Working with Azure Firewalls and User Defined Routes

Mike Brown
SENIOR CLOUD INSTRUCTOR
@mgbleeds

Overview

Discuss Azure firewall and DDoS protection options

Discuss User Defined Routes

Learn about the different firewall protection options available

Understanding of Firewall options

- Leads to a more secure Azure deployment
- Leads to a more cost-effective Azure deployment

Azure Firewall and DDoS

What Is Azure Firewall?

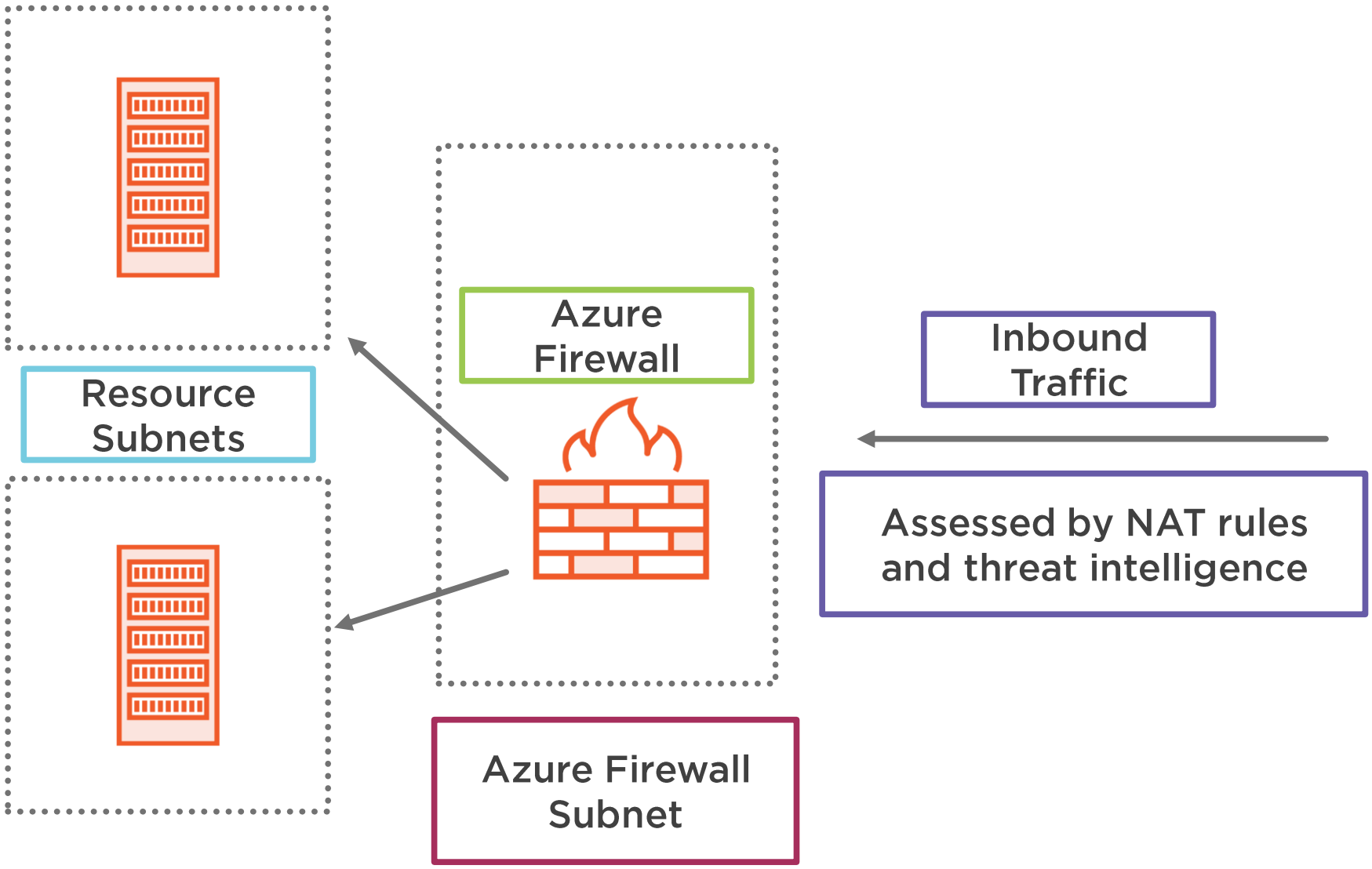
Azure managed stateful firewall service

Protects access to virtual networks

Highly available

Features include

- Threat intelligence
- Outbound and inbound NAT support
- Integration with Azure Monitor
- Network traffic filtering rules
- Unrestricted scalability


Azure Firewall
Resource Subnets
Inbound Traffic
Assessed by NAT rules and threat intelligence
Azure Firewall Subnet

What Is Azure DDoS Protection?

DDoS mitigation for networks and applications

Always-on monitoring

Application layer protection

Integration with Azure monitor

Features offered

- Multi-layered protection
- Attack analytics
- Scale and elasticity
- Protection against unplanned costs

Azure DDoS Service Tiers

Basic

Active traffic monitoring and always on detection

Availability Guarantee

Backed by an SLA

Free

Standard

Everything offered by the basic tier

Real time Metrics

Post attack reports

Access to DDoS experts during and active attack

Security information and event management (SIEM) integration

Monthly fee and usage based

Think About Your Azure Networks

Will you need Azure firewall?

Do you use a network firewall now? What rules will need to configure?

Which DDoS tier will you need?

The Basic tier is free but might not offer the SLA, reporting or response you might need.

