

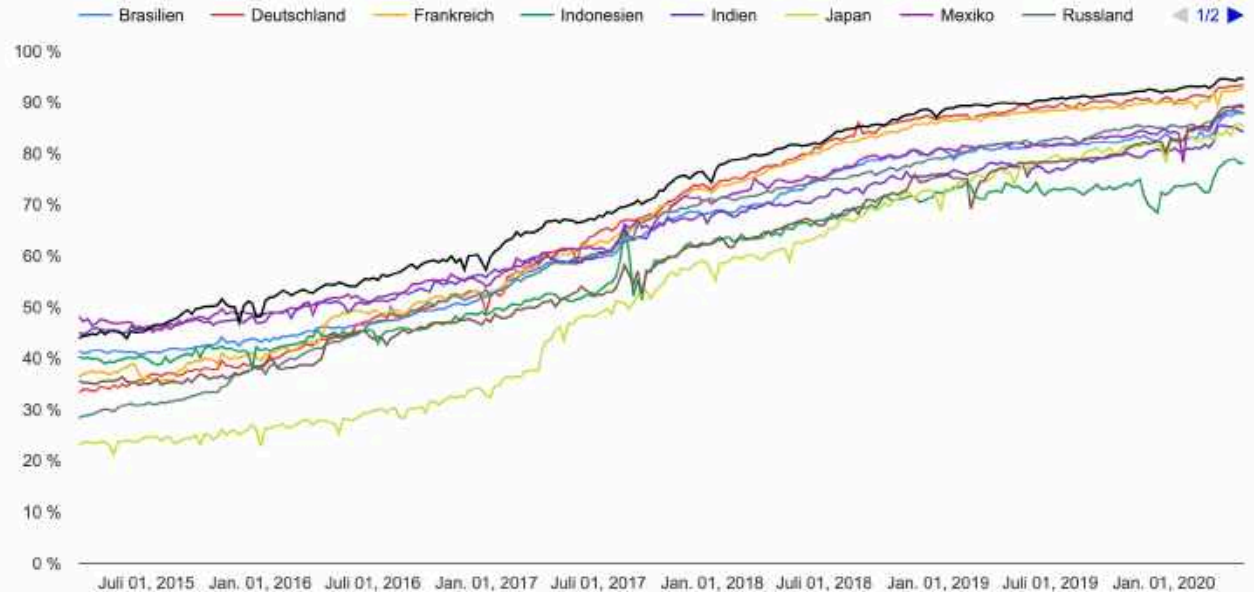
Best Practices HTTPS Content Inspection

Jonas Spieckermann | Senior Sales Engineer
Jonas.Spieckermann@watchguard.com
WatchGuard Technologies Inc.

Verschlüsselter Web-Traffic



Prozentsatz der in Chrome über HTTPS geladenen Seiten nach Land/Region



<https://transparencyreport.google.com/https/overview>

Cybercrime nutzt HTTPS

- „Den ... Analysen zufolge kann für Phishing-Angriffe in Deutschland von einem Verhältnis von ca. 55 % HTTP zu 45 % HTTPS ausgegangen werden. Eine entsprechende Entwicklung hin zur vermehrten Verwendung von HTTPS ist seit Mitte 2017 verstärkt zu beobachten.“
- „Hinsichtlich der Kommunikation von Schadsoftware mit den dazugehörigen Command-and-Control-Servern ist ein deutlicher Zuwachs an HTTPS-Kommunikation zu beobachten.“

