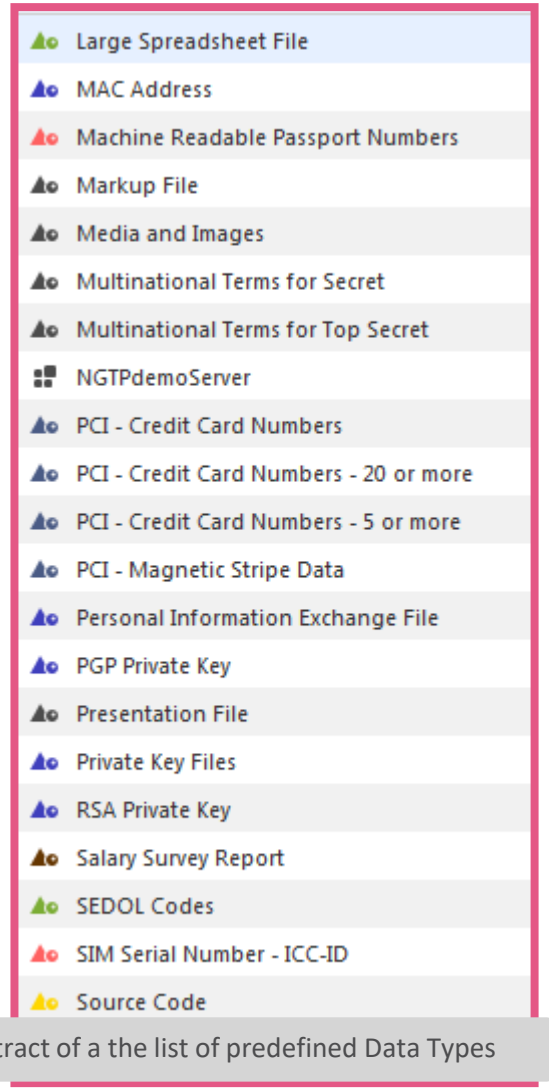
Introduction to Content Awareness

Predefined Data Types

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







Extract of a the list of predefined Data Types

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)

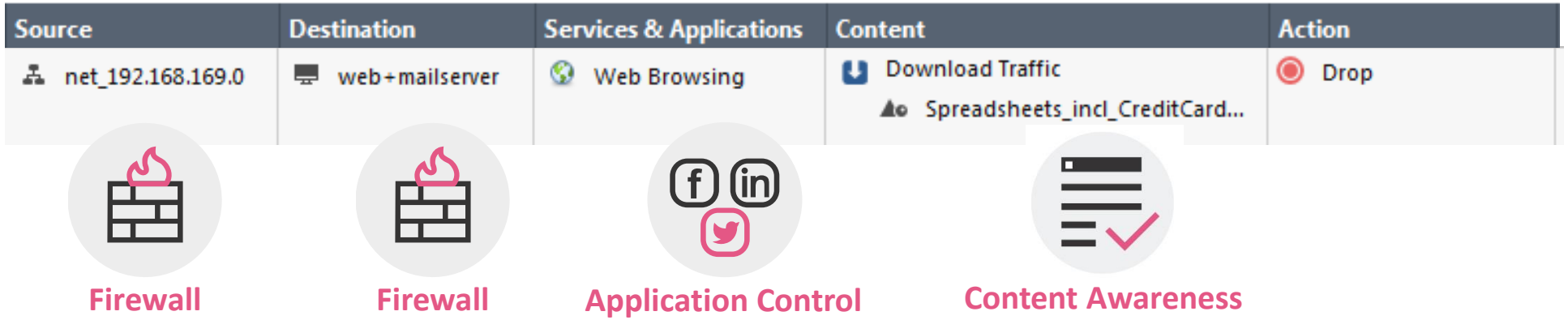
Source	Destination	Services & Applications	Content	Action
net_192.168.169.0	web+mailserver	Web Browsing	Download Traffic PCI - Credit Card Numbers Spreadsheet File	Drop

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



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
How you can propose it to customers

- The “CheckUp Approach”
  - Create **a dedicated Ordered Layer** for Content Awareness
  - Create rules for **monitoring** content transmitted through a gateway
  - Assign the layer to a gateway policy
  - **Start monitoring** and use **SmartEvent** functionalities obtaining visibility and generating reports
- Once you have sufficient information start a planning phase for enforcing Content Awareness
  - Decide if you want to use an Ordered Layer or an Inline Layer policy
  - Consider creating informative UserCheck messages to educate users

Content Awareness
How you can propose it to customers

- The “Enforcement Approach”
  - Decide if you want to
    - Use a dedicated Ordered Layer performing Content Awareness
    - Add Content Awareness functionality to an existing Ordered Layer
    - Add Content Awareness to an existing Layer of a Unified Policy as Inline Layer
- Using dedicated policy layer allows
  - Reusing the layer in multiple policies
  - Being able to define **dedicated administrative roles** managing this layer
    - Doing so the security administration team is getting “help from the content team” managing the business security requirements
  - Reducing the complexity of the policy
  - **Use SmartEvent** functionalities obtaining visibility and generating reports

Content Awareness

How you can propose it to customers

- Please respect the legal framework that applies to data traffic control in your geographical region
  - You may need to engage human resources and workers council organizations before activating the functionality

Time	B...	Action	Type	..	Origin	Source	Destination	Service	Application Name	Data Type
25 Apr 17, 18:55:41		Drop	Session		gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	ContentDemo	Archive File
25 Apr 17, 18:55:27		Block	Session		gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	ContentDemo	PCI - Credit Card Numbers
25 Apr 17, 18:55:24		Accept	Session		gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	ContentDemo	Spreadsheet or CSV File
25 Apr 17, 18:55:21		Accept	Session		gwR8010	192.168.169.1	web+mailserver...	http (TCP/80)	ContentDemo	Document File

Extract from SmartConsole: Logs & Monitor

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.

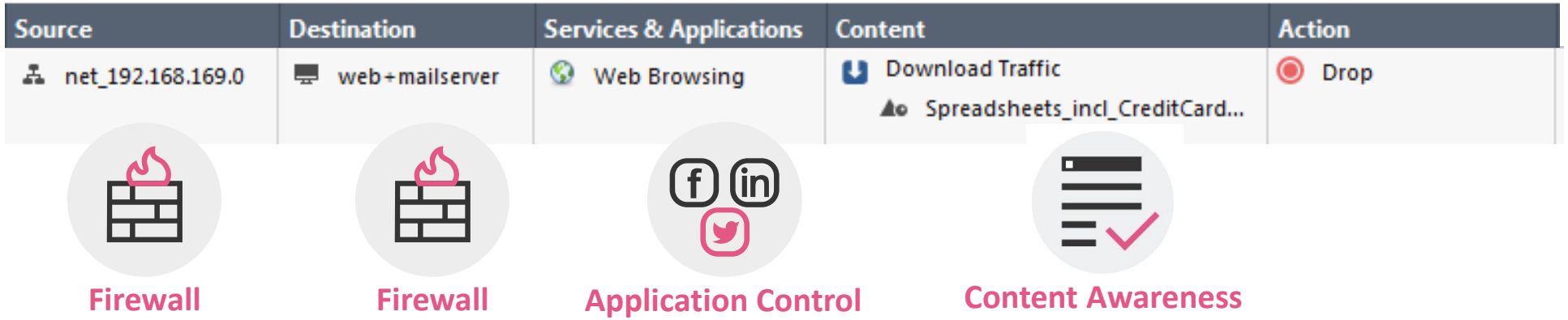
WHAT YOU WANT TO KEEP IN MIND

Content Awareness
What you want to keep in mind

- The Content Awareness Blade is enforcement engine is running the kernel
  - It is running in the fw_worker instance of CoreXL like any other NGTP/NGTPX Blade
- The matching is part of the Unified Policy matching process allowing you to achieve complex requirements

Example:

The rule will block downloading spreadsheets including credit card content from the web+mailserver using Web Browsing application when you are located in network 192.168.169.0



Content Awareness
What you want to keep in mind

- Controlling File Types and Content types, direction and the application transporting them

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)							

- Looking at the rules above we see that the application must be “Web Browsing” when accessing the destination “web+mailserver” to download spreadsheet files
- We don’t see the whole rule base but you can define a final cleanup rule to block any other application downloading content from “web+mailserver”

There is a lab about this example

Content Awareness – Monitoring Content

What you want to keep in mind

- This rule will not create any log message about the content

No.	Hits	Name	Source	Destination	Services & Applications	Content	Action	Track
1	0	Monitor rule	* Any	* Any	* Any	* Any	Accept	Extended Log Accounting

- For usability and performance reasons the “Any” object will not match on content
- This rule will log **any file content** traversing the gateway

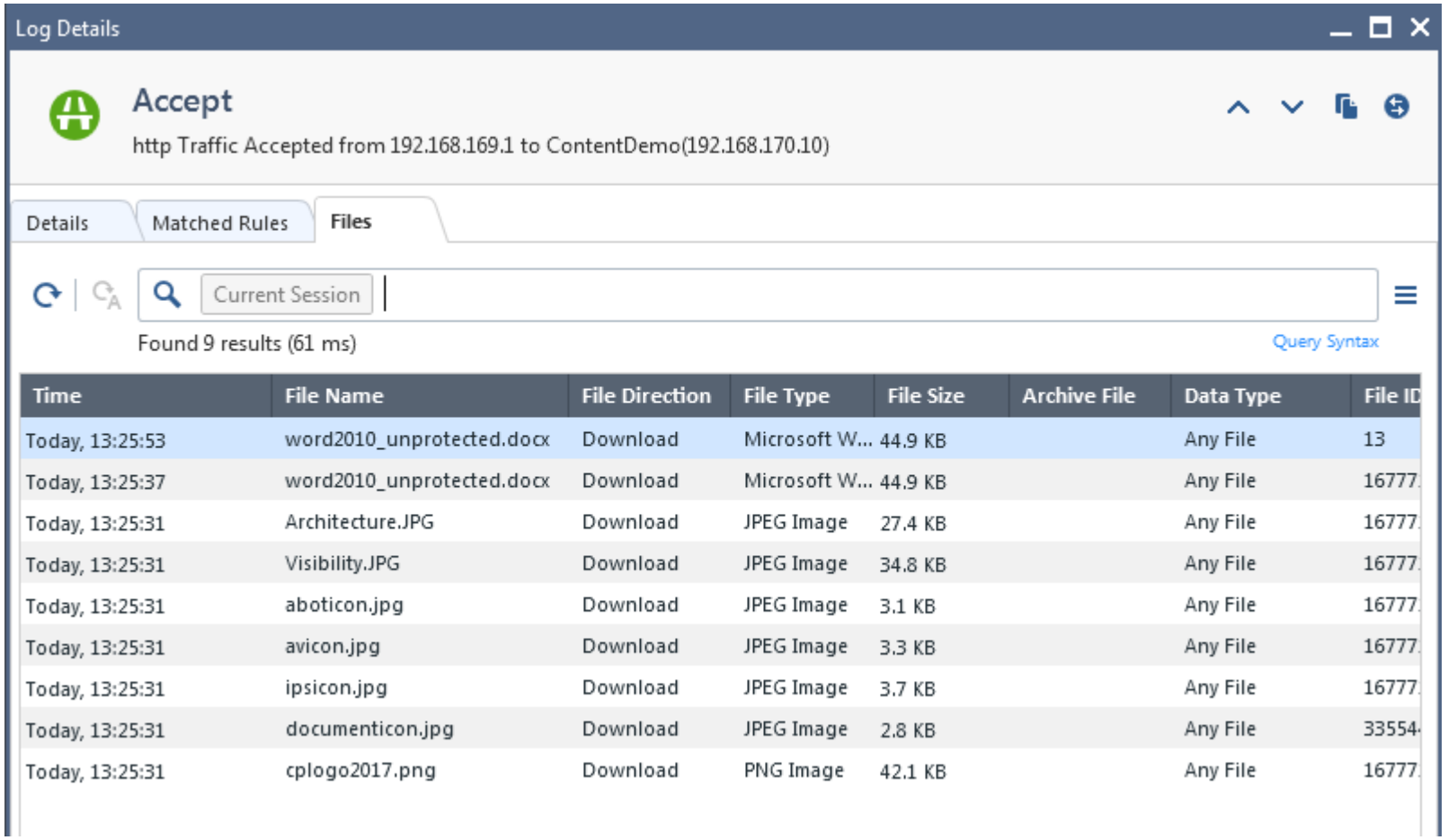
No.	Hits	Name	Source	Destination	Services & Applications	Content	Action	Track
1	202	Monitor rule	* Any	* Any	* Any	Any Direction Any File	Accept	Extended Log Accounting
Missing cleanup rule - Unmatched traffic will be accepted and not logged								

- If HTTP traffic will pass the gateway, web page elements will be noticed as files and you will get dedicated log messages

Content Awareness – Monitoring Content

What you want to keep in mind

- The “Any File” content object in combination with “Extended Log” logs all files including jpg used in the web page



Time	File Name	File Direction	File Type	File Size	Archive File	Data Type	File ID
Today, 13:25:53	word2010_unprotected.docx	Download	Microsoft W...	44.9 KB		Any File	13
Today, 13:25:37	word2010_unprotected.docx	Download	Microsoft W...	44.9 KB		Any File	16777
Today, 13:25:31	Architecture.JPG	Download	JPEG Image	27.4 KB		Any File	16777
Today, 13:25:31	Visibility.JPG	Download	JPEG Image	34.8 KB		Any File	16777
Today, 13:25:31	aboticon.jpg	Download	JPEG Image	3.1 KB		Any File	16777
Today, 13:25:31	avicon.jpg	Download	JPEG Image	3.3 KB		Any File	16777
Today, 13:25:31	ipsicon.jpg	Download	JPEG Image	3.7 KB		Any File	16777
Today, 13:25:31	documenticon.jpg	Download	JPEG Image	2.8 KB		Any File	33554
Today, 13:25:31	cplogo2017.png	Download	PNG Image	42.1 KB		Any File	16777

Content Awareness – Monitoring Content

What you want to keep in mind

When working with an Inline Layer with Content Awareness enabled:

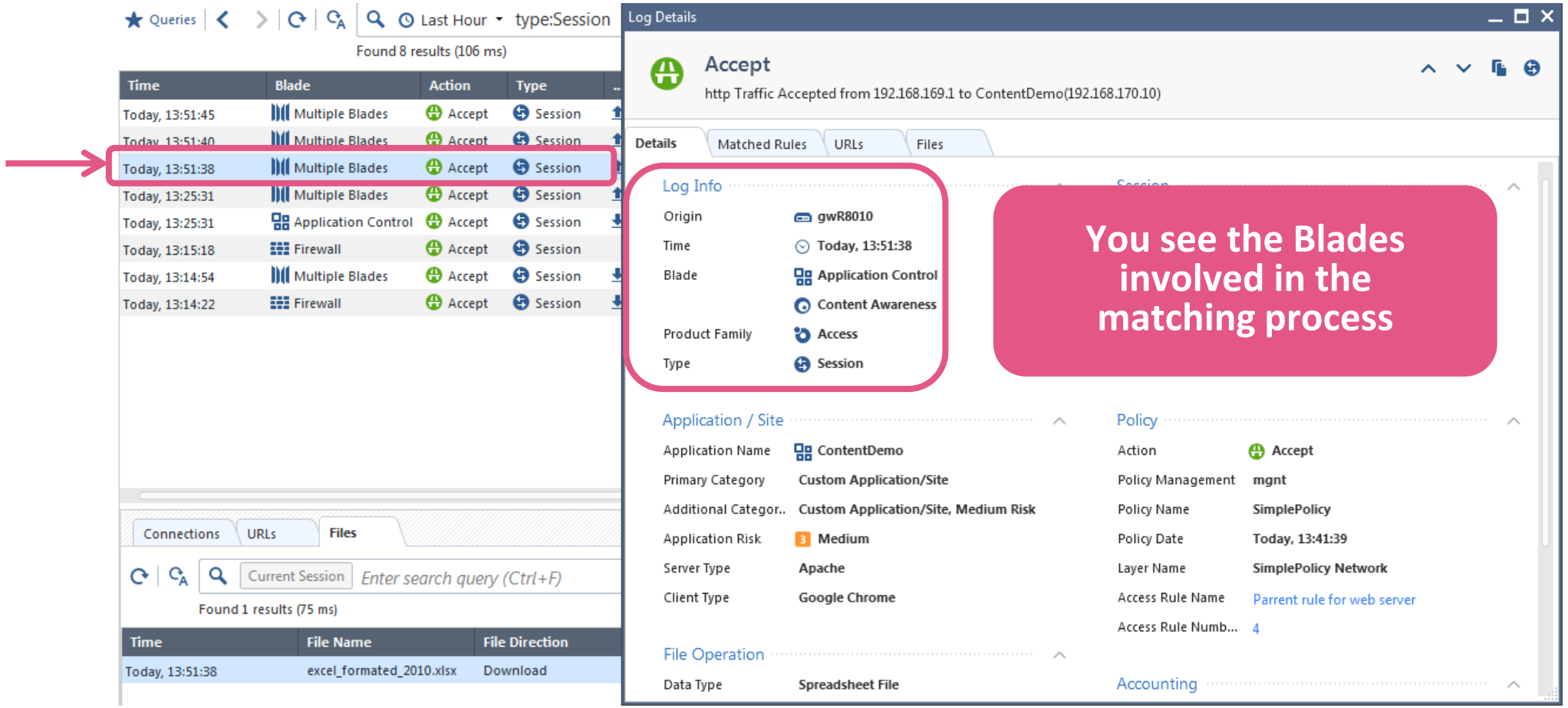
- Create specific rules monitoring content using “Extended Log” as track option
- Have a cleanup rule with “Any” object in the Content column and using “Log”
  - This will generate log information only for the content you are interested in

Content Awareness (11)							
11	Parent rule	InternalZone	PublishedServices	Web Browsing	Any	Content_Layer Network	N/A
11.1	Spreadsheets including credit card details	MonitorSources	ContentServers	Web Browsing	Download Traffic Spreadsheets including credit card details	Accept	Extended Log Accounting
11.2	Block credit card numbers in any other file or as text	MonitorSources	ContentServers	Web Browsing	Any Direction PCI - Credit Card Numbers	Drop Blocked Message -...	Extended Log
11.3	Documents	MonitorSources	ContentServers	Web Browsing	Upload Traffic Document File	Accept	Extended Log Accounting
11.4	Spreadsheets	MonitorSources	ContentServers	Web Browsing	Download Traffic Spreadsheet File	Accept	Extended Log Accounting
11.5	Last rule of Content Layer	Any	Any	Any	Any	Accept	Log
Outbound (12)							

Content Awareness – Monitoring Content

What you want to keep in mind

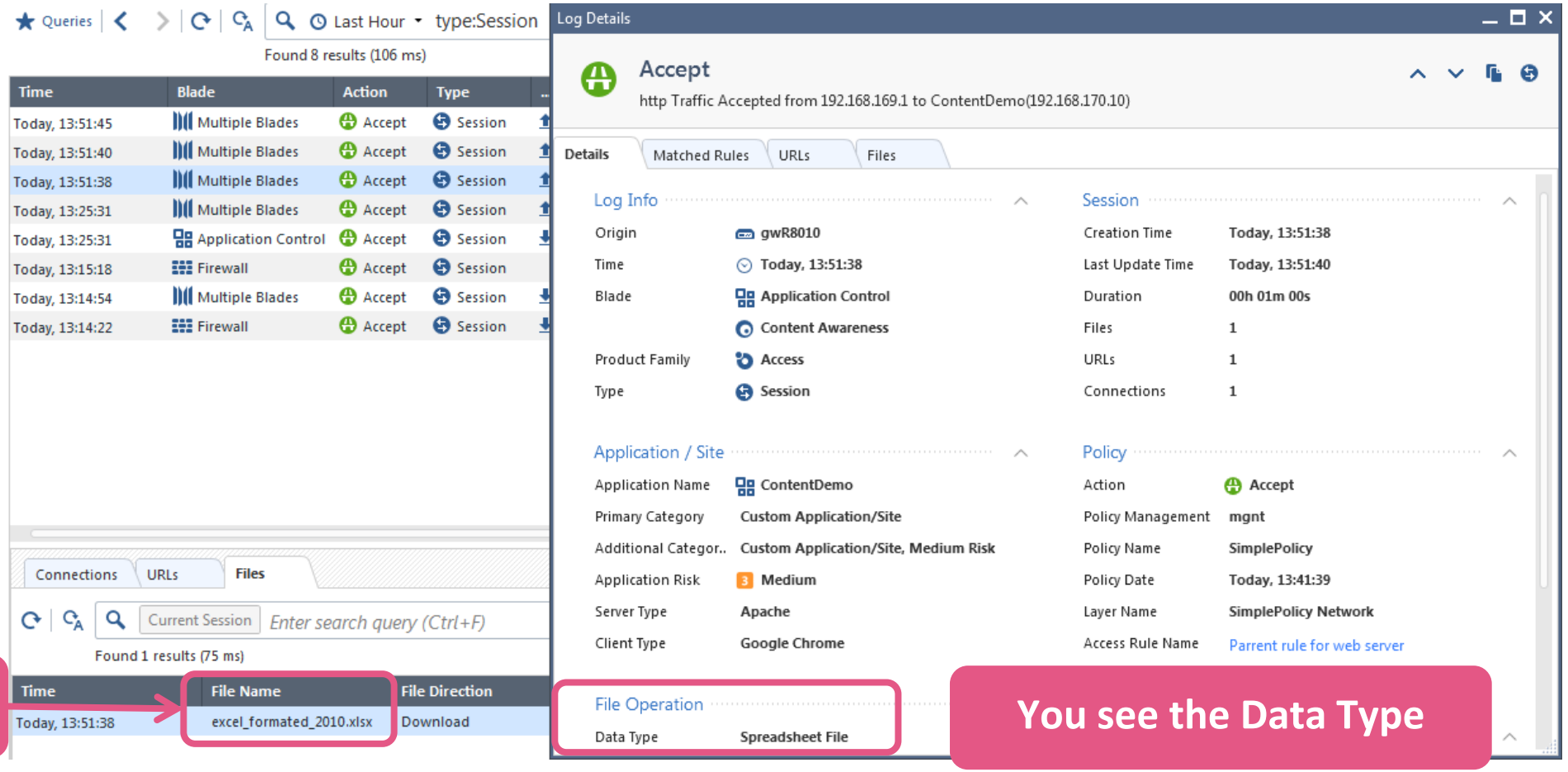
- You can now filter for “type:Session” and look at the log messages



Content Awareness – Monitoring Content

What you want to keep in mind

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

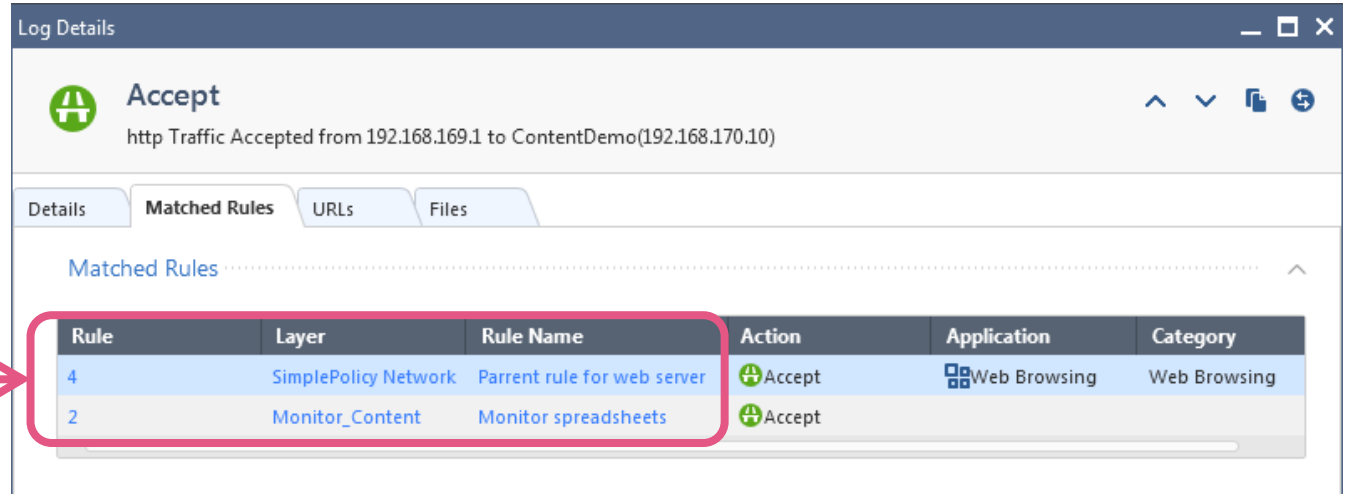


Content Awareness – Monitoring Content

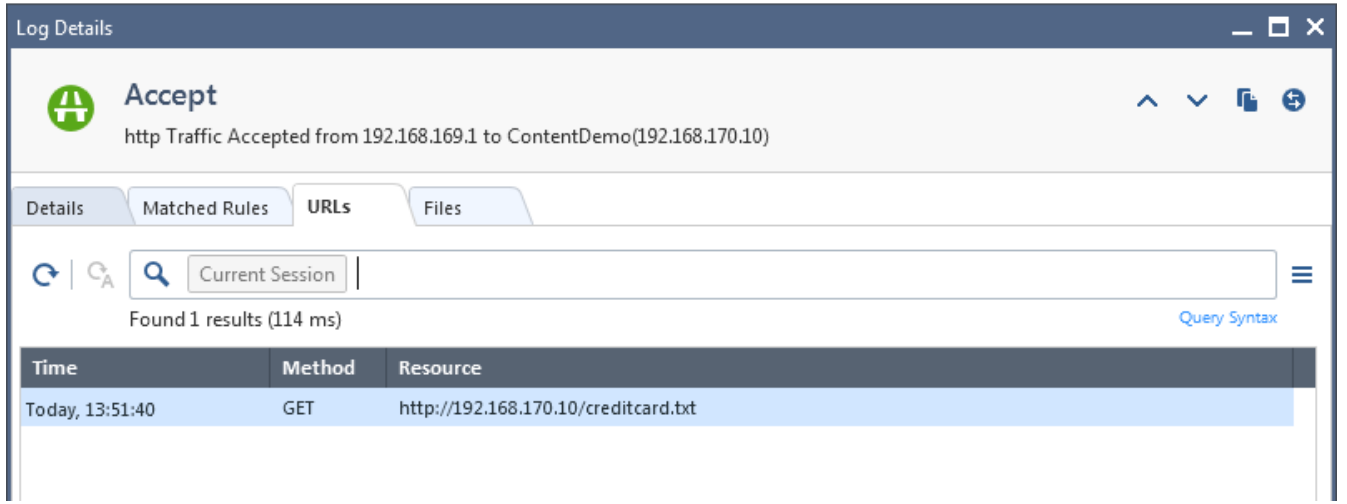
What you want to keep in mind

- You can see the rules that have matched

Rule number and Policy Layer



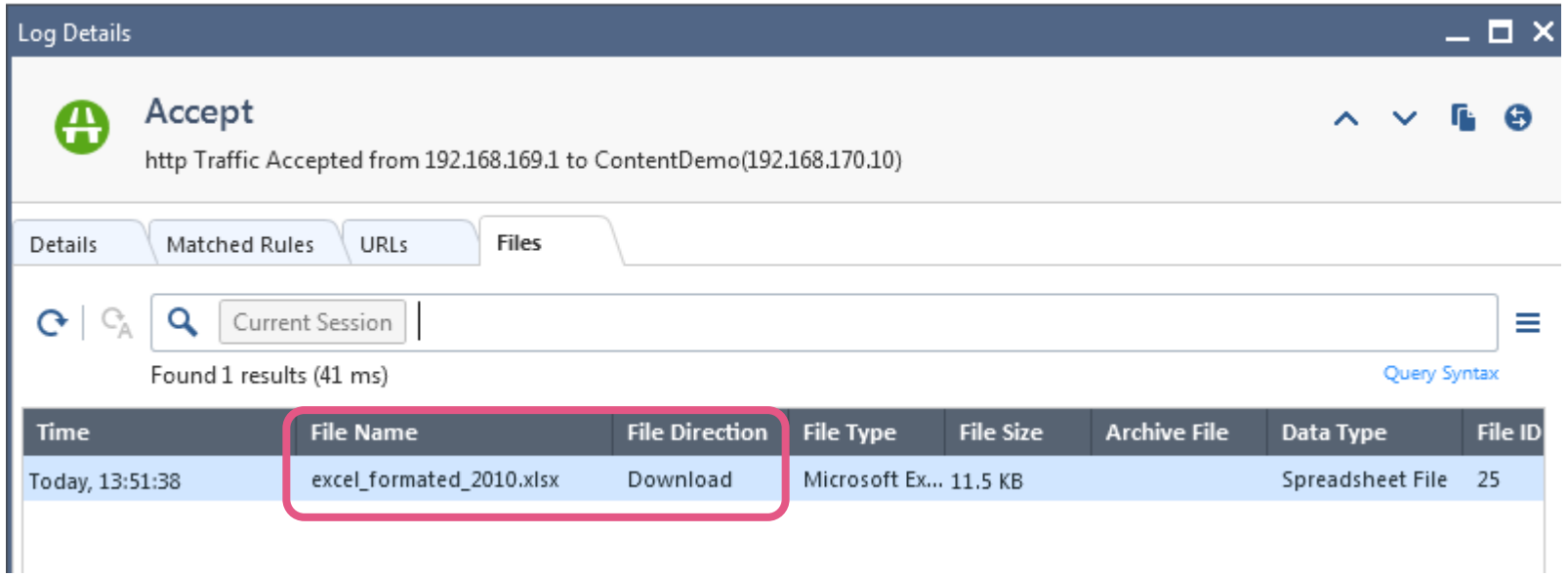
- You can see the URLs that have been accessed



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)



DETAILS ABOUT CONTENT TYPES

Content Awareness – File and Content Types

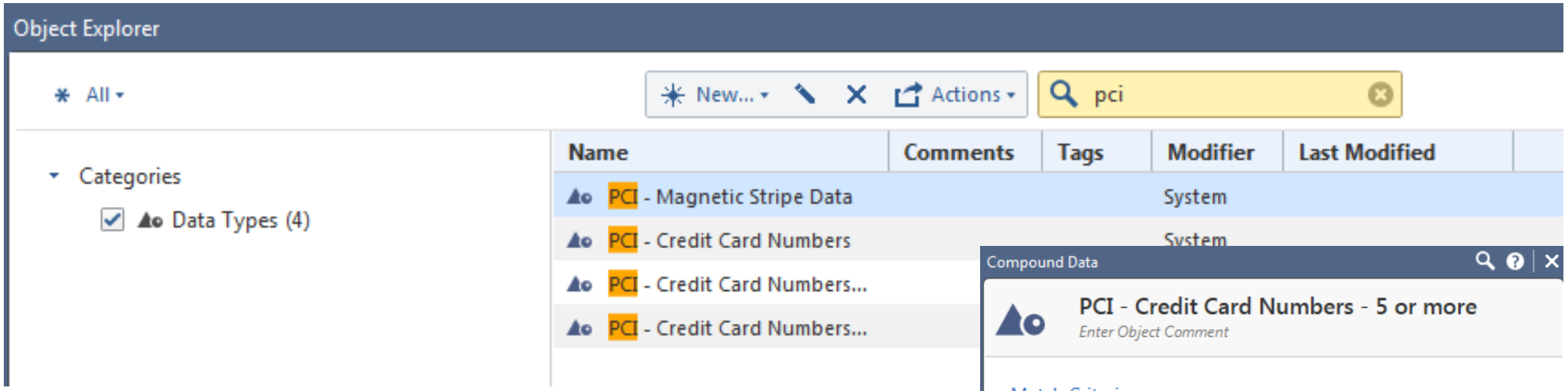
- Supported File and Content Types – sk114640
  - Detection is done locking at the beginning of the file
  - Some file types can be extracted from archives (check sk114640 for details)

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

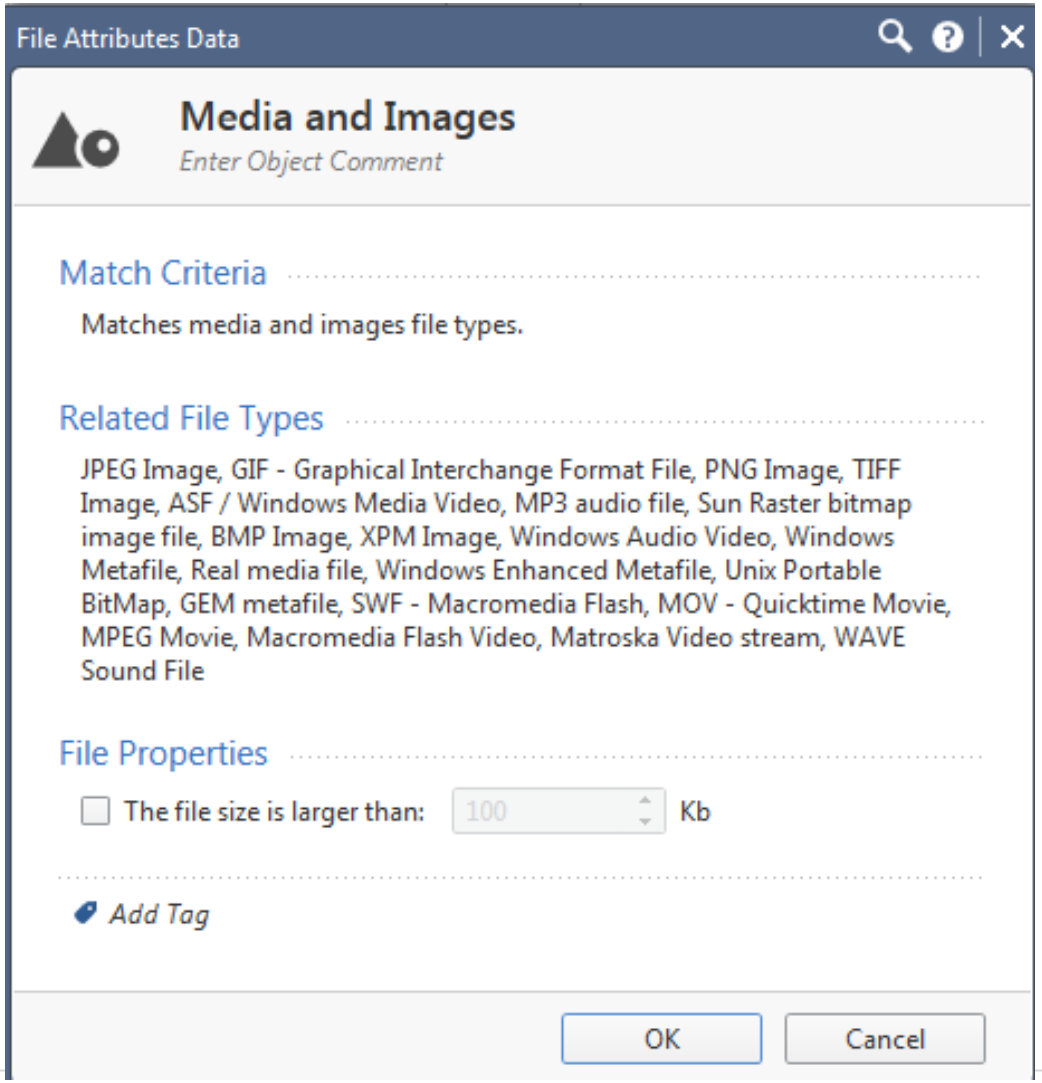
- Use the Object Explorer for getting an overview about file types and data types



- Use the right click and edit to see details

Content Awareness – File and Content Types

- Some Data Type objects are based on groups of file type like for example “Media and Images”
- You can create your own group of file types following the instructions in sk114935 “How to create a specific Data Type file in R80.10 Content Awareness blade”

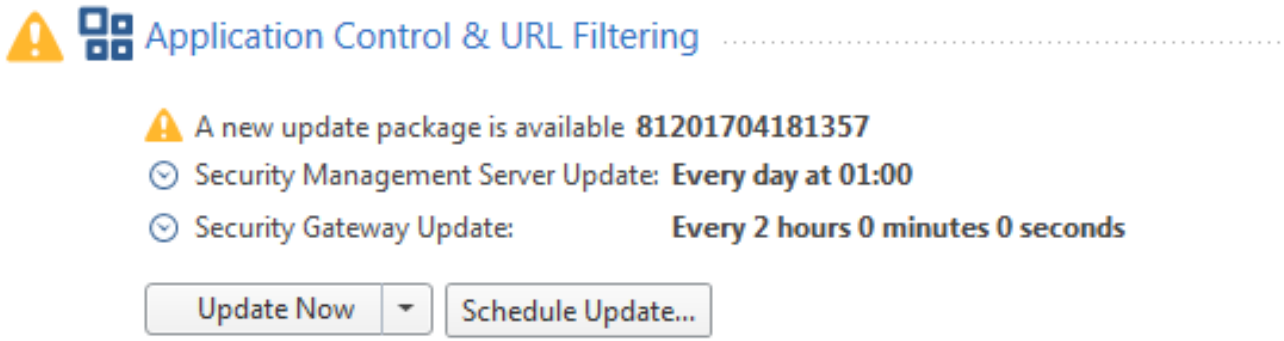


Content Awareness – File and Content Types

- Each file type has a default configuration what content action shall be applied to it
  - File Attribute and Content scan - scan file for its File Attributes and its content
  - File Attribute scan - scan file for its File Attributes only and ignore its content
  - Explicit scan - if rule match on 'Any' content and track level 'Detailed' or 'Extended' - don't log this file
  - Don't scan - ignore file
- These actions can be changed per file type following sk114954 “How to configure actions for a specific file type in R80.10 Content Awareness blade”
- In this way you can configure certain file types not to be scanned or not to be logged

Content Awareness – File and Content Types

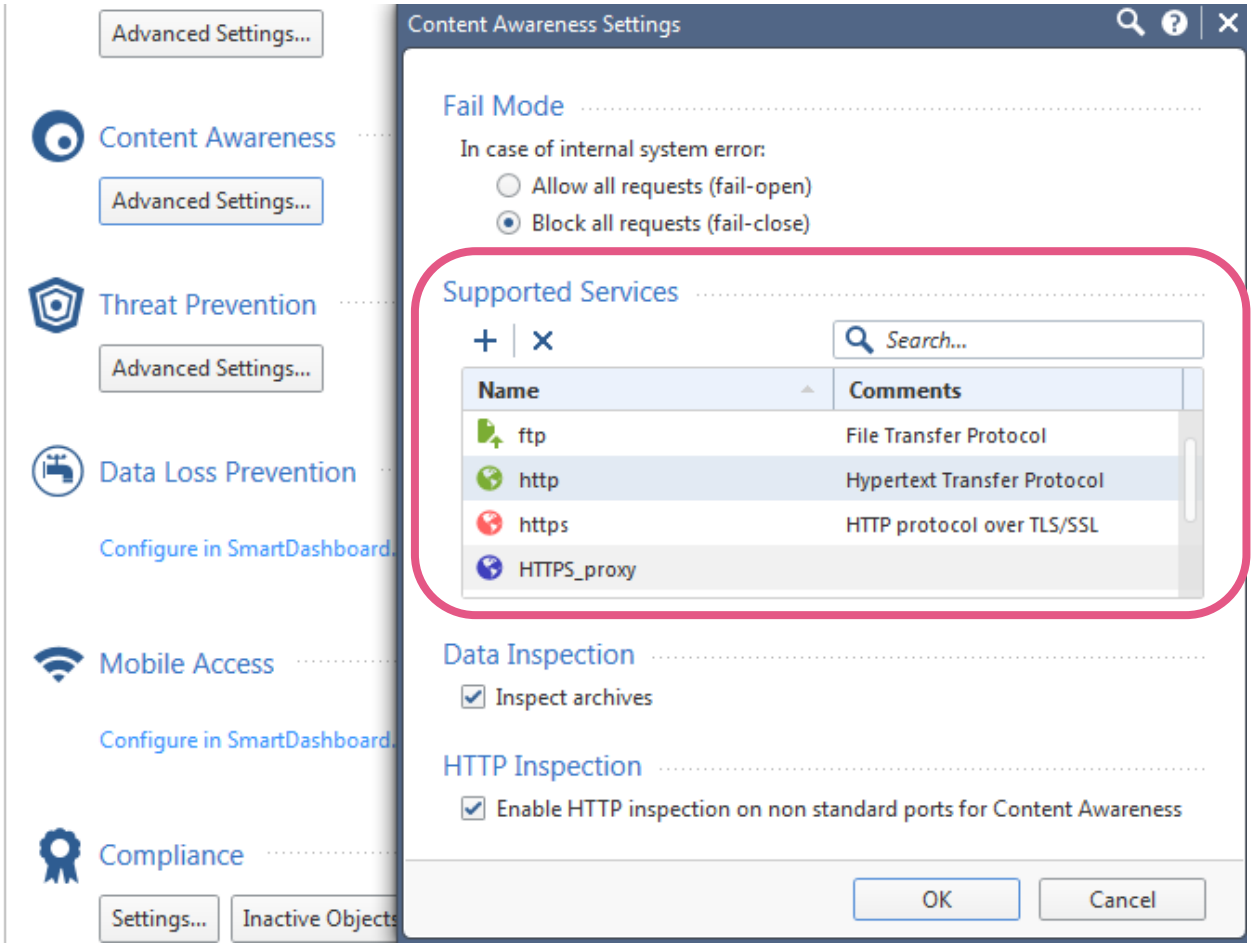
- Data types are updated from the cloud using the same process like Application Control
- Access Policy > Updates



- This process may change in the future

Content Awareness – Supported Services

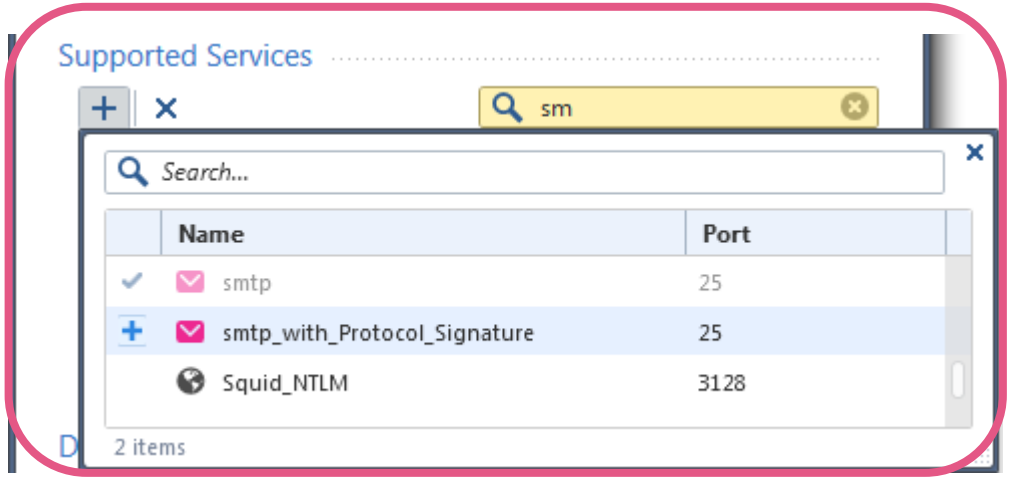
- You can see the services associated with the Content Awareness Blade in Manage & Settings > Blades > Content Awareness > Advanced Settings
  - Services are http, https, http_proxy, https_proxy, ftp and smtp.
  - You can add services that are based on http, https, ftp or smtp protocols
  - Currently 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.

