Vertrouw niets, Controleer alles

Beveiligen van de digitale ruimte in een wereld waarin alles met alles verbonden is

Verschuivende bedreigingen en grenzen

- De tijd dat data zich enkel binnen de muren van systemen bevindt is radicaal voorbij
- Alle bestaande IT-grenzen zijn nagenoeg vervaagd
- Van netwerk perimeter beveiliging naar Zero-Trust en identiteit beveiliging
- Alles is data, alles is software, alles gevirtualiseerd
- Strategische infrastructuur draagt bij aan data centrisch perspectief

Eigenschappen Digitale Ruimte

- Een gemengde architectuur
  - Concrete basis of infrastructuur met virtuele uitbreidingen
- Een interface architectuur
  - Naar technische componenten binnen dezelfde infrastructuur als in verbinding met mensen en technologie buiten de eigen infrastructuur
  - Actieve input- en outputstromen
- Architectuur van onderlinge verbindingen
  - Hoofddoelstelling niet inhoud statisch herbergen maar functioneren als uitwisselingssysteem (of verbindingssysteem) tussen hier en elders.
  - Het hier is net zo grenzeloos zoals elders dat ook is….

Architectuur van de Digitale Ruimte

- Gemengde architectuur
- Interfacearchitectuur
- Architectuur van onderlinge verbindingen
- Van netwerk perimeter naar Zero-Trust en identiteit beveiliging
- Security- en defense architectuur

