Microsoft

Microsoft Azure Network Security

Securing Your Cloud Workloads at the Network Level

Nicholas DiCola
Anthony Roman

Foreword by Jonathan Trull, General Manager, Security Solutions and Incident Response Business, Microsoft

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Microsoft

Microsoft Azure Network Security

Nicholas DiCola
Anthony Roman

Microsoft Azure Network Security

Published with the authorization of Microsoft Corporation by
Pearson Education, Inc.

Copyright © 2021 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-13-725204-6
ISBN-10: 0-13-725204-8

Library of Congress Control Number: 2021933677

ScoutAutomatedPrintCode

TRADEMARKS

Microsoft and the trademarks listed at http://www.microsoft.com on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

WARNING AND DISCLAIMER

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the programs accompanying it.

SPECIAL SALES

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or(800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

SPONSORING EDITOR
Charvi Arora

DEVELOPMENT EDITOR
Songlin Qiu

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Charlotte Kughen

INDEXER
Cheryl Ann Lenser

PROOFREADER
Donna Mulder

TECHNICAL EDITOR
Mike Martin

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
codeMantra

Contents at a Glance

	Acknowledgments	*x*
	About the authors	*xi*
	Foreword	*xii*
	Introduction	*xiii*
Chapter 1	**Introduction to Azure Network Security**	**1**
Chapter 2	**Secure Azure Network architectures**	**17**
Chapter 3	**Controlling traffic with Azure Firewall**	**35**
Chapter 4	**Traffic Inspection in Azure Networks**	**61**
Chapter 5	**Secure application delivery with Azure Web Application Firewall**	**79**
Chapter 6	**Mitigating DDoS attacks**	**103**
Chapter 7	**Enabling Network Security log collection**	**123**
Chapter 8	**Security monitoring with Azure Sentinel, Security Center, and Network Watcher**	**141**
Chapter 9	**Combining Azure resources for a wholistic network security strategy**	**165**
	Index	*181*

This page intentionally left blank

Contents

Acknowledgments x
About the authors xi
Foreword xii
Introduction xiii

Chapter 1 Introduction to Azure Network Security 1

Network connectivity 1
Current threats and challenges 9
Azure Network Security 12
Core security and firewall features 13
Summary 15

Chapter 2 Secure Azure Network architectures 17

Best practices 17
Network architectures 22
Cloud native 23
Hybrid connectivity 24
Hub and spoke 28
Azure Virtual WAN 29
Summary 33

Chapter 3 Controlling traffic with Azure Firewall 35

The role of Azure Firewall in secure architecture 36
Network segmentation for security 36
What is Azure Firewall? 37
Understanding Firewall components 37
Getting traffic to Azure Firewall 38
Integrating with other traffic management 42
Advanced features 45
DNS settings 45
Forced tunneling 46

SNAT Control 47
Traffic inspection 48
Rule types 49
Network rules 49
Application rules 50
DNAT rules 51
Rule processing 53
Azure Firewall Manager 53
Firewall policies 54
Hub virtual networks 57
Secured virtual hubs 58
Third-party security services 59
Summary 60

Chapter 4 Traffic Inspection in Azure Networks 61

Azure Firewall Premium 61
Deploying Azure Firewall Premium 63
TLS inspection 64
Intrusion detection and prevention 68
Using full URLs for traffic management 70
Network Watcher packet capture 74
Summary 77

Chapter 5 Secure application delivery with Azure Web Application Firewall 79

Integrating WAF into app delivery architecture 80
Load Balancing Options 81
WAF types 83
WAF deployment. 84
Before deployment 84
Policy creation 85
Policy management 91
WAF rules and tuning. 92
Policy deployment and tuning process 92

OWASP rules 93
Bot management rules 97
Custom rules 98
Exclusions 100
Policy assignment for tuning 101
Summary 102

Chapter 6 Mitigating DDoS attacks 103

How Azure DDoS Protection Works 103
The mitigation pipeline 104
DDoS Protection Basic versus Standard 106
DDoS Protection Options for PaaS Services 108
Enabling Azure DDoS Protection Standard. 108
Create a DDoS Protection plan 109
Associate VNets to the DDoS Protection plan 110
Finishing deployment 111
Validation and testing 112
Metrics 112
Validation with BreakingPoint Cloud 115
Log samples 119
Application resiliency 120
Summary 121

Chapter 7 Enabling Network Security log collection 123

Azure Firewall 124
Web Application Firewall 129
Azure DDoS Protection Standard. 132
Azure Bastion 134
Network Security Groups 136
Diagnostic settings at scale 139
Summary 140

Chapter 8 **Security monitoring with Azure Sentinel, Security Center, and Network Watcher** **141**

Security Center . . . 141

Security policies 142

Custom policy definitions 144

Azure Defender 147

Azure Sentinel . . . 148

Data connectors for network security 149

Analytic rules and incidents 150

Custom Rules 153

Workbooks 153

Playbooks 156

Hunting 159

Network Watcher . . . 161

Topology 161

IP Flow Verify 162

Summary . . . 163

Chapter 9 **Combining Azure resources for a wholistic network security strategy** **165**

Simple virtual network design . . . 165

Virtual network isolation 166

Network security groups 166

Hub-and-spoke topology . . . 167

VNet peering 167

Routing 168

Hybrid Access 168

Integrating PaaS services 169

Secure administrative access . . . 170

Remote access 171

Role-based access control (RBAC) 171

Application design scenarios **172**
Application Gateway behind Front Door **173**
Azure Kubernetes application **175**
Firewall or WAF? **176**
Network Security Monitoring **176**
Data collection strategy **176**
Cloud secure posture management **177**
Summary **178**
Index *181*

Acknowledgments

The authors would like to thank Loretta Yates and the entire Microsoft Press/Pearson team for their support in this project, Jonathan Trull for writing the foreword, and also the Azure Network Security Engineering Team (Yair Tor, Ido Frizler, Teresa Yao), Ajeet Prakash, David Fosth, Ken Hollis, and Mark Simos.) Thanks also goes to Mike Kassis for the great work writing Chapter 8. We would also like to thank Mike Martin for reviewing this book.

Nicholas would also like to thank: My wife and children for supporting me while I worked on this book and my co-author and friend, Anthony Roman, for his hard work on this book.

Anthony would also like to thank: My wife and kids for tolerating groggy mornings after late nights spent working on these chapters. Thanks to Nicholas for suggesting this project and holding me to deadlines.

About the authors

Nicholas DiCola

Nicholas is the principal director of the Cloud Security Customer Experience Engineering (CxE) team. CxE helps customers with deployments of Cloud Security products such as Azure Security Center, Azure Sentinel, Azure Network Security, Azure Information Protection, Microsoft Defender for Identities, and Microsoft Cloud Application Security. CxE is responsible for driving use of Cloud Security products and taking feedback from customers to improve the products. Nicholas has been with Microsoft since 2006 when he started in Microsoft Consulting Services. He has a Master of Business Administration with a concentration in information systems and various industry certifications such as CISSP and CEH. You can follow Nicholas on Twitter at @mastersecjedi.

Anthony Roman

Anthony is the senior PM manager leading the Azure network security Get-To-Production team within Cloud Security CxE. The team works with customers and network security engineering to ensure that products are fulfilling customer security requirements. Anthony joined Microsoft in 2019 and has held positions in IT and security since he made the transition from bartender to IT security professional a decade earlier. His Bachelor of Arts degree in philosophy is complemented by several industry certifications and plenty of on-the-job and home lab experience. He currently lives in Philadelphia with his wife and two children and can often be seen walking around the city in search of parks and restaurants.

Foreword

I am writing this foreword amid one of the largest and most invasive cybersecurity breaches in history—Solorigate. A sophisticated, nation-state actor was able to infiltrate a well-known supplier of network monitoring and management solutions. The threat actor injected a backdoor into the supplier's build system, and the backdoor was then signed with a valid certificate and pushed to approximately 18,000 customers. What made this attack particularly novel was the fact that the threat actor leveraged their access to on-premises systems to then pivot and begin accessing cloud services, which appeared to be their primary target. The attacker also attempted to hide their level of access by leveraging Azure Service Principals to blend in with standard traffic and access patterns.

With attacks like Solorigate, it is essential to have a strong understanding of how to properly segment, protect, and monitor your cloud estate. Microsoft Azure is one of the dominant public clouds available in the market today and is used extensively by both governments and commercial enterprises. Microsoft Azure offers hundreds of different cloud computing solutions to organizations that allow them to innovate quickly, increase the digital experiences for customers and employees, and reduce large outlays in capital for data centers and hardware.

While cloud computing offers amazing benefits, it also introduces risks that security and IT teams must properly manage. In this book, Nicholas and Anthony cover the foundational security services and design patterns that organizations should adopt to protect and monitor their Azure workloads. I can think of no more qualified individuals than Nicholas and Anthony to provide practical, real-world implementation guidance regarding the design of secure Azure networking architectures. From preventing volumetric DDoS attacks to monitoring security logs with Azure Sentinel, this book covers everything you need to jump-start your journey into Azure security architecture and engineering.

