

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

Peter Lenzke and Christopher Brumm





We are:

www.wpninjas.eu
#WPNinjaS

Identity and Access Ninjas



Peter Lenzke
Product Manager
@ Microsoft

Chris Brumm
Cyber Security Architect
@ glueckkanja



[/in/peter-lenzke-bb95813a/](https://www.linkedin.com/in/peter-lenzke-bb95813a/)



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



Demo

www.wpninjas.eu
#WPNinjaS

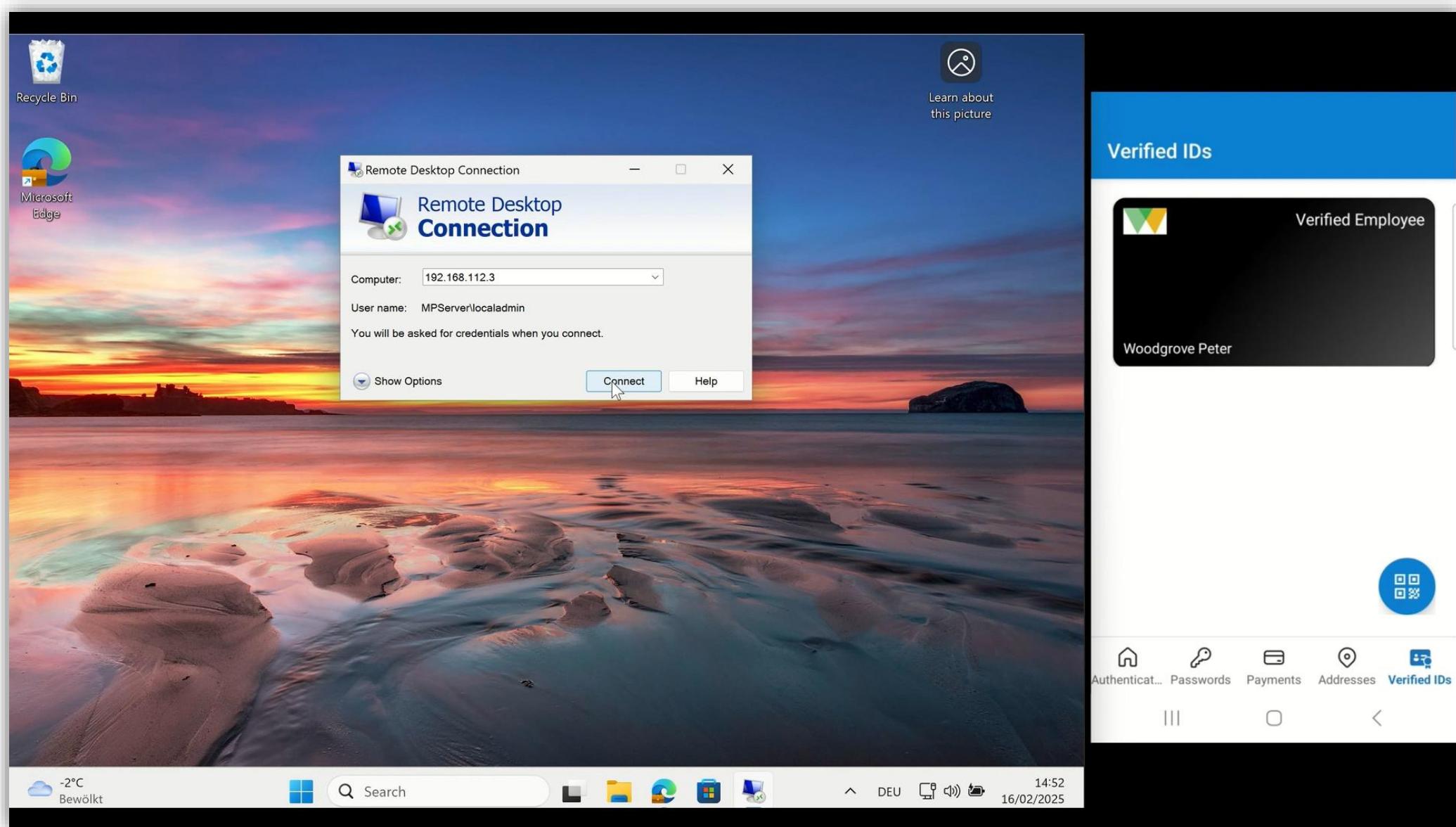
Entra Suite in action





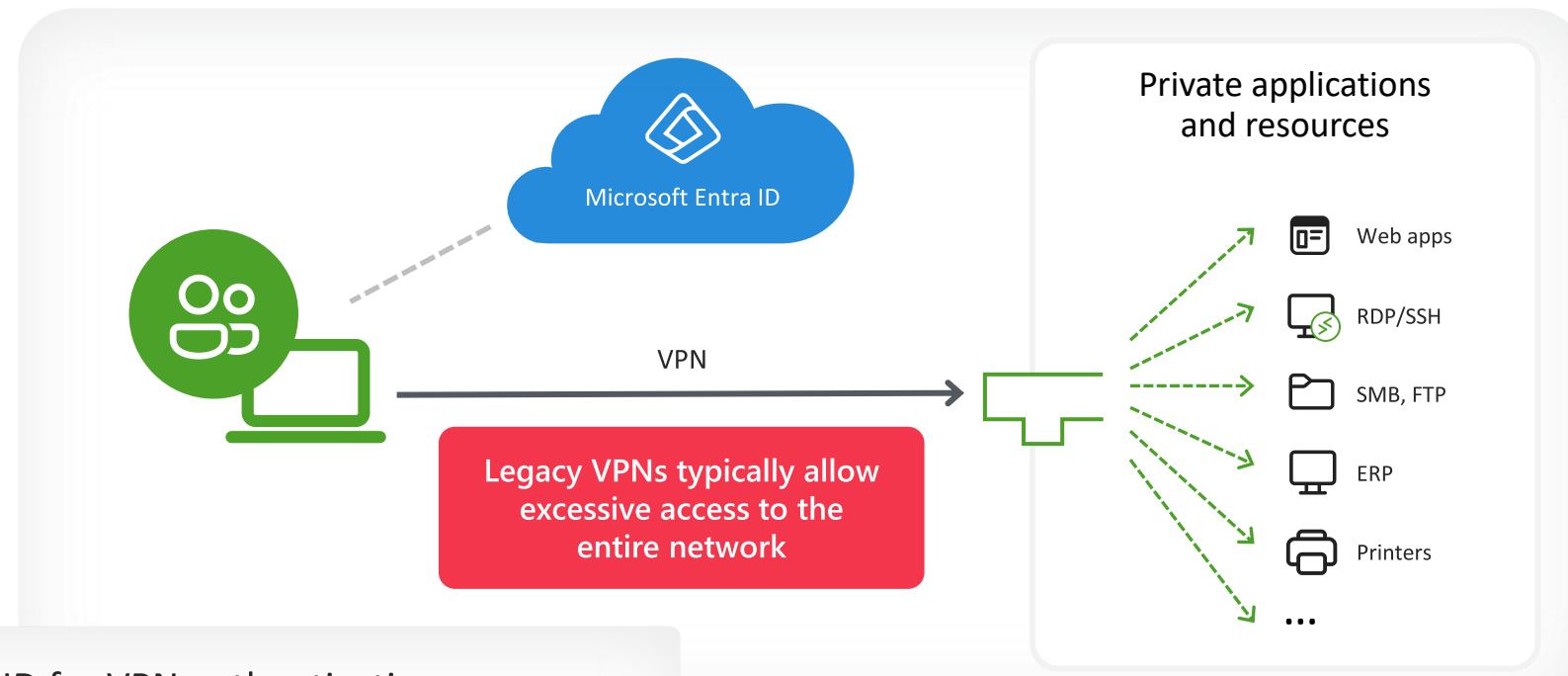
Entra Suite in action

www.wpninjas.eu
