Customer-On-Premise

Required To Login:
(configured once)
- SQL-Servername
- Username
- Password
- Database-Name

Usually not exposed
to the Internet.

SQL-Connection

CCA9-Workstation

CCA-Database

Share a common
network with the
database server

File-Storage and Email-Integration

Text

Customer-Provided Office-365 Integration

Customer-Provided
Sharepoint Server

Customer-Provided
Exchange Server

Customer-On-Premise

Required To Login:
(configured once)
- SQL-Servername
- Username
- Password
- Database-Name

CCA9-Workstation

SQL-Connection

Together-CCA Cloud

CCA-Cloud-Database
(cca-cloud-db-01.cca.online)

Connection-Security 1)

plain-text sql-connections might leak information / passwords

Connection-Security 2)

Database is accessible to the public

Connectivity 1)

- SQL-Servername must not change
- SQL-Username must not change
- SQL-Password must not change
- Database-Name must not change

Multi-Tenant-Security 1)

- SQLUser of Tenant A must not be able to access the Database of Tenant B

(tenants must not be able to access other tenants)

Multi-Tenant-Security 2)

- Usernames / Passwords might be weak

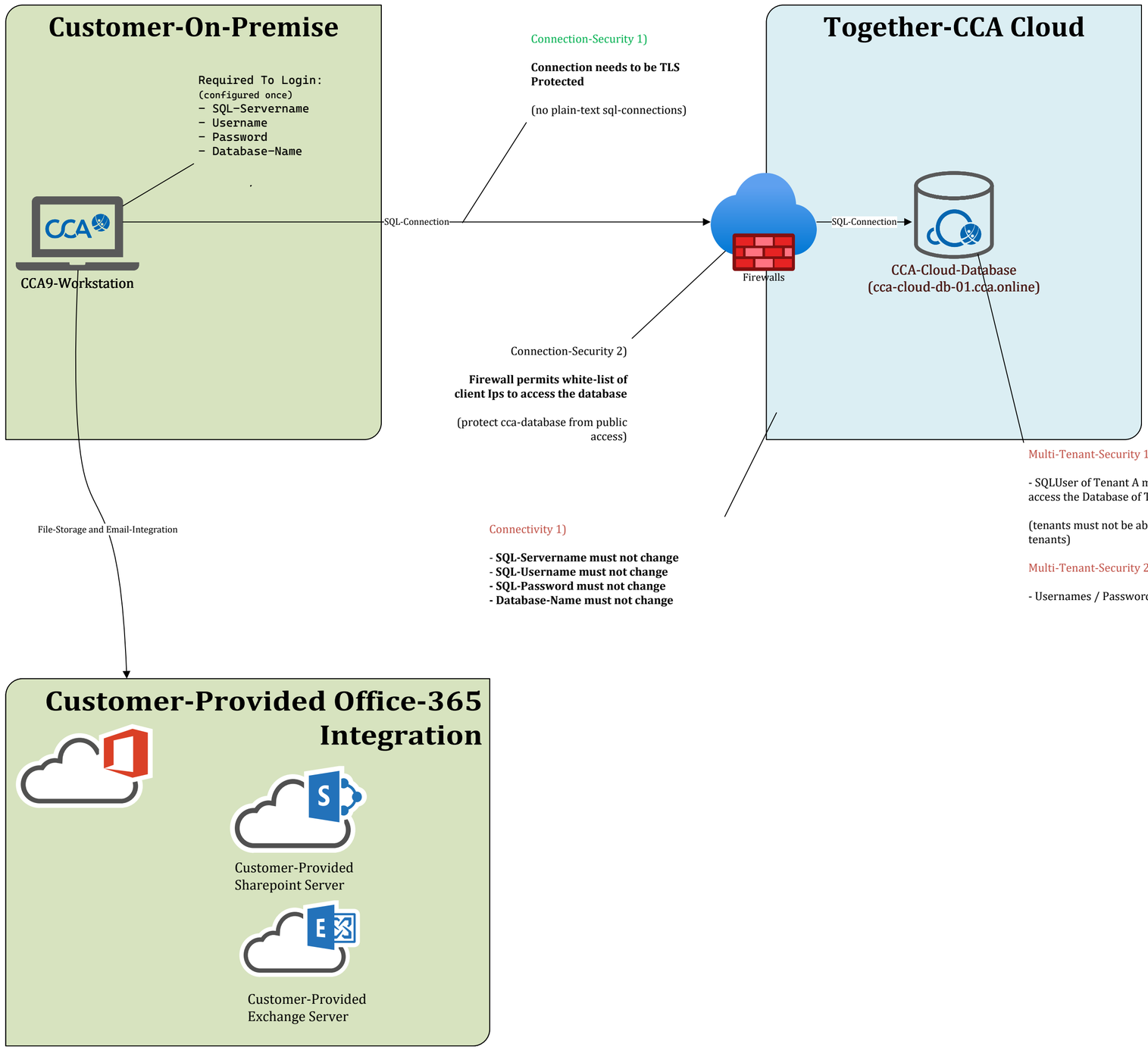
File-Storage and Email-Integration

Customer-Provided Office-365 Integration

Customer-Provided
Sharepoint Server

Customer-Provided
Exchange Server

