

Como utilizar a blade Content Awareness

Security Engineering Brazil
09/2023



YOU DESERVE THE BEST SECURITY

Índice

Introdução.....	3
Pré-Requisitos	4
Caso de uso #1 – Bloqueio de tráfego de cartões de crédito (PCI)	5
Caso de uso #2 – Bloqueio de tráfego com CPF	6

Introdução

Este documento tem o objetivo de exemplificar o uso da blade de **content awareness**. Essa blade tem o foco de controlar de conteúdo passante pelos gateways Check Point considerando extensões dos arquivos e o conteúdo dentro dos arquivos.

O Content Awareness se encontra disponível desde o licenciamento NGFW conforme tabela abaixo:

	NGFW Basic access control with IPS	NGTP Prevent known threats	SandBlast Prevent zero-day threats
Security Gateway Feature Sets			
Firewall	✓	✓	✓
IPsec VPN	✓	✓	✓
Mobile Access	✓	✓	✓
Advanced Networking & Clustering	✓	✓	✓
Identity Awareness	✓	✓	✓
Application Control	✓	✓	✓
Content Awareness	✓	✓	✓
IPS	✓	✓	✓
URL Filtering		✓	✓
Antivirus		✓	✓
Anti-Spam		✓	✓
Anti-Bot		✓	✓
DNS Security		✓	✓
SandBlast Threat Emulation			✓
SandBlast Threat Extraction			✓
Zero Phishing			✓
DLP	Optional	Optional	Optional
IoT Protect	Optional	Optional	Optional
SD-WAN Network Optimization	Optional	Optional	Optional
Security Management Feature Sets			
Network Policy Management	✓	✓	✓
Logging & Status	✓	✓	✓

Optional security capabilities can be ordered a-la-carte or separately

As informações contidas nos procedimentos abaixo foram validadas e testadas em um laboratório com a versão R81.10 e podem servir como referência mas não como documentação oficial.

Todos os detalhes e informações mais atualizadas sobre o Content Awareness se encontram no sk119715.