#WPNinjaS





Legacy VPNs typically grant excessive access to the entire network



Configure Microsoft Entra ID for VPN authentication

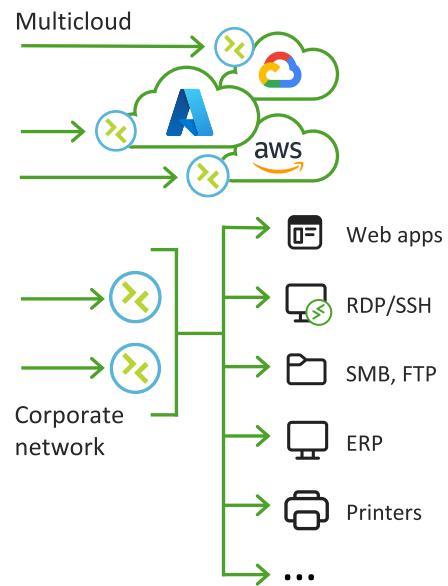
- + Explicit user and device trust validation
- Provides full network access by putting device in the network (sometimes segmented)



Legacy VPNs typically grant excessive access to the entire network



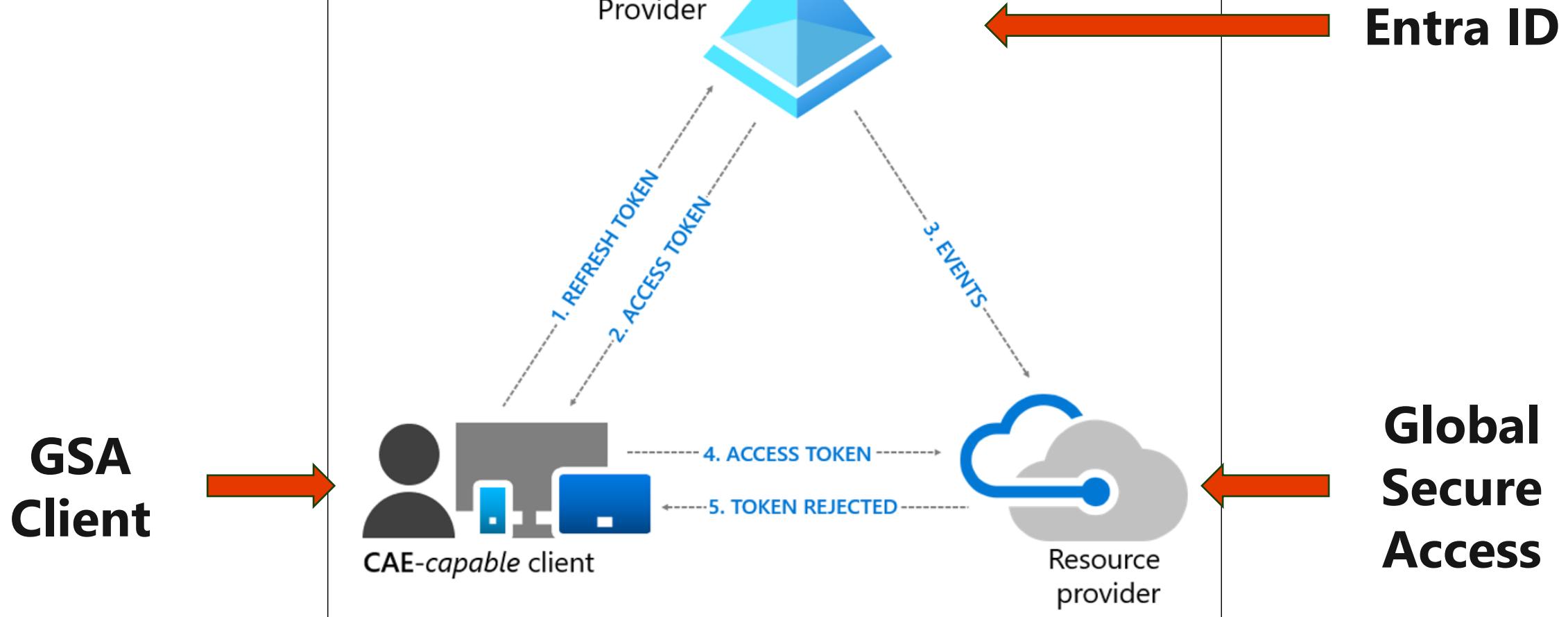
- + Explicit user and device trust validation
- + Provides access to only private apps (with seamless user experience)
- + Device does not get network level access





