We use
optional
cookies to
improve
your
experience
on our
websites,
such as
through
social media
connections,
and to
display
personalized
advertising
based on
your online
activity. If
you reject
optional
cookies,
only cookies
necessary to
provide you
the services
will be used.
You may
change your
selection by
clicking
"Manage
Cookies" at
the bottom
of the page.
[Privacy Statement](#)
[Third-Party Cookies](#)

Accept

Reject

Manage cookies

Azure

🔍   Sign in

🏠   [Blog](#) / [Management and Governance](#)   [Subscribe](#)

Best practices, Management and Governance, Networking, Virtual Network

Dive deep into NAT gateway's SNAT port behavior

By Aimee Littleton Product Manager 2, Azure Networking

Posted on August 18, 2022

4 min read

In our last blog, we examined a scenario on how network address translation (NAT) gateway mitigates connection failures happening at the same destination endpoint with its randomized source network address translation (SNAT) port selection and reuse timers. In addition to handling these scenarios, NAT gateway's unique SNAT port allocation is beneficial to dynamic, scaling workloads connecting to several different destination endpoints over the internet. In this blog, let's deep dive into the key aspects of NAT gateway's SNAT port behavior that makes it the preferred solution for different outbound scenarios in Azure.

Why SNAT ports are important to outbound connectivity

For anyone working in a virtual cloud space, it is likely that you will encounter internet connection failures at some point. One of the most common reasons for connection failures is SNAT port exhaustion, which happens when the source endpoint of a connection runs out of SNAT ports to make new connections over the internet.

Source endpoints use ports through a process called SNAT, which allows destination endpoints to identify where traffic was sent and where to send return traffic. NAT gateway SNATs the private IPs and ports of virtual machines (VMs) within a subnet to NAT gateway's public IP address and ports before connecting outbound, and in turn provides a scalable and secure means to connect outbound.
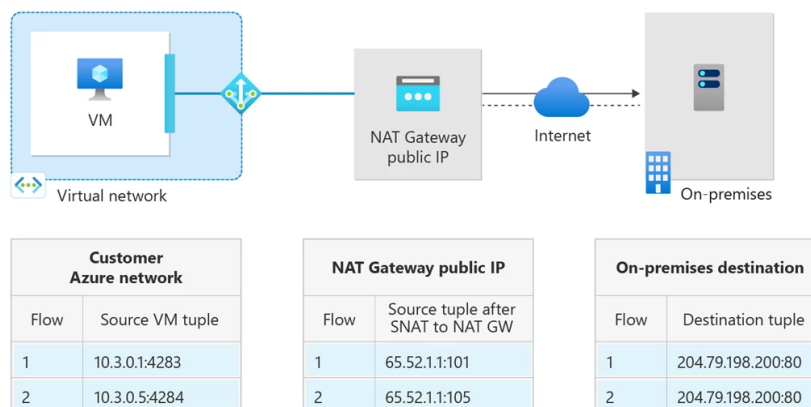
Customer Azure network		NAT Gateway public IP		On-premises destination	
Flow	Source VM tuple	Flow	Source tuple after SNAT to NAT GW	Flow	Destination tuple
1	10.3.0.1:4283	1	65.52.1.1:101	1	204.79.198.200:80
2	10.3.0.5:4284	2	65.52.1.1:105	2	204.79.198.200:80

Figure 1: Source network address translation by NAT gateway: connections going to the same destination endpoint

over the internet are differentiated by the use of different source ports.

With each new connection to the same destination IP and port, a new source port is used. A new source port is necessary so that each connection can be distinguished from one another. SNAT port exhaustion is an all too easy issue to encounter with recurring connections going to the same destination endpoint since a different source port must be used for each new connection.

How NAT gateway allocates SNAT ports

NAT gateway solves the problem of SNAT port exhaustion by providing a dynamic pool of SNAT ports, consumable by all virtual machines in its associated subnets. This means that customers don't need to worry about knowing the traffic patterns of their individual virtual machines since ports are not pool-based in fixed amounts to each virtual machine. By providing SNAT ports on-demand to virtual machines, the risk of SNAT exhaustion is significantly reduced, which in turn helps prevent connection failures.
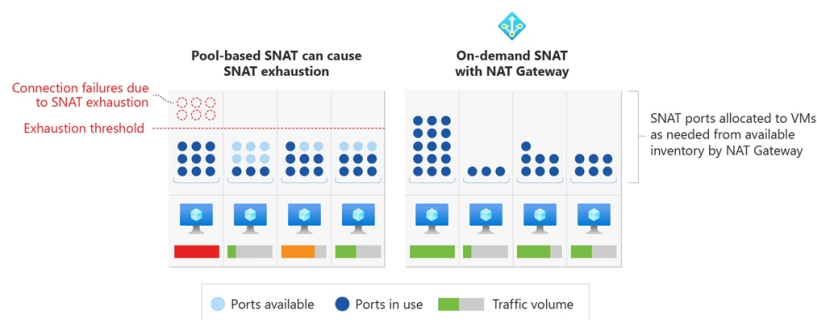
Figure 2: SNAT ports are allocated on-demand by NAT gateway, which alleviates the risk of SNAT port exhaustion.

