Designing for Network Security using Azure Cloud Native Services

Insight Digital Innovation

Agenda

- Introduction
- Background
- Azure Network Services
    - DDoS Protection
    - App Gateway
    - Azure Firewall
    - NSGs and ASGs
- Accessing Services
- Services Endpoints vs Private Endpoints
- Network Visibility
- Demos and Uses Cases
- Questions and Wrap Up

Insight

Introduction

Stephen Tulp

Technology Strategist at Insight

Greater Perth Area · Contact info

500+ connections

Open to | Add section | More

Insight

Edith Cowan University

Insight

Introduction

Stephen Tulp

Technology Strategist at Insight

Greater Perth Area · Contact info

500+ connections

Open to | Add section | More

Insight

Edith Cowan University

Can configure multiple ExpressRoute private peering connections using BGP Communities

Can't plug in a blue Cat 5 cable or console into a switch

Insight

Traditional Systems Security vs Cloud Security

Securing a house

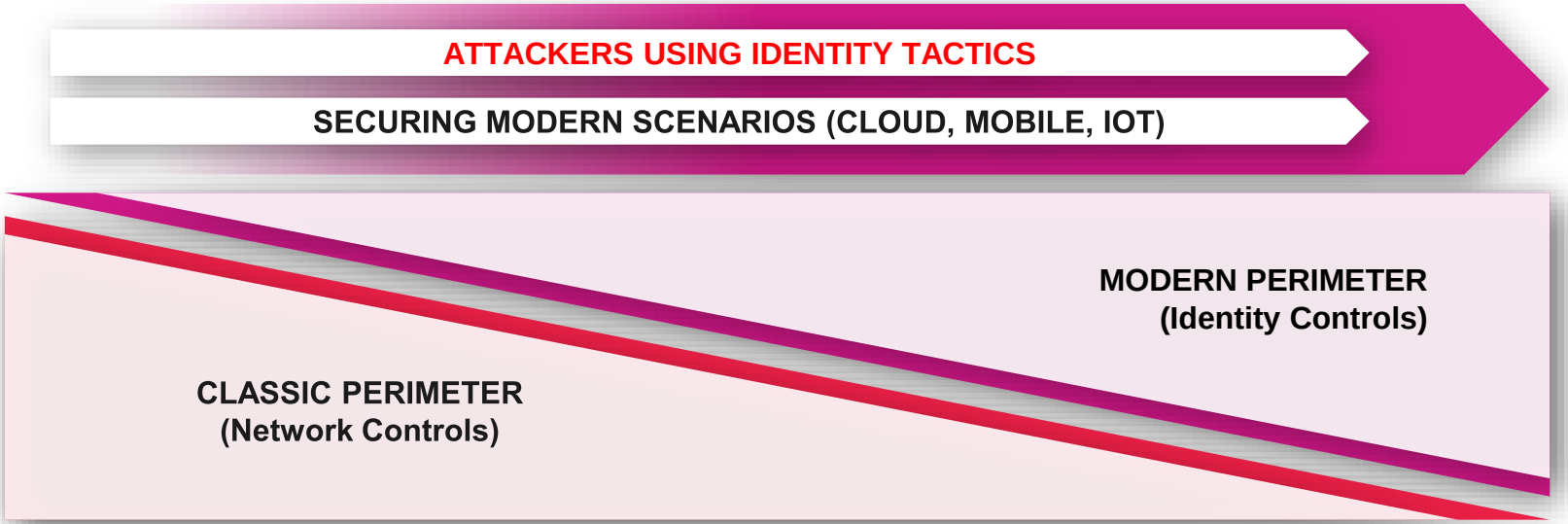
Biggest user concerns
Securing perimeter
Checking for intruders
Securing assets

Securing a motel

Biggest user concern
Securing room against (the bad guy in next room | hotel owner)

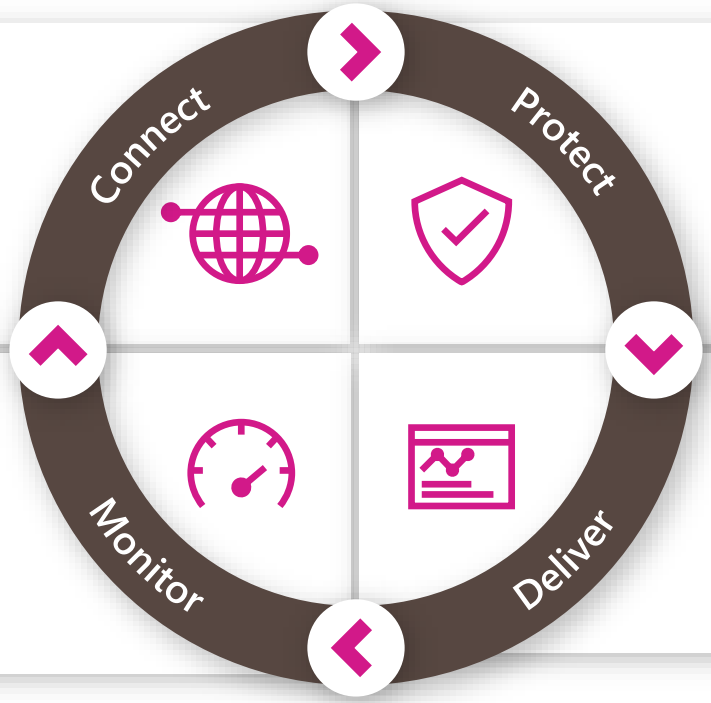
Insight

Running Dual Perimeters



Insight

Azure Network Services



- Virtual Network
- Virtual WAN
- ExpressRoute
- VPN
- DNS

- DDoS Protection
- Firewall
- Network Security Groups
- Web Application Firewall
- Virtual Network Endpoints

