Exchange User Group
{Online Edition}

19. August 2021

Meetup Q3 2021

- Talk 1 – Exchange Server – Komponenten für den sicheren Zugriff

  Thomas Stensitzki

- Talk 2 - Hunting Basic Authentication in Exchange Online

  Andres Bohren

Die Talks werden aufgezeichnet. The sessions will be recorded.

Exchange Server – Komponenten für den sicheren Zugriff

Thomas Stensitzki

Thomas Stensitzki

Enterprise Consultant
Granikos GmbH & Co. KG

MVP | MCT Regional Lead | MCSM

@stensitzki
thomas.stensitzki@granikos.eu

Exchange Server – Protokolle

E-Mail-Versand

- SMTP
  - Server-zu-Server (MTA) Kommunikation
    - TCP 25, STARTTLS initiiert den Aufbau einer verschlüsselten TLS-Verbindung
    - TCP 465, TLS-abgesicherte SMTP-Verbindung, nicht mehr RFC-compliant
      - Nutzung von Exchange Server zur Frontend-Backend-Kommunikation für TCP 587 (Link)

    → https://go.granikos.eu/IANAPorts

  - Client-zu-Server Kommunikation
    - TCP 465, TLS-abgesicherte SMTP-Verbindung, nicht mehr RFC-compliant
    - TCP 587, TLS-abgesicherte SMTP-Verbindung mit Authentifizierung

Exchange Server – Protokolle

Postfach- und Serverzugriff

- HTTP/S
  - Server-zu-Server, Client-zu-Server
    - TCP 80, unverschlüsselt
    - TCP 443, TLS-verschlüsselt
- POP3
  - Client-zu-Server
    - TCP 110, unverschlüsselt
    - TCP 995, TLS-verschlüsselt
- IMAP4
  - Client-zu-Server
    - TCP 143, unverschlüsselt
    - TCP 993, TLS-verschlüsselt

Exchange Server – Protokolle

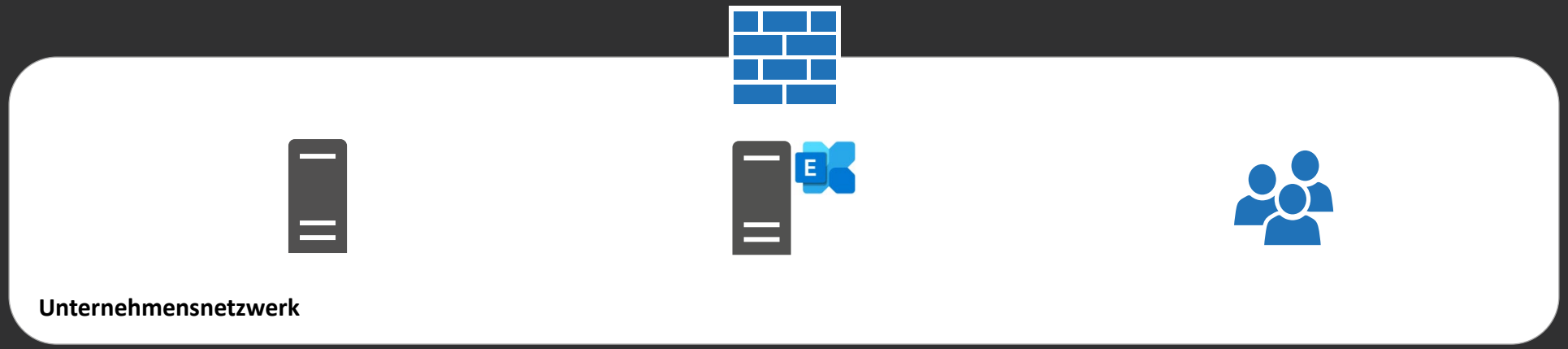
Exchange Server HTTPS

- HTTPS
  - AutoDiscover
  - MAPI
  - Exchange Web Services (/EWS)
  - ActiveSync (/Microsoft-Server-ActiveSync)
  - Offline Adressbuch (/OAB)
  - Outlook on the Web (/OWA)
  - Admin Center (/ECP)
  - REST (/API)
  - PowerShell
  - RPC

