Azure Networking deep dive

Azure User Group Iceland
Virtual Meetup
10.11.2023

Haflidi Fridthjofsson

Principal Cloud Architect at Sopra Steria

- IT specialist since 2011.
- Microsoft Certified Professional (MCP) since 2014.
- Microsoft MVP within Security since 2023.
- Co-founder of the Microsoft Security User Group.

- Specialist within.
  - Azure Infrastructure.
  - Infrastructure as code.
  - Security.

- Free Time
  - Spending time with my family.
  - Check out and learn new technology
  - Bit of gaming, primarily FPS here and there when I got time.

Microsoft Security
USER GROUP

Follow me on:

@haflidif | in/haflidif | azureviking.com | haflidif

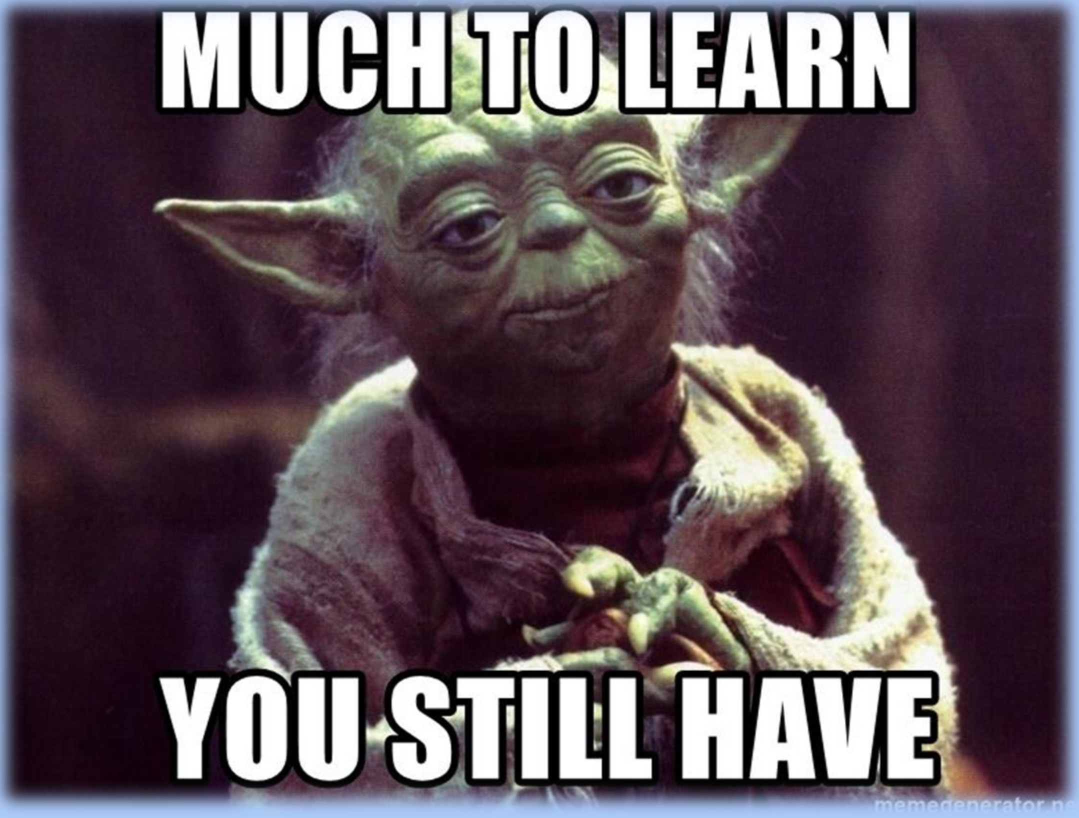
AzUG.is

AZURE VIKING

What do we want to achieve

Your takeaways from this session.

- Understand what Azure Network is built on.
- Get more insights on what's new in Azure Networking, especially on the newly announced Global Secure Access in preview.
- Get answers to the questions and concerns from the real-life experience that you posted on Facebook.



Azure Network

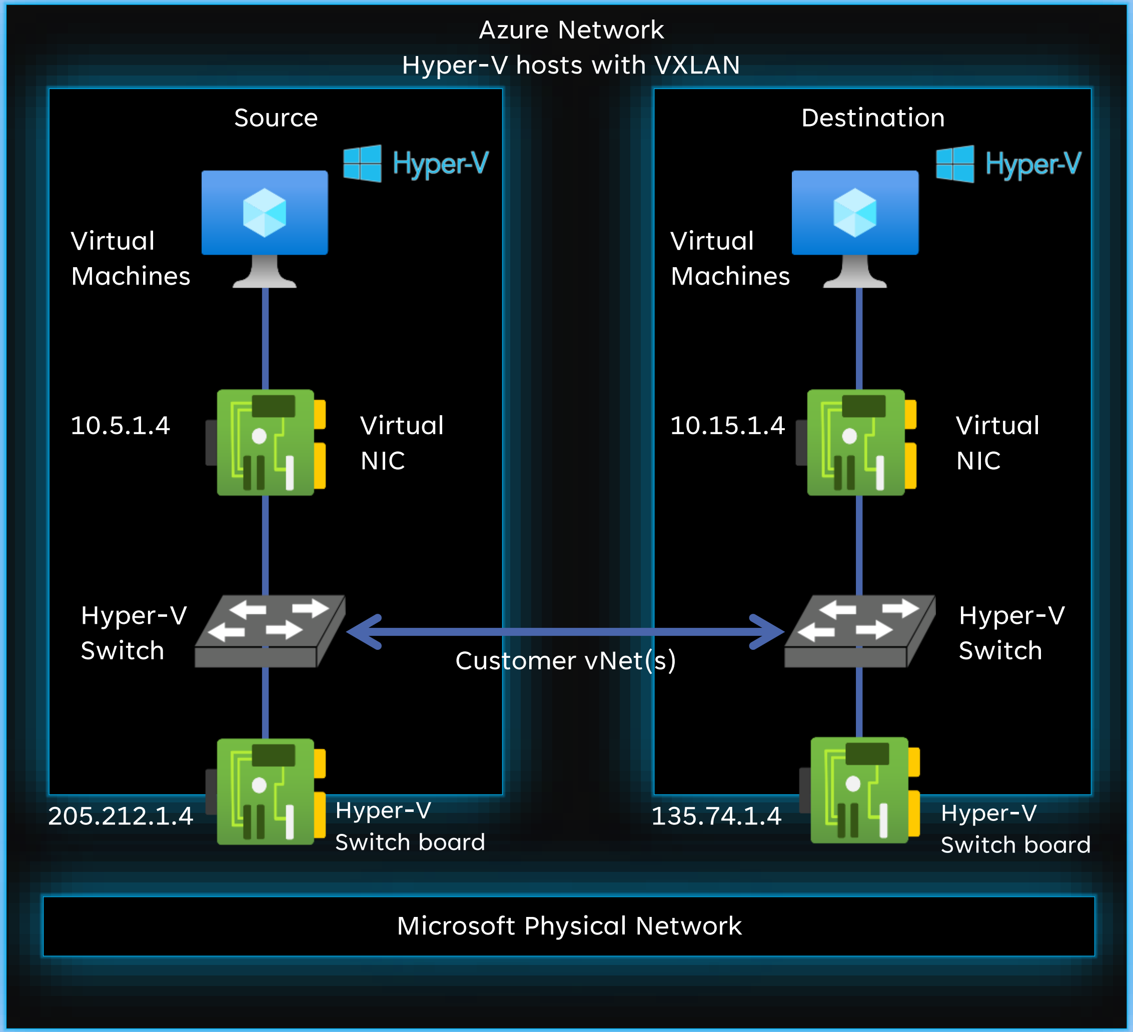
What is Azure Network ?