- Network Watcher
- ExpressRoute Monitor
- Azure Monitor
- Virtual Network TAP

- CDN
- Front Door
- Traffic Manager
- Application Gateway
- Load Balancer

Insight

Azure Network Protection Services

DDoS Protection

DDOS protection tuned to your application traffic patterns

Web Application Firewall

Centralized inbound web application protection from common exploits and vulnerabilities

Azure Firewall

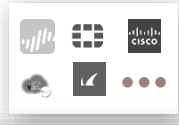
Centralized outbound and inbound (non-HTTP/S) network and application (L3-L7) filtering

Network Security Groups

Distributed inbound and outbound network (L3-L4) traffic filtering on VM, Container or subnet

Private/Service Endpoints

Restrict access to Azure service resources (PaaS) to only your Virtual Network



Security Appliances

Leverage your existing skillsets, processes, and licenses by adding technologies from the Azure Marketplace

Application protection

Segmentation

And more…

Insight

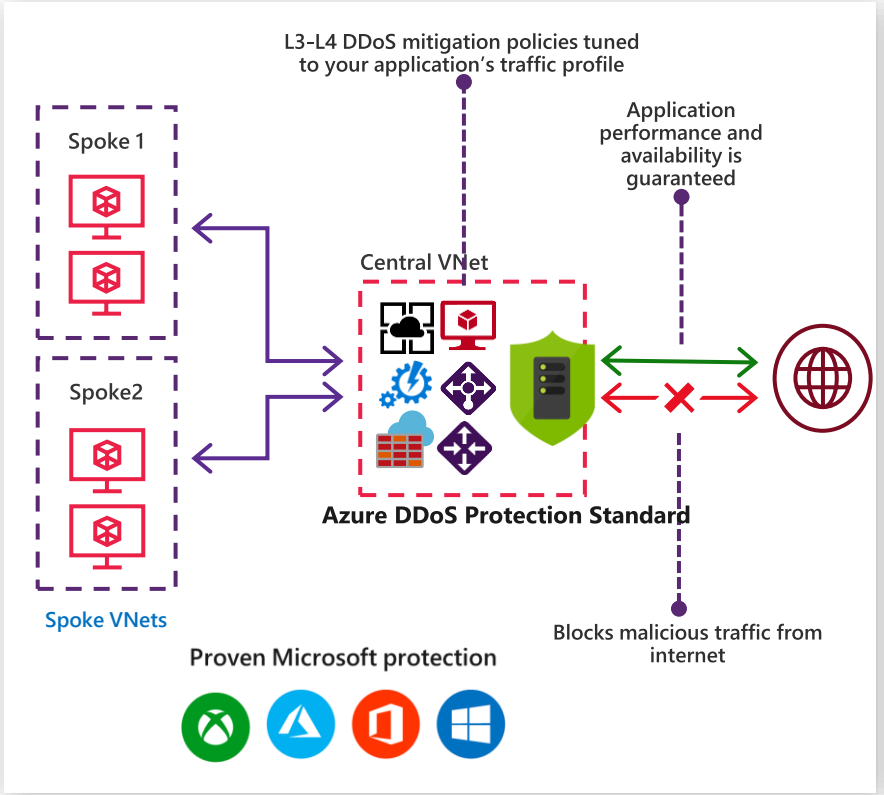
Azure DDoS Protection

Standard

- Tuned to your apps
- Logging, alerting and telemetry via Azure Monitor
- L7 Protection via Web App Firewall (WAF)
- Availability Guarantee and Rapid Response Support

Basic

- Always on L3/L4 attack protection
- Deployed today in all Azure regions
- No additional charge and available to all Azure Customers