Klassieke opzet met DMZ

5G

Edge/
Fog

ODC

AWS

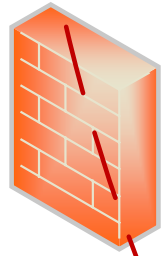
O365

Google

Azure

Salesforce

Gebruiker



AD/
LDAP

Service Directory

SSH
>_

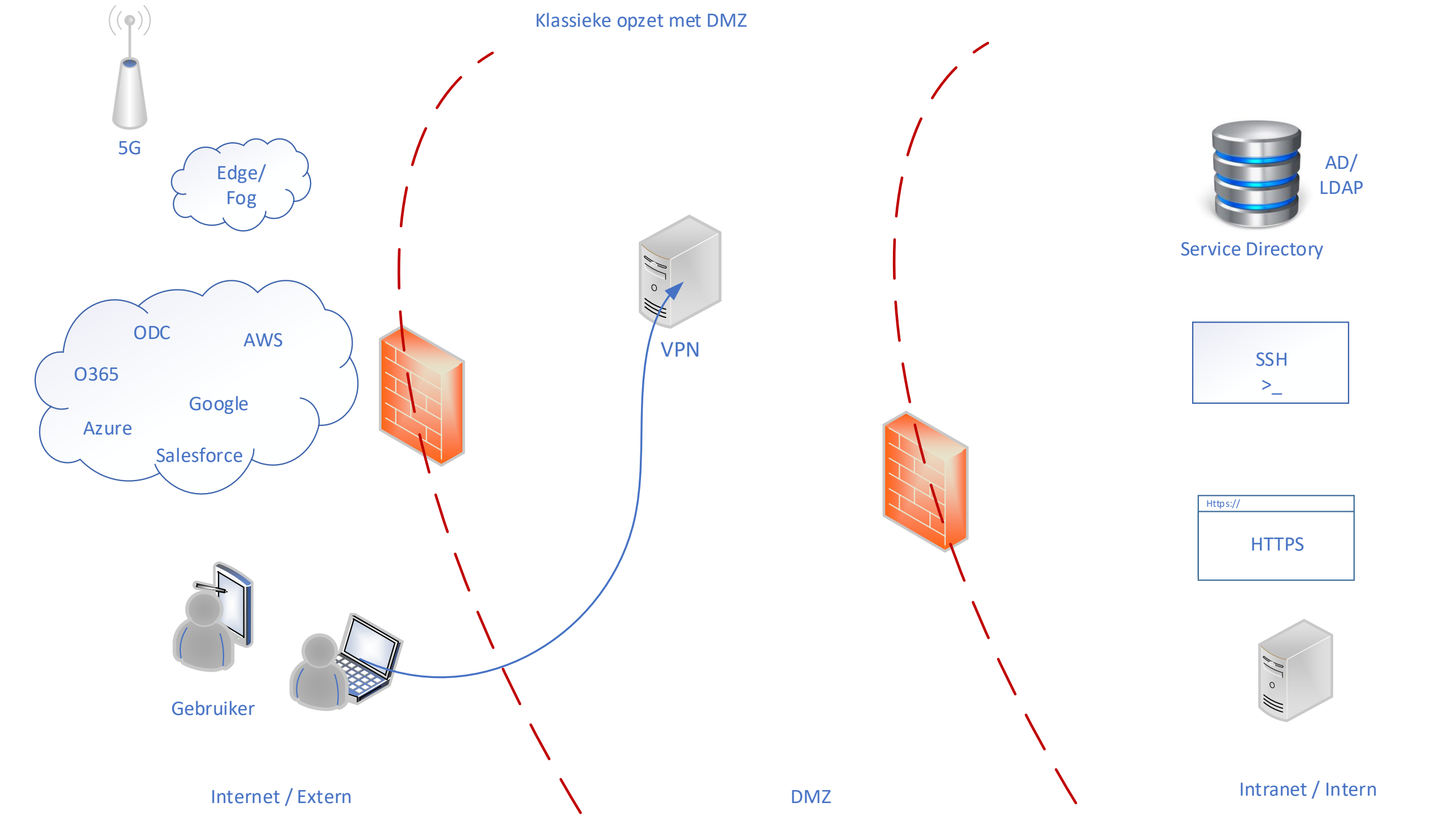
Https://

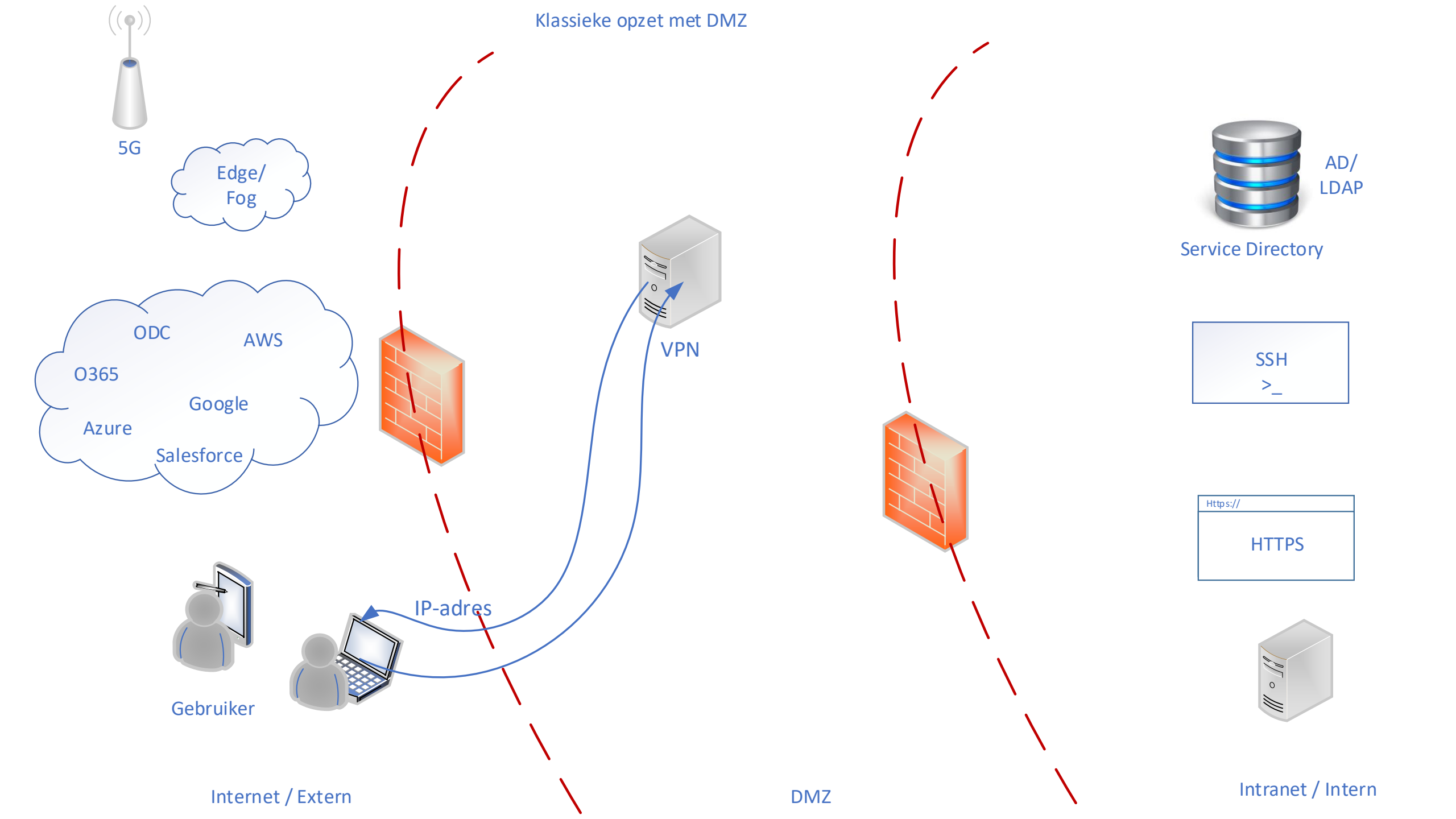
HTTPS

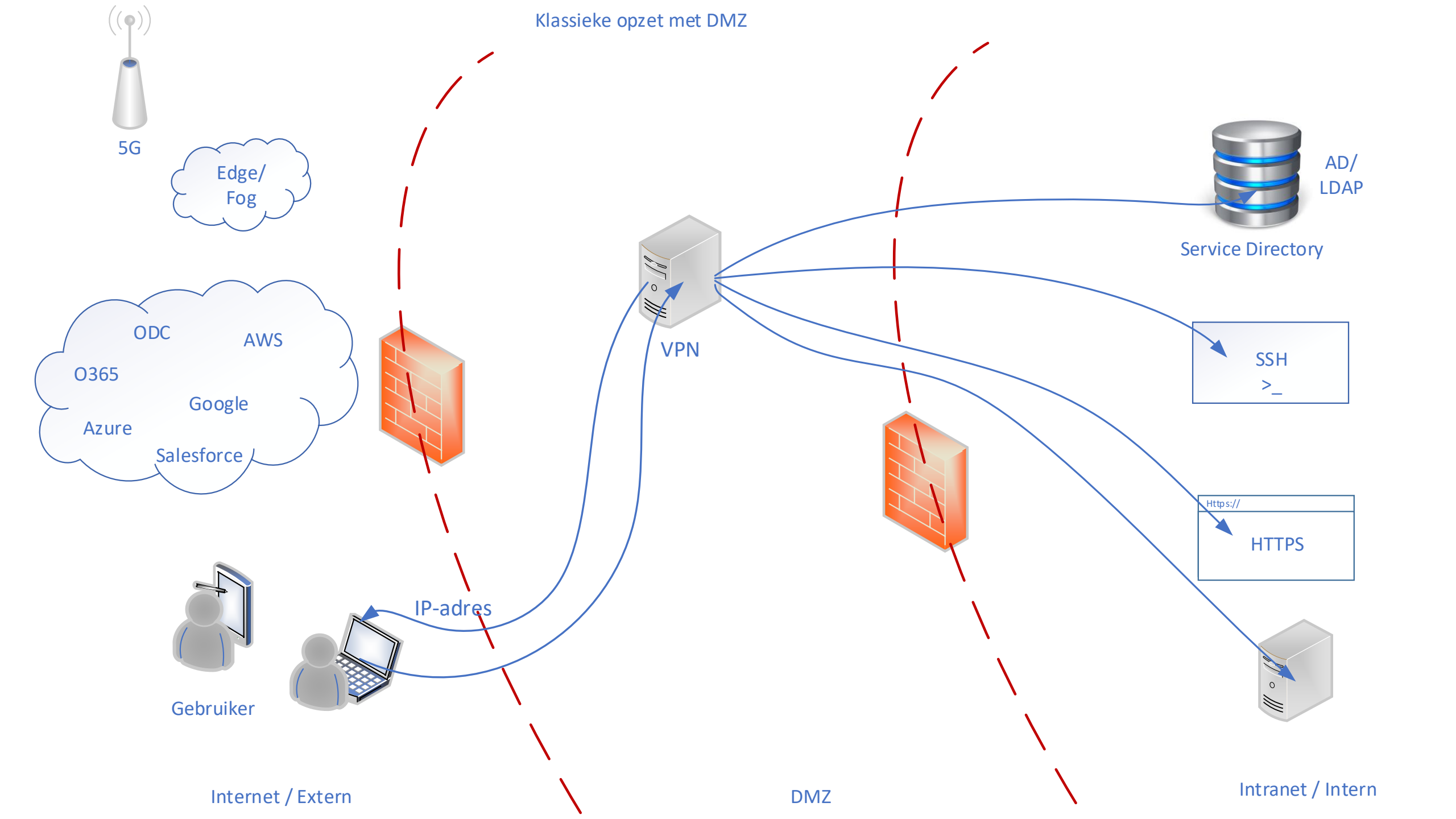
Internet / Extern

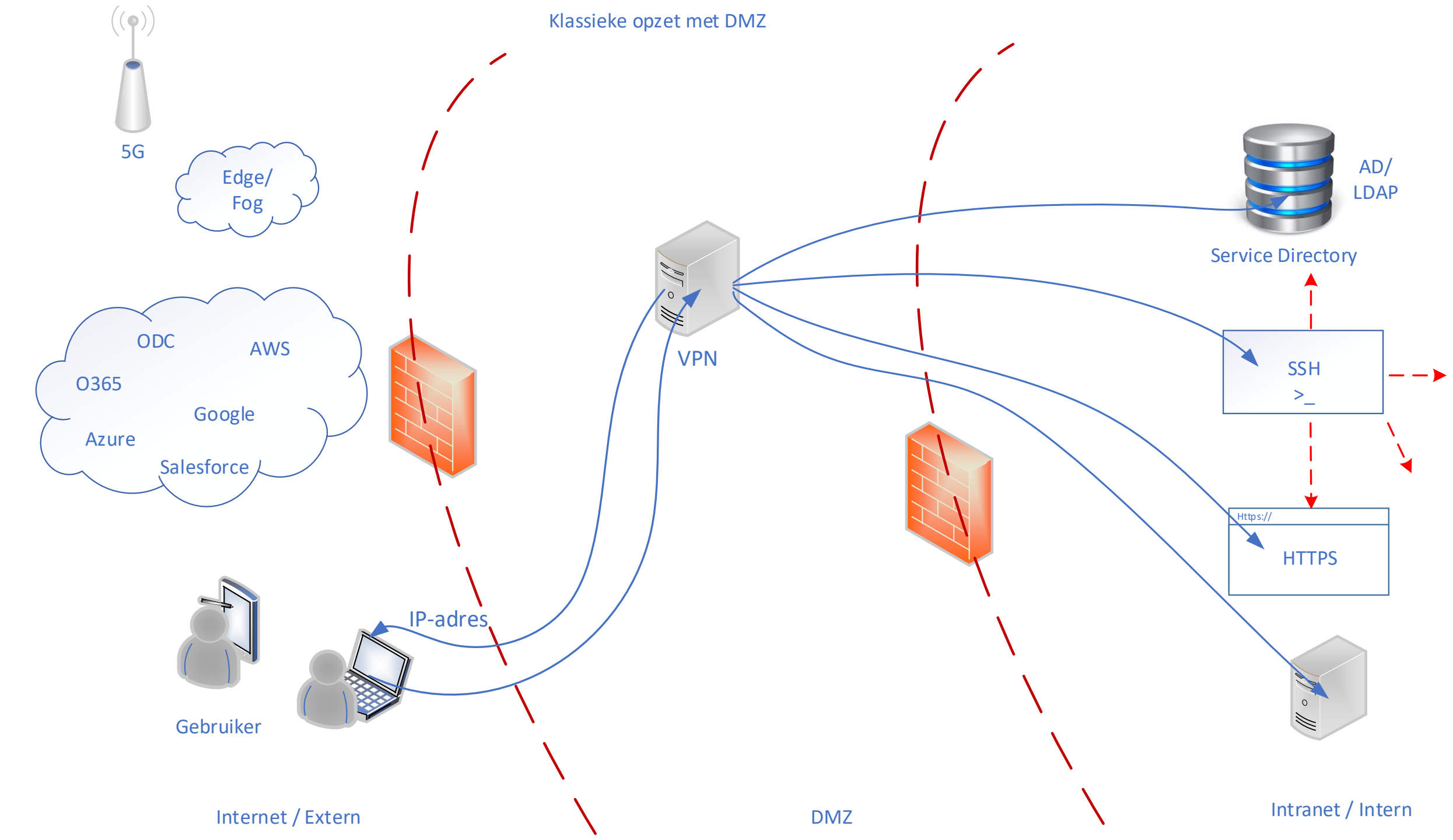
DMZ

Intranet / Intern


Klassieke opzet met DMZ
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
VPN
Gebruiker
AD/
LDAP
Service Directory
SSH
>_
Https://
HTTPS
Internet / Extern
DMZ
Intranet / Intern


Klassieke opzet met DMZ
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
VPN
IP-adres
Gebruiker
AD/
LDAP
Service Directory
SSH
>_
Https://
HTTPS
Internet / Extern
DMZ
Intranet / Intern


Klassieke opzet met DMZ
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
VPN
AD/
LDAP
Service Directory
SSH
>_
Https://
HTTPS
IP-adres
Gebruiker
Internet / Extern
DMZ
Intranet / Intern


Klassieke opzet met DMZ
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
VPN
AD/
LDAP
Service Directory
SSH
>_
Https://
HTTPS
IP-adres
Gebruiker
Internet / Extern
DMZ
Intranet / Intern

