Securing Azure Virtual Networks

Mike Brown
SENIOR CLOUD INSTRUCTOR

@mgbleeds

Overview

Learn about network security groups (NSGs)

Demonstrate NSGs

Learn about application security groups

Demonstrate application security groups

Discuss

- Globomantics security group requirements
- Highlight areas where security groups can help secure your Azure deployments

Plan your security with defense-in-depth at its heart

Defense-in-depth

Physical security

Managed by Microsoft

Identity and access

Managed by you using Azure AD

Perimeter

Standard DDoS protection enabled by default

Network and application

Network security groups, firewalls and gateways

Compute and data

OS security, access control and encryption

Network Security Groups

What Are Network Security Groups (NSGs)?

NSGs filter traffic

NSGs allow or deny inbound and outbound traffic

NSGs contain rules

Rules are ordered based on a number from 100 (processed first) to 4096 (processed last)

Network Security Groups

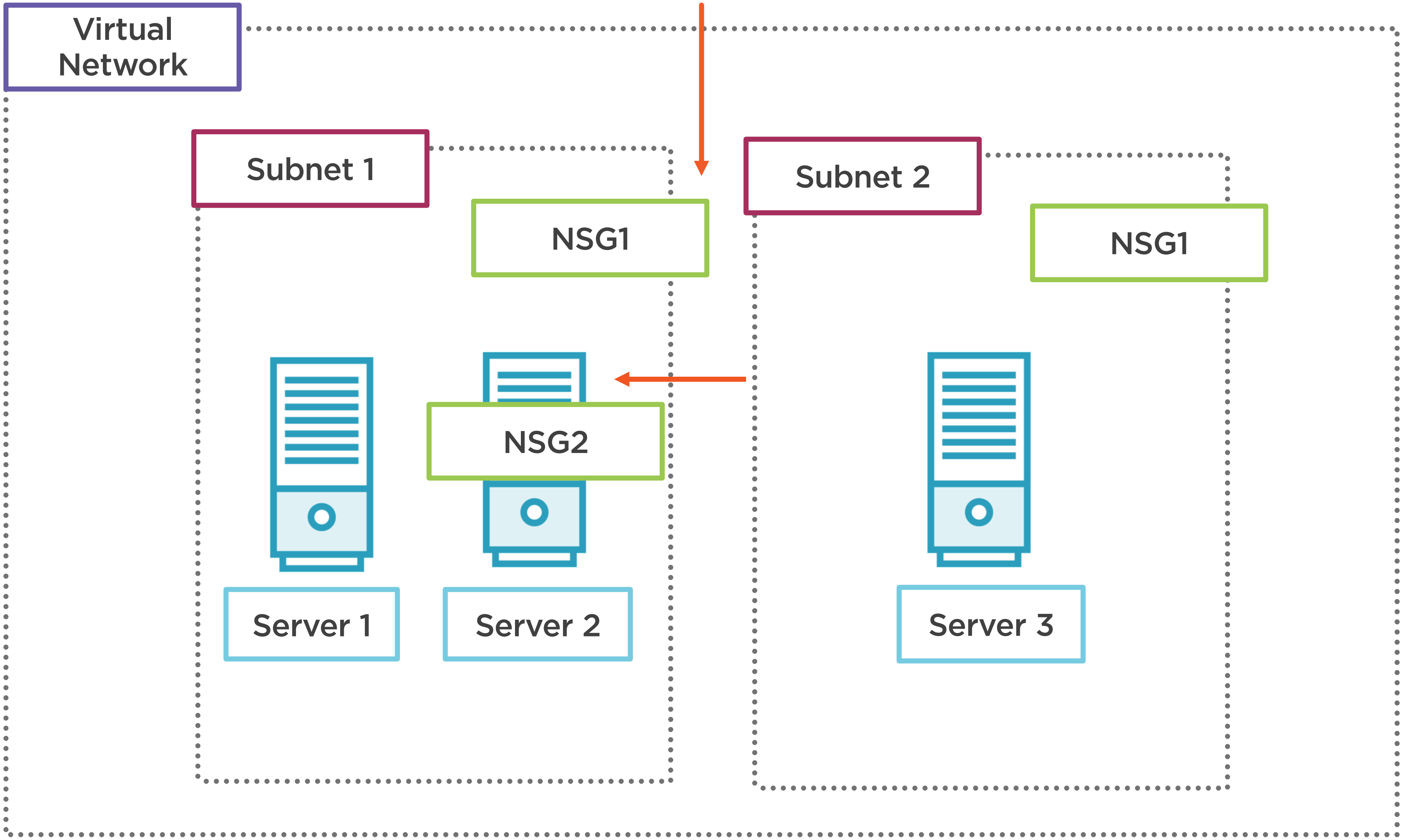
Attached to subnets or network cards

Each NSG can be linked to multiple resources

NSGs are stateful

NSGs properties include

- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action


Virtual Network
Subnet 1
NSG1
Subnet 2
NSG1
NSG2
Server 1
Server 2
Server 3

Globomantics' Requirements

GLOBOMANTICS

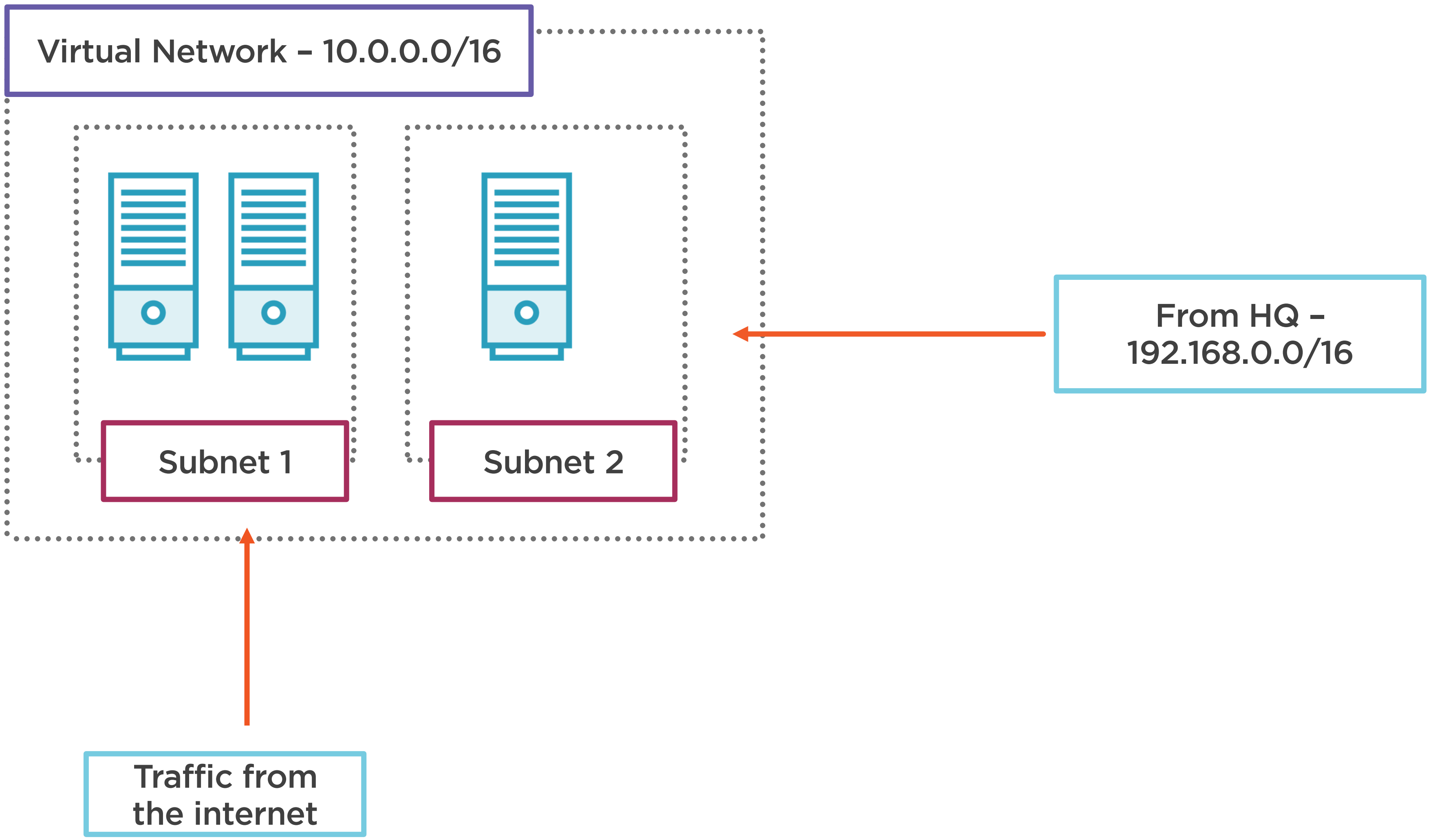
Traffic will flow into Globomantics Azure network from the internet and from Globomantics HQ

Traffic with a destination of TCP port 80 and 443 from the internet should be allowed

