Application Control/URL Filtering

Module 9: Application Control/URL Filtering

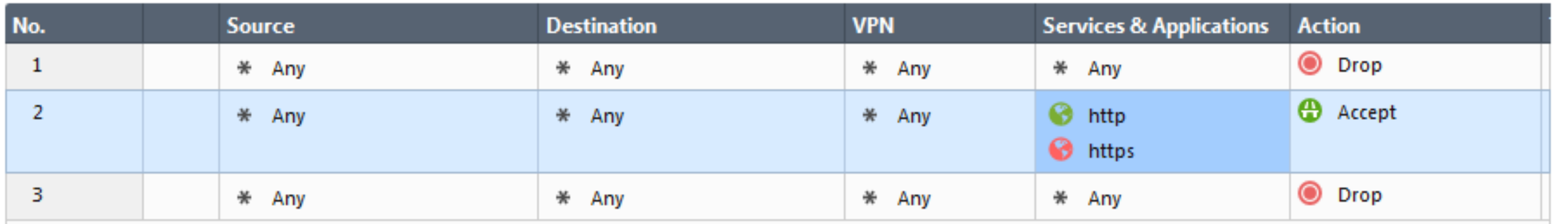
Instructor: Kim Winfield

Objectives

- Create and implement an Application Control Policy
- Create a URL Filtering Policy to block undesirable web sites for employees
- Use SSL Inspection to inspect traffic to Secure Web Sites

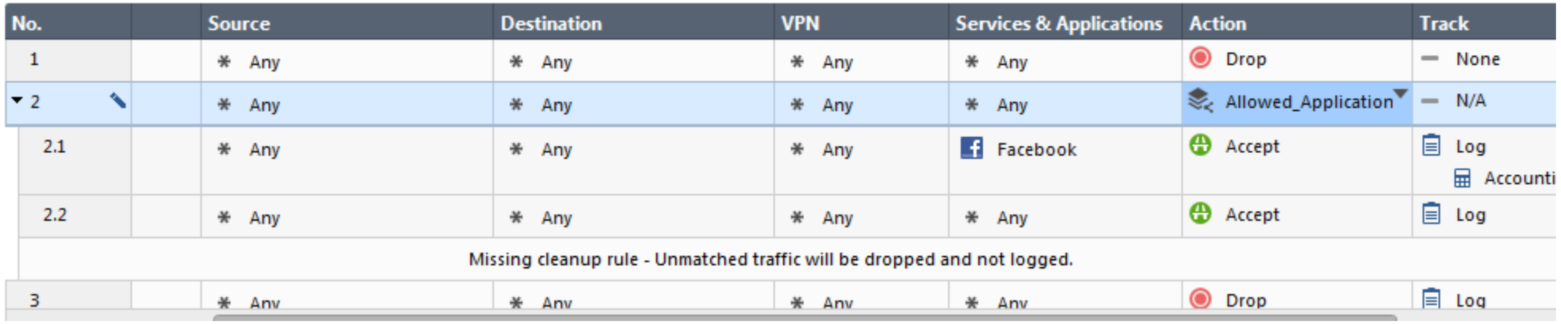
Application Control

- Traditional Firewall policies only limit traffic by destination IP address and Service



No.		Source	Destination	VPN	Services & Applications	Action
1		✱ Any	✱ Any	✱ Any	✱ Any	Drop
2		✱ Any	✱ Any	✱ Any	http https	Accept
3		✱ Any	✱ Any	✱ Any	✱ Any	Drop