Software-Defined Networking

Azure Network

The rules are bit different

- On-premises network
  - Where packets flow are controlled by cables.
  - Cut the cable or no cable = No connection.
  - A + B = C
  - Secure Network = Core Network Switch, Firewall and router between those cables.
- Azure Network
  - Where packets flow between source and destination.
  - A + B ≠ C
  - Everything is running on a Virtual Machine or within a Virtual Machine
  - Secure network, then you need to think a bit differently.



Source: Aidan Finn: Routing - The Virtual Cabling of Secure Azure Networking

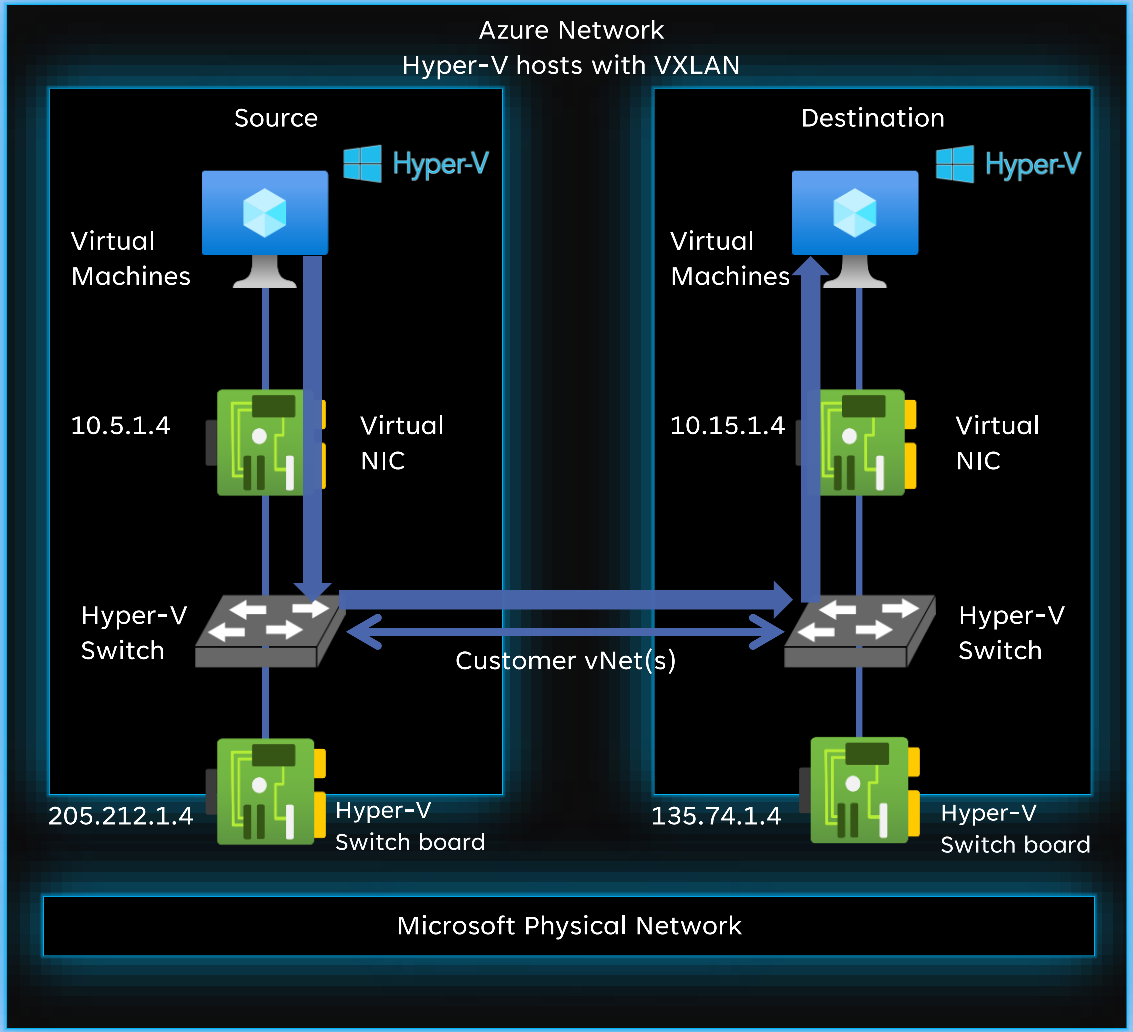
AzUG.is

AZURE VIKING

Azure Network

The rules are bit different

- On-premises network
  - Where packets flow are controlled by cables.
  - Cut the cable or no cable = No connection.
  - A + B = C
  - Secure Network = Core Network Switch, Firewall and router between those cables.
- Azure Network
  - Where packets flow between source and destination.
  - A + B ≠ C
  - Everything is running on a Virtual Machine or within a Virtual Machine
  - Secure network, then you need to think a bit differently.