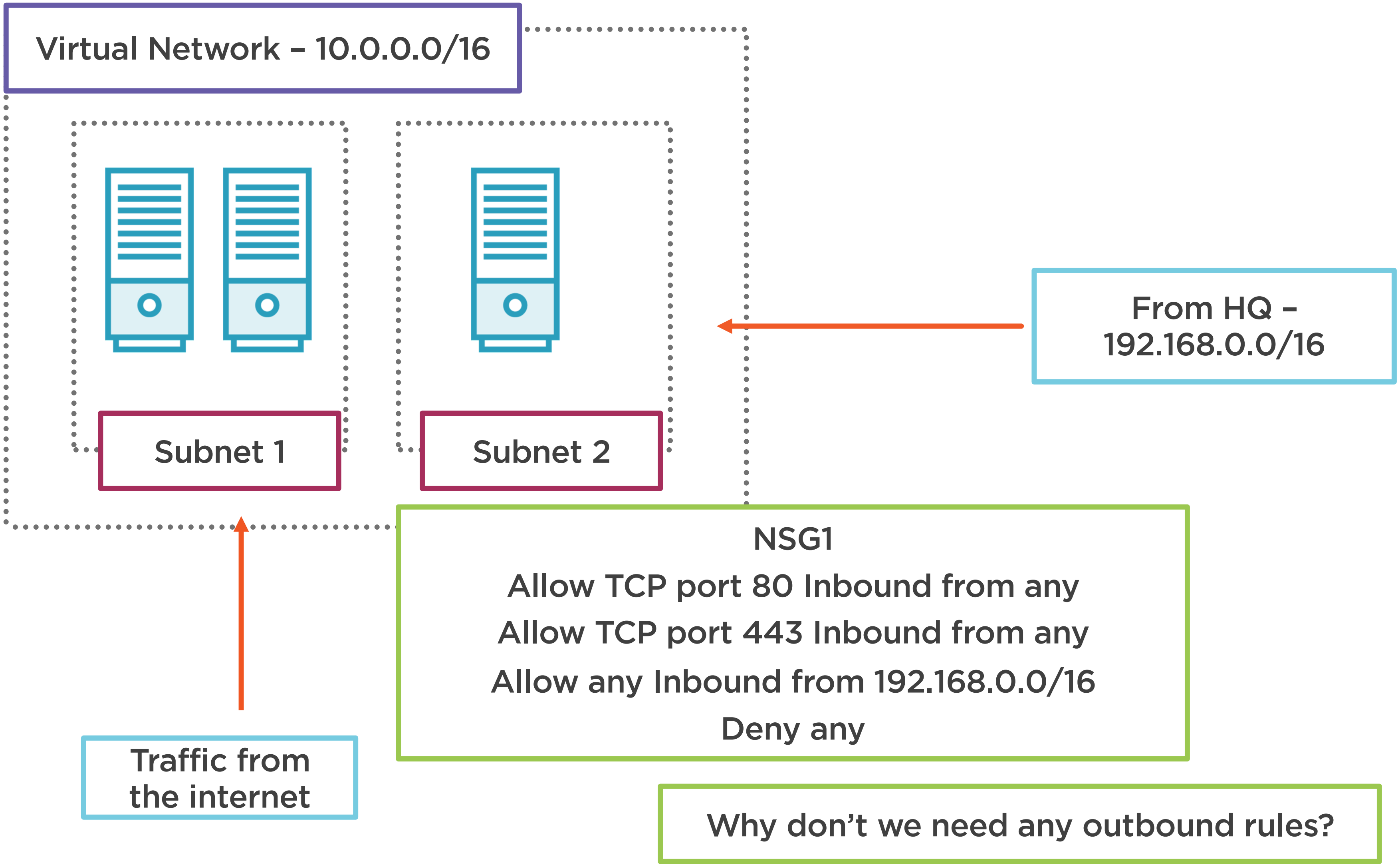
All traffic from Globomantics HQ network should be allowed

Globomantics has asked us to

- Design the network security groups need to allow the correct traffic and deny everything else


Virtual Network – 10.0.0.0/16
Subnet 1
Subnet 2
From HQ – 192.168.0.0/16
Traffic from the internet

Considering Globomantics NSG requirements, what NSGs would you create?



Virtual Network – 10.0.0.0/16

Subnet 1

Subnet 2

From HQ –
192.168.0.0/16

NSG1
Allow TCP port 80 Inbound from any
Allow TCP port 443 Inbound from any
Allow any Inbound from 192.168.0.0/16
Deny any

Traffic from
the internet

Why don’t we need any outbound rules?