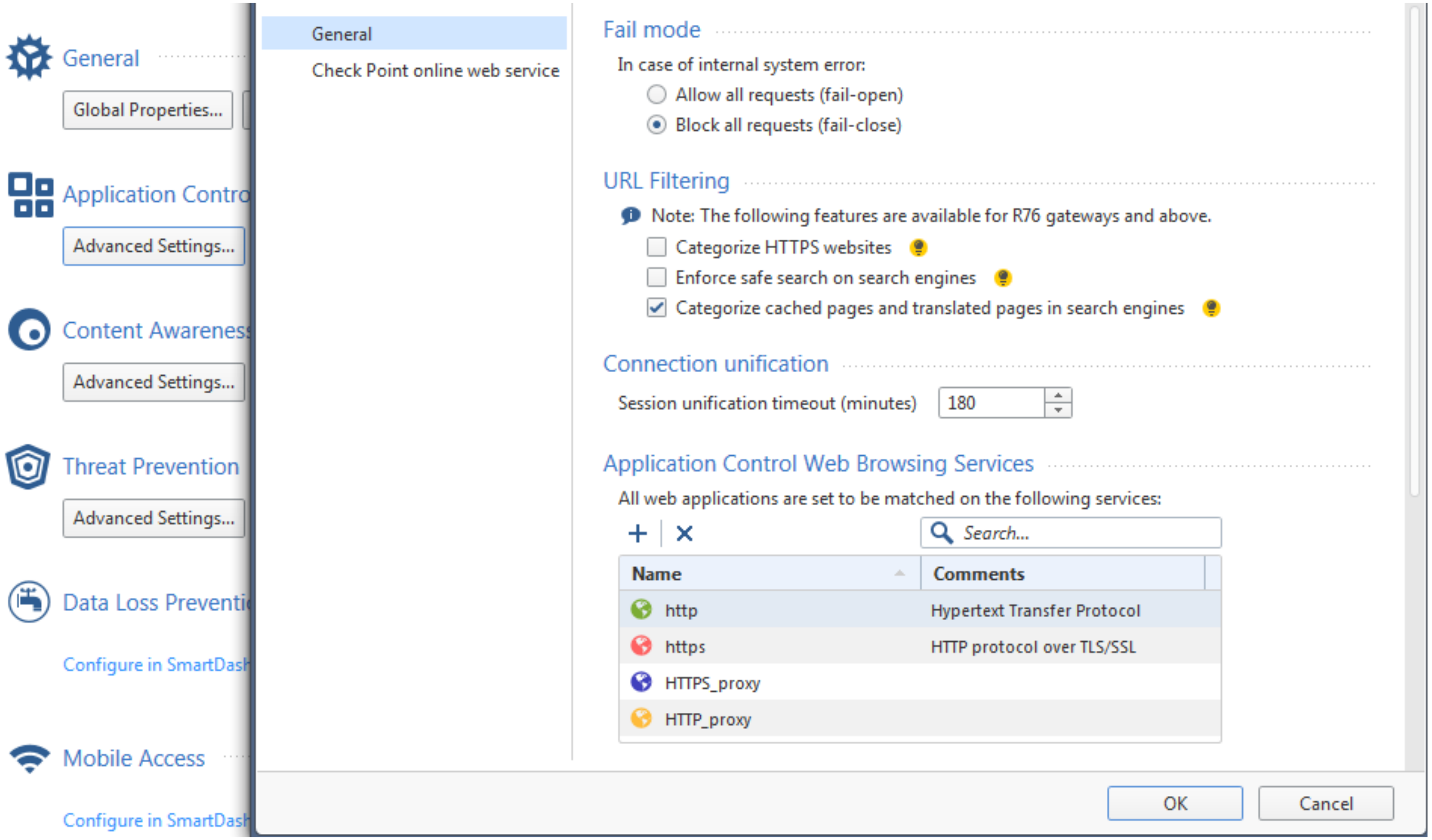
- Application Control allows access based on application signatures



No.		Source	Destination	VPN	Services & Applications	Action	Track
1		✱ Any	✱ Any	✱ Any	✱ Any	Drop	None
2		✱ Any	✱ Any	✱ Any	✱ Any	Allowed_Application	N/A
2.1		✱ Any	✱ Any	✱ Any	Facebook	Accept	Log Accounti
2.2		✱ Any	✱ Any	✱ Any	✱ Any	Accept	Log
Missing cleanup rule - Unmatched traffic will be dropped and not logged.							
3		✱ Any	✱ Any	✱ Any	✱ Any	Drop	Log

Application Control

- Manage Settings
- Blades



General

Global Properties...

