# **Lab: Network Address Translation**

## **Overview**

NAT (Network address translation) is a technique performed by routers whereby the IP address in a packet header is altered in transit so that the destination interprets the packet as coming from the new IP instead of the actual originating IP. One-to-many NAT has played a vital role globally in delaying [IPv4 address exhaustion](https://en.wikipedia.org/wiki/IPv4_address_exhaustion), greatly reducing the need to transition at a large scale to IPv6.

In network administration, you may encounter sub-optimal situations where two LANs share the same network addressing scheme. For example, the 192.168.1.1/24 network address is extremely common amongst consumer grade routers. 1:1 NAT can offer a workaround for this kind of issue.

## **Scenario**

GlobeX has made a strategic acquisition and needs to share resources over a VPN tunnel. However, your manager wishes to obfuscate the corporate network architecture for security reasons. You’ve been tasked with working up a proof of concept as to how GlobeX can conceal the IP addresses of critical resources such as file servers.

## **Prerequisites**

* Two networks with pfSense at the edge, connected via IPsec VPN
* A VM on the Corporate network
* A VM on the External network

## **Objectives**

* Successfully ping from the VM on the Corporate network to the VM on the External network.
* Create a 1:1 NAT rule that alters the IP address of the Corporate VM for hosts accessing it from over the VPN tunnel.

## **Resources**

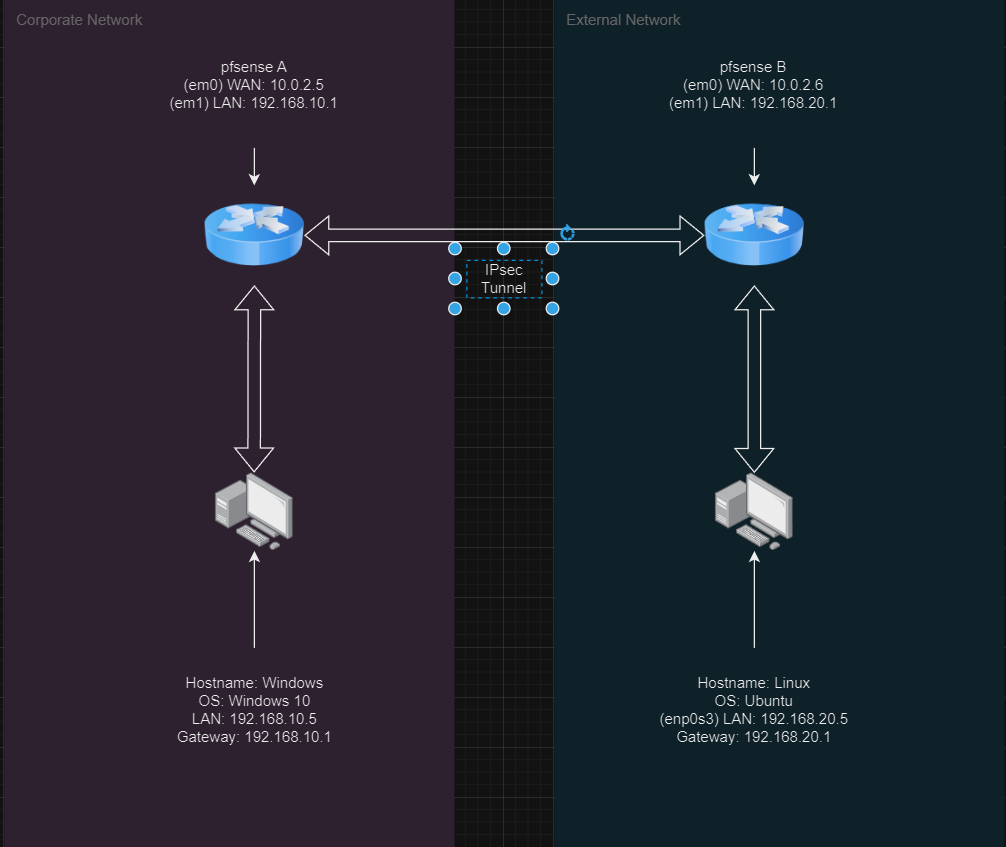
* [Netgate Docs - 1:1 NAT](https://docs.netgate.com/pfsense/en/latest/nat/1-1.html)
* [Troubleshooting NAT](https://docs.netgate.com/pfsense/en/latest/troubleshooting/nat.html)
* [Troubleshooting NAT 1:1](https://docs.netgate.com/pfsense/en/latest/troubleshooting/nat-1-1.html)
* [Troubleshooting NAT Port Forwards](https://docs.netgate.com/pfsense/en/latest/troubleshooting/nat-port-forwards.html)