Simple Security Meassures



Pros:

- pretty much supported today?
- no additional software needs to be installed on the client-side

Cons:
- IP – Address Whitelisting must be managed manually by Together-CCA (moving to home-office / using phone to connect / …)

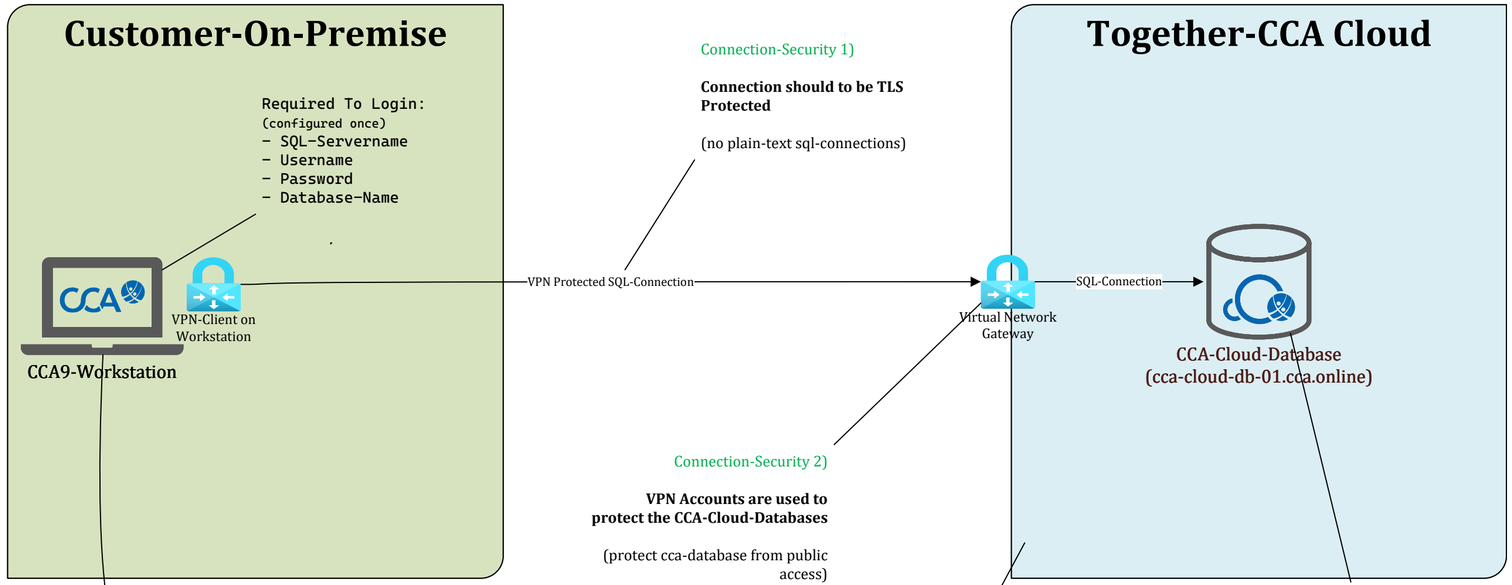
- Password Management must be done manually by Together-CCA (forgotten/ leaked)

- Conflicting Username / Passwords

- When moving the database server *every* affected client must be reconfigured.

- When an IP Address is part of a public network, this would open the cca-database to attacks.

VPN – Client for Protecting Together-CCA-Cloud



Connection-Security 1)

Connection should to be TLS Protected

(no plain-text sql-connections)

Connection-Security 2)

VPN Accounts are used to protect the CCA-Cloud-Databases

(protect cca-database from public access)

Connectivity 1)

- VPN Access must be configured on client
- SQL-Servername must not change
- SQL-Username must not change
- SQL-Password must not change
- Database-Name must not change

Multi-Tenant-Security 1)

- SQLUser of Tenant A must not be able to access the Database of Tenant B

(tenants must not be able to access other tenants)

Multi-Tenant-Security 2)

- Usernames / Passwords might be weak

Pros:

- IP Address Management is not necessary anymore.

