



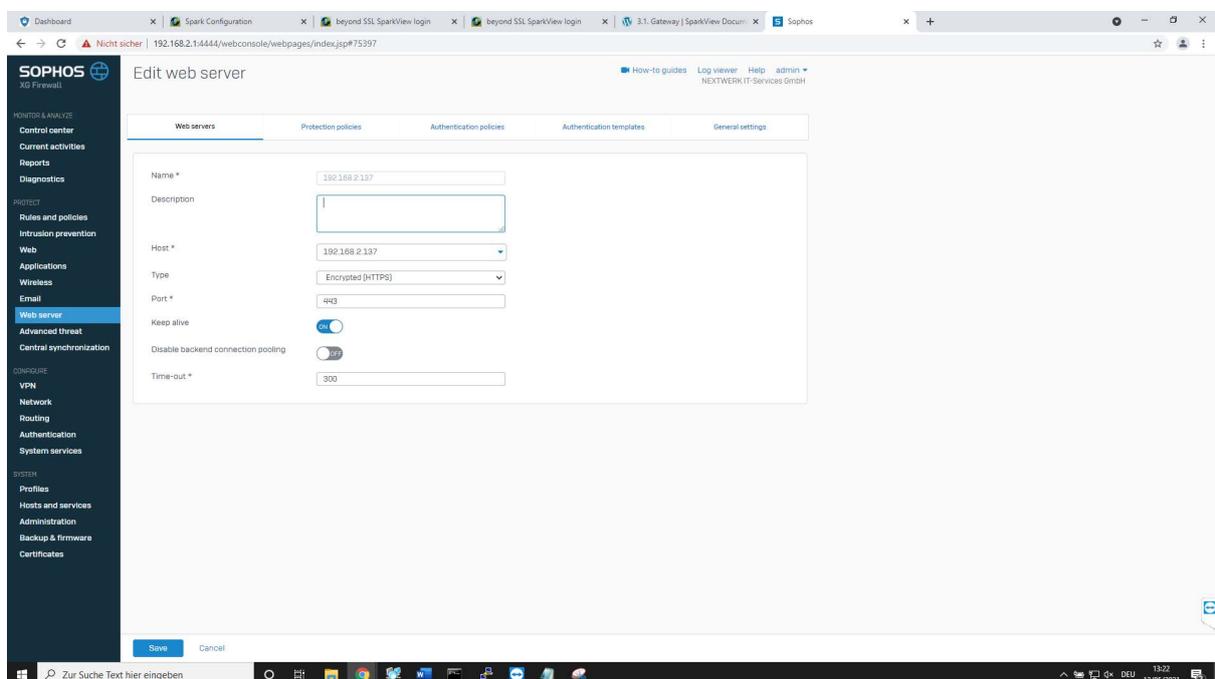
SparkView Integration  
mit  
Sophos XG Firewall

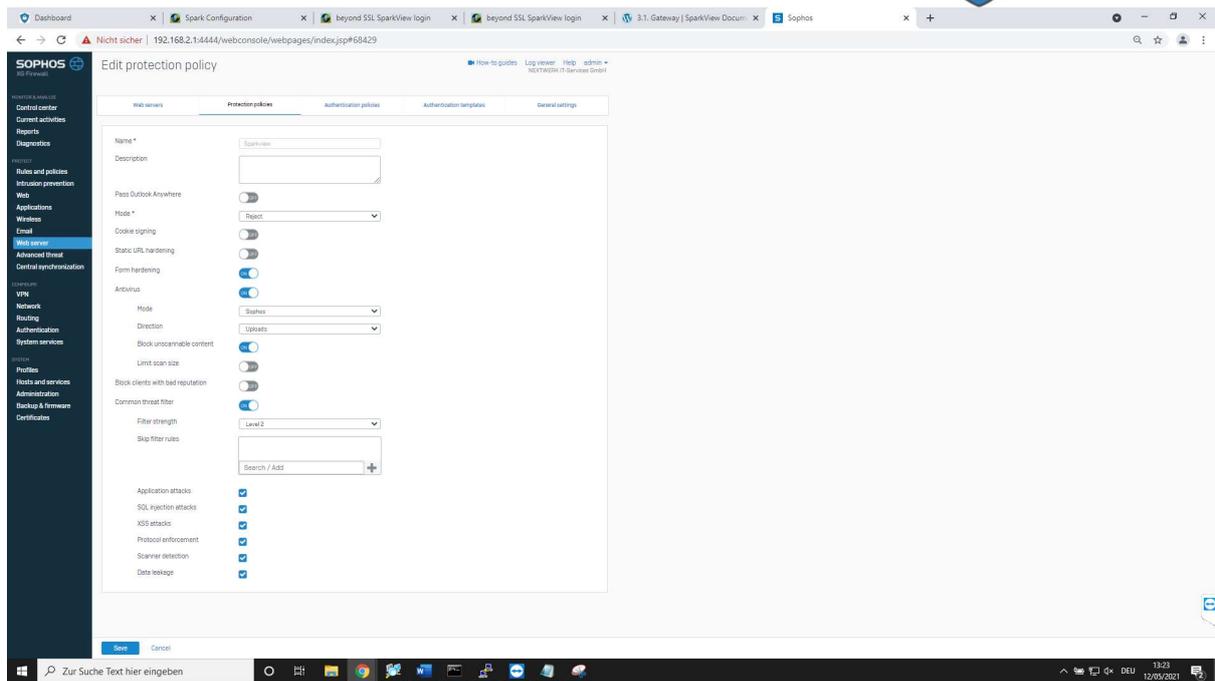
Diese Anleitung beschreibt die Beispielkonfiguration für eine Sophos XG Firewall im Zusammenspiel mit SparkView.

