February 6th-7th

NIC 20/20 VISION

Oslo Spektrum

Secure Azure Network Architecture

Aidan Finn, MVP, Innofactor Norway

Introduction

- 13 year MVP – currently Microsoft Azure (3)
  - Previously Hyper-V and SCCM
- Principal Consultant for Innofactor Norway
  - Azure infrastructure – networking & security
- Working as consultant/sys admin since 1996
- Windows Server, Hyper-V, System Center, desktop managment, and Azure

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

INNOFACTOR®

nic

Infrastructure *and* Platform

There Is Always A Network

- It’s the cloud
- Networks:
  - Connection to/from Internet
  - Between components of your service
- Resource include (but not limited to):
  - Virtual machines
  - App Services
  - Azure Kubernetes Service
  - Logic Apps
  - And everything else

Network Security

- Control:
  - Inbound flows
  - Flows between components of your service
  - Data access
  - Outbound flows
- Log & report:
  - Flows
  - Classification of threats
- Alert
  - Security threats

Essential Term Of The Day

- Usual data center approach:
  - “Open up everything inside the network”
  - It’s easy for admins … and malware and attackers
- Micro-Segmentation
  - Breaking up a network into smaller secure zones
  - Right down to the workload
  - Yes, I know “secure zone” is a special term in Norway!

Back To Basics – Virtual Network (VNet)

Your On-Premises Network Knowledge

- I have never created a VLAN
  - Never!
- But I am the Azure networking guy at work
- Who struggles with Azure networking?
  - The network admin
- Who ends up being best at Azure networking?
  - The person who forgets/doesn't know on-prem networking

Virtual Network

- Software-defined network
  - NSX
- An abstraction of physical network
  - Overlapping address ranges are possible (if not routed)
- Data transmission is encapsulated on a physical network
  - A memory transfer between physical hosts
- There is no Default gateway
- Handled in the fabric:
  - Routing
  - Load balancing

Virtual Network Scenarios

- The obvious:
  - VNets are needed for virtual machines
- The useful:
  - VNet-integrated PaaS resources
- The hidden:
  - Platform services are often built using VMs under-the-covers
  - VMs require VNets!

Distributed Denial of Service (DDoS) Attacks

- A threat against business of all sizes
- Attackers:
  - State-sponsored
  - Professional criminals
  - Amateurs: rented botnets!

Azure DDoS Protection Options

- Every VNet has DDoS Basic
- You pay (a lot) for Standard
- Enabled on VNets with public IP addresses
- It takes 2 weeks for the machine learning to “learn” your network
  - Don’t wait until you are attacked!

Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	Yes	Yes
Automatic attack mitigations	Yes	Yes
Availability guarantee	Azure Region	Application
Mitigation policies	Tuned for Azure traffic region volume	Tuned for application traffic volume
Metrics & alerts	No	Real time attack metrics & diagnostic logs via Azure monitor
Mitigation reports	No	Post attack mitigation reports
Mitigation flow logs	No	NRT log stream for SIEM integration
Migration policy customizations	No	Engage DDoS Experts
Support	Best effort	Access to DDoS Experts during an active attack
SLA	Azure Region	Application guarantee & cost protection
Pricing	Free	Monthly & usage based

https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview

Public IP Addresses

Long-Story-Short

- Azure services tend to be public by default
  - A public IP address (PIP)
- Limit your attack surface:
  - Centralise PIPs
  - Limit creation by Azure Policy
  - Force everything through a secure network core

Network Security Groups (NSGs)

Basic Layer-4 Security

- A free form of allow/deny Layer-4 firewall
- An NSG resource associated with a subnet
  - Best practice: 1 NSG : 1 Subnet
- Contains inbound and outbound rules
- Inbound default rules:
  - Allow everything from VNet in, allow Azure load balancer in, deny everything else
- Outbound default rules:
  - Allow everything out

Rule Components

- Priority
  - Order that rules are applied: low (1) to high (4096)
- Name
  - User friendly label
- Port
  - TCP/UDP port
- Protocol
  - TCP, UCP, ICMP, Any
- Source
  - IP address, range, CIDR, service tag, application security group
- Destination
  - IP address, range, CIDR, service tag, application security group
- Action
  - Allow | Deny

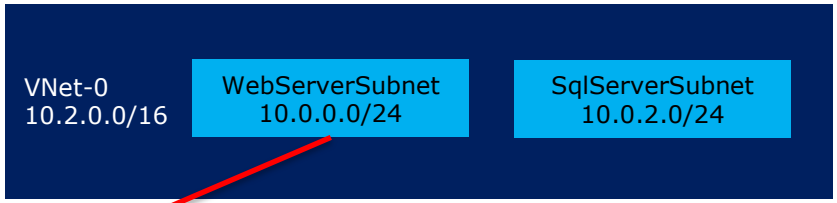
User Friendly Labels

- Source/Destination IP addresses can be unfriendly:
  - Complex subnets with many Azure virtual machines
  - Azure services
- Service Tags
  - Abstracts the IP addresses of Azure Services, e.g. AzureLoadBalancer, GatewayManager, VirtualNetwork, Internet
- Application Security Groups
  - A label, associated with NICs of Azure virtual machines
  - Can be used to more-easily micro-segment a single subnet

The VirtualNetwork Service Tag

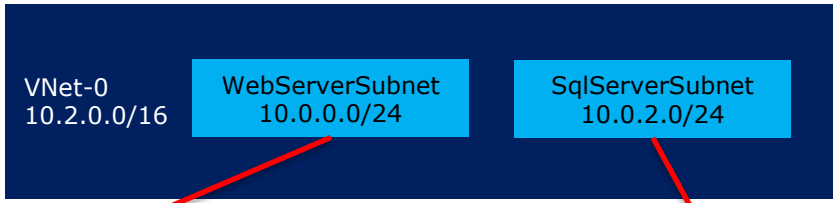
- It’s not just the virtual network!
- It’s the current virtual PLUS:
  - Every other connected virtual network
  - Peering
  - ExpressRoute
  - VPN
- So the default rule of AllowVnetInbound breaks micro-segmentation

Building Up A Simple NSG Ruleset



Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowHttpAndHttps	80, 443	TCP	Internet	WebServersAsg	Allow
200	AllowLoadBalancer	Any	Any	AzureLoadBalancer	WebServersAsg	Allow
300	DenyEverythingElse	Any	Any	Any	Any	Deny

Building Up A Simple NSG Ruleset



Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowHttpAndHttps	80, 443	TCP	Internet	WebServersAsg	Allow
200	AllowLoadBalancer	Any	Any	AzureLoadBalancer	WebServersAsg	Allow
300	DenyEverythingElse	Any	Any	Any	Any	Deny

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowSQLFromWeb	1433	TCP	WebServersAsg	SqlServersAsg	Allow
200	AllowLoadBalancer	Any	Any	AzureLoadBalancer	SqlServersAsg	Allow
300	DenyEverythingElse	Any	Any	Any	Any	Deny

But There's Likely Much More!

