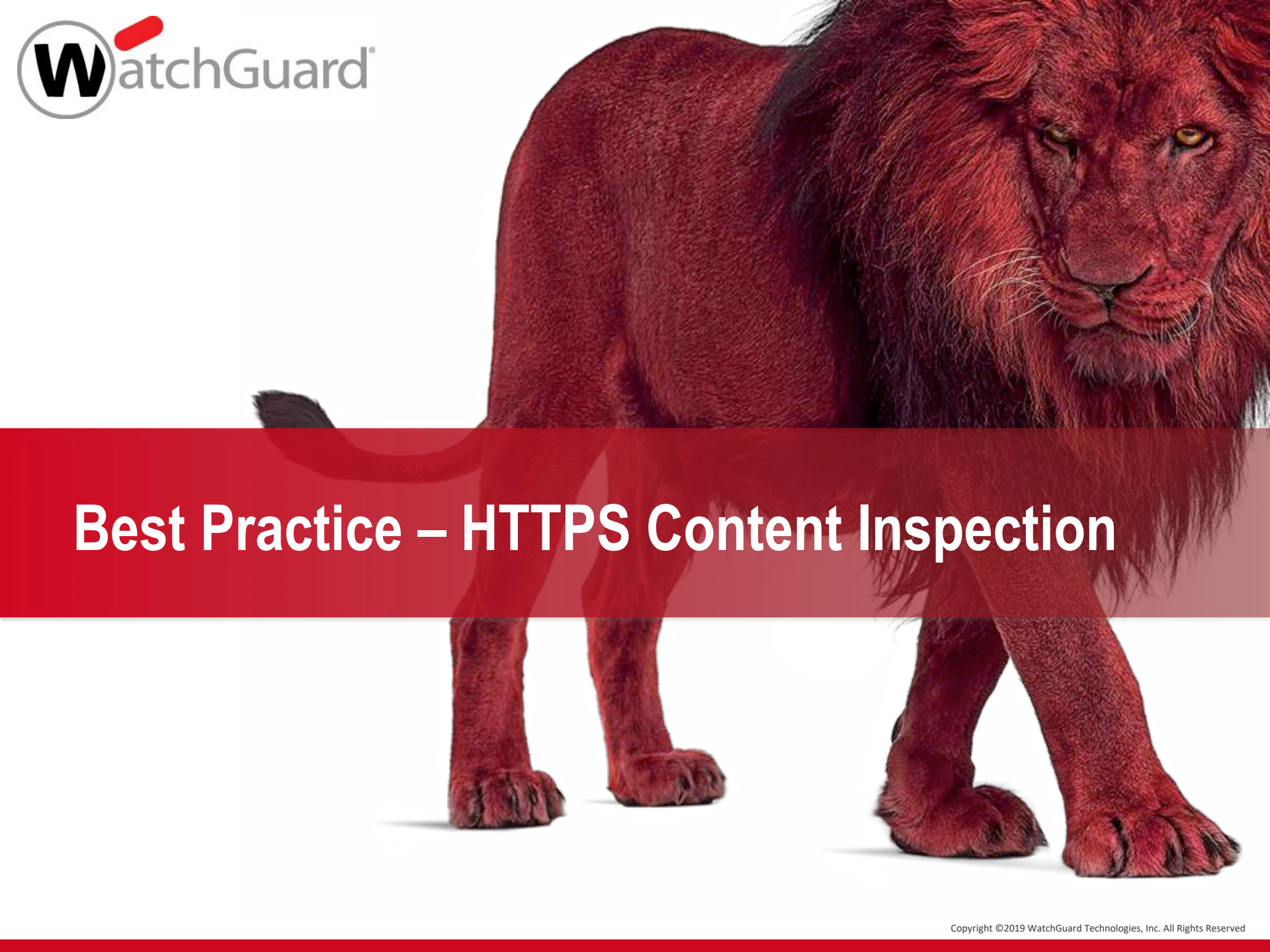
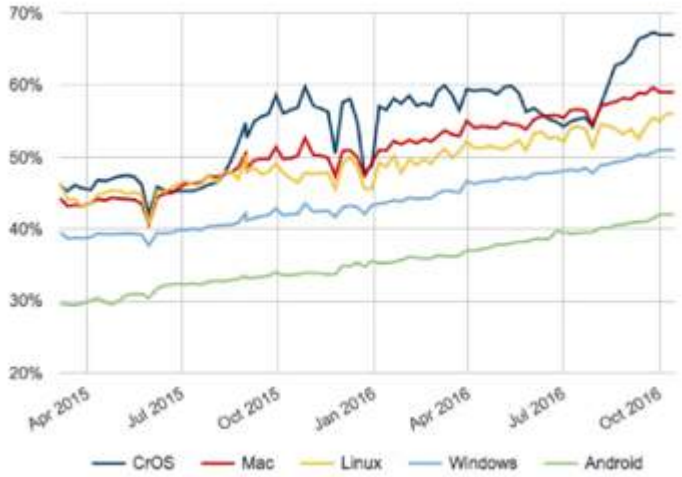


