NIC

2019

Artificial Edition

6-8 February

Secure Azure Network Architecture

Aidan Finn, MVP
Innofactor Norway

About Aidan Finn

- 11 year MVP – currently Microsoft Azure
- Principal Consultant for Innofactor Norway
- Working as consutlant/sys admin since 1996
  - Windows Server, Hyper-V, System Center, desktop managment, and Azure

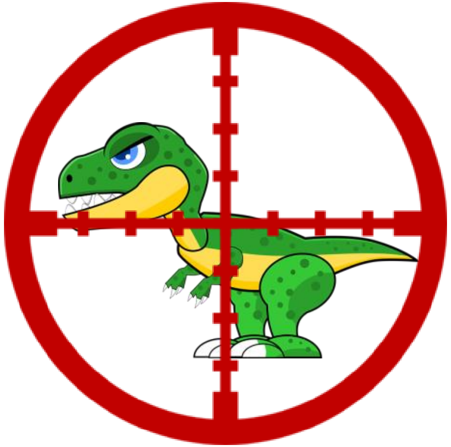
- http://aidanfinn.com
- http://petri.com
- @joe_elway

What We Will Cover

- Virtual network (VNet) basics – really quickly
- Virtual Machine NICs
- Service Endpoints
- Public IP Addresses
- Azure load balancer
- Network Security Groups
- (Azure) Web Application Firewall
- (Third-party) Network virtualisation appliances
- Azure Firewall
- VNet Peering

Caution!

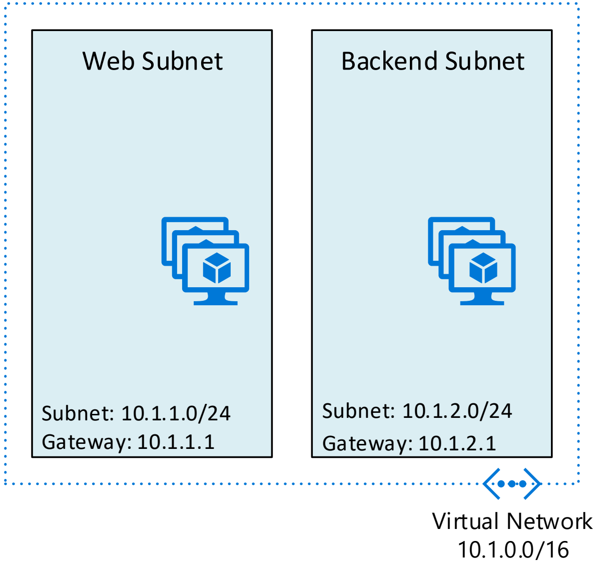
- The topics in this session focus on Azure Resource Manager (ARM)
- If you are using Azure Service Management (ASM / Classic)
  - None of this applies to you
  - Are you still listening to Vanilla Ice?



Virtual Network Basics

A Virtual Network (VNet)

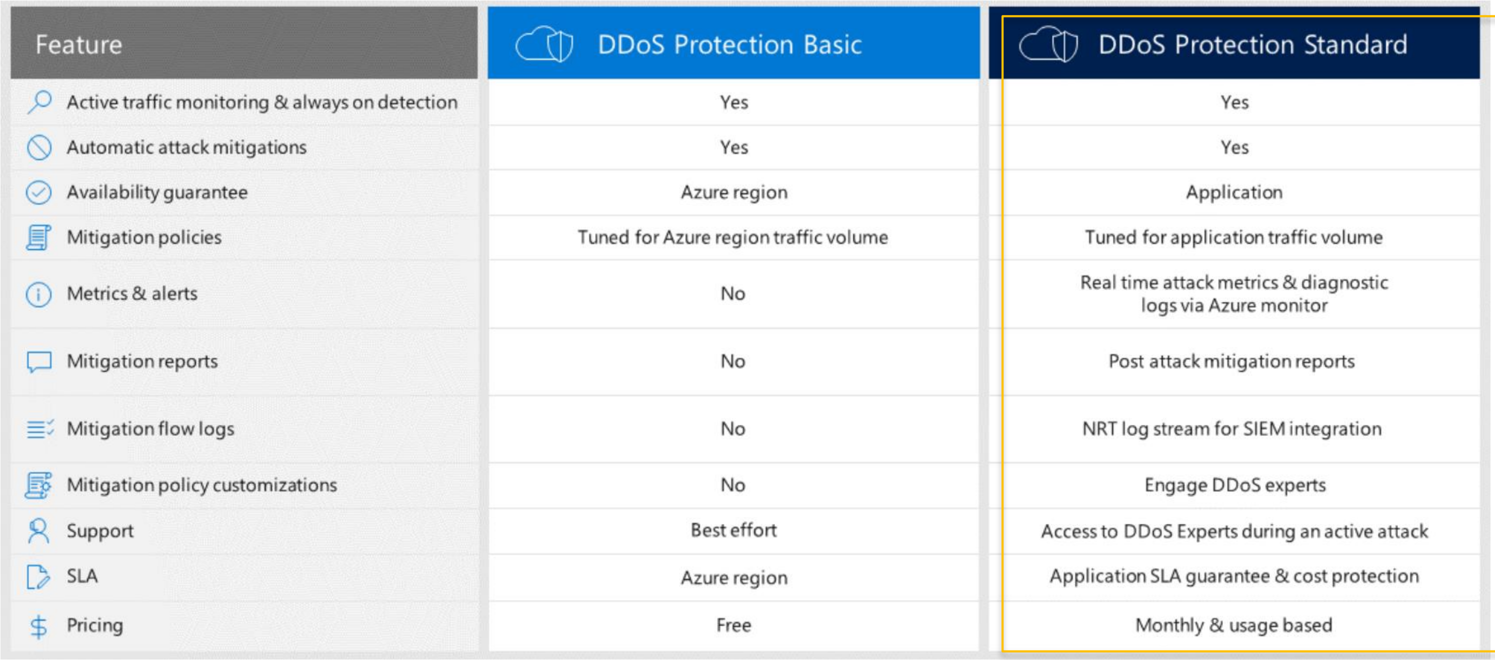
- Software defined (NVGRE)
- Isolated from all other VNets
- Network address
  - Primary scope of all possible subnet addresses
- Subnets
  - Division of VNet network address
  - Automatic unrestricted routing inside the VNet
  - First IP is the gateway/router
  - Once the packet hits the network, Azure takes over



Not Just an IaaS VM Thing

- VNets bring:
  - Isolation
  - Self-service control
  - Industry & regulatory compliance
- Used by more than just VMs:
  - Service Fabric
  - App Services (preview) and App Service Environment
  - Containers

DDoS Protection



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 region traffic 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
Mitigation policy customizations	No	Engage DDoS experts
Support	Best effort	Access to DDoS Experts during an active attack
SLA	Azure region	Application SLA guarantee & cost protection
Pricing	Free	Monthly & usage based

