Protera

WHITE PAPER

Azure Landing Zones
Part 3

Author:

Eric MacDonald

VP of Cloud Transformation

TABLE OF CONTENTS

Protera

Networking & Connectivity Foundations

(HubSpoke, Virtual WAN, Hybrid, Segmentation, and Governance)

Networking is the backbone of any Azure Landing Zone (ALZ) implementation.
It determines how workloads communicate, how traffic flows between subscriptions, how hybrid integration occurs, and how governance and security are enforced.
The Cloud Adoption Framework (CAF) defines Network Topology and Connectivity as one of the eight foundational design areas.

This part of the series expands on that guidance explaining how to design, deploy, and operate a scalable, governed, and secure network platform for Azure.

1. Why networking is the backbone of every landing zone

Every Azure resource from VMs to App Services to storage accounts depends on network reachability.

If your landingzone network isn't wellstructured, you'll face immediate challenges: overlapping address spaces, adhoc peerings, unmonitored internet egress, and inconsistent firewall policies.
Microsoft's CAF calls networking "central to almost everything inside a landing zone."
A wellarchitected network model provides:

- Predictability – consistent address planning, route control, and DNS resolution.
- Security – centralized ingress/egress filtering, NSGs, and traffic inspection.
- Scalability – repeatable peering or Virtual WAN onboarding for new subscriptions.
- Governance – ability to enforce guardrails via management groups and Azure Policy.

Reference: Network topology and connectivity design area

2. The connectivity layer and the Platform Subscription

The CAF architecture divides the landingzone platform into functional layers: Identity, Connectivity, Management, and Security.

The Connectivity subscription (sometimes multiple) is where you host foundational networking components.

Key platform services:

Service	Purpose
Hub VNet or Virtual WAN Hub	Core routing and shared network services.
Azure Firewall / Firewall Policy	Central egress and ingress control.
Private DNS Zones	Centralized name resolution for private endpoints
VPN / ExpressRoute Gateway	Hybrid connectivity to onpremises.
Azure DDoS Protection Plan	Protects public endpoints across subscriptions.
Network Watcher & Flow Logs	Diagnostics and traffic analysis.

Each application landingzone (spoke) connects to this platform through VNet peering or Virtual WAN connections.

Reference: CAF – Platform and landingzone architecture

3. Choosing the right topology: HubSpoke vs Virtual WAN vs Hybrid

a. HubSpoke (classic enterprise pattern)

A hubspoke topology uses a central hub VNet that hosts shared services firewalls, DNS, and gateways with multiple spoke VNets for workloads.

Each spoke connects via VNet peering to the hub.

- Centralizes control and monitoring.
- Simplifies security by enforcing all egress through a shared firewall.
- Works well for smalltomedium environments or single regions.
- Requires manual management of peerings and route tables at scale.

Reference: Define an Azure network topology

b. Virtual WAN (largescale or global)

Azure Virtual WAN abstracts hubspoke management into a managed transit service.
It supports SDWAN integration, largescale VPN/ER connectivity, and global routing.
Each region can have a Virtual WAN hub automatically managing transit routing between spokes, VPNs, and ExpressRoute.

- Great for global organizations with many branches.
- Simplifies route propagation and transitive connectivity.
- Enables centralized security via Azure Firewall Manager.

Reference: Virtual WAN network topology

c. Hybrid or transitional approach

Many enterprises start with hubspoke and migrate to Virtual WAN over time.
You can combine both using Virtual WAN for global transit and regional hubspoke structures under it.
Azure Virtual Network Manager (AVNM) can enforce consistent peering and configuration across subscriptions.
Reference: Azure Virtual Network Manager overview

4. Addressing and segmentation strategy

Before deploying VNets, define an IP address plan that scales:

- Use nonoverlapping RFC 1918 ranges (10.x.x.x, 172.16.x.x, 192.168.x.x).
- Reserve large contiguous blocks for each region (e.g., 10.10.0.0/16 per region).
- Assign smaller /24/20 ranges per spoke or environment (dev/test/prod).
- Document allocations in version control to avoid overlap.
- Network segmentation should reflect both security tiers (frontend, backend, data) and organizational boundaries (business unit, environment).

