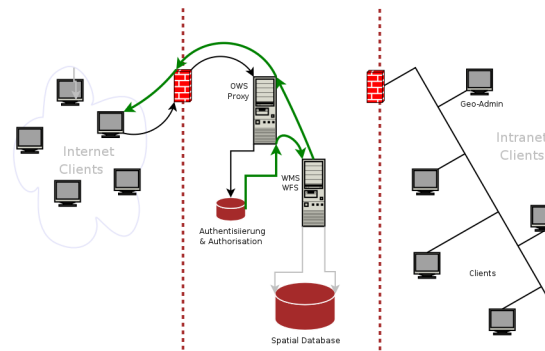


Introduction to the Mapbender OWS Security Proxy



Agenda

1 Introduction to the Architecture

- OWS from Bottom Up with the OSGeo SDI Software Stack
- Mapbender Application Framework, User Management and Orchestration

2 Proxy Technology as OWS Service Facade

- Basic Security IT: Authentication, Authorization, Encryption
- Basic Web IT: Proxy, Sessions and Caching Technology

3 Mapbender Implementation

- Authentication and Session Management
- Apache URL Rewrite Ticketing
- Web Based User Authorization with OWS Service Containers

3 Individual Development

- Personalized Object-based WFS-T Access
- Planned OGC Standards adoption

3333	12	Fawley	England	UK	United Kingdom	Other	7	Less than 50,000	SRID=4324, POINT(1.3332999946869 50.0166899816865)
333		Suchboatar	Selenge	MG	Mongolia	Provincial capital	7	Less than 50,000	SRID=4324, POINT(106.199996948242 50.25)
333		Ust-Kamenogor	East Kazakhstan	KZ	Kazakhstan	Provincial capital	4	250,000 to 500	SRID=4324, POINT(82.9999984741211 50)
333		Darhan	Darhan	MG	Mongolia	Provincial capital	6	50,000 to 100,0	SRID=4324, POINT(106.176330666406 49.9024620066152)
333		Cherbourg	Basse-Normandie	FR	France	Other	7	Less than 50,000	SRID=4324, POINT(1.633299994678437 49.6500015269789)
3333	17	Krasnoyarsk	Khakassia	RU	Russia	Other	5	100,000 to 250,000	SRID=4324, POINT(92.05 49.7000000000000)

Introduction to the Architecture

OSGeo SDI Software Stack:

- FreeBSD Operating System
- Apache http Web Server
- UMN MapServer OGC WMS, WFS
- GeoServer Transactional OGC WFS
- PostgreSQL object relational SQL database
- PostGIS spatial database extension SFS, WKT
- Mapbender Portal OGC OWS Management

Standards:

- Open Geospatial Consortium and ISO TC 211
- ISO meta data standards



Introduction to the Architecture

Implemented OGC Standards:

- WMS access for spatial objects in database via SFS (access restricted to dedicated and known host from same domain)
- Standard WMS 1.1.1 for map production in three security categories
 - unprotected access from everywhere
 - protected services for authorized access only (all data)
 - protected services for personalized access (selected data)
- WFS for query and search interfaces (read only, unprotected)
- WFS-T for edit access (read/write, protected, personalized)
- Web Context Document to start client with personalized area of interest, service and layer selection (protected)