Best Practice – HTTPS Content Inspection

Encrypted Traffic

NSS Labs: 75% of Web Traffic Will Be Encrypted by 2019

70% of malicious binaries in 2017 used some encryption



https://www.nsslabs.com/company/news/press-releases/nss-labs-predicts-75-of-web-traffic-will-be-encrypted-by-2019/
https://techcrunch.com/2017/10/20/https-is-booming-says-google/
https://www.theregister.co.uk/2018/02/21/cisco_survey_severity_of_cyber_attacks_doubled_in_one_year

HTTPS ohne Content Inspection

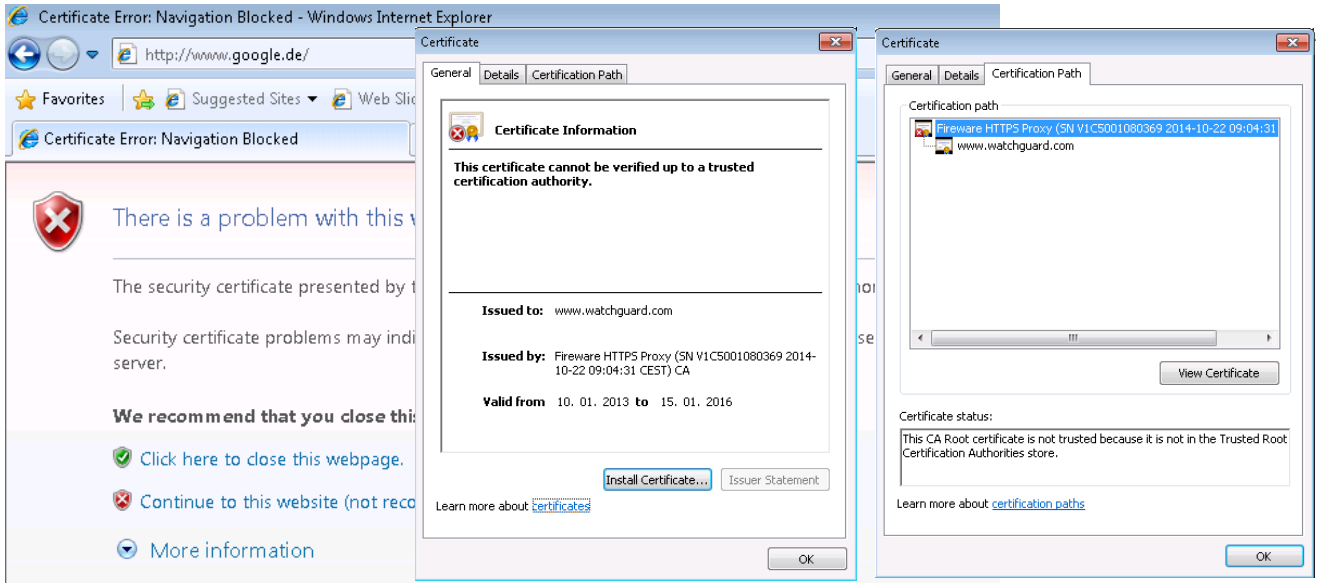
https://www.watchguard.com

HTTPS mit Content Inspection

https://www.watchguard.com

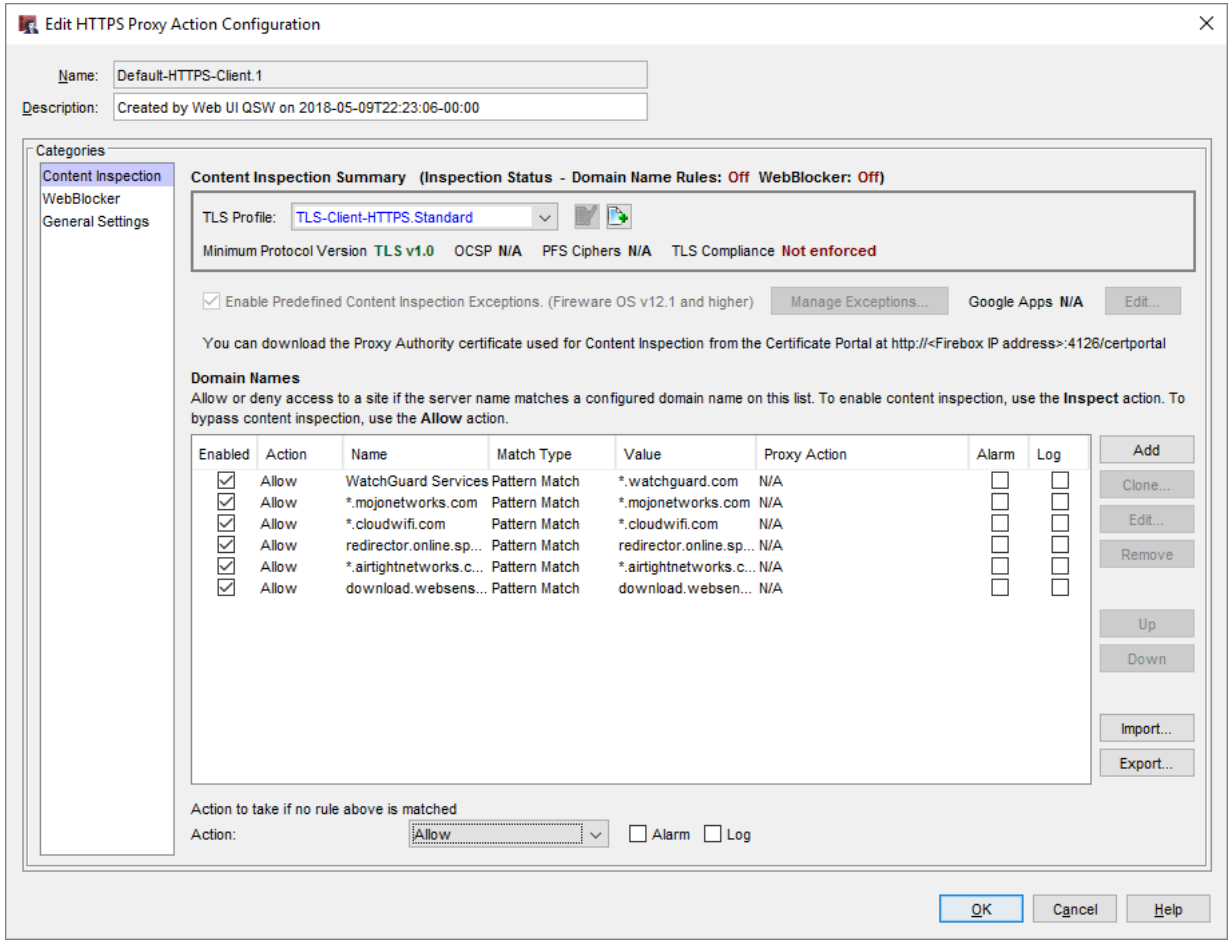
„Sichtbare“ Auswirkung

- Zertifikate werden erneut signiert
- Sicherheitswarnung im Browser (sofern Zertifikat der Firebox nicht vertrauenswürdig)