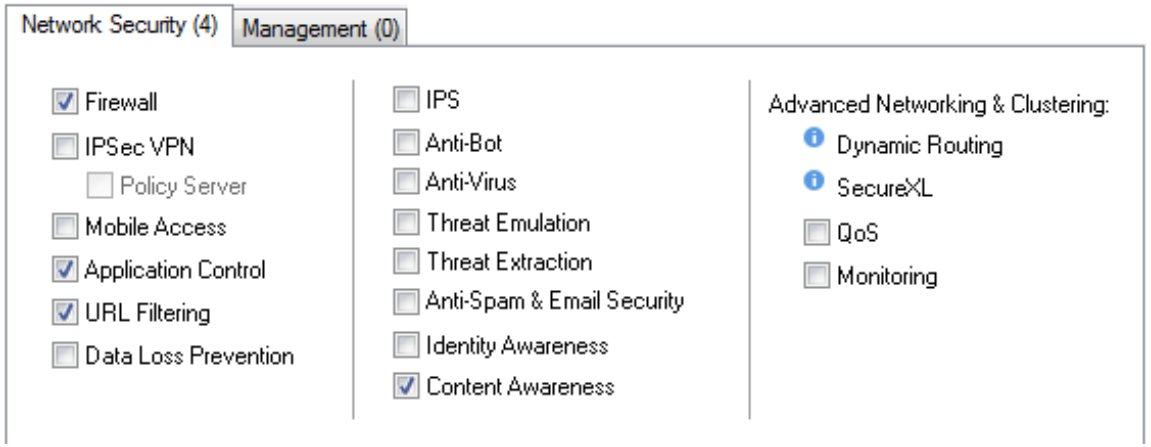
Content Awareness – Supported Services

- When you add a new service you will see all services listed that have protocol http, https or smtp defined.

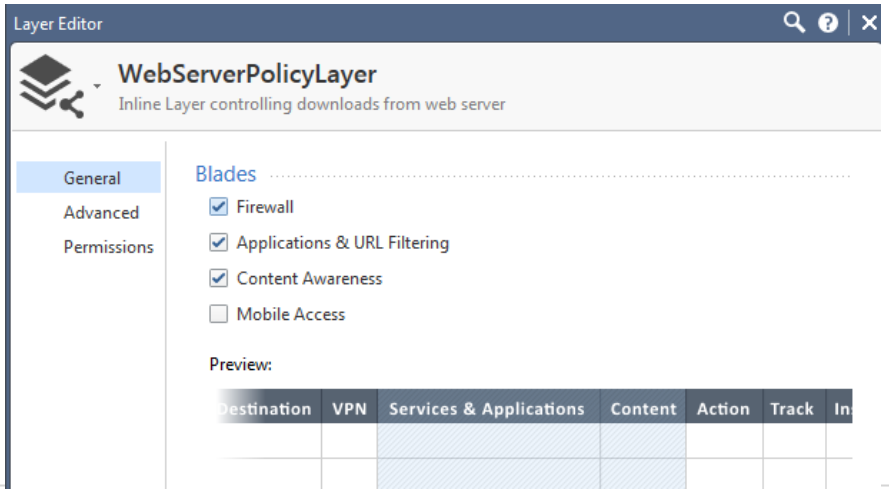


Content Awareness – Enabling the Blade

- 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 8th 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."

Summary

- Matching for Content Awareness is part of the Unified Rule Base matching process
- Content Awareness is a building block for a business aware security policy
- Ordered and Inline Layers are allowing to cover complex use cases
- Predefined content types can be used as they are and even grouped to achieve specific scenarios

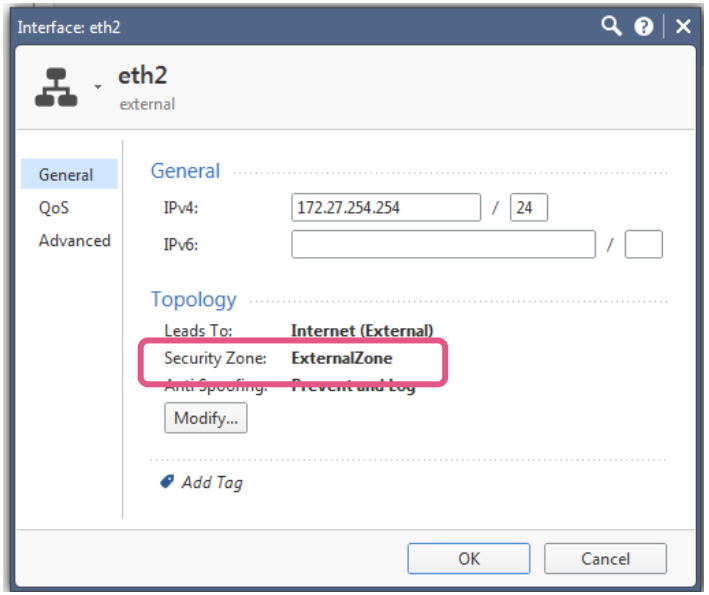
Check Point
SOFTWARE TECHNOLOGIES LTD

SECURITY ZONES

A method describing the topology

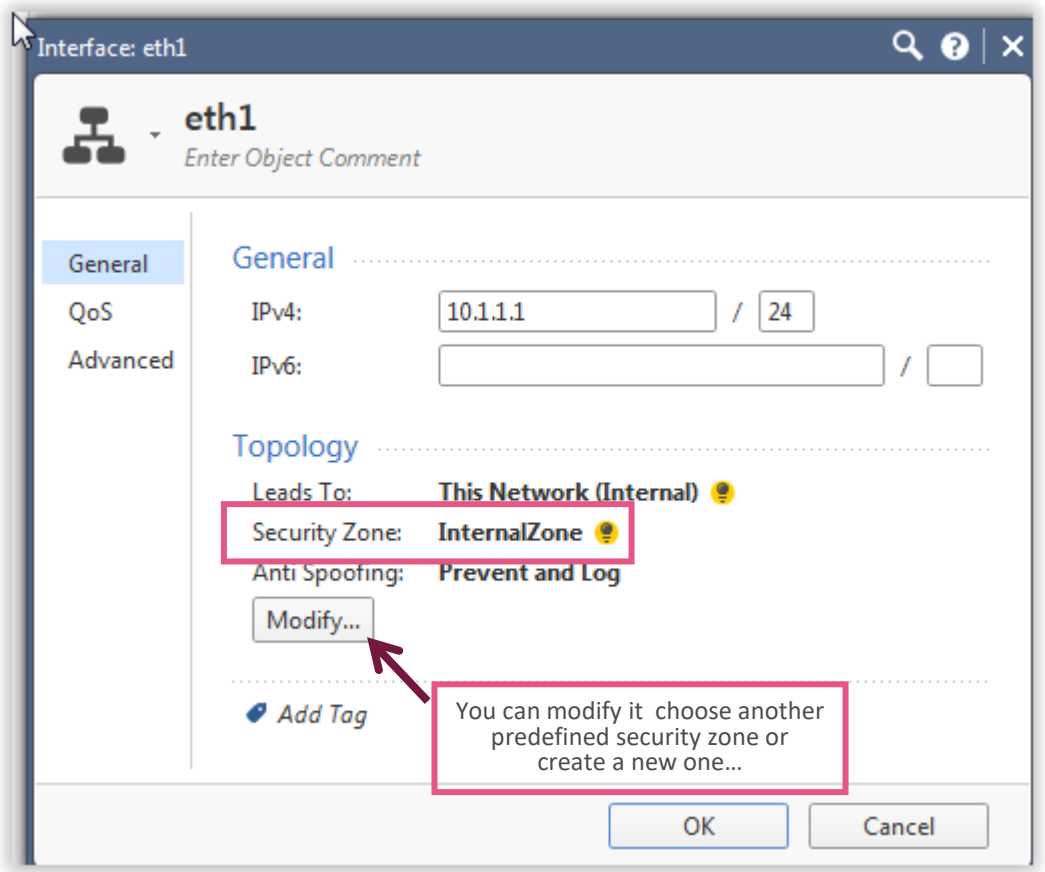
Security Zones – What they are

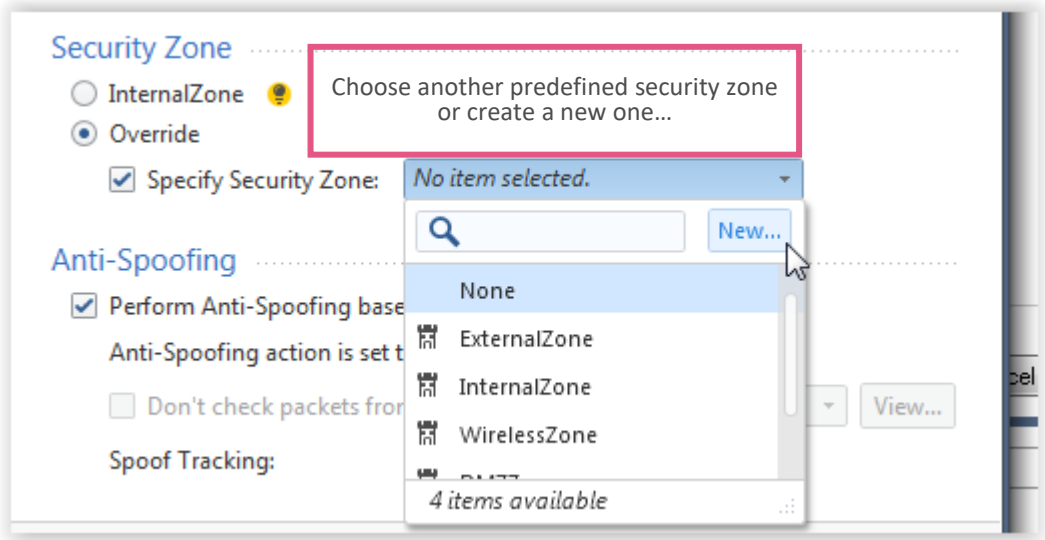
- Security zones are logical objects to which one or more network interfaces are associated used to define the network topology
- Benefits:
  - Simplified security policy where the same granular rule can be applied on many gateways
  - Allows the administrators to add internal networks without updating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



Security Zones – How you can use them

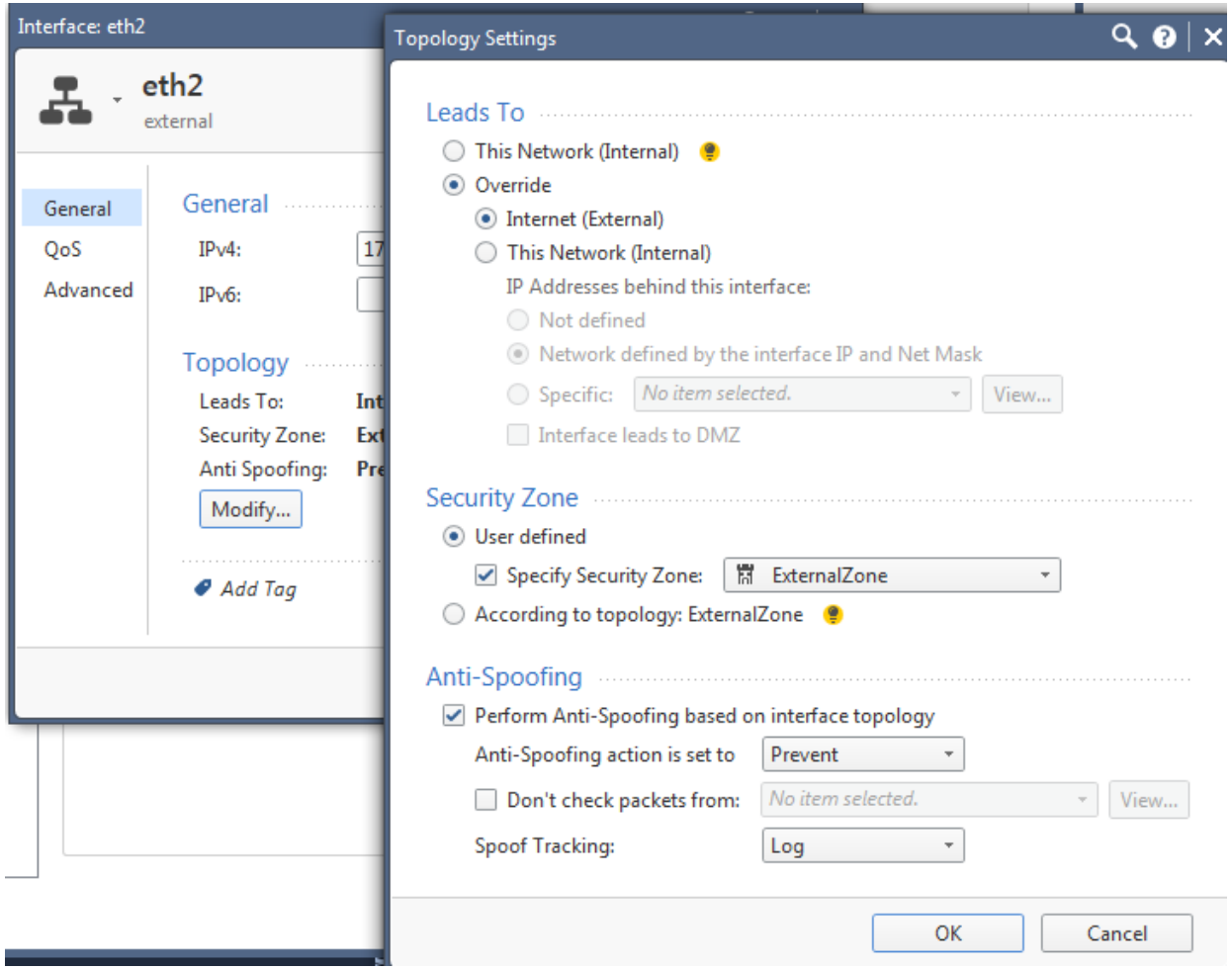
- Set the security zone on the interface





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



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	dnsserver OpenDNS	Any	dns	Any	Accept

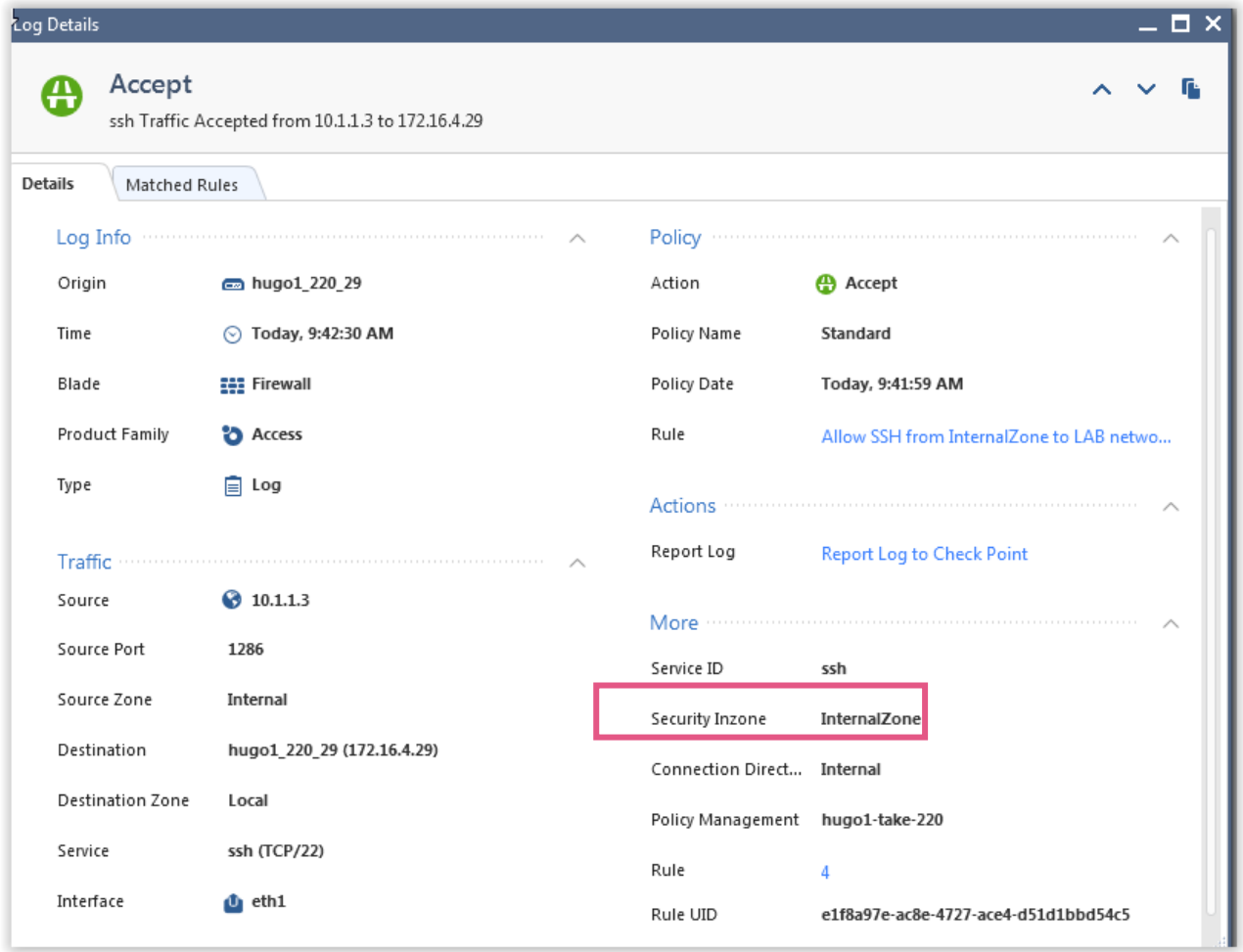
- You can use Security Zone objects as well in Threat Prevention rules

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 uses them

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



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

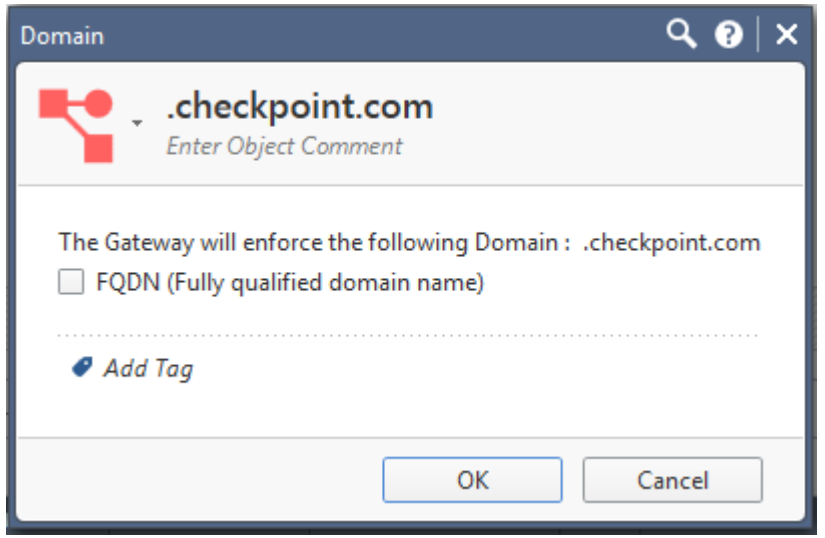
REGULAR MODE

How to describe a Domain as an object?

Working with R77.30 based security gateways.

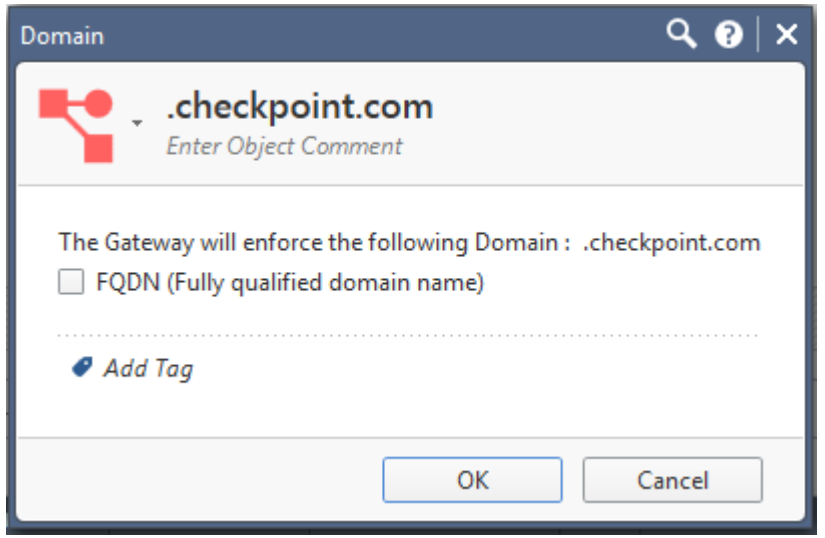
Domain Object – Regular mode

- Regular mode (supported in older gateway versions)
  - Will match checkpoint.com 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.



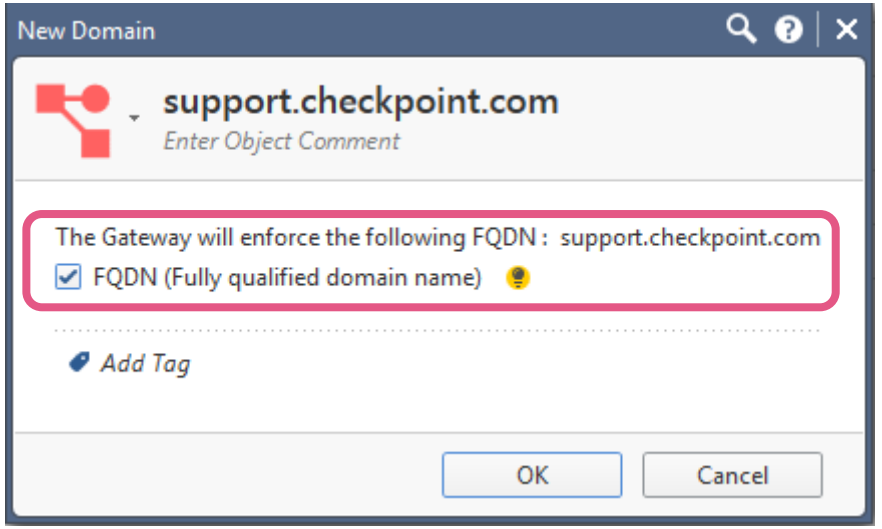
FQDN MODE

The new Domain Object based on “FQDN mode”

Overcoming incumbent challenges with Dynamic Objects and performance obstacles.

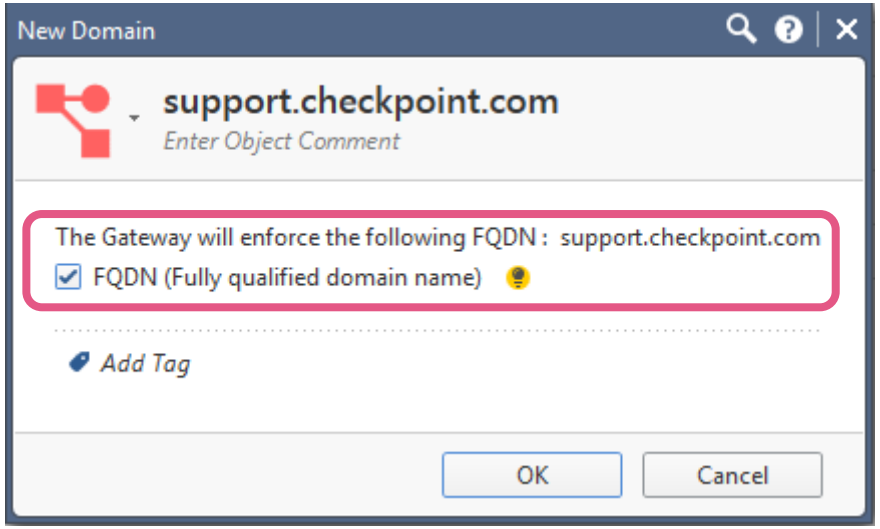
Domain Object - FQDN mode (recommended)

- 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



Domain Object - Acceleration

- Both Domain object modes support accept templates
  - In previous versions, accept templates are disabled starting from the first rule that uses domain objects



Domain Object - Kernel Configuration Parameters

rad_kernel_domain_cache_refresh_interval

- default 30 seconds
- A refresh interval for resolving domain objects from the policy

rad_kernel_domain_cache_name_lookup_timeout

- default 3600 seconds (1 hour)
- An IP resolved directly from a domain object in the policy will enter to the cache for 1 hour.

Domain Object - Kernel Configuration Parameters

rad_kernel_domain_cache_ip_success_lookup_timeout

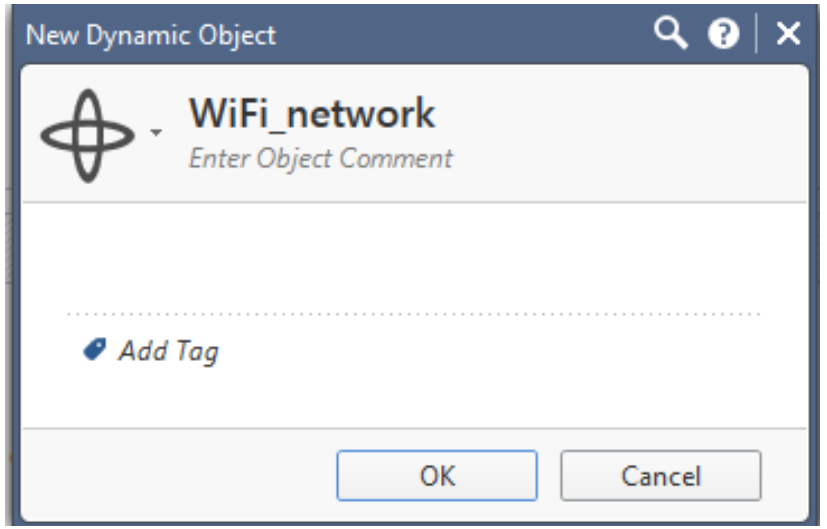
- default 7200 seconds (2 hours)
- A reverse resolved IP that is matched to one of the domain objects will enter to the cache for 2 hours.

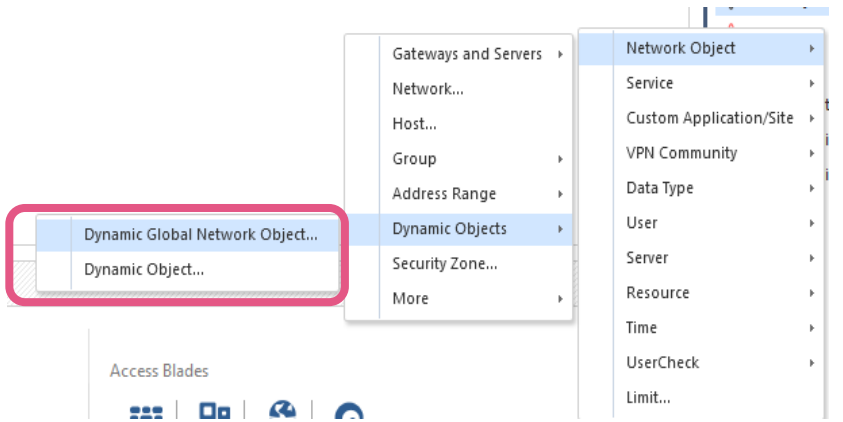
rad_kernel_domain_cache_ip_negative_lookup_timeout

- default 600 seconds (10 min.)
- A resolved IP that is NOT matched to any of the domain objects (or that get an error response from the DNS) will enter to the unmatched_cache for 10 minutes.

