

—

# Let's replace your VPN with a real Zero Trust Network Access !

---

Christopher Brumm

# Christopher Brumm

Cloud Security Architect @glueckkanja

## Focus

Identity + Security  
in Microsoft Cloud

## From

Hamburg, Germany

## My Blog

[chris-brumm.com](https://chris-brumm.com)



## Certifications

CISSP, various MS certs

## Hobbies

Family, Traveling, Pen & Paper RPG

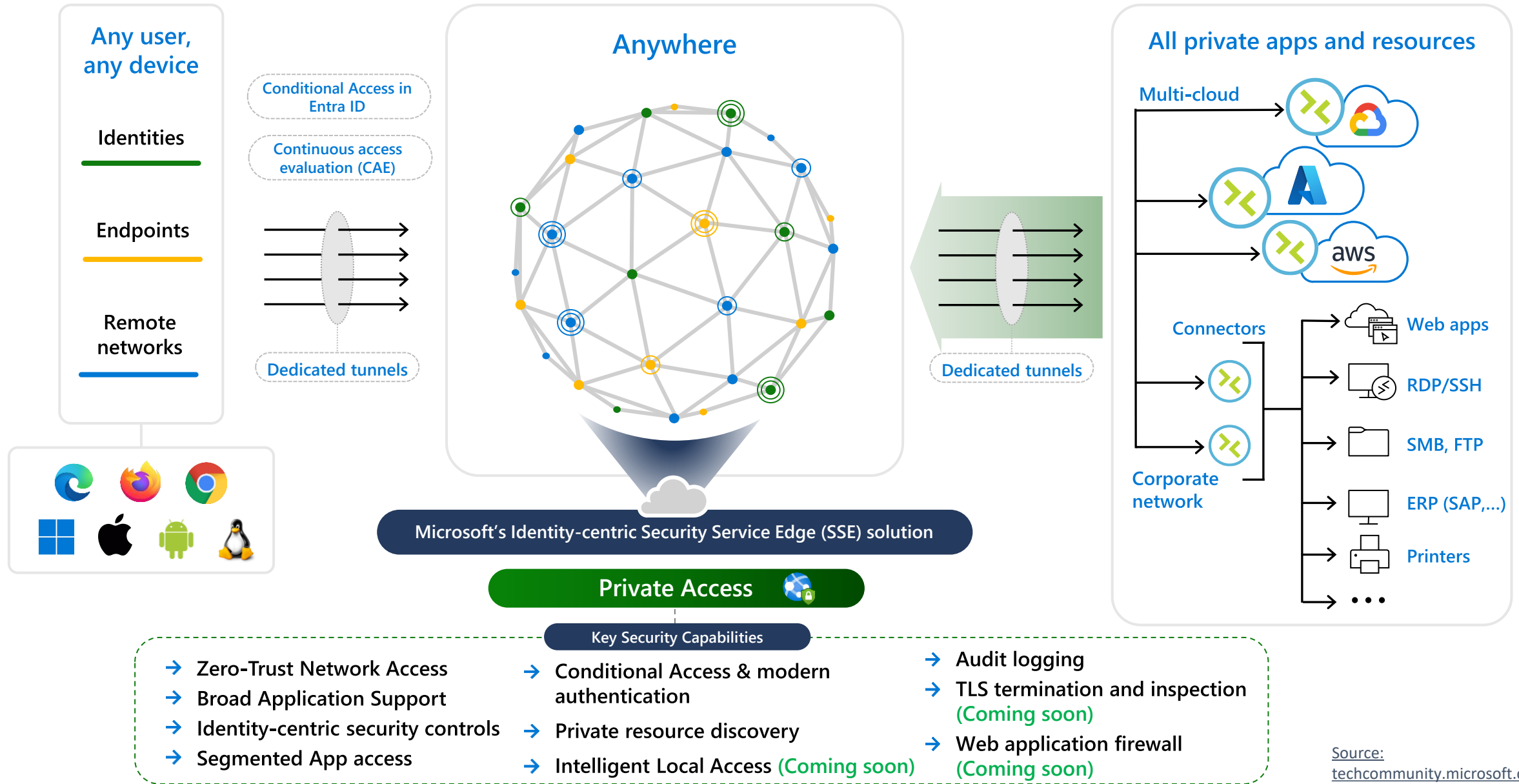
## Contact

 [/christopherbrumm](https://www.linkedin.com/company/christopherbrumm)

---

What is the Zero Trust solution  
for OnPrem Access?

# Microsoft Entra Private Access





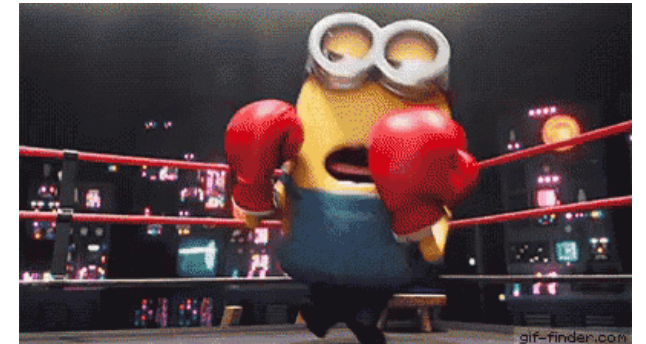
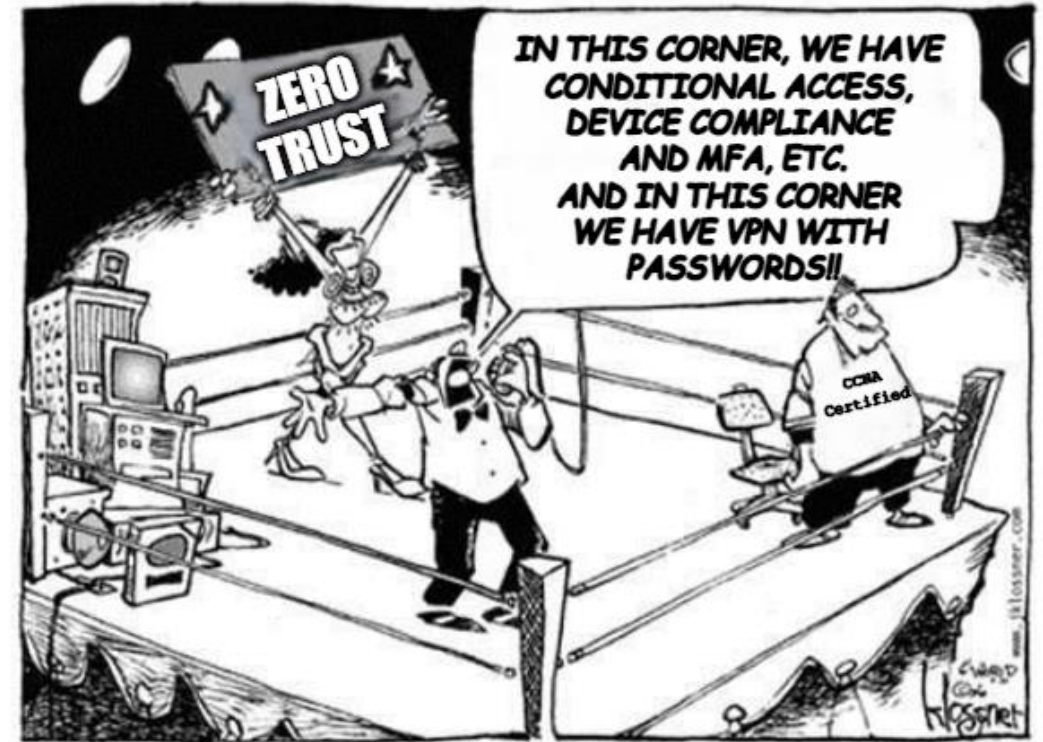
# A match in 4 rounds