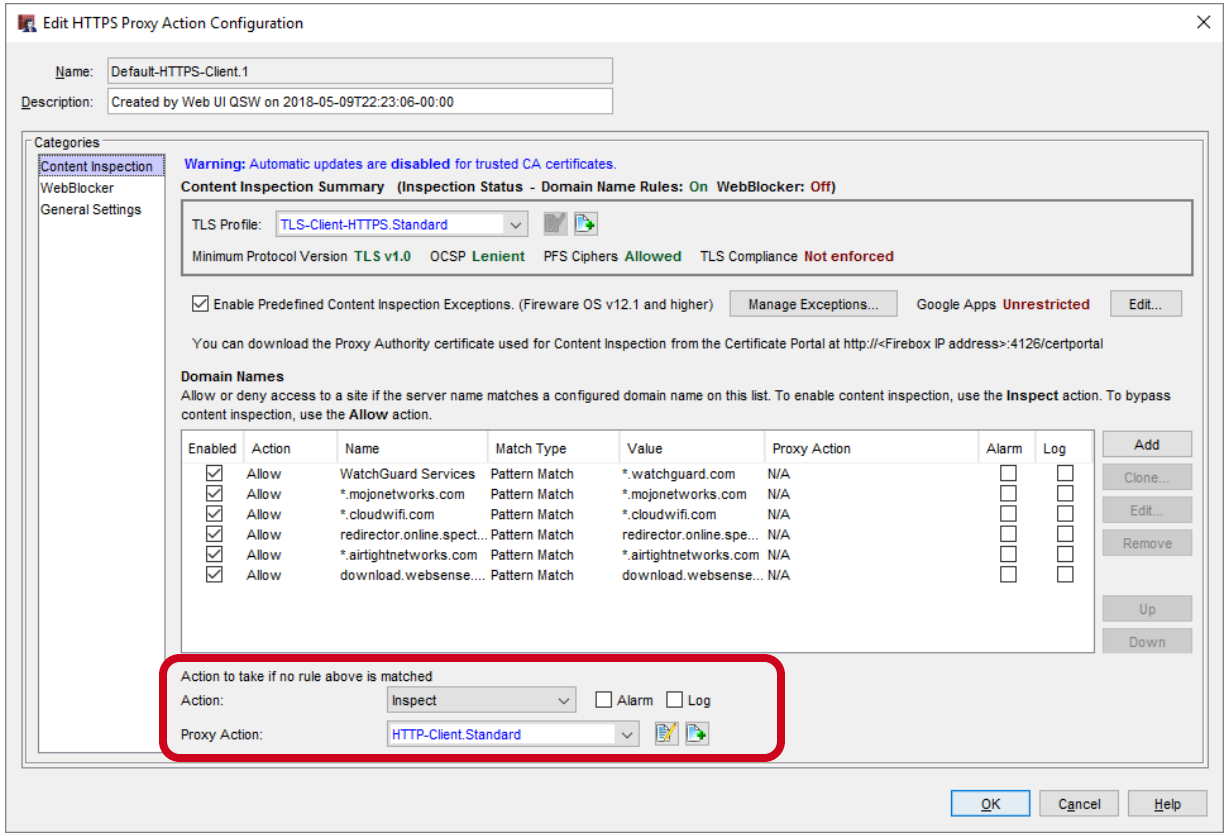
Konfiguration innerhalb des HTTPS Proxy

- Kontrolle des verschlüsselten Web Traffic (HTTPS)