Dynamic Objects

- A Dynamic Object is a logical object, where the IP address is resolved differently for each gateway using the `dynamic_objects` CLI command
- In R80.10 Dynamic Objects are supported by SecureXL Connection Acceleration templates
  - In earlier versions all rules below a rule including a Dynamic Object did no longer benefit from SecureXL Connection Acceleration
- Dynamic Global Network Objects can be created in Multi-Domain Management environments





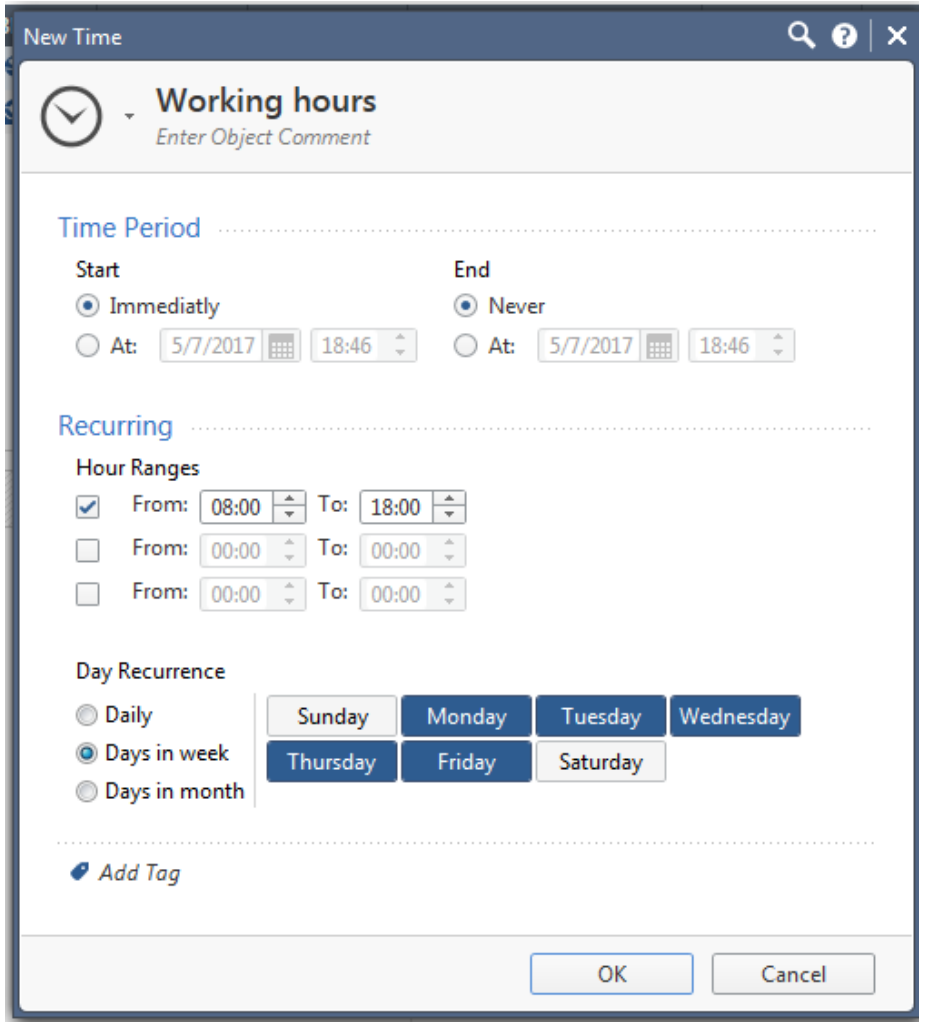
Time Objects

- 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



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

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

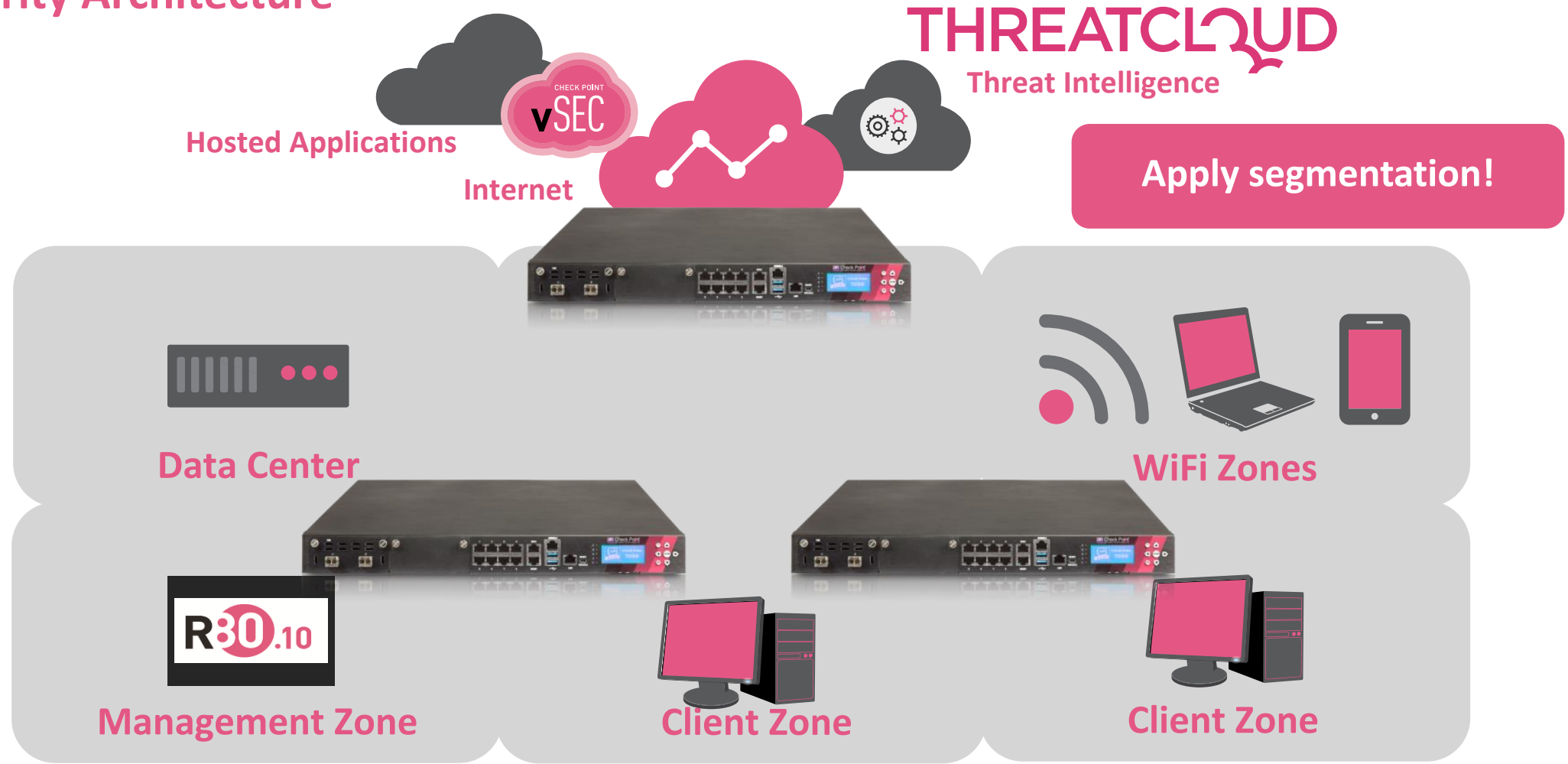
Preventing Threats By Architecture
Overview of the NGTP Software Blades

- 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

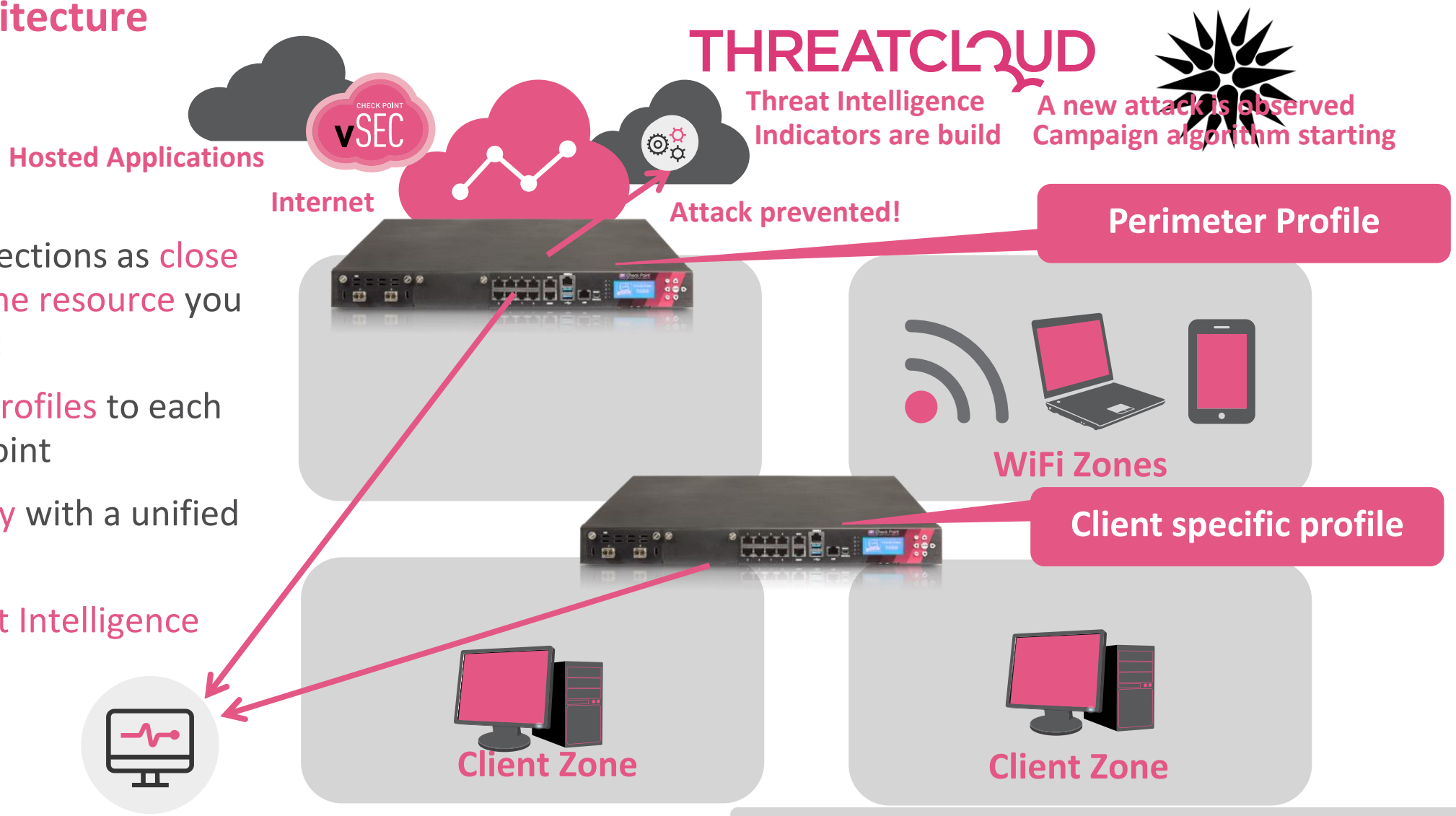
Security Architecture



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

Integrating Threat Prevention
Security Architecture

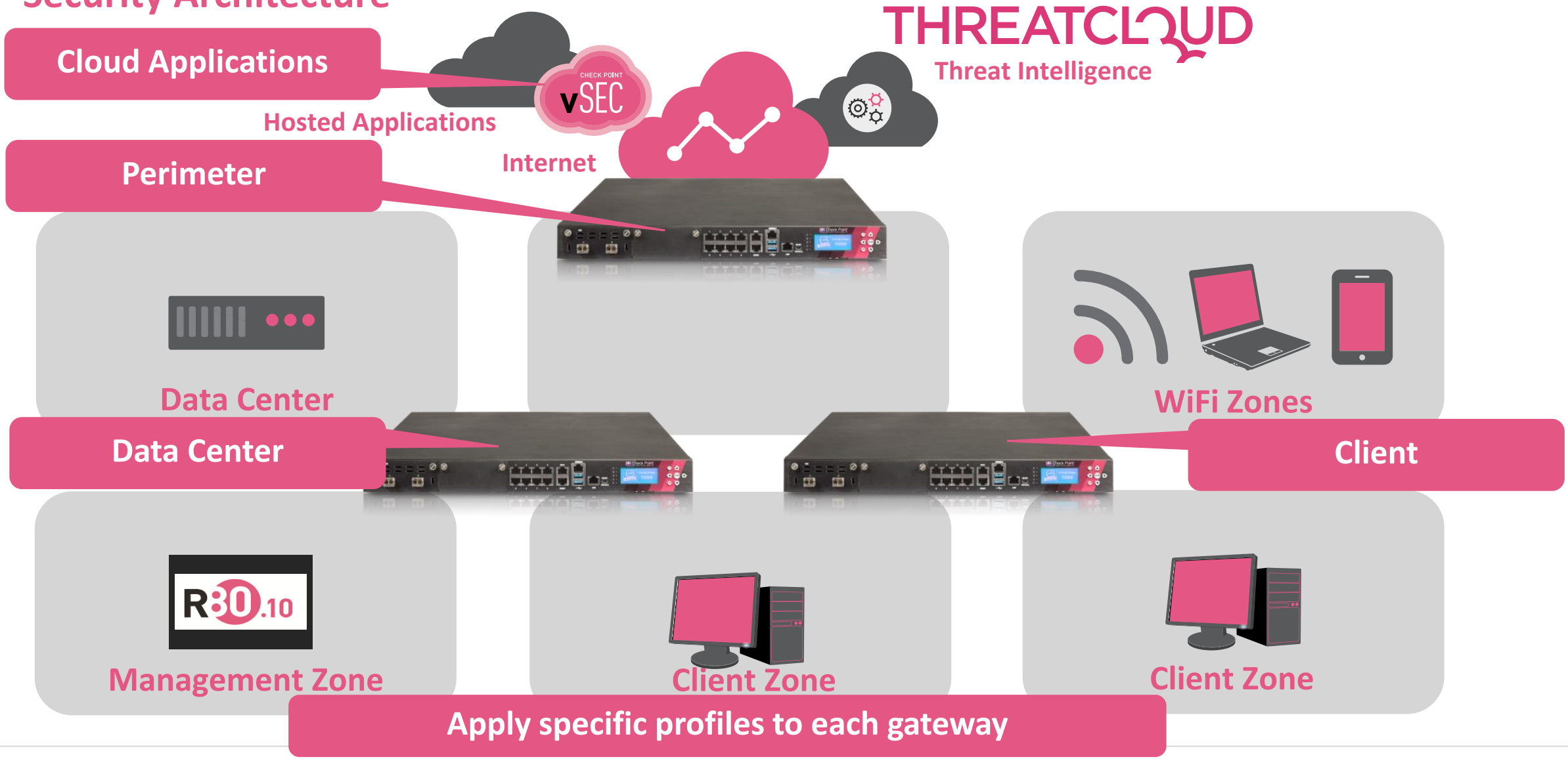
- Place your protections as close as possible to the resource you want to protect
- Apply specific profiles to each enforcement point
- Achieve visibility with a unified management
- Leverage Threat Intelligence



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!

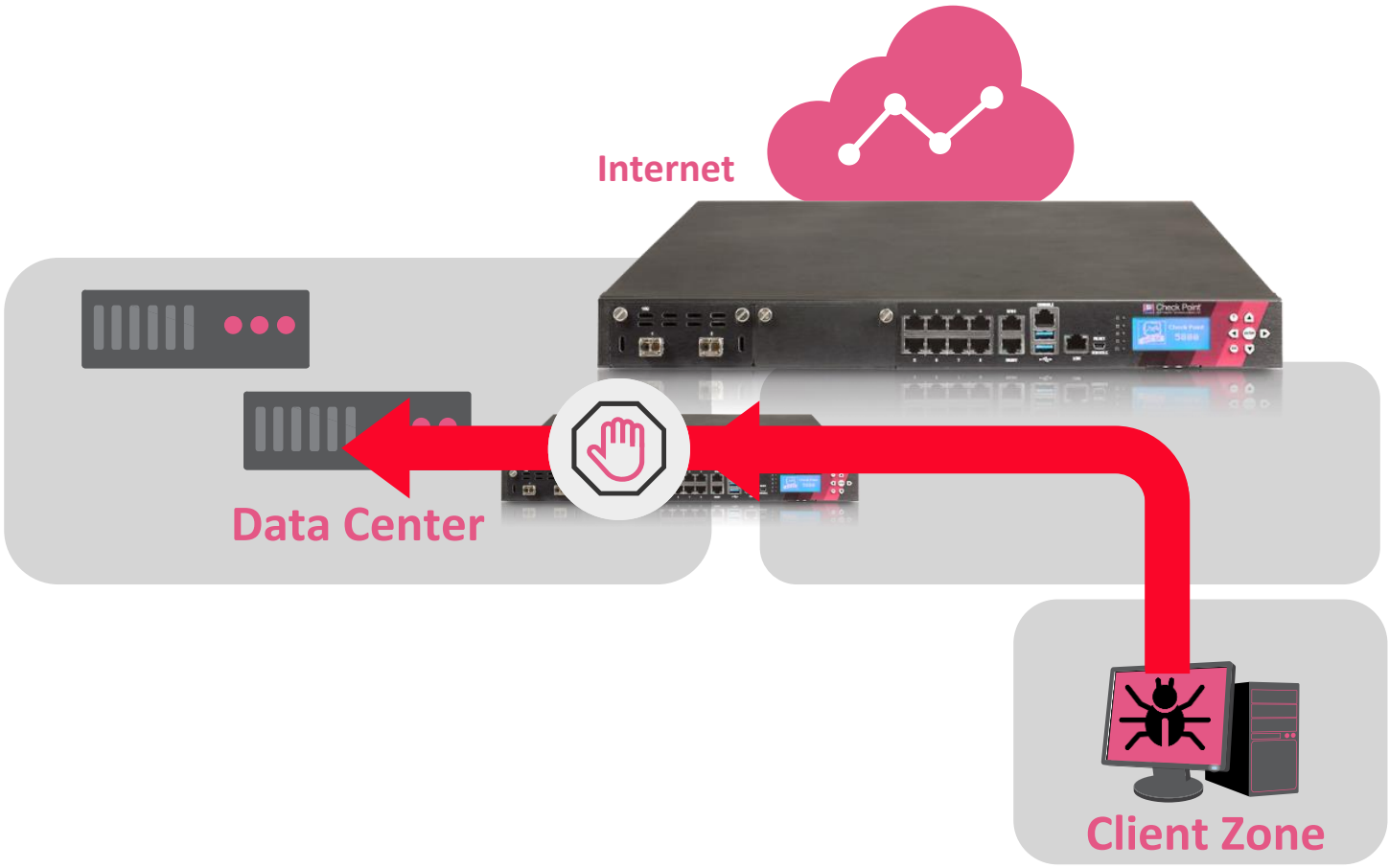
Remember that a recent Ransomware attack

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

Check Point
SOFTWARE TECHNOLOGIES LTD

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			
Ransomware Shared Folder Access	None	30/08/2016	14/05/2017			
PDF File Containing Ransomware Downloader	None	21/05/2017	28/05/2017			

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

Ransomwares access shared folder in order to encrypt files. Successful exploitation might lead to loss of sensitive data.

No Industry Reference – Released 30th Aug 2016 – Updated 14th May 2017

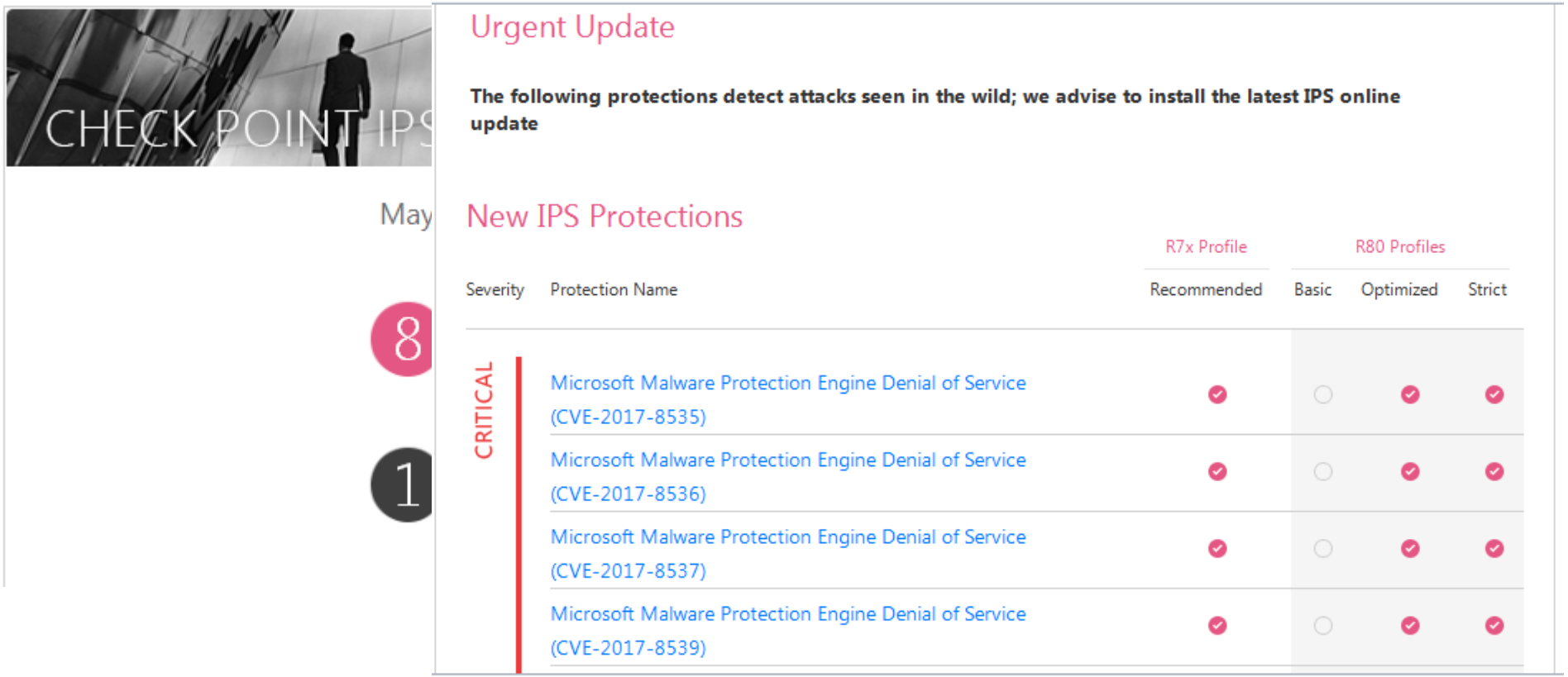
We are innovative – we started early – we don't stop improving

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

IPS Protections Update Service

Keep yourself and customers informed

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

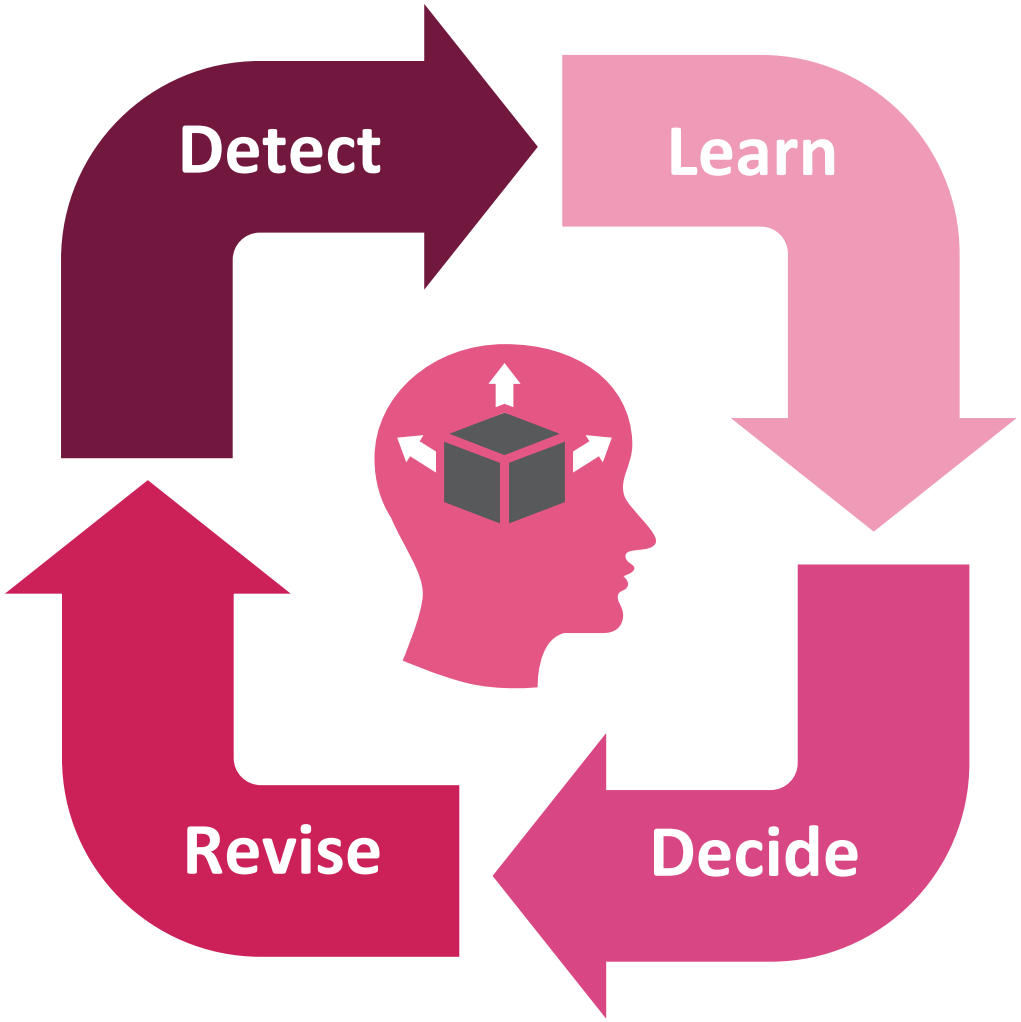


Subscribe to: https://www.checkpoint.com/advisories/

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

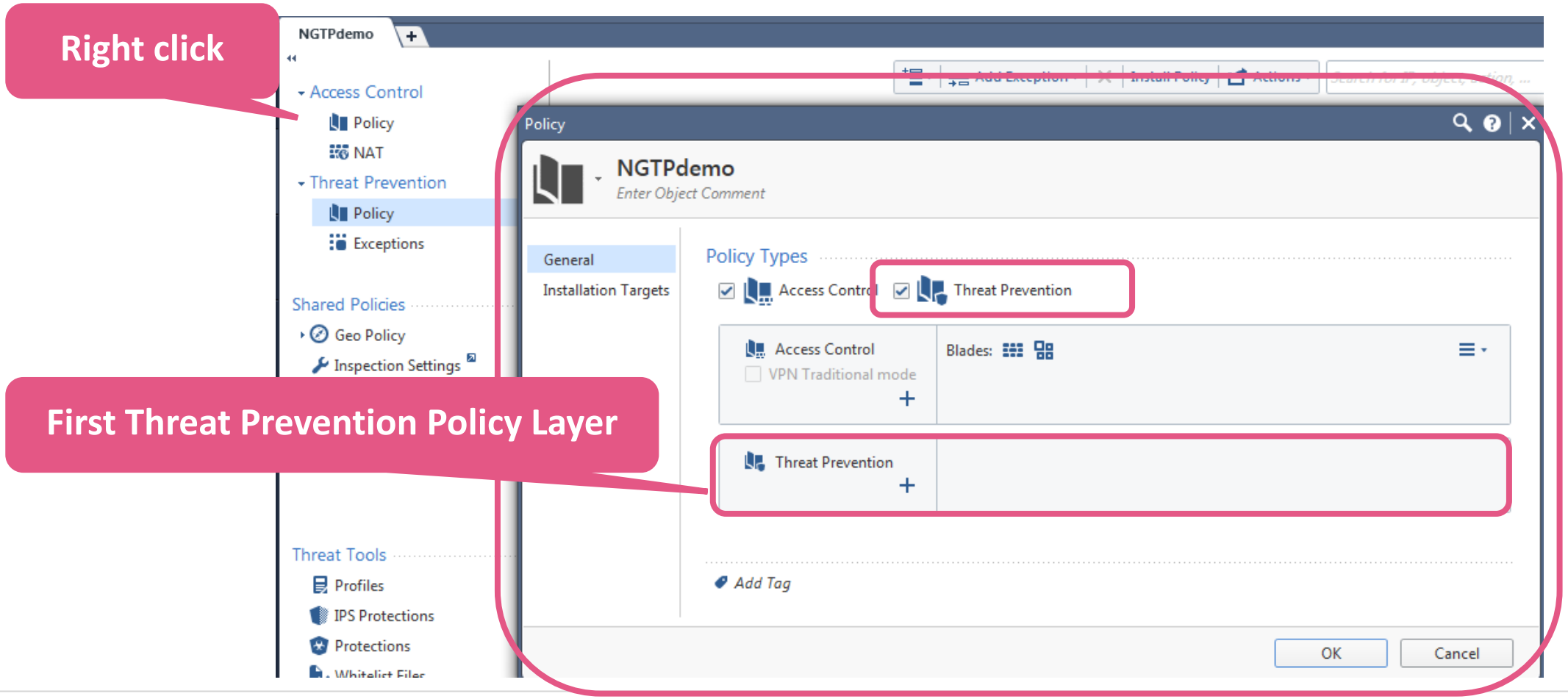
Understanding The Components

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)

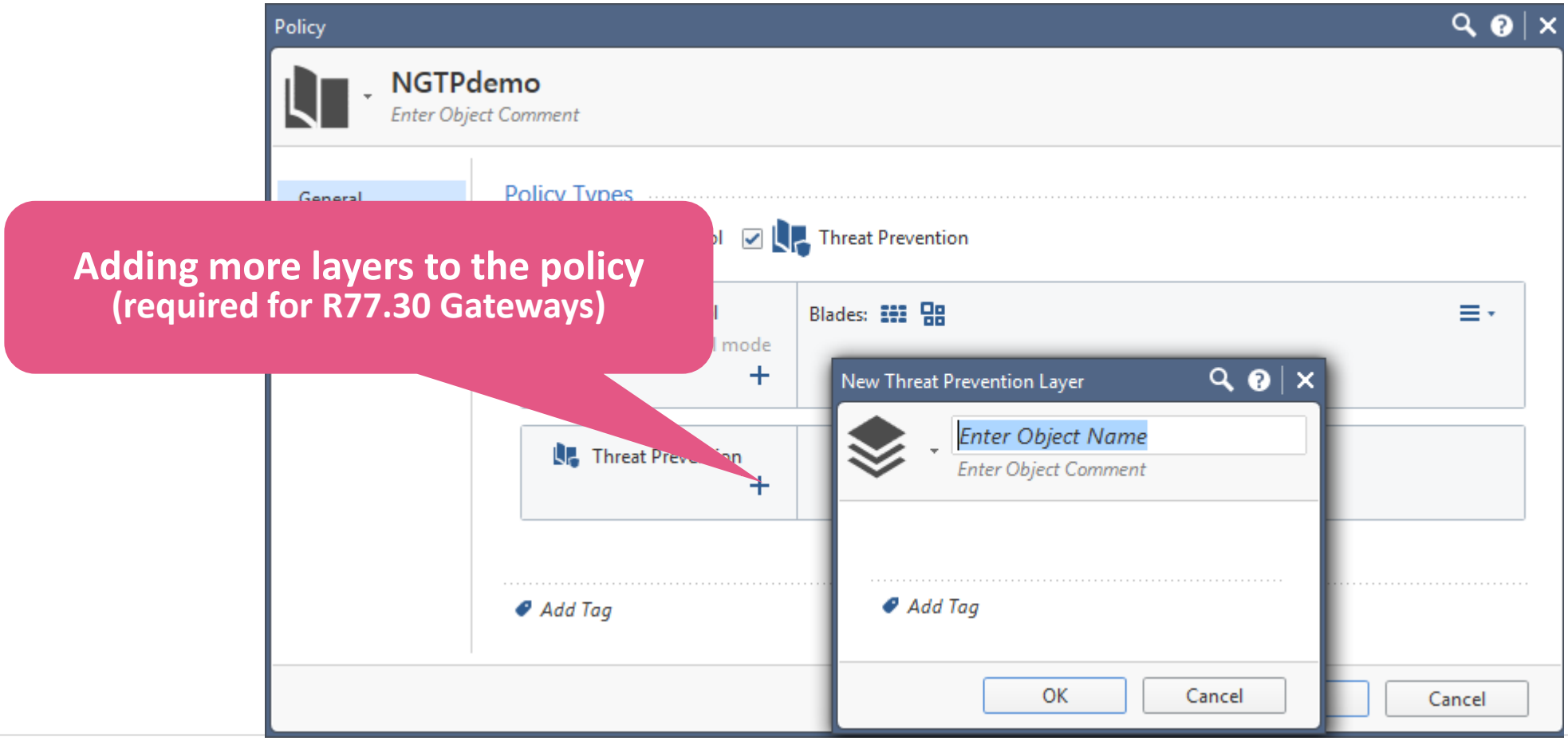
Understanding The Components
Threat Prevention Policy Layers

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



Understanding The Components
Threat Prevention Policy Layers for R77.30 Gateways

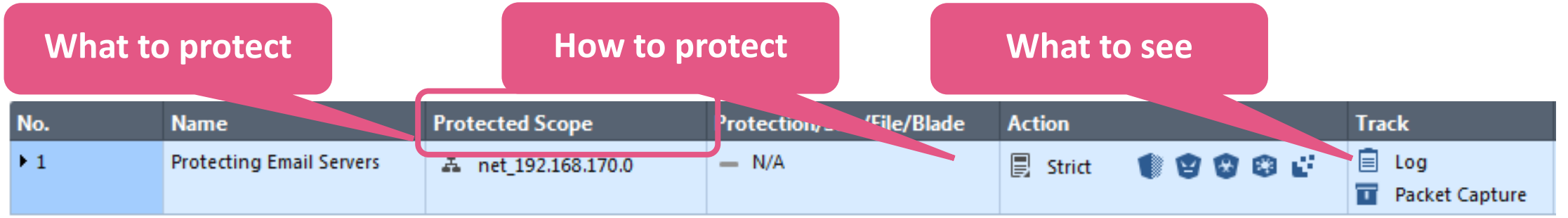
- Each layer will have it's own rule base



Understanding The Components

Threat Prevention Policy Rule Base using Protected Scope structure

- Threat Prevention policy rule using Protected Scope object



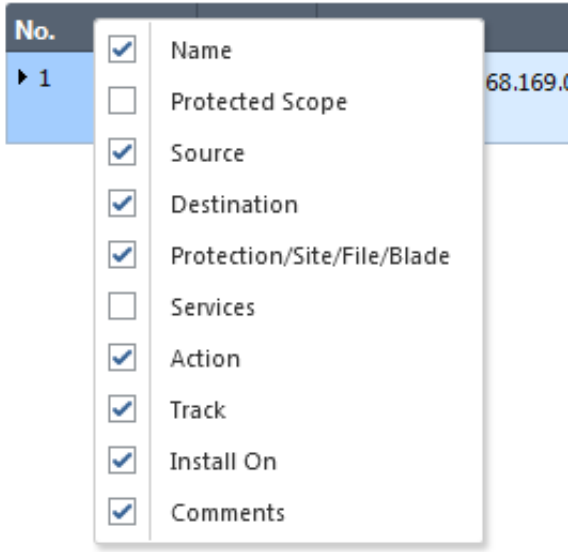
- Protected Scope
  - The network or zone we want to protect
- Action
  - The profile that will be applied to traffic directed to the Protected Scope
- Track
  - Packet capture will be performed for the first match of a signature but not for suppressed logs

Understanding The Components

Threat Prevention Policy Rule Base using Source and Destination structure

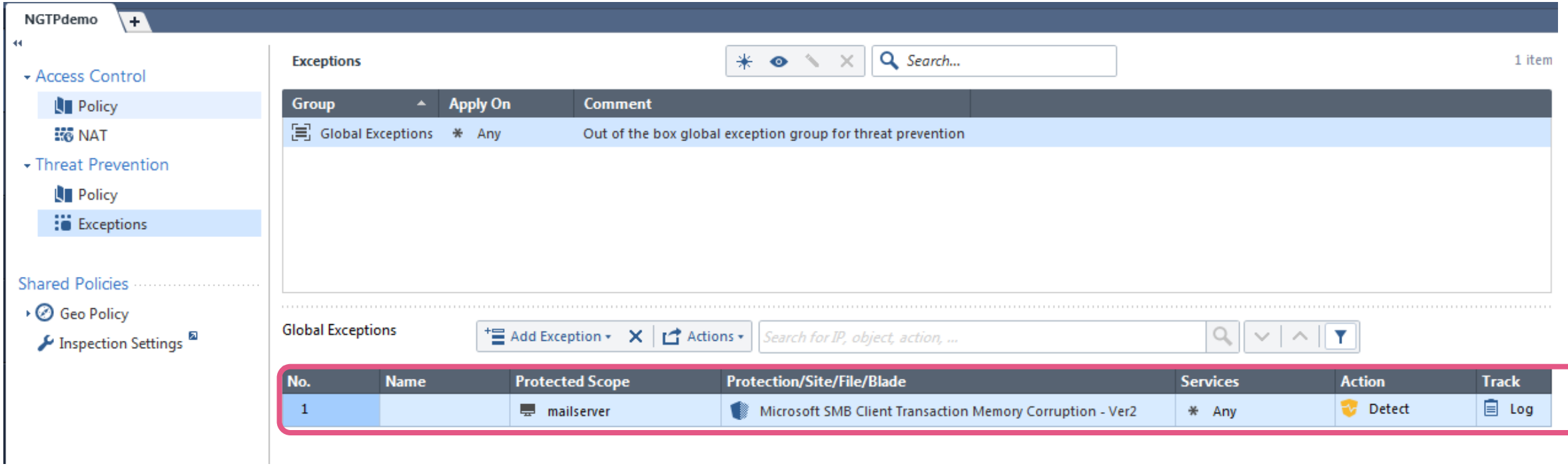
- Threat Prevention policy rule using source and destination objects

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



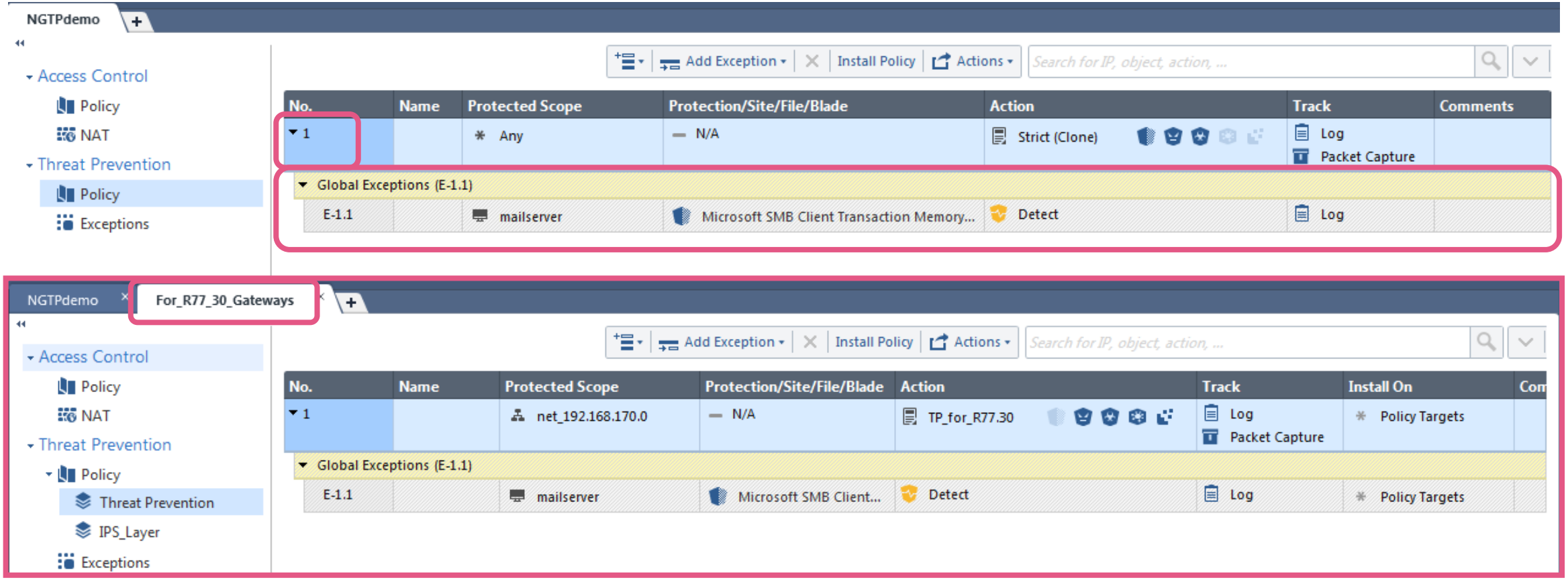
Understanding The Components
Threat Prevention Policy Rule Base – Global Exceptions

- Global Exceptions apply to all Threat Prevention policies



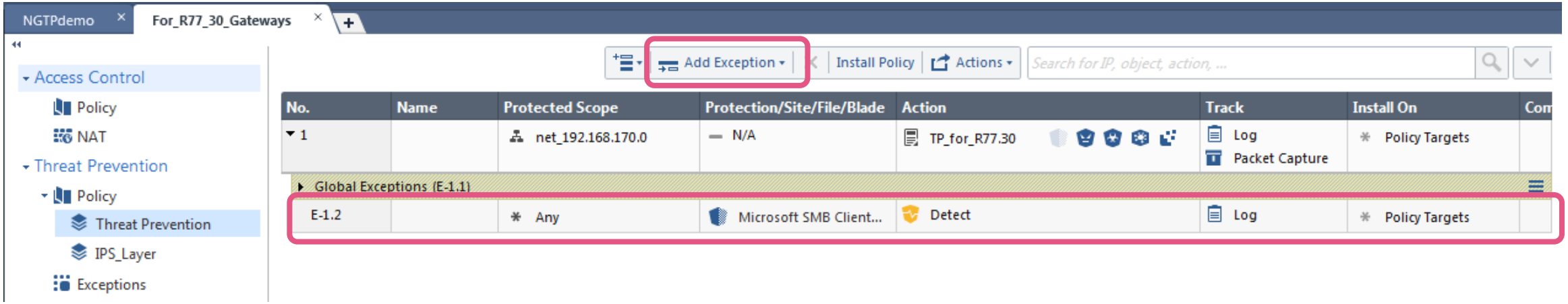
Understanding The Components
Threat Prevention Policy Rule Base – Global Exceptions

