What's New and What's Next in Global Secure Access

Peter Lenzke and Christopher Brumm

Workplace Ninja Summit 2025

We are:

www.wpninjas.eu
#WPNinjaS

Identity and Access Ninjas

Peter Lenzke

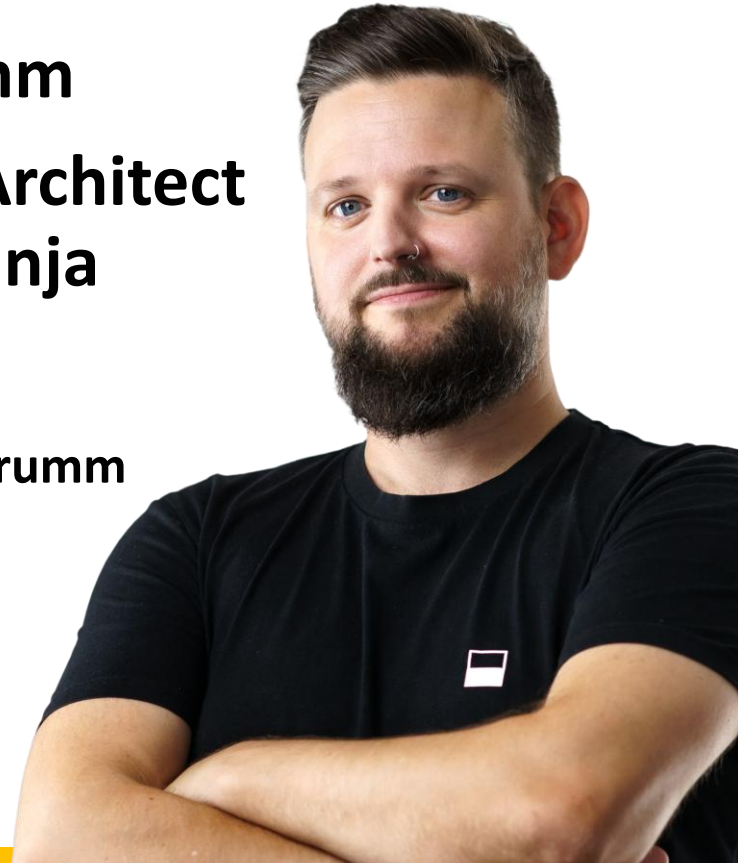
Product Manager
@ Microsoft

/in/peter-lenzke-bb95813a/

Chris Brumm

Cyber Security Architect
@ glueckkanja

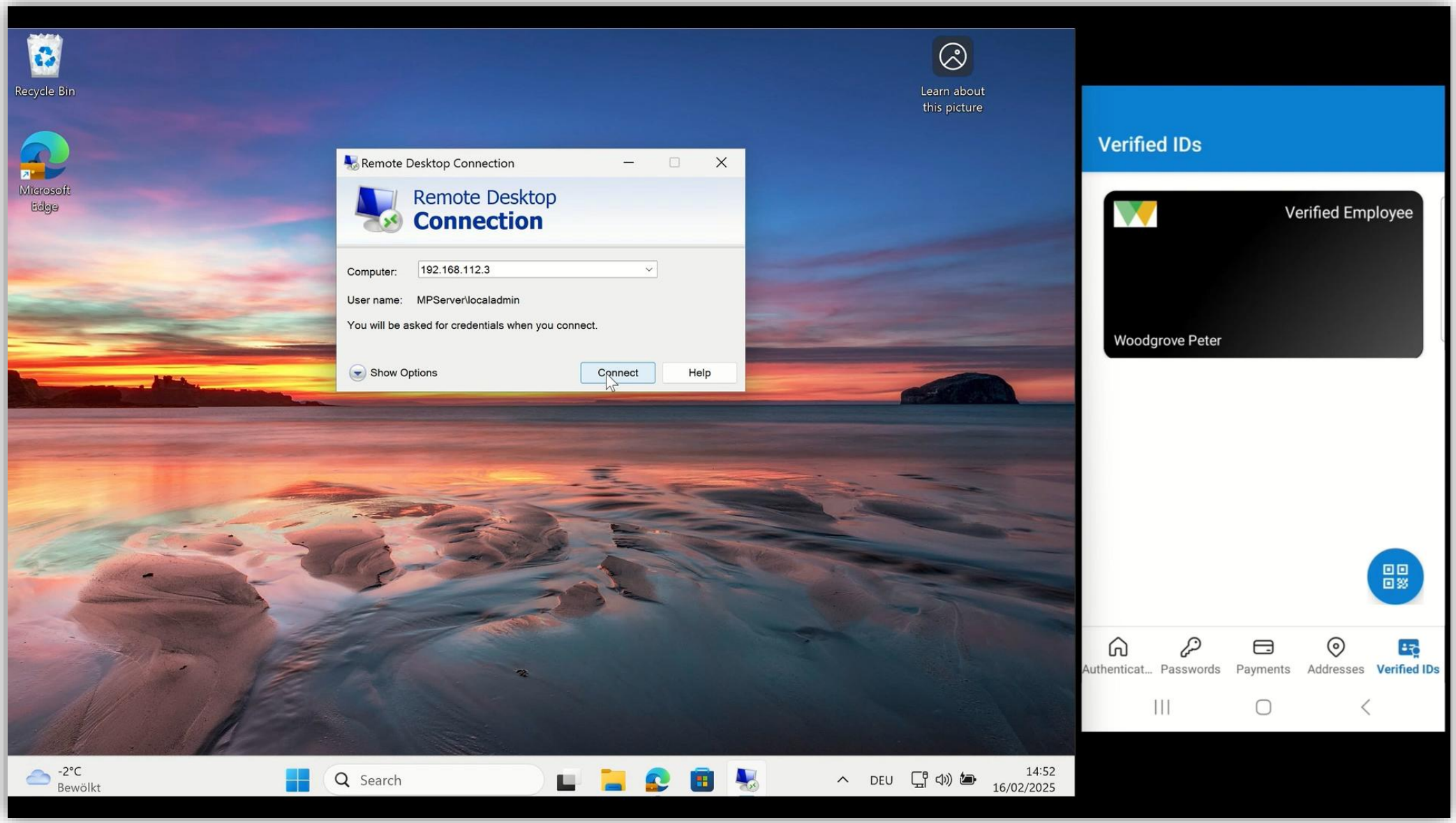
/in/christopherbrumm



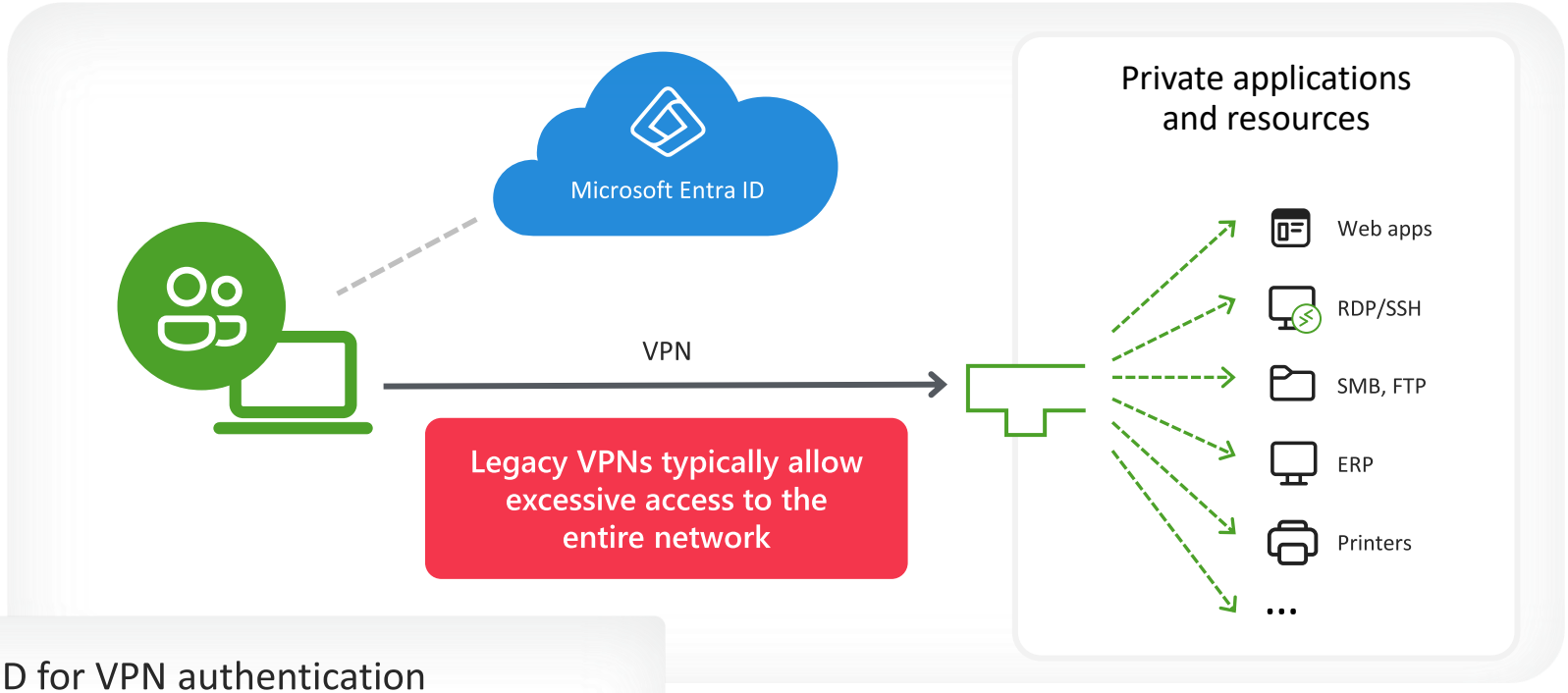
Demo

Entra Suite in action

Entra Suite in action



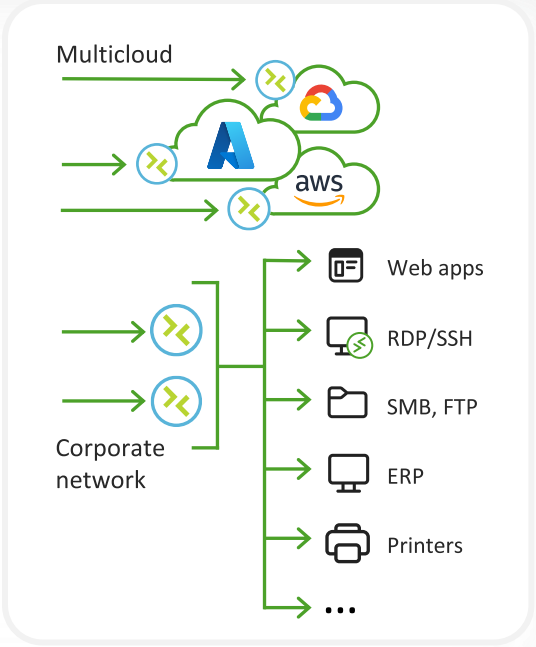
Legacy VPNs typically grant excessive access to the entire network



