Designing Zero Trust Azure Networks

Aidan Finn, MVP

Cloud Mechanix

Introducing Aidan Finn

- Cloud Mechanix
- 18 year MVP – currently Microsoft Azure
- Based in Kildare, Ireland (+5 hours from EST)
- Working as consultant/sys admin since 1996
- Windows Server, Hyper-V, System Center, desktop managment, and Azure

- http://aidanfinn.com
- http://cloudmechanix.com
- @joe_elway


Cloud Mechanix

Cloud Mechanix – Azure Consulting

- Training
- Cloud strategy
- Reviews
- Security
- Migration
- System design & build
- Cloud Adoption by Mentorship
- Small/medium business
- Microsoft partners

http://cloudmechanix.com

Online Course

Designing Secure Azure Networks

January 26/27

Discount Code For NIC

NicThePacket

25% off

Cloud Mechanix

Why Are We Here?

We have determined that something isn’t right

Cloud Mechanix

Security Is Important

- There have never been so many threats
  - Cybercrime
  - National attacks
- Compliance requirements
  - NISv2 (EU & EEA)
  - GDPR (anyone storing EU resident data)
  - Zero Trust (A growing requirement in Europe)
- Ongoing attacks demonstrate that previous defenses are insufficient

How Many (Most) Defend Networks Today

- Network designs from the 1990s
- Protect the edge
- Run antivirus
- Deploy patches
- And ransomware is still running riot!

Cloud Mechanix

Traditional Network Designs

The Egg Shell

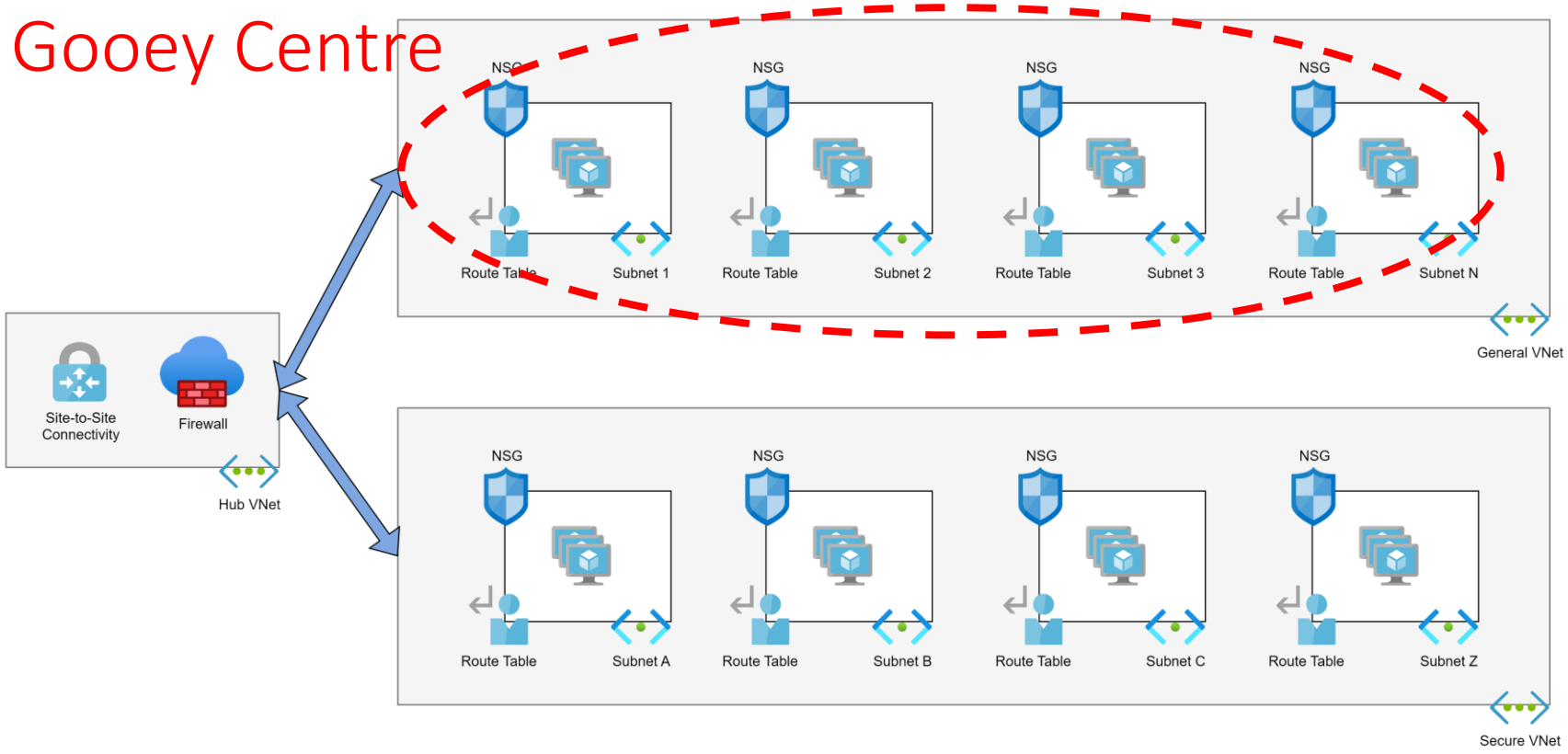
Cloud Mechanix

How Attackers Get In

- Email & web downloads
- Identity
- Supply channel
- DevOps pipelines
- Legitimate firewall ports
- Compromised code
- …

