6.Azure Networking

Cloud Advanced

Klaas Thys
klaas.thys@pxl.be

6.Azure Networking

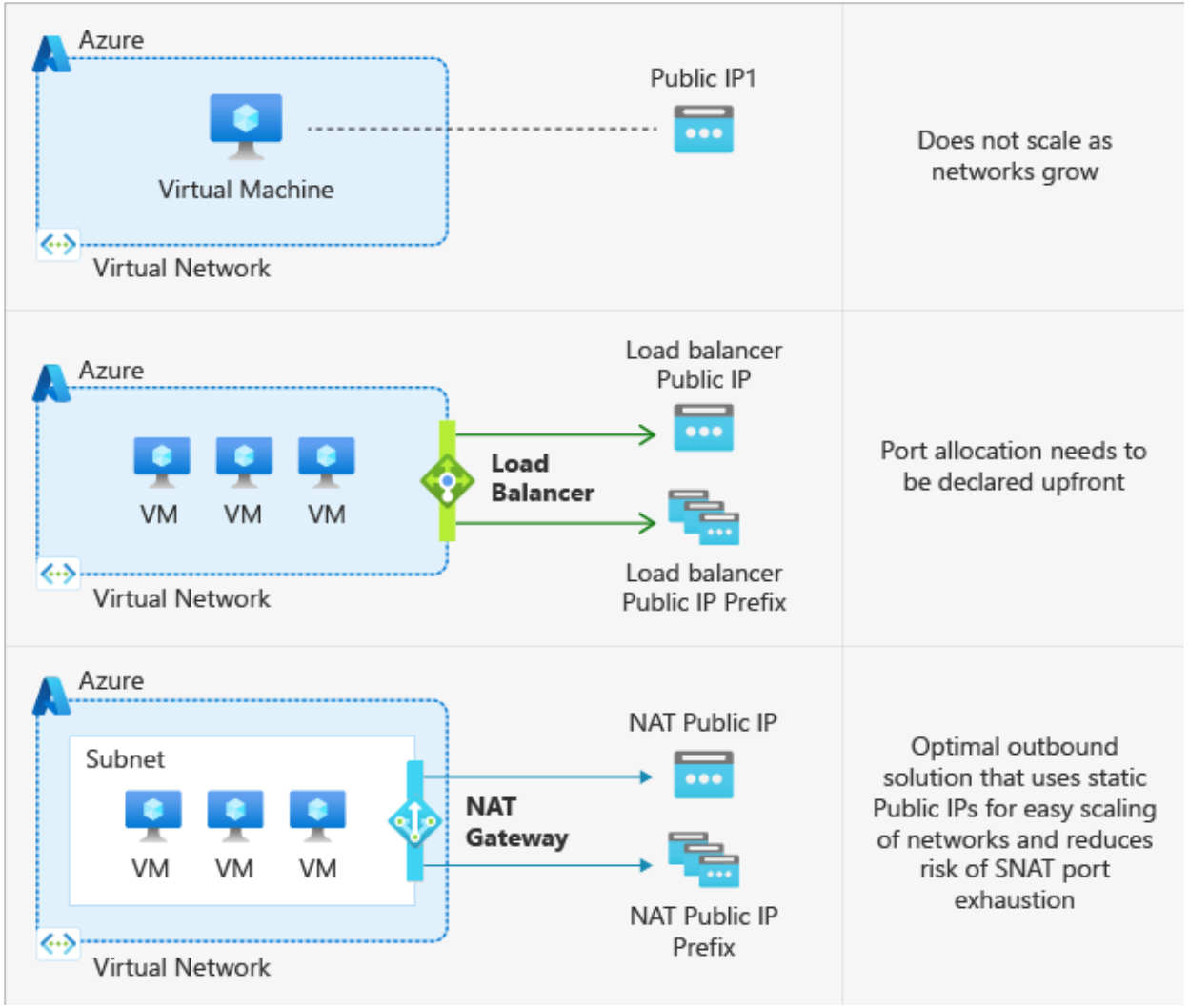
1.Connectivity

2.Remote Management

3.VPN solutions

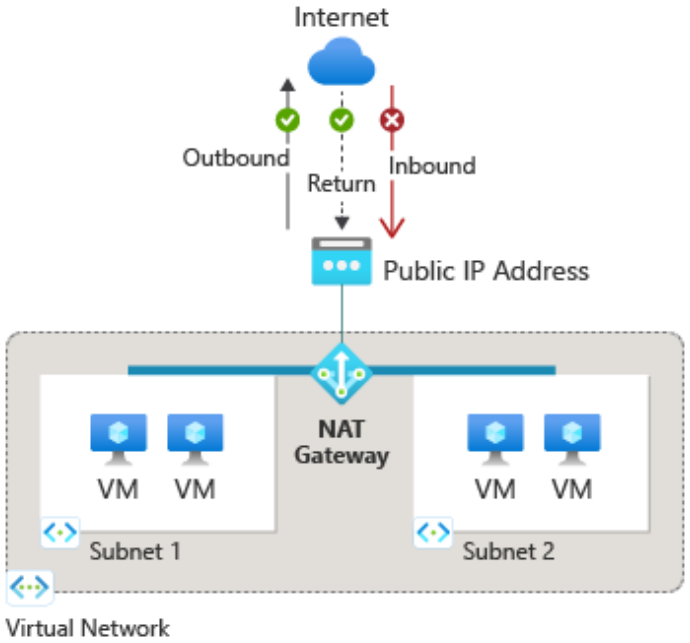
There are three ways to provide **outbound** access:

- Assign a **public address** to each virtual machine.
- Route outbound traffic through a **load balancer.**
- Use a **NAT gateway** for a single point for outbound internet traffic. Private VMs without public IPs can still access the internet



1. NAT Gateway

Azure NAT Gateway is a managed service that lets VMs in **a private subnet** access the internet, without allowing inbound connections. It uses dynamic SNAT to scale outbound traffic and prevent port exhaustion.



1. NAT gateway

- **Security:** NAT Gateway is built on the zero trust network security model and is secure by default. With NAT gateway, private instances within a subnet don't need public IP addresses to reach the internet.
- **Resiliency:** Azure NAT Gateway is a fully managed, distributed service that doesn't rely on individual VMs or hardware. Its software-defined design ensures high resilience and can withstand multiple failures without downtime
- **Performance:** Azure NAT Gateway is a software defined networking service. Each NAT gateway can process up to 50 Gbps of data for both outbound and return traffic. A NAT gateway doesn't affect the network bandwidth of your compute resources.

1. NAT gateway

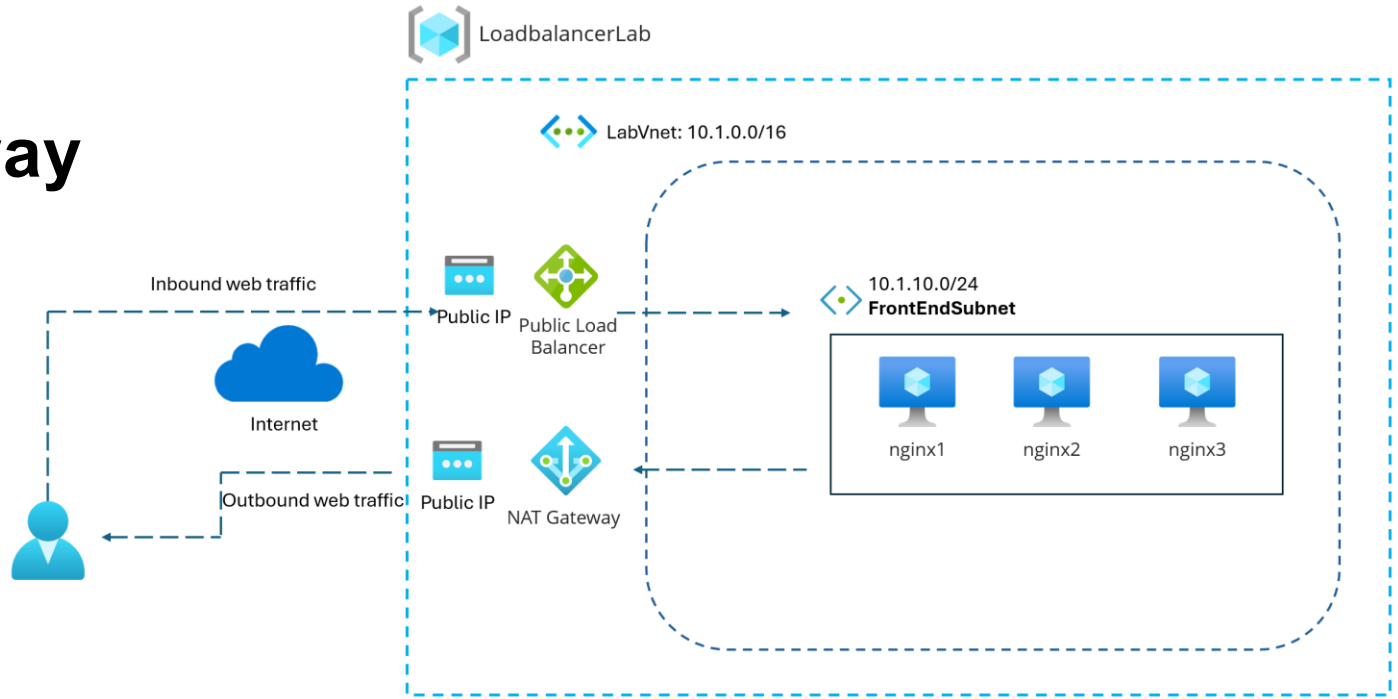
NAT Gateway properties

- The subnet has a **system default route that routes traffic with destination 0.0.0.0/0** to the internet automatically. Once NAT gateway is configured to the subnet, communication from the virtual machines existing in the subnet to the internet will prioritize using the public IP of the NAT gateway.
- Multiple subnets within the same virtual network can either use different NAT gateways or the same NAT gateway.
- A NAT gateway can’t span multiple virtual networks.