SMTP

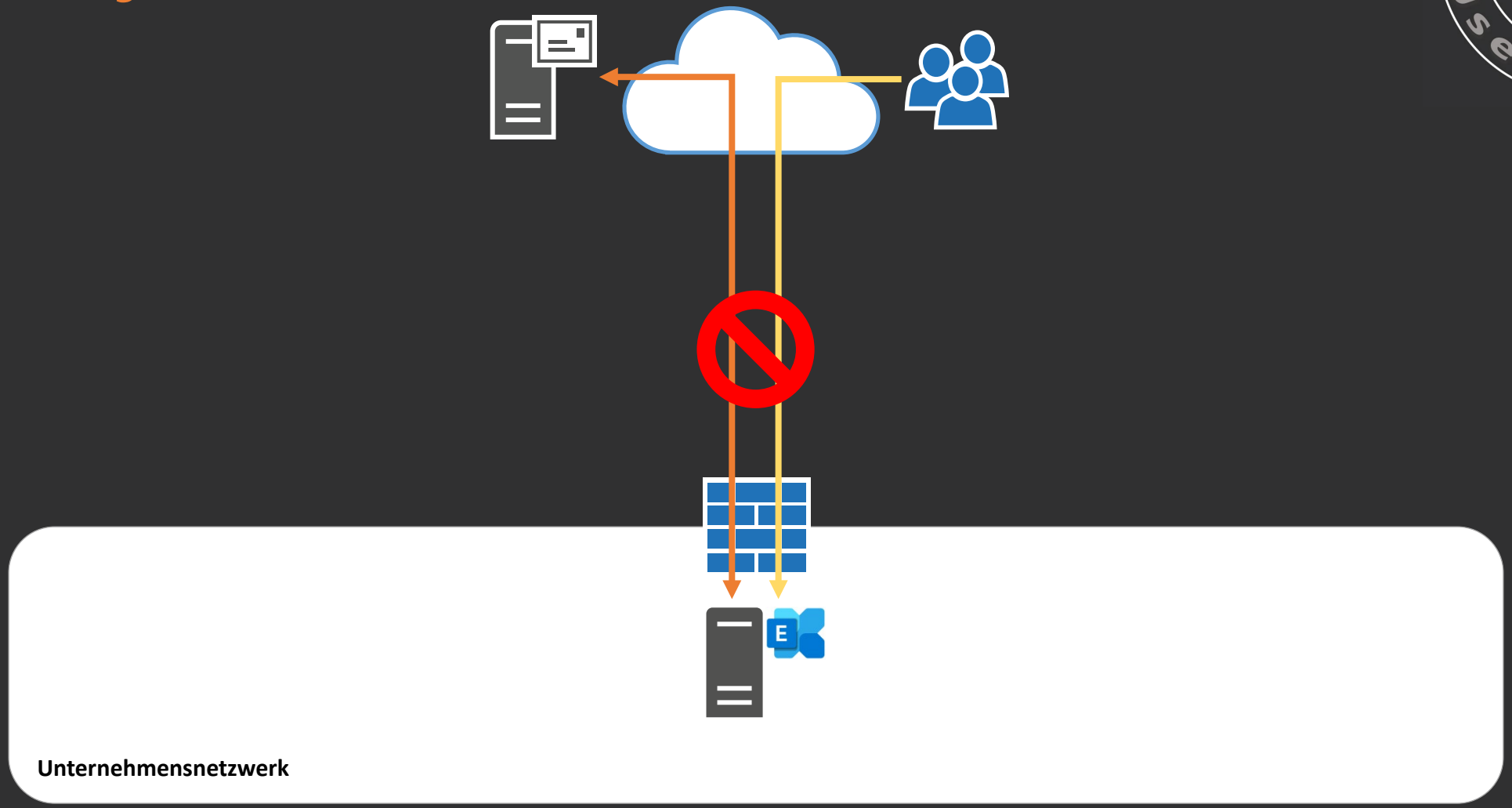
Exchange Server Protokolle

Exchange Server – Komponenten



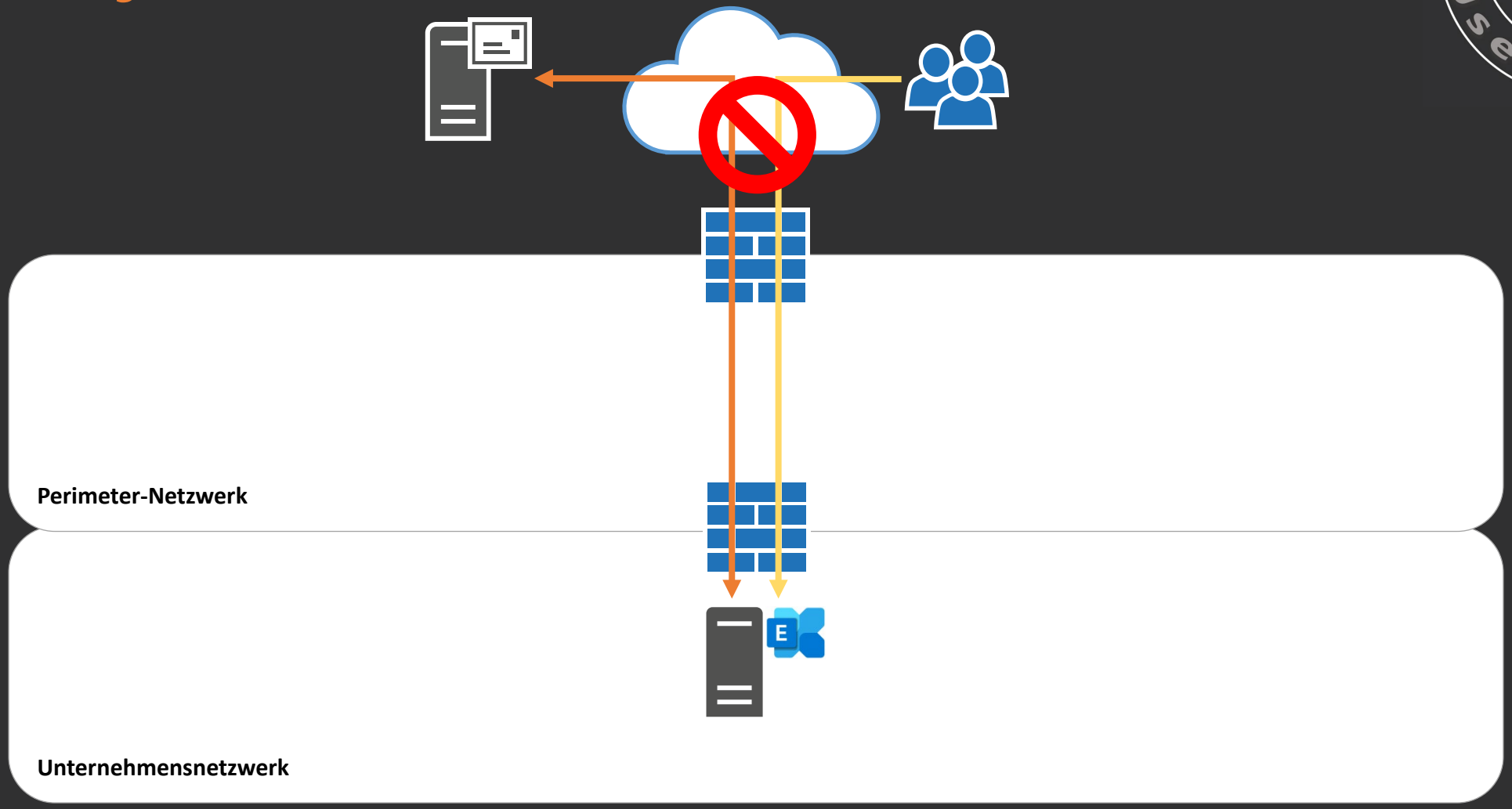
Exchange Server – Komponenten

Direkter Zugriff



