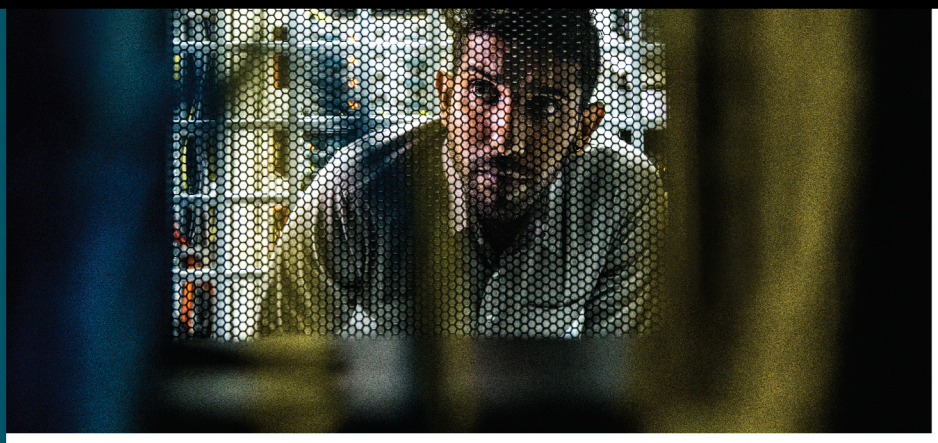

CCIE Professional Development

Integrated Security Technologies and Solutions

Volume I

Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content Security

Aaron Woland, CCIE® No. 20113
Vivek Santuka, CCIE® No. 17621
Mason Harris, CCIE® No. 5916
Jamie Sanbower, CCIE® No. 13637

ciscopress.com

Integrated Security Technologies and Solutions - Volume I

Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content Security

Aaron Woland, CCIE® No. 20113
Vivek Santuka, CCIE® No. 17621
Mason Harris, CCIE® No. 5916
Jamie Sanbower, CCIE® No. 13637

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

Example 4-13 *Debugging EIGRP*

```
asa(config)# debug eigrp ?
exec mode commands/options:
  fsm         EIGRP Dual Finite State Machine events/actions
  neighbors   EIGRP neighbors
  packets     EIGRP packets
  transmit    EIGRP transmission events
```

ASA Clustering Best Practices

Checking the health of a cluster involves understanding what is happening at a cluster level as well as for each individual cluster member. Because the cluster member slaves replicate their configuration from the master, it can be confusing to troubleshoot and maintain individual ASAs. As mentioned earlier in this chapter, best practice is to change the prompt to make it easy to know the name and state of the member to which the console is attached, as follows:

```
prompt cluster-unit state
```

Optionally, if this is a multi-context cluster, add the **context** keyword:

```
prompt cluster-unit context state
```

During the CCIE lab exam, time must be used as efficiently as possible. Using command aliases on the ASA helps you save time and keystrokes. ASA clustering allows for commands to be sent to all cluster members simultaneously via the **cluster exec** command. This is useful when you're saving a configuration or doing other similar tasks that need to be sent to the cluster as a whole. For example, you can use **ce** in order to reference the command **cluster exec**, which saves keystrokes:

```
command-alias exec ce cluster exec
```

It is best practice during the lab exam to set other common commands using **command-alias** in the same fashion.

Traffic with the ASA

All modern firewalls, including the ASA, provide some level of address translation capability. The ASA's features have evolved over time to become more IOS-like in their command structure as the use cases for translation continue to grow.

Network Address Translation (NAT)

In the early days of the Internet there was no need for NAT as there were more IPv4 addresses than there were hosts. But as the Internet grew, so did the need to come up with methods to conserve the address space to accommodate the growth. Like most other

features, ASA NAT evolved to be more granular in order to fit more extreme use cases. Today NAT is more than just a security mechanism. It has become a common tool for fixing overlapping address spaces and connecting dissimilar networks together. NAT is supported in both routed and transparent mode on the ASA, which makes it nearly universal in its application. This section examines different types of NAT and the ways it is configured.

ASA 8.3+ NAT Configuration Changes

Note that the ASA NAT configuration changed significantly in the 8.3 release. Cisco reworked the ASA to make NAT easier to configure and troubleshoot. Candidates familiar with older versions of the ASA need to understand the differences between older and newer versions as they are significant. The biggest change is that IP addresses referenced in ACL configuration (in 8.3 and newer) now use the real IP address, whereas older versions of code referenced the global (translated) IP address. Cisco has detailed documentation on its website highlighting more differences between the old and new configuration methods: https://www.cisco.com/c/en/us/td/docs/security/asa/asa83/upgrading/migrating.html

A CCIE candidate needs to have a strong understanding of the various ways NAT is configured on the ASA. In concept NAT is fairly simple; after all, you are exposed to it every day as you surf the Internet. However, ASA NAT configuration has some nuances that can only be absorbed by thoroughly exploring the vast configuration options offered. This section introduces NAT using the Cisco nomenclature.