For every IT leader using Microsoft Azure, put this on your team's required reading list!

We are in the fight to deter cyberattacks together, and I applaud the effort that Nicholas and Anthony have put into making this essential material accessible to a broader audience. For all those who are working tirelessly to protect your organizations' data and computer systems, thank you! Look after yourselves and each other.

—Jonathan C. Trull

Introduction

Welcome to *Microsoft Azure Network Security*, a book that is intended to provide detailed information about the capabilities of the major network security components of Azure along with recommendations for how to put them all together. We pay the closest attention to what we consider the core network security resources: Azure Firewall, Azure WAF, and Azure DDoS Protection Standard. Going beyond the function of the network security components themselves, we also emphasize the value of logging and integration with other security services like Azure Sentinel.

We wrote this book from a vantage point inside Engineering at Microsoft, working closely with both the product groups in control of the development of the technology and with customers who implement the technology in their networks. Network security is a complex intersection of networking, security, and cloud operations, and our hope is that we have covered the important pieces of all of these.

This book was finished just before the public release of Azure Firewall Premium, so details are as complete as possible. Please expect the product to evolve over time.

Who is this book for?

Microsoft Azure Network Security is for anyone who has a technical role that involves Azure deployments. Cloud administrators, engineers, and architects will find value in the how-to implementation details. Networking teams can gain context for how to integrate Azure native services into the broader architecture. Security professionals will be able to use this book as a guide for both secure Azure network architecture and network security monitoring strategy.

How is this book organized?

This book is arranged into nine chapters, which represent some broad themes:

- Chapters 1 and 2 discuss the broad theme of cloud network security and introduce the Azure components that address it.
- Chapters 3, 4, 5, and 6 concentrate on the core Azure network security resources: Azure Firewall, Azure WAF, and Azure DDoS Protection Standard.

- Chapters 7 and 8 address logging, monitoring, and integration with other Azure security components such as Azure Sentinel and Security Center.
- Chapter 9 brings everything together to connect the concepts of secure network architecture and security monitoring as they apply to all the Azure network security tools.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/AzureNetworkSecurity/errata

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit *MicrosoftPressStore.com/Support*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

Stay in touch

Let's keep the conversation going! We're on Twitter:
http://twitter.com/MicrosoftPress.

Chapter 2

Secure Azure Network architectures

Chapter 1, “Introduction to Azure Network Security,” covers some basics to Azure networks and the current threat landscape. Given this, it is ever more important to define your Azure network architecture to meet needs but allow for network security and containment in the event of a breach.

Many organizations used perimeter-based networks that assume all systems behind the perimeter are trusted. This type of network defense is obsolete. Zero Trust networks are the next evolution that eliminates the trust based on network location. Zero Trust typically integrates user and device information, such as location and health state, which is run through a policy engine to determine whether access should be permitted or denied. In Zero Trust, a user in the corporate office on a managed machine might be able to access a cloud-based highly sensitive application, but when they go home, the same access may be limited (block downloading) or denied.

Layering cloud security into your Azure deployments as part of a Zero Trust approach allows for limiting or containing an attack if it does occur. In a simple form, having all IaaS VMs on one subnet would allow an attacker to quickly pivot between machines. Breaking the machines into groups by function and moving them to separate virtual networks (vNet) and applying Network Security Groups (NSGs) to the virtual networks can prevent an attacker from pivoting at all.

This chapter explains the best practices to a good network architecture, various types of network architectures in Azure, and how network security services can be layered in to protect these architectures.

Best practices

Before diving into network architectures, it’s important that we quickly mention Azure Well-Architected Framework. The framework consists of the following five pillars:

- Cost Optimization
- Operational Excellence
- Performance Efficiency

- Reliability
- Security

NOTE To read more on Azure Well-Architected Framework, see *https://aka.ms/AzNSBook/AWAF*.

The Azure Well-Architected Framework gives you a way to apply the best practices and principles to your applications or services. Security is one of the most important aspects of architecture. It provides assurance for the CIA (confidentiality, integrity, and availability) triad against attacks and loss of data. Losing these assurances can hurt an organization's reputation, business operations, and revenue. If you don't cost optimize your architecture, your return might be lower, but if you don't secure your architecture, there might be no returns at all.

Under the pillar of security, network security and containment is a key topic that organizations must adhere to for protecting their cloud deployments. Here are the best practices for network security and containment:

- Align network segmentation with enterprise segmentation strategy
- Centralize network management and security
- Evolve security beyond network controls
- Build a security containment strategy
  - Define an internet edge strategy
  - Decide on an internet ingress/egress policy
  - Mitigate DDoS attacks
  - Design virtual network security technology
- Decide use of legacy network security technology
- Enable enhanced network visibility

The first best practice is to align network segmentation with enterprise segmentation. Organizations need to define how they will segment the enterprise starting from the top so that all teams (identity, network, app teams, and so on) are building and working to the same strategy. The following graphic depicts a reference enterprise segmentation from the Well-Architected Framework. Here the organization has created a central identity store, uses Management Groups to apply central policies and permissions, and has broken networks into segments that align with enterprise segments of subscriptions and resources. Figure 2-1 shows a segmentation reference model that can be used as a starting point.

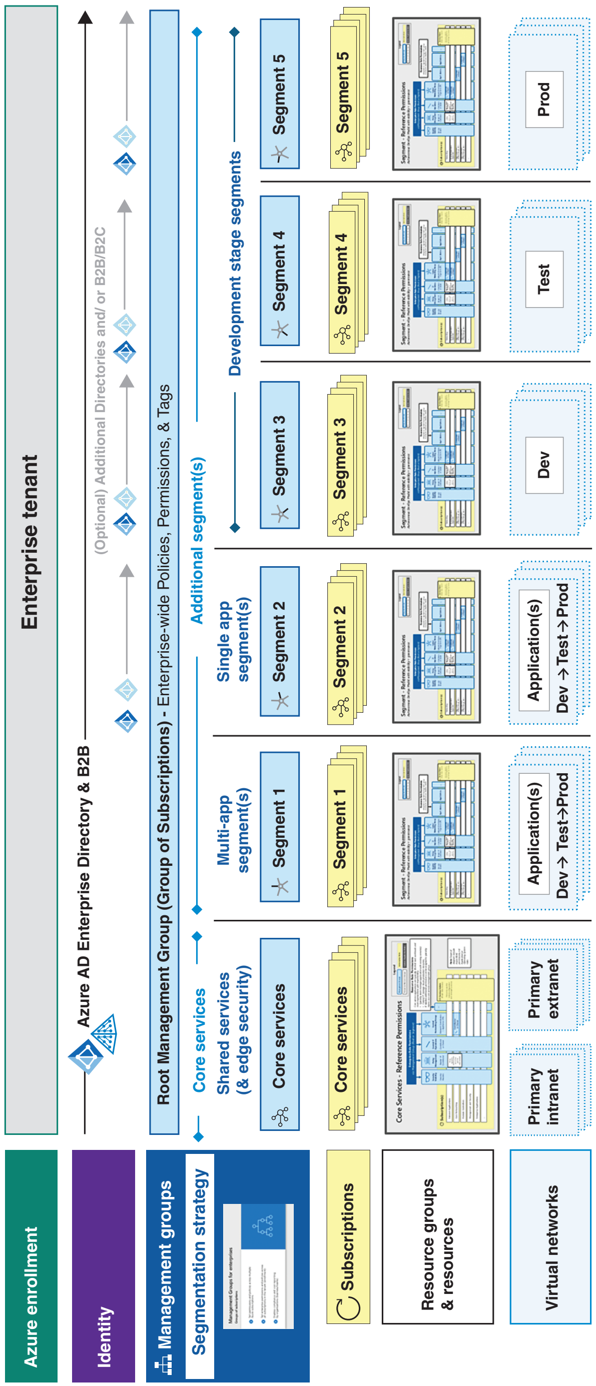

FIGURE 2-1 Reference model for segmentation

Under the core services, the organization has centralized network management and security. This is the second best practice for network security. By centralizing network management and security, the organization can prevent applications or segments from being created that do not adhere to the network security strategy. Very often organizations that don't centralize have new resources created in the cloud with a direct connection to the internet and little to no network security applied. This results in attacks against those resources that we know are unavoidable! Centralizing network management and security ensures new segments are protected and leverages the tools and expertise of the network and security teams. The following graphic depicts the reference for network security applied using the enterprise segmentation strategy. Figure 2-2 is a possible model for centralized network management and security.

