



**VyOS**  
Networks



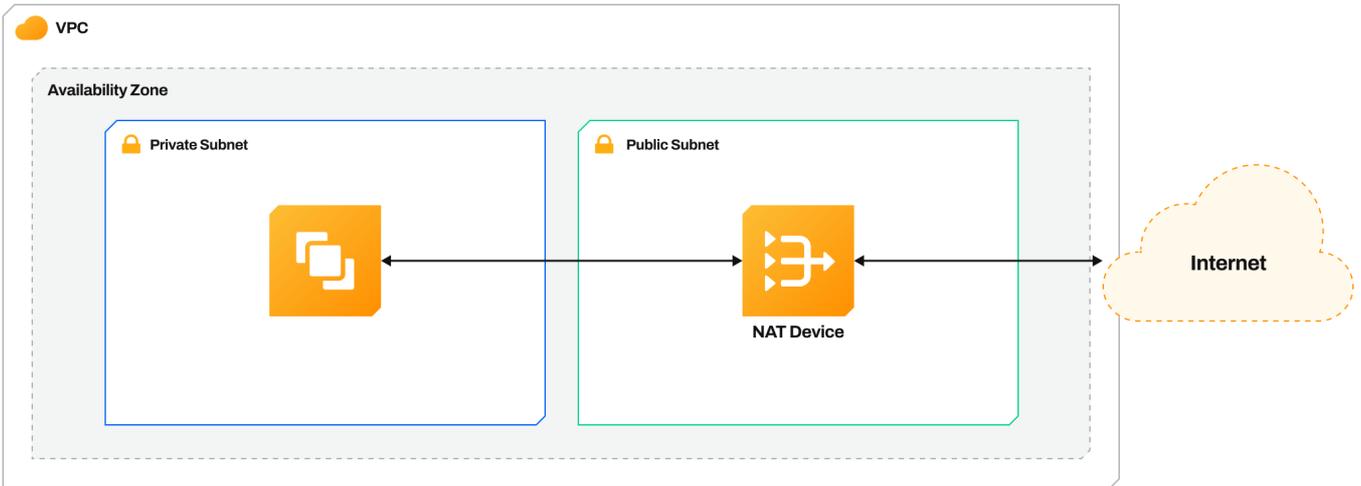
Whitepaper

# **AWS NAT GATEWAY AND NAT INSTANCE**

July 2025

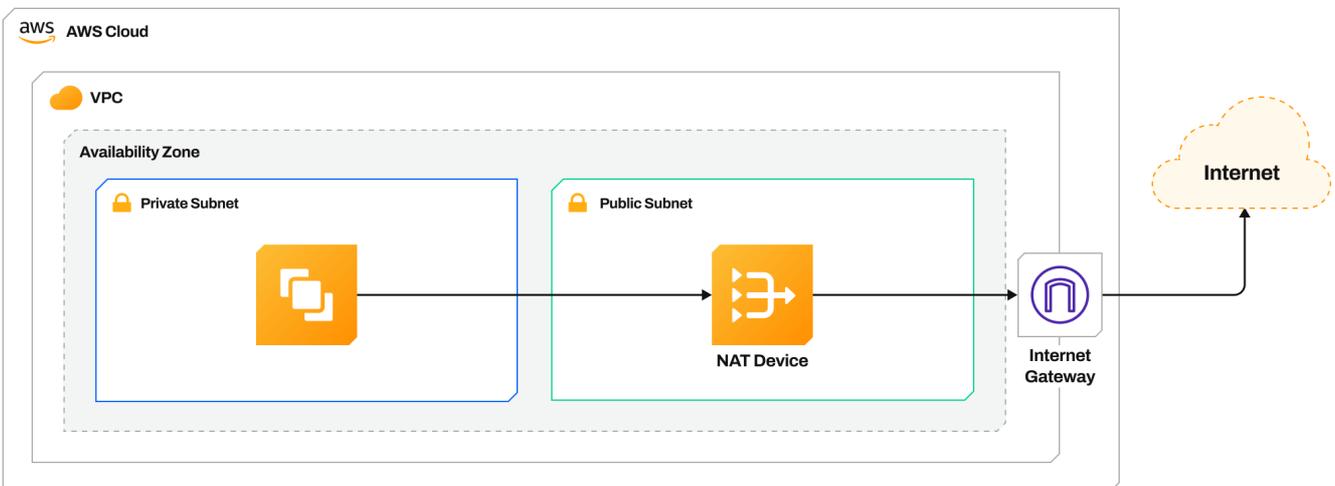
## AWS NAT Gateway and NAT Instance

When designing network architectures in AWS, securely enabling internet access for resources in private subnets is a common requirement. To achieve this, AWS provides two primary solutions: the NAT Gateway and the NAT Instance. Both allow outbound internet traffic from private instances while blocking unsolicited inbound connections, but they differ significantly in terms of cost, scalability, management, and flexibility. Understanding the differences between these two options is essential for choosing the right solution based on your performance needs, security requirements, and budget.