Configure Microsoft Entra ID for VPN authentication

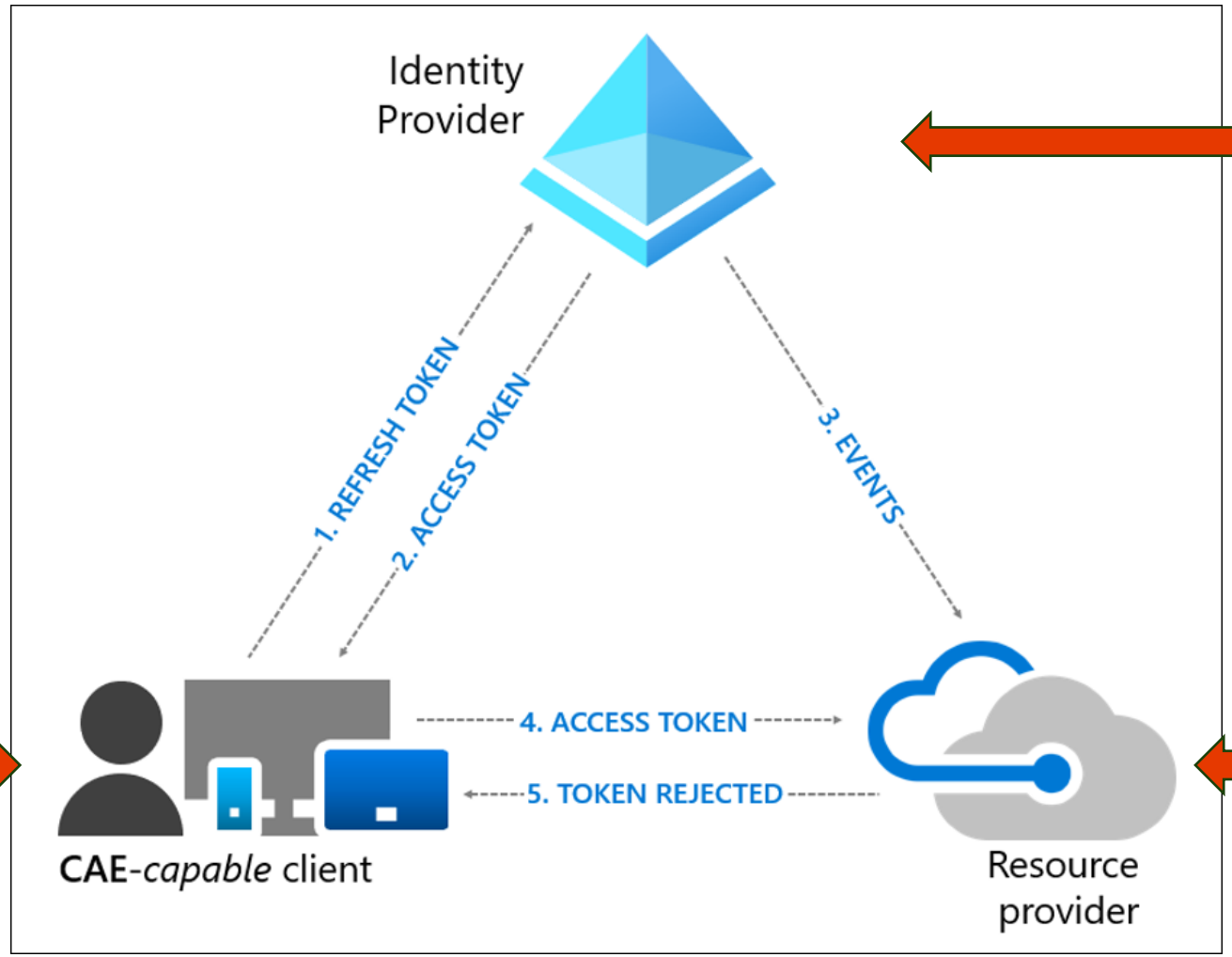
- ✓ Explicit user and device trust validation
- ✗ Provides full network access by putting device in the network (sometimes segmented)

Legacy VPNs typically grant excessive access to the entire network



- Explicit user and device trust validation
- Provides access to only private apps (with seamless user experience)
- Device does not get network level access

Universal Continuous Access Evaluation



Entra ID

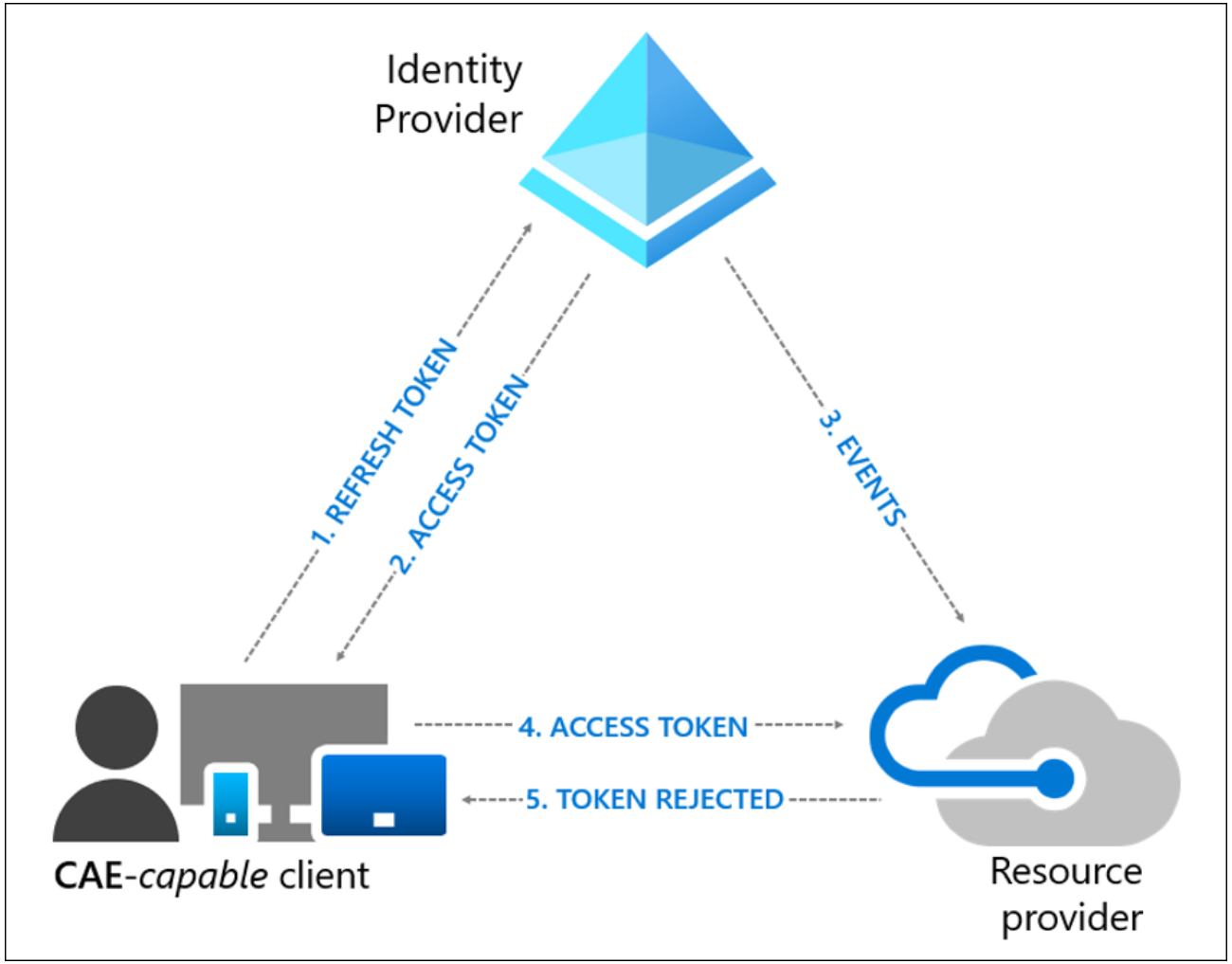
GSA Client

Global Secure Access

Universal Continuous Access Evaluation

Trigger events for Universal CAE:

- User Account is deleted or disabled
- Password for a user is changed or reset
- Multifactor authentication is enabled for the user
- Administrator explicitly revokes all refresh tokens for a user
- High user risk detected by Microsoft Entra ID Protection



