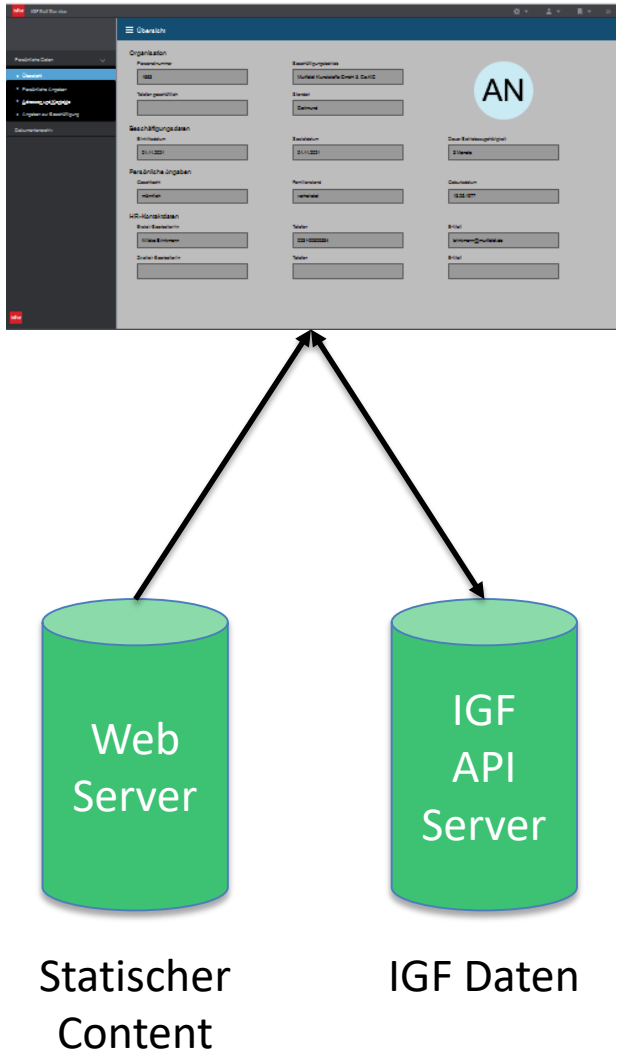
Untersuchung bezüglich der Anwendungs-Sicherheit

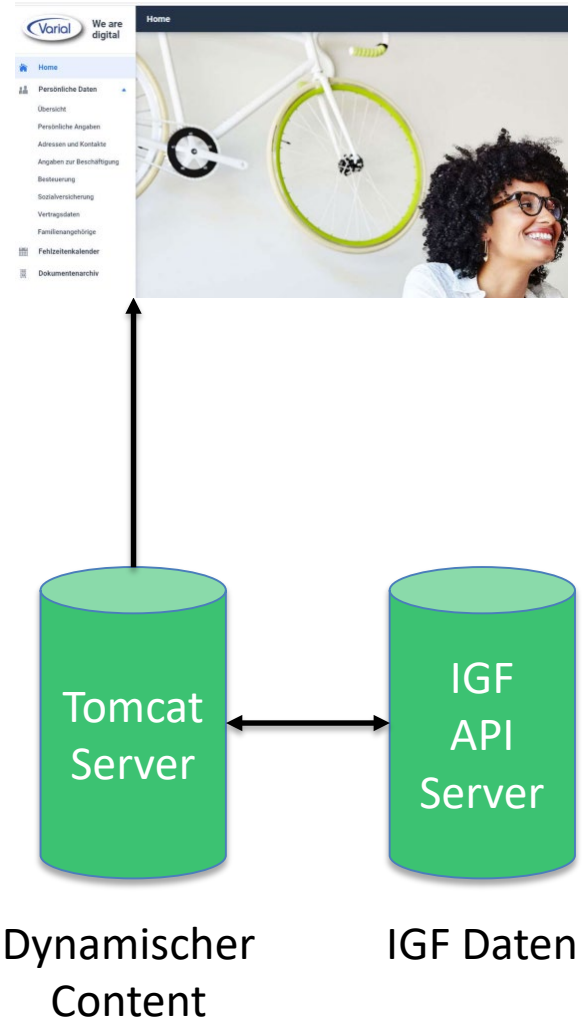
Sichere Veröffentlichung des IGF Self-Service Portals

- Java-Script (Angular) basierte Client-Variante
- Java SpringBoot basierte Server-Variante

- Angular Single-Page App
- Vollständige Verarbeitung per Javascript im Browser
- Direkte Kommunikation mit IGF-Backend per API



- Server-basierte Java Anwendung auf Basis des SpringBoot Frameworks
- Tomcat Web-Application Server
- Kapselung der API-Kommunikation durch Verarbeitung auf dem Server
- weiterhin moderne JS Anwendung mit Möglichkeit der asynchronen Kommunikation per Websocket
- Möglichkeit der Anpassung von Designs, Hintergründen, etc.
  - ➢ von Infor aktuell unterstütze Variante (mind. seit 2.91.1)