Insight

App Gateway with Web Application Firewall

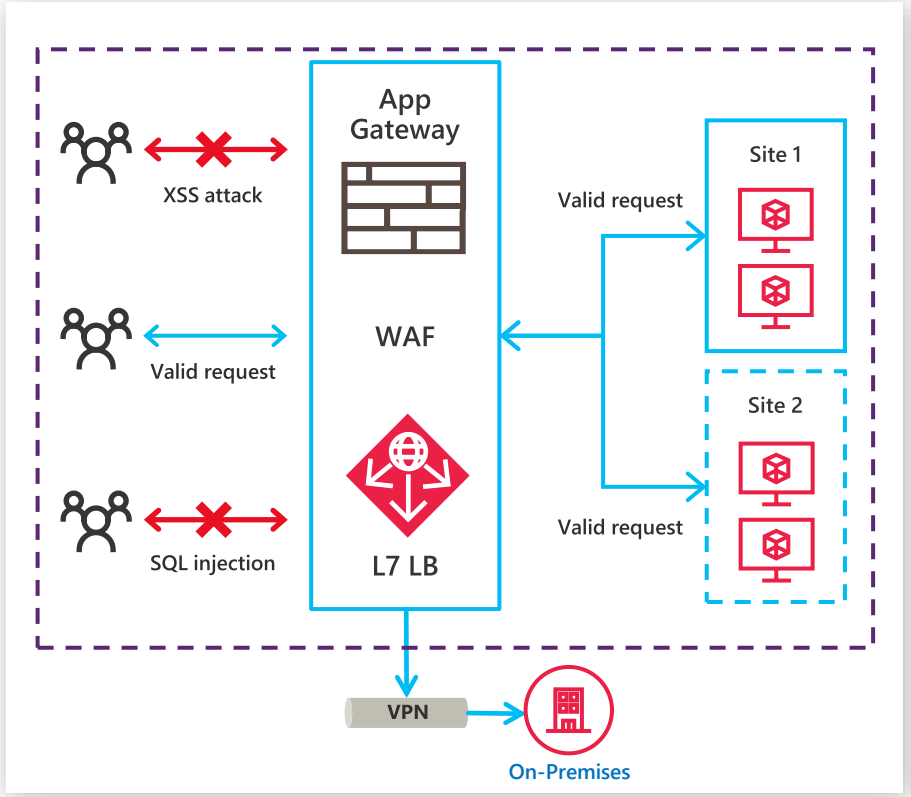
Cloud native Web Application Protection

Azure App Gateway

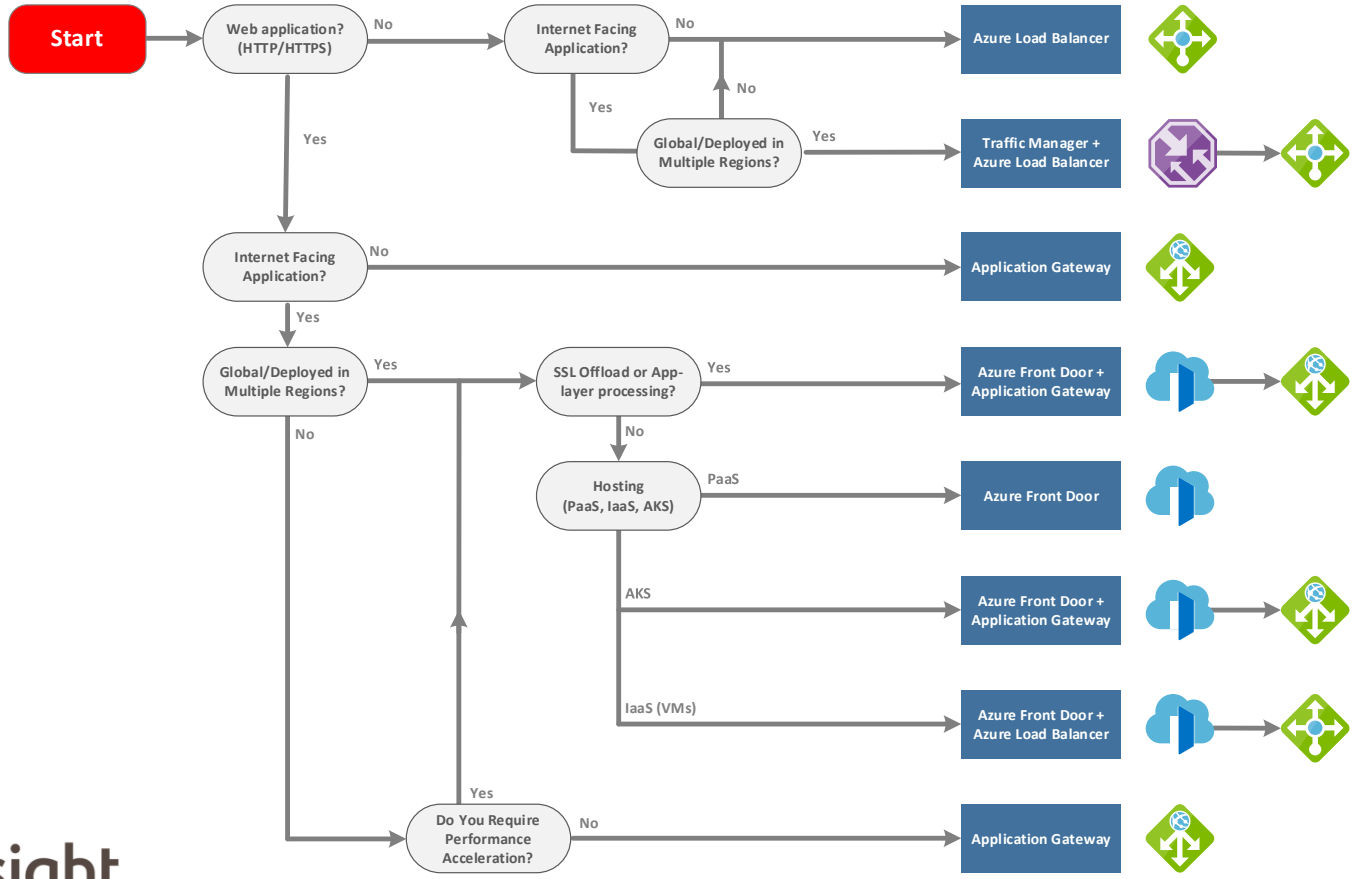
- High availability and scalability built in and managed by platform
- Layer 7 load balancing URL path, host based, round robin, session affinity, redirection
- Centralized SSL management SSL offload and SSL policy
- Public or ILB public internal or hybrid
- Rich diagnostics Azure monitor, Log analytics