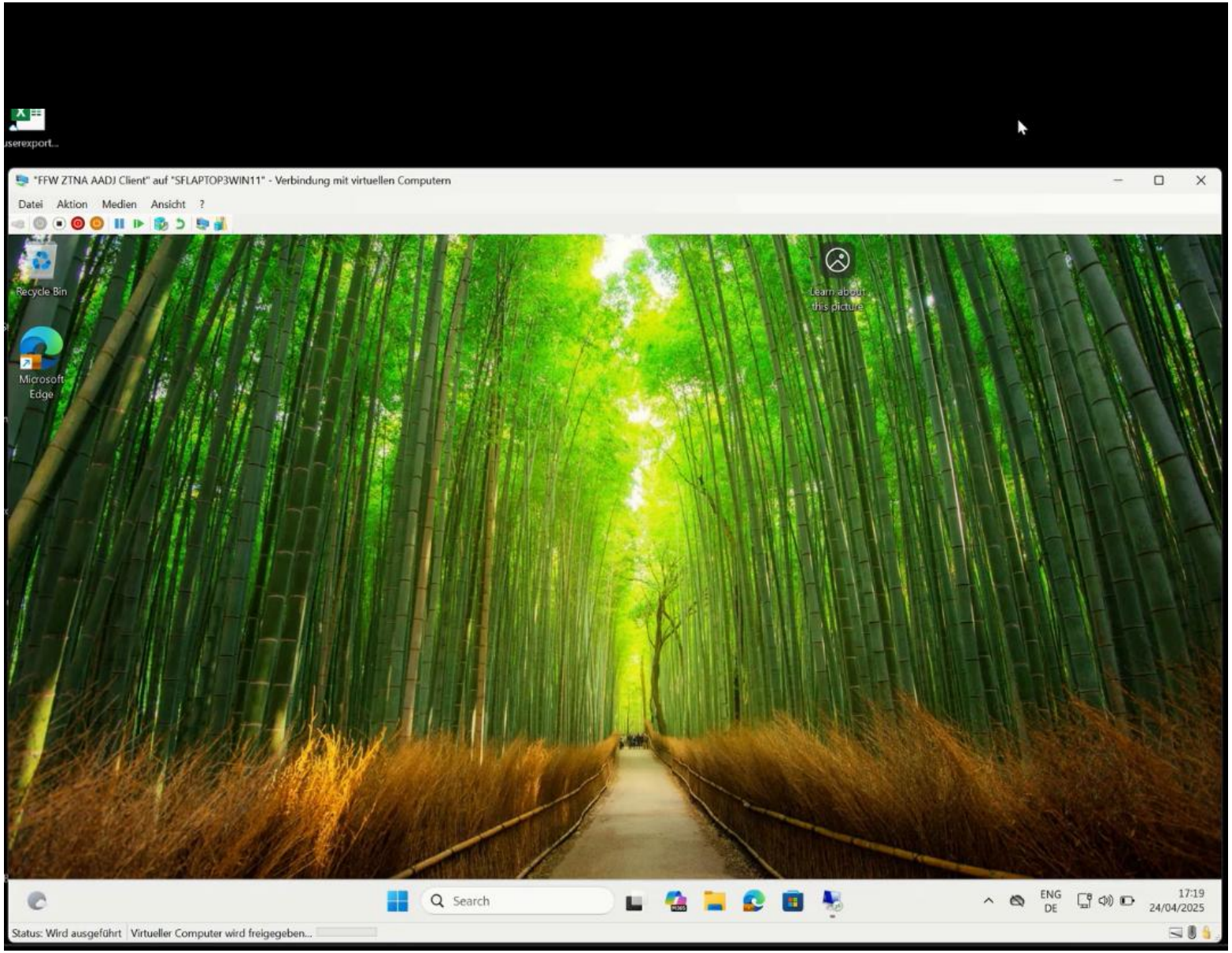
Demo

Universal Continuous Access Evaluation

Universal Continuous Access Evaluation

Trigger events for Universal CAE:

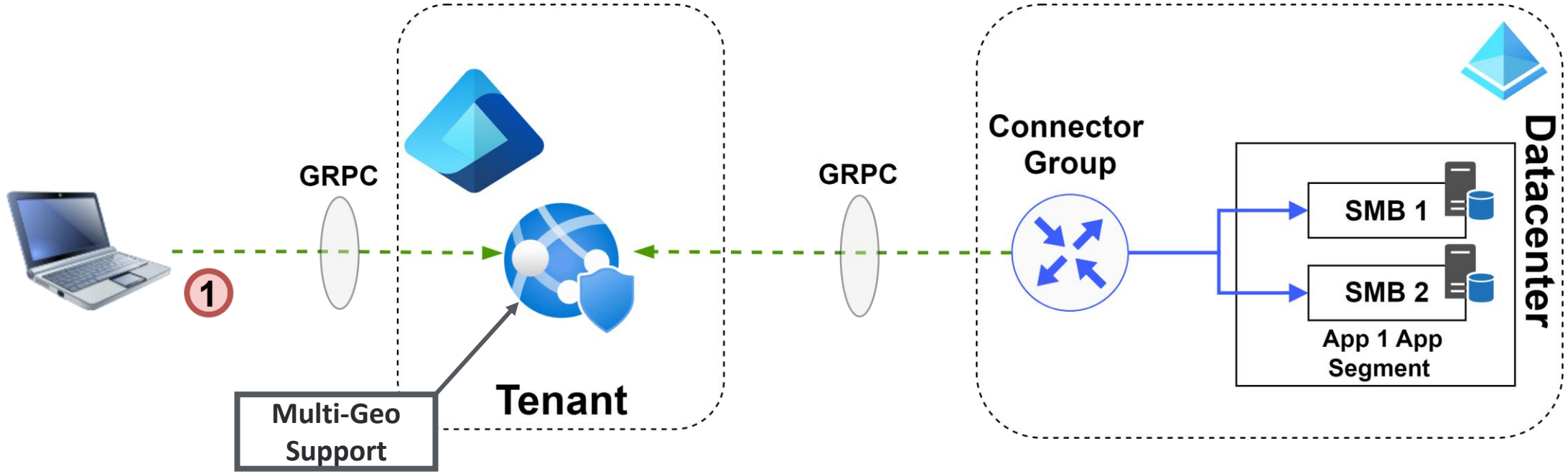
- User Account is deleted or disabled
- Password for a user is changed or reset
- Multifactor authentication is enabled for the user
- Administrator explicitly revokes all refresh tokens for a user
- High user risk detected by Microsoft Entra ID Protection



Entra Private Access

Optimize for performance

Entra Private Access connections



Hop 1: User to the Global Secure Access service

Hop 2: Global Secure Access service to the Entra private network connector

Hop 3: Entra private network connector to the target application

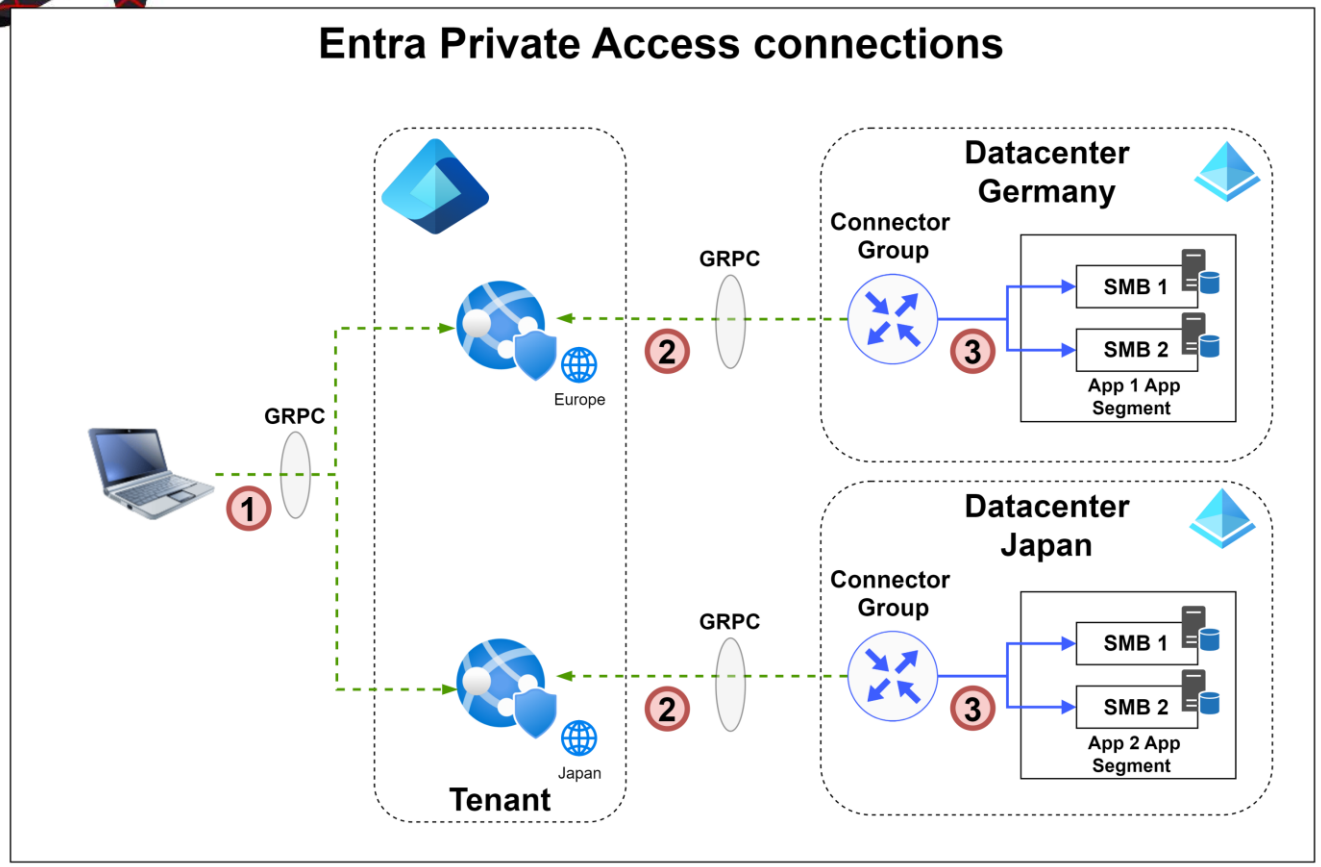
Pattern 1: Put the connector close to the application

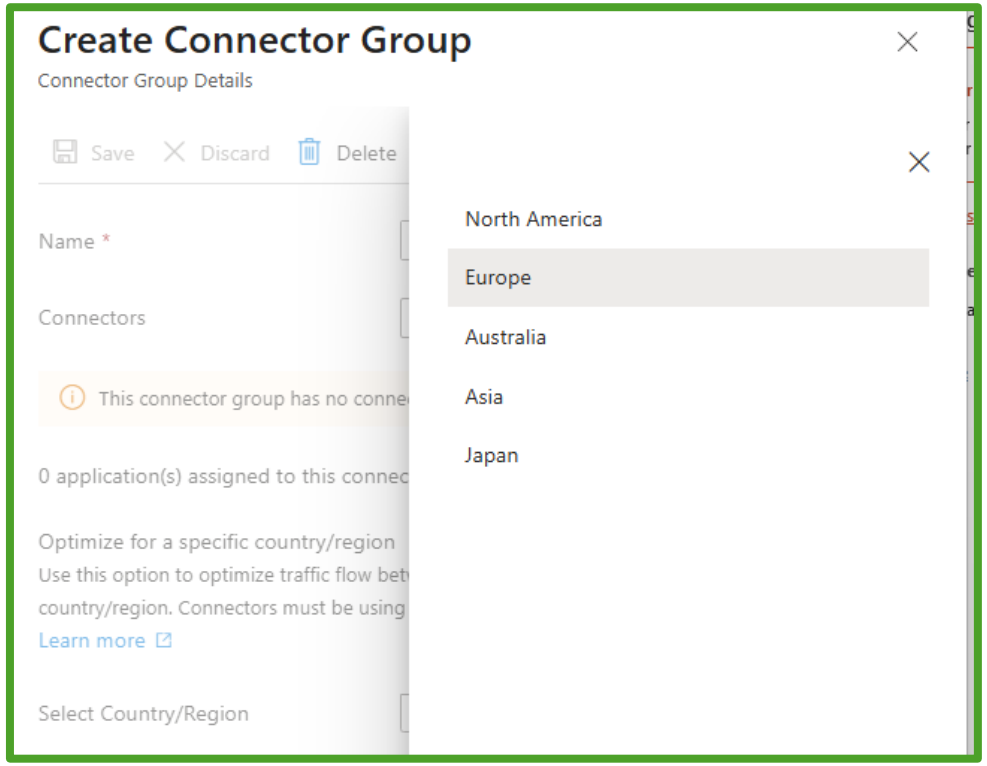
Pattern 2: Take advantage of ExpressRoute with Microsoft peering

