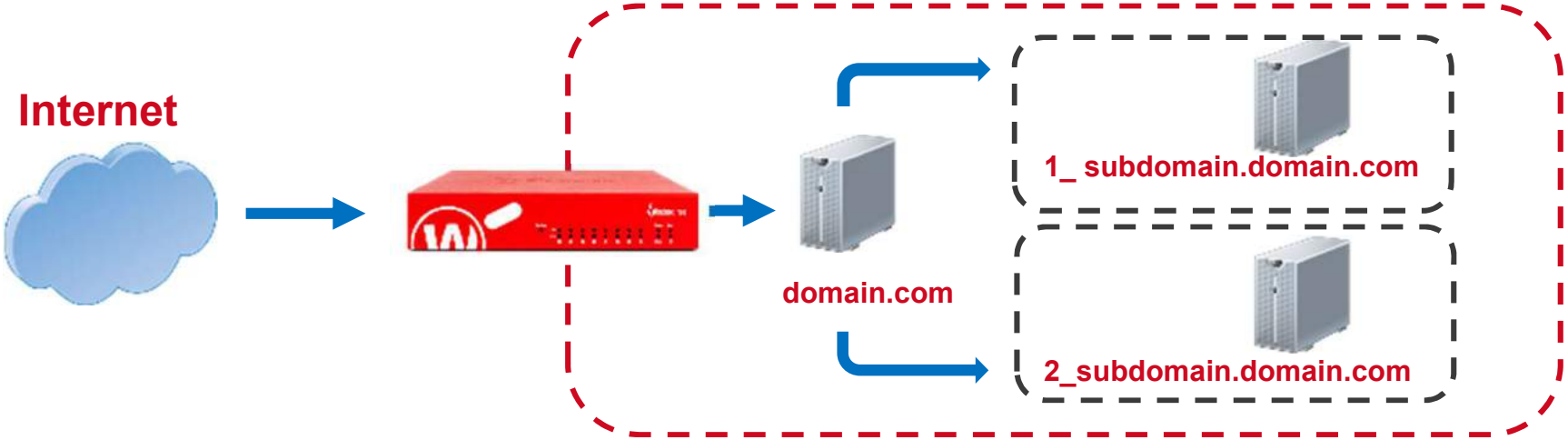
Webinar Best Practices - Firebox - Host Header Redirection ermöglicht eine flexible Veröffentlichung von Webservern auch bei einzelner öffentlicher IP Adresse

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



Content Actions und Routing Actions

- Eine Content Action ist eine Art von Proxy-Aktion für eingehende HTTP-Proxy-Richtlinien und HTTPS Server-Proxy-Action
  - Mithilfe einer Content Action kann die Firebox eingehende HTTP- und HTTPS-Anfragen 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

Content Actions und Routing Actions

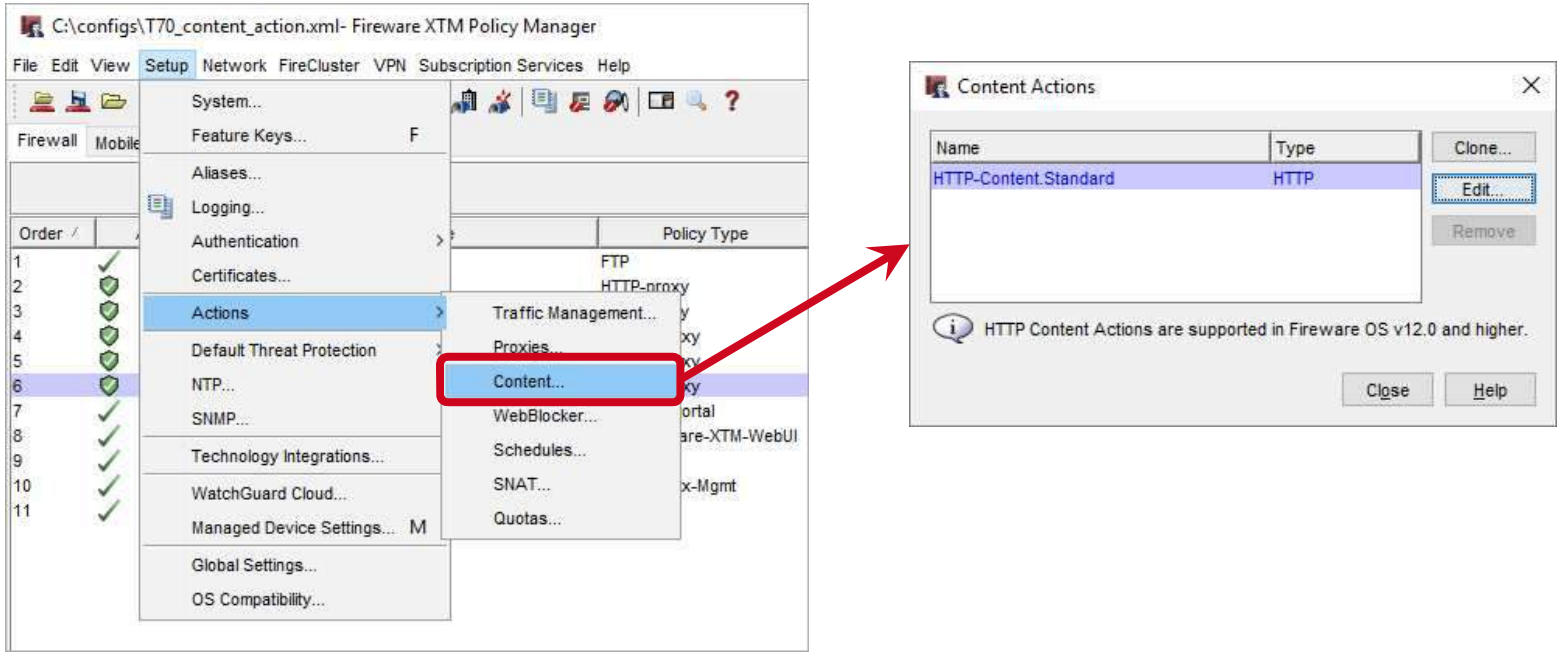
- Content Action haben zwei Hauptfunktionen:
  - Host-Header-Weiterleitung
    - Sendet eingehende HTTP- und geprüfte HTTPS-Anfragen an verschiedene interne Server basierend auf dem Pfad und der Domäne in der HTTP-Anfrage
  - TLS / SSL-Offloading
    - Entlastet einen internen Webserver von der Verarbeitungslast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

