ETAT DE FRIBOURG
STAAT FREIBURG

Service du cadastre et de la géomatique SCG
Amt für Vermessung und Geomatik VGA

ArcGIS for Server 10.1 - 10.2 : Sicherung von Diensten und Anwendungen

Erfahrung von Kanton Freiburg

—

Fabien Hamel

Workshop IGArc, Wabern **17. September 2014**

—

Direction des finances **DFIN**
Finanzdirektion **FIND**

Sicherung von ArcGIS for Server

Basisprinzipien

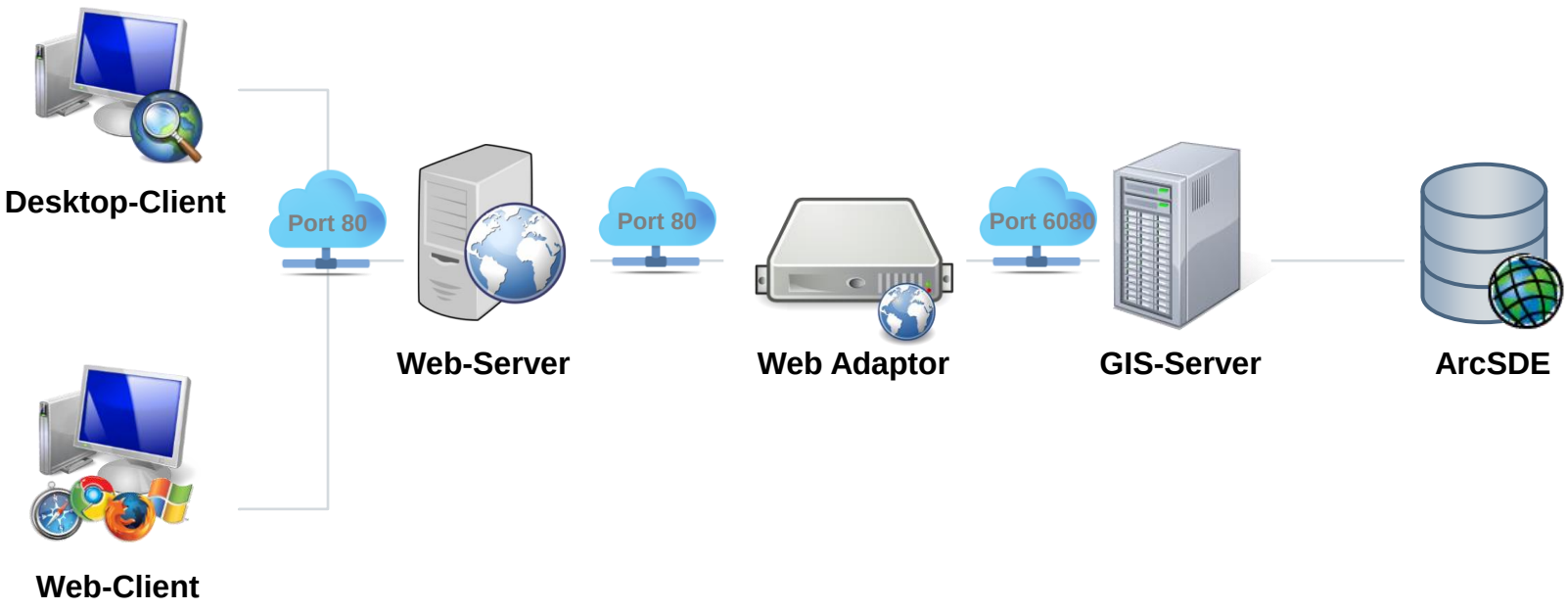
> Unterscheiden Sicherung von **Diensten** und **Anwendungen**

> ArcGIS for Server (GIS-Server) behandelt Sicherung von Web-Diensten

> Anwendungen sind durch ein Web-Server gesichert

Sicherung von ArcGIS for Server

Standard-Architektur



Sicherung von ArcGIS for Server

Authentifizierung: wie und wo?