Connectivity and Name Resolution

Access Management and  
Authentication

Authorization and  
Entitlement Management

Threat Intel and  
Incident Response



# Connectivity and Name Resolution

## Entra Private Access

**All sessions are cloud terminated**

Transparent integration of Complex,  
disconnected environments

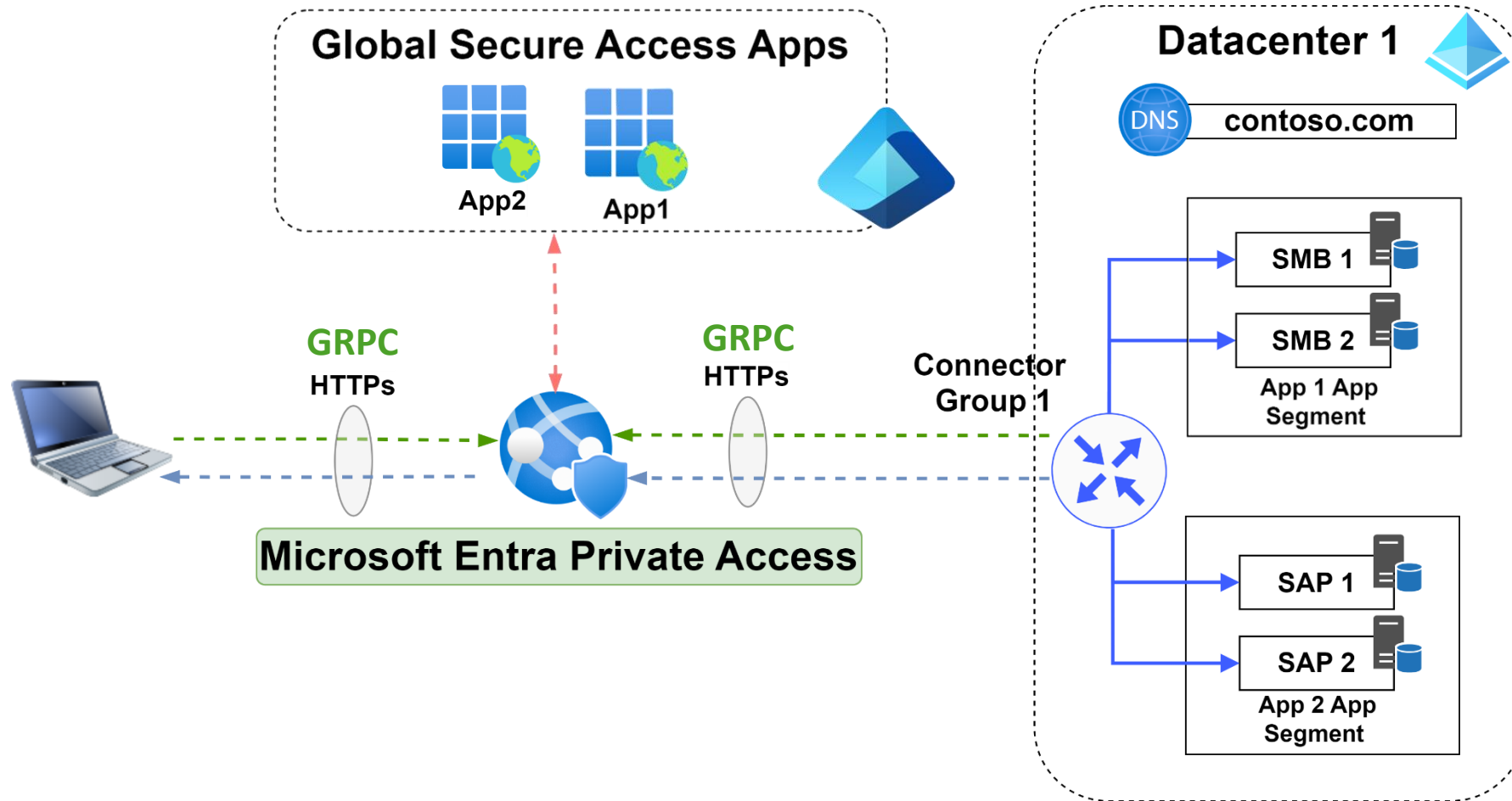


## Traditional VPN

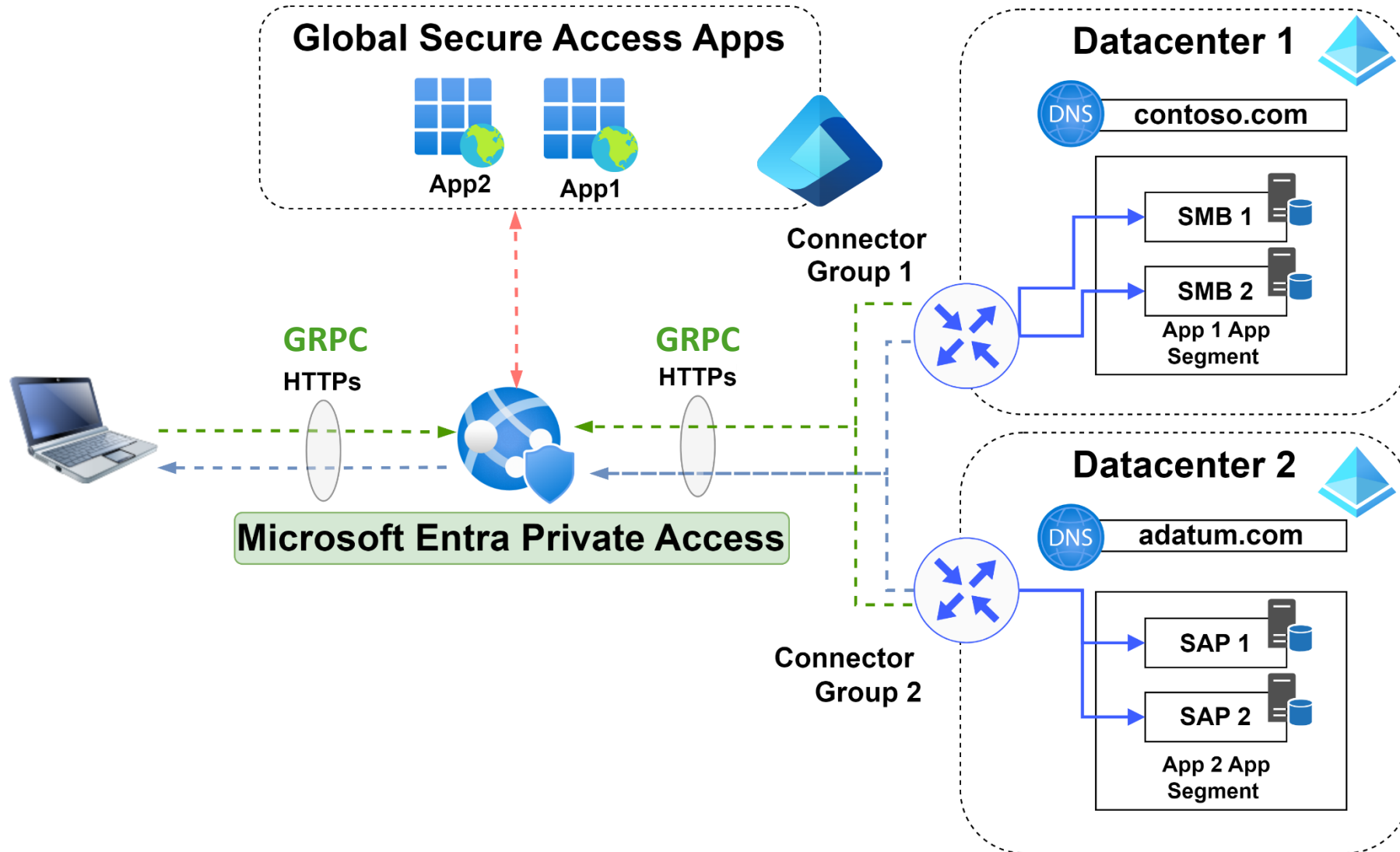
**Please choose your datacenter**

and route traffic to the others through  
your WAN

# Let's start with a simple Deployment



# and move to a more complex scenario





# Enabling the builtin DNS feature

Name ⓘ \* QuickAccess

Connector Group ⓘ ZTNA ▼

ⓘ We recommend at least two active connectors in selected group 'ZTNA'. [Click here to download a connector or manage your connector groups.](#)



Application Segment **Private DNS** PREVIEW

☒ Enable Private DNS  
Add DNS Suffix(s) to use for private DNS. [Learn more](#) ⓘ

+ Add DNS suffix



---

DNS suffix

gkfelucia.net  

Global Secure Access Client - Advanced diagnostics

Overview Health check **Forwarding profile** Hostname acquisition Traffic ...