NAT Terminology

Cisco uses specific terminology to explain NAT configuration:

- A *real address* is an address prior to translation. Typically this is the inside, or private side, network.
- A *mapped address* is an address that a real address is translated to. Typically this would be the outside or untrusted network.
- *Bidirectional initiation* indicates that NAT applies to both directions: traffic to the host and from the host.
- *Source and destination NAT* compares both source and destination to NAT rules. One or both can be translated or not.

Types of NAT

Cisco has defined specific applications of NAT:

- **Dynamic NAT:** Real addresses are translated to mapped addresses (many-to-many), which is commonly used for Internet access, as an example.
- **Dynamic Port Address Translation (PAT):** Real addresses are translated to a single mapped address (many-to-one). Often in the egress interface address, ports are used to differentiate between real hosts.

- **Static NAT:** This is a static (one-to-one) mapping between a real address and a mapped address. This mapping will always translate bidirectionally and is common for mail servers, web servers, and so on.
- **Identity NAT:** This is a unique application of NAT in which a real address is translated to itself. This is a common way to exempt certain hosts from NAT translation.

Applying NAT

Like many other features on the ASA, NAT has evolved to meet the needs of a variety of uses and deployment scenarios. The vast majority of NAT configurations are covered by network object NAT. This is the easiest way to configure NAT on the ASA because it is defined at the same time as the network object. A network object can be a single IP host, a range, or a whole subnet. These objects can then be referenced in network groups to simplify policy creation on the ASA. Because NAT is configured at the object level, it offers easy differentiation between hosts that require NAT and those that don't.

NAT and IPv6

The ASA has a long history of robust features with IPv6. Accordingly, NAT features have evolved to incorporate IPv6. The ASA can translate between IPv4 and IPv6 (NAT46), IPv6 and IPv4 (NAT64), and IPv6 and IPv6 (NAT66) at the same time. The recommended best practice for NAT46 and NAT66 is to use static NAT due to the large amount of available IPv6 address space. Dynamic PAT is recommended for NAT64 because the IPv4 mapped address space is often more constrained.

Dynamic NAT

Dynamic NAT is the most common and easiest NAT configuration on the ASA. It translates real addresses to mapped addresses where the mapped address pool is typically smaller than the real address pool. Addresses are translated on a first-come, first-served basis from the mapped pool. A NAT translation exists only for the duration of the connection, and there is no guarantee that a given host will receive the same mapped address. Dynamic NAT usage is very common for allowing hosts to communicate on the Internet.

Figure 4-9 illustrates basic dynamic NAT.

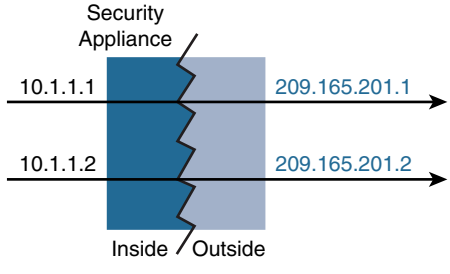

Figure 4-9 *Dynamic NAT*

Dynamic NAT has some limitations. Most obvious is that the mapped pool can run out of addresses if there are more real hosts than mapped addresses. New real host connections would not be allowed. Dynamic PAT, covered in the next section, is often used in conjunction to assist where hosts may overload a dynamic pool.

Another downside to dynamic NAT is that it may consume a larger number of mapped addresses. Some networks may not have the address space to dedicate for this function.

Dynamic PAT

Dynamic PAT is similar to dynamic NAT except that only a single mapped address is used for translation. This allows multiple real hosts to communicate with translation while minimizing the number of mapped addresses that are in use. It also serves as a method to protect the network from exhausting mapped address space when used in conjunction with dynamic NAT.

Real hosts are tracked via port numbers. If possible, the actual source port number is used; otherwise, a unique port number is assigned to a connection (see Figure 4-10).

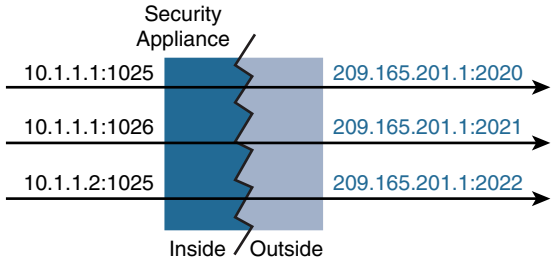

Figure 4-10 *Dynamic PAT (NAT Overload)*

Like dynamic NAT, dynamic PAT has some drawbacks:

- Some multimedia applications and protocols don't work with PAT if their control plane is different than the data plane.
- When dynamic PAT is used, network traffic analytics show a large amount of traffic from a single address. This might affect thresholds for network packet dispersion.

Static NAT

Static NAT is used when continuous bidirectional address mapping is required for a host. Unlike dynamic NAT, which pools mapped addresses, static NAT creates a one-to-one

relationship for the host. Static NAT is commonly used when specific hosts need to be reachable from outside the network.

Static NAT operation is outlined in Figure 4-11. Note the directions of the arrows.