Traditional Network Designs

The Gooey Centre



Cloud Mechanix

Everything In Azure Is A VM

Lesson #1

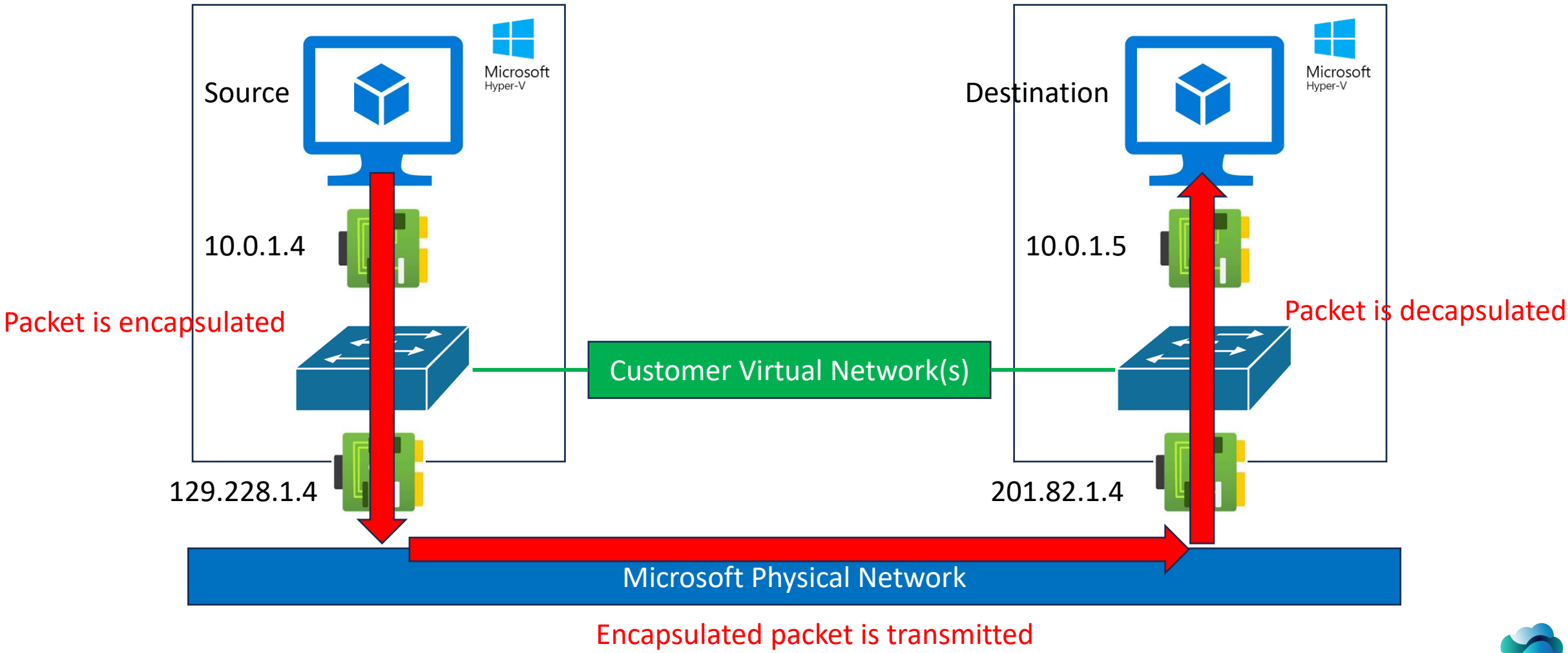
Cloud Mechanix

Packets Always Go Directly From Source To Destination

Lesson #2

Cloud Mechanix

Azure Networks Are Software Defined



Cloud Mechanix

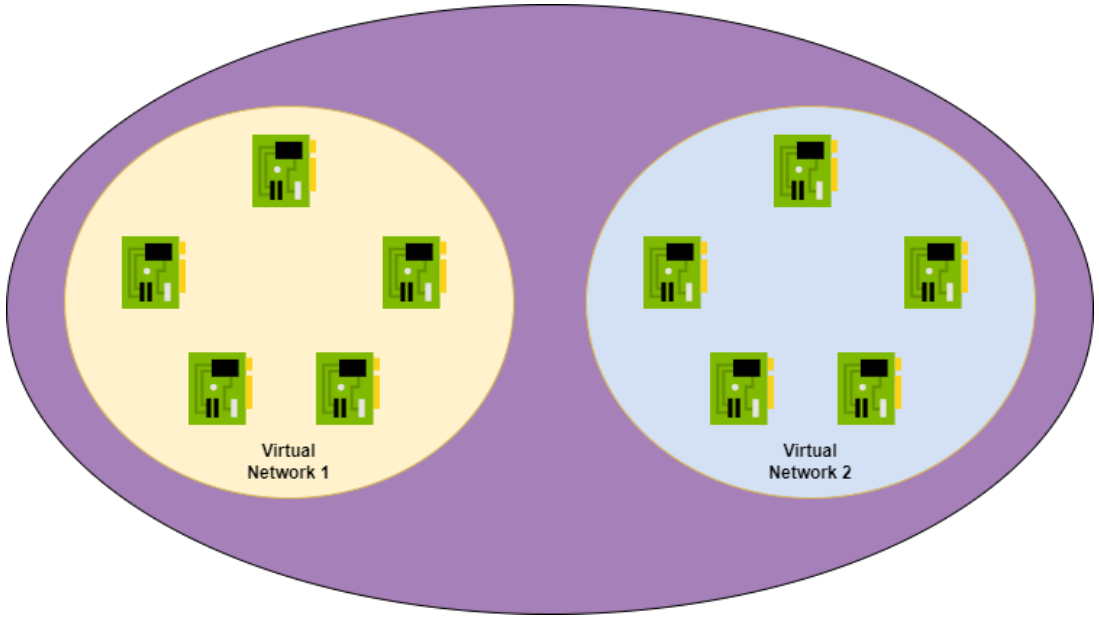
Virtual Networks Do Not Exist

Lesson #3

Cloud Mechanix

Virtual Network Peering

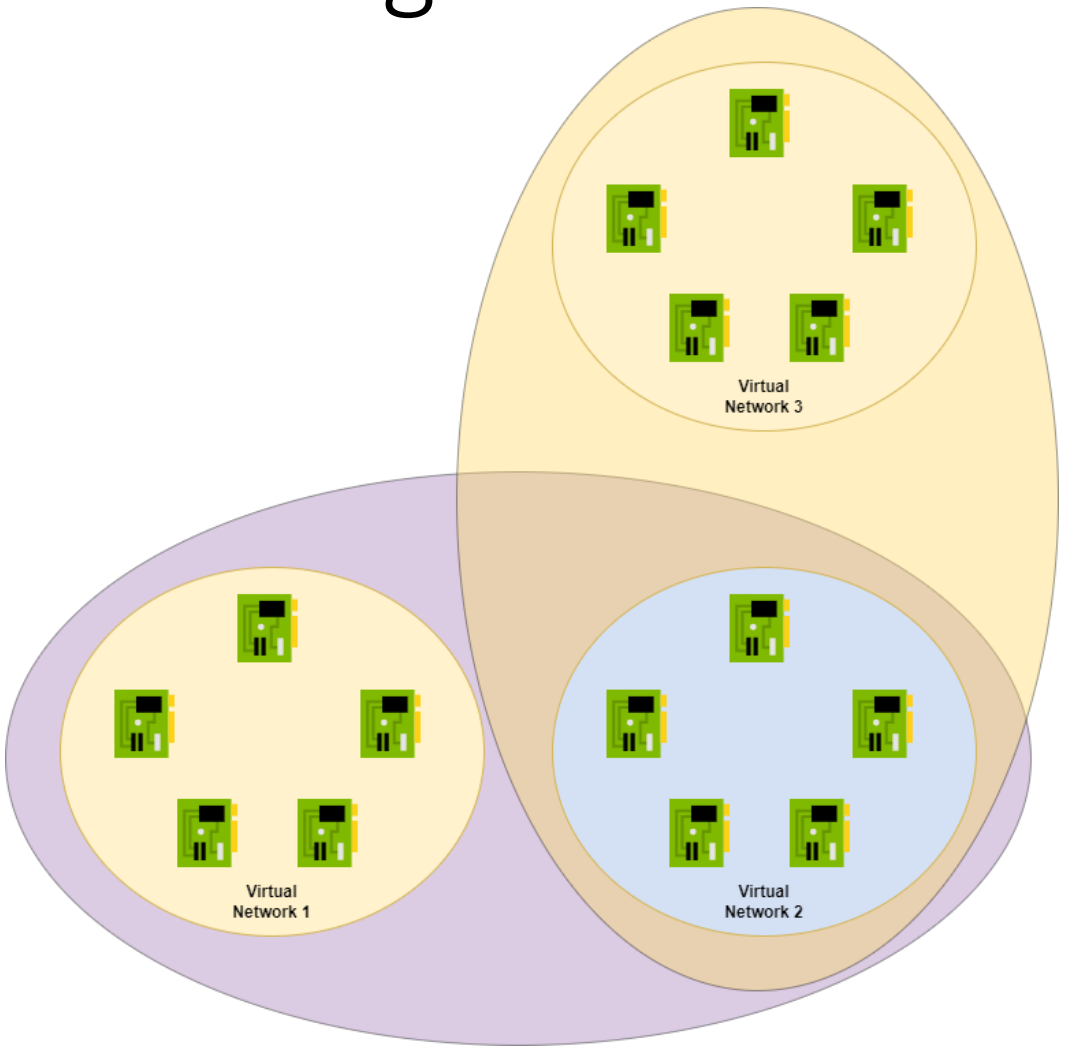
- We can easily connect two virtual networks
  - Same or different Azure regions
- Enables:
  - Connectivity at maximum source/destination NIC speed
  - Resource sharing, example: site-to-site networking
- There is no:
  - Wire
  - Magic pipe
- The fabric expands the mapping of connected NICs



Cloud Mechanix

Multiple Virtual Network Peering

- Scenario
  - VNet1 peered with VNet2
  - VNet2 peered with VNet3
- Works:
  - VNet1 <> VNet2
  - VNet2 <> VNet3
- Does ***NOT*** work:
  - VNet1 <> VNet3
- Solution:
  - Peer VNet1 with VNet3 (mesh)
  - Deploy a router in VNet2



Cloud Mechanix

Micro-Segmentation

- Definition: A method of isolating each NIC from every other NIC
- Virtual Networks do not exist
  - Therefore, subnets do not exist
- Something that doesn’t exist cannot provide security segmentation
  - Packets go directly from source to destination
- What will we use instead?
  - Fewer subnets
  - Network Security Groups

Routing

Azure’s cabling

Why We Care About Routing

- Every packet goes directly from source to destination
- We want traffic to go through a firewall
- We must understand routing
- Most people think “I’ll just add a User-Defined Route”
  - They have no idea that there are two other layers of routing in operation

How Routes Work

- Every source NIC is the router
- Once a packet hits the Azure NIC, the fabric takes over
- Multiple routes to a destination may exist
- Rules are used to pick the best route:
    1. Longest Prefix Match
    2. Routing preference

Longest Prefix Match

- Multiple active routes exist to a destination
- One must be picked
- An “AND” operation is performed to find the most precise route
- Example:
  - Destination: 192.168.1.4
  - Active matching routes:
    - 0.0.0.0/0 > Firewall (0 bits)
    - 192.168.0.0/16 > Virtual Network Gateway (16 bits)
    - 192.168.1.0/24 > NAT Appliance (24 bits)

Route Source Priority

1. User-Defined Routes
   - Created by us by associating a Route Table with a subnet
   - Override default or BGP routes
2. BGP (Border Gateway Protocol)
   - Used in VPN, ExpressRoute, and Virtual WAN
   - Unmanaged BGP routes cause egress traffic to bypass the firewall
3. System/Default
   - Created by Azure when we create/configure Virtual Networks
   - Example: Every subnet routes directly to the destination inside the VNet

Failure To Understand Routing Leads To …

Cloud Mechanix

Network Security Groups

Micro-segmenting subnets

Cloud Mechanix

Network Security Group (NSG)

- A free resource
- Based on Windows Server 2012 Hyper-V Port ACLs
- Can be associated with:
  - NIC: Rules deployed to just that NIC
  - Subnet (Recommended): Rules deployed to all NICs in that subnet
- Rules:
  - Inbound: Commonly used
  - Outbound: Rarely used
- NSG Flow Logs (Deprecated):
  - Trace flows for security monitoring, auditing, troubleshooting
  - VNet Flow Logs are superior

Rules Logic

- Inbound:
  - All packets are controlled AT THE DESTINATION NIC
  - Subnet-associated NSGs are processed before NIC-associated NSGs
- Outbound:
  - All packets are controlled AT THE SOURCE NIC
  - NIC-associated NSGs are processed before subnet-associated NSGs
- Action: Allow or Deny
- Rules in a single NSG are processed in Priority order
  - 1 = highest, 4096 = lowest
  - Built-in rules are 65000, 65001, 65500

Beware of Default NSG Rules

Allow all traffic from all connected networks

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Deny everything else

Cloud Mechanix

Enable Micro-Segmentation

Priority	Name	Port	Protocol	Source	Destination	Action
10	AllowWebToVm01	443	TCP	192.168.0.0/16	10.1.10.4	Allow
20	AllowSqlToSql01	1433	TCP	10.1.10.4	10.1.10.5	Allow
4000	DenyAll	Any	Any	Any	Any	Deny
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Recommendations

- One NSG per subnet
- Override the VirtualNetwork default rule 65000
- Use VNet Flow Logging
- Understand that Azure uses 168.63.129.16 and 169.254.169.254

Microsoft Zero Trust

A modern security architecture for Azure

Cloud Mechanix

Principles of Microsoft Zero Trust

- Verify explicitly
  - Always authenticate and authorize based on all available data points.
- Use least privilege access
  - Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
    - Landing zone/subscription
    - Control special roles with Entra (P2) Privileged Identity Management (PIM) & Conditional Access
- Assume breach
  - Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Aidan’s Zero Trust Concept

- The mission is critical
- Trust nothing
  - Outside
  - Inside
- Isolation:
  - From the outside world
  - Inside to counter penetration
- Depend on nothing outside
- Have a recovery plan

Cloud Mechanix

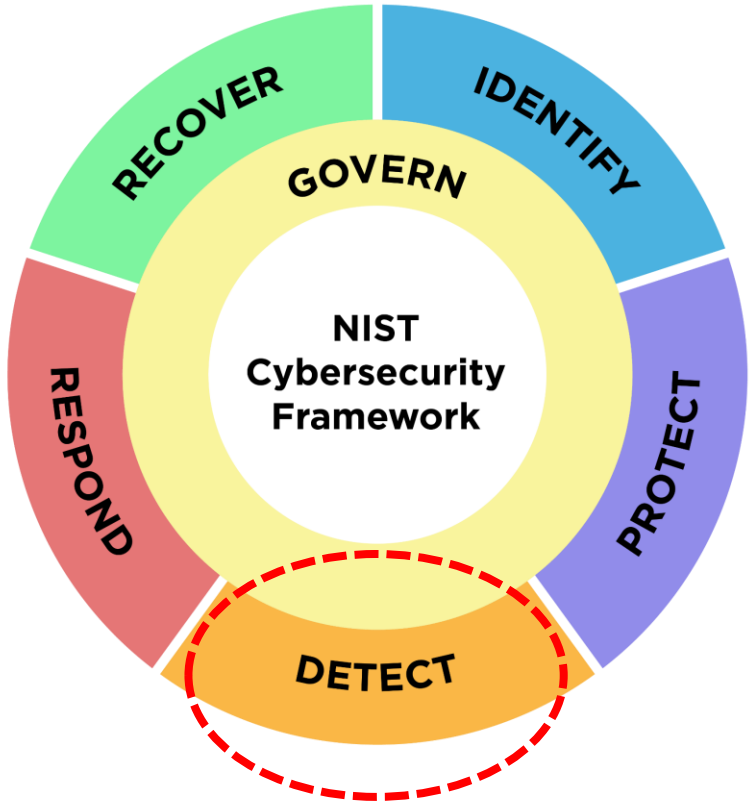
Security Monitoring

Observability and awareness

Cloud Mechanix

The Importance of Monitoring

- The global average to detect a successful penetration is 277 days – 9 months!
- Why:
  - Complex systems
  - Gaps in monitoring
  - Immature SOC/SIEM
- I am amazed how often *any* monitoring is not in-place
- Many national cybersecurity agencies stress monitoring



https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Tripwires

- Defender for Cloud
- VNet Flow Logs
  - NSG Rules
  - Malicious actors
- Resources:
  - Access logs
  - Firewall logs
- WAF rules
- Firewall
  - Rules
  - Threat Intelligence
  - IDPS

Cloud Mechanix

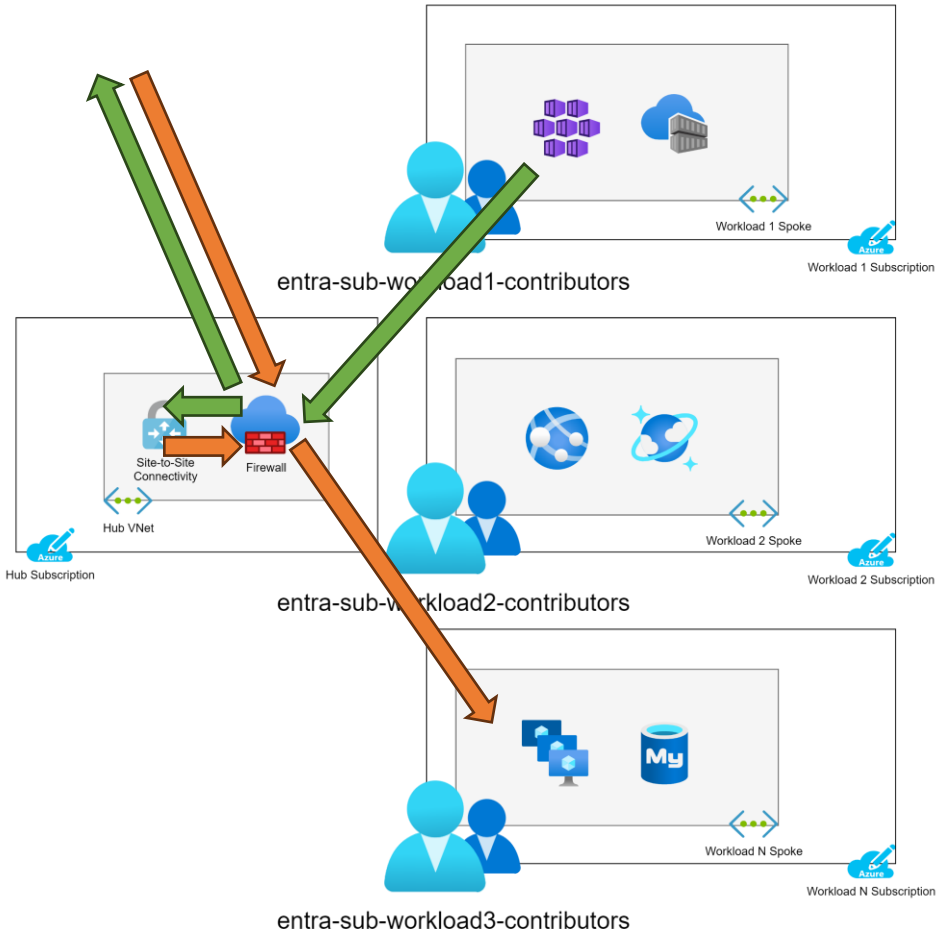
Hub & Spoke

Explaining the security and self-service benefits

Cloud Mechanix

Network Concept

- An old design pattern
- Based on
  - Network core: hub
  - Top-of-rack switches: spokes
- Small virtual networks
- Connected using virtual network peering
  - *Micro*-cost
- Scales *up to* 500 spokes *
- Ideally deployed in a single region
- Think of each hub & spoke as a data center