Pattern 3: Take advantage of ExpressRoute with private peering

Multi-Geo Support (Public Preview)

www.wpninjas.eu
#WPNinjaS





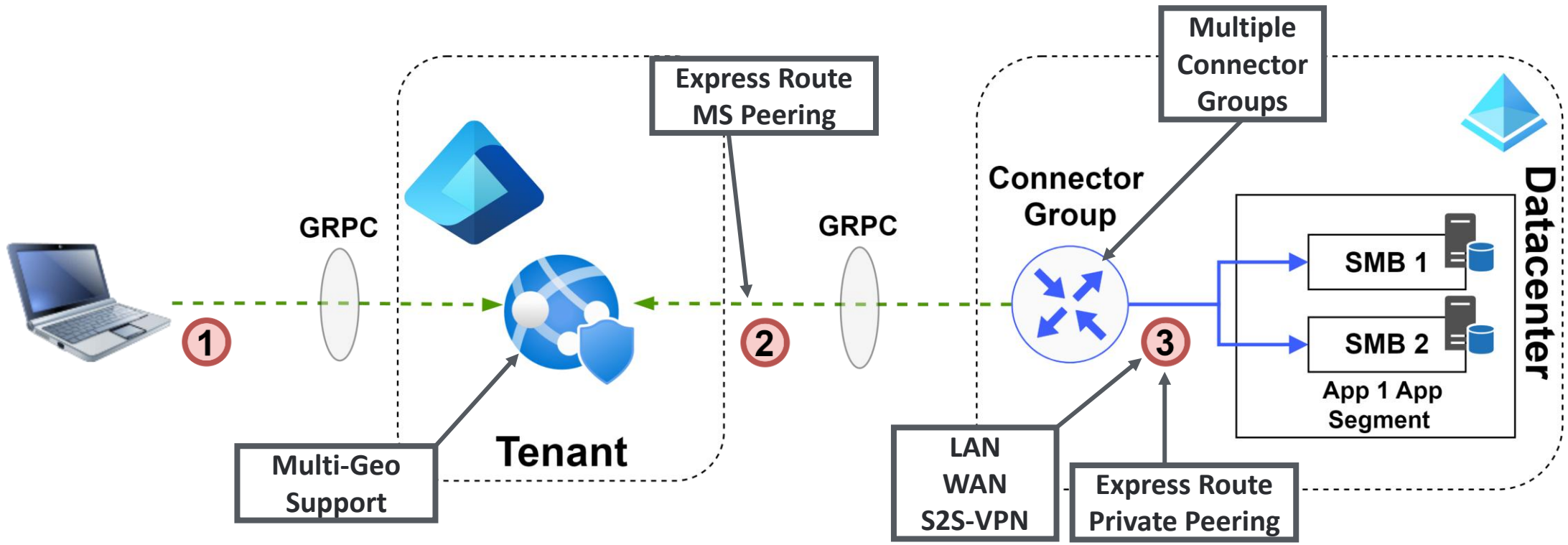
Hop 1: User to the Global Secure Access service

Hop 2: Global Secure Access service to the Entra private network connector

Hop 3: Entra private network connector to the target application

Entra Private Access connections

www.wpninjas.eu
#WPNinjaS



Hop 1: User to the Global Secure Access service

Hop 2: Global Secure Access service to the Entra private network connector

Hop 3: Entra private network connector to the target application

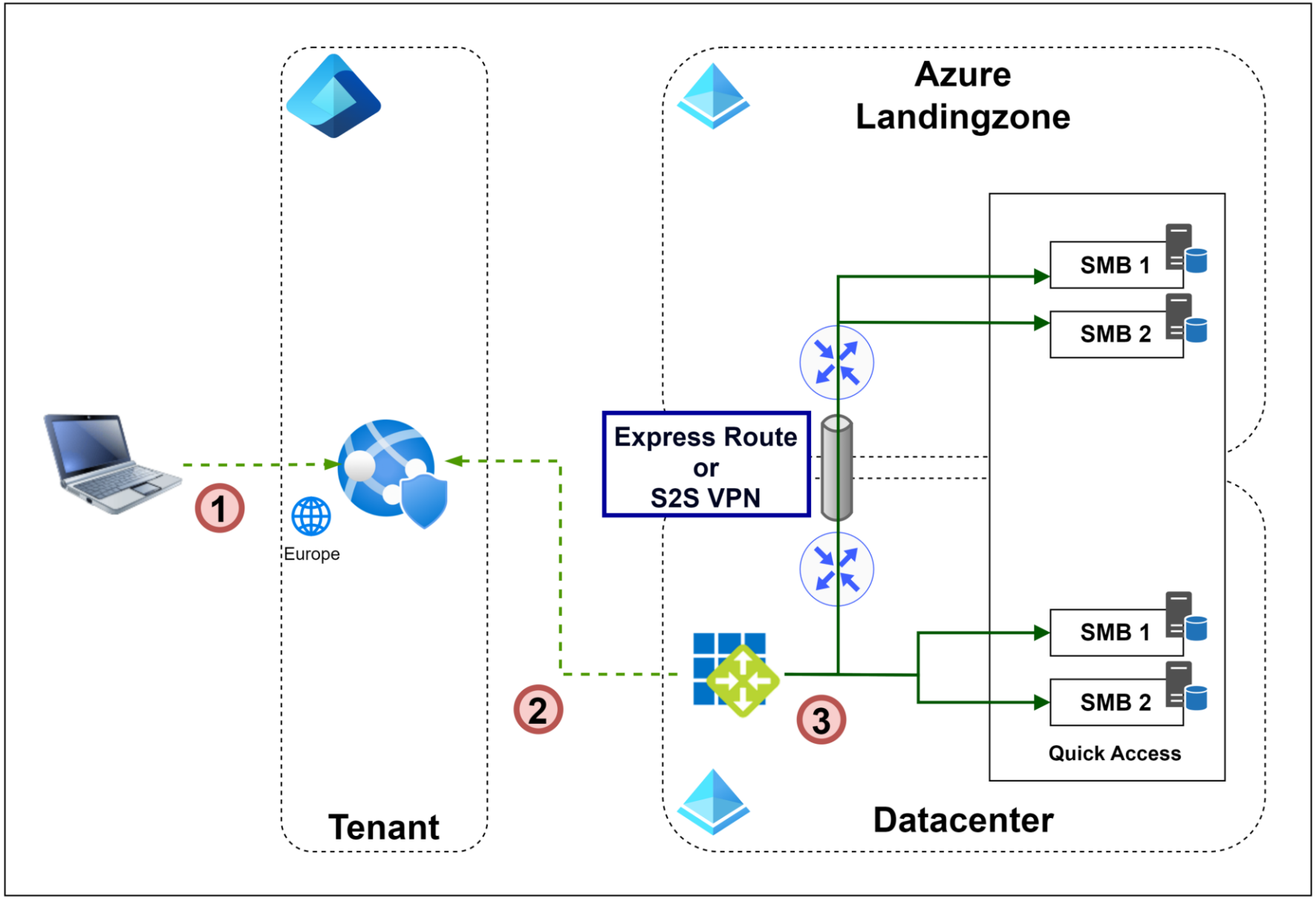
Pattern 1: Put the connector close to the application