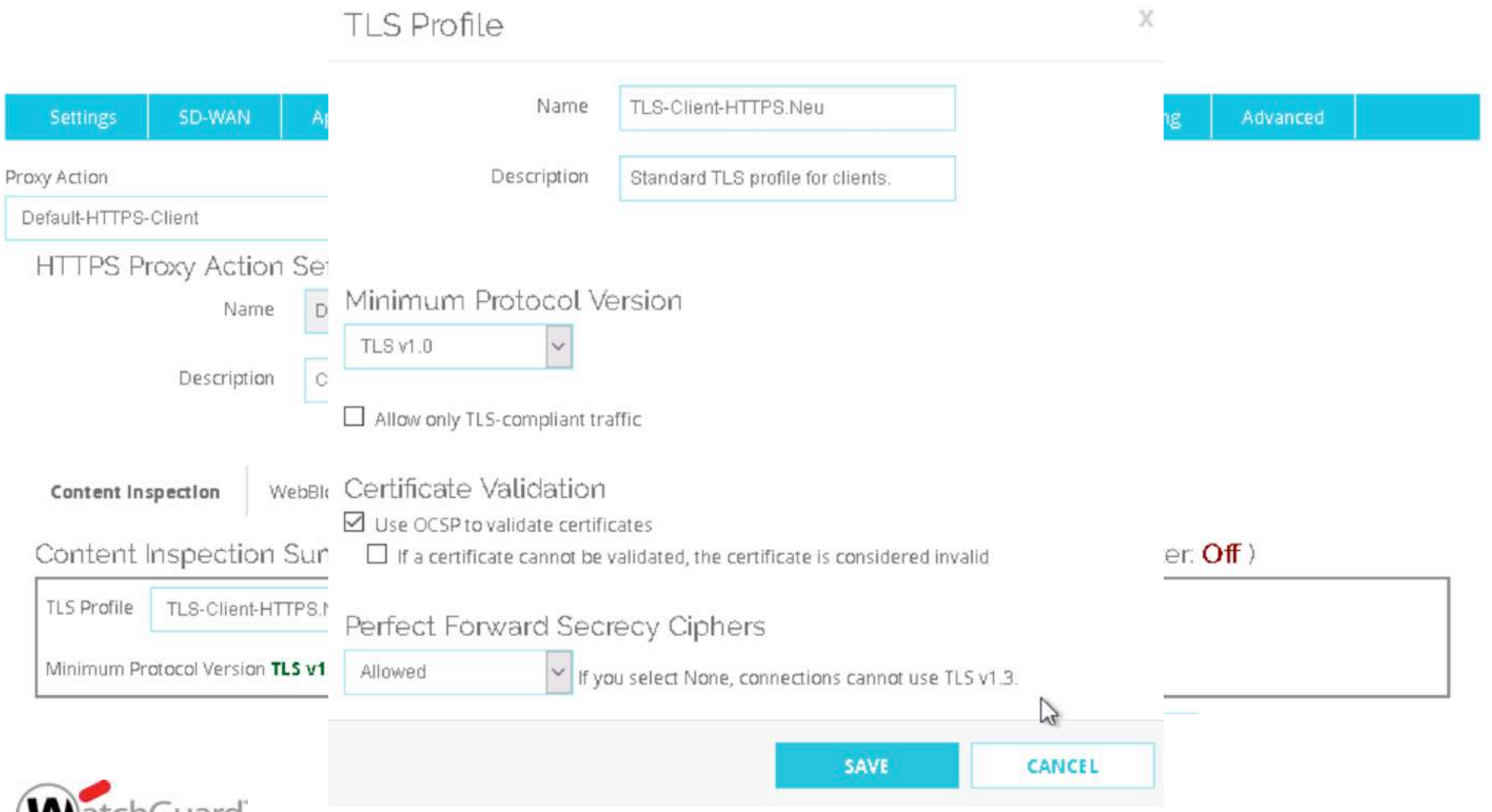


HTTPS Proxy und Content Inspection

- Um Content Inspection zu nutzen, muss die action **Inspect** angewendet werden.
  - **Predefined exceptions** vermeiden Probleme mit oft genutzten Diensten