## NAT Gateway

An AWS NAT Gateway is a managed network service that allows instances in a private subnet to securely access the internet or other AWS services. It ensures that outbound traffic is possible while blocking any unsolicited inbound connections. NAT Gateway is highly available, scalable, and designed for minimal administrative effort, making it ideal for secure and efficient internet access from private subnets.



## Pricing for NAT gateways

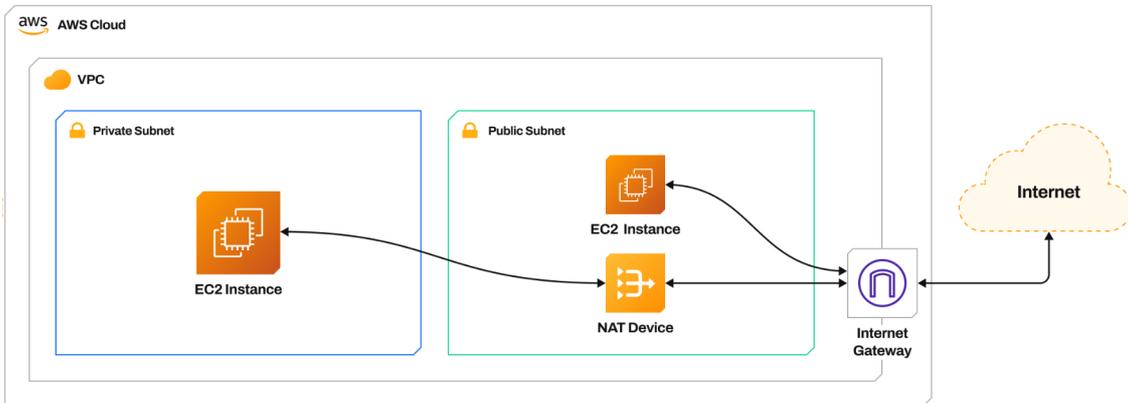
If you choose to create a NAT gateway in your VPC, you are charged for each “NAT Gateway-hour” that your gateway is provisioned and available. Data processing charges apply for each gigabyte processed through the NAT gateway regardless of the traffic’s source or destination. Each partial NAT Gateway-hour consumed is billed as a full hour. You also incur standard AWS data transfer charges for all data transferred via the NAT gateway.

Region	Price per NAT gateway (\$/hour)	Price per GB data processed (\$)
US East (Ohio)	\$0.045	\$0.045

For more information, see [Amazon VPC Pricing](#)

## NAT Instance

An AWS NAT Instance is a virtual machine configured to provide Network Address Translation (NAT) for instances in a private subnet. It allows these instances to initiate outbound traffic to the internet or other AWS services, while preventing unsolicited inbound connections. Unlike managed services, a NAT Instance requires manual configuration, maintenance, and scaling, offering greater flexibility for custom networking setups.



## Pricing for NAT Instance

Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size. e.g.,

Instance Name	On-Demand hourly rate	vCPU	Memory	Storage	Network Performance
t3a.medium	\$0.0376	2	4 GIB	EBS Only	Up to 5 Gigabit

For more information, see [Amazon EC2 Pricing](#)



## AWS NAT Gateway vs NAT Instance

### When to Use Each

- **Use NAT Gateway** when you need high availability, minimal maintenance, and scalable outbound internet access for private subnets in production environments.
- **Use NAT Instance** when you require custom routing or firewall rules, tight budget constraints, or you're operating in a development/test environment where high throughput and availability are less critical.

Feature	NAT Gateway	NAT Instance
Type	Managed service	Self-managed EC2 instance
High Availability	Built-in, across multiple Availability Zones (AZs)	Requires manual setup for HA (e.g., scripts, autoscaling)
Scalability	Automatically scales with traffic	Manual instance size selection and scaling
Bandwidth	Scale up to 100 Gbps	Depends on the bandwidth of the instance type
Performance	Optimized for high throughput (up to 100 Gbps)	Limited by EC2 instance type
Maintenance	Minimal—AWS handles patching and availability	Requires user to manage updates, monitoring, failover, etc.
Security Groups	Cannot be assigned directly	Supports security groups
Logging	VPC Flow Logs, CloudWatch	Full control with OS-level logging
Cost	Charged depending on the number of NAT gateways you use, duration of usage, and amount of data that you send through the NAT gateways.	Charged depending on the number of NAT instances that you use, duration of usage, and instance type and size.
Use Cases	Production environments- High-performance needs- Low operational overhead	Development or testing environments- Custom configurations- Budget-sensitive scenarios
Ease of Setup	Simple setup via console or CLI	Requires manual configuration and routing



## Benefits of Using VyOS as a NAT Instance in AWS

### ■ Full Control and Customization

VyOS gives you complete control over NAT rules, firewall policies, routing protocols, and traffic shaping –ideal for complex or non-standard networking requirements.

### ■ Unified Networking Functions

Beyond NAT, VyOS can serve as a firewall, VPN gateway (IPsec, OpenVPN, WireGuard), DHCP server, and more—consolidating multiple functions into a single instance.

