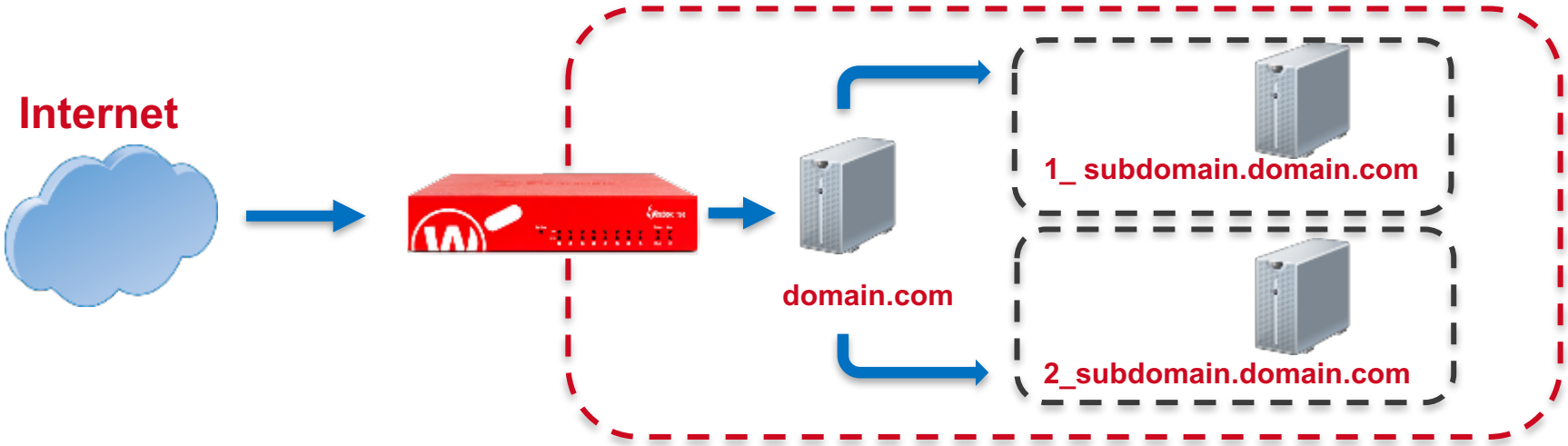
Best Practices –
Firebox - Host Header Redirection ermöglicht flexible Webserver-Veröffentlichung auch bei einzelner public IP

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

WatchGuard Training

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 Domänennamen 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

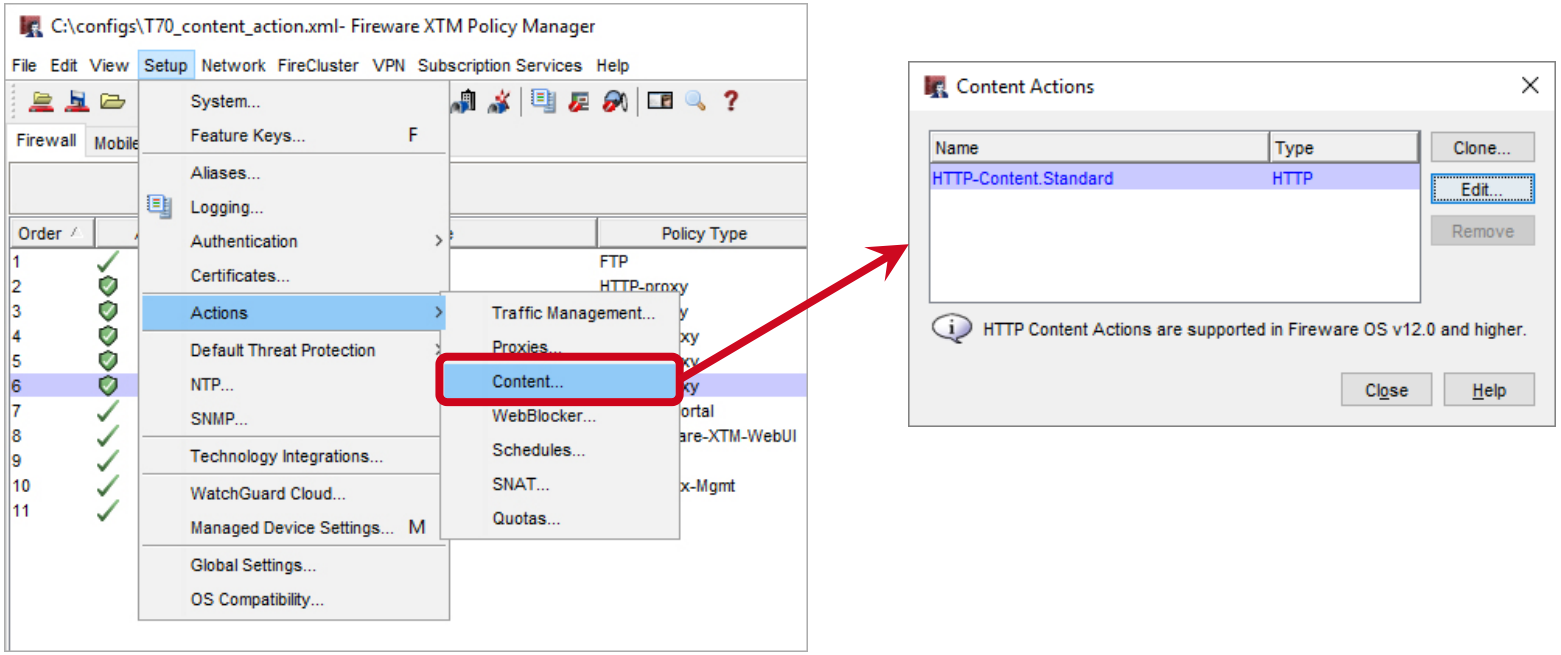
- Content Action haben zwei Hauptfunktionen:
  - Host-Header-Weiterleitung
    - Sendet eingehende HTTP- und geprüfte HTTPS-Anforderungen an verschiedene interne Server basierend auf dem Pfad und der Domäne in der HTTP-Anforderung
  - TLS / SSL-Offloadingg
    - Entlastet einen internen Webserver von 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