Recommended: Edge Networks

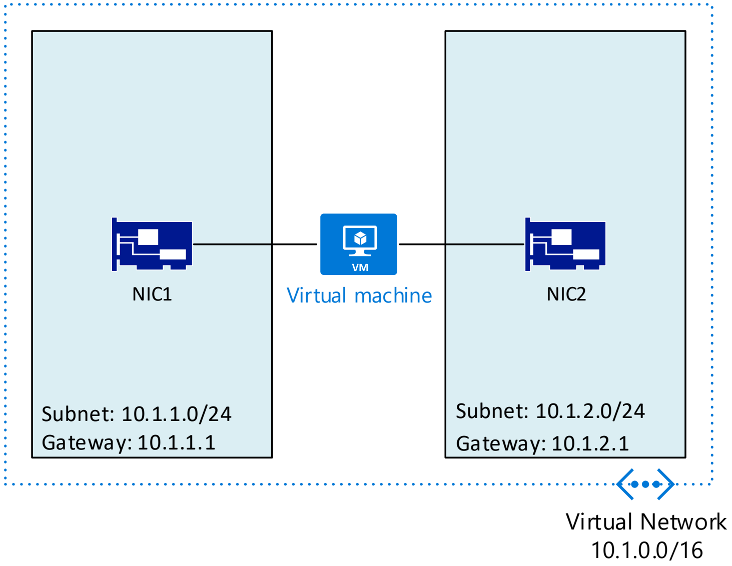
Virtual Machine NICs

VMs, NICs, VNets, and Subnets

- A virtual machine must have 1 NIC (at least)
- VMs connect to a subnet using a virtual network interface (NIC)
  - VM -> NIC -> Subnet [VNet]
- The NIC gets IPv4 configuration from the subnet/VNet
  - Uses the terms of DHCP but it isn’t DHCP
  - No broadcasts in Azure VNets
- NIC maximum speed determined by VM series/size
  - Relevant later!

Multiple NICs

- A VM can have multiple NICs
  - Not usually done for normal server workloads
  - Guest OS teaming not required / not supported
- Each NIC must connect to *different* subnets
  - Each subnet must be in the *same* VNet
- A NIC can change subnets
  - Cannot change VNets



Service Endpoints

Private Access to Azure Services

- By default, Azure Services are accessed from the VM:
  - Via the virtual network
  - Through the “public” Azure backbone
- Possible issues:
  - People concerned with “cloud security”
  - Regulatory/industrial certification
  - Indirect routing

Service Endpoints

- Provides direct connection to Azure platform through the subnet
    - Private connection
    - Lower latency
- Enabled in the VNet subnet
    - Per service, e.g. Azure.SQL
    - Per service/region, e.g. Azure.SQLWestEurope
- Supplemented by firewall functionality in the platform

Public IP Addresses

What is a Public IP Address (PIP)?

- An Azure-managed address on the Internet
  - Static: Preferred
  - Dynamic: Some Azure services require this
- Can have an Azure-managed DNS name

VMs & PIP

- When a virtual machine has a PIP
  - Actually, the NIC has a PIP
- The default configuration:
  - Azure Portal: Next > Next > Next > Create [Lazy]
- Not recommended
  - Use some other means to publish machines to the Internet
  - Possible exception is a “bastion host” or “jump box”

Azure Load Balancer

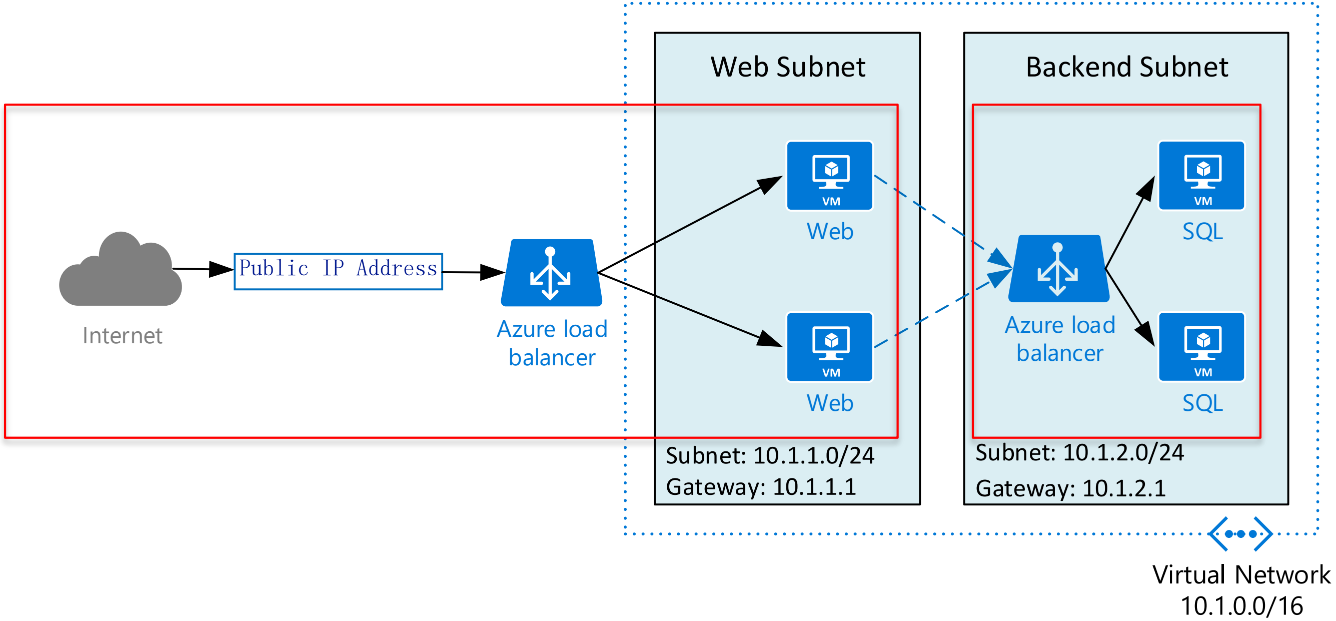
What is the Azure Load Balancer?

- Simple method for redirecting TCP/UDP traffic
- Can be used for:
  - Load balancing at Layer-4
  - NAT rules
- Tiers:
  - Basic: Free, Active/Passive flows
  - Standard: Paid for, Active/Active flows (HA Ports)

Load Balancer Deployments

- Backend Pool
  - Set of load balanced virtual machines
- Probe
  - Test availability of backend pool members
- Rules:
  - NAT and/or load balancing
- Addressing:
  - Internal: consumes an address from the subnet
  - External: associated with a public IP address

Internal & External Load Balancers



Network Security Groups

What are Network Security Groups (NSGs)?

- A free Azure resource type
- Foundational network security in Azure VNets
  - Not just VMs
  - Remember PaaS services are using VNets now!
- Layer-4 security
  - TCP
  - UDP
  - “Any”
- Used in all security designs

NSG Rules

- An NSG resource contains:
  - Inbound rules
  - Outbound rules
- Deny or allow traffic