Customers can ensure that they have enough SNAT ports for connecting outbound by scaling their NAT gateway with public IP addresses. Each NAT gateway public IP address provides 64,512 SNAT ports, and NAT gateway can scale to use up to 16 public IP addresses. This means that NAT gateway can provide over one million SNAT ports for connecting outbound.

How NAT gateway selects and reuses SNAT ports

Another key component of NAT gateway's SNAT port behavior that helps prevent outbound connectivity failures is how it selects SNAT ports. Whether connecting to the same or different destination endpoints over the internet, NAT gateway selects a SNAT port at random from its available
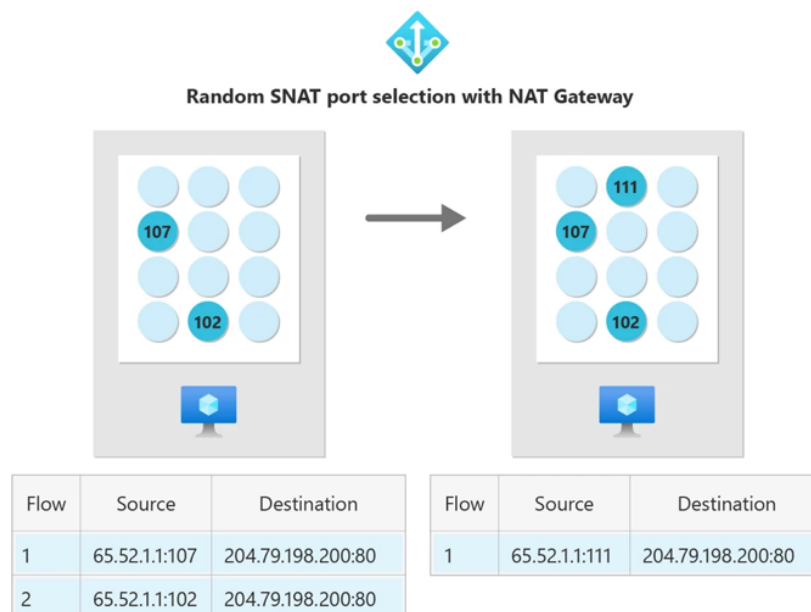
inventory.

Figure 3: NAT gateway randomly selects SNAT ports from its available inventory to make new outbound connections.

A SNAT port can be reused to connect to the same destination endpoint. However, before doing so, NAT gateway places a [reuse cooldown timer](#) on that port after the initial connection closes.

NAT gateway's SNAT port reuse cooldown timer helps prevent ports from being selected too quickly for connecting to the same destination endpoint. This is advantageous when destination endpoints have their own source port reuse cooldown timers in place.
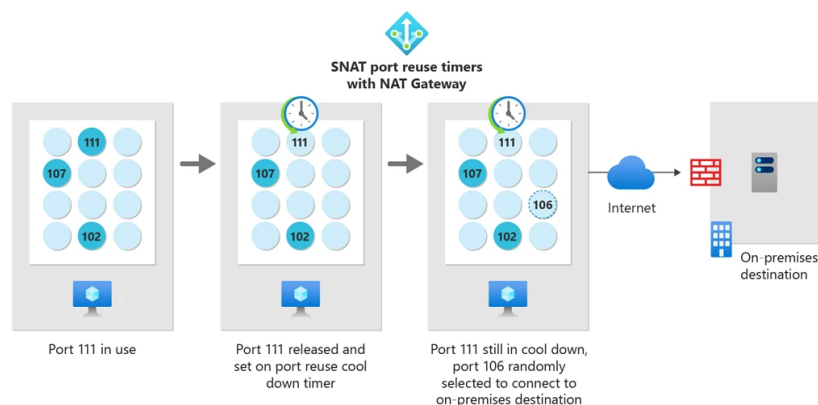
Figure 4: SNAT port 111 is released and placed in a cooldown period before it can connect to the same destination endpoint again. In the meantime, port 106 (dotted outline) is selected at random from the available inventory of ports to connect to the destination endpoint. The destination endpoint has a firewall with its own source port cooldown timer. There is no issue getting past the on-premise destination's firewall since the connection from source port 106 is new.

