# Sicherheitsmanagement beim Betreiben des Geodatenportals GeoPort.HRO

Hansestadt Rostock, Dr. Detlef Neitz email: detlef.neitz@rostock.de

CCGIS GBR, Bonn, Arnulf Christl email: arnulf.christl@ccgis.de

# Gefahrenpotential für Geodatenportalen

**Allgemeine Sicherheitsprobleme**

- Abwehr von Attacken aus Internet auf Webserver und interne Netze
- Verhindern von unberechtigten Zugriff auf beschränkte Geo-Webdienste

**Spezielle Sicherheitsprobleme**

- Einschränkung der räumlichen Ausdehnung von Abfragen
- Begrenzung der Datenmengen (z.B.WFS - Datenbestand kann mit einer Abfrage ausgelesen werden)

# Individuelle Risikobewertung

- Sicherheitsarchitektur ist Kompromiss aus individueller Risikobewertung
- Bewertungskriterien: Sicherheit, Kosten, Performance
- Wichtigster Aspekt: Abschätzung des Kosten/Nutzenverhältnisses von Aufwand für Sicherheitsmaßnahmen $\Leftrightarrow$ Kosten durch evt. Schäden
- Risikofaktor Mensch - Akzeptanz und Kenntnisse bei Administratoren und Anwender sind Grundlage für Funktion der Sicherheitsmechanismen

