

PROTECT YOUR AZURE VMs: ESSENTIAL CHANGES YOU CAN'T IGNORE COME MARCH 2026

WHAT'S CHANGING?

Starting March 31, 2026 (extended), Microsoft will implement new restrictions on outbound internet access for new Azure virtual machines (VMs). This will impact how organizations connect to external systems and services.

WHY THE CHANGE?

To enhance security measures and ensure a more robust network environment. These adjustments will help protect sensitive data and prevent potential security breaches.

WHAT TO EXPECT?

Organizations using Azure will need to re-evaluate their outbound access configurations and make necessary adjustments to comply with the upcoming changes. This approach will ensure a seamless transition and continuity of operations.

NAT GATEWAY AT A GLANCE

Each NAT Gateway can

- Provide up to a total of 50 Gbps of throughput
- Support up to 50,000 concurrent connections per public IP address
- Process 1M packets per second and scale up to 5M packets per second

ARE YOU PREPARED?

Yes, I have a plan in place!

Excellent! Best of luck to you



No! I don't know where to start

We've got you! Follow these steps



Step 1

Audit cloud infrastructure for dependencies on default outbound access.

Step 2

Redesign and reconfigure Azure networking infrastructure and policies.

Step 3

Choose from various outbound access options: Native Azure (Public IPs, Outbound Rules, Azure NAT Gateway) or Third-party solutions like Aviatrix Cloud Firewall.

Benefits of Aviatrix Cloud Firewall include:

Secure egress: Establish a zero trust framework for outbound traffic with features such as URL filtering, geo-blocking, geolocation-based monitoring, advanced threat detection, and network segmentation. This solution also recommends internet egress security policies and helps with constant monitoring and routine management.

Cost controls: This solution offers flat-rate billing, or an "all-you-can-eat" model with no additional throughput costs. Unlike metered billing, this gives you full cost transparency. Customers save an average of 25% in savings or more compared to first-party NAT gateway solutions.

Step 4

Collaborate across technical and business teams for proactive preparation.

Step 5

Start planning now to avoid future disruptions and optimize security, performance, resilience, and costs.

REMEMBER

Preparation is key to avoid disruptions.



Be proactive



Stay updated



Partner with a trusted cloud networking expert to navigate these changes smoothly

For more detailed information and personalized guidance on how these changes may affect your specific setup, contact our team of cloud networking experts today.

[Request a Free Trial](#)