Web Application Firewall

- Protects your application against prevalent X-Site Scripting and SQL Injection attacks
- Blocks threats based on OWASP core rule sets 3.0 or 2.2.9



Insight


Start
Web application? (HTTP/HTTPS)
No
Internet Facing Application?
No
Azure Load Balancer
Yes
No
Yes
Global/Deployed in Multiple Regions?
Yes
Traffic Manager + Azure Load Balancer
Yes
Internet Facing Application?
No
Application Gateway
Yes
Global/Deployed in Multiple Regions?
Yes
SSL Offload or App-layer processing?
Yes
Azure Front Door + Application Gateway
No
Hosting (PaaS, IaaS, AKS)
PaaS
Azure Front Door
AKS
Azure Front Door + Application Gateway
IaaS (VMs)
Azure Front Door + Azure Load Balancer
No
Yes
Do You Require Performance Acceleration?
No
Application Gateway

Insight

Azure Firewall

Cloud native stateful Firewall as a service

Central governance of all traffic flows

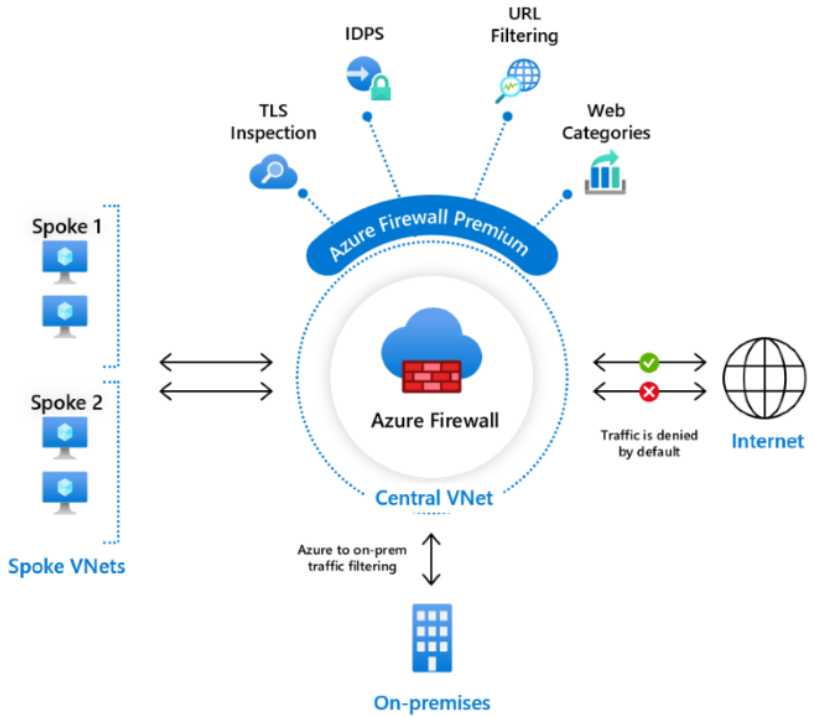
- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions

Complete VNET protection

- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)
- Threat intelligence-based filtering to alert/deny traffic from/to known malicious IP addresses and domains.

Centralised logging

- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice



https://docs.microsoft.com/en-us/azure/firewall/

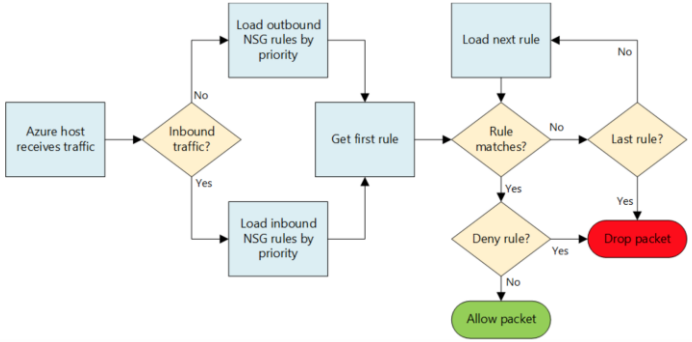
Network Security & Application Security Groups