## **Tasks**

### **Part 1: Topology 1/2**

Read through the entire lab:

* ~~use Draw.io to create an appropriate topology of the network you expect to construct.~~
* ~~Include as many details as you can such as:~~ 
  + ~~computer names,~~
  + ~~OS types,~~
  + ~~IP addresses, etc.~~
  + ~~Include a screenshot of this initial topology.~~

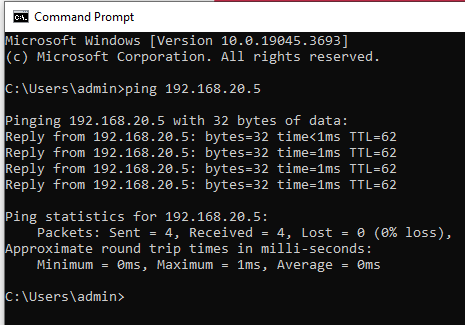


### **Part 2: Staging the Networks**

This lab requires that you’ve established a VPN tunnel between two pfSense networks in VirtualBox:

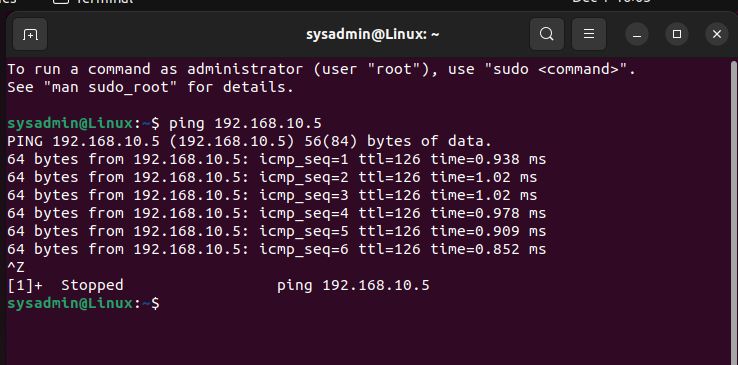
* ~~From another VM on the Corporate (internal) network, successfully ping the VM you will configure with NAT.~~

**Ping successful**



* ~~From External , ping the Corporate (internal) network via the VPN tunnel. Include a screenshot of this operation.~~

**Ping successful (seriously, didn’t we do all this on friday?)**

****

* ~~If you are using Windows 10 VMs,~~ [~~create a firewall rule to allow ICMP traffic~~](https://www.how2shout.com/how-to/allow-windows-10-ping-through-firewall-gui-powershell-netsh-command.html)~~. This will make testing your network easier, and will help you diagnose problems with you network.~~

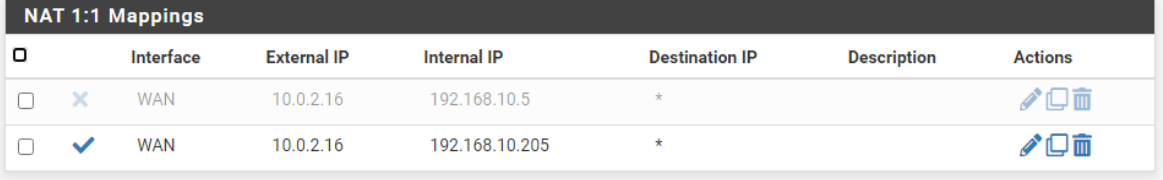
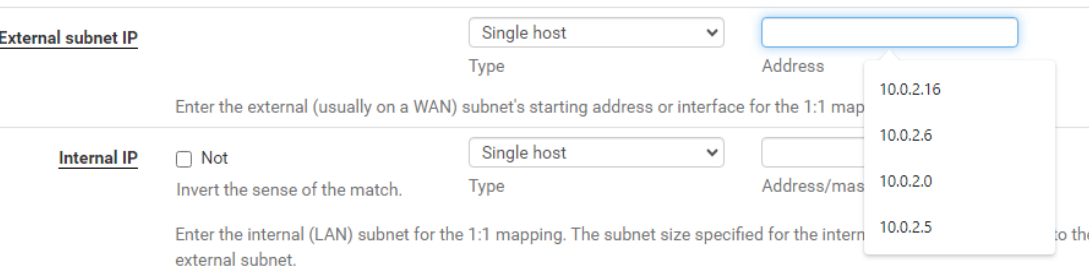
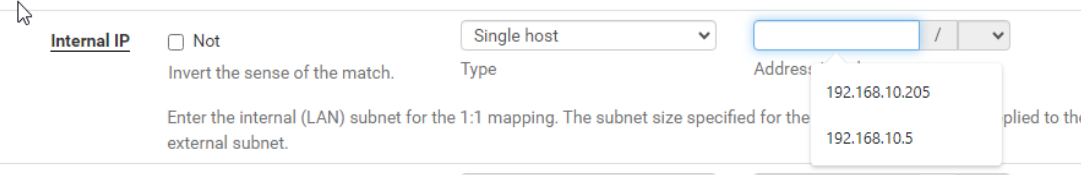
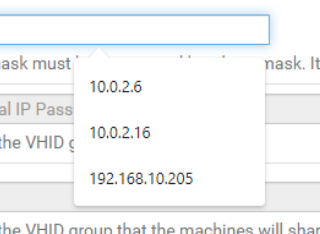
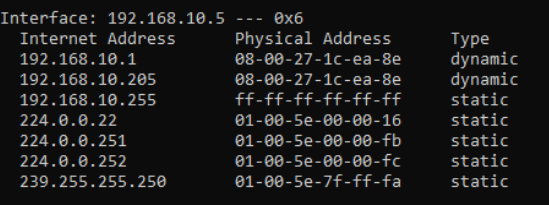
**Why do this as step 3, when it really needs to be step 2? Either way, I turned the firewall back on, and enabled the file and printer sharing - with a small edit, to the inbound rule everything is gravy.**

