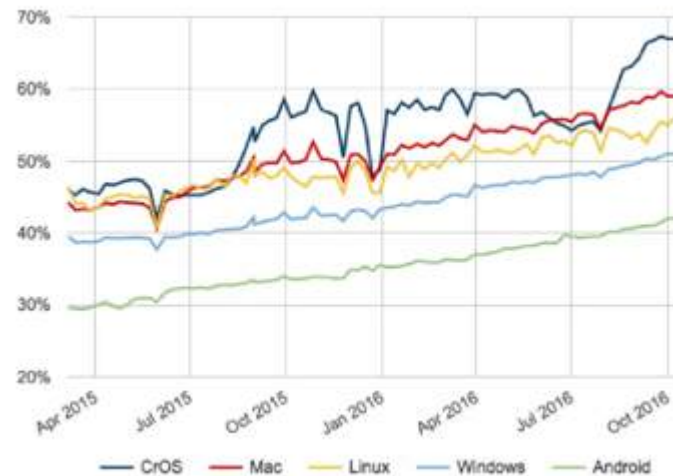


Best Practice – HTTPS Content Inspection

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

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	www.watchguard.com
Organization (O)	WatchGuard Technologies, Inc.
Organizational Unit (OU)	IT
Serial Number	0CF5:F9:7A:32:7D:85:02:51:F9:3C:7B:73:6A:CF:63

Issued By

Common Name (CN)	DigiCert High Assurance CA-3
Organization (O)	DigiCert, Inc.
Organizational Unit (OU)	www.digicert.com

Validity

Issued On	10.01.2013
Expires On	15.01.2016

Fingerprints

SHA1 Fingerprint	A197437C:11E64791D9D7487118F86414A30
MD5 Fingerprint	8A:5A:4B:5E:1E:1E:1E:1E:1E:1E:1E:1E:1E:1E:1E:1E

WatchGuard | Firewall Hardware

https://www.watchguard.com

WatchGuard

SOLUTIONS PRODUCTS & SERVICES RESOURCES PARTNERS ABOUT US SUPPORT

Smart Security, Simply Done.

Secure Cloud Wi-Fi

WatchGuard's Wi-Fi solutions provide the strongest protection from malicious attacks and rogue APs using patented WIPS technology.

Network Security

Award-winning, enterprise-grade protection for SMBs and distributed enterprises in one cost-effective, centrally managed solution.

Actionable Visibility

WatchGuard Dimension brings big-data visibility to network security for quick preventive or corrective action against threats.