Apply NSGs and Application Security Groups to isolate subnets within VNets.
Reference: Plan for landingzone network segmentation

5. Routing and egress control

Routing defines how traffic flows between VNets, regions, and the internet.

Hubspoke routing

- Configure User Defined Routes (UDRs) in spoke subnets to force traffic through the hub firewall.
- Disable “Allow gateway transit” unless you require spokes to use hub VPN/ER gateway.
- Use BGP for hybrid connections where available.

Egress design

- Default internet access directly from a spoke can violate compliance.
- Instead, force tunnel all egress via the hub firewall or ExpressRoute.
- Use firewall DNAT rules for inbound connections, or Application Gateway WAF for HTTP/S.

DNS integration

- Centralize name resolution with Private DNS Zones linked to all VNets.
- For hybrid, forward DNS queries from Azure to onprem resolvers through DNS proxies.

Reference: CAF – Egress and DNS considerations

6. Hybrid connectivity: VPN and Express Route

For hybrid or multisite deployments, you'll connect onpremises networks to Azure.

Option	Description	Use case
SitetoSite VPN	IPSec over public internet.	Quick setup, lower cost, suitable for dev/test or backup links.
ExpressRoute	Private MPLS/Carrier connection to Azure edge.	Production, regulated workloads, consistent performance.
Virtual WAN Hub	Aggregates VPN/ER, provides global routing.	Multibranch or global orgs.

Design notes:

- Use redundant VPN gateways or dual ExpressRoute circuits for HA.
- Enable BGP for route exchange.
- Avoid overlapping onprem CIDRs with Azure VNets.
- Test failover paths regularly.

Reference: Azure VPN Gateway documentation
Reference: ExpressRoute overview

7. Network security layers

Security should be enforced in multiple layers:

- Azure Firewall – central allow/deny and applicationlevel filtering.
- Network Security Groups (NSGs) – control intraVNet and subnet traffic.
- Application Security Groups (ASGs) – tag resources for policybased filtering.
- DDoS Protection Standard – shield public endpoints.
- Private Link / Private Endpoints – connect to Azure PaaS services without internet exposure.
- Web Application Firewall (WAF) – inspect HTTP/S traffic at Application Gateway or Front Door.

Apply policies through initiatives at your Platform and LandingZones management groups to enforce consistent configuration.
Reference: Azure network security best practices

Protera

8. Cross region and global connectivity

If your workloads span multiple regions:

- Deploy a hub (or Virtual WAN hub) per region.
- Connect hubs using global VNet peering or Virtual WAN interhub connectivity.
- Use consistent address schemes and firewall policies in each region.
- Store replicated logs in the Management subscription for global visibility.

Plan for region pairs Microsoft pairs each region with another for data residency and recovery (e.g., East US ↔ West US).
Design your network so that critical services can fail over between these pairs.

Reference: Azure regions and region pairs

9. Automation: NetworkasCode & guardrails

Networking must be automated and policydriven to remain consistent.
Infrastructure as Code (IaC):

- Use Bicep or Terraform modules for hubs, VNets, subnets, NSGs, peerings.
- Store templates in Git and deploy through pipelines.

Azure Virtual Network Manager (AVNM):

- Define network groups, topologies, and security rule collections.
- Apply configurations at the managementgroup scope for automatic compliance.
- Centralizes governance for multiple subscriptions.

Azure Policy examples:

- Allowed locations (for VNets).
- Deny public IP assignment.
- Enforce NSG on every subnet.
- Require DDoS Protection Plan on VNets.
- Tag “NetworkOwner” on all VNets.

These guardrails enforce alignment with the CAF principle: governance by design.

Reference: CAF – Platform automation design area

10. Monitoring and operations

Azure offers multiple native monitoring tools for network operations:

- **Network Watcher** – packet capture, topology visualization, connection troubleshooting.
- **Traffic Analytics** – NSG flow log visualization in Log Analytics.
- **Azure Monitor Metrics** – gateway throughput, packet loss, latency.
- **Connection Monitor** – continuous connectivity testing.
- **Defender for Cloud** – regulatory compliance view for network resources.