Cloud Mechanix

Zero Trust Hub

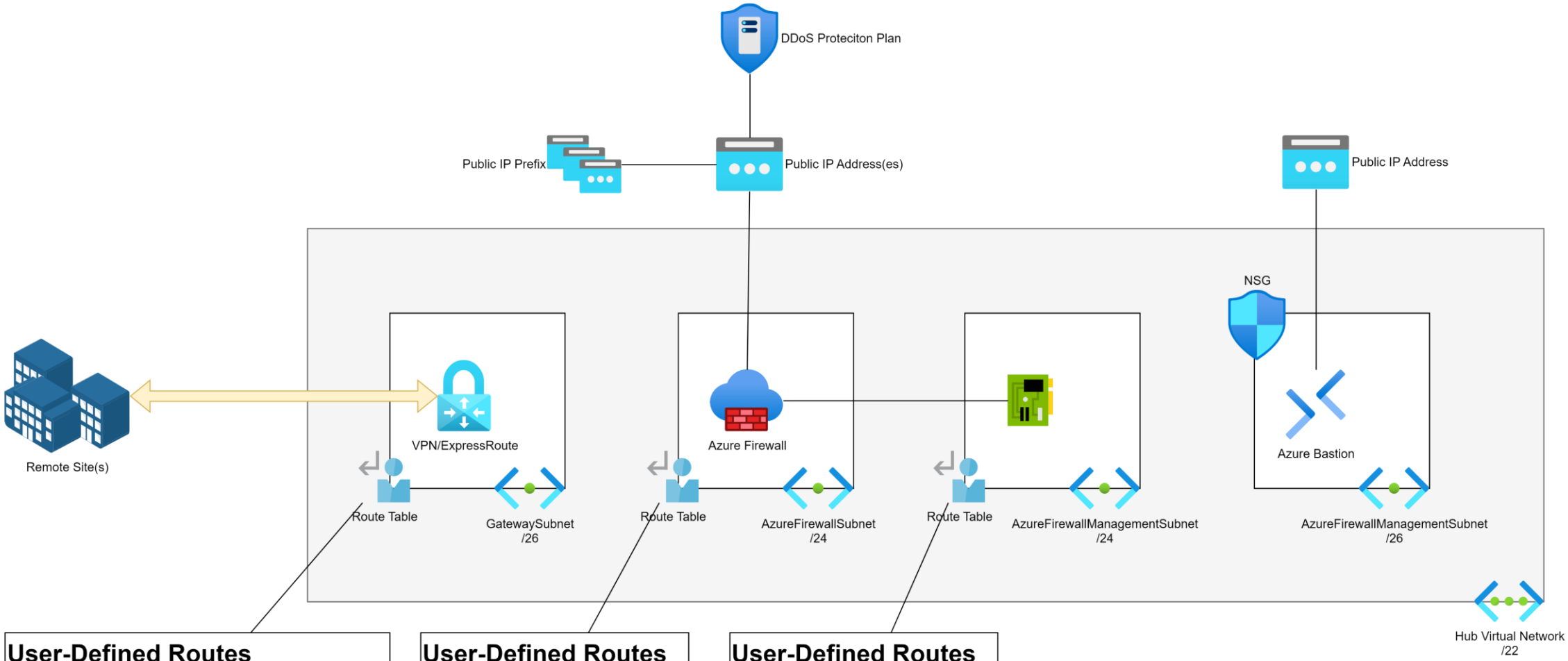
The Network Core

Cloud Mechanix

Where Is Virtual WAN?

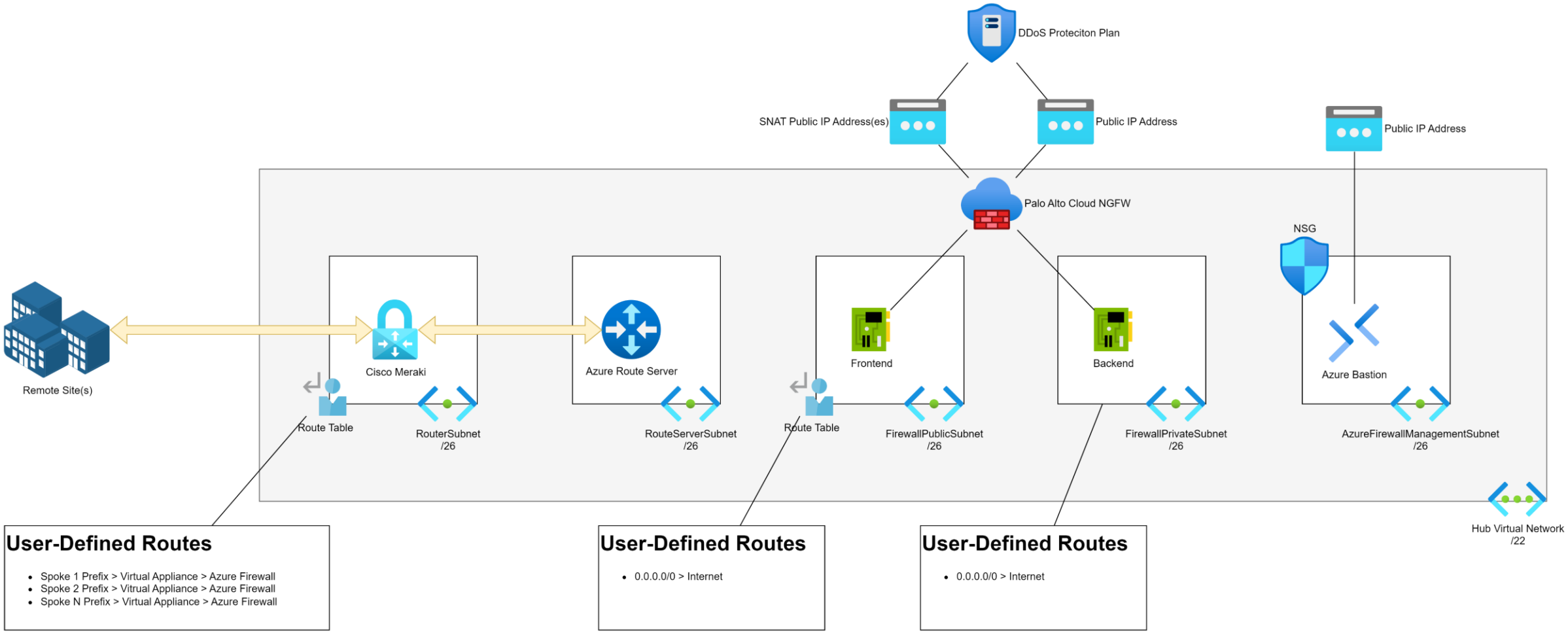
- I don’t understand why Virtual WAN exists
  - We can do everything it does in a virtual network hub
  - vWAN is very feature/architecture restrictive
- I can’t include everything
- The theory I teach here applies to Virtual WAN
- But you also must learn:
  - Routing Intent
  - Route Maps
  - Be prepared to put some **hub** third-party appliances **in spokes**

Zero Trust Hub Design (Azure)



Cloud Mechanix

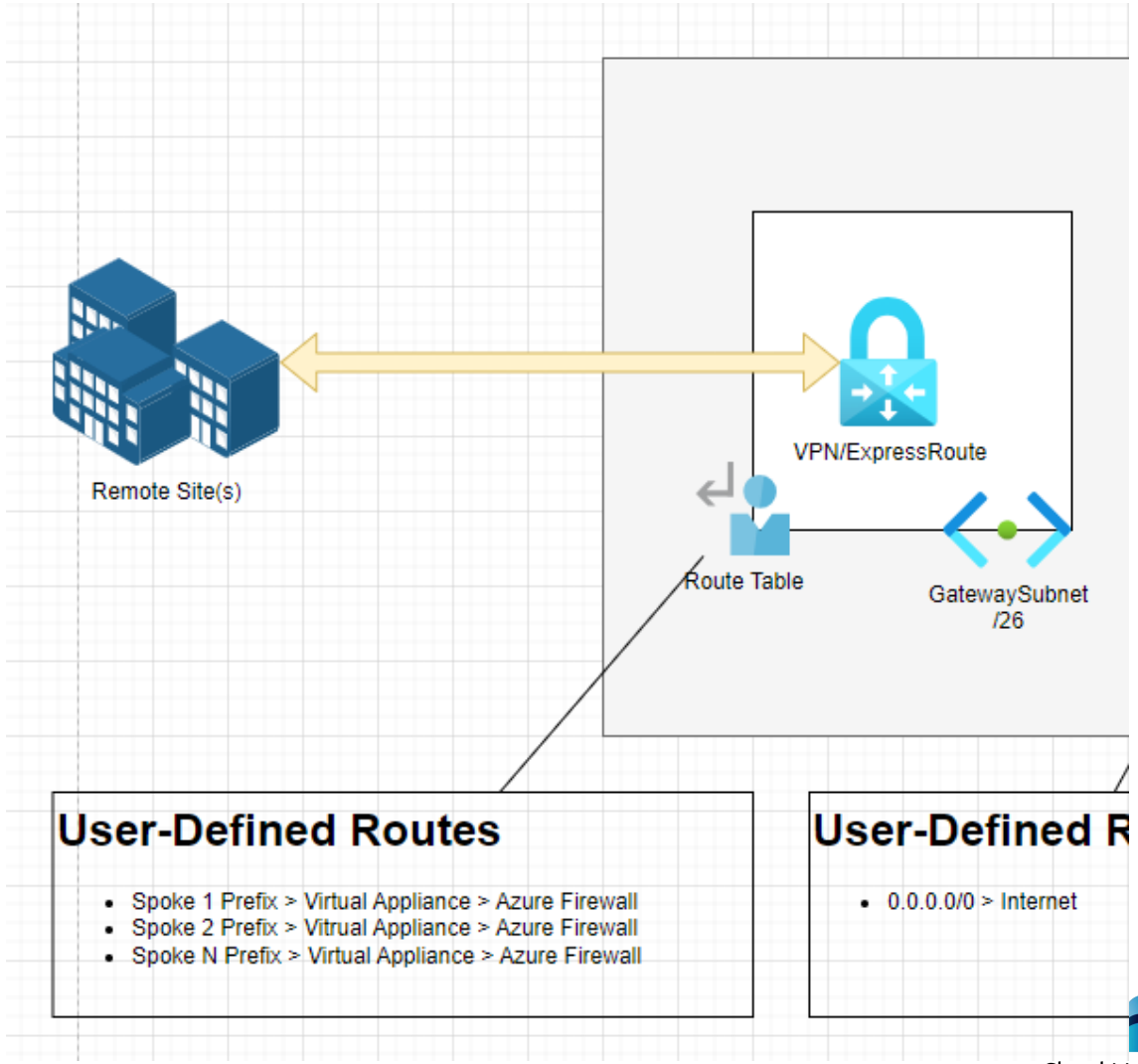
Zero Trust Hub Design (NVA)