### **Part 3: Configuring the Networks**

Now that we have established normal comms between the networks, and pings are working, let’s start experimenting with NAT. We can use a 1:1 NAT rule in pfSense to convert the IP address of our Corporate VM for VPN users:

**OK, here is where things run amiss. I have so far:**

**Created MANY virtual IPs 10.0.2.16, 10.0.2.6, 192.168.10.205**

**And I have created SOOOO many NAT 1:1s. And I have come to this conclusion… This sucks.**

**I have tried every combination I can think of, have reset IPsec more than I can count, watched youtube tutorials**

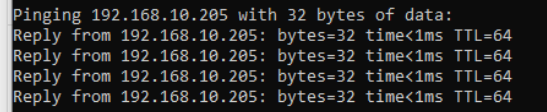
[**https://www.youtube.com/watch?v=HkJ8fTT9yqk**](https://www.youtube.com/watch?v=HkJ8fTT9yqk)

[**https://www.youtube.com/watch?v=IsUFzuhwsME&t=698s**](https://www.youtube.com/watch?v=IsUFzuhwsME&t=698s)

[**https://www.youtube.com/watch?v=rFGV0Jfeu5o**](https://www.youtube.com/watch?v=rFGV0Jfeu5o)

**This is all to say, I tried.**

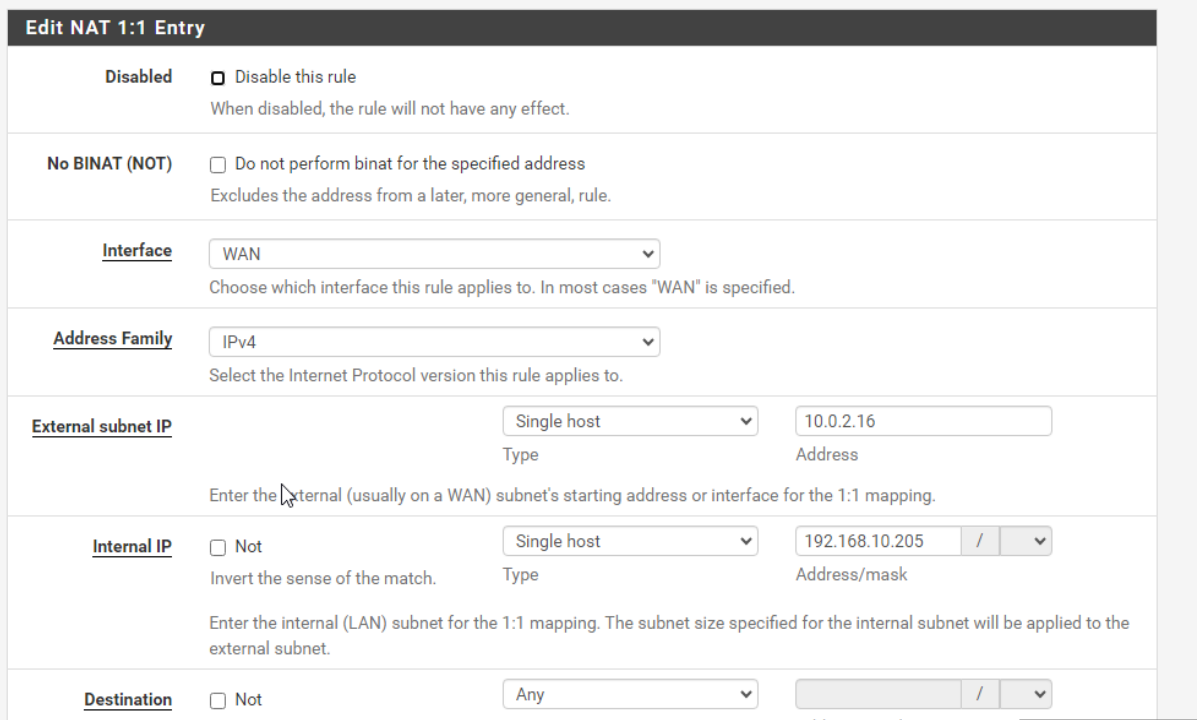
**Here is what I know… Without setting up a fileshare, or some other thing, I am failing to understand how I am supposed to know that my external VM (Linux) is presenting as an internal LAN ip.**

