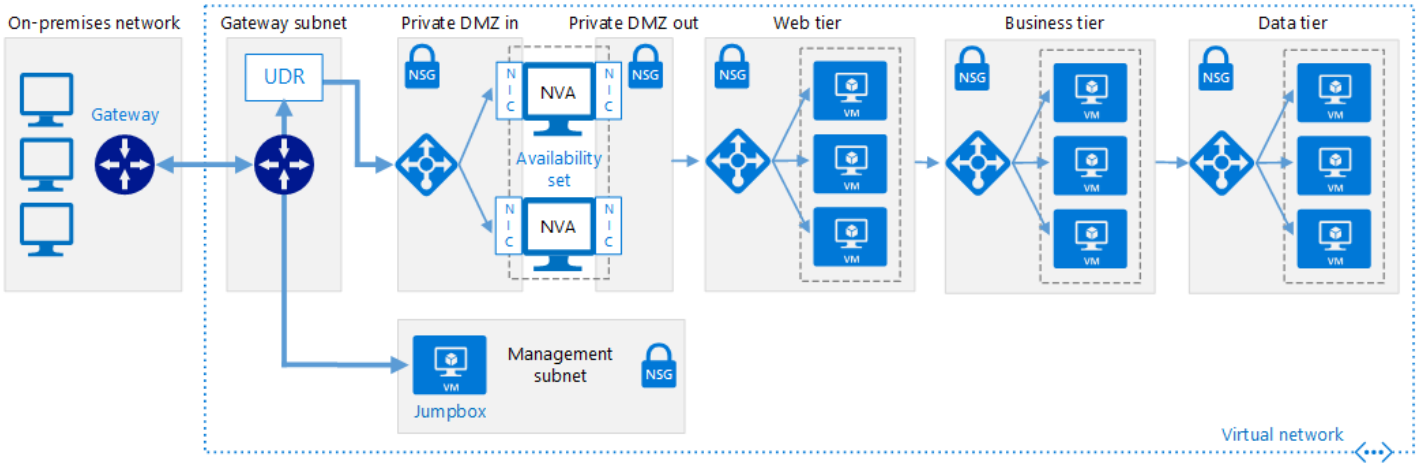
Software Defined Networking: Cloud DMZ

02/11/2019 • 2 minutes to read • Contributors

In this article

Cloud DMZ assumptions
Learn more

The Cloud DMZ network architecture allows limited access between your on-premises and cloud-based networks, using a virtual private network (VPN) to connect the networks. Although a DMZ model is commonly used when you want to secure external access to a network, the Cloud DMZ architecture discussed here is intended specifically to secure access to the on-premises network from cloud-based resources and vice versa.



This architecture is designed to support scenarios where your organization wants to start integrating cloud-based workloads with on-premises workloads but may not have fully matured cloud security policies or acquired a secure dedicated WAN connection between the two environments. As a result, cloud networks should be treated like a demilitarized zone to ensure on-premises services are secure.

The DMZ deploys network virtual appliances (NVAs) to implement security functionality such as firewalls and packet inspection. Traffic passing between on-premises and cloud-based applications or services must pass through the DMZ where it can be audited. VPN connections and the rules determining what traffic is allowed through the DMZ network are strictly controlled by IT security teams.

Cloud DMZ assumptions

Deploying a cloud DMZ includes the following assumptions:

- Your security teams have not fully aligned on-premises and cloud-based security requirements and policies.
- Your cloud-based workloads require access to limited subset of services hosted on your on-premises or third-party networks, or users or applications in your on-premises environment need limited access to cloud-hosted resources.
- Implementing a VPN connection between your on-premises networks and cloud provider is not prevented by corporate policy, regulatory requirements, or technical compatibility issues.
- Your workloads either do not require multiple subscriptions to bypass subscription resource limits, or they involve multiple subscriptions but don't require central management of connectivity or shared services used by resources spread across multiple subscriptions.

Your cloud adoption teams should consider the following issues when looking at implementing a Cloud DMZ virtual networking architecture:

- Connecting on-premises networks with cloud networks increases the complexity of your security requirements. Even though connections between cloud networks and the on-premises environment are secured, you still need to ensure cloud resources are secured. Any public IPs created to access cloud-based workloads need to be properly secured using a public facing DMZ or Azure Firewall.
- The Cloud DMZ architecture is commonly used as a stepping stone while connectivity is further secured and security policy aligned between on-premises and cloud networks, allowing a broader adoption of a full-scale hybrid networking architecture. However, it may also apply to isolated deployments with specific security, identity, and connectivity needs that the Cloud DMZ approach satisfies.

Learn more

For more information about implementing a Cloud DMZ in Azure, see:

- Implement a DMZ between Azure and your on-premises datacenter. This article discusses how to implement a secure hybrid network architecture in Azure.