 Add filter  Columns

Microsoft 365 rules

Private access rules

Internet access rules

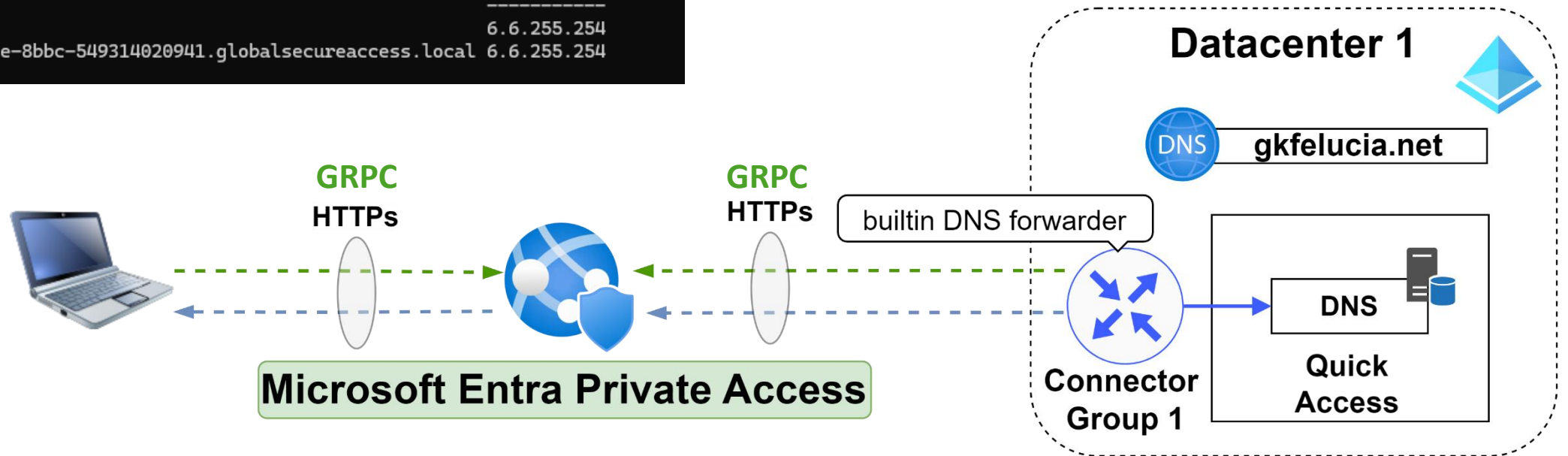
Private DNS rules

Single Label	DNS server address	Suffix
True	6.6.255.254	4e8c3b32-1ab6-471e-8...
False	6.6.255.254	gkfelucia.net

# How does it work?

```
Windows PowerShell
PS C:\Users\BigBird> Get-DnsClientNrptPolicy | select Namespace, Nameservers

Namespace                                     NameServers
-----
.gkfelucia.net                               6.6.255.254
.4e8c3b32-1ab6-471e-8bbc-549314020941.globalsecureaccess.local 6.6.255.254
```



