Kanton St.Gallen
Amt für Raumentwicklung und Geoinformation

Geplante Architektur der Geodienste der kantonalen Verwaltung SG mittels ArcGIS Server

(Datensicherheit, Zugriffssicherheit, Ausfallsicherheit)

Workshop IGArc Bern, 17.09.2014

erhalten
und
gestalten

St Gallen kann es.

Inhalt

Teil 1: Infrastruktur

- geplante technische Komponenten der Architektur Geodienste

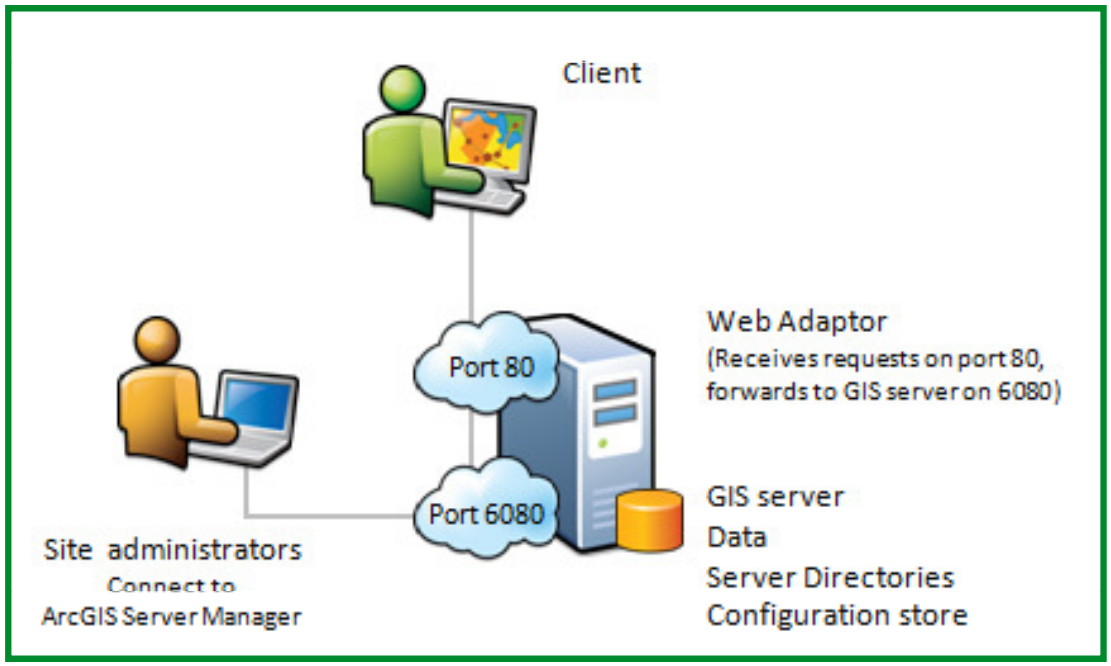
Teil 2: Management

- Datensicherheit, Zugriffssicherheit, Ausfallsicherheit

Aufbau ArcGIS Server Site

Infrastruktur

Site mit einem Computer



Quelle: Esri 2012

sämtliche Komponenten werden auf einem Rechner betrieben:

- Web Adaptor
- ArcGIS-Server
- Geodaten

Publikationszonen (I)

Infrastruktur

Nutzung innerhalb der kantonalen Behörden SG

öffentliche Nutzung (ausserhalb der kantonalen Behörden SG)

Kanton St.Gallen
Amt für Raumentwicklung und Geoinformation

Publikationszonen (II)