Demo

Deploy and test network security groups

Application Security Groups

Problems with Network Security Groups

Can become complex

Can contain lots of rules, the more rules we need the more complex the design

Can be difficult to maintain

If we add more resources, we may need to update several network security groups

Solving Network Security Group Problems

Use service tags

Represent services like Azure load balancer or API management and locations like internet

Use the default security rules

Default security allow and deny common traffic

Use application security groups

Application security groups allow us define a service made up of resources like virtual machines.

What Are Application Security Groups?

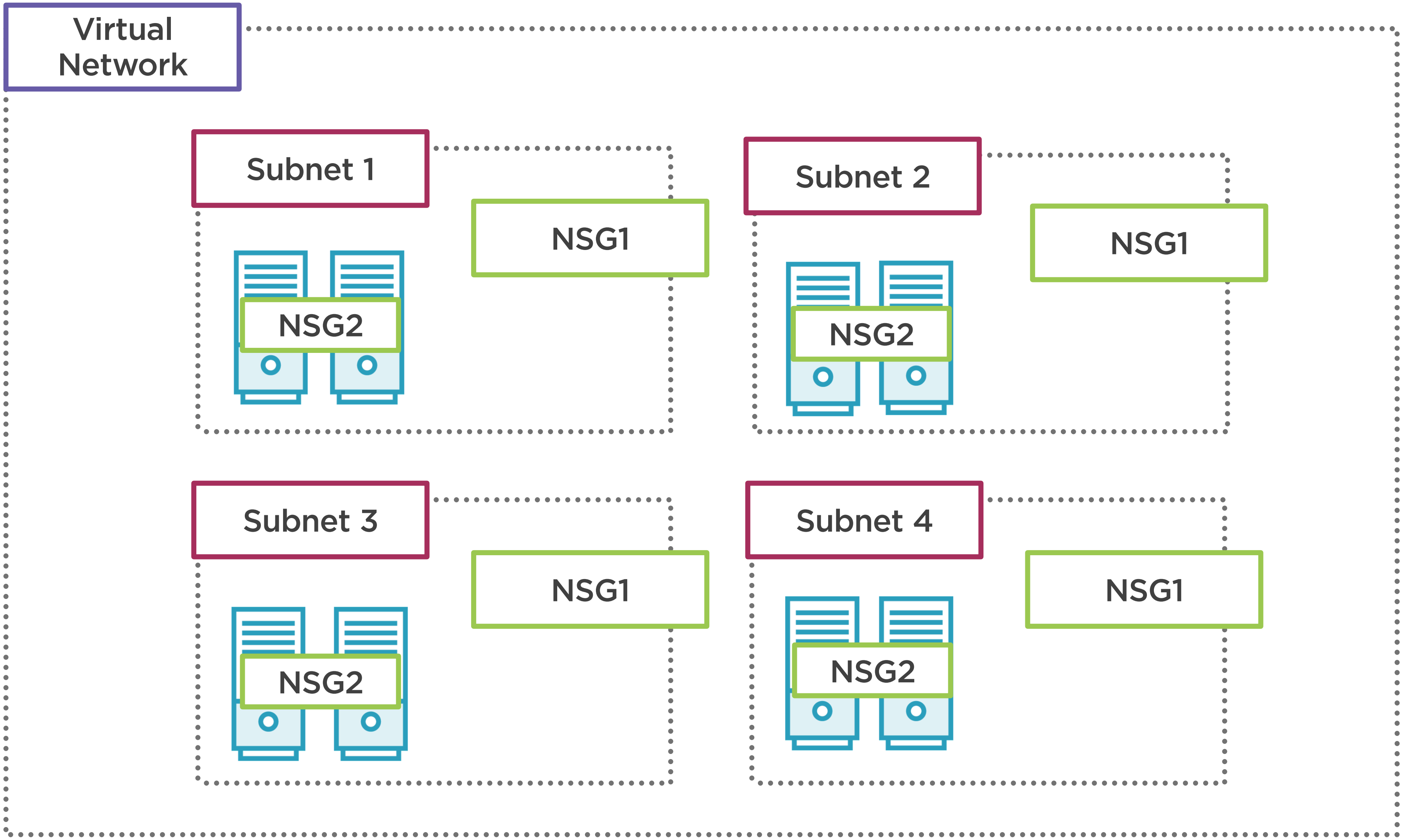
Allows us to reference a group of resources

