- Using NAT with PIX/ASA Devices -

NAT (Network Address Translation)

The rapid growth of the Internet resulted in a shortage of IPv4 addresses. In response, the powers that be designated a specific subset of the IPv4 address space to be *private,* to temporarily alleviate this problem.

A **public address** can be routed on the Internet. Thus, devices that should be Internet accessible (such web or email servers) must be configured with public addresses.

A **private address** is only intended for use within an organization, and can never be routed on the internet. Three private addressing ranges were allocated, one for each IPv4 class:

- Class A - **10.x.x.x**
- Class B - **172.16-31.x.x**
- Class C - **192.168.x.x**

NAT (Network Address Translation) is used to translate between private addresses and public addresses. NAT allows devices configured with a private address to be *stamped* with a public address, thus allowing those devices to communicate across the Internet.

NAT is *not* restricted to just public-to-private address translations, though this is the most common application of NAT. NAT can perform a public-to-public address translation, or a private-to-private address translation as well.

NAT provides an additional benefit – hiding the specific addresses and addressing structure of the internal network.

Both Cisco IOS devices and PIX/ASA firewalls support NAT.

(Reference: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a0080194af8.shtml)

* * *

Types of NAT

NAT can be implemented using one of three methods:

Static NAT – performs a static one-to-one translation between two addresses, or between a *port* on one address to a port on another address. Static NAT is most often used to assign a public address to a device behind a NAT-enabled firewall/router.

Dynamic NAT – utilizes a **pool** of global addresses to dynamically translate the outbound traffic of clients behind a NAT-enabled device.

NAT Overload or **Port Address Translation (PAT) –** translates the outbound traffic of clients to unique port numbers off of a *single* global address. PAT is necessary when the number of internal clients exceeds the available global addresses.

NAT Terminology

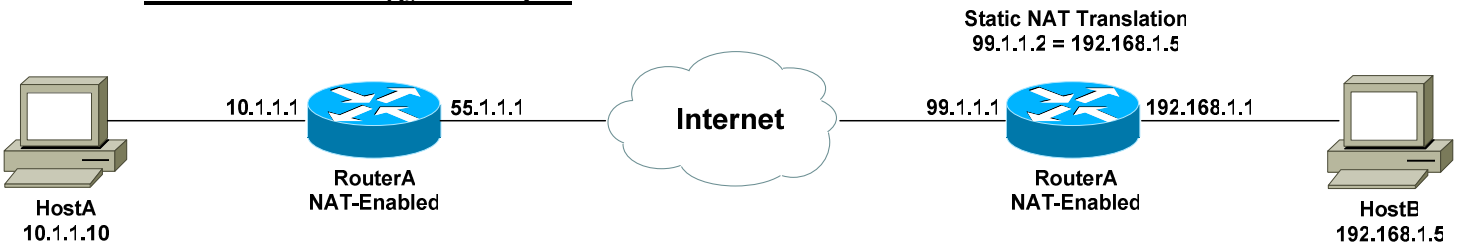
Specific terms are used to identify the various NAT addresses:

- **Inside Local –** the specific IP address assigned to an *inside* host behind a NAT-enabled device (usually a *private* address).
- **Inside Global –** the address that identifies an *inside* host to the *outside* world (usually a *public* address). Essentially, this is the dynamically or statically-assigned public address assigned to a private host.
- **Outside Global** – the address assigned to an *outside* host (usually a *public* address).
- **Outside Local** – the address that identifies an *outside* host to the *inside* network. Often, this is the **same** address as the Outside Global. However, it is occasionally necessary to translate an outside (usually *public*) address to an inside (usually *private*) address.

For simplicity sake, it is generally acceptable to associate **global** addresses with **public** addresses, and **local** addresses with **private** addresses. However, remember that public-to-public and private-to-private translation is still possible. **Inside** hosts are within the local network, while **outside** hosts are external to the local network.

* * *

NAT Terminology Example



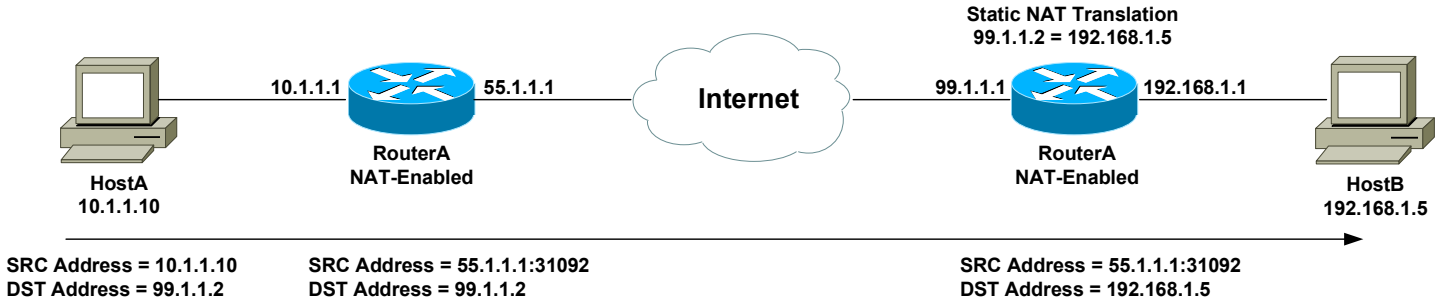
Consider the above example. For a connection *from* HostA *to* HostB, the NAT addresses are identified as follows:

- **Inside Local Address** - 10.1.1.10
- **Inside Global Address** - 55.1.1.1
- **Outside Global Address** – 99.1.1.2
- **Outside Local Address –** 99.1.1.2

HostA's configured address is *10.1.1.10*, and is identified as its *Inside Local* address. When HostA communicates with the Internet, it is stamped with RouterA's public address, using PAT. Thus, HostA's *Inside Global* address will become *55.1.1.1*.