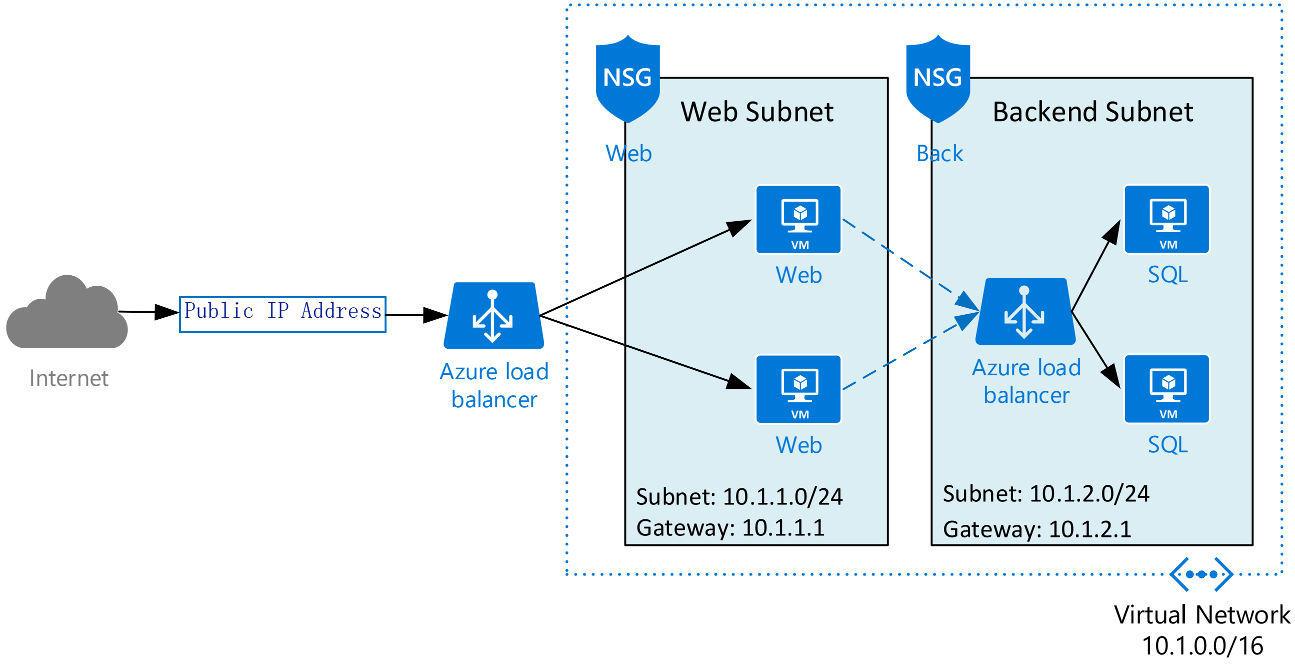
NSG Rule Properties

Source	Any | Address | CIDR block | Service Tag
Source Port	* | Port | Port Range
Destination	Any | Address | CIDR block | Service Tag
Destination Port	* | Port | Port Range
Protocol	TCP | UDP | Any
Action	Deny | Allow
Name	
Priority	1 – 4096

NSG Associations

Method	Inbound Rules	Outbound Rules	Comment
Per NIC	Entering NIC	Leaving NIC	Not scalable
Per Subnet	Entering subnet, incl. member NICs	Leaving subnet	Strongly Recommended

NSG Association Example



Default NSG Rules

- Inbound:
  - Allow Azure Load Balancer probe tests
  - Allow all traffic from the VNet
  - Deny everything from outside the VNet
- Outbound:
  - Allow everything out

Building Rules – Inbound Example

Priority	Source	Source Port	Destination	Destination Port	Protocol	Action	Name
4096	Any	*	10.1.1.0/24	Any	Any	Deny	DenyAll

Building Rules – Inbound Example

Priority	Source	Source Port	Destination	Destination Port	Protocol	Action	Name
100	192.168.1.0/24	*	10.1.1.0/24	80	TCP	Allow	AllowHTTP
4096	Any	*	10.1.1.0/24	Any	Any	Deny	DenyAll

Building Rules – Inbound Example

Priority	Source	Source Port	Destination	Destination Port	Protocol	Action	Name
100	192.168.1.0/24	*	10.1.1.0/24	80	TCP	Allow	AllowHTTP
200	192.168.1.0/24	*	10.1.1.0/24	443	TCP	Allow	AllowHTTPS
4096	Any	*	10.1.1.0/24	Any	Any	Deny	DenyAll

Building Rules – Inbound Example

Priority	Source	Source Port	Destination	Destination Port	Protocol	Action	Name
100	192.168.1.0/24	*	10.1.1.0/24	80	TCP	Allow	AllowHTTP
200	192.168.1.0/24	*	10.1.1.0/24	443	TCP	Allow	AllowHTTPS
4090	AzureLoadBalancer	*	10.1.1.0/24	Any	Any	Allow	AllowProbe
4096	Any	*	10.1.1.0/24	Any	Any	Deny	DenyAll

Building Rules – Outbound Example

Priority	Source	Source Port	Destination	Destination Port	Protocol	Action	Name
4096	Any	*	Any	*	Any	Deny	DenyAll

Service Tags

- Labels for services
  - Use a name instead of huge range of addresses
- Common ones:
  - Internet: Everything outside the *VNet*, including Azure!
  - VirtualNetwork: Everything inside the virtual network – more on this later!
  - AzureLoadBalancer: The probe of the Basic/Standard load balancer
- Azure services:
  - Worldwide
  - Region specific

Building Rules – Outbound Example

Priority	**Source**	**Source Port**	**Destination**	**Destination Port**	**Protocol**	**Action**	**Name**
100	10.1.1.0/24	*	Azure.StorageWestEurope	*	Any	Allow	AllowAzureStorageWestEurope
4096	Any	*	Any	*	Any	Deny	DenyAll

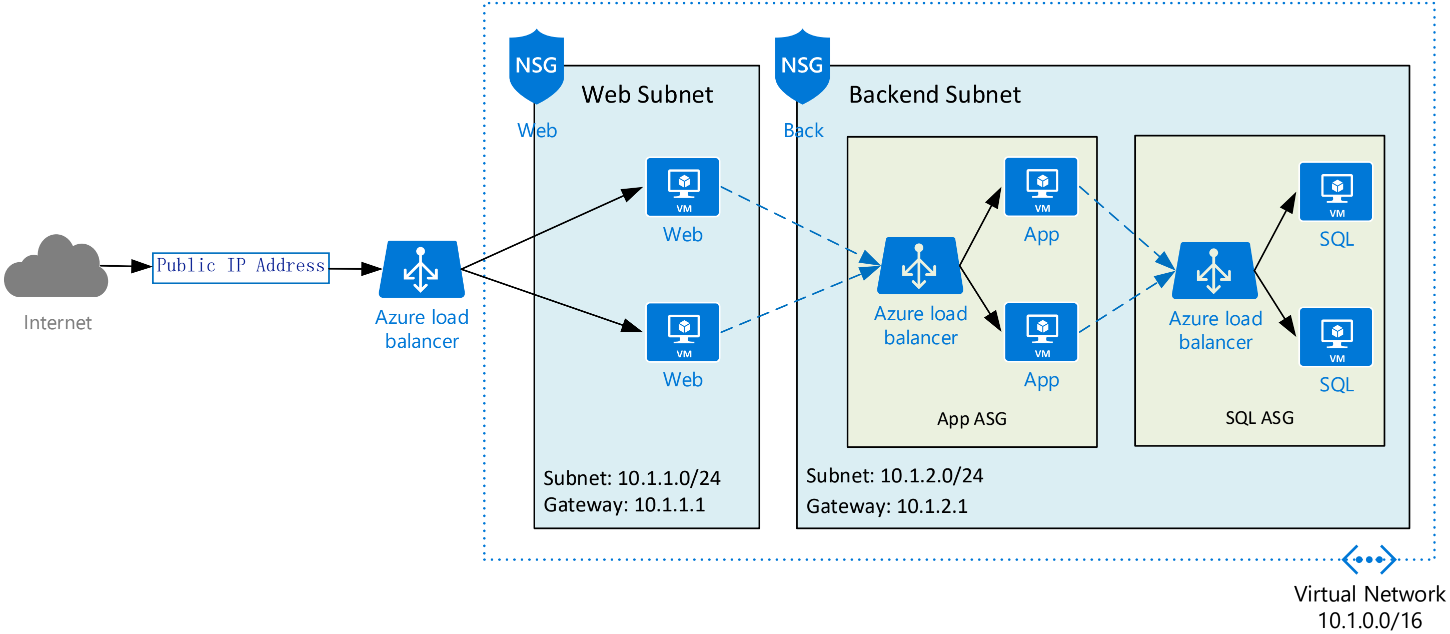
Classic NSG Best Practice

- Practice:
  - 1 subnet per service tier
  - 1 NSG per subnet
- Reality:
  - A service could have many tiers: RDGW, RDCB, RDSH, App, Storage, Web, Database, Management, Security, etc
  - Complex virtual networks & security
  - Difficult to troubleshoot traffic flows across NSGs