Universal Continuous Access Evaluation

www.wpninjas.eu
#WPNinjaS



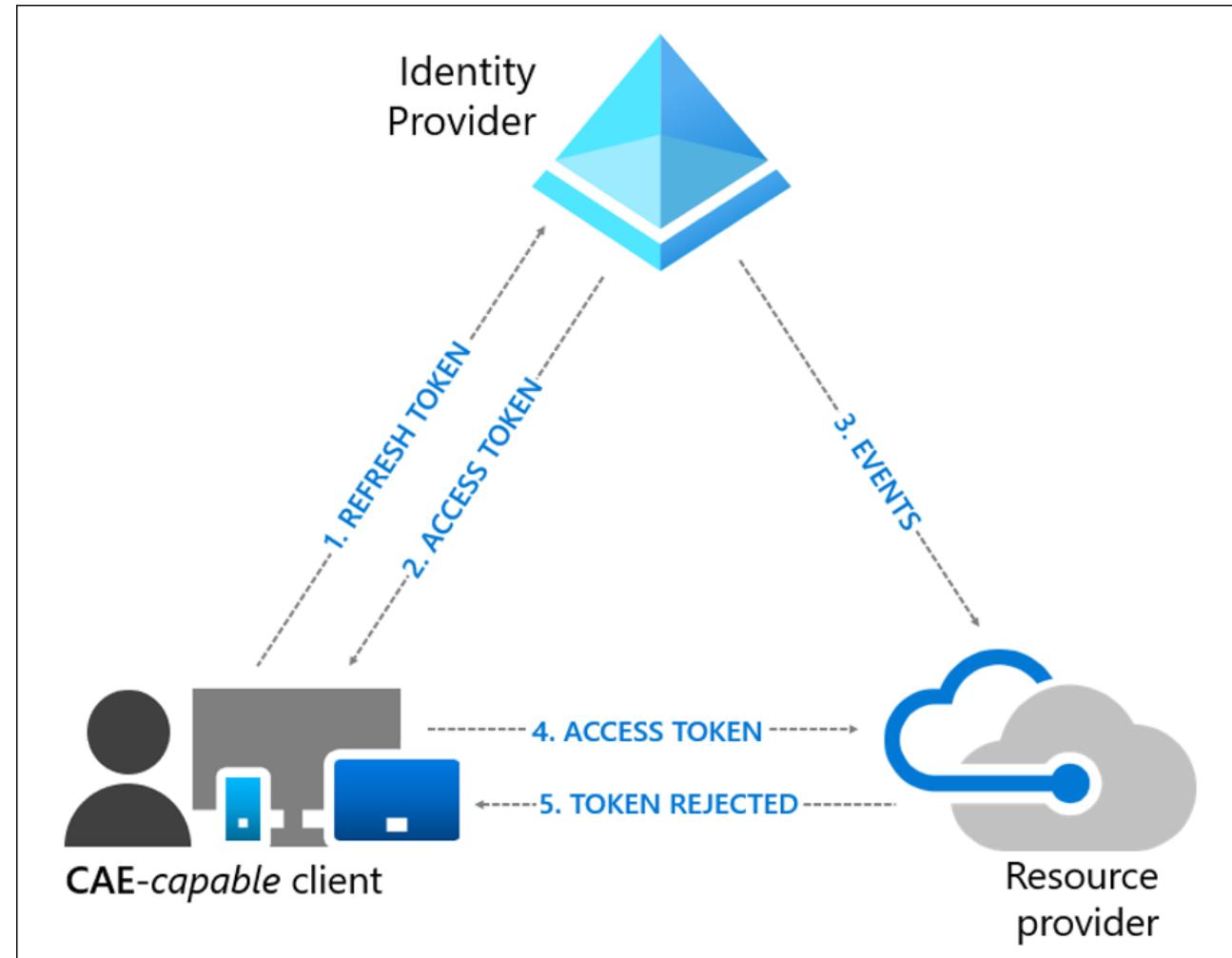


Universal Continuous Access Evaluation

www.wpninjas.eu
#WPNinjaS

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

www.wpninjas.eu
#WPNinjaS

Universal Continuous
Access Evaluation



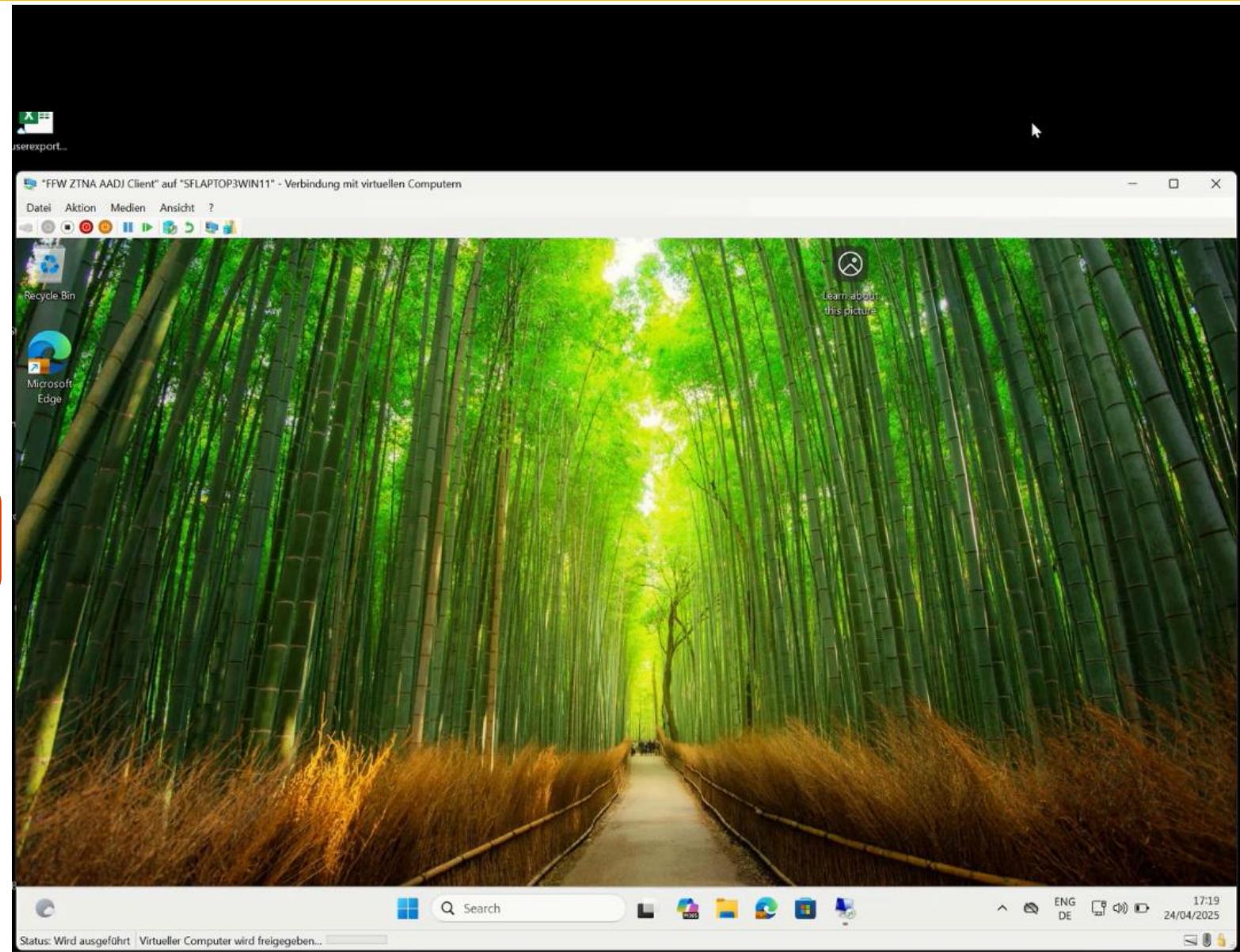


Universal Continuous Access Evaluation

www.wpninjas.eu
#WPNinjaS

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

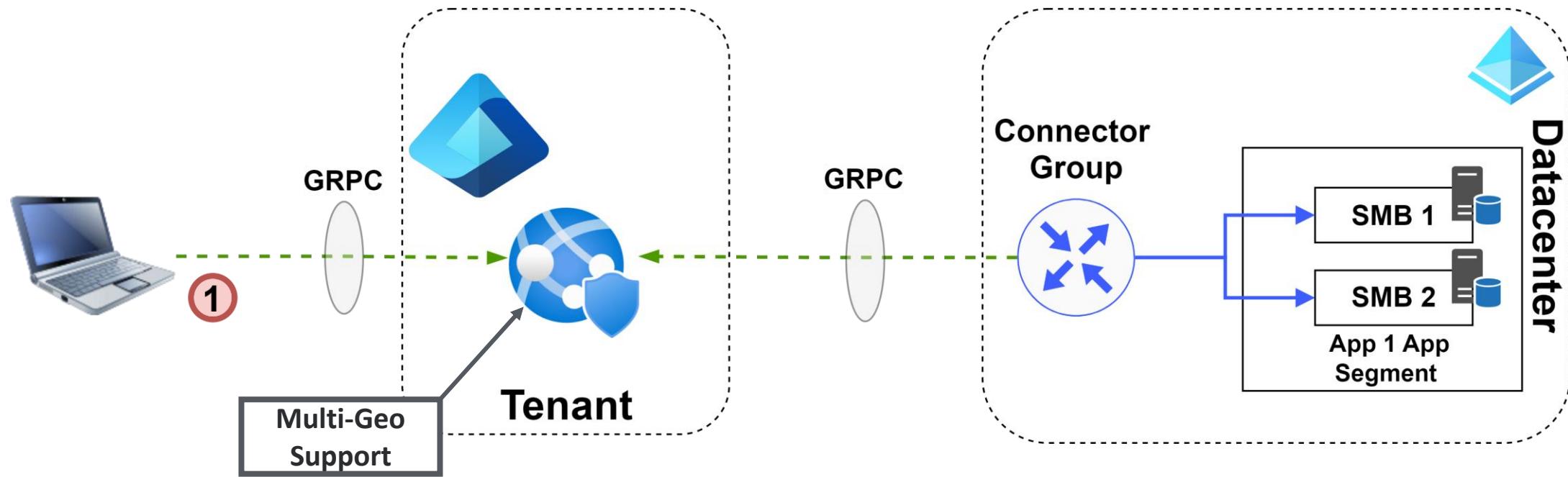
Optimize for performance





Entra Private Access connections

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