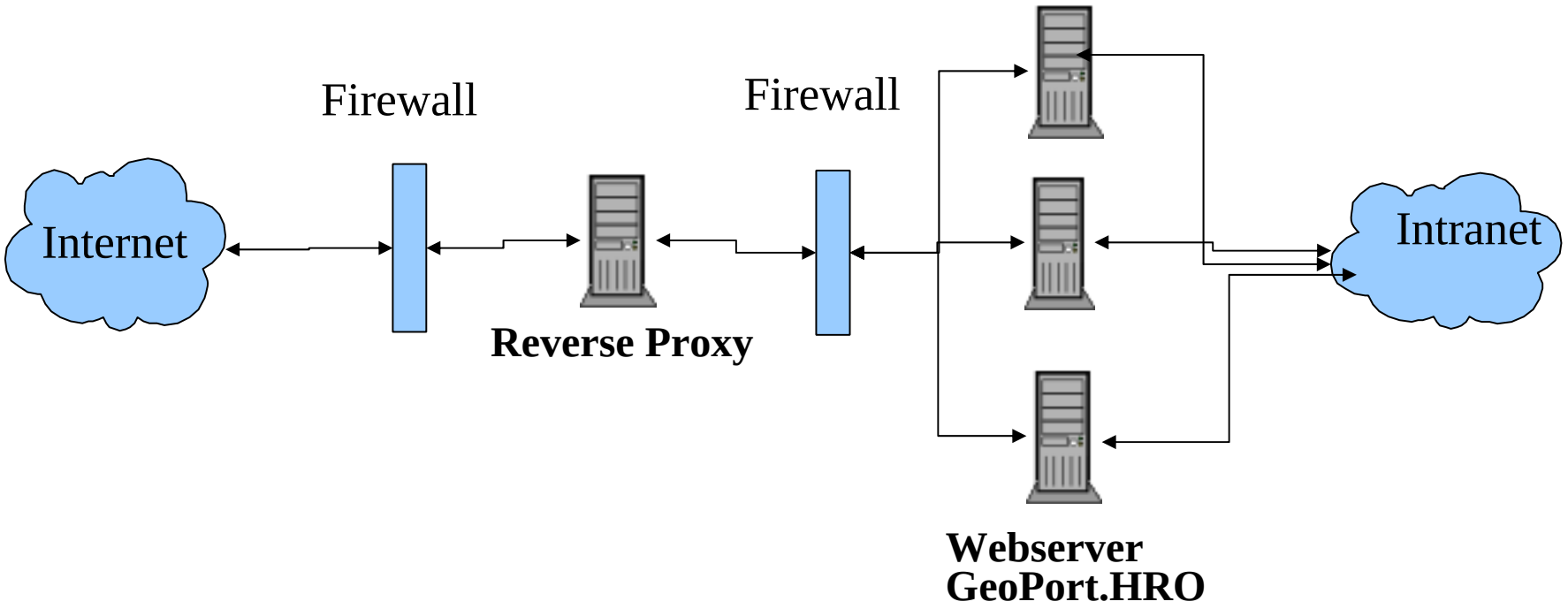
# Konzeption von Sicherheitsgateways

- Bundesamt für Sicherheit in der Informationstechnik „Konzeption von Sicherheitsgateways“
- Beschreibung der Struktur und Platzierung von Modulen, die in Abhängigkeit vom Schutzbedarf zwingend notwendig sind
- Empfohlen mehrstufiger Aufbau bestehend aus:
  Paketfilter – Application-Level-Gateway (ALG) – Paketfilter
- ALG durch HTTP Reverse-Proxy realisiert
- Höhere Schutzanforderung ⟺ Funktionserweiterung des Reverse-Proxy

# Was ist ein HTTP Reverse Proxy?

- arbeitet als Stellvertreter des Webserver
- nimmt HTTP-Anforderungen entgegen und leitet diese unter seinem Namen an einen Webserver weiter und gibt Antwort an Anfordernden zurück
- unterbricht TCP-Verbindung zwischen Anfordernden und Webserver
- wird mit konfigurierten Mappings zentral vor allen Webapplikations-Servern eingesetzt
- verbirgt die interne Netzstruktur
- Open Source Lösung: Apache mit mod_proxy Modul
- Grundlegender Konfigurationsbefehl: ProxyPass

# HTTP Reverse Proxy Architektur



# Vorteile eines HTTP Reverse Proxy

- Webserver mit minimaler Funktionalität ⇨ geringes Potenzial für Sicherheitslücken
- hohe Anforderungen an Sicherheits- und Patchlevel nur an diesem zentralen Webserver
- Funktionalitäten (Verschlüsselung, Authentisierung, Autorisierung) können hier zenrtal gelöst werden
- Zentrale Mapping ermöglicht flexibles Verteilen der Geo-Webdienste auf nachgelagerten Webservern ohne Einfluss auf Anwender

# Optimierung des Administration in einer verteilten GDI

- Viewer sollte Geo-Webdienste direkt anfordern
- Ausnahme im Intranet: Externe Dienste über internen Dienst kaskadieren für Nutzer ohne Internetberechtigung
    - Beachte: WMS GetFeatureInfo Befehl lässt sich nicht kaskadieren
- Kaskadierung von mehreren Diensten unter einem Dienst vermeiden:
    - Performance Probleme durch sequentielle Abarbeitung
    - Ausfall eines Dienstes führt zu keiner Antwort
- Eigene Dienste im Intra- und im Internet über gleichen Domainnamen erreichbar (keine IP-Adressen in den Capabilities)