Application Service Groups (ASGs)

- Group VM NICs together
  - Web NICs
  - App NICs
  - Database NICs
- Deploy fewer subnets / NSGs
  - Example: edge & backend
- Use ASGs in NSG rules as source/destination addresses

Application Service Groups (ASGs)



Example Rules with ASGs

Priority	Source	Source Port	Destination	Destination Port	Protocol	Action	Name
100	10.1.1.0/24	*	AppASG	443	TCP	Allow	AllowWebApp
200	AppASG	*	SqlASG	1433	TCP	Allow	AllowAppSql
4080	SqlASG	*	SqlASG	*	Any	Allow	AllowSqlClu
4090	AzureLoadBalancer	*	10.1.2.0/24	Any	Any	Allow	AllowProbe
4096	Any	*	10.1.2.0/24	Any	Any	Deny	DenyAll

Web Application Firewall

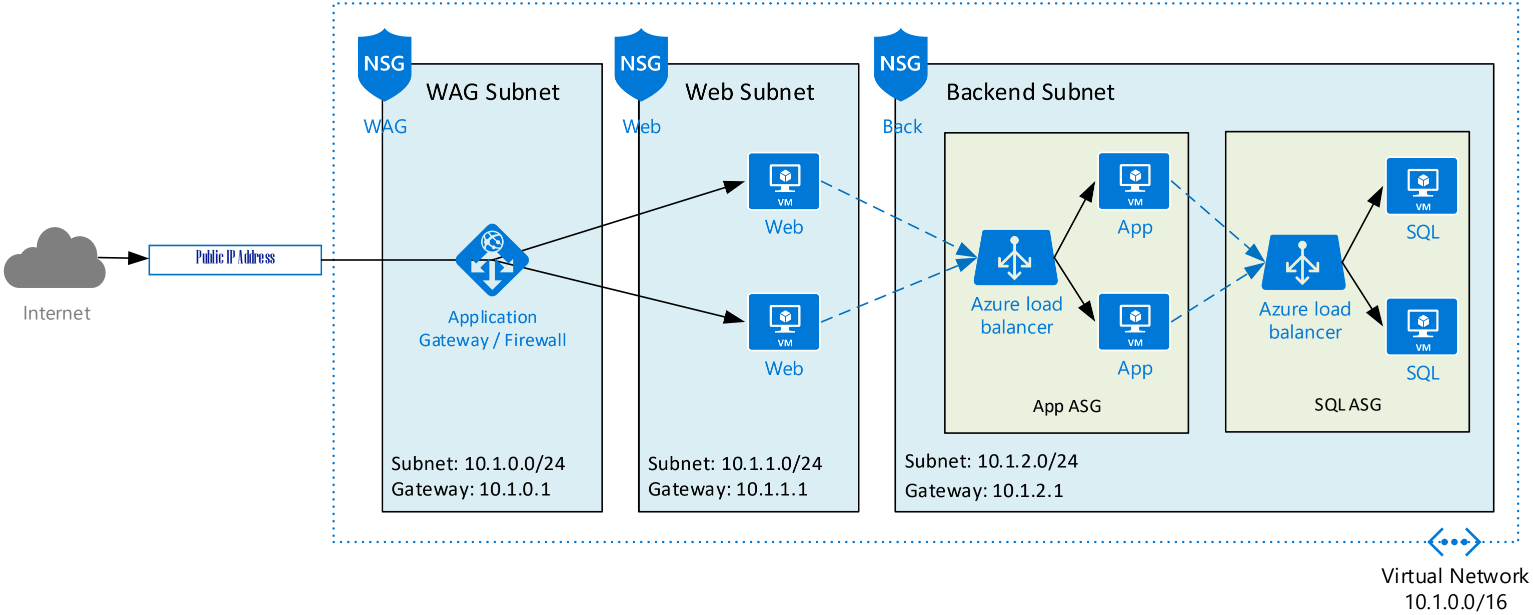
Web Application Gateway (WAG)

- A paid-for Azure resource
    - Paid for instances add more capacity/bandwidth
- Provides Layer-7 load balancing for HTTP/S (only) services
- Including:
    - SSL offload
    - End-to-end encryption
    - Multi-site hosting (single PIP)
    - URL redirection
    - Cookie-based affinity

Web Application Firewall (WAF)

- Additional feature/cost for the WAG
- Adds Layer-7 security
  - Detect-only (Default)
  - Protection
- Based on OWASP 3.0 or 2.2.9
  - All rules enabled by default
  - Individual rules can be disabled

Web Application Firewall (WAF)



Route Tables

Default Routes

- Azure fabric takes *complete* control over routing
  - Guest OS cannot override
- Subnet:
  - All traffic routes via the default gateway
- Virtual Machines -> outside world via:
  - Public IP address
  - Azure load balancer
  - Gateway for VPN/ExpressRoute

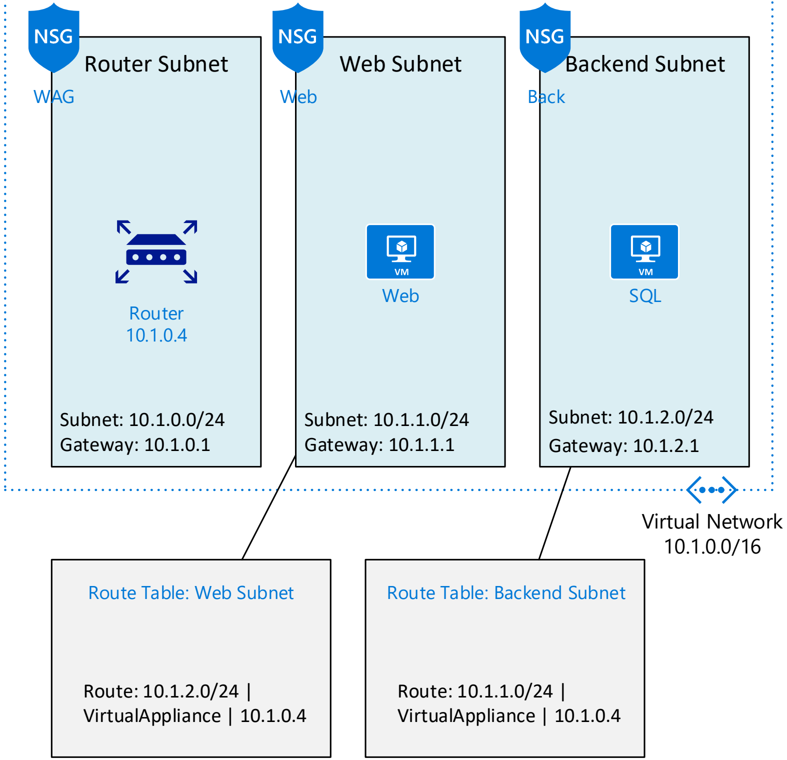
Route Table

- Take control of Azure routing
- Uses a free resource called a Route Table
  - Associated with subnets
- Routes:
  - Destination address: 0.0.0.0/0, 10.0.0.0/8, 10.1.2.0/24
  - Destination type: Virtual Network Gateway, Virtual Network, Internet, None, Virtual Network Peering, Virtual Service Endpoint, Virtual Appliance
  - IP Address: For virtual appliances