Implement alerts for:

- Gateway or peering failure.
- DDoS attack events.
- Unapproved network resource creation.
- Policy noncompliance.

Reference: Azure Network Watcher overview

11. Role separation: Platform vs Application networking

As with identity, enforce clear role boundaries.

Responsibility	Platform Team	Application Team
Hub / Virtual WAN deployment	✓	
ExpressRoute / VPN management	✓	
Firewall / DNS management	✓	
VNet creation (spokes)	(via vending pipeline)	✓
Subnet NSGs and ASGs		✓
App Gateway / WAF configs		✓
Policy governance	✓	

This model aligns with CAF's principle of subscription democratization giving application teams autonomy inside secure guardrails.

Reference: CAF – Design principles

12. Cost and performance considerations

Networking cost is often overlooked.

Key factors:

- Egress data transfer (to internet or between regions).
- Firewall Premium SKUs and Virtual WAN Hubs – fixed hourly charges.
- Private Link ingress/egress – metered per GB.
- ExpressRoute circuits – bandwidthtier and provider fees.

Use Azure Cost Management exports to attribute costs to connectivity subscriptions and allocate back to business units.

Performance tips:

- Place gateways close to workloads to minimize latency.
- Use accelerated networking and proximity placement groups for VMtoVM traffic.
- Monitor throughput with Azure Monitor metrics.

13. Operational playbooks

Every platform team should maintain network operations playbooks, for example:

- Hub or Virtual WAN outage – reroute traffic, switch to backup region.
- ExpressRoute failover – validate VPN tunnel backup.
- Firewall misconfiguration – emergency breakglass to restore baseline rules.
- Policy remediation – automated fix via pipeline when Azure Policy marks noncompliance.

Test playbooks quarterly and integrate them with your incident management process.

14. Example reference architecture (CAF aligned)

1. Root Management Group
   - Policy: allowed locations, tag inheritance.
2. Platform Management Group
   - Connectivity subscription: Hub VNet / Virtual WAN hub, Firewall, DNS, VPN / ExpressRoute.
   - Security subscription: Defender for Cloud, DDoS plan.
   - Management subscription: Log Analytics, Network Watcher.
3. Landing Zones Management Group
   - Application subscriptions: Spoke VNets peered to hub.
   - Policy: deny public IP, enforce NSG, route through hub.

Reference: CAF – Enterprise Scale architecture reference

15. Quickstart checklist

1. Decide topology (hubspoke, Virtual WAN, hybrid).
2. ✅ Reserve address space per region and per subscription.
3. ✅ Deploy a dedicated connectivity subscription.
4. ✅ Centralize firewalls, DNS, and DDoS plans.
5. ✅ Forcetunnel egress through approved paths.
6. ✅ Automate network provisioning with IaC and Policy.
7. ✅ Integrate Network Watcher and Traffic Analytics.
8. ✅ Define runbooks for hybrid connectivity and failover.

Field Kit & References

1. Network topology and connectivity (CAF) learn.microsoft.com/.../networktopologyandconnectivity
2. Define an Azure network topology learn.microsoft.com/.../defineanazurenetworktopology
3. Plan for landingzone network segmentation learn.microsoft.com/.../planforlandingzonenetworksegmentation
4. Virtual WAN network topology learn.microsoft.com/.../virtualwannetworktopology
5. Azure Virtual Network Manager learn.microsoft.com/azure/virtualnetworkmanager/overview
6. VPN Gateway overview learn.microsoft.com/azure/vpngateway/vpngatewayaboutvpngateways
7. ExpressRoute introduction learn.microsoft.com/azure/expressroute/expressrouteintroduction
8. Network security best practices learn.microsoft.com/azure/security/fundamentals/networkbestpractices
9. Network Watcher overview learn.microsoft.com/azure/networkwatcher/networkwatchermonitoringoverview
10. Platform automation design area learn.microsoft.com/azure/cloudadoptionframework/ready/landingzone/designarea/platformautomation

Protera

Protera.com