2. Load Balancer

Load Balancer is used for load balancing and forwarding traffic to resources. There are four differente Azure load balancing services:

1. **Azure load balancer**
2. **Azure application gateway**
3. **Azure traffic manager**
4. **Azure front door**



2. Load Balancers

Azure Load Balancer

- A Layer 4 (TCP/UDP) load balancer that distributes incoming traffic across multiple virtual machines (VMs) in a region to ensure high availability and reliability.
- Ideal for distributing traffic evenly across VMs in a cloud-based application, such as a web server farm.
- Operates at the transport layer (TCP/UDP) and is suited for scenarios requiring basic, low-latency load balancing of internal or external traffic.

2. Load Balancers

Azure Application gateway

- A Layer 7 (HTTP/HTTPS) load balancer that provides advanced features such as SSL termination, URL-based routing, and Web Application Firewall (WAF) integration.
- Best for web applications that need features like path-based routing or secure end-to-end encryption with SSL offloading. Focuses on application-layer (HTTP/HTTPS) traffic and is equipped with additional features like WAF and URL routing.

2. Load Balancers

Azure Traffic Manager

- A DNS-based traffic routing service that helps distribute user traffic across multiple geographic regions or endpoints to improve global application performance and reliability.
- Ideal for routing users to the closest region or data center, such as when running a global application with multiple data centers.

2. Load Balancers

Azure Front Door

- A global, Layer 7 (HTTP/HTTPS) load balancing service that provides fast, secure, and scalable routing of traffic to multiple backend services with added features like SSL offloading, WAF, and URL-based routing.
- Front Door caches content at global edge servers, routing user requests to the nearest point of presence, and keeping content cached until TTL expiration to boost performance for both dynamic and static content.
- Optimized for global traffic with features like dynamic site acceleration and integrated security at the edge, making it suitable for fast, secure, and highly available web apps.

6.Azure Networking

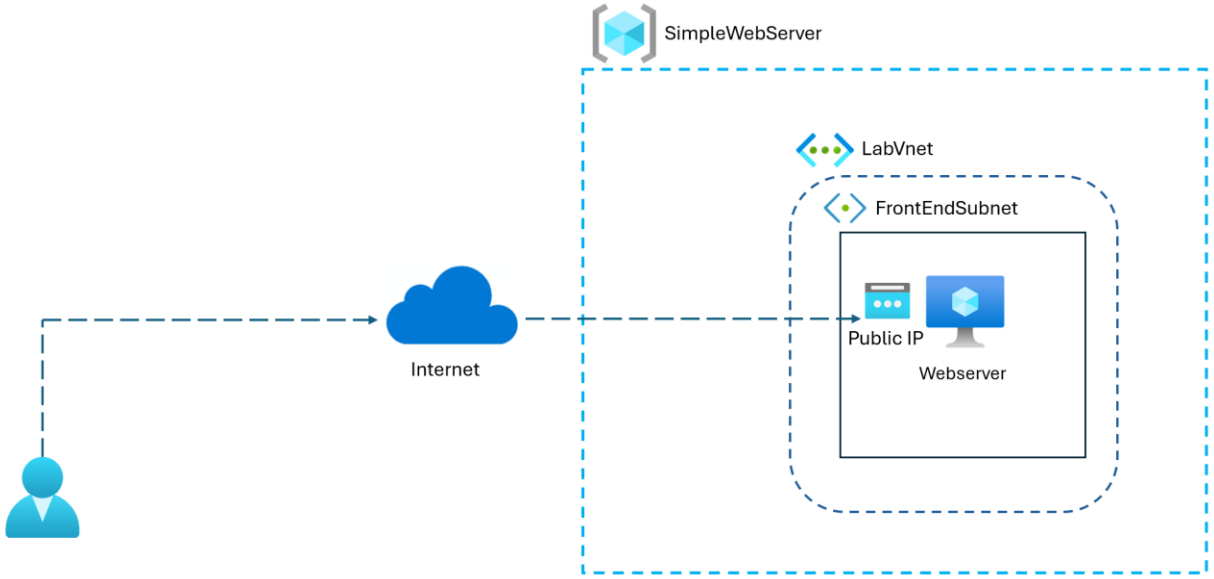
1.Connectivity

2.Remote Management

3.VPN Solutions

1.Virtual Machine with public IP

When creating a virtual machine with default settings, your virtual machine will have a public IP address with a remote protocol enabled (SSH for Linux, RDP for Windows). You manage this virtual machine by directly connecting to the server's public IP address.



1. Virtual machine with public IP

Advantages

- **Quick and easy:** Direct connection via public IP allows quick and simple access to the server.
- **No Cost:** No additional resources (Azure Bastion, VPN gateway or a jump server) needed for manning the virtual machine.
- **No additional configuration**