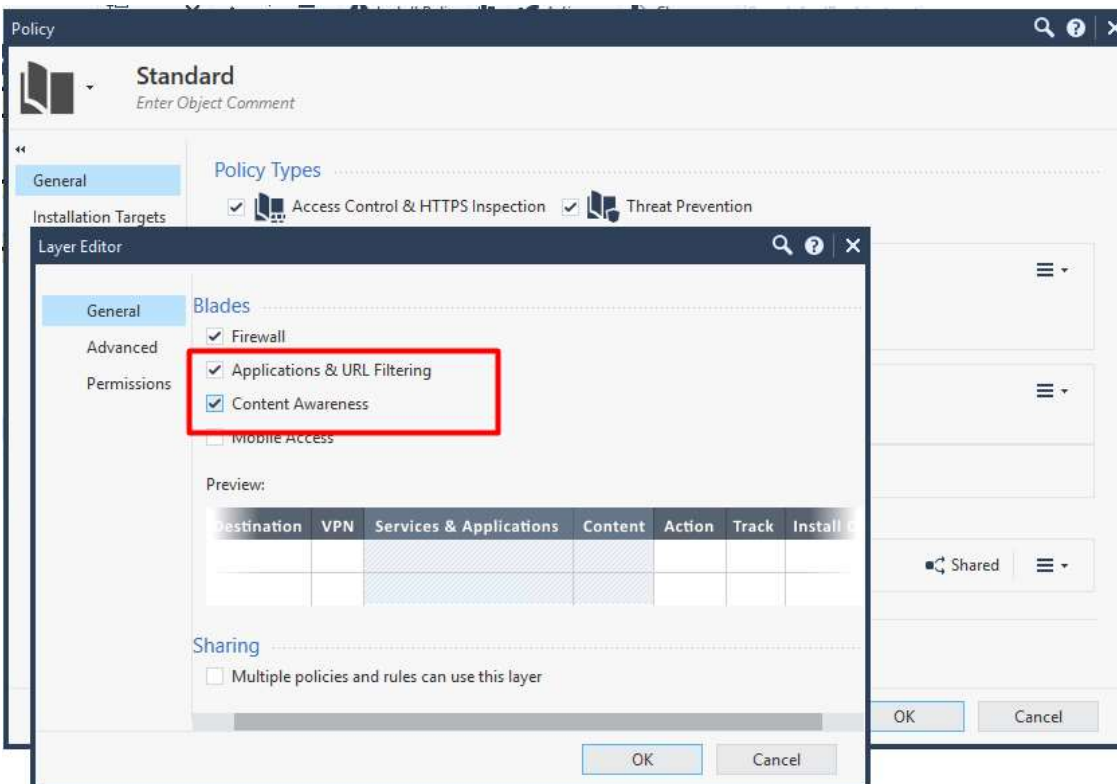
Pré-Requisitos

1. Possuir um gateway Check Point com as blades URL Filter, Application Control e Content Awareness habilitadas:



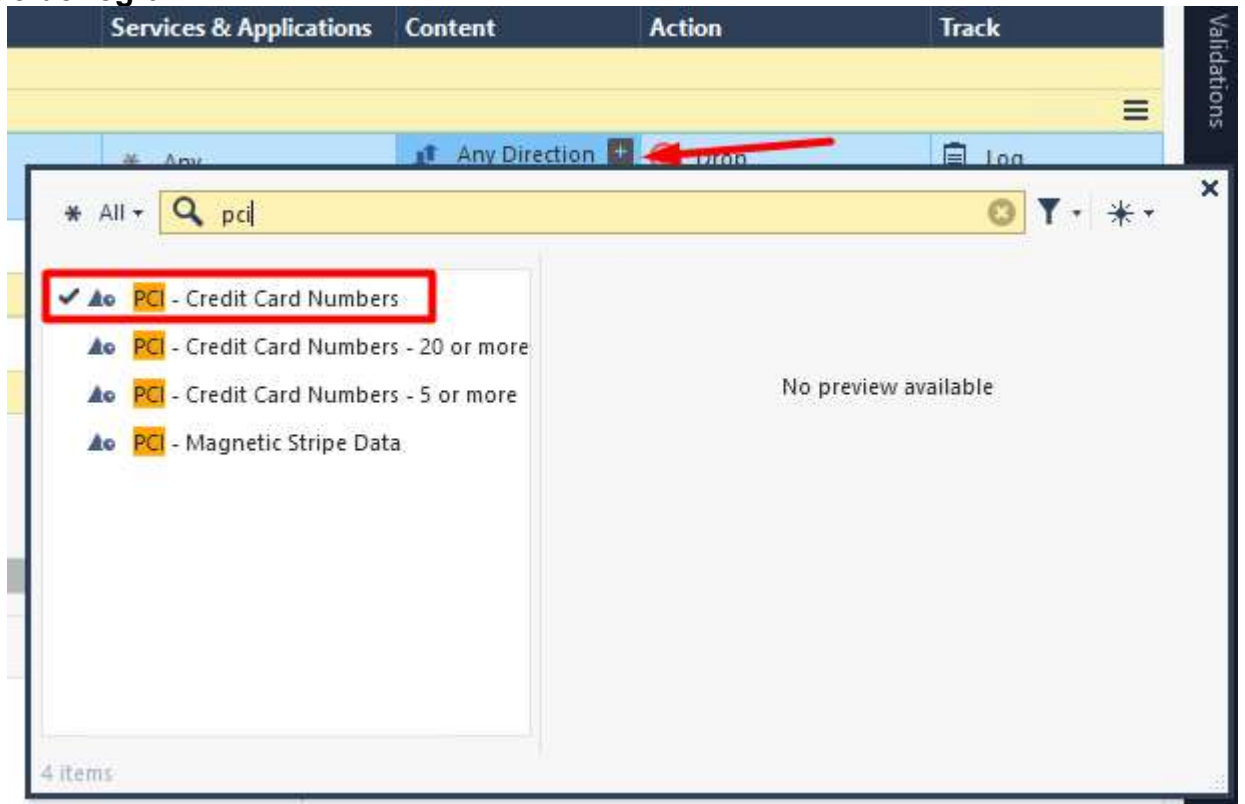
Obs.: se o objetivo for controlar conteúdos em conexões HTTPs é necessário que inspeção SSL esteja ativa.

