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

Christopher Brumm

About Me

Christopher Brumm

Cloud Security Architect @glueckkanja

Focus

Identity + Security
in Microsoft Cloud

From

Hamburg, Germany

My Blog

chris-brumm.com

Certifications

CISSP, various MS certs

Hobbies

Family, Traveling, Pen & Paper RPG

Contact

@cbrhh

What is the Zero Trust solution for OnPrem Access?

Microsoft Entra Private Access

www.wpninjas.eu
#WPNinjaS

Any user, any device

Identities

Endpoints

Remote networks

Conditional Access in Entra ID

Continuous access evaluation (CAE)

Dedicated tunnels

Anywhere

Dedicated tunnels

All private apps and resources

Multi-cloud

Connectors

Corporate network

Web apps

RDP/SSH

SMB, FTP

ERP (SAP,...)

Printers

Microsoft's Identity-centric Security Service Edge (SSE) solution

Private Access

Key Security Capabilities

- Zero-Trust Network Access
- Broad Application Support
- Identity-centric security controls
- Segmented App access
- Conditional Access & modern authentication
- Private resource discovery
- Intelligent Local Access (Coming soon)
- Audit logging
- TLS termination and inspection (Coming soon)
- Web application firewall (Coming soon)

Source: techcommunity.microsoft.com

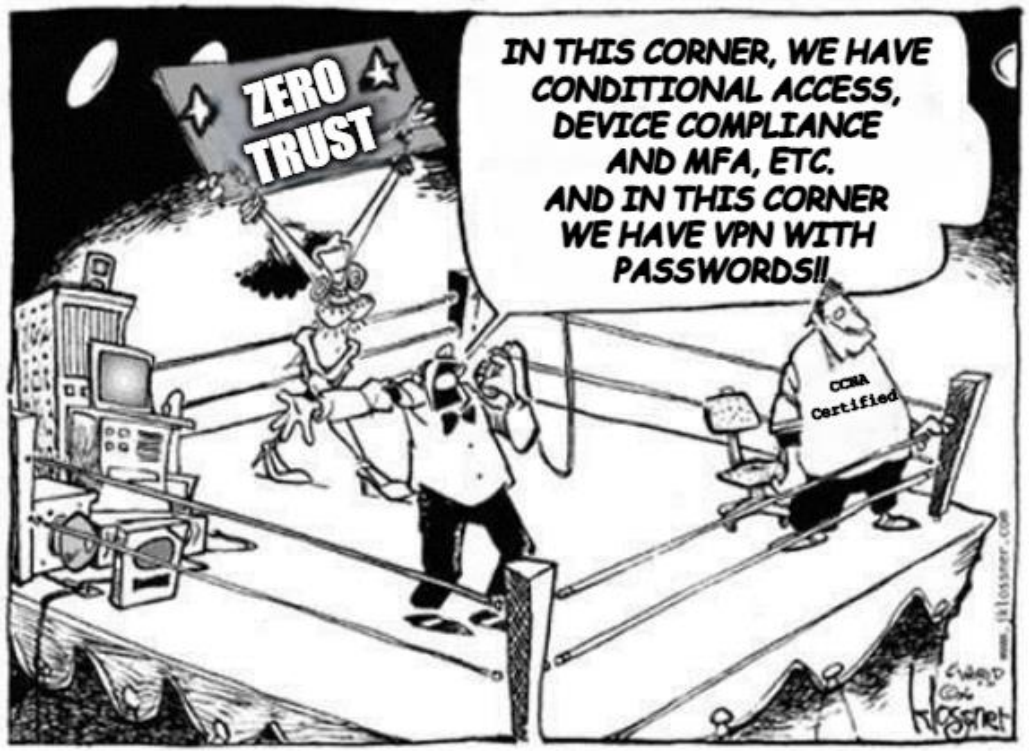
A match in 4 rounds

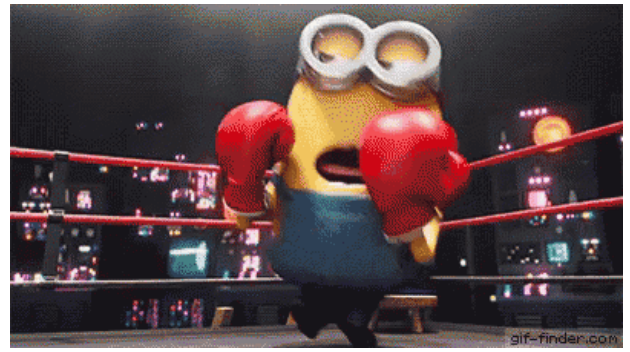
Connectivity and Name Resolution

Access Management and Authentication

Authorization and Entitlement Management

Threat Intel and Incident Response





Connectivity and Name Resolution

www.wpninjas.eu
#WPNinjaS

Entra Private Access

All sessions are cloud terminated

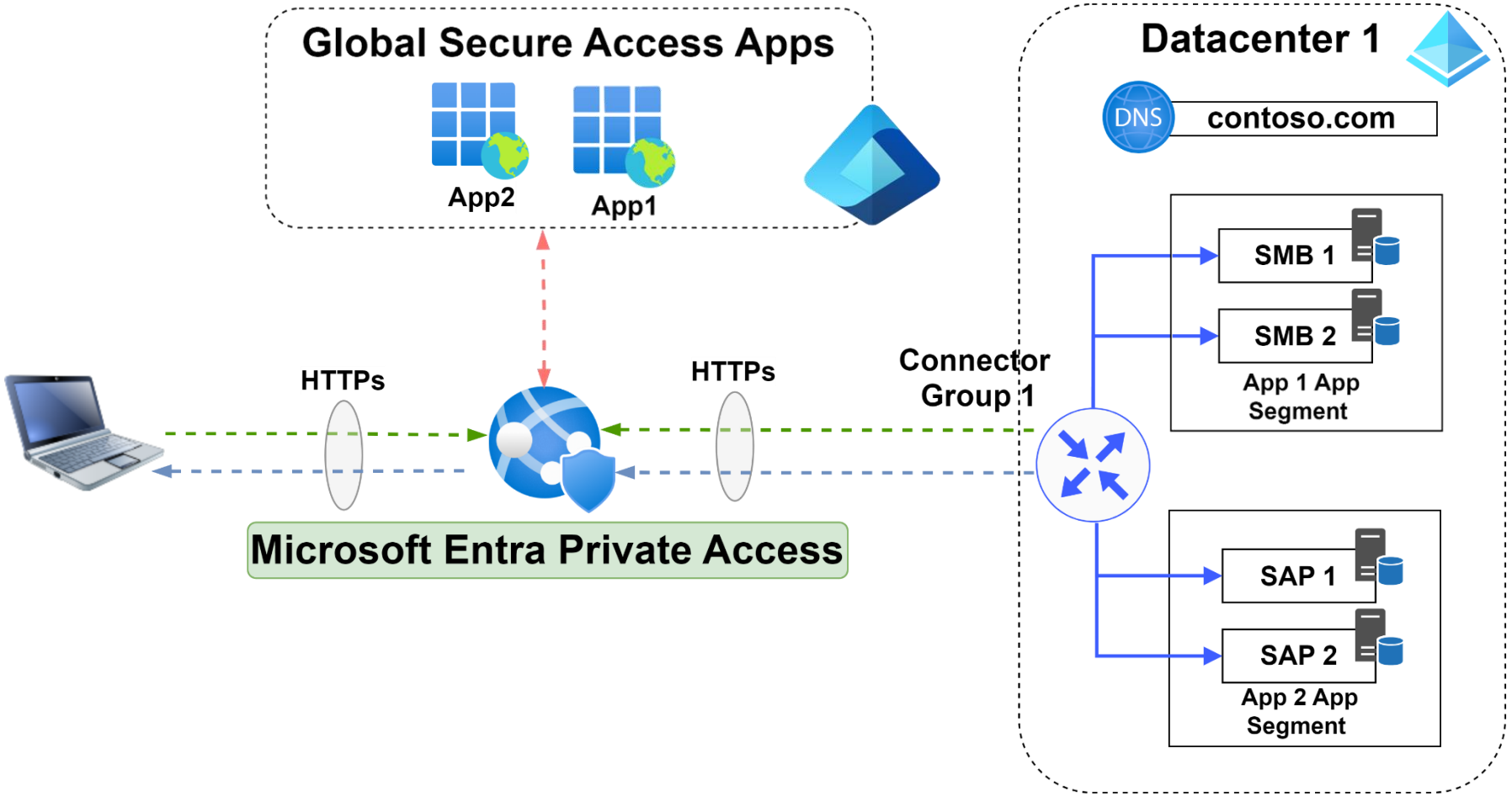
Transparent integration of Complex, disconnected environments