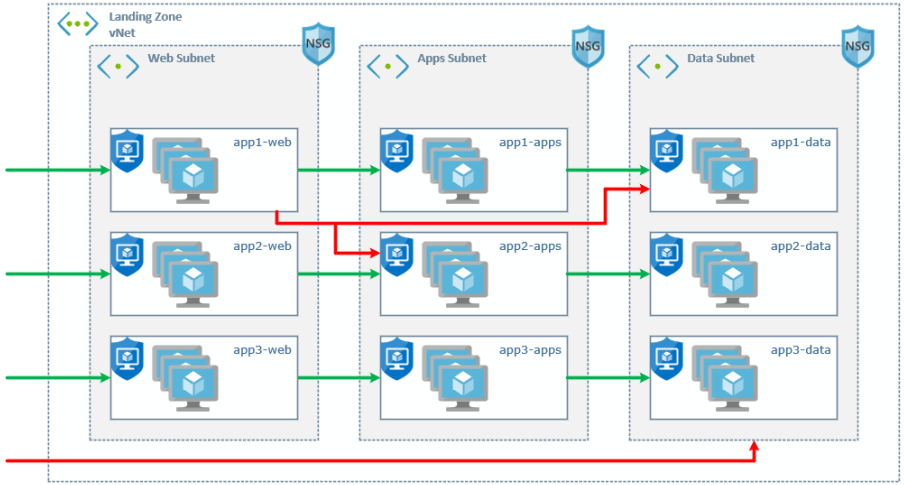
Network Security Groups

- Network Security Group is an Azure Resource that you can use to enforce and control the network traffic within a virtual network.

Application Security Group

- Application Security Group is an object reference within a Network Security Group.





Insight

Options for Accessing Services

Available for all Azure services

Public Endpoints

- **Shared instance** available via public networks

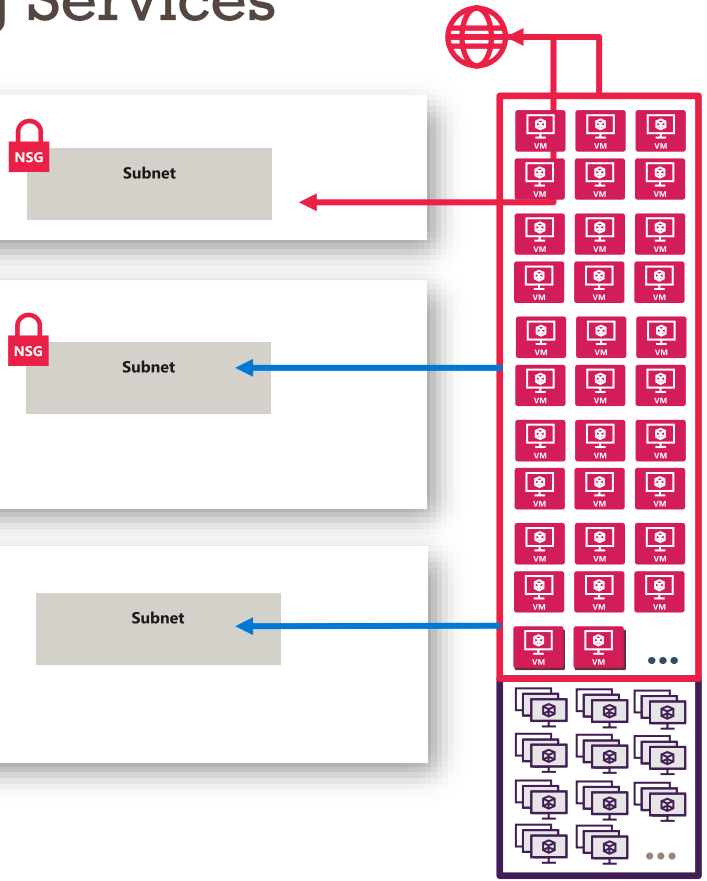
Available for subset of Azure services

Service Endpoints (Service Tunnel)

- **Additional path** of availability of service into your subnet

Private Endpoints & PrivateLink

- **Private access** to Azure PaaS services using private endpoints



Insight

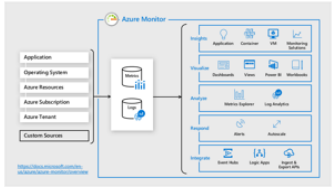
Service Endpoints vs Private Endpoints

Azure Private Link	Azure Service Endpoints
• Control Access to PaaS Services over Private Network	• Control Access to PaaS Services over the public internet.
• VNET to PaaS instance via Microsoft backbone	• VNET to PaaS service via the Microsoft backbone
• PaaS resource mapped to a private IP address. NSGs are restricted to Vnet space	• The destination is still a public IP address, NSG needs to be opened, service tags can help.
• In-built data exfiltration protection	• Traffic will need to be passed through an NVA/Firewall for exfiltration protection
• Easily extensible for On-prem network traffic via ExpressRoute or VPN.	• Restricting On-prem traffic is not straight forward

Network Visibility

Security Information and Event Management (SIEM)

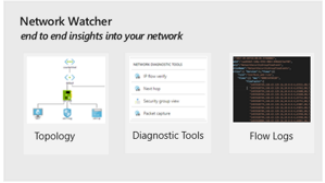
Azure Monitor
Log Aggregation



WAF | **NSG Logs** | **Azure Firewall**

Investigation Workflow

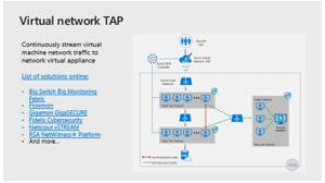
Network Watcher
Advanced Functions



NSG Flow Logs | **Packet Capture** (Point in Time)