Pattern 2: Take advantage of ExpressRoute with Microsoft peering

Pattern 3: Take advantage of ExpressRoute with private peering

Optimize traffic for multiple datacenter

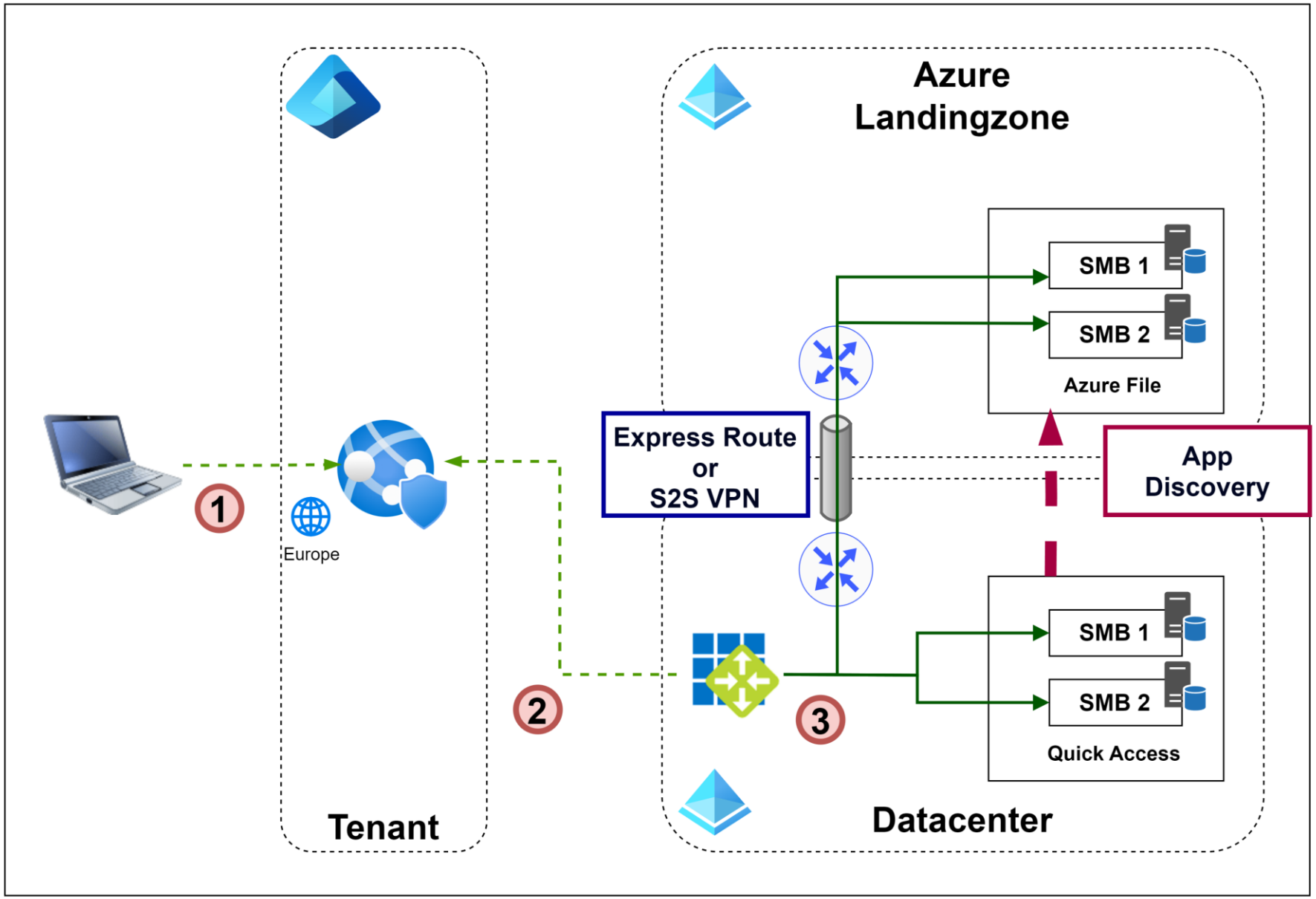
Start with Quick Access



Optimize traffic for multiple datacenter

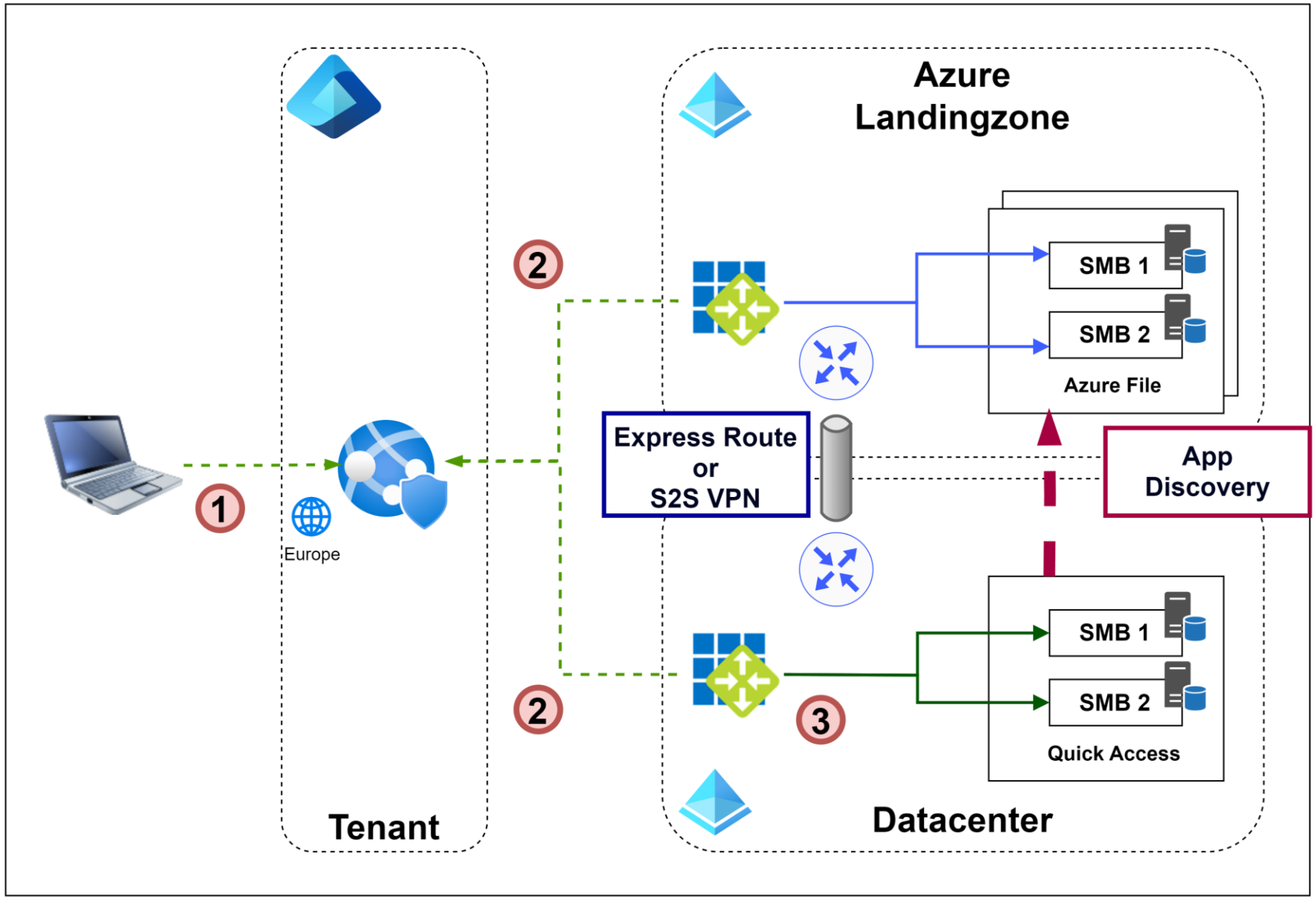
Start with Quick Access

Discover and configure Apps in Azure



Optimize traffic for multiple datacenter

- Start with Quick Access
- Discover and configure Apps in Azure
- Deploy a new connector group and reroute traffic

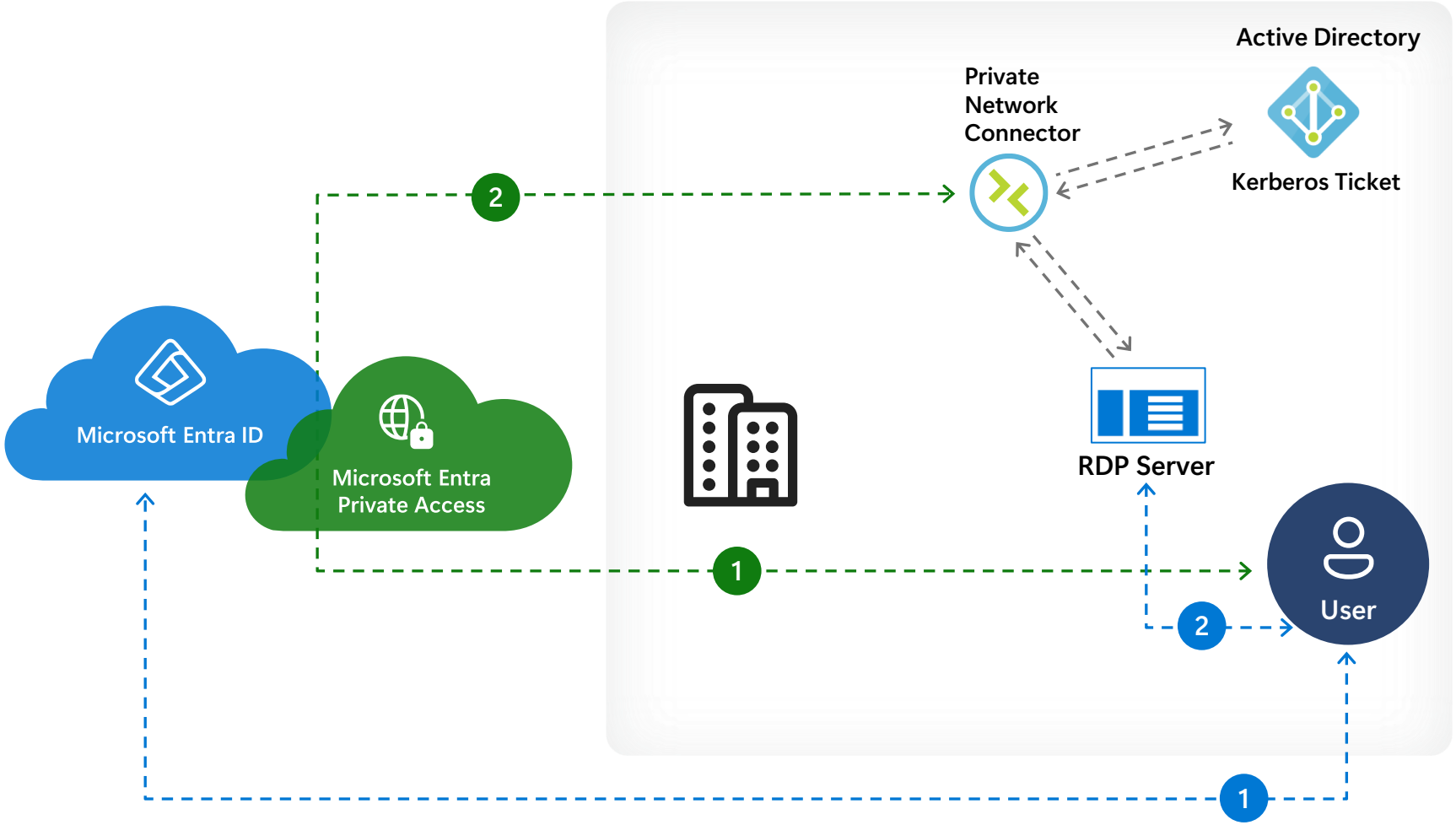


Intelligent Local Access

www.wpninjas.eu
#WPNinjaS

ILA - Intelligent Local Access

- By default, GSA always acquires traffic (green flow)
- ILA detects “inside corp net” via DNS probes
- AuthN / AuthZ is always done via Entra ID first
- Payload is then routed locally (blue flow)



Options…

Disabling the GSA client

- ⊖ No Conditional Access
- ⊖ Direct connection to the resource allowed
- ⊕ No latency challenges

Route all traffic through GSA

- ⊕ Conditional Access
- ⊕ No direct connection to the resource allowed
- ⊖ Latency challenges

Use Intelligent Local Access

- ⊕ Conditional Access
- ⊖ Direct connection to the resource allowed
- ⊕ No latency challenges

Route traffic through the connector

- ⊕ Conditional Access
- ⊕ No direct connection to the resource allowed
- ⊕ Latency challenges