Cons:

- VPN-Client software needs to be installed on the client-side

- VPN Clients needs evelated user-rights to add virtual interfaces(?)

- Password Management must be done manually by Together-CCA (forgotten/ leaked)

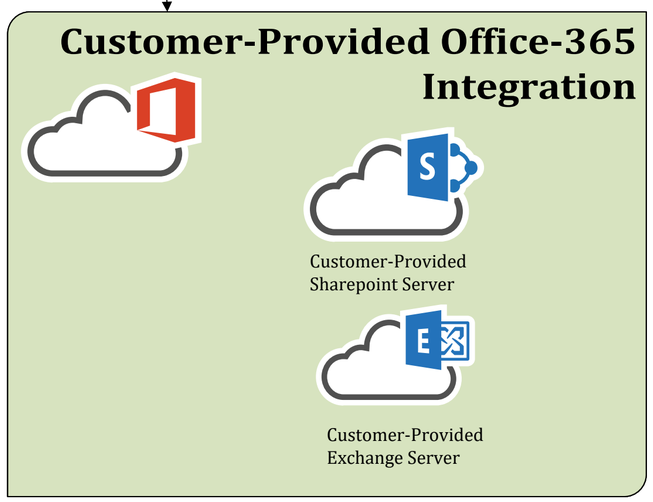
- Conflicting Username / Passwords

- When moving the database server *every* affected client must be reconfigured.

~~- When an IP Address is part of a public network, this would open the cca-database to attacks.~~

~~- IP – Address Whitelisting must be managed manually by Together-CCA (moving to home-office / using phone to connect / ...)~~

File-Storage and Email-Integration



SSH-Port-Forwarding for Protecting Together-CCA-Cloud

Customer-On-Premise

Required To Login:
(configured once)
- SQL-Servername
- Username
- Password
- Database-Name

CCA9-Workstation

SSH-Port-Forwarding

SSH-Tunnel Protected SQL-Connection

File-Storage and Email-Integration

Together-CCA Cloud

SSH-Jump-Host

SQL-Connection

CCA-Cloud-Database
(cca-cloud-db-01.cca.online)

Connection-Security 1)

Connection should to be TLS Protected

(no plain-text sql-connections)

Connection-Security 2)

SSH Credentials are used to protect the CCA-Cloud-Databases

(protect cca-database from public access)

Connectivity 1)

- SSH – Access must be configured on client
- SQL-Servername must not change
- SQL-Username must not change
- SQL-Password must not change
- Database-Name must not change

Multi-Tenant-Security 1)

- SQLUser of Tenant A must not be able to access the Database of Tenant B

(tenants must not be able to access other tenants)

Multi-Tenant-Security 2)

- Usernames / Passwords might be weak

Pros:

- IP Address Management is not necessary anymore.

Cons:

- SSH Client must be implemented in cca9
- Security Fixes mut be applied in cca9

- Password Management must be done manually by Together-CCA (forgotten/ leaked)

- Conflicting Username / Passwords

- When moving the database server *every* affected client must be reconfigured.

~~- VPN-Client software needs to be installed on the client-side~~

~~- VPN Clients needs evelated user-rights to add virtual interfaces(?)~~

~~- When an IP Address is part of a public network, this would open the cca-database to attacks.~~

