



Global Knowledge®

Expert Reference Series of White Papers

# Security Translated: An Overview of Cisco ASA NAT and PAT

# Security Translated: An Overview of Cisco ASA NAT and PAT

Jeffrey W. Hall, VCI, VCP, CCSI, CCNP Security, CCNP Voice, CCIP, CCDP, CCNP

## Two important caveats for this white paper:

1. The author will use only RFC 1918-compliant addressing in this whitepaper to avoid using someone's purchased IP addressing.
2. There are many advanced NAT and PAT configurations possible on the Cisco ASA, but this white paper will only discuss a sampling of these capabilities. For a complete coverage of the Cisco ASA's NAT and PAT capabilities and requirements, see the **Summary** section at the end of the paper.

## Introduction

By the early-to-mid 1990s, network architects and engineers began to realize that the number of potential addresses provided by the IPv4 standard would not last nearly as long as was once thought. In May 1994, RFC 1631, *The IP Network Address Translator (NAT)*, was released by authors Kjeld Borch Egevang and Paul Francis. This Request for Comment (RFC) introduced a mechanism that allowed for the reuse of private IP addresses, defined in RFC 1918, to combat the rapidly disappearing public IP address space.

Today, we take NAT for granted, but when this RFC was released in 1994, it was a considerable revelation. Even though RFC 1631 acknowledges that the authors were not the first to conceive the idea of using private addressing space that anyone could use and then simply translate it into real-world routable addressing, it was a thought that very few people had the foresight to envision at the time.

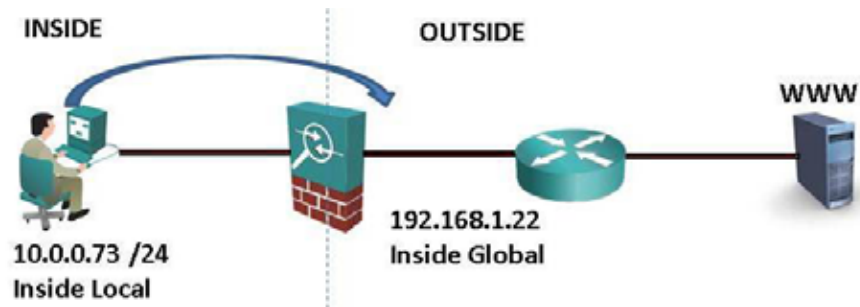
While many network administrators and engineers may have first learned to configure network address translation via NAT and the newer version PAT (Port Address Translation) on routers, it is predominantly a firewall function. As such, we will see in this whitepaper the real power of the Cisco ASA and its ability to combine variations of NAT and PAT in advanced configurations.

The Cisco ASA as a Translation Device The two primary types of address translation are inside source and outside source translation.

### 1. Inside Source Translation

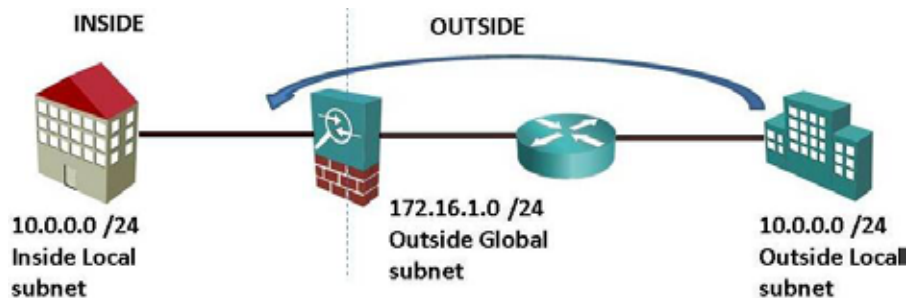
This method translates private addressing on the company's inside network, which is not routable on the global Internet, to addresses that are routable on the global Internet. An example of this method would be an employee sitting at her computer accessing an Internet website. When she browses to the website and the packets stream from her computer to the firewall appliance, it records her computer's private IP address and translates it to a globally-routable IP address and sends the packets on towards the destination web server. During this

process, the firewall maintains a translation table of these recorded addresses so that when the response comes back from the web server, the firewall will know how to properly translate the globally-routable IP address in the packet's Layer 3 header to the internal private IP address and send it back to the originating computer. This is the most common use of address translation, and it is generally the method focused on in most vendor training programs.



