

Azure Asymmetric Routing

There exists an asymmetric routing scenario between campus and Azure resources that is similar to that at AWS.

Description of Problem :

This issue is realized when there exists both :

- A VNet that is peered to the sharedservices VNet with gateway transit enabled thru ExpressRoute.
- A VM with an external IP that is being requested from the Cornell campus network.

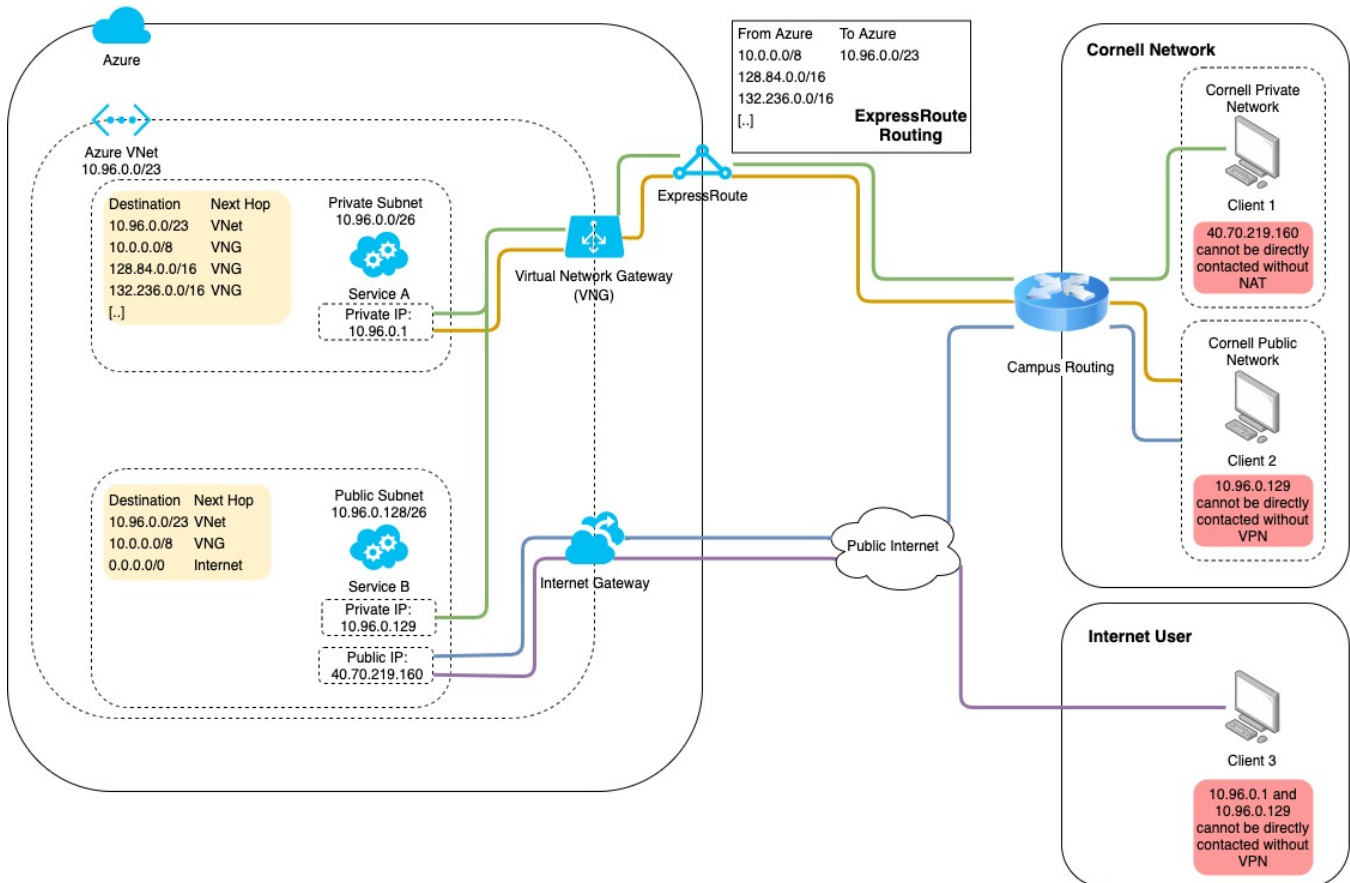
With all of these pieces in place, packets sent from campus to the external IP will return to campus via the ExpressRoute and be dropped by the initiating host.

Solution:

- We create two subnets in the customer VNet - one "private", one "public".
- A user defined route (UDR) will be created and then associated with the public subnet.
- The UDR will list all campus IP ranges with a next hop of "Internet".

Caveat:

- With the UDR in place the opposite asymmetric route will be true.
- A campus network system with a public IP, trying to reach the "10 space" address of an Azure VM on the subscription's public subnet, will fail.



IPv4 Global Address Blocks Owned and Managed by Cornell

Cornell owns and manages the following publicly routable IPv4 global address blocks:

- 128.84.0.0/16
- 128.253.0.0/16

- 132.236.0.0/16
- 192.35.82.0/24
- 192.122.235.0/24
- 192.122.236.0/24

<https://it.cornell.edu/dns/ip-addresses-and-subnets-cornell>