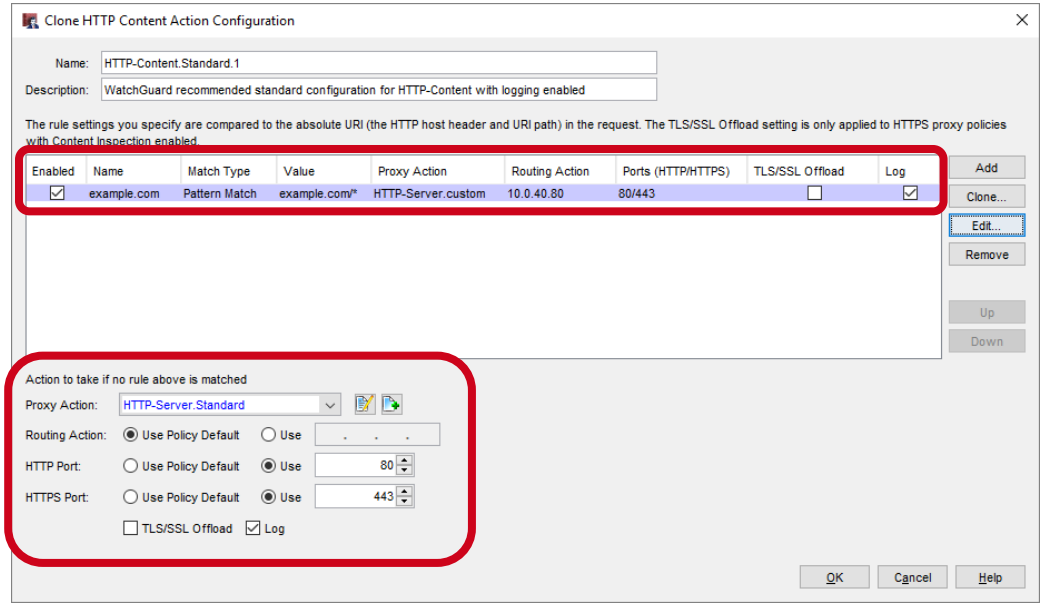
Content Action Konfiguration

- 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



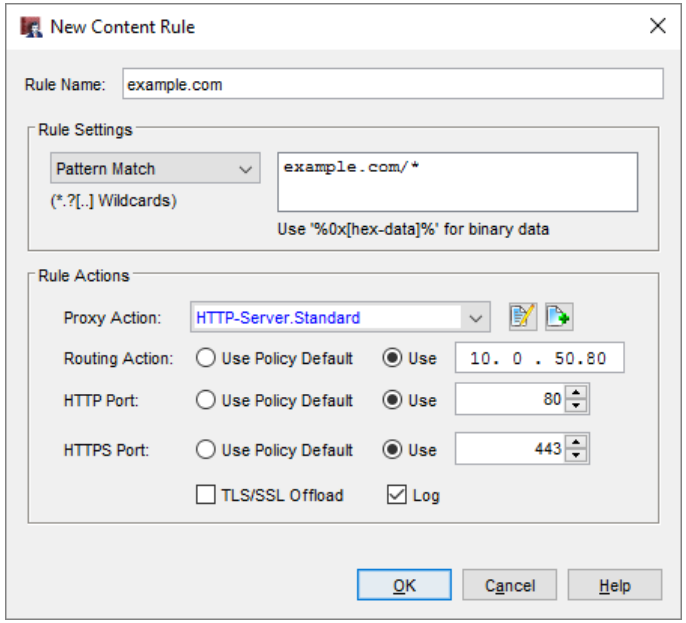
Content Action Konfiguration

- 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



Content Rules

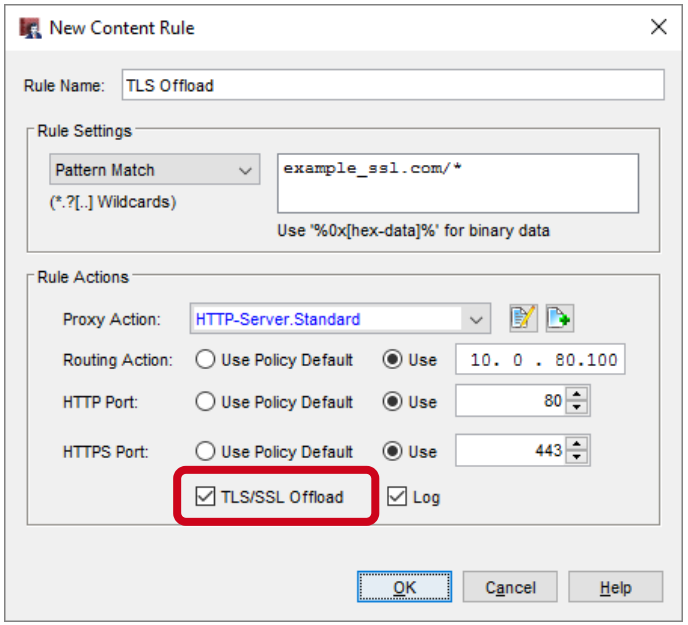
- Jede Content Action legt fest:
  - Ein passendes Pattern
  - HTTP Proxy Action
