R&D Document

Azure NAT Gateway

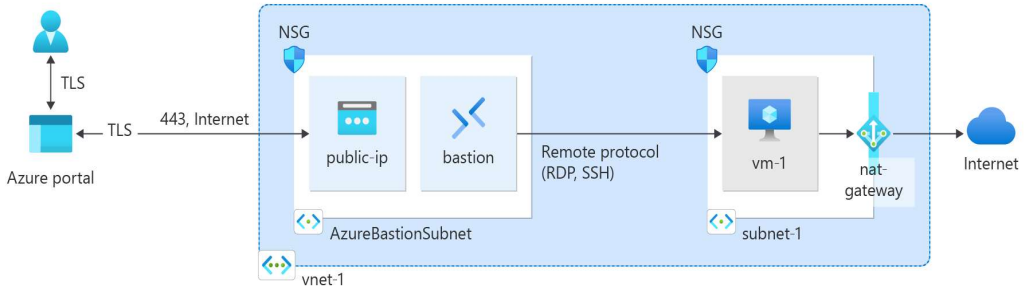
Ananya Srivastava

Cloud Infra
JIET

Table of Contents

Introduction to Azure NAT Gateway

- Azure NAT Gateway is a fully managed, highly available Network Address Translation (NAT) service that provides outbound internet connectivity for resources in your Azure virtual network. It allows private IP addresses within a subnet to connect outbound to the internet while remaining hidden from public view. Unlike traditional NAT devices, Azure NAT Gateway is a cloud-based service that offers scalability, redundancy, and ease of management. Azure virtual machines or VM scale-sets in a private subnet.



- NAT Gateway is a service that securely routes internet traffic from a private virtual network with enterprise-grade performance and low latency. With built-in high availability using software-defined networking, you can easily configure, scale, and deploy outbound connectivity for dynamic workloads with NAT Gateway.

Benefits of Azure NAT Gateway

- **Enhanced Security:**
  By keeping your virtual machines in a private subnet, Azure NAT Gateway adds a layer of security by hiding their private IP addresses from the public internet. This reduces the attack surface for your resources.

- **Simplified Management:**
  Azure NAT Gateway is a fully managed service, eliminating the need to provision and manage physical NAT devices. This reduces administrative overhead and simplifies your network infrastructure.

- **Scalability:**
  Azure NAT Gateway can automatically scale to meet the outbound internet traffic demands of your virtual network. This ensures consistent performance even during traffic spikes.

- **High Availability:**
  Azure NAT Gateway is deployed across multiple fault domains, ensuring high availability and resiliency in case of service disruptions.

- **Cost-Effective:**

  You only pay for the outbound bandwidth used by your virtual machines through the NAT Gateway. This allows for efficient resource utilization and cost optimization.

Azure NAT Gateway Basics

- **Outbound Connectivity**
  NAT Gateway is the preferred method for outbound connectivity in Azure. By configuring NAT Gateway, it takes precedence over other methods such as load balancers or instance-level public IP addresses. From September 30th, 2025, default outbound access for new deployments will be retired, making NAT Gateway the recommended solution for outbound connectivity.

- **Traffic Routing**
  The NAT Gateway redirects outbound traffic from subnets to the internet using the gateway's public IP addresses. User Defined Routes (UDRs) and virtual appliances can modify routing, but by default, traffic is directed through the NAT Gateway.