Traditional VPN

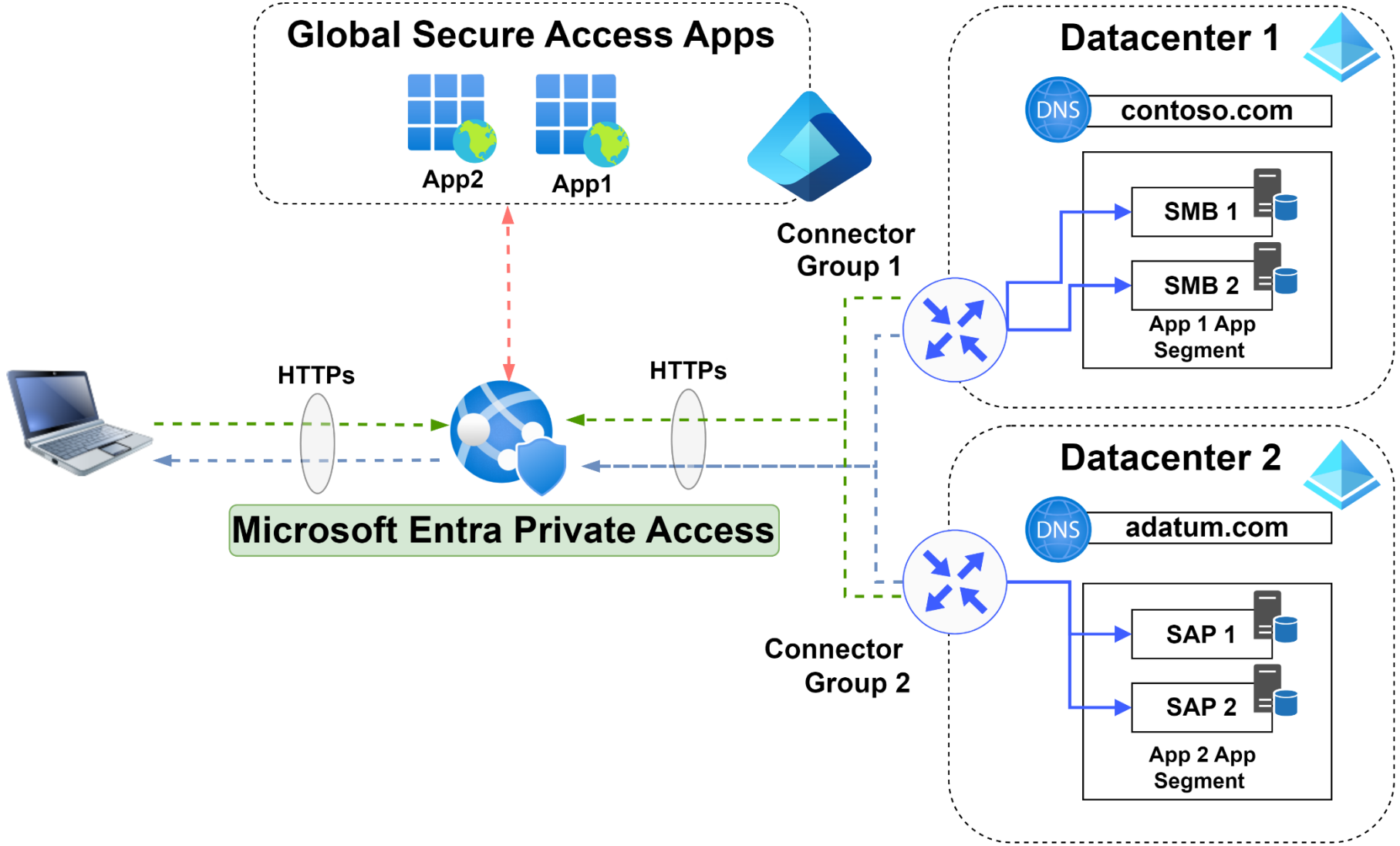
Please choose your datacenter

and route traffic to the others through your WAN

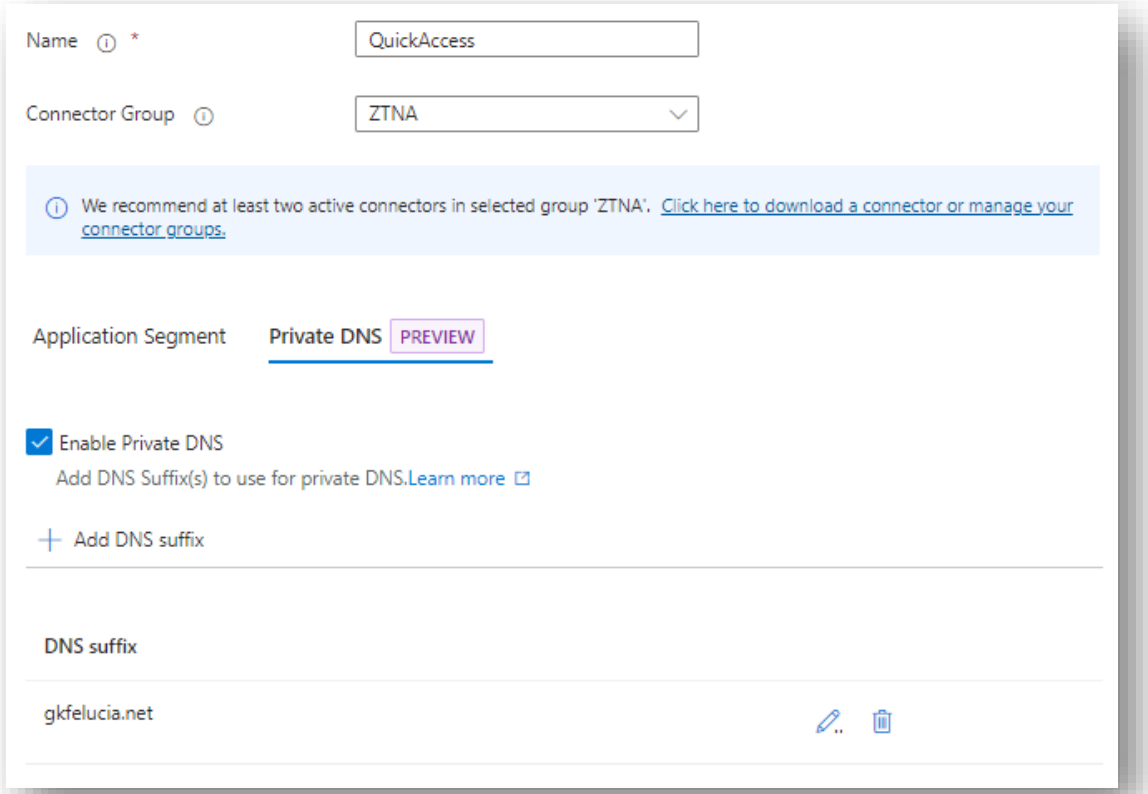
Let‘s start with a simple Deployment