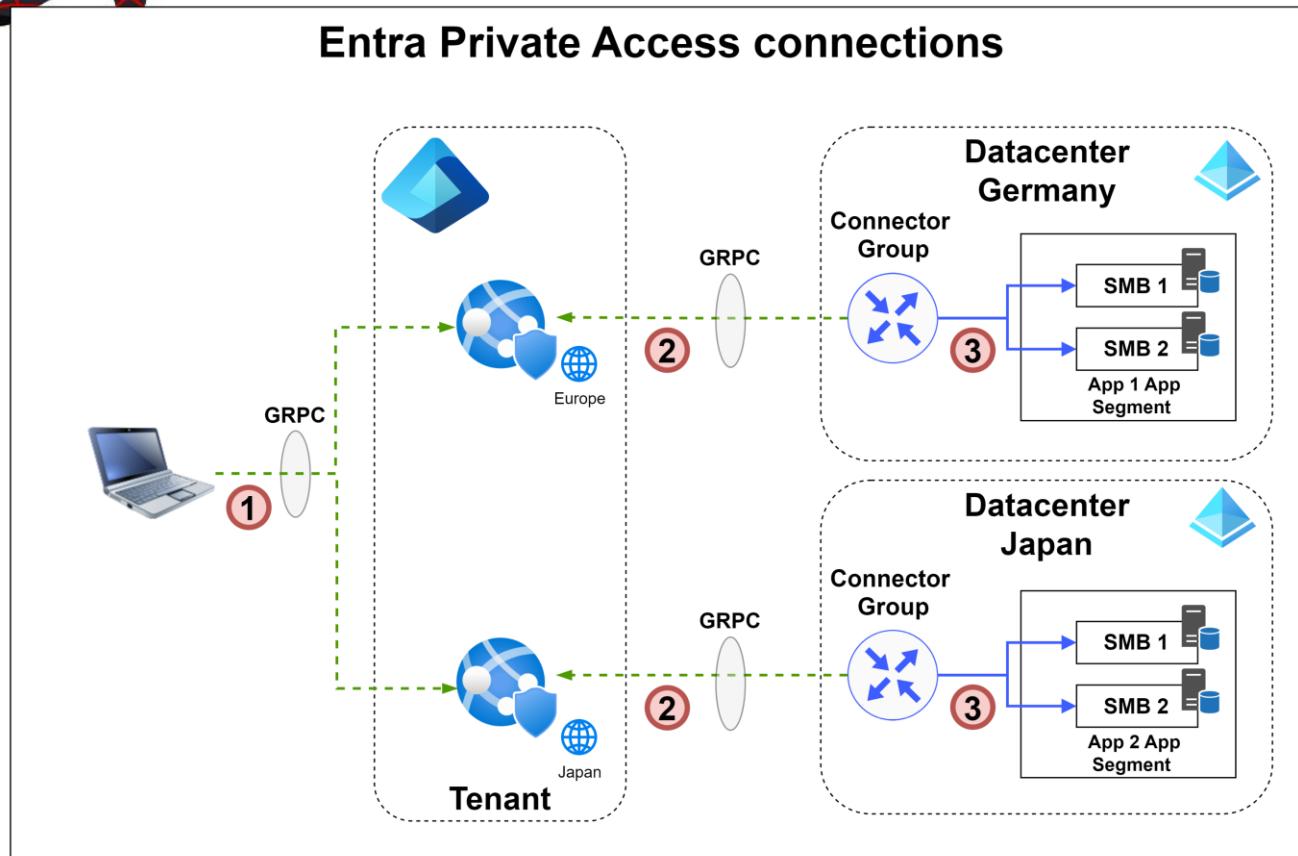
Pattern 2: Take advantage of ExpressRoute with Microsoft peering

Pattern 3: Take advantage of ExpressRoute with private peering



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

Create Connector Group

Connector Group Details

Save Discard Delete

Name *

North America

Europe

Australia

Asia

Japan

This connector group has no connectors assigned.

0 application(s) assigned to this connector group.

Optimize for a specific country/region. Use this option to optimize traffic flow between the country/region. Connectors must be using the same protocol.

