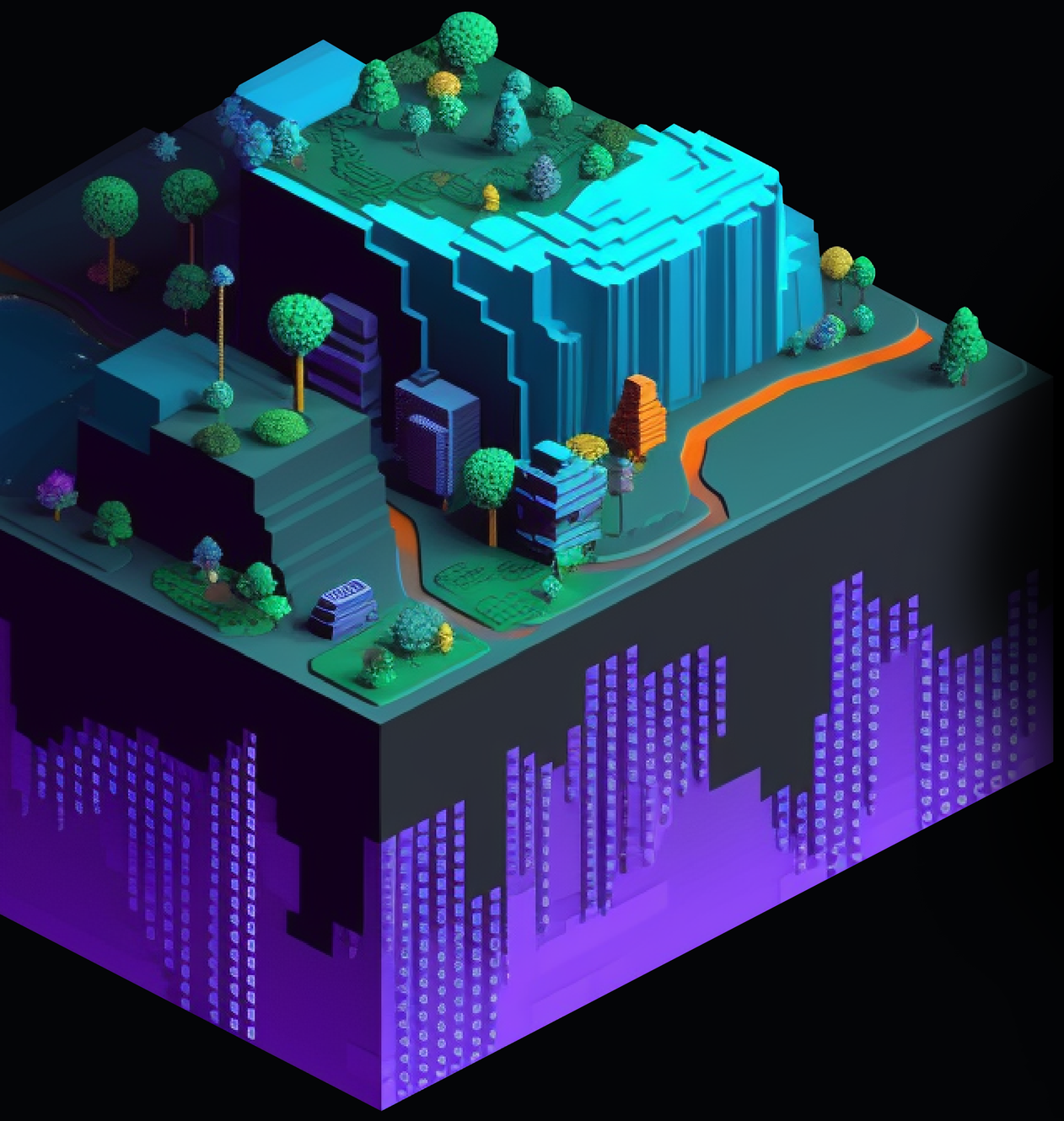
AZURE WITH NEO:

AZURE NETWORK SECURITY



FOLLOW THE
WHITE RABBIT

INTRODUCTION

Are you worried about the security of your Azure network? As a Microsoft Azure MVP, I understand the importance of securing your network to protect your business-critical applications and data. This comprehensive guide will take you through the top tips for Azure Network Security. You will learn about network patterns and anti-patterns. Further, I will discuss the latest technologies and their best security practices; you will learn about technologies such as Virtual Networks, Private Links, Azure DNS, Express Route, Firewall, Front Door, Load Balancer, Network Watcher, Route Server, VPN Gateway, NAT Gateway, and DDoS Protection.

1.1 SECURE NETWORK PATTERNS

Network Segmentation: To minimize the possibility of unauthorized entry, it is crucial to segregate network traffic. The utilization of Azure Network Security Groups (NSGs) can regulate access to network resources.

Hub and Spoke Architecture: The network design aims to enhance network security by centralizing traffic. The hub holds the connectivity the spokes require, and all data passes through a central point. You’re able to control and oversee the traffic from a central point.

1.2 SECURE NETWORK PATTERNS

Network Virtual Appliances (NVAs): Virtual machines known as NVAs are responsible for executing network services, such as load balancers and firewalls. They offer extra protection and oversight of network traffic.

Network Address Translation (NAT): To enhance security and avoid unauthorized access, it is recommended to utilize NAT (Network Address Translation) to conceal the IP addresses of endpoints from the public internet. This reduces the possibility of a cyber attack and safeguards the system. You can leverage Azure Firewall or NAT Gateway to achieve this.

1.3 SECURE NETWORK PATTERNS

DDoS Protection: Azure DDoS Protection is a tool that safeguards your applications and services from DDoS attacks by preventing service interruption or downtime.

Network Monitoring: To identify security risks, it is important to monitor traffic and activity consistently. You can utilize Azure Network Watcher, which can help monitor network performance, solve network problems, and identify irregularities.

Capacity Planning: It is important to ensure adequate capacity planning to avoid unnecessary expenses and over or under-provisioning network resources.

2.1 NETWORK ANTI-PATTERNS

Lack of Network Segmentation: When resources are not adequately isolated and grouped, it can lead to a flat network architecture vulnerable to lateral movement and increased attack surface.

Overly Permissive Network Security Groups: Allowing unrestricted traffic within or between networks can lead to unintended resource access and data breaches.

Inadequate Authentication and Authorization: Poor access controls and weak authentication mechanisms can lead to unauthorized access to resources and data.

2.2 NETWORK ANTI-PATTERNS

Failure to Use Encryption: Failing to encrypt sensitive data in transit and at rest can lead to data breaches and regulatory non-compliance.

Improper DNS Configuration: Misconfigured DNS settings can lead to DNS cache poisoning and other attacks.

Use of Deprecated Protocols and Services: Continuing to use deprecated protocols and services can lead to security vulnerabilities that are no longer patched by vendors.

2.3 NETWORK ANTI-PATTERNS

Unsecured Endpoints: Allowing endpoints to go unpatched and unprotected can lead to attackers using these endpoints to access the network and its resources.

Lack of Monitoring and Logging: Without monitoring and logging capabilities, it can be difficult to detect and respond to security incidents in a timely manner.

Unsecured Endpoints: Allowing endpoints to go unpatched and unprotected can lead to attackers using these endpoints to access the network and its resources.

3.1 VIRTUAL NETWORKS

An Azure Virtual Network is a foundational building block for your Azure networks; it allows you to create your own isolated and private network in the cloud.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

3.2 VIRTUAL NETWORKS

Security Best Practices

- Use subnets within a Virtual Network to separate different types of resources and enforce access control.
- Use Network Security Groups to filter network traffic to and from virtual machines.
- Use Azure Virtual Network Peering to establish communication between different Virtual Networks.
- Implement Virtual Network Service Endpoints to provide secure and direct connectivity to Azure services such as Azure Storage and Azure SQL Database.
- Use Azure Private DNS Zones to resolve hostnames within your Virtual Network without needing a public DNS server.

4.1 PRIVATE LINKS

Private Links in Azure are a secure way to access Azure PaaS services from your virtual network without exposing them to the public internet. With Private Links, you can enhance the security of your services, improve network performance, and simplify network architecture. Here are some tips to optimize your use of Private Links.

4.2 PRIVATE LINKS

Security Best Practices

- Plan your network topology carefully to avoid conflicts with your existing infrastructure. Consider using different IP address ranges and subnets for your Azure resources.
- Use Azure Private DNS Zones to create a private domain name for your Azure resources and resolve them using the Azure-provided DNS servers.
- Enable Virtual Network Service Endpoints to restrict access to Azure services to a specific virtual network or subnet. This ensures that traffic to Azure services stays within your virtual network and doesn't traverse the public internet.
- Monitor your Private Links to detect unauthorized access attempts or anomalous behavior. Use Azure Network Watcher to monitor your network traffic, and enable Azure Monitor to receive alerts and notifications when anomalies occur.

5.1 AZURE DNS

Azure DNS is a powerful tool for hosting DNS domains and managing DNS records in Azure. Here are some tips for using Azure DNS for network security:

Security Best Practices

- Create private DNS zones for your virtual networks to resolve internal DNS names, preventing your internal DNS requests from being forwarded to the public internet.
- Configure your Azure DNS zones with private endpoint connections for secure and private connectivity between your virtual network and Azure DNS.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

5.2 AZURE DNS

Security Best Practices

- Use Azure DNS to create DNS Firewall rules that block access to known malicious domains or IP addresses to prevent malware infections and data exfiltration attempts.
- Configure DNS over HTTPS (DoH) to encrypt your DNS queries and responses, protecting against third-party eavesdropping and tampering.
- Monitor Azure DNS logs and configure alerts to detect suspicious activity, such as failed DNS queries or unauthorized zone modifications, and respond to potential security incidents quickly.

6.1 EXPRESS ROUTE

Azure ExpressRoute is a service that provides dedicated, private network connectivity between your on-premises infrastructure and Azure. Use ExpressRoute to establish private connectivity between your on-premises infrastructure and Azure, avoiding the public internet and reducing your attack surface.

6.2 EXPRESS ROUTE

Security Best Practices

- Ensure your ExpressRoute circuit is secured with appropriate access controls and network segmentation to prevent unauthorized access.
- Use ExpressRoute to establish private connectivity to Azure PaaS services, such as Azure SQL Database, without exposing them to the public internet. This can help reduce your services' attack surface and improve network performance.
- Use Azure Firewall and Azure Firewall Manager to manage and secure your ExpressRoute traffic centrally, apply network security policies, and inspect and filter traffic based on application and network-layer criteria.
- Monitor your ExpressRoute circuit for potential security incidents, such as unauthorized access attempts or unusual traffic patterns, using Azure Network Watcher and Azure Monitor.

7.1 AZURE FIREWALL

Azure Firewall is a network security service that allows you to protect your Azure virtual network resources. It provides high availability, scalability, and built-in support for multiple protocols and threat intelligence.

Security Best Practices

- Use Azure Firewall to enforce application and network-level security policies, including filtering traffic based on source and destination IP addresses, ports, and protocols. This can help to prevent unauthorized access and block known threats.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

7.2 AZURE FIREWALL

Security Best Practices

- Configure Azure Firewall to inspect outbound traffic for malicious activity or data exfiltration attempts. This can help to prevent data loss and ensure compliance with data protection regulations.
- Utilize Azure Firewall's integration with Azure Monitor and Azure Sentinel to monitor and analyze network traffic and detect security incidents. This can help you quickly identify and respond to potential threats before they escalate.
- Implement Azure Firewall's high availability and disaster recovery features to ensure your network security is always operational and available, even during unexpected outages or disasters.
- To further enhance your network security posture, consider integrating Azure Firewall with other Azure security services, such as Defender Products and Azure Active Directory.

8.1 AZURE LOAD BALANCER

Azure Load Balancer is a highly available and scalable Layer-4 load balancer that helps distribute traffic to healthy service instances. It provides a variety of traffic distribution methods and supports inbound and outbound scenarios.

8.2 AZURE LOAD BALANCER

Security Best Practices

- Enable SSL/TLS encryption for your endpoints to secure communication between the client and the backend instances.
- Use custom health probes instead of the default ones to ensure that only the required ports and protocols are open on the instances.
- Configure load balancing rules to support different scenarios, such as directing traffic to a specific endpoint based on the request path.
- Use the outbound rules feature to route traffic from your backend instances to specific destinations, such as a specific IP address or a DNS name.
- Use multiple load balancers in different regions to ensure high availability and failover in case of a disaster.

9.1 AZURE APPLICATION GATEWAY

Azure Application Gateway is a Layer 7 load balancer that allows you to manage traffic to your web applications. It offers various features such as SSL offloading, URL-based routing, and session affinity, to name a few. In addition, it can scale up and down based on traffic patterns and provide high availability for your applications.

Security Best Practices

- Use HTTPS for all traffic to your web applications. Azure Application Gateway provides SSL offloading capabilities, which allow you to terminate SSL traffic at the gateway and send plain HTTP traffic to your web servers.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

9.2 AZURE APPLICATION GATEWAY

Security Best Practices

- Enable Web Application Firewall (WAF) protection for your web applications. Azure Application Gateway provides WAF capabilities to protect your applications from common web vulnerabilities, such as SQL injection and cross-site scripting (XSS).
- Use URL-based routing to direct traffic to the appropriate backend pool. This can help simplify your network architecture and improve your application's performance.
- Configure session affinity to ensure that client requests are directed to the same backend server. This can improve your application's performance and provide a better user experience.
- Monitor your Azure Application Gateway logs to detect unauthorized access attempts or suspicious activity. You can use Azure Monitor to create alerts and notifications when anomalies occur.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

10.1 AZURE FRONT DOOR

Azure Front Door is a global service that offers a scalable and secure entry point for your web applications and APIs. With Azure Front Door, you can improve the user experience by optimizing global routing and load balancing while providing advanced security features to protect against malicious attacks.

Security Best Practices

- Use Front Door features to improve your network's security. These include SSL offloading, Web Application Firewall, DDoS protection, and authentication and authorization.

10.2 AZURE FRONT DOOR

Security Best Practices

- Front Door allows you to route traffic to your backend based on multiple criteria, such as URL path, domain name, and geographic location.
- Use Front Door to segment your network by creating separate routing rules for different types of traffic or backend resources. This will limit the exposure of your sensitive resources to the public internet and reduce the risk of unauthorized access.
- Use Front Door built-in DDoS protection that can help mitigate a DDoS attack's impact.
- You can use Front Door to block traffic from specific geographic regions that may be associated with malicious activity.
- With Front Door, you can configure a custom domain name for your application, which can help to improve the user experience and brand recognition.

11.1 AZURE NETWORK WATCHER

Azure Network Watcher is a performance monitoring and diagnostic service for Azure networks. It provides a centralized and unified view of network resources and helps to diagnose network issues quickly and effectively.

Security Best Practices

- Enable Network Watcher in all your virtual networks to ensure that you have a centralized and unified view of network resources.
- Use Network Topology to view your network resources and ensure your virtual networks are properly segmented and isolated.
- Use Network Performance Monitor to monitor your network latency, packet loss, and network jitter to ensure that your network is performing optimally.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

11.2 AZURE NETWORK WATCHER

Security Best Practices

- Use Connection Monitor to monitor network connectivity between resources in different regions or virtual networks to detect issues early and prevent downtime.
- Use Packet Capture to capture network traffic for analysis and troubleshooting, especially for complex network issues.
- Use Network Security Group Flow Logs to analyze network traffic flowing through network security groups for security and compliance purposes.
- Monitor your Network Watcher logs and configure alerts to be notified of any suspicious activity, such as large numbers of failed network connections or unauthorized network modifications.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

12.1 AZURE ROUTE SERVER

Azure Route Server is a fully managed service that helps simplify your network topology and improve your network routing efficiency. Route Server allows you to route your traffic between virtual and on-premises networks without complex VPN gateways or routing appliances.

Security Best Practices

- Secure access to Route Server: Ensure that only authorized users have access to Route Server and follow the principle of least privilege. Use Azure AD for identity and access management, enabling multi-factor authentication for added security.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

12.2 AZURE ROUTE SERVER

Security Best Practices

- Implement network segmentation: Use Azure Virtual Networks to segment your network and restrict access to resources based on their roles and functions.
- Use route filters: Use route filters to restrict or allow traffic to and from specific IP addresses or address ranges and to enforce routing policies and traffic flow rules.
- Regularly monitor network traffic: Use Azure Network Watcher to monitor traffic and identify any anomalies or suspicious activity. Enable Azure Monitor to receive alerts and notifications when potential security incidents occur.
- Regularly review and update your routing policies: Regularly review and update your routing policies to ensure they align with your business objectives and security requirements.

13.1 AZURE VPN GATEWAY

Azure VPN Gateway enables users to establish a secure and encrypted connection between their on-premises infrastructure and Azure. It provides secure communication between remote sites, hybrid applications, and Azure services. The VPN Gateway service can be configured to support different VPN protocols, depending on the user's requirements. P2S VPN is used for remote access connections, while S2S VPN is used for site-to-site connectivity.

13.2 AZURE VPN GATEWAY

Security Best Practices

- Use strong authentication methods, such as Azure Active Directory, to authenticate VPN connections.
- Implement multi-factor authentication (MFA) to enhance security for VPN connections.
- Use a dedicated subnet for the VPN Gateway to ensure network isolation and prevent unauthorized access.
- Configure security rules and route tables to control inbound and outbound traffic.
- Monitor VPN Gateway traffic using Azure Network Watcher to detect and respond to security incidents.
- Implement Azure VPN Gateway redundancy for high availability and disaster recovery purposes.
- Use Azure Private DNS zones to resolve VPN Gateway endpoints, which can help to prevent DNS spoofing attacks.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

14.1 AZURE NAT GATEWAY

Azure NAT Gateway is a networking service in Azure that enables outbound Internet connectivity for virtual machines (VMs) within a virtual network. It provides source network address translation (SNAT) for virtual machines and can scale up to 64,000 active NAT rules. NAT Gateway is a highly available and resilient service deployed across multiple Azure Availability Zones.

Security Best Practices

- Apply network security groups (NSGs) to limit inbound traffic to the NAT Gateway. You can allow only traffic from specific IP addresses or ranges.
- Disable direct public IP address assignment for VMs in the virtual network. Use a NAT Gateway instead to ensure that all outbound traffic is sourced from a single IP address.

14.2 AZURE NAT GATEWAY

Security Best Practices

- Monitor NAT Gateway logs and enable Azure Monitor alerts to receive notifications about suspicious activity or traffic patterns.
- Use Standard tier NAT Gateway for greater scalability and resiliency. Basic tier NAT Gateway is limited to 16,000 active NAT rules and doesn't support high availability.
- Apply NSGs to limit traffic from the NAT Gateway to the Internet. You can allow only traffic to specific IP addresses or ranges and block all other traffic.
- Use Private Endpoints with NAT Gateway to ensure private and secure connectivity from on-premises networks to Azure. Private Endpoints enable you to access Azure services over a private IP address rather than a public IP address.
- Use Azure Bastion to securely access VMs in the virtual network over Remote Desktop Protocol (RDP) or Secure Shell (SSH) without exposing them to the public internet. This helps to reduce the attack surface of your network and prevent unauthorized access to your VMs.

15.1 AZURE DDOS PROTECTION

Azure DDOS Protection is a comprehensive, integrated solution designed to protect Azure resources from DDoS attacks. With Azure DDOS Protection, organizations can safeguard their networks against the most complex and sophisticated DDoS attacks, ensuring their applications and services remain available at all times.

15.1 AZURE DDOS PROTECTION

Azure DDOS Protection is a comprehensive, integrated solution designed to protect Azure resources from DDoS attacks. With Azure DDOS Protection, organizations can safeguard their networks against the most complex and sophisticated DDoS attacks, ensuring their applications and services remain available at all times.

15.2 AZURE DDOS PROTECTION

Security Best Practices

- Use Automatic attack mitigation: Azure DDOS Protection automatically detects and mitigates DDoS attacks in real-time, ensuring that your applications and services remain available.
- Use Integrated traffic monitoring: Azure DDOS Protection provides comprehensive traffic monitoring, giving you real-time visibility into your network traffic and enabling you to quickly detect and respond to potential attacks.
- Scale-out protection: Azure DDOS Protection scales out to protect your applications and services against even the largest DDoS attacks.

FOLLOW THE WHITE RABBIT

neopsyon
FOLLOW THE WHITE RABBIT

neopsyon.io

NEMANJA NEO JOVIĆ

MICROSOFT MVP

neopsyon.io

by x3.branding.com