## 2. Outside Source Translation

This method translates IP addressing from devices on the outside of your network as they come into your firewall device. An example of this scenario might show a corporation that has just purchased a competitor and made it one of their new branch offices. In this scenario, the former competitor is using the same private addressing as the company, so the company wants to translate the branch office traffic as it enters the firewall device from the outside. By doing this, the branch office will appear as different IP addressing inside of the main corporate network.



While both of these are valid, this white paper focuses on the Inside Source Translation method for all of the following examples.

## Terminology

To properly understand NAT and PAT, we must first cover some key terms.

1. **Inside Local address** represents the private internal IP address TO BE translated. This address is given to hosts within the corporate network and is not routable on the public Internet.

2. **Inside Global address** represents the globally routable IP address that the Inside Local address will be translated to. This address is assigned by the Network Information Center (NIC) or Internet Service Provider (ISP).
3. **Outside Local address** represents the IP address of a host on the outside of the corporate network as it appears to the inside network. This address is typically the "Inside Local" address of the remote corporation.
4. **Outside Global address** represents the globally routable IP address assigned to a remote corporation.

In short, a **Local Address** is any IP address that appears on the inside portion of a network and a **Global Address** is any address appearing on the outside portion of the network.

## NAT versus PAT

Network Address Translation (NAT) is the first-generation translation method and employs a purely Layer 3 solution.

With NAT, the Inside **Local** address is translated to an Inside **Global** address to be fully routable on the global Internet. When the responding packet returns from the remote host, the firewall device consults the translation table and converts the globally routable IP address back into the private internal address and delivers the packet to the destination host.

Port Address Translation (PAT) is what I've always referred to in a joking manner as NAT v2.0. Instead of doing a simple Layer 3 translation, it uses both Layers 3 and 4, which adds an incredible amount of scalability.

With PAT, the Inside Local address is translated to a single globally-routable IP address that is not part of a global pool, like dynamic NAT. While this address is typically assigned to the outside interface, this does not have to be the case. Additionally, the ASA will assign a port number within the range of 1-65,535 to both the **Inside Local** and **Inside Global** addresses. When the packet is sent out to the Internet and the destination responds, the return packet is checked against the ASA's translation table, and the packet is sent back to the originating Inside Local address.

Given the ever-decreasing size of the IPv4 address space and the fact that most small-to-medium sized companies are issued either a single static IP address or DHCP-assigned IP address from the Internet Service Provider, PAT is considered the modern implementation of network address translation. Using PAT, we don't have to purchase expensive, larger IP subnets to ensure we have enough global addresses to translate our local addresses to. We also don't have to worry about what IP address is assigned to the outside interface if we are using DHCP-assigned addressing. All we have to do is configure the appropriate interface to use and the ASA keeps track of the rest.

# Basic NAT Deployment Scenarios

## 1. Static NAT

For devices on your network that must always be known as the same globally-routable IP address on the outside of your network, the easiest translation method to use is static NAT. With this method, a private Inside Local address is always translated to the same Inside Global address.



In this scenario, we can see that the web server 172.16.1.15 located in the DMZ must be represented by the address 192.168.15.100 to the outside world.

To accommodate this requirement, we will configure the following command.

```
ASA(config)# static (dmz,outside) 192.168.15.100 172.16.1.15 net-  
mask 255.255.255.255
```

In this scenario, this web server is known to the outside world as 192.168.15.100, so this is the address that the packets will be addressed to as they show up at the outside interface. \ Make sure that you're either inspecting http traffic or have an Access Control List (ACL) permitting http traffic to this address applied inbound on the outside interface. After passing the inspection or ACL, the packet will be properly translated to 172.16.1.14 and delivered to the web server.