ÃÁ ĩ

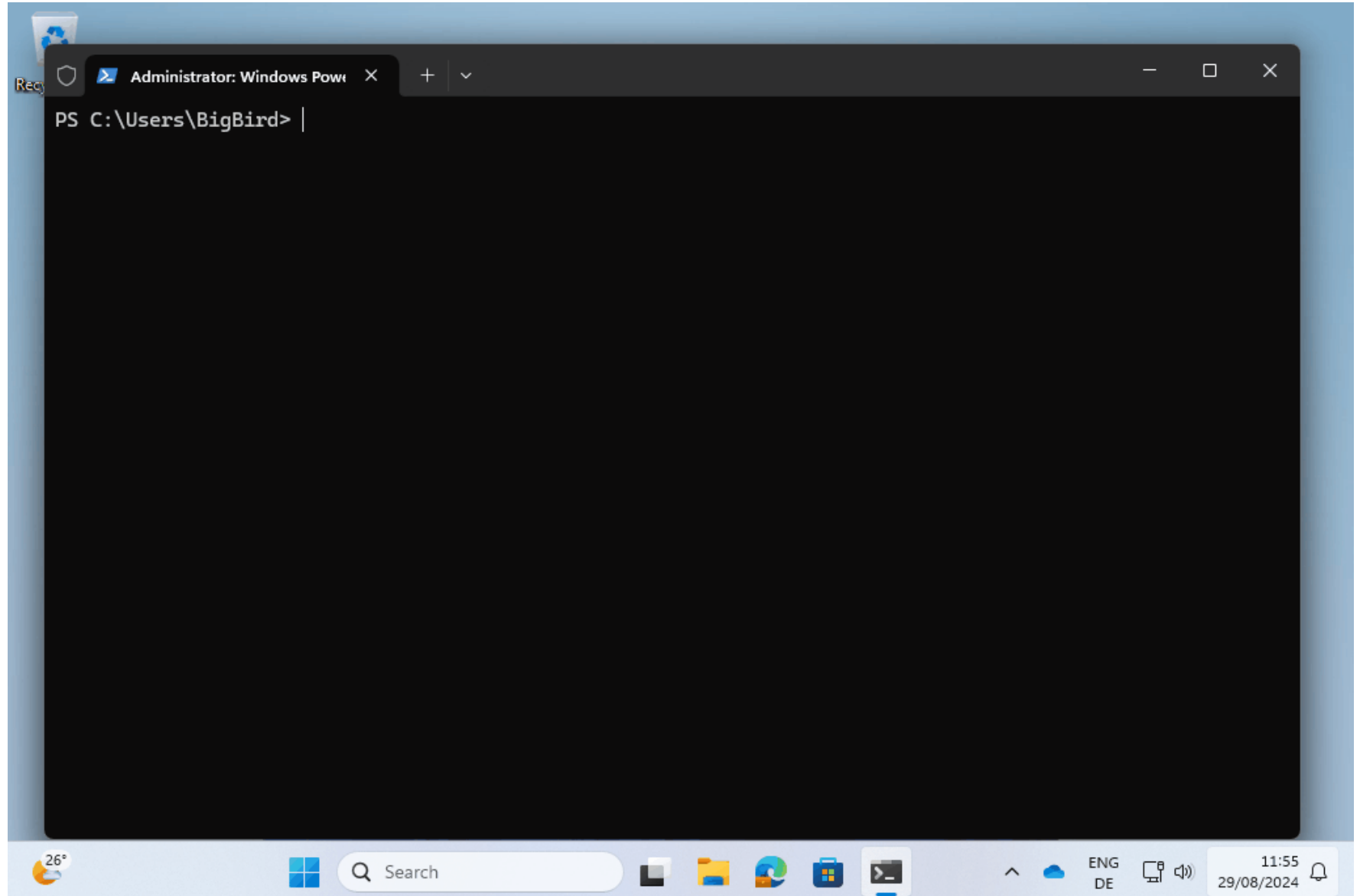
0Ń'6pŷqì í f6ì Łì ũþ; žþ6 Íþ;"> Ñf` ïì

# What's a Name Resolution Policy Table?

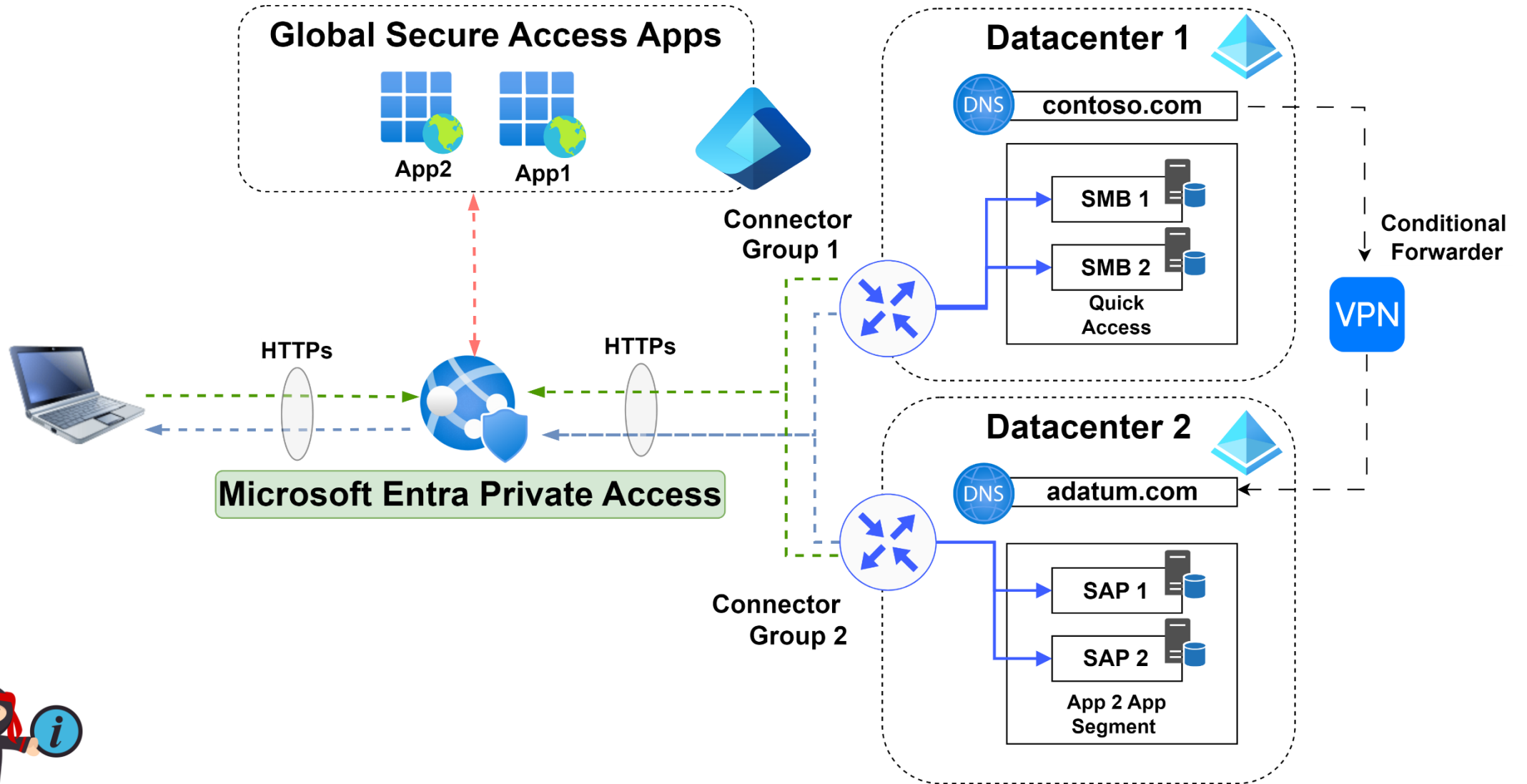
nslookup  
vs.  
Resolve-DnsName

## Custom entries

- Disconnected Environments
- Exclusions for split DNS



# Handling multiple environments



# Access Management and Authentication

## Entra Private Access



## Traditional VPN

### Authenticate