

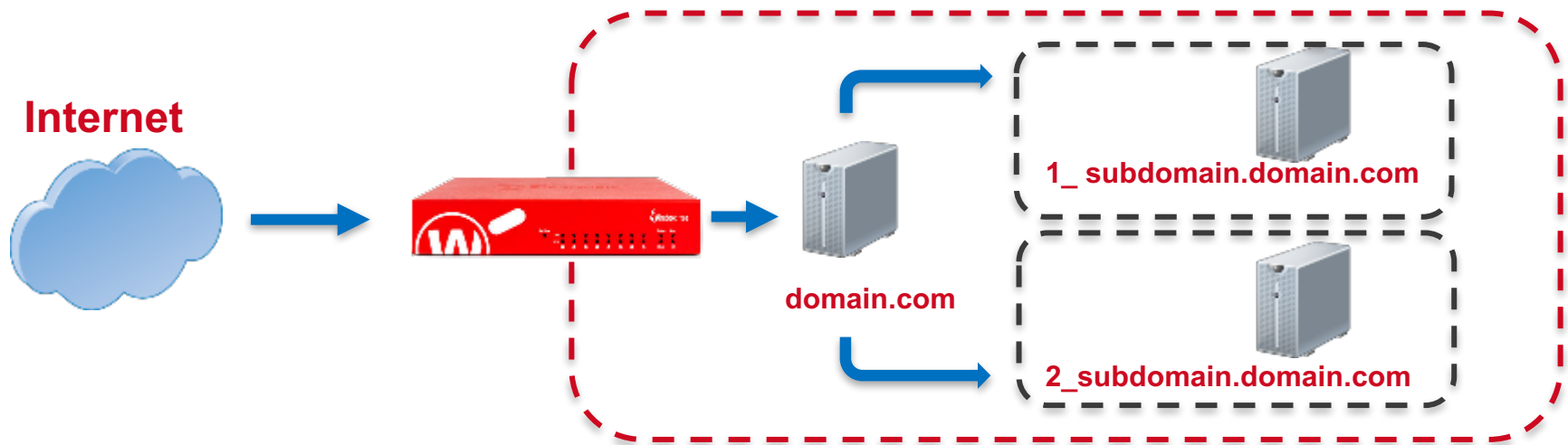


# Best Practices – Firebox - Host Header Redirection ermöglicht flexible Webserver-Veröffentlichung auch bei einzelner public IP

Thomas Fleischmann  
Senior Sales Engineer, Central Europe  
Thomas.Fleischmann@watchguard.com

# Host Header redirect

- Ein gängiges Reverse-Proxy-Szenario besteht darin, mehrere interne Webanwendungen verfügbar zu machen, die über einen einzigen Webserveranruf zugänglich sind, und zwar aufgrund der beschränkten IP-Adressierung (IPv4)
  - Firebox besitzt die Fähigkeit, eingehenden Datenverkehr auf verschiedenen Servern basierend auf dem Domain- und URL-Pfad in der HTTP-Anfrage weiterzuleiten



Ermöglicht das SSL-Offloading für HTTPS content inspection

# Content Actions und Routing Actions

- Eine Content Action ist eine neue Art von Proxy-Aktion für eingehende HTTP-Proxy-Richtlinien und HTTPS Server-Proxy-Action
- Wählen Sie eine Content Action aus, um dieselbe öffentliche IP-Adresse für mehrere öffentliche Webserver zu verwenden, die sich hinter der Firebox befinden
  - Mithilfe einer Content Action kann die Firebox eingehende HTTP- und HTTPS-Anforderungen für eine öffentliche IP-Adresse an mehr als einen internen Webserver routen
  - Dies reduziert die Anzahl der öffentlichen IP-Adressen, die Sie für Webserver in Ihrem Netzwerk benötigen
- Um HTTPS-Request, basierend auf dem Domännennamen ohne Content Inspection, umzuleiten, können sie in einer Domain Name Rule eine Routing-Action bei der HTTPS Server-Proxy-Action angeben