- Real-world experience:
  - There's always more than just the basic rules
  - Get comfortable with IPv4 subnetting
- Migration scenarios:
  - Log Analytics Service Map
- Troubleshooting
  - NSG Traffic Analytics

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowHttpAndHttps	80, 443	TCP	Internet	WebServersAsg	Allow
200	AllowDnsResponses	53	UDP	DnsServersAsg	WebServersAsg	Allow
300	AllowMonitoring	5001	TCP	MonitoringAsg	WebServersAsg	Allow
400	CiCd	…	…	…	…	…
…	…	…	…	…	…	…
1200	AllowLoadBalancer	Any	Any	AzureLoadBalancer	WebServersAsg	Allow
1300	DenyEverythingElse	Any	Any	Any	Any	Deny

Back To Basics – Routing

The Importance of Routing

- In the physical data centre
  - Cables control the connections
- In the cloud:
  - Software-defined networks
  - We have no access to cables!
  - Packets go from A-Z directly
- We control flows using routing
- This is the most important thing you will learn today!

How Routing Works

- Configuring routing in a guest OS has no influence
  - The fabric takes over when the packet hits the NIC
- Routing is only done in the fabric
  - Per-subnet route tables are always present
- Route table:
  - Destination
  - Next hop instruction
- Route chosen:
  - Longest path first (LPF)
  - Route type

Longest Path First (LPF)

- Example ….
- You want to get to 10.0.1.4
- Two routes exist:
  - 10.0.0.0/8 … 16-bit match
  - 10.0.1.0/24 … 32-bit match
- The chosen route is 10.0.1.0/24

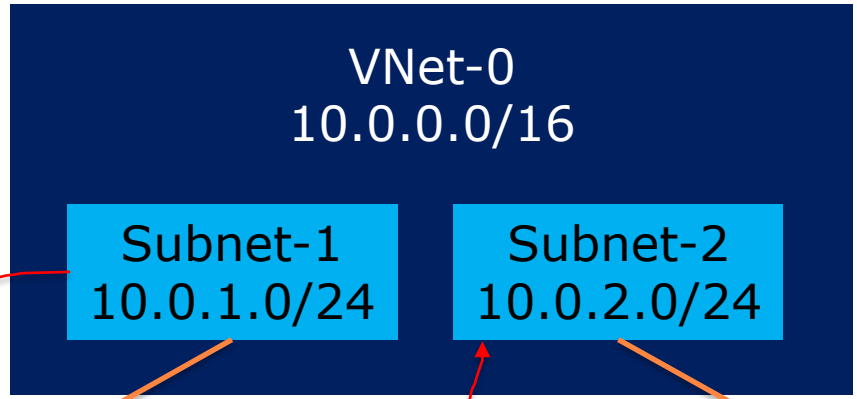
Route Type

1. Default routes
2. BGP
3. User-defined routes

Default / System Routes

- Routes that exist automatically
- Simply there for basic functionality
- Added when you enabled Azure features

Example – Simple Default Routes



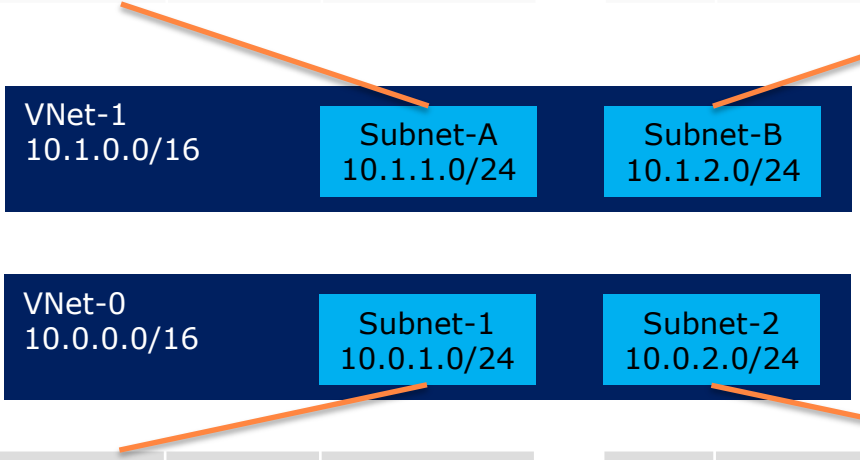
Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	

Example – Simple Default Routes | VNet Peering

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	



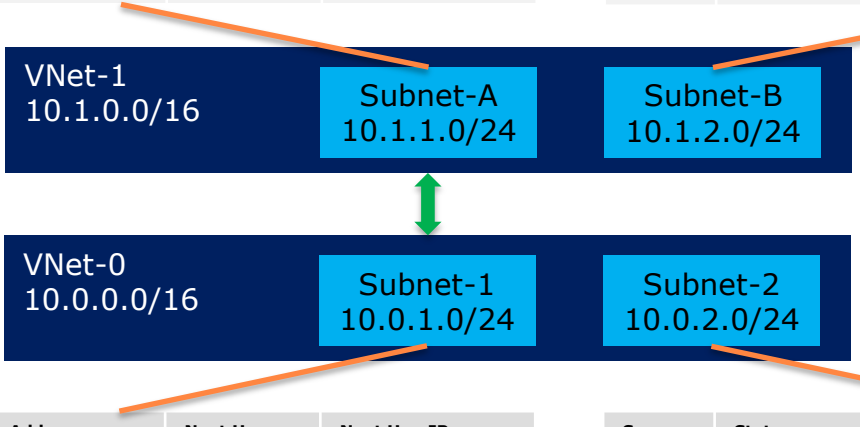
Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	

Example – Simple Default Routes | VNet Peering

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	10.0.0.0/16	Peering	

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	10.0.0.0/16	Peering	



Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	10.1.0.0/16	Peering	

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	10.1.0.0/16	Peering	

BGP Routes

- BGP is used when there is site-to-site networking
  - ExpressRoute
  - VPN
- Ways:
  - Propagate routes from to/from on-premises
    - ExpressRoute: required
    - VPN: Optional
  - Propagate routes from the GatewaySubnet to other subnets/VNets
    - Even if you don’t enable BGP in S2S VPN

BGP Summary

- A list of routes is maintained in a route table
- Routes are propagated to a neighbour(s)
- That neighbour propagates routes to it’s neighbour(s)
- The network learns how to get to any remote destination
  - Possibly over many hops

BGP & Site-to-Site

172.16.0.0/12

ExpressRoute/VPN

VNet-0
10.0.0.0/16

GatewaySubnet
10.0.0.0/24

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	

BGP & Site-to-Site

172.16.0.0/12

ExpressRoute/VPN

VNet Peering
Use Remote Gateway
Gateway Transit

VNet-0
10.0.0.0/16

GatewaySubnet
10.0.0.0/24

VNet-1
10.1.0.0/16

Subnet-1
10.1.1.0/24

VNet-2
10.2.0.0/16

Subnet-1
10.2.1.0/24

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	10.1.0.0/16	Peering	
Default	Active	10.2.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	10.0.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	10.0.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	

BGP Beats Default

- A BGP route that matches a Default Route *beats* the Default Route
- Scenario:
  - A Default route exists for 10.1.0.0/16
  - A BGP route to 10.1.0.0/16 propagates to the subnet
  - The Default route is marked by Azure as *Invalid* (disabled)
  - The BGP route is chosen instead

User-Defined Routes (UDRs)

- Sometimes you need to “cable” Azure
  - Force traffic via a particular destination
- This is always the case when you use a firewall … ah-ha!
  - Third-party firewall appliance
  - Azure Firewall
- And also when you use third-party routers/VPN appliances

Route Tables

- We can add UDR's via a Route Table
  - An Azure resource
- Associated with a subnet
  - Tip: 1 subnet per Route Table only!
- Common mistake:
  - People think the route table contains the only routes in a subnet
  - Don't forget about Default and BGP routes hidden in the fabric!

