



INFOTECH
[IT & Communication]

DANKE #30
FÜR
INSPIRIERENDE
AUSGABEN

30. InfoTechDay

HERZLICH WILLKOMMEN!

Sicherer Zugriff im Wandel – moderne Zugriffsarchitekturen

DI Franz Strasser, Systems Engineer
Markus Günzinger, Systems Engineer



- **Interne Ressourcen:**
 - (sensible) Dateien
 - Geräte (Drucker, Dongles, etc.)
 - Diverse Web-Apps
 - Legacy Applikationen
 - Cloud Services?
- **Veränderte Gegebenheiten:**
 - Home / Remote Office
 - Bring your own Device / „Zero Trust“
 - Datenschutz / NIS2
 - Cybersicherheit



- **Starke Einschränkungen (z. B. Home Office nicht/eingeschränkt möglich)**
- **Unsichere Varianten (Web-App, RDP usw. von extern erreichbar)**
- **Nicht ausreichend geschützte Dienste extern verfügbar (z. B. kein MFA)**
- **(Client-) VPN-Lösungen (... auf privatem Endgerät?)**



Ziel

- **Sicherer Zugriff ...**
- **... auf alle verschiedenen Ressourcen ...**
- **... auch von „unbekannten“ Geräten ...**
- **... von überall aus.**