Route Paths

- Inside a subnet:
  - Packets route directly between source & destination
- Inside a VNet:
  - Packets route directly between source & destination
- Using a virtual appliance:
  - Packets can be routed through the appliance
- Note:
  - Default direct routes are higher priority than 0.0.0.0/0

Routing Abstract



Router Subnet

Router
10.1.0.4

Subnet: 10.1.0.0/24
Gateway: 10.1.0.1

Web Subnet

Web

Subnet: 10.1.1.0/24
Gateway: 10.1.1.1

Backend Subnet

SQL

Subnet: 10.1.2.0/24
Gateway: 10.1.2.1

Virtual Network
10.1.0.0/16

Route Table: Web Subnet

Route: 10.1.2.0/24 |
VirtualAppliance | 10.1.0.4

Route Table: Backend Subnet

Route: 10.1.1.0/24 |
VirtualAppliance | 10.1.0.4

Network Virtualization Appliances

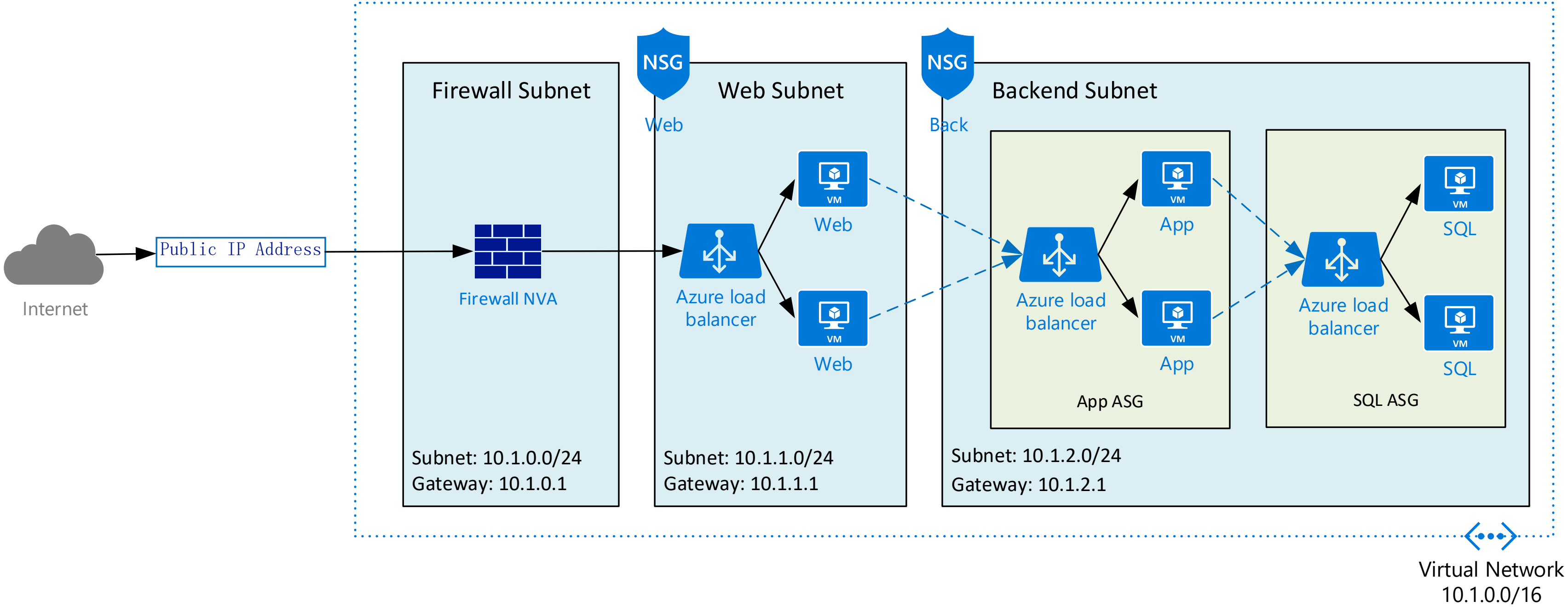
Network Virtualization Appliances (NVAs)

- Made up of:
  - Linux virtual machine (compute cost)
  - Network appliance software (additional cost)
- Deployed from Marketplace – certified for Azure
- Payment:
  - Bring your own license (BYOL)
  - Per-minute usage (not CSP subscriptions today)
- Firewalls, routers, load balancers, network optimization, etc