Azure Network
Hyper-V hosts with VXLAN

Source
Hyper-V
Virtual Machines
10.5.1.4
Virtual NIC
Hyper-V Switch
205.212.1.4
Hyper-V Switch board

Destination
Hyper-V
Virtual Machines
10.15.1.4
Virtual NIC
Hyper-V Switch
135.74.1.4
Hyper-V Switch board

Customer vNet(s)

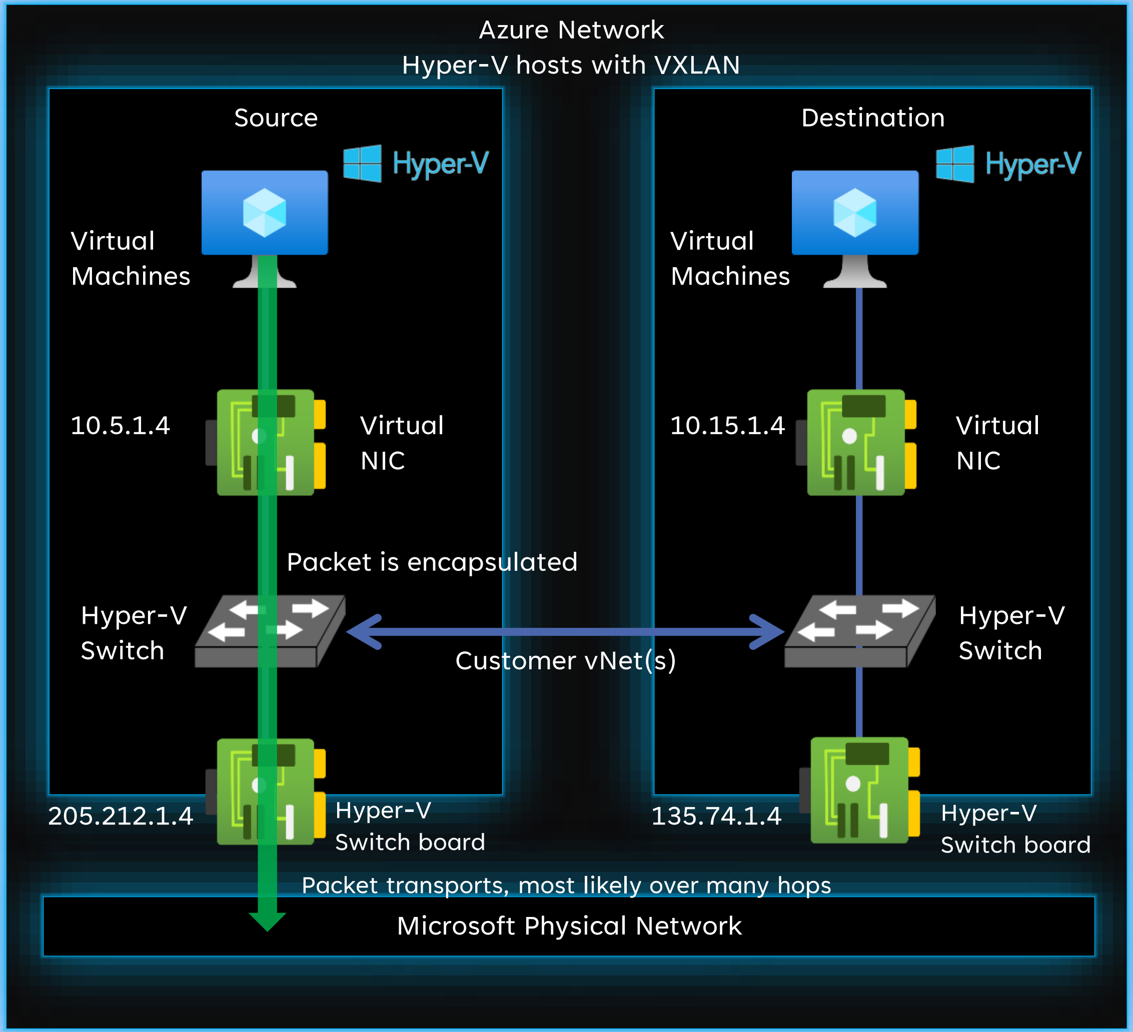
Microsoft Physical Network

Source: Aidan Finn: Routing - The Virtual Cabling of Secure Azure Networking

Azure Network

The rules are bit different

- On-premises network
  - Where packets flow are controlled by cables.
  - Cut the cable or no cable = No connection.
  - A + B = C
  - Secure Network = Core Network Switch, Firewall and router between those cables.
- Azure Network
  - Where packets flow between source and destination.
  - A + B ≠ C
  - Everything is running on a Virtual Machine or within a Virtual Machine
  - Secure network, then you need to think a bit differently.



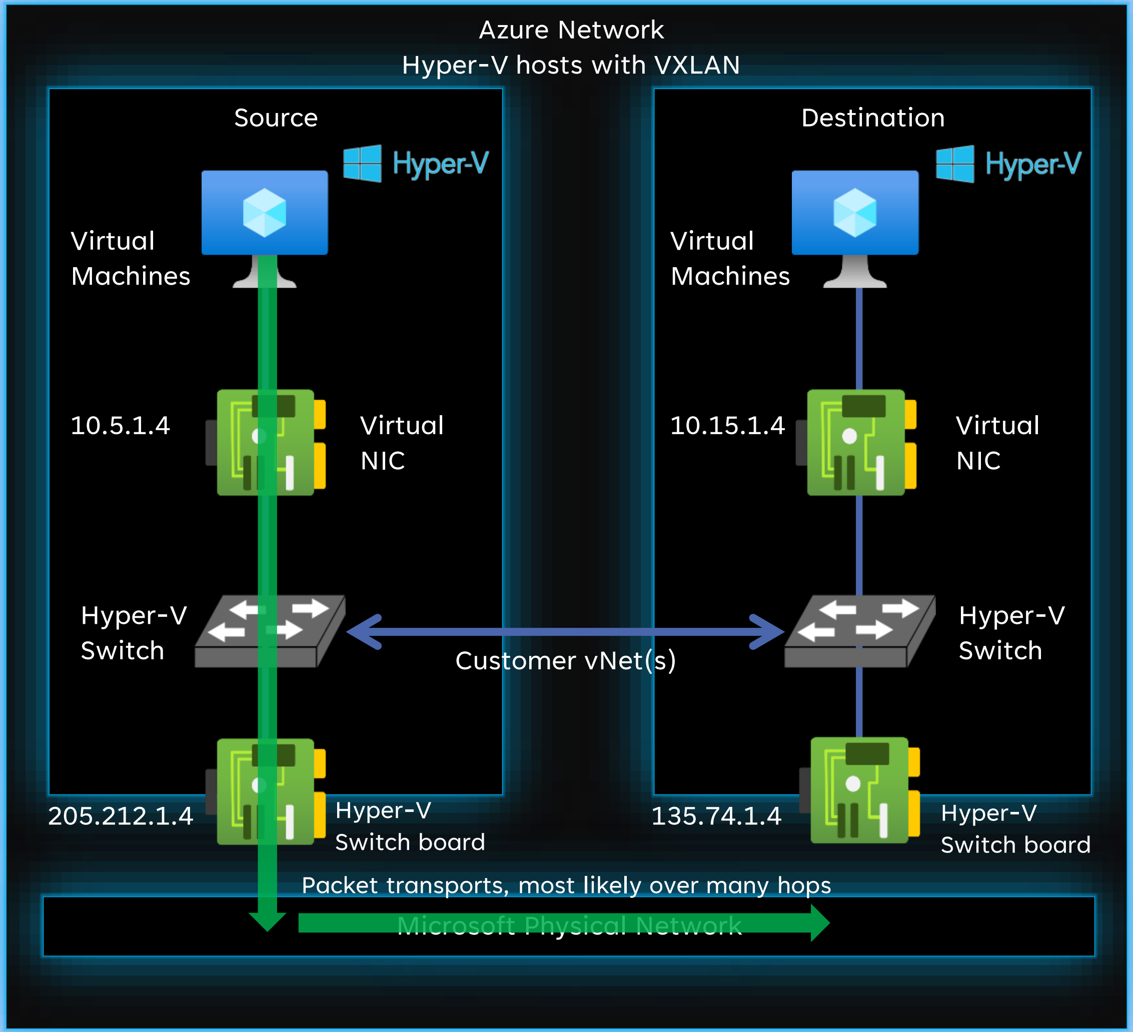
Source: Aidan Finn: Routing - The Virtual Cabling of Secure Azure Networking