Untersuchung bezüglich der Anwendungs-Sicherheit

- Token nur im Session Speicher, (Bearer-Authentication - keine Cookies)
  - ➢ Anfälligkeit für Cross-Site-Scripting minimiert

- Übermittlung der Login Daten als URL-Attribute (HTTP-GET)
  - ➢ Obwohl HTTP-POST unterstützt wird
  - ➢ Payload (Base64 encoded password) potentiell in Logs sichtbar

- API Authentifizierung per JSON Web Token (JWT)
  - ➢ Nicht manipulierbar
  - ➢ Rechteausweitung bei sicherer Implementierung nicht möglich

PAYLOAD: DATA


```
{
  "iss": "78f2d024-3f51-464a-ad27-f2c1f83eed0b",
  "aud": "igfC",
  "iat": 1648712573,
  "exp": 1648798973,
  "sid": "51956518-fa01-4f76-9cae-8c0ec501d678",
  "tokenType": "WEB_CLIENT_SESSION_TOKEN",
  "nbf": 1648712453,
  "sub": "001/1663",
  "uid": "935266389263623313",
  "authorities": [
    "USER"
  ]
}
```


- Software-Aktualität
  - ➢ Diverse **nicht-Kritische Lücken** wurden seit der laufenden Jetty Version behoben *https://www.eclipse.org/jetty/security_reports.php*

Powered by Jetty:// 9.4.24.v20191120

Table 1. Resolved Issues

Date	ID	Exploit	Severity	Affects	Fixed Version
2022/07/05	CVE-2022-2191	Med	High	<= 10.0.9, <= 11.0.9	10.0.10, 11.0.10
2022/07/05	CVE-2022-2047	Low	Low	<= 9.4.46, <= 10.0.9, <= 11.0.9	9.4.47, 10.0.10, 11.0.10
2022/07/05	CVE-2022-2048	Med	High	<= 9.4.46, <= 10.0.9, <= 11.0.9	9.4.47, 10.0.10, 11.0.10
2021/07/15	CVE-2021-34429	Med	Med	9.4.37 - 9.4.42, 10.0.1 - 10.0.5, 11.0.1 - 11.0.5	9.4.43, 10.0.6, 11.0.6
2021/06/22	CVE-2021-34428	Low	Low	<= 9.4.40, <= 10.0.2, <= 11.0.2	9.4.41, 10.0.3, 11.0.3
2021/06/08	CVE-2021-28169	Med	Med	<= 9.4.40, <= 10.0.2, <= 11.0.2	9.4.41, 10.0.3, 11.0.3
2021/04/01	CVE-2021-28165	Med	High	7.2.2 - 9.4.38, 10.0.0.alpha0 - 10.0.1, 11.0.0.alpha0 - 11.0.1	9.4.39, 10.0.2, 11.0.2
2021/04/01	CVE-2021-28164	Med	Med	9.4.37, 9.4.38	9.4.39
2021/04/01	CVE-2021-28163	Med	Med	9.4.32 - 9.4.38, 10.0.0.beta2 - 10.0.1, 11.0.0.beta2 - 11.0.1	9.4.39, 10.0.2, 11.0.2
2021/02/26	CVE-2020-27223	Med	Med	9.4.6.v20170531 - 9.4.36.v20210114, 10.0.0, 11.0.0	9.4.37, 10.0.1, 11.0.1
2020/11/17	CVE-2020-27218	Med	Med	9.4.0.RC0 - 9.4.34, 10.0.0.alpha0 - 10.0.0.beta2, 11.0.0.alpha0 - 11.0.0.beta2	9.4.35, 10.0.0.beta3, 11.0.0.beta3
2020/10/19	CVE-2020-27216	Med	High	< = 9.4.32	9.3.29, 9.4.33
2020/07/09	CVE-2019-17638	Med	High	>= 9.4.27, < = 9.4.29	9.4.30
2019/11/25	CVE-2019-17632	Med	Med	>= 9.4.21, < = 9.4.23	9.4.24

- Unnötige Directory Listings – /download/<CompanyCode>/

- Zugriff auf fremden Download Content (Directory Listing)
  - Aufgrund des möglichen Directory Listings kann zwischengespeicherter Download Content von Jedermann abgerufen werden
    (standardmäßig bleiben heruntergeladene Daten 5min auf dem IGF Server verfügbar)
    `com.infor.selfservice.expirydecryptedfile=5`
  - Es ist für diesen Vorgang keine Authentifizierung erforderlich!!!

