



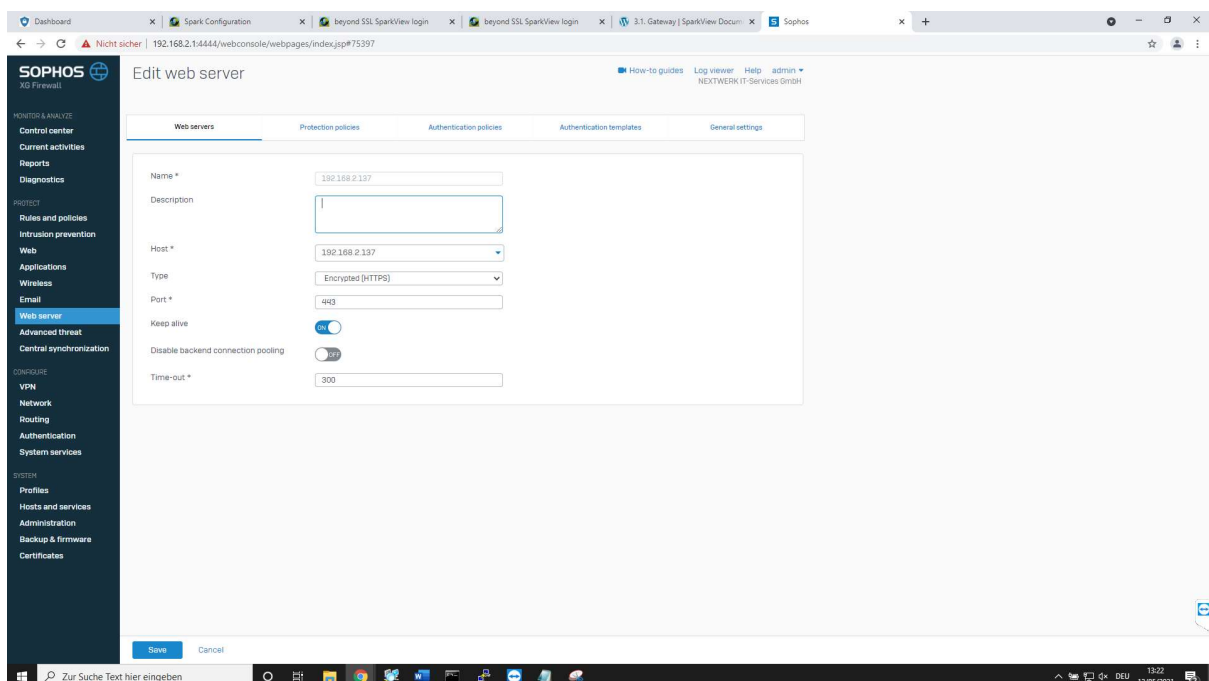
SparkView Integration
mit
Sophos XG Firewall

