CHECK POINT™

YOU DESERVE THE BEST SECURITY

Como utilizar a blade Content Awareness

Security Engineering Brazil
09/2023

©2023 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

CHECK POINT™

YOU DESERVE THE BEST SECURITY

Índice

©2023 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

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.

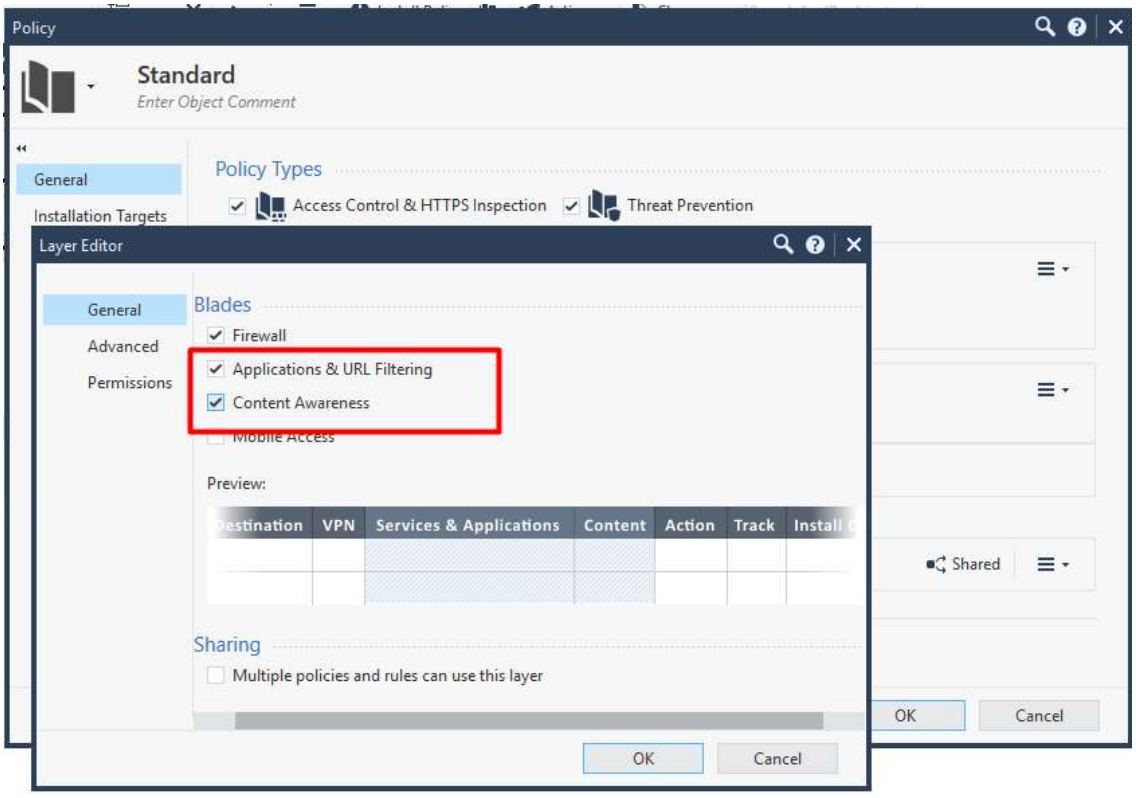
©2023 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Pré-Requisitos