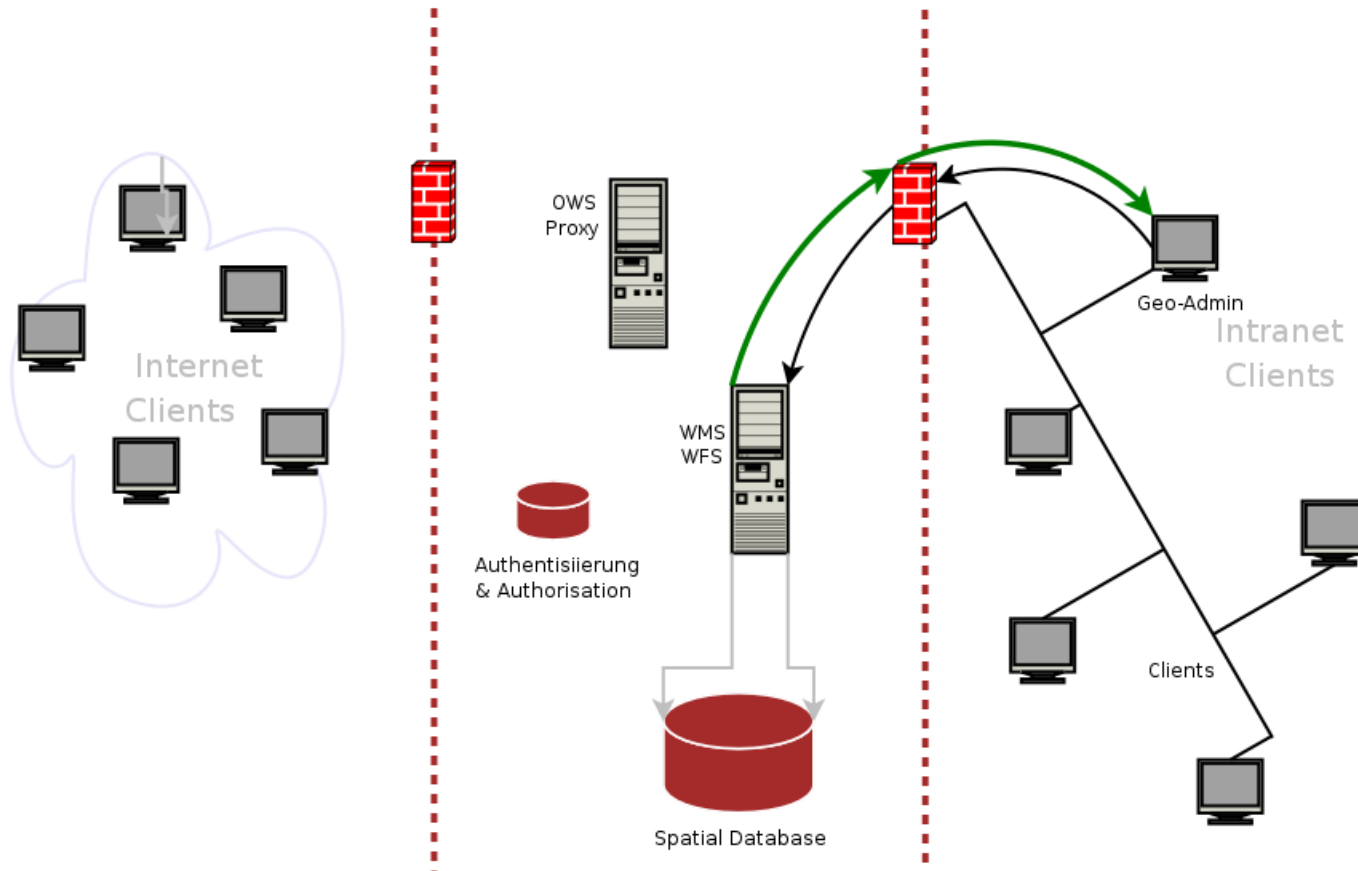
Introduction to the Architecture

Mapbender:

- Application to build user interface and provide functionality
 - View and Navigate: zoom, pan, search, find, activate, deactivate layers, etc.
 - Services: add, reorder, remove, overlay, metadata (CS-W 2.0 services)
 - Digitize: create, edit, delete, snap, break, unify, query, etc.
- User Management
 - Create users, allow access to services via user interface and/or group
- Service Orchestration
 - Upload, remove, edit, monitor WMS and WFS
 - Bind WMS and WFS into user interface, allow functionality **on** services