### ■ Support for Advanced Routing Protocols

VyOS supports dynamic routing protocols such as BGP, OSPF, and RIP, allowing seamless integration into hybrid and multi-cloud architectures.

### ■ Automation and Infrastructure as Code

VyOS is fully automatable using Ansible, Terraform, or custom scripts, enabling reproducible deployments and integration into DevOps workflows.

### ■ Logging and Monitoring

Advanced logging capabilities and support for SNMP, NetFlow, and Syslog give you deep visibility into traffic flows and system behavior.

### ■ Security and Fine-Grained Filtering

You can configure detailed firewall rules, zone-based policies, and traffic inspection, providing higher security granularity than default AWS solutions.

### ■ Cost Efficiency with Flexibility

For certain use cases, VyOS can be more cost-effective than a NAT Gateway, especially when you also need VPN, routing, and firewall features in the same instance.

### ■ Open Source and Vendor Neutral

VyOS is open source and hardware-agnostic, making it a flexible choice free from vendor lock-in.

Feature	VyOS NAT Instance	AWS NAT Gateway
Type	Self-managed EC2 instance running VyOS	Fully managed AWS service
NAT Functionality	Full control over NAT rules (SNAT, DNAT, MASQUERADE)	Basic managed SNAT functionality
Firewall Capabilities	Advanced: zone-based firewall, stateful inspection	Basic control via NACLs and Security Groups



Feature	VyOS NAT Instance	AWS NAT Gateway
Routing Support	Supports BGP, OSPF, static routes, policy-based routing	Only supports static routes via route tables
VPN Integration	Built-in IPsec, WireGuard, OpenVPN	Requires separate AWS VPN services
Logging & Monitoring	Full OS-level logs, NetFlow, Syslog, SNMP	Integrated with CloudWatch and VPC Flow Logs
Automation	Fully automatable with Ansible, Terraform, REST API	Simple provisioning via AWS CLI or Console
Scalability	Manual (resize instance or autoscaling group)	Auto-scaled by AWS
High Availability	Requires manual HA setup (e.g., multiple AZs + failover script)	Built-in multi-AZ availability
Security Groups	Fully supported (as it runs on EC2)	Cannot be attached directly
Cost	Lower per-hour EC2 cost; no data processing fee	Higher cost; charged per hour + per GB of data
Use Cases	Custom network setups, hybrid routing, VPN hub, budget-conscious users	Production NAT access with minimal config and high performance
Learning Curve	Requires networking/Linux knowledge	Simple to deploy and use

## Cost comparison

VyOS pricing is based on actual usage, with charges varying according to how much you consume. Subscriptions have no end date and may be canceled any time.

For more information, see [VyOS Universal Router for AWS](#)

Here's a detailed **cost comparison** between using a **VyOS NAT instance** (running on EC2) versus the **AWS NAT Gateway**

Component	AWS NAT Gateway	VyOS NAT Instance (EC2)
Hourly charge	\$0.045/hour (\$32.4/month)	Varies by instance: e.g., t3a.medium \$0.0376/hour + VyOS subscription \$0.1/hour ≈ \$99/month
Data processing fee	\$0.045/GB processed	None
Egress data transfer	\$0.09/GB (Standard AWS egress)	\$0.09/GB (Same egress fee)



Component	AWS NAT Gateway	VyOS NAT Instance (EC2)
Total per-GB cost	~\$0.135/GB (processing + egress)	~\$0.09/GB (egress only)
Monthly EC2 cost	N/A	~\$27 for t3a.medium
Monthly NAT Gateway cost	\$32.85	N/A

### Example Scenario: 10 TB/month of outbound data

#### AWS NAT Gateway

- Hourly charge:  $\$0.045 \times 730h = \$32.85$
- NAT processing:  $\$0.045 \times 10,000 \text{ GB} = \$450$
- Egress fee:  $\$0.09 \times 10,000 \text{ GB} = \$900$

TOTAL: **\$1,382.85/month**

#### VyOS NAT Instance (t3a.medium)

- Hourly charge:  $\sim\$0.0376 \times 720h = \$27$
- NAT processing:  $\$0.1 \times 720h = \$72$
- Egress fee:  $\$0.09 \times 10,000 \text{ GB} = \$900$

TOTAL: **\$999/month**

### Cost Example: 10 TB Outbound per Month

Scenario	NAT Gateway	VyOS NAT Instance
Monthly base cost	\$32.85	~\$99
10 TB data processing (@\$0.045/GB)	\$450	\$0
10 TB egress (@\$0.09/GB)	\$900	\$900
Total	\$1,382.85/month	\$999/month

✔ Savings with VyOS: **~\$383,85/month (~28%) in this scenario.**

## When VyOS NAT Instance Makes Sense

- You handle **significant outbound data volumes** (1 TB/month or more).
- You want **extra features** (firewalling, VPN, routing protocols).
- You can manage the **instance yourself** (updates, failover, etc.).
- You aim to **reduce costs** without losing flexibility.