Ziel ist es, dass sich der Benutzer, bevor er die SparkView Anwendung von außerhalb des Firmennetzes erreichen kann, an der Sophos XG Firewall authentifiziert und er nach erfolgreicher Authentifizierung weitergeleitet wird.

Die Bezeichnung „Sophos XG Firewall“ ist Eigentum der Firma Sophos.

## Konfiguration Webserver

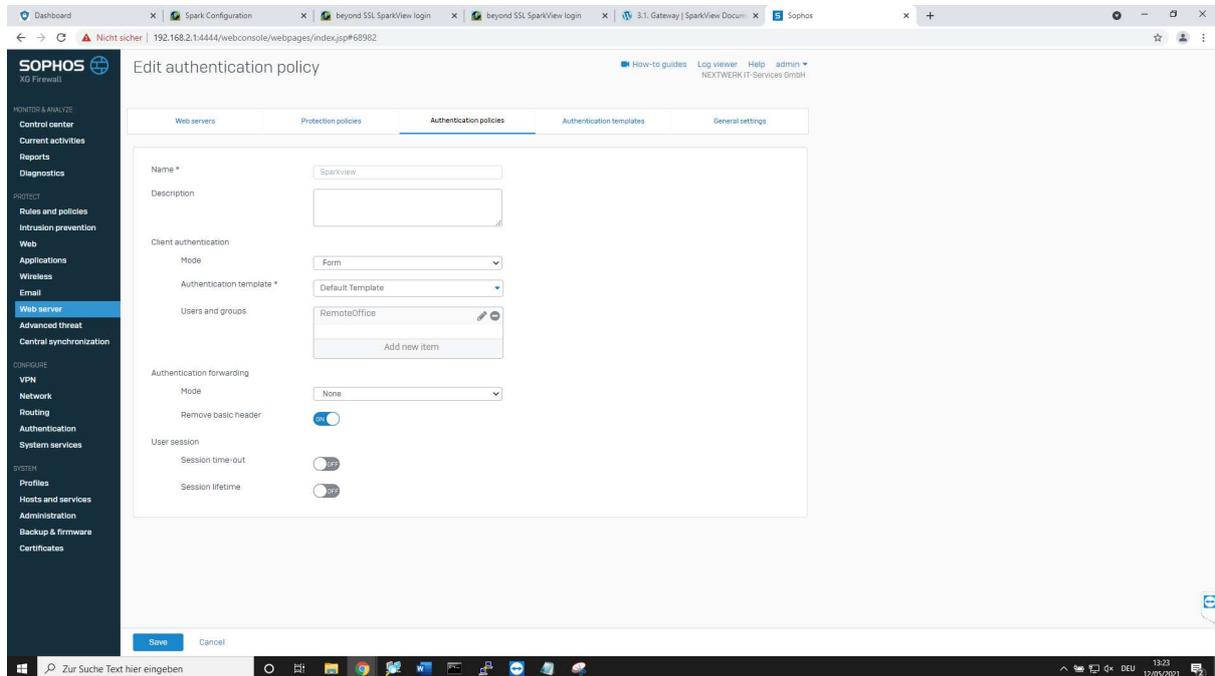
A screenshot of the Sophos XG Firewall web management interface. The browser address bar shows the URL '192.168.2.1:4444/webconsole/webpages/index.jsp#75397'. The page title is 'Edit web server'. The left sidebar contains a navigation menu with categories: MONITOR & ANALYZE (Control center, Current activities, Reports, Diagnostics), PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced threat, Central synchronization), CONFIGURE (VPN, Network, Routing, Authentication, System services), and SYSTEM (Profiles, Hosts and services, Administration, Backup & firmware, Certificates). The 'Web server' option is selected. The main content area shows configuration fields: Name (192.168.2.137), Description (empty), Host (192.168.2.137), Type (Encrypted (HTTPS)), Port (443), Keep alive (checked), Disable backend connection pooling (unchecked), and Time-out (300). At the bottom, there are 'Save' and 'Cancel' buttons. The Windows taskbar at the bottom shows the search bar and system tray with the date 12/05/2021 and time 13:22.