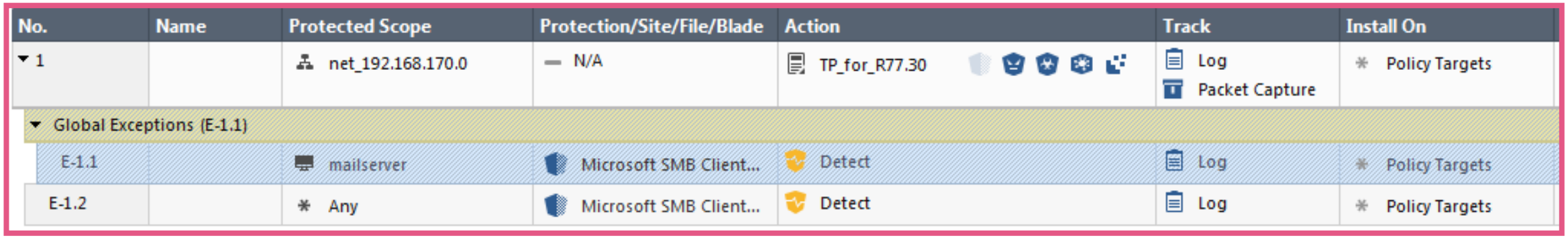
- Global Exceptions are visible in all the Threat Prevention policies



Understanding The Components
Threat Prevention Policy Rule Base – Exceptions

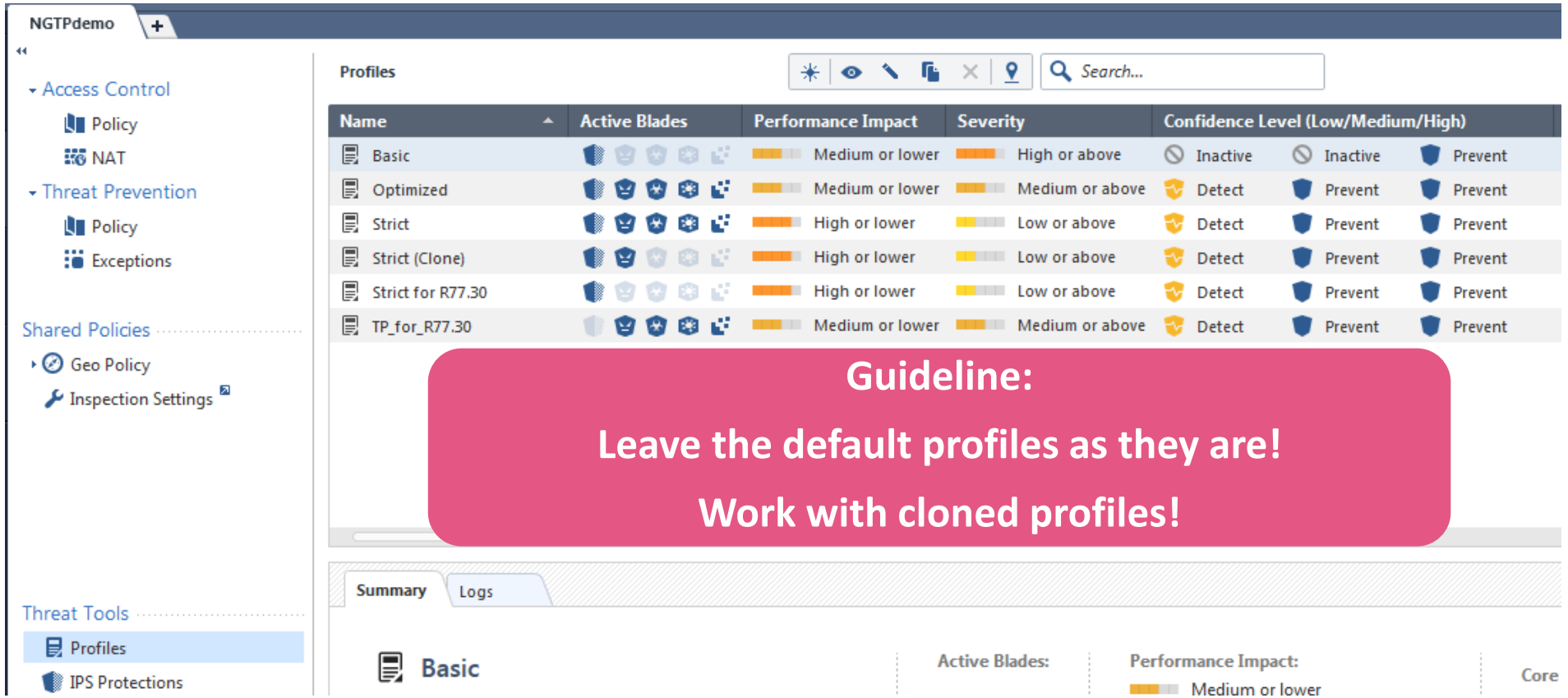
- Define Exceptions per policy and see them listed
- Click the arrow for the Global Exceptions to see all Exceptions that apply





Understanding The Components
Threat Prevention Profile

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

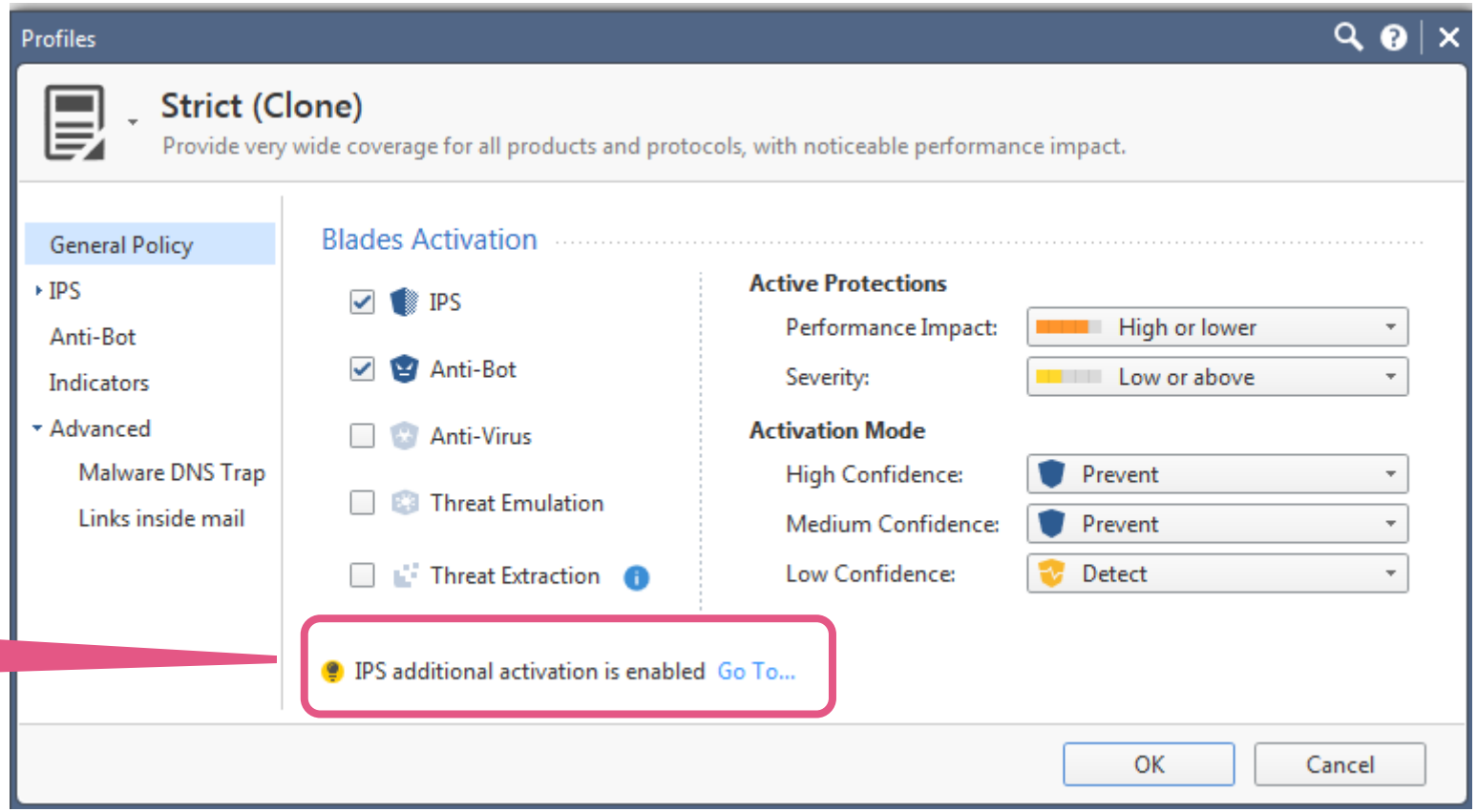


Understanding The Components
Threat Prevention Profile

Editing a profile

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

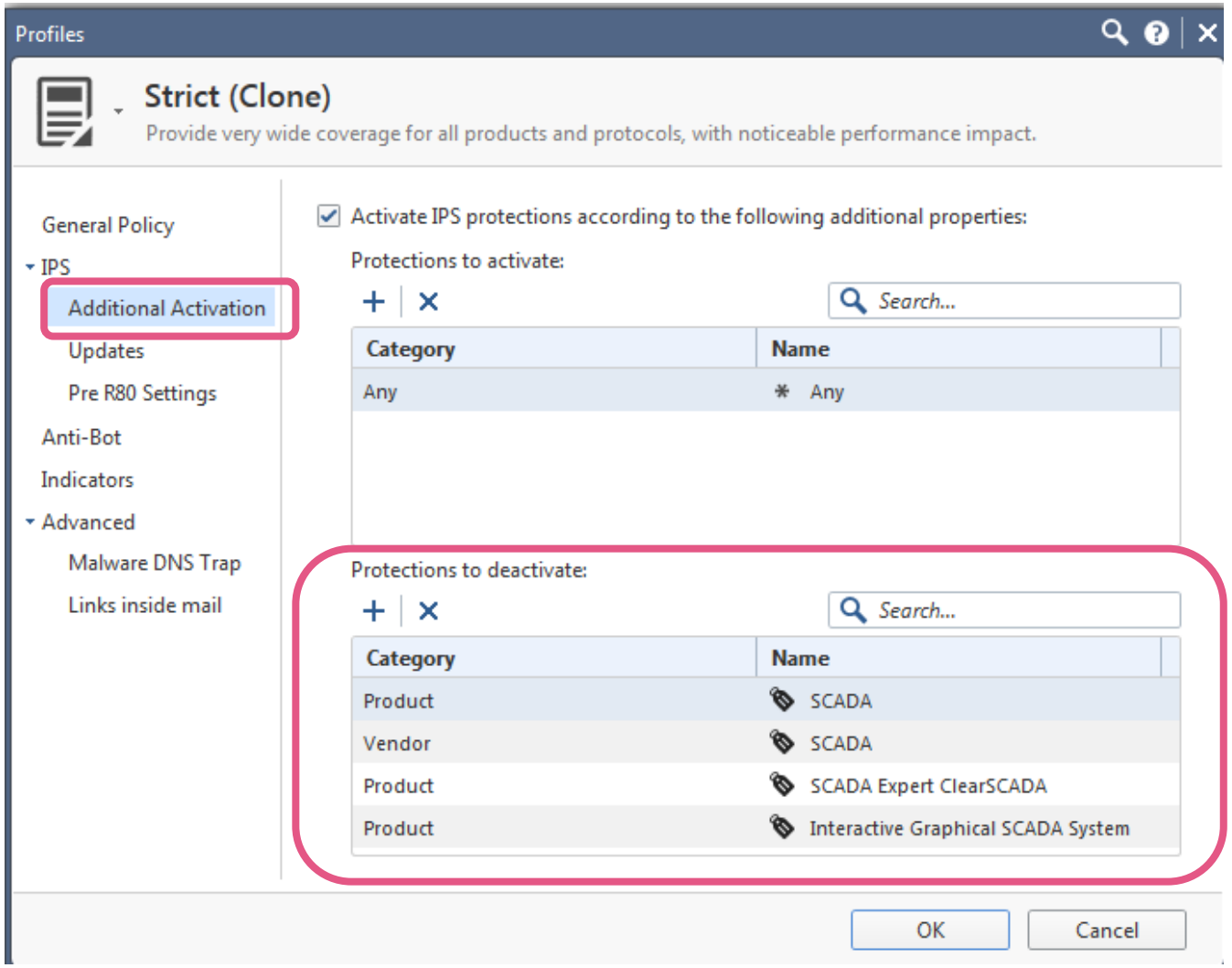
See IPS Profile is modified



Understanding The Components
Threat Prevention Profile

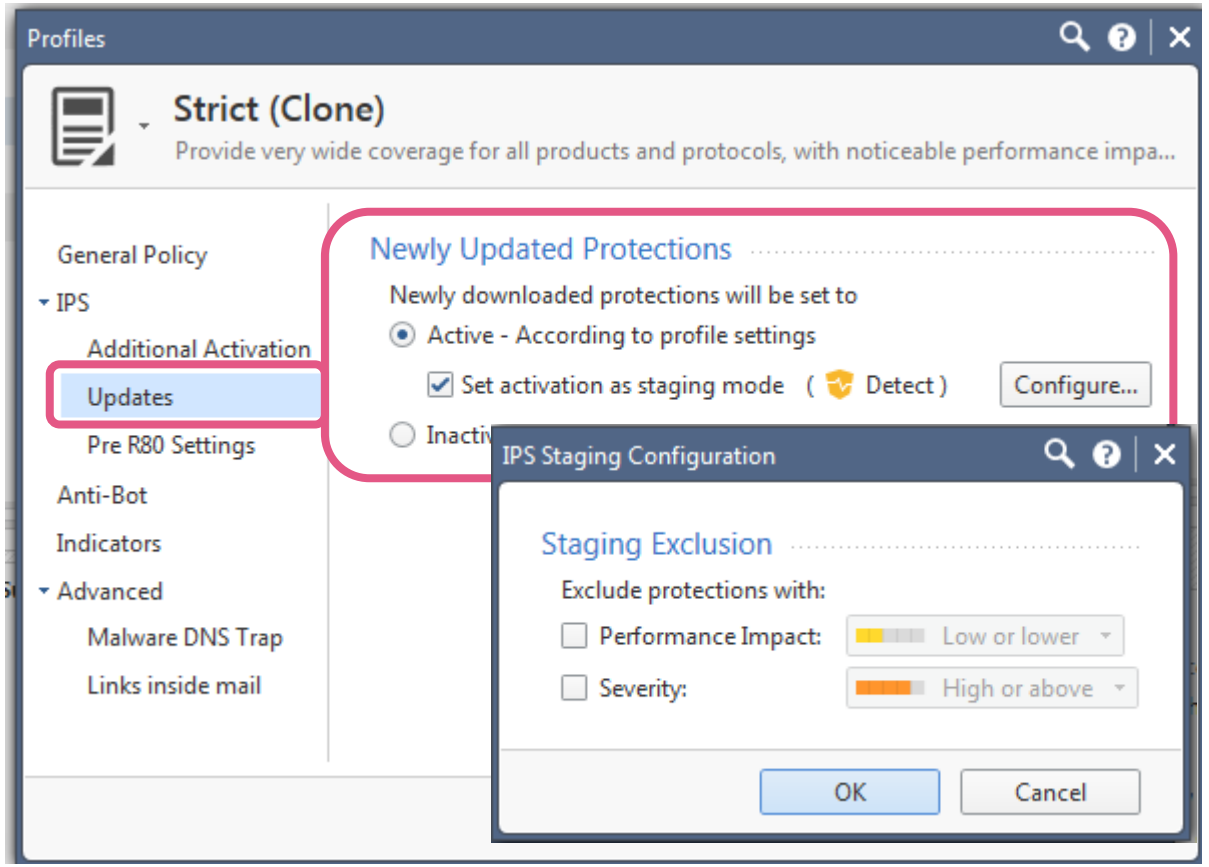
Editing IPS specific settings

- Activate or deactivate dedicated protections



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**.

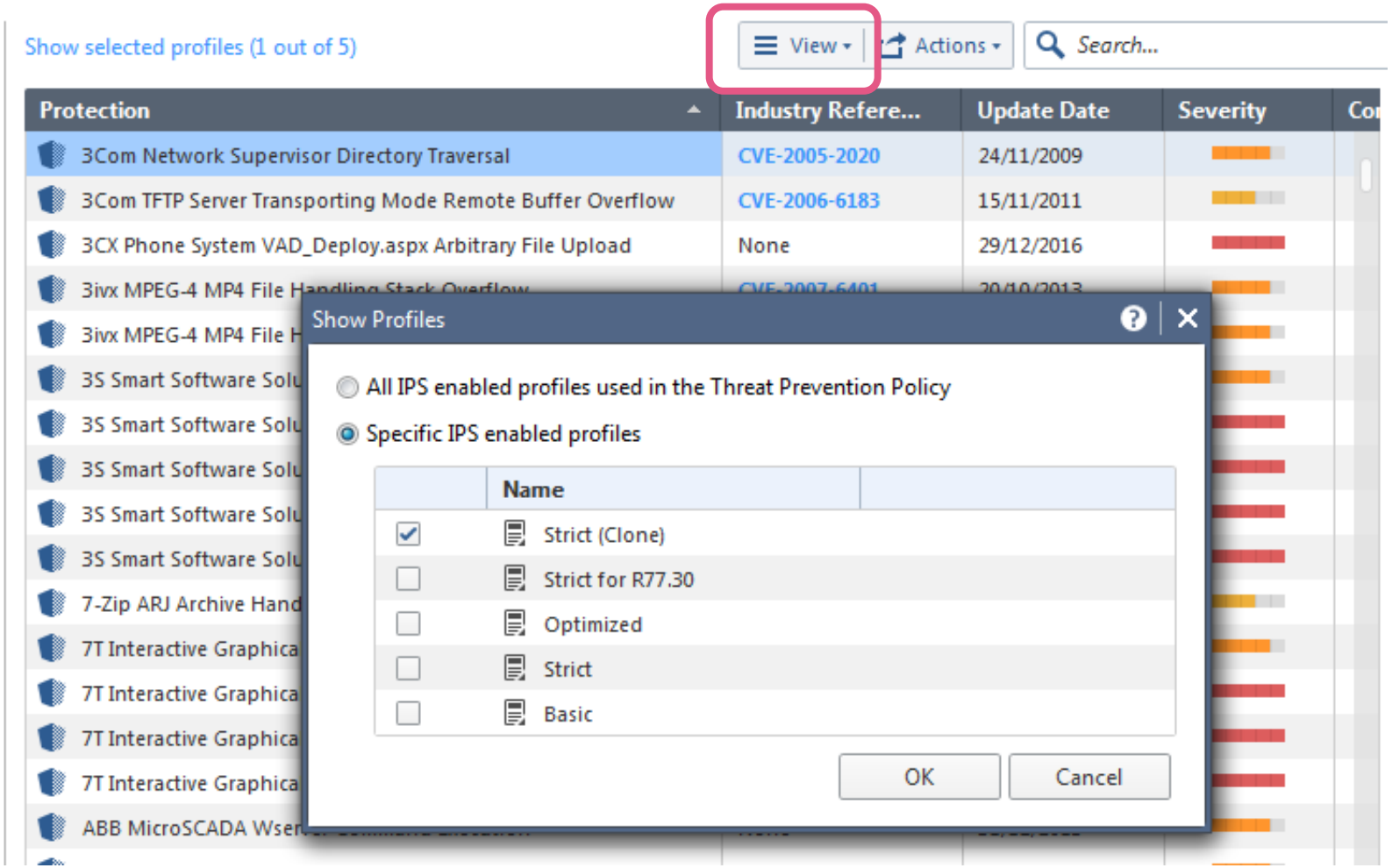
Now we learned about Policies and Profiles.

What about Protections?

Understanding The Components

Threat Prevention Profile

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



Understanding The Components
Protection Types: defining the meaning of “signatures”

There are different types of protections

- **Core protections**
  - Protections presenting configuration options
- **ThreatCloud protections**
  - Dynamically updated signatures

Protection Types

The IPS protections are divided into two main types:

- **Core protections** - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy
- **ThreatCloud protections** - Updated from the Check Point cloud ("Updating IPS Protections" on page 88). These protections are part of the Threat Prevention policy.

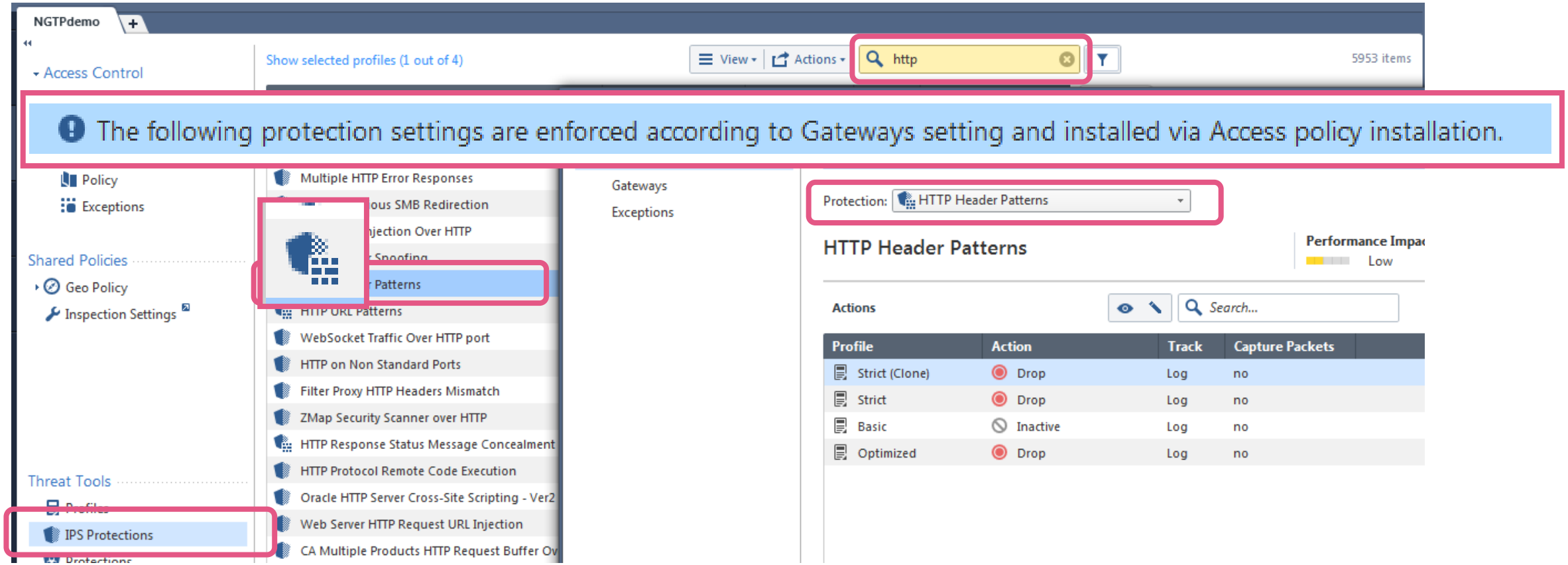
Source: R80.10 Threat Prevention Administration Guide page 86

Understanding The Components
Protection Types: defining the meaning of “signatures”

- **Core protections**
  - **Configuration settings** per gateway
  - Enforced with the help of the engine instance “**Protocol Parser**”
  - Managed in a **dedicated profile** with a **dedicated assignment to gateways**
  - **Installed** together **with** the **Access Control policy**
- **ThreatCloud protections**
  - **Dynamic signatures** updated from the ThreatCloud using the IPS Update process
  - Enforced with the help of engine instance “**Pattern Matcher**”
  - Managed as an element of the **Threat Prevention profile**
  - **Installed** together **with** the **Threat Prevention policy**

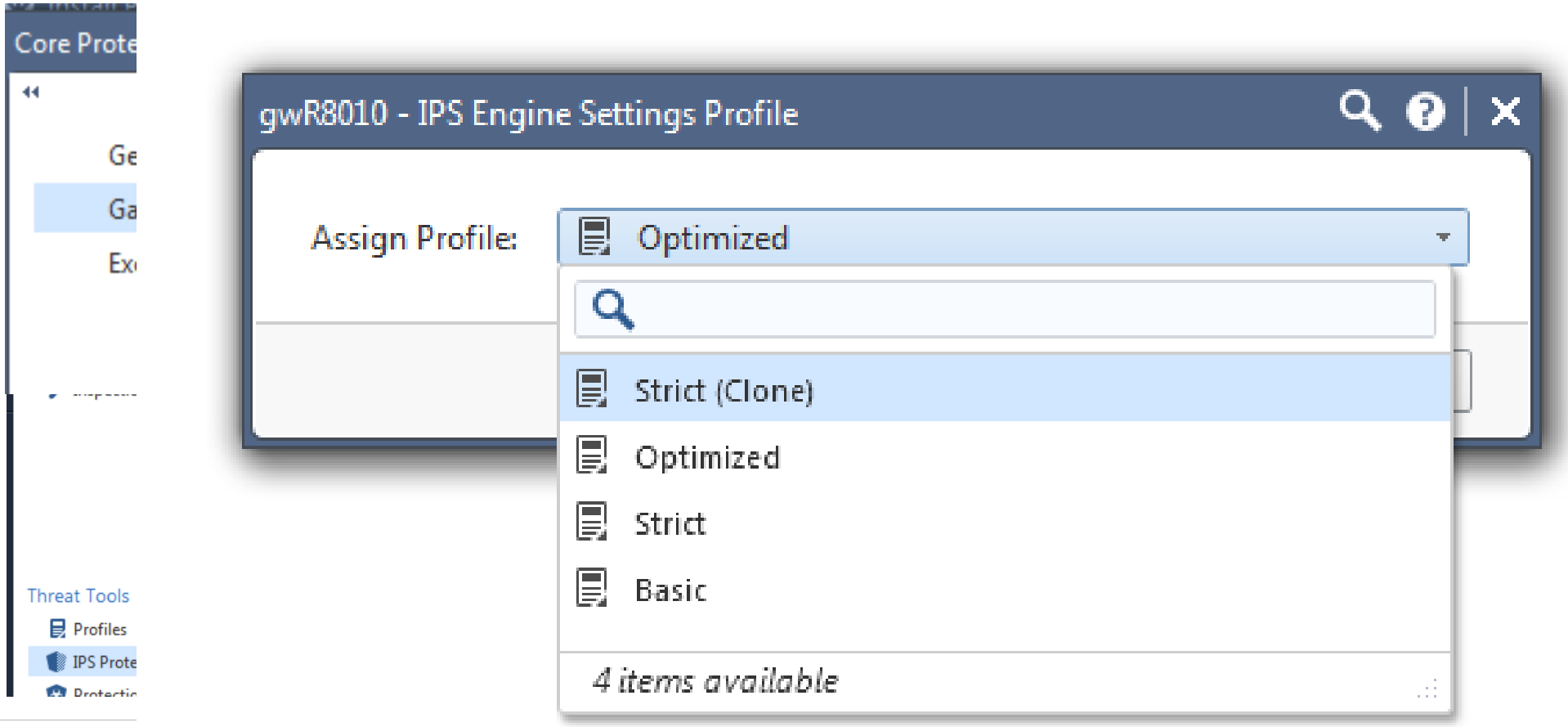
Understanding The Components
Core Protections

- Search for “http” under IPS Protections and double click on a protection
- Note the symbol and the information



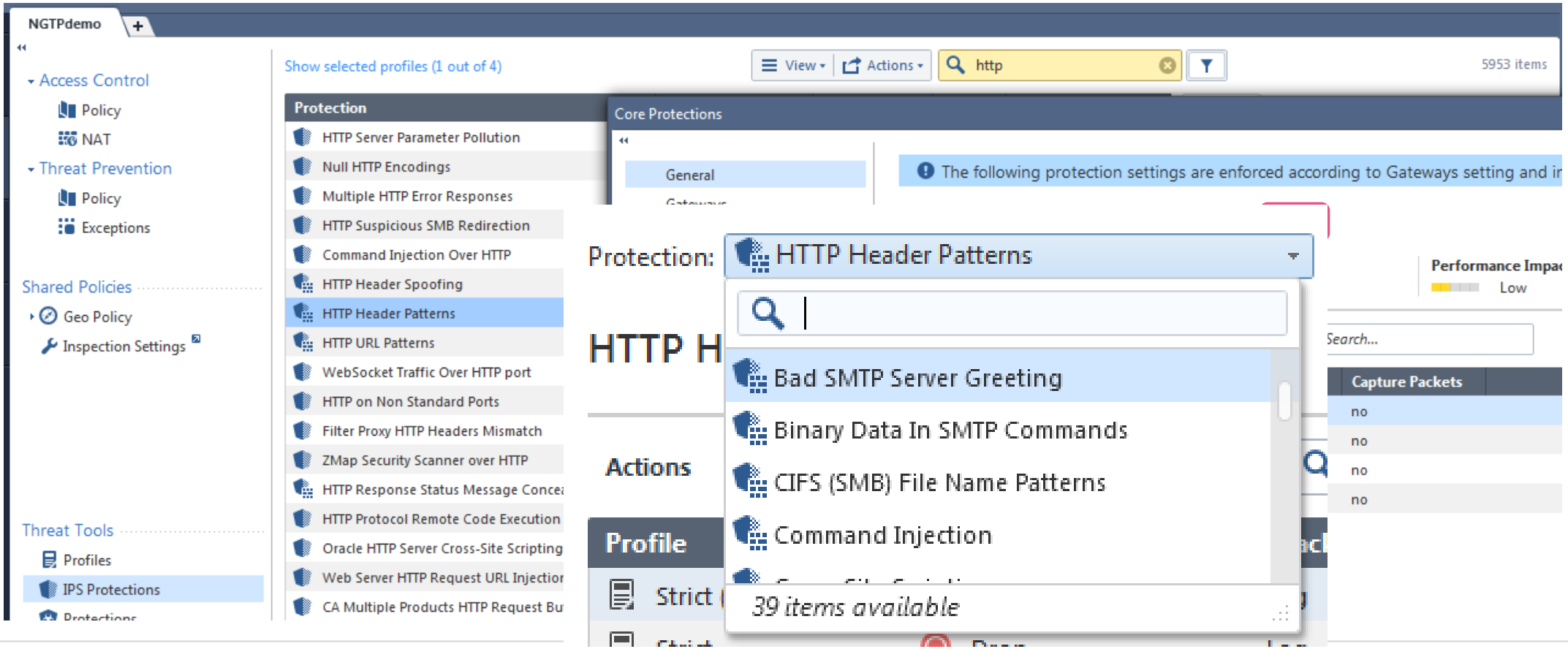
Understanding The Components
Core Protections

- Understand that Core Protections have their **dedicated assignment to gateways**
- By **default the Optimized Profile** is assigned to R80.10 Gateways



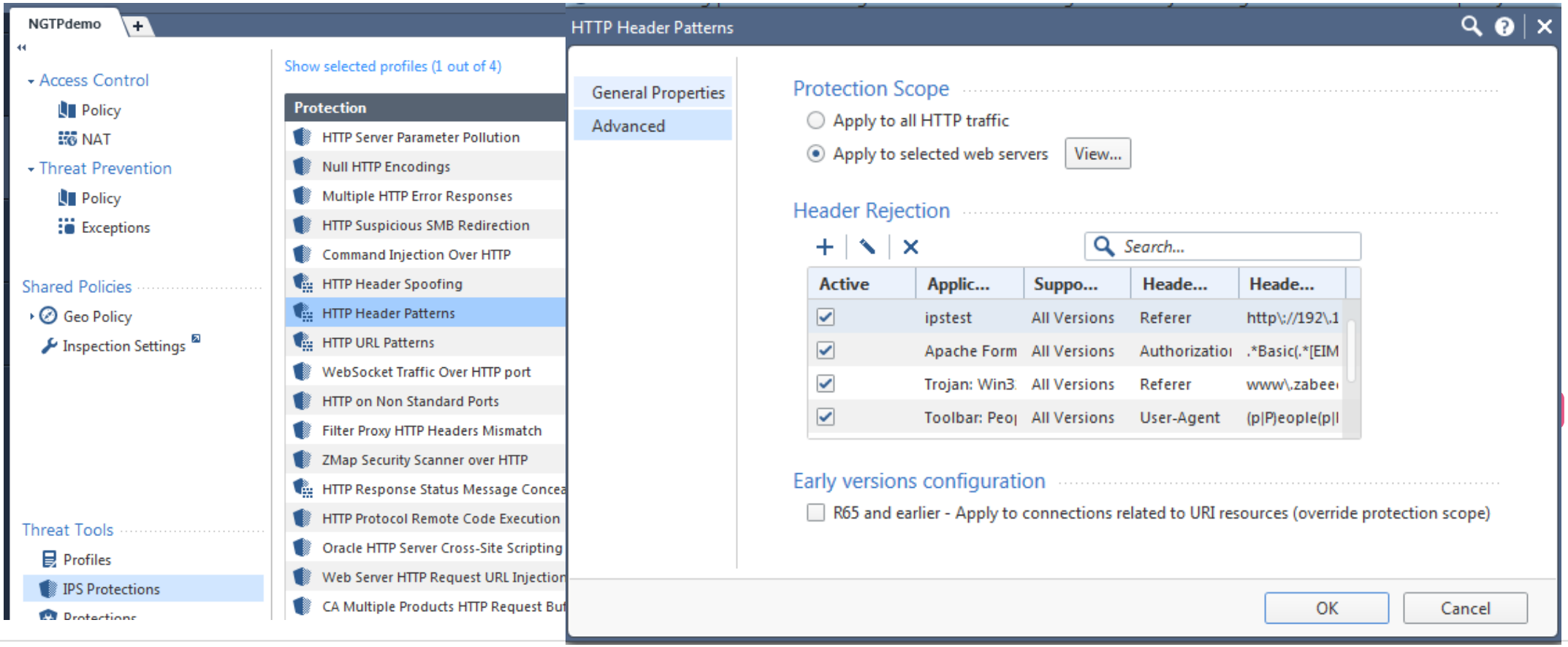
Understanding The Components
Core Protections

- Click to see other Core Protections
- Scroll and select



Understanding The Components
Core Protections

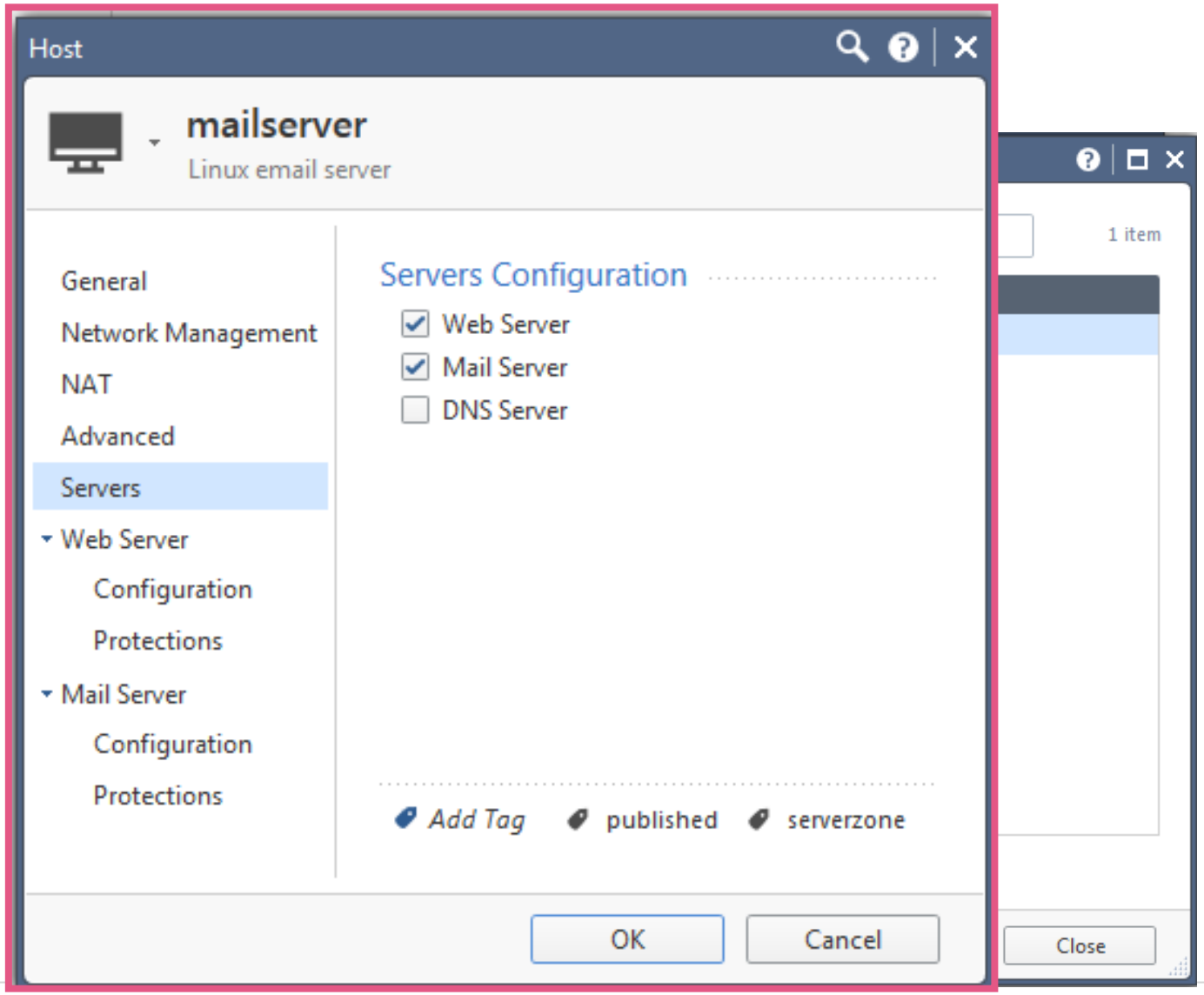
- Click to edit the Core Protection (Packet Capture will be done for **every match** if enabled)
- Edit the configuration under Advanced menu