UDR Components

- Name: A human friendly label
- Address Prefix: CIDR destination
- Next Hop Type:
  - Virtual Network Gateway
  - Virtual Network
  - Internet
  - Virtual Appliance *
  - None (black hole)
- * Next Hop IP Address
  - * Virtual Appliance IPv4 address

Inbound Flows Via Firewall

172.16.0.0/12 ExpressRoute/VPN

10.0.1.4

VNet-0
10.0.0.0/16

GatewaySubnet
10.0.0.0/24

AzureFirewallSubnet
10.0.1.0/24

VNet-1
10.1.0.0/16

Subnet-1
10.1.1.0/24

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	10.0.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	

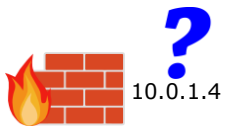
Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Inactive	10.1.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	
User	Active	10.1.0.0/16	Virtual Appliance	10.0.1.4

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Inactive	0.0.0.0	Internet	
Default	Inactive	10.1.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	
User	Active	0.0.0.0/0	Internet	

Outbound Flows Via Firewall

172.16.0.0/12

ExpressRoute/VPN



10.0.1.4

VNet-0
10.0.0.0/16

GatewaySubnet
10.0.0.0/24

AzureFirewallSubnet
10.0.1.0/24

VNet-1
10.1.0.0/16

Subnet-1
10.1.1.0/24

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Inactive	0.0.0.0	Internet	
Default	Active	10.0.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	
User	Active	0.0.0.0/0	Virtual Appliance	10.0.1.4

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Inactive	10.1.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	
User	Active	10.1.0.0/16	Virtual Appliance	10.0.1.4

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Inactive	0.0.0.0	Internet	
Default	Inactive	10.1.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	
User	Active	0.0.0.0/0	Internet	

UDR Beats BGP & Default

- A UDR route that matches a BGP/Default Route *beats* the BGP/Default Route
- Scenario:
  - A Default route exists for 10.1.0.0/16
  - A BGP route to 10.1.0.0/16 propagates to the subnet
  - You add a UDR to 10.1.0.0/16
  - The Default route is marked by Azure as *Invalid* (disabled)
  - The BGP route is marked by Azure as *Invalid* (disabled)
  - The UDR is chosen instead

But Remember – The Most Accurate Route Wins!

- A BGP route that matches a Default Route *beats* the Default Route
- Scenario:
  - A Default route exists for 10.1.0.0/16
  - A BGP route to 10.1.0.0/16 propagates to the subnet
  - You add a UDR to 0.0.0.0/0
- Send a packet to 10.1.1.4
  - The Default route is marked by Azure as *Invalid* (disabled)
  - The BGP route is a 16-bit match
  - The UDR is a 0-bit match
  - The BGP route is chosen!

Outbound Flows Via Firewall

Route Table > Disable BGP Propagation

172.16.0.0/12

ExpressRoute/VPN

Public IP Address

10.0.1.4

VNet-0
10.0.0.0/16

GatewaySubnet
10.0.0.0/24

AzureFirewallSubnet
10.0.1.0/24

VNet-1
10.1.0.0/16

Subnet-1
10.1.1.0/24

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Inactive	0.0.0.0	Internet	
Default	Active	10.0.0.0/16	Peering	
User	Active	0.0.0.0/0	Virtual Appliance	10.0.1.4

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Inactive	10.1.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	
User	Active	10.1.0.0/16	Virtual Appliance	10.0.1.4

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Inactive	0.0.0.0	Internet	
Default	Inactive	10.1.0.0/16	Peering	
BGP	Active	172.16.0.0/12	VirtualNetworkGateway	
User	Active	0.0.0.0/0	Internet	

Viewing Effective Route Tables

- Today:
  - Only possible via the NIC of an allocated (running) VM
- Desired:
  - See it via any subnet
- Tips:
  1. LEARN how routing really works (see previous)
  2. Try it out
  3. Draw how it works
  4. Put a “canary” subnet/VM into a complex VNet so you can see effective routes
     - VMs cannot be added to GatewaySubnet or AzureFirewallSubnet

ExpressRoute & VPN

- ExpressRoute
  - View/export routes propagated from on-premises
  - Circuit > Peerings > Private Peering
- VPN
  - Non-BGP: See Local Network Gateway
  - BGP: Query Log Analytics … AzureDiagnostics | where OperationName == "BgpRouteUpdate"

Firewalls

Do I Need A Firewall?

- Great question!
- Ideally – yes!
- Central point of:
  - Network security
  - Routing
- Can offer more than just simple “Allow TCP From X To Y”
  - Centrally control outbound and east-west flows
  - FQDN support for SQL and Web

Platform Versus Appliance

Feature	Appliance	Azure Firewall
Type	Virtual machines	Platform
Complexity	High	None
High availability	None to challenging	Availability Set/Zones
Scale-Out	1-2	Automatic
Maintenance/Upgrades	You (Guest OS)	Microsoft (Platform)
Layer-7	None-Little	Little (see Azure WAFv2)
IDS/IPS	Maybe	Azure Security Center/Sentinel
Documentation	Mostly awful	Good
Max throughput	Varies	30 Gbps (more with Support call)

Azure Firewall

- Architecture
  - Single subnet / Private IP
  - 1-100 Public IPv4 (SNAT and DNAT scale-out)
  - Availability sets/zones
- Features:
  - NAT Rules
    - DNAT from Internet
  - Network Rules
    - Layer-4 protection at central location
  - Application Rules
    - FQDN HTTP/S and SQL Server traffic
    - FQDN Tags
  - Threat Intelligence
    - Machine learning based alerting/blocking
  - Logging
    - Storage account, Event Hub, Log Analytics