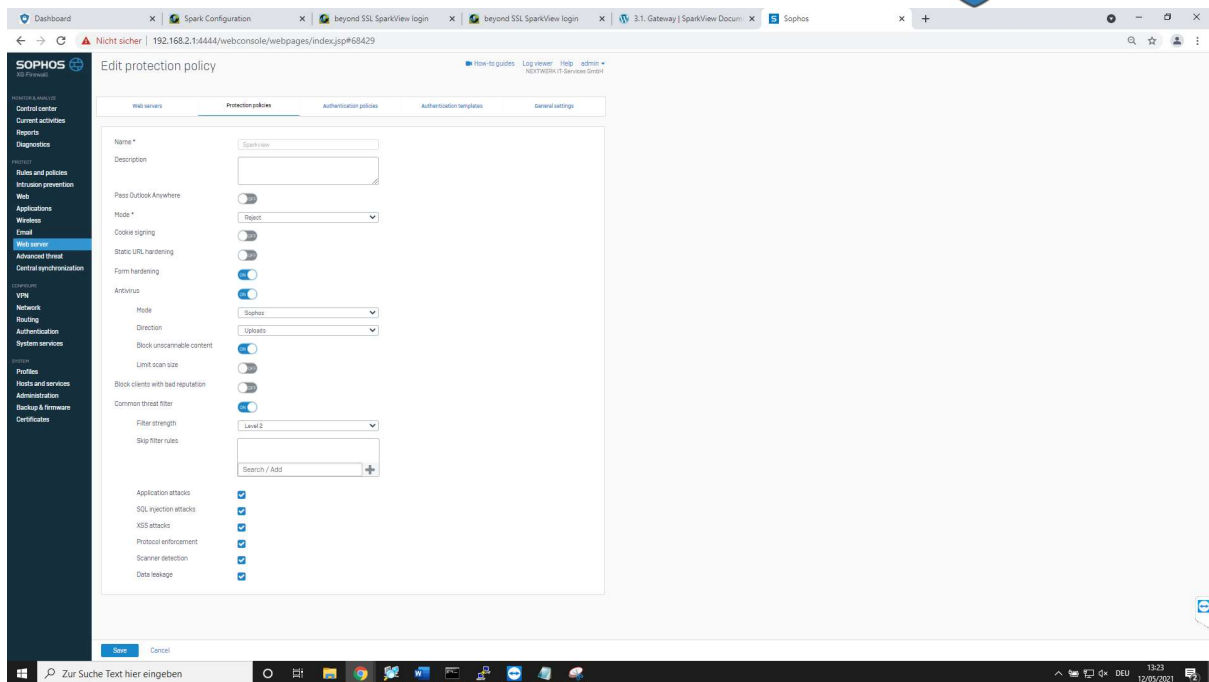
Diese Anleitung beschreibt die Beispielkonfiguration für eine Sophos XG Firewall im Zusammenspiel mit SparkView.

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

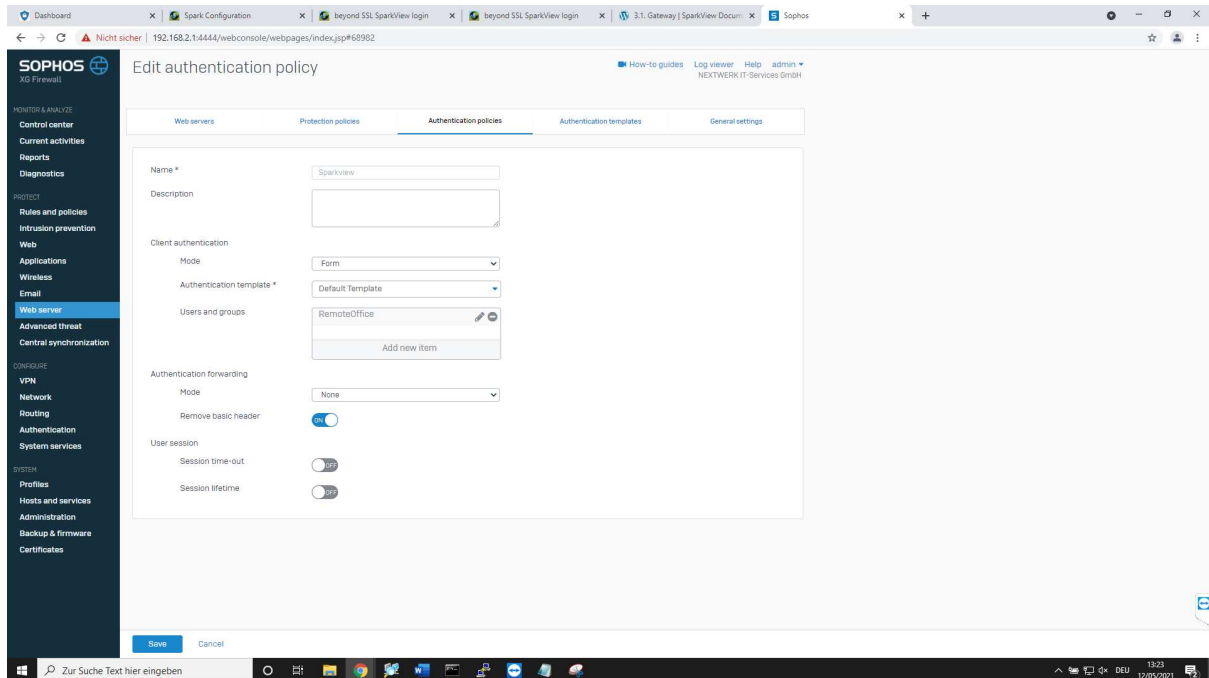
The screenshot shows the Sophos XG Firewall web management interface. The browser address bar shows the URL 192.168.2.1:4444/webconsole/webpages/index.jsp#75397. The page title is "Edit web server". The left sidebar contains navigation menus for "MONITOR & ANALYZE", "PROTECT", "CONFIGURE", and "SYSTEM". The main content area has tabs for "Web servers", "Protection policies", "Authentication policies", "Authentication templates", and "General settings". The "Web servers" tab is active, showing a form with the following 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 of the form are "Save" and "Cancel" buttons. The Windows taskbar at the bottom shows the search bar and system tray with the time 13:22 on 12/05/2021.