WatchGuard
Firebox M470

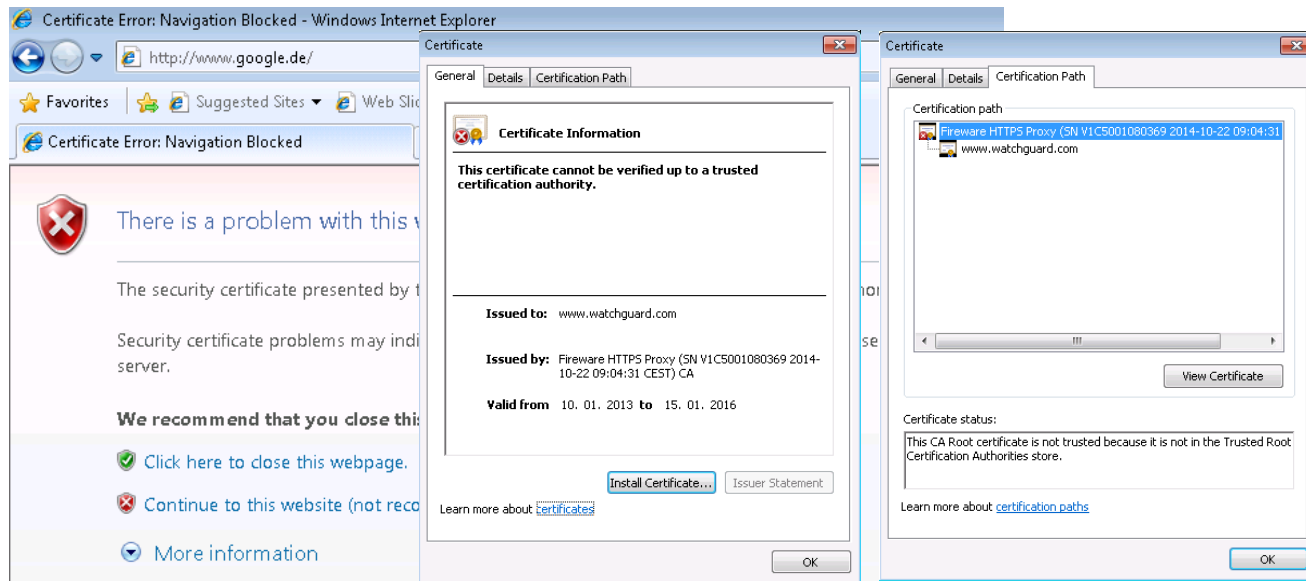
https://www.watchguard.com

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)

Edit HTTPS Proxy Action Configuration

Name: Default-HTTPS-Client.1
 Description: Created by Web UI QSW on 2018-05-09T22:23:06-00:00

Categories

- Content Inspection
- WebBlocker
- General Settings

Content Inspection Summary (Inspection Status - Domain Name Rules: Off WebBlocker: Off)

TLS Profile: **TLS-Client-HTTPS.Standard**

Minimum Protocol Version **TLS v1.0** OCSP **N/A** PFS Ciphers **N/A** TLS Compliance **Not enforced**

Enable Predefined Content Inspection Exceptions. (Fireware OS v12.1 and higher) **Manage Exceptions...** **Google Apps N/A** **Edit...**

You can download the Proxy Authority certificate used for Content Inspection from the Certificate Portal at <http://<Firebox IP address>-4126/certportal>

Domain Names
 Allow or deny access to a site if the server name matches a configured domain name on this list. To enable content inspection, use the **Inspect** action. To bypass content inspection, use the **Allow** action.

Enabled	Action	Name	Match Type	Value	Proxy Action	Alarm	Log
<input checked="" type="checkbox"/>	Allow	WatchGuard Services	Pattern Match	*.watchguard.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	*.mojonetworks.com	Pattern Match	*.mojonetworks.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	*.cloudwifi.com	Pattern Match	*.cloudwifi.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	redirector.online.sp...	Pattern Match	redirector.online.sp...	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	*.airtightnetworks.c...	Pattern Match	*.airtightnetworks.c...	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	download.websens...	Pattern Match	download.websen...	N/A	<input type="checkbox"/>	<input type="checkbox"/>

Action to take if no rule above is matched
 Action: **Allow** Alarm Log

OK **Cancel** **Help**

HTTPS Proxy und Content Inspection

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

Edit HTTPS Proxy Action Configuration

Name: Default-HTTPS-Client.1
Description: Created by Web UI QSW on 2018-05-09T22:23:06-00:00

Categories: Content Inspection, WebBlocker, General Settings

Warning: Automatic updates are disabled for trusted CA certificates.

Content Inspection Summary (Inspection Status - Domain Name Rules: On WebBlocker: Off)

TLS Profile: TLS-Client-HTTPS.Standard
Minimum Protocol Version TLS v1.0 OSCP Lenient PFS Ciphers Allowed TLS Compliance Not enforced

Enable Predefined Content Inspection Exceptions. (Fireware OS v12.1 and higher) [Manage Exceptions...](#) Google Apps **Unrestricted** [Edit...](#)

You can download the Proxy Authority certificate used for Content Inspection from the Certificate Portal at <http://<Firebox IP address>:4126/certportal>

Domain Names
Allow or deny access to a site if the server name matches a configured domain name on this list. To enable content inspection, use the **Inspect** action. To bypass content inspection, use the **Allow** action.

Enabled	Action	Name	Match Type	Value	Proxy Action	Alarm	Log	
<input checked="" type="checkbox"/>	Allow	WatchGuard Services	Pattern Match	*.watchguard.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>	Add
<input checked="" type="checkbox"/>	Allow	*.mojonetworks.com	Pattern Match	*.mojonetworks.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>	Clone...
<input checked="" type="checkbox"/>	Allow	*.cloudwifi.com	Pattern Match	*.cloudwifi.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>	Edit...
<input checked="" type="checkbox"/>	Allow	redirector.online.spe...	Pattern Match	redirector.online.spe...	N/A	<input type="checkbox"/>	<input type="checkbox"/>	Remove
<input checked="" type="checkbox"/>	Allow	*.airtightnetworks.com	Pattern Match	*.airtightnetworks.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>	Up
<input checked="" type="checkbox"/>	Allow	download.websense...	Pattern Match	download.websense...	N/A	<input type="checkbox"/>	<input type="checkbox"/>	Down

Action to take if no rule above is matched
Action: **Inspect** Alarm Log
Proxy Action: HTTP-Client.Standard

[OK](#) [Cancel](#) [Help](#)

TLS Profile

TLS Profile

X

Settings

SD-WAN

Ap

ng

Advanced

Name TLS-Client-HTTPS.Neu

Description Standard TLS profile for clients.

