AVIATRIX®

TECH UPDATE OVERVIEW

Understanding the Change To Azure VM Internet Access

At a Glance

Azure will no longer grant default outbound internet access to new VMs as of March 31, 2026 (extended).

Plan Ahead

- Review current VMs and default outbound access dependencies
- Identify at-risk dynamic workloads
- Understand all your outbound access options
- Take the opportunity to future-proof your cloud strategy

Aviatrix Solutions

- NAT Gateway for Azure
- Aviatrix Cloud Firewall with three upgradable tiers

What's changing

When you create an Azure virtual machine (VM) without specifying how it connects to the internet, Azure assigns a default public IP address, providing internet access without any additional configuration.

On March 31, 2026 (extended), Microsoft will retire this default outbound internet access for all new Azure virtual machines (VMs). This change will not affect existing VMs, but any VM built after this date will need an explicit method to allow outbound or inbound internet access.

Why this change is good

Removing default internet access eliminates a convenience, but it improves network security and aligns with the best-practice Zero Trust model which assumes no devices are trustworthy and requires access to be explicitly granted.

Action required: What you need to do

While this change is a net positive, you do need to prepare to avoid potential negative consequences. Existing VMs may seem unaffected, but this can create a false sense of security. For example, auto-scaling groups that create and delete VMs dynamically could face outages if outbound connectivity isn't explicitly configured. And, of course, you will need to determine how to proactively provide internet access to new Azure VMs going forward.

Understanding your options

Native Azure solutions: There are several ways to provide internet access to new VMs with native Azure capabilities, but each comes with its own drawbacks.

Option	Pros	Cons
Instance-level public IPs: Assigns a dedicated public IP address directly to individual VMs	Provides straightforward internet connectivity	Requires careful management of public IP resources and potentially increases security risks through direct exposure
Outbound rules: Configure load balancer rules to control and manage outbound connections from VMs	Offers more granular control over traffic flow	Requires additional configuration and management overhead
Azure NAT Gateway: Acts as a shared gateway service for outbound connectivity, providing a managed solution that allows multiple VMs in a subnet to share outbound IP addresses	Offers the best balance of scalability and manageability for most deployments, with simplified IP management and consistent connectivity	Doesn't inspect egress traffic, leaving your outbound traffic vulnerable to data exfiltration; additionally, you're charged for all the data being transferred from the NAT gateway, which can lead to expensive clouds bills with high variability, making it difficult to predict egress costs

Aviatrix solutions

Alternatively, you can look beyond the native Azure tools for secure, high-performance internet access for your Azure VMs. The Aviatrix Cloud Network Security Platform offers a range of offerings to meet a variety of needs.

A comprehensive and easy-to-use solution: The **NAT Gateway for Azure** offers a fully managed service that simplifies configuration and deployment, intelligently handles port allocation, and supports standalone VMs as well as VMs behind load balancers. By deploying the Azure NAT Gateway and assigning it one or more PIPs, you can quickly scale egress traffic requirements. The Azure NAT Gateway is also fully redundant and supports availability zones for high uptimes.

A solution for more functionality, choice, and control: If you are looking to add more capabilities to your internet egress strategy, consider the **Aviatrix Cloud Firewall**, featuring three upgradable tiers, for increased choice and control over how you want to deploy and scale your internet egress solution in Azure.

Tier	Best when	Advantages
Basic NAT	You want enterprise-grade, dynamic NAT capabilities on a per-VNet basis.	Can be easily scaled to handle large volumes of traffic and becomes the default internet gateway for its resident VNet through cloud-native orchestration.
Cloud Firewall for Egress	You want additional security features such as TLS/SSL decryption, FQDN whitelisting/ blacklisting, and intrusion detection.	Ensures trusted and secure outbound traffic. This tier also provides predictable billing, which does not meter on network data but only on hourly consumption, delivering potential savings.
Full Cloud Firewall solution	You want micro-segmentation and app-to-app (east/west) security.	Enables NSG automation, dynamic policy enforcement, and centralized policy control across the entire cloud network, including hybrid policy enforcement over VPN and ExpressRoute.

Plan now, prevent headaches later

To get ahead of this change, you should:

- Audit your cloud infrastructure to identify dependencies on default outbound access.
- Invest in enterprise-grade visibility tools to monitor and manage dynamic workloads effectively.
- Collaborate across technical and business teams to prepare proactively.

While this is undoubtedly extra work for your already very busy team, the Azure change is more than a technical update—it's a chance to future-proof your cloud strategy and ensure that security goes hand in hand with agility and reliability.

Are you ready for secure, high-performance internet access?

Aviatrix Platform-as-a-Service (Aviatrix PaaS) is a scalable service to help you minimize the complexities of cloud networking and network security without sacrificing performance. Request a free trial. We're also in the Azure Marketplace.

REQUEST A FREE TRIAL

About Aviatrix

For enterprises struggling to secure cloud workloads, Aviatrix® offers a single solution for pervasive cloud security. Where current cybersecurity approaches focus on securing entry points to a trusted space, Aviatrix Cloud Native Security Fabric (CNSF) delivers runtime security and enforcement within the cloud application infrastructure itself – closing gaps between existing solutions and helping organizations regain visibility and control. Aviatrix ensures security, cloud, and networking teams are empowering developer velocity, AI, serverless, and what's next. For more information, visit www.aviatrix.ai.