# Content Actions und Routing Actions

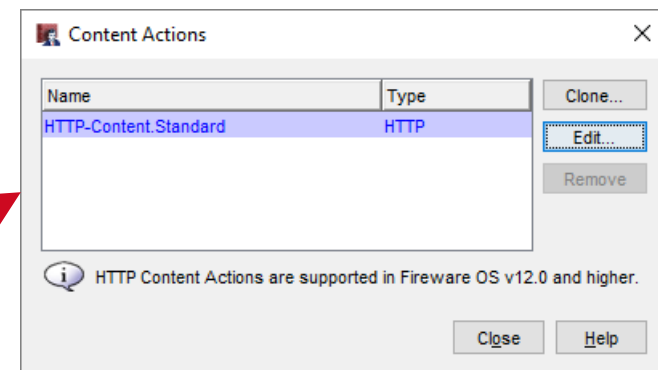
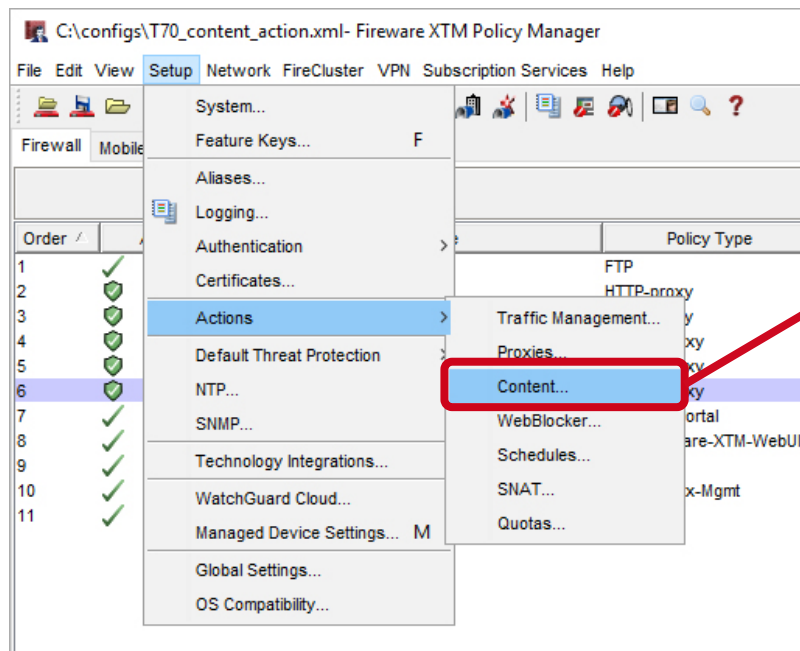
- Content Action haben zwei Hauptfunktionen:
  - Host-Header-Weiterleitung
    - Sendet eingehende HTTP- und geprüfte HTTPS-Anforderungen an verschiedene interne Server basierend auf dem Pfad und der Domäne in der HTTP-Anforderung
  - TLS / SSL-Offloadingg
    - Entlastet einen internen Webserver von der Verarbeitungslast für die Ver- und Entschlüsselung von TLS- und SSL-Verbindungen
      - Verschlüsselter (HTTPS) Datenverkehr zwischen externen Clients und der Firebox
      - Clear-Text (HTTP) Verkehr zwischen der Firebox und dem internen Server
- In einer HTTPS Server-Proxy-Action wird durch Routing-Actions eingehende HTTPS-Request, basierend auf dem Domain Names, an interne Server weitergeleitet, ohne das eine Inhaltsprüfung erfolgt.