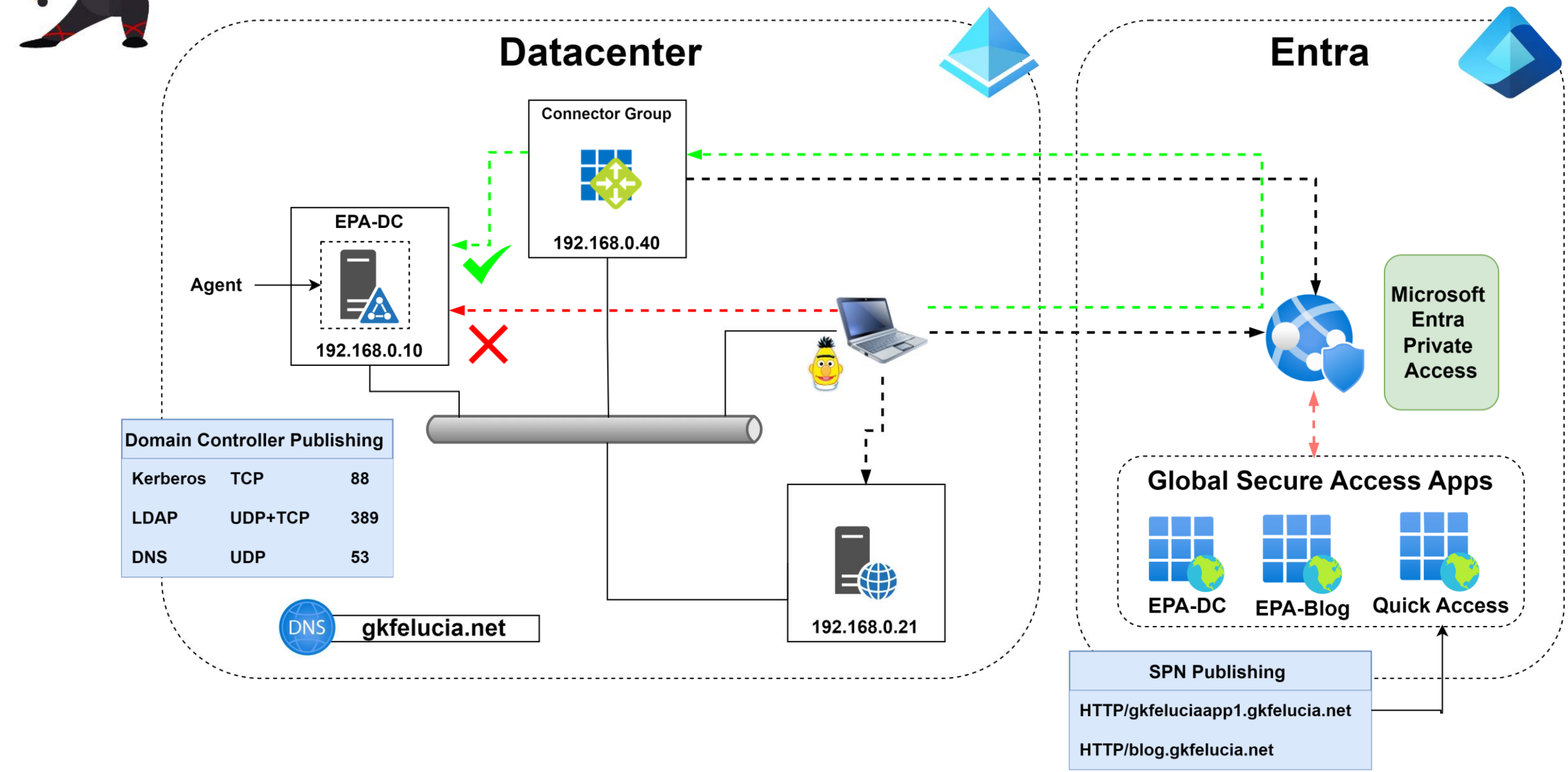
*Chris' wish for the future

Demo

Private Access for Domain Controllers

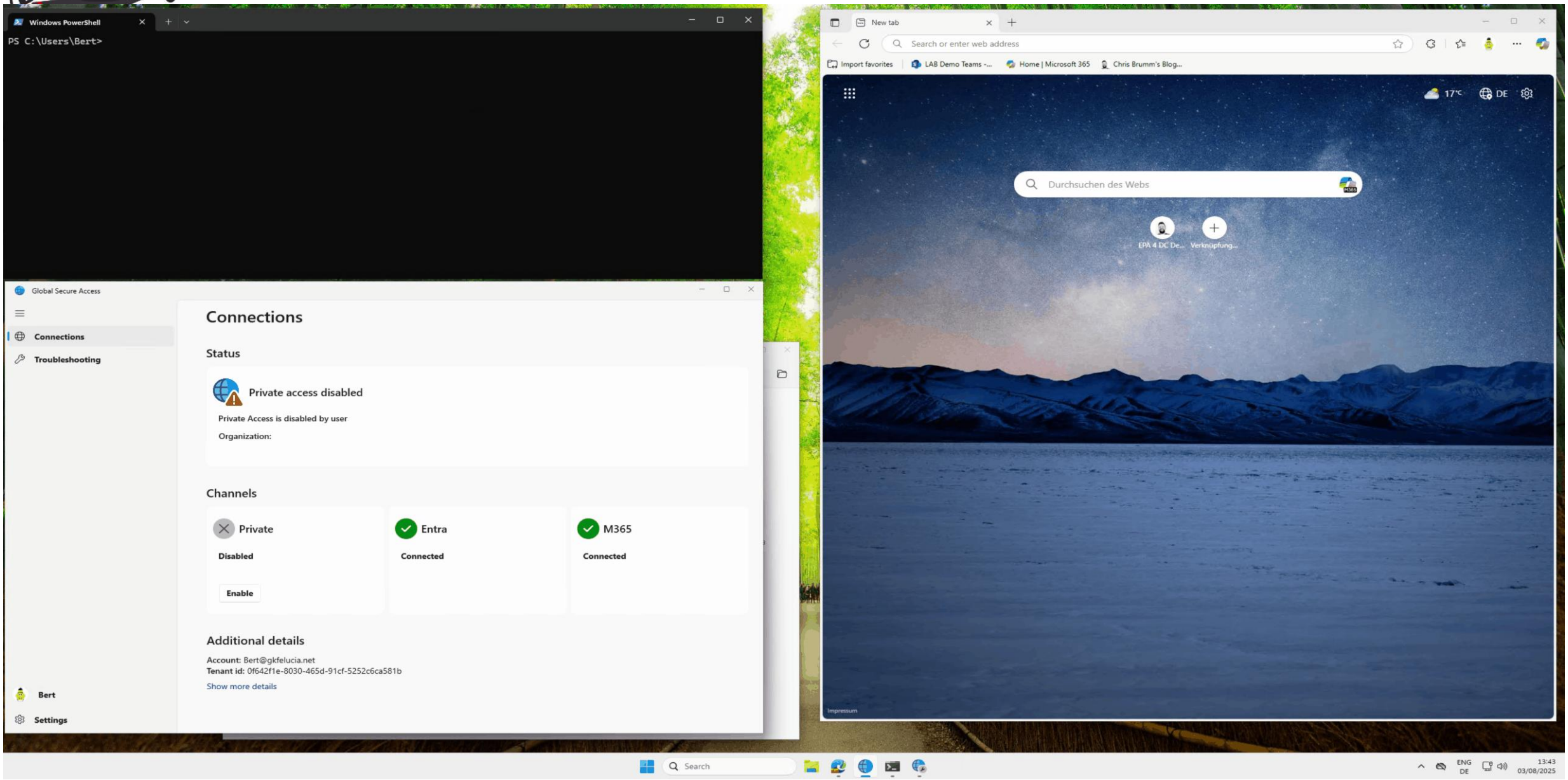
Private Access for Domain Controllers

www.wpninjas.eu
#WPNinjaS



Private Access for Domain Controllers

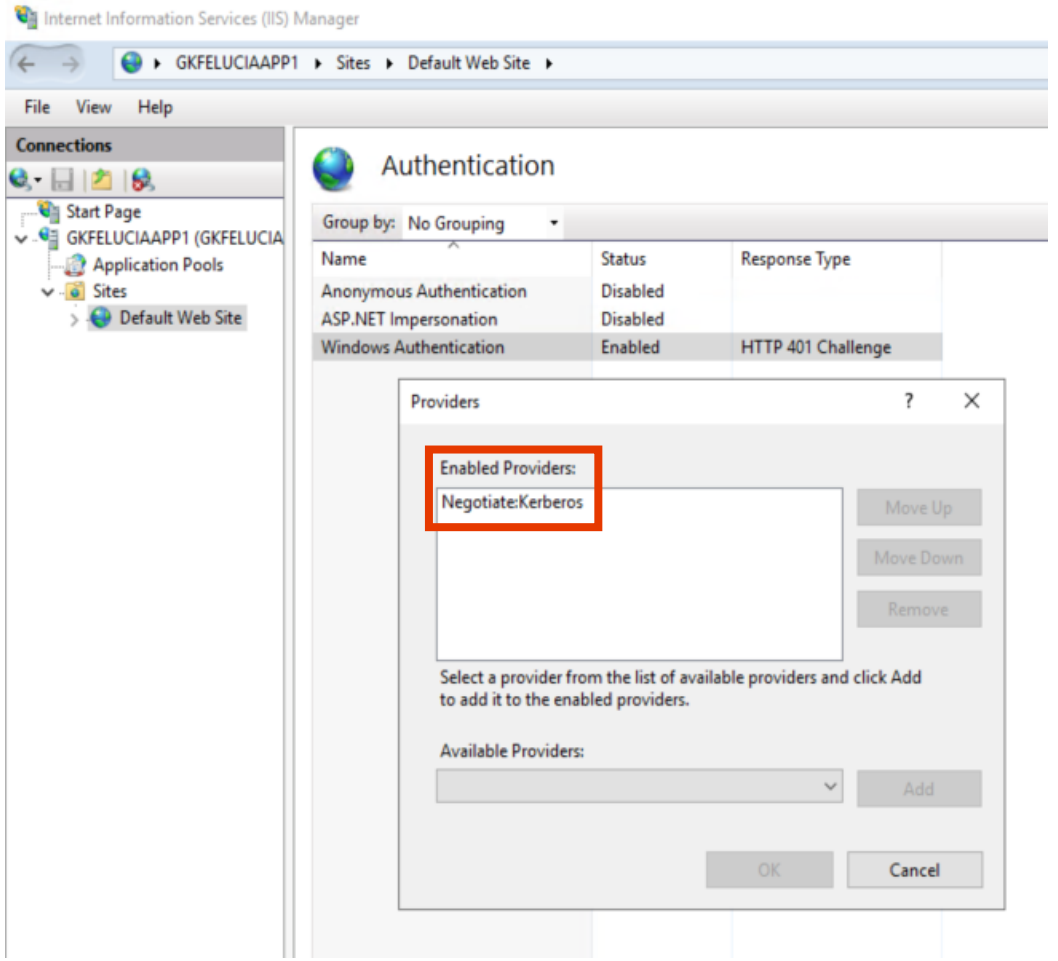
www.wpninjas.eu
#WPNinjaS



What about NTLM?