Content Actions und Routing Actions

- Content Action
  - Sendet ein HTTP-Request an eine bestimmte IP-Adresse und einen bestimmten Port
  - Content Actions 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

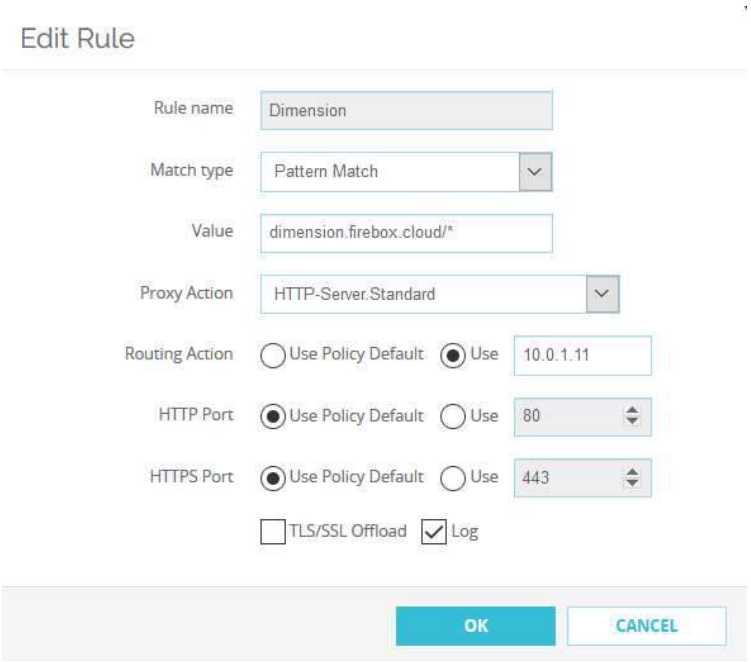
Content Action Konfiguration

- 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 Rules

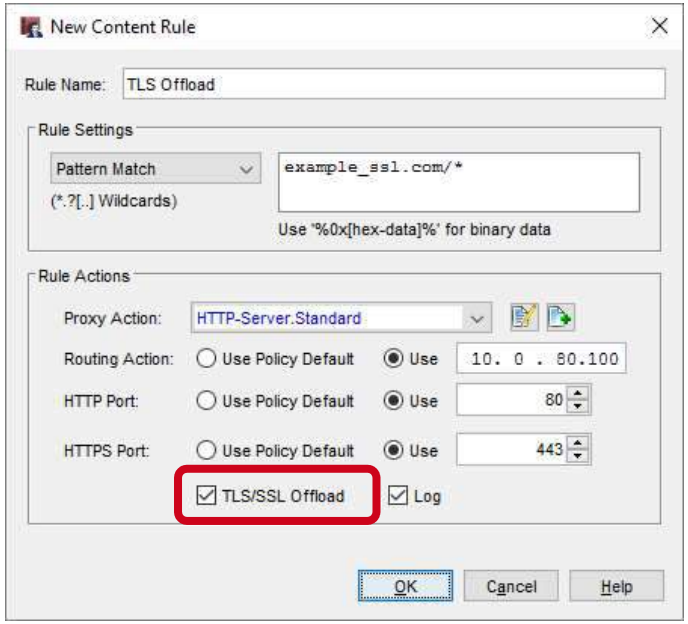
- Jede Content Action legt fest:
  - Ein passendes Pattern
  - HTTP Proxy Action
  - Routing Action (IP Adresse)
  - HTTP und HTTPS Ports
  - TLS/SSL Offload Einstellung
  - Log Einstellung