every App Segment

Use Conditional Access to enforce your ruleset

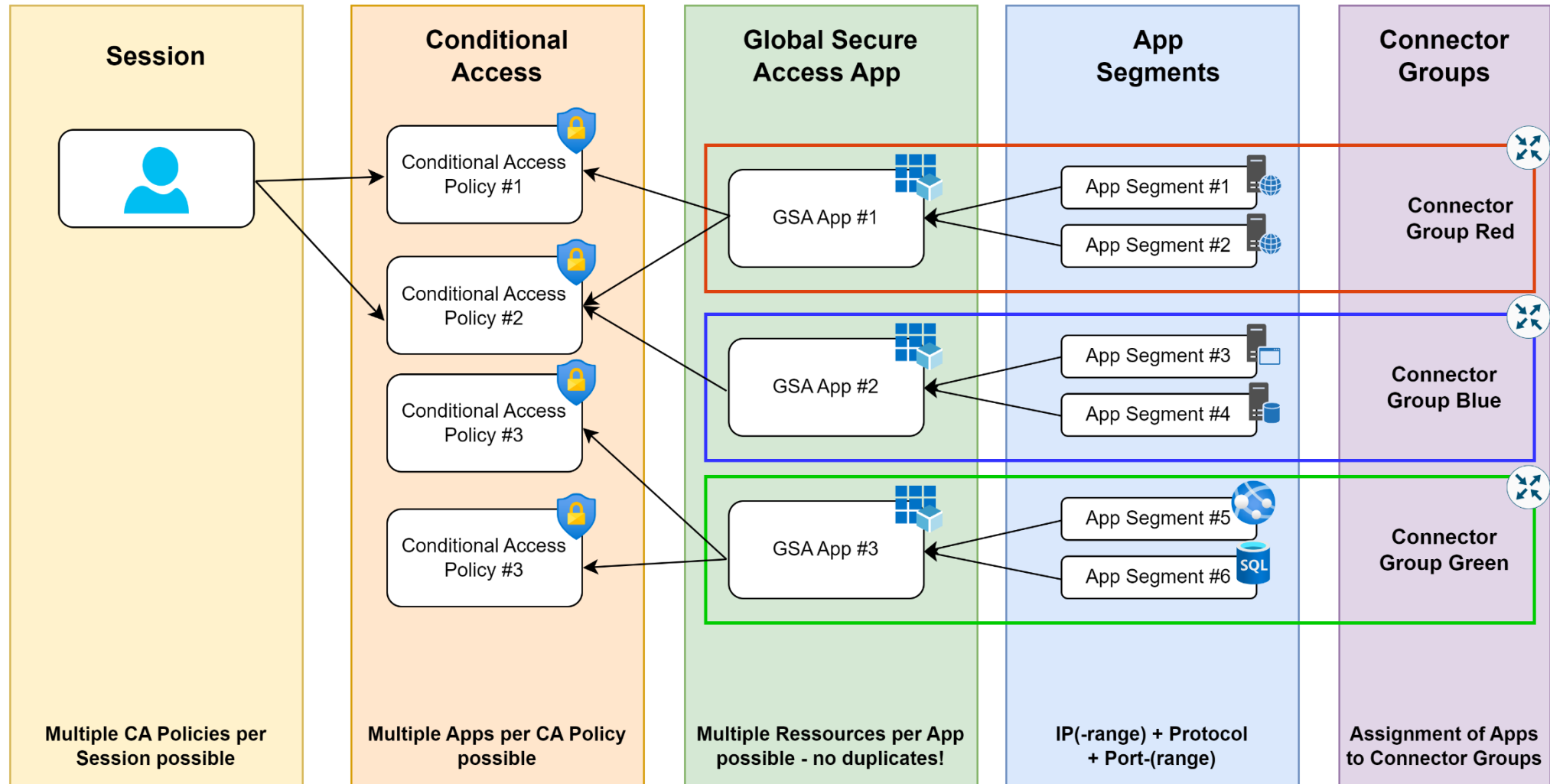


### Authenticate the VPN

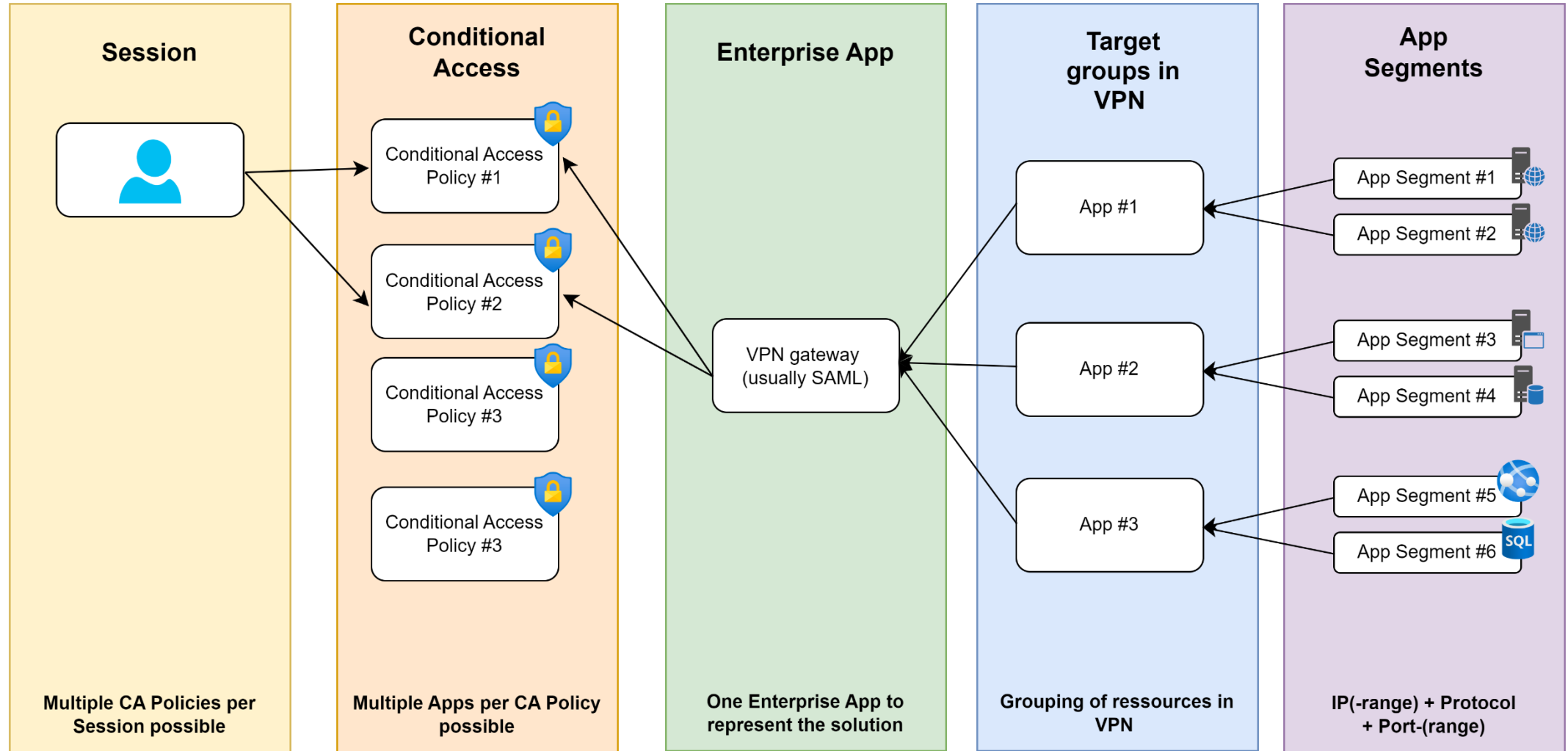
One Authentication for all – usually with long-lived cookies.



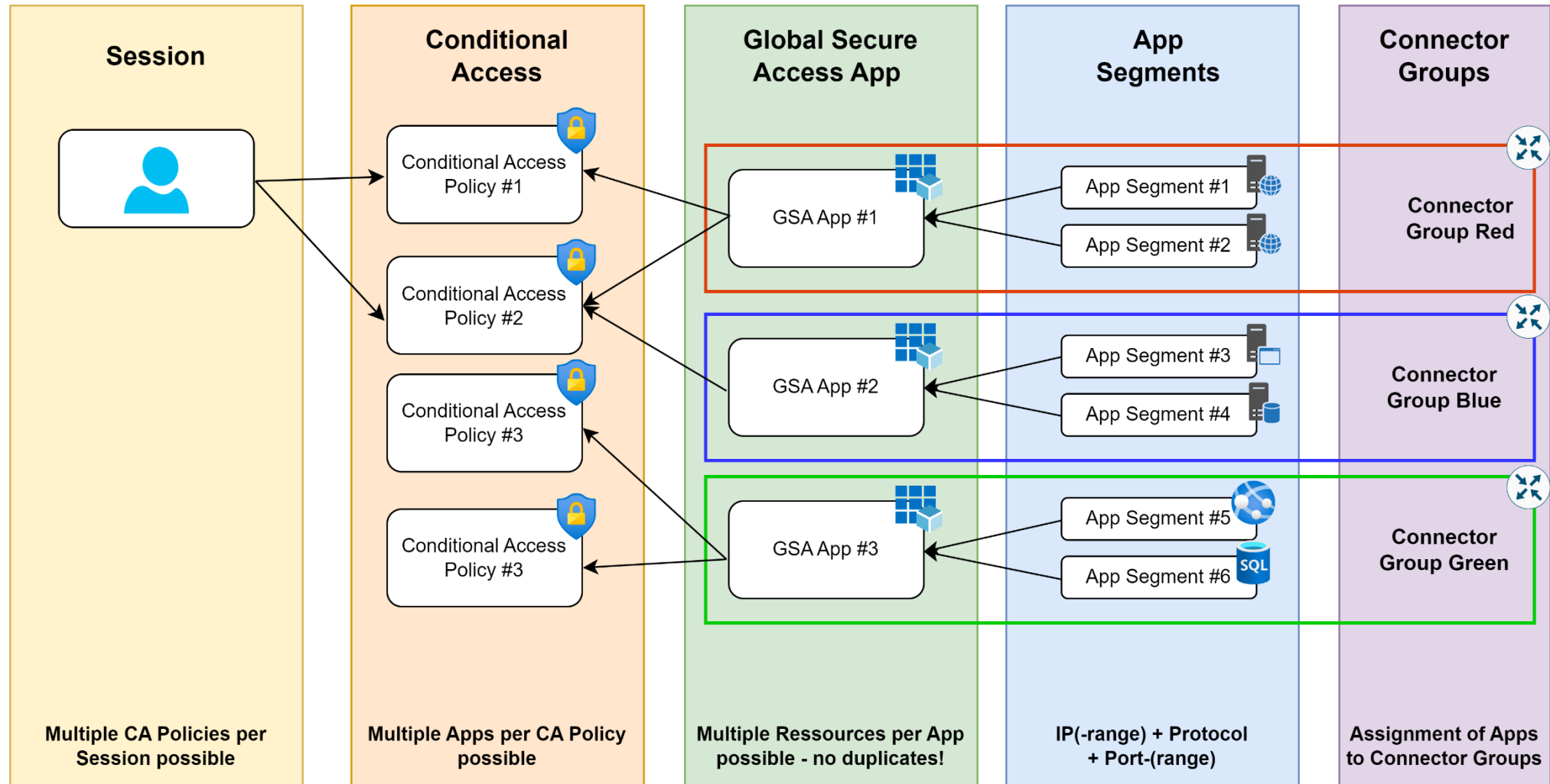
# GSA Conditional Access Integration



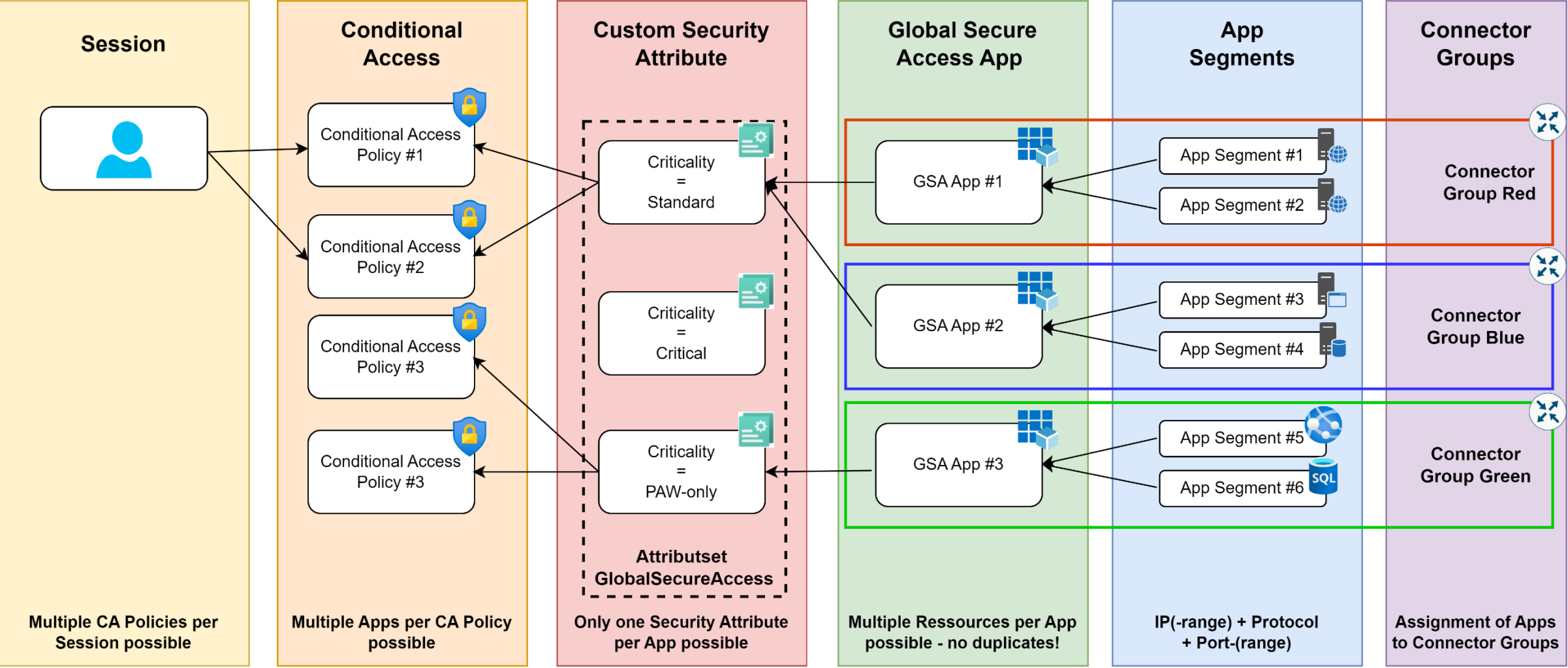
# Conditional Access Integration for VPN