Proxy Action

Default-HTTPS-Client

HTTPS Proxy Action Set

Name D

Minimum Protocol Version

TLS v1.0

Description C

Allow only TLS-compliant traffic

Content Inspection

WebBlk

Certificate Validation

Use OCSP to validate certificates

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

er: Off)

Content Inspection Sur

TLS Profile TLS-Client-HTTPS.N

Minimum Protocol Version **TLS v1**

Perfect Forward Secrecy Ciphers

Allowed

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

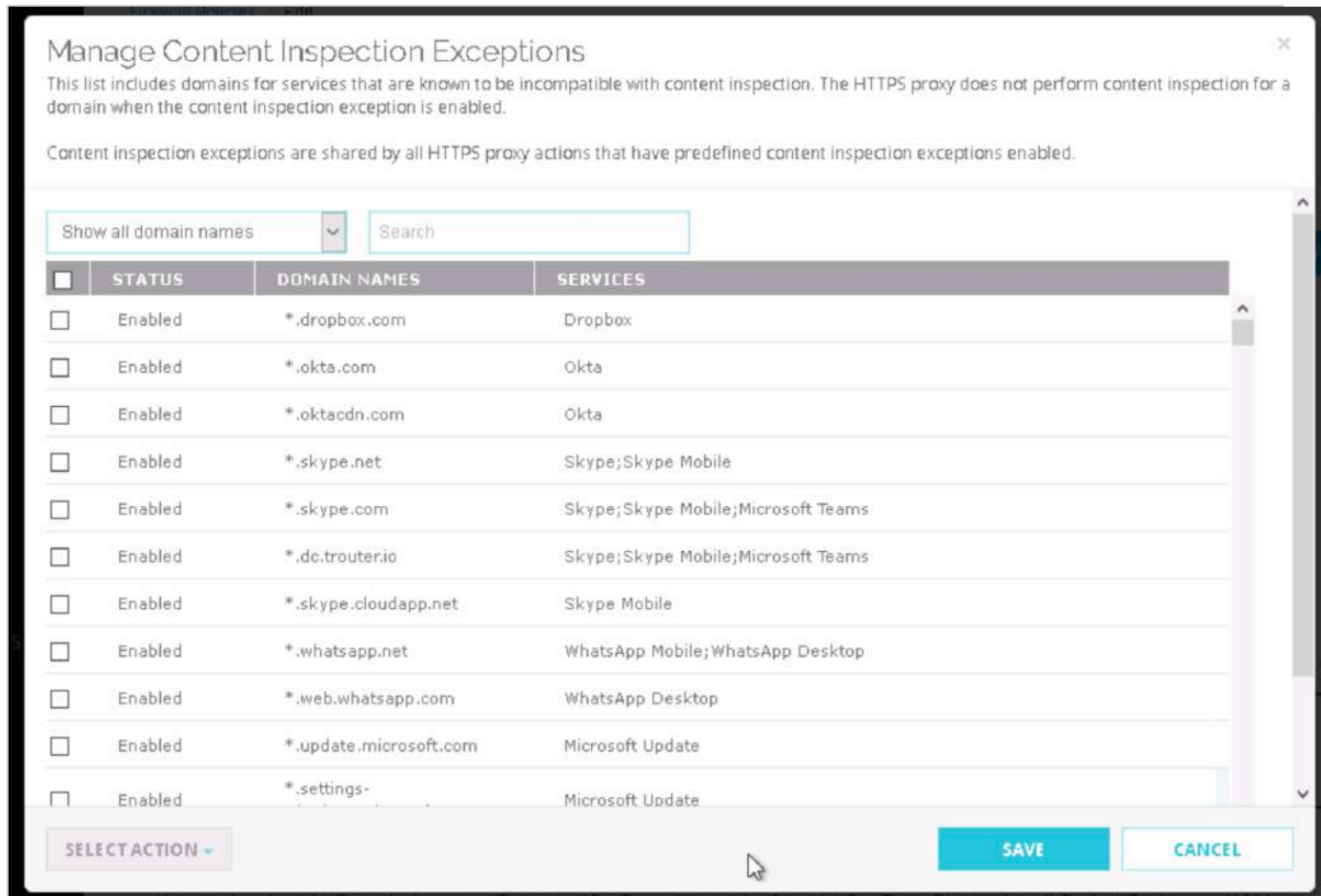
SAVE

CANCEL



Predefined Content Inspection Exceptions

- Seit Version 12.1 verfügbar.



Manage Content Inspection Exceptions

This list includes domains for services that are known to be incompatible with content inspection. The HTTPS proxy does not perform content inspection for a domain when the content inspection exception is enabled.