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

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

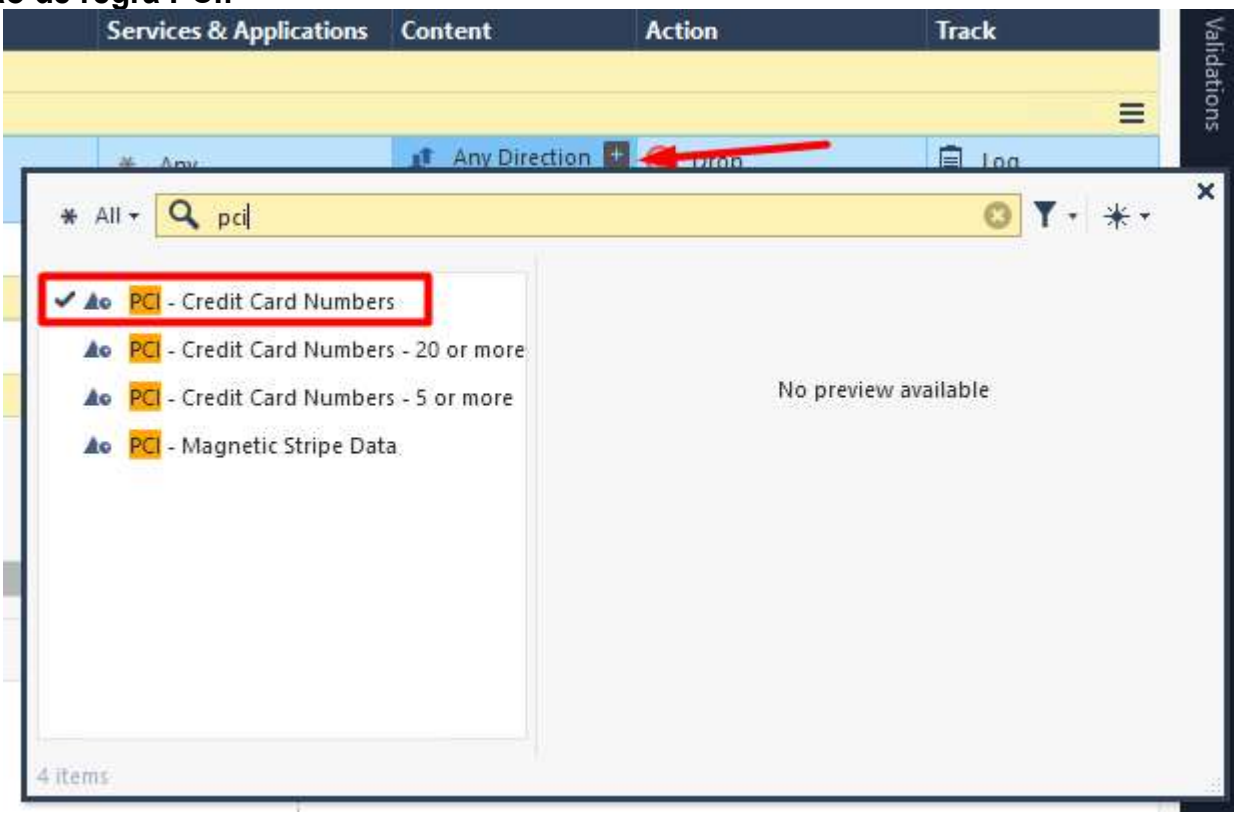
2. Habilitar as blades Application & URL Filtering e Content Awareness na política que será utilizada:



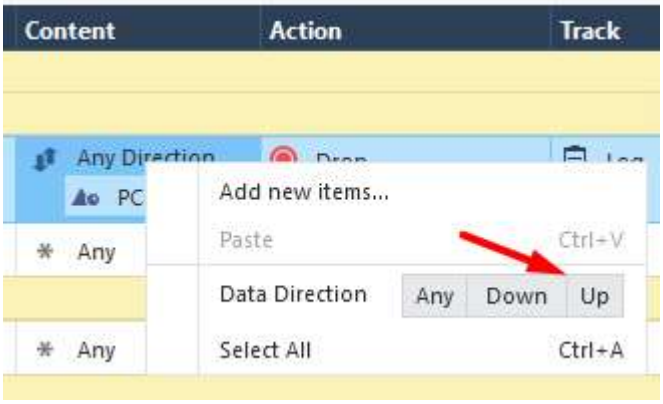
©2023 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