Azure Network

The rules are bit different

- On-premises network
  - Where packets flow are controlled by cables.
  - Cut the cable or no cable = No connection.
  - A + B = C
  - Secure Network = Core Network Switch, Firewall and router between those cables.

- Azure Network
  - Where packets flow between source and destination.
  - A + B ≠ C
  - Everything is running on a Virtual Machine or within a Virtual Machine
  - Secure network, then you need to think a bit differently.

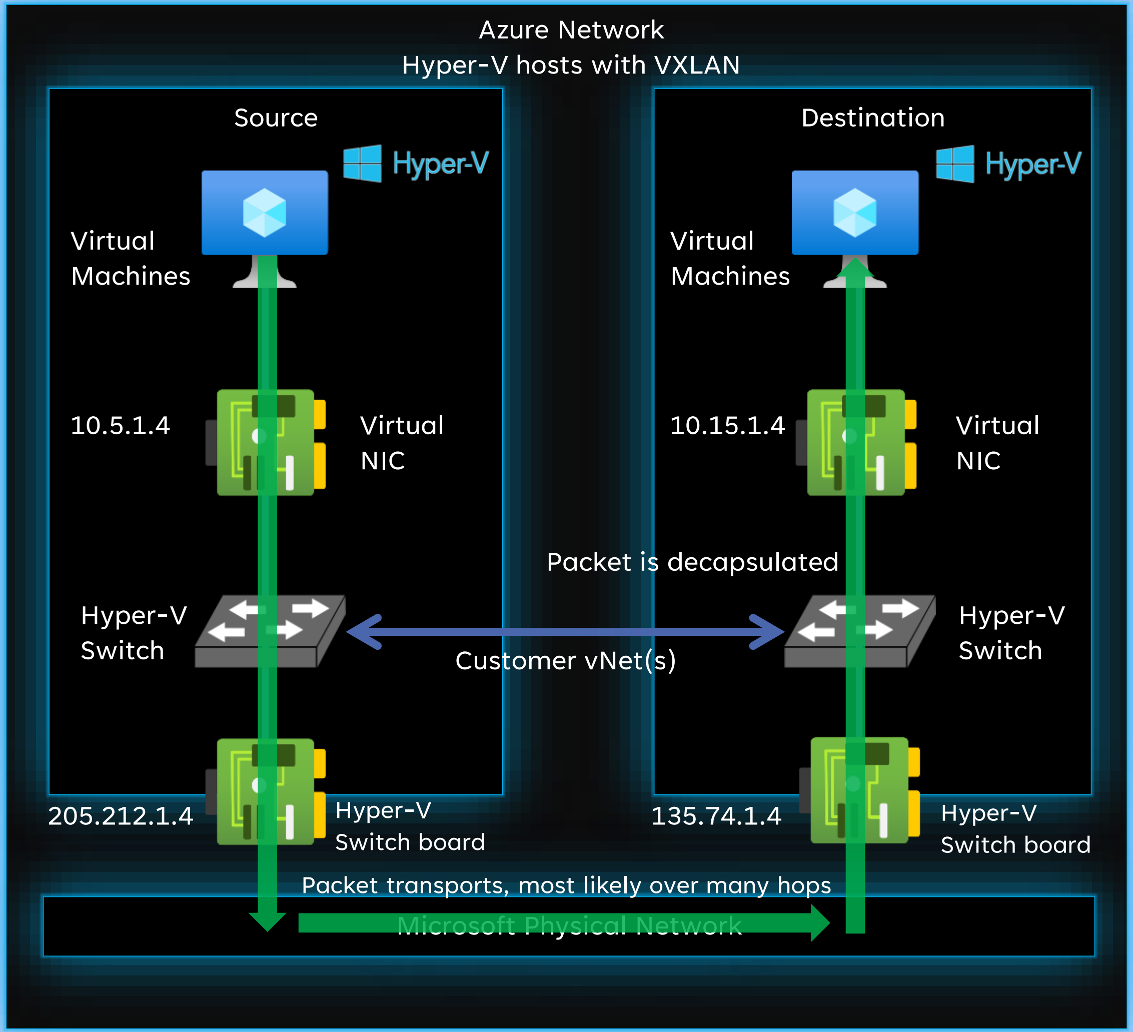


Source: Aidan Finn: Routing - The Virtual Cabling of Secure Azure Networking

Azure Network

The rules are bit different

- On-premises network
  - Where packets flow are controlled by cables.
  - Cut the cable or no cable = No connection.
  - A + B = C
  - Secure Network = Core Network Switch, Firewall and router between those cables.
- Azure Network
  - Where packets flow between source and destination.
  - A + B ≠ C
  - Everything is running on a Virtual Machine or within a Virtual Machine
  - Secure network, then you need to think a bit differently.