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7

Ein mehrschichtiger Sicherheitsansatz

1. Gateway Antivirus

signaturbasierte AV Engine



2. Intelligent AV

KI-unterstützte Malware Erkennung

3. APT Blocker

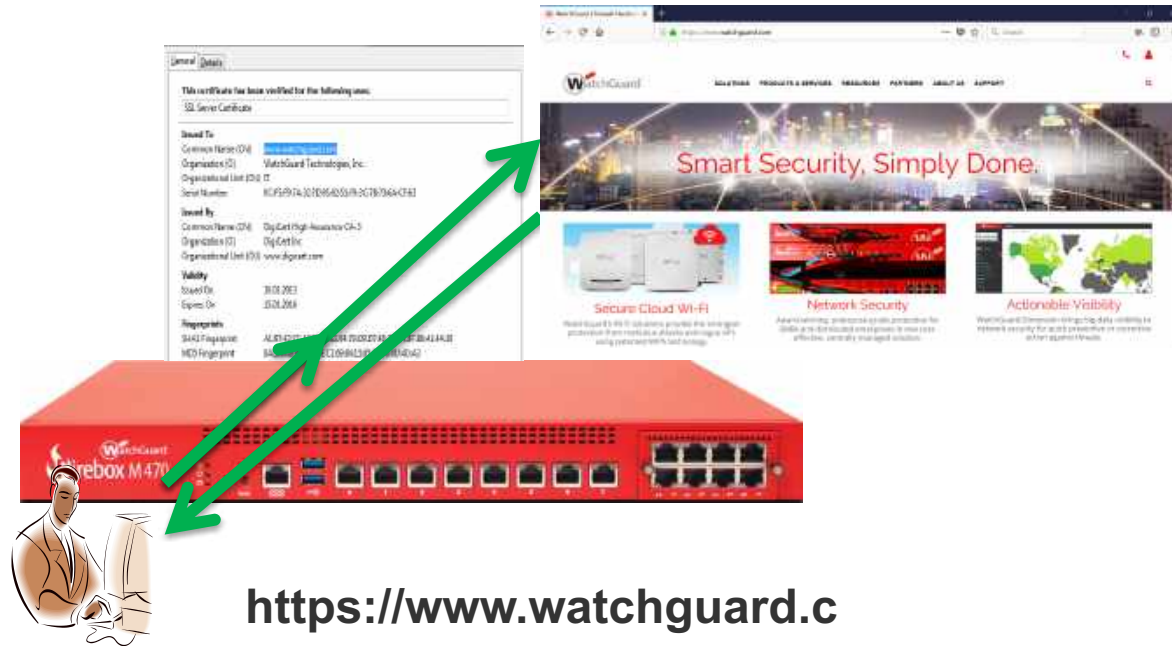
Sandbox Technologie

Gold (24x7)

Standard (24x7)