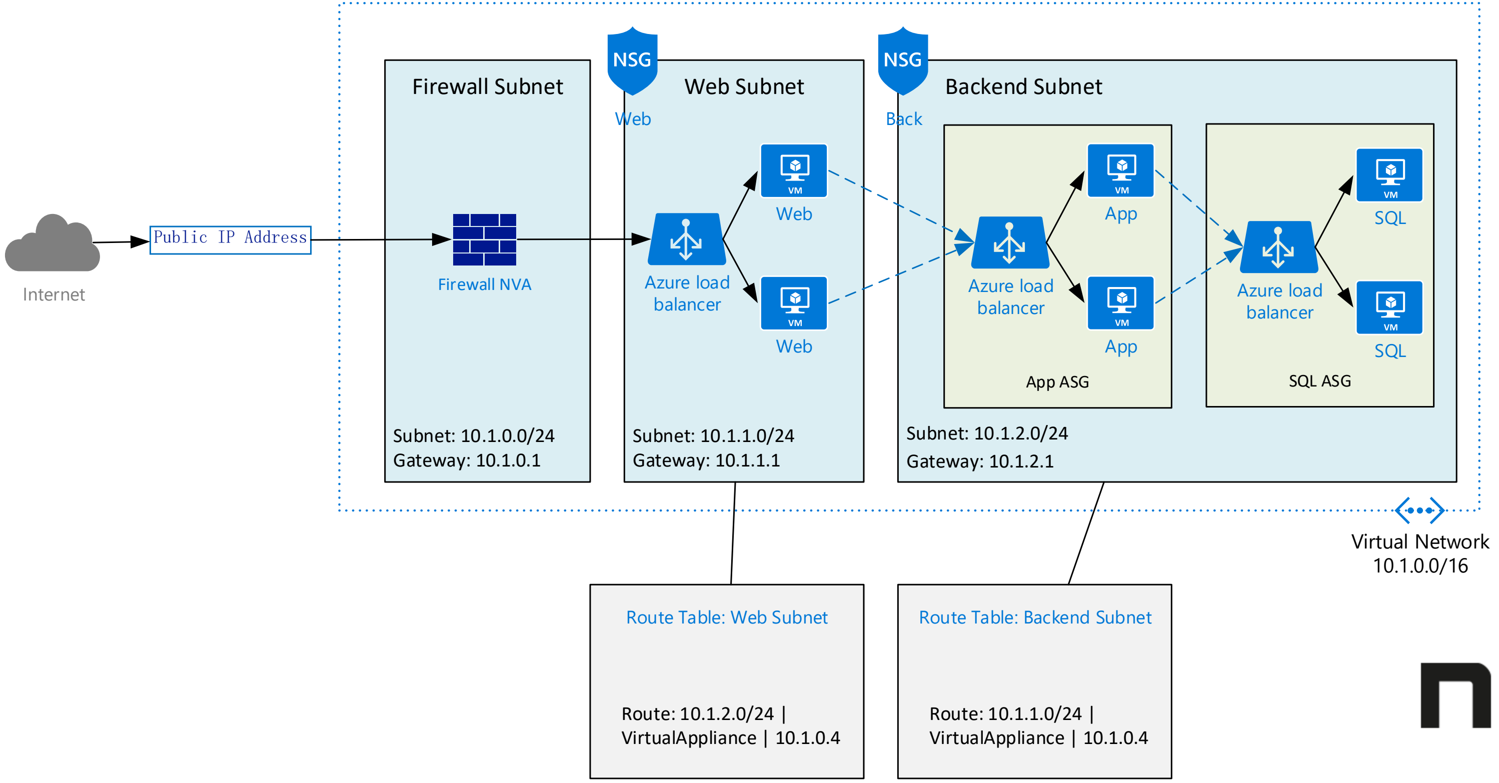
Performance Notes

- Spec of VM: CPU (Azure Compute Units/ACUs) and NIC speed
- Enable Network Acceleration (depends on VM guest OS/series/size)
- Number of VMs