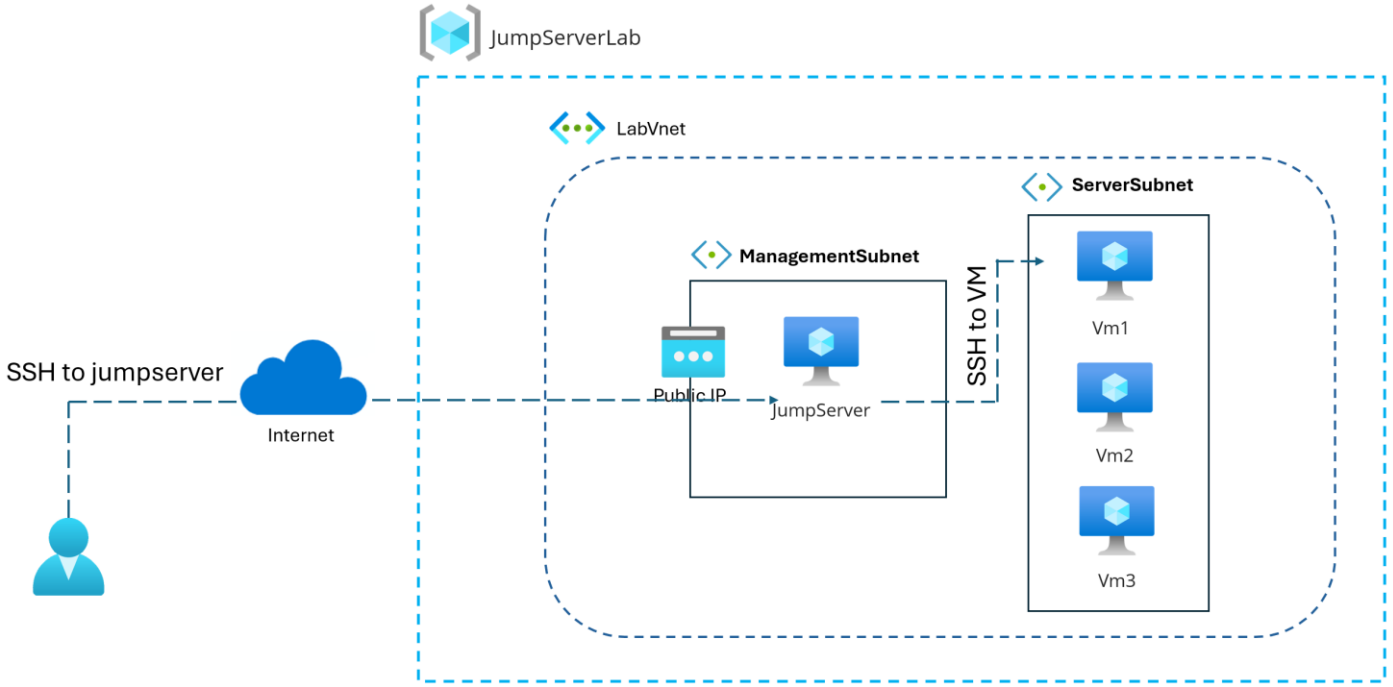
1. Virtual machine with public IP

Disadvantage: Insecure in many ways

- **No centralized access control:** Managing each VM separately doesn't scale well and makes access harder to manage.
- **Public IP means open to the world:** Anyone with the IP address can try to connect using SSH, RDP, or VNC.
- **Bots constantly scan public IPs:** Automated bots scan the internet for open management ports on public IPs.
- **Brute-force attacks are common:** Once found, bots often try to break in using brute-force methods. Can affect performance, these attacks use resources and can slow down your VM.

2.Jump Box

A jump box, also known as a jump server or bastion host, is a secure intermediary server used to access and manage in a remote network. It acts as a gateway between your device and the remote server.



2. Jump box

Advantages

- **Enhanced security:** By requiring all administrative access to go through the jump box, it **reduces the attack surface** and helps prevent direct attacks on critical servers. This centralized access point can be heavily fortified with security measures such as multi-factor authentication, strict access controls, and extensive logging.
- **Monitoring and auditing:** all By funneling all administrative access through a jump box, organizations can more easily monitor and log activities. This centralized logging makes it simpler to audit access and detect any suspicious behavior.
- **Simplified access control** through centralized user authentication and streamlined management of user permissions.