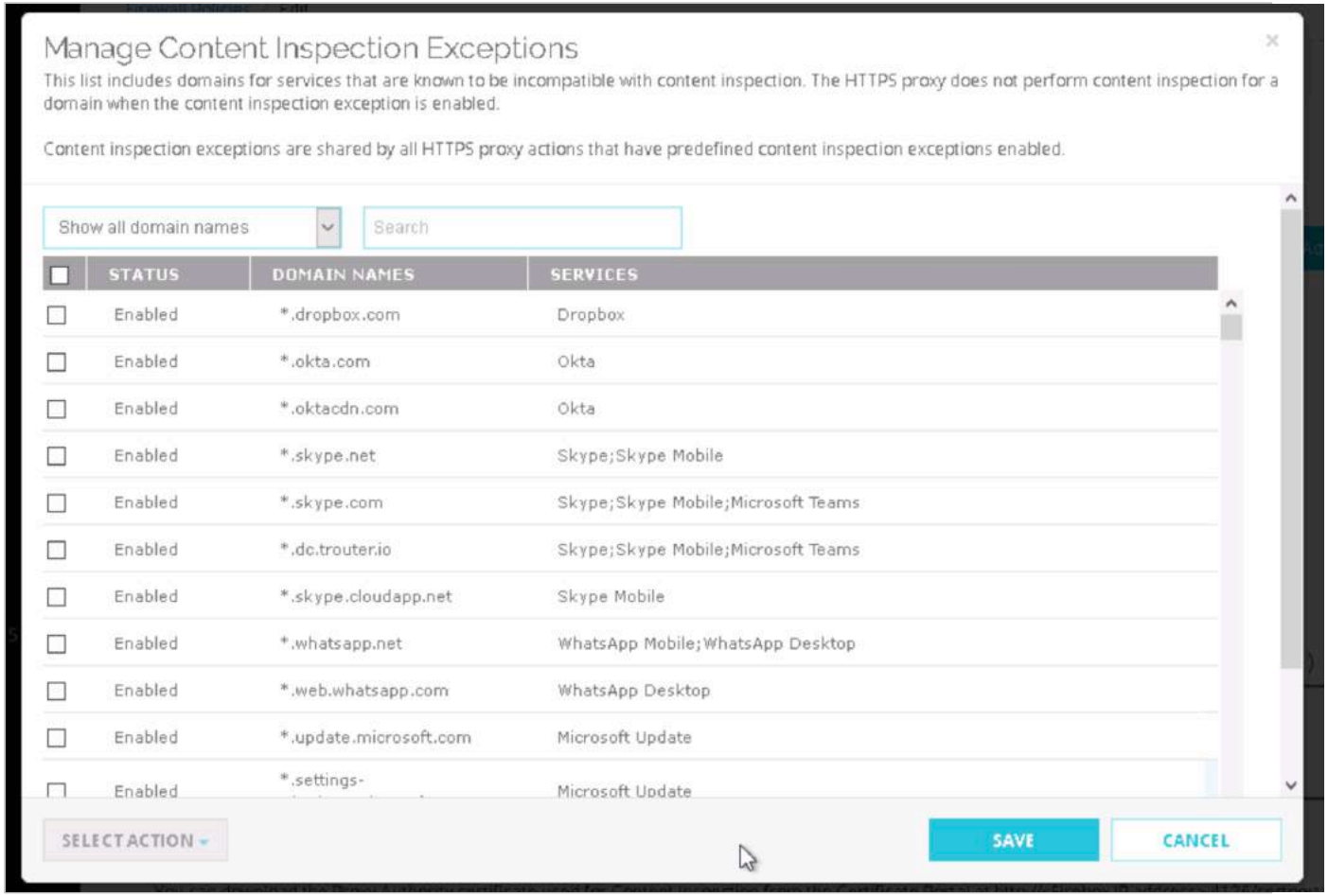


TLS Profile



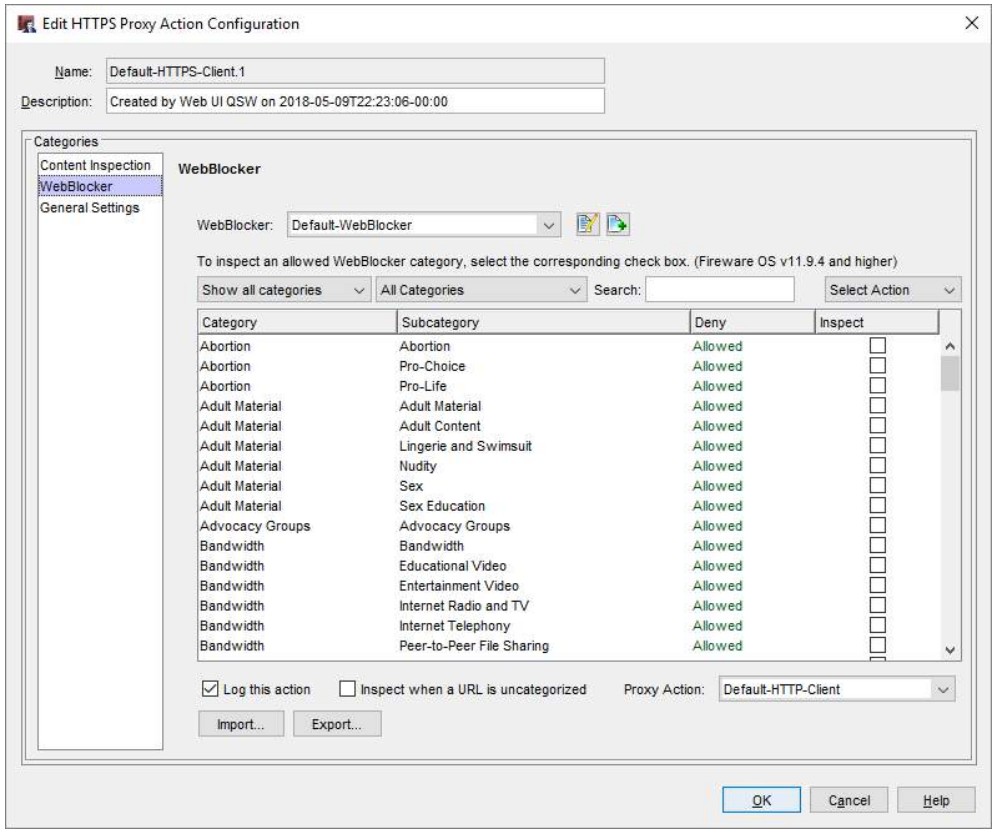
Predefined Content Inspection Exceptions

- Seit Version 12.1 verfügbar.