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

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

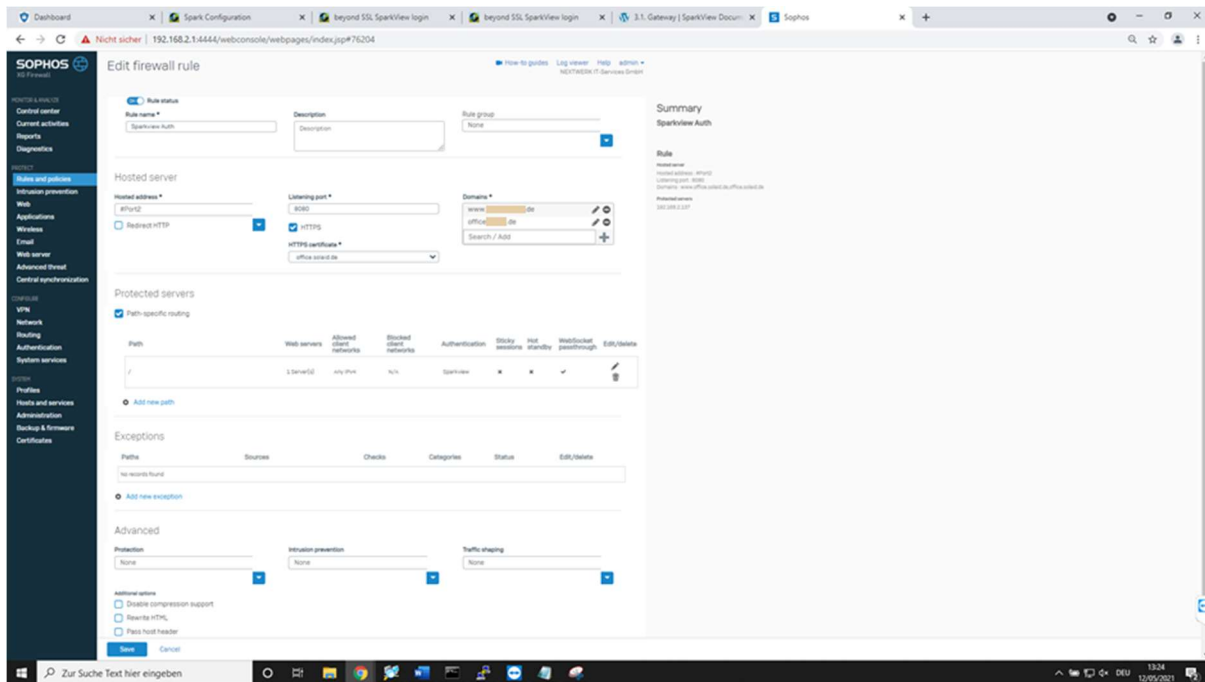
Konfiguration Authentication Policy



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

- Client authentication:**
 - Mode: Form
 - Authentication template: Default Template
 - Users and groups: RemoteOffice
 - Add new item:
- Authentication forwarding:**
 - Mode: None
 - Remove basic header:
- User session:**
 - Session time-out: 300
 - Session lifetime: 300