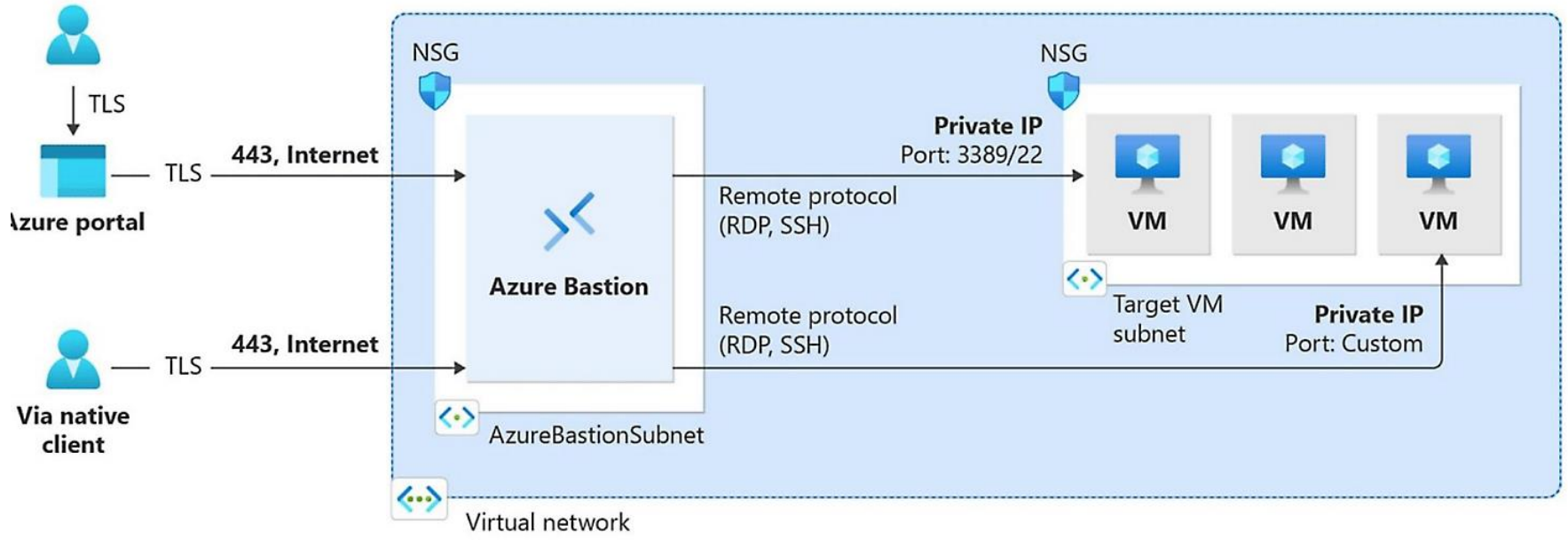
2. Jump box

Disadvantages

- **Single Point of Failure:** If the jump box goes down or is compromised, it can disrupt access to the entire network or critical systems, potentially leading to significant downtime or security breaches
- **Complexity and maintenance**: Implementing and maintaining a jump box can add complexity to the network infrastructure. It requires ongoing management, updates, and monitoring to ensure it remains secure and functional.
- **Potential Performance Bottlenecks:** Routing all administrative traffic through a single jump box can create performance bottlenecks, especially in large or high-traffic environments. This centralization can lead to delays or reduced efficiency in accessing and managing systems.

3. Azure Bastion

Azure Bastion is a fully managed service that lets you securely connect to virtual machines using their private IP addresses. It enables secure RDP/SSH access directly from the Azure portal over a TLS connection. Essentially, Azure Bastion acts as a jump server, but as a service.



3. Azure Bastion

Azure Bastion - jump box similarities

- Both act as a secure intermediary to access virtual machines or resources in a private network.
- They eliminate the need for direct exposure of internal systems to the public internet.
- Both provide a controlled point of entry for administrators to manage remote resources securely.
- They support secure access, typically through protocols like RDP or SSH, without requiring VPNs.

3. Azure Bastion

Advantages over traditional jump boxes

- **Simplified access management:** Azure Bastion is integrated with Entra ID, making the setup and management of secure access easier. MFA already implemented on Entra user.
- **Reducing attack surface:** Azure Bastion service does not require a public IP address, reducing the attack surface. Connections are made through the Azure portal using a secure TLS connection.
- **Scalability and Performance:** Azure Bastion is designed to scale automatically with demand, ensuring consistent performance even under high load.
- **Fully Managed Service:** Azure Bastion is a fully managed PaaS service eliminating the need for manual setup, configuration, and maintenance of the underlying infrastructure. This reduces administrative overhead and security.

3. Azure Bastion

Azure Bastion potential disadvantages

- **Cost** Azure Bastion uses a pay-as-you-go model, where you are charged per hour (https://azure.microsoft.com/en-us/pricing/details/azure-bastion/)

  You can reduce costs by implementing automation, such as deploying the Azure Bastion service at the start of each workday and removing it at the end of the day.

- **Vendor Lock-In:** Using Azure Bastion ties your infrastructure to the Azure ecosystem, which can lead to vendor lock-in. This may limit flexibility if you decide to migrate to another cloud provider or use a multi-cloud strategy. Traditional jump boxes offer more flexibility in this regard.

- **Limited Customization:** As a managed service, Azure Bastion may have limitations in terms of customization and control compared to a traditional jump box. Organizations with specific requirements or the need for extensive customization might find a traditional jump box more suitable.

