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
Microsoft Azure
Network Security

Nicholas DiCola
Anthony Roman
Microsoft Azure Network Security

Table of Contents

Cover
Title
Copyright
Contents at a Glance
Contents
Acknowledgments
About the authors
Foreword
Introduction
Chapter 1 Introduction to Azure Network Security
  Network connectivity
  Current threats and challenges
  Azure Network Security
    Core security and firewall features
  Summary
Chapter 2 Secure Azure Network architectures
  Best practices
  Network architectures
    Cloud native
    Hybrid connectivity
    Hub and spoke
    Azure Virtual WAN
Table of Contents

Summary

Chapter 3 Controlling traffic with Azure Firewall

The role of Azure Firewall in secure architecture
  Network segmentation for security
  What is Azure Firewall?
  Understanding Firewall components
  Getting traffic to Azure Firewall
  Integrating with other traffic management

Advanced features
  DNS settings
  Forced tunneling
  SNAT Control
  Traffic inspection

Rule types
  Network rules
  Application rules
  DNAT rules
  Rule processing

Azure Firewall Manager
  Firewall policies
  Hub virtual networks
  Secured virtual hubs
  Third-party security services

Summary

Chapter 4 Traffic Inspection in Azure Networks

Azure Firewall Premium
  Deploying Azure Firewall Premium
  TLS inspection
Table of Contents

Intrusion detection and prevention
Using full URLs for traffic management
Network Watcher packet capture
Summary

Chapter 5 Secure application delivery with Azure Web Application Firewall
Integrating WAF into app delivery architecture
Load Balancing Options
WAF types
WAF deployment
Before deployment
Policy creation
Policy management
WAF rules and tuning
Policy deployment and tuning process
OWASP rules
Bot management rules
Custom rules
Exclusions
Policy assignment for tuning
Summary

Chapter 6 Mitigating DDoS attacks
How Azure DDoS Protection Works
The mitigation pipeline
DDoS Protection Basic versus Standard
DDoS Protection Options for PaaS Services
Enabling Azure DDoS Protection Standard
Create a DDoS Protection plan
# Table of Contents

Associate VNets to the DDoS Protection plan  
Finishing deployment  
Validation and testing  
Metrics  
Validation with BreakingPoint Cloud  
Log samples  
Application resiliency  

Summary  

Chapter 7 Enabling Network Security log collection  
Azure Firewall  
Web Application Firewall  
Azure DDoS Protection Standard  
Azure Bastion  
Network Security Groups  
Diagnostic settings at scale  
Summary  

Chapter 8 Security monitoring with Azure Sentinel, Security Center, and Network Watcher  
Security Center  
Security policies  
Custom policy definitions  
Azure Defender  

Azure Sentinel  
Data connectors for network security  
Analytic rules and incidents  
Custom Rules  
Workbooks  
Playbooks
Table of Contents

Hunting
Network Watcher
   Topology
   IP Flow Verify
Summary

Chapter 9 Combining Azure resources for a wholistic network security strategy
Simple virtual network design
   Virtual network isolation
   Network security groups
Hub-and-spoke topology
   VNet peering
Routing
   Hybrid Access
   Integrating PaaS services
Secure administrative access
   Remote access
   Role-based access control (RBAC)
Application design scenarios
   Application Gateway behind Front Door
   Azure Kubernetes application
   Firewall or WAF?
Network Security Monitoring
   Data collection strategy
   Cloud secure posture management
Summary
Index