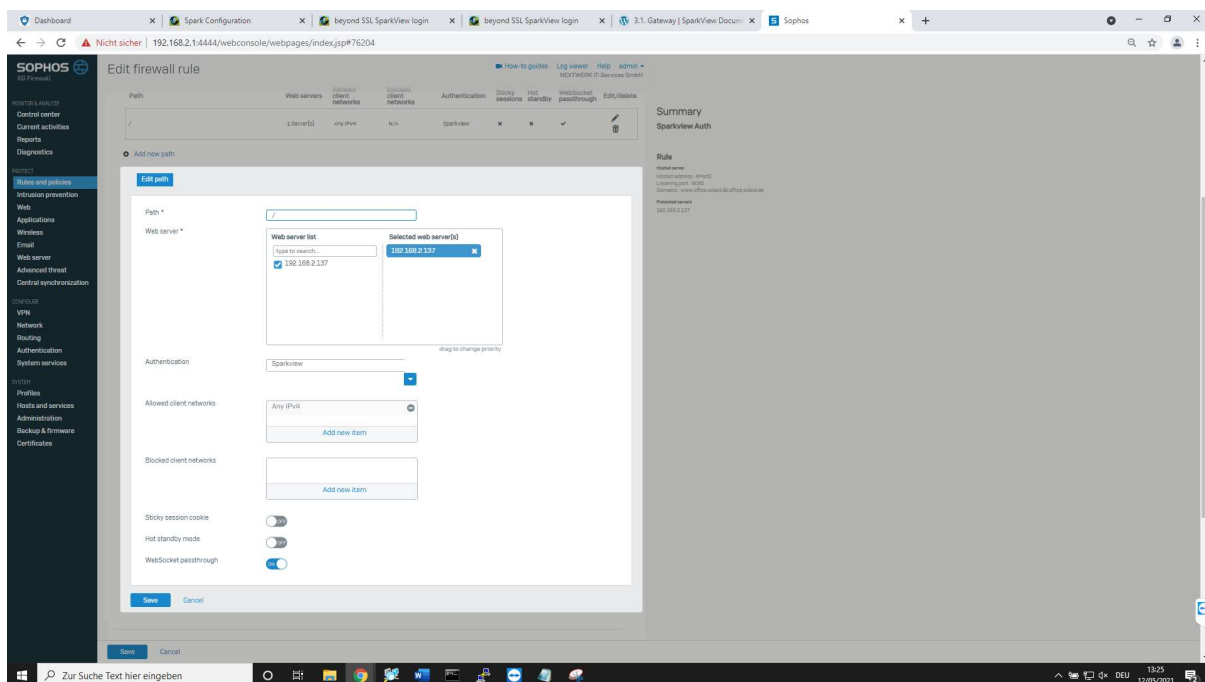
Konfiguration Firewall Rule



The screenshot shows the 'Edit firewall rule' configuration page in the Sophos Firewall web interface. The rule is named 'SparkView Auth' and is part of the 'None' rule group. The configuration includes:

- Hosted server:** Hosted address is 'http://192.168.2.1:8080', listening port is '8080', and domain is 'office.192.168.2.1.de'. The 'Advanced' section has 'Protection' set to 'None', 'Intrusion prevention' set to 'None', and 'Traffic shaping' set to 'None'.
- Protected servers:** A table with one entry:

Path	Web servers	Allowed client networks	Blocked client networks	Authentication	Sticky sessions	Hot standby	WebSocket passthrough	Edit/Delete
/	1 server(s)	Any IPv4	None	SparkView	Yes	Yes	Yes	
- Exceptions:** No exceptions are found.
- Additional options:** 'Disable compression support', 'Rewrite HTML', and 'Pass host header' are all disabled.



This screenshot shows the 'Edit path' dialog box within the 'Edit firewall rule' configuration. The dialog is used to manage the 'Web server list' for the path '/'. It shows:

- Web server list:** A search box with '192.168.2.137' entered. A list of servers is shown, with '192.168.2.137' selected.
- Authentication:** Set to 'SparkView'.
- Allowed client networks:** Set to 'Any IPv4'.
- Blocked client networks:** Empty.
- Sticky session cookie:** Enabled.
- Hot standby mode:** Disabled.
- WebSocket passthrough:** Enabled.