3. Azure Bastion Developer

Azure Bastion potential disadvanteges

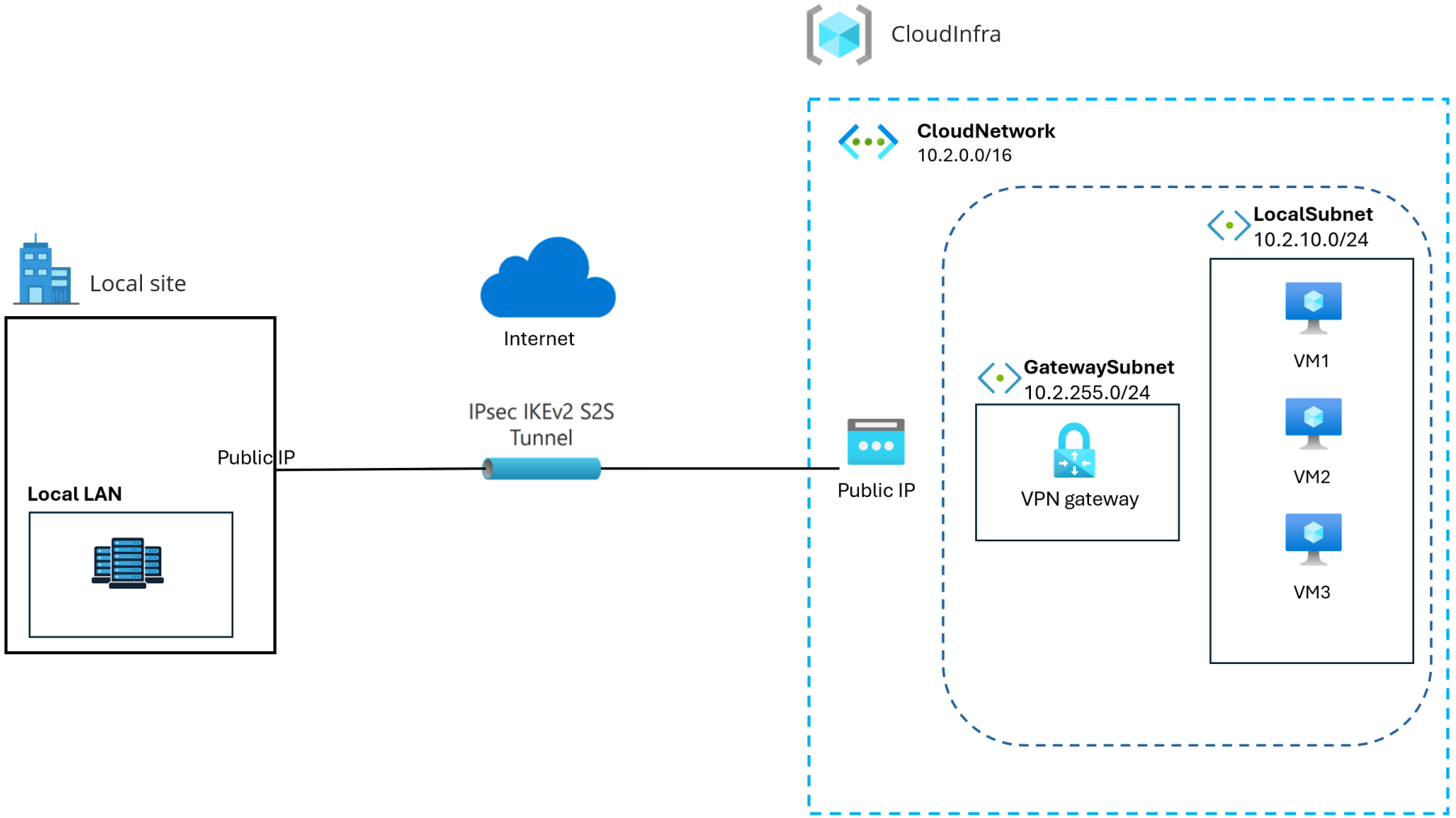
6.Azure networking

1.Connectivity

2.Remote Management

3.VPN Solutions

1. Site-To-Site VPN



1. Site-to-Site VPN

Use cases

1.Hybrid Cloud

- Some services running on-prem and some services running in cloud. Securely connect your local datacenter with cloud environment.

2.Gradual Cloud migration

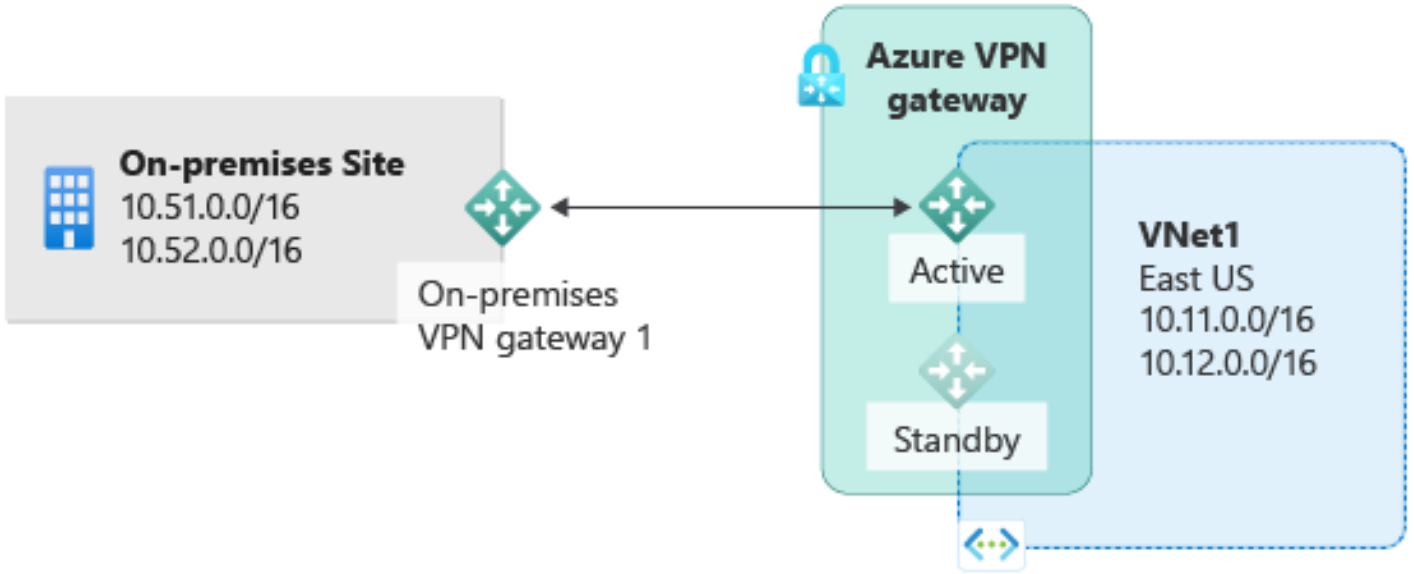
- Migrating workloads to the cloud over time enabling seamless data and app transitions.