Application Contro

Advanced Settings...

Content Awarenes

Advanced Settings...

Threat Prevention

Advanced Settings...

Data Loss Preventi

Configure in SmartDash

Mobile Access

Configure in SmartDash

Fail mode

In case of internal system error:

○ Allow all requests (fail-open)

● Block all requests (fail-close)

URL Filtering

Note: The following features are available for R76 gateways and above.

□ Categorize HTTPS websites

□ Enforce safe search on search engines

☑ Categorize cached pages and translated pages in search engines

Connection unification

Session unification timeout (minutes) 180

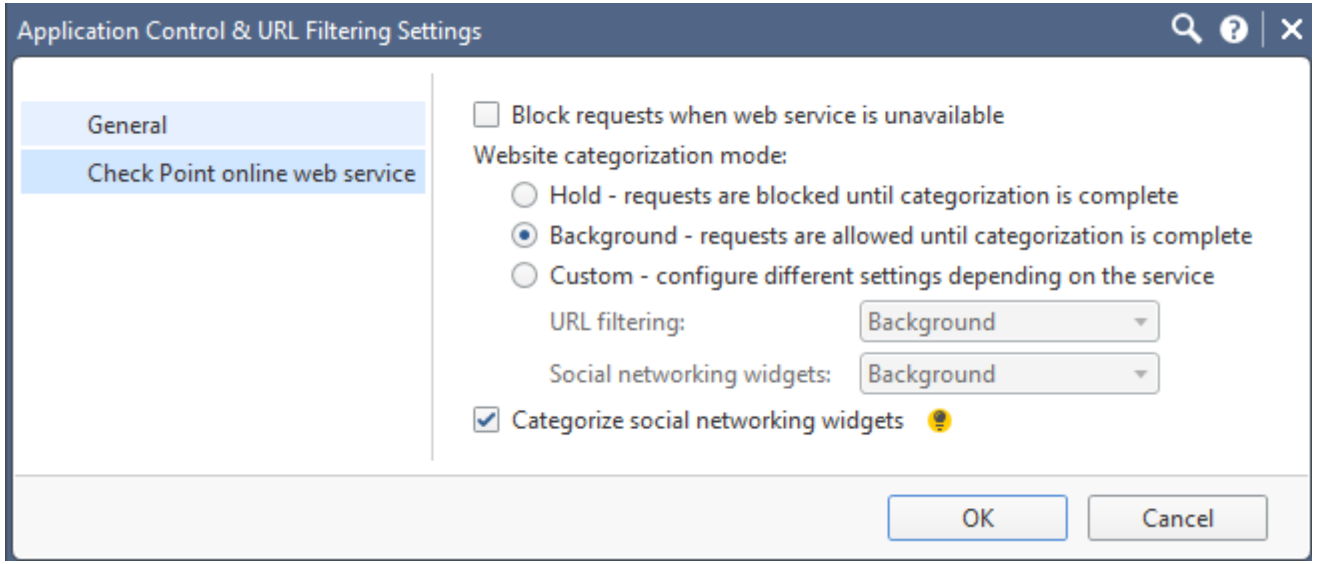
Application Control Web Browsing Services

All web applications are set to be matched on the following services:

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

Application Control

- Settings for Online Web Service
  - Hold
  - Background
  - Custom



Application Control & URL Filtering Settings
General
Check Point online web service
OK
Cancel

□ Block requests when web service is unavailable

Website categorization mode:

○ Hold - requests are blocked until categorization is complete
● Background - requests are allowed until categorization is complete
○ Custom - configure different settings depending on the service

