# Connecting to your Remote Instances without a Public IPv4 Address

## A cost-effective strategy to optimize AWS bills

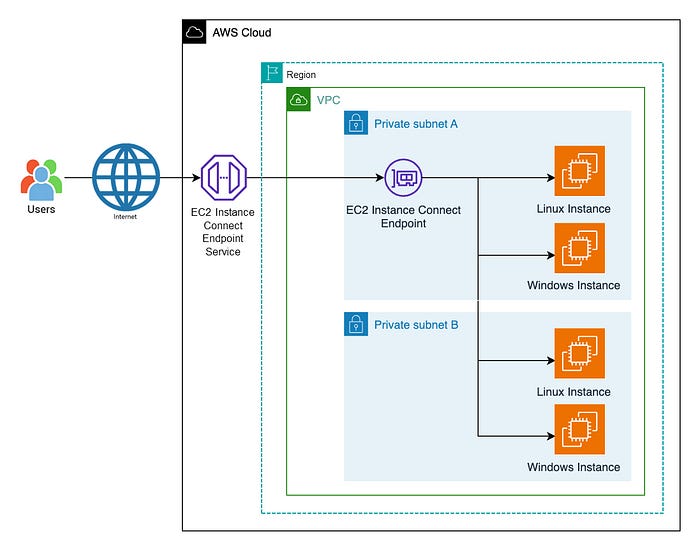
[[](https://medium.com/@rogernem?source=post_page-----c20fee85a4b2--------------------------------)](https://medium.com/@rogernem?source=post_page-----c20fee85a4b2--------------------------------)

[Roger Nem](https://medium.com/@rogernem?source=post_page-----c20fee85a4b2--------------------------------)

5 min read

·

Jan 12



— Diagram of users connecting to private EC2 instances through an EIC Endpoint.

# Table of Contents

1. [Introduction](https://medium.com/@rogernem/connecting-to-your-remote-instances-without-a-public-ipv4-address-c20fee85a4b2#58db)
2. [Bastion Hosts](https://medium.com/@rogernem/connecting-to-your-remote-instances-without-a-public-ipv4-address-c20fee85a4b2#3f1b)
3. [The Usual Approach](https://medium.com/@rogernem/connecting-to-your-remote-instances-without-a-public-ipv4-address-c20fee85a4b2#9a6e)
4. [Challenges using a Bastion Host](https://medium.com/@rogernem/connecting-to-your-remote-instances-without-a-public-ipv4-address-c20fee85a4b2#cda2)
5. [EC2 Instance Connect Endpoint](https://medium.com/@rogernem/connecting-to-your-remote-instances-without-a-public-ipv4-address-c20fee85a4b2#0185)
6. [Azure Bastion](https://medium.com/@rogernem/connecting-to-your-remote-instances-without-a-public-ipv4-address-c20fee85a4b2#0c0b)
7. [Conclusion](https://medium.com/@rogernem/connecting-to-your-remote-instances-without-a-public-ipv4-address-c20fee85a4b2#53ce)

# Introduction

Given the [AWS announcement](https://medium.com/@rogernem/aws-to-charge-public-ipv4-addresses-ea6a284d3462) on the imposition of charges on public IPv4 addresses starting **February 1, 2024** and acknowledging the widespread use of these addresses for connecting to remote instances, this article aims to elucidate an alternative method for connectivity that **doesn’t require a public IPv4 address**.

# Bastion Hosts

Before going any further it’s essential to provide an explanation about bastion hosts, commonly known as jump hosts, jump boxes, or jump servers.

Bastion hosts are **strategically positioned and intentionally designed and configured servers**, named by analogy to the [bastion](https://en.wikipedia.org/wiki/Bastion), a military fortification.

They are **intended to resist attacks**, functioning as intermediaries between an organization’s internal network and an external network, typically the internet.

The primary purpose of a bastion host is to **provide secure access to internal resources**, especially in environments where direct access to internal servers is restricted for security reasons.

# The Usual Approach

For many years, when trying to connect to an [Amazon Elastic Compute Cloud (Amazon EC2)](https://aws.amazon.com/ec2/) instance within a [Amazon Virtual Private Cloud (Amazon VPC)](https://aws.amazon.com/vpc/) over the Internet, users will typically connect first to a **bastion host with a public IP address** set up over an [Internet Gateway (IGW)](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html) in their VPC, and then use port forwarding to reach their destination via SSH (Secure Shell), or Remote Desktop Protocol (RDP).

# Challenges using a Bastion Host

Using a bastion host introduces several challenges and considerations, despite its benefits in enhancing security:

1. **Complex Configuration:** Properly configuring and maintaining a bastion host can be complex, involving setting up secure authentication mechanisms, managing firewall rules, and ensuring proper logging and monitoring.
2. **Single Point of Failure:** If configured as a single entry point for external access, any failure or compromise of the bastion host can disrupt or potentially compromise access to internal resources.
3. **Security Risks:** If not configured securely, the bastion host itself can become a target for attacks. Security vulnerabilities, misconfigurations, and/or weak authentication on them can pose significant risks.
4. **Maintenance Overhead:** Regular maintenance and updates are crucial for the security of the bastion host. Ensuring that security patches are applied promptly without disrupting the services it provides requires careful planning.
5. **User Training:** Users need to be trained on the proper procedures for connecting through the bastion host. Misuse or lack of understanding can lead to security incidents or connectivity issues.
6. **Logging and Monitoring:** Setting up effective logging and monitoring systems for the bastion host is essential. Analyzing logs, detecting unusual activities, and responding to security incidents require dedicated resources and expertise.
7. **Scalability:** As an organization grows, scaling the bastion host solution to accommodate increased user access may require adjustments to the infrastructure and architecture.
8. **Network Latency:** The additional hop through the bastion host can introduce network latency, affecting the responsiveness of remote connections, especially for real-time or bandwidth-sensitive applications.
9. **Compliance Considerations:** Organizations subject to specific compliance standards may face challenges in ensuring that the bastion host solution meets the required regulatory requirements.
10. **Dynamic Environments:** In dynamic environments where IP addresses or configurations frequently change, maintaining up-to-date access controls and configurations for the bastion host can be challenging.
11. **Costs:** The deployment and maintenance of a bastion host may involve additional costs in terms of infrastructure, security tools, and ongoing management.

On June 27, 2019, AWS [introduced *Amazon EC2 Instance Connect*](https://aws.amazon.com/about-aws/whats-new/2019/06/introducing-amazon-ec2-instance-connect/), but there is still a need of a public IP address to be able to use it.

# EC2 Instance Connect Endpoint

On June 14, 2023, AWS launched [Amazon EC2 Instance Connect (EIC) Endpoint](https://aws.amazon.com/about-aws/whats-new/2023/06/amazon-ec2-instance-connect-ssh-rdp-public-ip-address/), a new feature that allows users to connect securely to their instances from the Internet.

With EIC Endpoint, **you no longer need** an [Internet Gateway (IGW)](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html) in your VPC, a public IP address on your resource, a bastion host, or any agent to connect to your resources.

As an additional benefit, the organizational administrator is freed from the operational burden of maintaining and updating bastion hosts for connectivity, and I bet they will be very happy to know about that. 😃🙌

EIC Endpoint, an identity-aware TCP proxy, works with the [AWS Management Console](https://aws.amazon.com/console/) and [AWS Command Line Interface (AWS CLI).](https://aws.amazon.com/cli/) Furthermore, you can continue using your favorite tools, such as PuTTY and OpenSSH.

# Azure Bastion

At Ignite 2019, [Microsoft announced](https://azure.microsoft.com/en-us/updates/azure-bastion-is-now-generally-available/) the general availability of Azure Bastion, a fully managed platform as a service (PaaS) service that provides more secure and seamless RDP and SSH access to virtual machines using private IP addresses directly over TLS through the Azure portal\*.

With Azure Bastion, there is no requirement for your virtual machines to have a public IP address, an agent, or any specific client software.

Azure Bastion is provisioned directly in a customer’s virtual network (VNet) and supports all VMs in their virtual network (VNet) using SSL without any exposure through public IP addresses.

\* Alternatively, you can connect via the native SSH or RDP client already installed on your local computer.

# Conclusion

Effective **February 1, 2024**, AWS will initiate charges for public IPv4 addresses. To optimize your AWS expenses, consider leveraging the [Amazon EC2 Instance Connect (EIC) Endpoint](https://aws.amazon.com/about-aws/whats-new/2023/06/amazon-ec2-instance-connect-ssh-rdp-public-ip-address/) where there is **no longer a requirement** for an Internet Gateway (IGW) in your Virtual Private Cloud (VPC), a **public IP address** on your resource, a bastion host, or any intermediary agent **for connecting to your remote resources.**

Microsoft also provides [Azure Bastion](https://azure.microsoft.com/en-us/products/azure-bastion), a service that **eliminates the need for public IP addresses** on your Virtual Machines (VMs). With Azure Bastion, you can securely access your VMs through a single hardened access point, simplifying remote connectivity.

And stay tuned for my upcoming article where I will explore the detailed steps on setting up this streamlined approach for connecting to remote resources using the Amazon EC2 Instance Connect (EIC) Endpoint.

**If you enjoyed this article and found it helpful, please don’t forget to leave a heart** ❤**, comment** 💬**, clap** 👏🏻**, and share** ➦ **it to show your support.**

**Also, don’t forget to** [**connect**](https://www.linkedin.com/in/rogertn/) **and** [**follow me**](https://medium.com/@rogernem) **for more articles. Thank you!**

References:  
- <https://en.wikipedia.org/wiki/Bastion_host>  
- <https://aws.amazon.com/about-aws/whats-new/2019/06/introducing-amazon-ec2-instance-connect/>  
- <https://aws.amazon.com/blogs/compute/secure-connectivity-from-public-to-private-introducing-ec2-instance-connect-endpoint-june-13-2023/>

[AWS](https://medium.com/tag/aws?source=post_page-----c20fee85a4b2---------------aws-----------------)

[Aws In Plain English](https://medium.com/tag/aws-in-plain-english?source=post_page-----c20fee85a4b2---------------aws_in_plain_english-----------------)

[Azure](https://medium.com/tag/azure?source=post_page-----c20fee85a4b2---------------azure-----------------)

[Security](https://medium.com/tag/security?source=post_page-----c20fee85a4b2---------------security-----------------)

[Cloud Computing](https://medium.com/tag/cloud-computing?source=post_page-----c20fee85a4b2---------------cloud_computing-----------------)