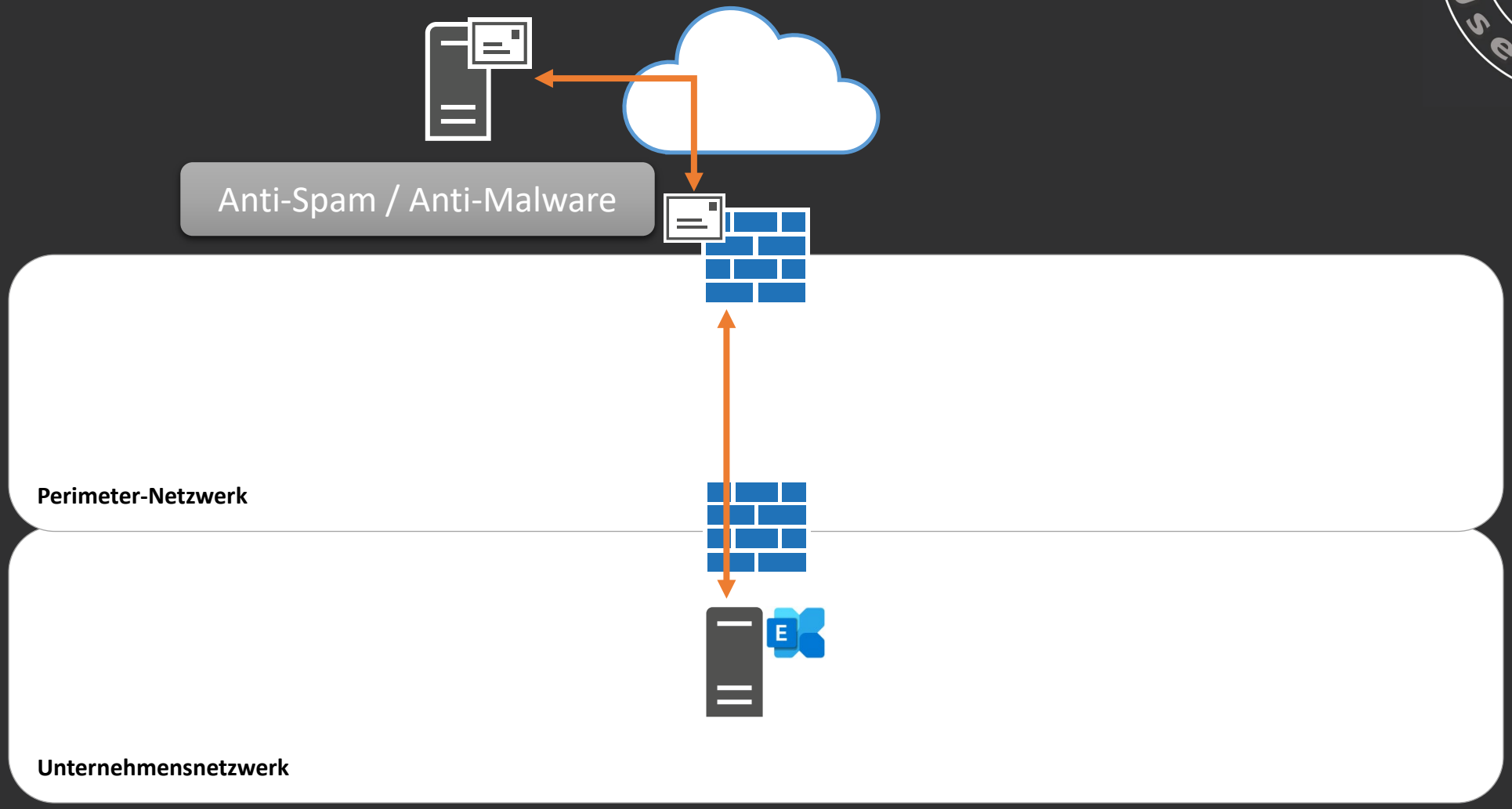
Exchange Server – Komponenten

Direkter Zugriff durch ein Perimeter-Netzwerk



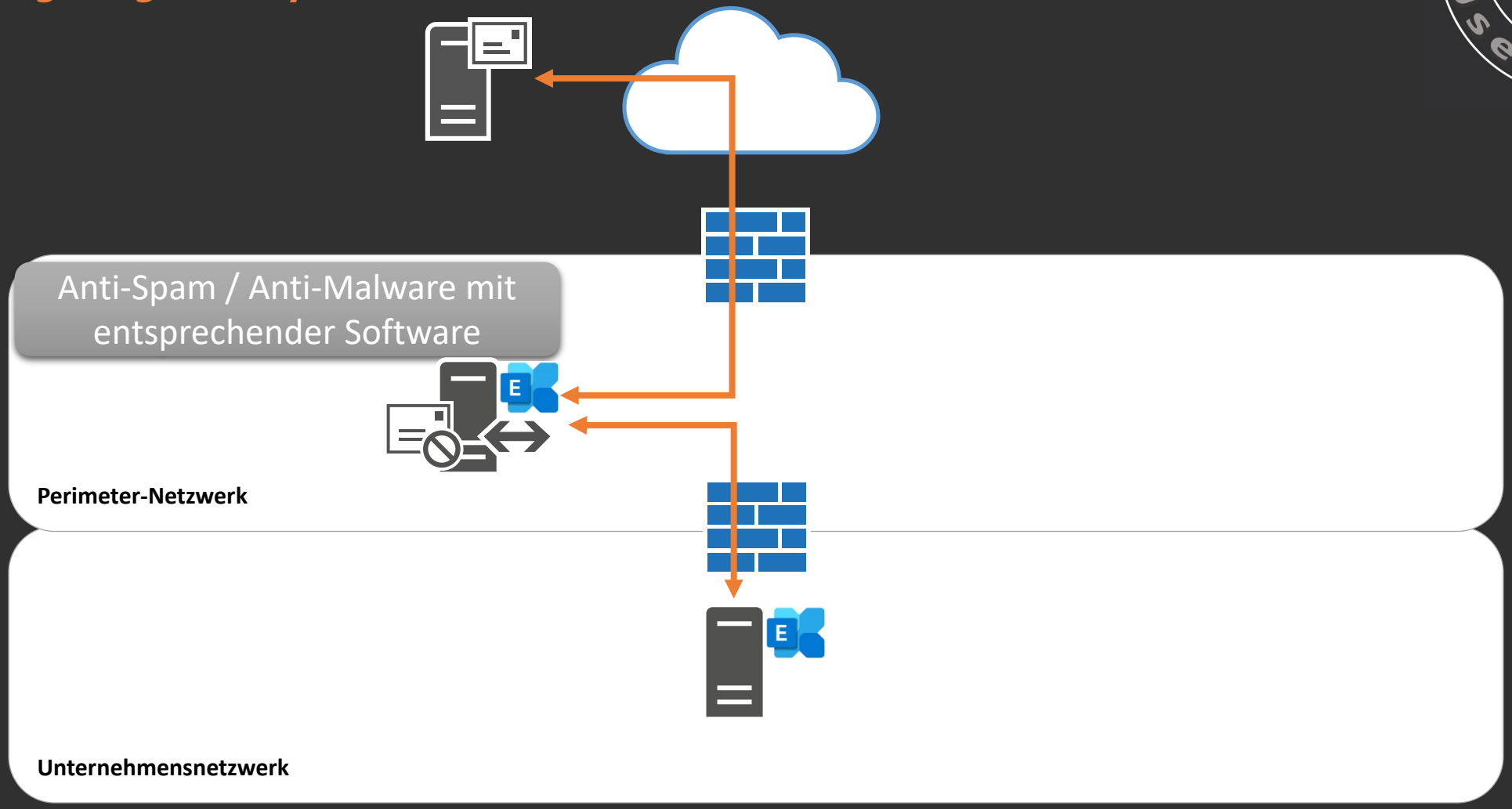
Exchange Server – Komponenten