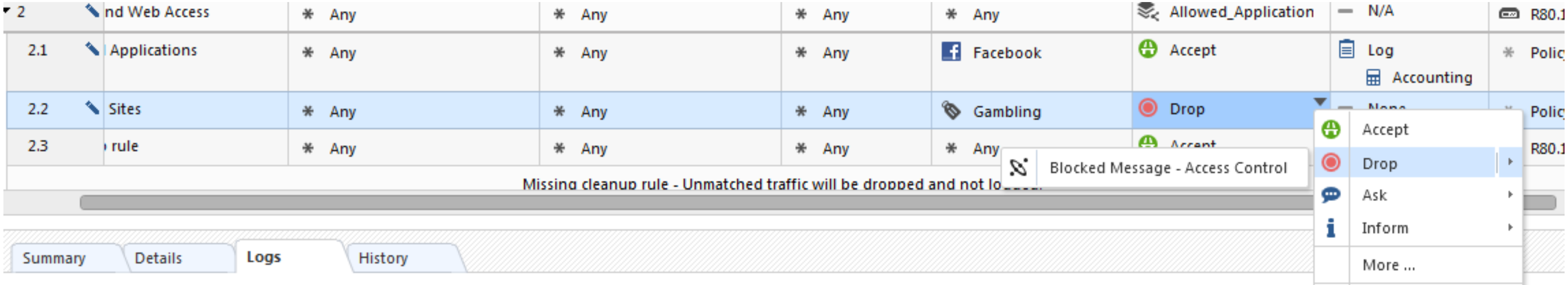
URL filtering: Background

Social networking widgets: Background

☑ Categorize social networking widgets

URL Filtering

- Allowing or Blocking Traffic based on category
- Block Message that can be customized.
- Blocking Gambling Sites



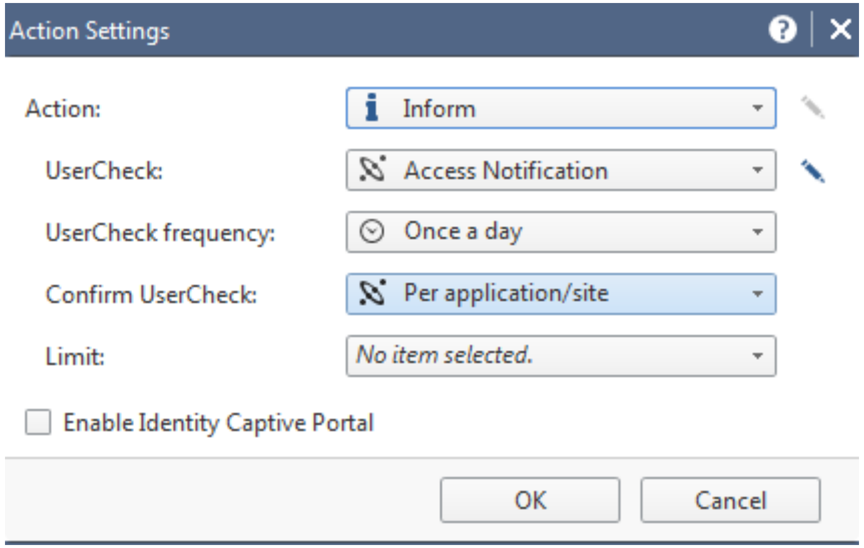
2	nd Web Access	Any	Any	Any	Any	Allowed_Application	N/A	R80.1
2.1	Applications	Any	Any	Any	Facebook	Accept	Log Accounting	Polic
2.2	Sites	Any	Any	Any	Gambling	Drop	None	Polic
2.3	rule	Any	Any	Any	Any	Accept		R80.1

Missing cleanup rule - Unmatched traffic will be dropped and not lo...