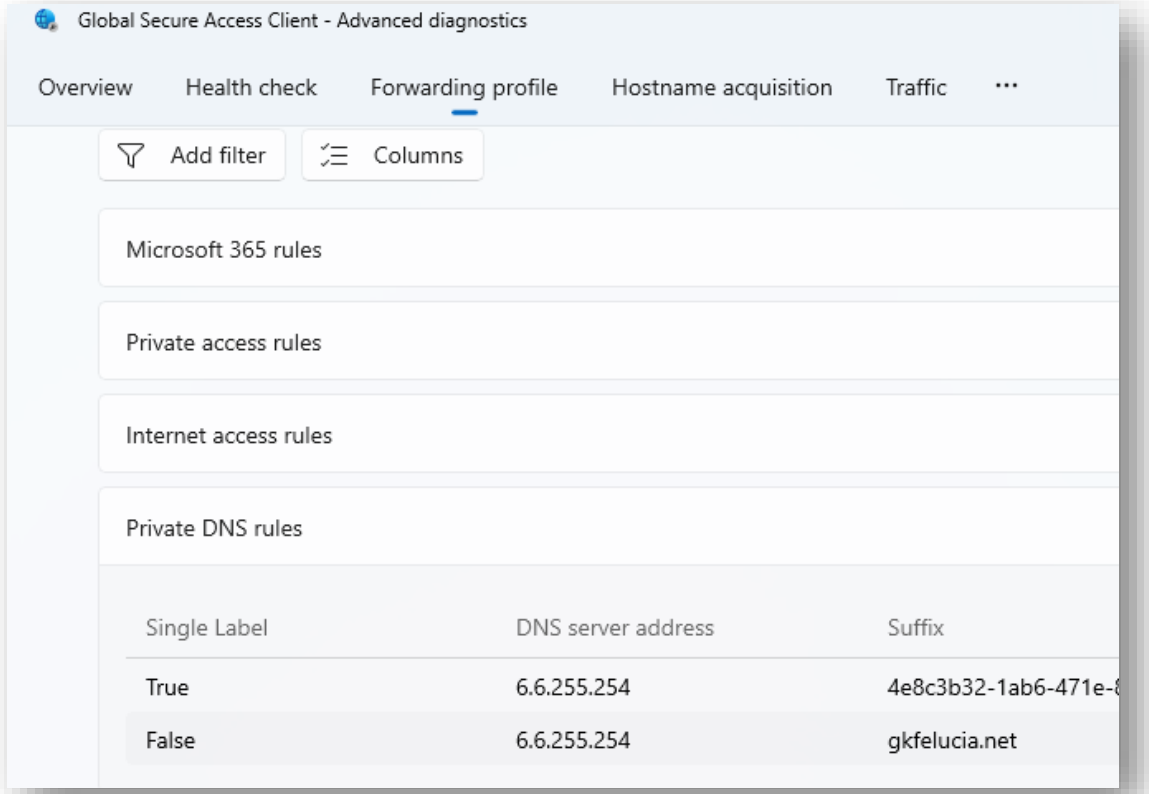


and move to a more complex scenario



Enabling the builtin DNS feature

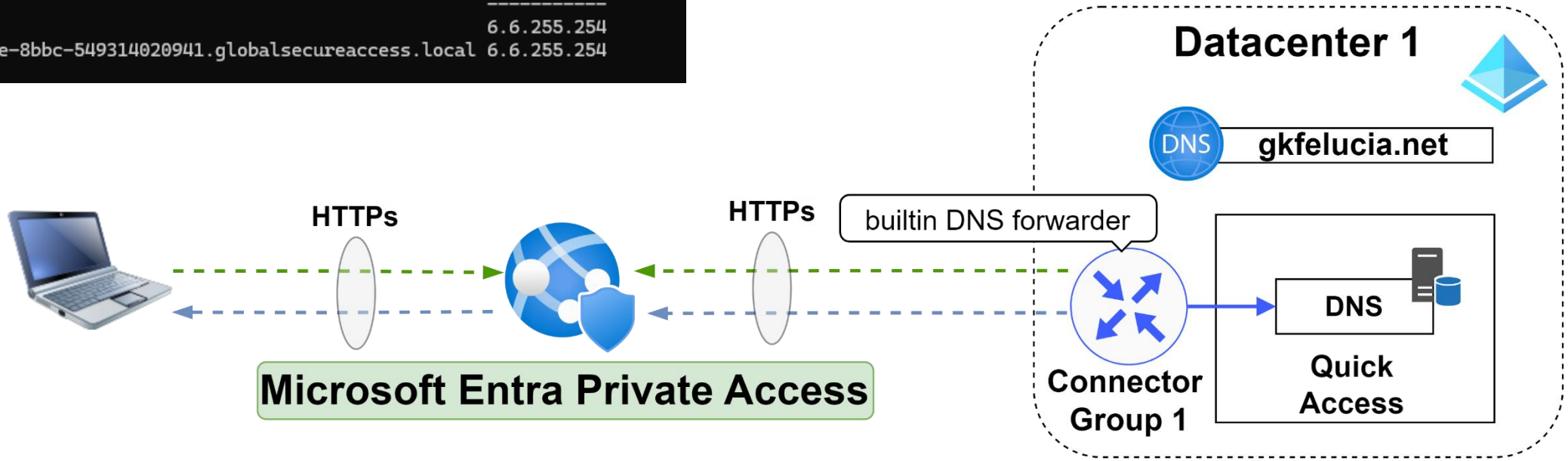




How does it work?


```
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
```