Cloud Mechanix

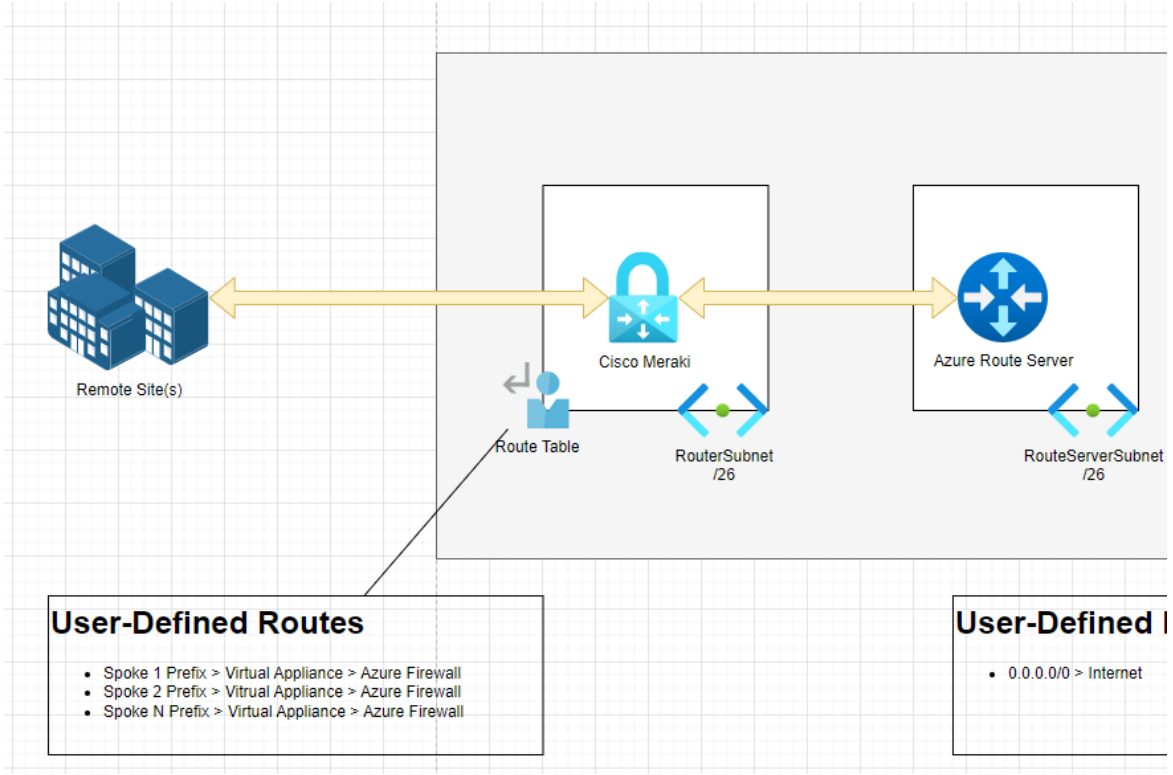
Virtual Network Gateway / Router

- Purpose:
  - Private connections to remote locations
- Security Configurations
  - Zone redundant
  - Route Table
    - Remote sites > Spoke prefixes via firewall



SD-WAN/Third-Party VPN

- Purpose:
  - Enable prefix propagation with router NVA via BGP
    - Hub & Spokes > NVA
    - NVA > Hub
  - Optional (Preview): Enable private range auto-learning in Azure Firewall
- Security Configurations
  - Zone redundant (automatic)



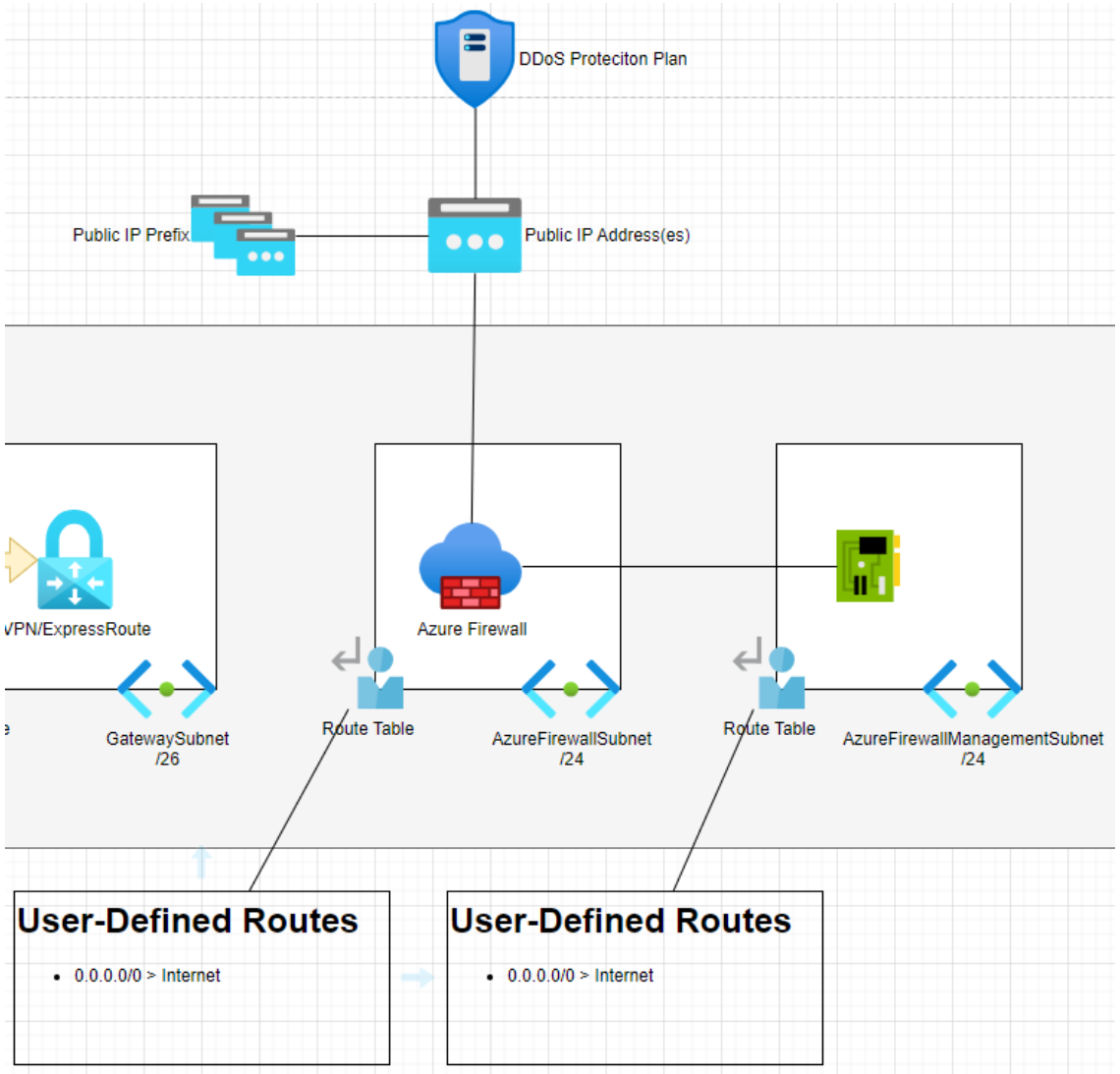
Cloud Mechanix

Private != Encrypted

- Azure Express Route:
  - Privately operated
  - Shared ISP/Microsoft hardware
  - Has an SLA
- Azure Local/Standard/Premium:
  - *Not encrypted*
- Options:
  - Layer VPN over ExpressRoute: Performance impact
  - ExpressRoute Direct: Cost impact
    - MACsec Encryption
    - Dedicated ISP/Microsoft hardware

Firewall

- Purpose:
  - Isolation & routing
- Security Configurations
  - Zone redundant
  - Route Table
    - Default route to Internet
    - Custom routing to other locations
  - DDoS Protection Plan on PIP(s)
  - Management Subnet (AzFw)
    - Force tunnelling for Internet traffic



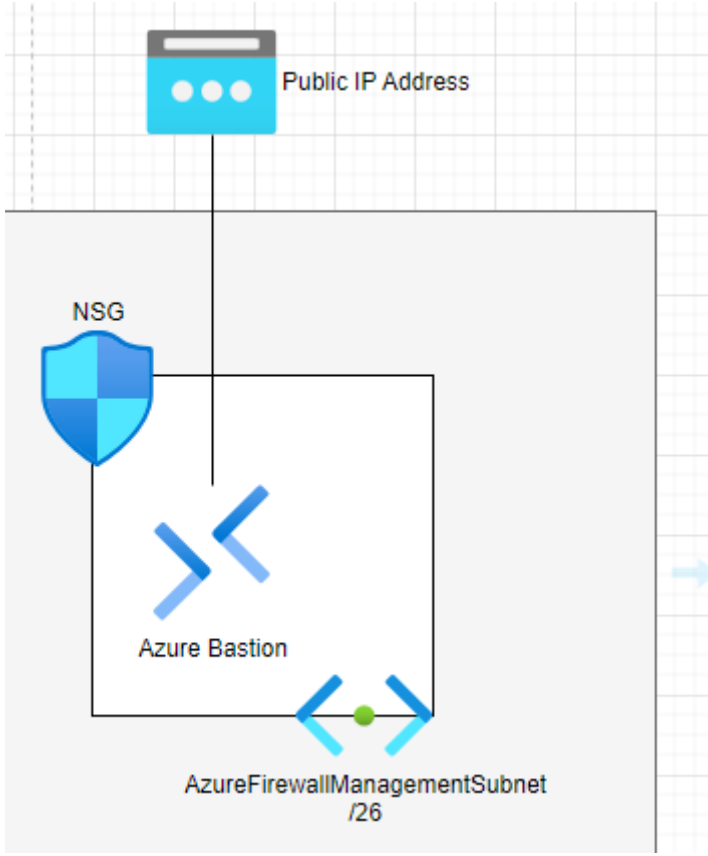
Cloud Mechanix

Firewall As A Router

- The firewall (frontend) subnet will have routes to:
  - Remote locations (BGP from site-to-site networking)
  - Other hub & spoke prefixes
- All spoke subnets (with rare exceptions) will have a route:
  - 0.0.0.0/0 > Hub Firewall
- Spokes do not need to know how to get to remote location prefixes
  - The firewall (frontend) subnet knows how
  - They just need to get to the firewall (backend) subnet
  - Have a rule in the firewall to allow the traffic

Azure Bastion

- Purpose:
  - Enable secure SSH/RDP connections
- Security Configurations
  - Zone redundant
  - NSG
    - Rules forced by Azure
  - RBAC
    - Limited rights for users
      - Reader role on the Azure Bastion resource.
      - Reader role on the hub virtual network



Cloud Mechanix

https://learn.microsoft.com/en-us/azure/bastion/bastion-nsg#apply

Shared Azure Bastion Gotcha

- “Reader role on the hub virtual network”
- Any user of the Bastion will see all the peering links
  - A map of the full hub and spoke
  - Should this be shared with external service providers
- External service provider scenario
  - Dedicated Bastion in the spoke

Shared Resources In The Hub

- Nooooooooooooooooooooooooooooooooooooooo!
- Making routing more complex
- Creates a possible “hop” between spokes
- Putting shared apps in the hub doesn’t reduce latency
  - Peering is not a cable
- Aren’t all enterprise apps “shared” apps?
  - Put everything in the hub?
  - Bye-bye, security!