Entra Application Proxy

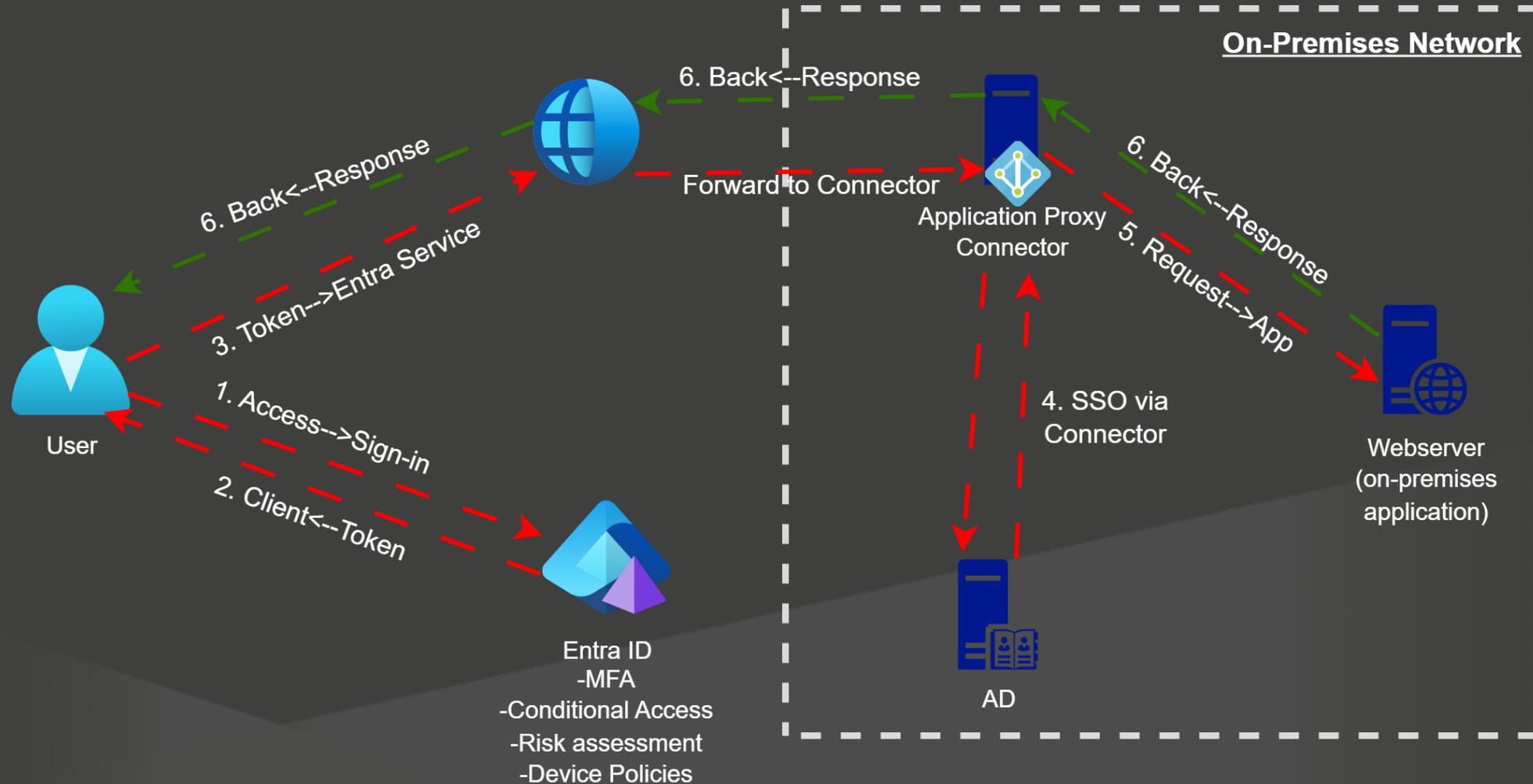


Was ist Entra Application Proxy?

- **Lokaler Connector für Remote-Zugriff auf interne Web-Apps**
- **Kein VPN/Programm notwendig**
- **Keine eingehenden Ports**
- **Entra ID Auth (MFA, Conditional Access, Geräte-Compliance, ...)**
- **Einfache Hybrid-Szenarien**
- **Entra ID P1 Lizenz**



Verbindungsaufbau – Entra Application Proxy



Entra Private Access



Was ist Entra Private Access?

- **Lokaler Connector + Client auf allen Endgeräten**
- **Remotezugriff auf interne Ressourcen (TCP/UDP)**
- **Teil von Entra Global Secure Access**
- **Entra ID P1 + Entra Private Access Lizenz**

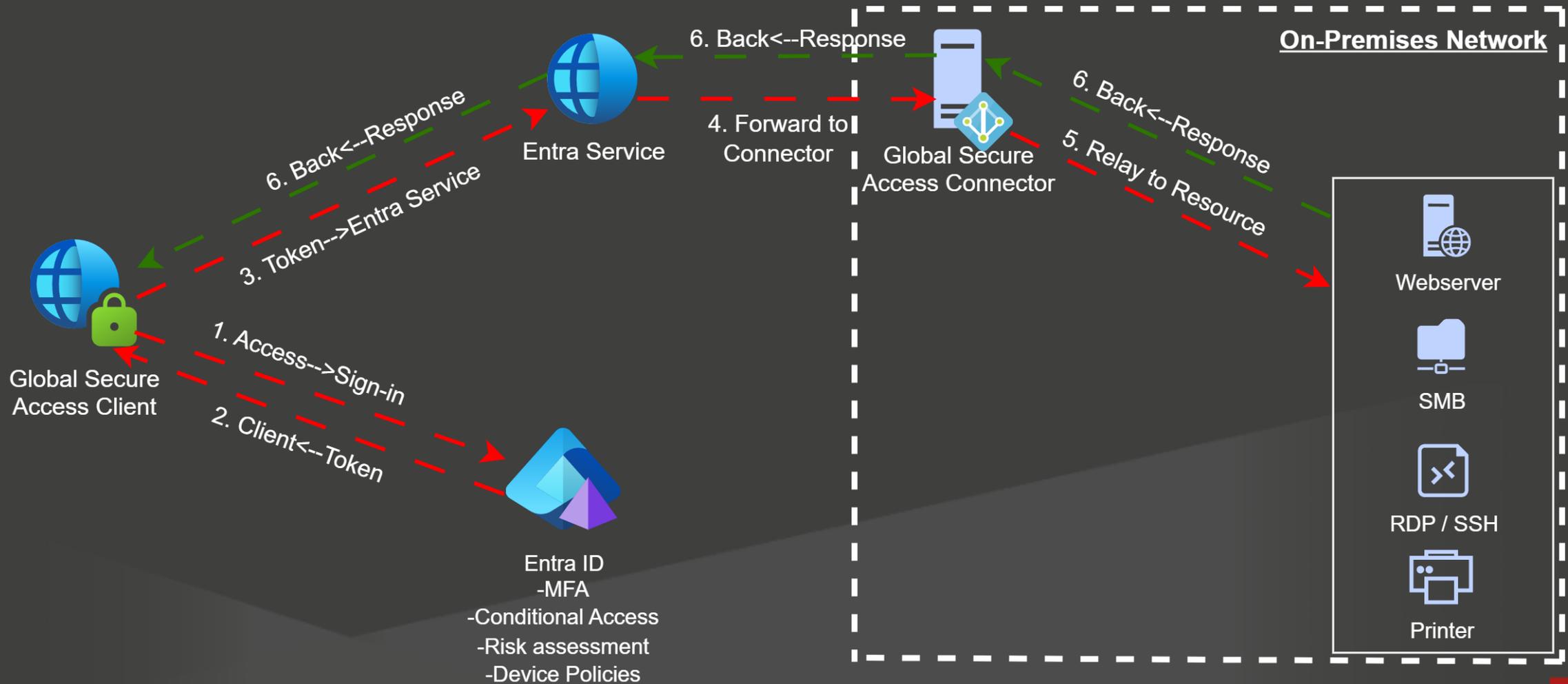


Was ist Entra Private Access?