## 2. Dynamic NAT

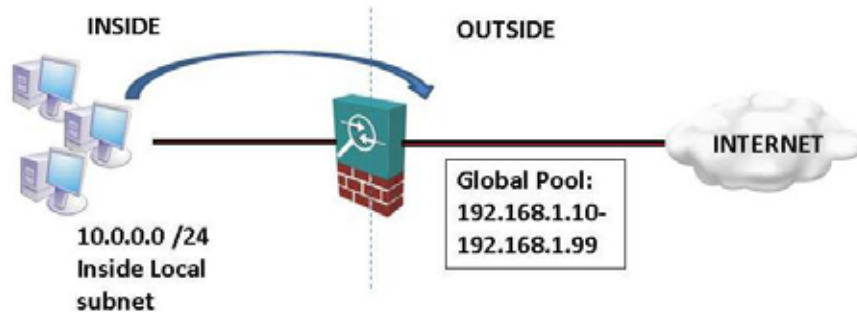
Host devices, such as employee workstations, make up the majority of network nodes. For these, we will use dynamic NAT. This method allows us to build a pool of addresses that the Inside Local addresses will be translated to as they are sent to the outside network. This pool comprises the Inside Global addresses that each flow will select as the first packet is processed. Using dynamic NAT is much more convenient when you have many devices that need translating, since you don't have to build separate static NAT statements for each device.

To configure dynamic NAT, we must complete two steps.

1. Define who will be translated via the **nat** command

2. Define what we will translate these addresses to by creating a global address pool with the **global** command

Consider the following scenario.



**Step 1:** We must first define the Inside subnet that will be translated using the **nat** command:

```
ASA(config)# nat (inside) 1 10.0.0.0 255.255.255.0 tcp 0 0 udp 0
```

**Note:** The parameters `tcp 0 0 udp 0` refer to connection limits we can place on TCP, UDP, and Embryonic connections. While these parameters are part of the **nat** command, they are outside the scope of this whitepaper. For a complete coverage of these parameters and their benefits and requirements, see the Summary section at the end of the paper.

**Step 2:** We then define the pool of globally-routable IP addresses that the Inside network devices will be translated into as the packets pass through the ASA.

```
ASA(config)# global (outside) 1 192.168.1.10-192.168.1.99 netmask  
255.255.255.0
```

**Note:** You may be wondering how the ASA keeps track of which local addresses get translated to which global addresses. The answer lies with the **NAT ID**, which is highlighted in red in the configurations shown above. Translations will occur between the **nat** and **global** statements that have the same NAT ID.

### 3. Identity NAT

What if you have a server in your DMZ that is already configured with a globally-routable IP address and must be known as this exact address outside of your company network? If your ASA is configured to require translations for any packet flowing through the firewall (i.e., NAT-Control), then we can configure Identity NAT.



Given this scenario, the configuration for Identity NAT, which is also known as “NAT 0”, is as follows.

```
ASA(config)# nat (dmz) 0 192.168.15.100 255.255.255.255 tcp 0 0 udp 0
```

In this scenario, our web server is located in the DMZ and is accessed from the outside network via its IP address 192.168.15.100. Notice that the statement begins with **nat (dmz) 0**. The 0 always means that the configured addressing is being translated to itself. The subnet mask of 255.255.255.255 indicates that we are translating this single IP address.

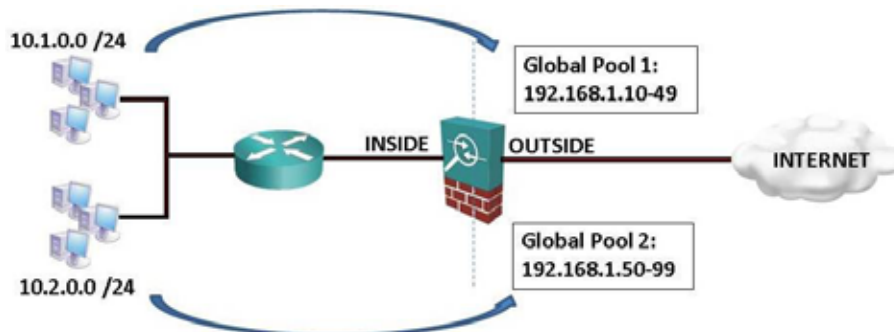
While this may appear that no translation is actually happening, this is known as a transparent mapping and creates a null translation between the DMZ and the Outside networks.