Firewall NVA Example



Micro-Segmentation



Internet

Public IP Address

Firewall Subnet

Firewall NVA

Subnet: 10.1.0.0/24
Gateway: 10.1.0.1

NSG
Web

Web Subnet

Azure load balancer

Web

Web

Subnet: 10.1.1.0/24
Gateway: 10.1.1.1

NSG
Back

Backend Subnet

Azure load balancer

App

App

App ASG

Azure load balancer

SQL

SQL

SQL ASG

Subnet: 10.1.2.0/24
Gateway: 10.1.2.1

Virtual Network
10.1.0.0/16

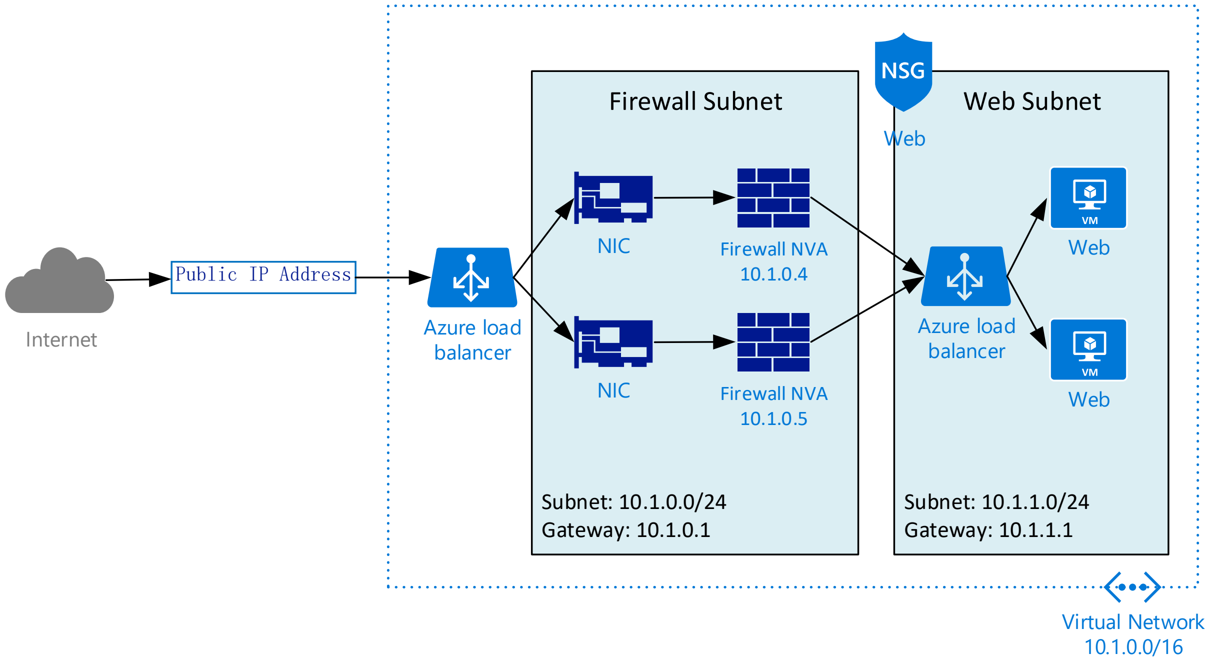
Route Table: Web Subnet

Route: 10.1.2.0/24 |
VirtualAppliance | 10.1.0.4

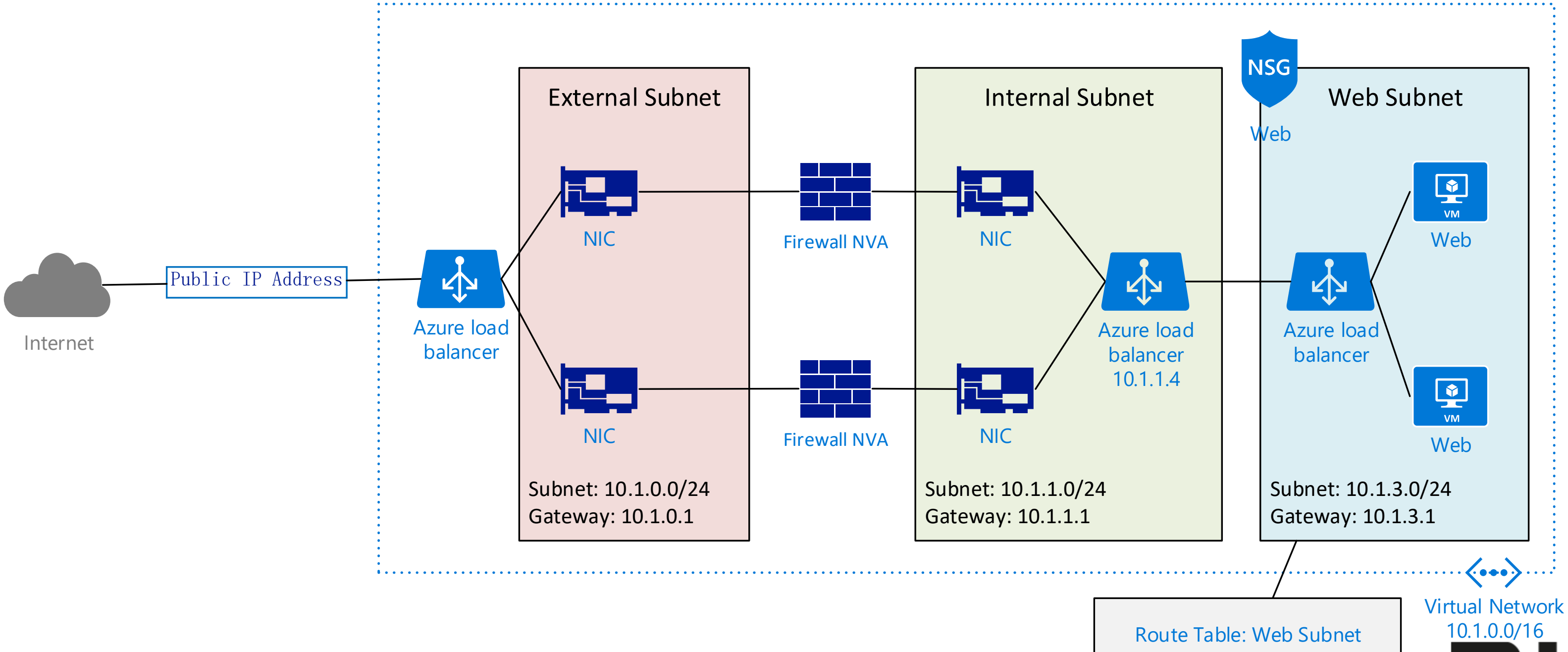
Route Table: Backend Subnet

Route: 10.1.1.0/24 |
VirtualAppliance | 10.1.0.4

Firewall Clusters



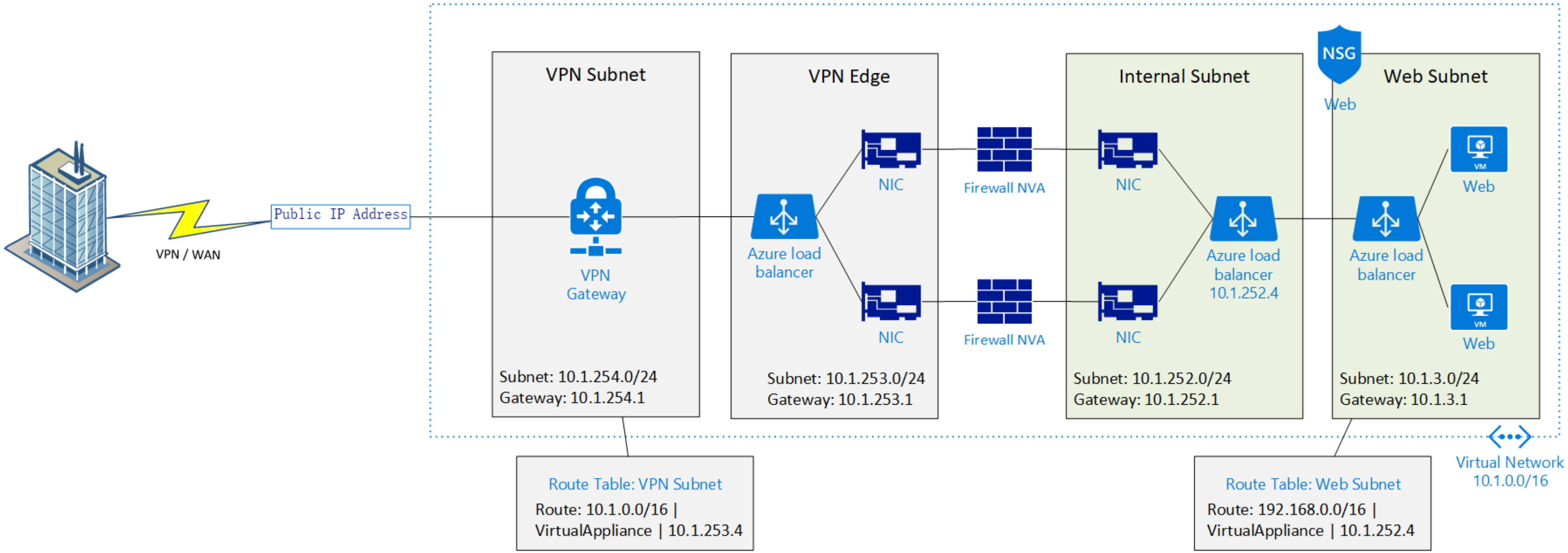
Egress Inspection & Micro-Segmentation



Route Table: Web Subnet

Route: 0.0.0.0/0 |
VirtualAppliance | 10.1.1.4

Secure VPN Access



Azure Firewall

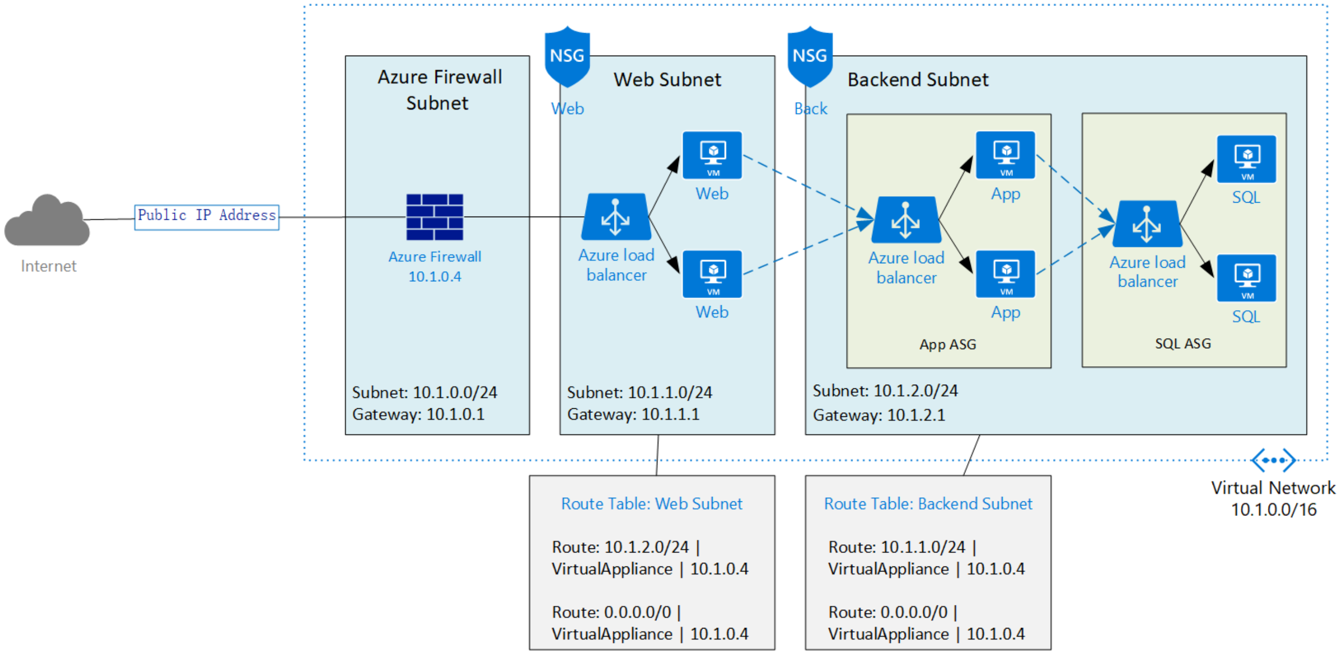
Firewall-as-a-Service

- Platform solution from Azure
- Logging
- Filtering:
  - NAT: For external->internal access
  - Network Rules: Internal->internal traffic
  - Application Rules: HTTP/S

Azure Firewall Versus NVA

	Azure Firewall	**NVA**
Deployment	Platform	Linux VM + Software
Licensing	Consumption: instance + GB	Linux VM + Software
Scaling	Automatic	Add VMs + Software
Ownership	Set & monitor	Manage VM / OS / Software
Layer -7	Logging & filtering	Potentially deep inspection