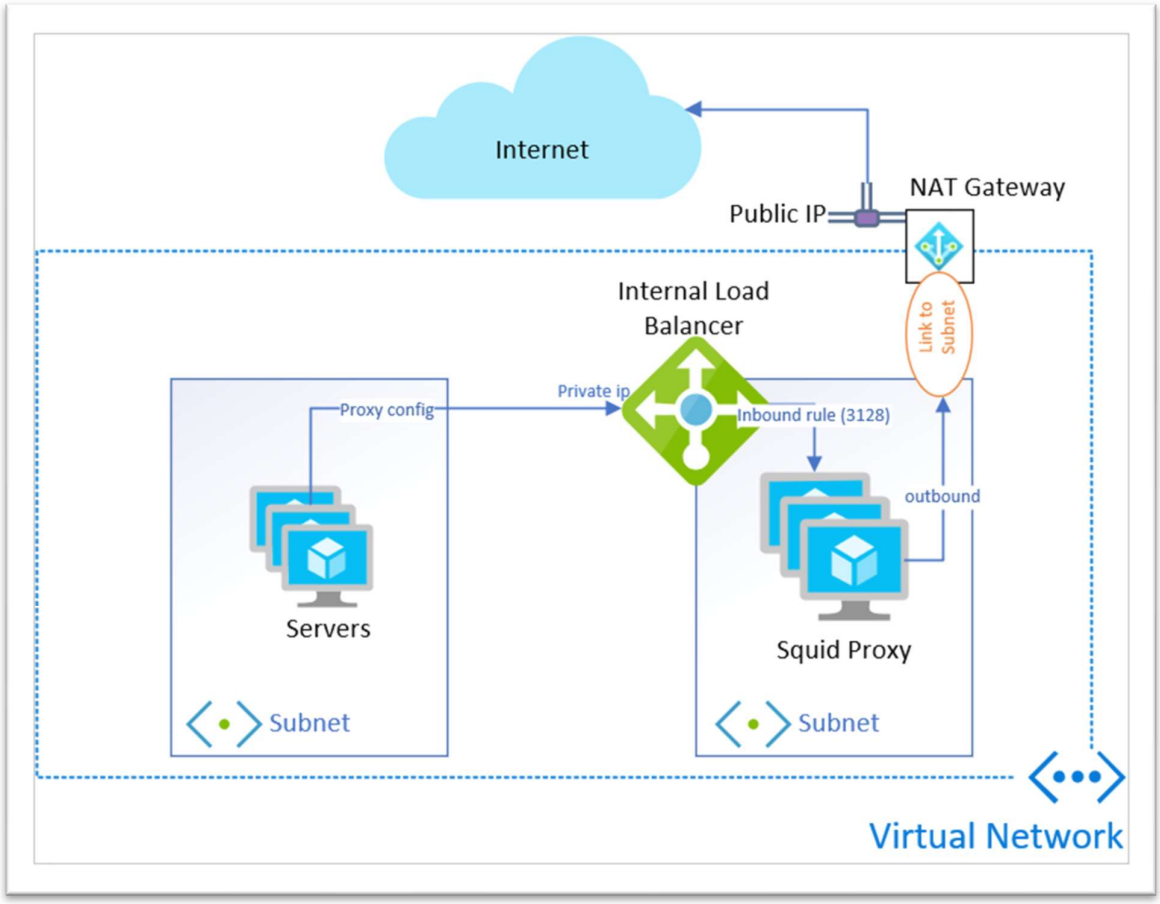
- **Configurations**
  Multiple subnets can use the same or different NAT Gateways.

  - Only one NAT Gateway can be attached to a single subnet.
  - NAT Gateways cannot span multiple virtual networks or be deployed in gateway subnets.
  - Up to 16 IP addresses can be assigned to a NAT Gateway, using public IP addresses or prefixes.
  - NAT Gateway does not support IPv6.

- **Availability Zones**
  NAT Gateway can be created in a specific availability zone or placed in no zone. Default deployment places the NAT Gateway in a zone automatically, but specific zone deployment is possible for zone isolation scenarios.

- **Compatibility**
  NAT Gateway is compatible with standard public IP addresses or prefixes but not with basic resources like basic load balancers or public IPs. Upgrading basic resources to standard is necessary for NAT Gateway compatibility.

- **Connection Timeouts and Timers**
  NAT Gateway has specific idle timeout settings for TCP and UDP traffic, with default and customizable timers to manage connection flow and port reuse.



Pricing and Service Level Agreement (SLA)

Pricing and Service Level Agreement (SLA) are two separate but related concepts in cloud services, like Azure NAT Gateway.