## Advanced NAT Deployment Scenarios

### 1. Dynamic NAT with a single interface for multiple inside subnets

So far, we’ve only looked at scenarios involving a single local subnet. What if you have multiple subnets on the inside of your network, and you want to translate them each to different globally-routable IP addresses? This scenario is easily doable by configuring multiple nat/global combinations with different NAT IDs.

Consider this scenario.



Here, we have two different subnets on the inside of our network that each needs to be translated to different global ranges. To accomplish this, we must create a **nat** and **global** configuration using NAT ID 1 for the **10.1.0.0 /24** subnet and repeat this process using NAT ID 2 for the **10.2.0.0 /24** subnet, as shown below.

```
ASA(config)# nat (inside) 1 10.1.0.0 255.255.255.0 tcp 0 0 udp 0
ASA(config)# global (outside) 1 192.168.1.10-192.168.1.49 net-
mask 255.255.255.0

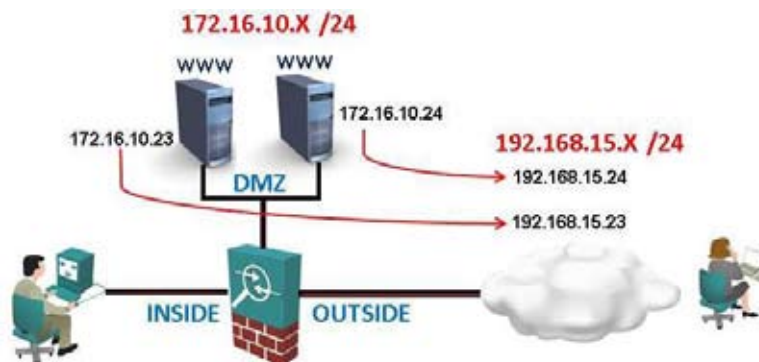
ASA(config)# nat (inside) 2 10.2.0.0 255.255.255.0 tcp 0 0 udp 0
ASA(config)# global (outside) 2 192.168.1.50-192.168.1.99 net-
mask 255.255.255.0
```

## 2. Net Static

What if you have many servers in your DMZ that all must appear as specific globally-routable IP addresses on the outside of your network, but you don't want to deal with either the configuration or administrative overhead of many separate static NAT statements? You're in luck, because we can use a configuration called **Net Static** on the ASA to translate entire subnets at one time.

Net Static works by identifying the configured networking portion of the subnet and then only translating those bits of the IP address. The remaining bits are not translated and, thus, remain the same.

Consider this scenario.



While there are only two servers shown in the DMZ network in this example, this could easily be 200 servers. Therefore, configuring 200 separate static NAT statements is enough to make any administrator want to run and hide. Instead, we'll create a single-line configuration that allows us to translate the entire local subnet to a globally-routable IP subnet on the outside network, leaving the host addressing in the fourth octet the same.