Azure Firewall Example



Internet

Public IP Address

Azure Firewall Subnet

Azure Firewall
10.1.0.4

Subnet: 10.1.0.0/24
Gateway: 10.1.0.1

NSG
Web

Web Subnet

Azure load balancer

Web

Web

Subnet: 10.1.1.0/24
Gateway: 10.1.1.1

NSG
Back

Backend Subnet

Azure load balancer

App

App

App ASG

Azure load balancer

SQL

SQL

SQL ASG

Subnet: 10.1.2.0/24
Gateway: 10.1.2.1

Virtual Network
10.1.0.0/16

Route Table: Web Subnet

Route: 10.1.2.0/24 |
VirtualAppliance | 10.1.0.4

Route: 0.0.0.0/0 |
VirtualAppliance | 10.1.0.4

Route Table: Backend Subnet

Route: 10.1.1.0/24 |
VirtualAppliance | 10.1.0.4

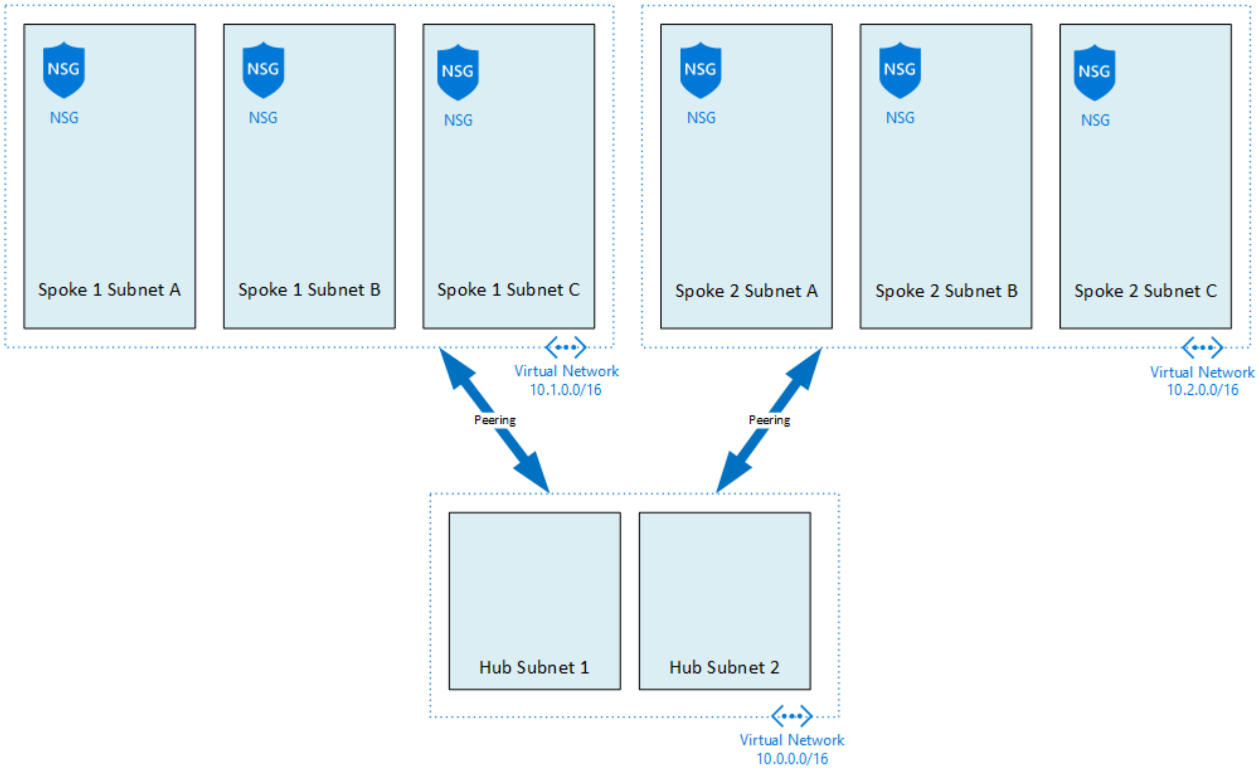
Route: 0.0.0.0/0 |
VirtualAppliance | 10.1.0.4

VNet Peering

VNet Connectivity

- Join VNets together
  - 2 joined NSGs are 1 “VirtualNetwork” in an NSG
- Simple solution:
  - Requires both admins to do it
  - Cross-subscription
- Enables more granular designs:
  - Cost centers
  - Governance
  - Ownership
  - Resource re-use

Hub & Spoke

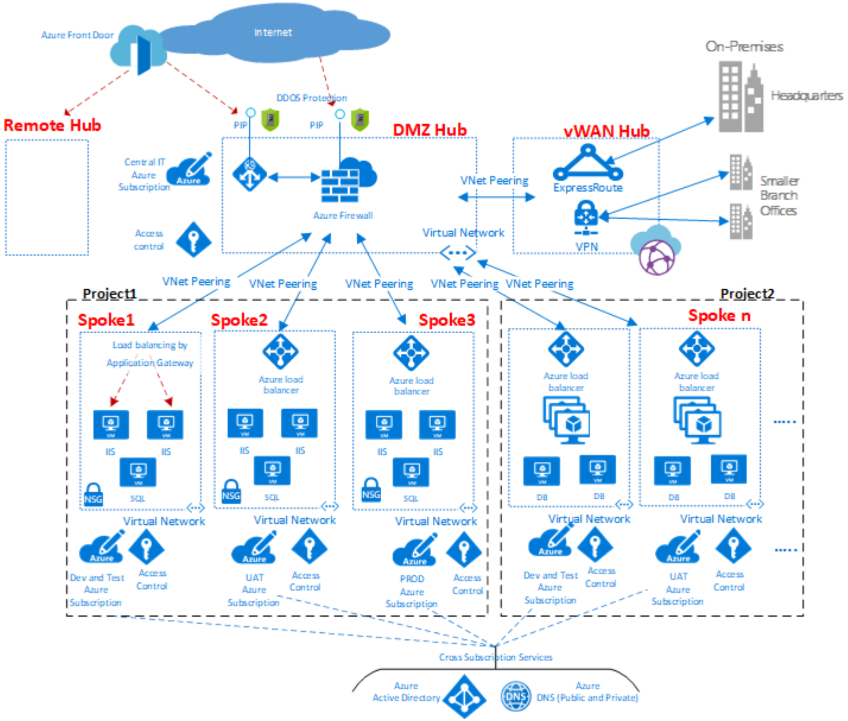

NSG
NSG
Spoke 1 Subnet A
NSG
NSG
Spoke 1 Subnet B
NSG
NSG
Spoke 1 Subnet C
NSG
NSG
Spoke 2 Subnet A
NSG
NSG
Spoke 2 Subnet B
NSG
NSG
Spoke 2 Subnet C
Virtual Network
10.1.0.0/16
Virtual Network
10.2.0.0/16
Peering
Peering
Hub Subnet 1
Hub Subnet 2
Virtual Network
10.0.0.0/16

Virtual Data Center

Putting It All Together

- A design reference
- Uses:
  - All the pieces we have discussed
  - Good security & governance practices
- Adapt as required
- https://docs.microsoft.com/azure/architecture/vdc/networking-virtual-datacenter

Sample Virtual Data Center



Some Thoughts

My Comments

- Get to know the components
- Routing & NSGs are critical:
  - Knowledge, naming standards, governance
  - Remember to associate w/ subnets!
- Hub & Spoke recommended:
  - Re-use expensive resources versus cost of peering
  - Stick to hub/spoke
  - Hub/sub-hub/spoke will have horrible routing
- Micro-segmentation
  - Do you need it every where?
  - Consider security zones – let NSGs do all internal filtering

The End

MVP
Microsoft®
Most Valuable
Professional

Thank you!

Aidan Finn

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

INNOFACTOR®

NIC