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

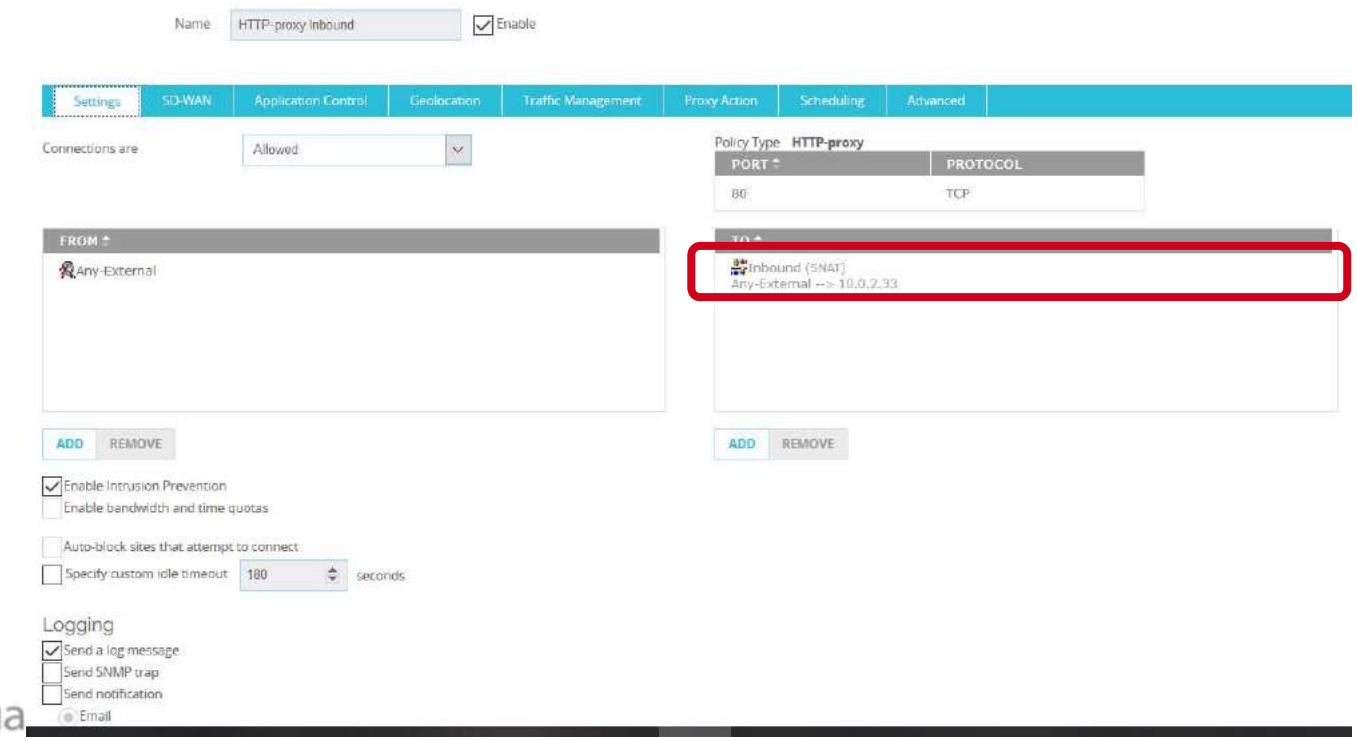
TLS/SSL Offloading

- 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.