- Zugriff auf fremden Download Content (bekanntes Namensschema)
  - Aufgrund der bekannten Namensvergabe *<Dokument>-<aktueller Unix Timestamp><xyz>.pdf* könnte ein Script **selbst bei deaktiviertem Directory Listing** auf fremde Dateien zugreifen.

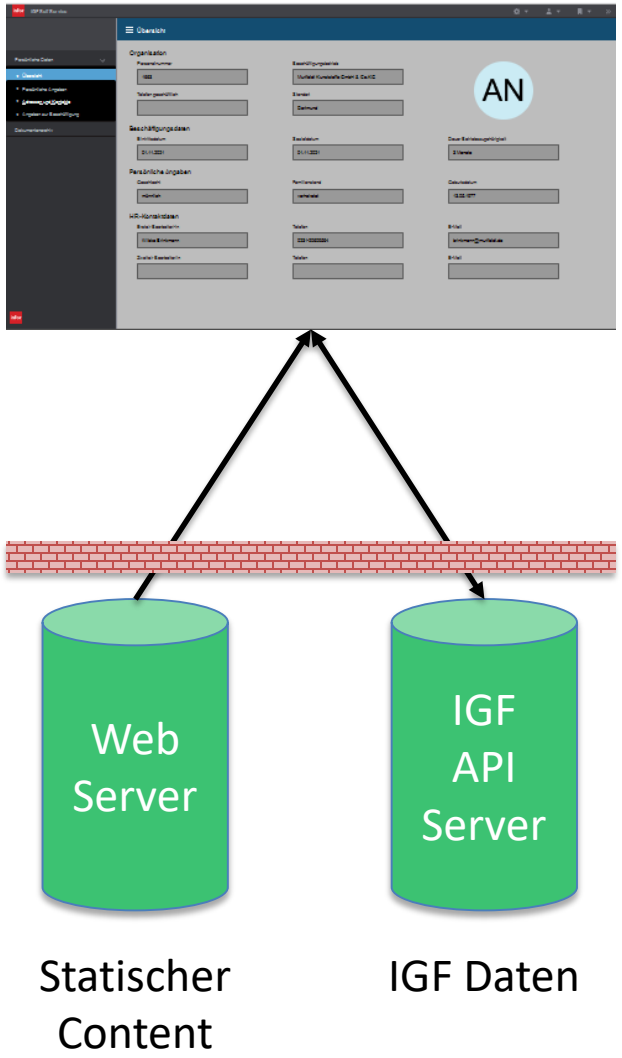
Directory: /download/001/

Name ⇧	Last Modified	Size
Parent Directory	-	-
1006-2021-01-27-162101.zip	27.01.2021, 16:21:01	69.885 bytes
1136-2021-01-26-122411.zip	26.01.2021, 12:24:11	86.140 bytes
1588-2021-01-25-121500.zip	25.01.2021, 12:15:00	81.807 bytes
VDN_202002-1611660092977952.pdf	26.01.2021, 12:21:32	68.672 bytes
VDN_202008-1611760775586042.pdf	27.01.2021, 16:19:35	69.328 bytes
VDN_202009-1611761064377042.pdf	27.01.2021, 16:24:24	68.784 bytes
VDN_202009-1611775762189042.pdf	27.01.2021, 20:29:22	68.784 bytes

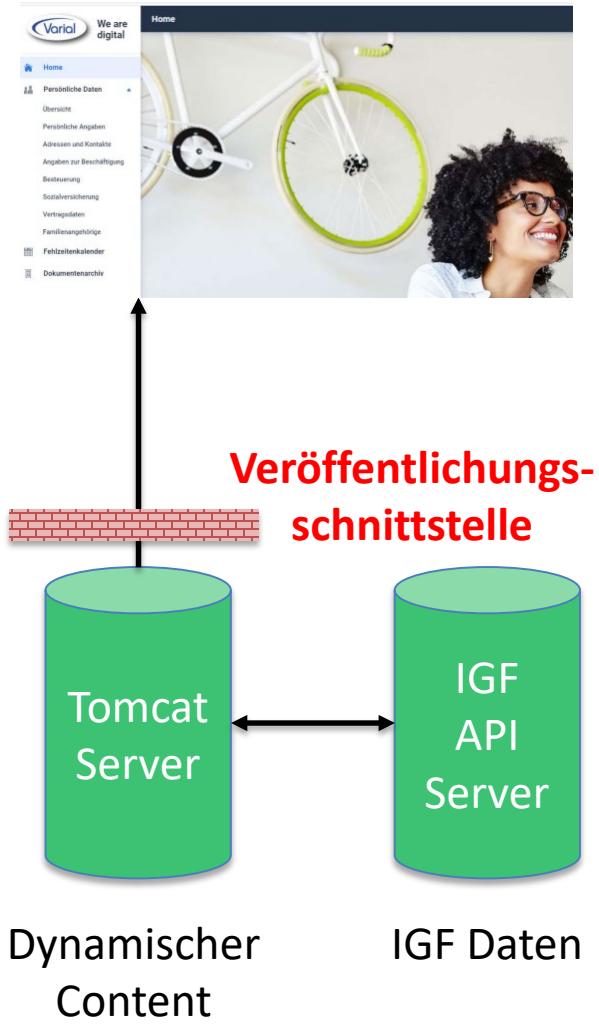
- Directory Listing abschalten
  - `<Set name="directoriesListed">true</Set>` in *jetty-download-context.xml*
- Windows Firewall auf API-Server aktivieren
  - Bei Verwendung der Java Variante, ausschließlich Verbindungen vom Frontend-Server bzw. IGF-Clients auf API Server erlauben
- (@Infor) UUIDs an Stelle von bekanntem Namensschema oder Authentifizierung im Download Server