- Auf dem GIS-Server
  - **Unbedingt Benutzername + Passwort**
  - ArcGIS-Token
  - Automatische Erwerben ermöglich

- Auf dem Web-Server
  - Klassischen Web-Methoden
  - Web Adaptor obligatorisch

Sicherung von ArcGIS for Server

Identitätsspeicher

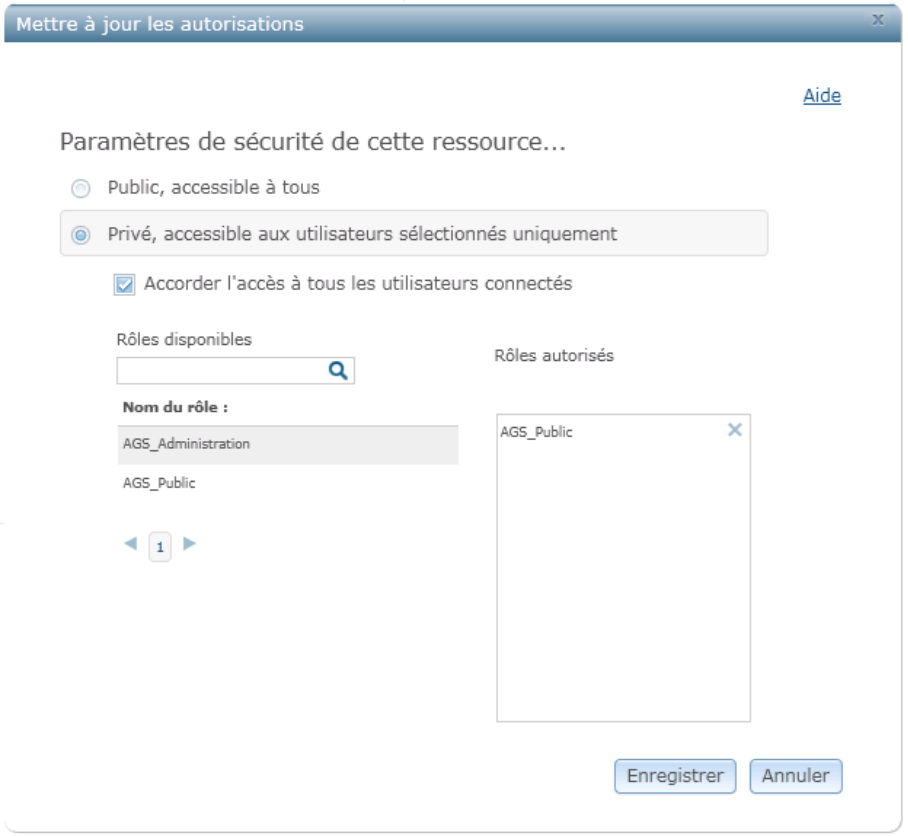
- Windows Active Directory oder LDAP
  - Read-Only (kein Verwaltung)

- Integrierter Speicher des ArcGIS for Server
  - Wenn keine vorhandene Benutzerspeicher
  - Manchmal leichter eigene Benutzerspeicher zu haben
  - Unabhängigkeit von IT-Dienstleistung

Sicherung von ArcGIS for Server

Einschränken des Zugriffs auf Web-Diensten

> Pro Dienst
> Pro Ordner
> Gesamte Site



Sicherung von ArcGIS for Server

Tokenbasierte ArcGIS-Authentifizierung

> Um zu vermeiden, jedes mal ein gesicherter Dienst angerufen ist ein Passwort zu geben, gibt es die Möglichkeit ein ArcGIS-Token zu verwalten

> Ihre Authentifizierungsdaten (Benutzer + Passwort) bleiben für eine begrenzte Zeit gespeichert (60 minutes oder 1 Tag standardmässig)

> Der Token ist eine Folge von Zeichen, die in einer Textvariablen gespeichert werden können

Generated Token: **JJ47Kjtbo7mIAlK005eZNU2iByoX8VyKbbiCqDbICxXATwl5dGeoc7fw6UUfXU2z**

Sicherung von ArcGIS for Server

Tokenbasierte ArcGIS-Authentifizierung

> Wie ein Token zu erhalten? http://<server>/arcgis/tokens

> Es ist möglich eine **serverseitige** Funktion zu automatisieren
  > Vorteil: kein Passwort sichtbar