Understanding The Components

Core Protections

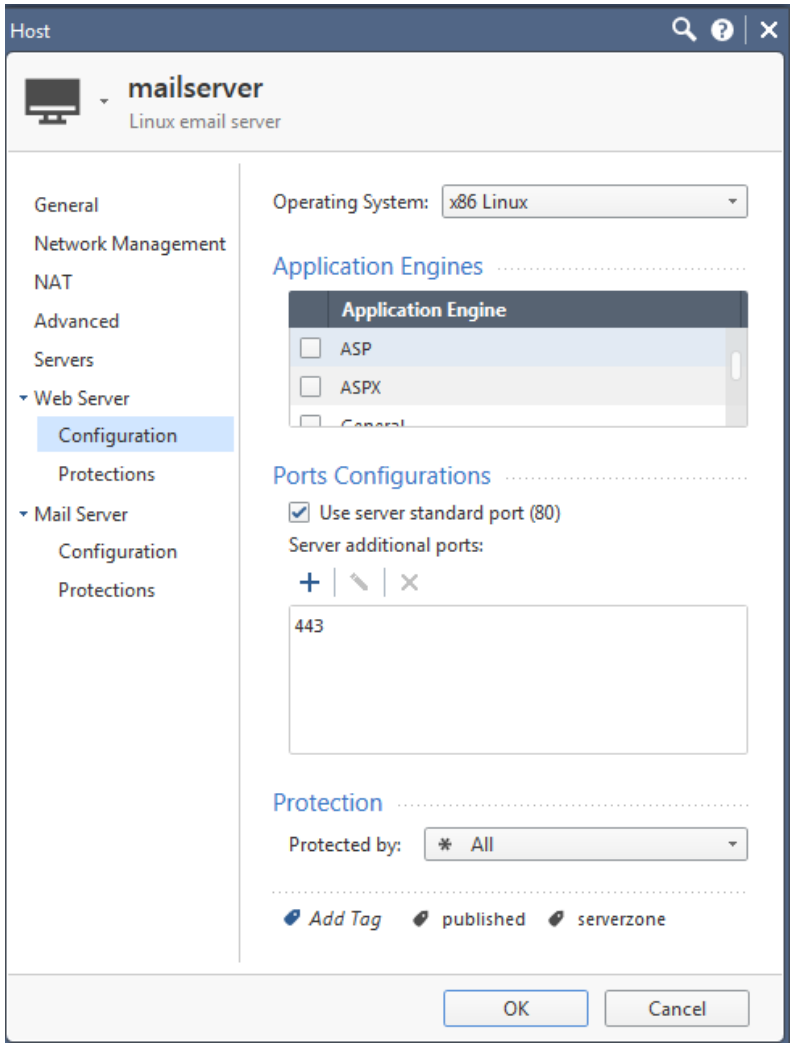
- Assignment of Core Protections to dedicated servers
- Configure Web, DNS and Mail server objects to benefit from Core Protections

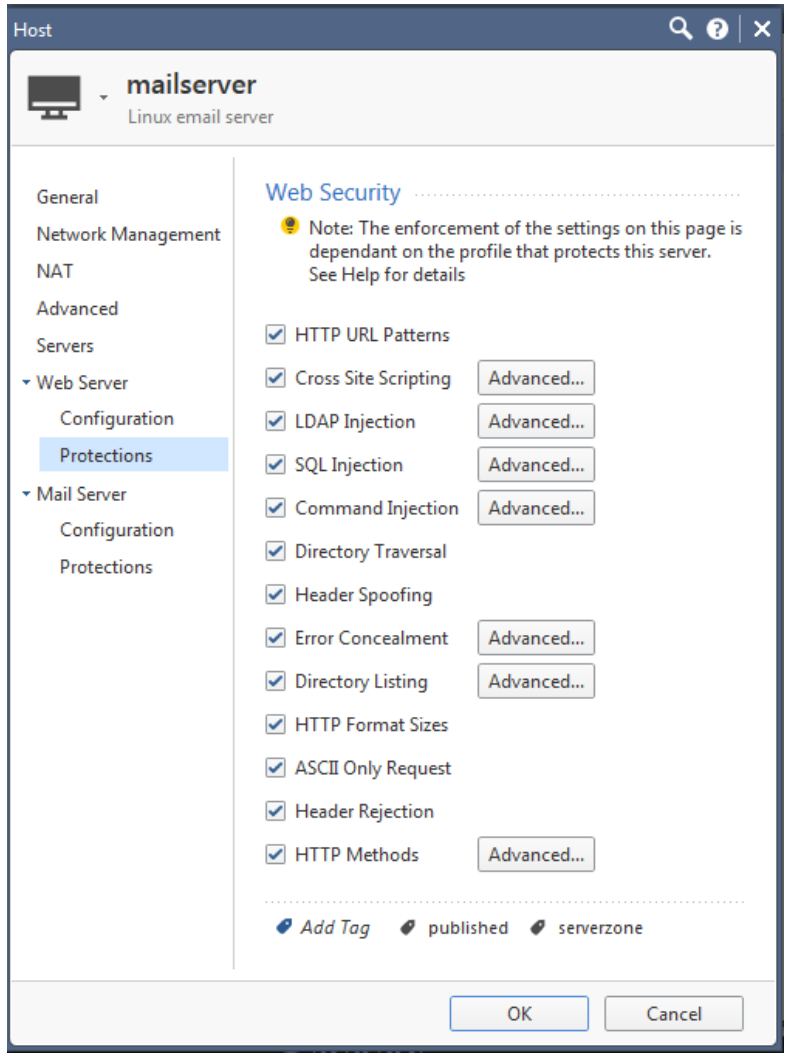


Understanding The Components

Core Protections

- Activate the Core Protections from the host objects “Servers” menu

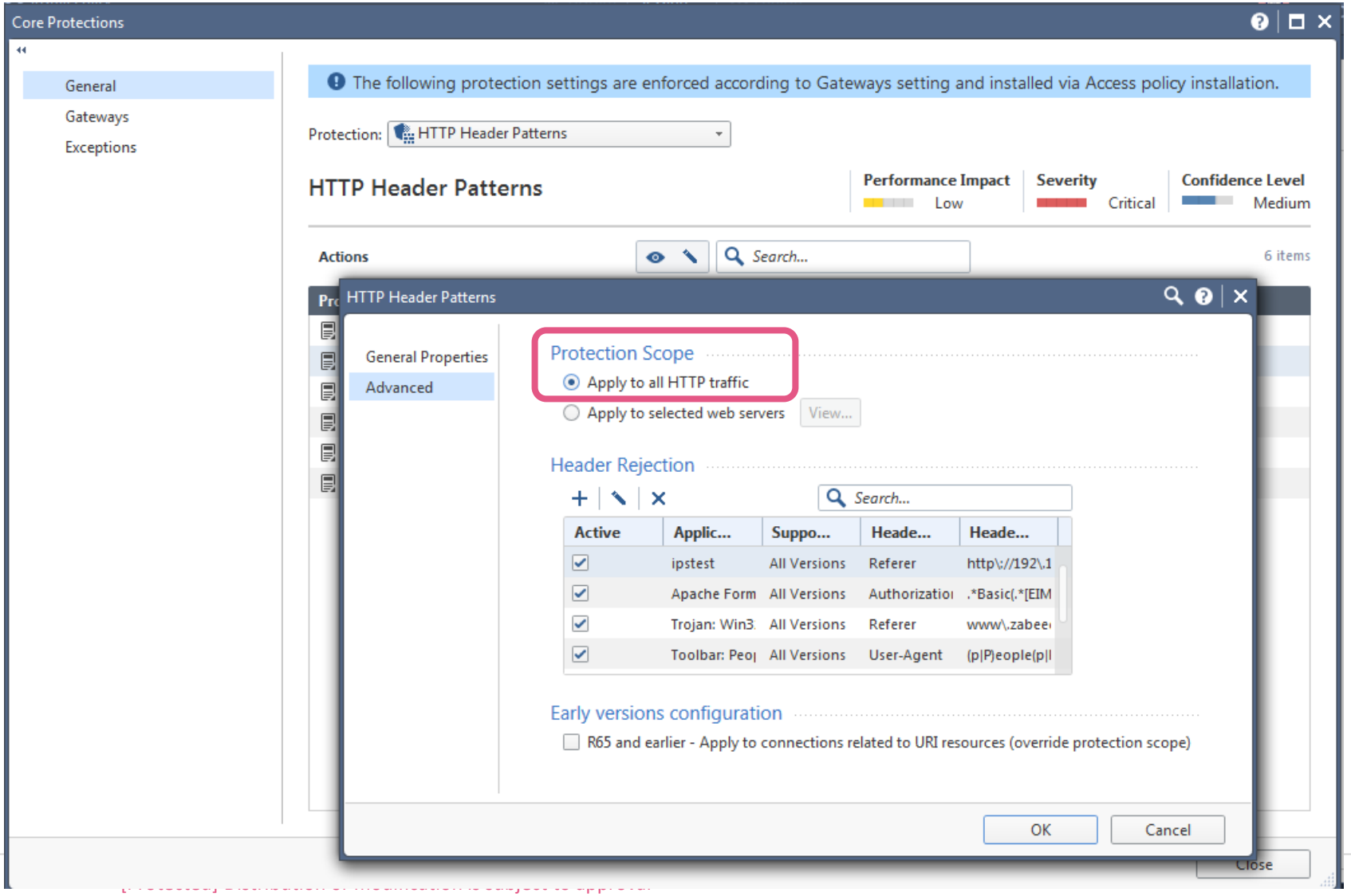




Understanding The Components

Core Protections

- When you don't know your Web, DNS and Mail servers apply the Core Protections to all HTTP traffic
- This is particular important when running an IPS test where the servers are generated on the fly by the test software



Understanding The Components
Working with Core Protections using Filters

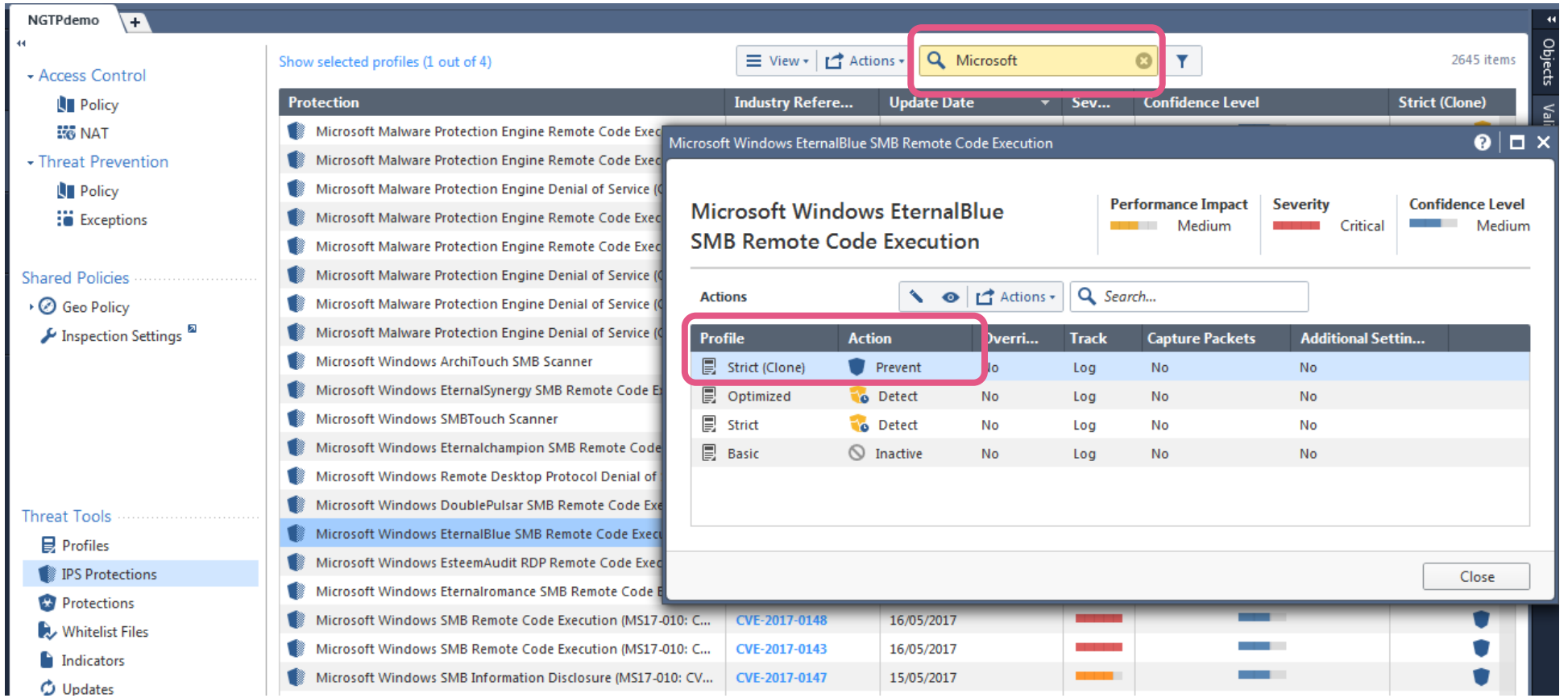
- You can use Filter functionality to see Core Protections
  - Open the Filter menu add Filter “Type” and select “Core”

So far so good about Core Protections.

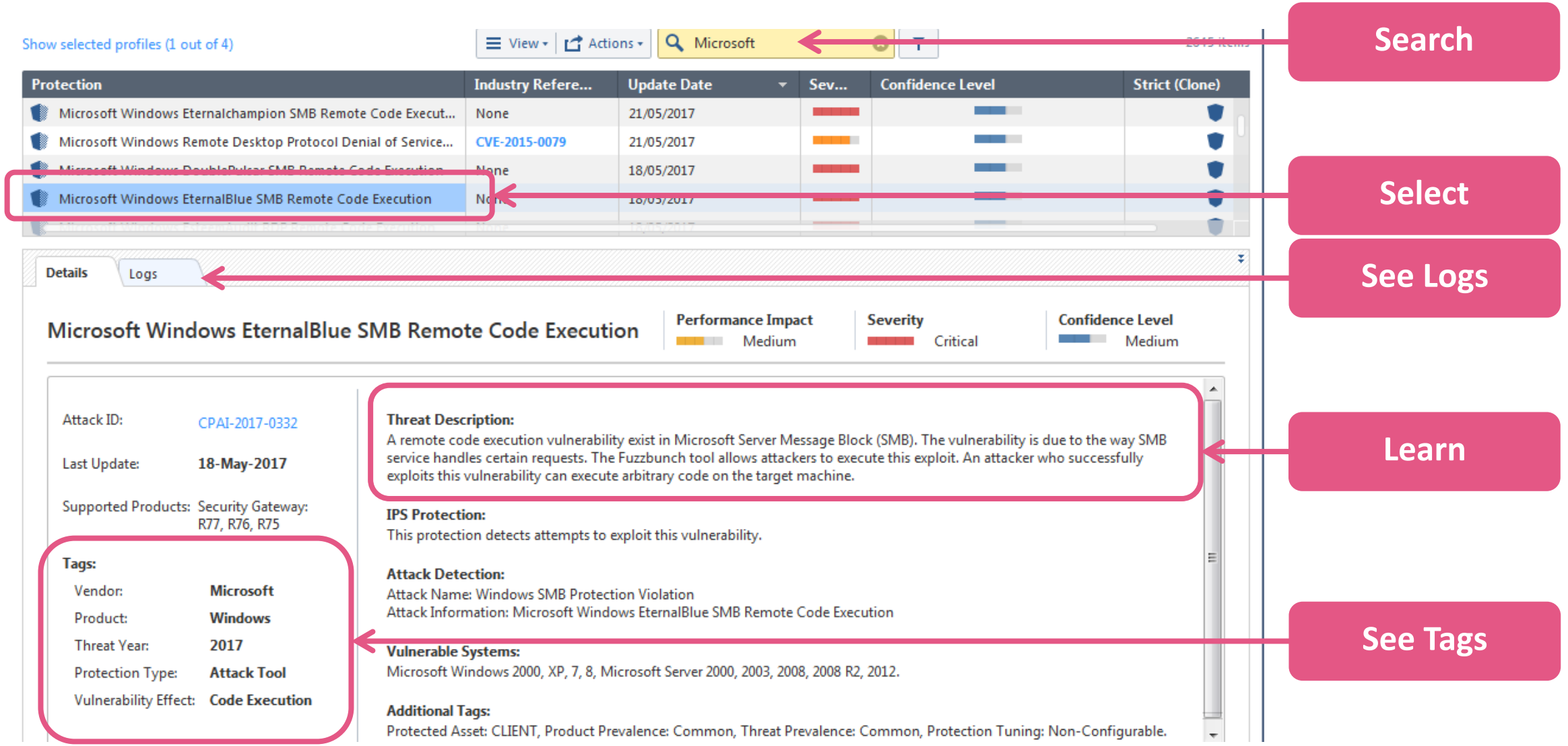
What about ThreatCloud Protections?

Understanding The Components
ThreatCloud Protections (Signatures)

- Search using a keyword or industry reference
- Change the action if needed

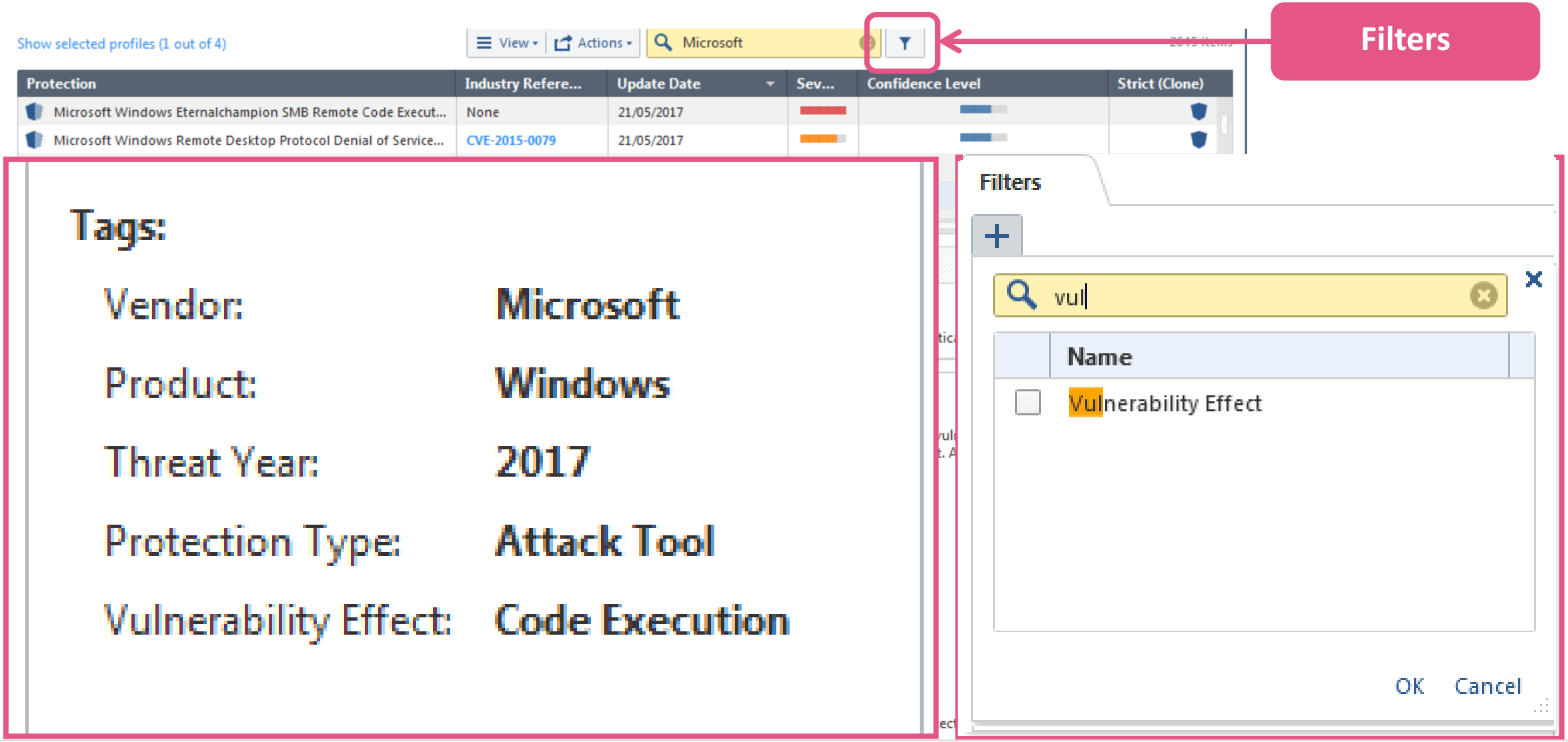


Understanding The Components
ThreatCloud Protections (Signatures)



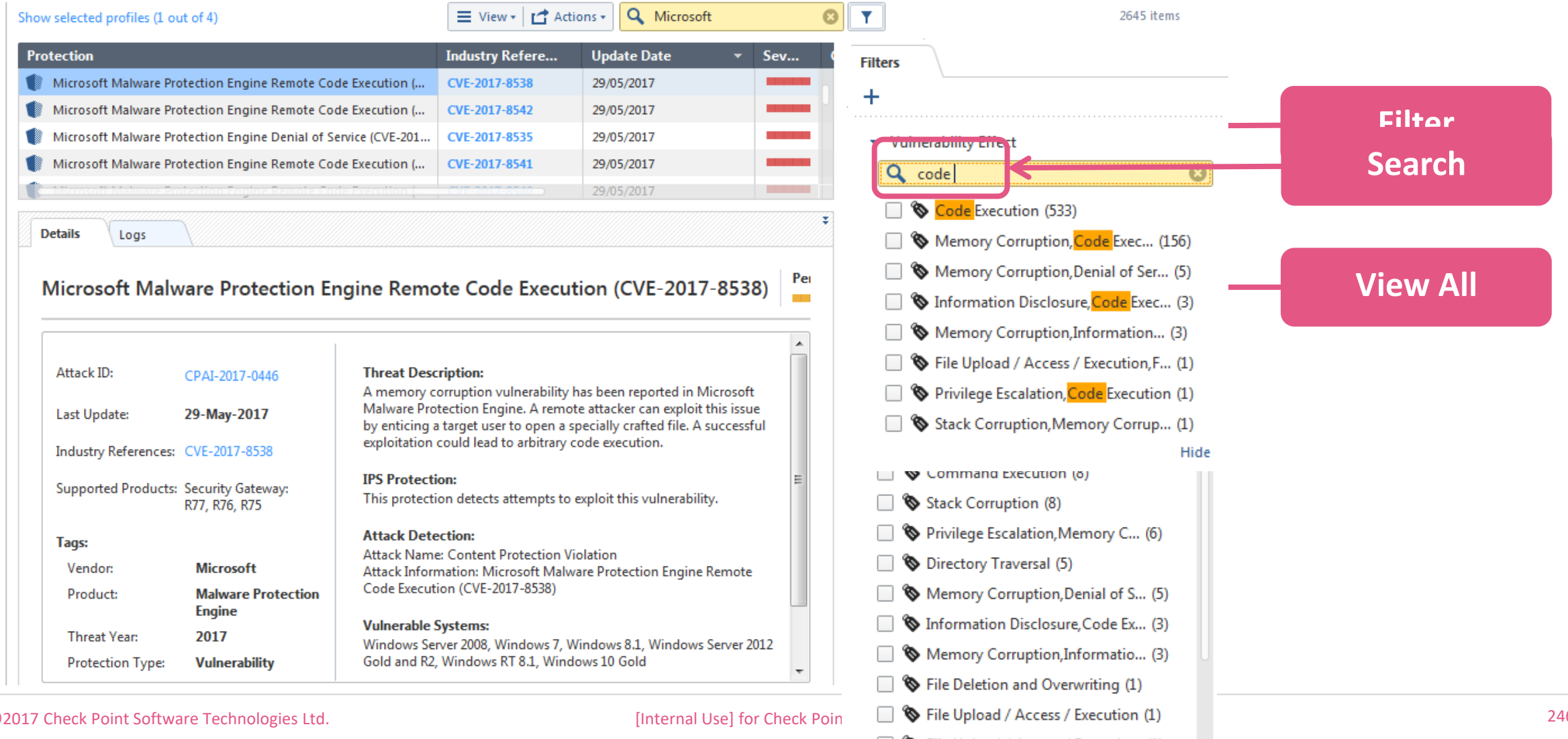
Understanding The Components

ThreatCloud Protections (Signatures) Tags and Filters



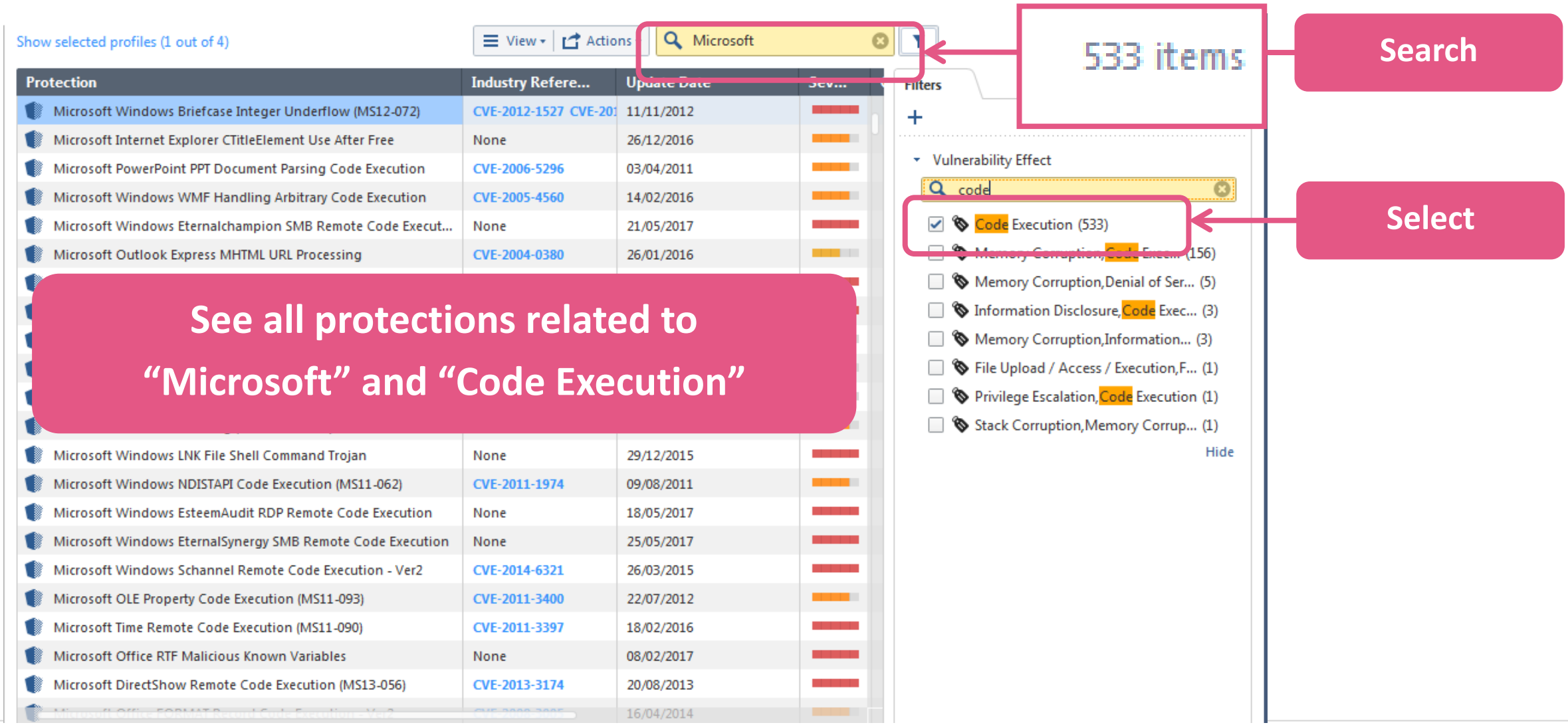
Understanding The Components

ThreatCloud Protections (Signatures) Tags and Filters: Vulnerability Effect



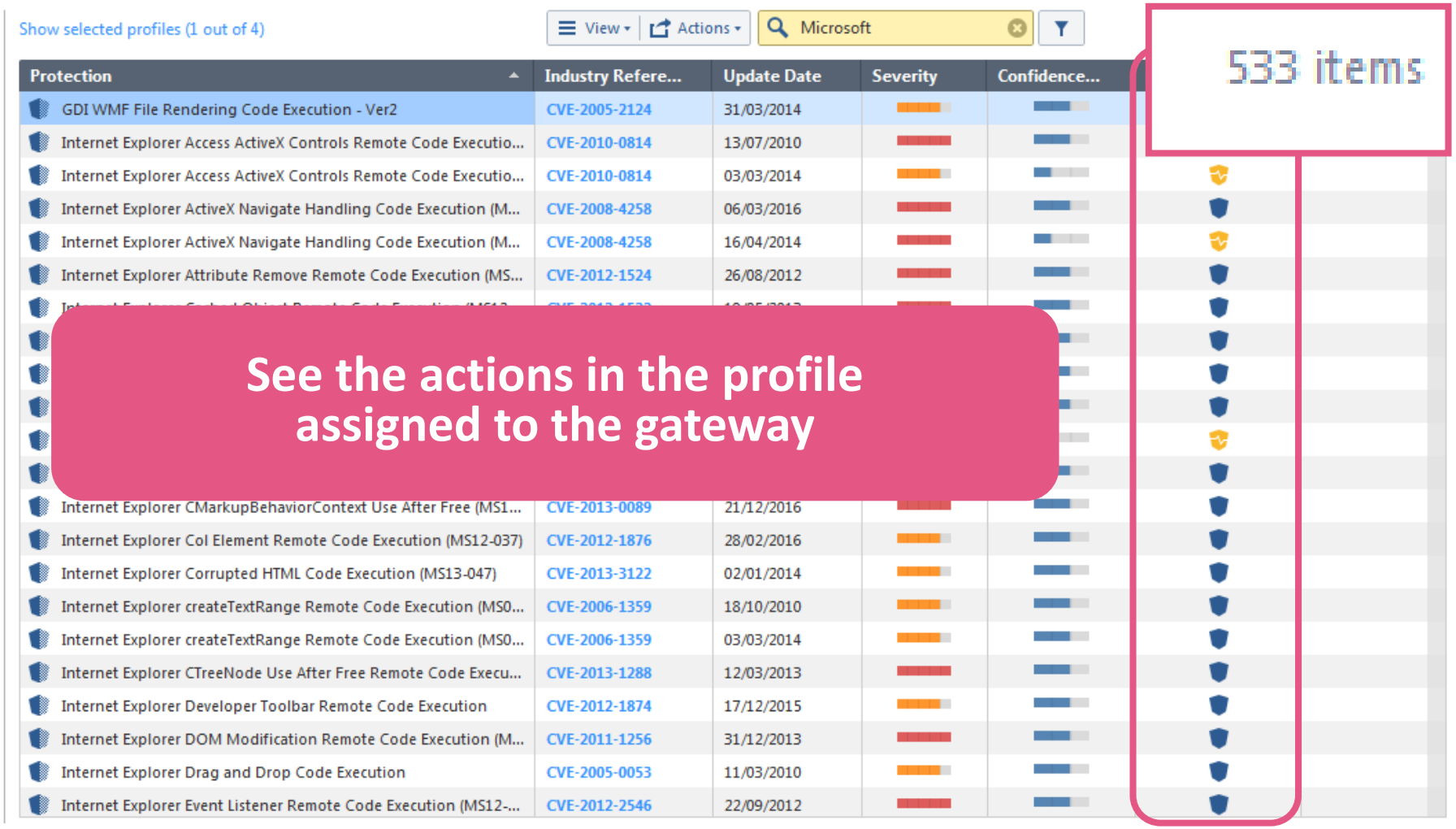
Understanding The Components

ThreatCloud Protections (Signatures) Tags and Filters: Vulnerability Effect



Understanding The Components

ThreatCloud Protections (Signatures) Tags and Filters: Vulnerability Effect



See the actions in the profile assigned to the gateway

Note: even if the Filter is hidden it remains active

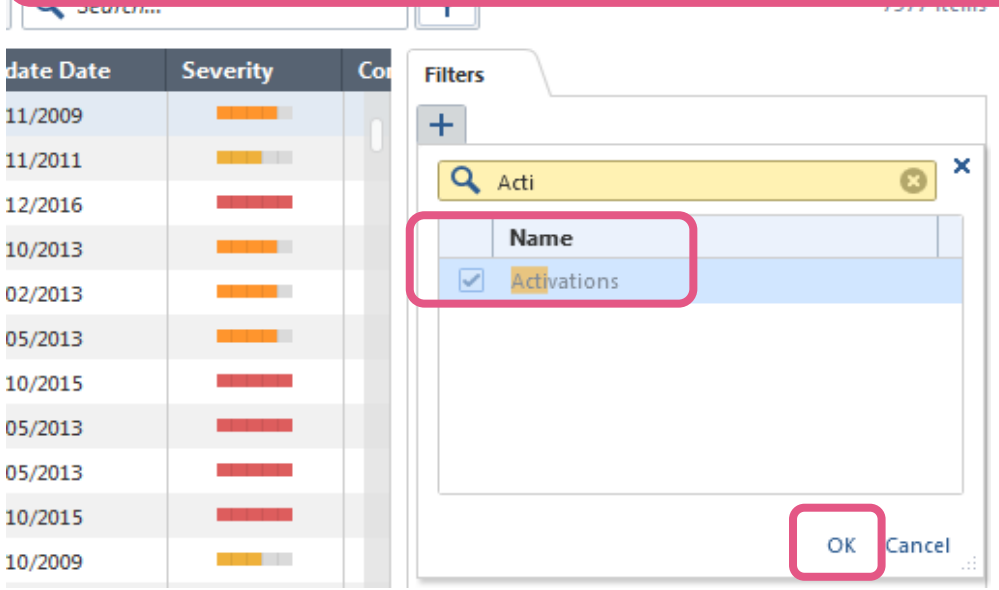
Understanding The Components

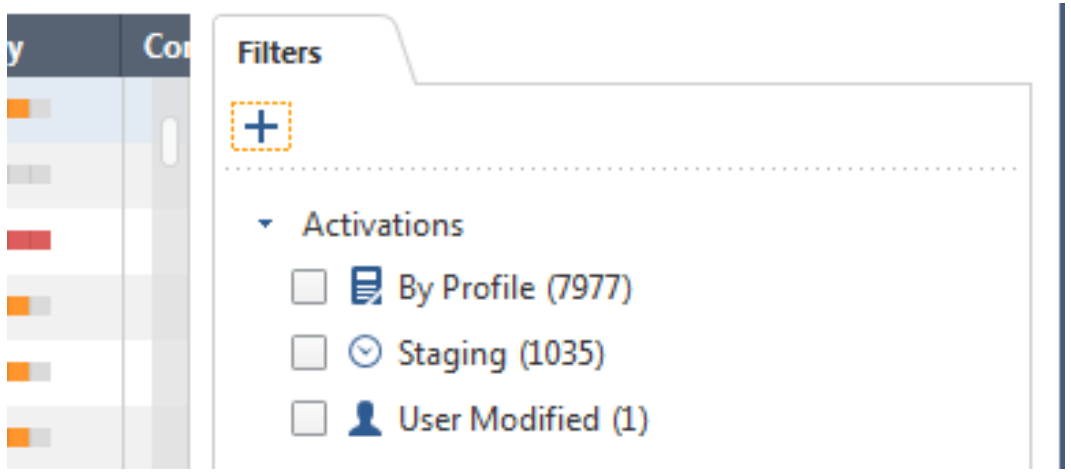
ThreatCloud Protections (Signatures) Tags and Filters: Staging

Following up newly downloaded ThreatCloud Protections (signatures)

- Remember the profile configuration: IPS > Update > Staging
- Using the filter Activations > Staging you see protections with Staging tag

Select “Activations”, click “Ok” and see the “Staging” filter option appearing

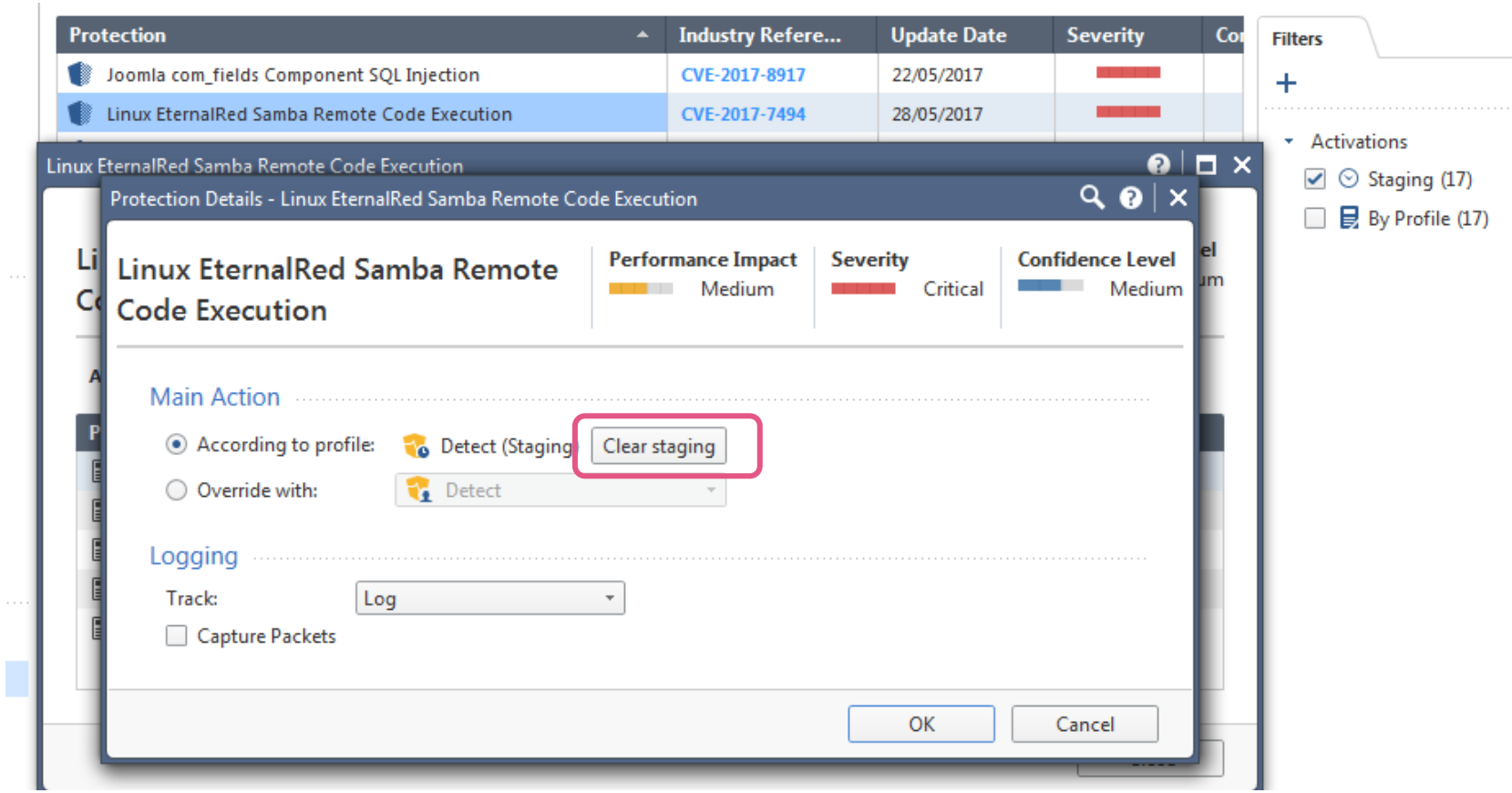




Understanding The Components

ThreatCloud Protections (Signatures) Tags and Filters: Staging

- See protections with “Staging” tag enabled
- Edit the protection to clear the tag

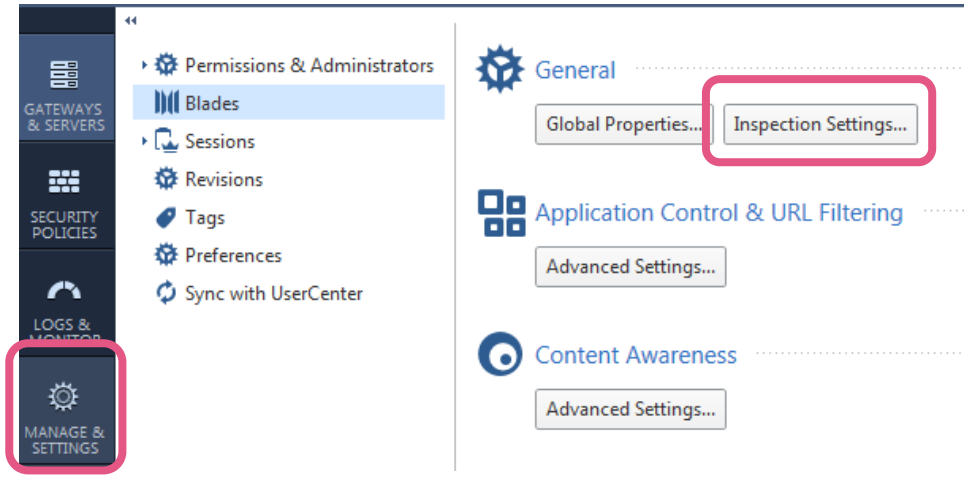


Ok, done with ThreatCloud Protections.