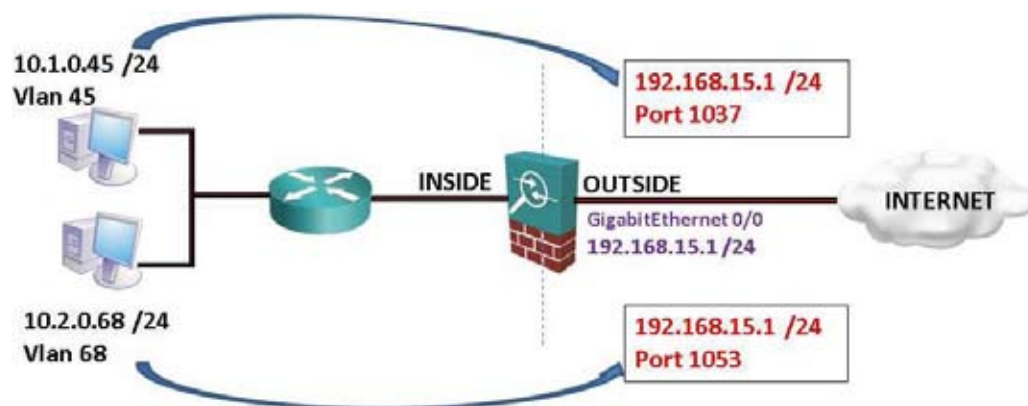
The configuration for this scenario is as follows.

```
ASA(config)# static (dmz,outside) 192.168.15.0 172.16.10.0 netmask  
255.255.255.0 tcp 0 0 udp 0
```

## Basic PAT Deployment Scenarios

As mentioned earlier, what if you have many hundreds of devices in your inside network, but have been assigned either a single static IP address or DHCP-assigned addressing by your Internet Service Provider (ISP) for your **Outside** interface of your Cisco ASA? Using Port Address Translation (PAT), you have the option of configuring your ASA device to use either of these addressing methods.

Consider the following scenario.



### 1. PAT translating to an Outside IP Address

If you have been assigned a static IP address by your ISP, then you can configure this address on your Outside interface and then configure the ASA to translate all inside addresses on this single IP address. By configuring this method, you assume that the IP address will not change automatically. You also assume that any changes to this IP address will require administrative configuration.

Configuring PAT is very similar to configuring dynamic NAT in that we have to specify the following:

1. Who will be translated?
2. To what will we translate them?

**Step 1:** Identify the traffic to be translated with the **nat** command. In this basic scenario, we will translate all inside traffic, so our configuration will be:

```
ASA(config)# nat (inside) 1 0.0.0.0 0.0.0.0 tcp 0 0 udp 0
```

**Step 2:** Configure the IP address that all traffic identified in Step 1 will be translated to, using the **global** command.

```
ASA(config)# global (outside) 1 192.168.15.1 netmask 255.255.255.255
```

### Items To Note

1. The NAT IDs are the same in both of these statements, thus indicating that all traffic will be translated to the single IP address specified in the global command.
2. The **nat** command uses the **0.0.0.0 0.0.0.0** subnet name/subnet mask configuration to indicate that all traffic will be translated.
3. The **global** command uses the netmask **255.255.255.255** configuration to indicate that all traffic will be translated using this single IP address.

## 2. PAT translating to an Outside Interface

What if you've been given a DHCP-assigned address by your ISP? Then configuring the translation with a specified IP address will not be possible, since you won't necessarily know when the address has changed. At the very least, you would never want to manage constantly checking the current IP address and correcting the ASA's configuration to match.

Because of this, we can simply point to the Outside interface in our nat/global configuration instead of configuring the IP address. Using the same scenario as above, our two configurations would look like this:

```
ASA(config)# nat (inside) 1 0.0.0.0 0.0.0.0 tcp 0 0 udp 0
ASA(config)# global (outside) 1 interface
```

### Items To Note

1. The NAT IDs are the same in both of these statements, thus indicating that all traffic will be translated to the interface's IP address specified in the global command.
2. The **nat** command uses the **0.0.0.0 0.0.0.0** subnet name/subnet mask configuration to indicate that all traffic will be translated.
3. The **global** command simply uses the keyword **interface** to indicate that all translations will use the interface's IP address. Which interface is it referencing? It is referencing the interface name between the parentheses, which is the **outside** interface, thus the translations will use the **192.168.15.1** ip address.