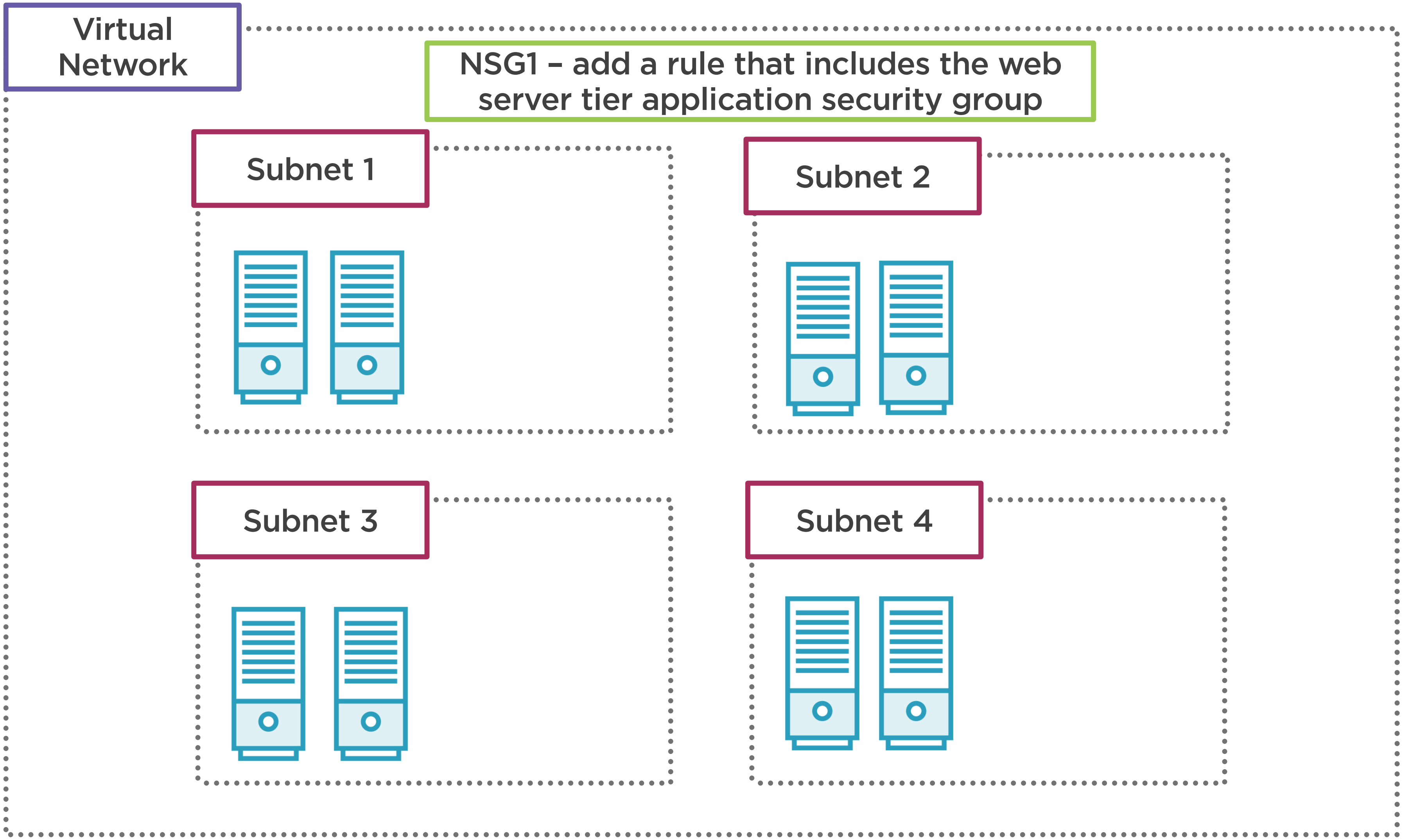
Used as a source or destination in network security groups

Network security groups are still required

Working with application security groups

- Create the application security group
- Link the group to resources
- Use the group when working with network security groups


Virtual Network
Subnet 1
NSG1
NSG2
Subnet 2
NSG1
NSG2
Subnet 3
NSG1
NSG2
Subnet 4
NSG1
NSG2



Virtual Network

NSG1 – add a rule that includes the web server tier application security group

Subnet 1

Subnet 2

Subnet 3

Subnet 4

Think About Your Requirements

N-Tier applications

Each tier would have its own application security groups

DMZ

Resources in your DMZ would be added to their own application security groups

Automation

When automating deployments include application security groups

Demo

Deploy and test application security groups

Summary

Learned the importance of network and application security groups

Learned how to create network and application security groups

Discussed how you could use network and application security groups on your networks

In the next module

- Azure firewalls
- User defined routes
- Choosing an appropriate security solution