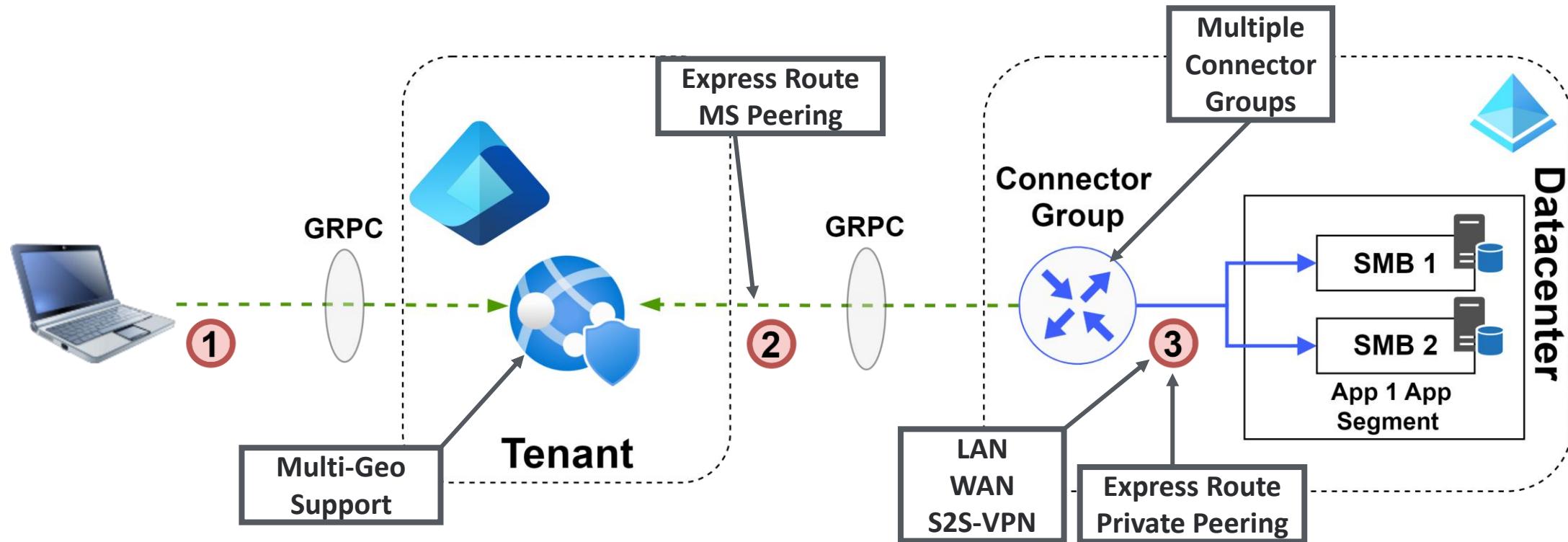
Learn more

Select Country/Region



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

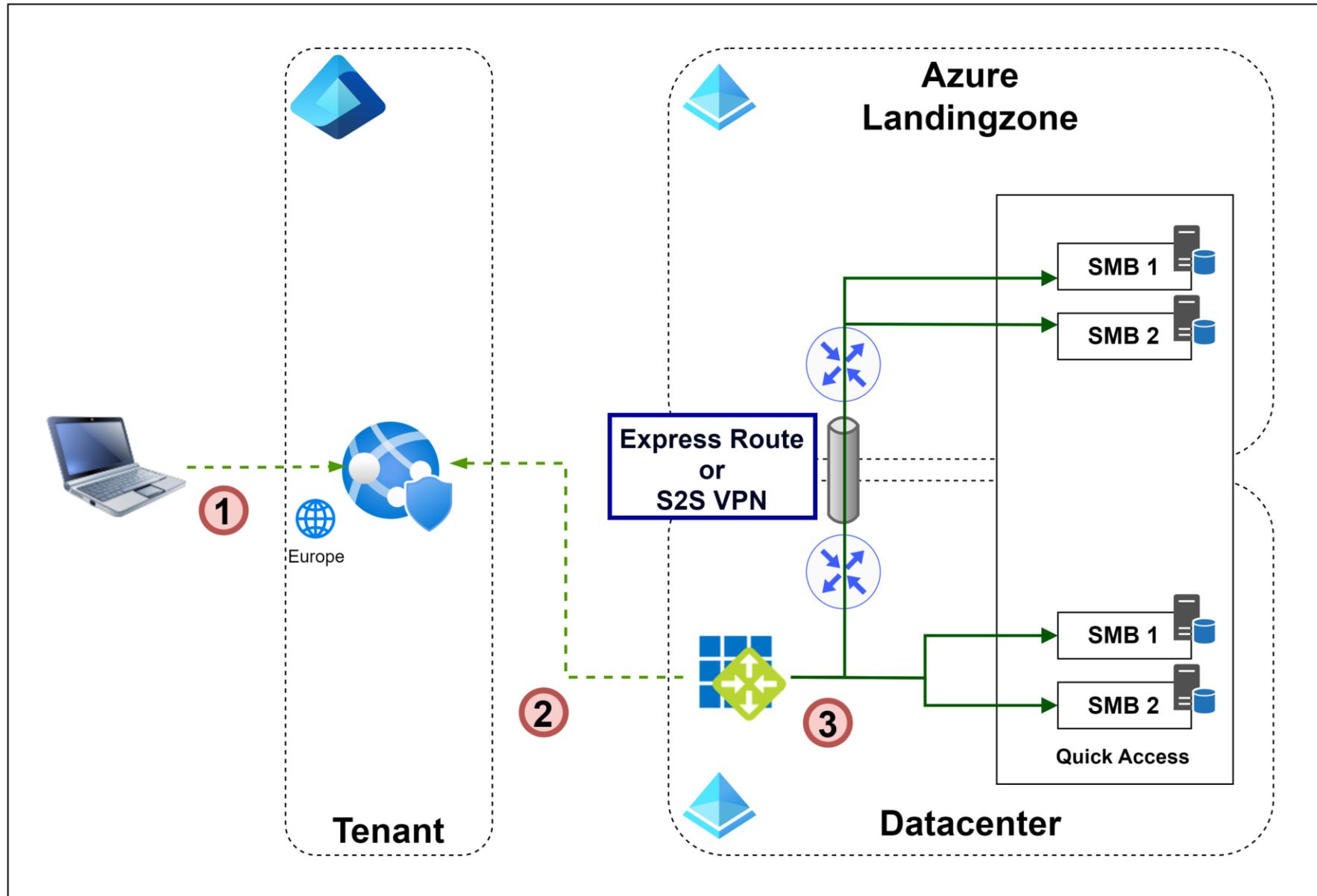
Pattern 3: Take advantage of ExpressRoute with private peering



Optimize traffic for multiple datacenter

www.wpninjas.eu
#WPNinjaS

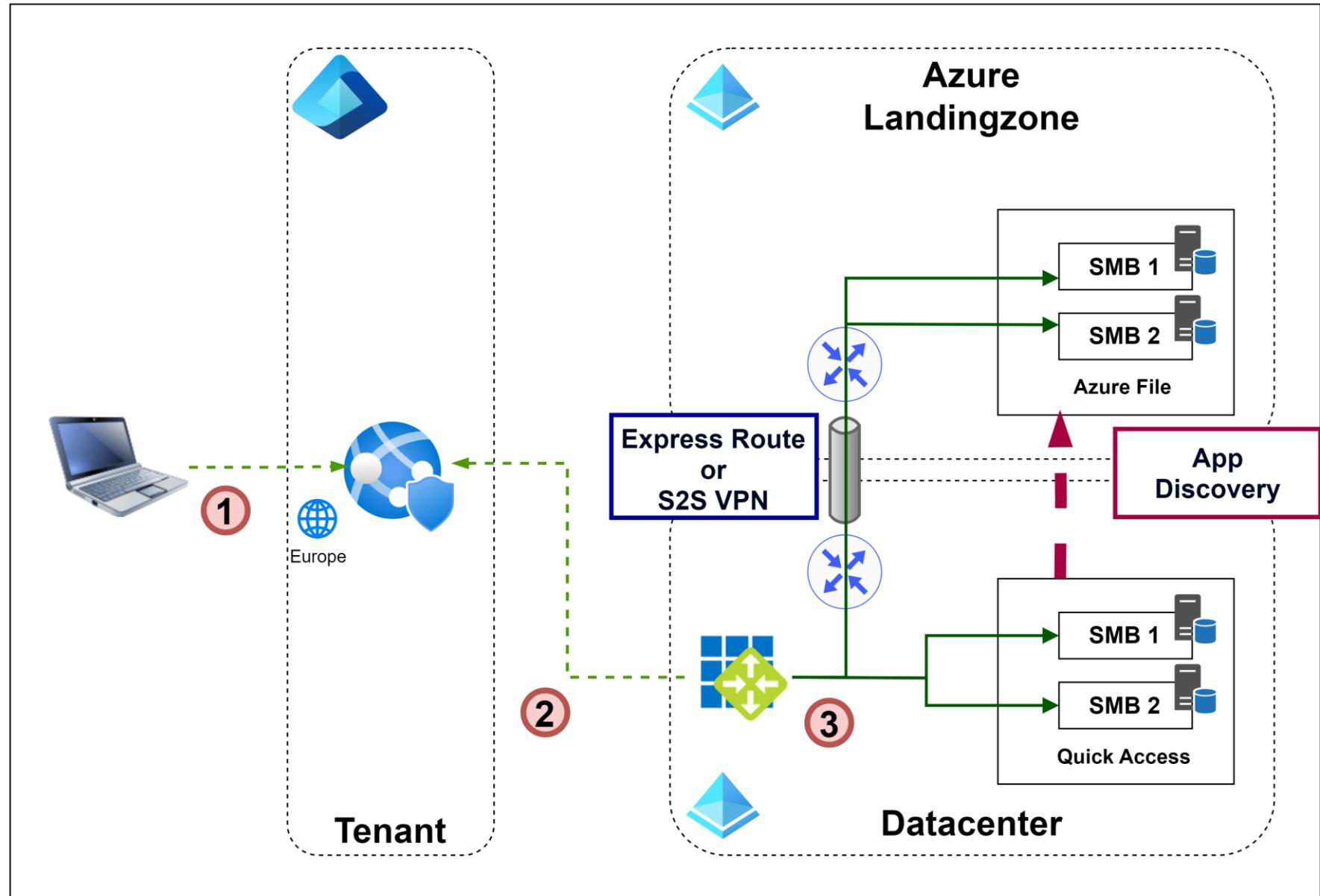
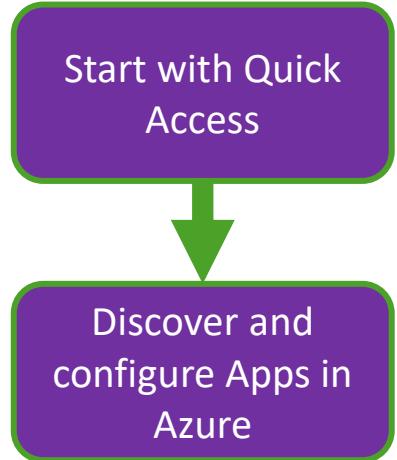
Start with Quick Access