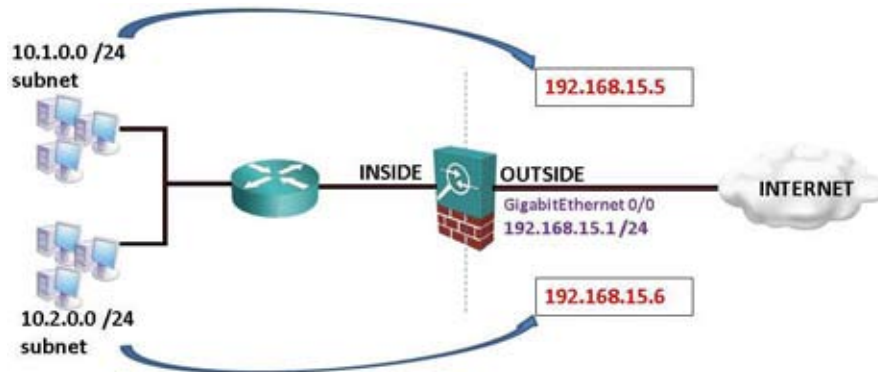
## Advanced PAT Deployment Scenarios

If the basic PAT configuration doesn't offer the level of granularity you need for your given network requirements, then there are also multiple advanced configuration options supported by the Cisco ASA appliance. In this section, we'll explore a few of them.

## 1. Mapping multiple subnets to different PAT addresses

Instead of having a single IP subnet on the inside of your network, you likely have multiple subnets that need to be addressed. This variation allows you to dedicate PAT addresses to each of your inside subnets.

Consider the following scenario.



Here, we can see that we want to translate all traffic coming from the **10.1.0.0 /24** subnet using the **192.168.15.5** IP address. We also want to translate traffic coming from the **10.2.0.0 /24** subnet to the **192.168.15.6** IP address.

To accomplish this requirement, we simply need to remember the rule regarding that NAT IDs will be the same and enter the following commands.

```
ASA(config)# nat (inside) 110.1.0.0 255.255.255.0 tcp 0 0 udp 0
ASA(config)# global (outside) 1192.168.15.5 netmask 255.255.255.255

ASA(config)# nat (inside) 210.2.0.0 255.255.255.0 tcp 0 0 udp 0
ASA(config)# global (outside) 2192.168.15.6 netmask 255.255.255.255
```

This configuration technique would be best suited for companies that have purchased a small subnet from their ISP and want to take advantage of the additional IP addresses. By using this method, the company can realize the following benefits.

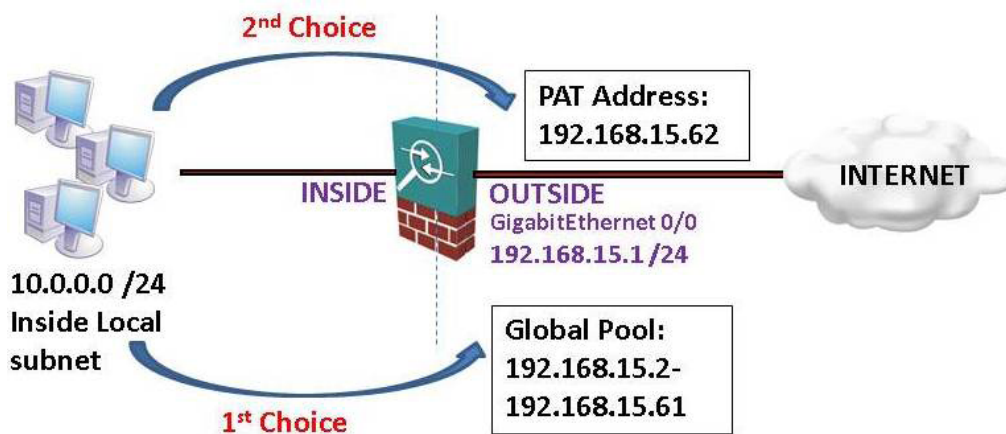
1. The company can organize which local subnets translate to which PAT addresses.
2. Since each PAT IP address has 65,536 possible Layer 4 ports, the company can greatly increase the capacity of potential translations.
3. The company can make the best use of an IP subnet they've already purchased from their ISP.