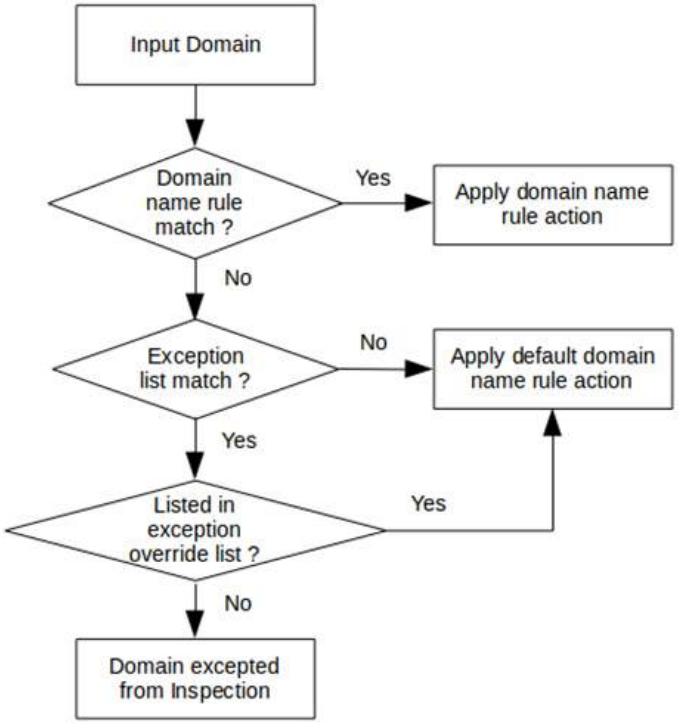
HTTPS Proxy und WebBlocker

- Webblocker kann auch ohne Content Inspection genutzt werden
- Content Inspection kann pro Kategorie aktiviert/deaktiviert werden.