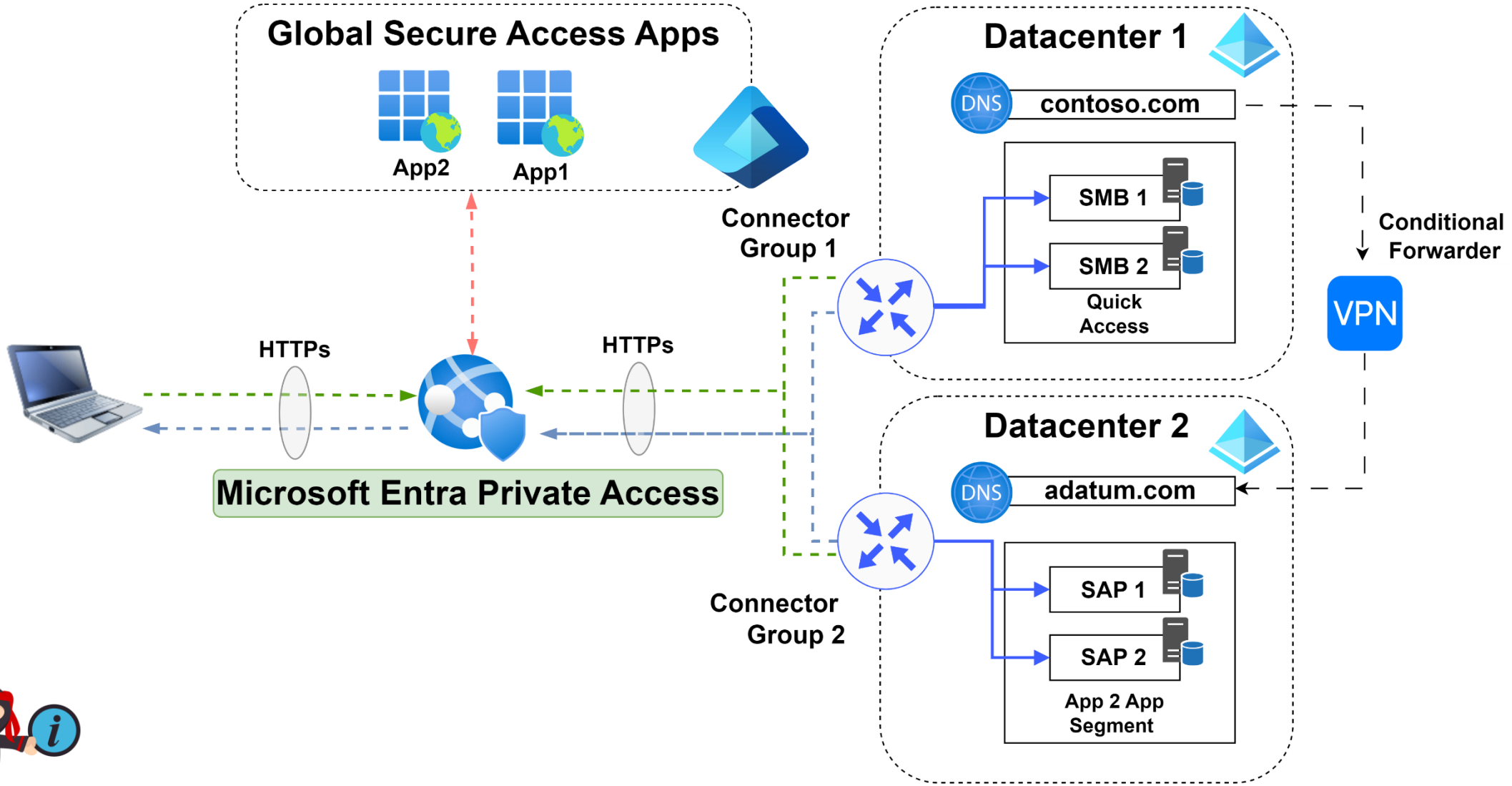


Demo

Using the Name Resolution Policy Table

Handling multiple environments

www.wpninjas.eu
#WPNinjaS



Access Management and Authentication

www.wpninjas.eu
#WPNinjaS

Entra Private Access

Authenticate every App Segment

Use Conditional Access to enforce your ruleset

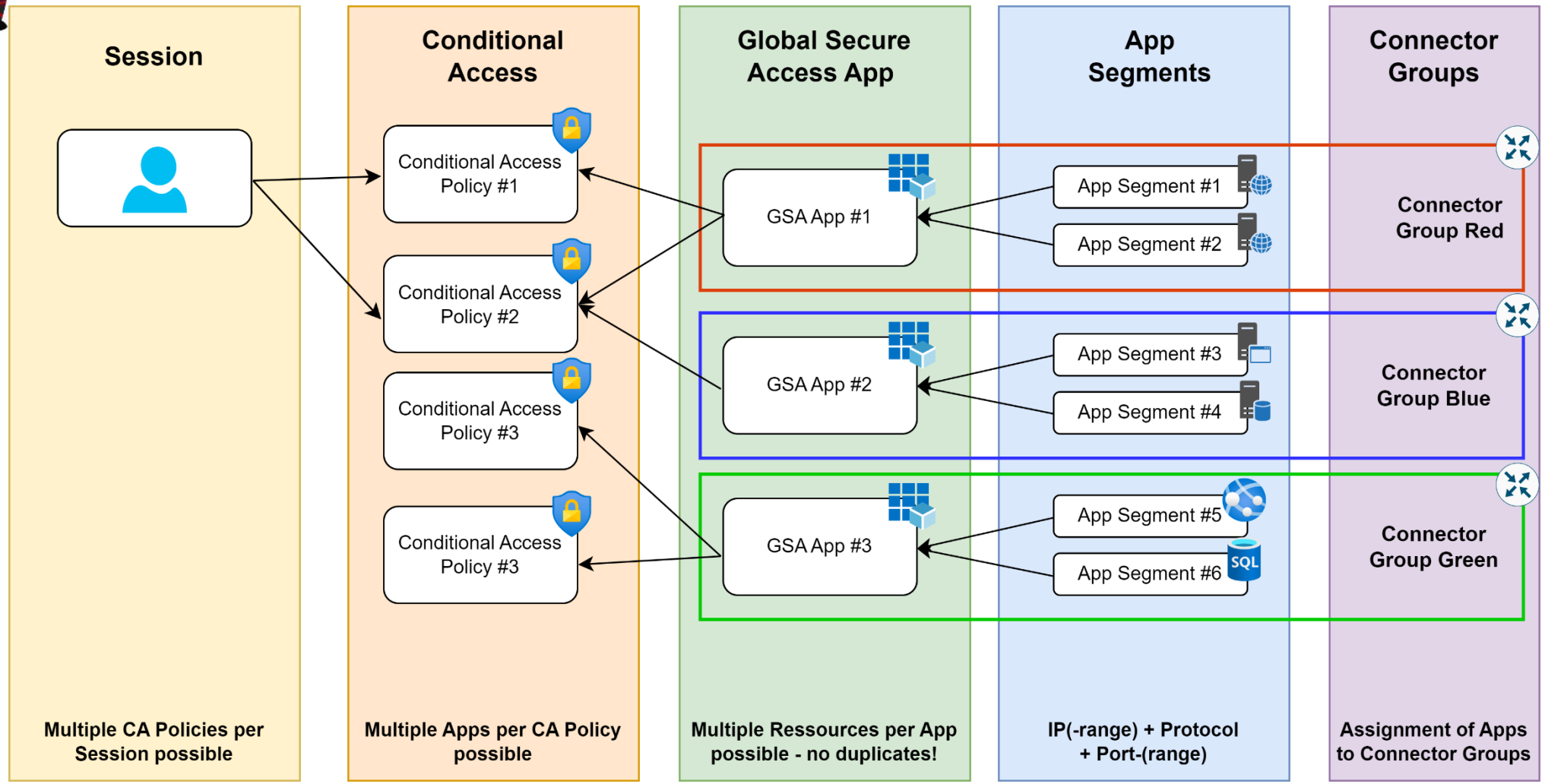
Traditional VPN

Authenticate the VPN

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

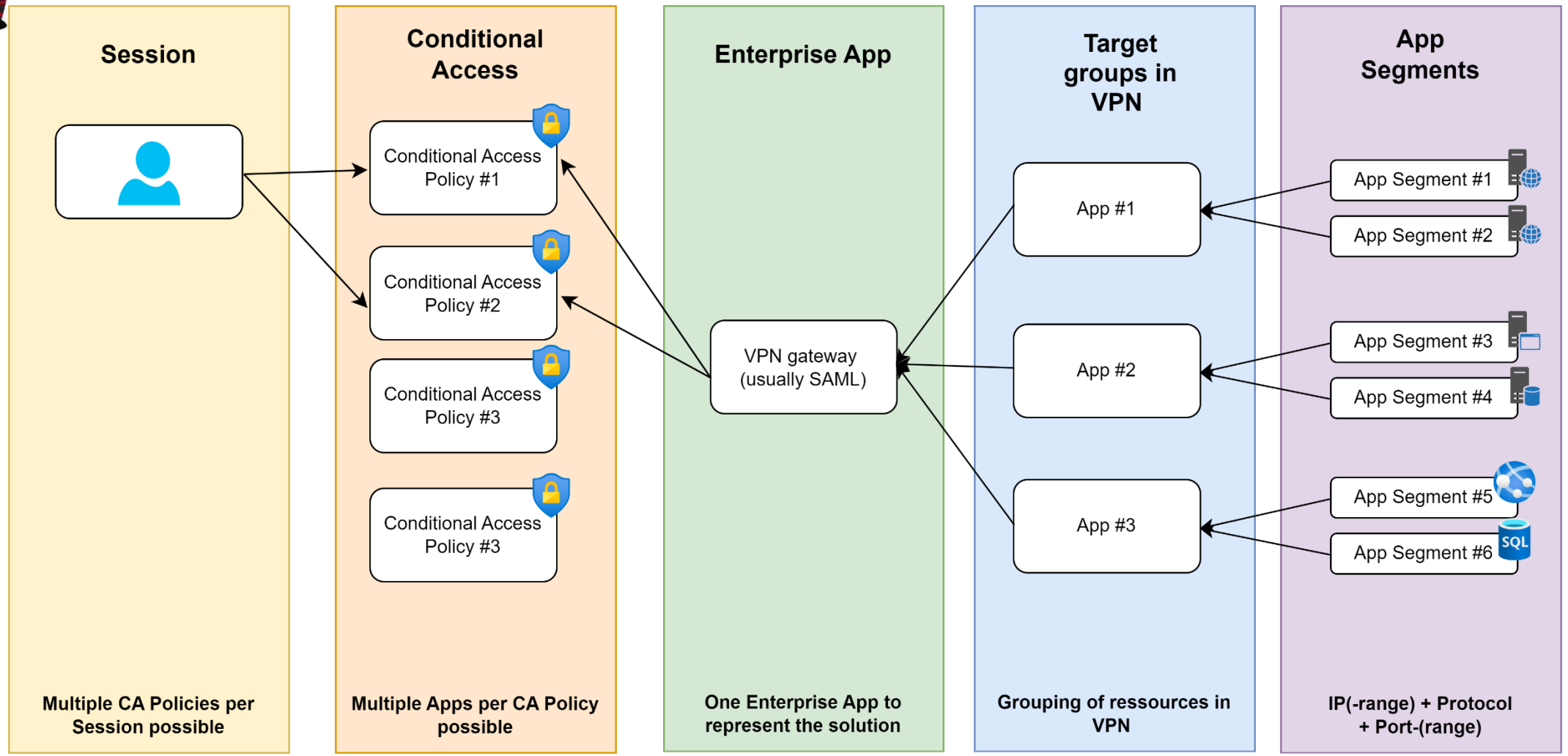
GSA Conditional Access Integration