> Die Funktion ist clientseitig angerufen
  > Ergebnis ist in einer temporären Variablen gespeichert
  > GIS-Token wird verwendet, wenn ein gesicherter Dienst verbraucht ist

Sicherung von ArcGIS for Server

Tokenbasierte ArcGIS-Authentifizierung

> Beim Laden der JavaScript-API ist es möglich, ein ArcGIS-Token direkt zu erhalten

```
// Appel de la page ASP.NET demandant un jeton valide
var xmlHttpReq = createXMLHttpRequest();
xmlHttpReq.open("GET", "http://sdarcgis01/TopoMaps/config/GetToken.ashx", false);
xmlHttpReq.send(null);
_t_k = xmlHttpReq.responseText;
```

> Die Liste von Dienste wird so konfiguriert, dass die ArcGIS-Token automatisch verwendet ist

```
MapResource.LIMITES_ADMINISTRATIVES = new TT_MAPRESOURCE('LIMITES_ADMINISTRATIVES');
MapResource.LIMITES_ADMINISTRATIVES.LayerType = "Dynamic";
MapResource.LIMITES_ADMINISTRATIVES.Url = 'http://sdarcgis01/arcgis/rest/services/Commun/Limites_administratives/MapServer?token=' + _t_k;
MapResource.LIMITES_ADMINISTRATIVES.Transparency = 0;
```

> Nichts mehr zu tun auf der Anwendungsebene

Sicherung von ArcGIS for Server

Architekturszenarien

Szenario	Benutzer-speicher	Authentifizierungs ebene	Authentifizierungs modus	Anwendung	Verschlüsselung (HTTPS)
Single Sign On	Windows AD	Web (IIS)	Windows (IIS)	Alle die SSO unterstützt	Optional
Benutzer und Rollen von Firma	Windows AD, LDAP	Alle	Alle	Alle *	Empfohlen
Web-Editierung	Alle	Alle	Alle	Alle *	Empfohlen
Mobile-Anwendungen	Alle	Alle	Alle	Alle *	Empfohlen
SharePoint	Alle	Alle	Alle	Alle *	Empfohlen
Benutzer von Firma, integrierte Rollen	Windows AD, LDAP	Alle	Alle	Alle *	Empfohlen
ArcGIS Online	Alle	Alle	Alle	Alle *	Empfohlen