Azure Network
Hyper-V hosts with VXLAN

Source

Destination

Hyper-V

Virtual Machines

10.5.1.4

10.15.1.4

Virtual NIC

Packet is decapsulated

Hyper-V Switch

Customer vNet(s)

205.212.1.4

135.74.1.4

Hyper-V Switch board

Packet transports, most likely over many hops

Microsoft Physical Network

Source: Aidan Finn: Routing - The Virtual Cabling of Secure Azure Networking

What’s new!

Latest technology within Azure Networking

Global Secure Access

PREVIEW

PREVIEW

PREVIEW

Microsoft´s solution for SASE (Secure Access Service Edge)

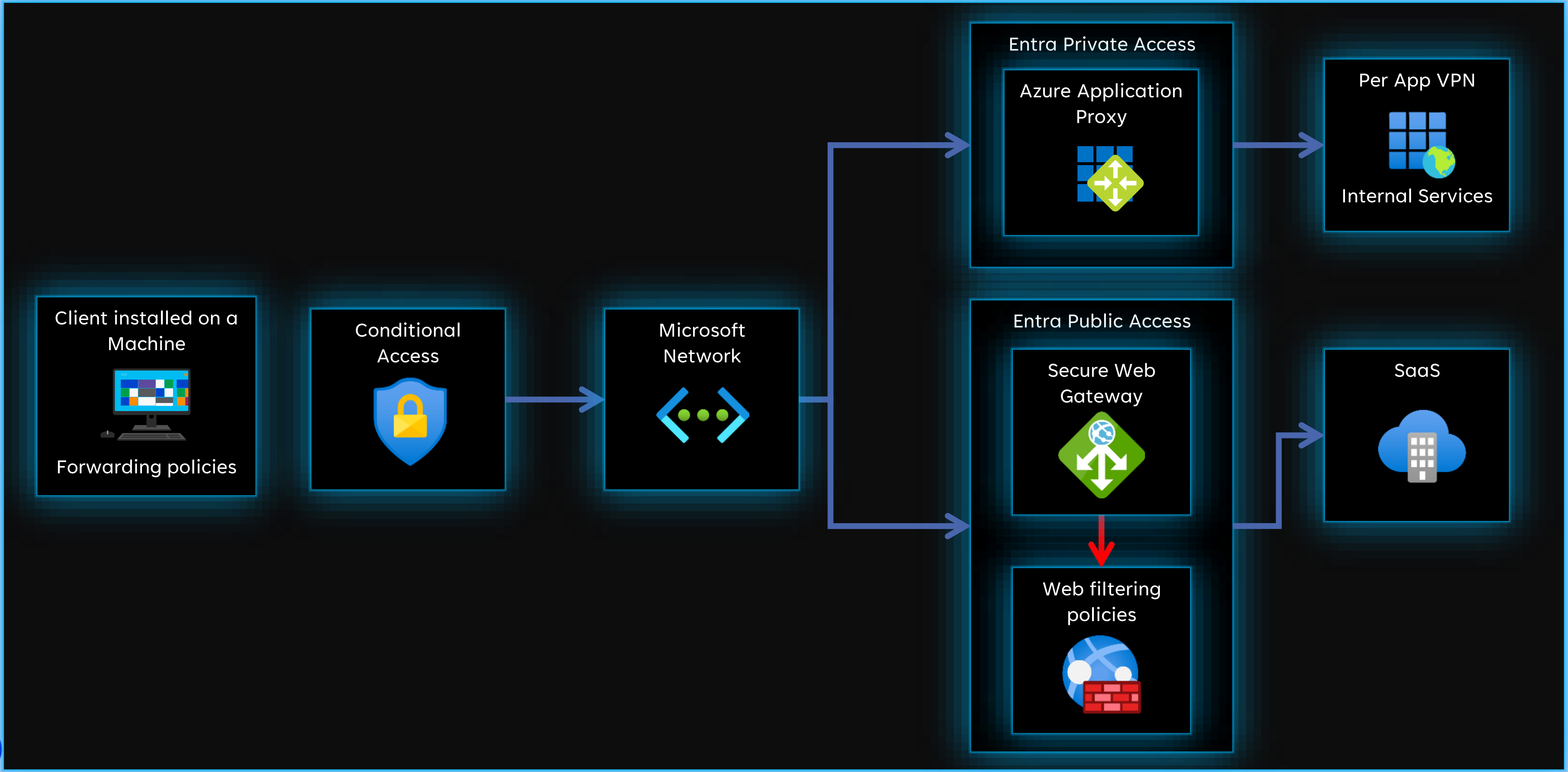
What's New!

Global Secure Access (Preview)

- Global Secure Access is Microsoft's Security Service Edge Solution (SASE)
- Was announced and made available in Preview in July.
  - Microsoft Entra Private Access (Public Preview)
  - Microsoft Entra Internet Access (Private Preview)
- Think about it as providing security on the network layer
- Price ? No clue will probably get more information about it at Ignite.
- Windows 10/11 Supported (MAC, iOS and Android to follow)
- Built on Entra ID, Conditional Access and Application Proxy.
- Connect either using client or office network (S2S VPN)

What’s New!