- **Kein klassisches VPN**
- **Authentifizierung über EntraID (MFA, Conditional Access, Geräte-Compliance, ...)**
- **Zero Trust Prinzip – granularer Zugriff statt vollem Netzwerk**



Verbindungsaufbau - Entra Private Access

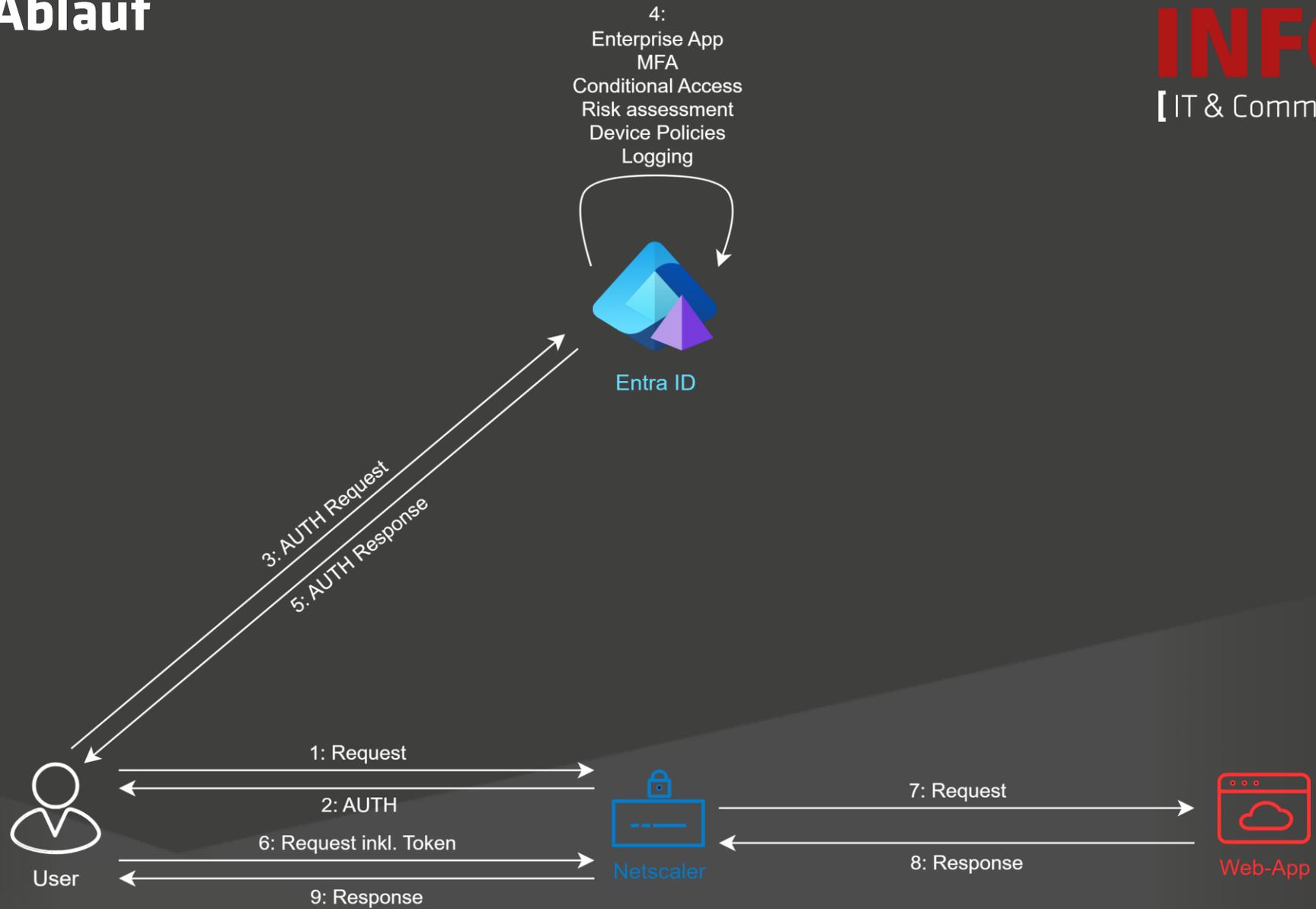


Netscaler ADC



- **Citrix Netscaler (VPX) in DMZ**
- **SAML- oder OIDC-Authentifizierung gegen IdP (z. B. Entra ID)**
- **Zugriff auf Ressourcen nach Authentifizierung und Authorisierung**
- **Vorwiegend für Web-Anwendungen**
 - Weitere Möglichkeiten für andere Ressourcen