* *Silverlight und SharePoint brauchen ein Proxy um Tokens zu verwalten*

Sicherung von ArcGIS for Server

Szenario 1: interne Web-Anwendung

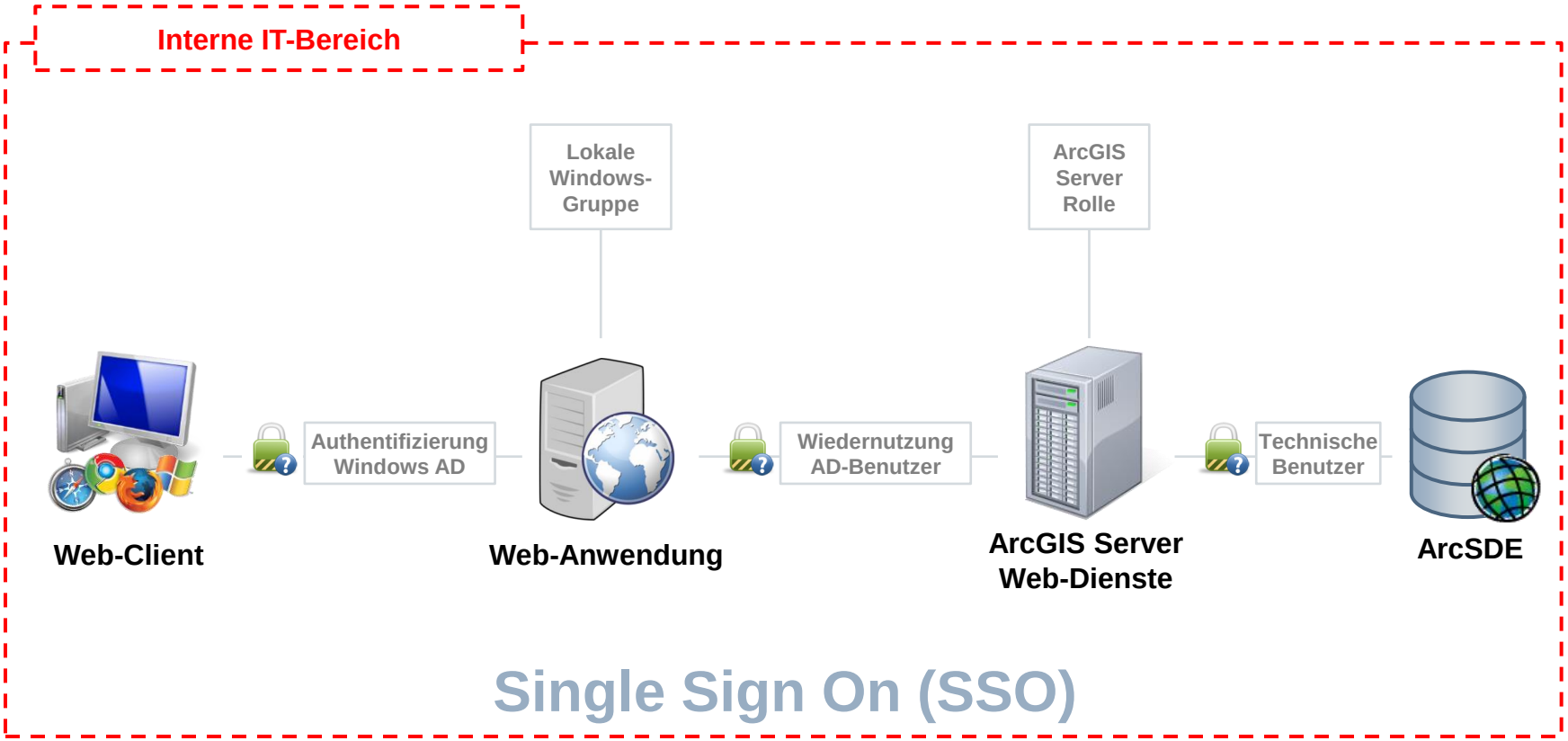
- GIS-Server Einstellungen
  - Benutzerspeicher: Windows Active Directory
  - Rollespeicher: ArcGIS Server
  - Authentifizierungsebene: GIS-Server
  - Authentifizierungsmodus: ArcGIS-Token

- Sicherung von Diesten:
  - Für gemeinsame Dienste: einfache Authentifizierung
  - Für bestimmte Dienste: Benutzer muss zu einer ArcGIS-Rolle gehören

- Sicherung von Anwendungen (Web-Server):
  - Benutzer muss zu einer lokalen Windows-Gruppe gehören