Internet-Firewall als MTA



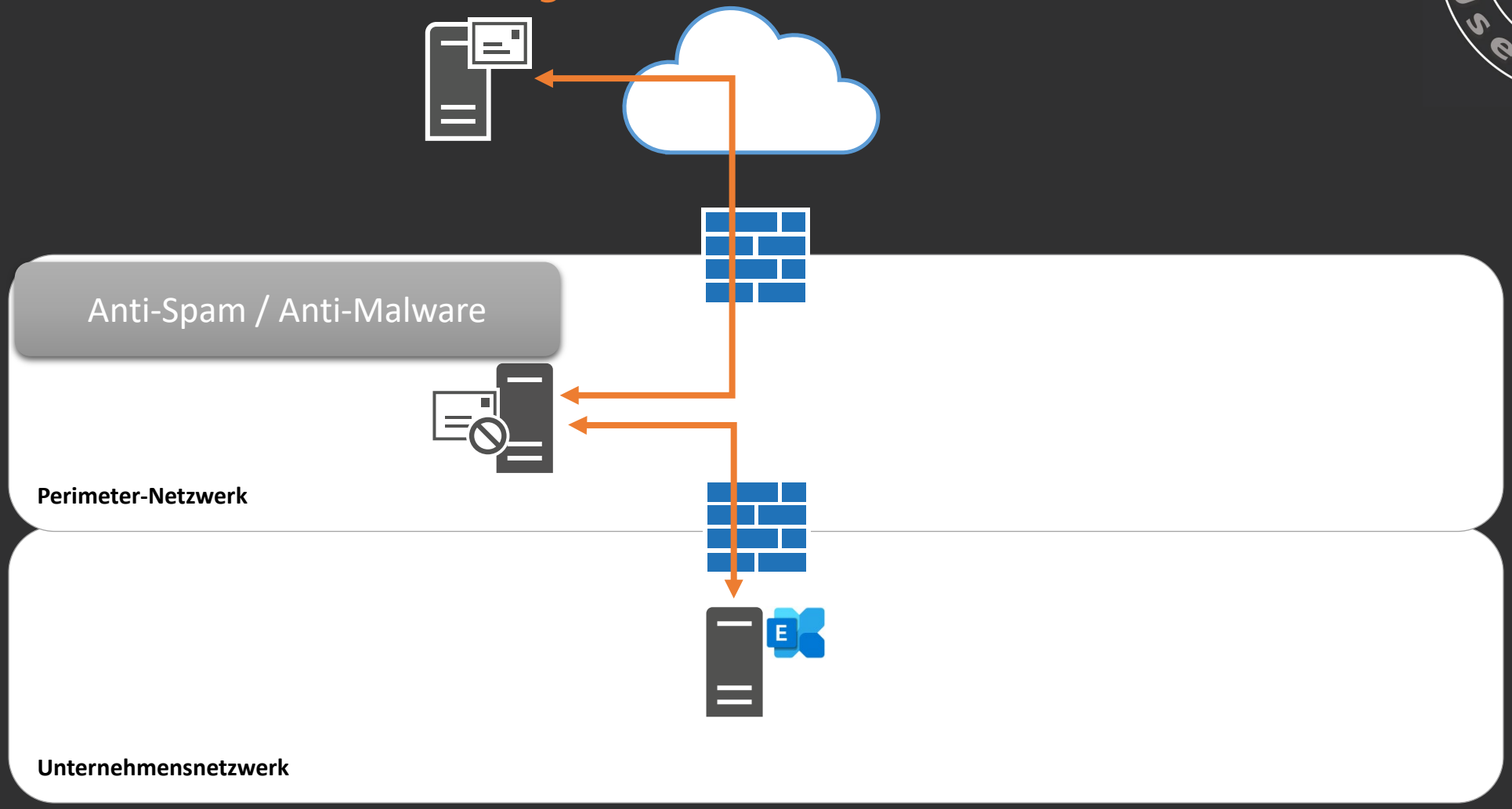
Exchange Server – Komponenten

Exchange Edge Transport Rolle



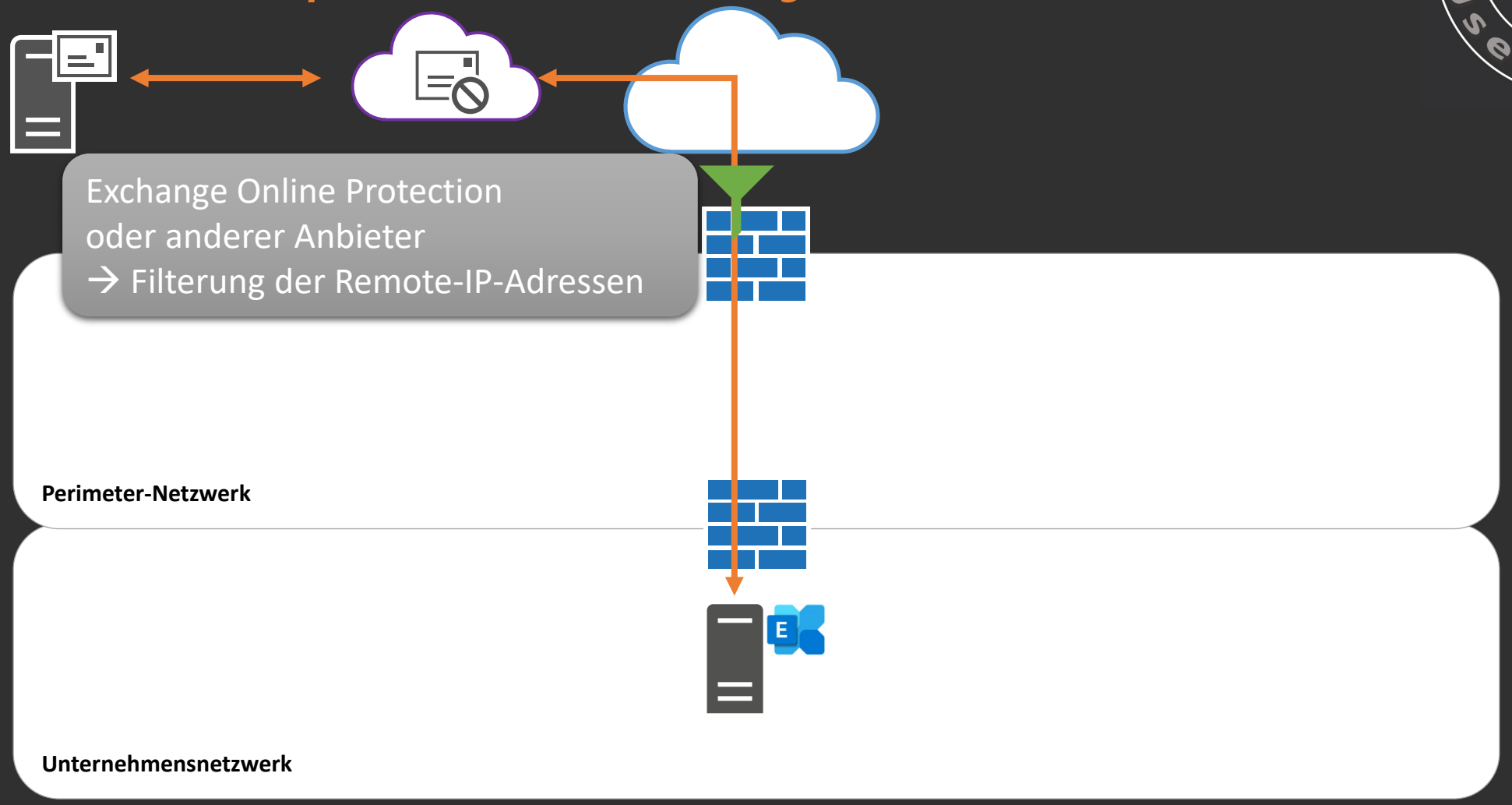
Exchange Server – Komponenten