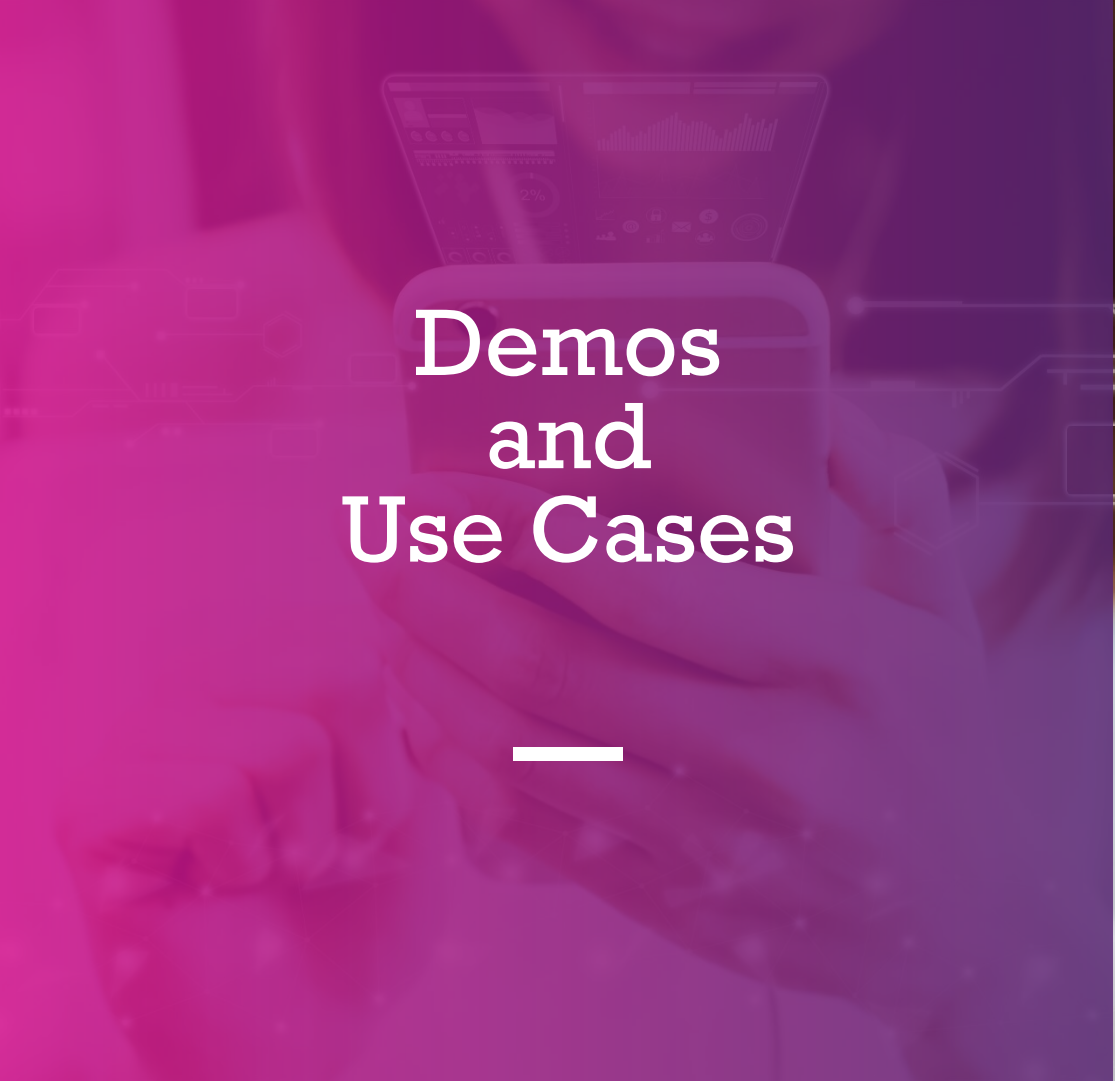
Analytics

Virtual Tap (Preview)
Raw Traffic Access



Virtual Network

Insight



Demos and Use Cases

Insight | Digital Innovation

Use Case / Demo # 1

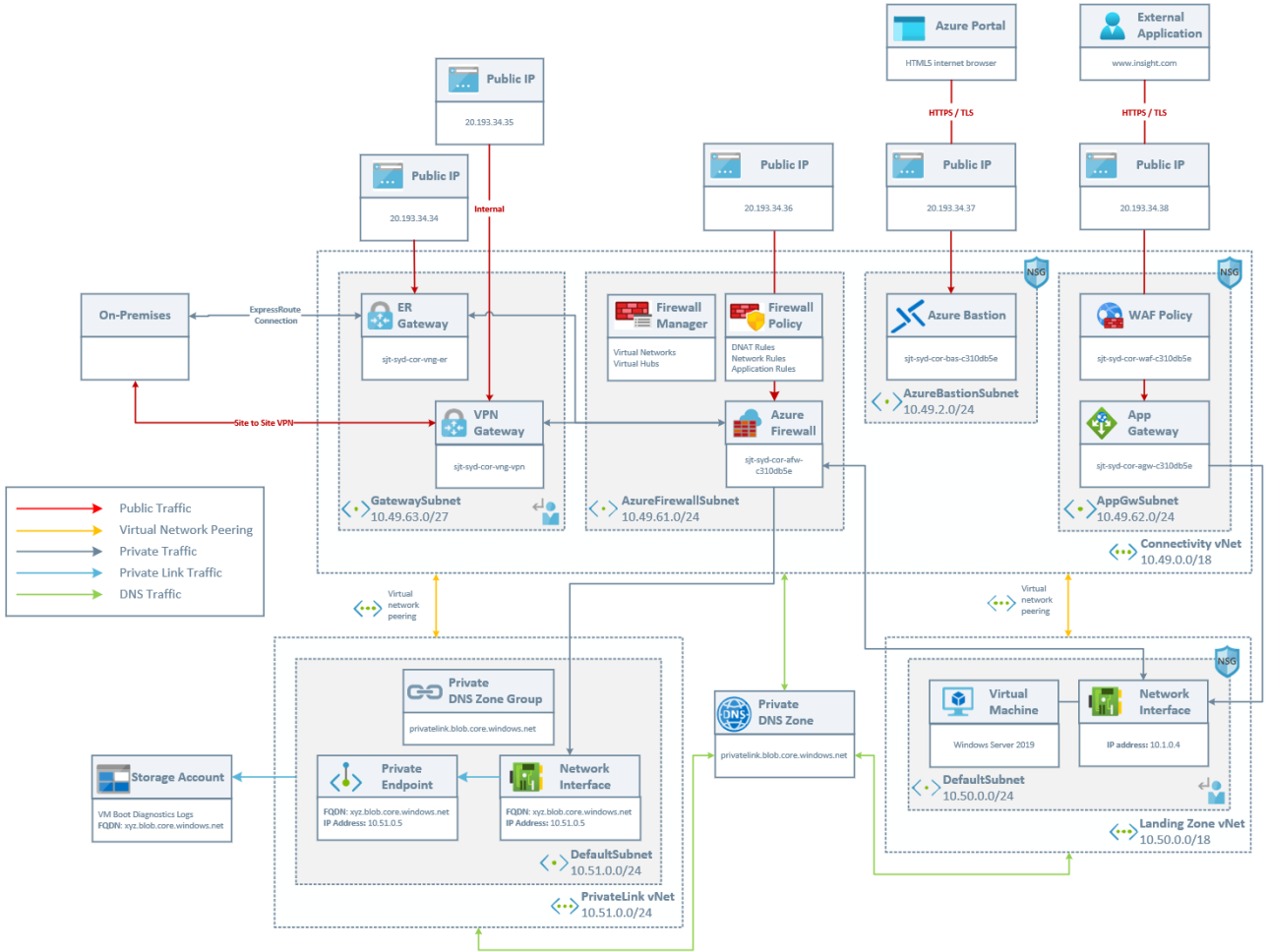
Use Case: "I want to deploy an Enterprise Azure topology using Azure Cloud Native network services"

Solution: Enterprise Scale Hub and Spoke Network Architecture using Azure native services

Insight

Cloud Native Hub and Spoke Network Architecture

- Hub and Spoke network topology to segregate centralised network services from workloads.
- A Connectivity Hub virtual network for centralised network services in a dedicated Subscription
- Landing Zone Spoke virtual network(s) for workloads and applications.
- Dedicated Private Link virtual networks for secure Azure PaaS access via Private Endpoints.
- NSG and ASGs for network segmentation in a Landing Zone
- ExpressRoute and VPN gateway network connectivity pattern.
- Azure Firewall for East/West and North/South traffic, managed by Azure Firewall Manager.
- Azure Bastion for remote access to the platform using RDP/SSH over HTTPS.
- Azure Application Gateway with Web Application Firewall for the external presentation of applications using TLS.
- Azure Private DNS Zones for auto-registration of Private Endpoints.
- Azure DDoS Protection Standard enabled across the tenant for DDoS Protection