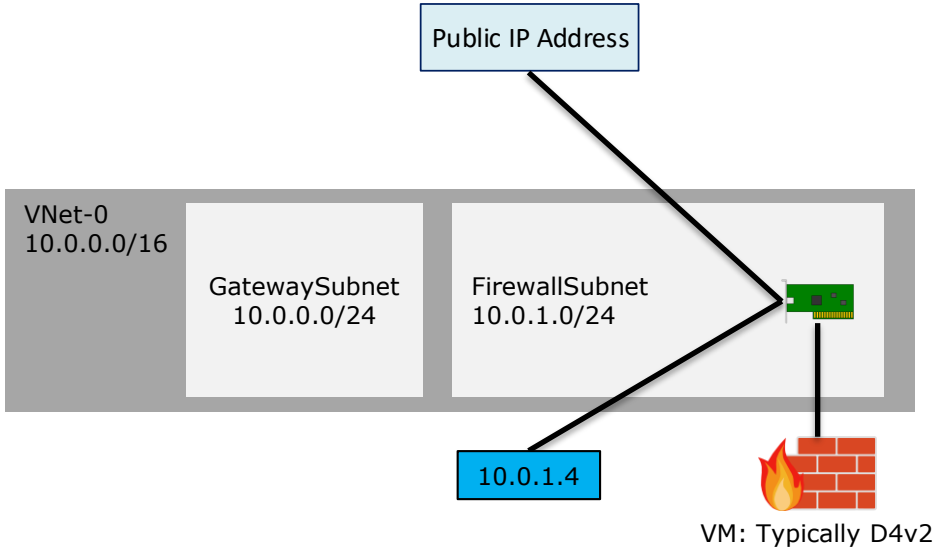
Azure Firewall SKUS

- Network
  - A single resource
  - Managed via the resource
- Secure Virtual Hub (Preview)
  - A hub (hub and spoke)
  - Firewall *and* Azure WAN hub
  - Managed via hub and Azure Firewall Policy
    - AFP not in the Network SKU

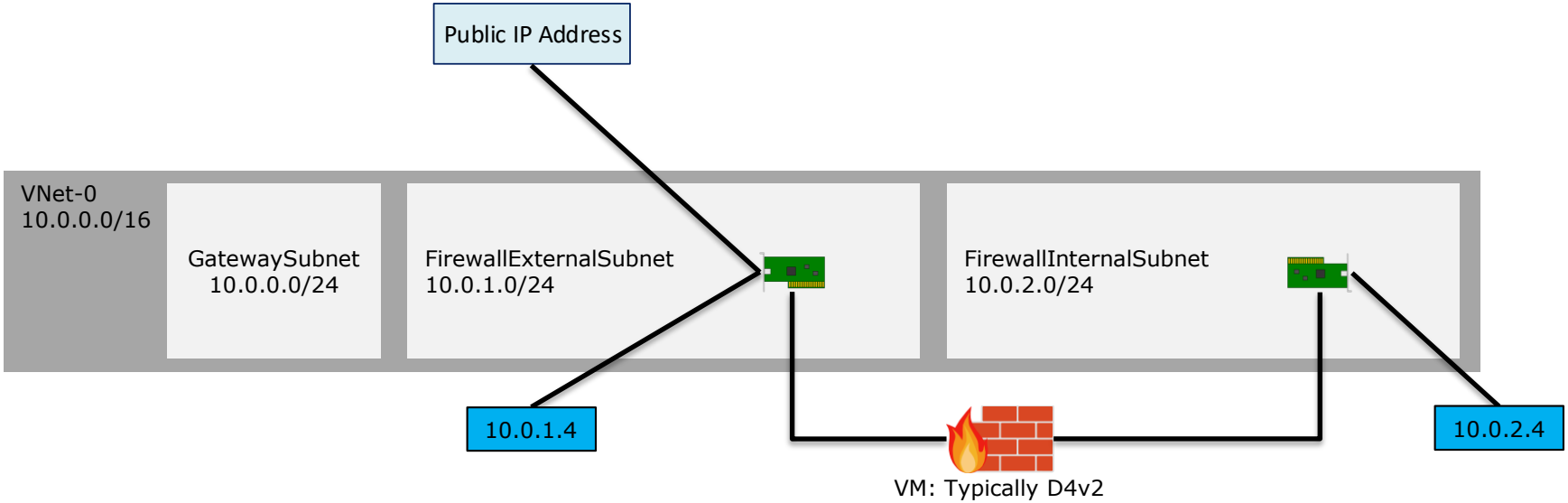
Third-Party Firewall Appliance Architecture

- It depends – consult whatever documentation the vendor has
- Caution: some major vendors sell you ticking timebombs!
  - Beware of appliance clusters that don’t have 2 Azure load balancers
  - And don’t use any brand that expects you to program Azure UDRs via their appliance

Simple Firewall Appliance Architecture



Split-Subnet Firewall Appliance Architecture

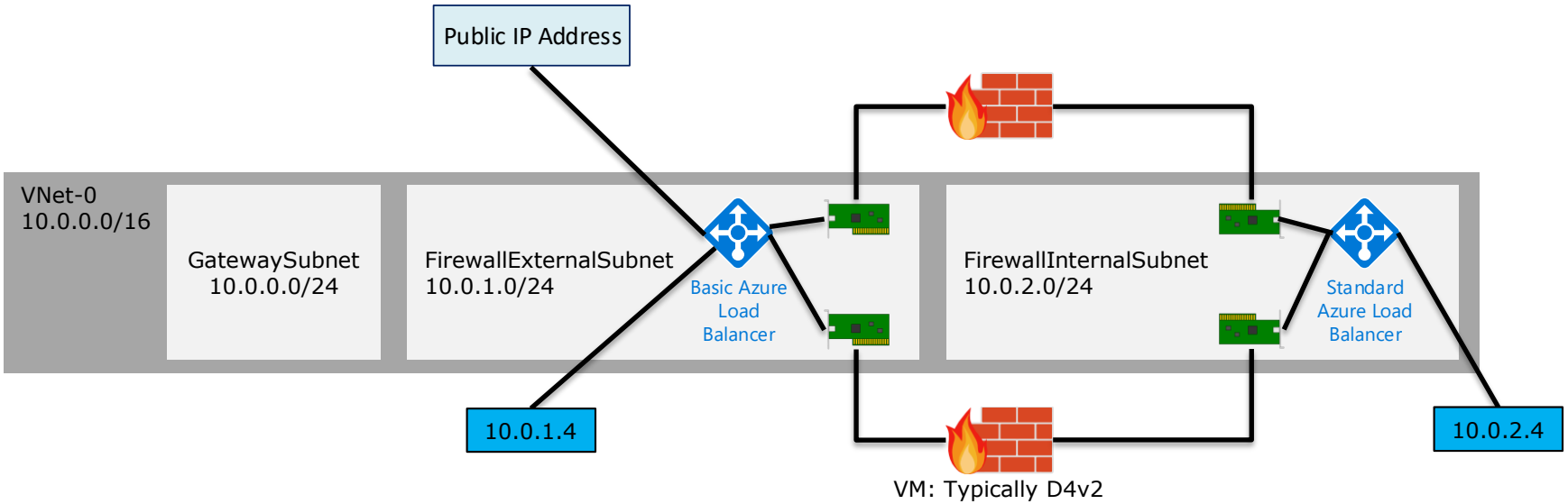


Note: Additional firewall management subnet typically required

UDRs For This Scenario

- GatewaySubnet
  - Address Prefix : Spoke CIDR
  - Next Hop Type: Virtual Appliance
  - Next Hop IP Address: External NIC private IP address
- Spoke Subnets
  - Address Prefix : 0.0.0.0/0
  - Next Hop Type: Virtual Appliance
  - Next Hop IP Address: Internal NIC private IP address