What happens then when all SNAT ports are in use? When NAT gateway cannot find any available SNAT ports to make new outbound connections, it can reuse a SNAT port that is currently in use so long as that SNAT port connects to a different destination endpoint. This specific behavior is beneficial to any customer who is making outbound connections to multiple destination endpoints with NAT gateway.
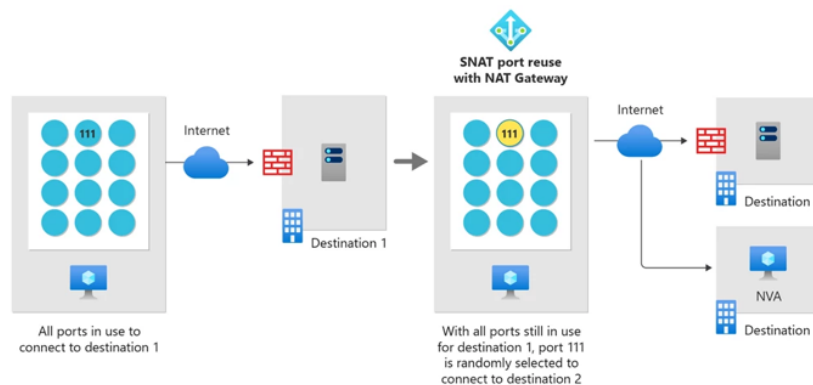
Figure 5: When all SNAT ports are in use, NAT gateway can reuse a SNAT port to connect outbound so long as the port actively in use goes to a different destination endpoint. Ports in use by destination 1 are shown in blue. Port connecting to destination 2 is shown in yellow. Port 111 is yellow with a blue outline to show it is connected to destinations 1 and 2 simultaneously.

What have we learned about NAT gateway's SNAT port behavior?

In this blog, we explored how NAT gateway allocates, selects, and reuses SNAT ports for connecting outbound. To summarize:

Function	NAT gateway SNAT port	Benefit

	behavior	
SNAT port capacity	Up to 16 public IP addresses. 64,512 SNAT ports / NAT gateway public IP addresses.	Easy to scale for large and variable workloads.
SNAT port allocation	Dynamic and On-demand.	Great for flexible, unknown, and large-scale workloads.
SNAT port selection	Randomized.	Reduces risk of connection failures to the same destination endpoint.
SNAT port	Reuse to a different	Reduces risk of

reuse	destination —connect outbound immediately. Reuse to the same destination —set on a cooldown timer.	connection failures to the same destination endpoint with source port reuse cooldown timers.

Deploy NAT gateway today

Whether your outbound scenario requires you to make many connections to the same or to several different destination endpoints, NAT gateway provides a highly scalable and reliable way to make these connections over the internet. See the [NAT gateway SNAT behavior](#) article to learn more.

NAT gateway is easy to use and can be deployed to your virtual network with just a few clicks of a button. Deploy NAT gateway

today and follow along on how with: [Create
a NAT gateway using the Azure portal](#).

Related posts

[Compute](#),
[Networking](#),
[Thought
leadership](#), [Virtual
Machines](#), [Virtual
Network](#)

Microsoft
Innovation in
RAN Analytics
and Control >

[Networking](#),
[Thought
leadership](#), [Virtual
Network](#)

Visualize and
monitor Azure
& hybrid
networks with
Azure Network
Watcher >

[AI + Machine
Learning](#),
[Compute](#),
[Thought
leadership](#), [Virtual
Machines](#), [Virtual
Network](#)

Advancing
anomaly
detection with
AIOps—
introducing
AiDice >

[Compute](#),
[Networking](#),
[Thought
leadership](#), [Virtual
Machines](#), [Virtual
Network](#)

Ensure zone
resilient
outbound
connectivity
with NAT
gateway >

Get the Azure mobile app

Explore Azure

Explore Azure

What is Azure?

Get started

Global infrastructure

Datacenter regions

Trust your cloud

Customer enablement

Customer stories

Products and pricing

Products and pricing

Products

Pricing

Free Azure services

Flexible purchase options

Cloud economics

Optimize your costs

Solutions and support

Solutions and support

Solutions

Resources for accelerating growth

Solution architectures

Support

Azure demo and live Q&A

Partners

Partners

Azure Marketplace

Find a partner

Technology partners

Resources

Resources

Training and certifications

Documentation

Blog

Developer resources

Students

Events and webinars

Analyst reports, white papers, and e-books

Videos

Cloud computing

Cloud computing

What is cloud computing?

What is cloud migration?

What is a hybrid cloud?

What is AI?

What is IaaS?

What is SaaS?

What is PaaS?

What is DevOps?

Change language

English (US)

Your Privacy Choices

Diversity and Inclusion   Accessibility   Privacy & Cookies   Data Protection Notice   Trademarks   Terms of use

Privacy Data Management   Manage cookies   Contact us   Feedback   Sitemap   **© Microsoft 2023**