Sichere Veröffentlichung des IGF Self-Service Portals

- Angular Single-Page App
- Vollständige Verarbeitung per Javascript im Browser
- Direkte Kommunikation mit IGF-Backend per API



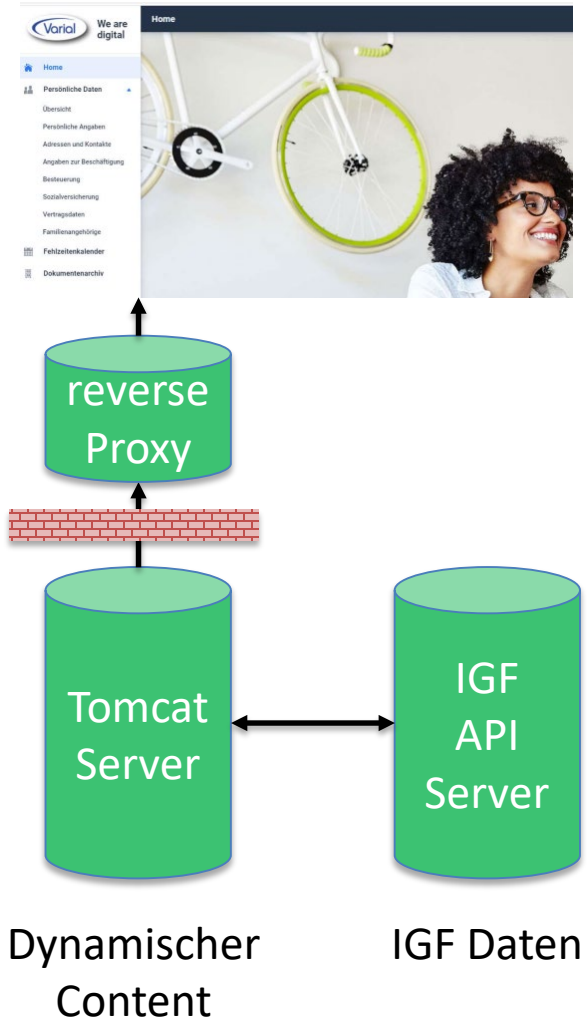
- Server-basierte Java Anwendung auf Basis des SpringBoot Frameworks
- Tomcat Web-Application Server
- Kapselung der API-Kommunikation durch Verarbeitung auf dem Server
- weiterhin moderne JS Anwendung mit Möglichkeit der asynchronen Kommunikation per Websocket
- Möglichkeit der Anpassung von Designs, Hintergründen, etc.
  - ➢ von Infor aktuell unterstütze Variante (mind. seit 2.91.1)



	Pro	Kontra
JS - Variante	• „leichtgewichtig“ da Verarbeitung im Browser	• Komplexes Proxy-Szenario aufgrund verschiedener Routen • API-Kommunikation kaum zusätzlich absicherbar
Java - Variante	• Zusätzliche (Proxy) Authentifizierung möglich	• Komplexer Technologie Stack • Anfälligkeit für Sicherheitslücken ➢ Log4j ➢ Spring4Shell

- Zusätzliche Möglichkeiten zur Erhöhung der Sicherheit per Web-Application-Firewall (WAF) im Reverse Proxy

- Aufgrund der synchronen Kommunikation mit dem Application Server kann eine zusätzliche Authentifizierung erfolgen