DNS

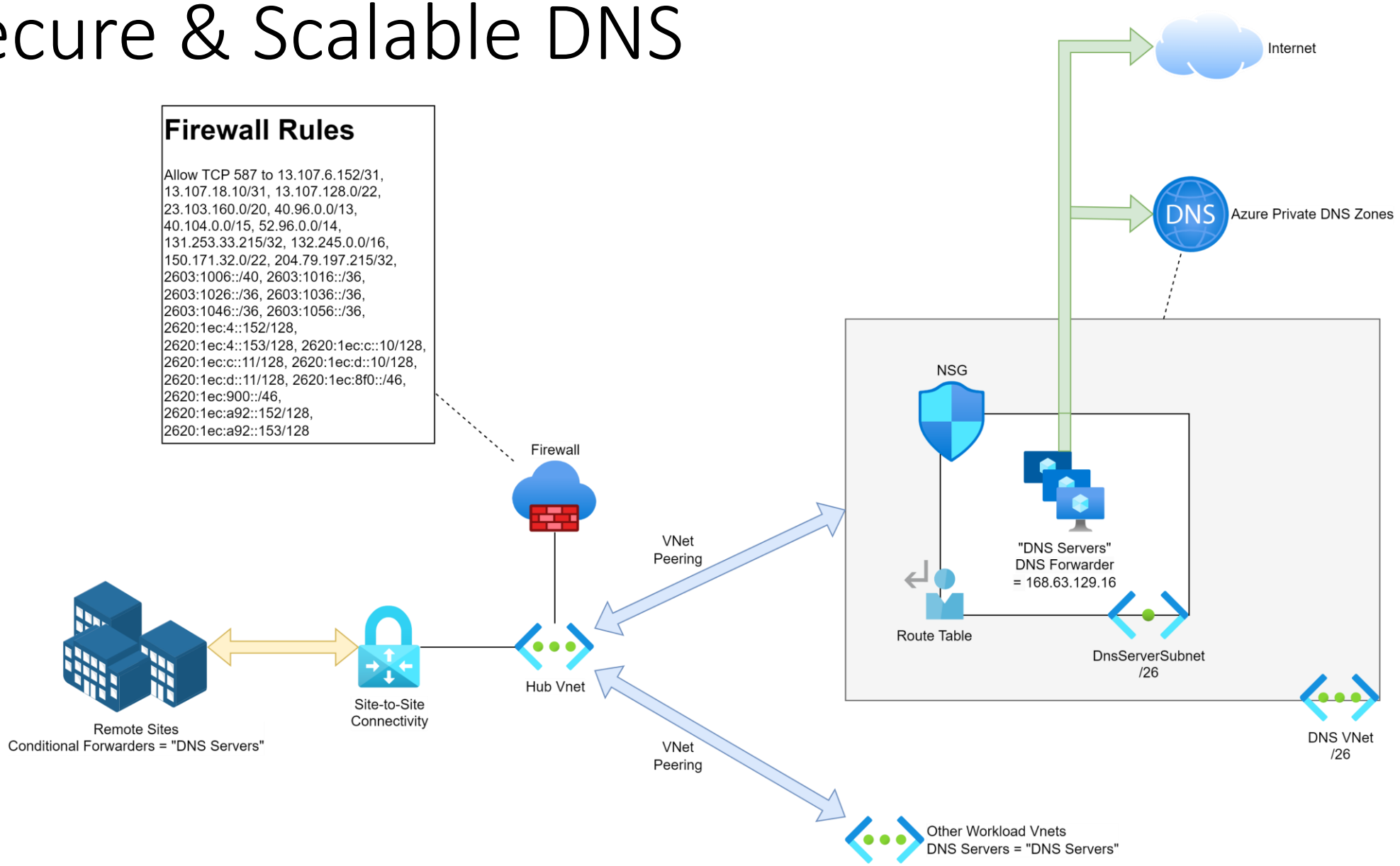
Public and private name resolution

Cloud Mechanix

“It’s Always DNS”

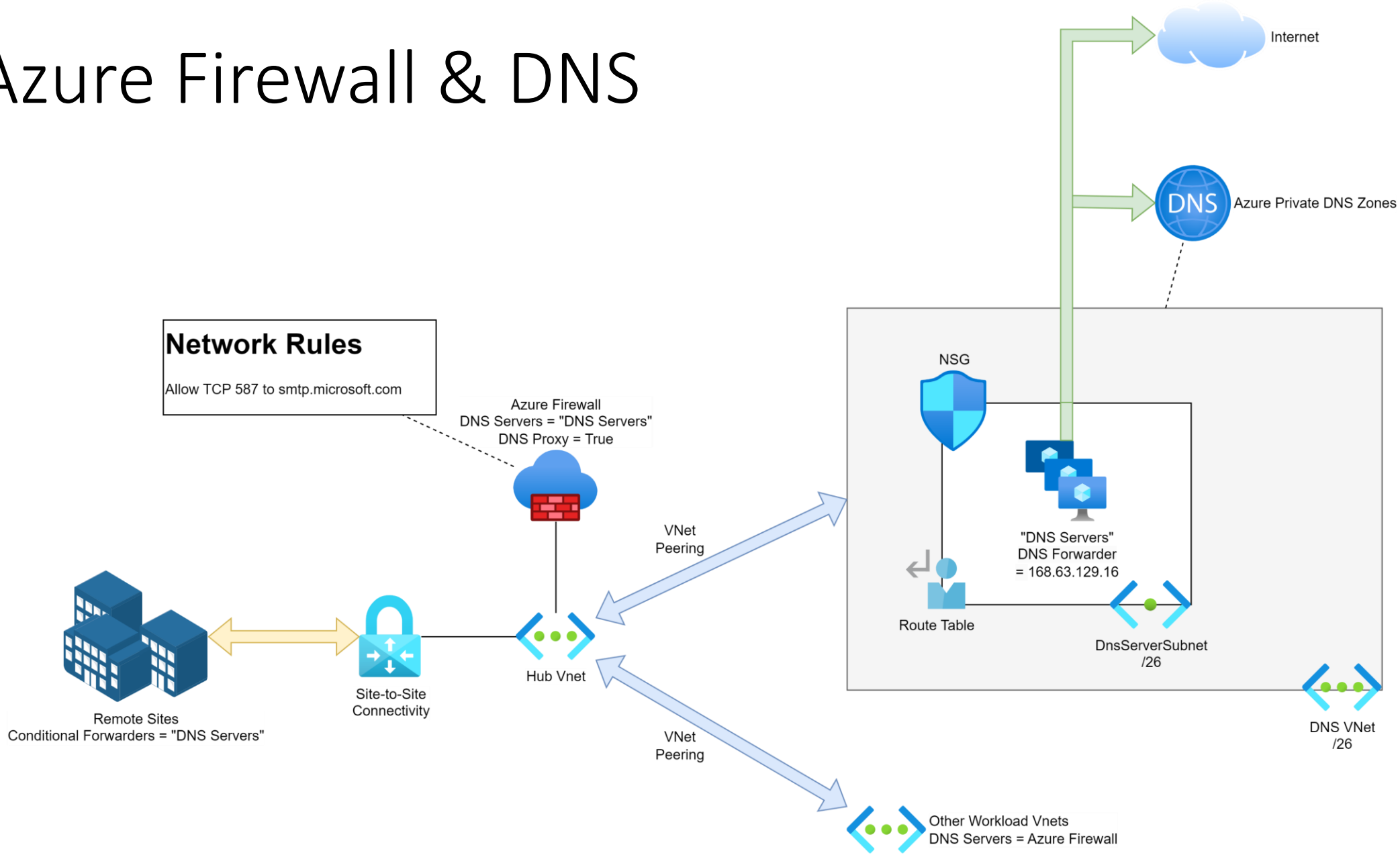
- Resolve
  - External names: Azure and Internet
  - Internal names: Azure and remote sites
- DNS Servers include:
  - Azure (default)
  - Windows DNS, including ADDS Domain Controllers
  - BIND
  - Azure Private DNS Resolver
  - Azure Firewall
- Forwarders set to something external

Secure & Scalable DNS



Cloud Mechanix

Azure Firewall & DNS



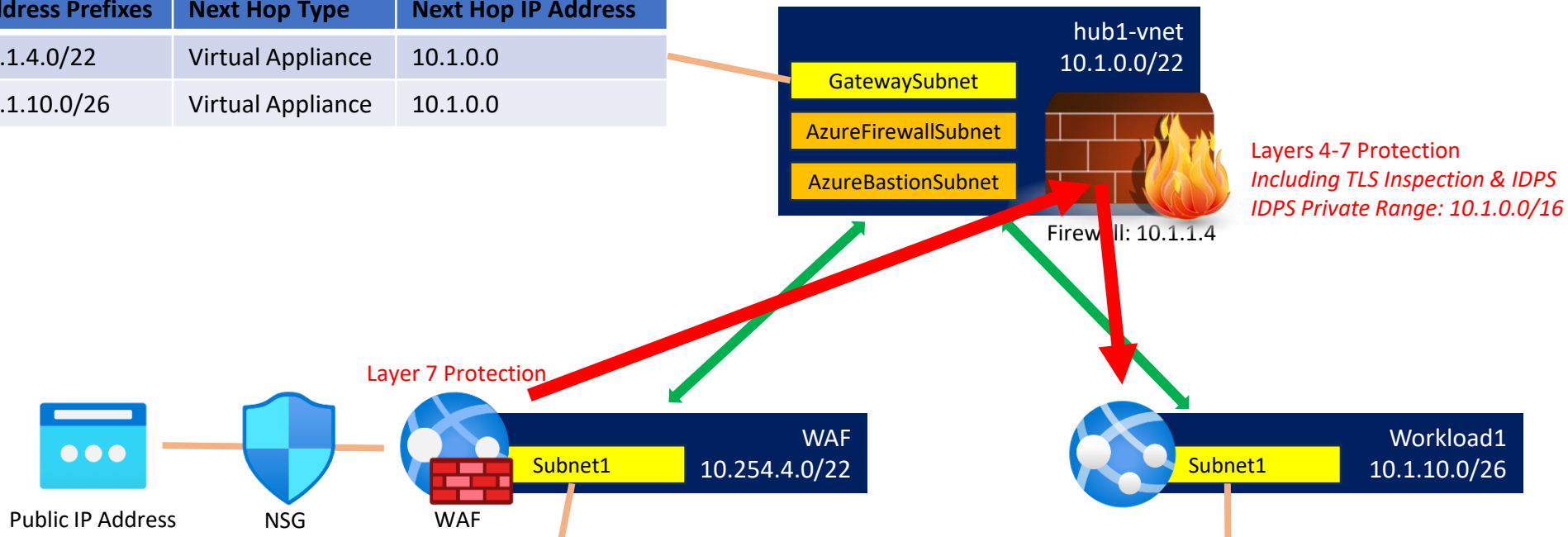
Cloud Mechanix

Application Gateway / Web Application Firewall

Regional application sharing

Shared WAF Design

Address Prefixes	Next Hop Type	Next Hop IP Address
10.1.4.0/22	Virtual Appliance	10.1.0.0
10.1.10.0/26	Virtual Appliance	10.1.0.0



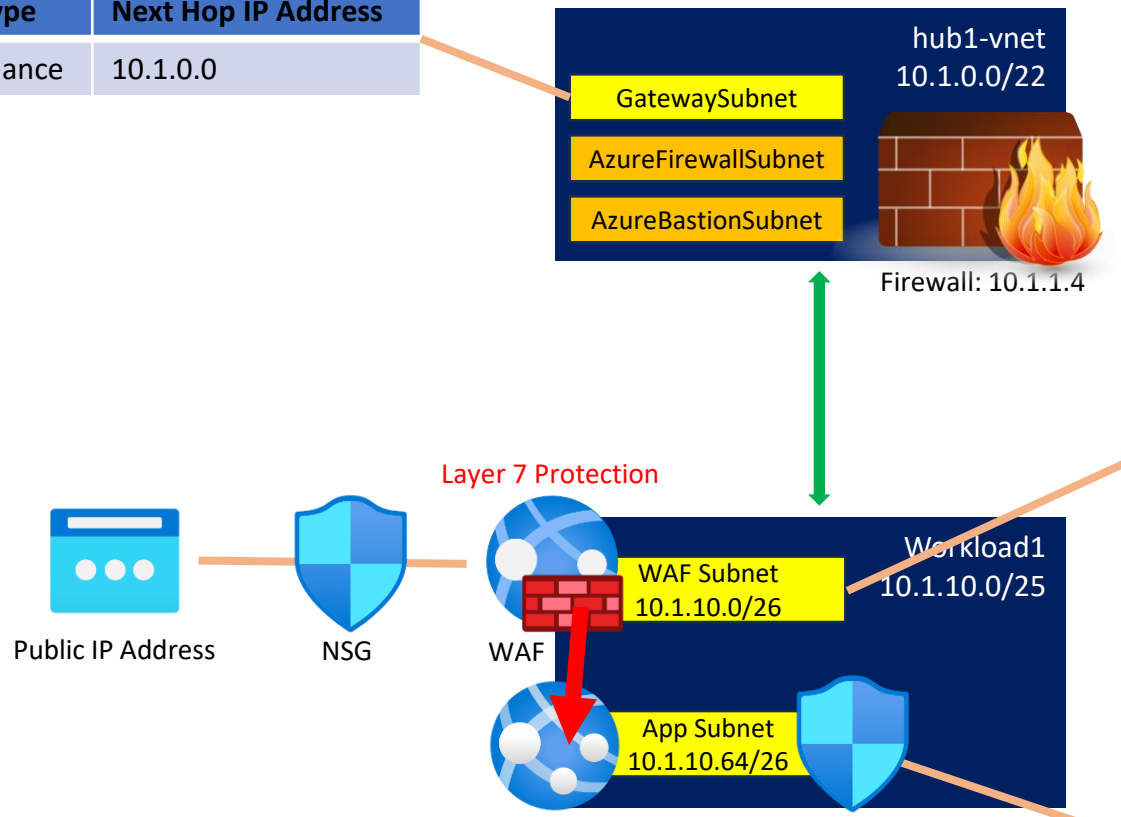
Address Prefixes	Next Hop Type	Next Hop IP Address
0.0.0.0/0	Internet	
10.1.0.0/16	Virtual Appliance	10.1.1.4
BGP Propagation: Disabled		