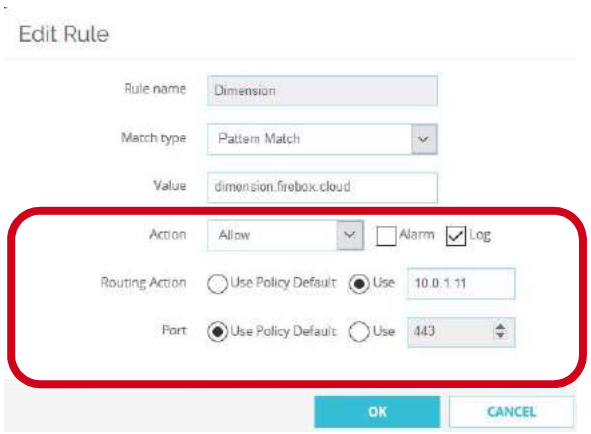
Content Action mit dem HTTP(S) Proxy

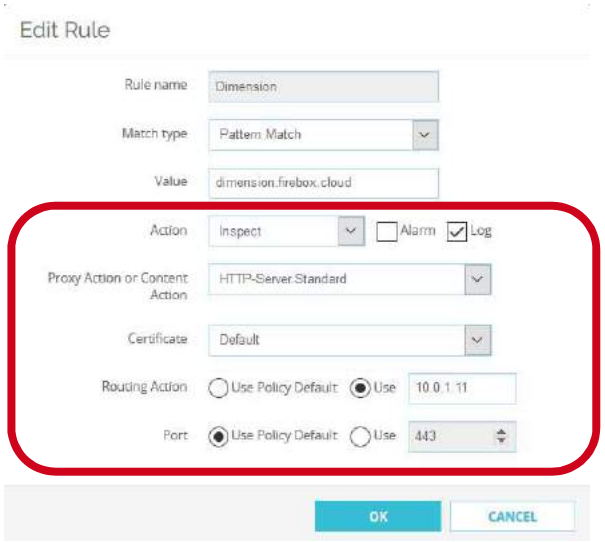
- Im HTTP Proxy Policy, wähle **Content Action**
  - Die Drop-Down Liste umfasst jeweils Proxy Action und Content Action
- In der Policy **To** Liste, füge eine **Static NAT** Regel ein, oder nutzte 1-to-1 NAT
  - Die Policy NAT Einstellungen werden nicht verwendet, außer eine Rounting Action in der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



Routing Action in einem HTTPS Server Proxy

- So routen Sie HTTPs Request ohne Content Inspection in einer Domain Name Rule :
  1. Wähle die **Allow** Action
  2. Konfiguriere eine Routing Action und den Port





Routing Action in einem HTTPS Server Proxy

Name: HTTPS-proxy Inbound ☑ Enable

Settings | SD-WAN | Application Control | Geolocation | Traffic Management | Proxy Action | Scheduling | Advanced

Proxy Action: HTTPS-Server.Standard.Inbound

Warning: Automatic updates are **disabled** for trusted CA certificates. Enable updates now.

HTTPS Proxy Action Settings

Name: HTTPS-Server.Standard.Inbound

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

Content Inspection | Proxy Alarm | General

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

TLS Profile: TLS-Server-HTTPS.Standard | EDIT | CLONE

Minimum Protocol Version **TLS v1.0** PFS Ciphers **Allowed** TLS Compliance **Not enforced**

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

Control access to protected servers based on Server Name Indication (SNI) in the incoming TLS client hello, if SNI is present. To enable content inspection, use the **Inspect** action. To bypass content inspection, use the **Allow** action.

ENABLED	ACTION	NAME	MATCH TYPE	VALUE	PROXY ACTION	CERTIFICATE	ROUTING ACTION	PORT	ALARM	LOG
☐	Inspect	Dimension	Pattern Match	dimension.firebox.cloud	HTTP-Server.Standard	Default	10.0.1.11	Policy Default	☐	☑
☐	Inspect	WordPress	Pattern Match	wordpress.firebox.cloud	HTTP-Server.Standard	Default	10.0.1.6	Policy Default	☐	☑
☐	Inspect	RDWeb	Pattern Match	rdweb.firebox.cloud	HTTP-Server.Standard	Default	10.0.1.5	Policy Default	☐	☑

ADD | CLONE | EDIT | REMOVE | MOVE UP | MOVE DOWN

Action to take if no rule above is matched

Action: Inspect ☐ Alarm ☑ Log

Proxy Action or Content Action: HTTP-Content.Standard.Inbound (Content)

Certificate: Default

SAVE | CANCEL

Routing Action in einem HTTPS Server Proxy

Edit HTTPS Proxy Action Configuration

Name: HTTPS-Server.Standard.1

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

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** 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 Action	Port	Alarm	Log
☑	Allow	example.com	Pattern Match	example.com	N/A	Policy Default	Policy Default	☐	☑
☑	Allow	example_web.com	Pattern Match	example_web.com	N/A	10.0.60.80	Policy Default	☐	☑

Add | Clone... | Edit... | Remove | Up | Down | Import... | Export...

Action to take if no rule above is matched

Action: Allow ☐ Alarm ☐ Log

Routing Action: ○ Use Policy Default ◉ Use 10. 0 . 60.90

Port: ◉ Use Policy Default ○ Use 443

OK | Cancel | Help

Beispiele

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

  HTTP Content Action and Domain Name Rule Examples

  https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/proxies/examples/content_action_examples_c.html?Highlight=Name%20Rule%20Examples

Live