Sicherung von ArcGIS for Server

Szenario 1: interne Web-Anwendung



Sicherung von ArcGIS for Server

Szenario 2: öffentliche Verbreitung über Internet

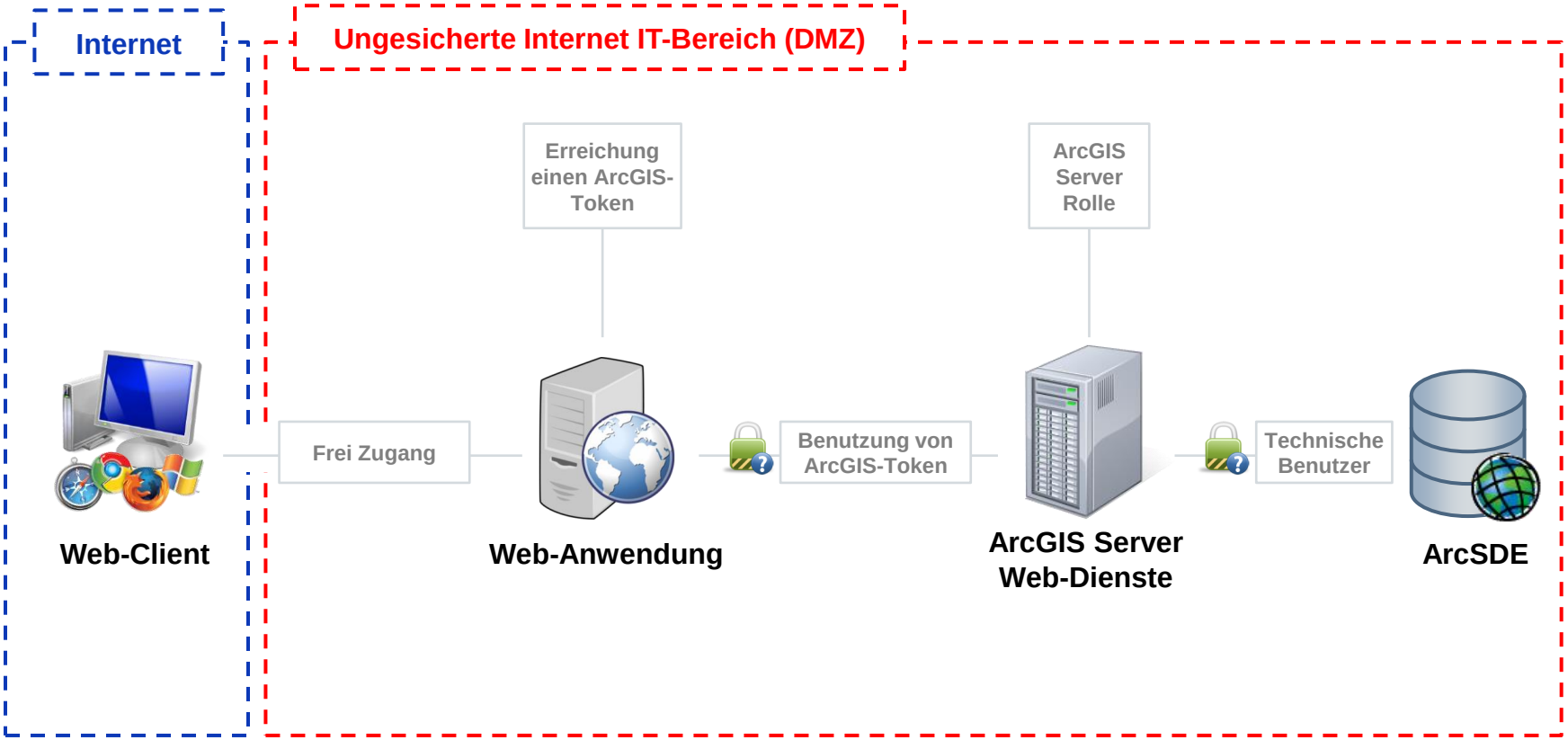
- GIS-Server Einstellungen
  - Benutzerspeicher: ArcGIS Server
  - Rollespeicher: ArcGIS Server
  - Authentifizierungsebene: GIS-Server
  - Authentifizierungsmodus: ArcGIS-Token

- Sicherung von Diesten:
  - Durch einem technischen Benutzer
  - Erreichung einen ArcGIS-Token