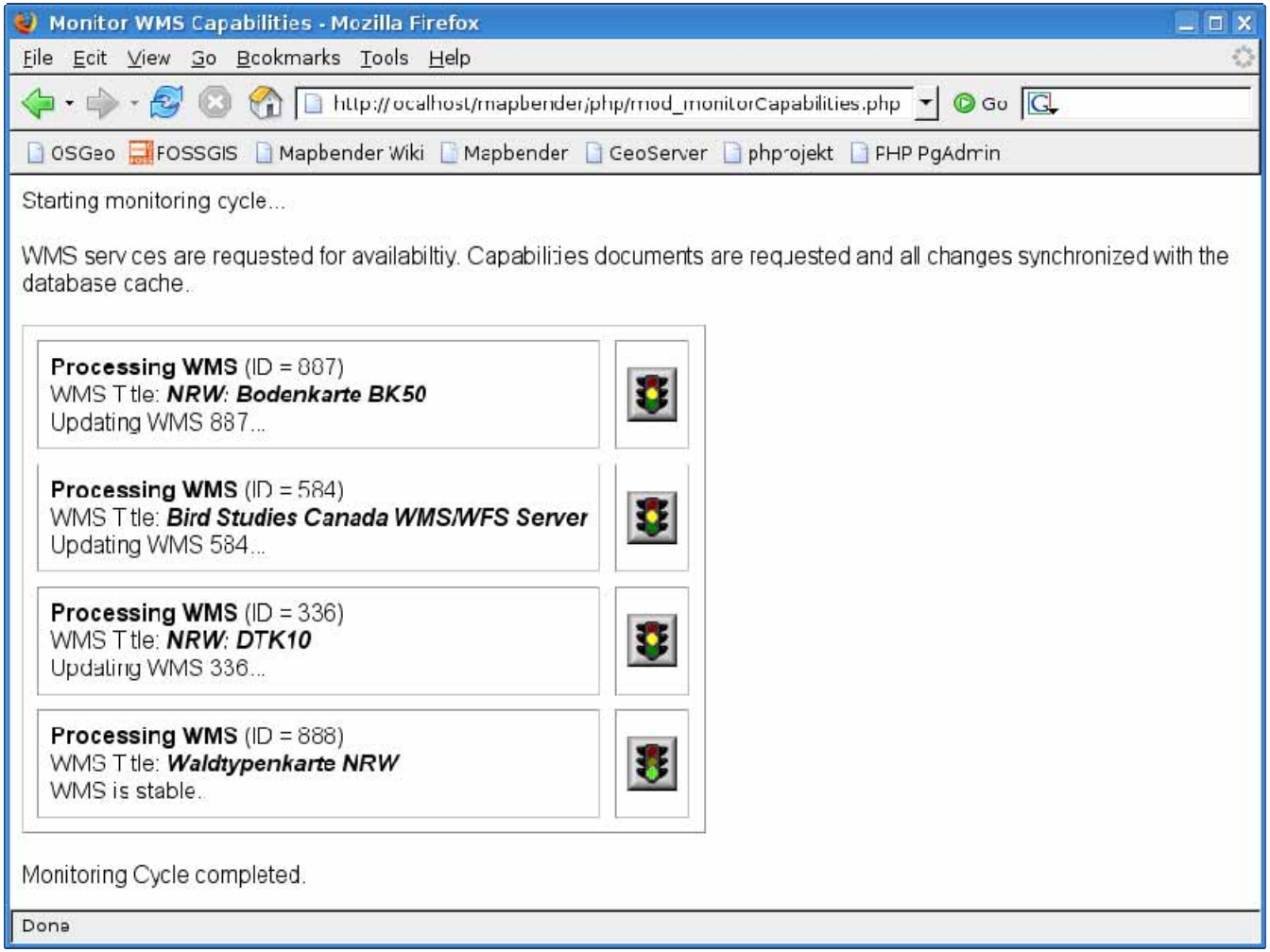
# Geo-Webdienste Monitoring

- Funktionsüberwachung komplexer verteilter Geodateninfrastrukturen
- GeoPortHRO besteht aus ca 60 eigenen und 10 externen WMS + WFS
- Monitoring Modul aus Mapbender Client-Suite testet in regelmäßigen Abständen die Dienste
- Email-Benachrichtigung der Administratoren bei Ausfall
- Reaktion auf Monitoring-Anfragen in Logdatei festgehalten
- Statistik zur Verfügbarkeit der Dienste (Prozentangaben und Diagramme)

# Monitoring Modul aus Mapbender Client-Suite

- Die Funktionsüberwachung der Dienste erfolgt mehrstufig und kann manuell oder automatisiert durchgeführt werden.
- Die manuelle Option ermöglicht es dem Administrator oder Betreiber der Geodateninfrastruktur direkt Gegenmaßnahmen zu ergreifen und bietet sich vor allem für eigene Dienst an.
- Der Intervall der automatischen Überwachung kann eingestellt werden
- Die Betreiber der ausgefallenen oder fehlerhaften Dienste werden per Email benachrichtigt.

Ansicht der Monitoring Oberfläche



## Mandantenfähigkeit

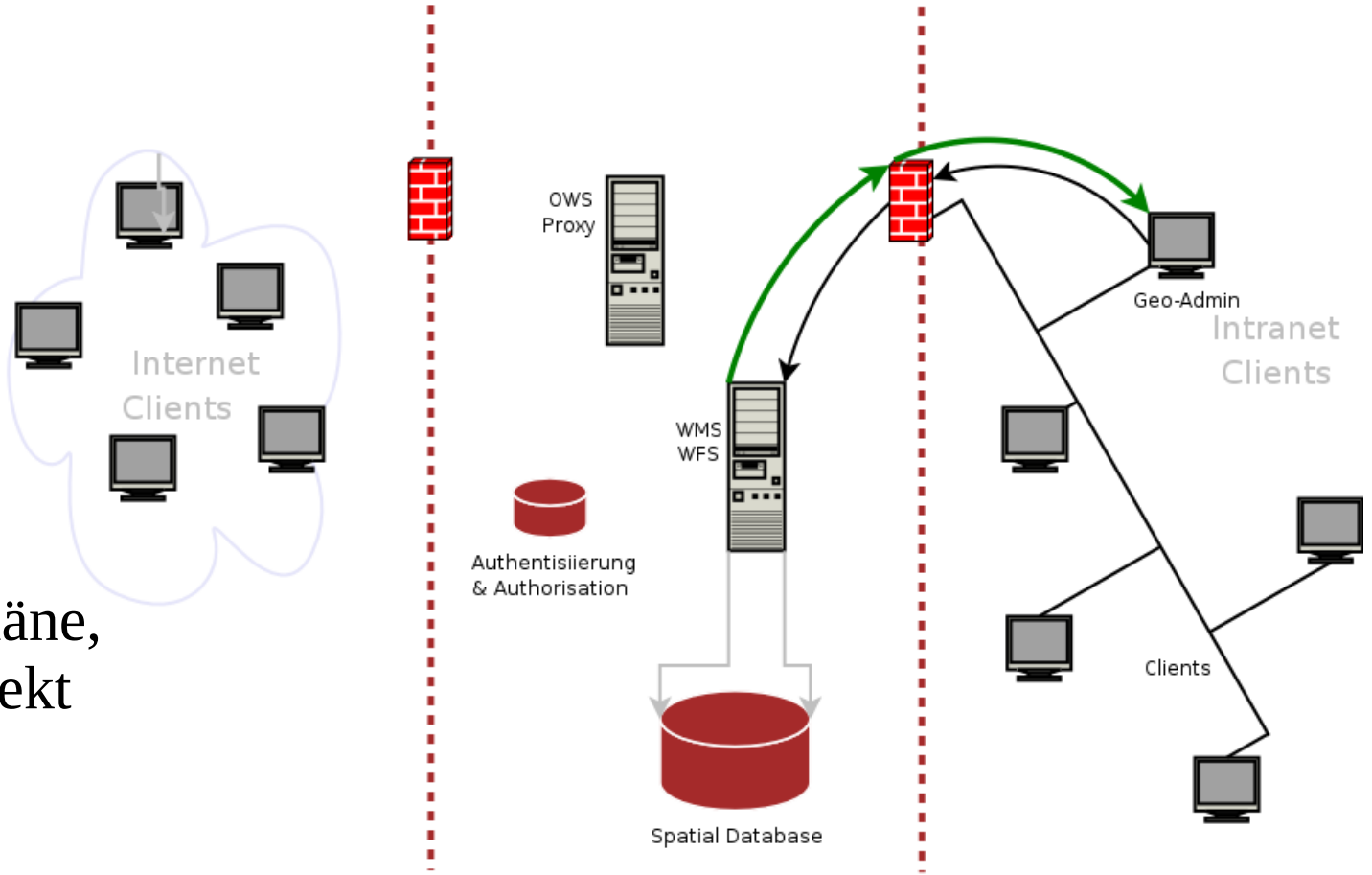
- Externe Dienste können von dem zuständigen Betreiber selbst konfiguriert und gepflegt werden
- Zentrale Verwaltung der Kennungen erleichtert Administration
- Reduzierung des Arbeitaufwandes bei Aktualisierungen
- Erhöhte Verfügbarkeit der Systeme

## Weitere Ausbaustufen

- Direkte Einbindung in Metadatensyyteme
- Automatisierte Aktualisierung durch Anfragen
- Metadaten-Trigger

# Zugriff durch WMS Clients (Trusted )

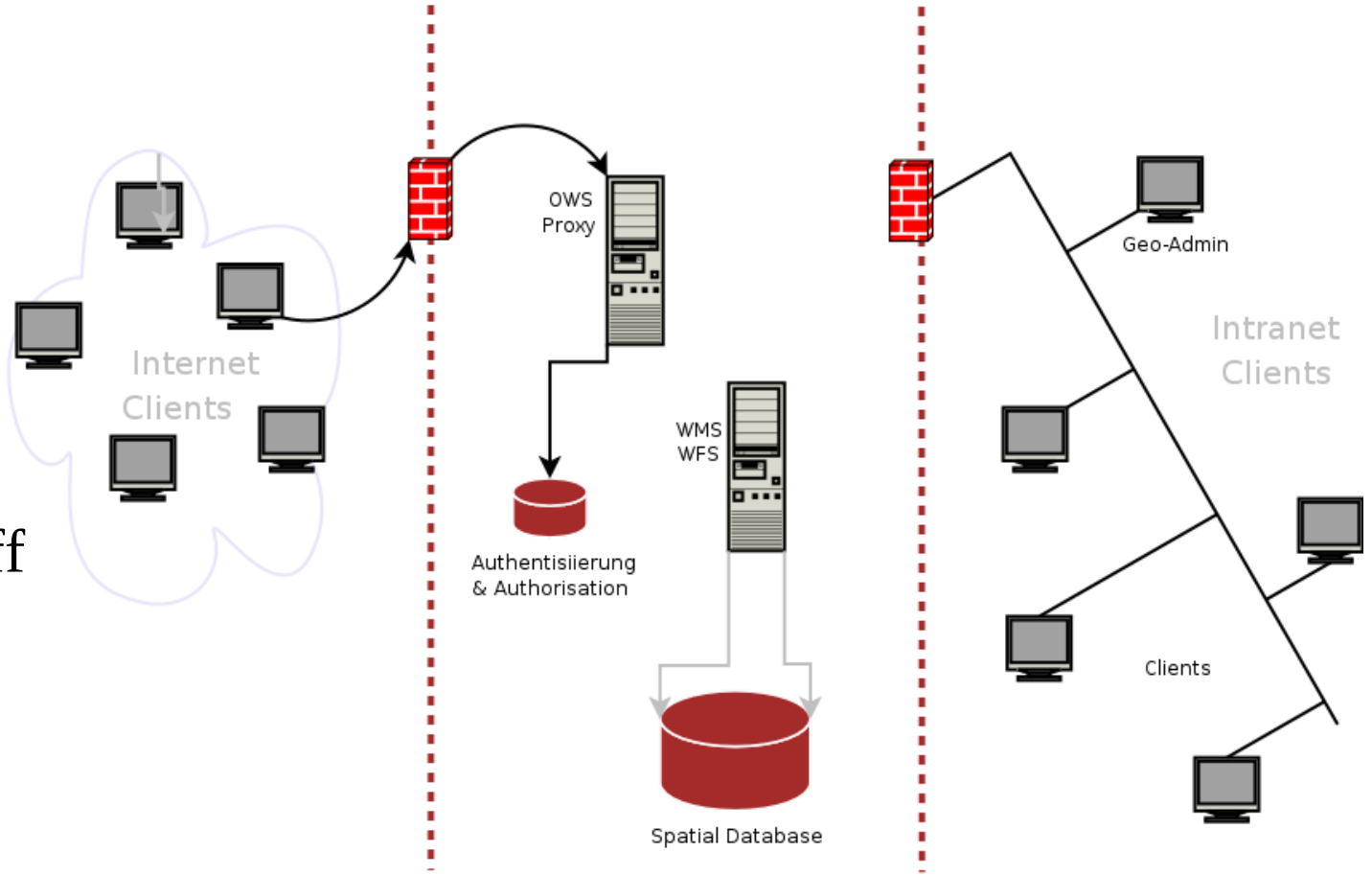
Zugriff aus autorisierter Domäne, Ergebnis wird direkt ausgeliefert



# Zugriff durch WMS Clients auf Security Proxy

Authentisierung erforderlich.

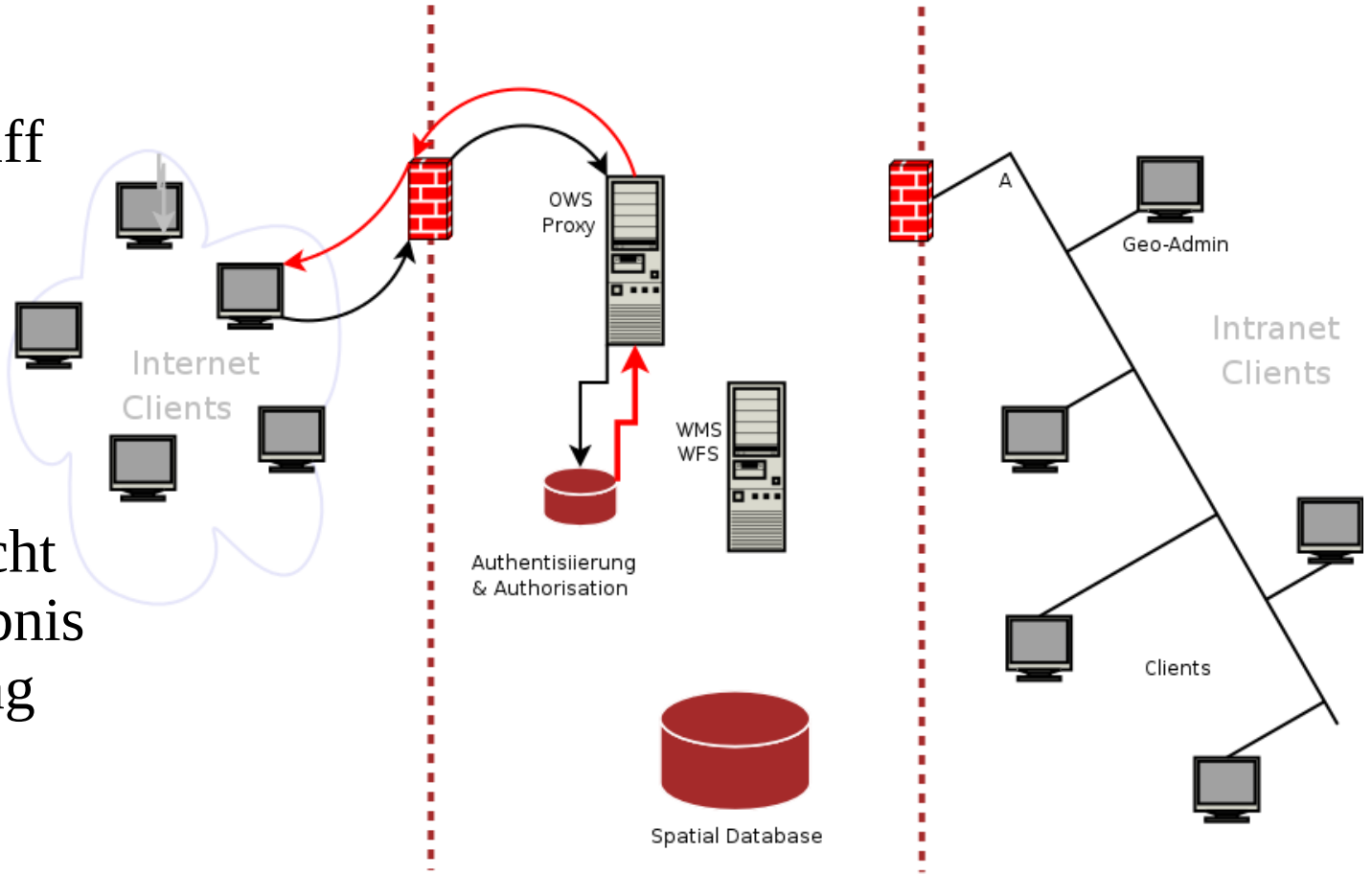
Kein Direktzugriff auf OWS Dienste möglich.



# Security Proxy verwehrt WMS Clients Zugriff

Authentisierung erfolgreich, Zugriff gestattet.

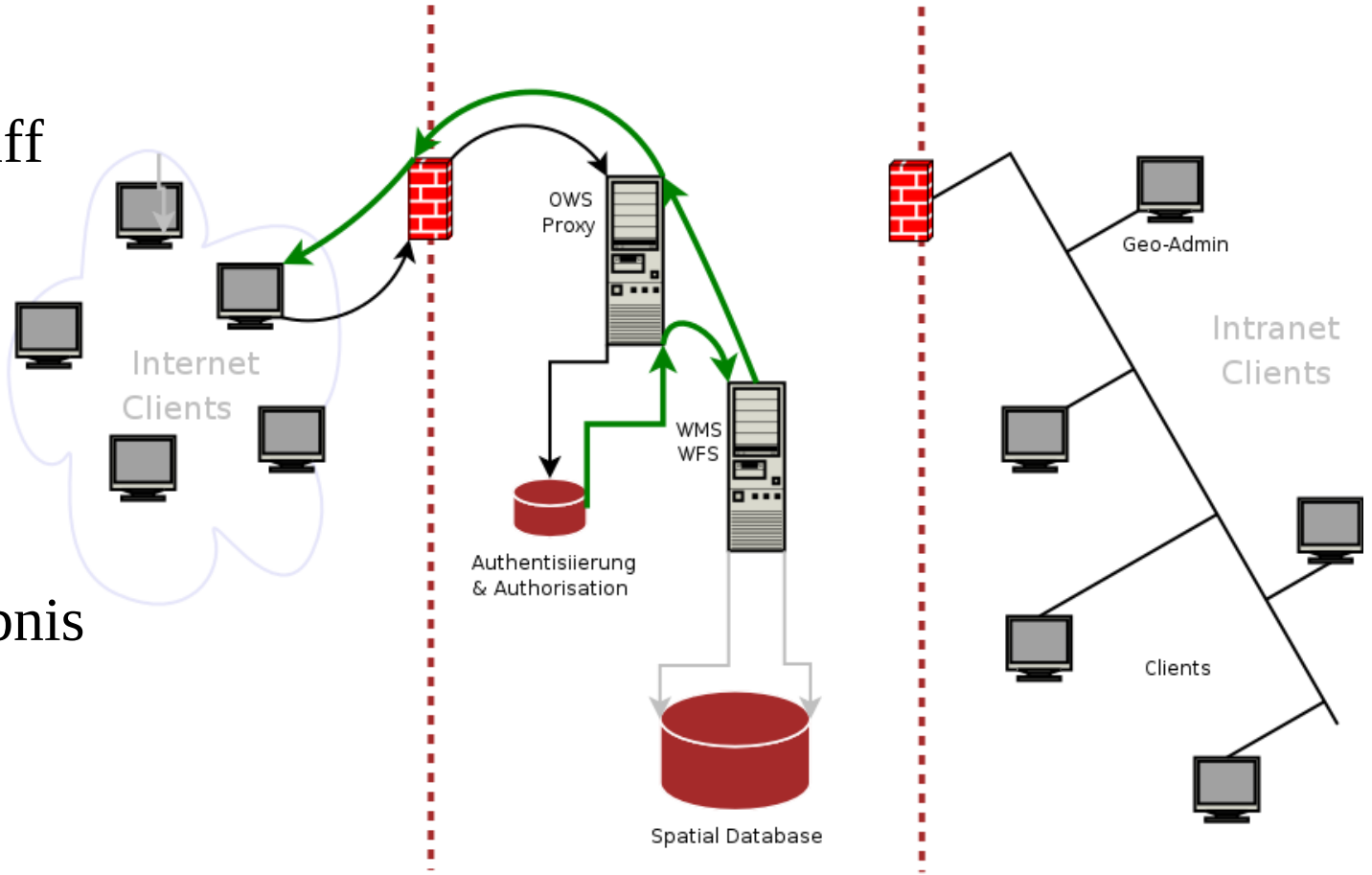
Autorisierung nicht erfolgreich, Ergebnis mit Fehlermeldung



# Zugriff durch WMS Clients über Security Proxy

Authentisierung erfolgreich, Zugriff gestattet.