Anything else?

Understanding The Components
Inspection Settings

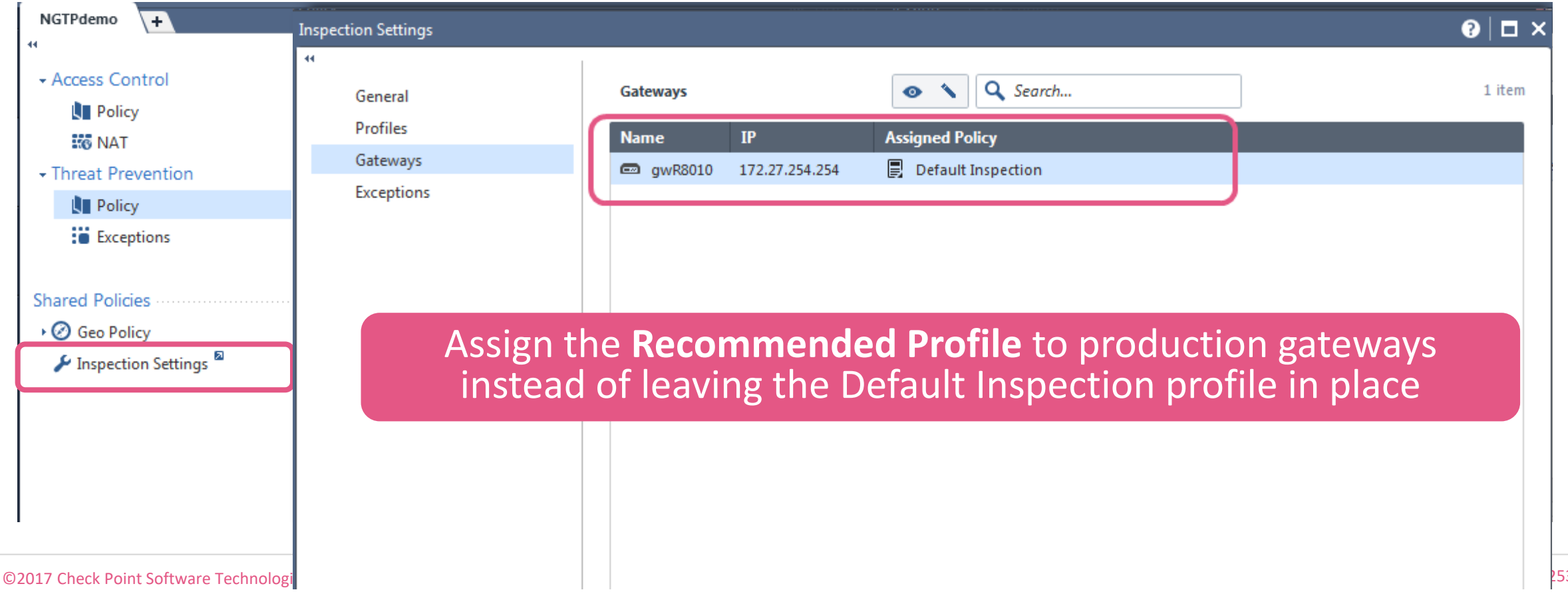
- **Inspection Settings**
  - Present **configuration settings** influencing the lower levels of the NGTP enforcement engine
  - **Enforce security independent of the Threat Prevention** Software Blades
  - Managed using the **Inspection Settings** menu
  - Assigned in a **dedicated profile** to each gateway
  - **Installed with** the **Access Control Policy**



Changing default values of Inspection Settings may impact performance and security enforcement of the gateway!

Understanding The Components
Inspection Settings

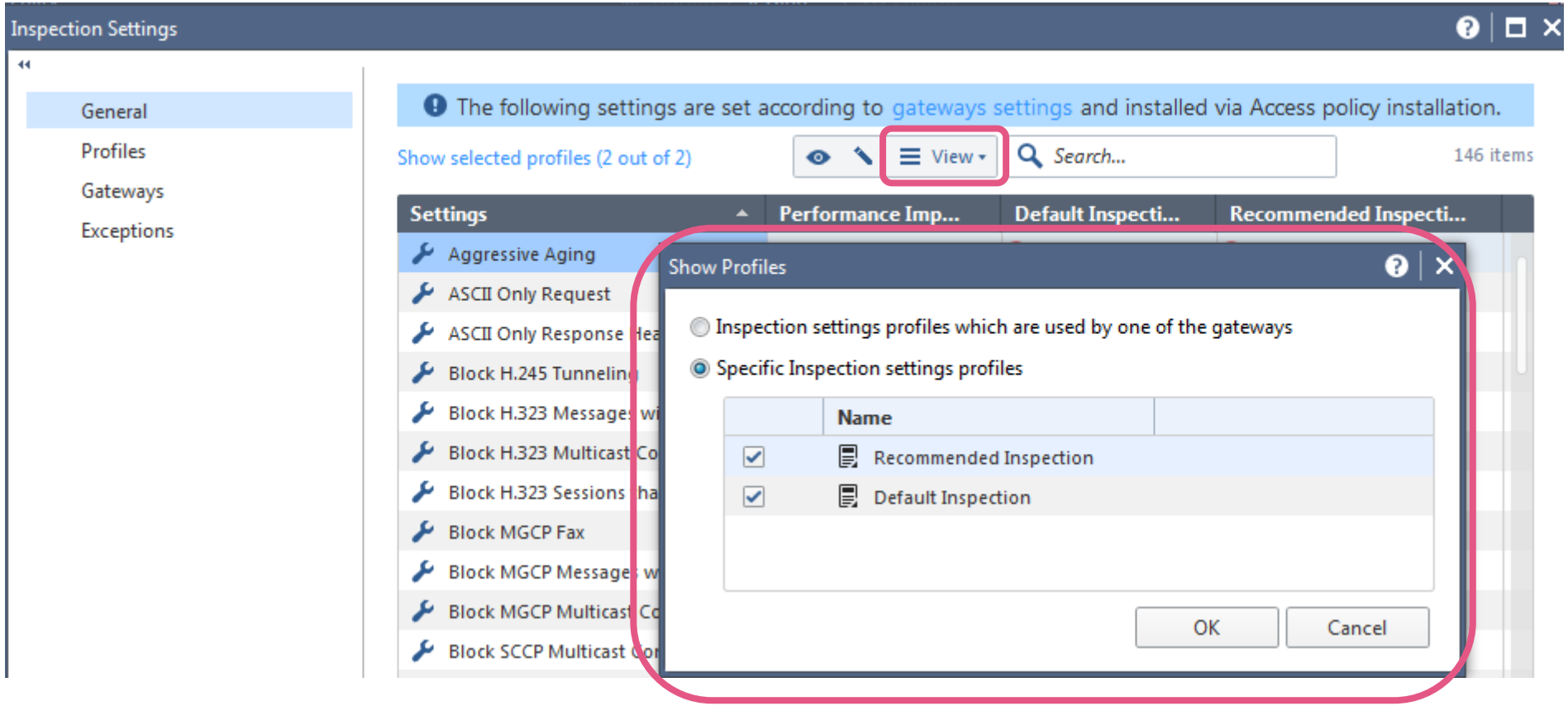
- Configurations related to the Streaming Engine
- Assigned as dedicated profile to gateways



Assign the **Recommended Profile** to production gateways instead of leaving the Default Inspection profile in place

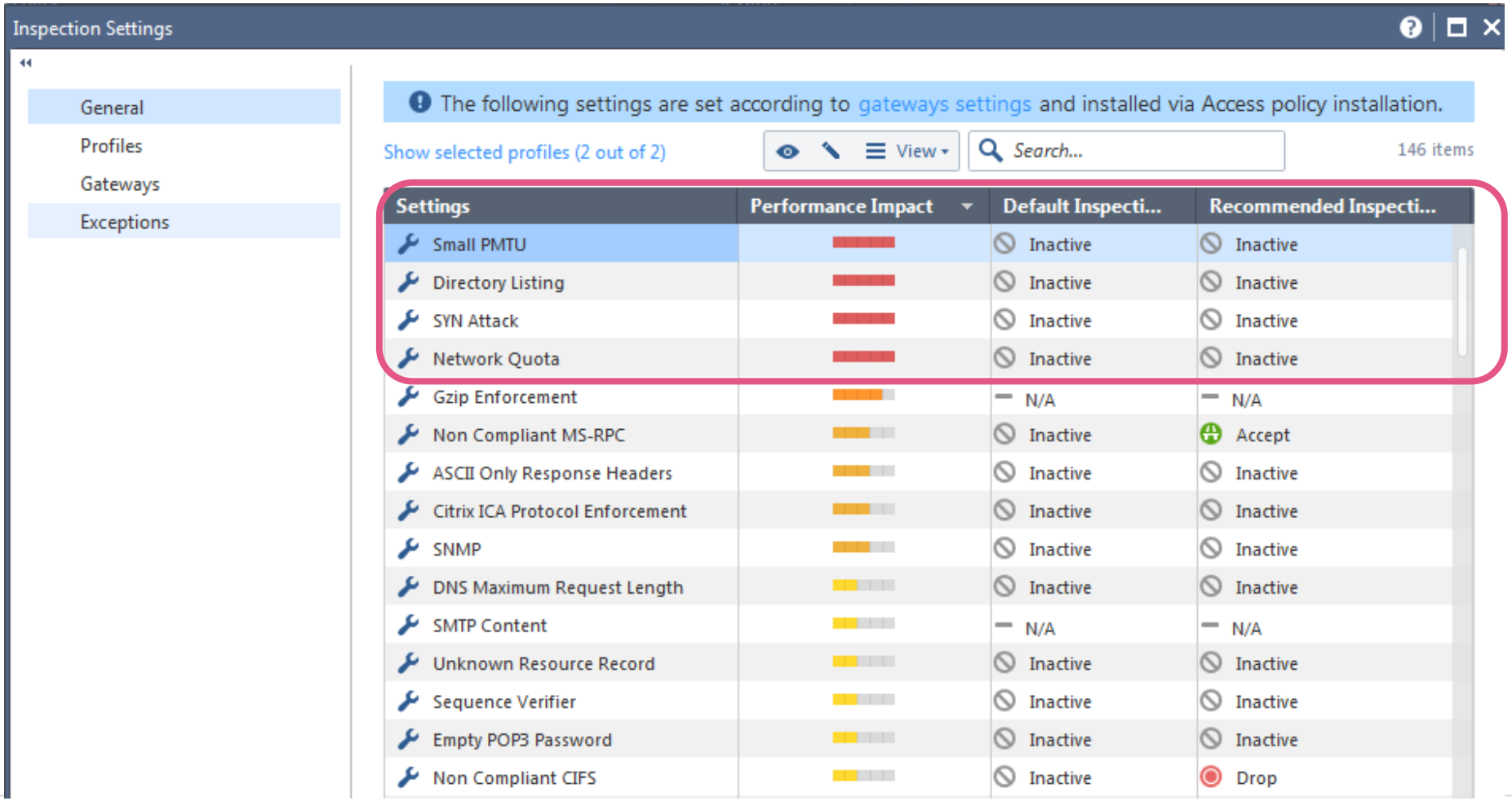
Understanding The Components
Inspection Settings

- View allows selecting the profile(s) you want to see in the overview table



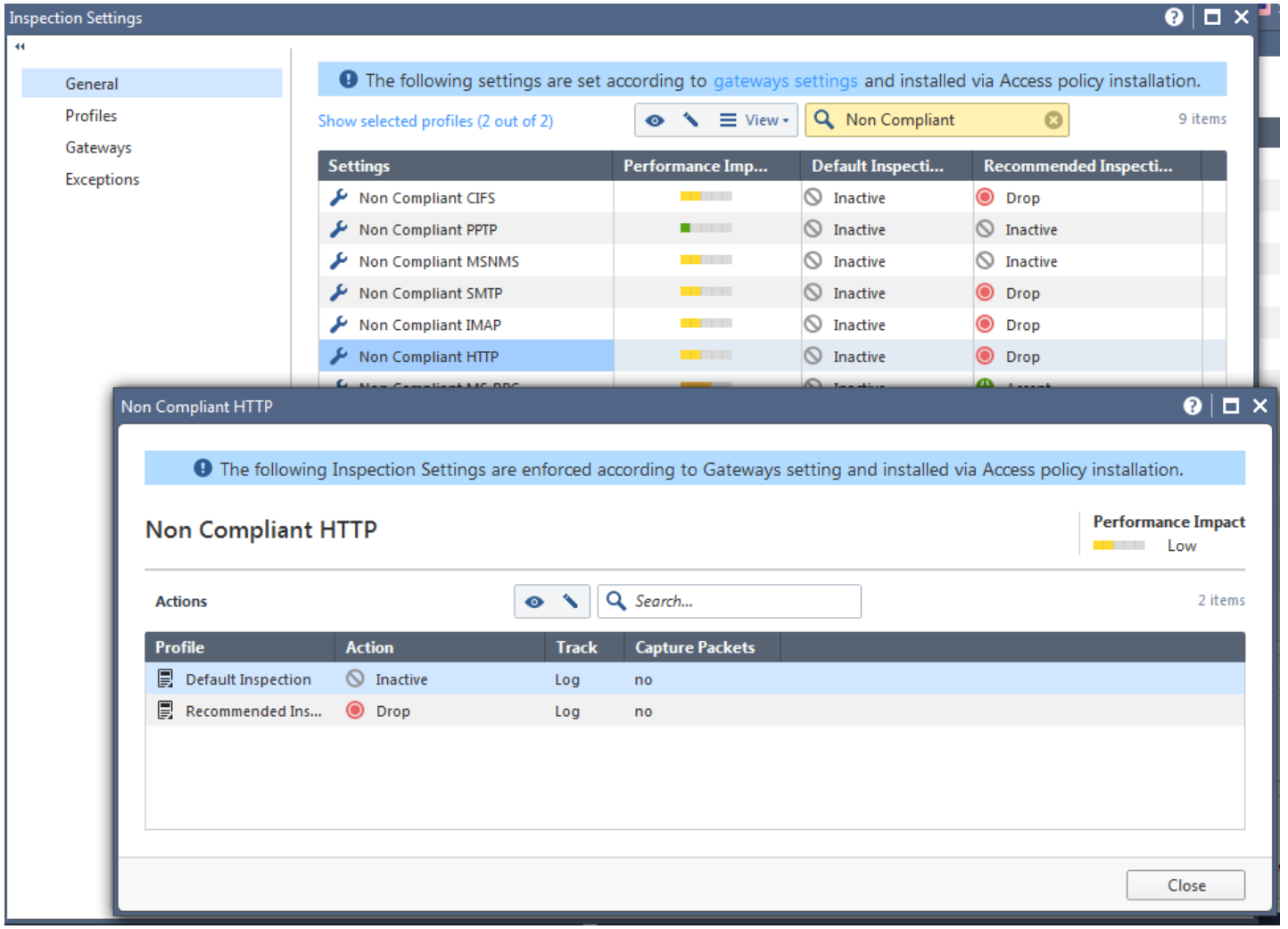
Understanding The Components
Inspection Settings

- Review the profile settings and their performance impact



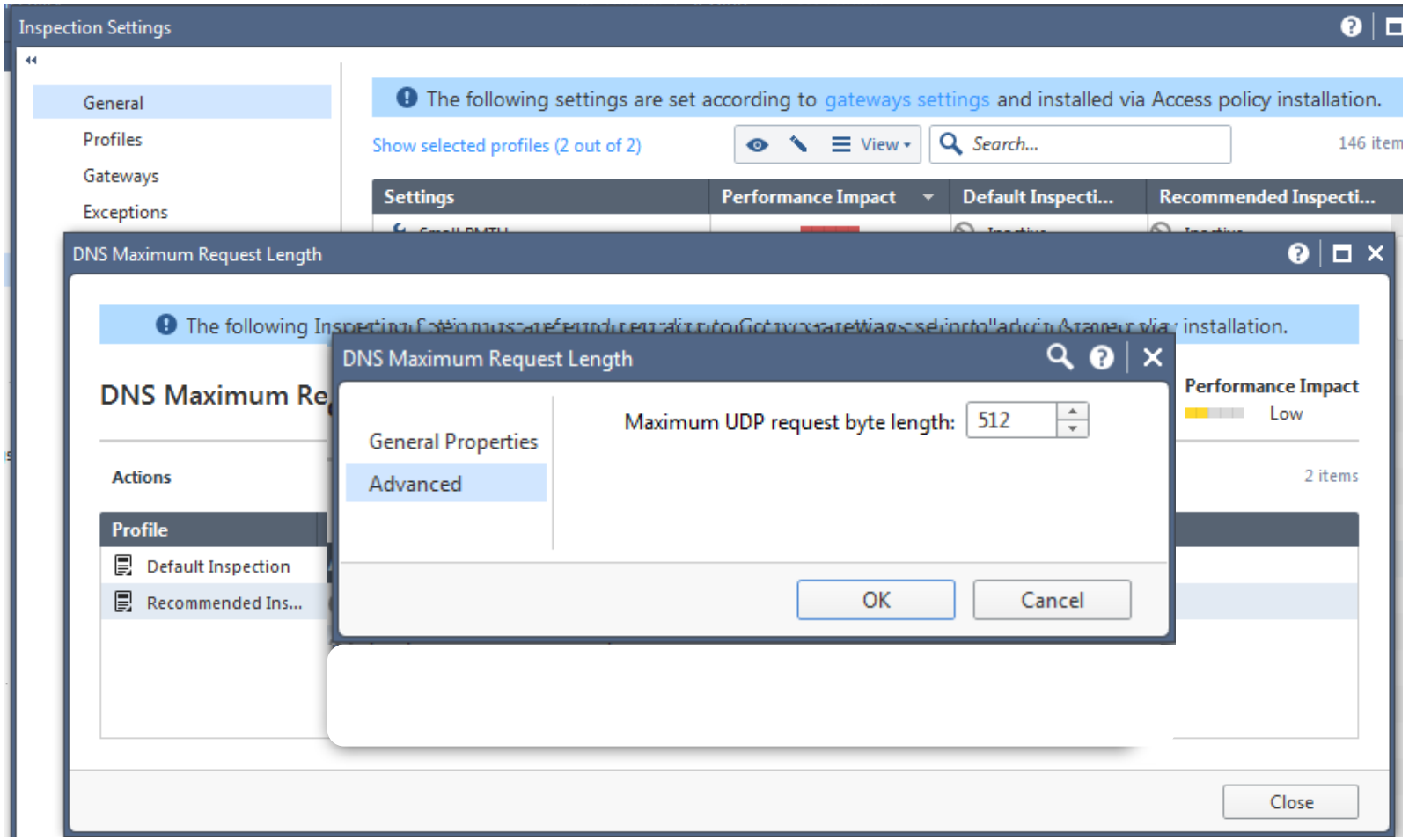
Understanding The Components
Inspection Settings

- Well known protections like “Non Compliant HTTP” are covered by the Inspection Settings profile



Understanding The Components
Inspection Settings

- Change the default settings if really needed
- Make sure you understand what you are doing



Let’s digest this!

We have three different profiles enforcing security:

Threat Prevention Profile
(installed with Threat Prevention Policy)

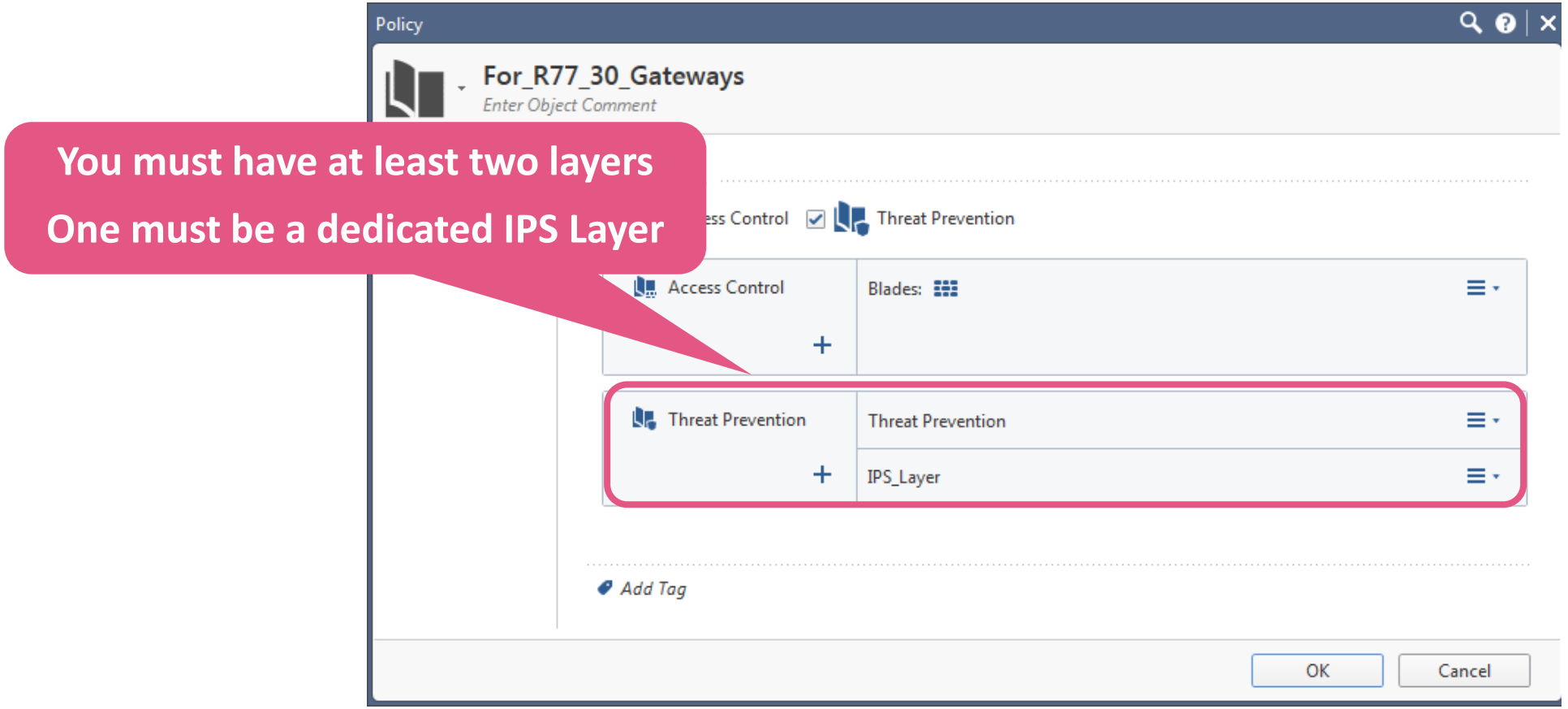
Core Protections Profile
(installed with Access Control Policy)

Inspection Settings Profile
(installed with Access Control Policy)

WORKING WITH R77.30 GATEWAYS

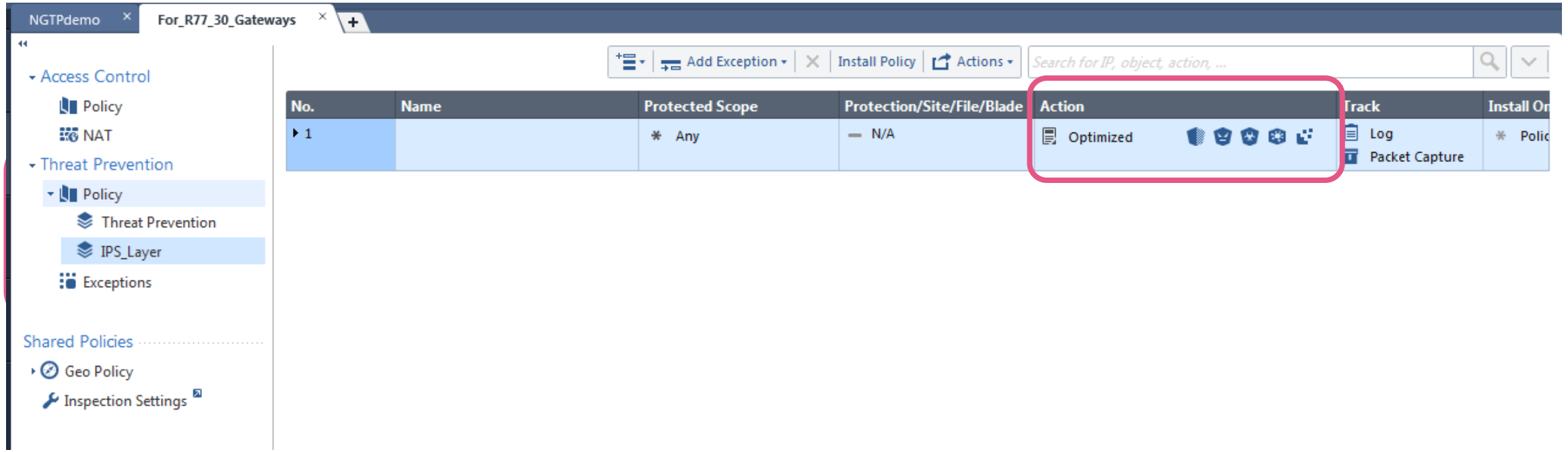
Understanding The Components
Threat Prevention Policy Layers for R77.30 Gateways

- In the Threat Prevention policy a dedicated IPS Layer is needed



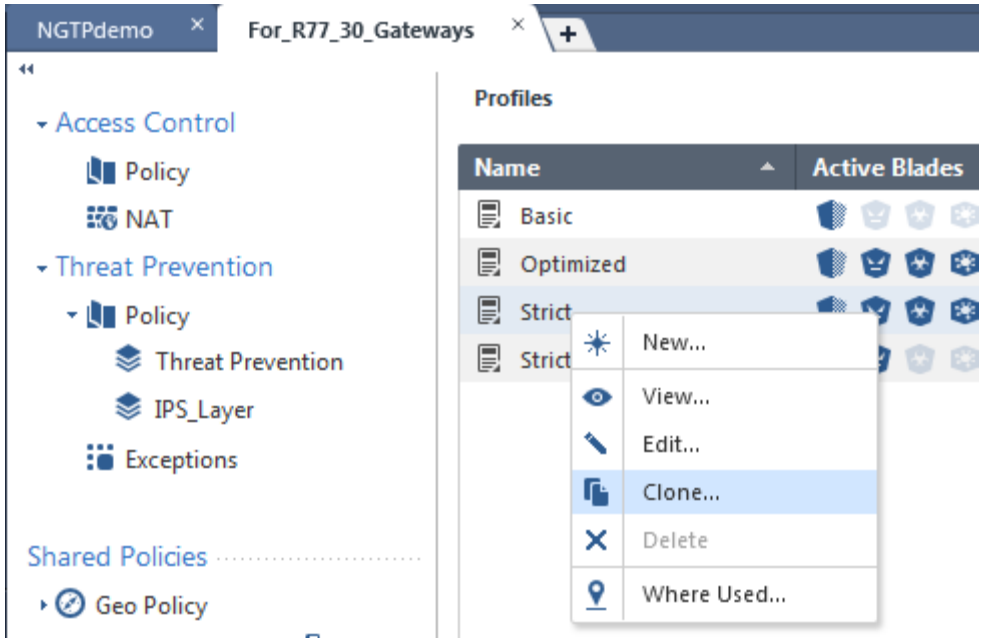
Understanding The Components
Threat Prevention Policy Layers for R77.30 Gateways

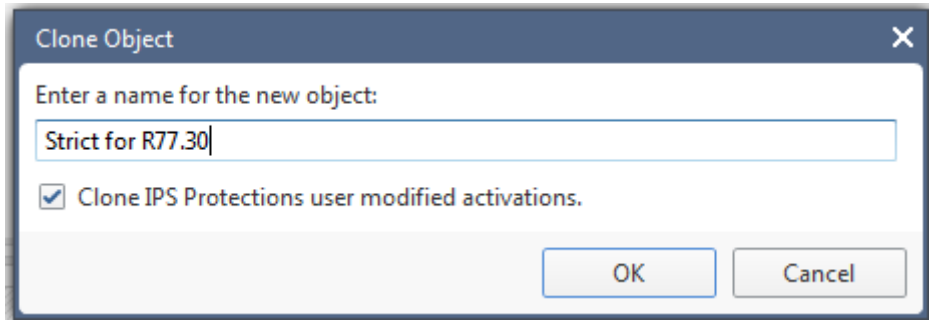
- Threat Prevention Layer and the IPS Layer will have the Optimized Profile assigned
- The Optimized Profile has all Threat Prevention Blades enabled
- This default setting will not work for an R77.30 Gateway

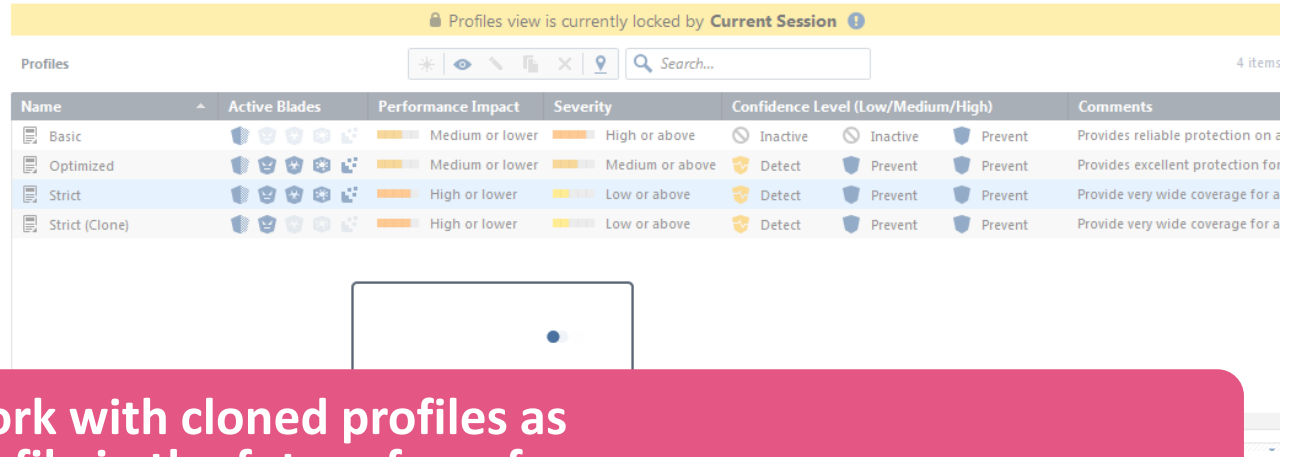


Understanding The Components
Threat Prevention Policy Layers for R77.30 Gateways

- Clone the Strict Profile and include a description related to R77.30



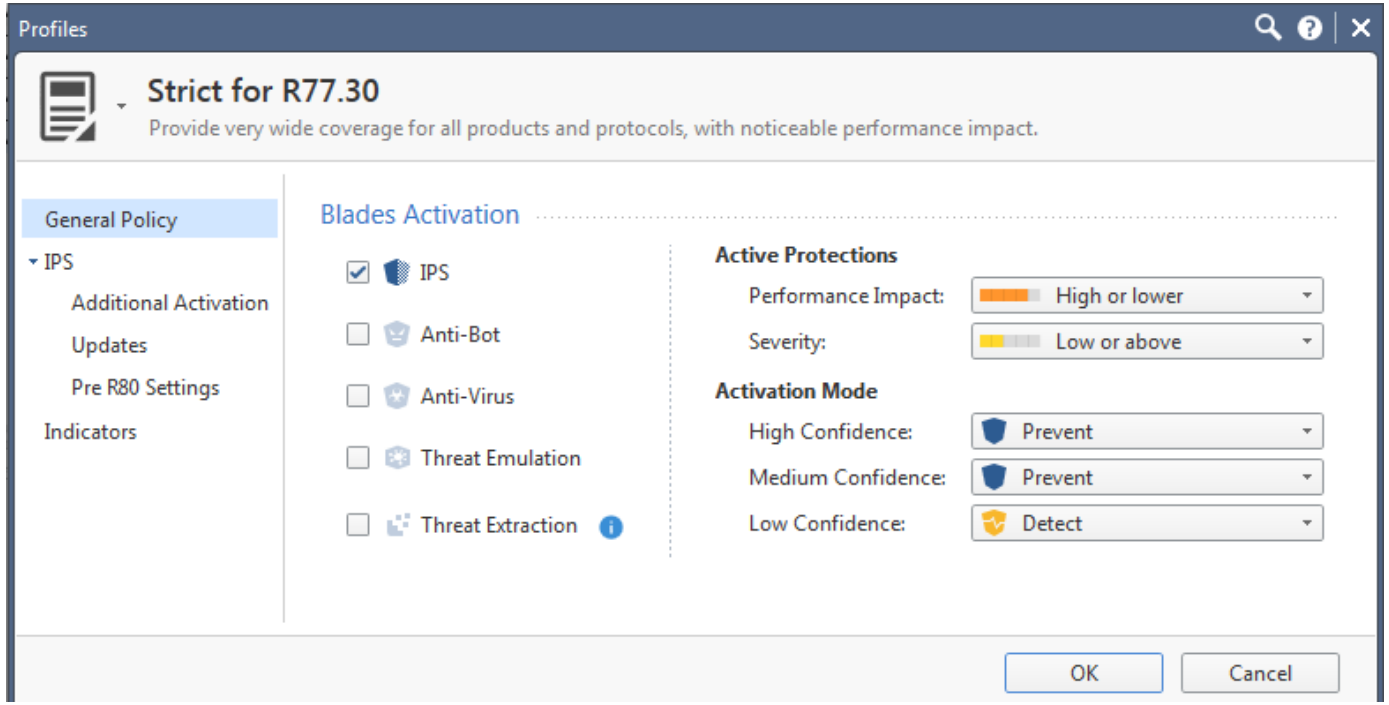


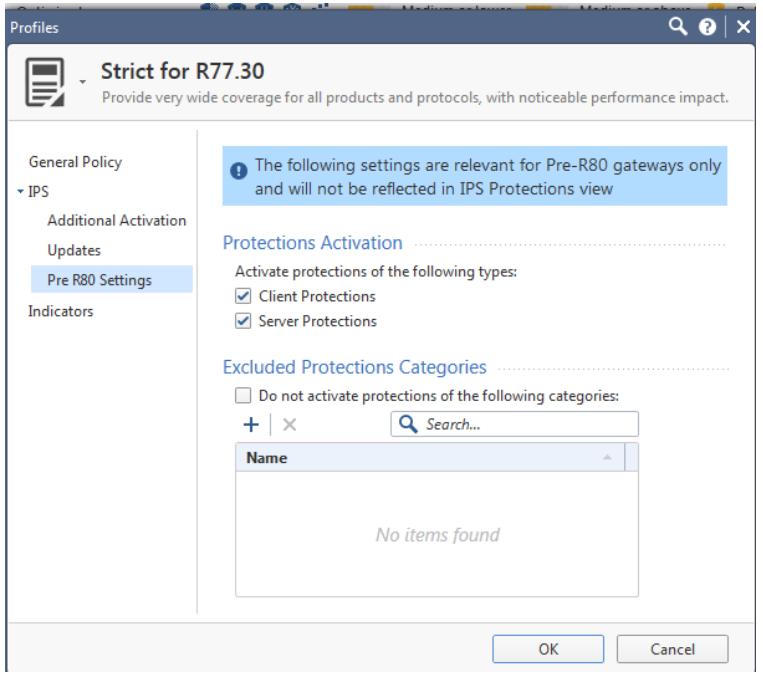


You want to work with cloned profiles as you may need the original profile in the future for reference purposes