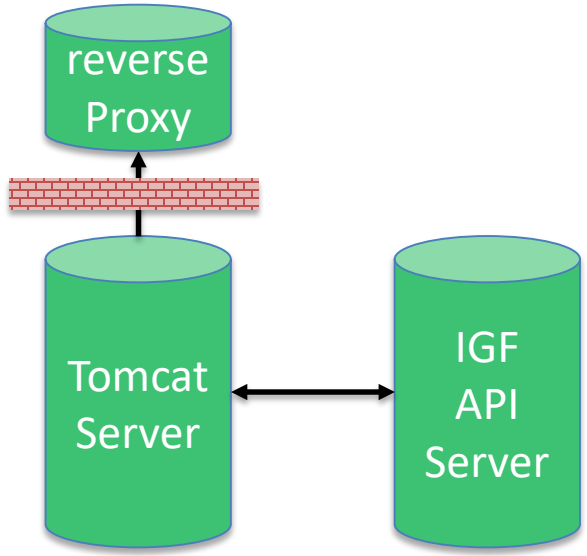
- Erweiterung der Tomcat *server.xml* um einen weiteren Connector:

```
<Connector protocol="HTTP/1.1"
           connectionTimeout="20000"
           port="8088"
           proxyName="extern.firma.de"
           proxyPort="443"
           scheme="https"
           secure="true" />
```

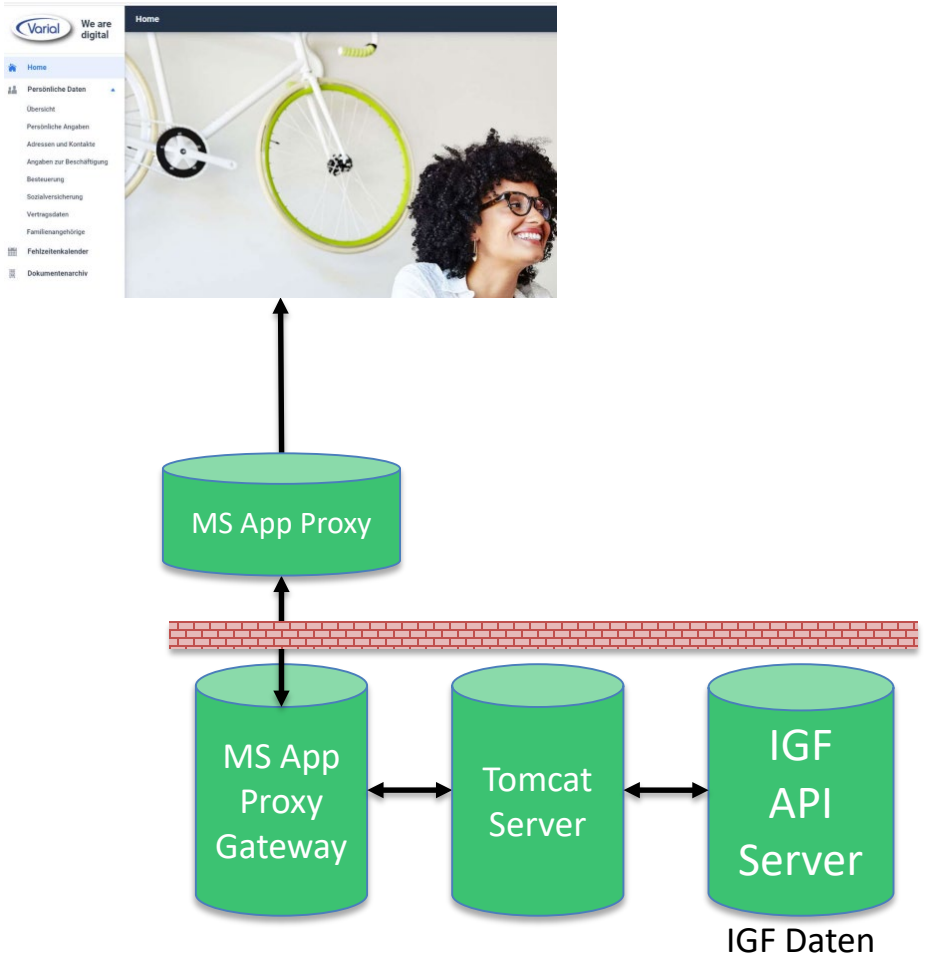
- Reverse-Proxy (Bsp. Nginx):

```
location /igf-selfservice/{
 proxy_pass http://intern.firma.de:8088\
            /igf-selfservice
}
```

- Bei Verwendung des **tomcat:9.0** Docker Images auf Java 11 Basis muss die Datei *WEB-INF\lib\feign-core-8.18.0.jar* aus dem WAR-File gelöscht werden (z.B. per 7zip Manager)