# GSA Conditional Access Integration



# Custom Security Attribute Extension



Ãá ï

Nj 2/3 2/3 üq 4pũũ2/3>"-> f 2/3/ũ p6 i 6ũũ

# Step-up auth for specific app segments

Home > Conditional Access | Policies >

## EPA 1 - Require YubiKey for Admin Access

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

EPA 1 - Require YubiKey for Admin Access

Assignments

Users or workload identities ⓘ

[Specific users included and specific users excluded](#)

Target resources ⓘ

1 app included

Network **NEW** ⓘ

[Not configured](#)

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

[Sign-in frequency - Every time](#)

## Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multifactor authentication ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

☒ Require authentication strength ⓘ

YubiKey Only ▾

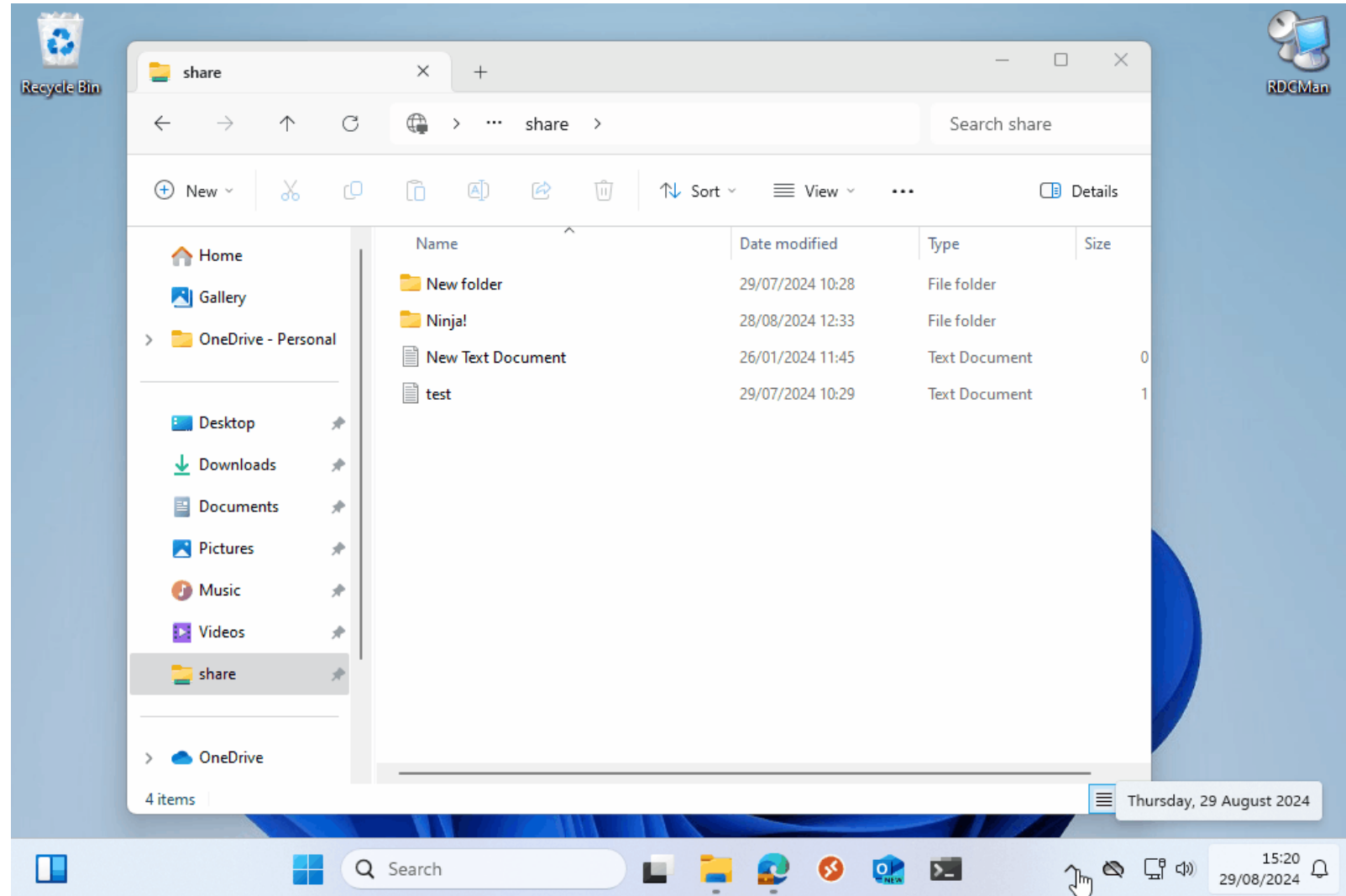
ⓘ To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. [Learn more](#)

☐ Require device to be marked as compliant ⓘ

☐ Require Microsoft Entra hybrid joined device ⓘ

☐ Require approved client app ⓘ  
[See list of approved client apps](#)

☐ Require app protection policy ⓘ  
[See list of policy protected client apps](#)