Lokale Software- / Hardwarelösung



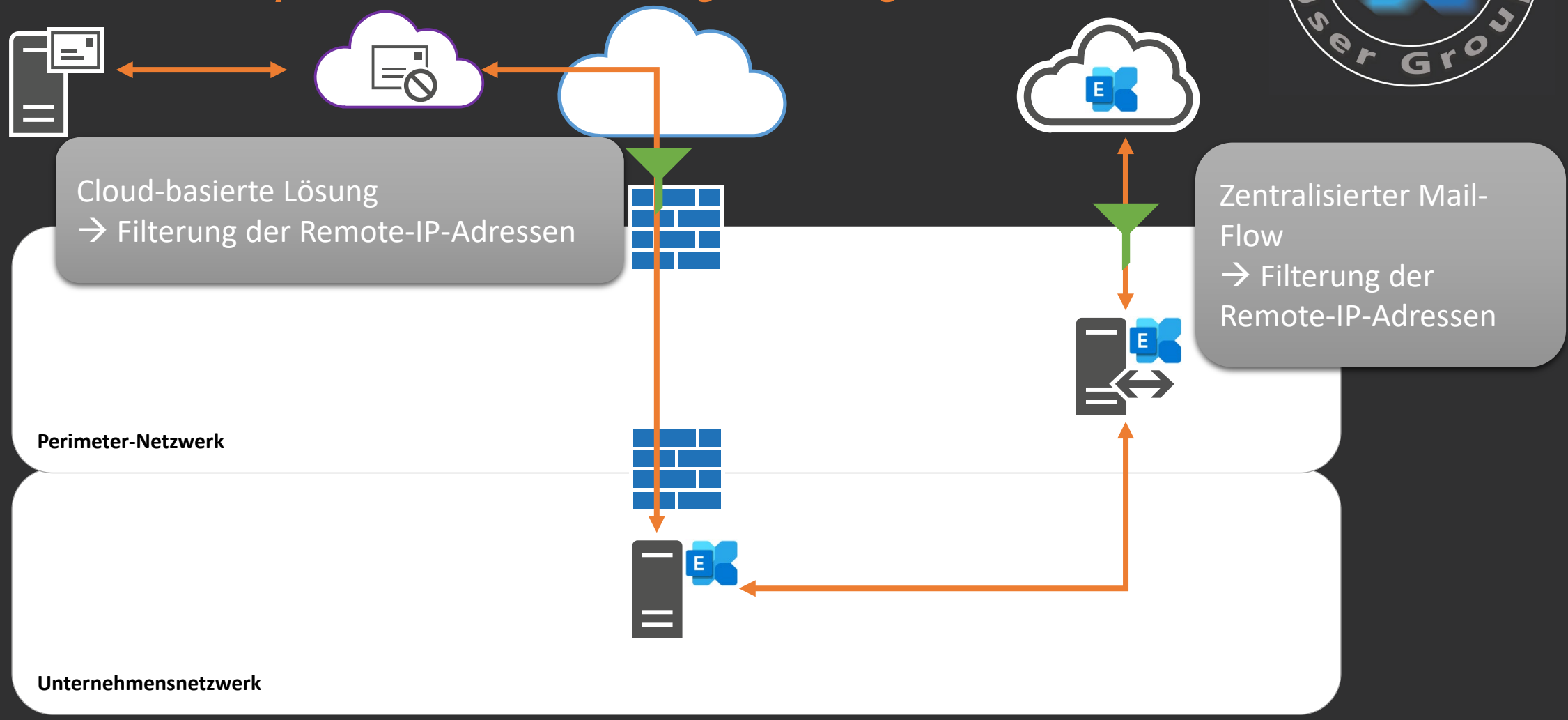
Exchange Server – Komponenten

Cloud-basierte Anti-Spam/Anti-Malware Lösung



Exchange Server – Komponenten

Cloud-basierte Anti-Spam/Anti-Malware Lösung + Exchange Online



Cloud-Anbieter für Mail-Filterung

- Exchange Online Protection
- Gemakom
- Mimecast
- NoSpamProxy
- ProofPoint
- SecuMail
- Sophos
- SpamTitan
- …