www.wpninjas.eu
#WPNinjaS



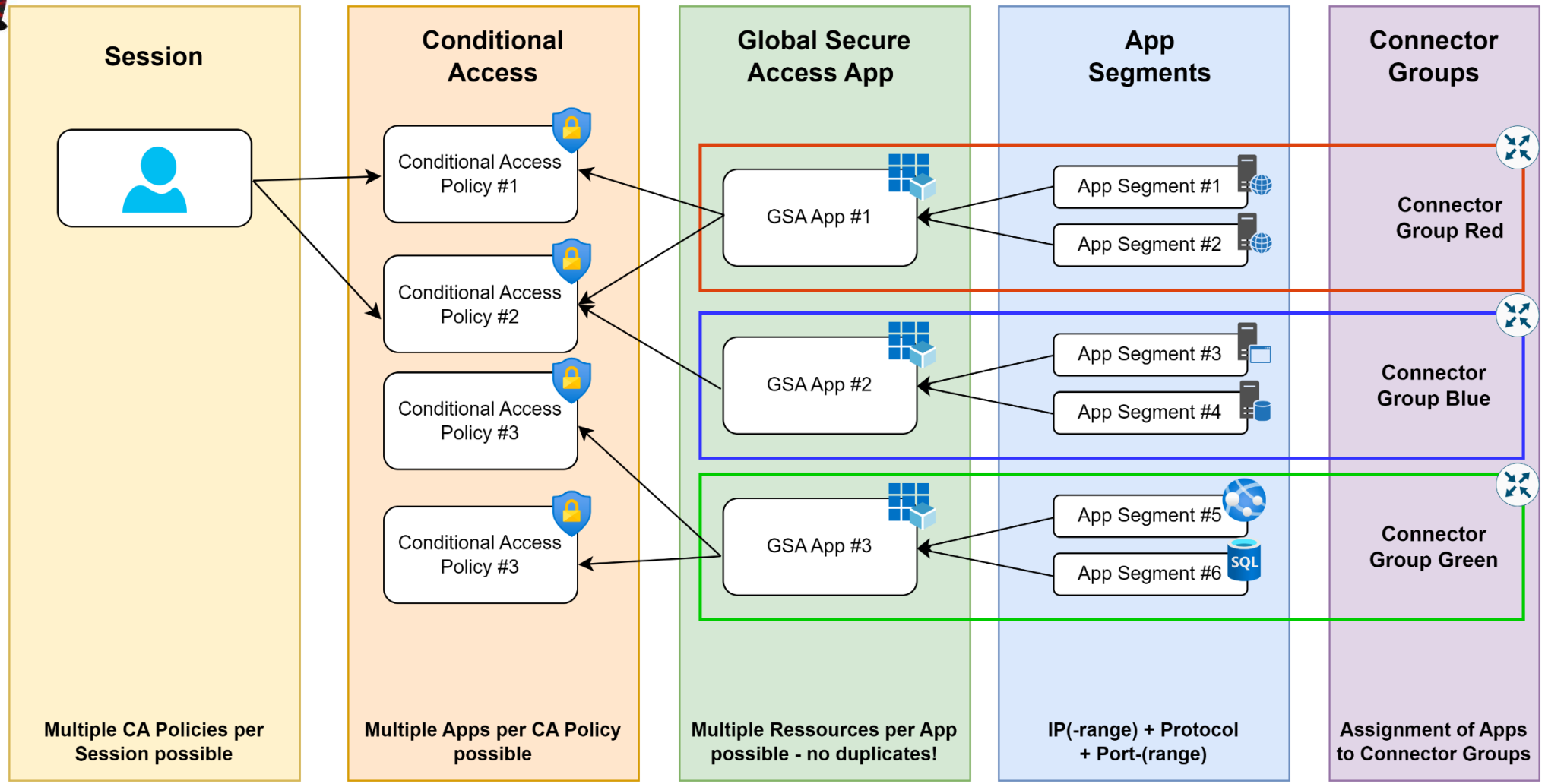
Conditional Access Integration for VPN

www.wpninjas.eu
#WPNinjaS



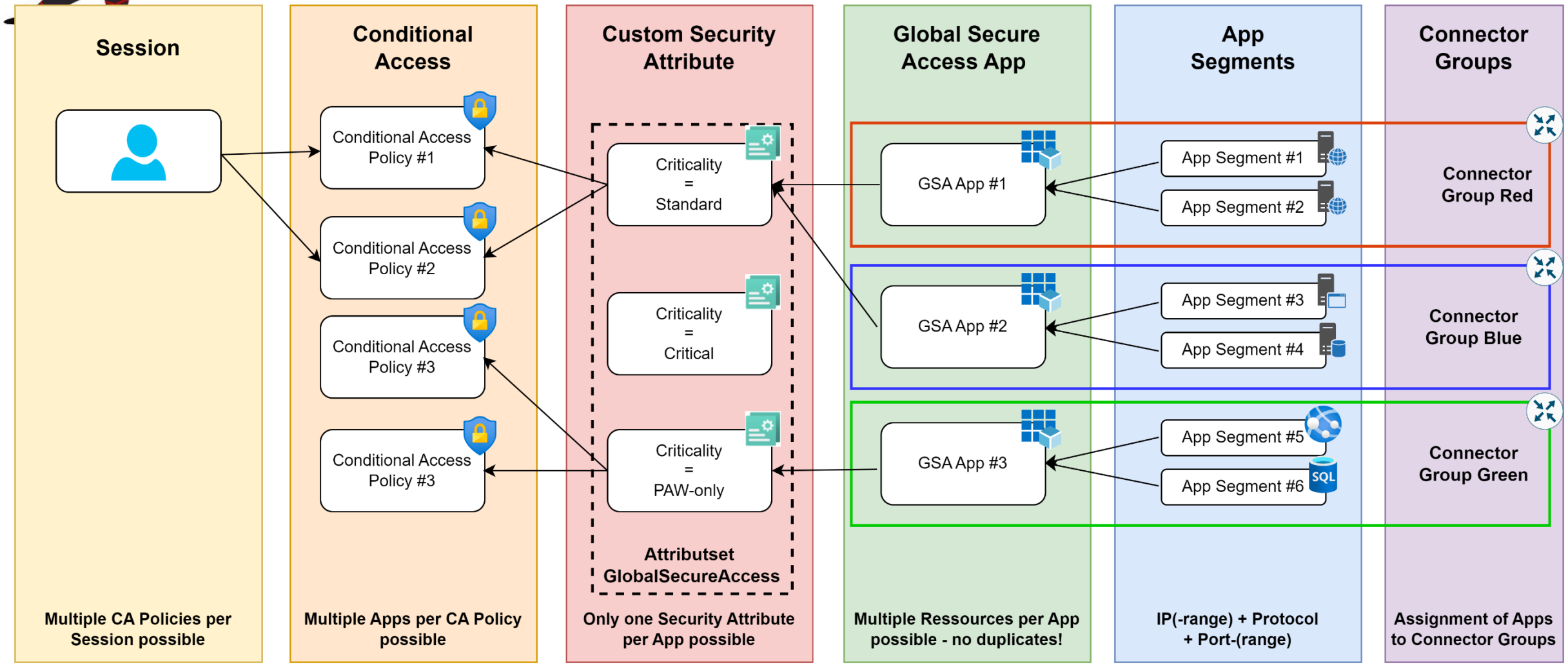
GSA Conditional Access Integration

www.wpninjas.eu
#WPNinjaS



Custom Security Attribute Extension

www.wpninjas.eu
#WPNinjaS



Demo

Step-up auth for specific app segments

Authorization and Single SignOn

www.wpninjas.eu
#WPNinjaS

Entra Private Access

Native Entra ID integration

Modern AuthN with OAuth2