# Content Actions und Routing Actions

- Content Action
  - Passt den Host-Header / Pfad für jede HTTP-Request an
  - Sendet ein HTTP-Request an eine bestimmte IP-Adresse und einen bestimmten Port
  - Die Inhaltsaktionen überschreiben keine Daten in der Request oder Response
- Anwendungsfälle für Content Action:
  - Umleiten von HTTP-Request basierend auf der Domäne und dem Host
  - Umleiten von HTTPS-Request mit Content Inspection
  - SSL-Offloading für HTTPS-Request mit Content Inspection
- Anwendungsfall für Routing Actions im HTTPS Server-Proxy:
  - Umleiten von HTTPS ohne Content Inspection

# Content Action Konfiguration

- Content Actions sind von anderen Proxy-Aktionen getrennt
- Wählen Sie im Policy Manager **Setup> Actions> Content**
- Um eine neue Content Action zu erstellen, klonen oder bearbeiten Sie die vordefinierte Content Action



# Content Action Konfiguration

- In einer Content Action können Sie Folgendes konfigurieren:
  - Content Action: Action für jedes Ziel basierend darauf, ob der Content mit den Host-Header oder SNI der angegebenen Domäne und dem angegebenen Pfad übereinstimmen
  - Die zu ergreifende Action, wenn keine Content Action übereinstimmt

Clone HTTP Content Action Configuration

Name:

Description:

The rule settings you specify are compared to the absolute URI (the HTTP host header and URI path) in the request. The TLS/SSL Offload setting is only applied to HTTPS proxy policies with Content Inspection enabled.

Enabled	Name	Match Type	Value	Proxy Action	Routing Action	Ports (HTTP/HTTPS)	TLS/SSL Offload	Log
<input checked="" type="checkbox"/>	example.com	Pattern Match	example.com*	HTTP-Server.custom	10.0.40.80	80/443	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Action to take if no rule above is matched

Proxy Action:

Routing Action:  Use Policy Default  Use

HTTP Port:  Use Policy Default  Use

HTTPS Port:  Use Policy Default  Use

TLS/SSL Offload  Log

OK Cancel Help

# Content Rules

- Jede Content Action legt fest:
  - Ein passendes Pattern
  - HTTP Proxy Action
  - Routing Action (IP Adresse)
  - HTTP und HTTPS Ports
  - TLS/SSL Offload Einstellung
  - Log Einstellung
  
- Pattern Übereinstimmung mit Domäne und Host :
  - Domain only                      wiki.example.net/\*
  - Path                                      \*/blog/\*
  - Domain und Pfad                      “blog.example.net/resource/\*”

The screenshot shows the 'New Content Rule' dialog box. The 'Rule Name' field contains 'example.com'. Under 'Rule Settings', the 'Pattern Match' dropdown is set to 'example.com/\*', with a note below it: '(\*.?.\*) Wildcards' and 'Use %0x[hex-data]%' for binary data. Under 'Rule Actions', the 'Proxy Action' is set to 'HTTP-Server.Standard'. The 'Routing Action' is set to 'Use' with the IP address '10.0.50.80'. The 'HTTP Port' is set to 'Use' with the value '80'. The 'HTTPS Port' is set to 'Use' with the value '443'. The 'Log' checkbox is checked, and the 'TLS/SSL Offload' checkbox is unchecked. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.