Blocked Message - Access Control

URL Filtering

- Additional Options for Action Column
  - Accept
  - Drop
  - Ask
  - Inform



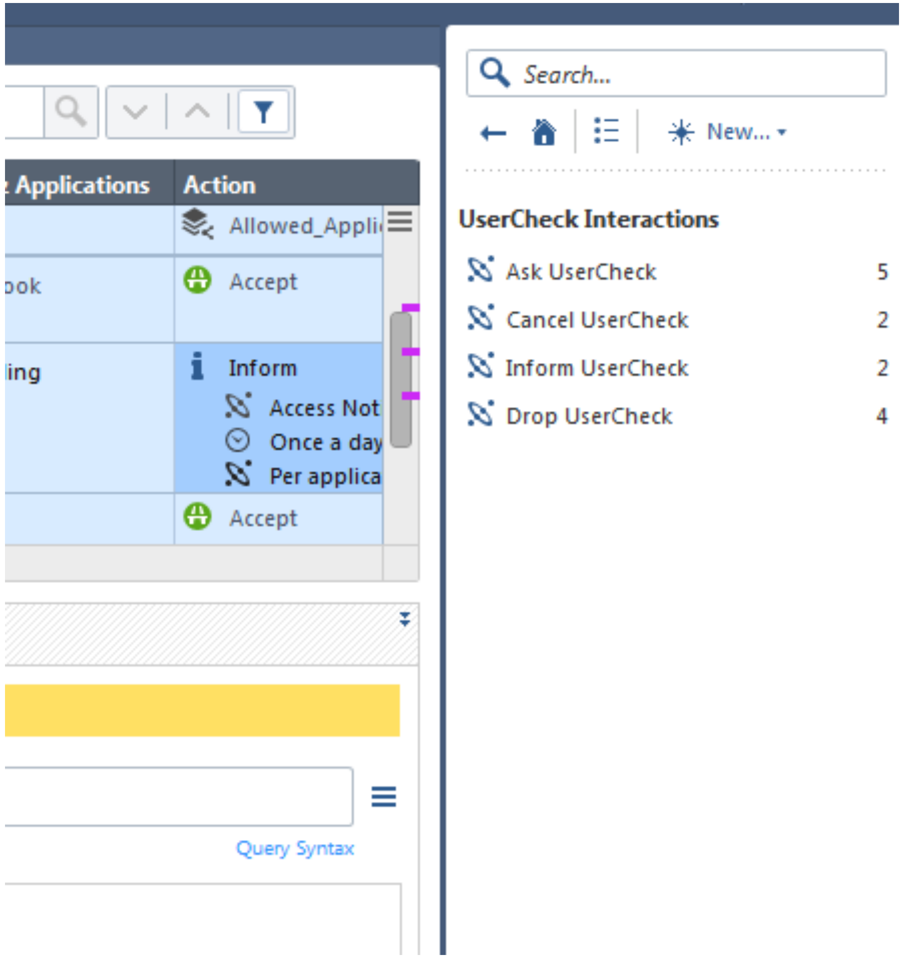
Action Settings

Action:	Inform
UserCheck:	Access Notification
UserCheck frequency:	Once a day
Confirm UserCheck:	Per application/site
Limit:	*No item selected.*

□ Enable Identity Captive Portal

URL Filtering

- User Check Interactions
  - Ask UserCheck
  - Cancel UserCheck
  - Inform UserCheck
  - Drop UserCheck