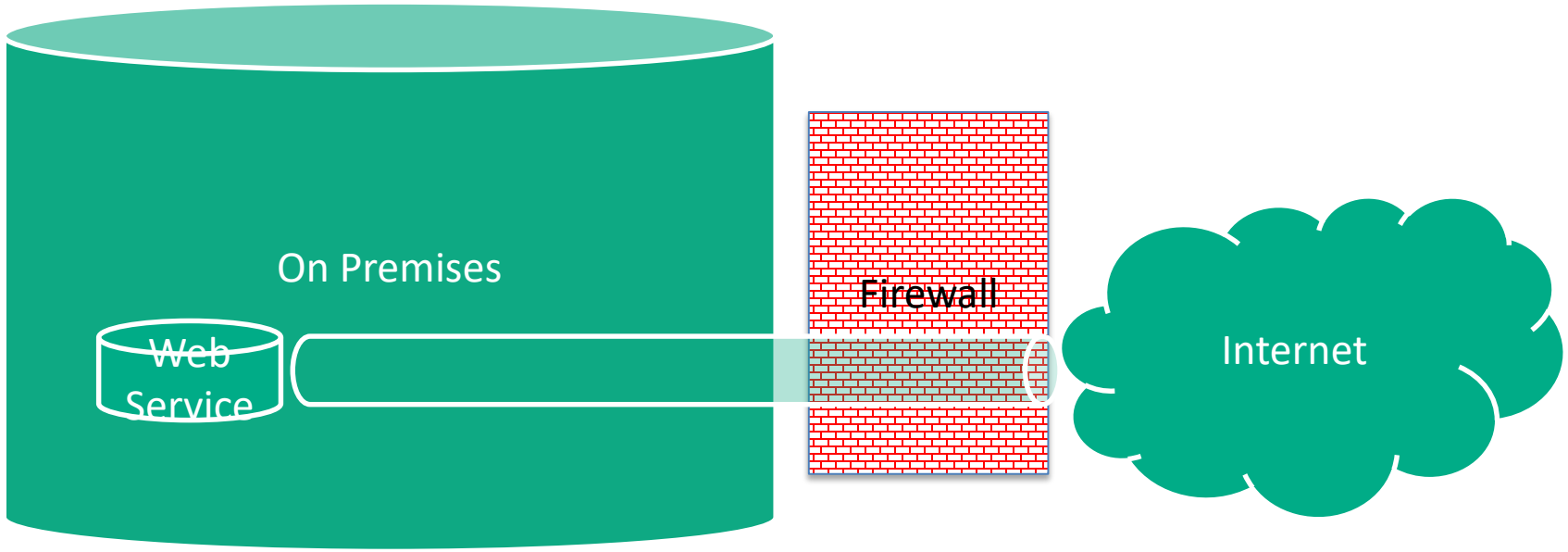
- Nutzung des MS Azure Application Proxys zur Erhöhung der Anwendungssicherheit (AzureAD Vorauthentifizierung)
  - ➢ nur zugewiesene Benutzer können die Anwendung extern Nutzen (Zero-Trusted-Networks Konzept)



Anhang: Konzepte zur Sicheren Veröffentlichung von Intranet Anwendungen

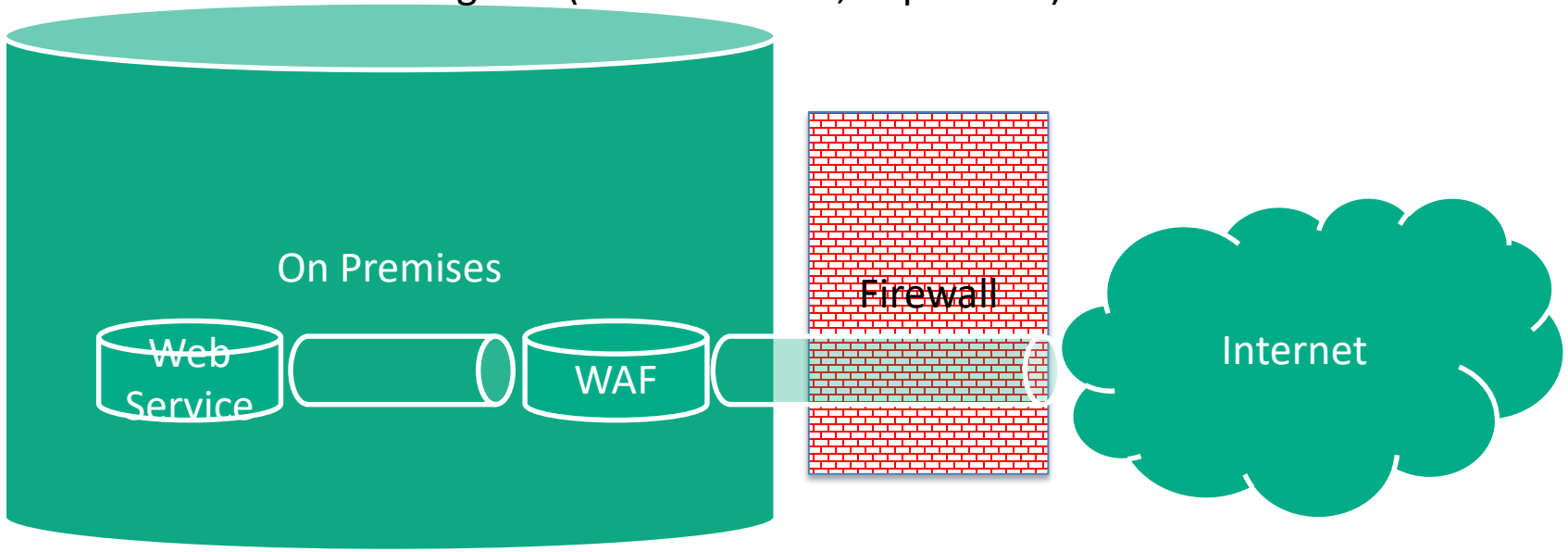
- VPN-Verbindung und „quasi-lokaler“ Zugriff
- Direkte Port-Weiterleitung in der Unternehmensfirewall
- Reverse-Proxy, optional mit Web-Application-Firewall (WAF)
- Cloud-basierte Tunnel