Address Prefixes	Next Hop Type	Next Hop IP Address
0.0.0.0/0	Virtual Appliance	10.1.1.4
BGP Propagation: Disabled		

Cloud Mechanix

Dedicated WAF Design

Address Prefixes	Next Hop Type	Next Hop IP Address
10.1.10.0/26	Virtual Appliance	10.1.0.0



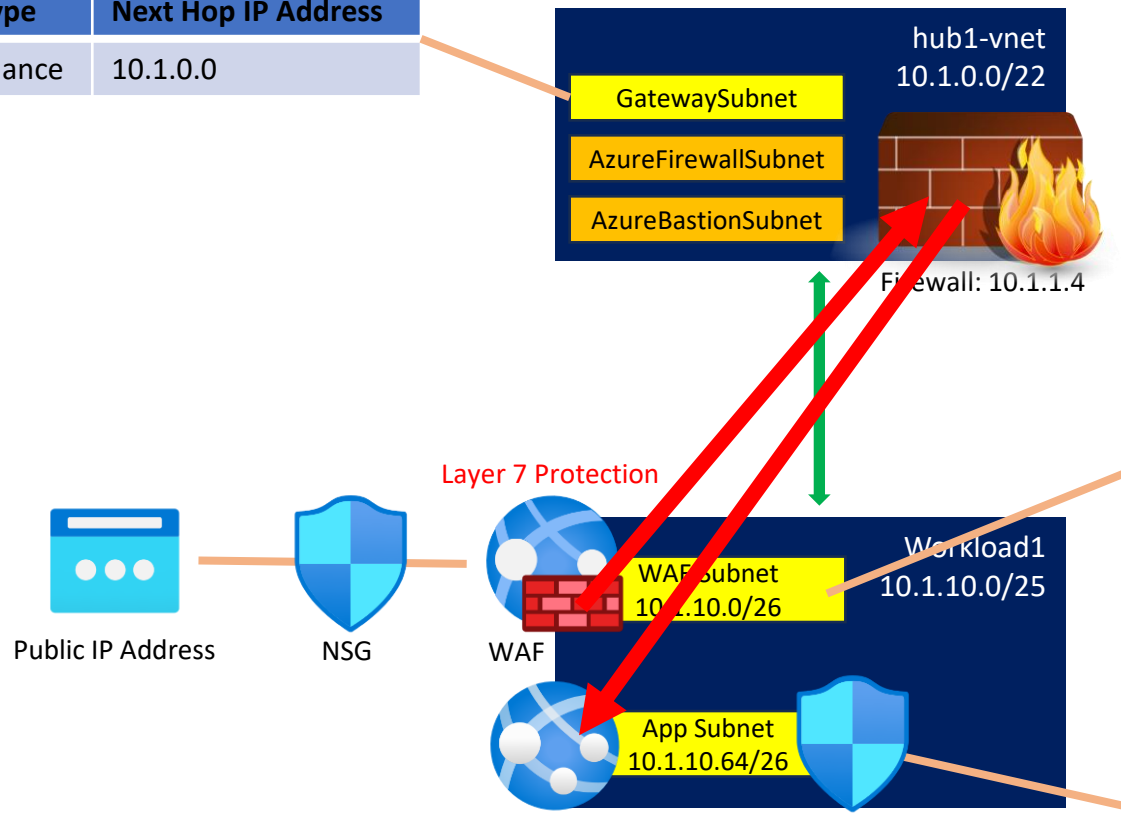
Address Prefixes	Next Hop Type	Next Hop IP Address
0.0.0.0/0	Internet	
10.1.0.0/22	Virtual Appliance	10.1.1.4
BGP Propagation: Disabled		

Address Prefixes	Next Hop Type	Next Hop IP Address
0.0.0.0/0	Virtual Appliance	10.1.1.4
BGP Propagation: Disabled		

Cloud Mechanix

Dedicated WAF Design With Firewall

Address Prefixes	Next Hop Type	Next Hop IP Address
10.1.10.0/26	Virtual Appliance	10.1.0.0



Address Prefixes	Next Hop Type	Next Hop IP Address
0.0.0.0/0	Internet	
10.1.0.0/22	Virtual Appliance	10.1.1.4
10.1.10.64/26	Virtual Appliance	10.1.1.4
BGP Propagation: Disabled		

Address Prefixes	Next Hop Type	Next Hop IP Address
0.0.0.0/0	Virtual Appliance	10.1.1.4
10.1.10.0/16	Virtual Appliance	10.1.1.4
BGP Propagation: Disabled		

Cloud Mechanix

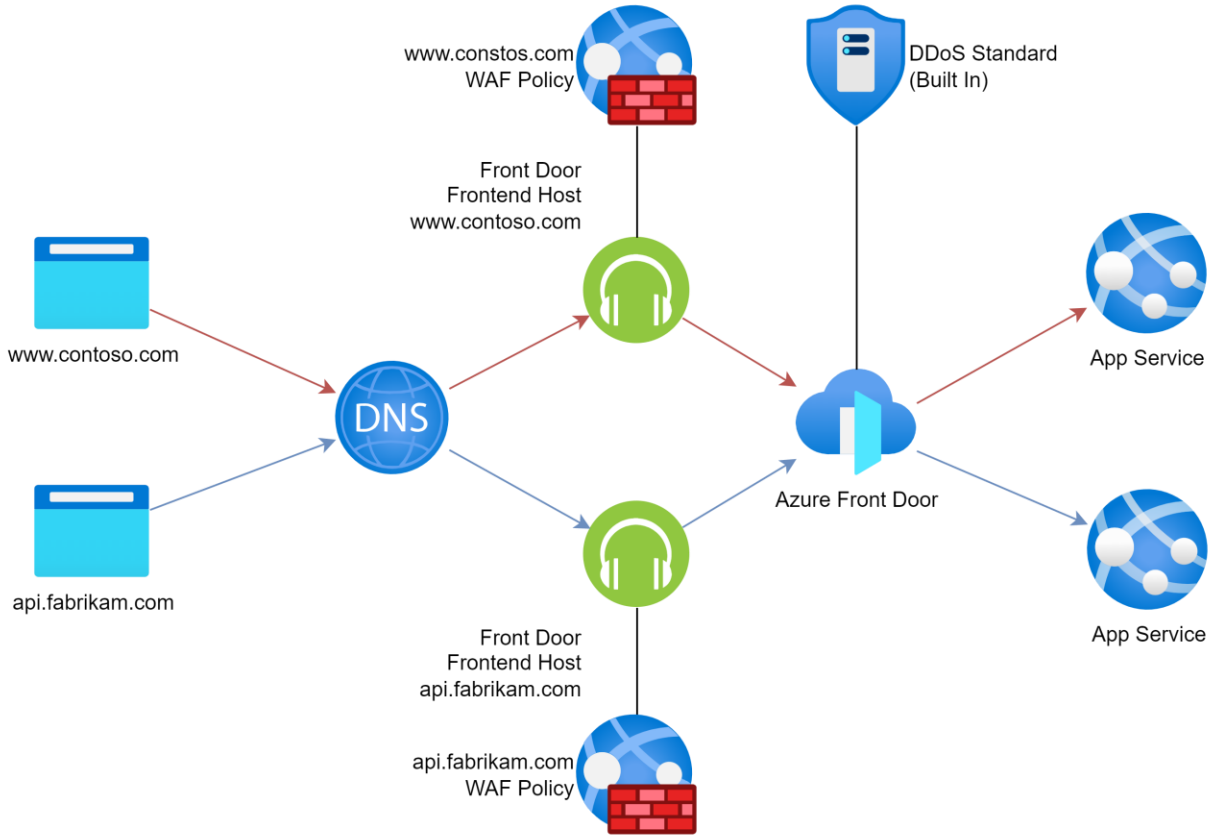
Front Door

Global application sharing

Cloud Mechanix

Front Door Standard

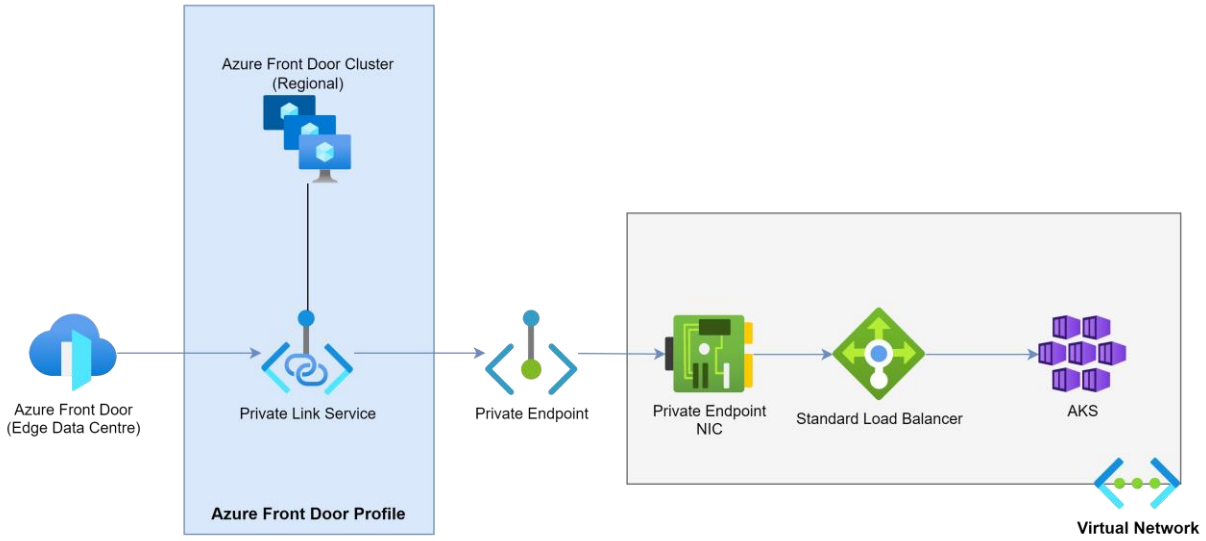
- Origin (backend) hosts have public endpoints
- DDoS Protection built-in
  - Equivalent to Standard SKU
- WAF Policy associated with frontend host
  - AKA custom domain
- Private Preview - WAF association with:
  - Front Door profile (global)
  - Backend Route



Cloud Mechanix

Front Door Premium – Private Link Service

- Enable Front Door to work with supported VNet-connected resources
  - Origin must have a Standard Load Balancer
- Supported resource types:
  - App Service (Web App, Function)
  - Storage Account: Blob, Static Web App
  - Azure Load Balancer: VM, VMSS, AKS, etc
  - API Management
  - Application Gateway
  - Azure Container Apps