HTTPS ohne Content Inspection



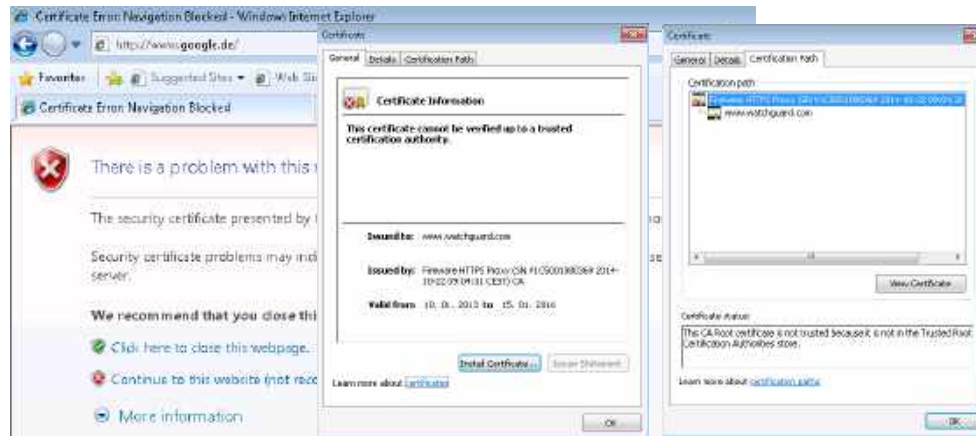
<https://www.watchguard.com>

HTTPS mit Content Inspection



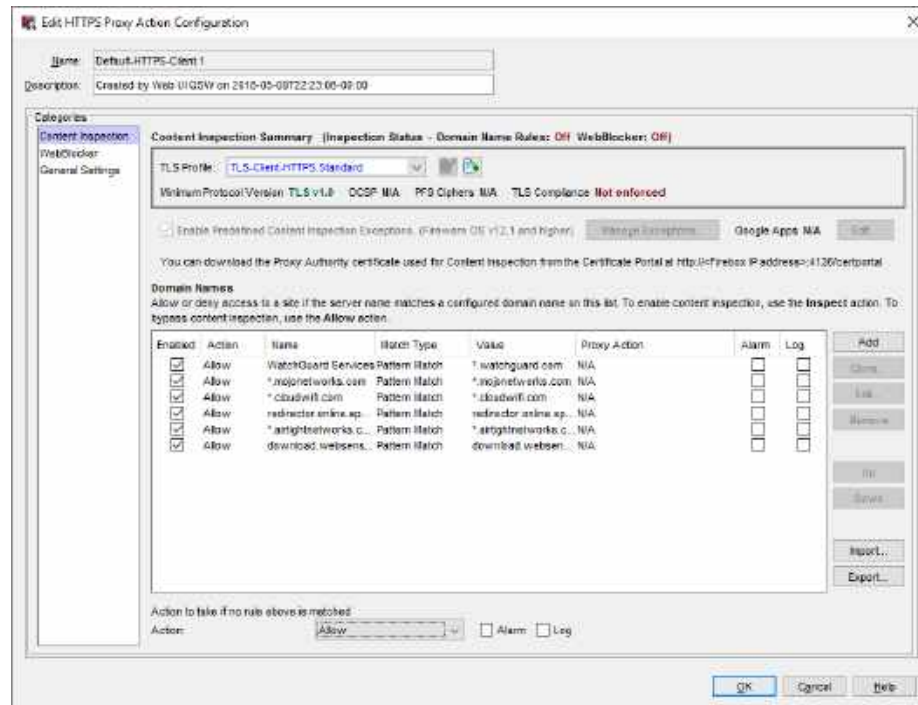
„Sichtbare“ Auswirkung

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



Konfiguration innerhalb des HTTPS Proxy

- Kontrolle des verschlüsselten Web Traffic (HTTPS)



TLS Profile

Settings

SD-WAN

Advanced

Proxy Action

Default-HTTPS-Client

HTTPS Proxy Action Settings

Name

Description

Content Inspection

Web Browser

Content Inspection Summary

TLS Profile

Minimum Protocol Version

Save

Cancel

TLS Profile

Name

Description

Minimum Protocol Version

☐ Allow only TLS-compliant traffic

Certificate Validation

☒ Use OCSP to validate certificates

☐ If a certificate cannot be validated, the certificate is considered invalid

Perfect Forward Security Ciphers

Allowed

If you select None, connections cannot use TLS v1.3.