3.Backup and Disaster recovery

- Replicate data from oprem to cloud for backup or distaster recovery

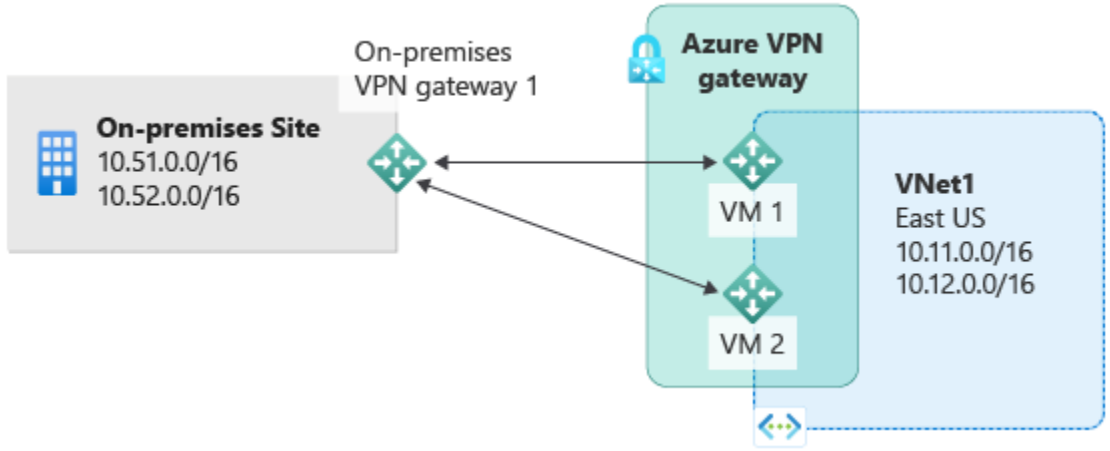
1. Site-to-Site VPN

1.Active-Passive VPN gateway: In an active-passive VPN setup, one VPN instance is active while the other remains on standby. If the active instance fails, the standby automatically takes over, providing high availability but no loadbalancing.