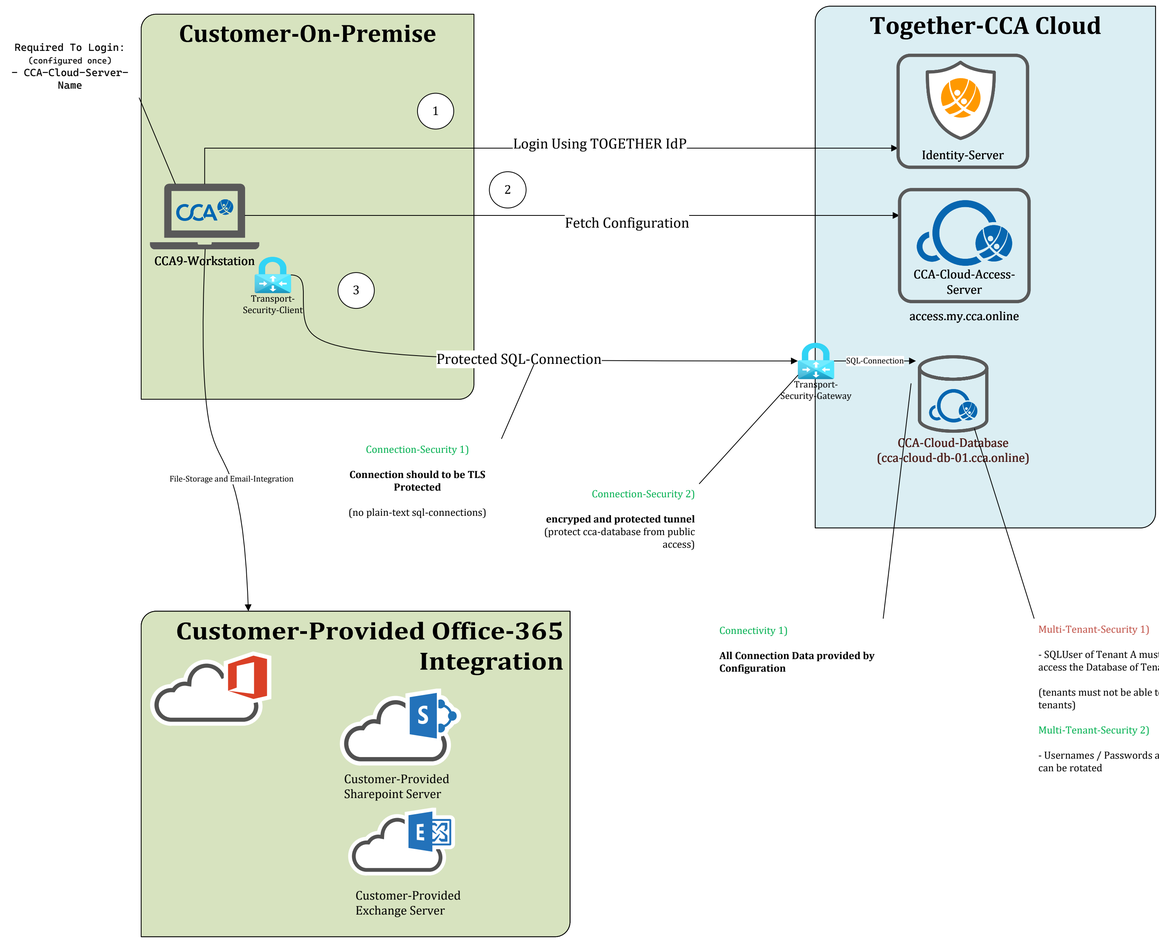
~~- IP – Address Whitelisting must be managed manually by Together-CCA (moving to home-office / using phone to connect / ...)~~

Customer-Provided Office-365 Integration

Customer-Provided
Sharepoint Server

Customer-Provided
Exchange Server

Together-Login + fetching Configuration



Connection-Security 1)

Connection should to be TLS Protected

(no plain-text sql-connections)

Connection-Security 2)

encryped and protected tunnel (protect cca-database from public access)

Connectivity 1)

All Connection Data provided by Configuration

Multi-Tenant-Security 1)

- SQLUser of Tenant A must not be able to access the Database of Tenant B

(tenants must not be able to access other tenants)

Multi-Tenant-Security 2)

- Usernames / Passwords are always strong – can be rotated

Pros:

- IP Address Management is not necessary anymore.
- Changes on the Infrastructure Side will be automatically available for clients.

Cons:

~~- Password-Management must be done manually by Together-CCA (forgotten/ leaked)~~