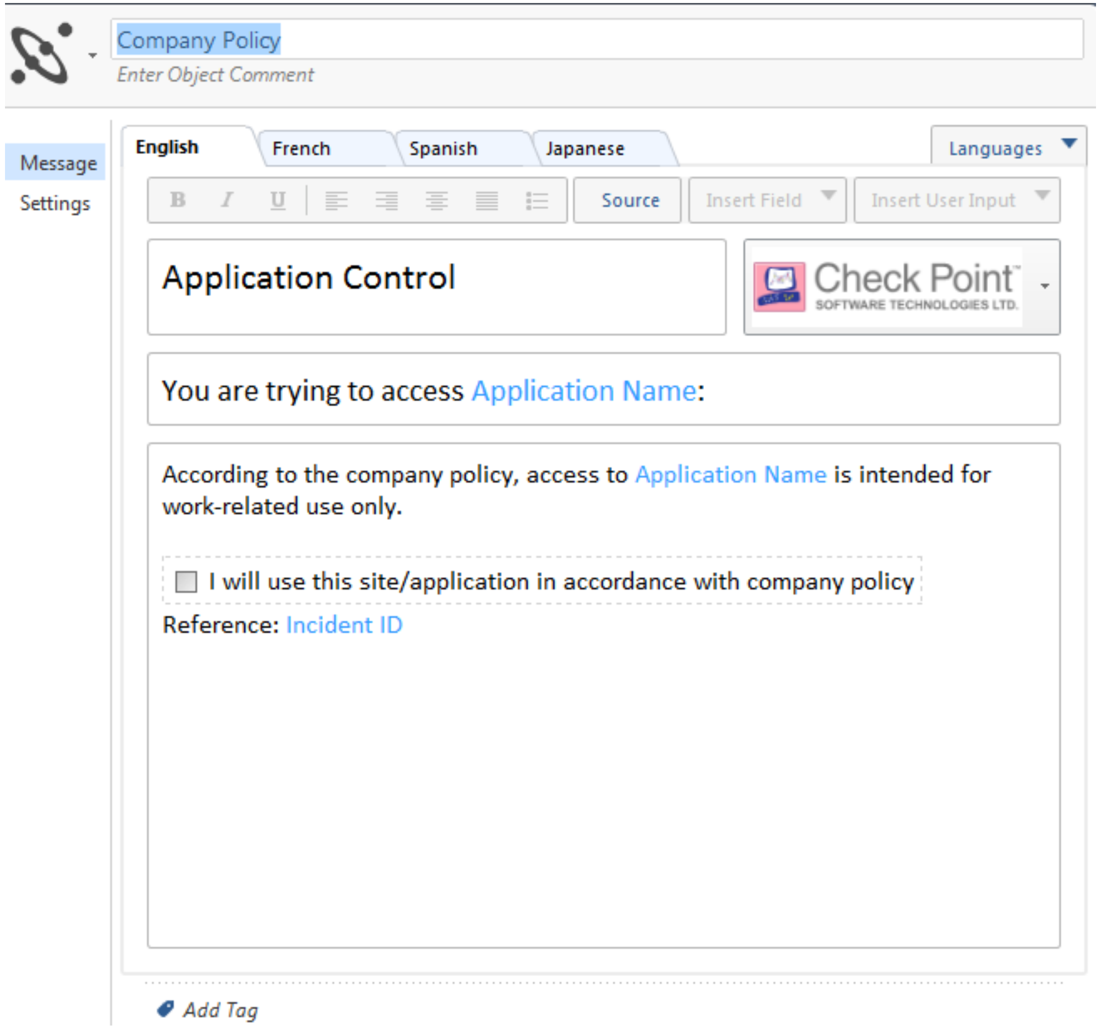
Applications	Action
	Allowed_Appli
ook	Accept
ing	Inform Access Not Once a day Per applica
	Accept

UserCheck Interactions

Ask UserCheck	5
Cancel UserCheck	2
Inform UserCheck	2
Drop UserCheck	4

URL Filtering

- User Check
- Ask UserCheck
  - Company Policy Page


Company Policy

Enter Object Comment

Application Control

You are trying to access Application Name:

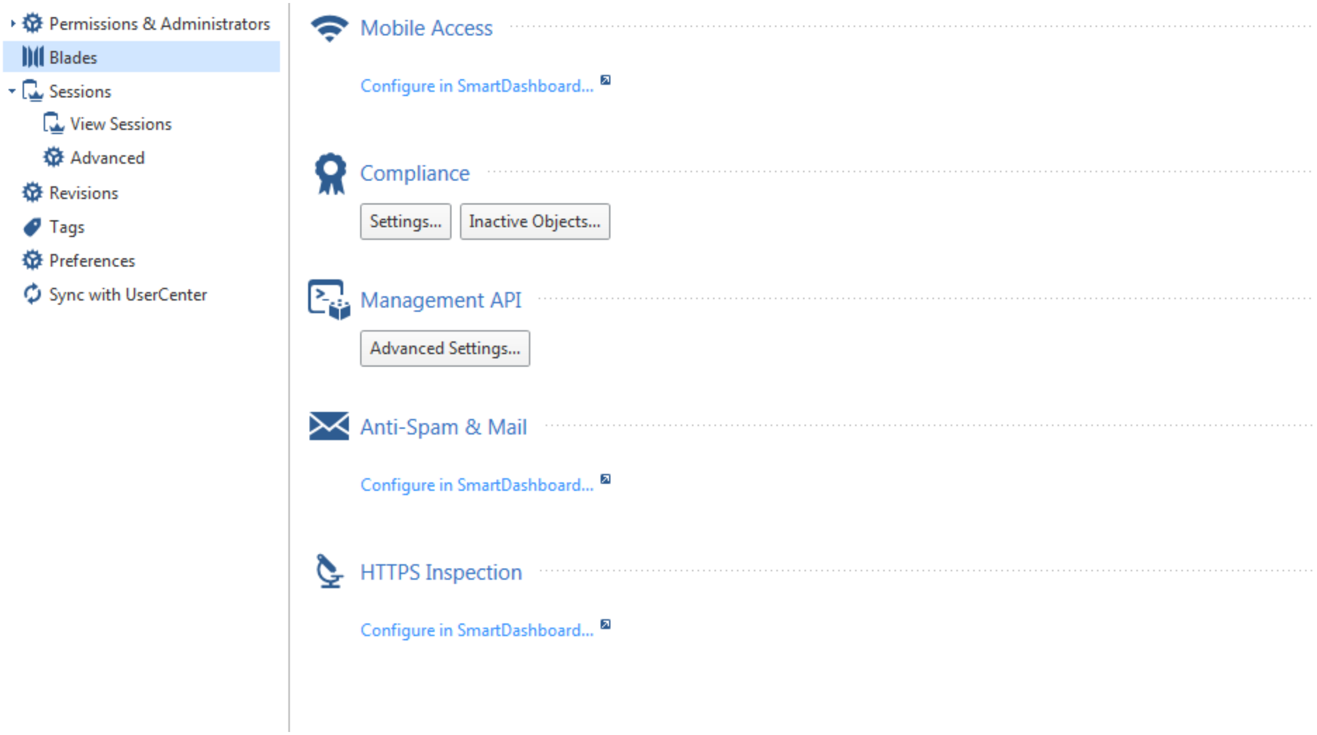
According to the company policy, access to Application Name is intended for work-related use only.