Highly Available Firewall Appliance Architecture



Note: Additional firewall management subnet typically required

UDRs For This Scenario

- GatewaySubnet
  - Address Prefix : Spoke CIDR
  - Next Hop Type: Virtual Appliance
  - Next Hop IP Address: External Load Balancer Private IP address
- Spoke Subnets
  - Address Prefix : 0.0.0.0/0
  - Next Hop Type: Virtual Appliance
  - Next Hop IP Address: Internal Load Balancer Private IP address

Variations On This Scenario

- Most vendors will add management subnet/NICs
  - Not load balanced
- Some vendors require Azure Service Bus for configuration replication
- There is an option for another subnet with load balanced NICs:
  - Internet traffic
  - ExpressRoute/VPN traffic

Layer-7 Web Application Firewall (WAF)

What is a WAF?

- Specialised firewall for HTTP/S traffic
  - Think of it as a reverse proxy with firewall features for HTTP/S servers
- Different to your firewall
  - Focused on simple allow/deny traffic
- WAF focus:
  - Attacks on HTTP/S servers

Product Options

- Third-party
  - Complexities of appliances
  - See firewall appliances (previous)
- Azure Application Gateway
  - Enable Azure Application Firewall (additional cost)
- Azure Front Door
  - Web Application Firewall

WAF Placement

- Question you need to ask yourself …
- Where will you place the WAF?
  - Centrally:
    - Managed by security experts
    - Requires process for change requests
  - With each application
    - Flexible for Devs/Operators
    - Security handled by the wrong people!
- Typically *not* in-front or behind the network firewall
  - Isolated flow to protect against DDoS
  - Protected at Layer-4 by NSG

Azure Application Gateway WAFv2 Features

- Application Gateway:
  - Availability sets/zones
  - SSL Offload
  - SSL storage in Azure Key Vault – delegated access via User Managed ID
  - End-to-end encryption
- WAF:
  - OWASP 3.1 rules, SQL injection, malformed requests, etc
  - Extends DDoS Standard Tier to Layer-7
  - Optional management via WAF Policy resource
    - Extended rules customisation
    - Bot protection rule (preview)
    - Geomatch filtering (limited region preview)

Azure Front Door WAF Features

- Azure Frontdoor:
  - Located at every Microsoft edge data centre
    - Reduce latency between global customers and your service
    - Keeping the threat further from your assets
  - SSL Offload
  - End-to-end encryption
- WAF Policy:
  - OWASP 3.1 rules, SQL injection, malformed requests, etc
  - Extended rules customisation
  - Bot protection rule (preview)
  - Geo-match filtering (preview)

Decisions

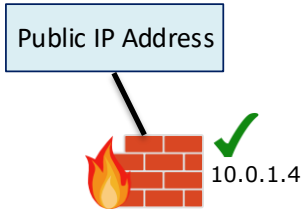
- Use Third-Party / Azure Application Gateway WAF
  - In-VNet protection
- Use Azure Front Door WAF
  - Global client reach
  - Push the threat to the Microsoft WAN edge

NSG, WAF, and Firewall

172.16.0.0/12

ExpressRoute/VPN

A, internal.joeelway.com = 10.0.2.4
A, sql.joeelway.com = 10.19.3.8



Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
User	Active	10.0.0.0/16	Virtual Appliance	10.0.1.4
User	Active	10.0.2.0/24	Virtual Network	

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowHealthProbe	65200-65535	TCP	GatewayManager	Any	Allow
200	AllowWeb	80, 443	TCP	172.16.0.0/12	10.0.2.0/24	Allow
300	AllowLoadBalancer	Any	Any	AzureLoadBalancer	10.0.2.0/24	Allow
400	DenyEverythingElse	Any	Any	Any	Any	Deny

NSG, WAF, and Firewall

172.16.0.0/12

ExpressRoute/VPN

Public IP Address

10.0.1.4

A, internal.joeelway.com = 10.0.2.4
A, sql.joeelway.com = 10.19.3.8

VNet-0
10.0.0.0/16

GatewaySubnet
10.0.0.0/24

AzureFirewallSubnet
10.0.1.0/24

InternalWafSubnet
10.0.2.0/24

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
User	Active	10.0.0.0/16	Virtual Appliance	10.0.1.4
User	Active	10.0.2.0/24	Virtual Network	

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowHealthProbe	65200-65535	TCP	GatewayManager	Any	Allow
200	AllowWeb	80, 443	TCP	172.16.0.0/12	10.0.2.0/24	Allow
300	AllowLoadBalancer	Any	Any	AzureLoadBalancer	10.0.2.0/24	Allow
400	DenyEverythingElse	Any	Any	Any	Any	Deny