SMTP

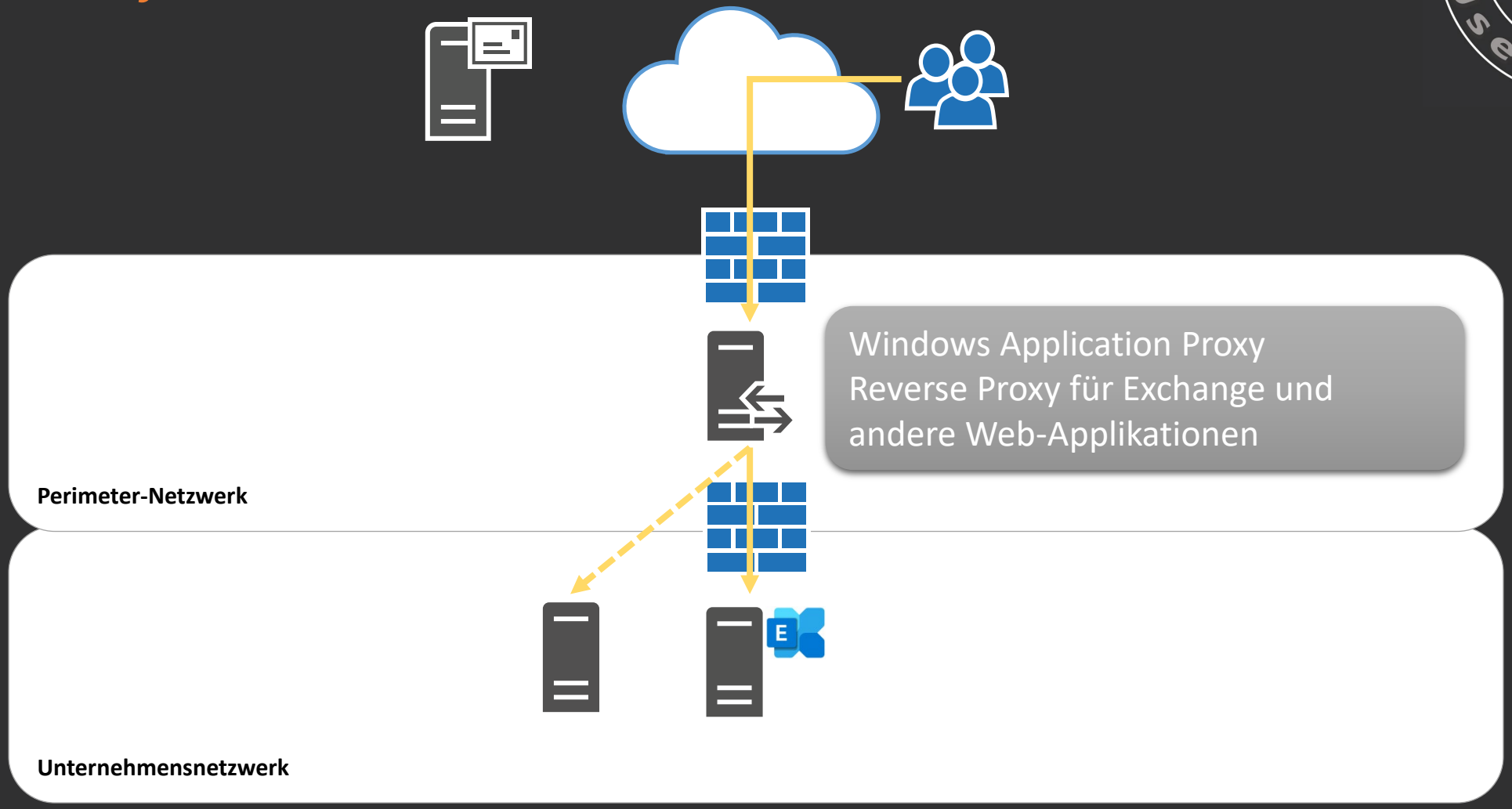
Welche Implementierung nutzt ihr?