Proxy Technology as OWS Service Facade

Unprotected Open Access from Authorized Domain



Proxy Technology as OWS Service Facade

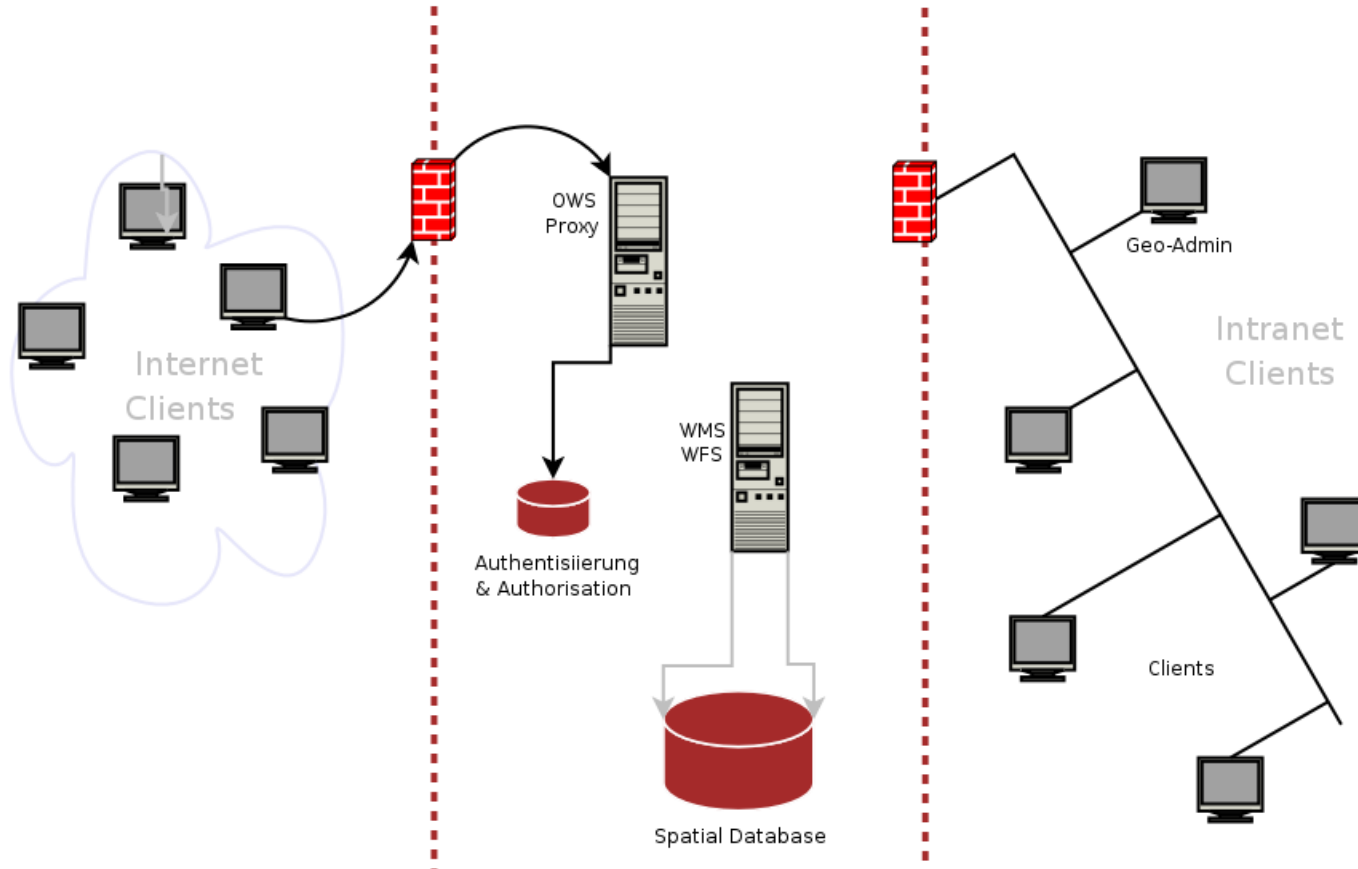
The OpenGIS architecture needs to be protected and secured by an additional layer of security. Use standard IT solutions for standard requirements.

Requirements:

- Only authenticated users are allowed to access the system
- Users can only see and edit their own (authorized) objects
- Data transport is encrypted on a lower level (SSL, TLS)
- Sessions have to expire after a timeout limit is reached
- Everything needs to be logged
- Integrity of the data and services have to be ensured