Infrastruktur

getrennte Dienste und Daten für INTRANET und INTERNET

\+ hohe Sicherheit durch strenge Trennung der Bereiche

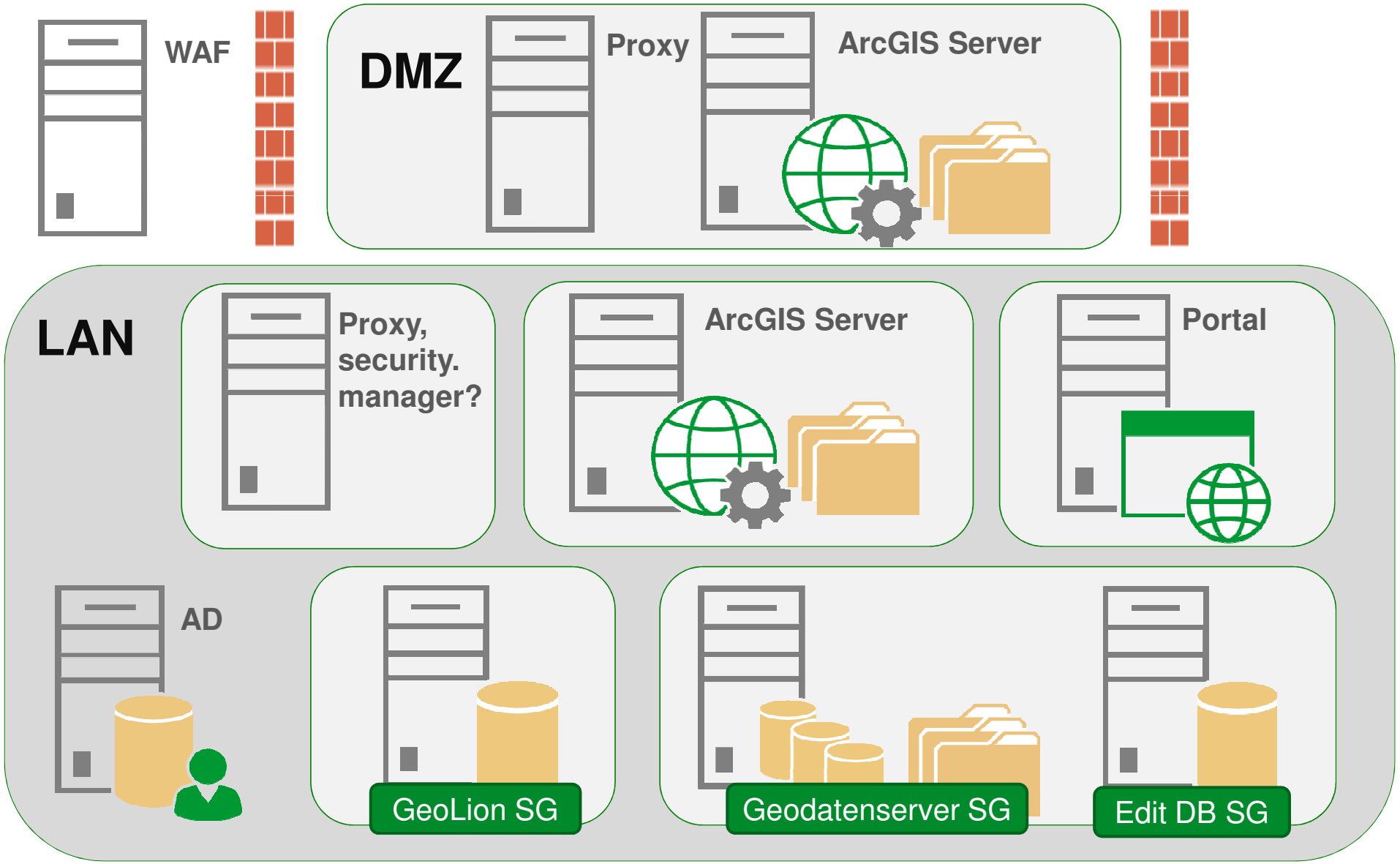
Publikationszonen (II)

Infrastruktur

getrennte Dienste und Daten für INTRANET und INTERNET
+ hohe Sicherheit durch strenge Trennung der Bereiche
- erhöhter Administrationsaufwand
- Datenredundanz

Übersicht Infrastruktur-Komponenten

Infrastruktur



Kanton St.Gallen
Amt für Raumentwicklung und Geoinformation

Publikationszonen (III)

Infrastruktur

	INTRANET Zone	INTERNET Zone
Nutzung	ausschliesslich für die Nutzung innerhalb der **kantonalen Behörden SG**	**öffentliche Nutzung** (ausserhalb der kantonalen Behörden SG)
Erreichbarkeit	nur aus dem Intranet	nicht aus dem Intranet
Benutzer	Kanton, Gemeinden SG	grundsätzlich unbeschränkt
Benutzer-verwaltung	bestehende Benutzer-verwaltungen von Kanton und Gemeinden	ArcGIS integrierter Speicher
Rollen-verwaltung	ArcGIS integrierter Speicher?	ArcGIS integrierter Speicher
Authentifiz./ Autorisierung	über Web-Server	über GIS-Server mittels ArcGIS-Token

Geodienst-Rollen für Publikation und Nutzung

Management

Rolle	Geodaten / Darstellung	Dienst + Konfig.	Metadaten	Berechtig. auf Dienste	Monitoring / Administrat.
Daten-Autor	erstellen / nachführen / löschen		erzeugen	festlegen	
Dienste-Autor		erstellen / nachführen / löschen	erzeugen / eintragen	setzen	
Administrator	kontrollieren / freigeben	kontrollieren / freigeben	freigeben	freigeben	Dienste / Infrastruktur
Named User				zugewiesene	
Unnamed User				nur freie	

Datensicherheit

Management

es werden nur Kopien produktiver Geodaten publiziert
- **File-GDB**

INTRANET Zone: es wird eine eigenständige «Edit»-Datenbank für transaktionale Geodienste aufgebaut
- **getrennt vom Geodatenserver SG**

Zugriffssicherheit (I)

Management

Verschlüsselung von Benutzerdaten mittels SSL und Transport über HTTPS

Verzeichnisse mit Geodaten und Kacheln sind gesichert und nur durch Dienste aufrufbar

Zugriff auf die Server Infrastruktur wird beschränkt auf die Rolle Geodienst Administrator

Zugriffssicherheit (II)

Management

INTERNET-Zone: vorgeschaltete Web Application Firewall unterbindet eingehende Anfragen und ausgehende Antworten mit verdächtigem Inhalt

INTERNET Zone: Ausgehende Verbindungen von der Server Site zur übrigen Infrastruktur der kantonalen Verwaltung werden nicht erlaubt

- **Datenverbindung vom Geodatenserver SG zu den Publikationsdaten besteht ausschliesslich aus dem Intranet in DMZ**

Ausfallsicherheit und Datensicherung

Management

Redundante Auslegung
Server, Netzwerk, Storage

Datensicherung
Geodaten und Cache
Geodienst Konfigurationen
Server & System Konfigurations-Dateien / Nutzerdaten (System Backup)