When HostA communicates with HostB, it will access HostB's *Outside Global* address of *99.1.1.2*. In this instance, the *Outside Local* address is also *99.1.1.2*. HostA is never aware of HostB's configured address.

It is possible to map an address from the local network (such as 10.1.1.5) to the global address of the remote device (in this case, 99.1.1.2). This may be required if a legacy device exists that will only communicate with the local subnet. In this instance, the *Outside Local* address would be *10.1.1.5*.



The above example demonstrates how the source (SRC) and destination (DST) IP addresses within the Network-Layer header are translated by NAT.

(Reference: *http://www.cisco.com/warp/public/556/8.html*)

* * *

Configuring Dynamic Inside NAT Translations

To configure the PIX/ASA to dynamically translate *inside* addresses to one or more *outside* addresses, the addresses to be *NAT*ed (or *translated*) must be identified. The *nat* command will accomplish this:

pixfirewall(config)# *nat (inside) 1 172.16.0.0 255.255.0.0*

The above command states that any addresses on the *172.16.0.0 255.255.0.0* subnet, located off of the *inside* interface, are eligible for translation. The *1* is the **NAT ID**, which will be referenced later.

To specify that *all* addresses off the inside interfaces should be translated:

pixfirewall(config)# *nat (inside) 1 0.0.0.0 0.0.0.0*

Once traffic to be translated has been identified, the address (or addresses) this traffic will be translated *to* must be identified. The *global* command will accomplish this:

pixfirewall(config)# *global (outside) 1 66.1.1.9 netmask 255.255.255.255*

The above *global* command will translate all addresses from the *nat* statement to the *66.1.1.9* address on the *outside* interface. Since only one global address was specified, **Port Address Translation (PAT)** or **NAT overload** will be employed.

Please NOTE: The NAT ID must match between *nat* and *global* statements. This *connects* them together, as multiple *nat/global* pairings can exist.

To specify a range of global addresses:

pixfirewall(config)# *global (outside) 1 66.1.1.9-66.1.1.14 netmask 255.255.255.248*

The *global* command can alternatively reference the IP address **currently active** on an interface. This is useful when the public interface is obtaining an address dynamically through DHCP:

pixfirewall(config)# *global (outside) 1 interface*

The above command will translate addresses specified in the *nat* statement to the currently active IP address on the *outside interface.*

* * *

Configuring Dynamic Inside NAT Translations (continued)

Recall that the NAT ID must match between *nat* and *global* statements. This *connects* them together, as multiple *nat/global* pairings can exist:

pixfirewall(config)# *nat (inside) 1 192.168.1.0 255.255.255.0*
pixfirewall(config)# *global (outside) 1 66.1.1.9-66.1.1.14 netmask 255.255.255.248*

pixfirewall(config)# *nat (inside) 2 192.168.2.0 255.255.255.0*
pixfirewall(config)# *global (outside) 2 66.1.1.17-66.1.1.22 netmask 255.255.255.248*

Inside hosts on the *192.168.1.0/24* subnet will be translated to an outside address on the *66.1.1.8/29* subnet, while inside hosts on the *192.168.2.0/24* subnet will be translated to an outside address on the *66.1.1.16/29* subnet.

Note that the NAT IDs match between *nat/global* pairs.

Preventing Addresses from Being Translated

It is possible (and sometimes required) to prevent NAT from translating specific addresses. Situations when this might be necessary include:

- If a 'trusted' interface contains hosts with public addresses, that need to be Internet-accessible.
- If traffic is traversing a VPN, from one private network to another.

To specify addresses that *should not* be NATed:

pixfirewall(config)# *nat (inside) 0 77.1.1.1 255.255.255.255*

The NAT ID of *0* has been reserved for disabling NAT for specific addresses. If NAT must be disabled for a large number of addresses/devices, an *access-list* can be used in conjunction with the *nat* statement.

pixfirewall(config)# *access-list NONAT permit ip any 172.16.1.0 255.255.255.0*
pixfirewall(config)# *access-list NONAT permit ip any 172.16.2.0 255.255.255.0*

pixfirewall(config)# *nat (inside) 0 access-list NONAT*

* * *

Configuring Static NAT Translations

Static NAT translations perform a static one-to-one translation between two addresses, or between a *port* on one address to a port on another address. The most common application for static translations is to allow outside (*less trusted*) hosts access an inside (*more trusted*) host.

Please Note: Simply creating a Static NAT translation is not sufficient to provide outside hosts access to an inside host. An **access-list** must be used in conjunction with the static NAT to actually *permit* the access.

Static translations **take precedence** over dynamic translations.

The *static* command is used to configure a static NAT translation. Consider the following scenario:

- A web server exists on the *inside* interface of the PIX/ASA firewall, and is configured with a private address of 10.5.1.5.
- This web server should be publicly accessible from the *outside* interface using a public address of 66.1.1.9.

The proper syntax to create this static NAT translation would be as follows:

pixfirewall(config)# *static (inside,outside) 66.1.1.9 10.5.1.5*

Confusing, right?

The interfaces in the parenthesis indicate the **prenat interface** and **postnat interface.** From the PIX/ASA's perspective, an outside address is *not* being translated to an inside address. Instead, *an inside address is being translated to an outside address*. Thus, the *static* commands logic is:

(*prenat,postnat)*

However, following the *prenat/postnat* interface parameter, the *outside* address (*66.1.1.9)* is specified first, and then the *inside* address (*10.5.1.5)*.

Why, oh why, do you torture us so, Cisco?

* * *