How does Outbound Traffic Work on a Cloud Network in a MCP 1.0 location

Description

Describes how outbound traffic from a Cloud Network works in MCP 1.0, including Public IP Traffic, Private IP traffic, and Global SNAT address translation technology in place between data centers.

NOTE: This article applies only to MCP 1.0 locations. For details on MCP 2.0 behavior, see Introduction to Routing, Network Domain Static Routes, and SNAT in MCP 2.0 Locations.

Content / Solution:

TRAFFIC DESTINED FOR PUBLIC INTERNET

By default, Cloud Networks have a SNAT (Source NAT) set up for outbound traffic so that traffic destined for any public IP address uses a single public IP address associated with that network. You can identify this IP address by connecting to http://whatismyipaddress.com from a server inside the network.

You can change this behavior by setting up a NAT that maps your server's private IP address to a single public IP address. In that case, the server NAT will take precedence and all traffic from that private IP address will route using the public IP address established by the NAT. For instructions on how to set up a NAT, see the instructions at How to Create a NAT Rule on a Network or Network Domain

TRAFFIC DESTINED FOR PUBLIC IP ADDRESSES OF CLOUD NETWORKS

Traffic destined for a public IP addresses associated with a Cloud Networks work the same as traffic destined for the public Internet with one exception. The exception involves traffic destined for a public IP addresses bound to the same Cloud Network. In those cases, the behavior depends on the nature of the public IP address:

1. You can **NOT** reach the public IP address of a NAT from the Cloud Server to which the NAT is bound. For example, if I have a Cloud Server of 10.166.0.11 with a NAT of 207.20.46.1, you will not be able to connect to the 207.20.46.1 IP address from the 10.66.0.11 Cloud server or any other cloud server in the same network as 10.66.0.11. However, note that you can reach that public IP address from other Cloud Servers on another Cloud Network.
2. By default, you cannot reach the public IP address of a VIP from any Cloud Server on the same Cloud Network unless "Server to VIP" functionality has been established for the IP block associated with the VIP. See How to Manage Public IPv4 Addresses on a Network or Network Domain for more details.

TRAFFIC DESTINED FOR CLOUD NETWORK PRIVATE IP ADDRESS SPACE

Traffic between private IP addresses on different Cloud Networks is routable by default, even if the Cloud Networks are owned by different clients. Such traffic works differently than traffic destined for Public IP addresses:

1. Traffic between Private IP addresses in different data centers is automatically encrypted as it travels across a private VPN connection established between each Cloud data center. These connections are in place both between data centers in the same Geographic region (i.e between US-East and US-West) and data centers in different Geographic regions (i.e. between US-East and Amsterdam).
2. Traffic destined for a Private IP address of any other Cloud Network does not go through a SNAT as it leaves the source Cloud Network. Instead, the traffic will appear to the destination Cloud Network as coming from the source private IP address rather than a public SNAT.
3. Default ACL Rules governing such behavior are in the process of changing - The current default ACL rules will **allow** such traffic on the standard HTTP, HTTPS, and PING ports, meaning that unless you establish changes to the ACL rules, these ports are available from any private IPv4 address space in the MCP 1.0 universe - even from other clients. However, at some future date, this behavior is changing and all private IPv4 traffic will be **denied** on newly deployed MCP 1.0 Cloud Networks. A notification with further details will be sent out well before any changes are made.

NOTE: For networks deployed prior to September 29, 2010, the notes listed above about private IP traffic do NOT apply. Instead, the default behavior is identical to traffic destined for the Public Internet as described above. That means the traffic leaves the network as public traffic and is neither encrypted or accelerated. If you need to know whether you deployed a specific network prior to this date, contact Support and we will verify for you.

Related Articles

- Introduction to the Compute Menu
- New Features by Release
- Introducing the New Red Hat Update Infrastructure
- Introduction to the UI
- Introduction to Cloud Backup Metering and Billing