- Direkte Port-Weiterleitung in der Unternehmensfirewall
- !!! Achtung keinerlei Schutzwirkung !!!

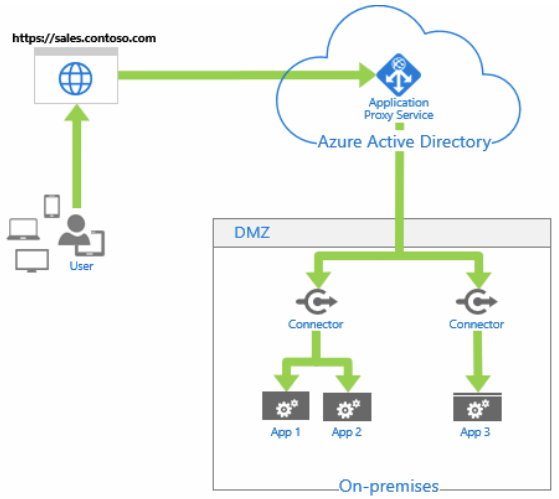


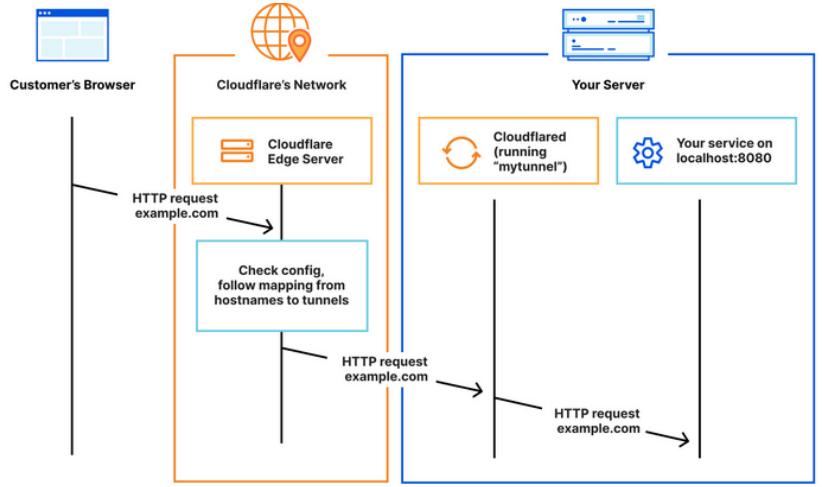
- Reverse-Proxy, optional mit Web-Application-Firewall (WAF)
  - Apache: mod_security
  - Nginx: NAXSI