## 2. Supplementing Dynamic NAT with PAT

What if you've already purchased a sizable subnet from your ISP and want to move to a PAT configuration, but you don't want to lose all of the addresses in this subnet? As an example, you purchased a subnet containing 62 usable addresses back when your company was much smaller and this subnet was large enough to provide all users an available IP address for basic NAT translation. Now, however, your company has grown to over 200 users, and this subnet is no longer sufficient for your needs.

To move to a PAT configuration while also making use of this existing subnet, it is possible to simply back up the existing dynamic NAT configuration with an additional PAT address. Given the above scenario, we have 62 useable IP addresses in the ISP-assigned subnet. From this subnet, we can identify one or more addresses as PAT addresses and then use the remaining IP addresses in our dynamic NAT global pool.

Consider the following diagram for this scenario:



The configuration for this given scenario would look like the following:

```
ASA(config)# nat (inside) 10.0.0.0 0.0.0.0 tcp 0 0 udp 0
ASA(config)# global (outside) 1 192.168.1.1-192.168.1.61 netmask
255.255.255.0
ASA(config)# global (outside) 1 192.168.1.62 netmask
255.255.255.255
```

### Items to Note:

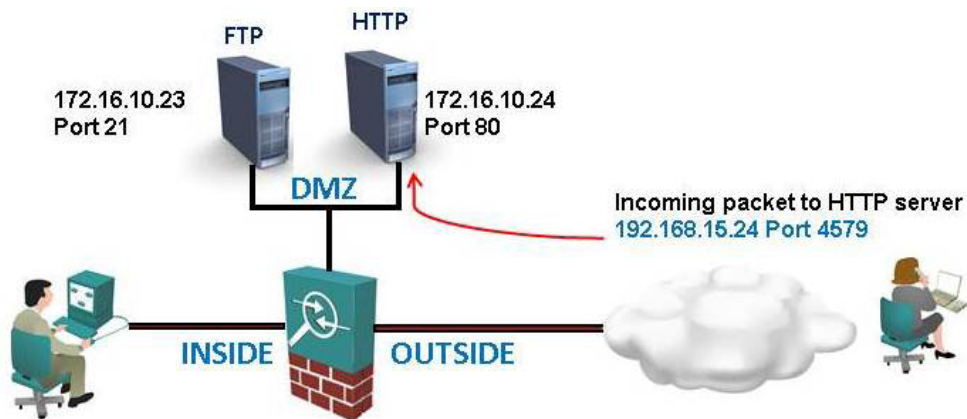
1. The NAT IDs are the same in all three of these statements, thus indicating that all traffic will be translated to the configurations specified in the following global commands.
2. Each of these statements will be read sequentially by the ASA, so all traffic will first be translated to the addresses in the global pool. Once these addresses become exhausted, only then will the firewall use the PAT address configured in the 3rd statement.

- This configuration is easily extendable to backing up the dynamic NAT configuration with multiple PAT addresses by simply configuring additional **global (outside) 1 x.x.x.x 255.255.255.255** commands, where **x.x.x.x** is the new IP address.

### 3. Static PAT (port redirection)

If you maintain devices in your network that must be accessed from users on the outside network, such as Web and FTP servers, you probably have them in your DMZ network. An advanced variation on the basic PAT configuration is to allow the use of custom port numbers and redirect translated packets to different Layer 4 port numbers than were used by users accessing these servers from the outside network. This is a great scenario if you're interested in forcing external users to manually type in non-standard port numbers in their local client browsers or applications (i.e., **http://www.mywebsite.com:4579**).

Consider the following scenario:



In this scenario, an external user is accessing your web server 172.16.10.24 by typing in the following URL in her web browser: "http://www.mywebsite.com:4579 (DNS resolves to the globally-routable 192.168.15.24 IP address).