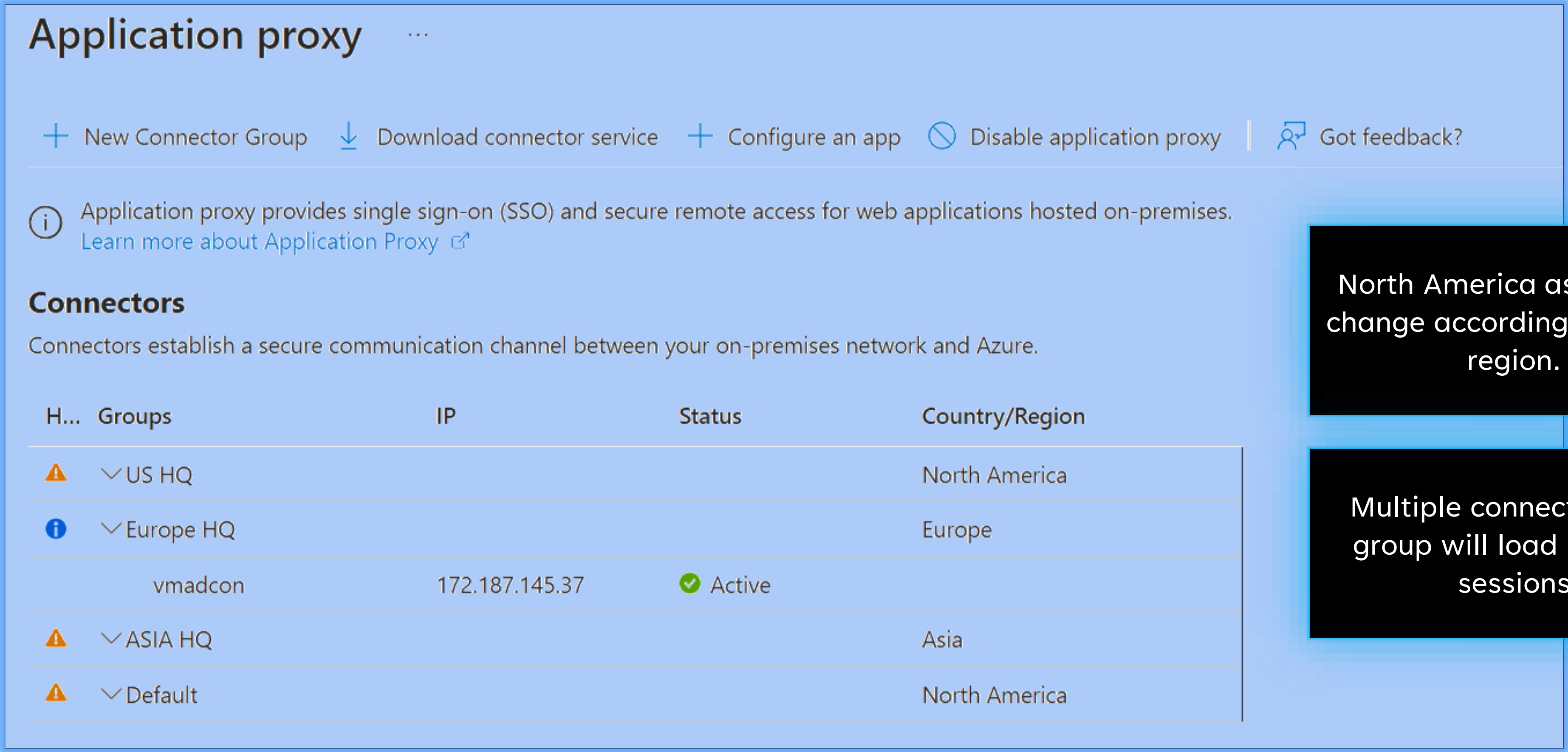
Global Secure Access (Preview) overview



© 2023 Haflidi Fridthjofsson @haflidif - www.azureviking.com

What's New!

Global Secure Access (Preview) – Microsoft Entra Private Access – Application Proxy



Application proxy ...

Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises.
Learn more about Application Proxy

Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

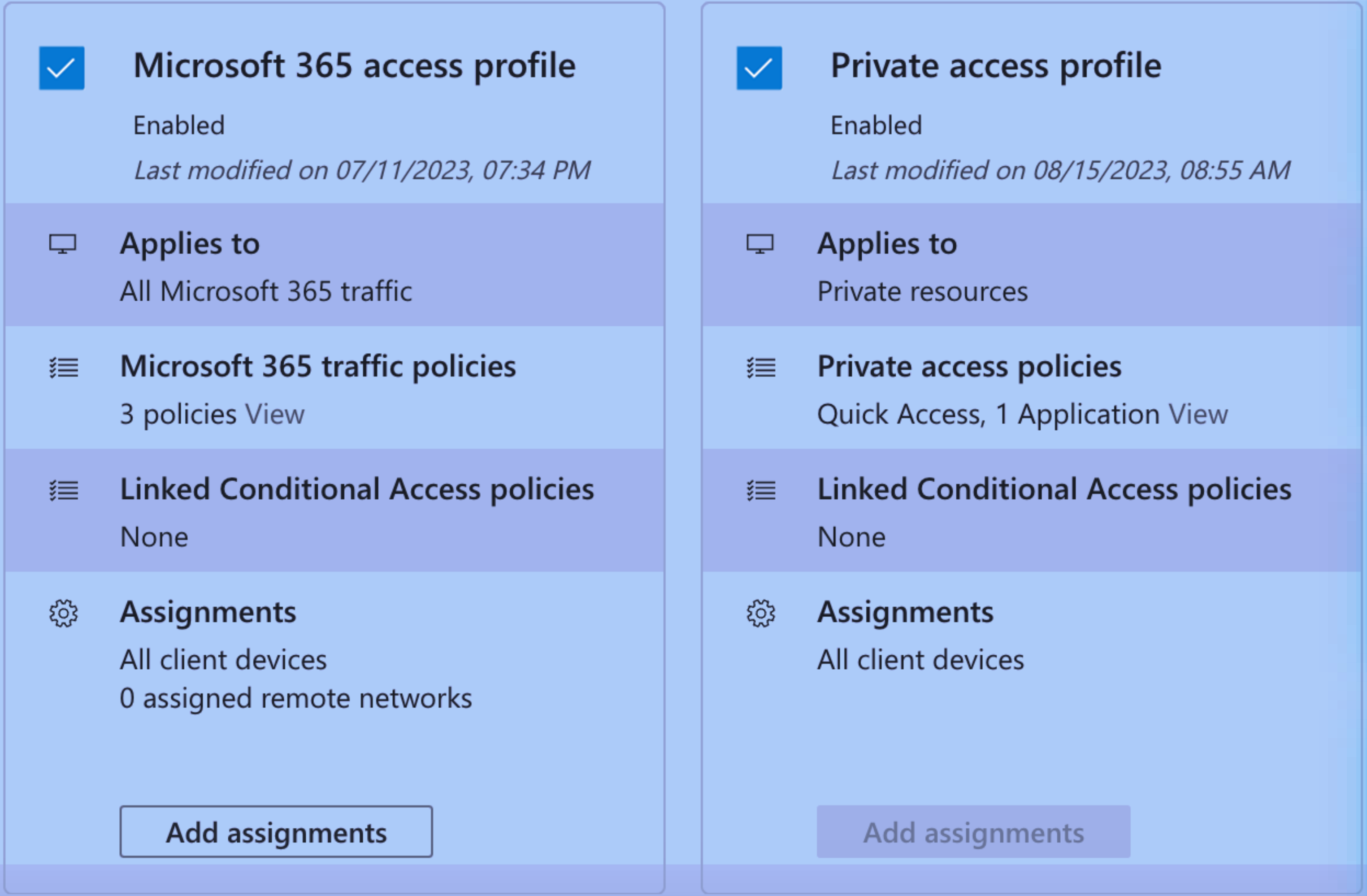
H...	Groups	IP	Status	Country/Region
⚠	US HQ			North America
ℹ	Europe HQ			Europe
	vmadcon	172.187.145.37	✓ Active	
⚠	ASIA HQ			Asia
⚠	Default			North America

North America as default, change accordingly to each region.