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

1. **Criação de regra PCI:**



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

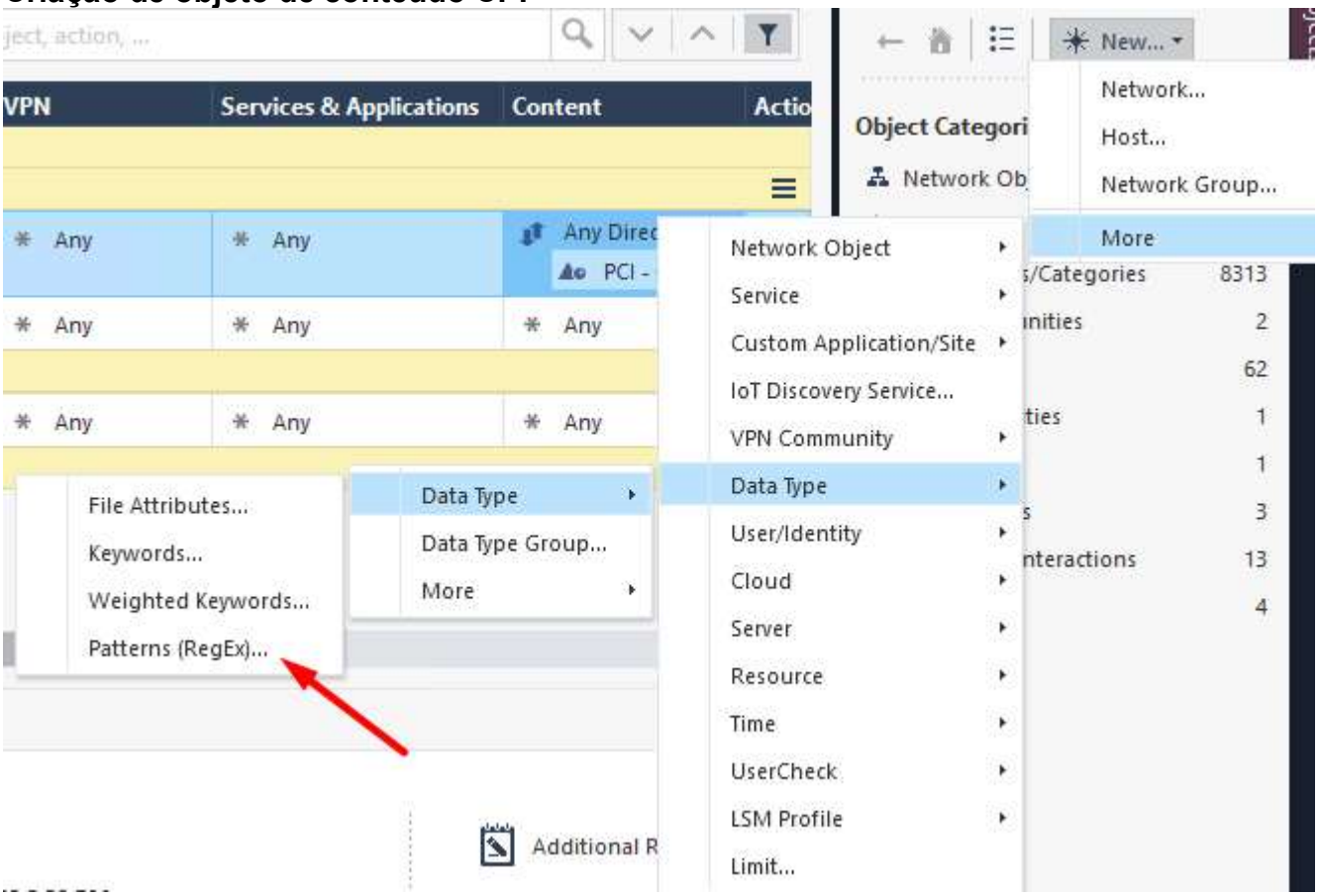


3. **Resultado**

©2023 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

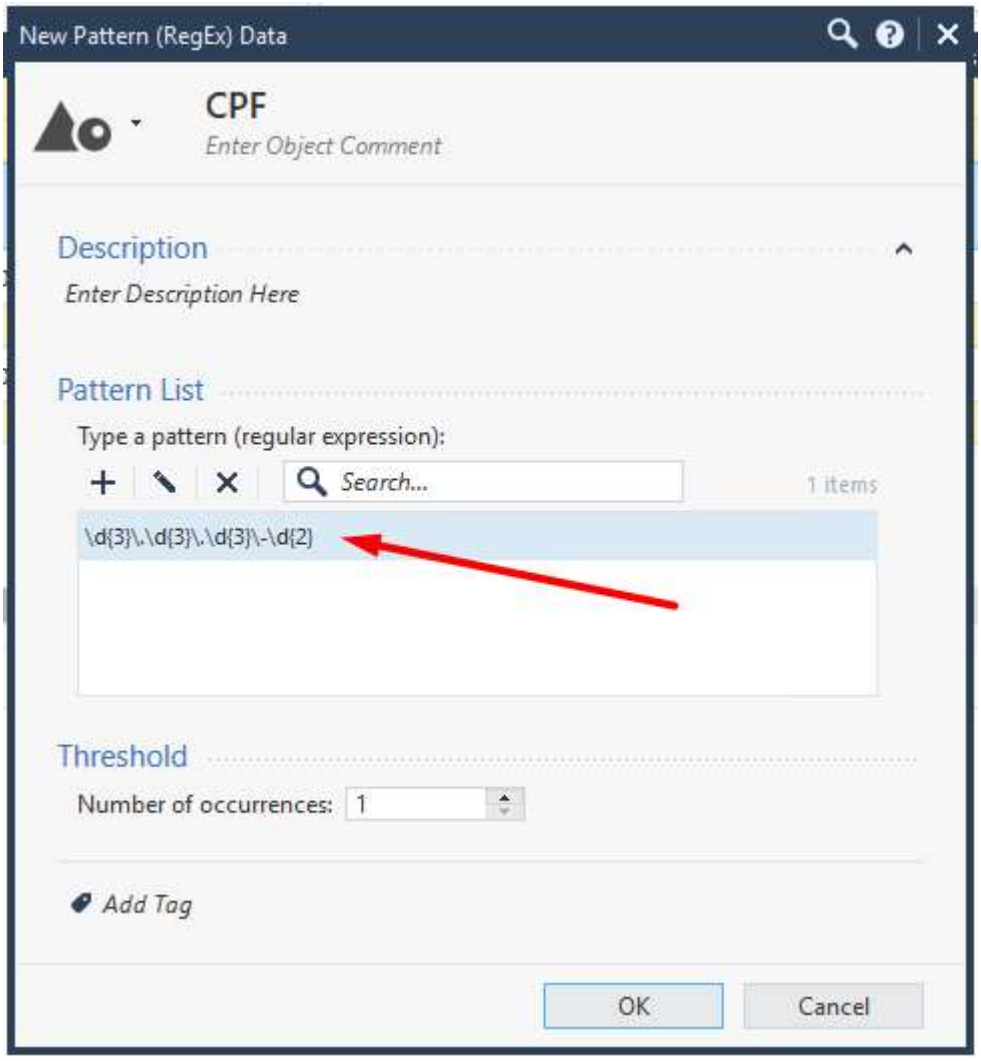
Caso de uso #2 – Bloqueio de tráfego com CPF