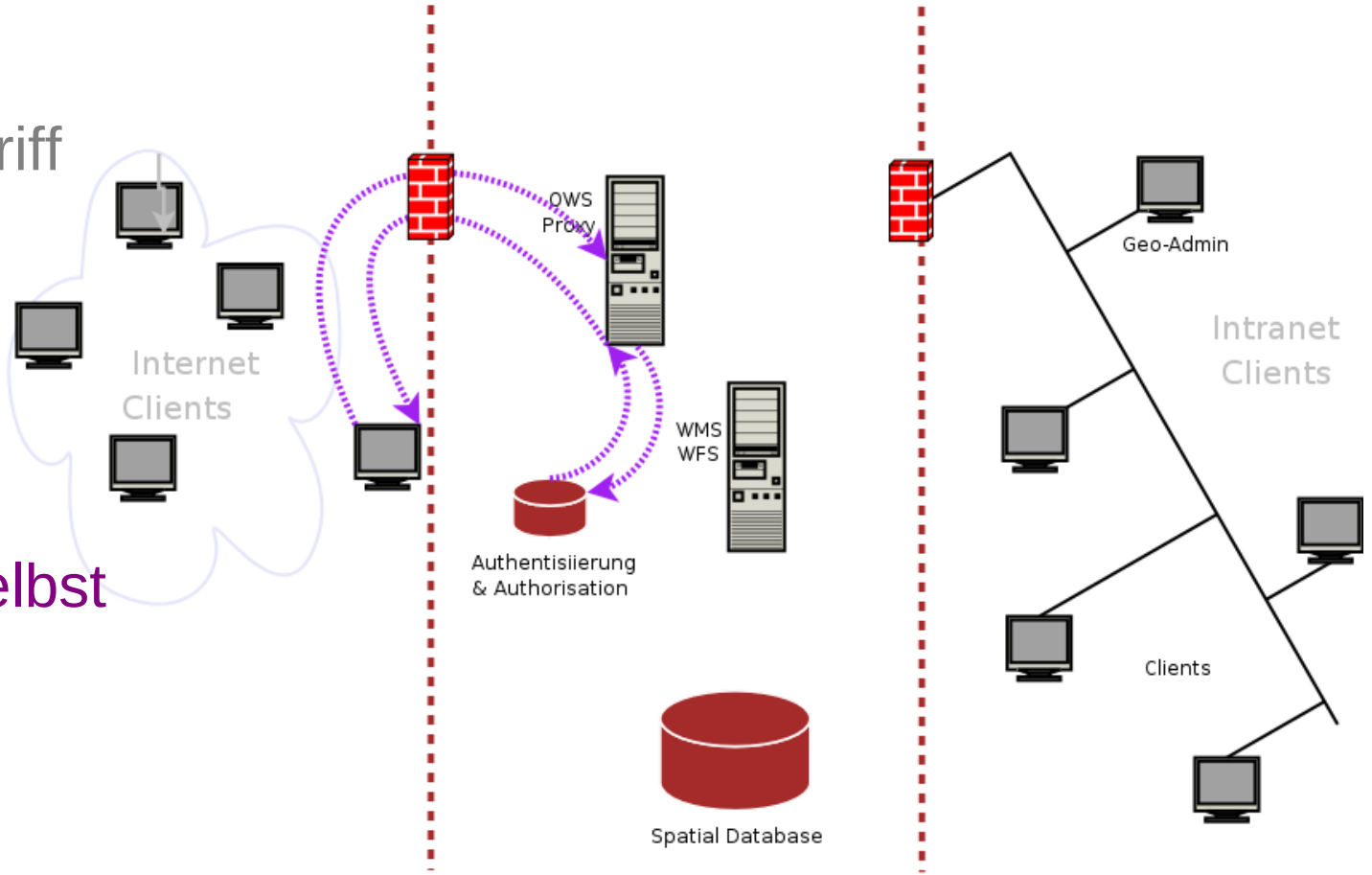
Autorisierung erfolgreich, Ergebnis wird ausgeliefert



# Verwaltung des Security Proxy durch Trusted Clients

Authentisierung erfolgreich, Zugriff gestattet.

Mandant kann Autorisierung selbst administrieren.



# Vielen Dank für die Aufmerksamkeit

## Fragen & Diskussion

Für weiteren Fragen wenden Sie sich bitte an:

Hansestadt Rostock, Dr. Detlef Neitz email: **detlef.neitz@rostock.de**

CCGIS GBR, Bonn, Arnulf Christl email: **arnulf.christl@ccgis.de**