Virtual appliances can be deployed to add additional protection

Azure User Defined Routes

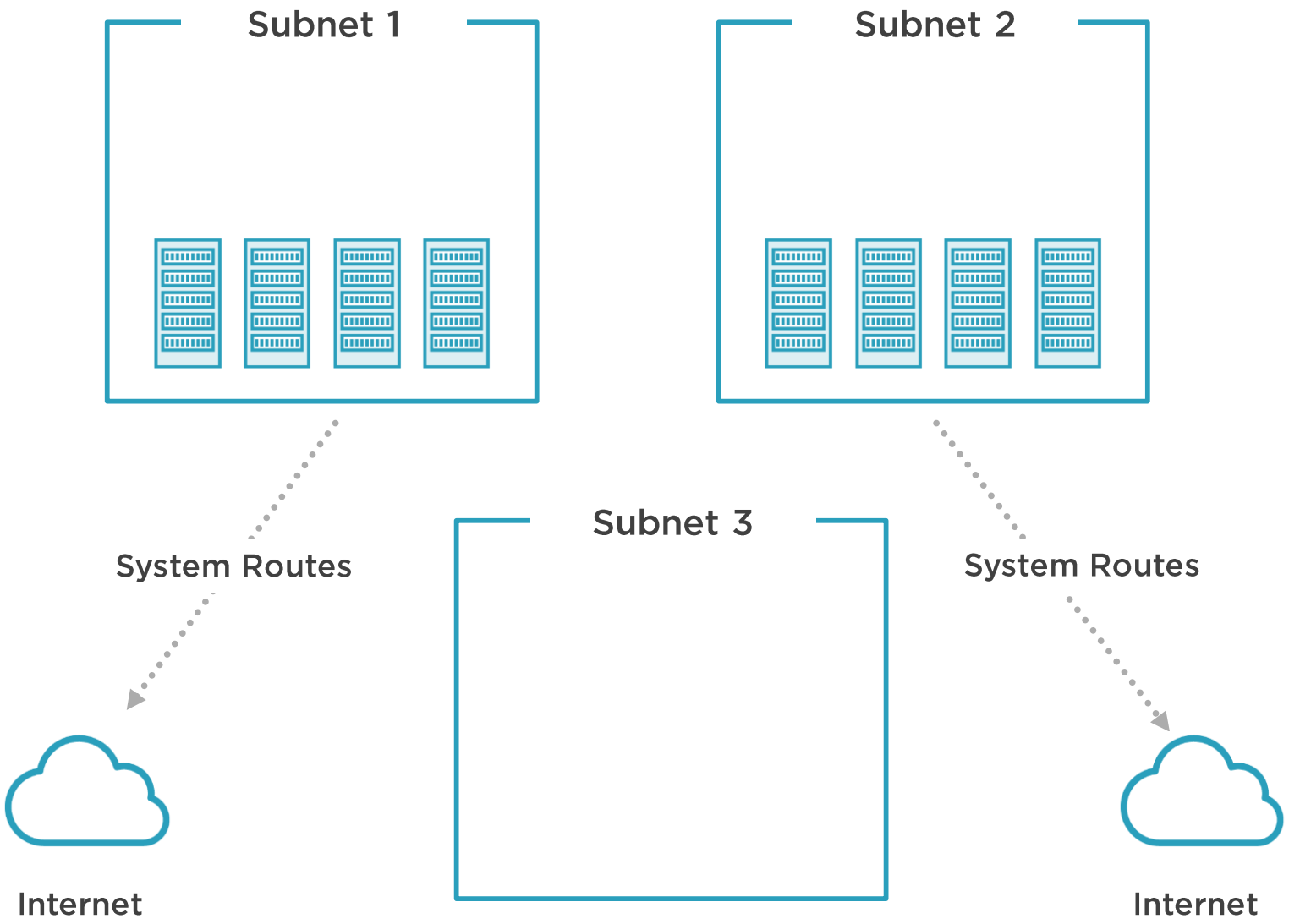