1. **Criação de objeto de conteúdo CPF**



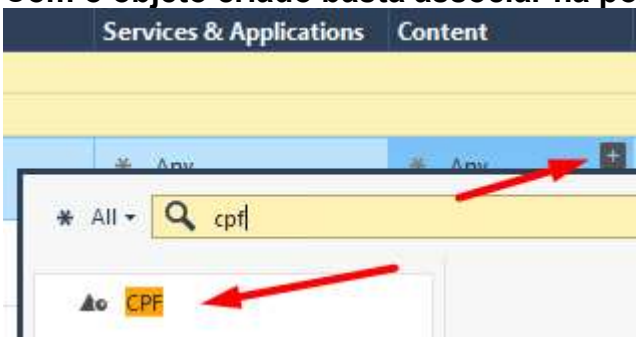
2. **Designar padrão RegEx:**

©2023 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



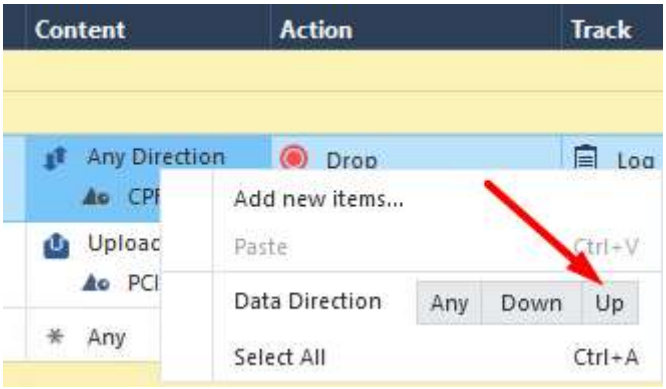
Obs.: Este padrão identifica apenas CPFs no formato 123.456.789-00. Caso outros formatos seja necessários é preciso criar novas expressões