In this design, the shared services segment is a hub virtual network providing core services, connectivity to on-prem, and public connectivity. By using this design, the organization can control ingress/egress (north-south) traffic from the hub and apply to all spokes. The next best practice is to define an internet edge strategy. Organizations need to choose how they will protect against from internet-based attacks. There are two primary choices:

- **Use cloud native controls, such as Azure Firewall and Web Application Firewall** This approach typically implements basic security that is good enough for common attacks but is well integrated into the platform.
- **Use partner virtual network appliances (available in the Azure Marketplace)** This approach often provides advanced features that protect against sophisticated attacks, but can cost more. An organization may also have existing knowledge/skills on the partner virtual network appliances.

The organization must decide based on experience and requirements. Once decided, the next detail is to apply ingress/egress policy baseline. In perimeter-based networks, many organizations would allow network traffic from internal to internet over HTTP/80 and HTTPS/443. This was fine until attackers started using HTTP(s) outbound to conduct command and control of exploited machines. In the era of Zero Trust, the concept starts with deny all outbound and only allows what is needed. It can't be as broad as HTTP(s), and it must be more restrictive to allow HTTP(s) to specific domain names. Using this approach makes it significantly harder for attackers because they can't use their command and control nodes and need to find another way.

Let's take a look at the ingress side, too. By using cloud native controls, instead of having to allow RDP/SSH inbound on the firewall, organizations can use services like Azure Bastion and Azure Security Center (ASC) Just-in-time VM (JIT) access. Azure Bastion allows remote management access using HTTPs and would not require opening the firewall at all. Because Bastion is integrated into the Azure portal, organizations could apply Azure Active Directory Conditional Access to the Azure portal, which would apply Zero Trust to remote management of VMs. ASC JIT integrates with Azure Firewall, which again means RDP/SSH would not need to be open all the time to all sources but could be opened on demand to only specific sources (client machine IP or a specific subnet). Both of these examples are part of the best practice to evolve security beyond network controls. They now factor in identity, device, and application as part of access to the VM incorporating Zero Trust principles.

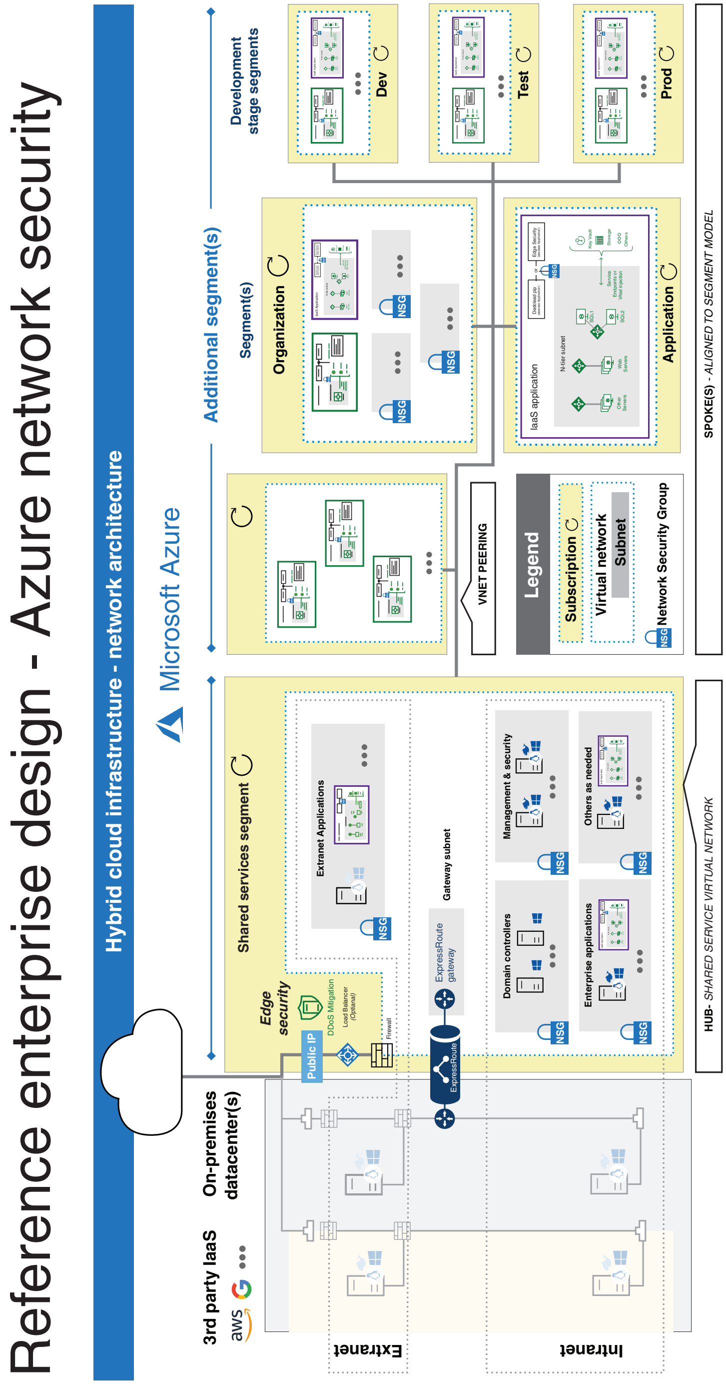

FIGURE 2-2 Centralized network management and security

For public-facing applications and services, it's imperative to protect against DDoS attacks. Cloud providers, including Azure, provide DDoS protection at the network layer to protect the platform. Organizations should also apply DDoS protection at higher layers to protect their applications. This type of protection typically profiles the application usage and uses machine learning to look for anomalous traffic. The service should proactively protect the application before degradation. Azure provides DDoS protection service, which is covered in Chapter 6, "Mitigating DDoS attacks."

Moving inward, organizations need to design network subnet security for their network segments. It is recommended that you plan for growth of resources in subnets over time and group resources in subnet by common roles and functions. Allow for larger IP address subnets on virtual networks to support expansion. If an organization has one subnet with five different resources, it needs to create NSG rules to support the different roles. Grouping resources allows for NSG configuration to be simplified and not get out of hand over time. It's important to apply the principle of least privilege at the NSG to limit and contain traffic between subnets and virtual networks (east-west traffic). If an attacker somehow makes it into a virtual machine, maybe due to an application vulnerability, they won't be able to pivot to other machines in other virtual networks. This is also referred to as micro-segmentation.

Organizations should enable enhanced network visibility as a best practice. Network logs should be integrated with the organization SIEM (security information and event management). This provides better visibility either through network log detection rules, the ability to query the data in the event of an incident for further investigation, or the ability to dashboard the data to look for trends and interesting changes for the central network and security teams. We cover monitoring in Chapter 8, "Security monitoring with Azure Sentinel, Security Center, and Network Watcher."

Lastly, organizations have some existing or legacy network security technologies, like IDS/IPS, that they must decide whether to bring to the cloud. The recommendation is to evaluate these technologies and favor newer Zero Trust technologies where appropriate and look to cloud-native versions of where machine learning and artificial intelligence can be provided to replace or advance these types of technologies.

Network architectures

When planning or designing any service or application deployment to the cloud it's imperative you start with a well-architected design. After defining a network strategy based on the previously discussed best practices, an organization can apply that to the architecture that meets their needs. The following architectures are just a few of the commonly used examples and how the best practices for network security are applied to them.

Cloud native

In recent years, it is entirely possible that a company was created and running with an entirely cloud-based set of services, which means they have no on-prem servers running, and they are using SaaS applications and hosting their service purely in the cloud. The following graphic depicts a simple cloud-native architecture where the organization might be using a few public services. The company has deployed its web application in Azure using purely PaaS services. This architecture is simple and can be secured by leveraging firewall features built into storage and SQL PaaS. Storage and SQL could be configured to block internet access and restrict it to the App Service web app. The following list covers some advantages and disadvantages:

- Advantages
  - Simple
  - Leverages network security services built into PaaS
- Disadvantages
  - Traffic is not routed through any central controlling service or device.
  - Each PaaS service has its own network security configuration.

Figure 2-3 shows a simple cloud-only set of services that an organization might be using.

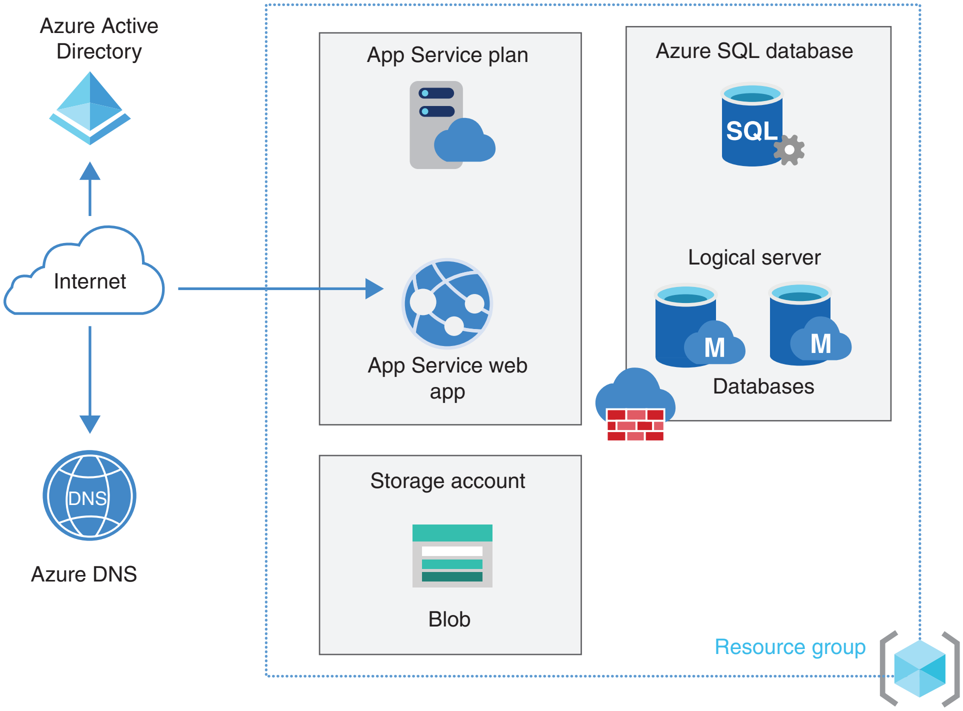

FIGURE 2-3 Diagram of cloud-only native services

As you can see from the next example, most architectures are not that simple. A startup may be, but as the company's service grows, it may need to expand to something more complex. Picture a company that has built a purely cloud-based application. It needs to deliver this application globally to its customers.

Here the application is global, which means traffic needs to be load balanced for both HTTP(s) and non-HTTP(s) traffic using Front Door and Traffic Manager. Front Door and Traffic Manager provide that load balancing. Web Application Firewall (WAF) is enabled on Front Door to defend the application at the network edge. Moving deeper in the stack, application gateway is then used in each region to load balance traffic to the VMs running the web application. WAF is also enabled on App Gateway to further protect the application. Why? WAF on Front Door supports geo-filtering, rate limiting, and Azure managed default rule sets, whereas WAF on App Gateway supports ModSec Core Rulesets (CRS). WAF is covered in depth in Chapter 5, "Secure application delivery with Azure Web Application Firewall." As another protection, DDoS Protection Standard is enabled in the tenant and applied to all virtual networks. DDoS protects any public IPs (PIP) of the application gateways in this architecture. DDoS is covered in Chapter 6. Lastly, NSGs are added to control east-west traffic. This layered approach provides additional defense in depth to the application. Following are the advantages and disadvantages:

- Advantages
  - Leverages network security at all layers.
  - Various network security services provide protection against many types of attacks.
- Disadvantages
  - Traffic between virtual networks is not routed through any central controlling service or device.
  - Each PaaS service has its own network security configuration.

Figure 2-4 is an architecture for a global web application with the various services used across the regions.

Hybrid connectivity

Next up are more common architectures used as there are many organizations with existing on-premise networks that need to be connected to Azure and their workloads deployed there.

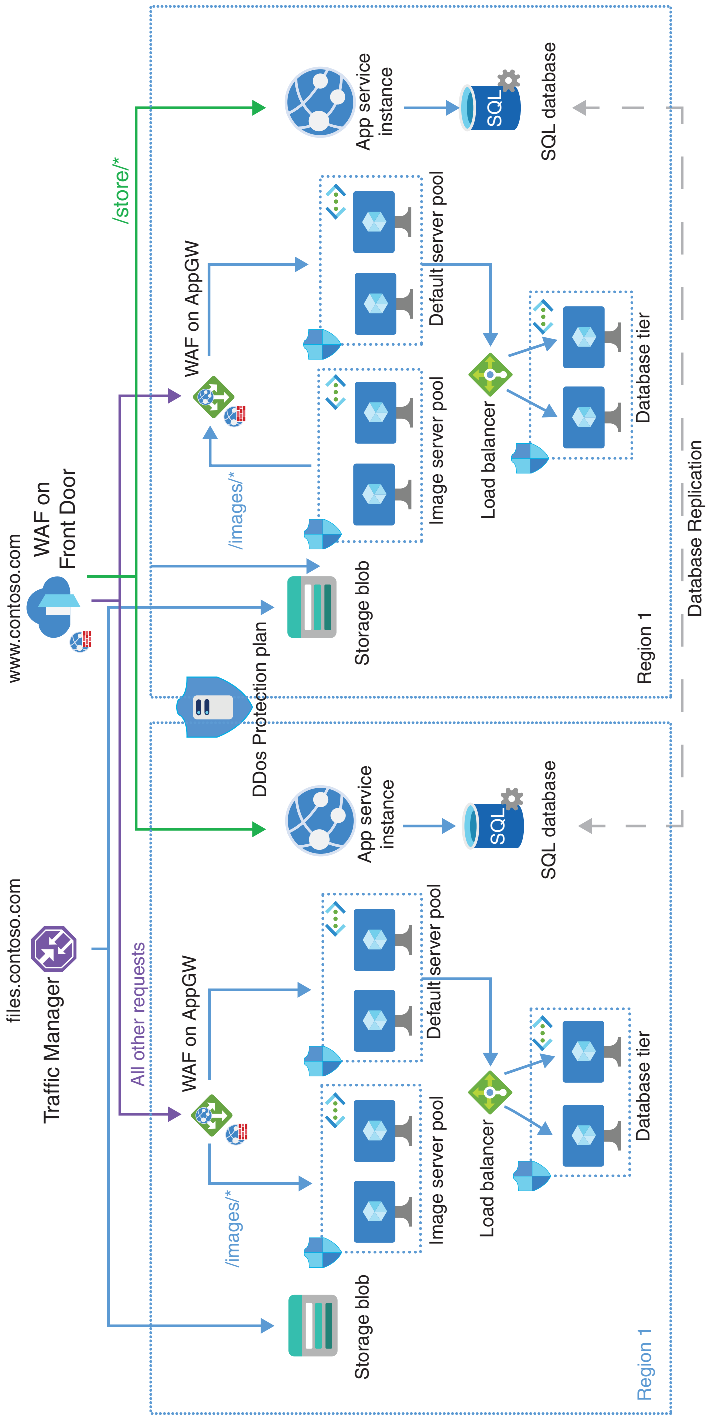

FIGURE 2-4 Complex global web application

ExpressRoute with VPN (ER/VPN) failover

In this architecture, ExpressRoute provides a connection that does not route over the internet and, in case of failure, a VPN backup path. The traffic is secured from on-premise to Azure. Once in Azure, WAF on App Gateway protects the web tier. Each subnet has an NSG to limit and contain traffic to only what is needed with rules appropriate for each subnet. For example, a rule to allow RDP or SSH from the management subnet IP range to the web tier and business tier IP range. The SQL database is configured with a service endpoint to provide direct connectivity to the service. No services or VMs have public internet access in this architecture. The following are the advantages and disadvantage:

- Advantages
  - Various network security provides protection against attacks.
  - Connectivity from on-premise is secure.
  - Remote management is secured from the management subnet only.
- Disadvantage
  - Traffic between virtual networks is not routed through any central controlling service or device.

Figure 2-5 is an ER/VPN architecture where on-premise connects to Azure over ExpressRoute and VPN.

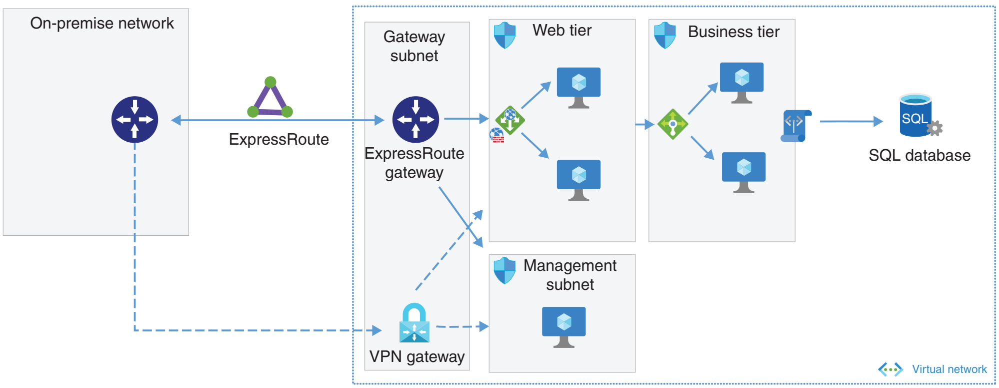

FIGURE 2-5 ER/VPN architecture

DMZ

The DMZ (demilitarized zone) architecture enables a secure hybrid network that extends an on-premises network to Azure. This forces traffic coming from on-premise bound for the internet to route through the network virtual appliance (NVA) in the cloud. The advantage to this design is that all traffic passes through the NVA, which can control and provide advanced inspection of the traffic. Because the NVA has a PIP, applying DDoS to protection against attacks adds another layer of protection to the workload. The following are the advantages and disadvantage:

- Advantages
  - Traffic is routed through a central device, which can control and limit traffic flows.
  - Various network security services provide protection against many types of attacks.
- Disadvantage
  - NVA requires additional management and configuration for HA.

Figure 2-6 shows the DMZ architecture and connections.

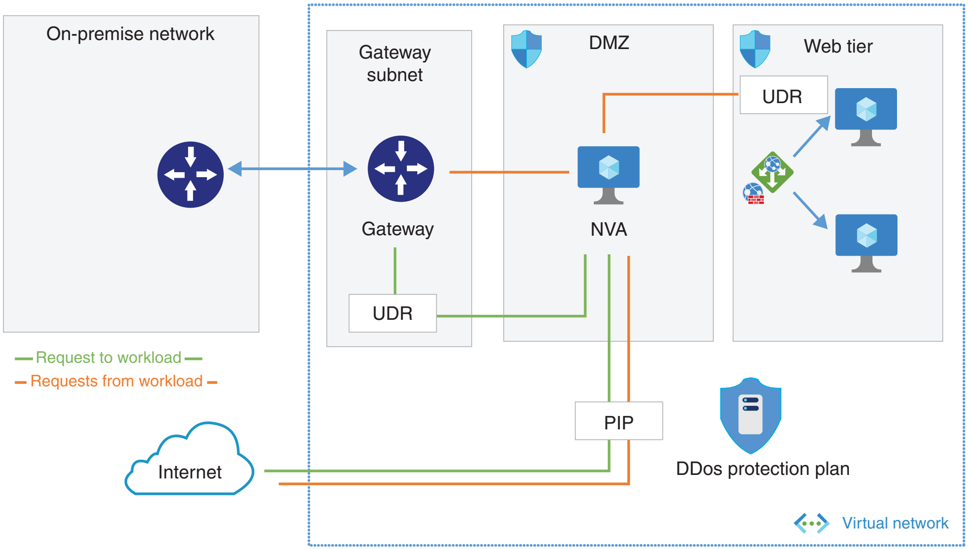

FIGURE 2-6 DMZ architecture

Expanding on this architecture, in Figure 2-7 we see that the architecture layers in Azure Bastion, which provides secure RDP (remote desktop protocol) and SSH (secure shell) access to the virtual machines. Azure Firewall has replaced the NVA to provide a cloud native approach. Azure Firewall has the advantages of being a fully managed PaaS. It can auto-scale as needed and provide built-in high availability. With an NVA, organizations must manage high availability, load balancing, and the appliance software themselves. Following are the advantages and disadvantage:

- Advantages
  - Cloud native services such as Azure Firewall and Bastion require less management and configuration.
  - Key traffic is routed through a central device, which can control and limit traffic flows.
  - Various network security services provide protection against many types of attacks.

- Disadvantage
    - Workloads are not fully isolated behind the firewall.

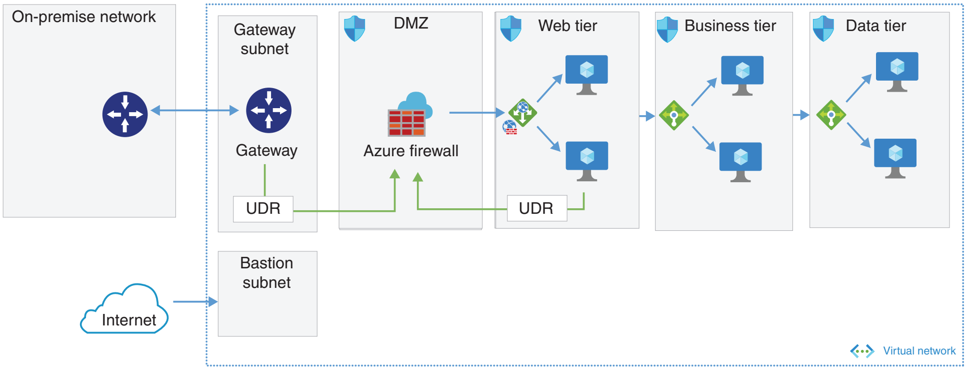

FIGURE 2-7 DMZ architecture with Azure Bastion

Hub and spoke

The hub virtual network acts as a central point of connectivity for on-premise networks, meaning on-prem is just another spoke. All traffic is routed through the hub virtual network. The spoke virtual networks create an isolated network to contain traffic to the specific workloads. This could be spokes for prod versus dev or workload or front end vs back end. Central services could be deployed in the hub as a separate subnet or a spoke virtual network. In the hub, Azure Firewall or an NVA is deployed to provide additional protection to east-west traffic between the spokes. This is an ideal architecture because it allows for expansion and contraction over time by adding or removing spokes. For multiregion, additional hubs are deployed to the region with region spokes connected. Hubs between regions can be connected using vNet peering, site-to-site VPN, or virtual WAN. The main difference between virtual WAN and hub and spoke is that virtual WAN is a managed offering. The following are the advantages and disadvantages:

- Advantages
    - Central services can provide cost savings by sharing them across workloads.
    - Hub virtual network can create separation of duties for IT (security, infrastructure) and workload (DevOps).
- Disadvantages
    - It is complex to manage as spoke numbers grow.
    - Spoke-to-spoke traffic must pass through the hub.

Figure 2-8 is a hub and spoke architecture.

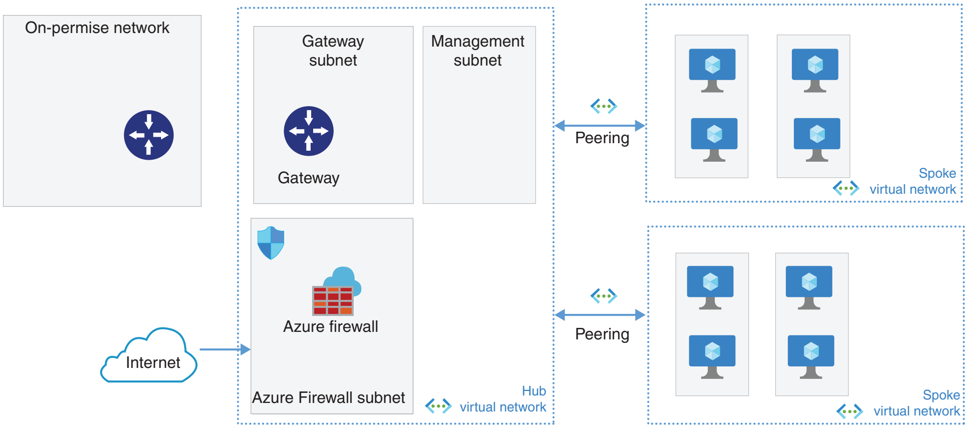

FIGURE 2-8 Hub-and-spoke architecture

Azure Virtual WAN

Azure vWAN is a service that brings together all of the benefits of previously discussed hybrid architectures into a single interface. Virtual WAN (vWAN) includes functionalities for branch, site-to-site VPN, point-to-site VPN, ExpressRoute, intra-cloud connectivity, routing, and Azure Firewall. vWAN is built on the hub and spoke architectures and enables global network connectivity.

The following resources are part of vWAN:

- **virtualWAN** This resource is an overlay of the Azure network and contains multiple resources.
- **Hub** This is a Microsoft-managed virtual network. It contains various endpoints like VPN Gateway and ExpressRoute gateway to provide connectivity to on-premise or mobile users.
- **Hub virtual network connections** This is a connection resource to connect the hub to spoke virtual networks.
- **Hub-to-hub communication** Hubs are deployed in regions and connected to each other in the virtual WAN. This creates a full-mesh architecture allowing traffic between virtual networks, on-premise, and branch sites.
- **Hub route table** This allows the addition of routes to the hub route table.

Figure 2-9 is the basic diagram of vWAN.

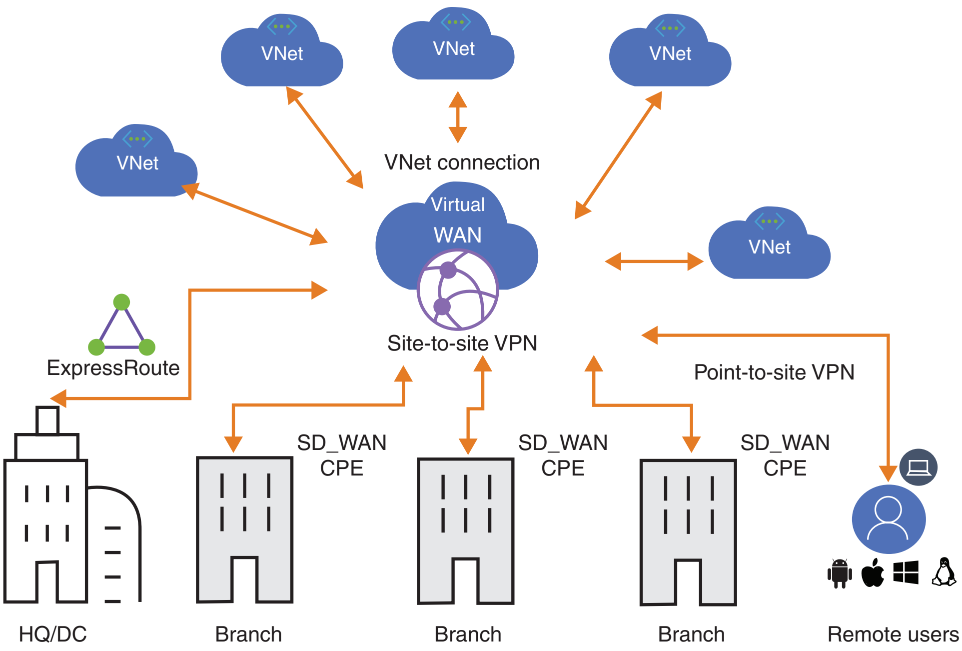

FIGURE 2-9 vWAN

Connectivity

Virtual WAN provides many types of connectivity, and the advantage is that an organization can use one or all of the various types. They can start with one that is needed today and expand over time as new connectivity requirements arise. There are various methods to connect on-premise to virtual WAN. Site-to-site VPN connections allow on-premise connectivity over an IPSec/IKE connection. Organizations must employ a VPN device or virtual WAN partner device on-premise to establish the S2S VPN. If there is a need for mobile users to have VPN access, a virtual WAN can be configured to provide VPN for users and require a VPN client on the endpoint. ExpressRoute lets organizations connect over a private connection.

Transit connectivity is also provided in virtual WAN. Once connected to the hub, on-premise traffic can be routed to spoke virtual networks. This means user traffic coming from on-prem will route over S2S VPN or ExpressRoute, hit the hub, and use the virtual network connection to the spoke to reach a server. This traverses the same path the opposite way. Virtual WAN also allows transit connectivity between VPN and ExpressRoute. A mobile user over VPN could reach on-premise via the hub. Spoke virtual networks can talk to each other through the hub.

Traffic can travel between two spokes via the hub. Multiple hubs can be added to virtual WAN as well. This will allow spoke virtual networks to talk over the hub-to-hub connection going from spoke to hub to the other hub to the other spoke.

Security

Virtual WAN allows organizations to apply virtual hub routing and manage traffic flow within the virtual WAN. Specifically, this can be used to isolate virtual networks, create shared services virtual networks, or route traffic through one of the Azure partner NVAs or Azure Firewall. There is also an option to use Azure Firewall in the hub and integrate partner offerings like zScaler, iBoss, and Checkpoint. In this configuration, Azure Firewall protects private traffic in the hubs and internet/SaaS traffic is routed to the partner service. An organization might have a need to isolate the virtual networks allowing traffic from on-premise to all virtual networks but not virtual network to virtual network. Or perhaps, the organization wants to configure shared services such as domain controllers or file services but doesn't want to allow all virtual network to virtual network traffic. By applying routing these scenarios are achievable.

NOTE To route traffic in a virtual WAN, it must be a standard type virtual WAN. See more at *aka.ms/AzNSBook/vWAN*.

In the Shared Services example, nonshared services virtual networks do not learn routes to other nonshared virtual networks but do learn about the shared services virtual network. Shared services are propagated to all virtual networks and branches/VPN using the default table. It is important to understand how routing can be used to limit traffic to only sources and destinations needed. Figure 2-10 depicts an example of the shared services routing.

To layer in security, organizations can deploy an NVA into a virtual network. When using NVA, spokes must be created off of the NVA virtual network that resides in the virtual WAN. This will allow having traffic from workload virtual networks to pass through the NVA. Figure 2-11 shows the NVA VNet added with spokes behind it.

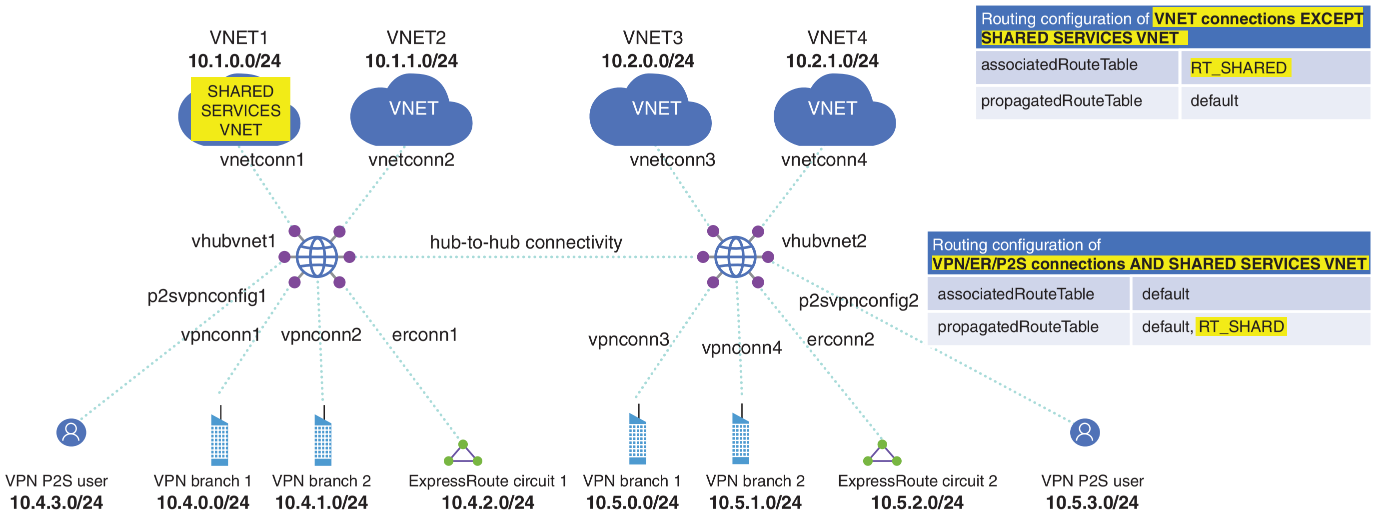

FIGURE 2-10 Shared services routing

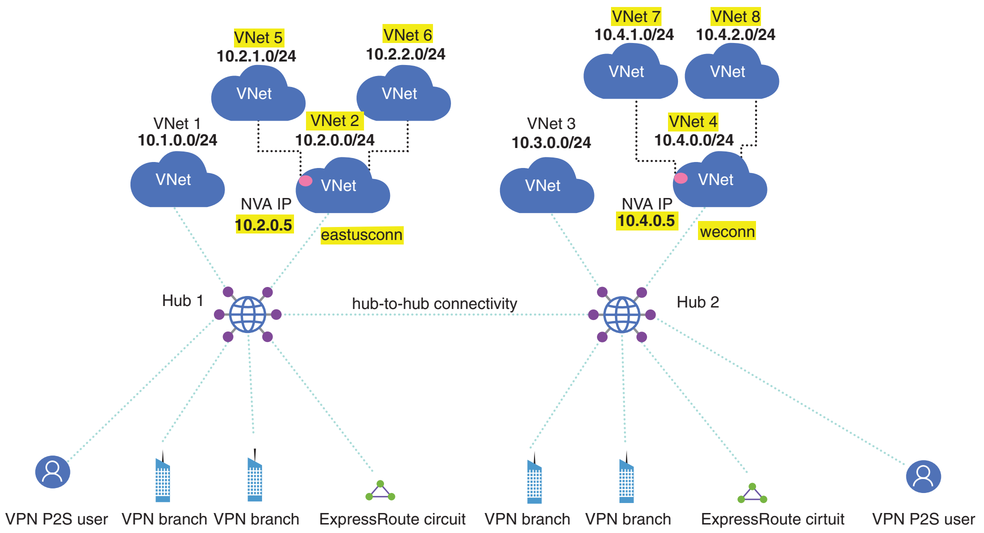

FIGURE 2-11 NVA VNet

If an organization wants to use cloud native network security, vWAN offers a secure virtual hub, which includes an Azure Firewall instead of using an NVA. Figure 2-12 shows the difference that additional spoke networks are not needed because Azure Firewall can be deployed in the vWAN hub.

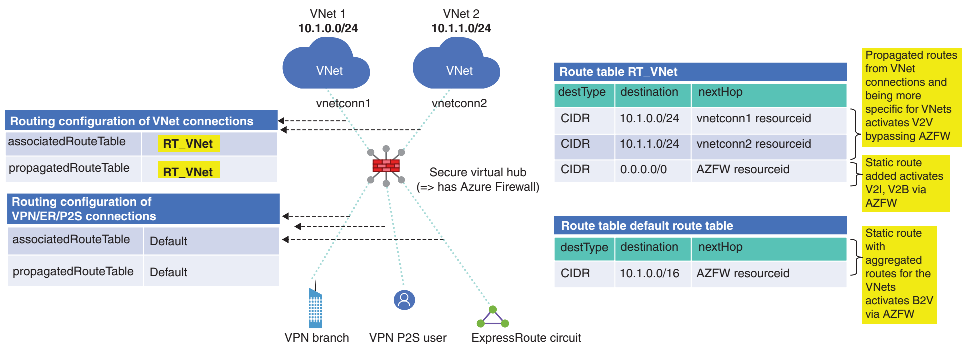

FIGURE 2-12 vWAN with Azure Firewall

Summary

In this chapter, we covered the importance of using Azure Well-Architected Framework to use best practices when designing networks and network security in Azure. We then reviewed various network architectures that can be used to deploy services and applications in Azure. Each architecture has its advantages and disadvantages and allows for network security in different ways. It is important to leverage the framework at the start and use those practices combined with the sample architectures to meet the needs and requirements of the application being deployed.

Index

A

access (distribution) routers, 13
access control, 170–172
Active Directory Certificate Services, 65–66
administrative access, 170–172
AKS (Azure Kubernetes Service), 175
anomaly scoring, 96
application design, 172–176
Application Gateway
  anomaly scoring, 96
  bot management rules, 98
  documentation, 9
  load balancing with, 81–82
  overview, 5
  OWASP rule tuning, 96–97
  policy creation, 86–89
  rule exclusions, 101
  rule logic, 93–96
  with WAF (Web Application Firewall), 173–174
application resiliency in DDoS attacks, 120–121
application rules
  in Azure Firewall, 50–51
  full URL filtering with, 70–74
application security. *See* WAF (Web Application Firewall)
architectures (Azure), 12–13
  administrative access, 170–172
  application design, 172–176
  Azure Firewall in, 36
  best practices, 17–22
  cloud native, 23–25
  hub and spoke, 28–29, 167–168
  hybrid, 24–28, 168–169
  isolated, 44, 166
  in-line, 44
  PaaS service integration, 169–170
  security monitoring, 176–178
  segmentation, 36
  side-by-side, 44
  simple virtual network, 165–167
ASC (Azure Security Center). *See* Security Center
associating VNets with DDoS Protection plan, 110–111
attack types, 9–10
Azure
  architectures, 12–13
    administrative access, 170–172
    application design, 172–176
    Azure Firewall in, 36
    best practices, 17–22
    cloud native, 23–25
    hub and spoke, 28–29, 167–168
    hybrid, 24–28, 168–169
    isolated, 44, 166
    in-line, 44
    PaaS service integration, 169–170
    security monitoring, 176–178
    segmentation, 36
    side-by-side, 44
    simple virtual network, 165–167
  firewall features, 13–15
  network security overview, 12–13
Azure Bastion, 20
  logs
    configuring, 134–135
    viewing, 135–136
  remote access, 171–172
Azure DDoS Protection
  Basic versus Standard versions, 106–108
  deploying Standard tier
    associating VNets with DDoS Protection plan, 110–111
    DDoS Protection plan creation, 109–110
    logging and metrics setup, 111–112
    steps in, 108
  logs
    configuring, 132–133
    samples, 119–120
    viewing, 134
  mitigation pipeline, 104–105
  for PaaS services, 108
  types of attacks covered, 103–104
  validating and testing

        with BreakingPoint Cloud, 115–117
        metrics, 112–115
        purpose of, 112
Azure Defender, 147–148
Azure Firewall
    components of, 37–38
    configuring for TLS inspection, 66–68
    DNS settings, 45–46
    logs
        configuring, 124–126, 145–147
        viewing, 126–129
    purpose of, 35, 37
    remote access, 171
    rule processing, 53
    rule types, 49
        application rules, 50–51
        DNAT rules, 51–53
        firewall policies and, 55–57
        network rules, 49–50
    traffic inspection, 48
    traffic management
        forced tunneling, 46–47
        NSGs (network security groups), 42
        NVAs (network virtual appliances), 43–44
        Private Link, 43
        routing, 40–42, 168
        SNAT (Source Network Address Translation), 47
        virtual network peering, 39–40
    in vWAN, 33
    WAF (Web Application Firewall) versus, 176
Azure Firewall Manager
    firewall policies, 54–57
    hub virtual networks, 57–58
    purpose of, 35, 53–54
    secured virtual hubs, 58
    third-party security services, 59–60
Azure Firewall Premium
    deploying, 63–64
    full URL filtering, 70–74
    IDPS settings, 68–70
    purpose of, 61–62
    TLS inspection, 64–68
        configuring Azure Firewall for, 66–68
        creating certificates, 65–66
        validating, 72–74
Azure Kubernetes Service (AKS), 175
Azure Monitor Log Analytics, 123
Azure Private Link. *See* Private Link
Azure Security Center (ASC). *See* Security Center
Azure Security Center (ASC) Just-in-time VM (JIT) access, 20, 171
Azure Sentinel
    custom rules, 153
    data connectors, 149–150
    hunting, 159–161
    playbooks, 156–159
    purpose of, 148–149
    rule templates, 150–152
    workbooks, 153–156
Azure vWAN. *See* vWAN (virtual WAN)
Azure Web Application Firewall. *See* WAF (Web Application Firewall)
Azure Well-Architected Framework, 17–18

B

best practices for network architectures, 17–22
    administrative access, 170–172
    application design, 172–176
    hub and spoke, 167–168
    hybrid, 168–169
    isolated, 166
    PaaS service integration, 169–170
    security monitoring, 176–178
    simple virtual network, 165–167
bot management rules, 97–98
BreakingPoint Cloud, 115–117

C

CDN (Content Delivery Network), 7–8
centralized management and security, 20
certificates
    creating, 65–66
    trust methods for, 64–65
cloud native architectures, 23–25
Cloud Secure Posture Management (CSPM), 177–178
cloud services
    attack types, 9–10
    shared responsibility model, 11
configuration monitoring, 177–178
configuring
    Azure Firewall for TLS inspection, 66–68
    logs
        for Azure Bastion, 134–135
        for Azure DDoS Protection, 132–133
        for Azure Firewall, 124–126, 145–147

for WAF (Web Application Firewall), 129–130
Traffic Analytics, 137–138
connectivity in vWAN, 30–31
Content Delivery Network (CDN), 7–8
CSPM (Cloud Secure Posture Management), 177–178
custom policy definitions, 144–146
custom rules, 98–100, 153

D

data breaches, 9–10
data collection strategy, 176–177
data connectors in Azure Sentinel, 149–150
DDoS (distributed denial of service) attacks, 13, 22. *See also* Azure DDoS Protection
application resiliency, 120–121
goals and targets, 103
DDoS Protection. *See* Azure DDoS Protection
Deep Packet Inspection. *See* traffic inspection
default LAN architecture (DLA), 12
demilitarized zone (DMZ) architecture, 26–28
deploying
Azure DDoS Protection Standard
associating VNets with DDoS Protection plan, 110–111
DDoS Protection plan creation, 109–110
logging and metrics setup, 111–112
steps in, 108
Azure Firewall Premium, 63–64
WAF (Web Application Firewall)
policy creation, 85–91
policy management, 91–92
requirements, 84–85
WAF policies, 92–93
destination network address translation (DNAT) rules in Azure Firewall, 51–53
diagnostic logs. *See* logs
distributed denial of service (DDoS) attacks, 13, 22. *See also* Azure DDoS Protection
application resiliency, 120–121
goals and targets, 103
distribution (access) routers, 13
DLA (default LAN architecture), 12
DMZ (demilitarized zone) architecture, 26–28
DNAT (destination network address translation) rules in Azure Firewall, 51–53
DNS settings for Azure Firewall, 45–46
documentation for networking services, 8–9
dual perimeters, 10–11

E

edge routers, 13
enabling. *See* configuring; deploying
enhanced network visibility, 22
ER/VPN (ExpressRoute with VPN) failover, 26
exclusions for WAF rules, 100–101
ExpressRoute
documentation, 9
overview, 6
ExpressRoute with VPN (ER/VPN) failover, 26

F

filtering routers, 13
firewall policies (Azure Firewall Manager), 54–57
firewalls. *See also* Azure Firewall; WAF (Web Application Firewall)
features in Azure, 13–15
host firewalls, 14
hypervisor firewalls, 14
Windows Firewall, 14
flow logs (NSGs), 136
forced tunneling in Azure Firewall, 46–47
Front Door
Application Gateway with, 173–174
bot management rules, 98
documentation, 9
load balancing with, 82–83
overview, 5
OWASP rule tuning, 96–97
policy creation, 89–91
rule exclusions, 100–101
rule logic, 93–96
full URL filtering, 70–74

H

host firewalls, 14
hub and spoke architectures, 28–29, 167–168
hub virtual networks, 57–58
hunting, 159–161
hybrid architectures, 24–28, 168–169
hypervisor firewalls, 14

I

IDPS (intrusion detection and prevention systems), 68–70
incidents in Azure Sentinel, 150–152

ingress/egress policy baselines, 20–22
in-line architecture, 44
inspection. *See* traffic inspection
internet edge strategies, 20
intrusion detection and prevention systems (IDPS), 68–70
IP Flow Verify, 162–163
isolated architecture, 44, 166

K

Kubernetes, 175

L

Layer 3 attacks, 104
Layer 4 attacks, 104
Layer 4 load balancing, 81
Layer 7 load balancing, 81
least privilege principle, 36
legacy technologies, 22
Load Balancer
  documentation, 9
  overview, 4
load balancing
  in application design, 172–173
  with Application Gateway, 81–82
  with Front Door, 82–83
  Layers 4 and 7 load balancing, 81
logs. *See also* monitoring
  for Azure Bastion
    configuring, 134–135
    viewing, 135–136
  for Azure DDoS Protection, 119–120
    configuring, 132–133
    viewing, 134
  for Azure Firewall
    configuring, 124–126, 145–147
    viewing, 126–129
  data collection strategy, 176–177
  for NSGs (network security groups), 136–139
  purpose of, 123–124
  scaling, 139–140
  in Traffic Analytics
    configuring, 137–138
    viewing, 139
  for WAF (Web Application Firewall)
    configuring, 129–130
    viewing, 131

M

metrics for Azure DDoS Protection, 112–115
mitigation pipeline, 104–105
monitoring. *See also* logs
  architecture best practices, 176–178
  with Azure Sentinel
    custom rules, 153
    data connectors, 149–150
    hunting, 159–161
    playbooks, 156–159
    purpose of, 148–149
    rule templates, 150–152
    workbooks, 153–156
  with Network Watcher
    IP Flow Verify, 162–163
    purpose of, 161
    topology maps, 161–162
  with Security Center
    Azure Defender, 147–148
    custom policy definitions, 144–146
    purpose of, 141–142
    security policy recommendations, 142–144

N

network architectures. *See* architectures (Azure)
network attacks, 104
network controls, evolving security beyond, 20
network rules in Azure Firewall, 49–50
network security groups (NSGs)
  architecture best practices, 166–167
  Azure Firewall versus, 42
  logs, 136–139
network segmentation. *See* segmentation
network traffic logging. *See* logs
network virtual appliances (NVAs)
  Azure Firewall and, 43–44
  in DMZ architectures, 26–28
  in vWAN, 31–33
Network Watcher
  IP Flow Verify, 162–163
  overview, 7–8
  packet capture with, 74–77
  purpose of, 161
  topology maps, 161–162
networking services
  documentation, 8–9
  types of, 1–8
NSGs (network security groups)
  architecture best practices, 166–167
  Azure Firewall versus, 42
  logs, 136–139
NVAs (network virtual appliances)
  Azure Firewall and, 43–44
  in DMZ architectures, 26–28
  in vWAN, 31–33

O

Open Web Application Security Project, 93
OWASP rules, 93–97
  anomaly scoring, 96
  rule logic, 93–96
  tuning, 96–97

P

PaaS services
  Azure DDoS Protection for, 108
  integration, 169–170
  with Private Link
    documentation, 9
    overview, 2–3
packet capture with Network Watcher, 74–77
peering
  architecture best practices, 167–168
  in Azure Firewall, 39–40
  documentation, 8
  overview, 2
perimeter models, 10–11
perimeter-based networks, 17, 20
playbooks (Azure Sentinel), 156–159
policies
  logs, 139–140
  Security Center
    custom definitions, 144–146
    recommendations, 142–144
  WAF (Web Application Firewall). *See also* rules
    creating, 85–91
    deployment and tuning, 92–93, 101–102
    managing, 91–92
principle of least privilege, 36
Private Link
  Azure Firewall and, 43
  documentation, 9
  overview, 2–3
protocol attacks, 104
public IP addresses, 38, 104–105

Q

Q10 (Quantum 10 architecture), 12

R

RBAC (role-based access control), 171–172
remote access, 171–172
resource logs. *See* logs
routing in Azure Firewall, 40–42, 168
rule processing (Azure Firewall), 53
rules
  Azure Firewall, 49
    application rules, 50–51
    DNAT rules, 51–53
    firewall policies and, 55–57
    network rules, 49–50
  Azure Sentinel
    custom, 153
    templates, 150–152
  WAF (Web Application Firewall)
    bot management, 97–98
    custom, 98–100
    exclusions, 100–101
    OWASP, 93–97
    policy deployment and tuning, 92–93, 101–102
    purpose of, 92

S

scaling logs, 139–140
secured virtual hubs, 58
security architecture, 10–11
Security Center
  Azure Defender, 147–148
  purpose of, 141–142
  security policies
    custom definitions, 144–146
    recommendations, 142–144
security monitoring. *See* monitoring
security policies
  custom definitions, 144–146
  recommendations, 142–144
segmentation
  principle of least privilege, 36
  reference model, 18–19
service endpoints
  documentation, 9
  overview, 2–3
shared responsibility model, 11
shared services, 31–32
side-by-side architecture, 44
simple virtual network architecture, 165–167
SNAT (Source Network Address Translation), 47
subnet security, 22

T

templates for Azure Sentinel rules, 150–152
testing Azure DDoS Protection with BreakingPoint Cloud, 115–117
  metrics, 112–115
  purpose of, 112

third-party security services with Azure Firewall Manager, 59–60
TLS inspection, 64–68
  configuring Azure Firewall for, 66–68
  creating certificates, 65–66
  full URL filtering, 70–74
  validating, 72–74
topology maps, 161–162
Traffic Analytics
  configuring, 137–138
  viewing logs, 139
traffic inspection
  Azure Firewall, 48
  Azure Firewall Premium
    deploying, 63–64
    full URL filtering, 70–74
    IDPS settings, 68–70
    purpose of, 61–62
    TLS inspection, 64–68
  components of, 61
  packet capture with Network Watcher, 74–77
traffic management in Azure Firewall
  forced tunneling, 46–47
  NSGs (network security groups), 42
  NVAs (network virtual appliances), 43–44
  Private Link, 43
  routing, 40–42, 168
  SNAT (Source Network Address Translation), 47
  virtual network peering, 39–40
Traffic Manager
  documentation, 9
  overview, 4
transit connectivity, 30–31
transport layer attacks, 104
tuning
  OWASP rules, 96–97
  WAF policies, 92–93, 101–102

U

URL filtering, 70–74

V

validating
  Azure DDoS Protection
    with BreakingPoint Cloud, 115–117
    metrics, 112–115
    purpose of, 112
  TLS inspection, 72–74
viewing logs
  for Azure Bastion, 135–136
  for Azure DDoS Protection, 134
  for Azure Firewall, 126–129
  in Traffic Analytics, 139
  for WAF (Web Application Firewall), 131
Virtual Networks. *See* VNets (Virtual Networks)
virtual WAN. *See* vWAN (virtual WAN)
visibility, 22
VNets (Virtual Networks)
  associating with DDoS Protection plan, 110–111
  documentation, 8
  hub virtual networks, 57–58
  isolation, 166
  overview, 1–2
  peering
    architecture best practices, 167–168
    in Azure Firewall, 39–40
    documentation, 8
    overview, 2
  Private Link
    documentation, 9
    overview, 2–3
  routing, 168
  service endpoints
    documentation, 9
    overview, 2–3
volumetric attacks, 104
VPN Gateway
  documentation, 9
  overview, 6
vWAN (virtual WAN), 29–33
  connectivity, 30–31
  documentation, 9
  overview, 7
  resources, 29–30
  secured virtual hubs, 58
  security, 31–33

W

WAF (Web Application Firewall)
  Application Gateway with, 173–174
  Azure Firewall versus, 176
  deploying
    policy creation, 85–91
    policy management, 91–92
    requirements, 84–85
  integration of, 80
  load balancing
    with Application Gateway, 81–82
    with Front Door, 82–83
    Layers 4 and 7 load balancing, 81
  logs
    configuring, 129–130
    viewing, 131
  overview, 5
  purpose of, 79–80
  rule types
    bot management, 97–98
    custom, 98–100
    exclusions, 100–101
    OWASP, 93–97
    policy deployment and tuning, 92–93, 101–102
    purpose of, 92

types of, 83–84
web application security. *See* WAF (Web Application Firewall)
web categories (Azure Firewall), 71
Windows Firewall, 14
workbooks (Azure Sentinel), 153–156

Z

Zero Trust, 10–11, 17, 20