# Traffic Flow of Destination NAT through Edge Gateway

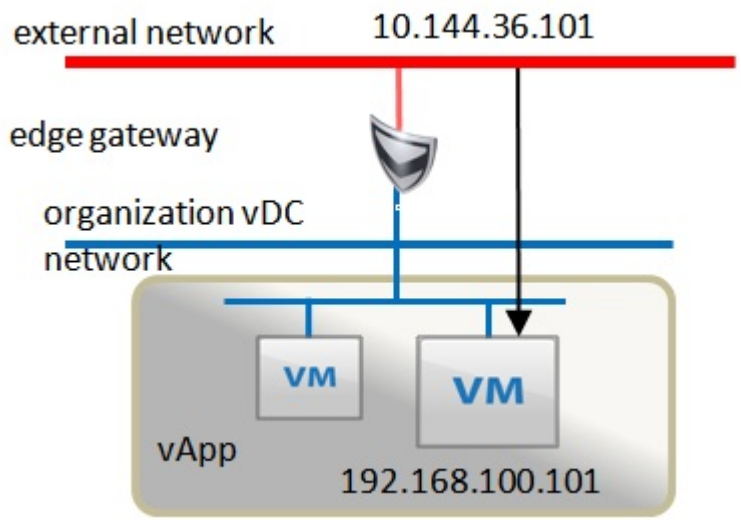
Did you ever wonder how the traffic flows when you create a Destination NAT? If the answer is Yes then you should follow the rest and if no then you already know how it works

Destination NAT (DNAT) maps an unregistered IP address to a registered IP address from a group of registered IP addresses. Destination NAT also establishes a 1:1 mapping between unregistered and registered IP address, but the mapping could vary depending on the registered address available in the pool, at the time of communication.

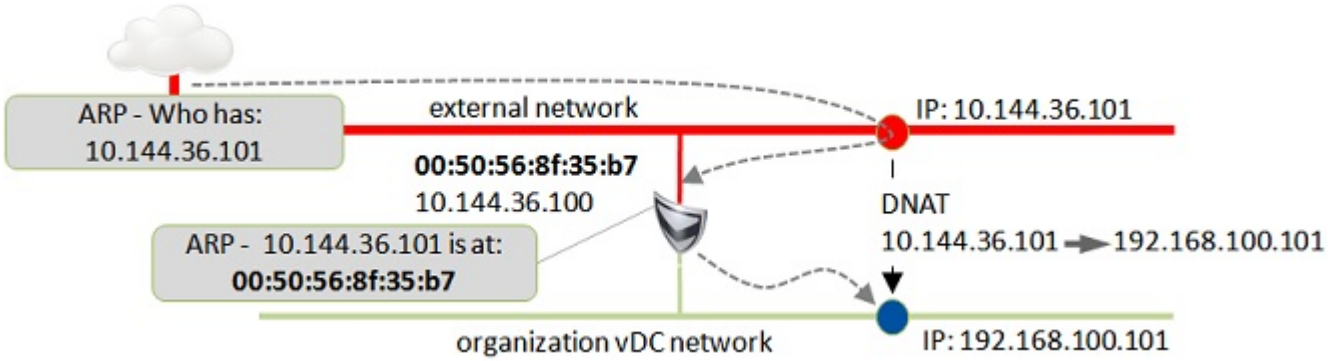
The typical usage of this is to redirect incoming packets with a destination of a public address/port to a private IP address/port inside your network.

The internal network is usually a LAN (Local Area Network), commonly referred to as the stub domain. A stub domain is a LAN that uses IP addresses internally. Most of the network traffic in a stub domain is local, it doesn't travel off the internal network. A stub domain can include both registered and unregistered IP addresses. Of course, any computers that use unregistered IP addresses must use Network Address Translation to communicate with the rest of the world.

So now let me show you a example design where we are mapping (DNAT) an External IP Address to an Internal IP Address.




In this example we are mapping 10.144.36.101 to an internal VM IP which is 192.168.100.101. This is pretty straight forward and does not need any explanation. I will now show you the flow diagram and will explain how the packet flows.




Now look at the above diagram. Lets say we have a client in the external network who is trying to connect to the internal VM which is inside the Org vDC network and has an internal IP Address (192.168.100.101).

Now the client will send an ARP for the external address which is 10.144.36.101. Your Edge device's external interface has an external IP address. That will listen and will reply saying that ARP is in his external MAC. Once this is done, then your Edge will query the database (Routing Table?) and will see that there is a 1:1 mapping of its internal IP, it will send the packet through the internal interface to the appropriate VM.

So destination NAT changes the destination address in IP header of this packet. It may also change the destination port in the TCP/UDP headers.