Hub-Spoke Network Topology

Internet

On-Premises
10.100.0.0/16

*VPN / ExpressRoute
(hybrid connectivity)*

Hub VNet: vnet-hub-{env}-{location}
Address Space: 10.0.0.0/16

AzureFirewallSubnet
10.0.1.0/24

GatewaySubnet
10.0.2.0/24

ManagementSubnet
10.0.3.0/24
SE: KeyVault, Storage

DNSResolverSubnet
10.0.4.0/24

Azure Firewall Premium
IDPS: Deny | Threat Intel: Deny
TLS Inspection: Configurable

VPN Gateway
VpnGw2 SKU
(toggleable)

ExpressRoute GW
(toggleable)

Private DNS Zones
- privatelink.vaultcore.azure.net
- privatelink.blob.core.windows.net
- privatelink.file.core.windows.net
- privatelink.database.windows.net
- privatelink.azurecr.io

pip-azfw
(Static, Standard)

DDoS Protection Plan
(toggleable, ~$2,944/mo)

peer-hub-to-production
allow_forwarded_traffic: true
allow_gateway_transit: conditional

peer-hub-to-staging

peer-hub-to-shared-services

Spoke VNet: Production
vnet-spoke-production-{env}-{location}
Address Space: 10.1.0.0/16

snet-web-production
10.1.1.0/24
SE: KeyVault

snet-app-production
10.1.2.0/24
SE: KeyVault, Sql

snet-data-production
10.1.3.0/24
SE: Sql, Storage

snet-private-endpoints
10.1.4.0/24
Network Policies: Disabled

RT: Forced Tunnel
0.0.0.0/0 → Firewall IP
BGP propagation: disabled

Spoke VNet: Staging
vnet-spoke-staging-{env}-{location}
Address Space: 10.2.0.0/16

snet-web-staging
10.2.1.0/24
SE: KeyVault

snet-app-staging
10.2.2.0/24
SE: KeyVault, Sql

snet-data-staging
10.2.3.0/24
SE: Sql, Storage

snet-private-endpoints
10.2.4.0/24
Network Policies: Disabled

Spoke VNet: Shared Services
vnet-spoke-shared-services-{env}-{location}
Address Space: 10.3.0.0/16

snet-tools
10.3.1.0/24
SE: KeyVault, Storage

snet-infrastructure
10.3.2.0/24
SE: KeyVault, Storage, ACR

snet-private-endpoints
10.3.3.0/24
Network Policies: Disabled

Legend

| Hub Subnet | Firewall | Spoke Subnet | Toggleable | VNet Peering | *SE = Service Endpoints* |