Multiple connectors in a group will load balance sessions

What’s New!

Global Secure Access (Preview) – Forwarding policies



☑ **Microsoft 365 access profile**

Enabled

Last modified on 07/11/2023, 07:34 PM

Applies to
All Microsoft 365 traffic

Microsoft 365 traffic policies
3 policies View

Linked Conditional Access policies
None

Assignments
All client devices
0 assigned remote networks

☑ **Private access profile**

Enabled

Last modified on 08/15/2023, 08:55 AM

Applies to
Private resources

Private access policies
Quick Access, 1 Application View

Linked Conditional Access policies
None

Assignments
All client devices

Policies that define what kind of traffic should be routed

Services / Networks that are not defined will not be routed via the service

Can be viewed as a split-tunnelling mechanism.

Note: Currently only, the agent can use private access.

What’s New!

Global Secure Access (Preview) – Quick Access vs per app access.

- Quick Access
  - Used to define access to larger subset of resources, such as IPs, IP Ranges or FQDN + Ports that you want to allow access to.
  - Only one conditional access policy can be assigned to that scope.

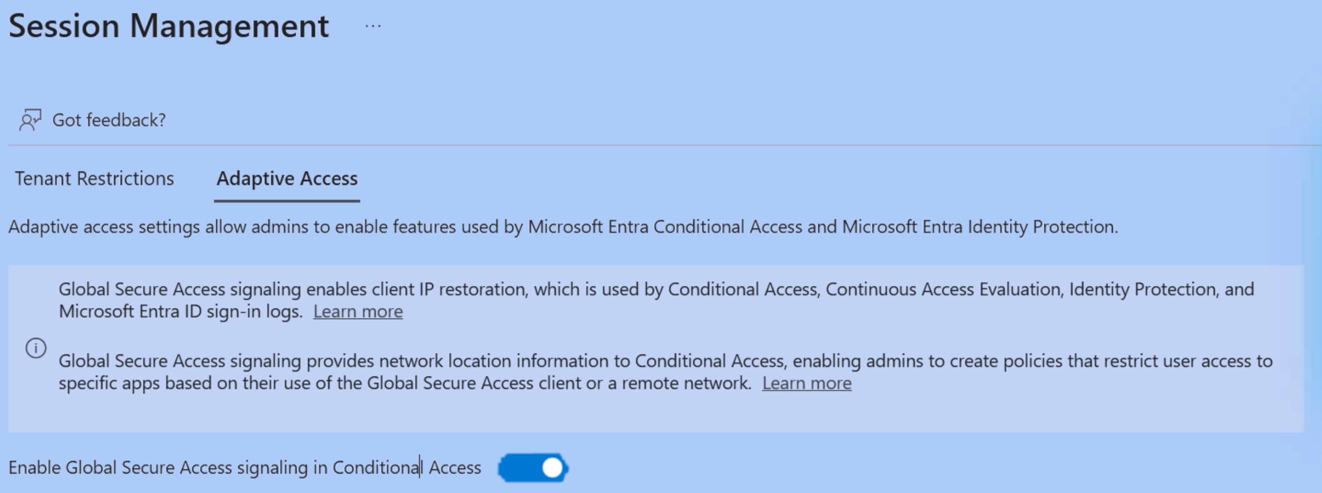
- Per app Access
  - Used to define access to subset of private services.
  - Allows for more granular conditional policies for specific applications.

What’s New!

Global Secure Access (Preview) – Other usable features to be aware of.

- Tenant Restriction
  - Restrict users from other Entra ID directories to access services using our devices.

- Adaptive Access
  - Provides Network signals to conditional access.



Session Management

Got feedback?

Tenant Restrictions | Adaptive Access

Adaptive access settings allow admins to enable features used by Microsoft Entra Conditional Access and Microsoft Entra Identity Protection.

Global Secure Access signaling enables client IP restoration, which is used by Conditional Access, Continuous Access Evaluation, Identity Protection, and Microsoft Entra ID sign-in logs. Learn more

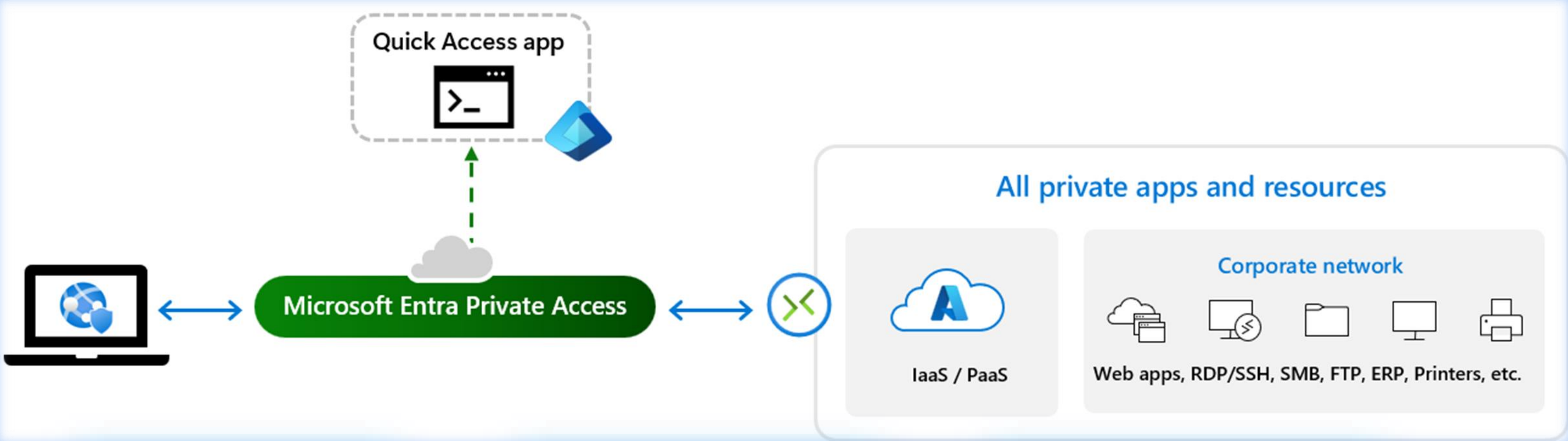
Global Secure Access signaling provides network location information to Conditional Access, enabling admins to create policies that restrict user access to specific apps based on their use of the Global Secure Access client or a remote network. Learn more

Enable Global Secure Access signaling in Conditional Access: On

If this is not enabled your outgoing IP address will be the Global Secure access one and not the actual public IP that the client uses.