  - Routing Action (IP Adresse)
  - HTTP und HTTPS Ports
  - TLS/SSL Offload Einstellung
  - Log Einstellung



- Pattern Übereinstimmung mit Domäne und Host :
  - Domain only wiki.example.net/*
  - Path */blog/*
  - Domain und Pfad “blog.example.net/resource/*”

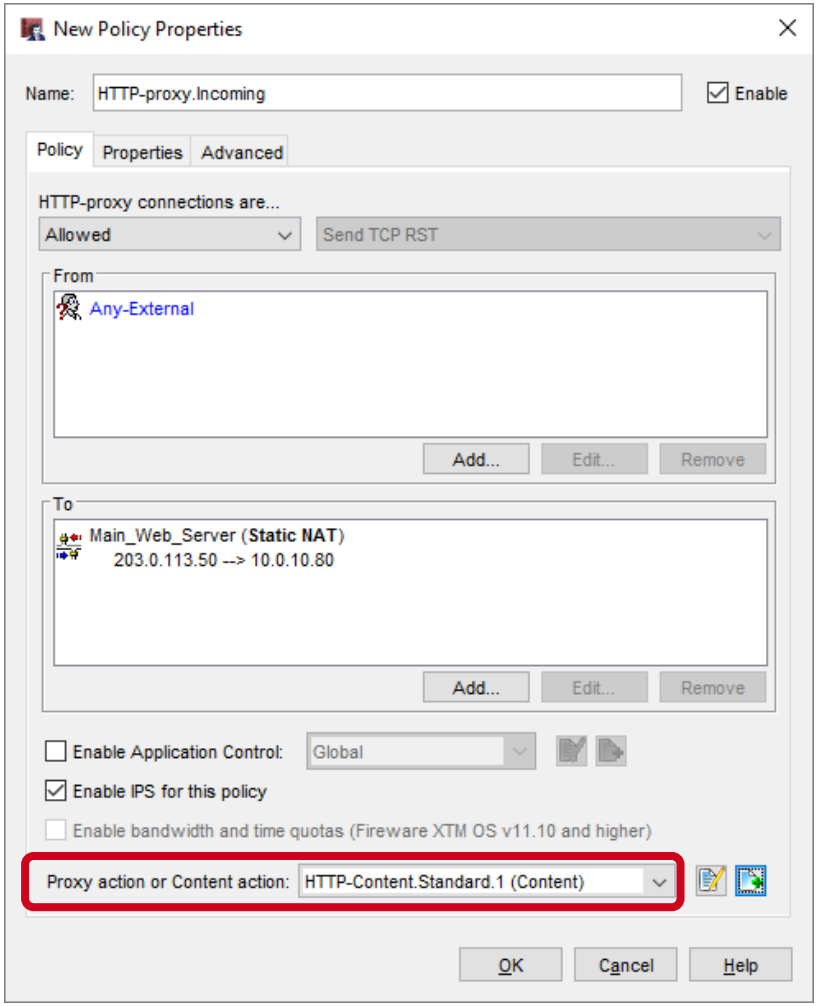
TLS/SSL Offloading

- 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.