- Sicherung von Anwendungen (Web-Server):
  - Freie Zugang

Sicherung von ArcGIS for Server

Szenario 2: öffentliche Verbreitung über Internet



Sicherung von ArcGIS for Server

Szenario 3: gesicherte Verbreitung über Internet

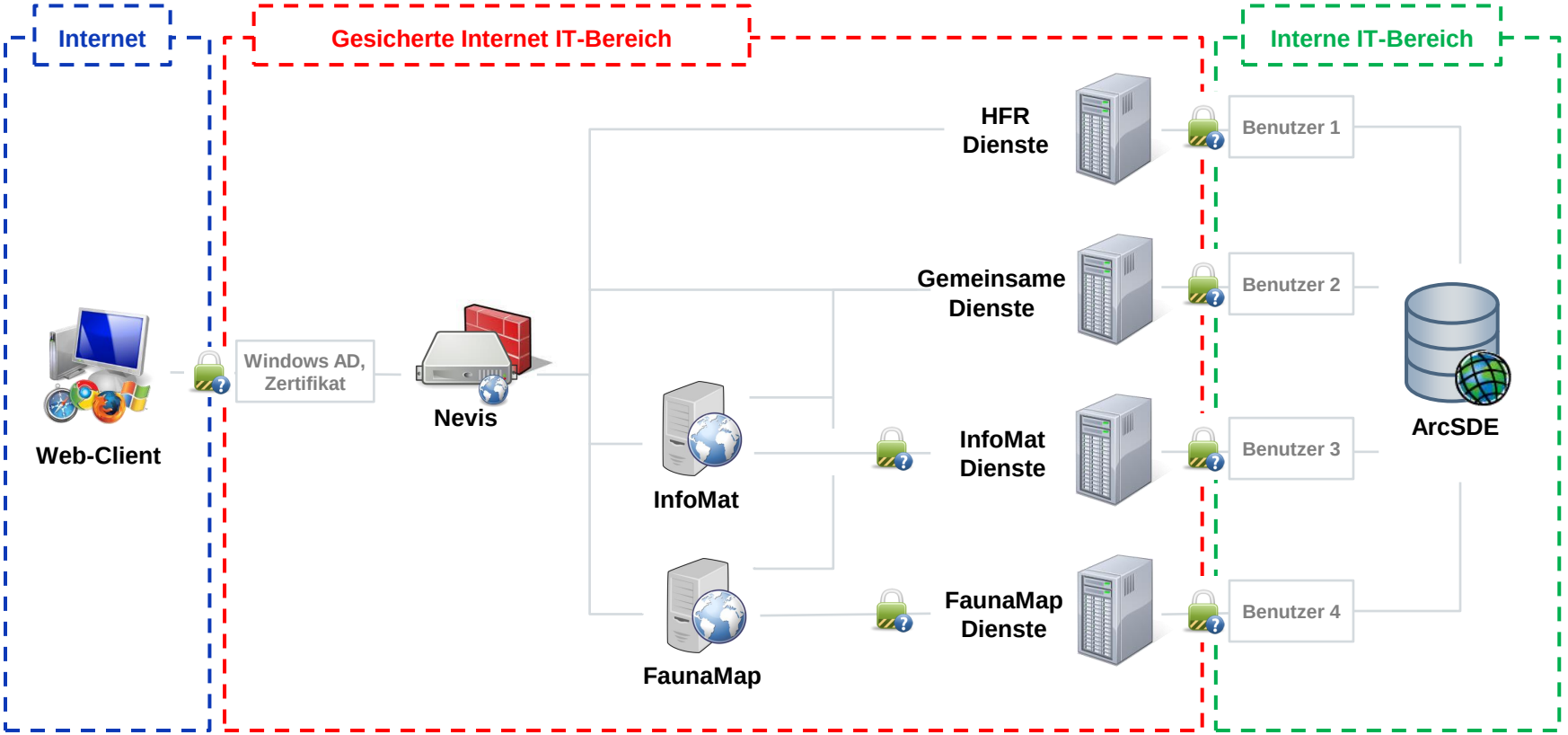
- GIS-Server Einstellungen
  - Benutzerspeicher: LDAP
  - Rollespeicher: ArcGIS Server
  - Authentifizierungsebene: GIS-Server
  - Authentifizierungsmodus: ArcGIS-Token

- Sicherung von Diesten:
  - Jetzt, keine Sicherung

- Sicherung von Anwendungen (Web-Server):
  - Authentifizierung durch Nevis (mehr weiter)
  - URL-Filterung nach Benutzer

Sicherung von ArcGIS for Server

Szenario 3: gesicherte Verbreitung über Internet



Sicherung von ArcGIS for Server

Was ist Nevis?

- Allgemeine Freiburgeren Lösung für Internet-Sicherung
  - Gesicherte Reverse-Proxy
  - Integrierte Web Application Firewall (WAF)
  - Authentifizierung und Ausbreitung von Benutzerinformationen in gesicherten Tokens (URL, Cookie)
  - HTTPS Protokoll