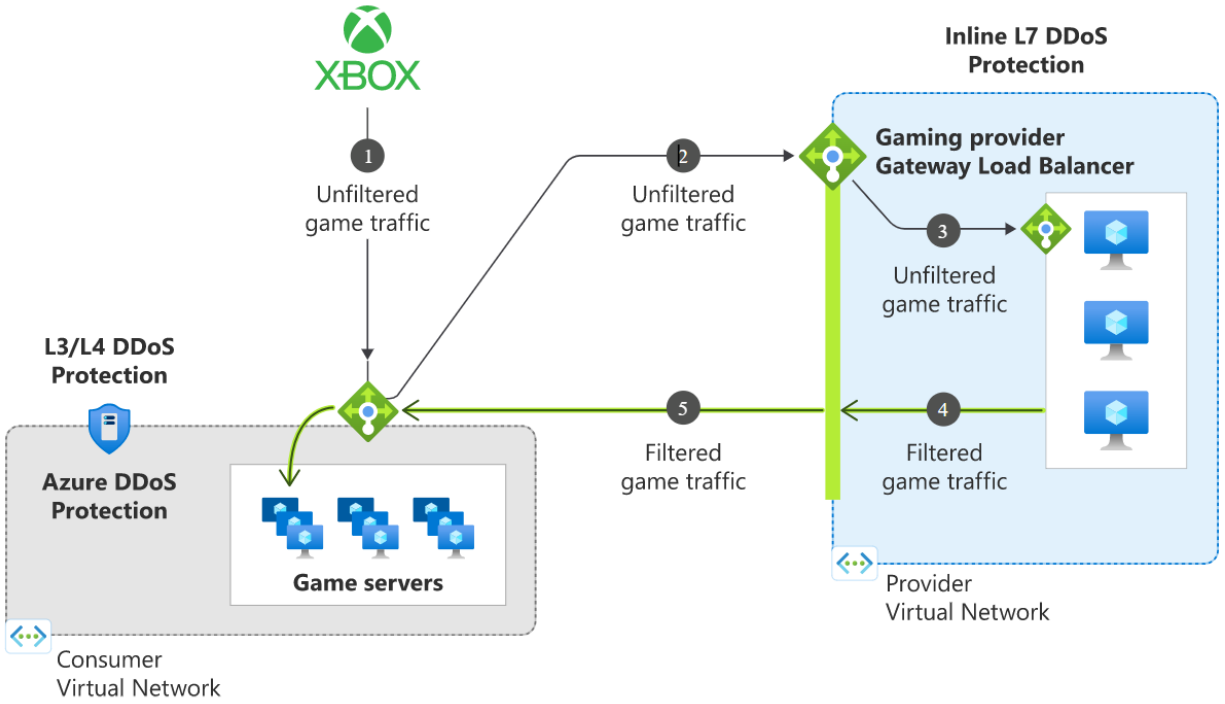
Cloud Mechanix

DDoS Protection

Protecting Azure Public IP Addresses

Cloud Mechanix

Azure Gateway Load Balancer



- Inline scanning
- Azure Marketplace partners:
  - A10 networks
  - Check Point CloudGuard
  - Cisco Secure Firewall
  - Citrix ADC
  - cPacket cCloud Visibility Suite
  - F5 BIG-IP
  - FortiGate-VM
  - Glasnostic
  - Palo Alto Networks VM-Series
  - Trend Micro Cloud One
  - Valtix Gateway

https://learn.microsoft.com/azure/load-balancer/gateway-partners

Cloud Mechanix

Comparing IP and Network Protection

Feature	DDoS IP Protection	DDoS Network Protection
Active traffic monitoring & always on detection	Yes	Yes
L3/L4 Automatic attack mitigation	Yes	Yes
Automatic attack mitigation	Yes	Yes
Application based mitigation policies	Yes	Yes
Metrics & alerts	Yes	Yes
Mitigation reports	Yes	Yes
Mitigation flow logs	Yes	Yes
Mitigation policies tuned to customers application	Yes	Yes
Integration with Firewall Manager	Yes	Yes
Microsoft Sentinel data connector and workbook	Yes	Yes
Protection of resources across subscriptions in a tenant	Yes	Yes
Public IP Standard SKU protection	Yes	Yes
Public IP Basic SKU protection	No	Yes
DDoS rapid response support	Not available	Yes
Cost protection	Not available	Yes
WAF discount	Not available	Yes
Price	Per protected IP	Per 100 protected IP addresses

Zero Trust Spoke

The workload / service / application

Cloud Mechanix

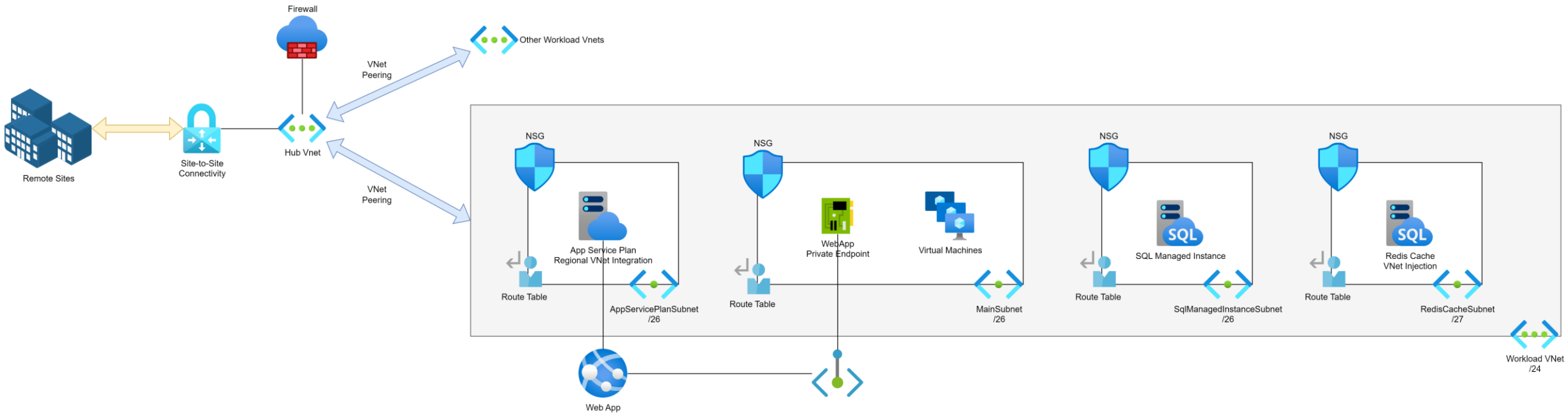
A Spoke

- A virtual network
- Dedicated to a specific workload
- Deployed to an Application Landing Zone
  - Dedicated subscription
  - Dedicated virtual network

Do All Workloads Need A Virtual Network?

- This should be decided by your security policies
  - Is there PCI, HIPAA, GDPR data?
  - Does the compute connect directly/indirectly to sensitive data?
  - If yes, then maybe privacy/security are critical!
- Brochure website
  - App Service & Blob storage can use public endpoints
  - Application landing zone deployed without a virtual network
  - Other governance features (e.g. “Bronze” policy) still apply
- API connecting to database with partner data
  - Probably going to be “gold” and should be protected
  - Disable all public endpoints
  - All resources connect to a virtual network

Example Zero Trust Spoke Design

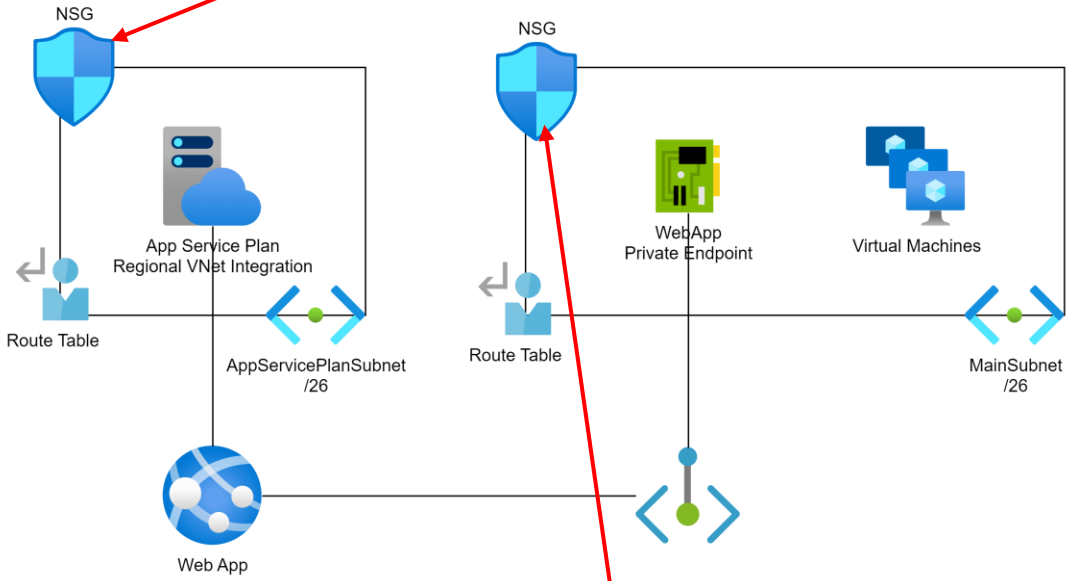


Cloud Mechanix

NSGs

- Purpose:
  - Micro-segmentation of subnets/VNets
- Security Configuration
  - 1 NSG per subnet, where supported
  - Low priority “DenyAll” rule
  - Rules to permit required traffic only
- Tip:
  - Use Inbound rules only
  - Use the hub firewall default “Deny All” to control outbound traffic

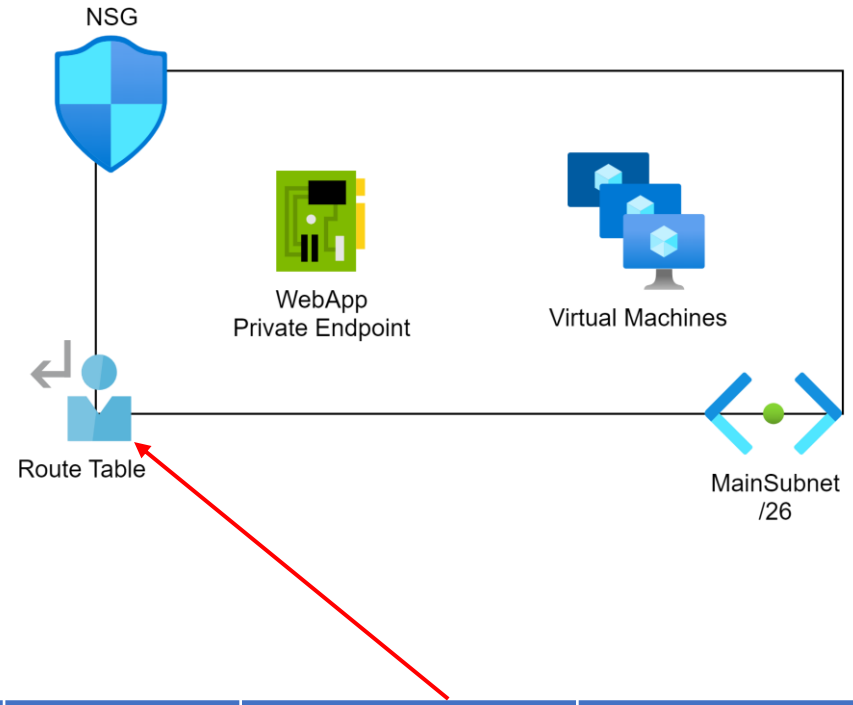
Priority	Name	Ports	Protocols	Source	Destination	Action
4000	DenyAll	Any	Any	Any	Any	Deny



Priority	Name	Ports	Protocols	Source	Destination	Action
100	AllowHttpsToWebapp	443	TCP	192.168.0.0/16	webapp-asg	Allow
200	AllowHttpsToApp	443	TCP	10.1.10.0/26	app-asg	Allow
4000	DenyAll	Any	Any	Any	Any	Deny