Content Action mit dem HTTP Proxy

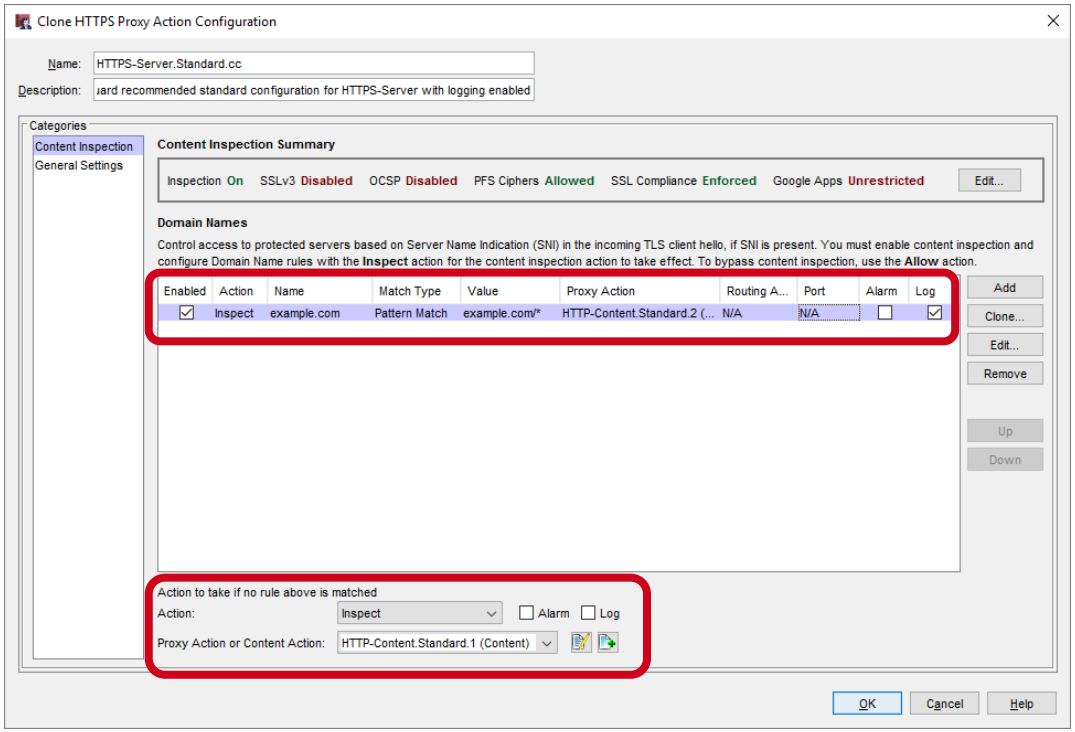
- Im HTTP Proxy Policy, wähle **Content Action**
  - Die Drop-Down Liste umfasst jeweils Proxy Action und Content Action
- In der Policy **To** Liste, füge eine **Static NAT** Regel ein, oder nutzte 1-to-1 NAT
  - Die Policy NAT Einstellungen werden nicht verwendet, außer eine Rounting Action in der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



Content Action mit einem HTTPS Server Proxy

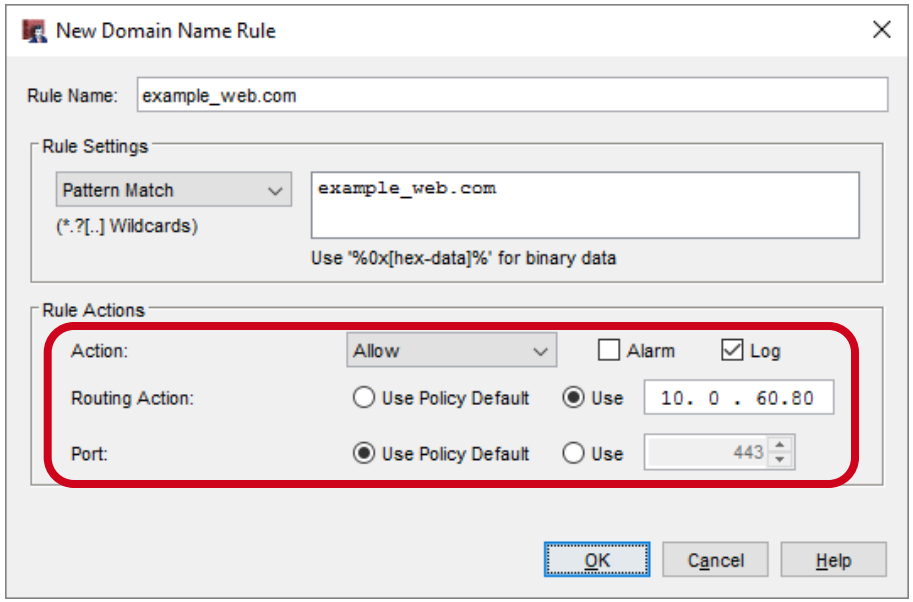
- So verwenden Sie eine Content Action in einer Domain Name Rule oder in der Standard Action, wenn keine Regel übereinstimmt:

1. Wähle die **Inspect** Action
2. Wähle eine Content Action



Routing Action in einem HTTPS Server Proxy

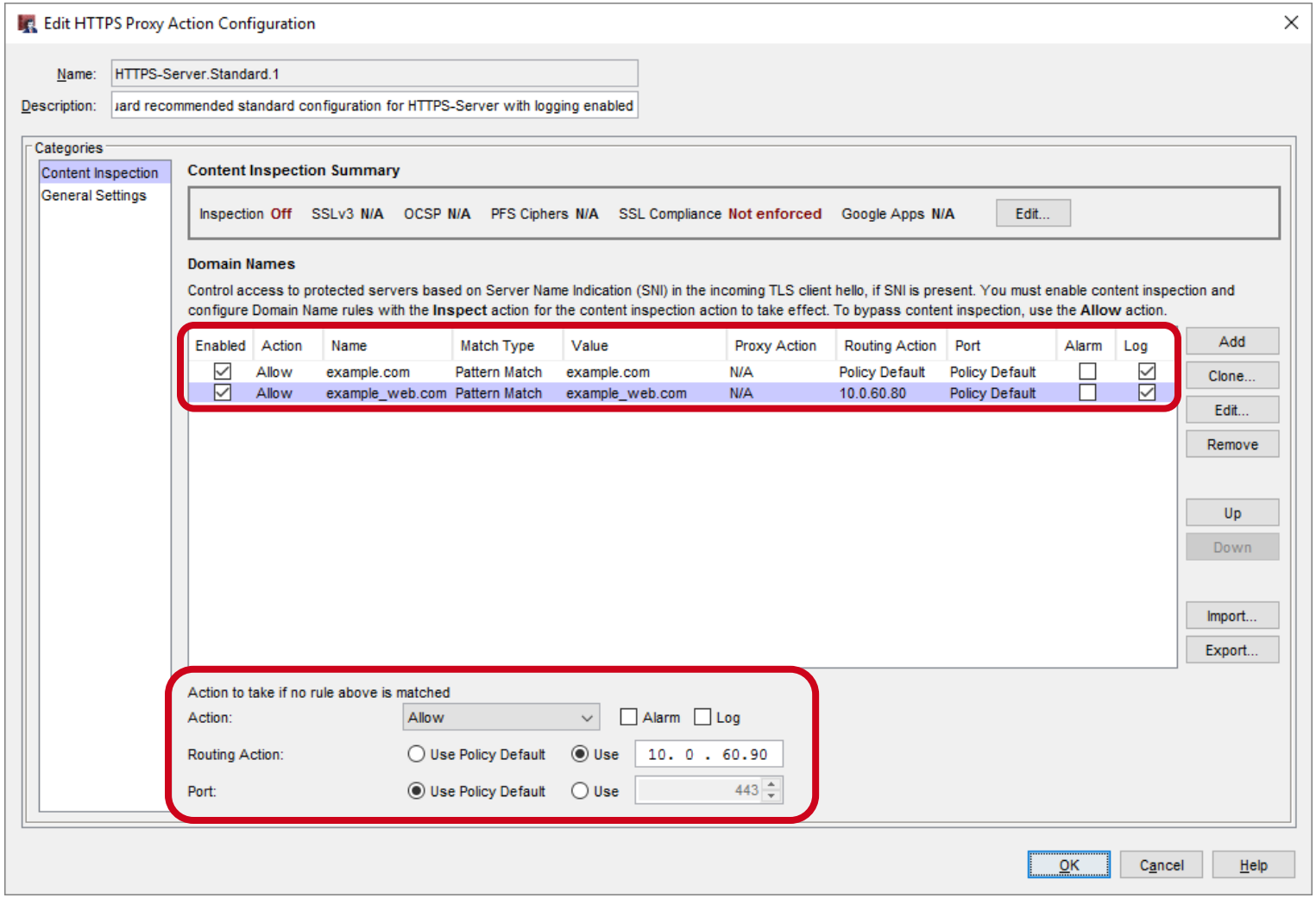
- So routen Sie HTTPs Request ohne Content Inspection in einer Domain Name Rule oder in der Standard Action, wenn keine Regel übereinstimmt :
  1. Wähle die **Allow** Action
  2. Konfiguriere eine Routing Action und den Port



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 Zielservers an
  - SNI ist in RFC 6066 TLS Extensions beschrieben