AuthZ with Groups and Access Packages

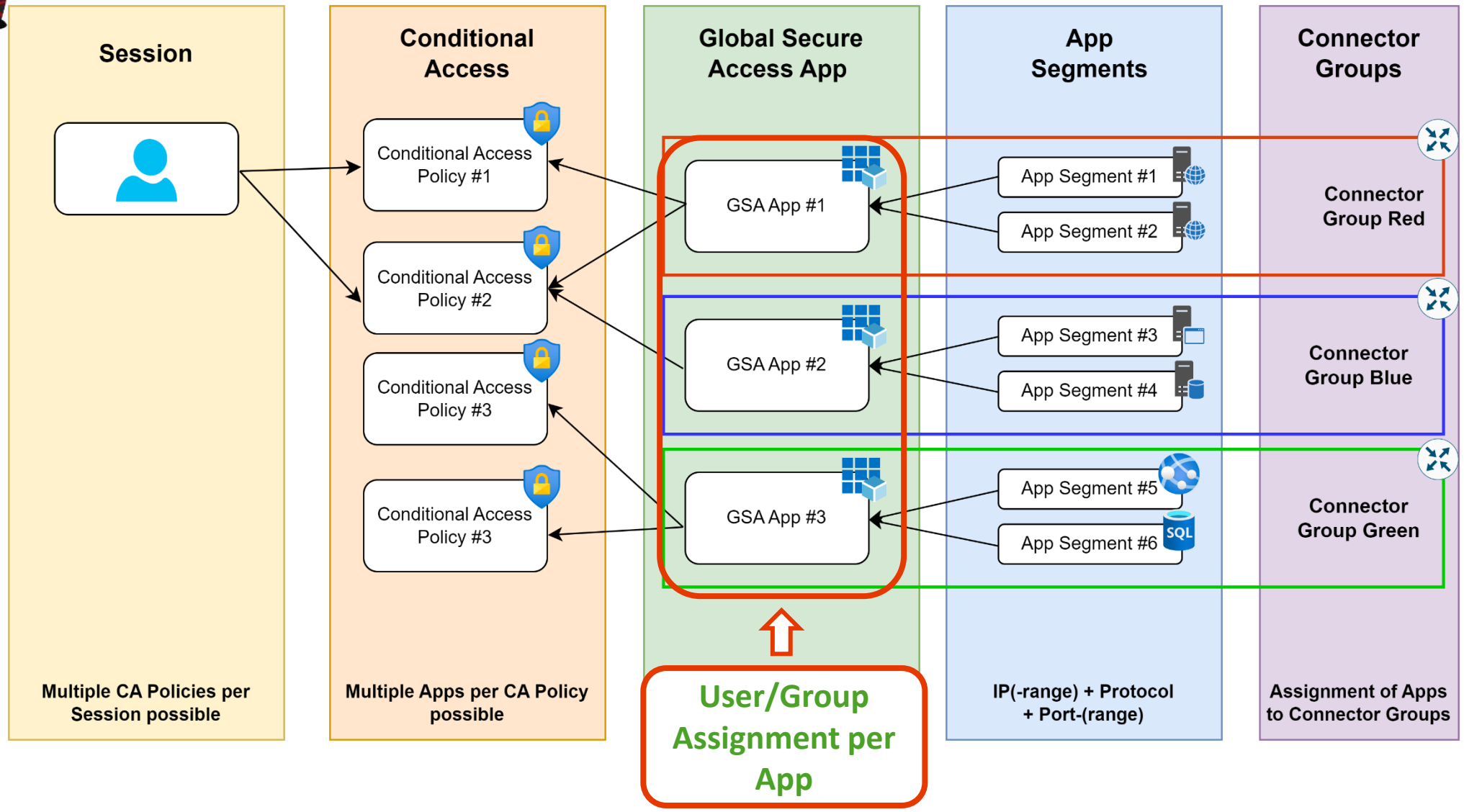
Traditional VPN

Loose IDP integration

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

Entitlement Management

www.wpninjas.eu
#WPNinjaS



Global Secure Access – Portal View

www.wpninjas.eu
#WPNinjaS

Private Access - GKFelucia File Service | Network access properties

Global secure access application

Got feedback?

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

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 thi