Content inspection exceptions are shared by all HTTPS proxy actions that have predefined content inspection exceptions enabled.

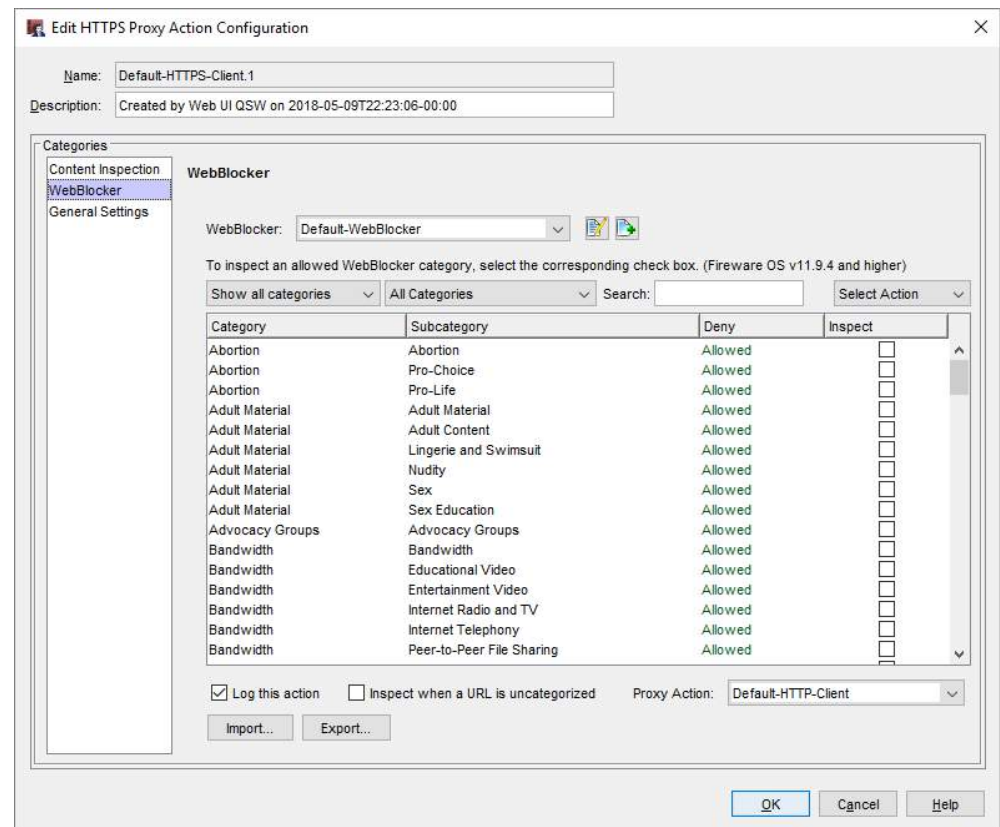
Show all domain names

<input type="checkbox"/>	STATUS	DOMAIN NAMES	SERVICES
<input type="checkbox"/>	Enabled	*.dropbox.com	Dropbox
<input type="checkbox"/>	Enabled	*.okta.com	Okta
<input type="checkbox"/>	Enabled	*.oktacdn.com	Okta
<input type="checkbox"/>	Enabled	*.skype.net	Skype;Skype Mobile
<input type="checkbox"/>	Enabled	*.skype.com	Skype;Skype Mobile;Microsoft Teams
<input type="checkbox"/>	Enabled	*.dc.trouter.io	Skype;Skype Mobile;Microsoft Teams
<input type="checkbox"/>	Enabled	*.skype.cloudapp.net	Skype Mobile
<input type="checkbox"/>	Enabled	*.whatsapp.net	WhatsApp Mobile;WhatsApp Desktop
<input type="checkbox"/>	Enabled	*.web.whatsapp.com	WhatsApp Desktop
<input type="checkbox"/>	Enabled	*.update.microsoft.com	Microsoft Update
<input type="checkbox"/>	Enabled	*.settings-	Microsoft Update