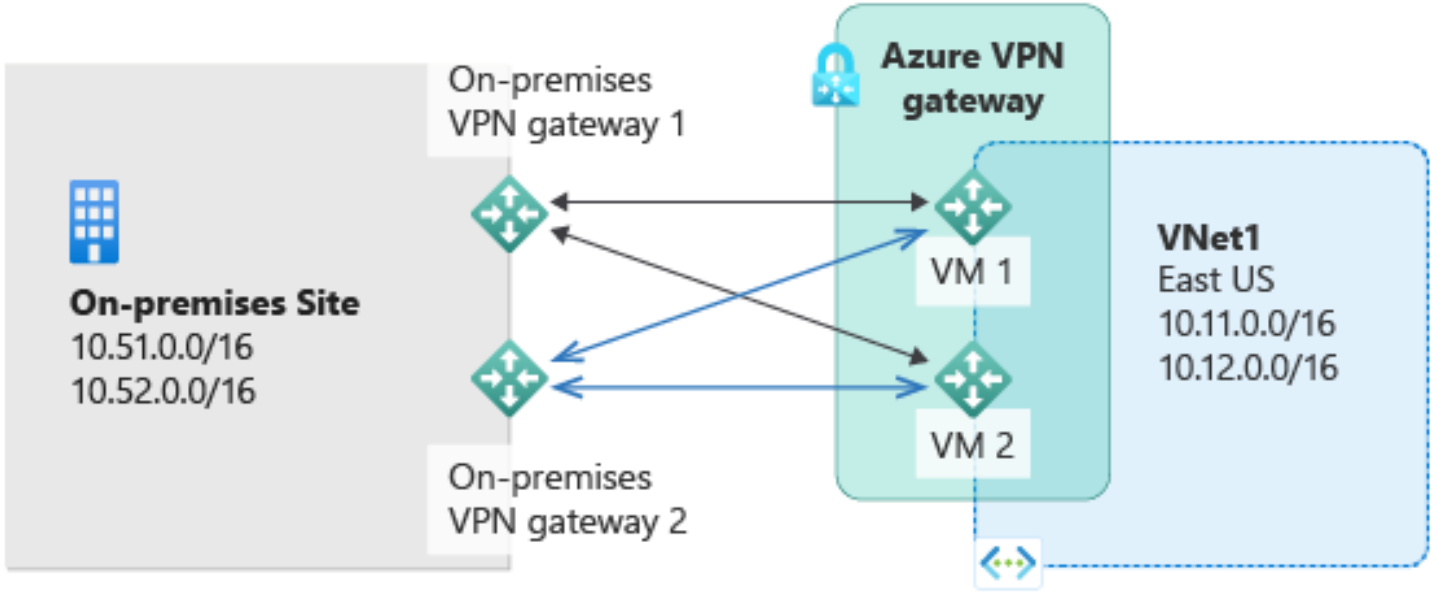
1. Site-to-Site VPN

2.Active-Active VPN gateway: In active-active mode, both instances of the gateway VMs establish S2S VPN tunnels to your on-premises VPN device, as shown the following diagram. Both VPN tunnels are active simultaneously and share the traffic, providing high availability and load balancing.

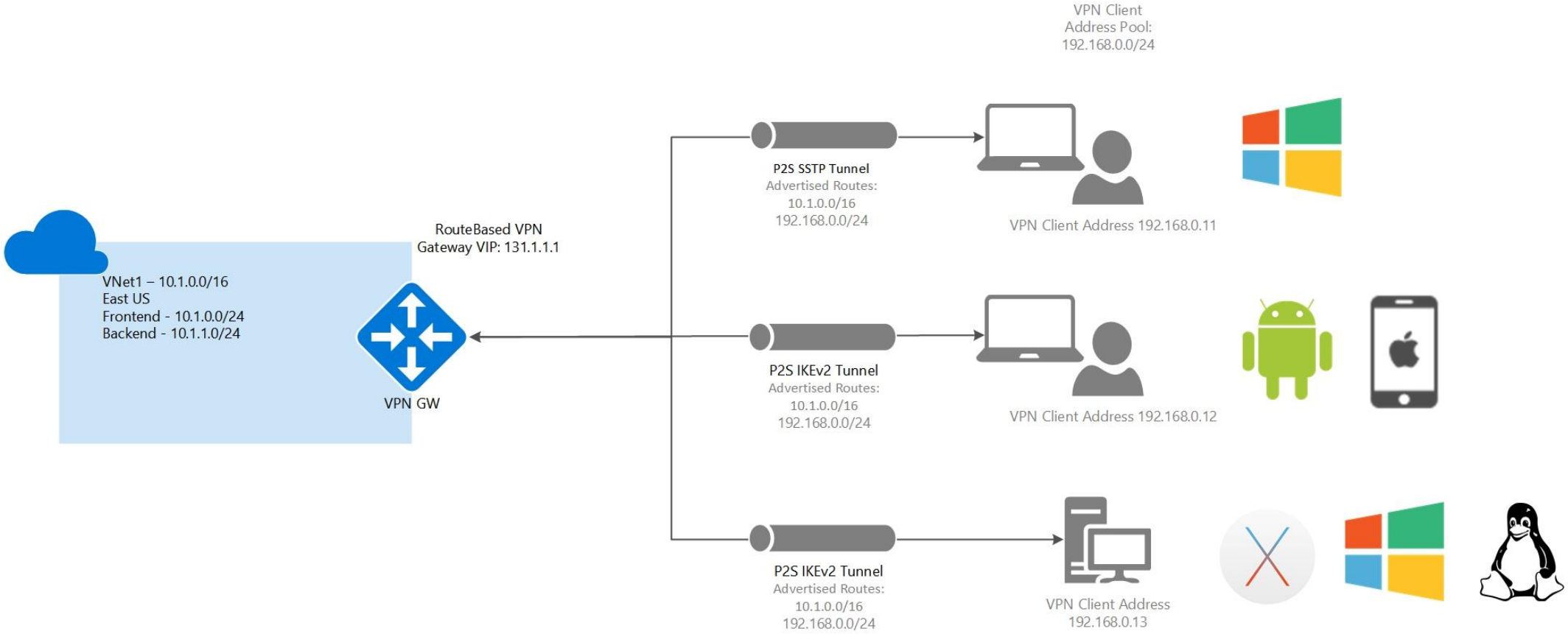


1. Site-to-Site VPN

2.Dual-redundancy active-active mode design: The most reliable design option is to combine the active-active gateways on both your network and Azure, as shown in the following diagram.



2. Point-To-Site VPN



2. Point-to-Site VPN

Use cases

1.Secure Remote Access to Cloud services

- Securily connect and access to cloud services without exposing public IP’s of the cloud services.

2.Access to Private API’s and services

- Developers or testers can connect to private endpoints, internal API’s or microservices that aren’t exposed to the internet.

3.Jumpbox/Bastion alternative

- Instead of setting up a bastion host to access private VMs, users can connect over P2S VPN and directly SSH/RDP into VMs securely.

Microsoft Learn: VPN quickstart

1.Site-to-site VPN

Tutorial - Create S2S VPN connection between on-premises network and Azure virtual network: Azure portal - Azure VPN Gateway | Microsoft Learn

2.Point-to-site VPN

Configure P2S VPN gateway for Microsoft Entra ID authentication: Microsoft-registered client - Azure VPN Gateway | Microsoft Learn

Azure VPN Gateways compared