NSG, WAF, and Firewall

172.16.0.0/12

ExpressRoute/VPN

Public IP Address

10.0.1.4

A, internal.joeelway.com = 10.0.2.4
A, sql.joeelway.com = 10.19.3.8

VNet-0
10.0.0.0/16

GatewaySubnet
10.0.0.0/24

AzureFirewallSubnet
10.0.1.0/24

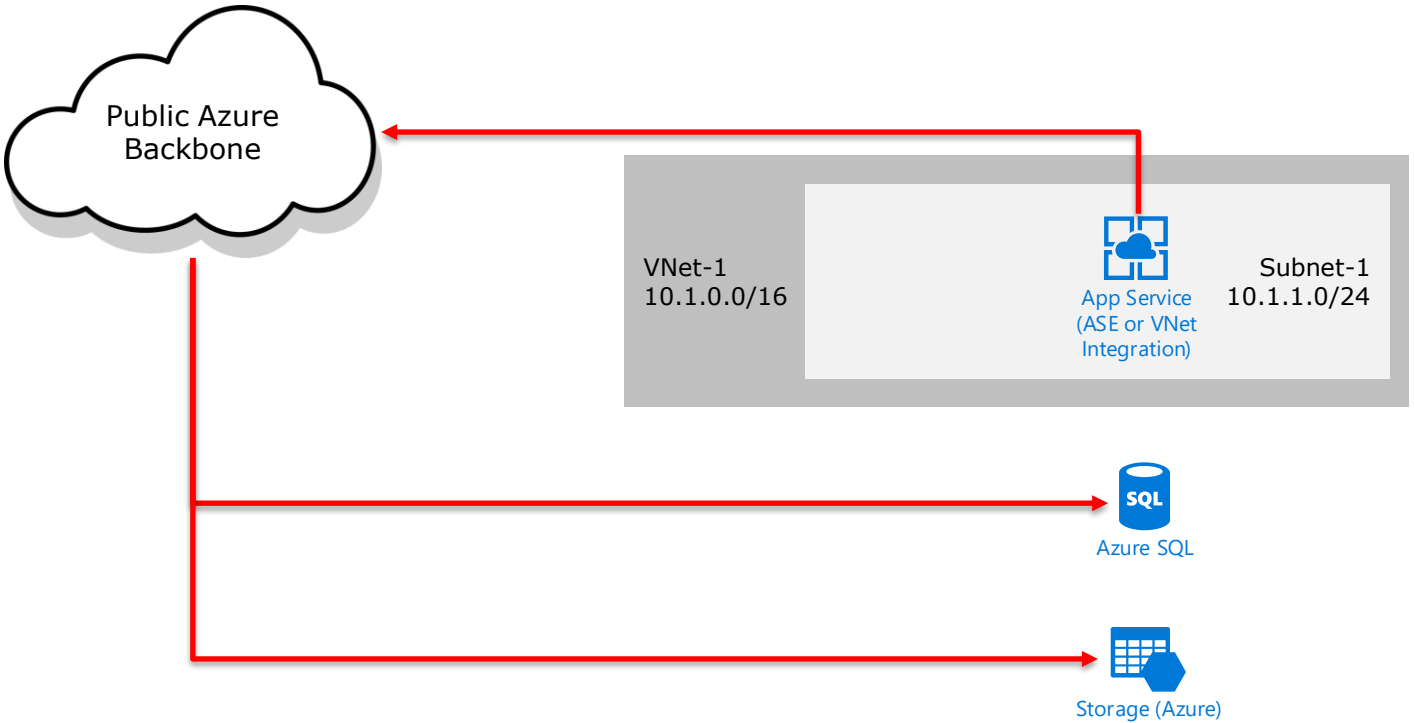
InternalWafSubnet
10.0.2.0/24

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
User	Active	10.0.0.0/16	Virtual Appliance	10.0.1.4
User	Active	10.0.2.0/24	Virtual Network	

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowHealthProbe	65200-65535	TCP	GatewayManager	Any	Allow
200	AllowWeb	80, 443	TCP	172.16.0.0/12	10.0.2.0/24	Allow
300	AllowLoadBalancer	Any	Any	AzureLoadBalancer	10.0.2.0/24	Allow
400	DenyEverythingElse	Any	Any	Any	Any	Deny

Service Endpoints

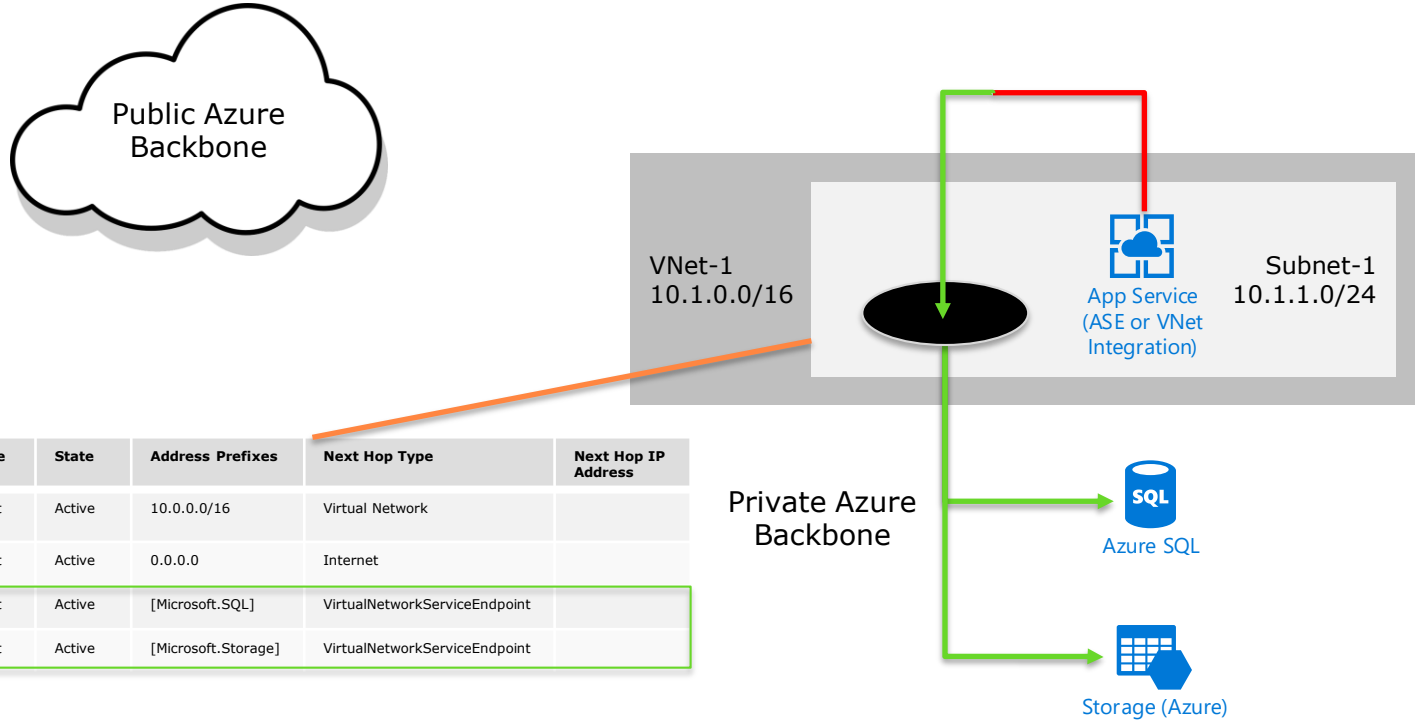
How A VNet Resource Talks To Azure Services



Service Endpoints

- Enabled per-subnet
- A trick of routing
  - Kind of the same idea as ExpressRoute Azure Public Peering
- Uses Default routes
  - Redirects traffic to certain Azure services
  - Direct path: not public, lower latency
  - Extend network security to PaaS (see Access Rules)

How A VNet Resource Talks To Azure Services



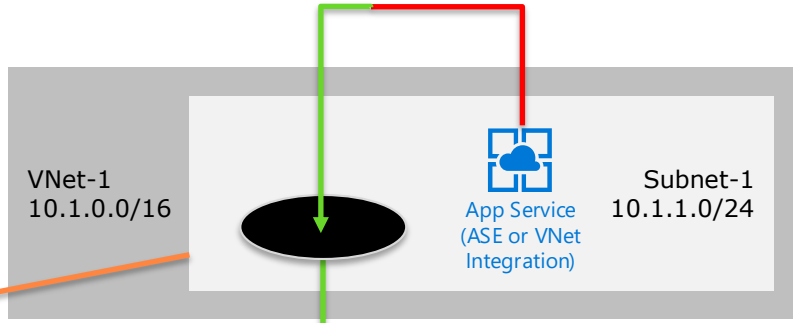
Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	[Microsoft.SQL]	VirtualNetworkServiceEndpoint	
Default	Active	[Microsoft.Storage]	VirtualNetworkServiceEndpoint	