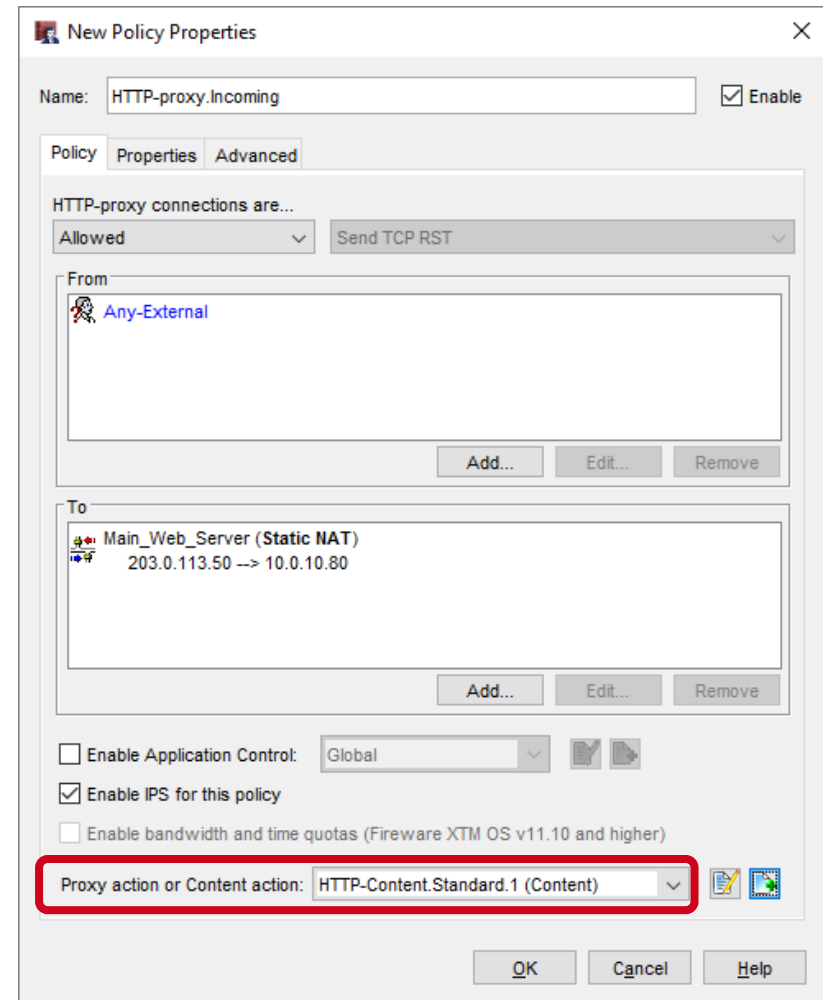
# TLS/SSL Offloading

- Um TLS/SSL Offloading für HTTPS zu aktivieren, muss man unter der Content Rule Action, die **TLS/SSL Offload** check box anhaken.
- Mit TLS/SSL Offloading:
  - HTTPS wird zwischen externen Clients und der Firebox verwendet
  - HTTP wird zwischen der Firebox und den internen Server verwendet.

The screenshot shows the 'New Content Rule' configuration window. The rule name is 'TLS Offload'. The 'Rule Settings' section shows a 'Pattern Match' of 'example\_ssl.com/\*'. The 'Rule Actions' section shows the following settings: Proxy Action: HTTP-Server.Standard; Routing Action: Use (selected) with IP 10.0.80.100; HTTP Port: Use (selected) with port 80; HTTPS Port: Use (selected) with port 443. The 'TLS/SSL Offload' checkbox is checked and highlighted with a red box. The 'Log' checkbox is also checked. Buttons for 'OK', 'Cancel', and 'Help' are at the bottom.