****

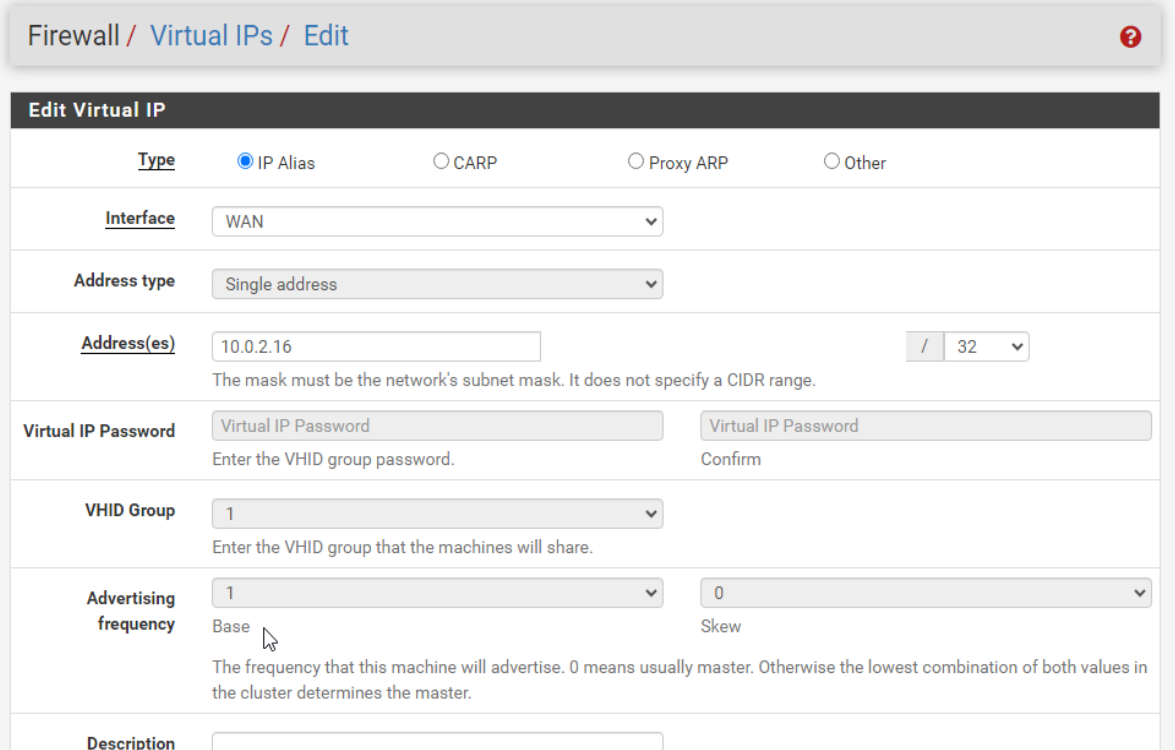
**Above is a ping to a virtual ip… BEFORE it has been setup 1:1. So pings aren’t enough. I included an arp -a which also shows it as there. What are we doing right now? I think there is a lack of guidance here.**

* ~~In pfSense, utilize 1:1 NAT to convert the Corporate VM IP to a different IP if accessed via VPN tunnel.~~
* ~~To accomplish this, you can use the 1:1 NAT features built into IPsec VPN in pfSense.~~
* ~~Include a screenshot of your configuration.~~