When this packet arrives at the Outside interface of your Cisco ASA, assuming you have the appropriate ACL allowing this traffic, we want to do two things.

- Translate the destination IP address from the global 192.168.15.24 address to the local 172.16.10.24.
- Redirect incoming packets whose Layer 4 header information indicates port 4579 to HTTP port 80.

The configuration that will satisfy these two requirements is as follows.

```
ASA(config)# static (dmz,outside) 192.168.15.24 4579 172.16.10.24  
80 netmask 255.255.255.255 tcp 0 0 udp 0
```

## Very Useful Commands

When troubleshooting or just verifying proper operation of either NAT or PAT, I have found the following three commands to be the most useful, by far.

**1. show xlate** – The Cisco ASA creates a “translation slot” for every created translation, which is contained in a translation table. This command shows you the contents of this translation table.

Example:

```
ASA# show xlate
3 in use, 3 most used
PAT Global 192.168.34.1(0) Local 10.11.12.45 ICMP id 270
PAT Global 192.168.34.1(1024) Local 10.11.12.45(1037)
PAT Global 192.168.34.1(1024) Local 10.11.12.45(798)
```

**2. show xlate detail** – This show command gives additional detail for each entry in the **show xlate** command.

Example:

```
ASA# show xlate detail
3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.11.12.15/1024 to outside:192.168.34.1/1037 flags ri
UDP PAT from inside:10.11.12.15/1024 to outside:192.168.34.1/798 flags ri
ICMP PAT from inside:10.11.12.15/17341 to outside:192.168.34.1/0 flags ri
```

**3. clear xlate** – Entered in privileged EXEC mode, this command allows you to clear the current translation and connection information contained in the translation table. When troubleshooting why translations are not happening at the moment, although this is definitely less than scientific, I have found that the NAT process sometimes just needs a little “boost” to start working. This command is extremely useful in accomplishing this very quickly and consistently.

In addition to helping you troubleshoot the translation process, the configuration of certain commands will also require that the translation table be cleared so that the translations will be forced to reestablish, using the new configuration. Examples of these commands are:

1. aaa-server
2. Access-list
3. alias
4. global
5. nat
6. route
7. static

## Summary

In this whitepaper, we have discussed what the translation process is, the two main approaches (inside source and outside source), and the two implementation methodologies (NAT and PAT). Additionally, we have discussed both basic and advanced implementation examples and their relevant uses.

While we have seen many great examples, this does not represent all of the potential configuration scenarios for either NAT or PAT. Additionally, this paper has not covered all of the requirements for proper translation to take place. Indeed, there are many moving parts when it comes to configuring the Cisco ASA appliance to process inbound and outbound traffic. Additional considerations would include the configuration of NAT Control, connection limits, access rules, service-policy rules, and many others.

## Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

[SECURE – Securing Networks with Cisco Routers and Switches](#)

[FIREWALL – Deploying Cisco ASA Firewall Solutions](#)

For more information or to register, visit [www.globalknowledge.com](http://www.globalknowledge.com) or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

## About the Author

Jeffrey Hall is an independent consultant and instructor with Global Knowledge. Jeffrey has more than 15 years of experience designing and administering Security, Unified Communications, and Virtualization solutions for

such organizations as the U.S. Army, SBC, AT&T, and Genesis Networks. Additionally, Jeffrey holds the following certifications: VCI, VCP, CCSI, CCNP Security, CCNP Voice, CCIP, CCDP, and CCNP and lives in the Memphis, TN area with his wife Tammy, and two daughters.

## References

1. RFC 1631, "The IP Network Address Translator (NAT)", <http://www.faqs.org/rfcs/rfc1631.html>, May 1994.
2. NAT: Local and Global Definitions, Cisco Systems, [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080094837.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094837.shtml)
3. Module 1 Lesson 5 "Translations and Connections" of the Securing Networks with ASAs Fundamental course, version 1.0.
4. "Cisco Security Appliance Command Reference, Version 8.0", [http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/cmd\\_ref.html](http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/cmd_ref.html)