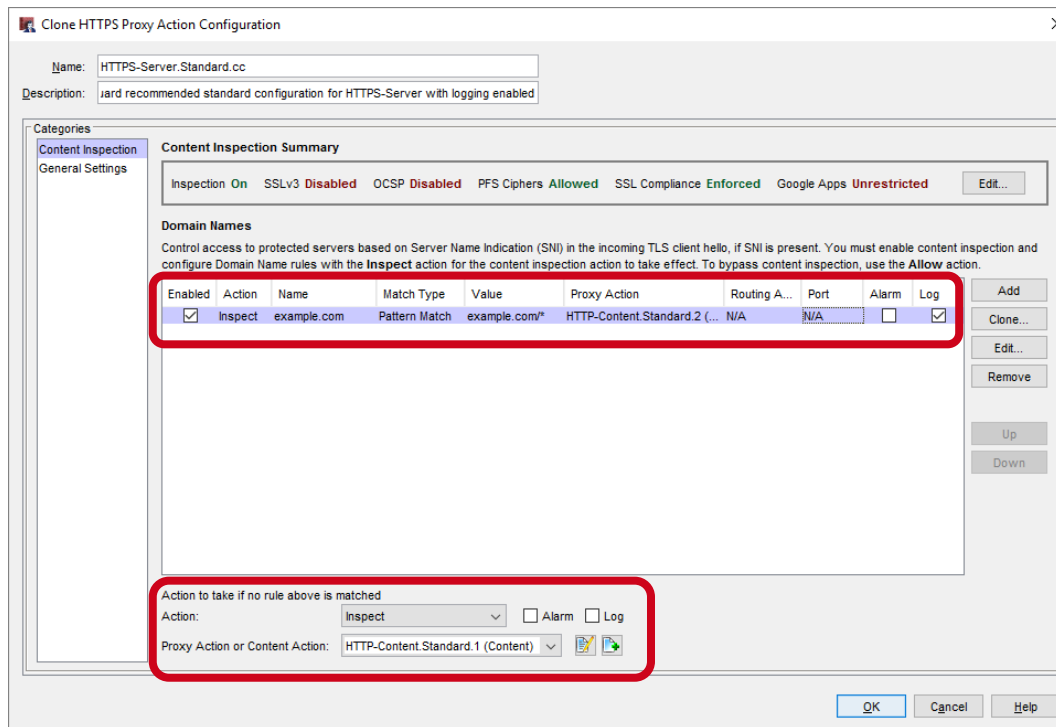
# Content Action mit dem HTTP Proxy

- Im HTTP Proxy Policy, wähle **Content Action**
  - Die Drop-Down Liste umfasst jeweils Proxy Action und Content Action
- In der Policy **To** Liste, füge eine **Static NAT** Regel ein, oder nutzte 1-to-1 NAT
  - Die Policy NAT Einstellungen werden nicht verwendet, außer eine Routing Action in der Content Action verweist auf **Use Policy Default**



# Content Action mit einem HTTPS Server Proxy

- So verwenden Sie eine Content Action in einer Domain Name Rule oder in der Standard Action, wenn keine Regel übereinstimmt:
  - Wähle die **Inspect** Action
  - Wähle eine Content Action



# Routing Action in einem HTTPS Server Proxy

- So routen Sie HTTPs Request ohne Content Inspection in einer Domain Name Rule oder in der Standard Action, wenn keine Regel übereinstimmt :
  1. Wähle die **Allow** Action
  2. Konfiguriere eine Routing Action und den Port

**New Domain Name Rule**

Rule Name:

Rule Settings

Pattern Match:   
(\*.[.] Wildcards)  
Use '%0x[hex-data]%' for binary data

Rule Actions

Action:   Alarm  Log

Routing Action:  Use Policy Default  Use

Port:  Use Policy Default  Use

# Routing Action in einem HTTPS Server Proxy

- Die Routing-Aktion vergleicht den Domainnamen, den Sie in einer Domain Name Action angeben haben, mit dem Domainnamen in der TLS- Server Name Indication (SNI) oder dem Common Name eines Servers im Serverzertifikat
  - Bei HTTPS-Anfragen gibt das SNI im TLS-Handshake die Domäne und den Pfad des Zielserver an
  - SNI ist in RFC 6066 TLS Extensions beschrieben

# Routing Action in einem HTTPS Server Proxy

Edit HTTPS Proxy Action Configuration

Name:

Description:

Categories

- Content Inspection
- General Settings

**Content Inspection Summary**

Inspection **Off** SSLv3 **N/A** OCSP **N/A** PFS Ciphers **N/A** SSL Compliance **Not enforced** Google Apps **N/A**

**Domain Names**

Control access to protected servers based on Server Name Indication (SNI) in the incoming TLS client hello, if SNI is present. You must enable content inspection and configure Domain Name rules with the **Inspect** action for the content inspection action to take effect. To bypass content inspection, use the **Allow** action.