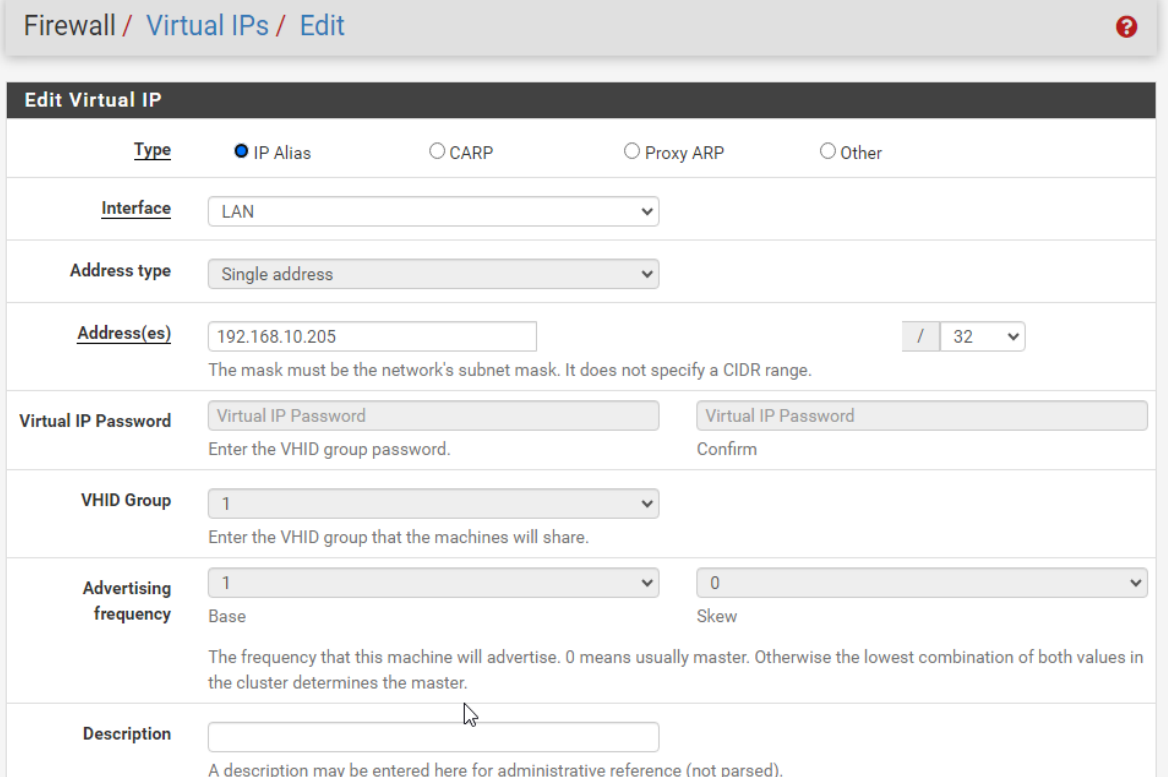
**NAT 1:1**



**Here is my virtual IP for the WAN**



**Here is my LAN Virtual IP**

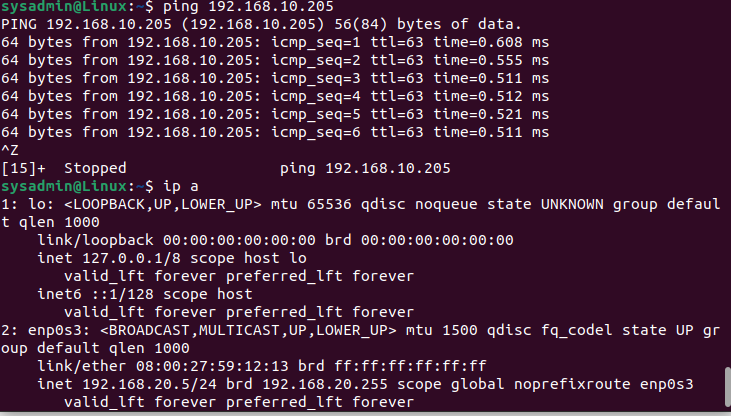


### **Part 4: Testing**

Now let’s test and verify that the NAT is translating the NAT IP address correctly and that we can ping it from the External VM:

* ~~Include a screenshot of successfully pinging the NAT IP from the external VM.~~

**Is this all you wanted? IDK. it pings though.**



### **Part 5: Topology 2/2**

When the other tasks are complete:

* ~~review the topology and update, revise, extend, or add details as necessary.~~

**Nothing needed to be changed.**

* ~~Was your initial topology accurate to the finished product? Why or why not?~~

**There were no changes because I didn’t “do” anything to the network. While there is a NAT rule in place, that is just encasing my IP, not actually changing it.**