Zero-Trust

5G

Edge/
Fog

ODC

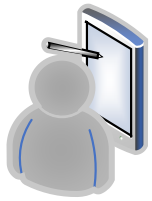
AWS

O365

Google

Azure

Salesforce



Gebruiker

AD/
LDAP

Service Directory

SSH
>_

Https://

HTTPS

Internet / Extern

DMZ

Intranet / Intern

Zero-Trust

5G

Edge/
Fog

ODC

AWS

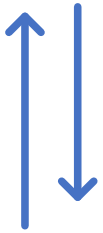
O365

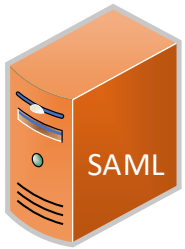
Google

Azure

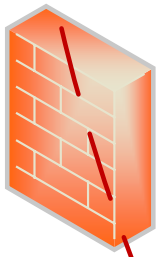
Salesforce

Reverse Proxy





SSO-gateway



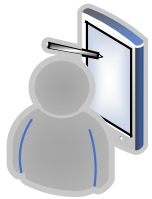
AD/
LDAP

Service Directory

SSH
>_

Https://

HTTPS

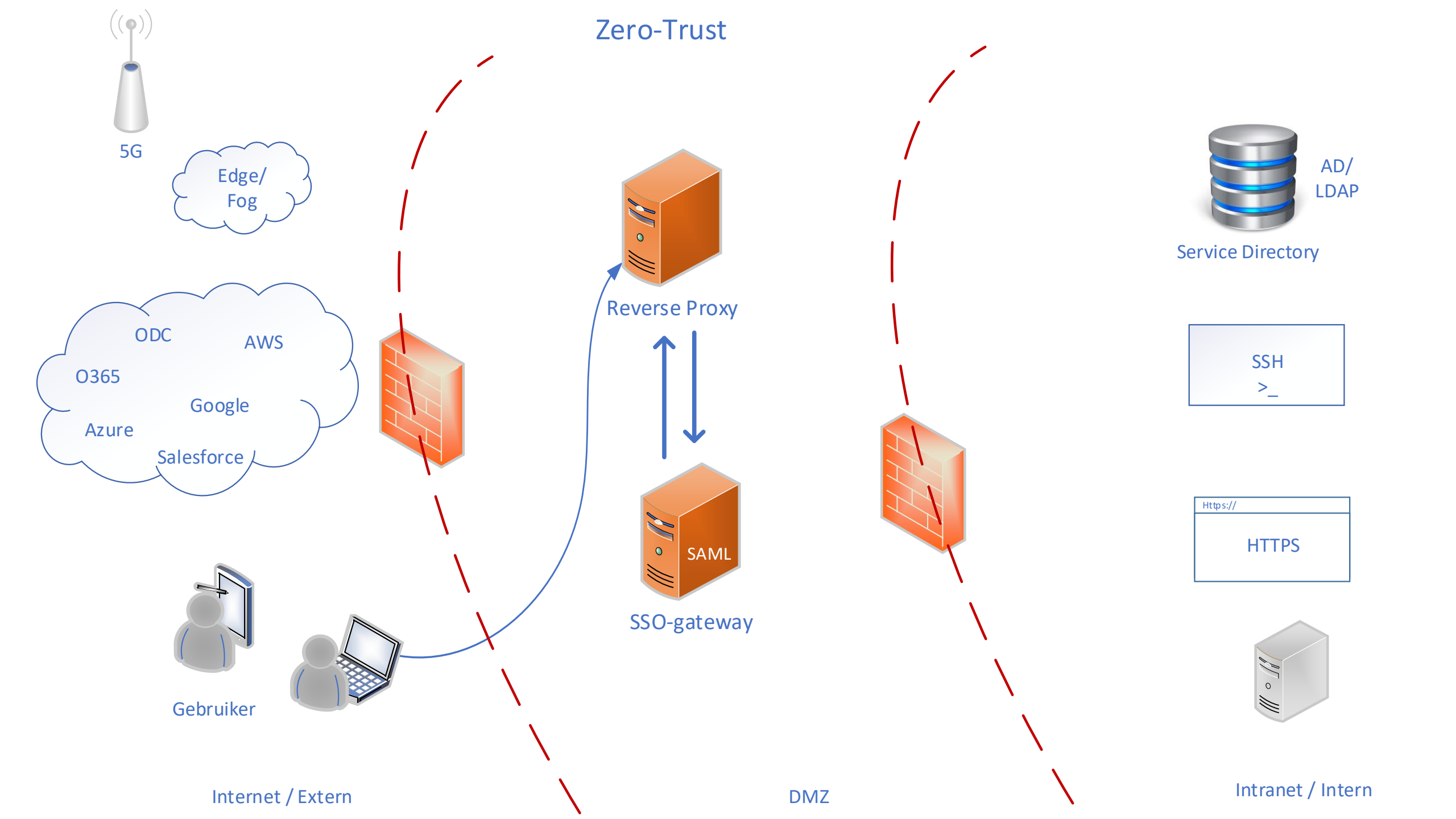


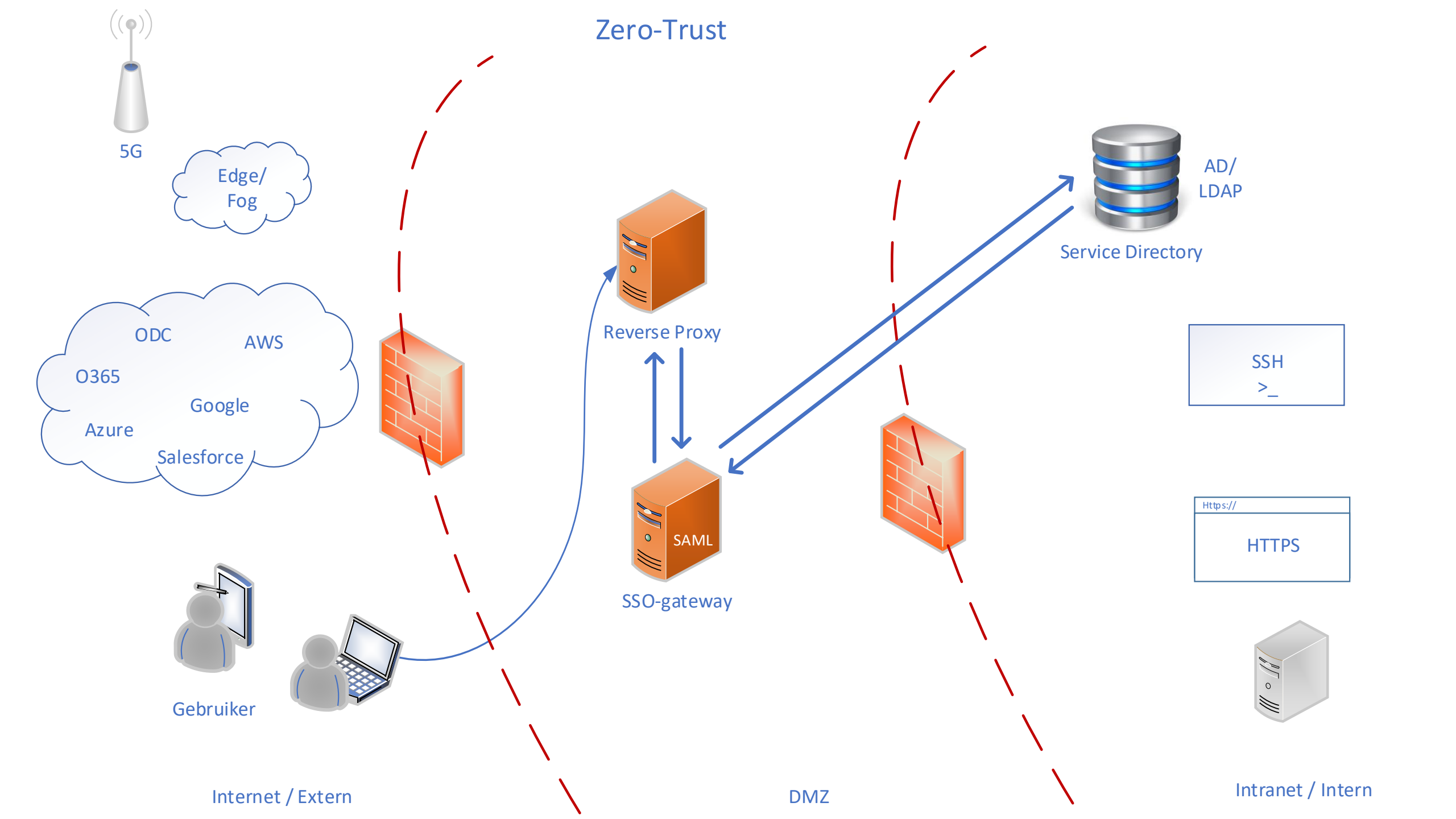
Gebruiker

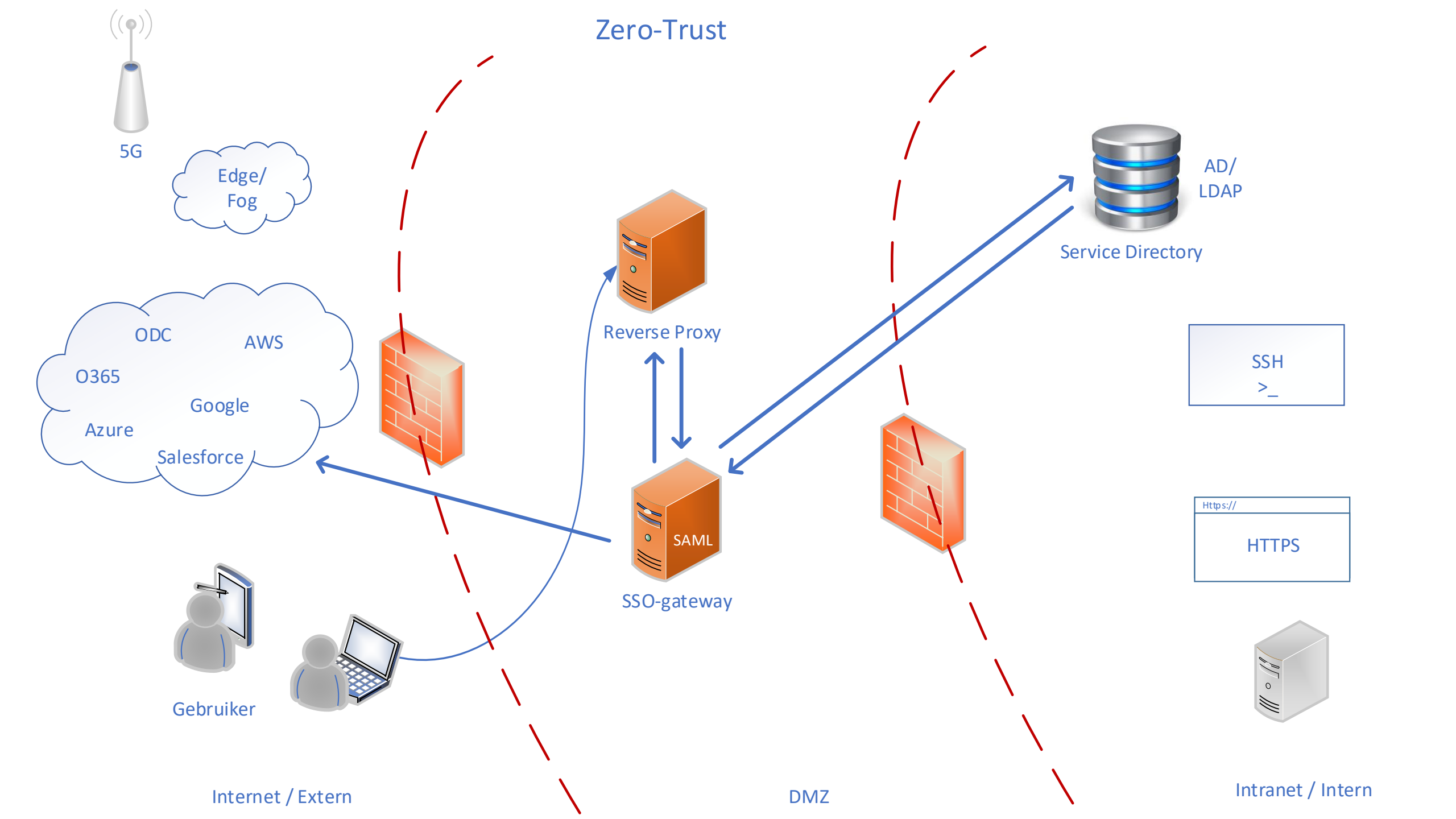
Internet / Extern

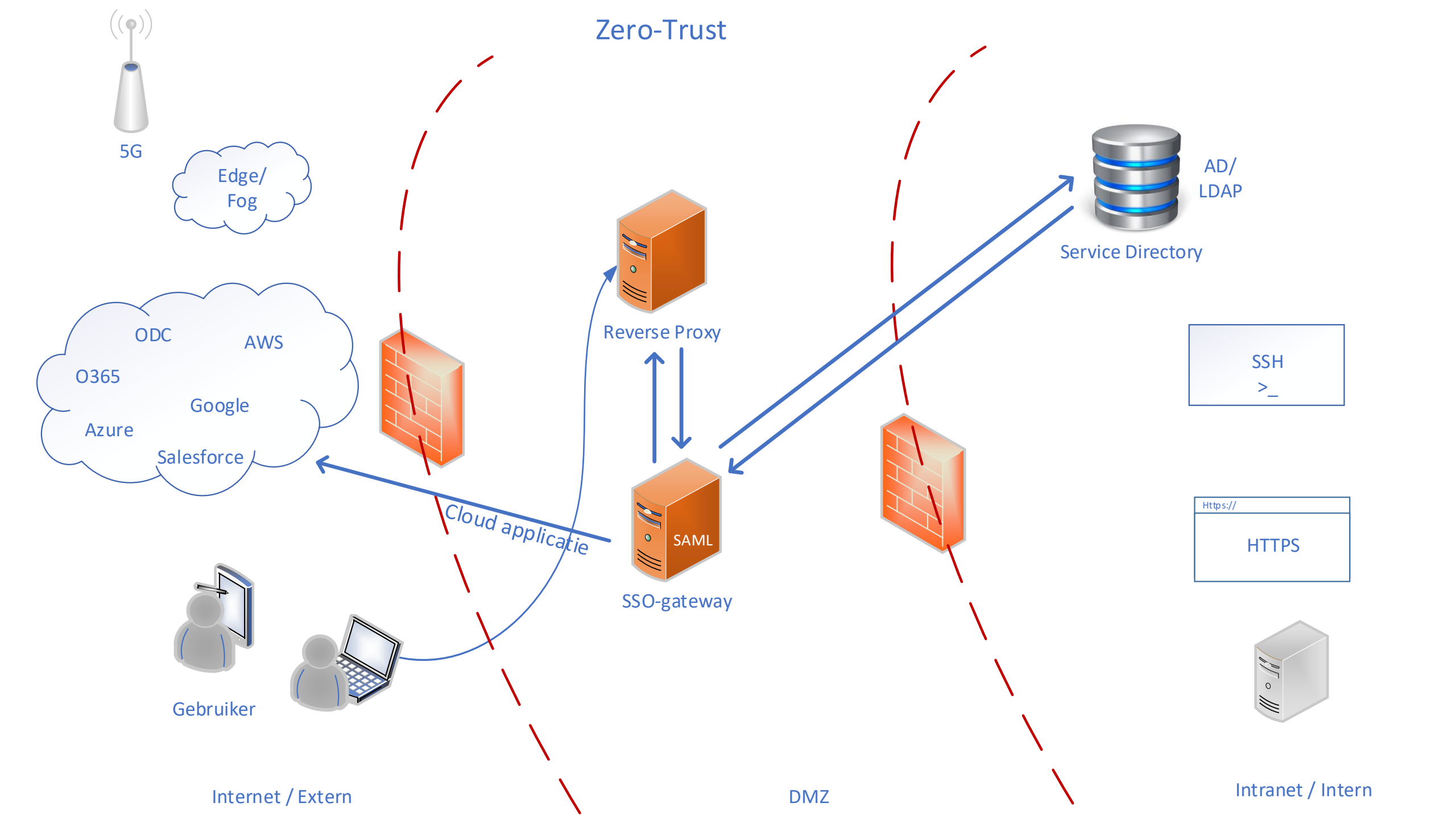
DMZ

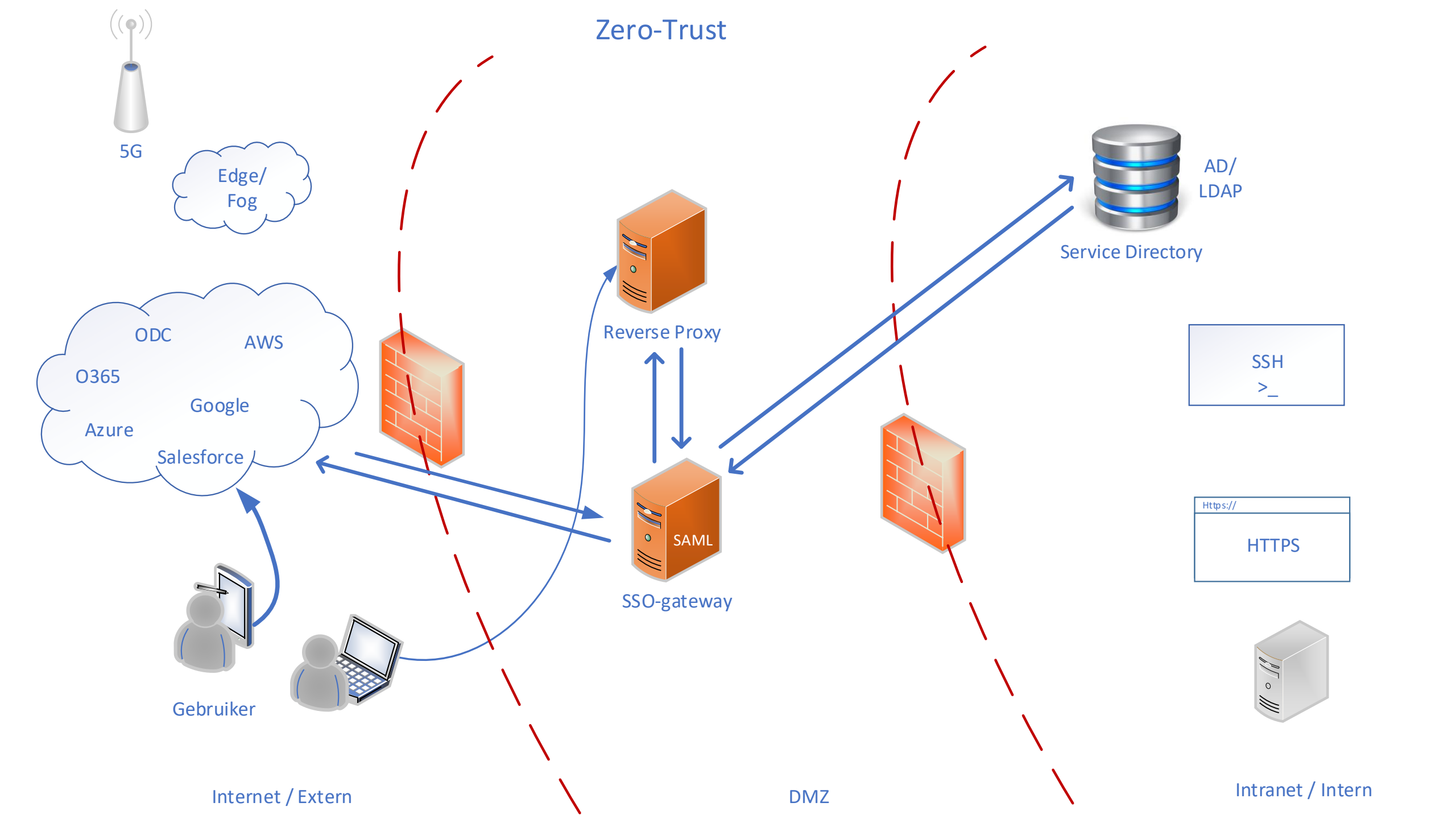
Intranet / Intern

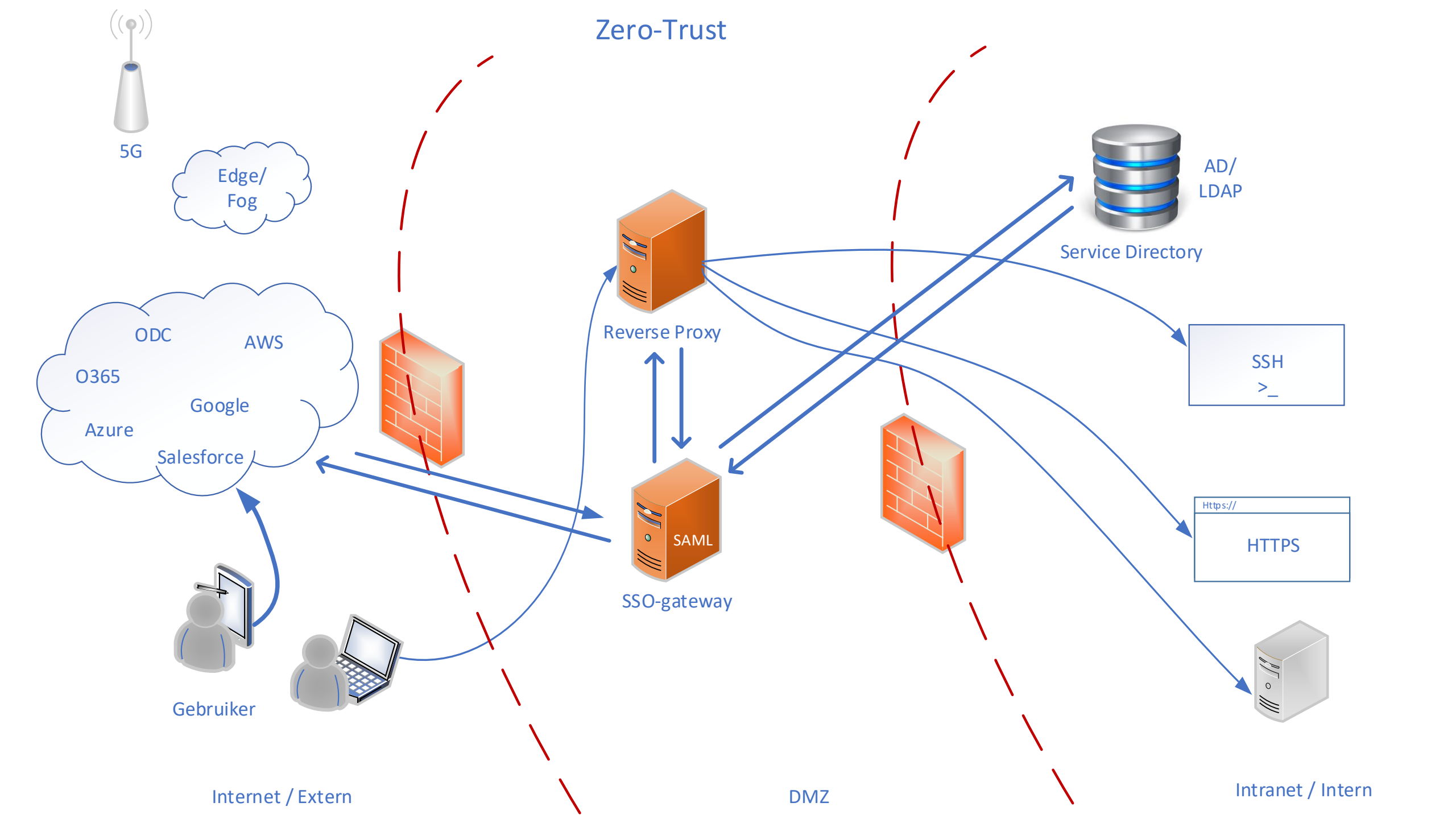

Zero-Trust
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
Reverse Proxy
SAML
SSO-gateway
Gebruiker
AD/
LDAP
Service Directory
SSH
>_
Https://
HTTPS
Internet / Extern
DMZ
Intranet / Intern


Zero-Trust
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
Reverse Proxy
SAML
SSO-gateway
AD/
LDAP
Service Directory
SSH
>_
Https://
HTTPS
Gebruiker
Internet / Extern
DMZ
Intranet / Intern