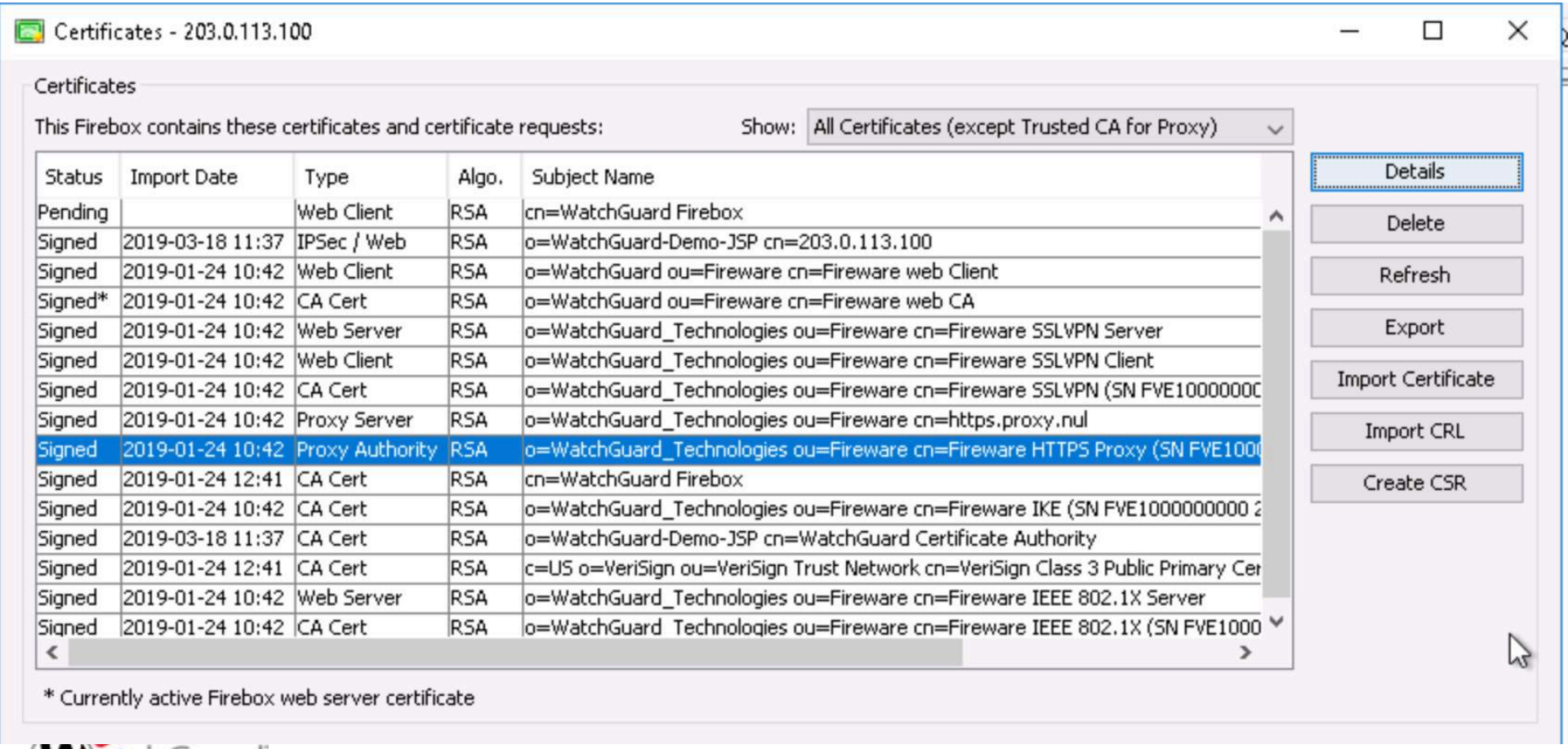
HTTPS Proxy Flow

- Domain name rules take higher precedence than any match in the predefined exception list
- If a domain name rule is matched, the action from that rule will always be applied



Zertifikate der Firebox

- **Proxy Authority** – Dieses Zertifikat wird für HTTPS Content Inspection für interne Clients genutzt



Aktivierung von Content Inspection

- Welches Zertifikat sollte wird für Content Inspection verwendet?
  - Self-signed der Firebox?
  - Gibt es eine interne PKI die ein Zertifikat ausstellen kann?
- Sicherstellen, dass die Clients und Browser dem Zertifikat vertrauen?
  - Installation über „Certportal“ der Firebox
  - Installation per Gruppenrichtlinien oder Softwareverteilung
- Welche Ausnahmen sind für Applikationen, Websites, Benutzergruppen, etc. nötig?
- **Inspection** innerhalb der HTTPS-Proxy Action aktivieren

Live Demo

Vielen Dank!

NOTHING GETS PAST RED.

WatchGuard