# Authorization and Single SignOn

## Entra Private Access



## Traditional VPN



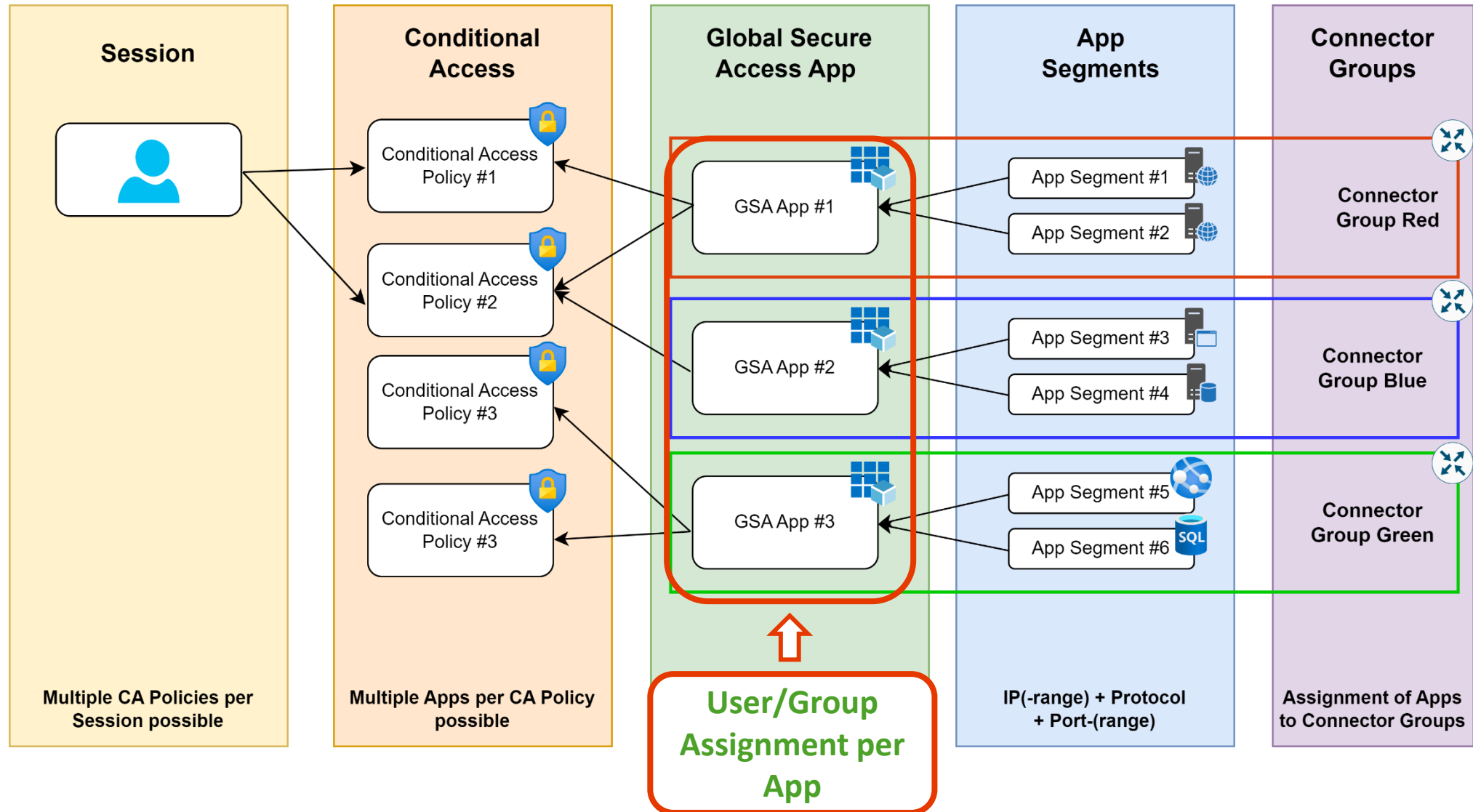
### Native Entra ID integration

Modern AuthN with OAuth2  
AuthZ with Groups and Access Packages

### Loose IDP integration

SAML or RADIUS AuthN  
AuthZ with local groups (or via LDAP )

# Entitlement Management



# Global Secure Access – Portal View

Private Access - GKFelucia File Service | Network access properties

Global secure access application

Overview

Manage

Properties

Owners

Roles and administrators

**Users and groups**

Single sign-on

Network access properties

Custom security attributes

Security

Conditional Access

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

« Got feedback?

Global Secure Access is now generally available. Licensing requirements have been updated. [Learn more](#)

Name \*

Private Access - GKFelucia File Serv...

Connector Group

ZTNA

We recommend at least two active connectors in selected group 'ZTNA'. [Click here to download a connector or manage your connector groups.](#)

Enable access with Global Secure Access client

☒

Application Segment

+ Add application segment

Destination type	Destination	Ports	Protocol	Status	Delete
IP address	192.168.0.21	445	TCP, UDP	Success	

+ Add user/group | Edit assignment | Remove | Update credentials

The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes

Assign users and groups to app-roles for your application here. To create new app-roles for this application, click here.

First 200 shown, to search all users & groups

Display Name	Object Type
<input type="checkbox"/> Bert	User
<input type="checkbox"/> Big Bird	User

# Private Access und Identity Governance

The screenshot displays the 'My Access' section of the Microsoft Entra ID portal. At the top, the user 'glueckkanja gab' is logged in, and the 'My Access' tab is selected. A search bar is available for finding packages by name, description, or resources. The main area is titled 'Access packages' and shows a list of available packages. One package, 'Global Secure Access - Private Access GKFelucia Fileservice', is highlighted. To the right, a detailed view of this package is shown, listing its resources: 'Groups and Teams (2)' and 'Applications (1)'. The 'Groups and Teams' section includes 'Entra Private Access - GKFEUCIAAPP1 - Share' and 'Software - GSA Client'. The 'Applications' section includes 'Private Access - GKFelucia File Service'. A green box labeled 'Writeback via Entra Cloud Sync' points to the 'Entra Private Access' resource.

glueckkanja gab My Access Search packages by name, description or resources

Access packages

**Access packages**

Access groups and teams, SharePoint sites, applications, and more in a single package. Select what you're looking for.

Available (6) Active (2) Expired (0)

Name ↑

Global Secure Access - Private Access Basic

Global Secure Access - Private Access GKFelucia Fileservice

**Global Secure Access - Private Access GKFelucia...**

Access to the share at GKFEUCIAAPP1

Resources (3)

Groups and Teams (2)

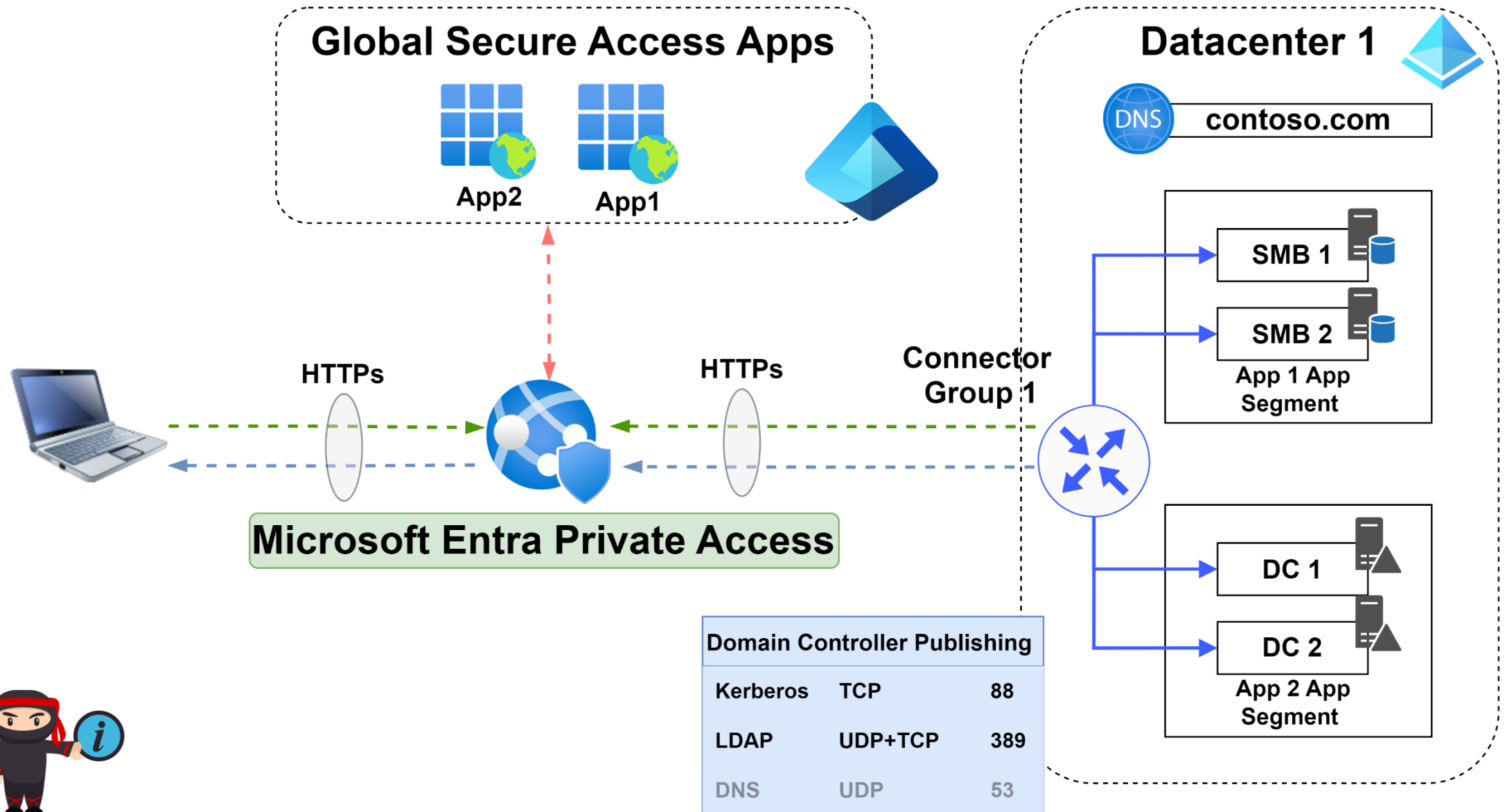
- E** **Entra Private Access - GKFEUCIAAPP1 - Share**  
Role assigned - Member
- SC** **Software - GSA Client**  
Role assigned - Member