Prerequisites:

If you use NT LAN Manager (NTLM) v1/v2 in your environment, you might need to restrict NTLM and use Kerberos auth in the domain.

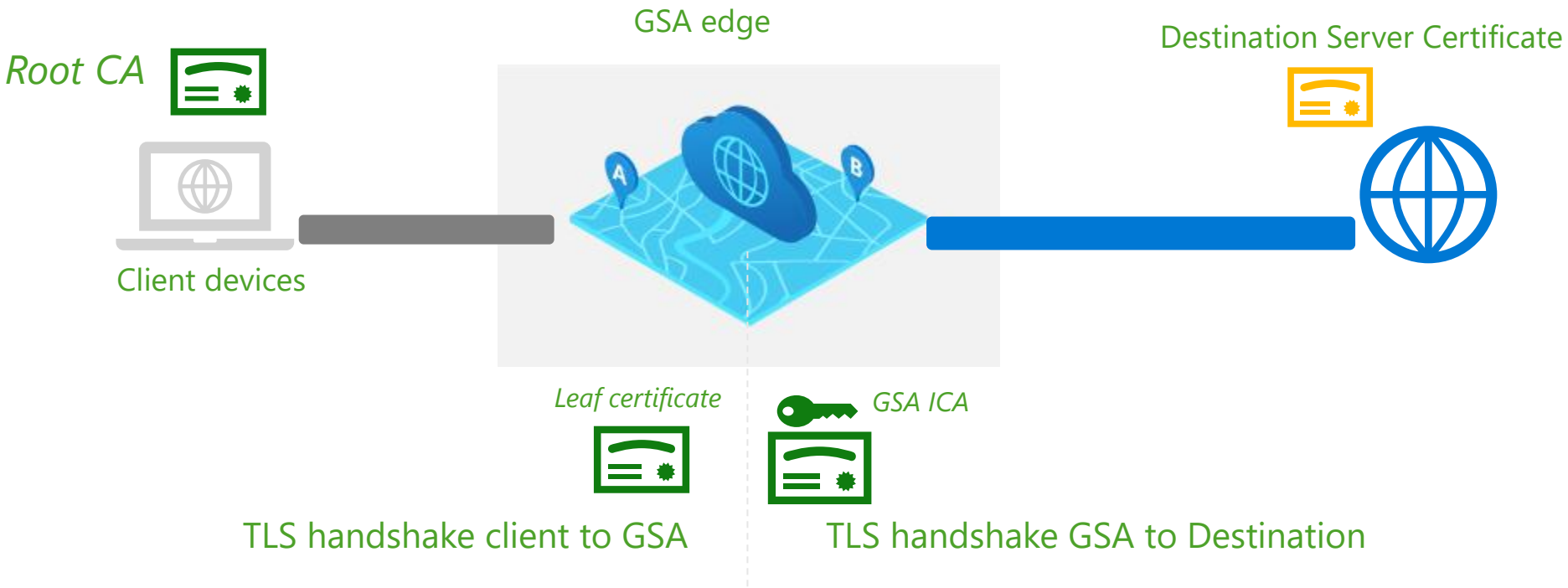


Why is TLS inspection a game changer?

for Entra Internet Access

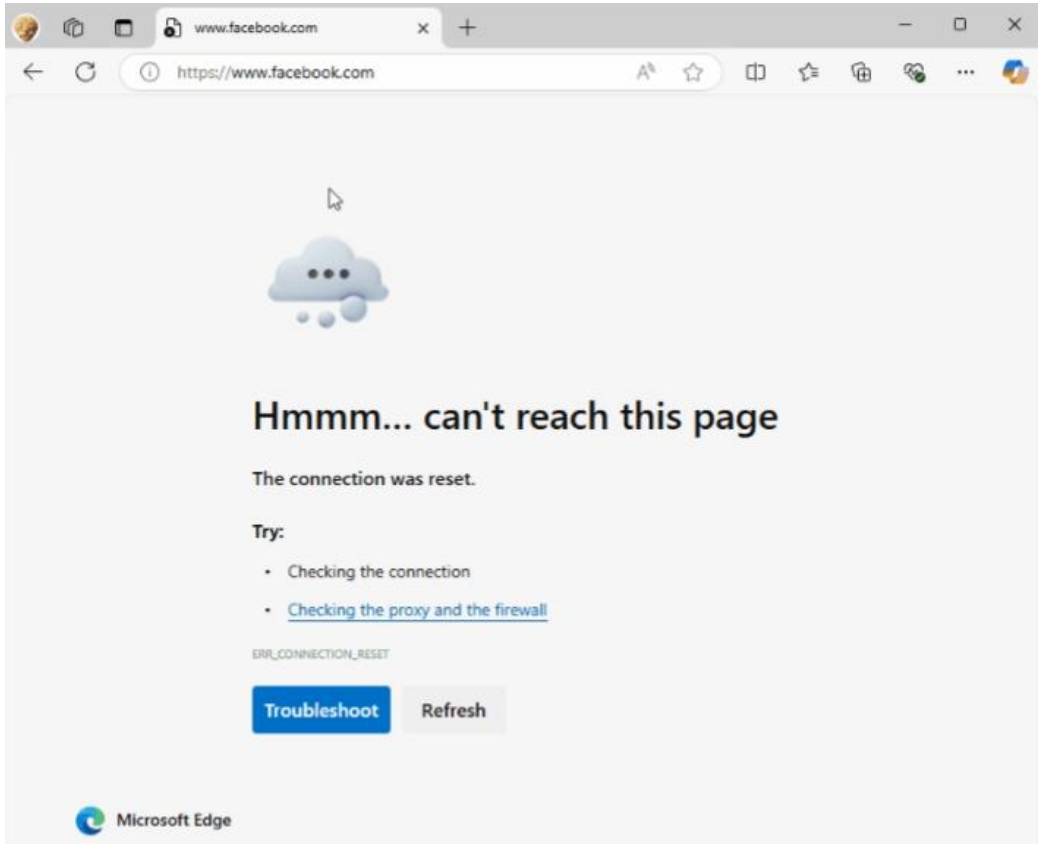
Entra Internet Access – TLSi Overview

www.wpninjas.eu
#WPNinjaS

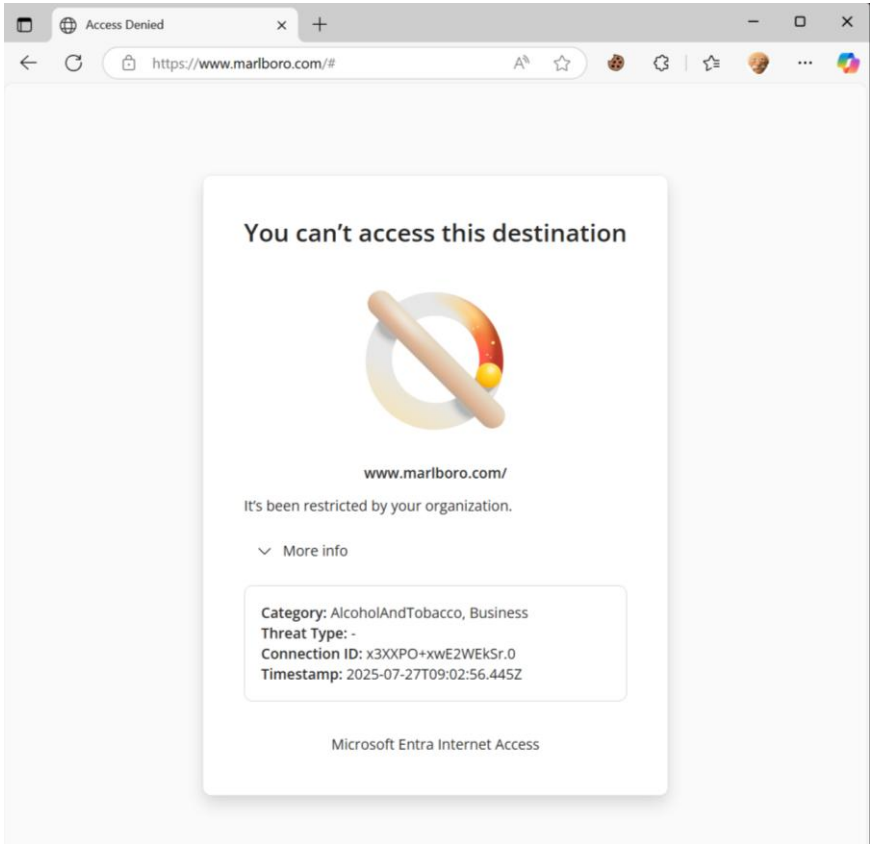


- Root and Issuing CA is customer owned and controlled
- Admins submits a request at the Entra Portal to create CSR
- Certificate is signed by the customer's PKI and then uploaded to the Entra Portal
- The Admin distributes their Root CA to their clients
- GSA issues leave certificates for the requested sites