Netscaler Ablauf

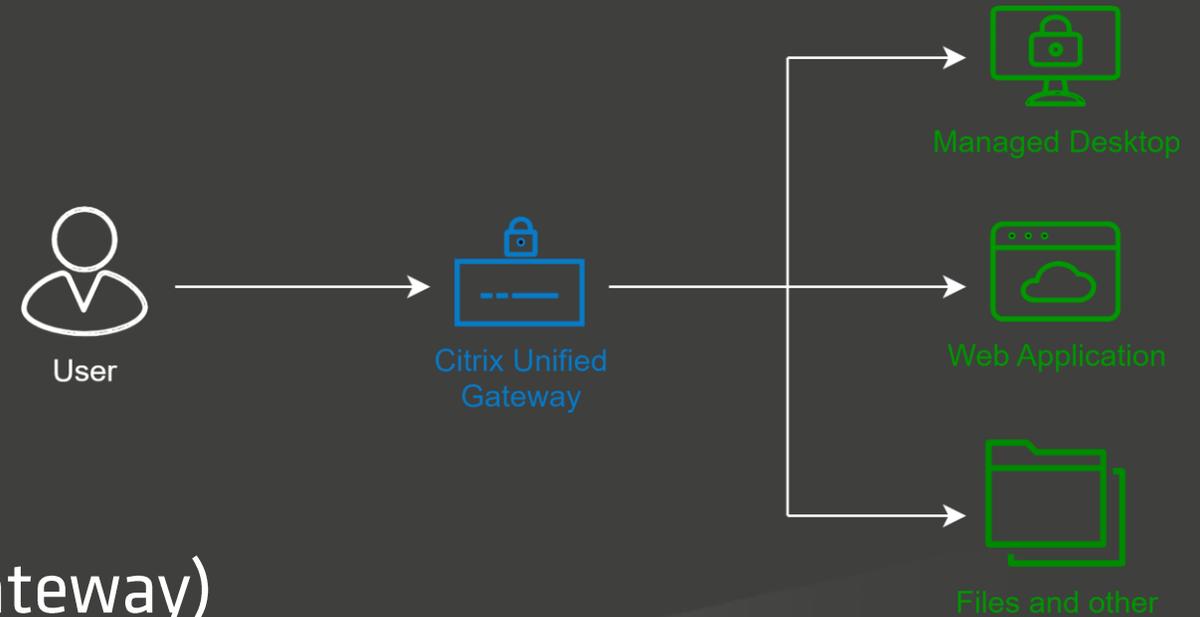


- **Netscaler verlangt Authentifizierung vor jeglichem Zugriff**
 - SAML | OIDC
 - RADIUS | WEBAUTHN (FIDO2)
- **Authentifizierung und Authorisierung beim IdP**
 - Inkl. MFA, Conditional Access, Berechtigungen, etc.
- **Wenn erfolgreich, Zugriff auf Ressourcen**
 - SSO zur Authentifizierung im Backend



■ Citrix Gateway für ...

- Zugriff auf VDI-Umgebungen
- VPN-Tunnel (Applikationsebene)
- All-in-One Lösung (mit Unified Gateway)



▪ **Entra Private Access**

- Cloud-nativ
- Identity-First, granular pro App
- Keine DMZ nötig
- Automatische Skalierung
- Vollständige VPN-Alternative

▪ **Netscaler**

- Self-Hosted (unabhängig)
- Flexibel und anpassbar
- Clientless
- Diverse Sicherheitsfeatures
- Keine „Pro-User“ Lizenz
(Bereitstellung von öffentlichen Diensten)



Fragen?

Sicherer Zugriff im Wandel – moderne Zugriffsarchitekturen

DI Franz Strasser, Systems Engineer

Markus Günzinger, Systems Engineer





INFOTECH
[IT & Communication]

Ihr Systemhaus.