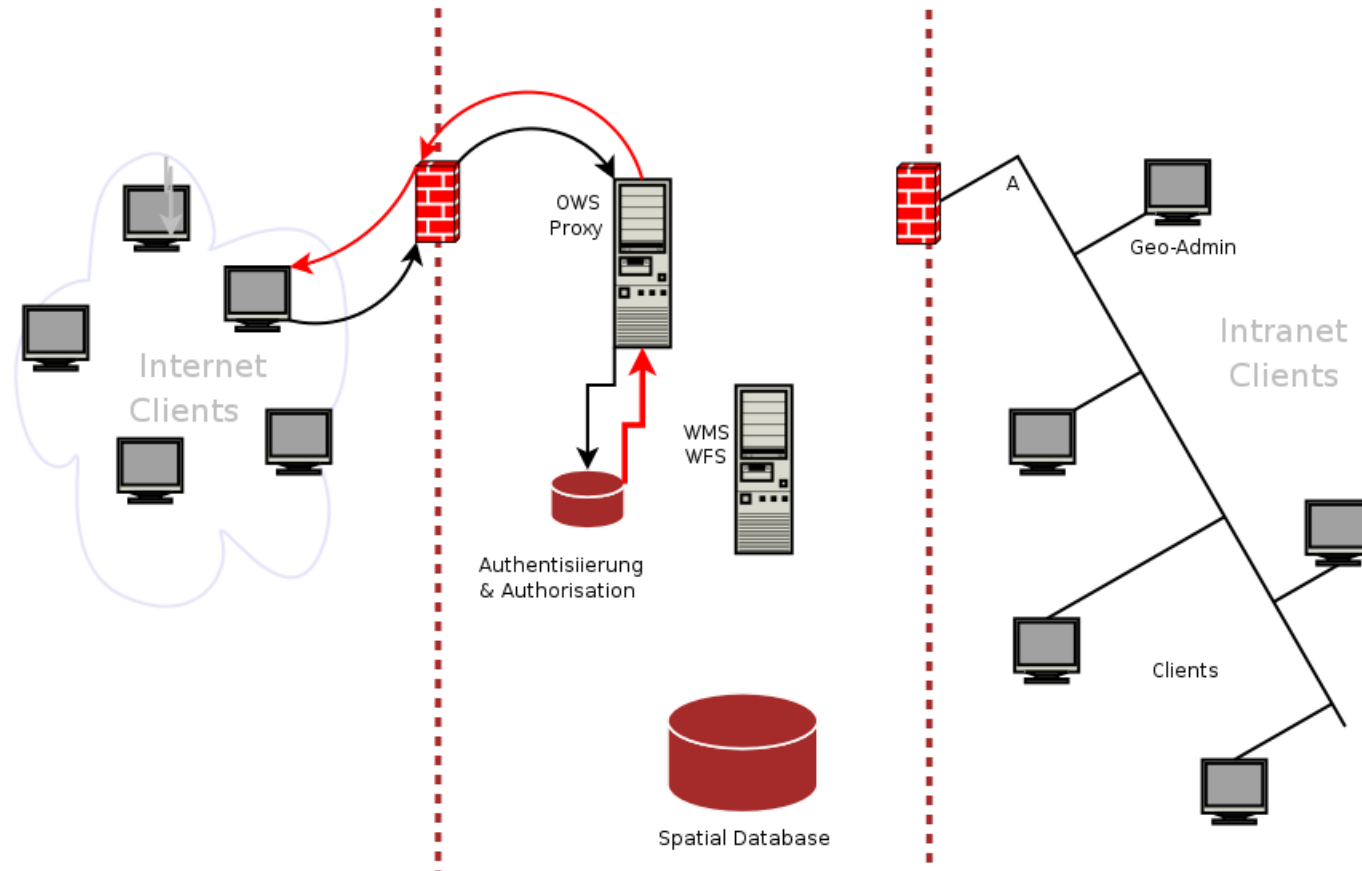
Mapbender Implementation

User authenticates at OWS Security Proxy before accessing services.