Pricing:

- This refers to the cost associated with using a service. In the case of Azure NAT Gateway, you are typically charged based on the **outbound bandwidth**

used by your virtual machines that leverage the NAT Gateway for internet access.

- The specific pricing details can be found on the Microsoft Azure website. They may include factors like region, data transfer amount, and any applicable discounts.

Service Level Agreement (SLA):

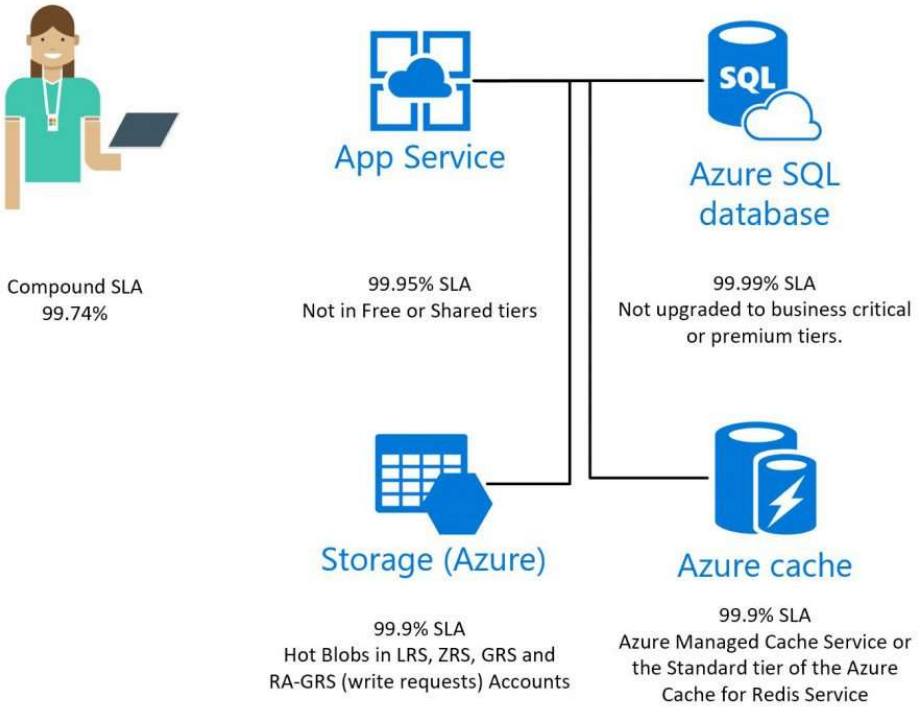
- An SLA is a formal agreement between a service provider (Microsoft Azure in this case) and a customer (you) that outlines the expected level of service for a specific offering.

- For Azure NAT Gateway, the SLA guarantees a certain level of uptime or performance. For example, the SLA for Azure NAT Gateway might be **99.9%** for outbound internet connectivity. This means you can expect the NAT Gateway to be available for outbound connections at least 99.9% of the time.

- If the service falls below the agreed-upon SLA metrics, the service provider may offer compensation or credits towards future use.

✓ Azure NAT Gateway is billed based on the outbound bandwidth used by your virtual machines. You can find the latest pricing details on the Microsoft Azure website.

✓ Azure NAT Gateway offers a 99.9% SLA for outbound internet connectivity. This ensures reliable and consistent outbound communication for your virtual machines.


App Service
SQL
Azure SQL database
Compound SLA
99.74%
99.95% SLA
Not in Free or Shared tiers
99.99% SLA
Not upgraded to business critical or premium tiers.
Storage (Azure)
Azure cache
99.9% SLA
Hot Blobs in LRS, ZRS, GRS and RA-GRS (write requests) Accounts
99.9% SLA
Azure Managed Cache Service or the Standard tier of the Azure Cache for Redis Service

References

- **Microsoft Azure Documentation:**
  - Azure NAT Gateway Overview: https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview
  - Azure NAT Gateway Pricing: https://azure.microsoft.com/en-us/pricing/details/azure-nat-gateway/
- **Microsoft Azure Trust Center:**
  - Service Level Agreements (SLAs): https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1