□ I will use this site/application in accordance with company policy

Reference: Incident ID

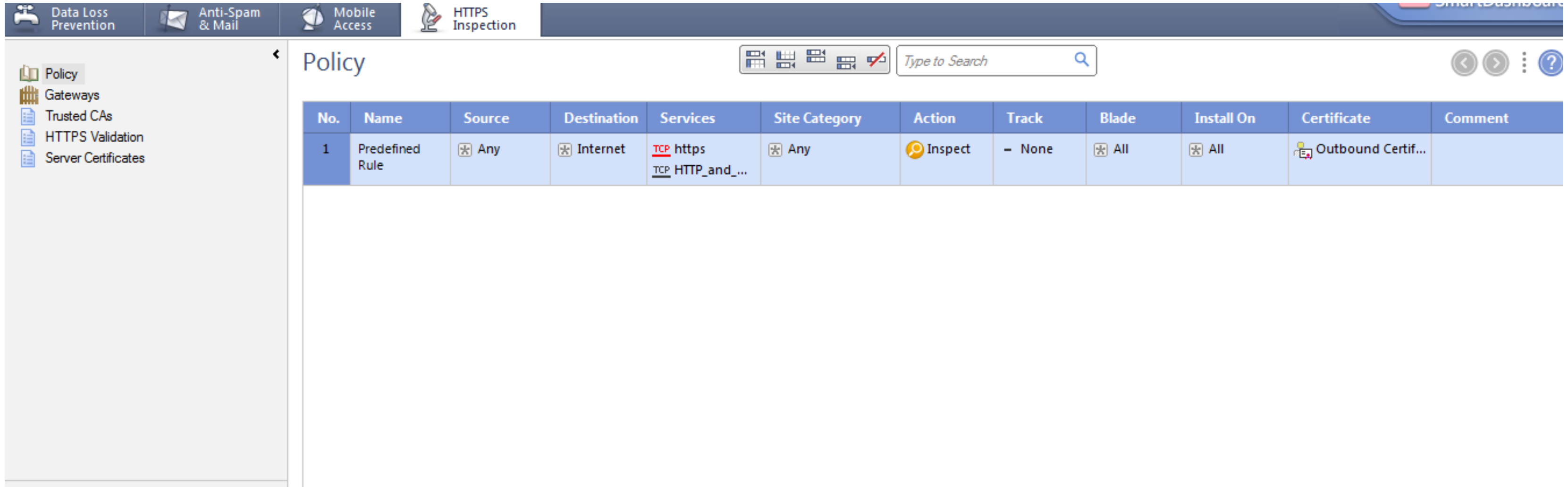
HTTPS Inspection

- Configured in SmartDashboard
  - Legacy Dashboard Configuration



HTTPS Inspection

- Policy
- Gateways
- Trusted CA's
- HTTPS Validation
- Server Certificates



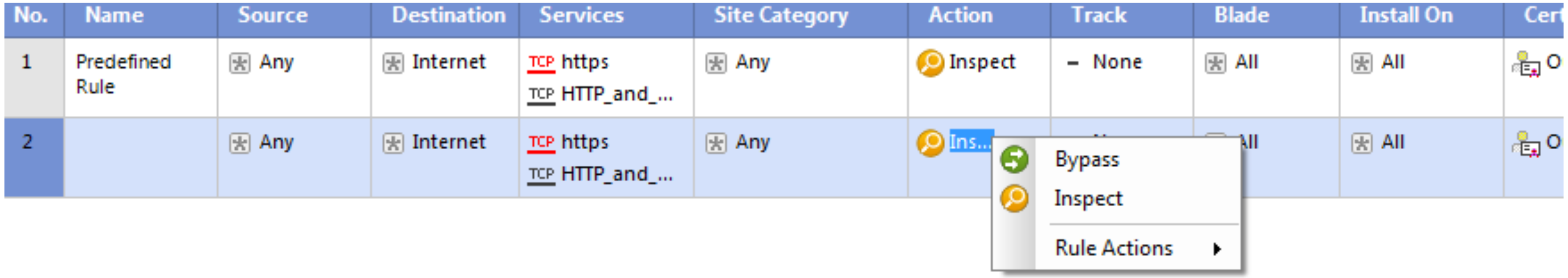
- Policy
- Gateways
- Trusted CAs
- HTTPS Validation
- Server Certificates

Policy

No.	Name	Source	Destination	Services	Site Category	Action	Track	Blade	Install On	Certificate	Comment
1	Predefined Rule	Any	Internet	TCP https TCP HTTP_and_...	Any	Inspect	– None	All	All	Outbound Certif...	

HTTPS Inspection Policy

- Rule Actions
  - Inspect
  - Bypass
    - Banking Sites
    - HealthCare Sites



No.	Name	Source	Destination	Services	Site Category	Action	Track	Blade	Install On	Cer
1	Predefined Rule	Any	Internet	TCP https TCP HTTP_and_...	Any	Inspect	– None	All	All	O
2		Any	Internet	TCP https TCP HTTP_and_...	Any	Ins...		ll	All	O

Summary

- Created and implemented an Application Control Policy
- Created a URL Filtering Policy to block undesirable web sites for employees
- Used SSL Inspection to inspect traffic to Secure Web Sites

Bibliography

R80.10 Next Generation Security Gateway Getting Started Guide California: USA

Check Point R80.10 Security Gateway Technical Administration Guide California: USA

R80.10 Security Management Admin Guide California: USA