First 200 shown, to search all users & gro...

Display Name	Object Type
Bert	User
Big Bird	User

Private Access und Identity Governance

www.wpninjas.eu
#WPNinjaS

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. Sele
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 GKFELUCIAAP1

Resources (3)

Groups and Teams (2)

E — Entra Private Access - GKFELUCIAAPP1 - Share
Role assigned - Member

SC — Software - GSA Client
Role assigned - Member

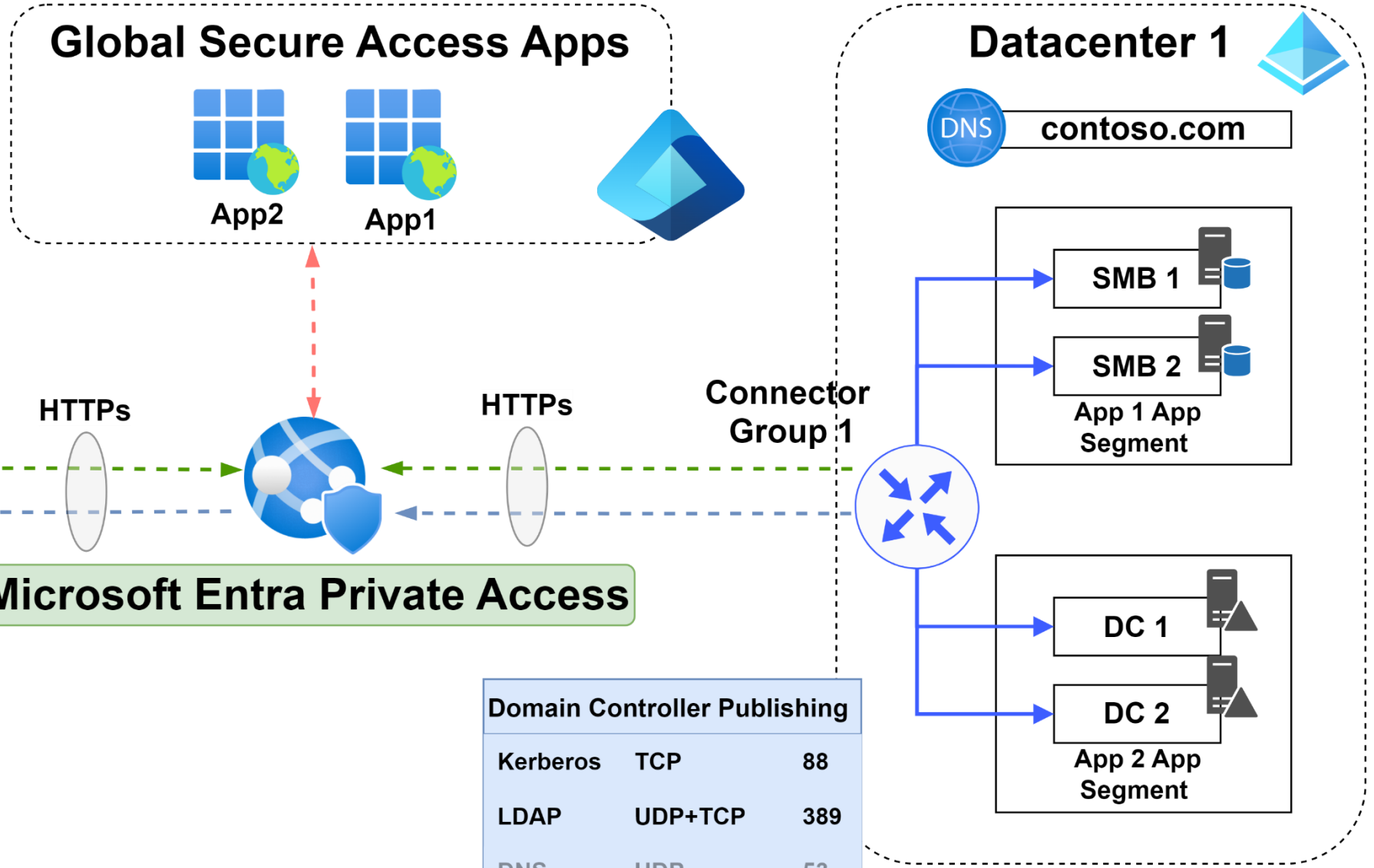
Applications (1)