Resource Access Policies

Platform Services Hidden Networking

- PaaS resources run on a VNet
- We cannot see that VNet
- But we can enable “firewall rules” on the PaaS resources:
  - App Service access rules
  - Azure SQL firewall rules
  - And more
- Often used with Service Endpoints

How A VNet Resource Talks To Azure Services



Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address
Default	Active	10.0.0.0/16	Virtual Network	
Default	Active	0.0.0.0	Internet	
Default	Active	[Microsoft.SQL]	VirtualNetworkServiceEndpoint	

Private Link & Private Endpoints

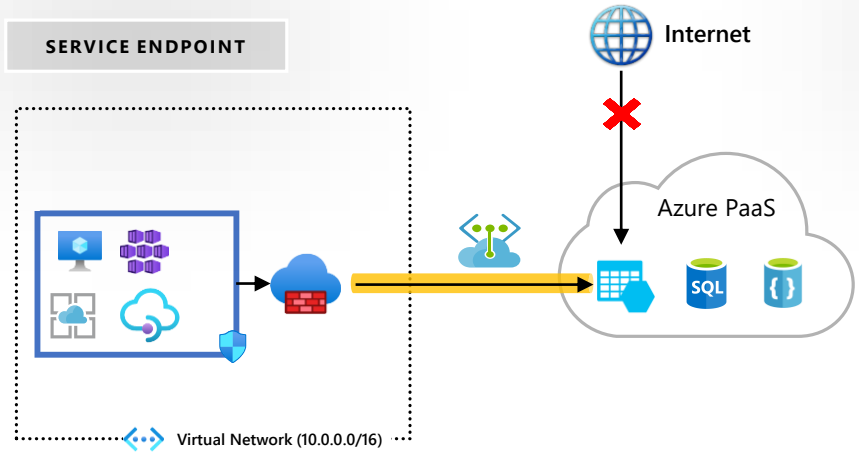
Challenge of Platform-as-a-Service (PaaS)

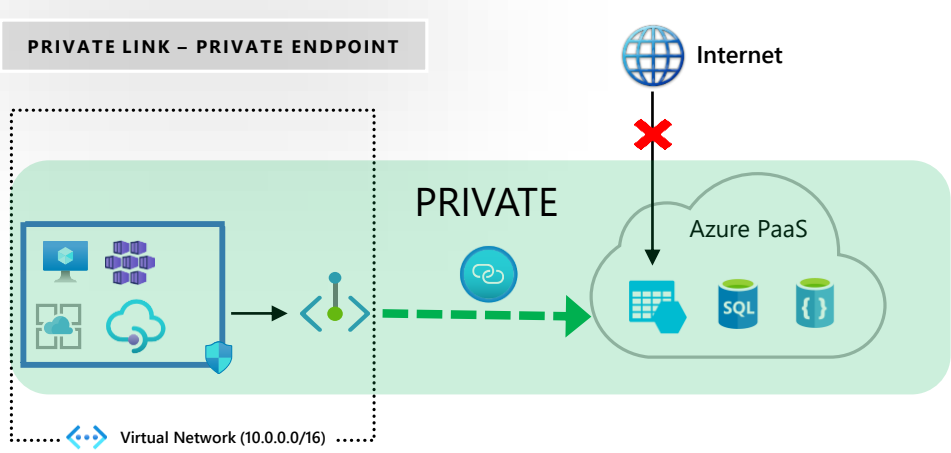
- PaaS *is* the cloud of services in The Cloud
- PaaS is natively public:
  - Your internal application is on The Internet
  - The Data Lake is publicly addressable
  - That database is addressable by everyone

PaaS Privacy Options

- VNet integration
  - Expensive SKUs
- Access Policies
  - Basic Layer-4 filters
- Service Endpoints
  - Maps an entire service, not an instance
- WAF with Service Endpoints, Access Policies, and basic VNet connectivity
  - Doesn’t control all network flows
- Hybrid connectivity agents
  - Only protects PaaS outbound connections to private services
- ExpressRoute Microsoft Peering with Access Policies
  - Maps an entire service, not an instance
  - ExpressRoute is less popular thanks to cost and SD-WAN (Azure WAN) option

Private PaaS (Preview)





VNet to PaaS service via the Microsoft backbone

Destination is still a public IP address. NSG opened to Service Tags

Need to pass NVA/Firewall for exfiltration protection

VNet Paas via the Microsoft backbone

PaaS resource mapped to Private IP Address. NSGs restricted to VNet space

In-built data exfiltration protection

Scenarios

- From Azure VMs to Azure PaaS resources
- Secure connection over VPN, SD-WAN, ExpressRoute via VNet Gateway
- Services shared via Standard tier Azure Load Balancer:
  - Enable overlapping IP address spaces
  - Privately share IaaS/PaaS as SaaS with customers

Points To Note

- Private Link
  - The fabric service that allows mapping
- Private Endpoint
  - The IP address for your PaaS resource in your VNet
- Private Endpoint maps a specific resource
  - Not just an instance like Service Endpoint or ExpressRoute Microsoft Peering
  - Provides protection against data exfiltration

Preview Limitations

- Limited preview with mixed support of:
  - Resources
  - Regions
- No support for NSG rules
  - Still can use NSG Flow Logs
- VNet Peering
  - Requires 1+ VMs on the Private Endpoint VNet
- Private Endpoint not addressable by some resource types:
  - App Service Plan, Azure Container Instance, Azure NetApp Files, Azure Dedicated HSM

Security Management & Monitoring

Security Center

- Features:
  - Compliance reporting
  - Recommendations
  - Monitoring
    - An Azure IDS that runs across the subscription
    - Not focused on just 1 virtual appliance!
- Be careful:
  - Some recommendations are not based on product best practices
  - Example: NSG should be per-subnet, NOT per-NIC
  - Example 2: Be careful of enabling Storage Account firewall feature

Monitoring

- Log Analytics
  - Send diagnostic & metrics data to a single Workspace
  - Add solutions – some from “OMS” gallery in Marketplace, some from GitHub
  - Add saved queries
  - Build workbooks for reporting
- NSG Flows
  - NSG Flow Logs: Send data to GPv2 storage account
  - Traffic Analytics: Forward blob data to Log Analytics

Alerting

- Azure Sentinel
  - Security Information & Event Management (SIEM)
- Features:
  - Log Analytics Workspace solution
  - Connect to Azure & third-party resources
  - Threat hunting
  - Automated responses
  - Alerting

Troubleshooting

- Azure Firewall
  - Traces in Log Analytics … AzureDiagnostics | where Category == "AzureFirewallNetworkRule"
  - Service Map to identify network requirements pre-migration
- NSGs
  - Traffic Analytics … AzureNetworkAnalytics_CL | where SubType_s == 'FlowLog'
- Routing
  - Effective Routes
    - VM NICs only
    - Truly understand routing to map it mentally/on-paper
  - Traffic Analytics
  - I don’t find Network Watcher to be useful
- WAF
  - Traces in Log Analytics … AzureDiagnostics | where Category == "ApplicationGatewayFirewallLog"
  - Most common problem is false positive SQL injection attack detection