User Defined Routes

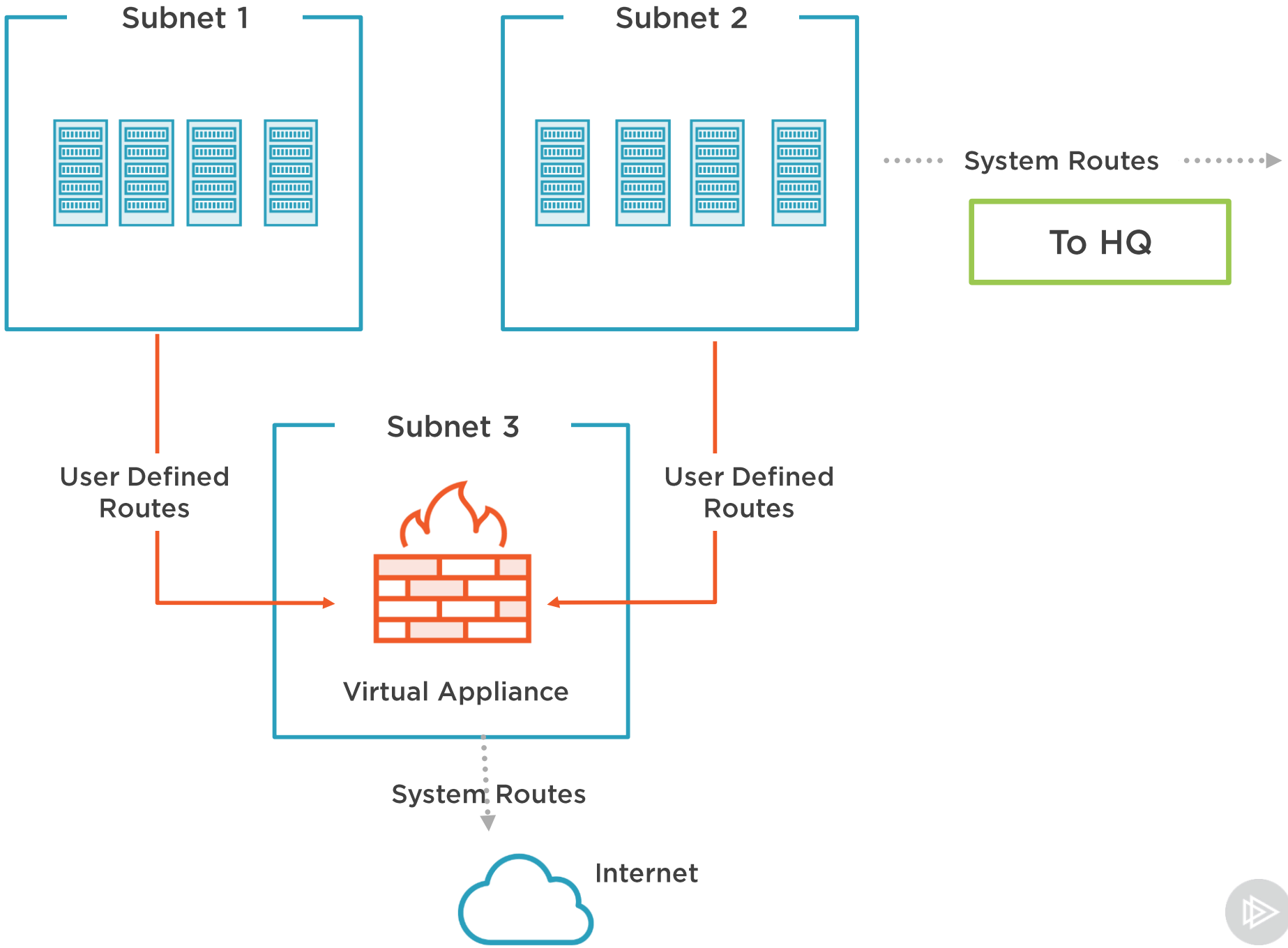
Default system routes are enabled by default