2. Habilitar as blades Application & URL Filtering e Content Awareness na política que será utilizada:

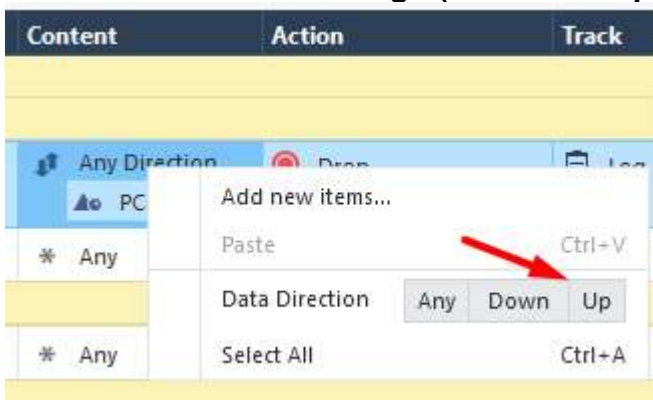


Caso de uso #1 – Bloqueio de tráfego de cartões de crédito (PCI)

1. Criação de regra PCI:



2. Escolher sentido do tráfego (Download/Upload):

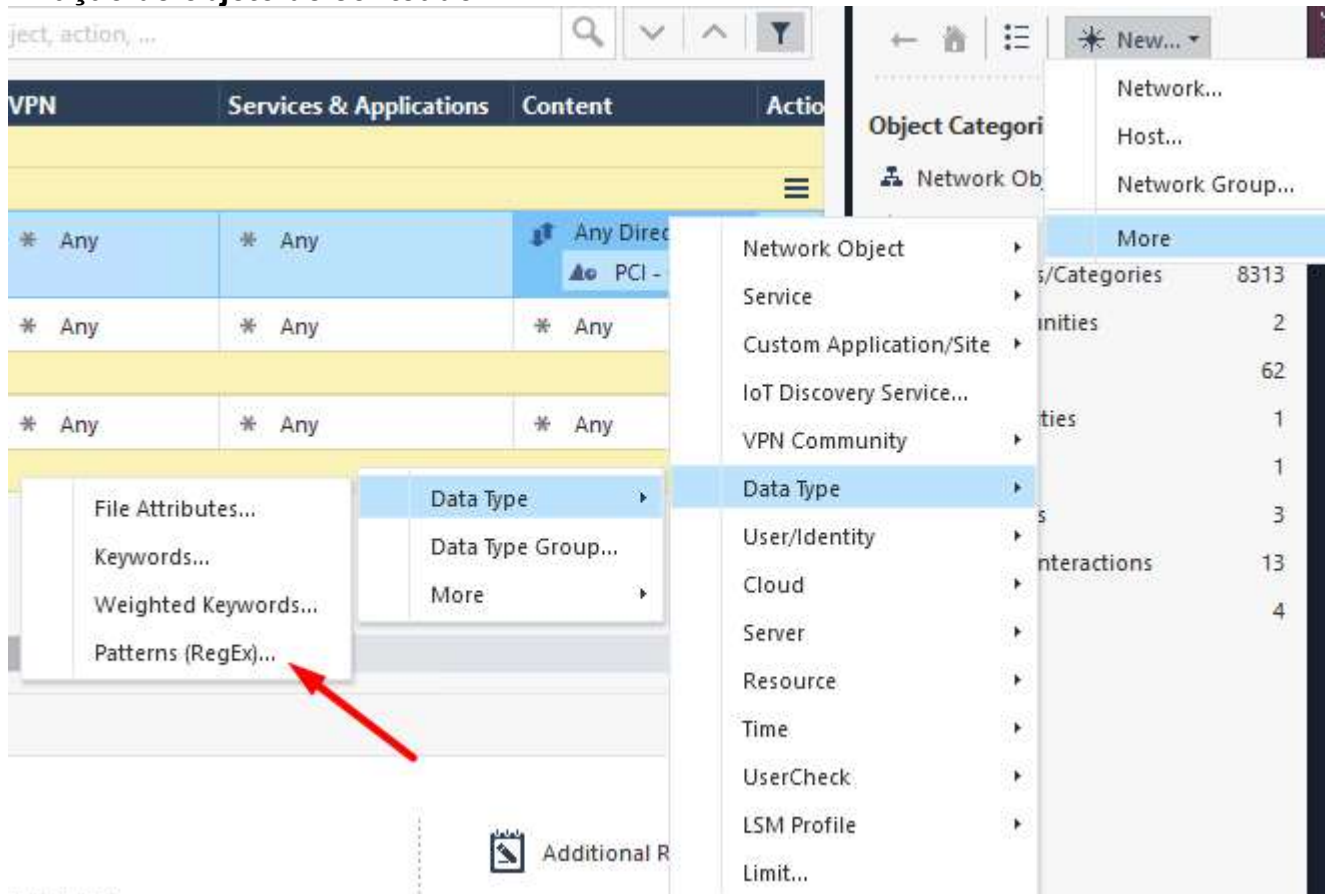


3. Resultado

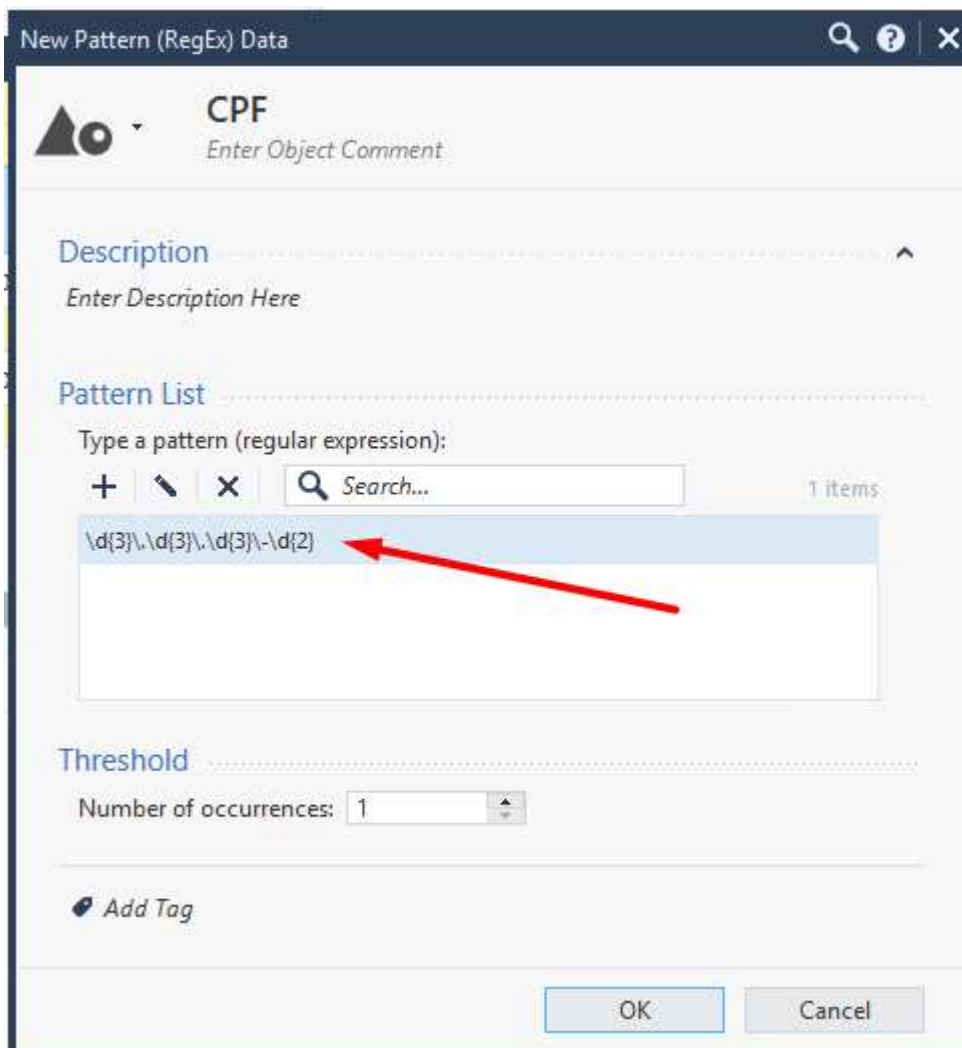
Services & Applications	Content	Action	Track
* Any	* Any	Any Direction	Drop
* Any	PCI - Credit...	Blocked Messa...	Log
Net_192.168.101.0	* Any	Accept	Log