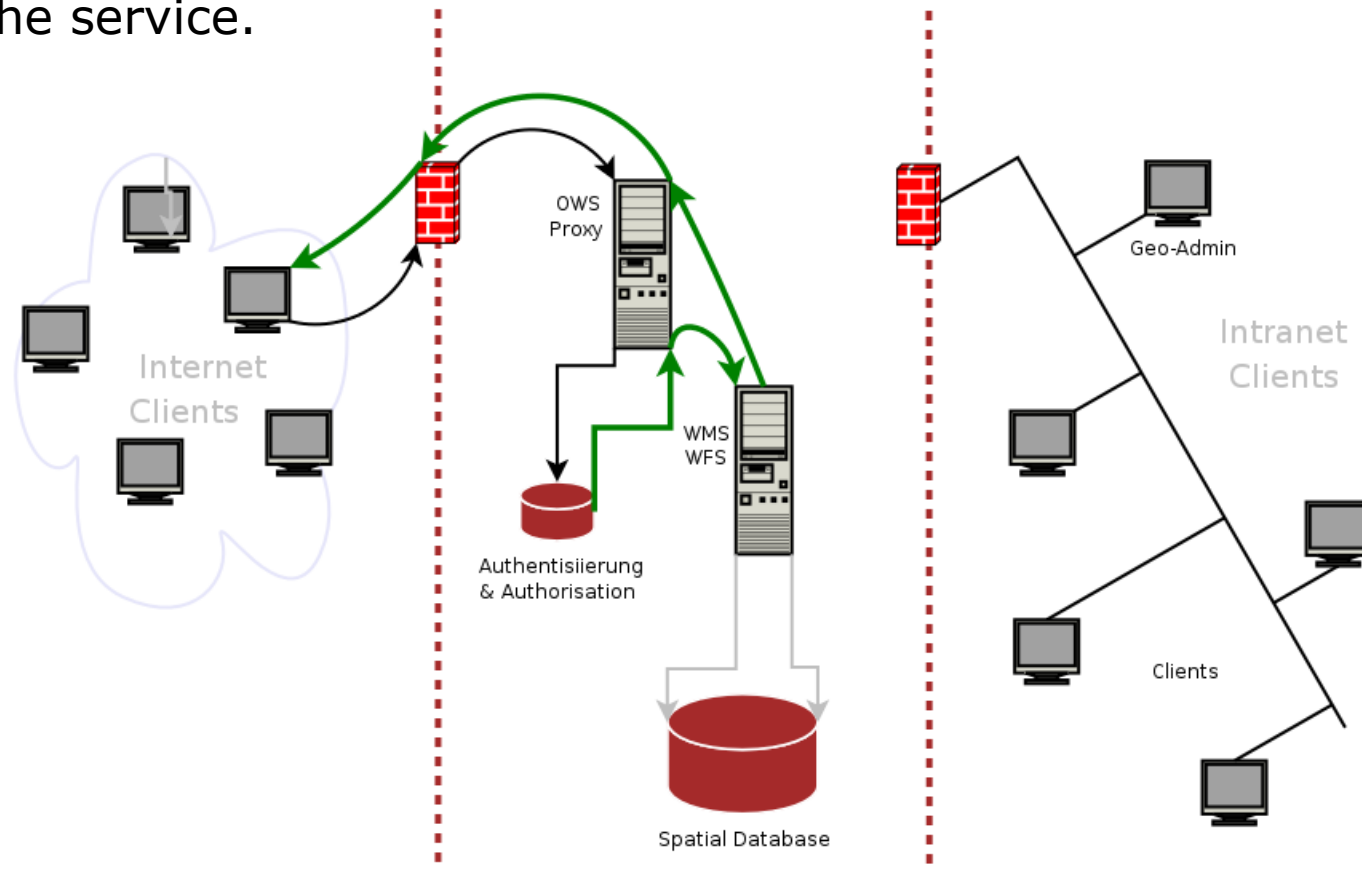
Authentication and Session Management

On unsuccessful authentication the request is rejected.



Apache URL Rewrite Ticketing

Valid authentication creates a session ID which becomes part of a dynamic WMS OnlineResource (ticket) directly routing the client to the service.



Apache URL Manipulation with Ticket

The OnlineResource parameter of the requests are manipulated by the proxy to identify the authenticated user and control the authorization for the requested service.

Original request:

`http://localhost/wms/germany.xml?VERSION=1.1.1&REQUEST=GetMap&SERVICE=WMS&LAYERS=my_polygons, ...`

Modified request sent to Proxy:

`http://127.0.0.1/owsproxy/50b3c6d6237efaaa7603f35faab17c18/63b3b2765758813b3a41265829ca5668?VERSION=1.1.1&REQUEST=GetMap&SERVICE=WMS&LAYERS=my_polygons, ...`

The Security Proxy identifies the user (the red parameter is the hashed session ID) and checks permissions for the unique wms ID (blue parameter). The rest of the request is unchanged.