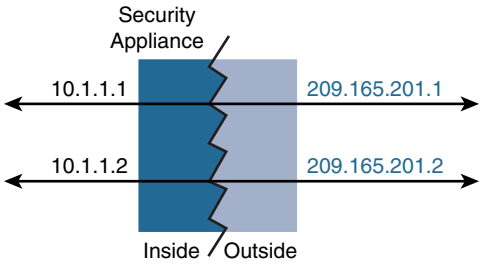

Figure 4-11 *Static NAT*

Static NAT can also statically map ports as well as addresses. This provides more flexibility when a variety of network services are offered (see Figure 4-12).

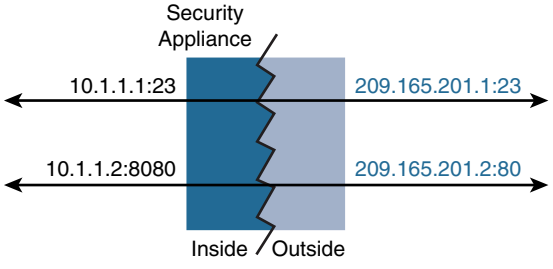

Figure 4-12 *Static NAT with Port Mapping*

It is also possible to use static NAT for a one-to-many mapping where a single real address maps to multiple mapped addresses. This is common in deployments where a load balancer is managing connectivity to a server farm. The load balancer is the single real IP address that is known by multiple mapped addresses. In this case, only the first mapped address is used for outbound traffic, but the additional mapped addresses are used for inbound traffic (see Figure 4-13).

Identity NAT

Identity NAT is a specialized mapping option in which a host maps an address to itself. It is typically used to exclude a specific host from translation when a large range of hosts are part of a NAT rule. It is also required for remote access VPN when host client traffic needs to be exempt from NAT. Identity NAT is shown in Figure 4-14.

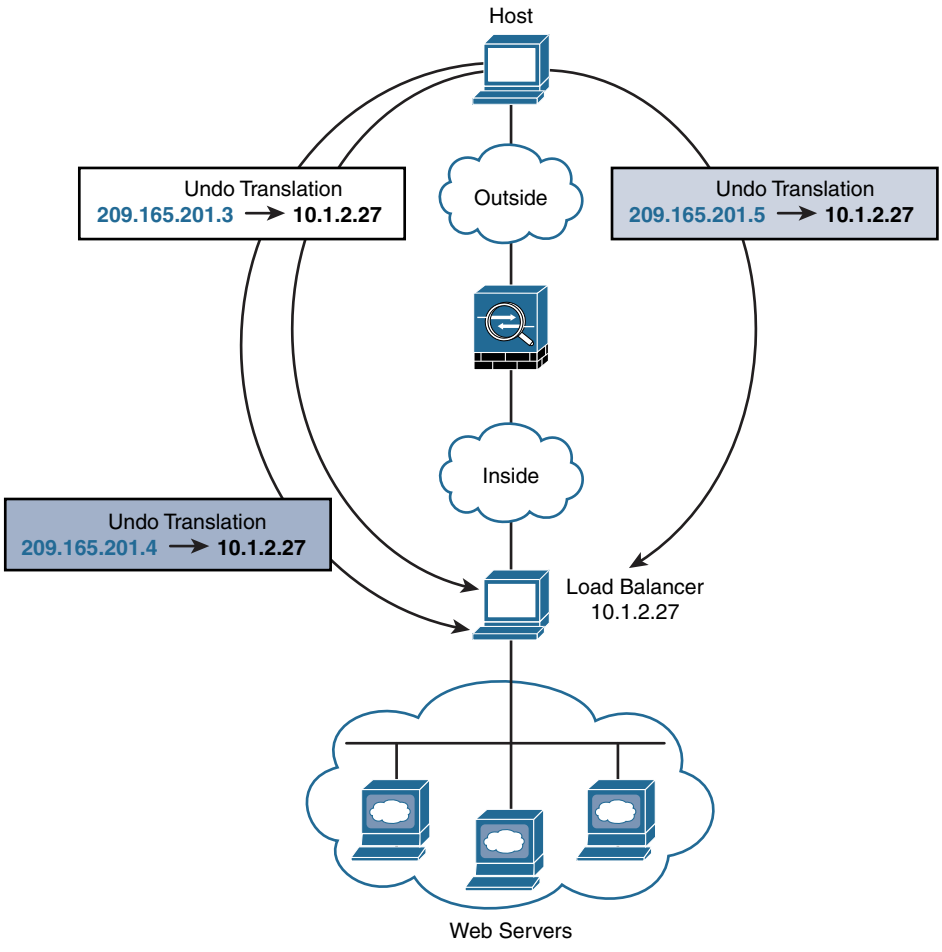

Figure 4-13 *Static NAT Mapped to Different Addresses*

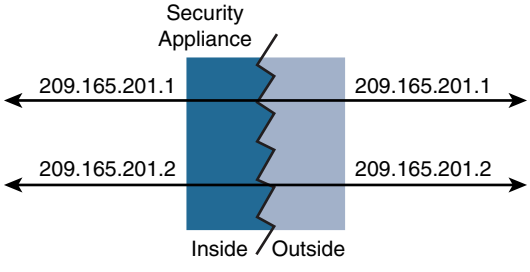

Figure 4-14 *Identity NAT*