Caso de uso #2 – Bloqueio de tráfego com CPF

1. Criação de objeto de conteúdo CPF

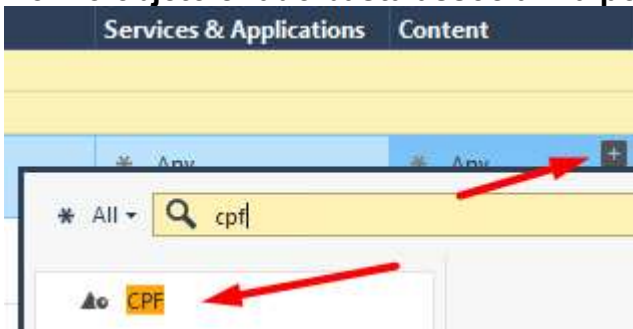


2. Designar padrão RegEx:

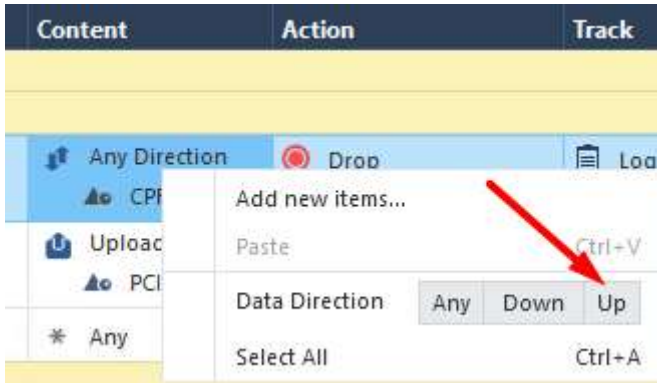


Obs.: Este padrão identifica apenas CPFs no formato 123.456.789-00. Caso outros formatos seja necessários é preciso criar novas expressões

3. Com o objeto criado basta associar na política:



4. Com o objeto associado, selecionar a direção:



5. Resultado

No.	Source	Destination	VPN	Services & Applications	Content	Action	Track
Management Access (1-3)							
Internal Access (4-6)							
4	* Any	* Any	* Any	* Any	Upload Traffic CPF	Drop Blocked Messa...	Log
5	* Any	* Any	* Any	* Any	Upload Traffic PCI - Credit...	Drop Blocked Messa...	Log
6	Net_192.168.101.0	* Any	* Any	* Any	* Any	Accept	Log

⊖ **Block**
 http Traffic Blocked from 192.168.101.201 to 35.209.95.242

Details
Matched Rules
Files

Log Info

Origin: Gateway

Time: Today, 5:13:41 PM

Blade: Content Awareness

Product Family: Access

Type: Session

UserCheck

UserCheck ID: 2D8D0DD2-8DAF-D6EF-FA1E-A64993...

User Check: 1

UserCheck Message to U...: Access to is blocked according to the...

Confirmation Scope: Application

Frequency: 1 days

UserCheck Interaction N...: Blocked Message

UserCheck Reference: 932F4AE7

File Operation

Data Type: CPF

Actions

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

Traffic

Source: WIN-victim (192.168.101.201)

Destination Country: United States

Service: http (TCP/80)

Protocol: HTTP

Interface: eth0

Connection Direction: Outgoing

Destination: 242.95.209.35.bc.googleusercontent...

More