Enabled	Action	Name	Match Type	Value	Proxy Action	Routing Action	Port	Alarm	Log
<input checked="" type="checkbox"/>	Allow	example.com	Pattern Match	example.com	N/A	Policy Default	Policy Default	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	example_web.com	Pattern Match	example_web.com	N/A	10.0.60.80	Policy Default	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Action to take if no rule above is matched

Action:   Alarm  Log

Routing Action:  Use Policy Default  Use

Port:  Use Policy Default  Use

# Proxy Action Änderungen

- Einige Proxy Action Einstellungen wurden aus den HTTP-Server- und HTTPS Server-Proxy Action entfernt, da sie nicht auf eingehende Verbindungen zu einem Webserver anwendbar sind
  - HTTP Server Proxy Action enthalten jetzt kein:
    - WebBlocker
    - Reputation Enabled Defense
  - HTTPS Server Proxy Action enthalten jetzt kein:
    - WebBlocker
    - OCSP (Online Certificate Status Protocol)
      - Keine Zertifikatüberprüfung in HTTPS Server Proxy Action

# HTTPS Proxy Action Änderungen

- WebBlocker wurde aus der Liste "Kategorien" entfernt.
- Content Inspection und Domain Names werden jetzt in der Kategorie "Content Inspection" zusammengefasst
- Um die Einstellungen für die Content Inspection zu ändern, klicken Sie im Abschnitt **Content Inspection Summary** auf Bearbeiten.

Clone HTTPS Proxy Action Configuration

Name: HTTPS-Server.Standard.cc

Description: Iard recommended standard configuration for HTTPS-Server with logging enabled

Categories

- Content Inspection
- General Settings

**Content Inspection Summary**

Inspection **On**   SSLv3 **Disabled**   OCSP **Disabled**   PFS Ciphers **Allowed**   SSL Compliance **Enforced**   Google Apps **Unrestricted**   [Edit...](#)

**Domain Names**

Control access to protected servers based on Server Name Indication (SNI) in the incoming TLS client hello, if SNI is present. You must enable content inspection and configure Domain Name rules with the **Inspect** action for the content inspection action to take effect. To bypass content inspection, use the **Allow** action.

Enabled	Action	Name	Match Type	Value	Proxy Action	Routing A...	Port	Alarm	Log
<input checked="" type="checkbox"/>	Inspect	example.com	Pattern Match	example.com/*	HTTP-Content.Standard.2 (...	N/A	N/A	<input type="checkbox"/>	<input checked="" type="checkbox"/>

[Add](#)  
[Clone...](#)  
[Edit...](#)  
[Remove](#)



# HTTPS Proxy Action Änderungen

- Die Einstellungen für die Inhaltsprüfung sind dieselben wie in Firewall v11.x, mit der Ausnahme, dass keine HTTP-Client-Proxy Action ausgewählt wird
- Jetzt legt man bei jeder Auswahl der Action "Inspect" eine HTTP-Client-Proxy Action fest
  - Sie können verschiedene HTTP-Proxy Actions für Domain Name Rules und WebBlocker verwenden

**Content Inspection Settings**

Allow only SSL compliant traffic

**Enable Content Inspection**

Content Inspection applies only to Domain Name rules with the Inspect action and to WebBlocker categories you select to inspect.

When Content Inspection is enabled you can download the Proxy Authority certificate from the Certificate Portal at <http://<Firebox IP address>:4126/certportal>

Allow SSLv3

**Certificate Validation**

[For Fireware OS v12.0 and higher, certificate validation does not occur for HTTPS proxy server actions](#)