Mapbender Implementation

Hands on demonstration:

Configuration of the web server (Apache) with a regular expression and the alias module to extract user and requested service from OGC request URL parameters

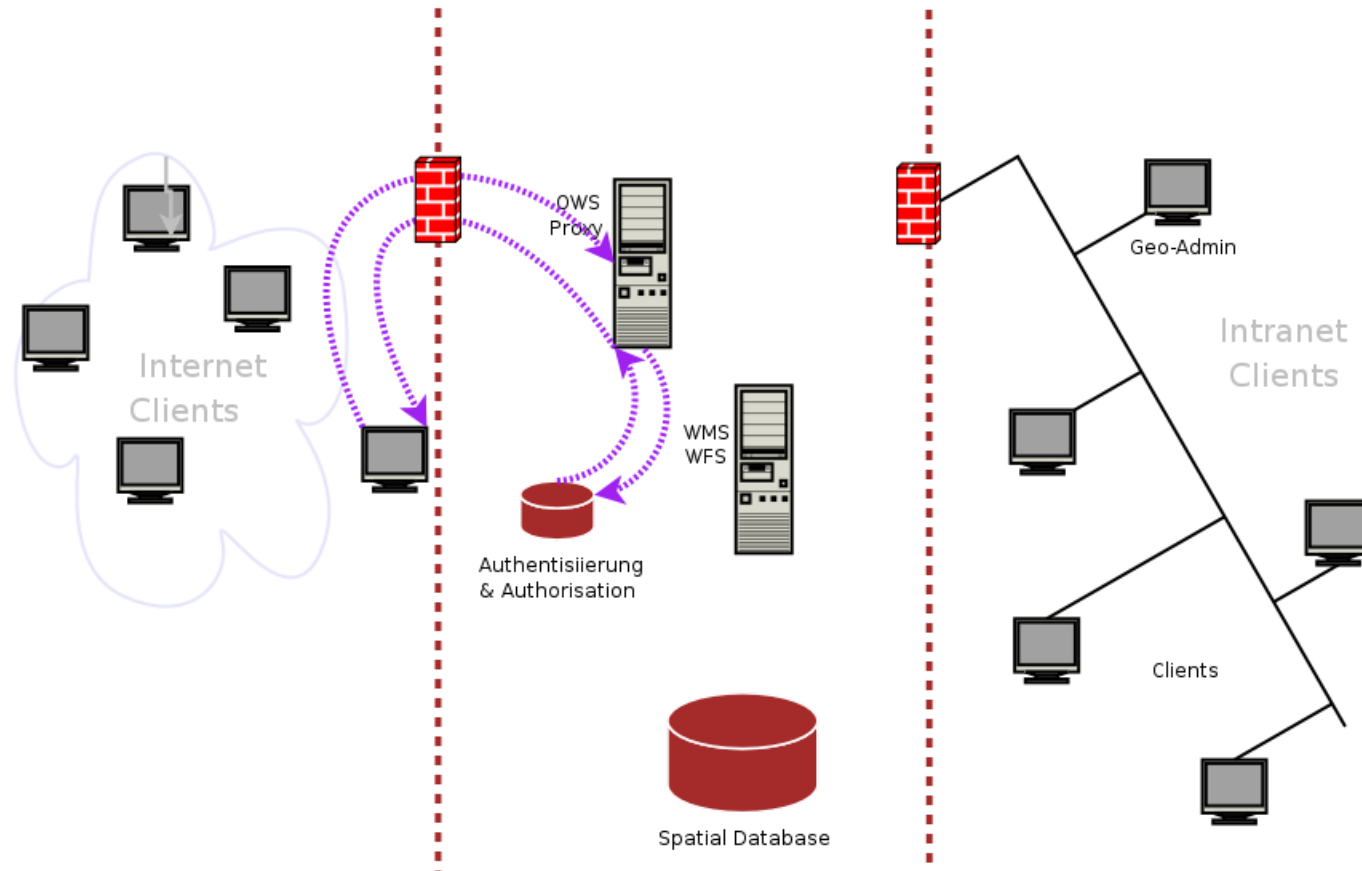
Configuration within Mapbender to use OWS Security Proxy

Protected WMS service (directly accessible only from within secure domain)

Web based interface to activate OWS Security Proxy for OGC WMS services in user interfaces