SELECT ACTION

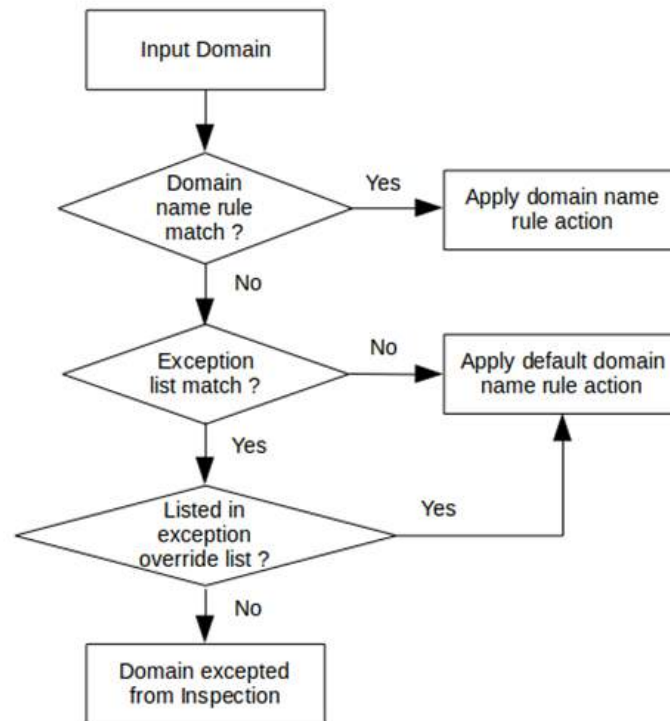
HTTPS Proxy und WebBlocker

- 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

Certificates - 203.0.113.100

Certificates

This Firebox contains these certificates and certificate requests: Show: All Certificates (except Trusted CA for Proxy) ▾

Status	Import Date	Type	Algo.	Subject Name
Pending		Web Client	RSA	cn=WatchGuard Firebox
Signed	2019-03-18 11:37	IPSec / Web	RSA	o=WatchGuard-Demo-JSP cn=203.0.113.100
Signed	2019-01-24 10:42	Web Client	RSA	o=WatchGuard ou=Fireware cn=Fireware web Client
Signed*	2019-01-24 10:42	CA Cert	RSA	o=WatchGuard ou=Fireware cn=Fireware web CA
Signed	2019-01-24 10:42	Web Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN Server
Signed	2019-01-24 10:42	Web Client	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN Client
Signed	2019-01-24 10:42	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN (SN FVE100000000
Signed	2019-01-24 10:42	Proxy Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=https.proxy.nul
Signed	2019-01-24 10:42	Proxy Authority	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware HTTPS Proxy (SN FVE1000
Signed	2019-01-24 12:41	CA Cert	RSA	cn=WatchGuard Firebox
Signed	2019-01-24 10:42	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware IKE (SN FVE1000000000 2
Signed	2019-03-18 11:37	CA Cert	RSA	o=WatchGuard-Demo-JSP cn=WatchGuard Certificate Authority
Signed	2019-01-24 12:41	CA Cert	RSA	c=US o=VeriSign ou=VeriSign Trust Network cn=VeriSign Class 3 Public Primary Cer
Signed	2019-01-24 10:42	Web Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware IEEE 802.1X Server
Signed	2019-01-24 10:42	CA Cert	RSA	o=WatchGuard Technologies ou=Fireware cn=Fireware IEEE 802.1X (SN FVE1000

* Currently active Firebox web server certificate

Details

Delete

Refresh

Export

Import Certificate

Import CRL

Create CSR

Aktivierung von Content Inspection

- Welches Zertifikat sollte verwendet werden für Content Inspection?
 - 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.***