Route Tables

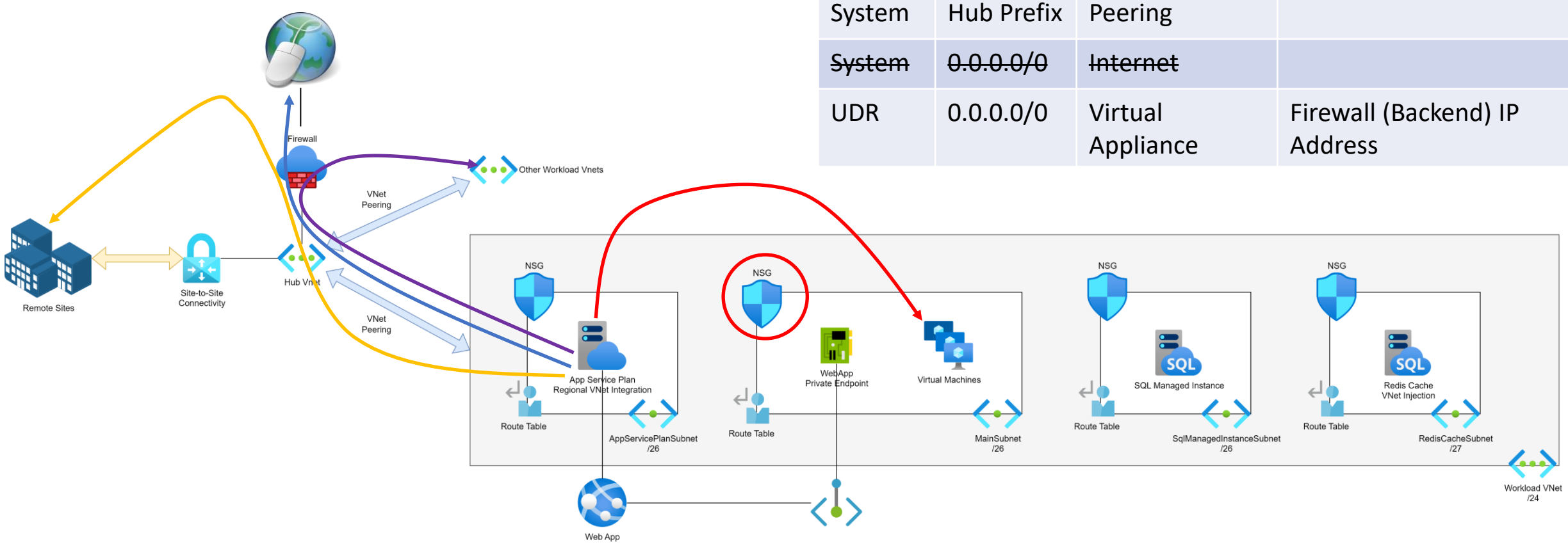
- Purpose:
  - Customise flows of traffic on a per-subnet basis
- Security Configuration
  - Propagate BGP Routes: Disabled
  - UDR: 0.0.0.0/0 > Hub Firewall – All traffic leaving the Vnets will to via the firewall



Type	Prefix	Next Hop Type	Next Hop IP Address
System	Spoke Prefix	Virtual Network	
System	Hub Prefix	Peering	
~~System~~	~~0.0.0.0/0~~	~~Internet~~	
UDR	0.0.0.0/0	Virtual Appliance	Firewall (Backend) IP Address

Zero Trust Spoke Design

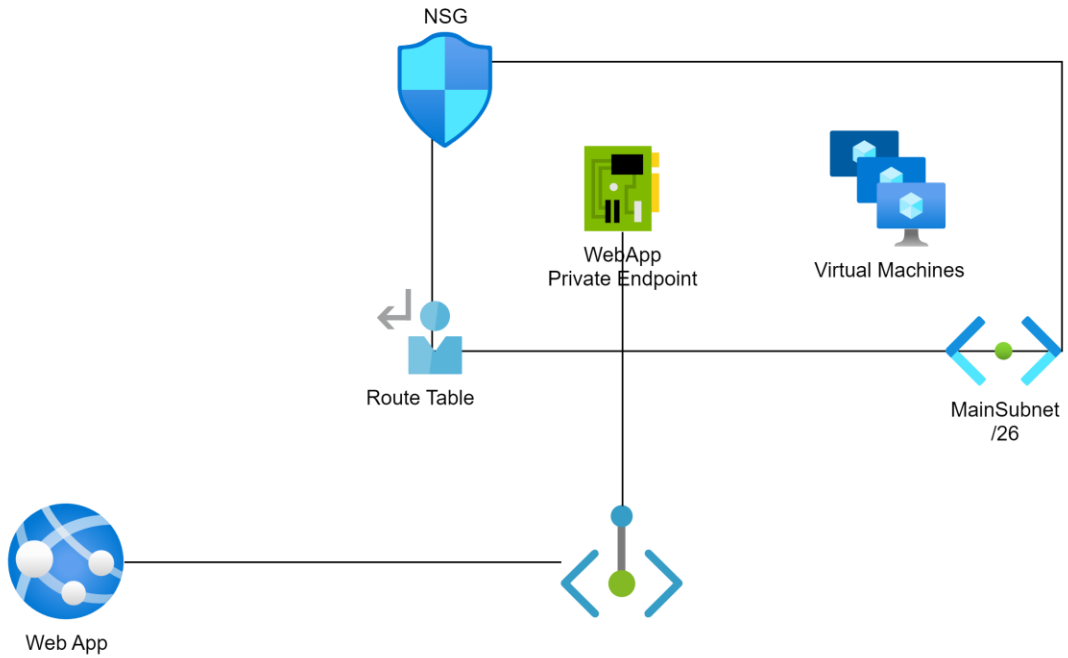
Type	Prefix	Next Hop Type	Next Hop IP Address
System	Spoke Prefix	Virtual Network	
System	Hub Prefix	Peering	
~~System~~	~~0.0.0.0/0~~	~~Internet~~	
UDR	0.0.0.0/0	Virtual Appliance	Firewall (Backend) IP Address



Cloud Mechanix

PaaS Private Endpoint

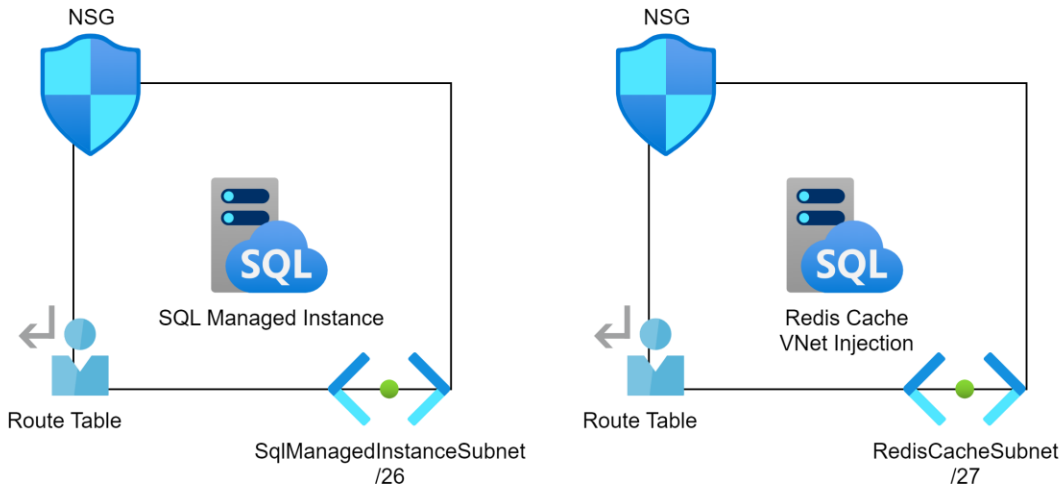
- Purpose:
  - Enable 1-way connections into PaaS resources via VNet
- Security Configuration:
  - NIC deployed to subnet
  - Azure Private DNS Zone to modify name resolution
  - Disable public endpoint access



Cloud Mechanix

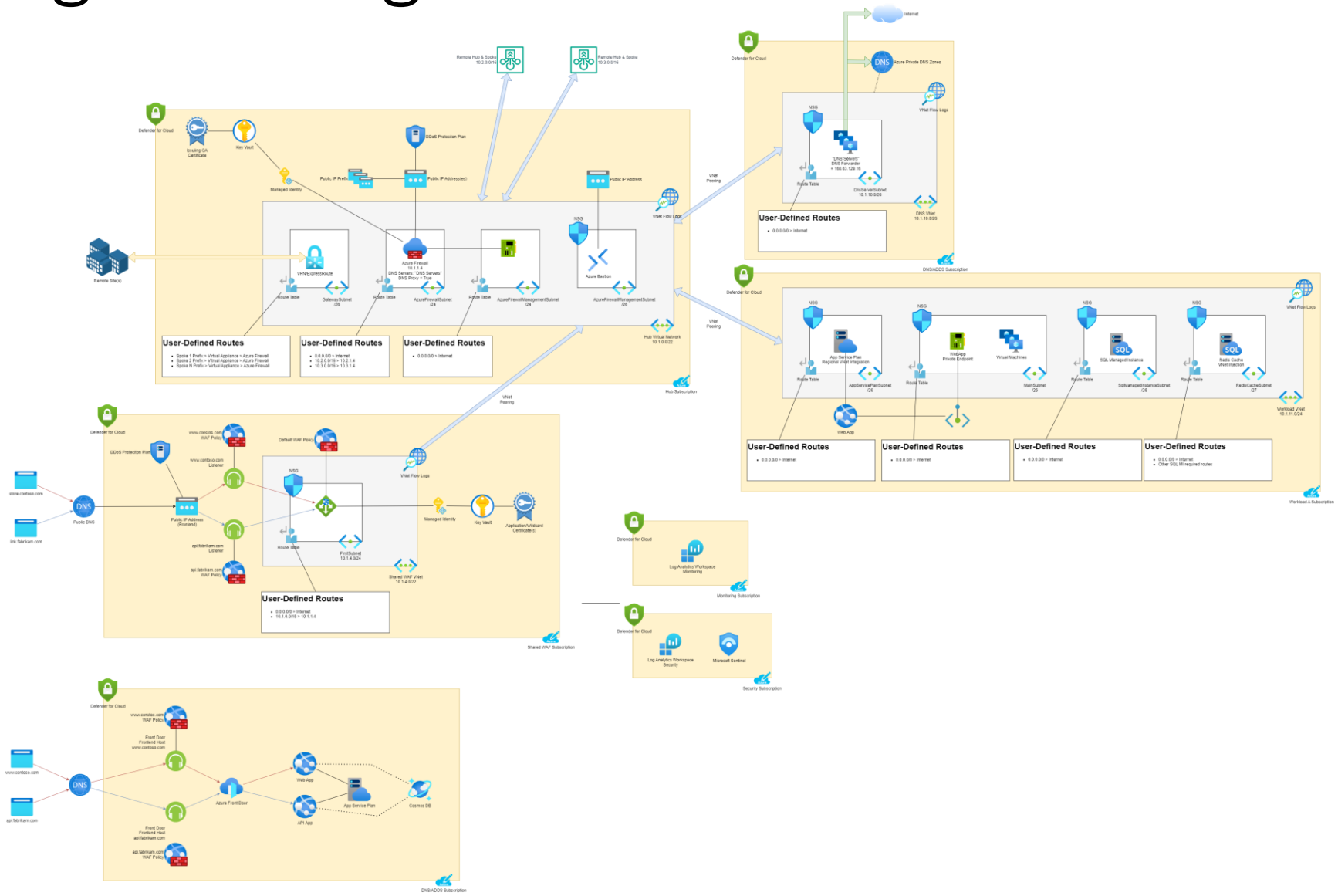
PaaS VNet Injection

- Purpose:
  - Completely dedicated PaaS resource
- Security Configuration
  - Dedicated (delegated) subnet
  - Connection via PaaS frontend private IP address



Cloud Mechanix

Putting It All Together



Cloud Mechanix

Wrapping Up

I doubt I completed that in the allowed time!

Cloud Mechanix

Summary

- Understand the fundamental features
- Adopt Zero Trust over traditional on-premises designs
- A hub is a hub and nothing but a hub
- Each workload gets its own landing zone
- Design a governance solution around the entire security lifecycle
- Security is nothing without monitoring

Thank You!

- Aidan Finn
- http://aidanfinn.com
- https://cloudmechanix.com
- @joe_elway

Online Course

Designing Secure Azure Networks

January 26/27

Discount Code For NIC

NicThePacket

25% off

Cloud Mechanix