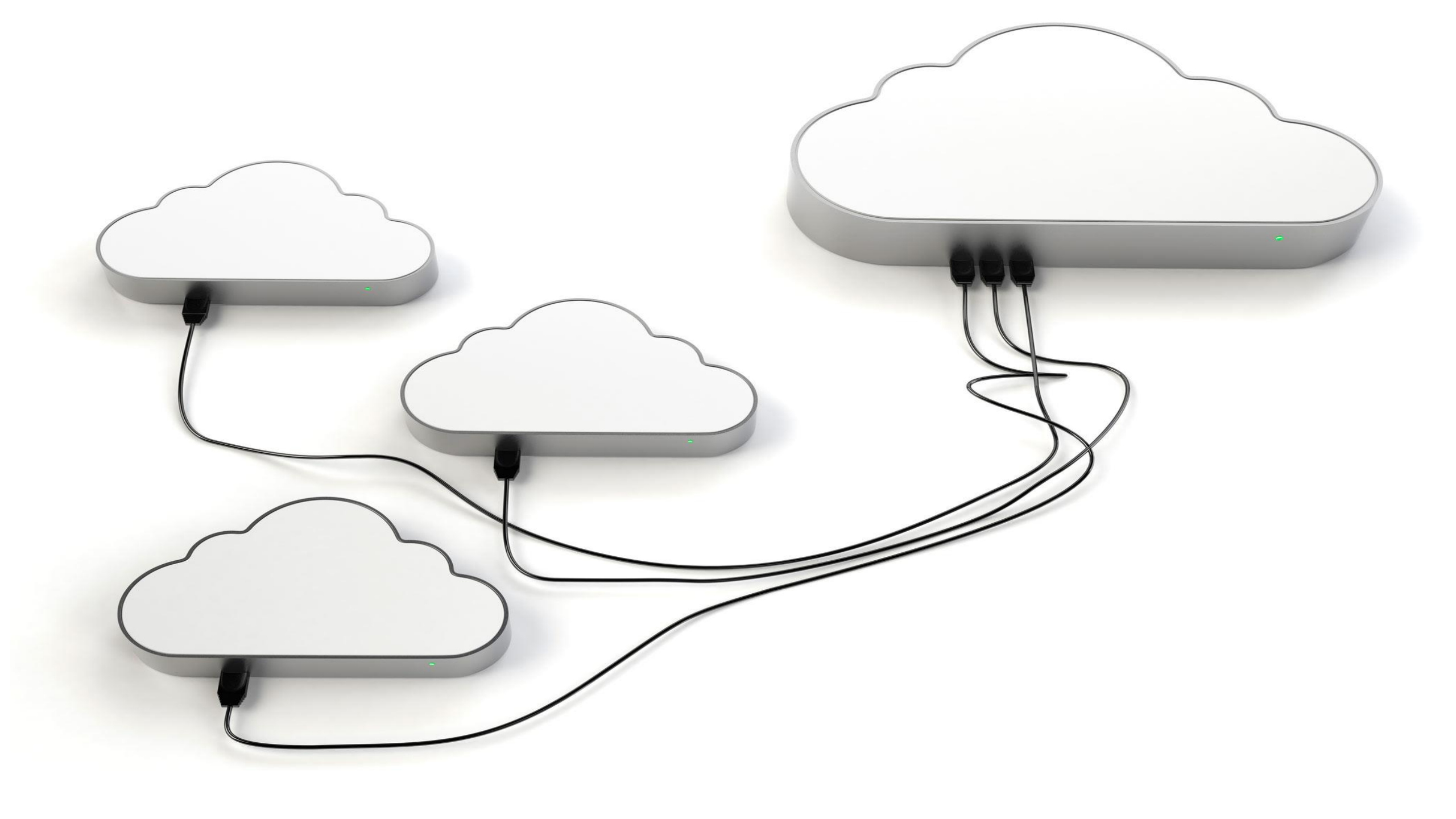

Zero-Trust
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
Reverse Proxy
AD/
LDAP
Service Directory
SSH
>_
SAML
SSO-gateway
Https://
HTTPS
Gebruiker
Internet / Extern
DMZ
Intranet / Intern


Zero-Trust
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
Reverse Proxy
AD/
LDAP
Service Directory
SSH
>_
Cloud applicatie
SAML
SSO-gateway
Https://
HTTPS
Gebruiker
Internet / Extern
DMZ
Intranet / Intern

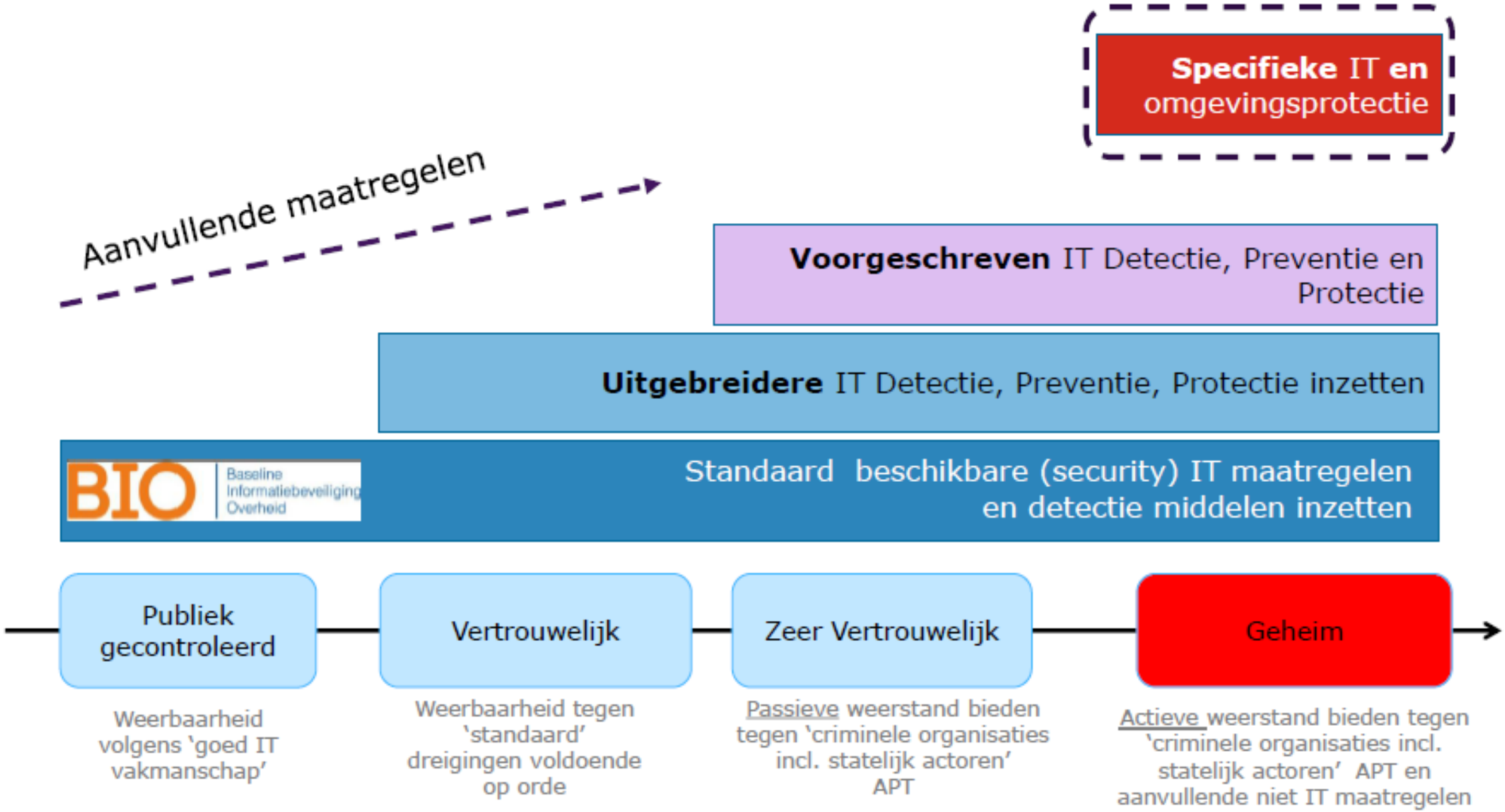

Zero-Trust
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
Reverse Proxy
AD/
LDAP
Service Directory
SSH
>_
SAML
SSO-gateway
Https://
HTTPS
Gebruiker
Internet / Extern
DMZ
Intranet / Intern


Zero-Trust
5G
Edge/
Fog
ODC
AWS
O365
Google
Azure
Salesforce
Reverse Proxy
AD/
LDAP
Service Directory
SSH
>_
SAML
SSO-gateway
Https://
HTTPS
Gebruiker
Internet / Extern
DMZ
Intranet / Intern