The screenshot shows the 'Edit protection policy' interface in the Sophos Web Security console. The policy name is 'Sparkview'. The configuration includes various security features:

- Pass Outlook-Anywhere:** Disabled
- Mode:** Protect
- Cookie signing:** Disabled
- Static URL hardening:** Disabled
- Form hardening:** Enabled
- Antivirus:** Enabled
- Mode:** Sophos
- Direction:** Updates
- Block unscannable content:** Enabled
- Limit scan size:** Disabled
- Block clients with bad reputation:** Disabled
- Common threat filter:** Enabled
- Filter strength:** Level 2
- Skip filter rules:** Search / Add
- Application attacks:** Enabled (includes SQL injection attacks, XSS attacks, Protocol enforcement, Scanner detection, Data leakage)

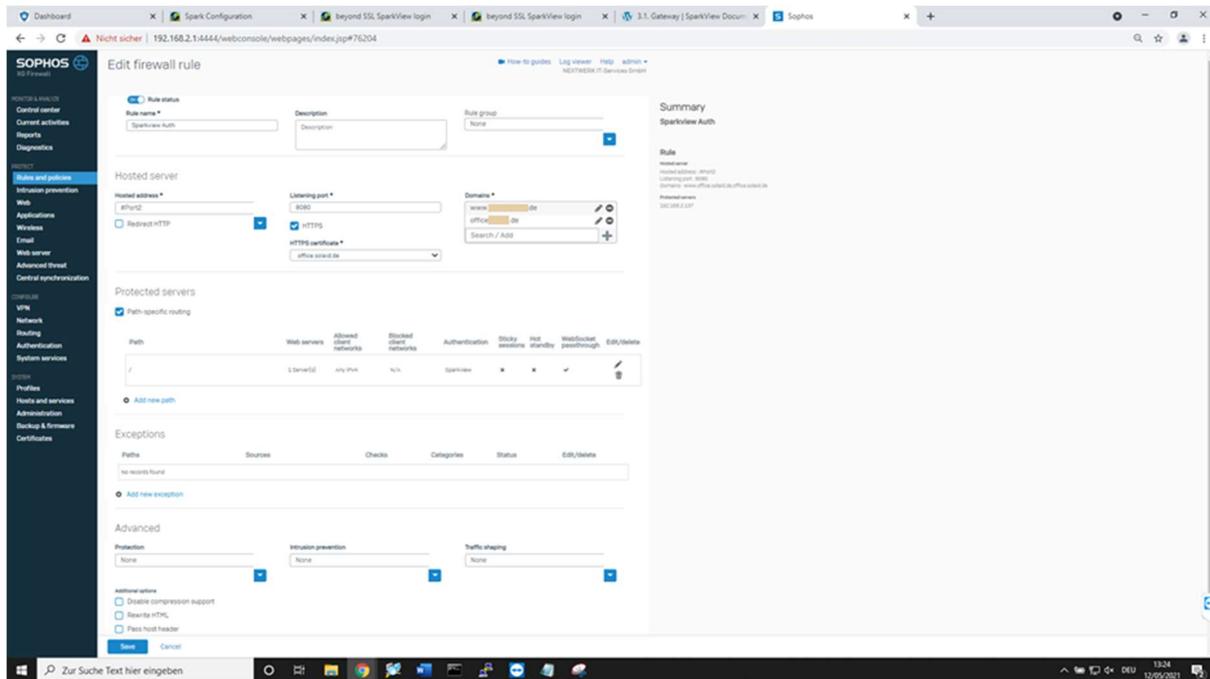
## Konfiguration Authentication Policy



The screenshot shows the 'Edit authentication policy' interface in the Sophos Web Security console. The policy name is 'Sparkview'. The configuration includes:

- Client authentication Mode:** Form
- Authentication template:** Default Template
- Users and groups:** RemoteOffice
- Authentication forwarding Mode:** None
- Remove basic header:** Enabled
- User session:**
  - Session time-out:** Disabled
  - Session lifetime:** Disabled

# Konfiguration Firewall Rule



**Dashboard** | Spark Configuration | beyond SSL, SparkView login | beyond SSL, SparkView login | 3.1. Gateway | SparkView Docum... | Sophos