HTTPS

Exchange Server Protokolle

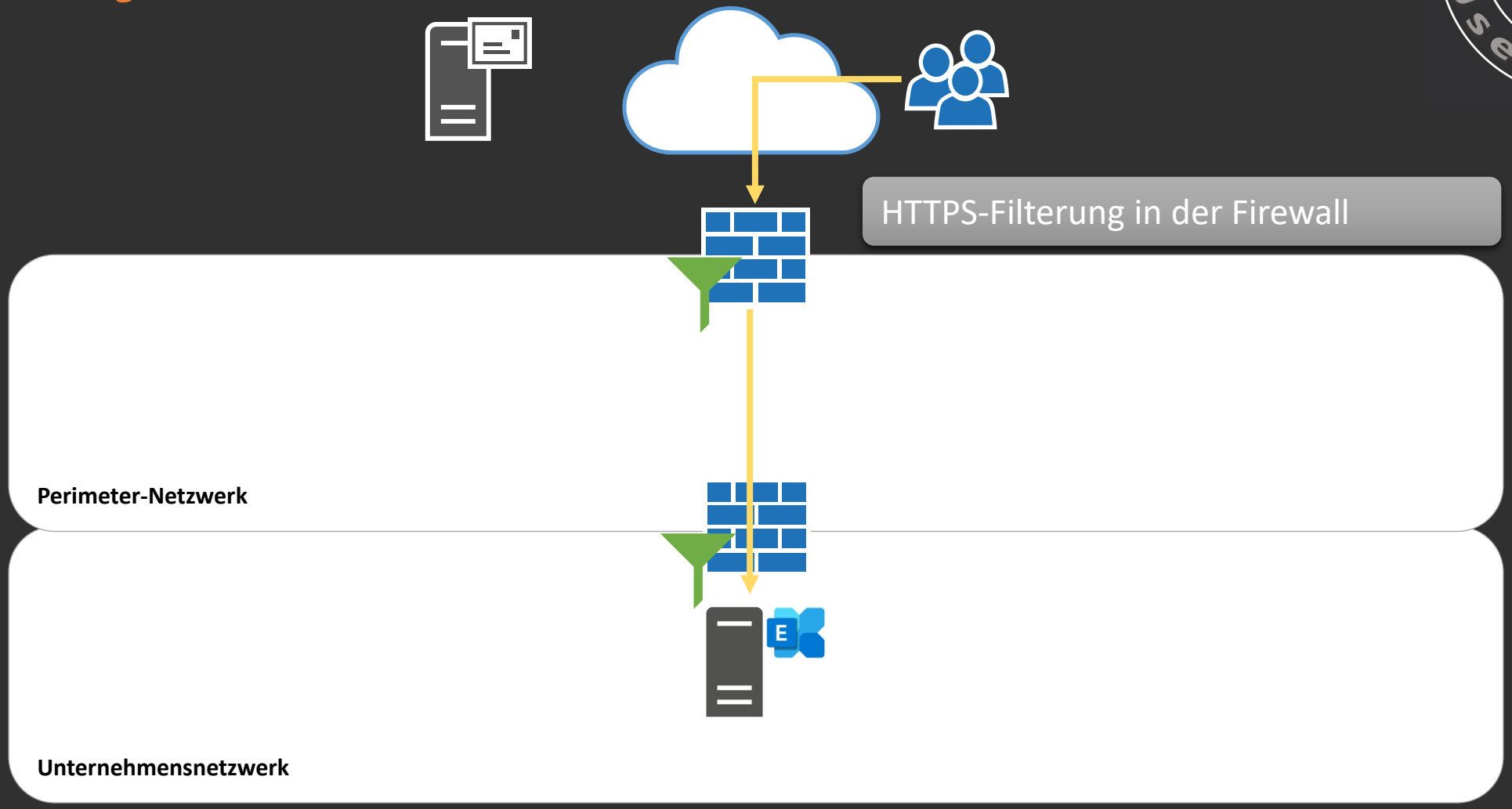
Exchange Server – Komponenten

Reverse Proxy im Perimeter-Netzwerk



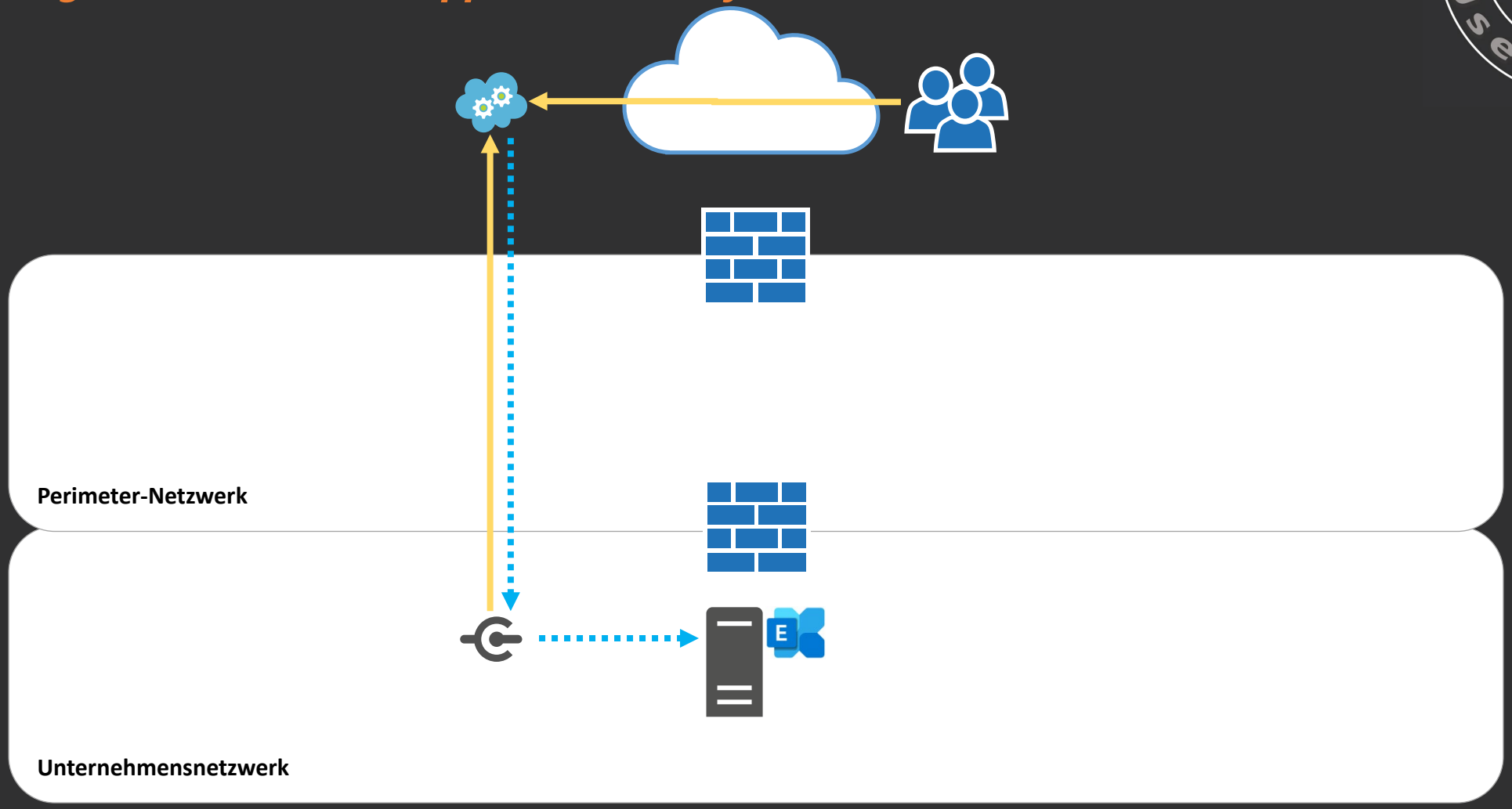
Exchange Server – Komponenten

Direkter Zugriff durch ein Perimeter-Netzwerk



Exchange Server – Komponenten

OWA Zugriff mit Azure AD Application Proxy



HTTPS

Welche Implementierung nutzt ihr?

Authentifizierung

Authentifizierung

- Eliminierung der Basic-Authentifizierung
- Föderierte Authentifizierung mit AD FS
- Hybrid Modern Authentication
  - Erfordert Exchange Hybrid
  - Bietet Azure MFA und Conditional Access
- Multi-Faktor-Authentifizierung
- Zertifikats-basierte Authentifizierung

Authentifizierung

Welche Implementierung nutzt ihr?


Exchange
EXUSG
User Group

Ressourcen

- Exchange Server 2016 + 2019 Maul Flow With Ports
- Service Name and Transport Protocol Port Number Registry
- Remote access to on-premises applications through Azure AD Application Proxy
- Hybrid modern authentication overview and prerequisites for using it with on-premises Skype for Business and Exchange servers

Hunting Basic Authentication in Exchange Online

Andres Bohren

Exchange User Group

Exchange User Group

Organisatorisches

Exchange
User Group

Nächster Termin: 4. November 2021

Homepage: https://exusg.de

Twitter: @exusg #exusg