

ACG FUNDAMENTALS

What is a Bastion Host?

A Bastion Host:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of a firewall or in a demilitarized zone (DMZ) and usually involves access from untrusted networks or computers.



The diagram illustrates a VPC (Virtual Private Cloud) configuration in the us-east-1 region. The VPC is labeled "VPC (acloudguruVPC) - 10.0.0.0/16". It contains two subnets: "PUBLIC SN (10.0.1.0/24)" and "PRIVATE SN (10.0.2.0/24)".

In the PUBLIC SN, there is a "Bastion" instance, a "NAT Instance", a "Security Group", and a "NAT Gateway".

In the PRIVATE SN, there is an "Instance" and a "Security Group".

The VPC is connected to the Internet Gateway via a "Router". The Router is connected to the Internet Gateway and has two "Route Table"s associated with it. The "Network ACL" is also associated with the VPC.

The diagram illustrates the network architecture for connecting to a VPC from the Internet. It shows the following components and flow:

- Internet Gateway:** The entry point for traffic from the Internet.
- Router:** Receives traffic from the Internet Gateway and directs it through the Route Tables.
- Route Tables:** Two tables that define the routing paths for traffic entering the VPC.
- Network ACL:** A layer of security that filters traffic at the subnet level.
- VPC (acloudguruVPC) - 10.0.0.0/16:** The Virtual Private Cloud containing the subnets and instances.
 - PUBLIC SN (10.0.1.0/24):** The public subnet where the **Bastion Instance** and a **NAT Gateway** are located. A **Security Group** is associated with the Bastion Instance.
 - PRIVATE SN (10.0.2.0/24):** The private subnet containing another **Instance** and a **Security Group**.

Traffic flow is indicated by arrows: from the Internet Gateway to the Router, then through the Route Tables and Network ACL to the Bastion Instance in the public subnet. The Bastion Instance then connects to the private instance via a NAT Gateway.

Remember the following;

- A NAT Gateway or NAT Instance is used to provide internet traffic to EC2 instances in a private subnets.
- A Bastion is used to securely administer EC2 instances (Using SSH or RDP). Bastions are called Jump Boxes in Australia.
- You cannot use a NAT Gateway as a Bastion host.