Routing Action in einem HTTPS Server Proxy

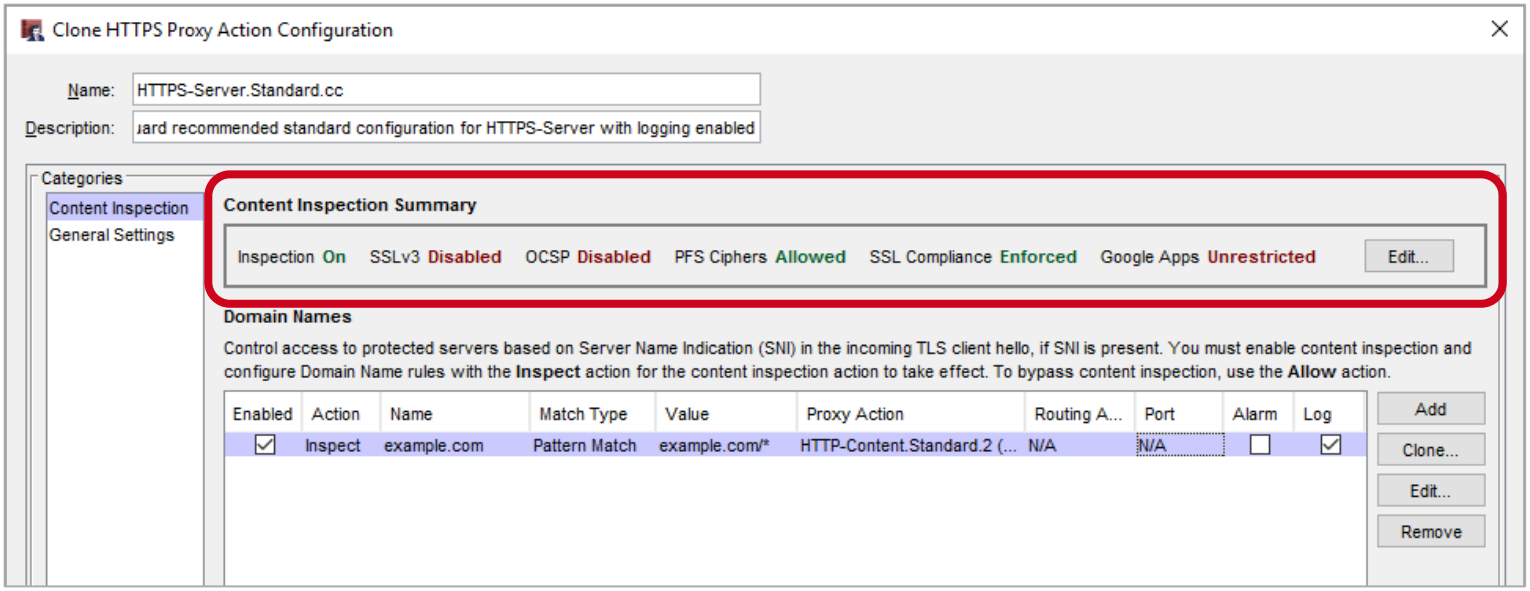


Proxy Action Änderungen

- 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

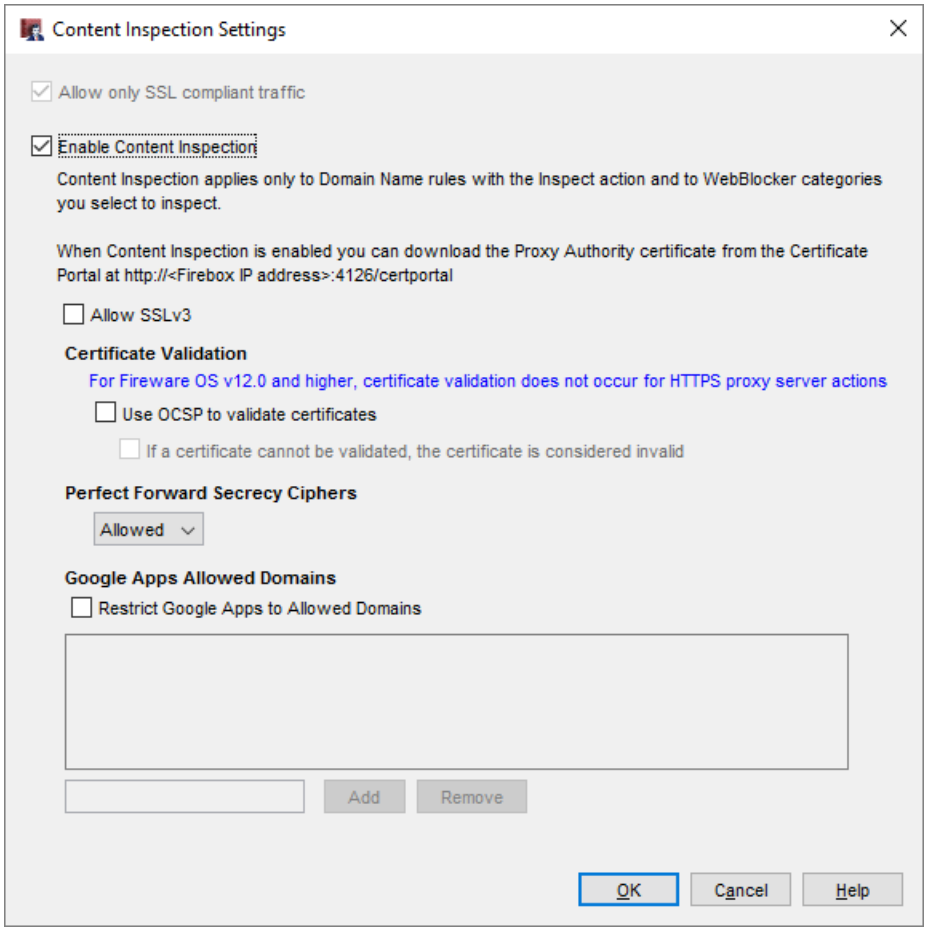
HTTPS Proxy Action Änderungen

- 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.