Save

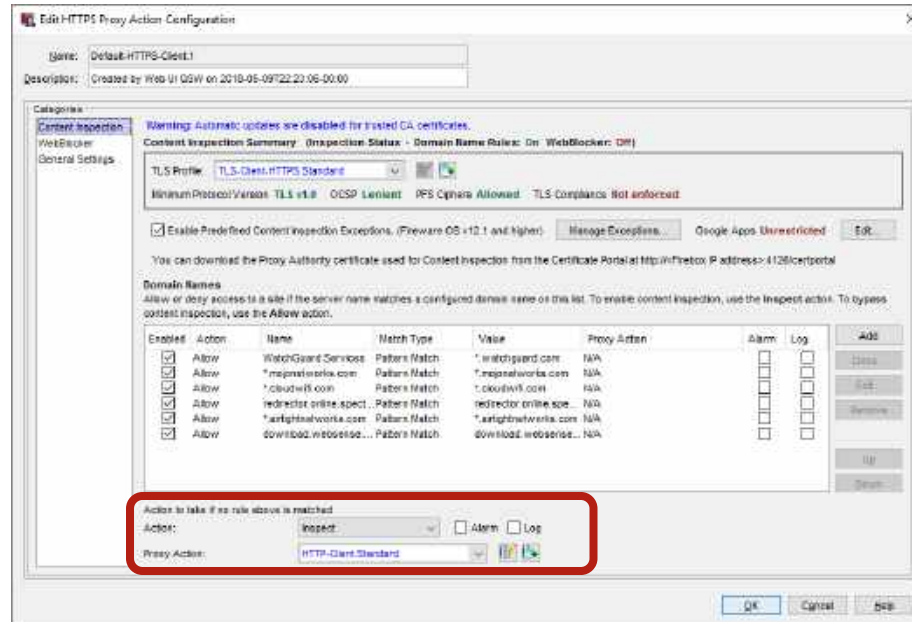
Cancel

Advanced

Server: Off

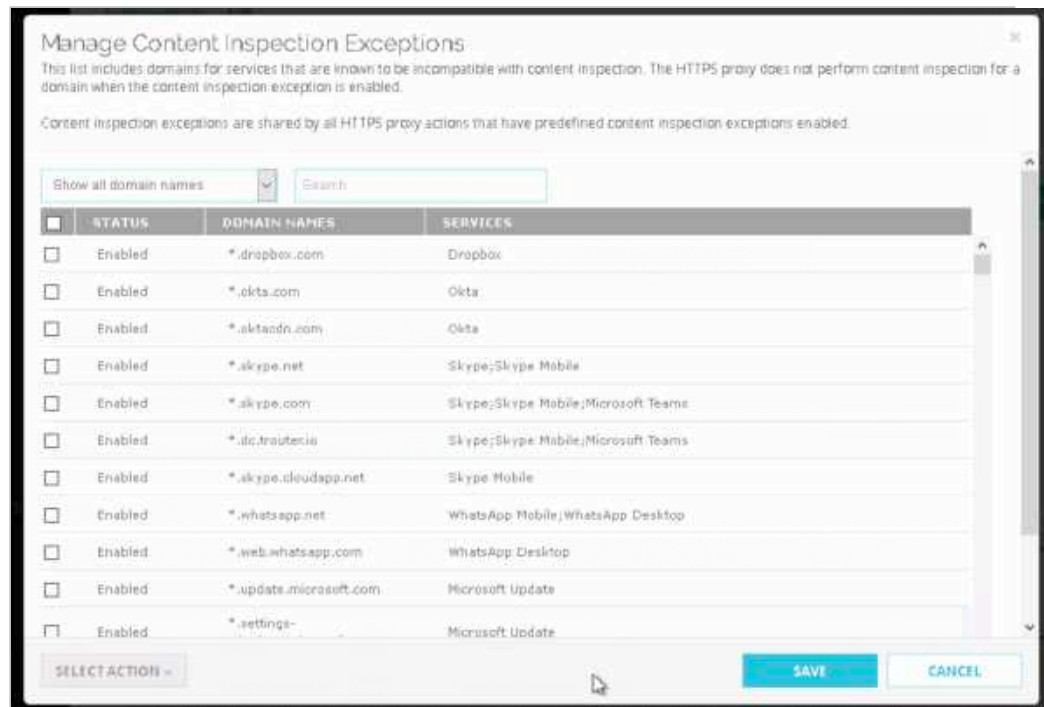
HTTPS Proxy und Content Inspection

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



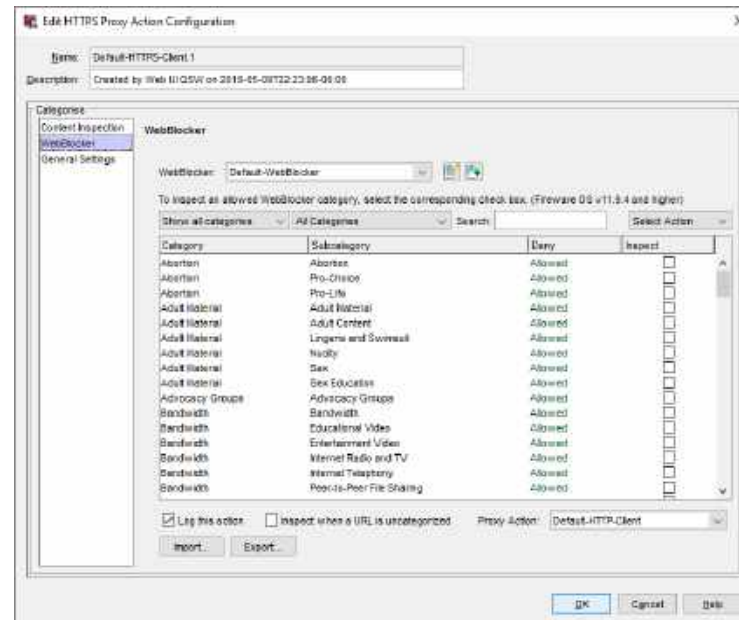
Predefined Content Inspection Exceptions

- Seit Version 12.1 verfügbar.



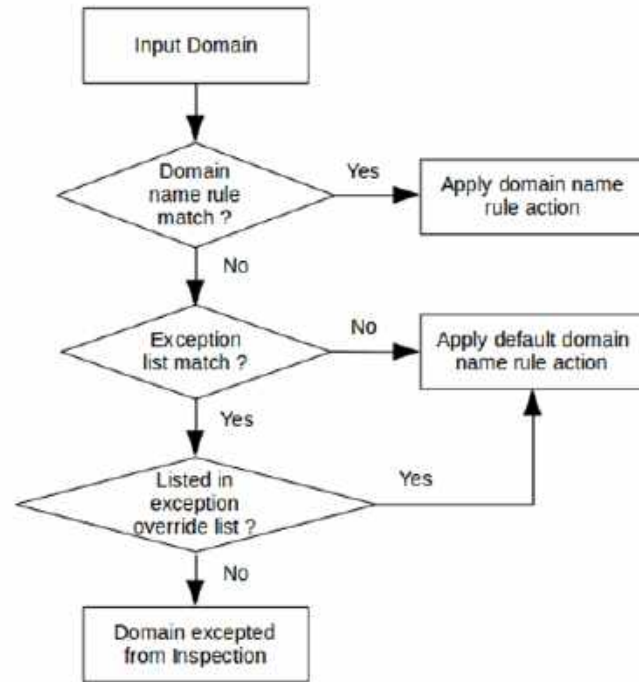
HTTPS Proxy und WebBlocker

- 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



- **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

Performance/Sizing

Firebox	M270	M370
THROUGHPUT¹		
Firewall (UDP 1518)	4.9 Gbps	8 Gbps
Firewall (IMIX)	1.8 Gbps	4.7 Gbps
VPN (UDP 1518)	1.6 Gbps	4.6 Gbps
VPN (IMIX)	480 Mbps	1.4 Gbps
HTTPS Content Inspection (IPS enabled)	480 Mbps	800 Mbps
Gateway AntiVirus	2.1 Gbps	3.0 Gbps
IPS (fast/full scan)	2.3/0.9 Gbps	4.8/2.5 Gbps
UTM (fast/full scan)	1.6/0.8 Gbps	2.6/1.7 Gbps

A background image showing a top-down view of several people's hands and forearms resting on a wooden desk. There are laptops, a smartphone, and a coffee cup visible. A red banner with a network diagram pattern is overlaid across the middle of the image.

Haben Sie noch Fragen?

A background image showing a top-down view of several people's hands and forearms gathered around a wooden desk. There are laptops, a smartphone, and a coffee cup on the desk. A red semi-transparent banner with a network diagram pattern is overlaid across the middle of the image.

Vielen Dank!

Jonas Spieckermann | Senior Sales Engineer
Jonas.Spieckermann@watchguard.com
WatchGuard Technologies Inc.