Applications (1)

- P** **Private Access - GKFelucia File Service**  
AppId: eae4a6dc-e5d5-4405-b6a0-2c1ff3bd9a11  
Role assigned - User

**Writeback via Entra Cloud Sync**

# Using Kerberos in Private Access

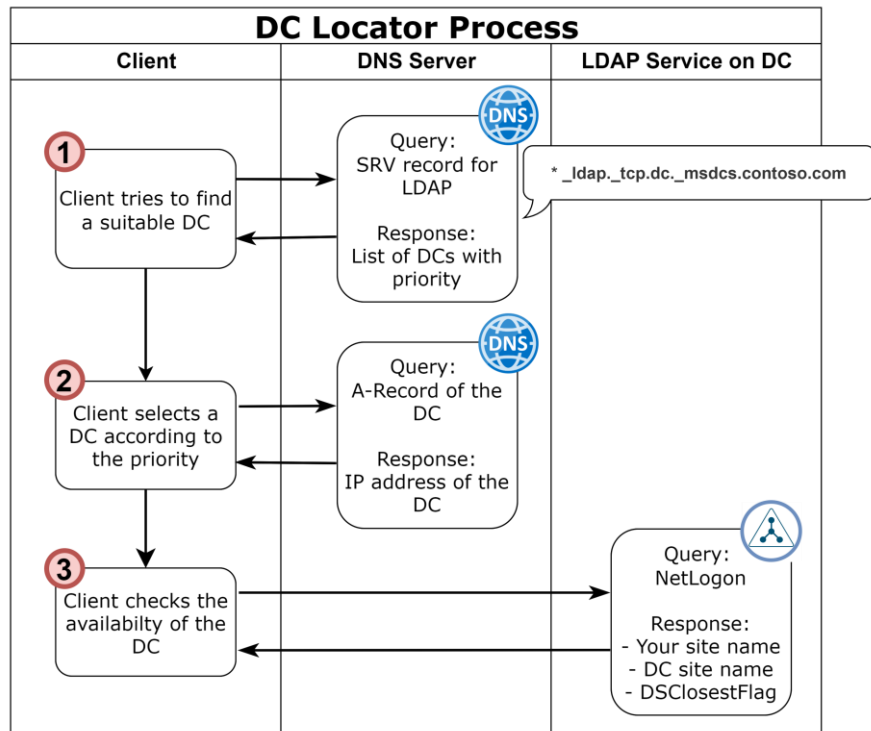


ÃÁ ĩ

Õ "óı þ ũÉì ð ð ũÀ ũ'óì ũ Āþ í  
Ñ ũ ĩ ũ' f ũ A>>ì ũ❤



# Kerberos Cloud Trust + Private Access



# Threat Intel and Incident Response

## Entra Private Access



### Full Integration with MS Security

Identity Protection + Sentinel Integration  
CAE is already at the architecture diagrams



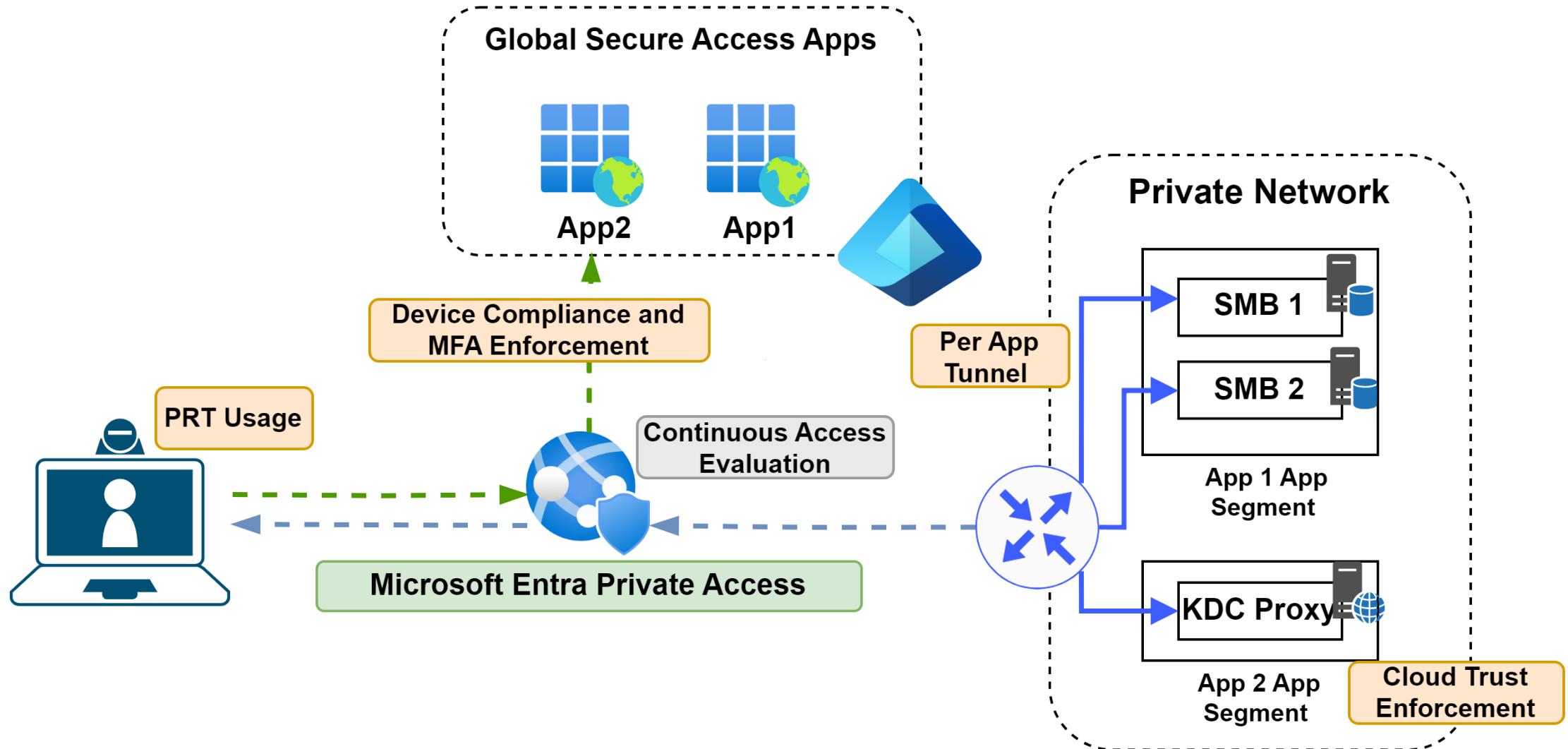
## Traditional VPN



### Revoke Sessions in the GUI

maybe there is a custom SOAR  
integration

# Overview Security Features



# Full integration in the MS Security Stack

## Integrations:

- Conditional Access + Identity Protection
- Easy Sentinel ingest via Entra Diagnostic Settings
- Unified Security Operations Platform
  - Sentinel
  - Defender XDR

## Native Alerts like:

- **Token and device inconsistency:** The original token is used on a different device.

### Inspect record

Assets

Process tree

All details

TimeGenerated	:	
Jul 31, 2024 8:37:56 PM		
UserPrincipalName	:	
BigBird@gkfelucia.net		
DeviceName	:	
<a href="#">appproxy1.gkfelucia.net</a>		
TrafficType	:	
private		
AccessType	:	
QuickAccess		
SourceIp	:	
95.81.19.76		
SourcePort	:	
50358		
DeviceOperatingSystem	:	
Windows 11 Enterprise		
ConnectorName	:	
AppProxy1.gkfelucia.net		
ConnectorInternalIP	:	
IPAddress	SubnetPrefix	AddressType
192.168.0.40	24	Private
DestinationPort	:	
88		
DestinationFqdn	:	
gkfeluciadc1.gkfelucia.net		

# What's new and next?



**NEW**

**macOS and iOS Client  
in public preview**

**NEW**

**App Discovery**

**NEW**

**Universal Continuous  
Access Evaluation**

**NEXT**

**Multi-geo connectors**

**NEXT**

**Private Access for  
Domain Controllers**

---

Thank you!