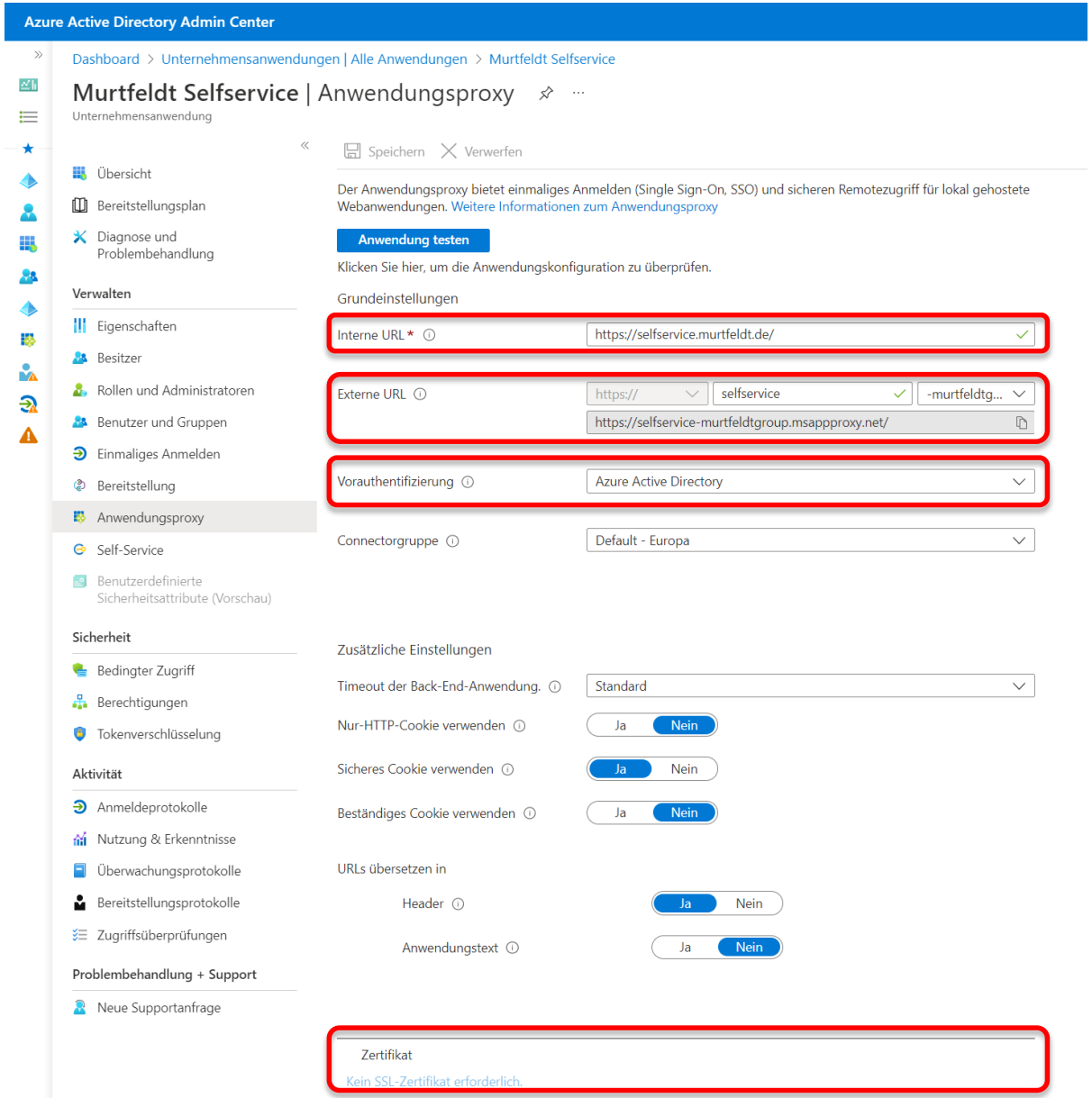
- WAF evtl. in Firewall integriert (z.B. OPNsense, Sophos XG)



- Cloud-basierte Tunnel:
  - Azure Application Proxy (mind. P1 Lizenz)
  - Cloudflare Tunnel (Teil des kostenlosen Cloudflare Zero Trust Free Plan)






Azure Active Directory Admin Center
Dashboard > Unternehmensanwendungen | Alle Anwendungen > Murtfeldt Selfservice
Murtfeldt Selfservice | Anwendungsproxy
Unternehmensanwendung
Übersicht
Bereitstellungsplan
Diagnose und Problembehandlung
Verwalten
Eigenschaften
Besitzer
Rollen und Administratoren
Benutzer und Gruppen
Einmaliges Anmelden
Bereitstellung
Anwendungsproxy
Self-Service
Benutzerdefinierte Sicherheitsattribute (Vorschau)
Sicherheit
Bedingter Zugriff
Berechtigungen
Tokenverschlüsselung
Aktivität
Anmeldeprotokolle
Nutzung & Erkenntnisse
Überwachungsprotokolle
Bereitstellungsprotokolle
Zugriffsüberprüfungen
Problembehandlung + Support
Neue Supportanfrage
Speichern
Verwerfen
Der Anwendungsproxy bietet einmaliges Anmelden (Single Sign-On, SSO) und sicheren Remotezugriff für lokal gehostete Webanwendungen. Weitere Informationen zum Anwendungsproxy
Anwendung testen
Klicken Sie hier, um die Anwendungskonfiguration zu überprüfen.
Grundeinstellungen
Interne URL *
https://selfservice.murtfeldt.de/
Externe URL
https://
selfservice
-murtfeldtg...
https://selfservice-murtfeldtgroup.msappproxy.net/
Vorauthentifizierung
Azure Active Directory
Connectorgruppe
Default - Europa
Zusätzliche Einstellungen
Timeout der Back-End-Anwendung.
Standard
Nur-HTTP-Cookie verwenden
Ja
Nein
Sicheres Cookie verwenden
Ja
Nein
Beständiges Cookie verwenden
Ja
Nein
URLs übersetzen in
Header
Ja
Nein
Anwendungstext
Ja
Nein
Zertifikat
Kein SSL-Zertifikat erforderlich.