Optimize traffic for multiple datacenter

www.wpninjas.eu
#WPNinjaS

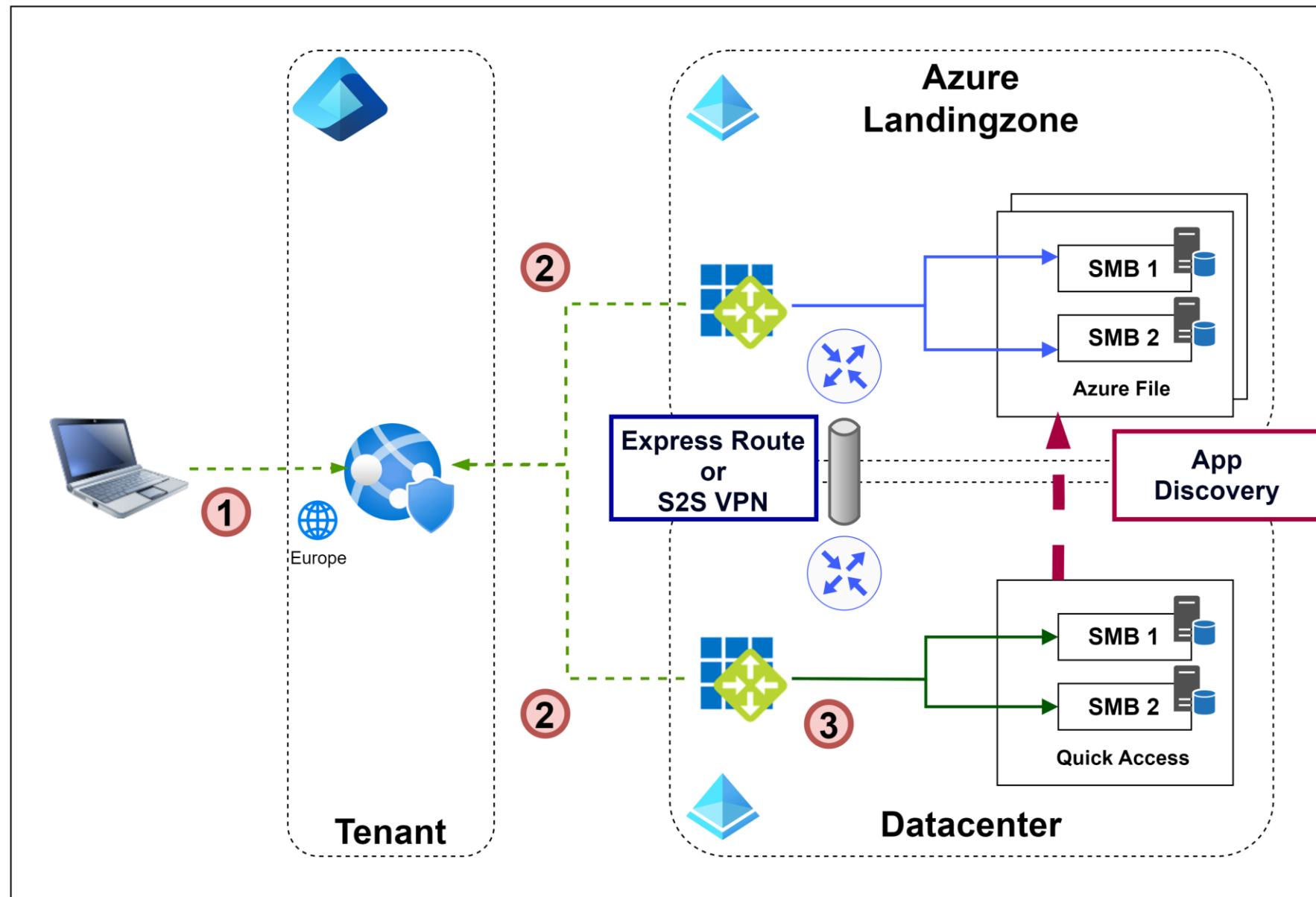




Optimize traffic for multiple datacenter

www.wpninjas.eu
#WPNinjaS

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



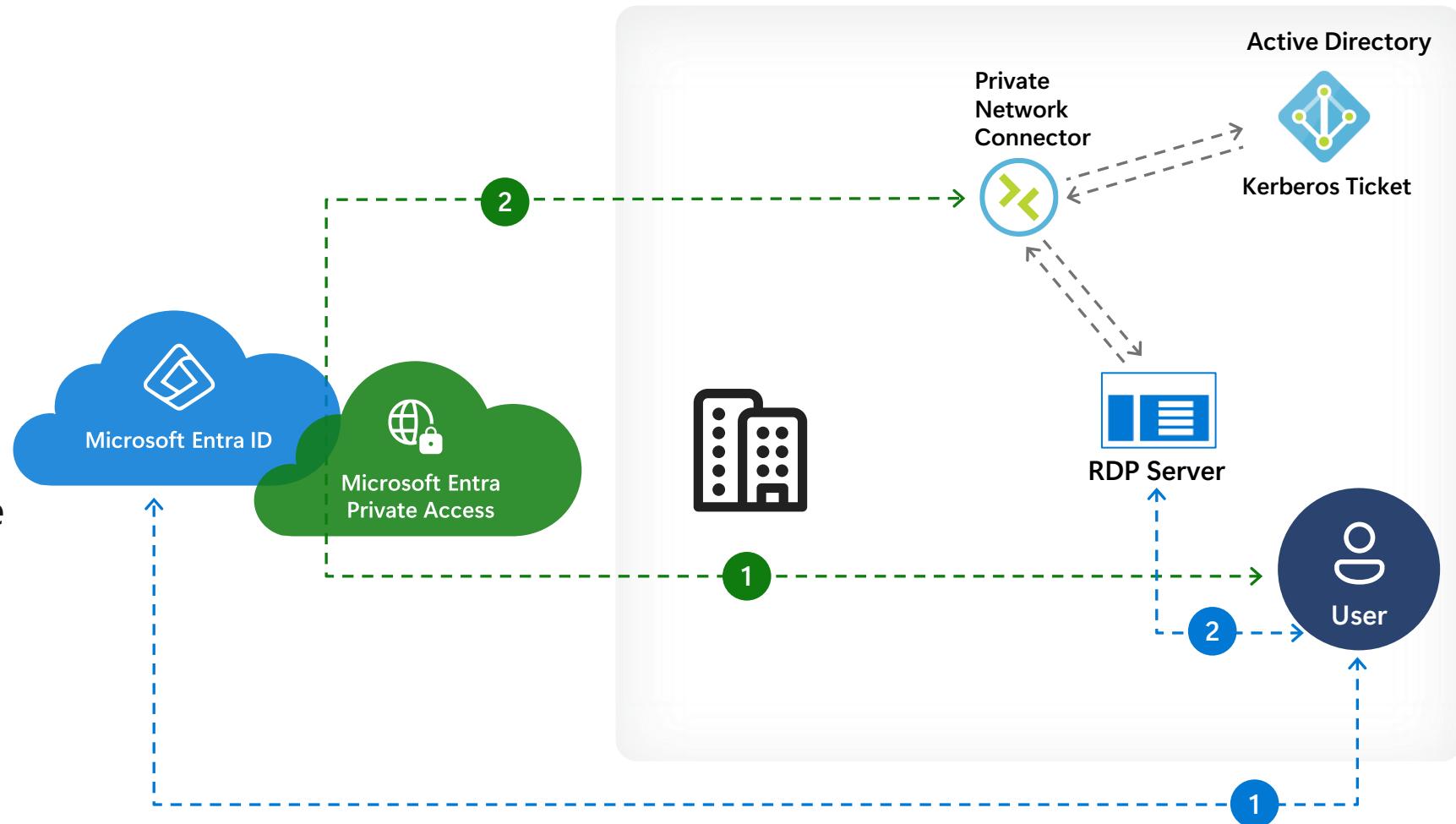


Intelligent Local Access

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...