3. **Com o objeto criado basta associar na política:**

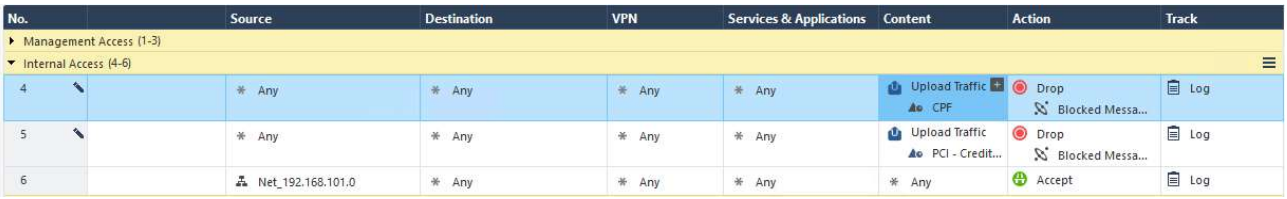


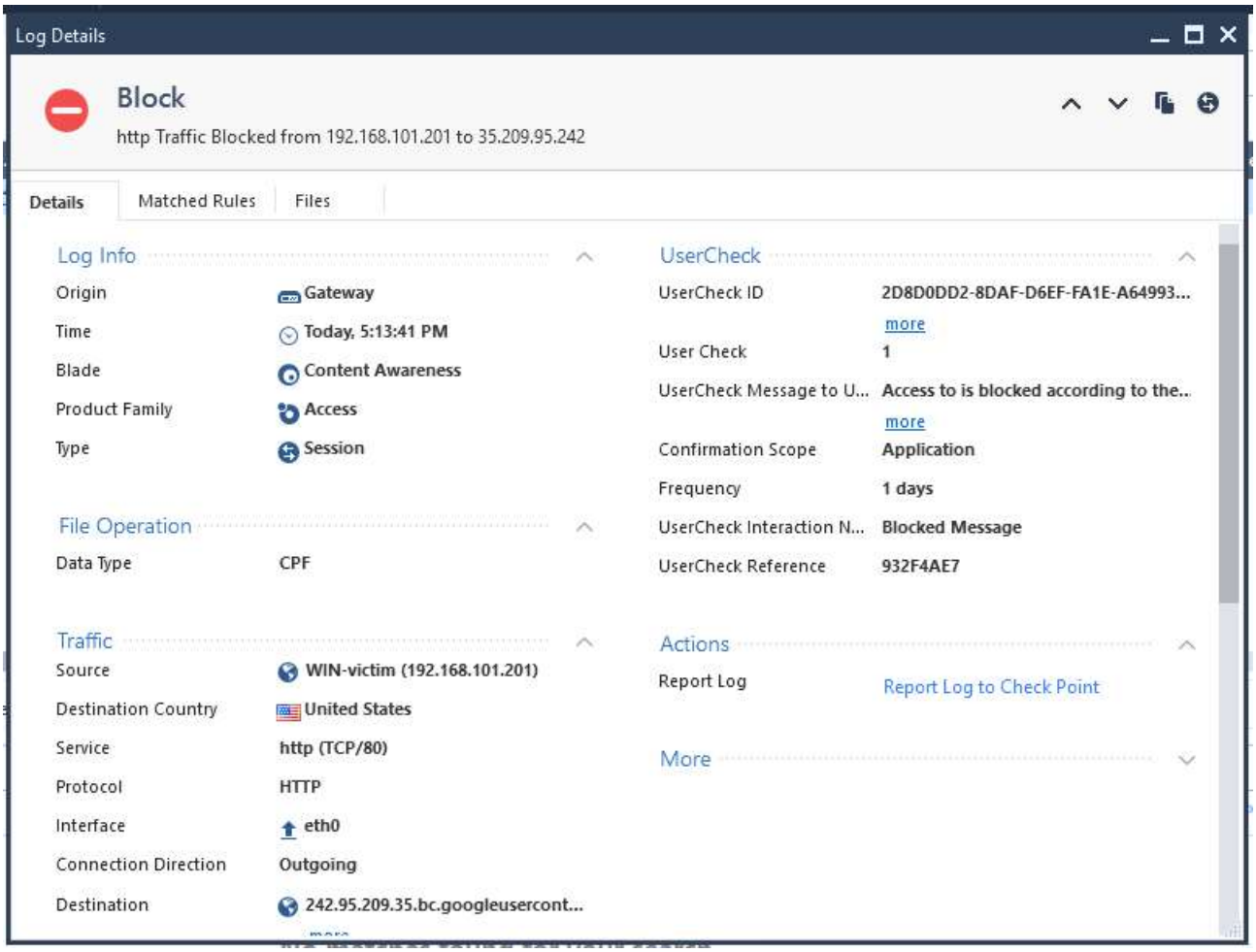
4. **Com o objeto associado, selecionar a direção:**

©2023 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



5. Resultado





©2023 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals