Securing Azure Solutions with Private Endpoints

Advanced Networking Strategies for Platform Engineers

Today we'll explore how to implement secure, private networking for your Azure services using Private Endpoints—a critical capability for modern cloud architectures.

Why Azure Private Networking?

Traditional public endpoints create exposed attack surfaces that increase risk. With growing regulatory requirements and the shift toward Zero Trust security models, organizations need better solutions.

> Our objective is to completely lock down cloud-native services while maintaining full functionality and compliance.

Attack Surface Reduction

Public endpoints represent an unnecessary exposure risk that can be eliminated

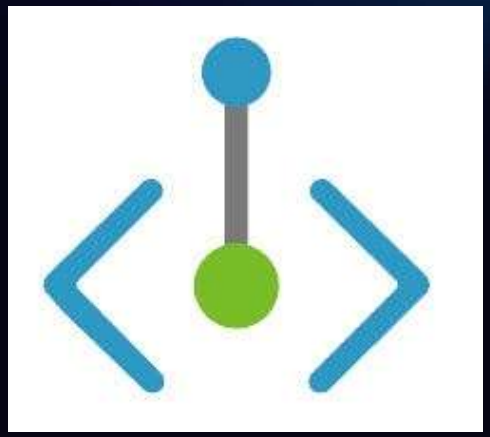
Regulatory Compliance

GDPR, HIPAA, and financial regulations increasingly require private network paths

Zero Trust Architecture

Private access is a foundational element of modern security frameworks

What is a Private Endpoint?



A Private Endpoint is a network interface that connects you privately and securely to Azure PaaS services through Private Link technology.

Private IP Address

Assigned from your VNet address space, making services appear as if they're inside your network

No Internet Exposure

Service resources are completely shielded from public internet access

DNS Integration

Private DNS zones automatically redirect service calls to private IPs

Key Components of Secure Private Endpoint Architecture

Azure VNet

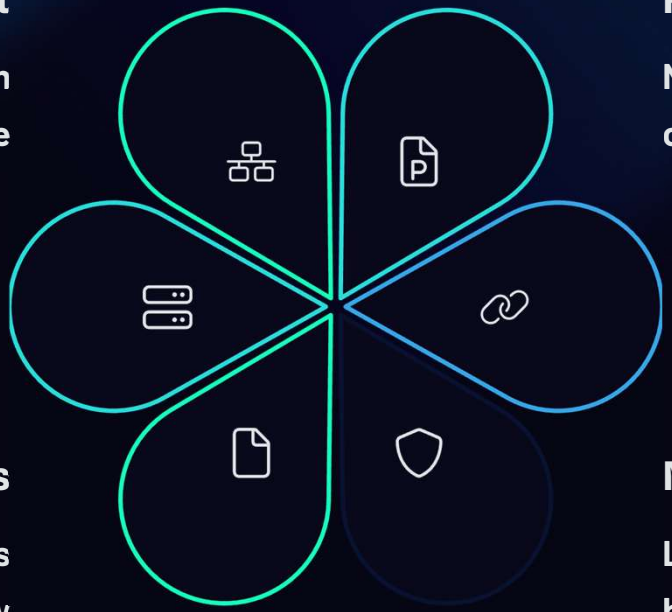
Your foundational network with private address space

Service Integration

Storage, SQL, Web Apps, Key Vault, and other Azure services

Private DNS Zones

Resolves service FQDNs to private IPs automatically



Private Endpoints

Network interfaces with private IPs connecting to services

Private Link Service

Optional component for exposing your own services privately

Network Security Groups

Layer 4 filtering for traffic control between subnets

Best Practices for Private Endpoint Deployment

1

Restrict Public Access First

Always disable or restrict public access to services before implementing Private Endpoints to prevent security gaps during transition

2

Implement Private DNS Zones

Set up and link Azure Private DNS Zones to your VNets to ensure transparent name resolution without application changes

3

Configure NSGs and UDRs

Lock down Network Security Groups and User Defined Routes to prevent potential data exfiltration paths and lateral movement

4

Monitor Network Traffic

Enable Azure Network Watcher and Defender for Cloud to gain visibility into private traffic patterns and detect anomalies

Security Benefits of Private Endpoints

Microsoft Backbone Traffic

Data stays within Microsoft's secure network infrastructure and never traverses the public internet

Defense in Depth

Adds network-level isolation beyond service-specific firewalls for true defense-in-depth

Zero Trust Implementation

Supports least-privilege access models by allowing granular network-level restrictions

Fine-Grained Control

Combines with Azure RBAC and NSGs for multi-layered access control to individual resources

Private Endpoint Scenarios

Secure Storage Access

Limit blob, file, and table storage access to private networks only, preventing data exfiltration while maintaining application functionality

Hybrid Connectivity

Connect on-premises networks to Azure PaaS services through ExpressRoute or VPN with private addressing end-to-end

Multi-Region Failover

Maintain private connections to services across regions for high availability while preserving security posture during failover events

Initial Network Design Before Private Endpoints

1

Public IP Exposure

All services have public endpoints accessible from the internet, protected only by service-level controls

2

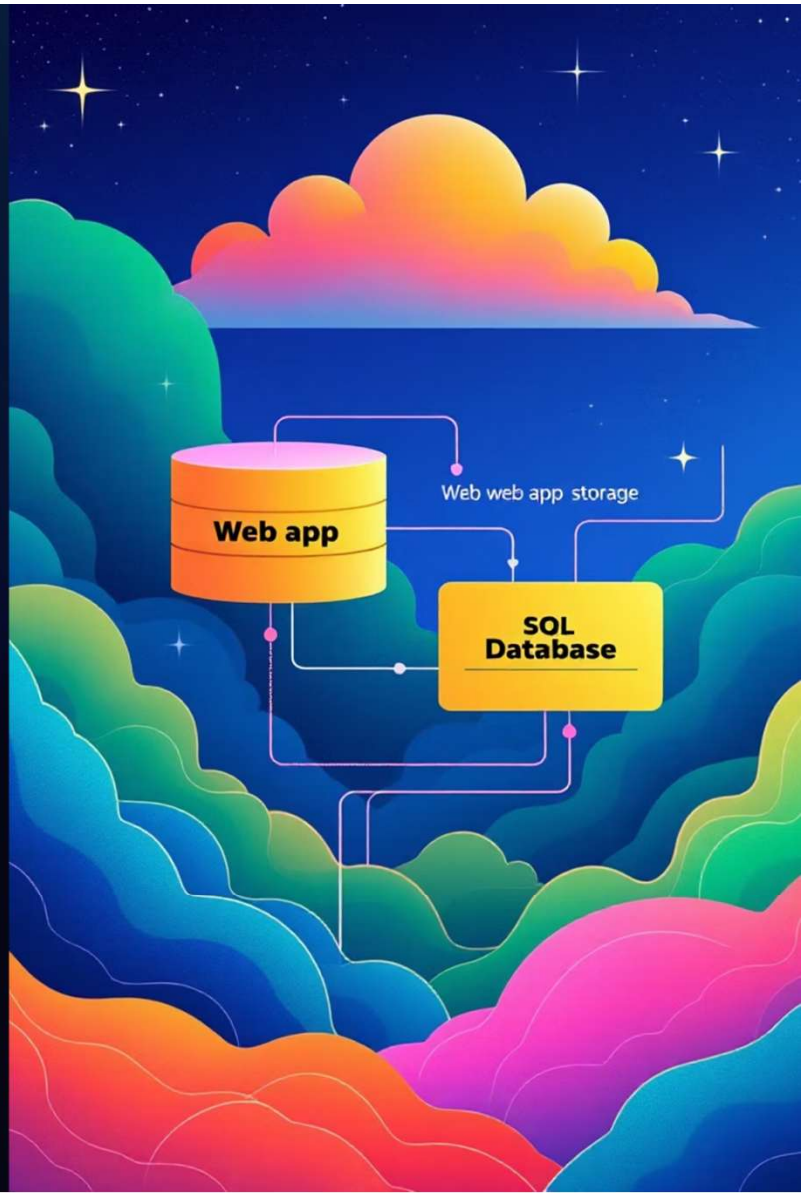
Limited Network Isolation

Resources communicate over public endpoints even when within the same virtual network

3

Service-Level Security Only

Reliance on service firewalls, access keys, and application-level authentication without network-layer protection



Adding Private Endpoints and Private DNS

Deploy Private Endpoints

Create private endpoints in your subnet for each Azure service you want to access privately

Configure Private DNS

Set up private DNS zones for each service and link to your VNet for automatic name resolution

Restrict Public Access

Configure service-level firewalls to deny public traffic while allowing private endpoint connections

Adding Private Endpoints and Private DNS

Deploy Private Endpoints

Create private endpoints in your subnet for each Azure service you want to access privately

Configure Private DNS

Set up private DNS zones for each service and link to your VNet for automatic name resolution

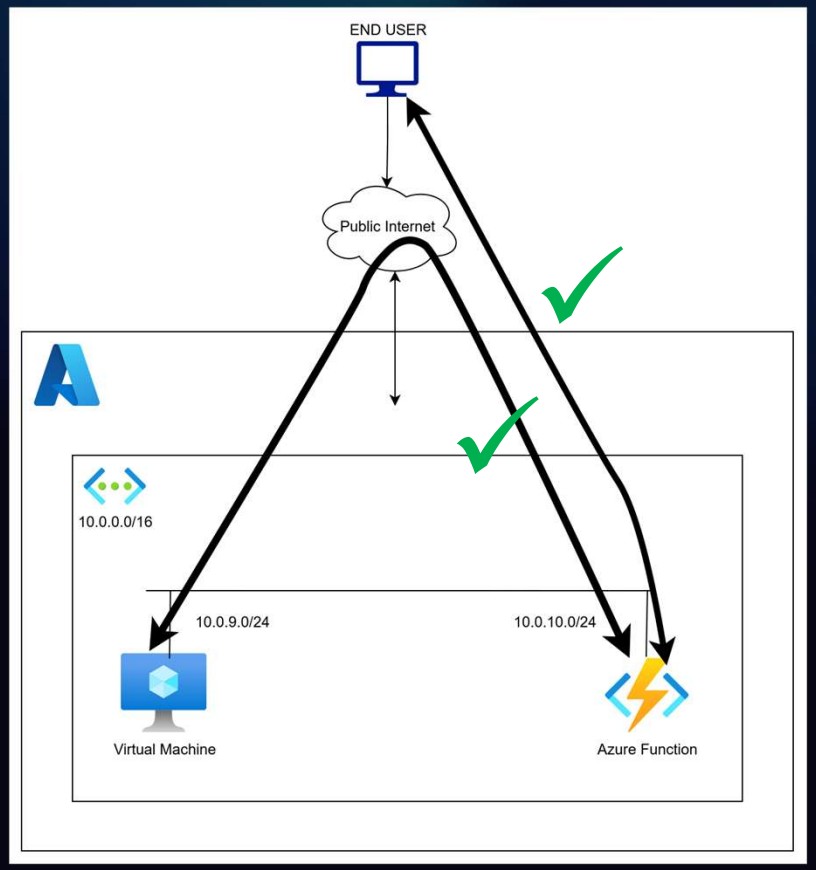
Restrict Public Access

Configure service-level firewalls to deny public traffic while allowing private endpoint connections

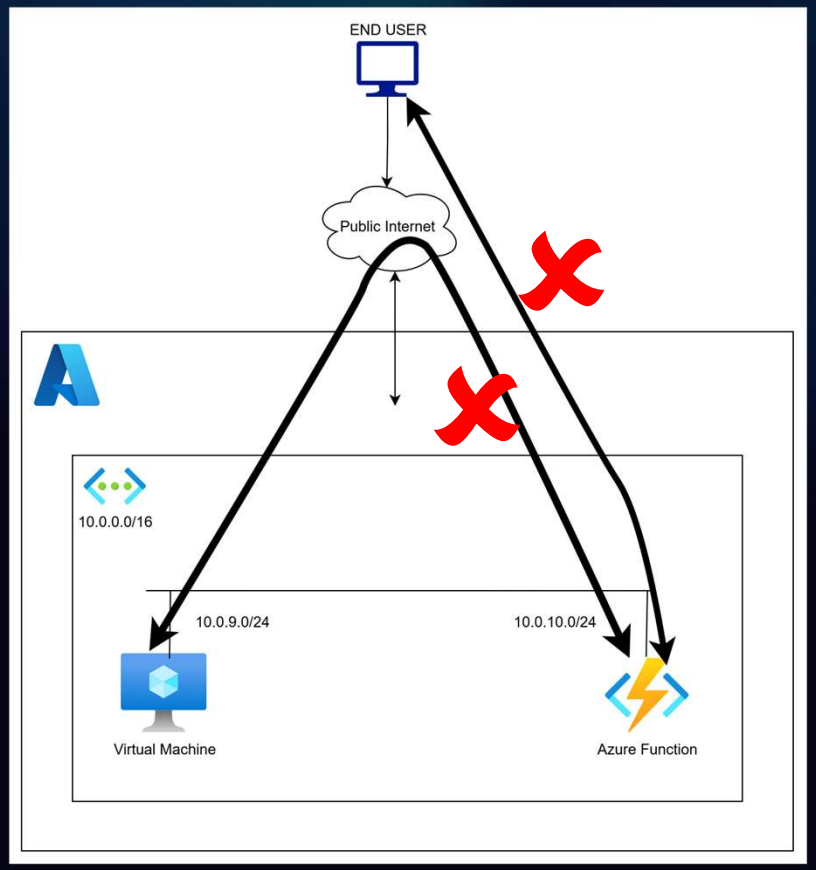
Lockdown: Live Demo

Time to see it in action!

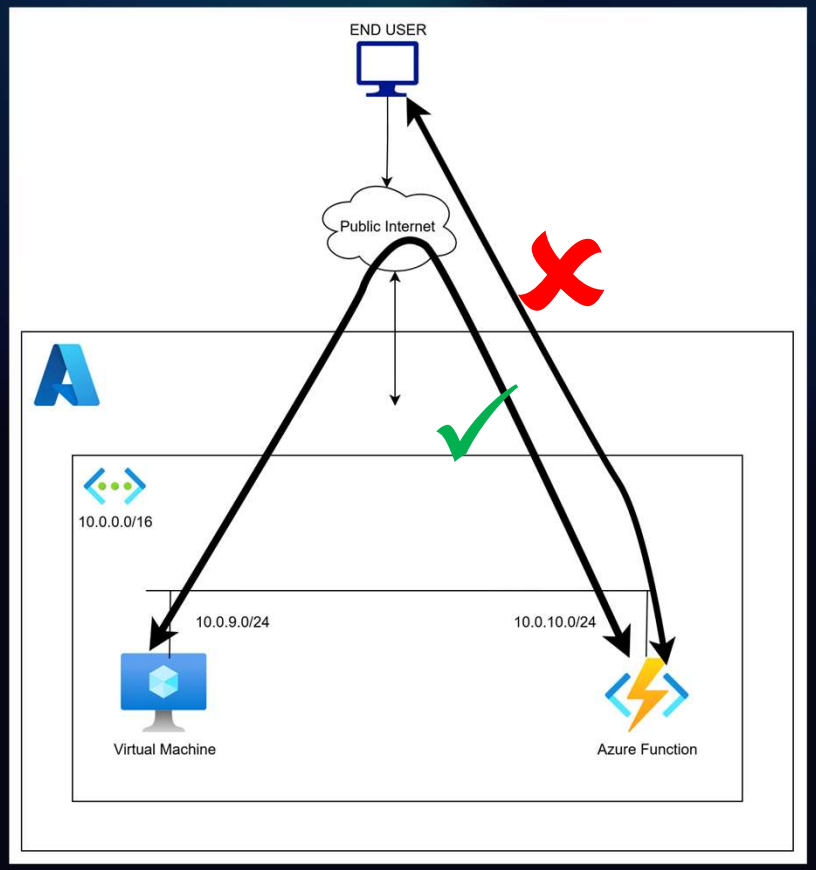
Phase 1: Wide Open



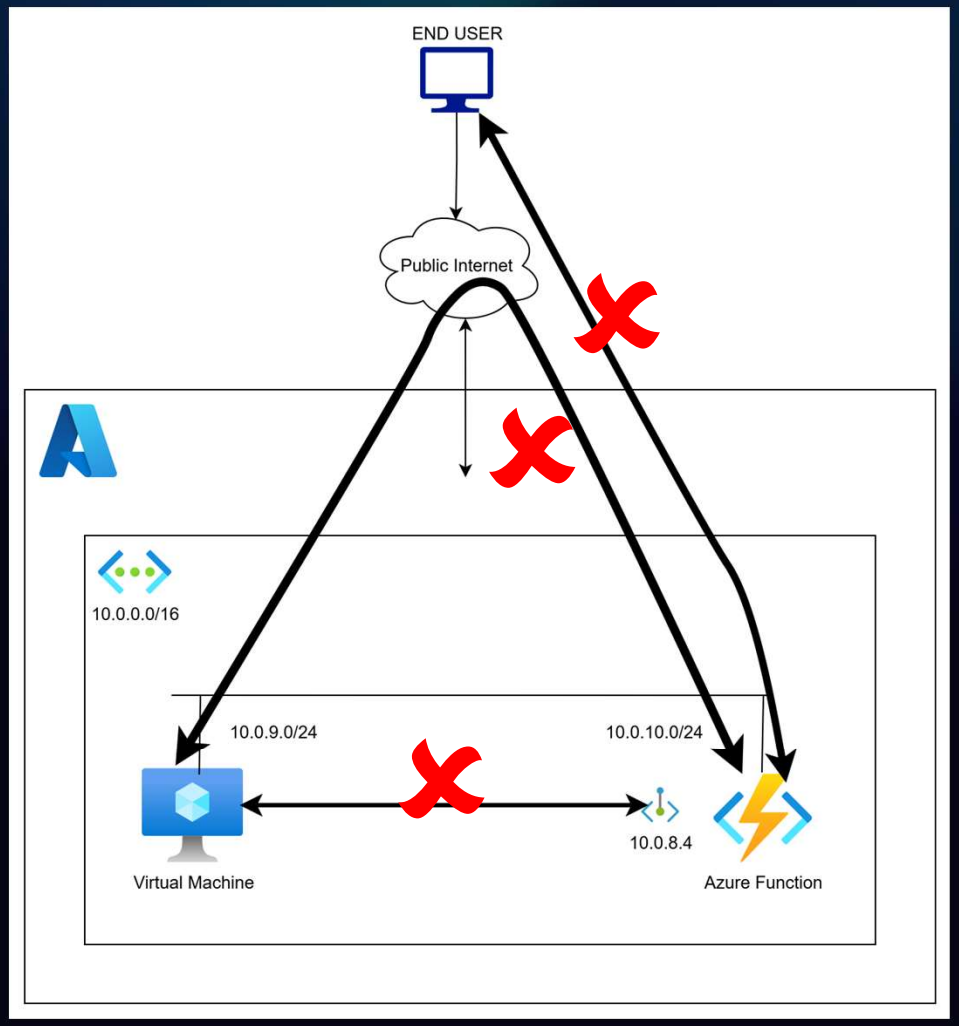
Phase 2: Locked Down



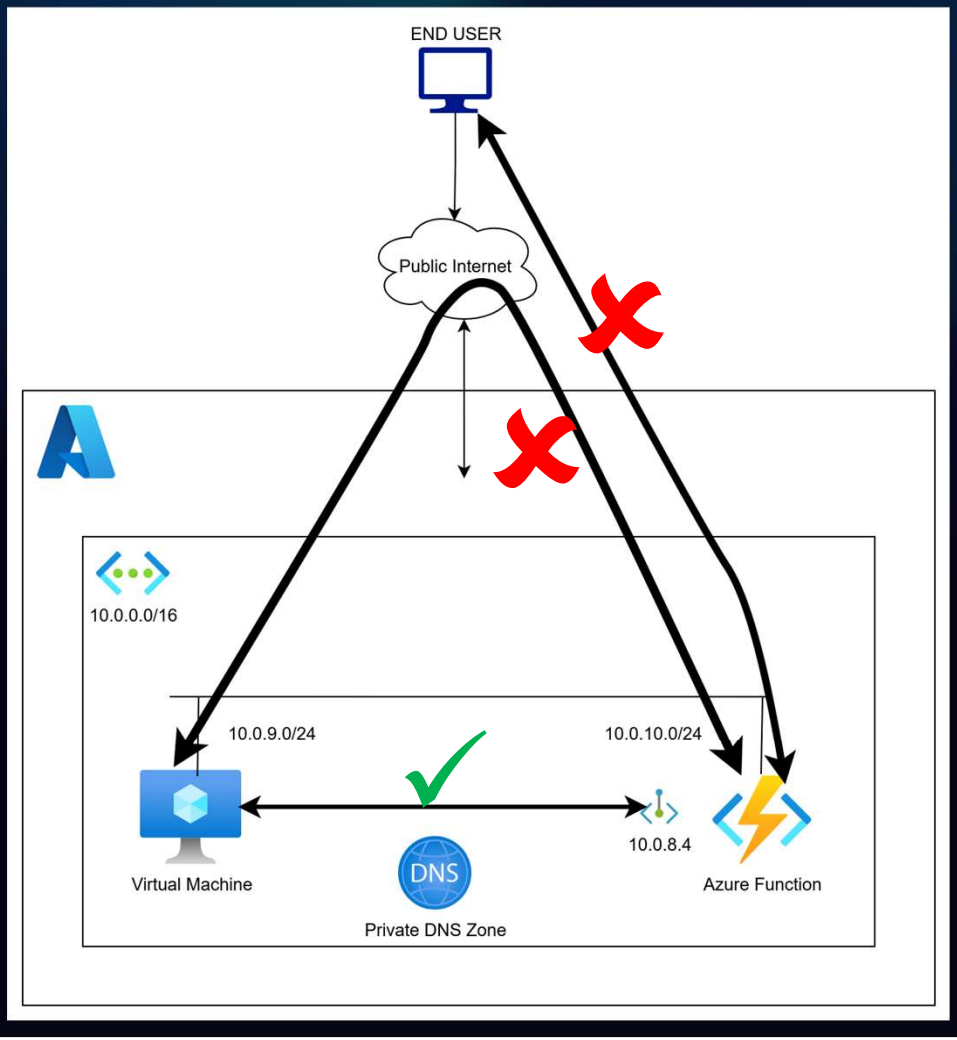
Phase 3: Locked Down with Firewall Allow List



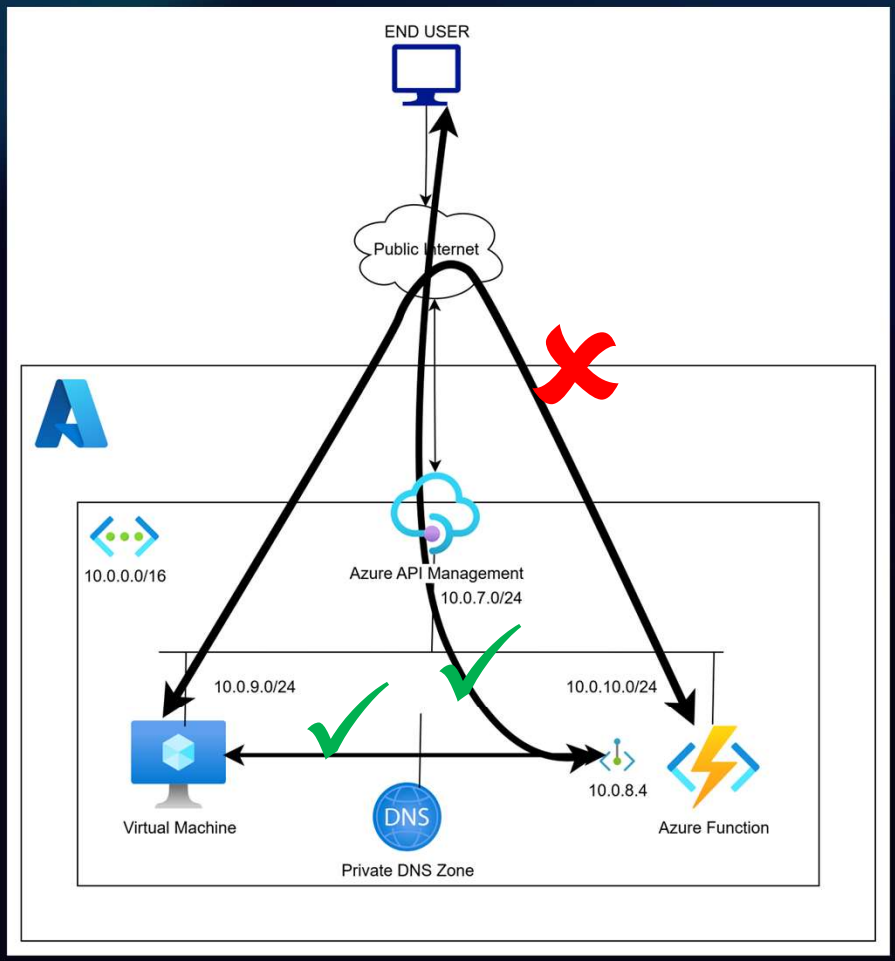
Phase 4: Locked Down with Private Endpoint



Phase 4: Locked Down with Private Endpoint + DNS



Phase 5: Locked Down with Private Endpoint + DNS + Public Access



Final Secure Design with Full Lockdown

Key Security Improvements:

- All service endpoints fully privatized with no public ingress
- NSGs configured to restrict traffic between subnets
- Private DNS resolution for seamless application connectivity
- API Management as the only controlled public entry point
- Complete network isolation of backend PaaS services

The final architecture achieves zero public exposure for critical Azure services while maintaining full functionality for authorized applications and users.