IT
VPN

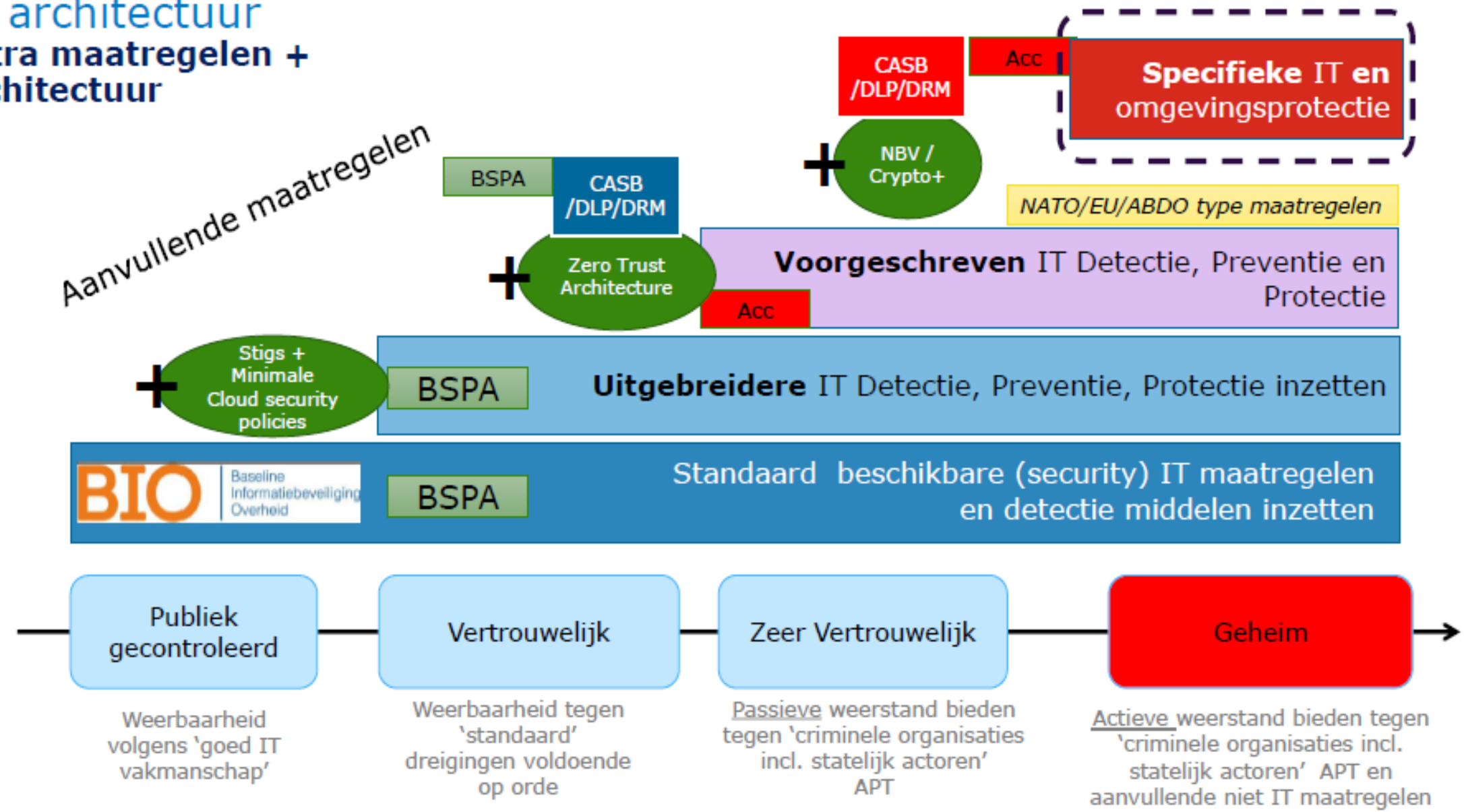


Basis beveiligingsniveaus en IB architectuur



Basis beveiligingsniveaus en IB architectuur

Extra maatregelen + architectuur



Behoefte en samenhang IB architectuur gebieden

NORA
Nederlandse Overheid Referentie Architectuur

EAR
Enterprise Architectuur Rijksdienst

Klassiek netwerkbeveiligingsmodel 'Defense in depth'

Focus op Architectuur

ISO 27001

BIO Baseline Informatiebeveiliging Overheid

Strategisch en Tactisch Normenkader met beperkte concrete handreikingen

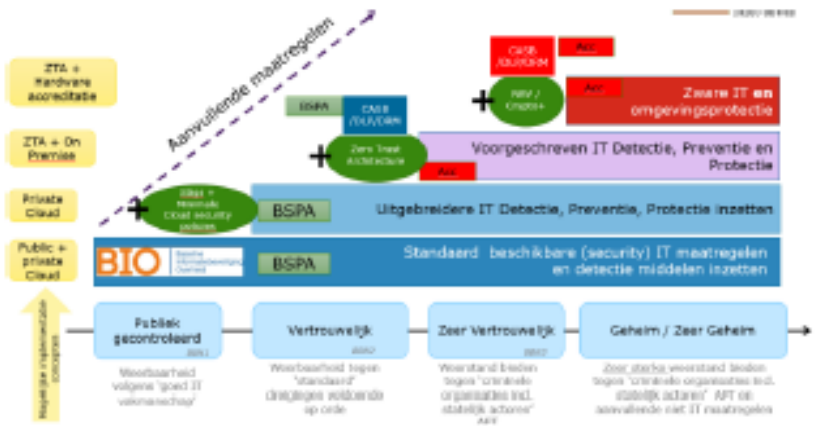
(**VNG IBD** heeft een set uitwerkingen beschreven)

BBN1 en BBN2 beperkte handreikingen
BBN3 invulling ontbreekt

Focus op risico management en compliance

- "Huis op orde"
- Voorschrift Informatiebeveiliging Rijksdient Vir-BI
- Forum Standaardisatie
- BSPA – NBV Voor BBN1-2
- NL Crypto strategie
- Verkenning Cloud beleid
- Identity management (SSOn)
- .....

Losse componenten



Versterken 'klassiek' Security – perimeter oplossingen:

- Ringen – Layers of defence
- Sterkere Protectie/NGFW
- Betere Detectie – Logging/SOC

Uitwerken operationele handreikingen:

- Best Practices Cloud
- Standard Implementation Guidelines (StIGs)
- Cloud kaders – Security posture management

Elementen toevoegen:

- Identity Trust Framework
- Cloud beleid verder uitwerken
- Stg omgeving
- etc

Nieuwe IB security modellen

- Zero Trust Architecture
- Cloud specifieke Security aanpak (CASB, DLP's etc.)
- Software Defined Perimeter (SASE/ZTNA)

Traditioneel en ZTA in één IB Architectuur

CARTA (Gartner)
Continuous Adaptive Risk & Trust Assessment
is een nieuwe strategisch normenkader voor Informatie beveiliging

Rob T model
v0.4 2020

Traditioneel

Zero Trust Architecture

Detectie NDN / SIEM/SOC

Sterke Identity & Access Management

Trust Framework

Authentiseer 'overal-altijd'
PEP strategy

Standaard Industrie
IT oplossing / basis cloudsecurity / BIO aanpak

ZTA elementen

BIO Baseline Informatiebeveiliging Overheid

Additioneel Zero Trust Architecture
Principes toepassen
(CASB,ZTNA,SDP)

Specifieke IT en omgevingsprotectie

NL Crypto strategie

CASB/DLP
DRM

NBV Accreditatie

Minimale cloud security configuraties eisen RIJK + cloud crypto
Cloud Security Posture Management (CSPM) NL Rijk

Publieke Cloud ⇔ Goedgekeurde Publieke Cloud

Private Cloud / ODC's

Eigen Infrastructuur /

RINGEN /

Compartimenten

Fundament **Fundament** **Fundament**

Publiek gecontroleerd *BBN1* — Vertrouwelijk *BBN2* — Zeer Vertrouwelijk *BBN3* — **Geheim**

ZERO
TRUST
Devolutions