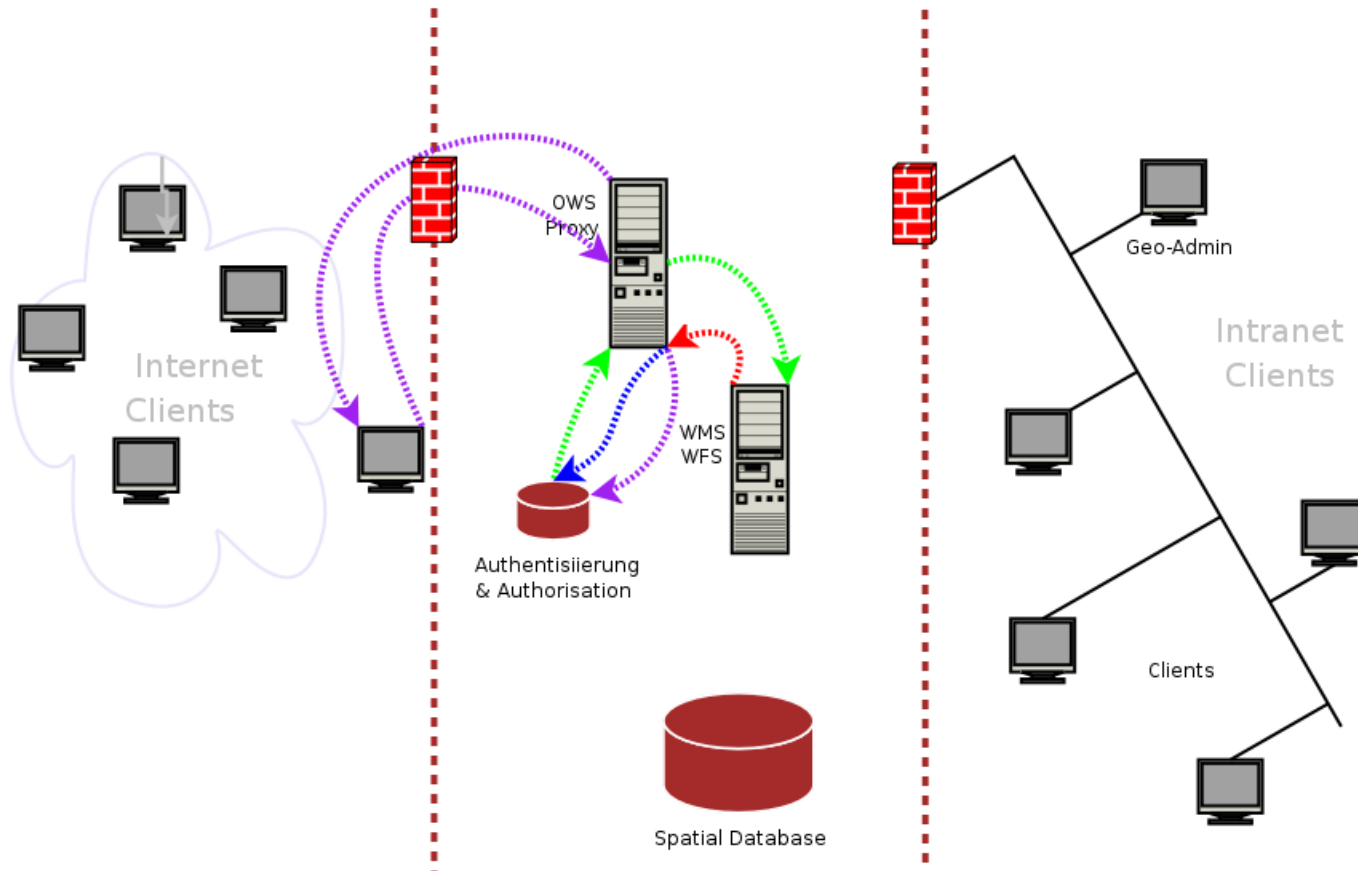
Web Based User Authorization

Multi-client capability of the software allows providers to manage access security for their own users and services themselves.



Management with OWS Service Containers

Service containers (Repository) allows for management, logging and monitoring of services stacks.



Personalized Object-based WFS-T Access

Personalized Access Implemented as Application Module

All requests are intercepted inside the secure domain

- User authorization for requested task is checked
- Request is logged and either rejected or executed

Example of a productive environment

The federal states of Rhineland Palatinate and Baden Wurttemberg in Germany operate similar infrastructures in an application for the European agricultural subsidy grant program since spring of 2005. In the first two years of operation 650.000 GML edit, modify and delete requests were processed through this framework.

<http://www.mapbender.org/index.php/FIONA>

Discussion

For further information contact:

Arnulf Christl
 arnulf.christl@wherogroup.com

Siemenstr. 8
 53121 Bonn
 Germany

This presentation is licensed and protected under the GNU FDL.

<http://www.gnu.org/licenses/fdl.txt>

Appendix: You are free to copy and redistribute this document, with or without modifying it, either commercially or noncommercially keeping this page and the author's name in place.