Micro-Segmentation

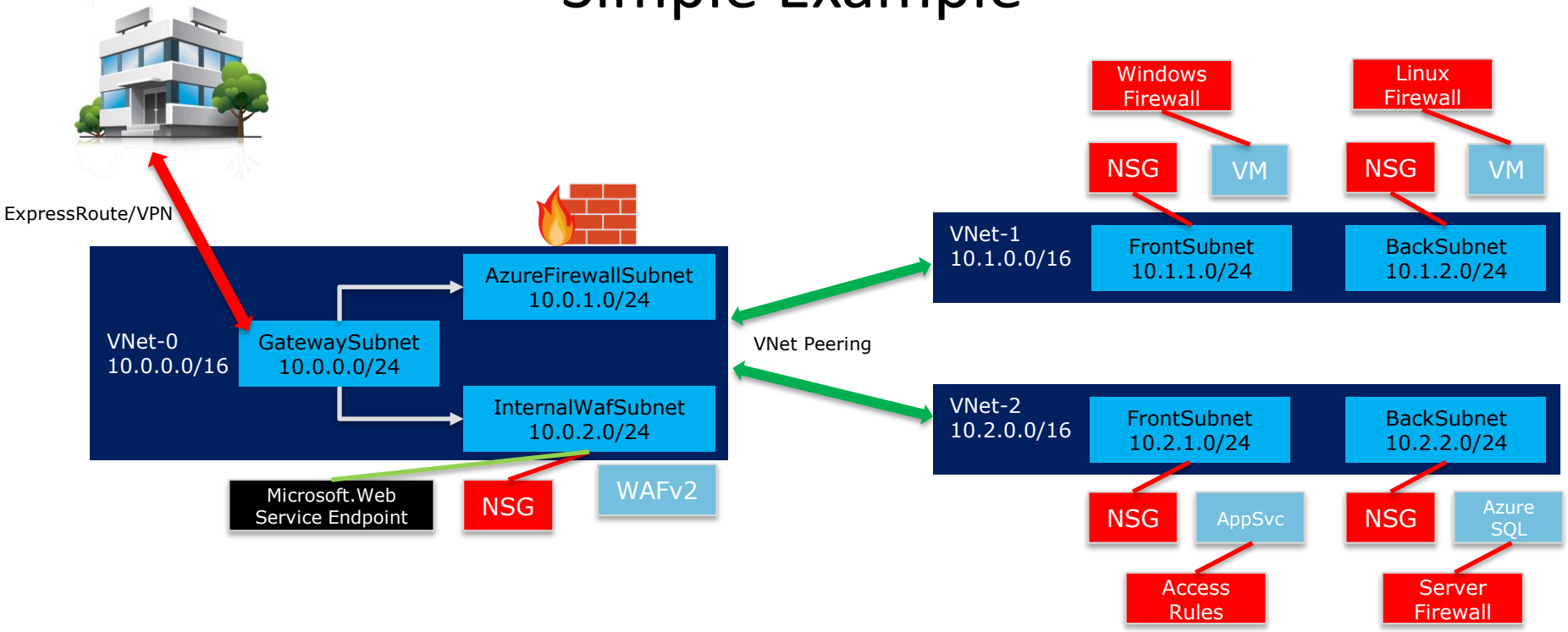
The Typical On-Premises Server Network

- Hard on the outside, gooey on the inside
  - Firewall at the edge
  - No port/VLAN protection
  - Windows/Linux firewall disabled
  - Direct remote access to machines
- How do attacks happen?
  - Find a weak spot (human) to bypass the firewall
  - Spread across open network in minutes
    - Used to be 24 hours for complete compromise

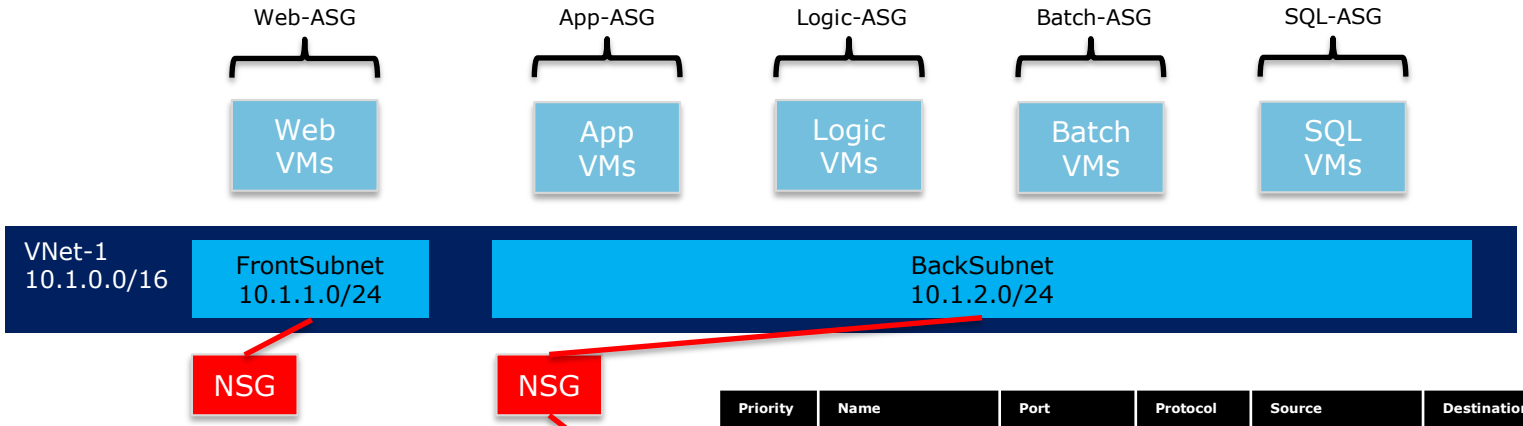
Micro-Segmentation

- Not a new concept
- Implement network protections throughout the entire network
  - Not just the edge

Simple Example



Micro-Segmentation In A Subnet



Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowWebToApp	443	TCP	Web-Asg	App-Asg	Allow
200	AllowAppToLogic	443	TCP	App-Asg	Logic-Asg	Allow
300	AllowLogicToBatch	443	TCP	Logic-Asg	Batch-Asg	Allow
400	AllowLogicToSql	1433	TCP	Logic-Asg	SQL-Asg	Allow
4096	DenyEverythingElse	Any	Any	Any	Any	Deny

Wrapping Up

Summary

- There’s a lot to learn
- Take the deck (when it’s shared) and read through the stuff I skipped
- Read lots!
- Play with the tech in a lab
  - Don’t assume something works
  - Try the positive and negative tests

Thank You!

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

INNOFACTOR®

nic