www.wpninjas.eu
#WPNinjaS

Disabling the GSA client

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

Use Intelligent Local Access

- + 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

Route traffic through the connector

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

*Chris' wish for the future



Demo

www.wpninjas.eu
#WPNinjaS

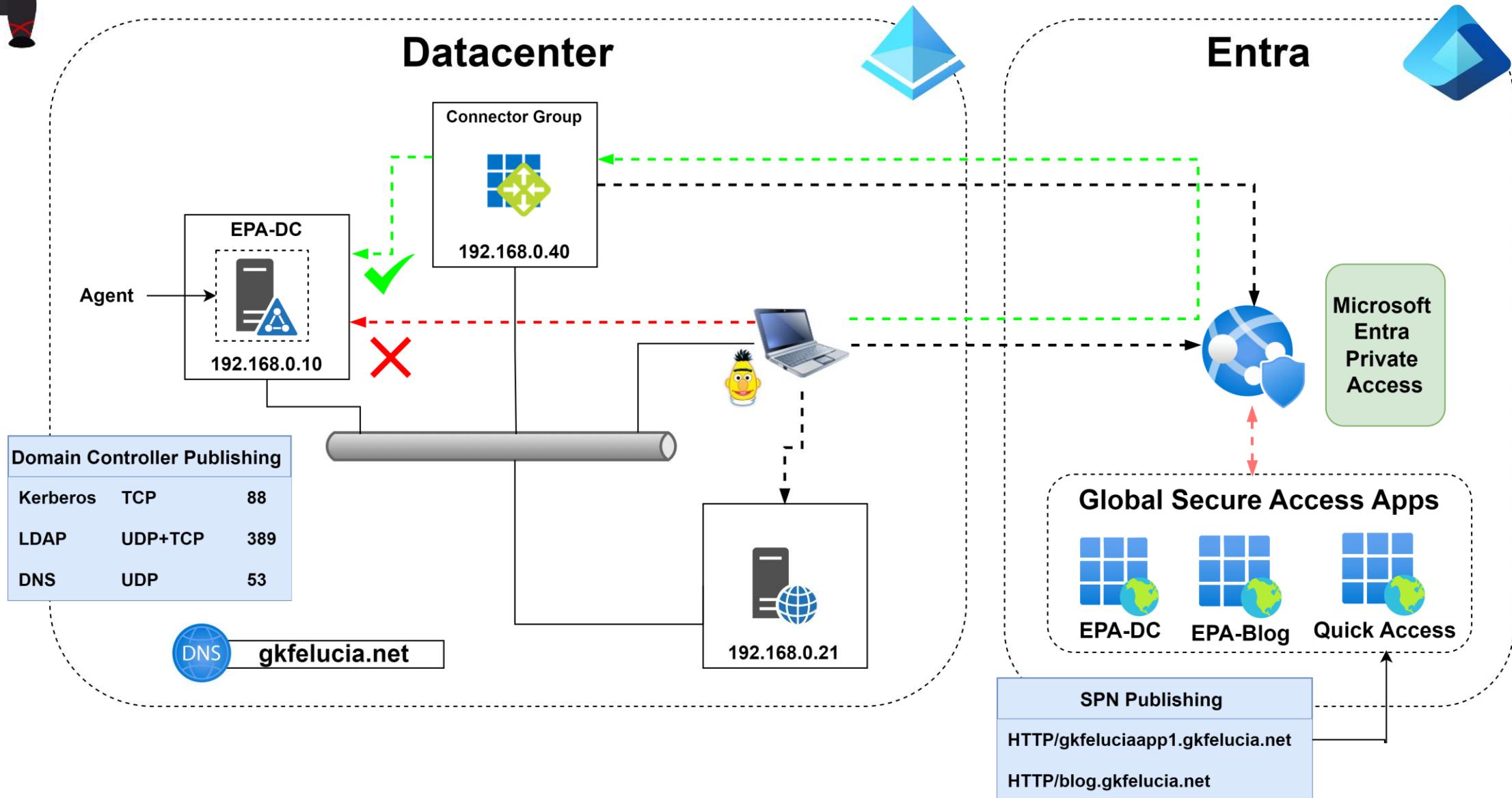
Private Access for Domain
Controllers





Private Access for Domain Controllers

www.wpninjas.eu
#WPNinjaS





Private Access for Domain Controllers

www.wpninjas.eu
#WPNinjaS

The image shows a Windows desktop environment with the following elements:

- Windows PowerShell** window: Shows the command PS C:\Users\Bert>.
- Global Secure Access** application window:
 - Status**: Private access disabled (Private Access is disabled by user).
 - Channels**:
 - Private: Disabled (button labeled "Enable")
 - Entra: Connected
 - M365: Connected
 - Additional details**: Account: Bert@gkfelicia.net, Tenant id: 0f642f1e-8030-465d-91cf-5252c6ca581b, Show more details.
 - User Profile**: Bert
 - Settings**
- Microsoft Edge browser** window:
 - Address bar: Search or enter web address
 - Favorites bar: Import favorites, LAB Demo Teams ~..., Home | Microsoft 365, Chris Brumm's Blog...
 - Weather: 17°C
 - System tray: DE, 3D65, battery status, network status, date/time: 03/08/2025, 13:43.



What about NTLM?

www.wpninjas.eu
#WPNinjaS

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.

The screenshot shows the Internet Information Services (IIS) Manager interface. The left pane displays the 'Connections' tree with 'Start Page', 'GKFELUCIAAPP1 (GKFELUCIA)', 'Application Pools', and 'Sites'. Under 'Sites', 'Default Web Site' is selected. The right pane is titled 'Authentication' and shows a table of authentication providers:

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Windows Authentication	Enabled	HTTP 401 Challenge

Below the table is a 'Providers' dialog box. It contains a list of 'Enabled Providers' with 'Negotiate:Kerberos' highlighted and enclosed in a red box. The 'Available Providers' dropdown is empty. Buttons for 'Move Up', 'Move Down', and 'Remove' are visible, along with 'OK' and 'Cancel' buttons at the bottom.