**SOPHOS** Edit firewall rule

How-to guides Log viewer Help admin

NextAdmin IT Services GmbH

**Summary**  
SparkView Auth

**Rule**  
Name: SparkView Auth  
Listening port: 8080  
Domain: office.192.168.2.137.de  
Protected servers: 192.168.2.137

**Hosted server**

Hosted address: http://192.168.2.1:8080  
Listening port: 8080  
Domains: office.192.168.2.137.de

**Protected servers**

Path	Web servers	Allowed client networks	Blocked client networks	Authentication	Sticky sessions	Hot standby	WebSocket passthrough	Edit/Delete
/	1 server(s)	Any IPv4	N/A	SparkView	x	x	✓	

**Exceptions**

Paths: No records found

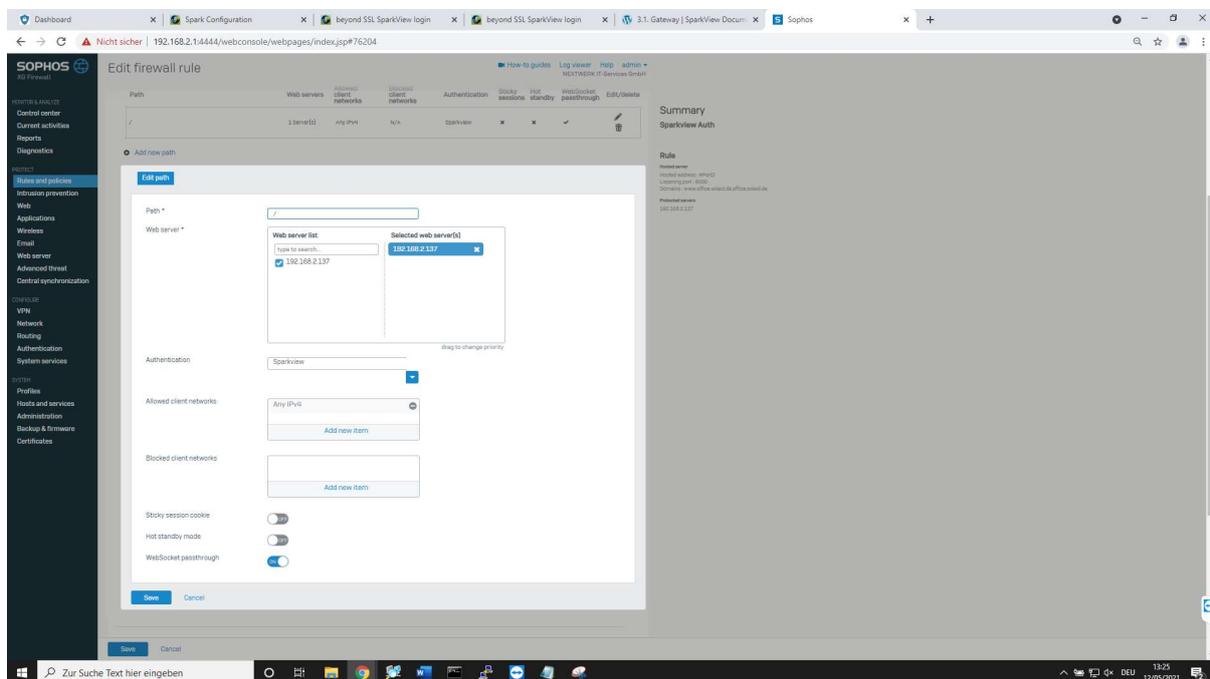
**Advanced**

Protection: None  
Intrusion prevention: None  
Traffic shaping: None

**Additional options**

Disable compression support:   
Rewrite HTML:   
Preserve host header:

Save Cancel



**Dashboard** | Spark Configuration | beyond SSL, SparkView login | beyond SSL, SparkView login | 3.1. Gateway | SparkView Docum... | Sophos

**SOPHOS** Edit firewall rule

How-to guides Log viewer Help admin

NextAdmin IT Services GmbH

**Summary**  
SparkView Auth

**Rule**  
Name: SparkView Auth  
Listening port: 8080  
Domain: office.192.168.2.137.de  
Protected servers: 192.168.2.137

**Path**

Path: /

**Web server list**

Web server: 192.168.2.137

**Authentication**

Authentication: SparkView

**Allowed client networks**

Allowed client networks: Any IPv4

**Blocked client networks**

Blocked client networks: (empty)

**Sticky session cookie**

Sticky session cookie:

**Hot standby mode**

Hot standby mode:

**WebSocket passthrough**

WebSocket passthrough:

Save Cancel