Azure Portal
HTML5 internet browser
External Application
www.insight.com
HTTPS / TLS
HTTPS / TLS
Public IP
20.193.34.35
Public IP
20.193.34.34
Internal
Public IP
20.193.34.36
Public IP
20.193.34.37
Public IP
20.193.34.38
NSG
NSG
On-Premises
ExpressRoute Connection
ER Gateway
sjt-syd-cor-vng-er
Firewall Manager
Virtual Networks
Virtual Hubs
Firewall Policy
DNAT Rules
Network Rules
Application Rules
Azure Bastion
sjt-syd-cor-bas-c310db5e
WAF Policy
sjt-syd-cor-waf-c310db5e
Site to Site VPN
VPN Gateway
sjt-syd-cor-vng-vpn
Azure Firewall
sjt-syd-cor-afw-c310db5e
App Gateway
sjt-syd-cor-agw-c310db5e
GatewaySubnet
10.49.63.0/27
AzureFirewallSubnet
10.49.61.0/24
AzureBastionSubnet
10.49.2.0/24
AppGwSubnet
10.49.62.0/24
Connectivity vNet
10.49.0.0/18
Public Traffic
Virtual Network Peering
Private Traffic
Private Link Traffic
DNS Traffic
Virtual network peering
Virtual network peering
Private DNS Zone Group
privatelink.blob.core.windows.net
Private DNS Zone
privatelink.blob.core.windows.net
Virtual Machine
Windows Server 2019
Network Interface
IP address: 10.1.0.4
Storage Account
VM Boot Diagnostics Logs
FQDN: xyz.blob.core.windows.net
Private Endpoint
FQDN: xyz.blob.core.windows.net
IP Address: 10.51.0.5
Network Interface
FQDN: xyz.blob.core.windows.net
IP Address: 10.51.0.5
DefaultSubnet
10.51.0.0/24
PrivateLink vNet
10.51.0.0/24
DefaultSubnet
10.50.0.0/24
Landing Zone vNet
10.50.0.0/18

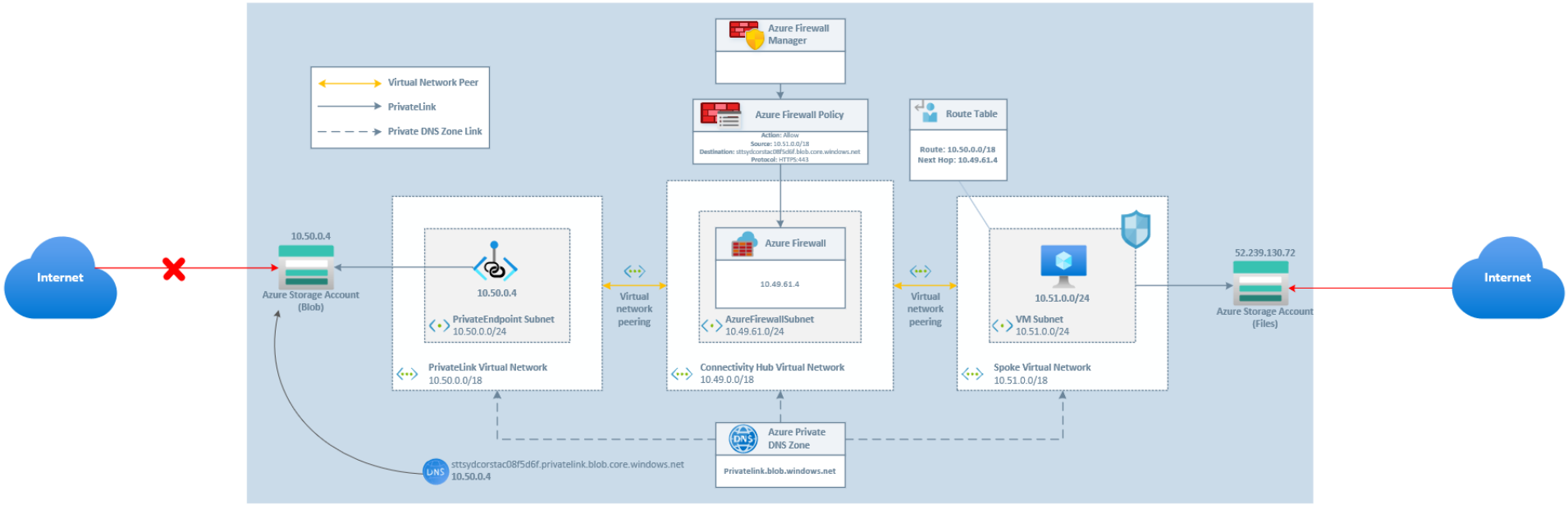
Insight

Use Case / Demo # 2

Use Case: “I want to inspect traffic destined to Private Endpoints”

Solution: Dedicated Virtual Network for Private Endpoints integrated with Azure Firewall.

Insight


Azure Firewall Manager
Virtual Network Peer
PrivateLink
Private DNS Zone Link
Azure Firewall Policy
Action: Allow
Source: 10.51.0.0/18
Destination: sttsydcorstac08f5d6f.blob.core.windows.net
Protocol: HTTPS:443
Route Table
Route: 10.50.0.0/18
Next Hop: 10.49.61.4
Internet
10.50.0.4
Azure Storage Account (Blob)
10.50.0.4
PrivateEndpoint Subnet
10.50.0.0/24
PrivateLink Virtual Network
10.50.0.0/18
Virtual network peering
Azure Firewall
10.49.61.4
AzureFirewallSubnet
10.49.61.0/24
Connectivity Hub Virtual Network
10.49.0.0/18
Virtual network peering
10.51.0.0/24
VM Subnet
10.51.0.0/24
Spoke Virtual Network
10.51.0.0/18
52.239.130.72
Azure Storage Account (Files)
Internet
Azure Private DNS Zone
Privatelink.blob.windows.net
sttsydcorstac08f5d6f.privatelink.blob.core.windows.net
10.50.0.4

Insight