Understanding The Components
Threat Prevention Policy Layers for R77.30 Gateways

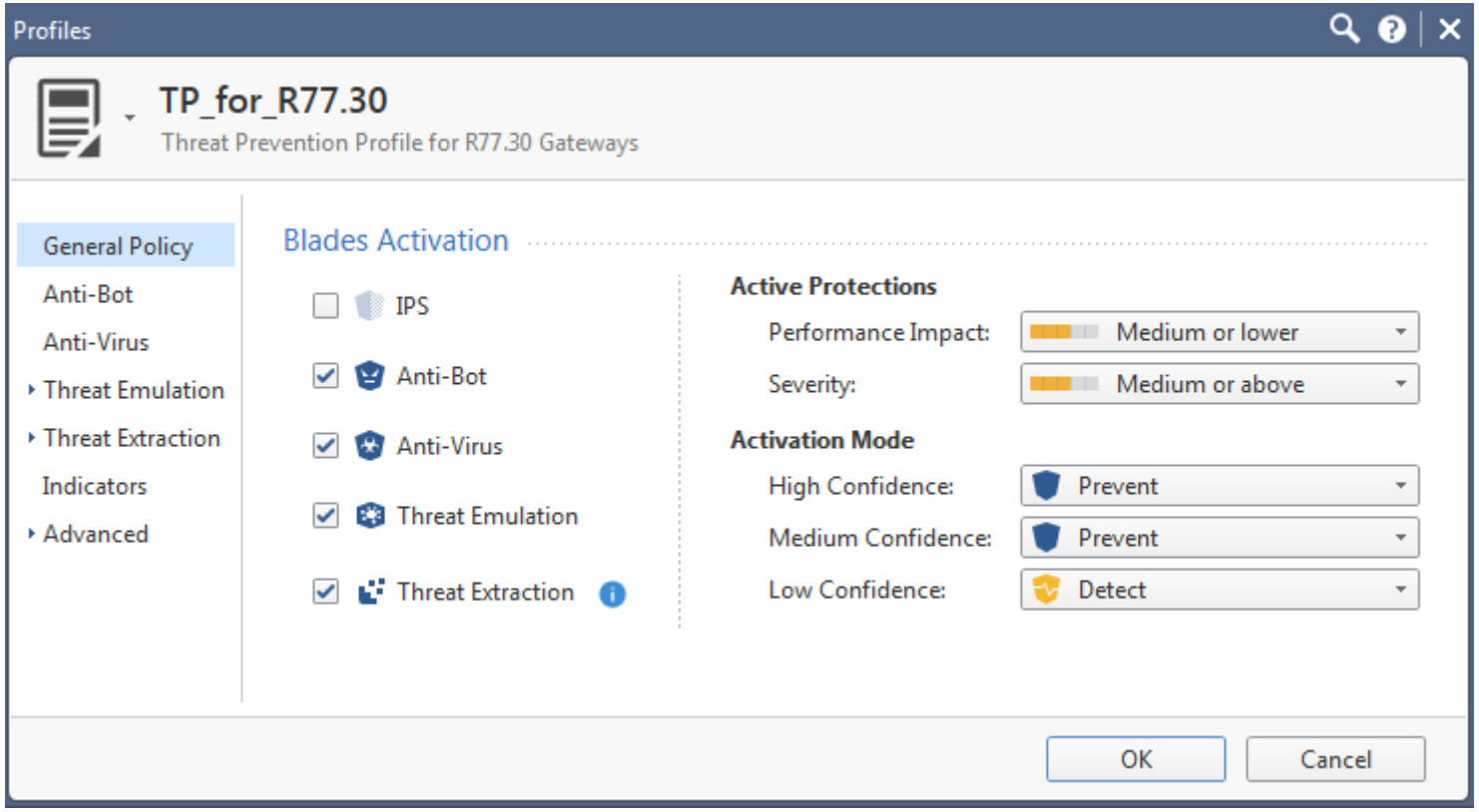
- Edit the cloned profile and disable all Blades but the IPS
- Define eventually Pre-R80 specific settings





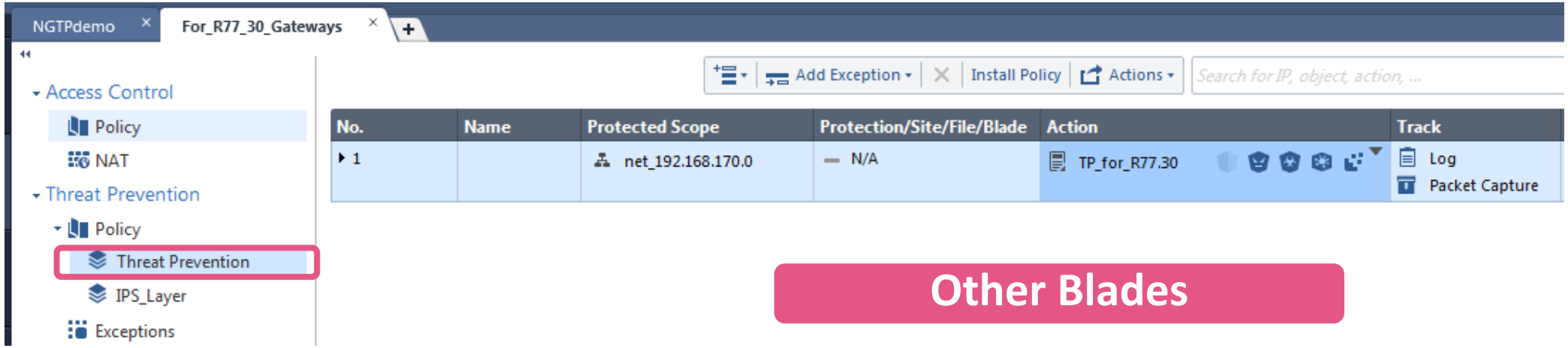
Understanding The Components
Threat Prevention Policy Layers for R77.30 Gateways

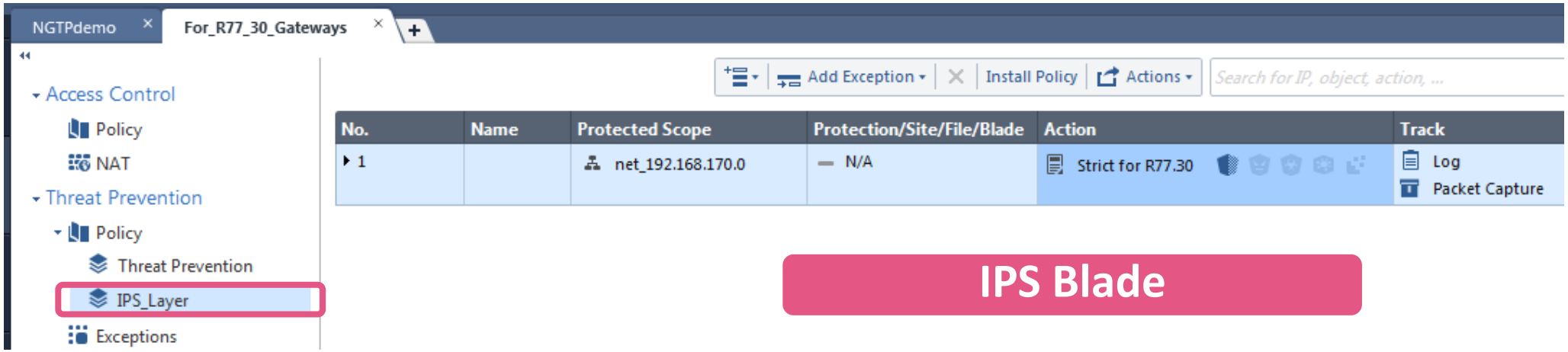
- Create a new profile for all other Threat Prevention Blades



Understanding The Components
Threat Prevention Policy Layers for R77.30 Gateways

- Create policy rules that use the profiles created as action



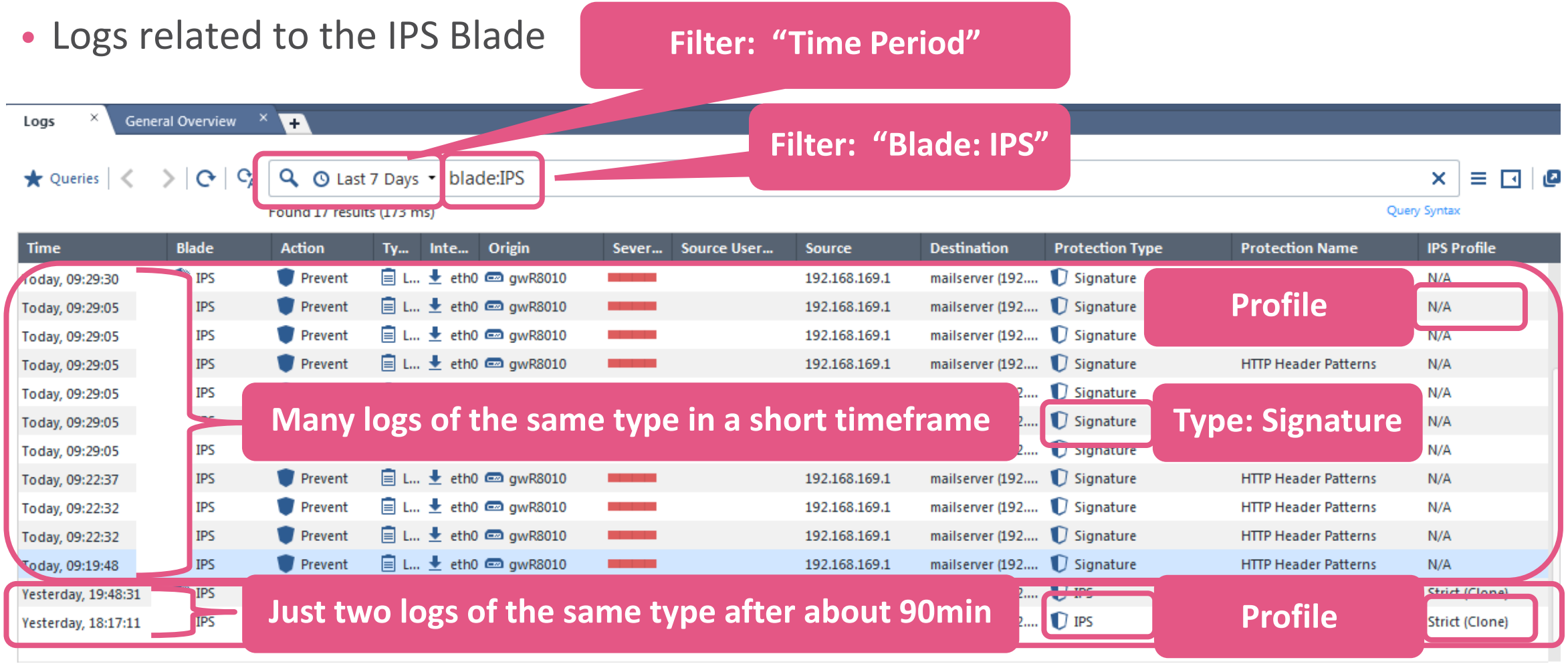


IPS LOGGING

Packet Capture And Suppressed Logs

ThreatCloud protections and Core protections logging

- Logs related to the IPS Blade



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?

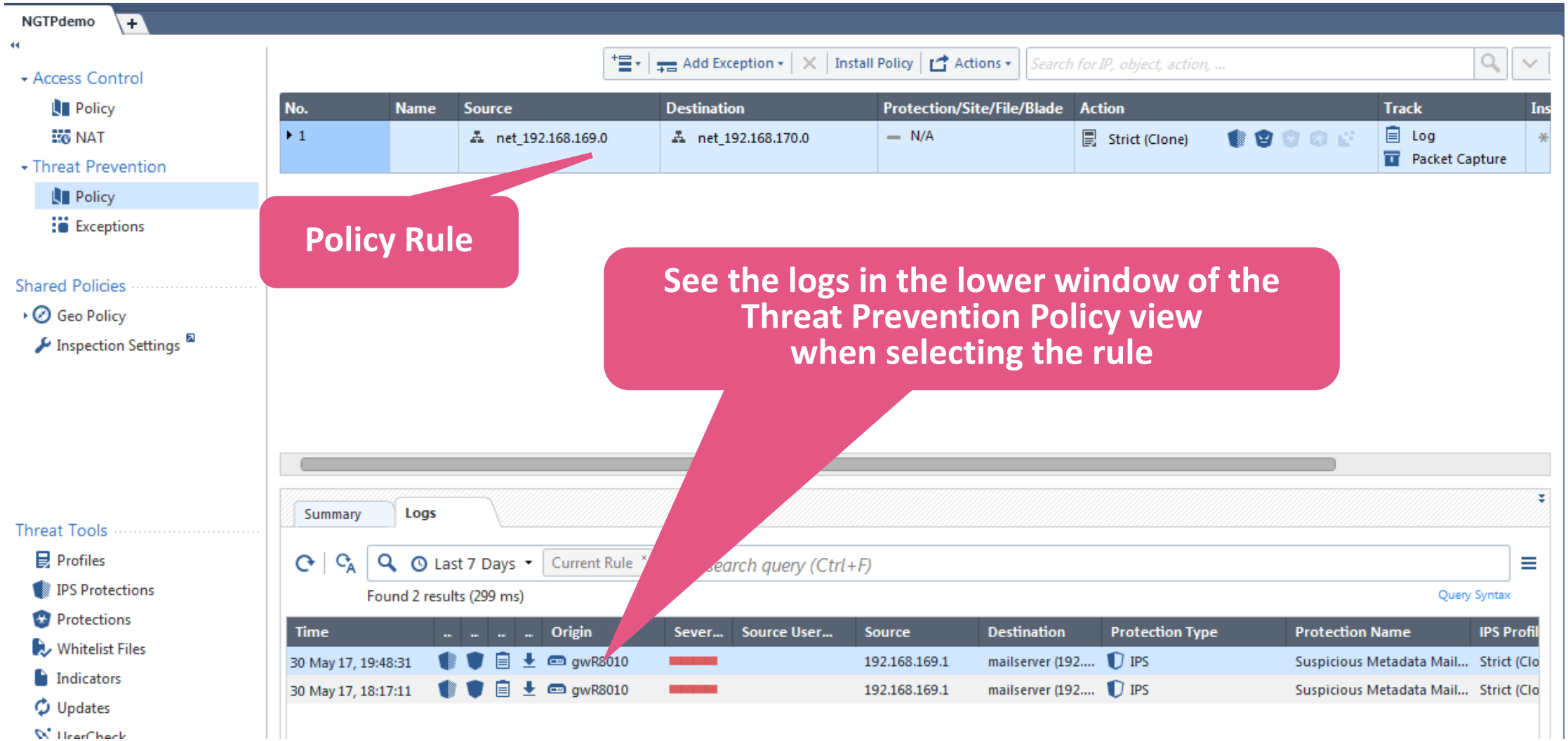
- By default the **first signature match** will be **logged and** a **packet capture** will be taken
- If the same **signature** will **match again in the period of less than two minutes**, no additional packet capture will be taken and no new log message will be sent
- The "**suppressed logs" counter** 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

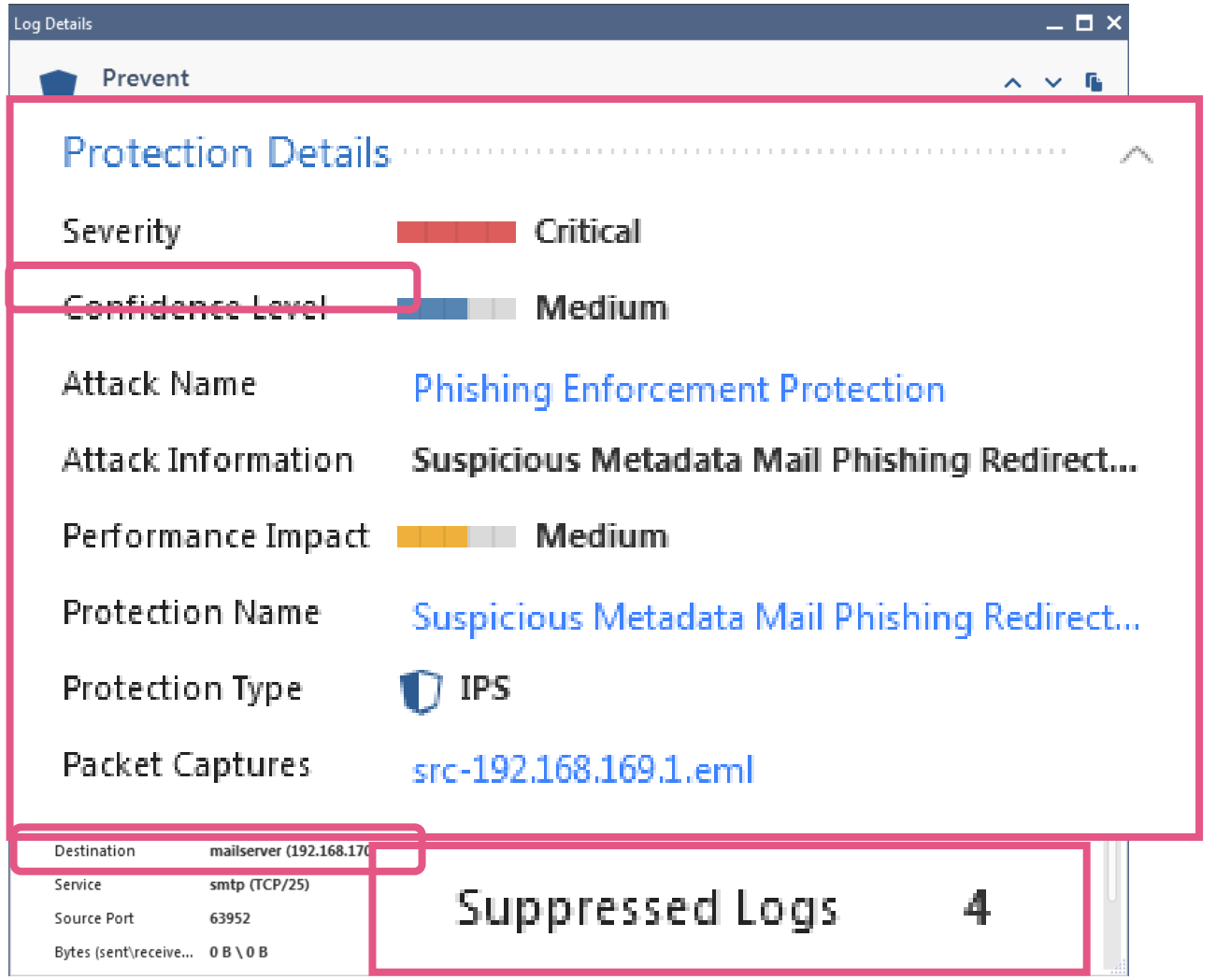
ThreatCloud protections logging



Packet Capture And Suppressed Logs

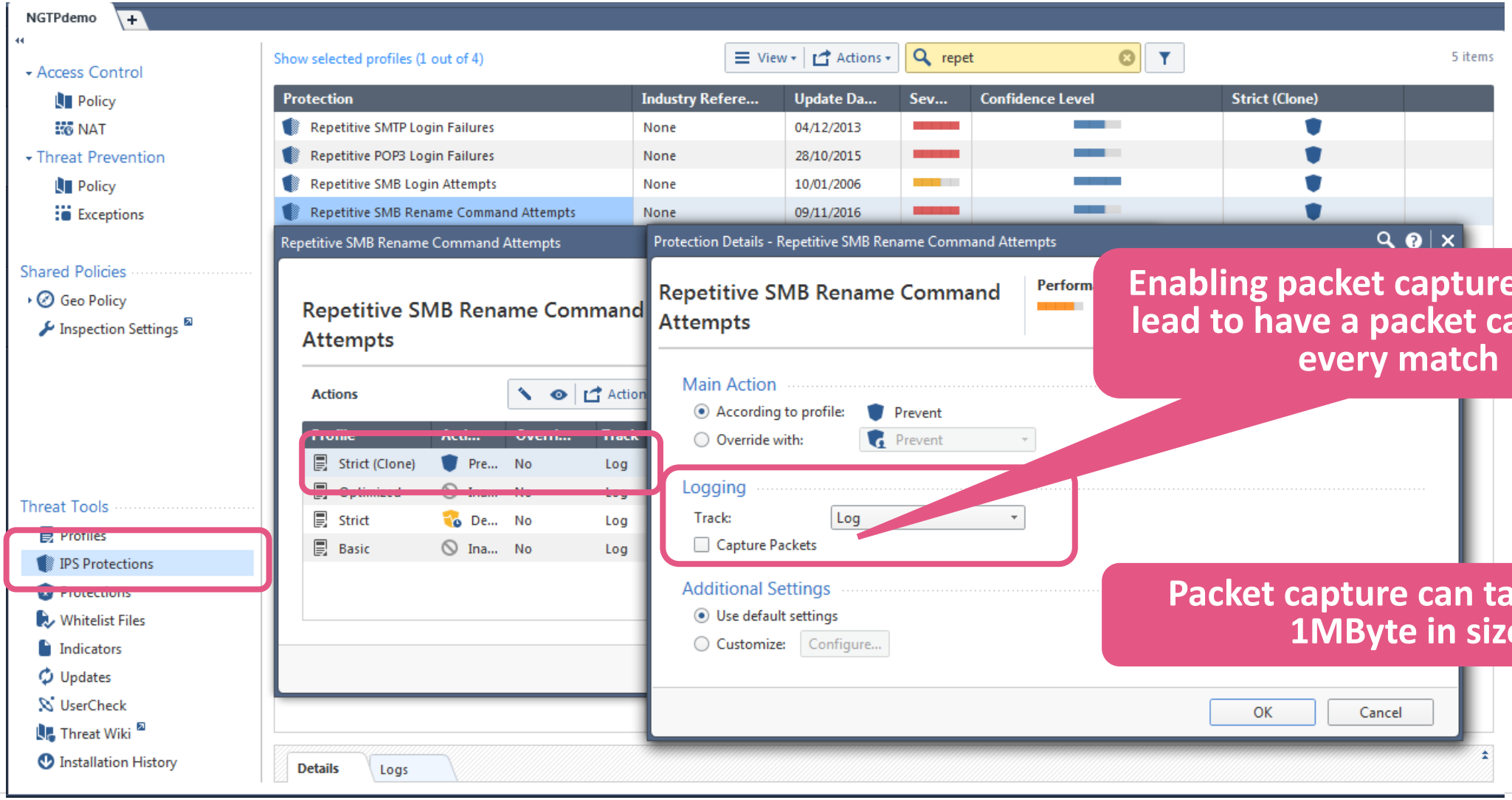
ThreatCloud protections logging

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



Packet Capture And Suppressed Logs

Configuring packet capture for ThreatCloud protections (signatures)

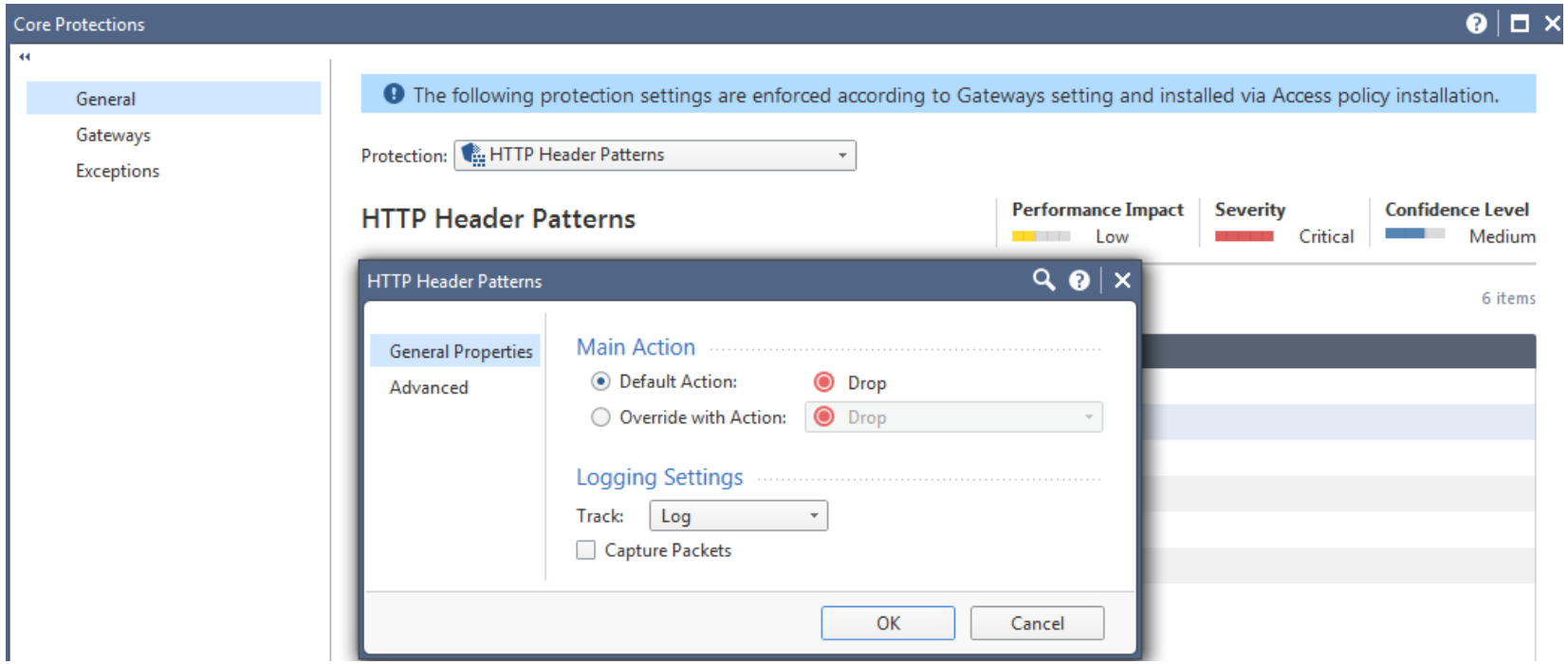


Packet Capture And Suppressed Logs

Core protections and Inspection settings matching

When Core protections or Inspection settings are matching

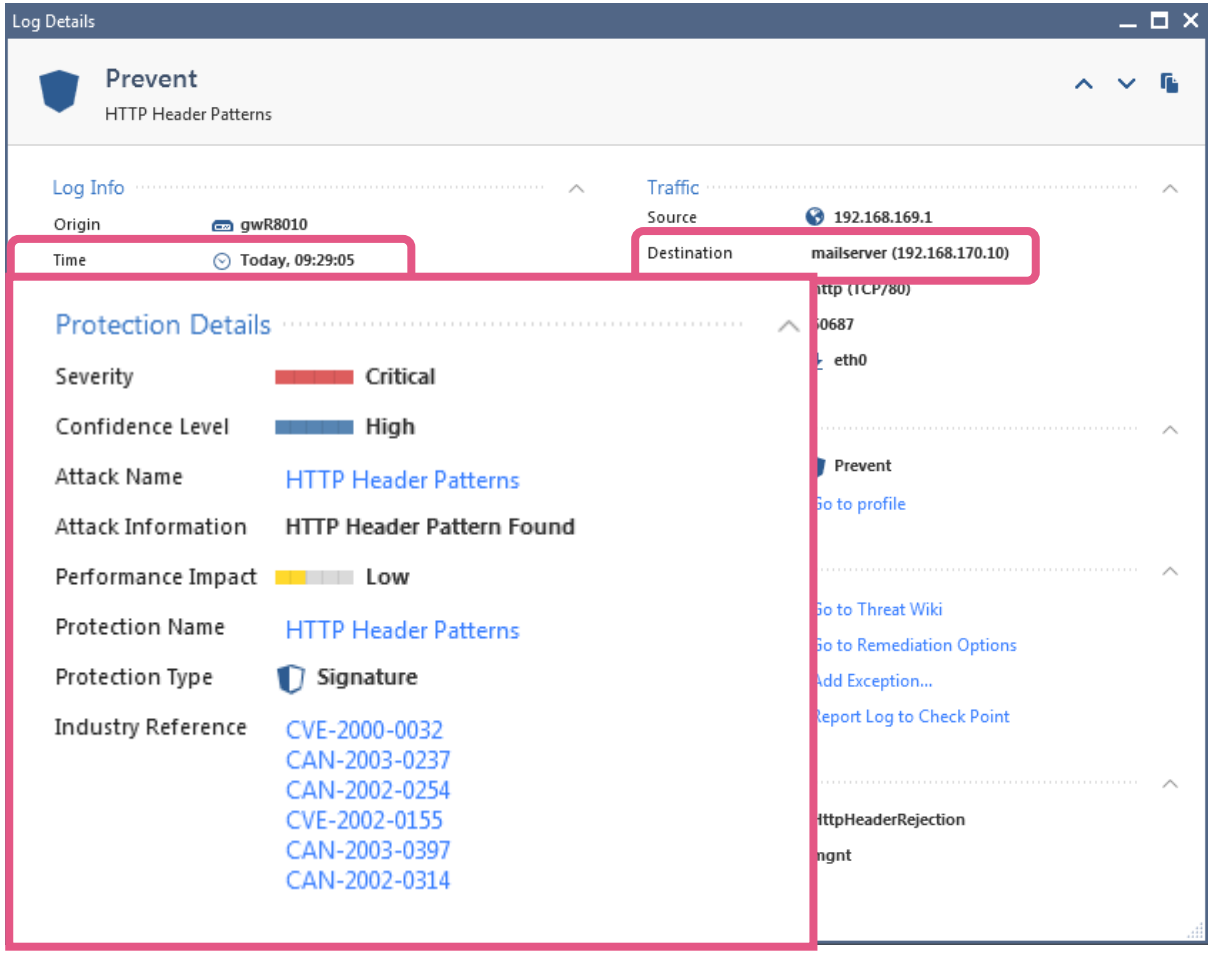
- No log suppression is performed
- No packet capture is performed unless the respective setting is enabled



Packet Capture And Suppressed Logs

Core protections logging

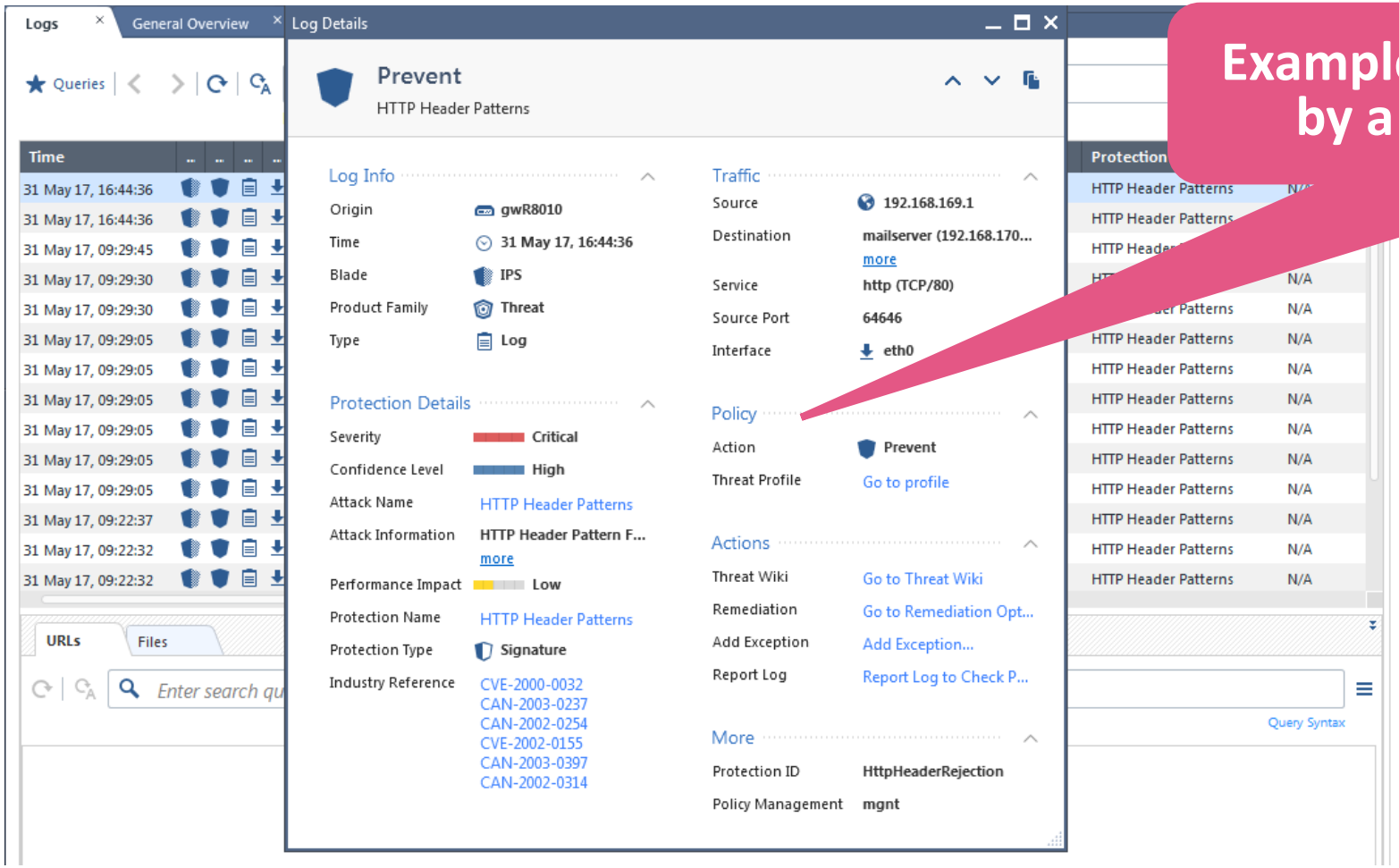
- Time
- Target
- Attack type



Packet Capture And Suppressed Logs

Core protections and Inspection settings matching

Check Point
SOFTWARE TECHNOLOGIES LTD



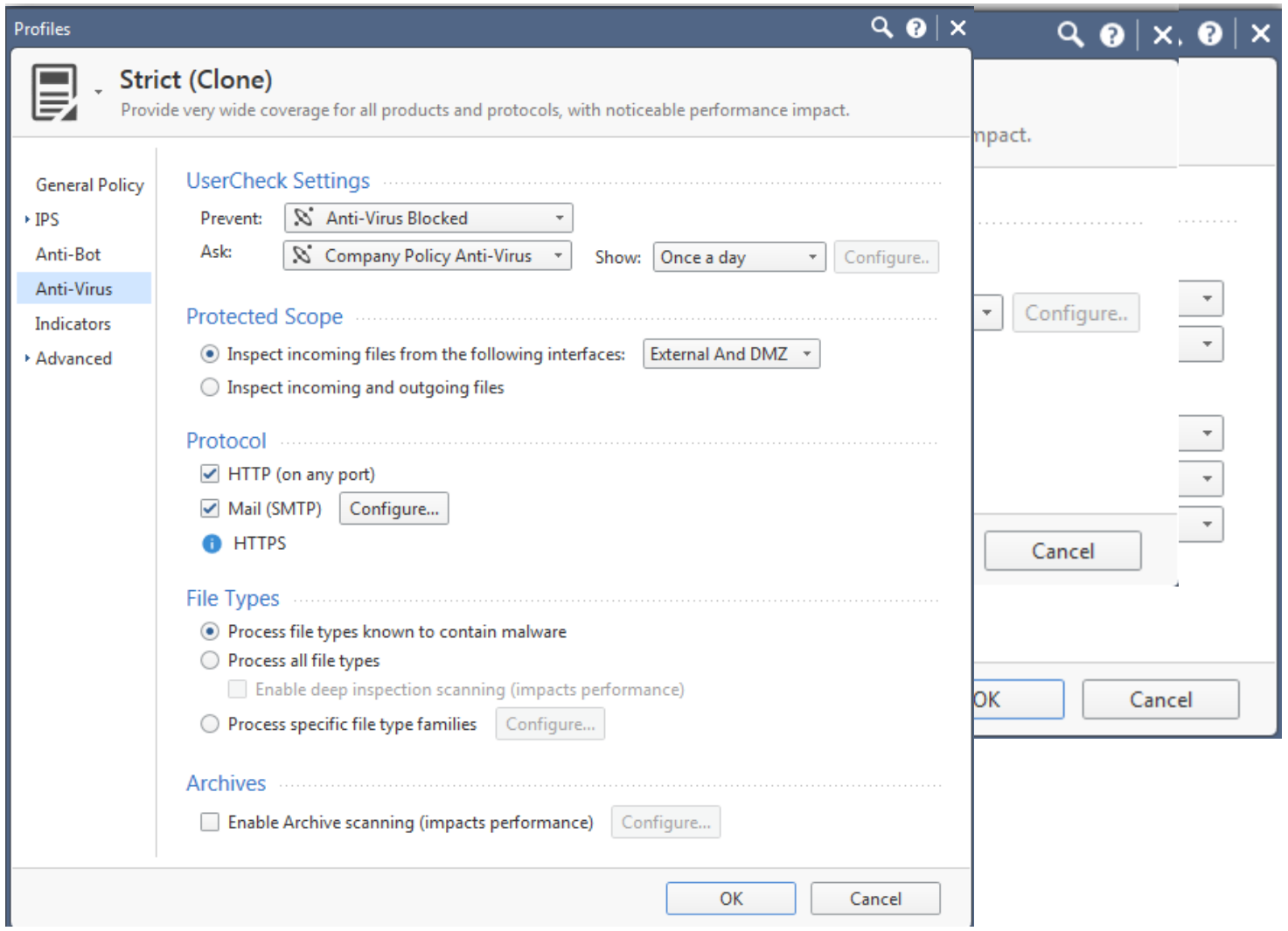
Example of a log message generated by a Core protecting matching