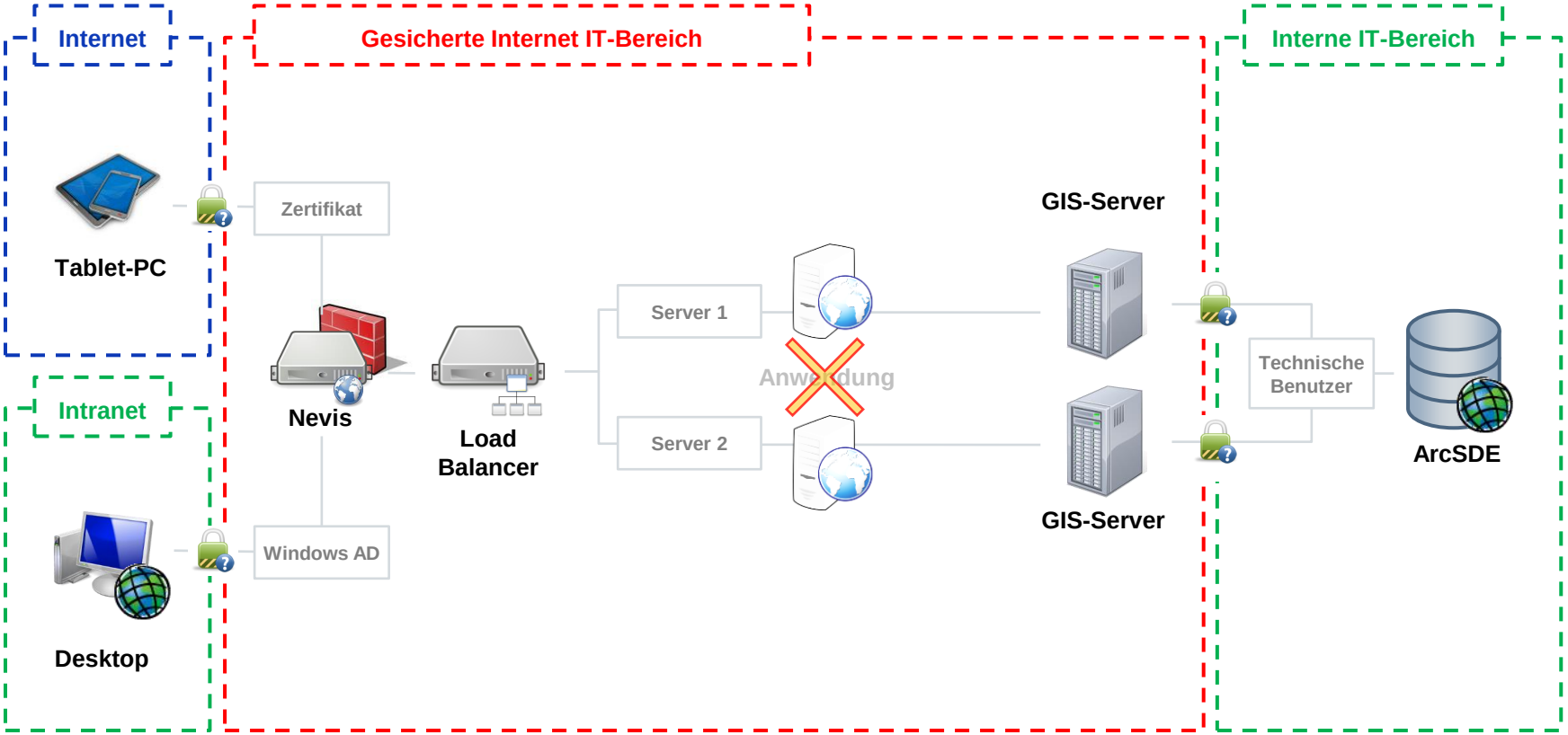
Sicherung von ArcGIS for Server

Wie arbeiten Nevis und ArcGIS zusammen?

- 2 ArcGIS Instanzen (2 Sites)
  - Klassisch Load Balancer vorher
- Jede Anwendung hat ihre eigene URL:
  - https://appls.fr.ch/sit/infomat
- Jede Dienstgruppe auch:
  - https://appls.fr.ch/sit/arcgis/rest/services/SAGA_144
- Zugriff auf interne ArcSDE-Datenbanken möglich