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

www.wpninjas.eu
#WPNinjaS



Domain Controller Publishing		
Kerberos	TCP	88
LDAP	UDP+TCP	389
DNS	UDP	53

Demo

Windows Hello for Business

+ Cloud Trust

+ Private Access

Threat Intel and Incident Response

www.wpninjas.eu
#WPNinjaS

Entra Private Access

Traditional VPN

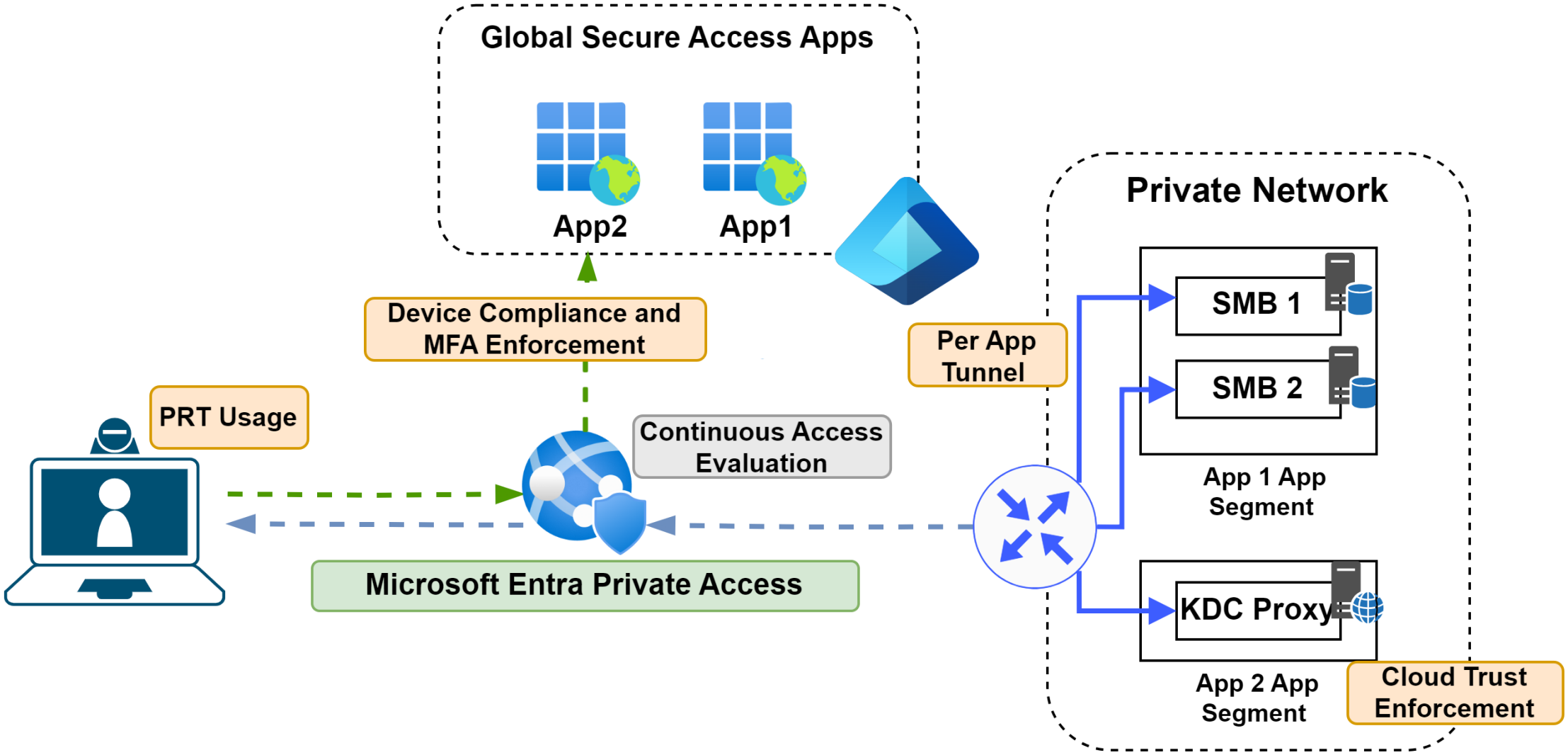
Full Integration with MS Security

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

Revoke Sessions in the GUI

maybe there is a custom SOAR integration

Overview Security Features



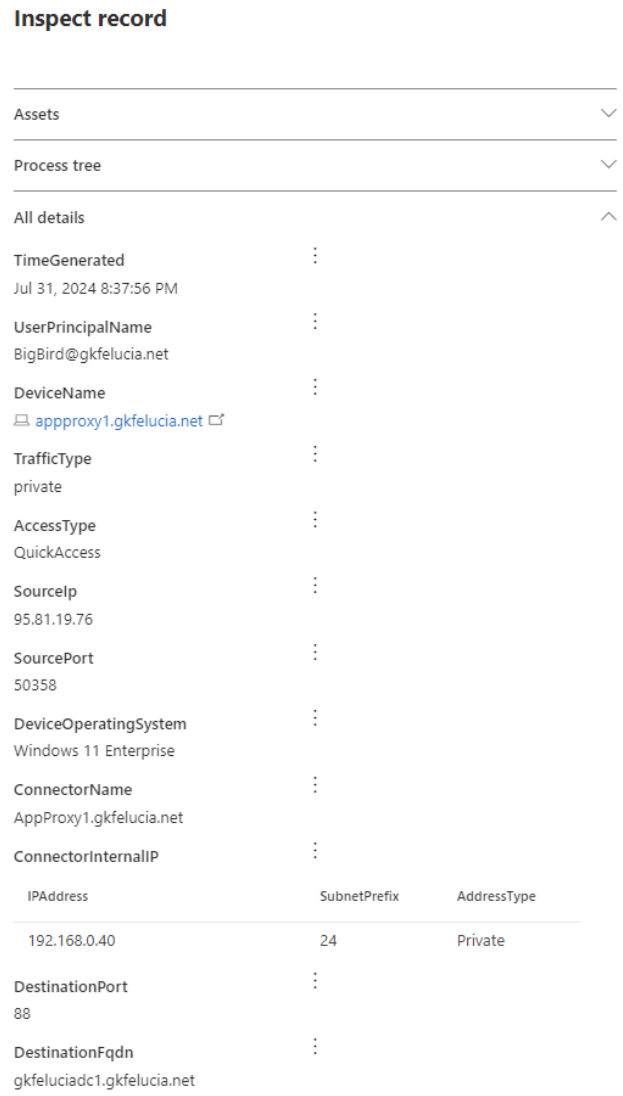
Full integration in the MS Security Stack

Integrations:

- Conditional Access
- Identity Protection
- Unified Security Operations Platform
  - Sentinel
  - Defender XDR

Native Alerts like:

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



Overview

Entra Private Access

All sessions are cloud terminated

Transparent integration of Complex, disconnected environments

Authenticate every App Segment

Use Conditional Access to enforce your ruleset

Native Entra ID integration

Modern AuthN with OAuth2
AuthZ with Groups and Access Packages

Full Integration with MS Security

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

Traditional VPN

Please choose your datacenter

and route traffic to the others through your WAN

Authenticate the VPN

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

Loose IDP integration

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

Revoke Sessions in the GUI

maybe there is a custom SOAR integration

Recommendation

Here more about Entra Private and Internet Access at Peter Lenzkes Sessions!

Thank you Sponsors

www.wpninjas.eu
#WPNinjaS

Diamond Sponsor

Microsoft

Platinum Sponsors

2Pint

PATCH MY PC

RECAST SOFTWARE

glueck kanja

Gold Sponsors

nerdio

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

controlUP

Rimo3

adaptiva

Silver Sponsors

APENTO

UMB creating time®

EPIC FUSION
BRING IT ALL TOGETHER

water
IT Security & Defense

www.wpninjas.eu
#WPNinjaS

We love Feedback

https://wpninjas24.sched.com/

Great Session!

Okay Session!

Not so okay Session!

Workplace Ninja Summit 2024