Tenants can choose from the following protocols for default tenant access:
- HTTPS
- ICMP
- Non

Customer creates NSGs to filter traffic from the tenant's workload.

Non-overlapping networks behind TI in tenant for fully routable environment. Overlapping space behind TI is supported as long as it is not routable beyond the TI and DNs are used.

For workload and tenant access:
- Options for the tenant to choose from for default routing to the Internet.
- Tenant A leverages the ExpressRoute connection to their own Azure VNet for Internet, so the default route is via ExpressRoute.
- Tenant B & C opted for a public IP on their Tier 1 for Internet access.

Tenant on-premises requires Internet connectivity from tenant workloads.

ExpressRoute.

Currently only Layer 7 LB is supported by Azure LB for tenant workloads.

NAT Rules for workload and tenant access.
- Customer will allocate public IPs in tenant’s subscription and NAT to the internal network IP of the tenant workload.

Tier Gateway firewall rules will govern access to tenant workloads.

Internet Load Balancers for Internet traffic workload.
- Currently only Layer 7 LB is supported by Azure LB or Azure VNet for tenant workloads.
- Tier Gateway will provide NAT of the external IP to the internal IP of the tenant segment.

Service Endpoint
This will allow connectivity to services leveraging Azure Native Services (Azure Blob Storage, Azure File Storage, Azure Synapse Analytics, etc.) and traditional Virtual Machines to tenants.
- Allow access from/to VNet subnets and External Network segments in the Compute Gateway and through Tier1, VPN and Firewall Rules.

Deploying infrastructure VMs inside Azure VMware Solution is recommended to provide reliability and performance to the application workloads. Usual infrastructure components are but not limited to:
- Active Directory (ADDC might be considered)
- DNS Server
- Backup Server

©2020 VMware, Inc. – Designed by the Cloud Provider Software Technical Product Management team
This reference architecture provides a generic guidance to start deploying VMware Cloud Director service with Azure VMware Solution as a multi-tenant solution accessed by customer end-users.

All networking information depicted here is generic examples and can be customized as per provider's need.

On-Prem connectivity
IPsec VPN or ExpressRoute between MSP on-prem datacenter and customer Vnet.
- Policy-based VNet. Subnets have to be declared on both sides during the setup. One tunnel is created per subnet. It is recommended to use large subnets.
- Route-based VNet. Subnets are automatically advertised through BGP. BGP configuration is mandatory, no static route can be configured on GCVE.

Firewall rules for vCenter Access.
If On-Prem connectivity is configured, allow infrastructure on-prem subnets to access vCenter & ESXi (allowing remote console, vMotion and possibly Hybrid Linked Mode).
- Otherwise, access can be allowed from public Internet but it is highly recommended to limit it to few trusted public IPs (not detailed here)

On-Prem Firewall
Access from on-prem subnets to Azure VMware Solution Management segment (or at least vcenter and ESXi). Access from GCVE to on-prem infrastructure services (Active Directory, DNS, Content Library, ...)

Routed Network Segments
- One infrastructure segment with privileged access to Management component (vCenter, NSX, ...)
- One or multiple workload segments where all the applications VMs will be deployed.

Firewall rules for Network segments
- Allow connectivity between Infra & Management
- Allow connectivity between Infra & on-prem infrastructure subnet
- Allow connectivity between workload segment, VNets and on-prem application subnets

Infrastructure VMs
Deploying infrastructure VMs inside Azure VMware Solution is recommended to provide reliability and performance to customer workloads. Usual infrastructure components are (but not limited):
- Active Directory (DDC might be considered)
- DNS Server
- Backup Server

DNS Configuration
On-prem DNS should be integrated with Azure DNS

Service Endpoint
This will allow connectivity from the Provider or the customer subscription to services leveraging Azure Native Services (Azure Blob Storage, Azure File Storage, Azure Synapse Analytics, etc) and traditional Virtual Machines to tenants
- Allow access from VNet subnets and External Network segments in the Compute Gateway and through IPsec VPN and Firewall Rules.