~~- Conflicting Username / Passwords~~

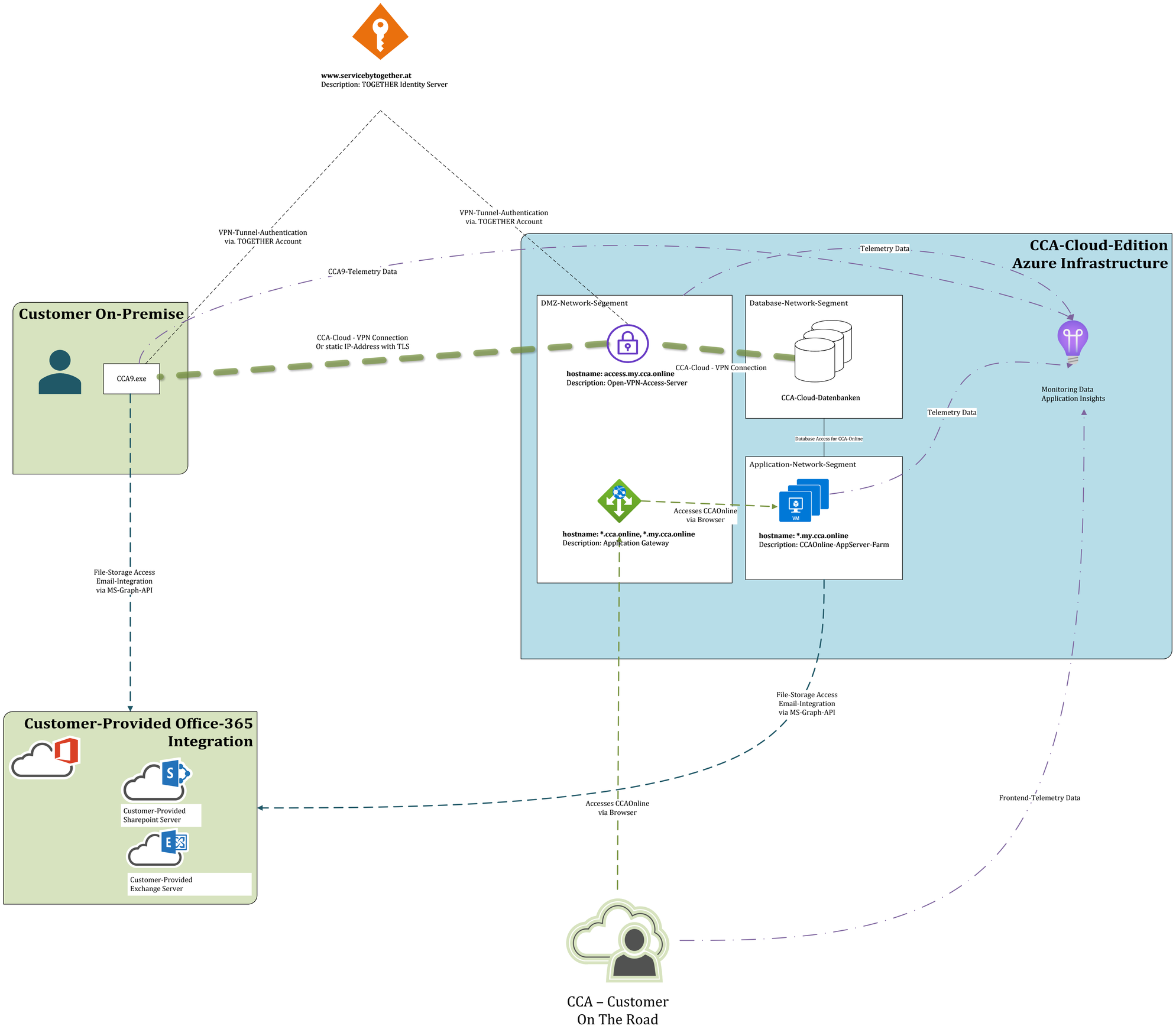
~~- When moving the database server *every* affected client must be reconfigured.~~

~~- VPN-Client software needs to be installed on the client-side~~

~~- VPN-Clients needs evelated user-rights to add virtual interfaces(?)~~

~~- When an IP-Address is part of a public network, this would open the cca-database to attacks.~~

~~- IP – Address-Whitelisting must be managed manually by Together-CCA (moving to home-office / using phone to -connect / ...)~~


www.servicebytogether.at
Description: TOGETHER Identity Server
VPN-Tunnel-Authentication
via. TOGETHER Account
VPN-Tunnel-Authentication
via. TOGETHER Account
CCA9-Telemetry Data
Telemetry Data
Customer On-Premise
CCA9.exe
CCA-Cloud - VPN Connection
Or static IP-Address with TLS
CCA-Cloud-Edition
Azure Infrastructure
DMZ-Network-Segement
hostname: access.my.cca.online
Description: Open-VPN-Access-Server
CCA-Cloud - VPN Connection
Database-Network-Segment
CCA-Cloud-Datenbanken
Monitoring Data
Application Insights
Telemetry Data
Database Access for CCA-Online
Application-Network-Segment
Accesses CCAOnline
via Browser
hostname: *.cca.online, *.my.cca.online
Description: Application Gateway
VM
hostname: *.my.cca.online
Description: CCAOnline-AppServer-Farm
File-Storage Access
Email-Integration
via MS-Graph-API
File-Storage Access
Email-Integration
via MS-Graph-API
Customer-Provided Office-365
Integration
Customer-Provided
Sharepoint Server
Customer-Provided
Exchange Server
Accesses CCAOnline
via Browser
Frontend-Telemetry Data
CCA – Customer
On The Road