Use OCSP to validate certificates

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

**Perfect Forward Secrecy Ciphers**

Allowed ▾

**Google Apps Allowed Domains**

Restrict Google Apps to Allowed Domains

Text input field for domains

Add Remove

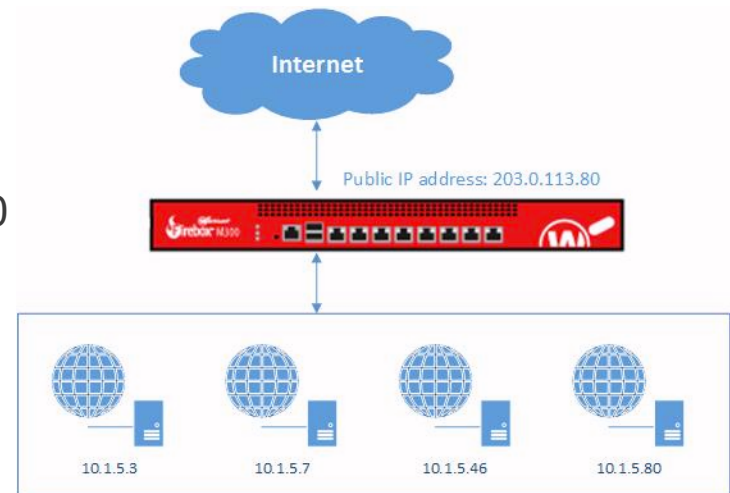
OK Cancel Help



# Beispiele

# HTTP Proxy mit einer HTTP Content Action

- Eine Organisation hat vier Server im privaten Netzwerk und möchte eine einzige öffentliche IP-Adresse für eingehende HTTP-Verbindungen zu allen Servern verwenden.
- Documentation library is on the web server at 10.1.5.3
- Image library is on the web server at 10.1.5.7
- Audio library is on the web server at 10.1.5.46
- Main website is on the web server at 10.1.5.80



# HTTP Proxy mit einer HTTP Content Action

- Die Content Action leitet HTTP-Anforderungen auf drei interne Server um, basierend auf der Domäne im HTTP-Host-Header und dem URI-Pfad in der HTTP-Anforderung.
- Alle anderen HTTP-Anforderungen werden an den Hauptwebserver gesendet, der in einer SNAT-Aktion in der Richtlinie angegeben ist.

Content Rule Name	Pattern Match Value	Routing Action
Documentation	*.example.com/docs/*	10.1.5.3
Images	*.example.com/images/*	10.1.5.7
Audio	*/audio/*	10.1.5.46
Action to take if no rule above is matched	N/A	Use Policy Default (10.1.5.80)

# HTTP Proxy mit einer HTTP Content Action

Firewall Policies / Edit

Name   Enable

Settings Application Control Traffic Management Proxy Action Scheduling Advanced

Proxy Action or Content Action

HTTP Content Action Settings

Name

Description

The rule settings you specify are compared to the absolute URI (the HTTP host header and URI path) in the request. The TLS/SSL Offload setting is only applied to HTTPS proxy policies with Content Inspection enabled.

ENABLED	NAME	MATCH TYPE	VALUE	PROXY ACTION	ROUTING ACTION	PORTS (HTTP/HTTPS)	TLS/SSL OFFLOAD	LOG
<input checked="" type="checkbox"/>	Documentation	Pattern Match	*.example.com/docs/*	HTTP-Server.Standard.1	10.1.5.3	80/443	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Images	Pattern Match	*.example.com/images/*	HTTP-Server.Standard.1	10.1.5.7	80/443	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Audio	Pattern Match	*/audio/*	HTTP-Server.Standard.2	10.1.5.46	80/443	<input type="checkbox"/>	<input checked="" type="checkbox"/>

ADD CLONE EDIT REMOVE MOVE UP MOVE DOWN

Action to take if no rule above is matched

Proxy Action

Routing Action  Use Policy Default  Use

HTTP Port  Use Policy Default  Use

HTTPS Port  Use Policy Default  Use

TLS/SSL Offload  Log

# HTTP Proxy mit einer HTTP Content Action

Firewall Policies / Edit

Name   Enable

Settings Application Control Traffic Management Proxy Action Scheduling Advanced

Connections are

Policy Type **HTTP-proxy**

PORT	PROTOCOL
80	TCP

**FROM**

- Any-External

**TO**

- main\_web\_server (SNAT)
- Any-External --> 10.1.5.80

ADD REMOVE

ADD REMOVE

# Weitere Beispiele

- Weitere Beispiele zum Thema finden sie in unserer Online Dokumentation unter

## **HTTP Content Action and Domain Name Rule Examples**

[https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/proxies/examples/content\\_action\\_examples\\_c.html](https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/proxies/examples/content_action_examples_c.html)



**Thank You!**