ANTI-VIRUS
ANTI-BOT

Anti-Virus and Anti-Bot

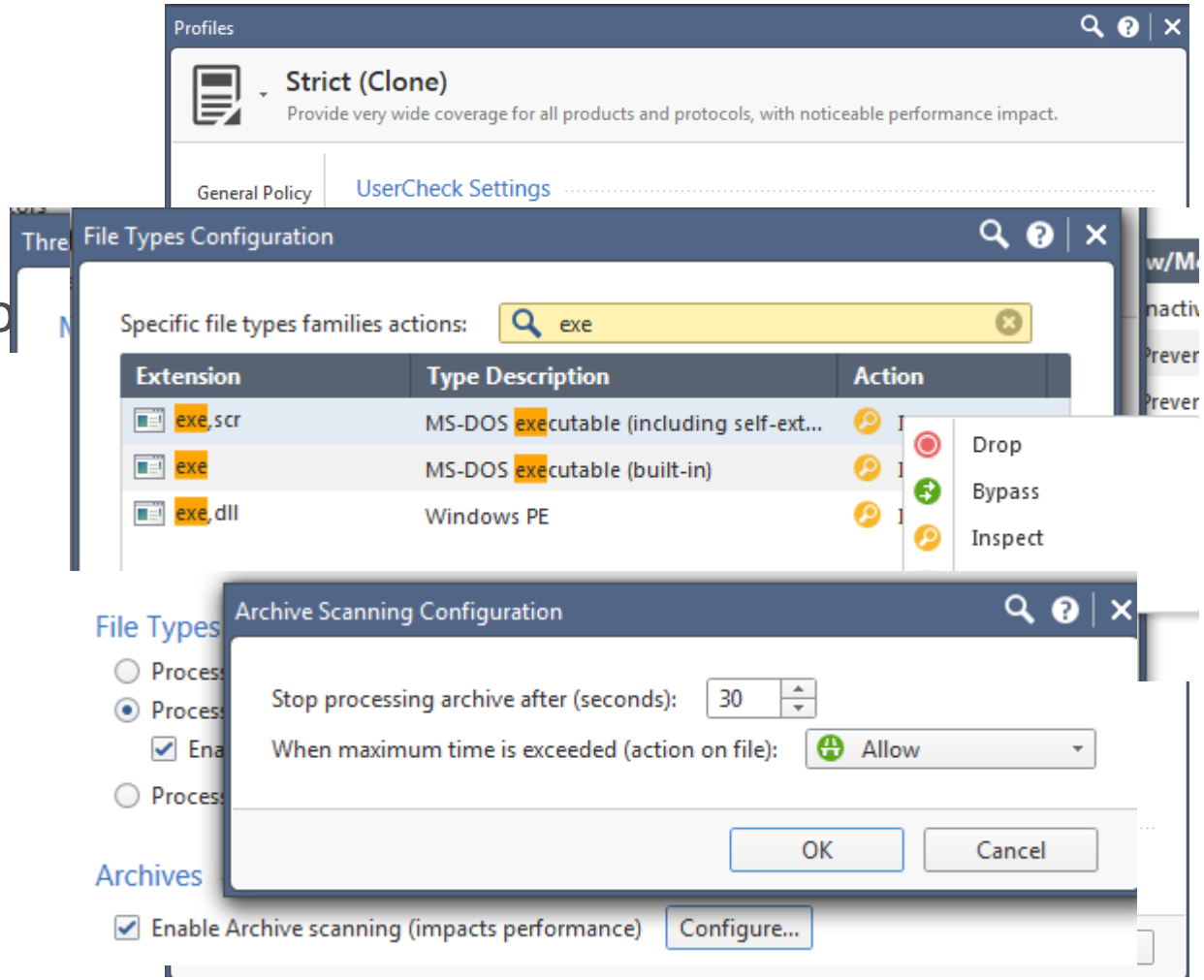
Manage their settings in the profile

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



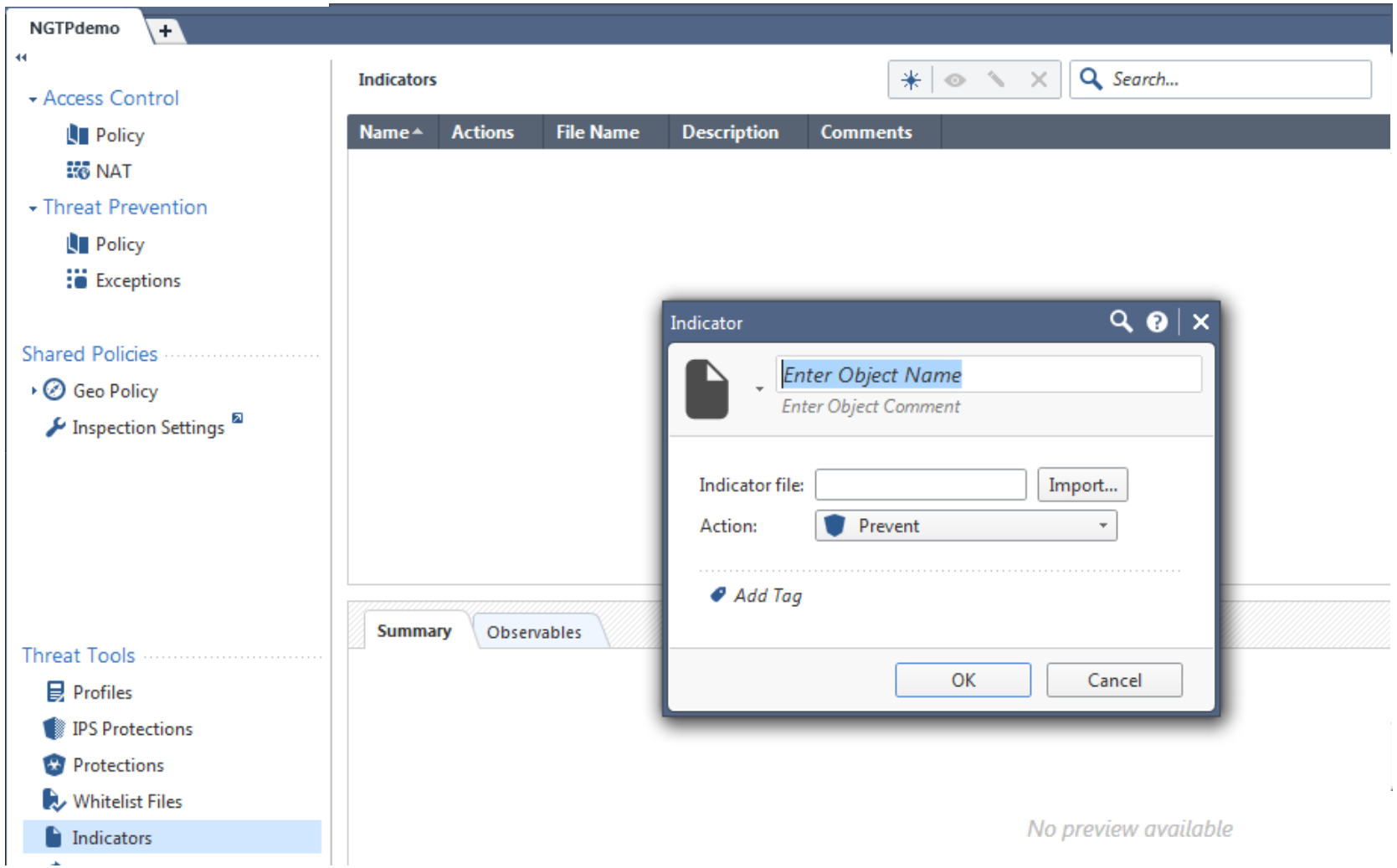
Anti-Virus and Anti-Bot
Manage their settings in the profile

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



Anti-Virus and Anti-Bot
Manage their settings in the profile

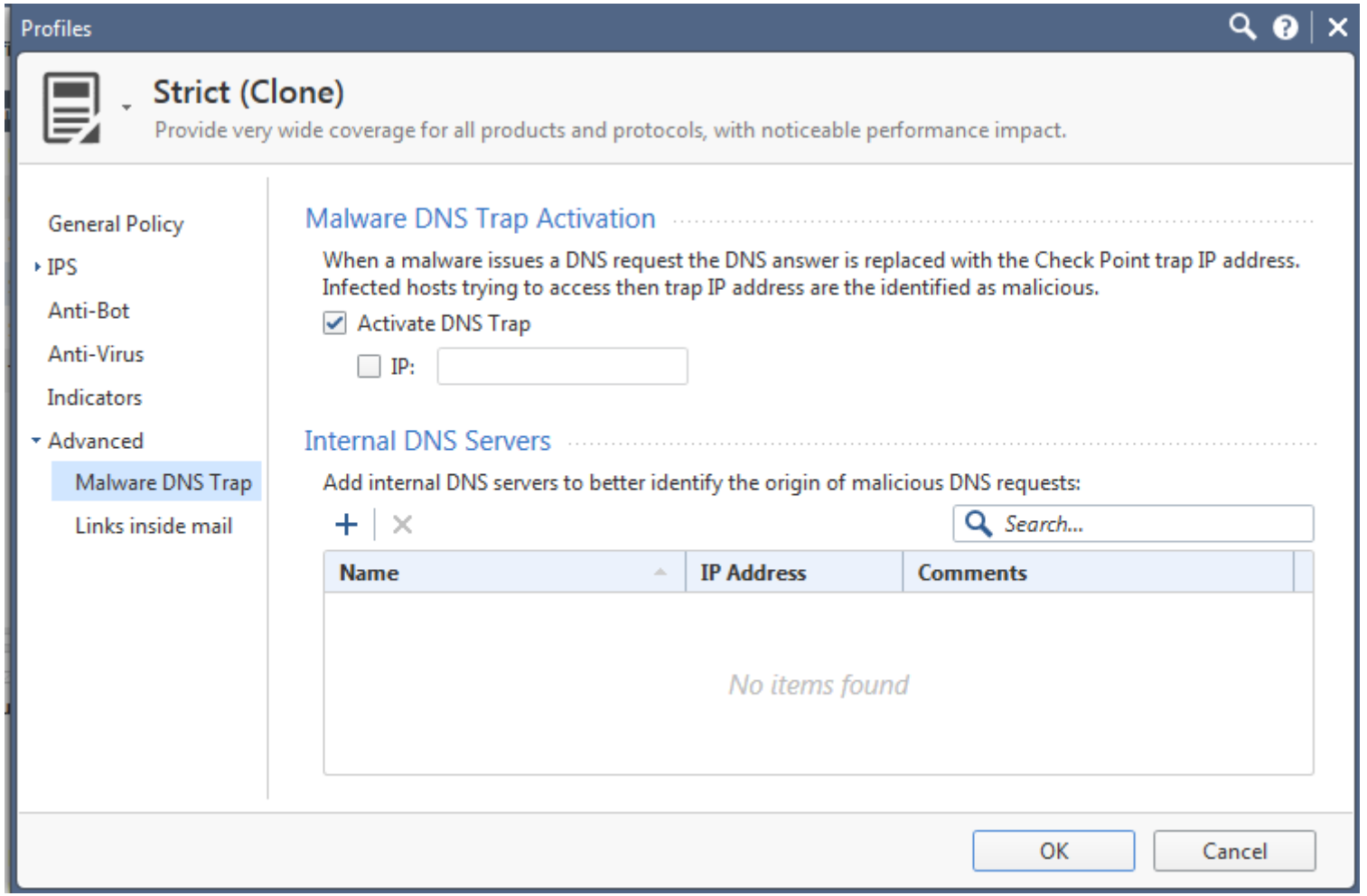
- Manage indicators
- Import indicators using the “Indicators” menu under the Threat Tools section



Anti-Virus and Anti-Bot

Manage their settings in the profile

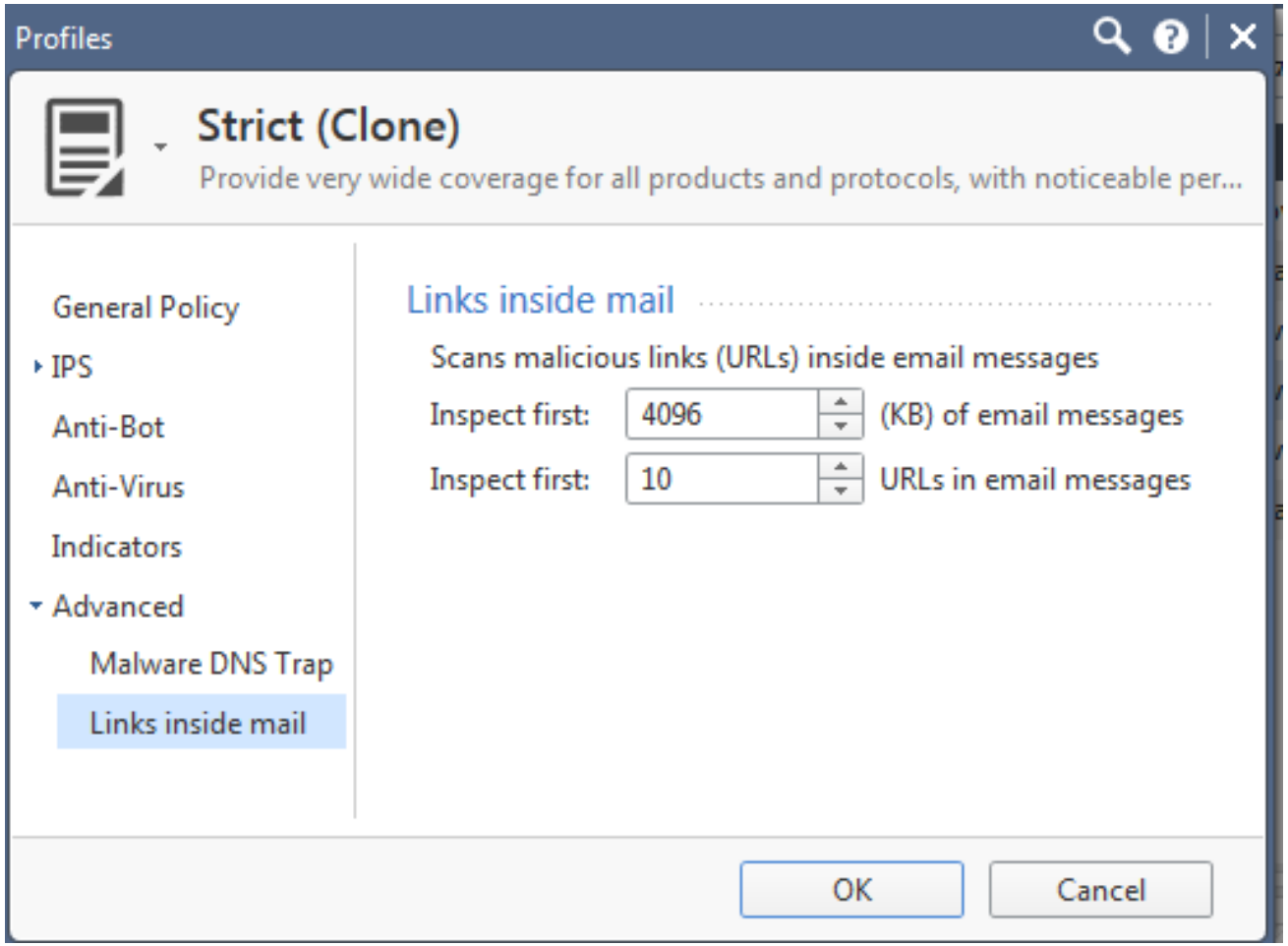
- By default a DNS query for a known Botnet is answered with the IP Address of the Check Point sinkhole
- Botnet communication can be analyzed by Check Point sinkhole
- Define corporate DNS Server IP Addresses



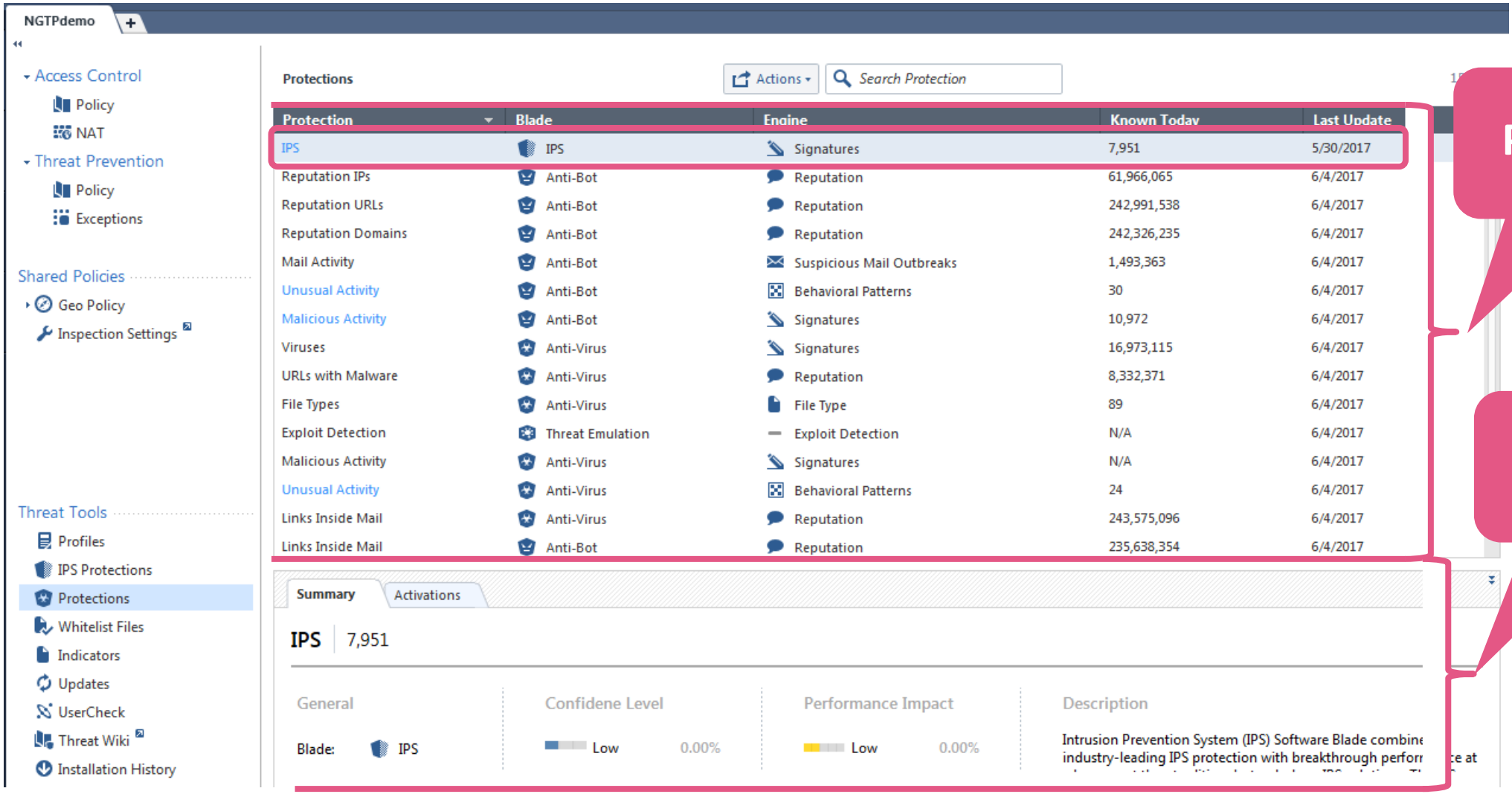
Anti-Virus and Anti-Bot

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



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

Summary | Activations

Reputation IPs 61,966,065

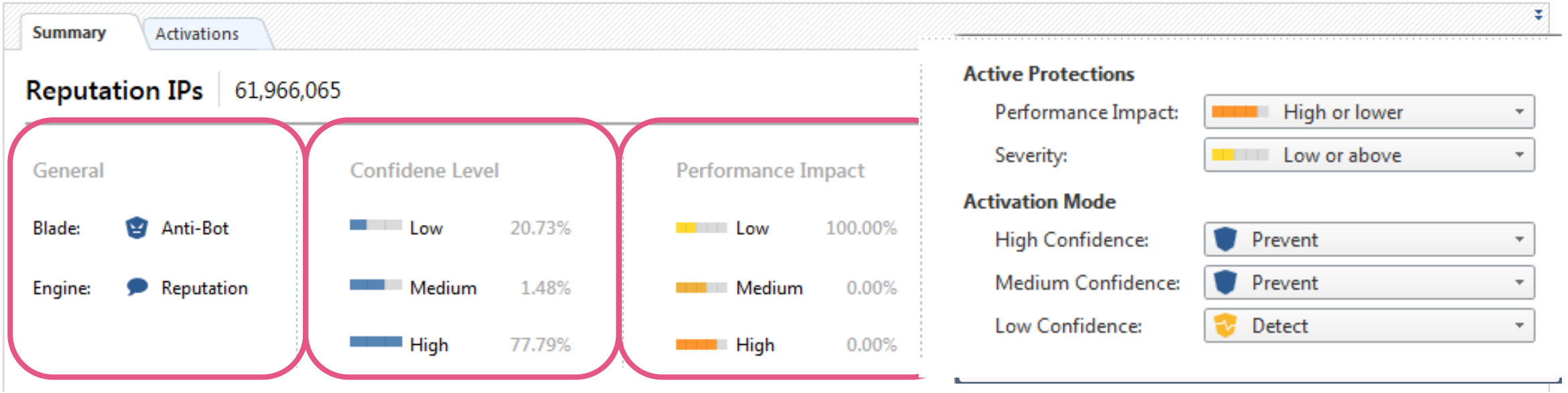
General	Confidene Level	Performance Impact	Description
Blade: Anti-Bot	Low 20.73%	Low 100.00%	For Reputation IPs protections, the Reputation layer of the ThreatSpect engine prevents "call home" connections to

Protections

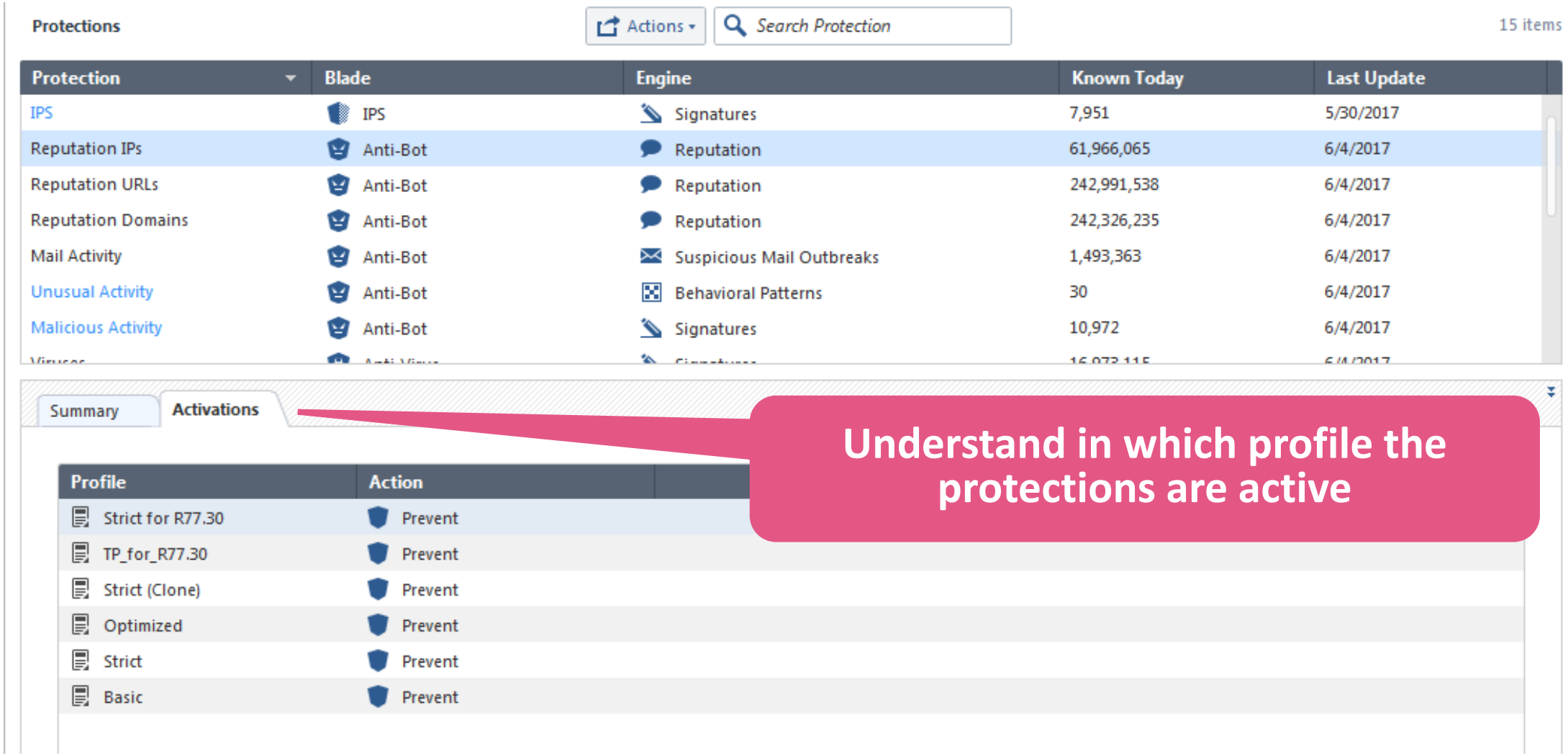
Details of selected

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



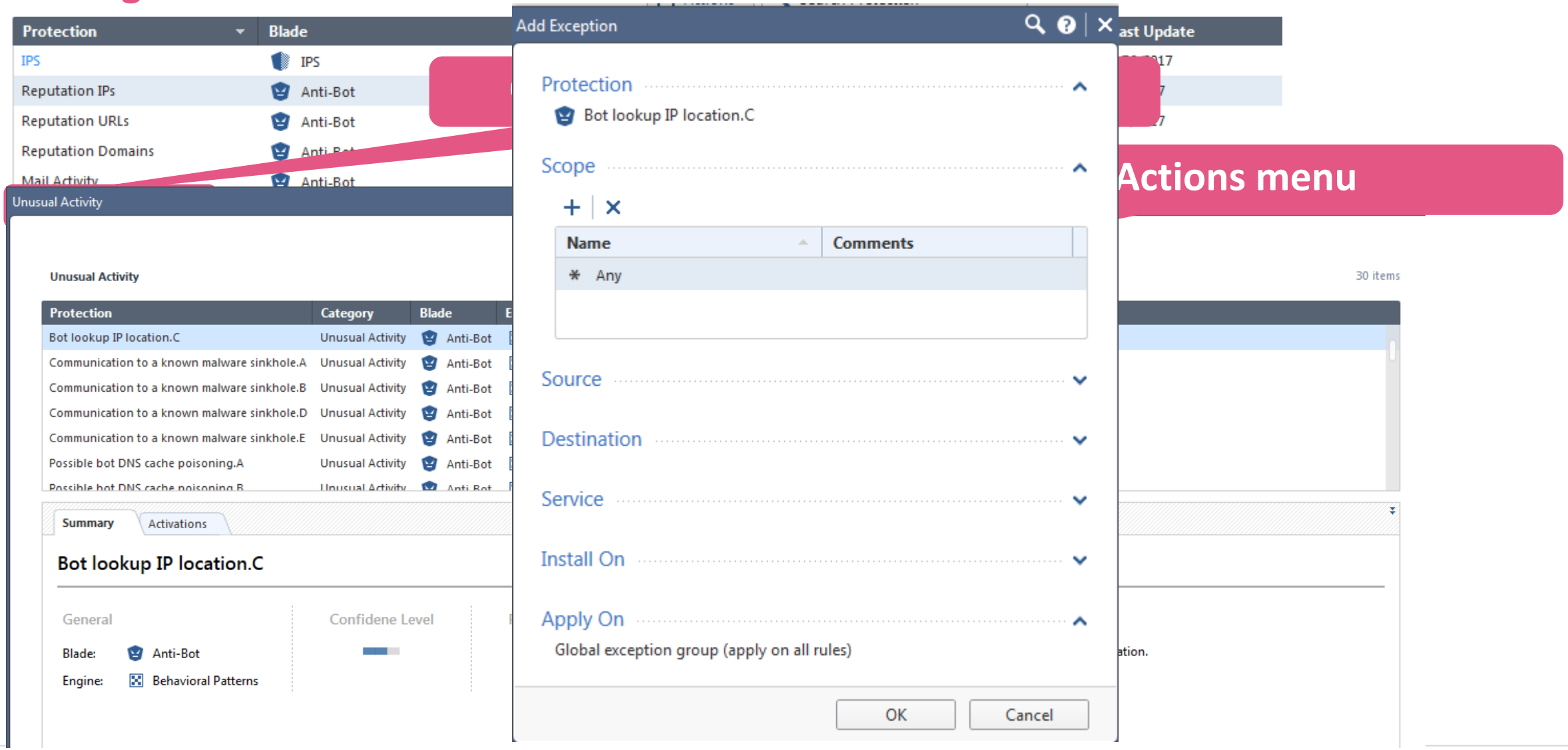
Anti-Virus and Anti-Bot
Manage Protections



Understand in which profile the protections are active

Anti-Virus and Anti-Bot

Manage Protections



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.

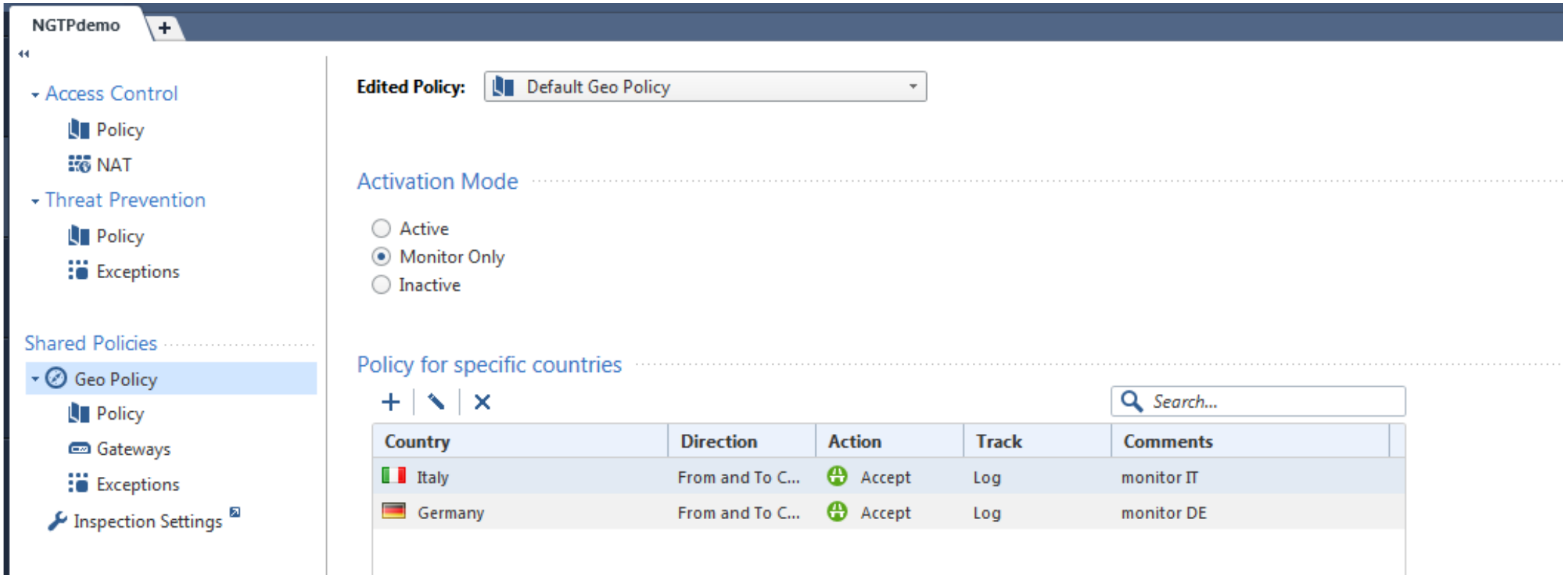
For Anti-Virus file:

- *# 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

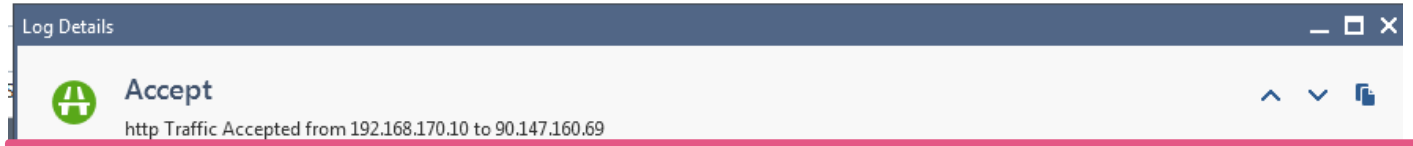
Geo Protections

- Enforced using a profile
- Installed with the Access Policy



Geo Protections

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




```
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, AsychronicNotif, 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
```

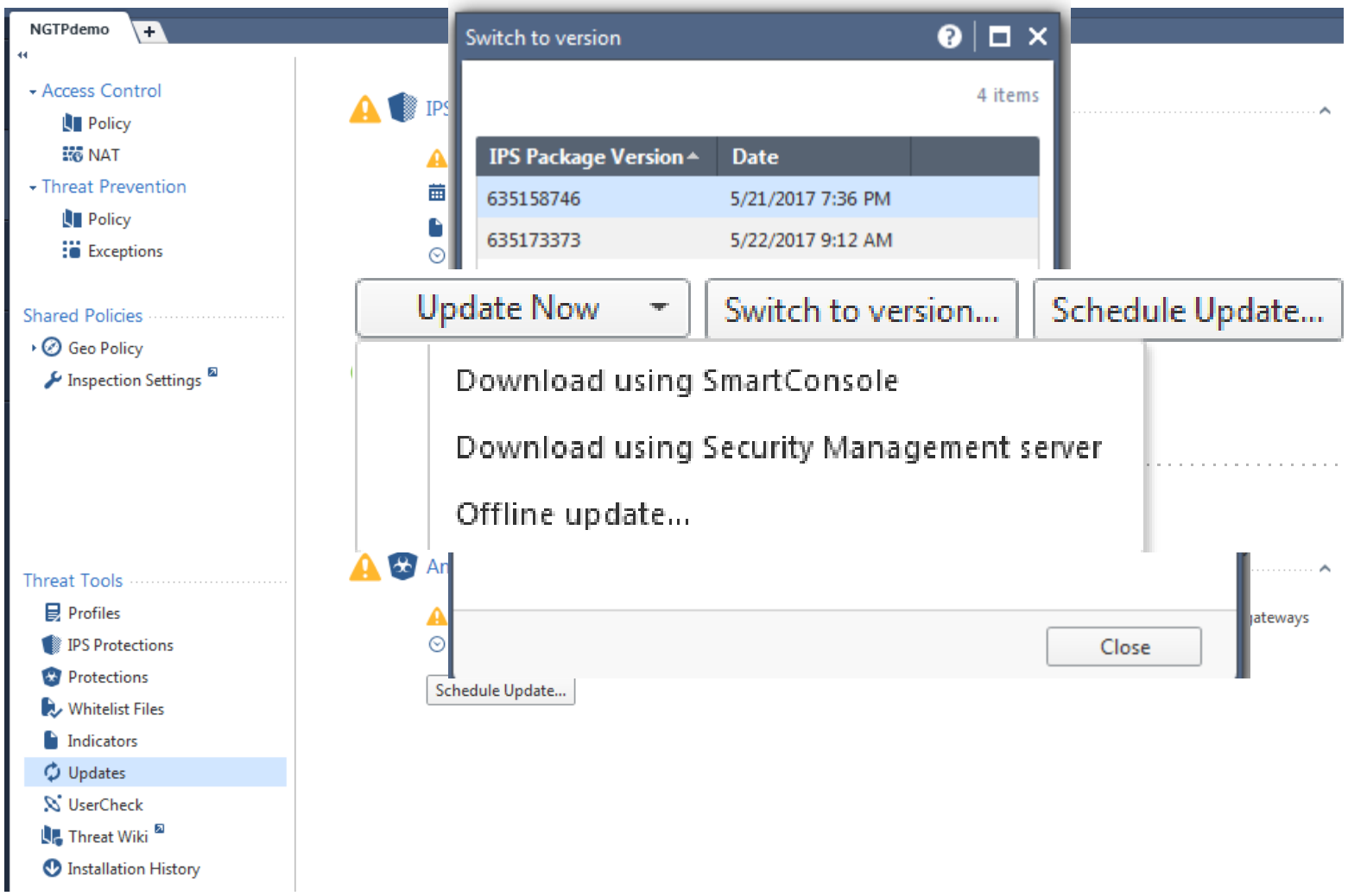
Updating Threat Prevention Protections
Challenges of the past

- 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



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