HTTPs Error Messages

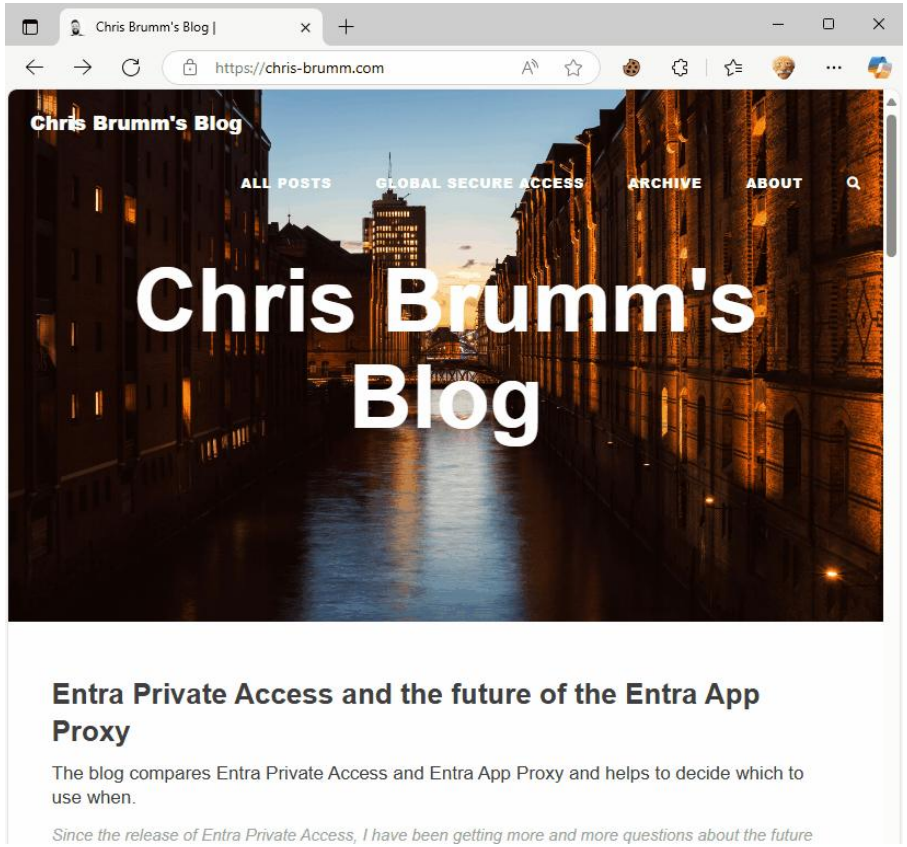


without TLS inspection



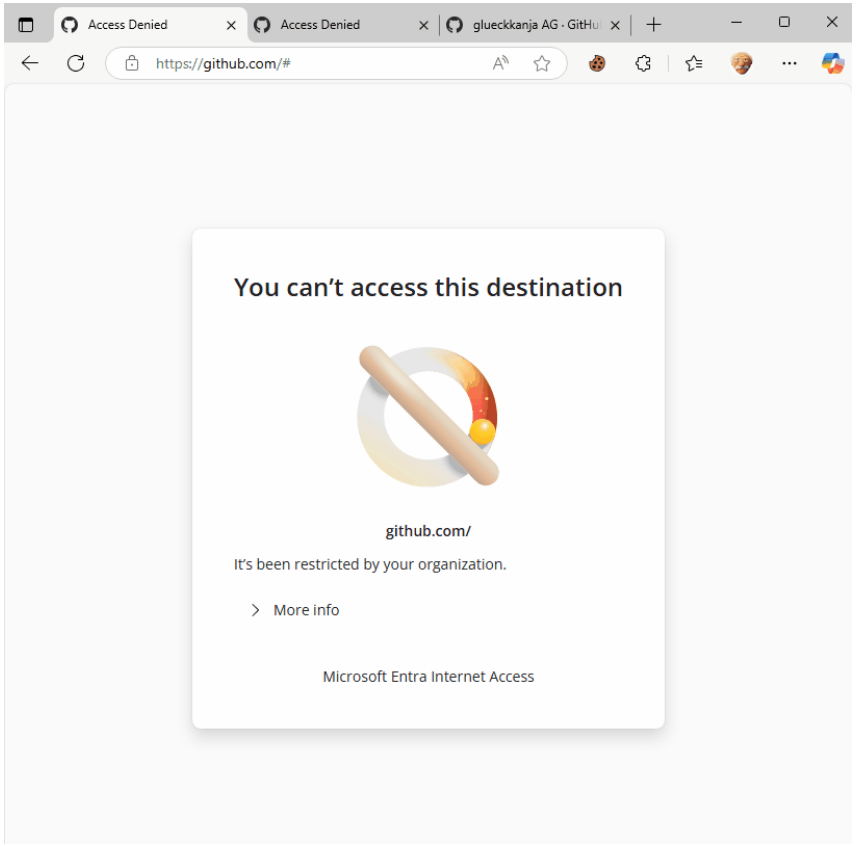
with TLS inspection

URL Filtering at path level



Block a specific subpage

URL Filtering at path level



allowlist specific repos

Should we really inspect TLS?

www.wpninjas.eu
#WPNinjaS

You are in control which traffic is inspected

Banking and Healthcare category is bypassed by default

URL Path filter and Custom error messages is only possible with TLSi

Almost all advanced threat intelligence needs TLSi

Your PKI provides the encryptions certs

Conflicts with HSTS, certificate pinning, etc.

Data protection issues with sensitive content

Possible latencies during extensive analysis

Installation of own root CA on end devices required

Lateral Movement from PKI possible

Use a modern PKI for the Issuing Cert

And what else is new?

GA

- MacOS Client

Public Preview

- 3rd Party Threat Intelligence
- Threat Intelligence Policies
- Windows ARM
- IOS Client
- China Support for traveling users
- Global Secure Access solution in Sentinel

Private Preview

- Internet Access for Remote Networks
- URL-Path Filter
- DLP + Purview
- AI Gateway
- B2B
- Connector Affinity
- Intelligent Local Access

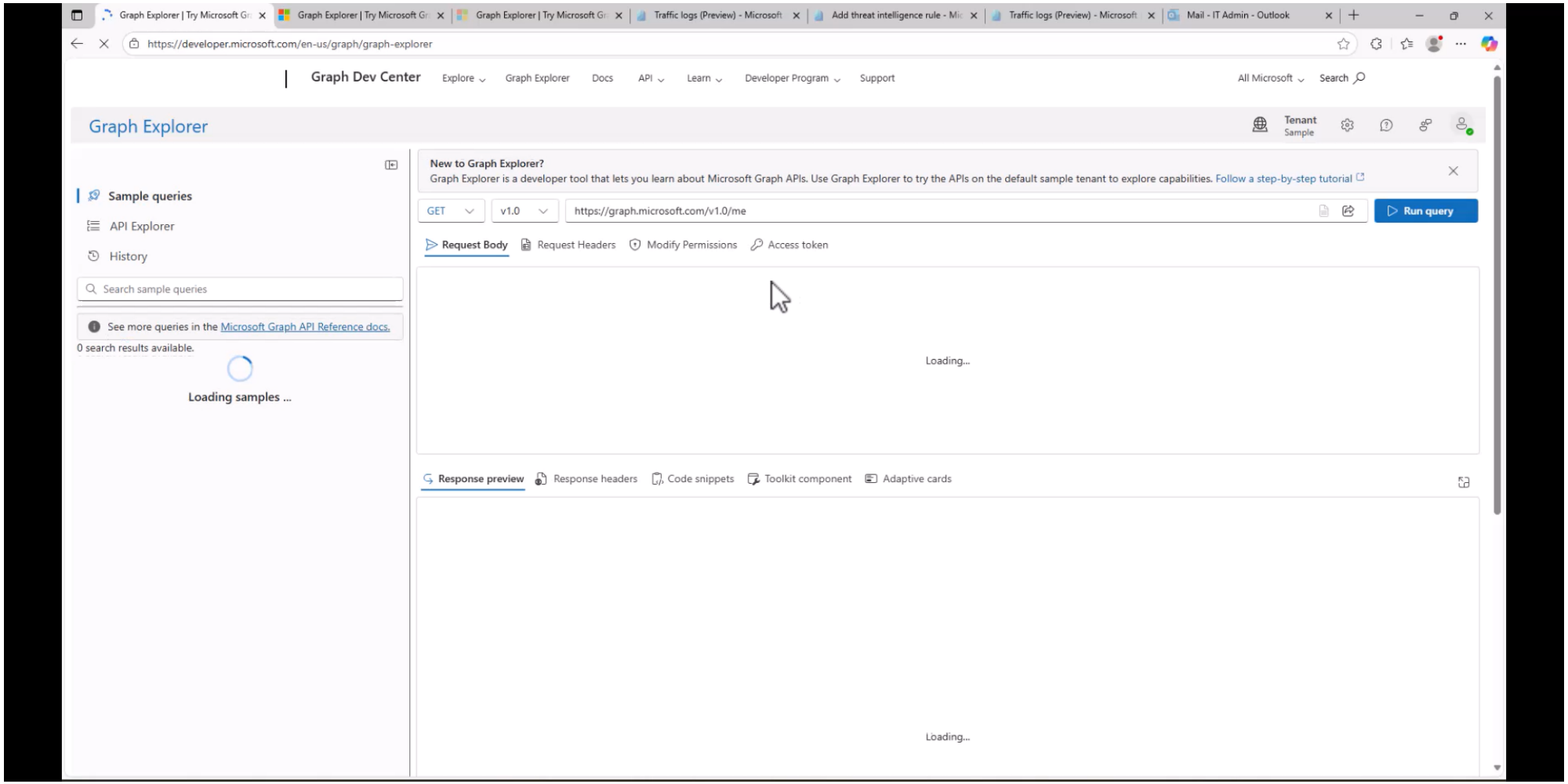
Still on the Roadmap

- Cloud Firewall
- DNS Logs
- BYOD
- Forwarding Proxy

Questions?

Web category checker tool

www.wpninjas.eu
#WPNinjaS



GET https://graph.microsoft.com/beta/networkaccess/connectivity/getWebCategoryByUrl(url='@url')
?@url=msn.com/en-us/sports

Bonus round

Do you need better troubleshooting?

- GSA Trace Route Tool
- Shipped with the client
- No admin permissions
- RTT, throughput, connectivity
- PoP geo location
- Use IP, FQDN, App ID

Wanna give it a spin?
plenzke@microsoft.com

```
.\GsaTracert.exe --app-id 36ddf384-89fd-439c-a7f2-1c01a0ea232b
🌐 Tracing route to GSA Private Access application 36ddf384-89fd-439c-a7f2-1c01a0ea232b
```

Next hop	RTT (ms)
PoP Private Access Gateway Connector Backend app	19 166 5

Upload Throughput Test

Next hop	Throughput (Mbps)	File Size	Location
PoP	571.43	50.0 MB	Tel Aviv, Israel

Download Throughput Test

Next hop	Throughput (Mbps)	File Size	Location
PoP	390.62	50.0 MB	

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

Rimo3

SOFTWARE CENTRAL

eido

EPIC FUSION
BRING IT ALL TOGETHER

Silver Sponsors

APENTO

PROACT

controlUP

UMB creating time®

water
IT Security & Defense

www.wpninjas.eu
#WPNinjaS

We love Feedback

https://wpninjas25.sched.com/

Great Session!

Okay Session!

Not so okay Session!

Workplace Ninja Summit 2025

www.wpninjas.eu
#WPNinjaS