System routes allow routing between subnet and to the internet

User defined routes allow us to override Azure's default system routes

Often used when we want traffic to be filtered through a virtual appliance


Subnet 1
Subnet 2
Subnet 3
System Routes
System Routes
Internet
Internet


Subnet 1
Subnet 2
System Routes
To HQ
Subnet 3
User Defined Routes
User Defined Routes
Virtual Appliance
System Routes
Internet

Azure Security Options

Azure Security Options

Azure firewall	Azure DDoS Protection	Azure web application firewall
Network security groups	Forced tunneling	Marketplace devices

Security Scenarios

Take a minute to think about the scenarios below. Which Azure security options would you choose for each?

Control internet traffic

You wish to control the flow of traffic heading to the internet so that it can be inspected at layer 7.

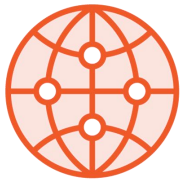
Azure hosted SQL Server

Only traffic from your Azure subnets should be allowed to access your Azure SQL server.

Route internet traffic

All internet bound traffic that is generated by your application servers must be routed through HQ

Security Solutions

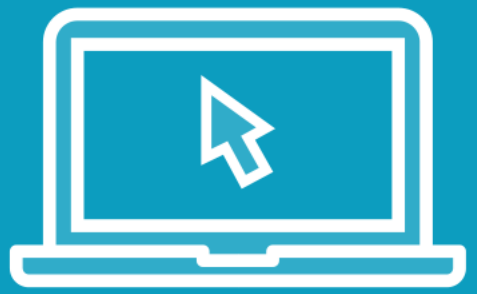


User defined routes, Azure firewall or marketplace device

Network security groups (NSGs)

Forced tunneling

Demo



Globomantics have the following requirements

- The need for a firewall
- DDoS mitigation
- A way to control the flow of network traffic

In this demonstration we will deploy the features that Globomantics needs

Summary

Learned about the different Azure firewall options available to you

Discussed user defined routes

Discussed the use of virtual appliances

In the next module

- Azure information protection
- Azure security center
- Azure key vault