What’s New!

Global Secure Access (Preview) – Microsoft Entra Private Access


Quick Access app
Microsoft Entra Private Access
All private apps and resources
IaaS / PaaS
Corporate network
Web apps, RDP/SSH, SMB, FTP, ERP, Printers, etc.

Traffic tunnelled over R-TCP

Access either on network or on application level

Requires Windows Server for App Proxy

What’s New!

Global Secure Access (Preview) – Some limitations to be aware of

- Does not support DoH (DNS-Over-HTTPS)
- Does not (yet..) support UDP for internal service
    - For instance, QUIC protocol needs to be blocked
- Does not fully support IPv6
- Can support Entra ID B2B If the device home is the main Entra ID Tenant.
- Single label domains are not supported
    - e.g. https://yourserver01
- Tunneling traffic by IP Address requires that the IP Range are outside of the end-user device local subnet.
    - e.g. If your local subnet has the same address range as the resource you are trying to connect to then that will be a problem.

Demo

Global Secure Access

Questions and concerns.

From real life experience

Questions and concerns

From real life experience

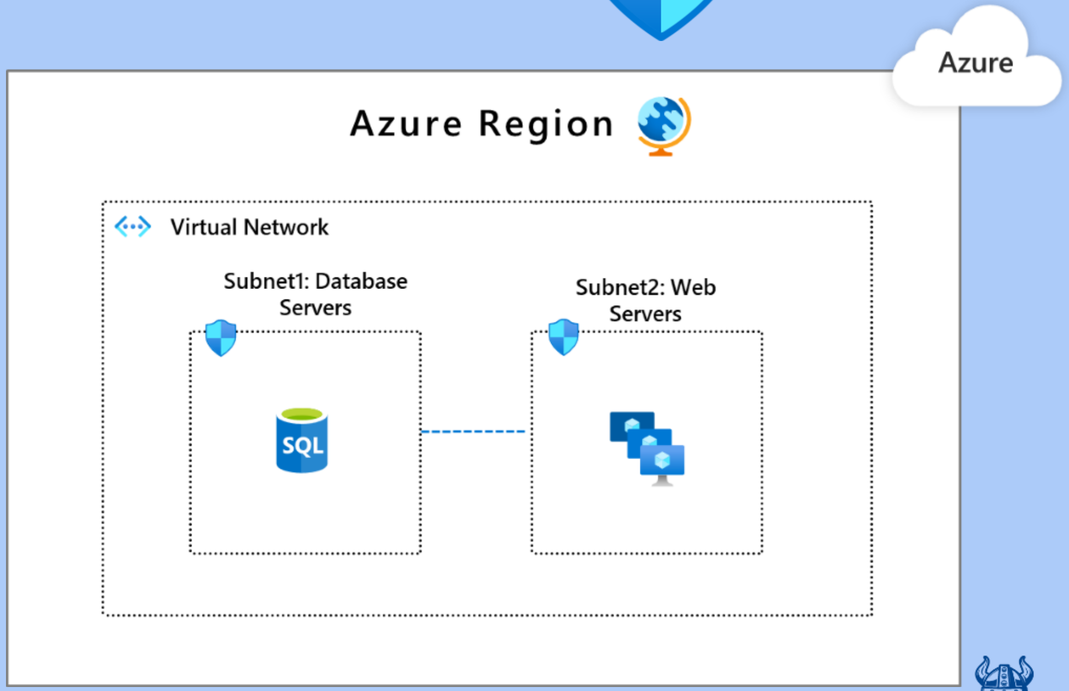
- What is your take on Network restrictions in complex Azure Environments.
  - Azure Firewall or 3rd party Network Virtual Appliances (NVA)
  - Network Security Groups (VNET, Subnet, NIC)
- What is your take on Web Application Firewalls (WAF)
  - Azure Front Door with WAF
  - Web Application Gateway with WAF
  - Web Application Firewall in NVAs
- *What is your take on Standard approach to simplify management and monitoring of Network Rules in complex Azure Environments.*
- *What is your take on Azure VPN Gateway when comparing it with other solutions that focus on Networking Solutions such as (Cisco, SonicWall, FortiGate etc)*

- Azure Landing Zone Deny Policies and using Terraform to deploy Subnets.
  - This has been a problem for a long long time.
  - Workarounds to run exceptions on the policies.
  - Or simply disable the policies.

Questions and concerns

What is your take on Network restrictions in complex Azure Environments.

- Azure Firewall or 3rd party Network Virtual Appliances (NVA)
  - Used mostly in Traditional Hub/Spoke architectures.
  - Used to inspect and control North-South network traffic.
  - Azure Firewall is a layer 7 firewall, capable of filtering traffic based on specific application-layer data.
- Network Security Groups (VNET, Subnet, NIC)
  - Used mostly to protect internal network between VNETs or even in environments that are depending on Zero Trust and are required to have micro segmentation on their network.
  - Used to filter east-west network traffic.



AzUG.is

AZURE VIKING

Questions and concerns

What is your take on Web Application Firewalls (WAF)

- Azure Front Door with WAF
  - Designed for multi-region deployments
  - Is an Edge Security Solution.
  - Rules are applied and filtered before the traffic hits the Data center / VNet.
  - Designed for Web-based attacks and has built in DDoS protection.
  - Way more costly than WAG w/WAF.
  - Offers variety of solutions such as
    - SSL Offloading
    - Load Balancing
    - Routing
- Web Application Gateway with WAF
  - Designed for single region.
  - Rules are applied and filtered when the traffic hits your VNET.
  - Doesn´t have built in DDoS protection, may come as additional cost.
  - Cost way less then Azure Front Door, so that might be a decision factor when it comes to finding the right solution.

Demo

Mitigating Azure deny policies when deploying subnets with Terraform.

Haflidi Fridthjofsson

Principal Cloud Architect at Sopra Steria

Takk fyrir mig.

Follow me on:

@haflidif | in/haflidif | azureviking.com | haflidif