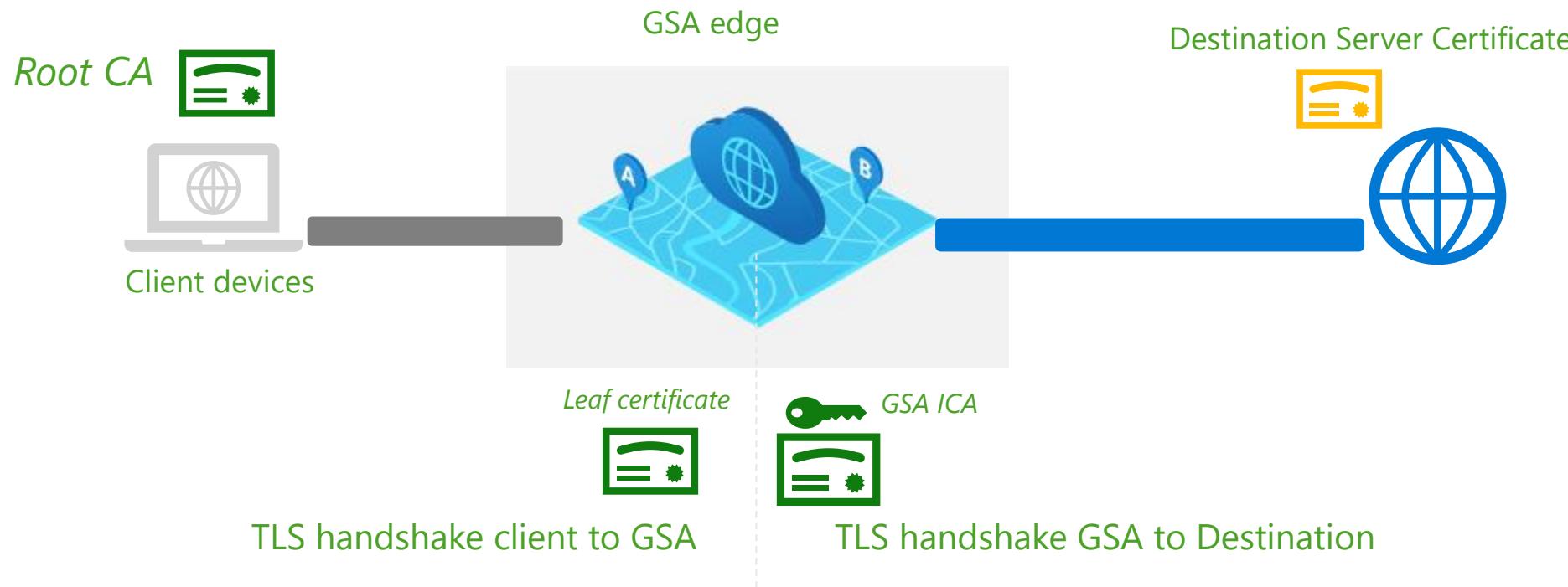
Why is TLS inspection a game changer? for Entra Internet Access





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

www.wpninjas.eu
#WPNinjaS

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_RESET

[Troubleshoot](#) [Refresh](#)

Microsoft Edge

without TLS inspection

You can't access this destination

www.marlboro.com/
It's been restricted by your organization.

More info

Category: AlcoholAndTobacco, Business
Threat Type: -
Connection ID: x3XXPO+xwE2WEkSr.0
Timestamp: 2025-07-27T09:02:56.445Z

Microsoft Entra Internet Access

with TLS inspection



URL Filtering at path level

www.wpninjas.eu
#WPNinjaS

A screenshot of a web browser displaying the homepage of "Chris Brumm's Blog". The page features a large banner image of a city street at night with reflections in water. The blog title "Chris Brumm's Blog" is prominently displayed in white text. A navigation menu at the top includes "ALL POSTS", "GLOBAL SECURE ACCESS", "ARCHIVE", and "ABOUT". Below the banner, there is a featured post titled "Entra Private Access and the future of the Entra App Proxy".

Entra Private Access and the future of the Entra App Proxy

The blog compares Entra Private Access and Entra App Proxy and helps to decide which to use when.

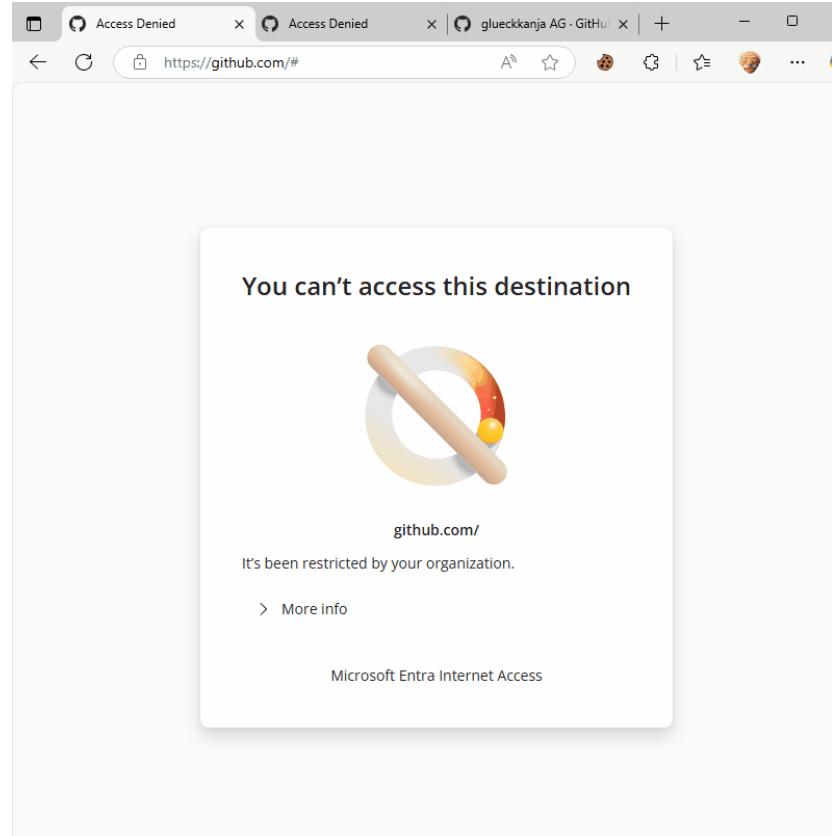
Since the release of Entra Private Access, I have been getting more and more questions about the future

Block a specific subpage



URL Filtering at path level

www.wpninjas.eu
#WPNinjaS



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.

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

www.wpninjas.eu
#WPNinjaS





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



And what else is new?

www.wpninjas.eu
#WPNinjaS

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

The screenshot shows the Microsoft Graph Explorer interface. The URL in the address bar is <https://developer.microsoft.com/en-us/graph/graph-explorer>. The request method is set to GET, version v1.0, and the endpoint is <https://graph.microsoft.com/v1.0/me>. The 'Request Body' tab is selected, showing a placeholder for the query. Below the request body, there are tabs for 'Response preview', 'Response headers', 'Code snippets', 'Toolkit component', and 'Adaptive cards'. The main pane is currently loading, indicated by a 'Loading...' message. The left sidebar includes sections for 'Sample queries', 'API Explorer', and 'History', along with a search bar and a link to the Microsoft Graph API Reference docs.

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



Bonus round

www.wpninjas.eu
#WPNinjaS

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	19
Private Access Gateway	166
Connector	5
Backend app	

Upload Throughput Test

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

Download Throughput Test

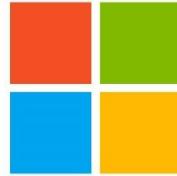
Next hop	Throughput (Mbps)	File Size	Location
PoP	390.62	50.0 MB	



Thank you Sponsors

www.wpninjas.eu
#WPNinjaS

Diamond Sponsor



Microsoft

Platinum Sponsors

W2Pint



RECAST SOFTWARE

glueck■kanja

Gold Sponsors



nerdio

Rimo3

eido



Silver Sponsors



APENTO

PROACT

control^{UP}
UMB creating time®





We love Feedback

<https://wpninja25.sched.com/>



Great Session!



Okay Session!



Not so okay Session!



Workplace Ninja
Summit 2025