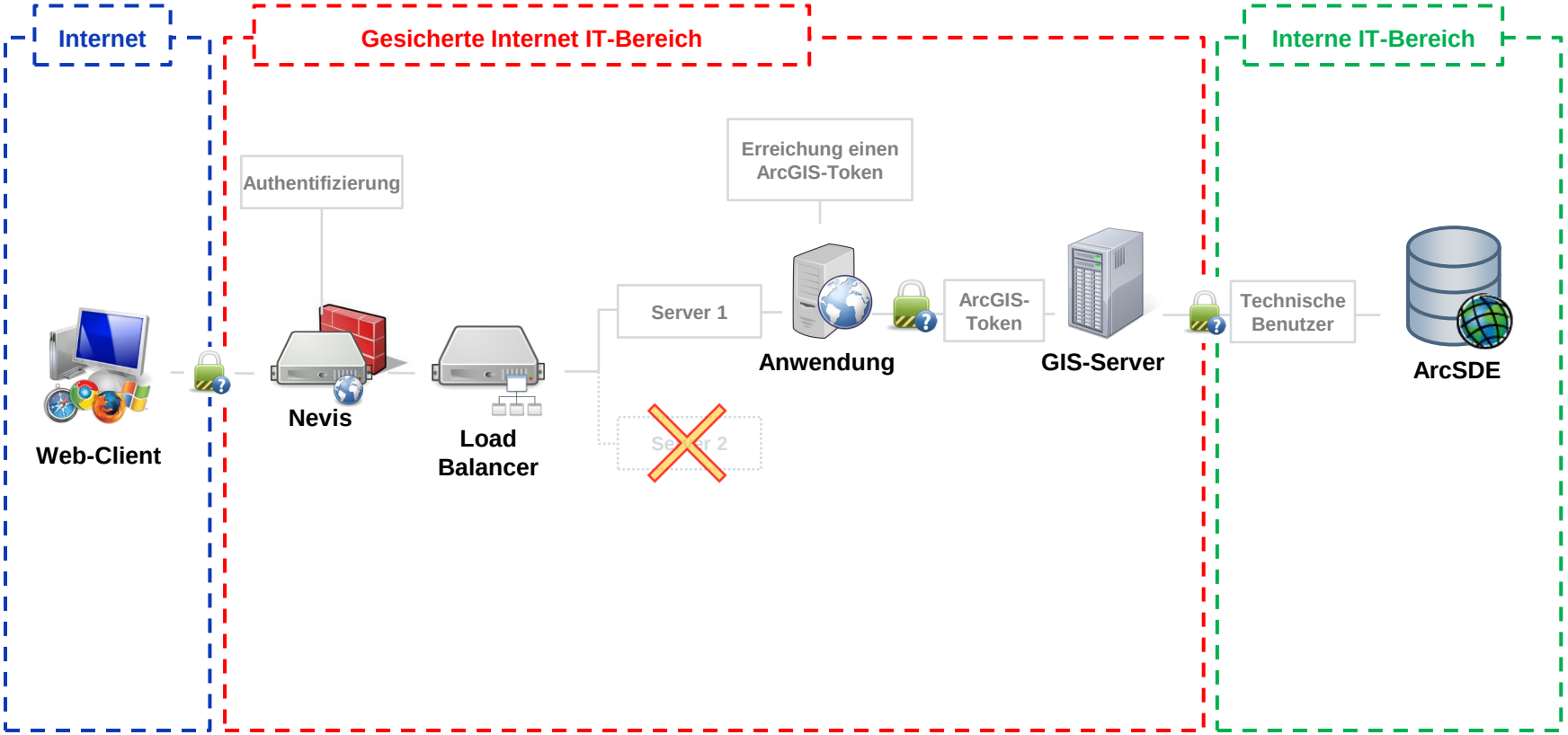
Sicherung von ArcGIS for Server

SAGA-144: freiburger Spital Krankenwagen



Sicherung von ArcGIS for Server

InfoMAT, FaunaMap



Sicherung von ArcGIS for Server

Spezifische Anfragen unserem Nutzen

- Authentifizierungszertifikat
  - Kein Benutzername, kein Passwort: leichter Für Krankenwagen-Team
  - URL-Filterung durch Nevis

- HTTP Referer
  - Technisch möglich, aber keine Lösung für Security-Team

- Offline-Erfassung
  - Jetzt kein Antwort: nicht genug Erfahrung