HTTPS Proxy Action Änderungen

- Die Einstellungen für die Inhaltsprüfung sind dieselben wie in Fireware v11.x, mit der Ausnahme, dass keine HTTP-Client-Proxy Action auswählt 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

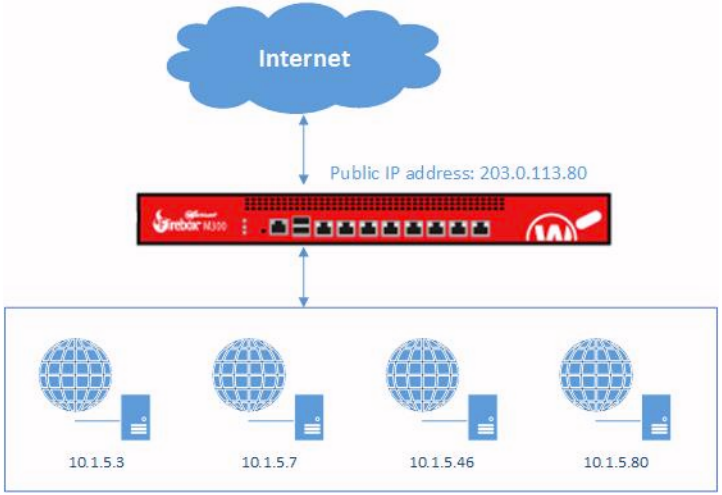


Beispiele

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

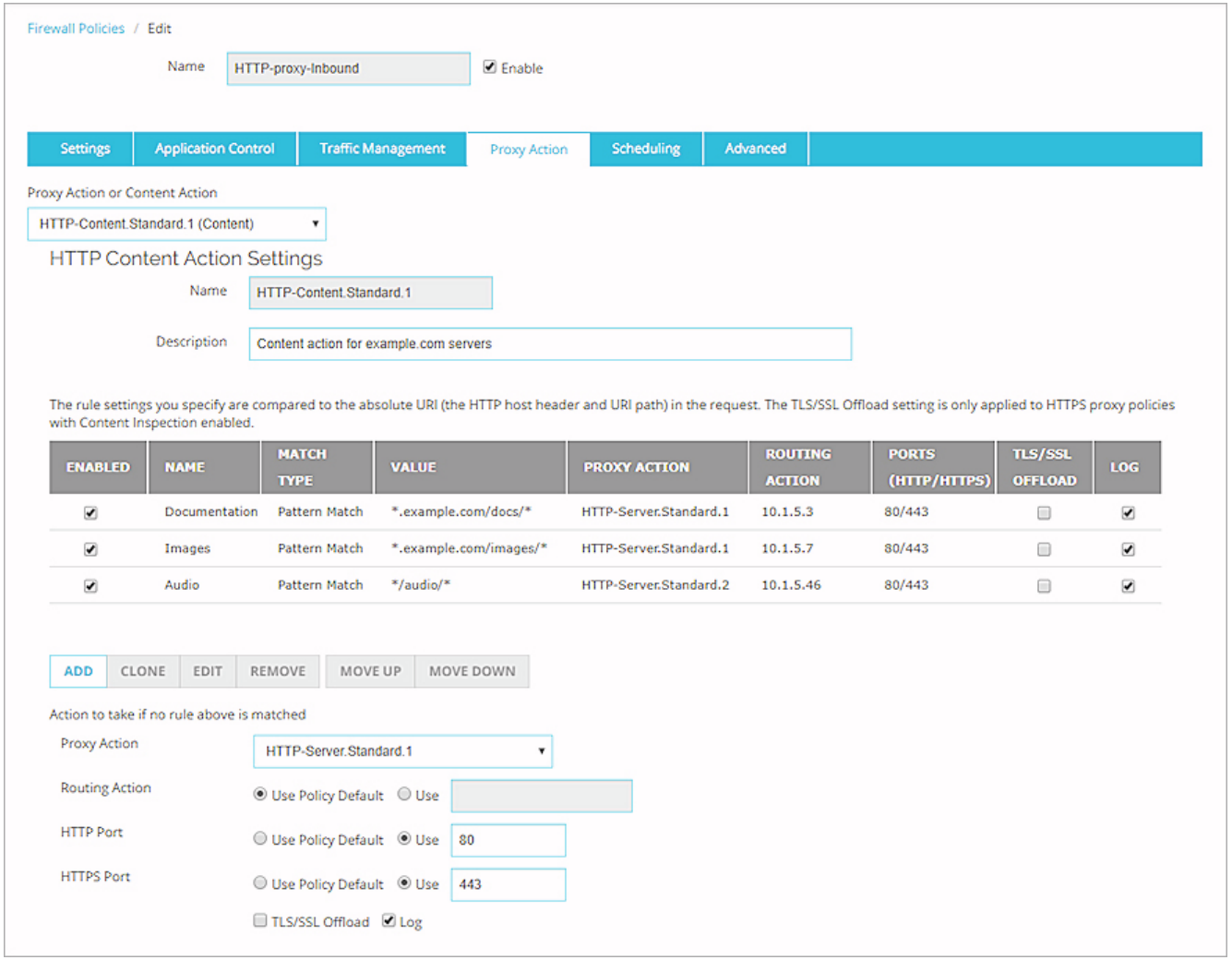


HTTP Proxy mit einer HTTP Content Action

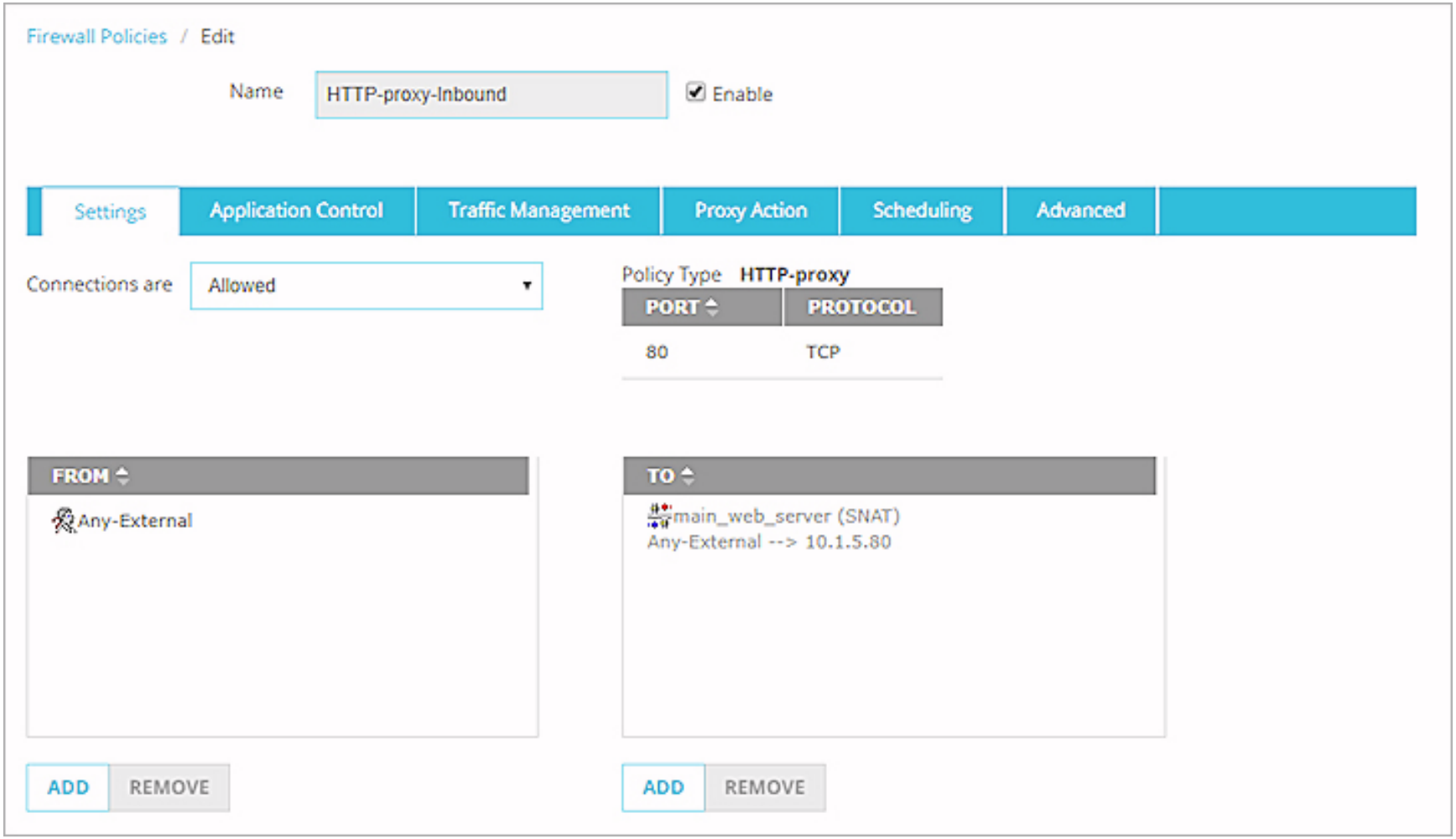
- Die Content Action leitet HTTP-Anforderungen auf drei interne Server um, basierend auf der Domäne im HTTP-Host-Header und dem URI-Pfad in der HTTP-Anforderung.
- Alle anderen HTTP-Anforderungen werden an den Hauptwebserver gesendet, der in einer SNAT-Aktion in der Richtlinie angegeben ist.

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



HTTP Proxy mit einer HTTP Content Action



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

Thank You!

WatchGuard Training