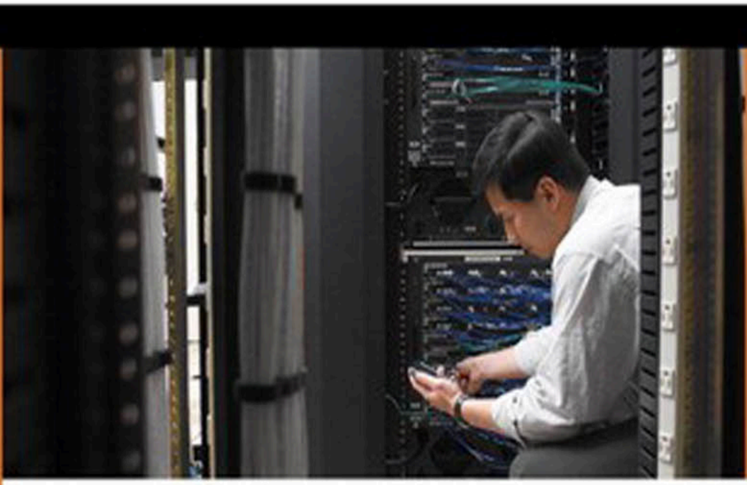
CISCO



SECURITY

Cisco® ASA

All-in-One Next-Generation Firewall, IPS, and VPN Services

Third Edition

Jazib Frahim, CCIE® No. 5459
Omar Santos, CISSP No. 463598
Andrew Ossipov, CCIE® No. 18483

ciscopress.com

Cisco ASA

All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition

Jazib Frahim, CCIE No. 5459

Omar Santos

Andrew Ossipov, CCIE No. 18483

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

This page intentionally left blank

Chapter 10

Network Address Translation

This chapter covers the following topics:

- Address translation types
- Address translation methods
- Security protection mechanisms within address translation
- Understanding address translation behavior
- Configuring address translation
- DNS doctoring
- Monitoring address translations

Cisco ASA acts as a network firewall and can help protect one or more networks from intruders and attackers. Chapter 8, "Controlling Network Access: The Traditional Way," and Chapter 9, "Implementing Next-Generation Firewall Services with ASA CX," discussed the use of access control lists and other identity-based enforcement features to protect an infrastructure. The other core security feature of a firewall is its capability to mask the network address on the trusted side from the untrusted networks. This technique, commonly referred to as *address translation*, allows an organization to hide the internal addressing scheme from the outside by displaying a different IP address space. Address translation is useful in the following network deployments:

- You use a private addressing scheme internally and want to assign global routable addresses to those hosts.
- You change to a service provider that requires you to modify your addressing scheme. Rather than redesigning the entire IP infrastructure, you implement translation on the border appliance.
- For security reasons, you do not want to advertise the internal addressing scheme to the outside hosts.

- You have multiple internal networks that require Internet connectivity through the security appliance, but only one global address (or a few) is available for translation.
- You have overlapping networks in your organization and you want to provide connectivity between the two without modifying the existing addressing scheme.

Types of Address Translation

Cisco ASA supports two types of address translation, namely *Network Address Translation* (NAT) and *Port Address Translation* (PAT).

Network Address Translation

Network Address Translation (NAT) defines a one-to-one address mapping when a packet passes through the security appliance and matches criteria for translation. The security appliance either assigns a static IP address (static NAT) or allocates an address from a pool of addresses (dynamic NAT).

Cisco ASA can translate an internal address to a global address when packets are destined for the public network. With this method, also known as *inside NAT*, the security appliance converts the global address of the return traffic to the original internal address. Inside NAT is used when traffic originates from a higher security–level interface, such as the inside interface, and is destined for a lower security–level interface, such as the outside interface. In Figure 10-1, a host on the internal network, 192.168.10.10, sends traffic to a host on the outside network, 209.165.201.1. The Cisco ASA converts the source IP address to 209.165.200.226 while keeping the destination IP address intact. When the web server responds to the global IP address, 209.165.200.226, the security appliance reverts the global IP address to the original internal IP address of 192.168.10.10.

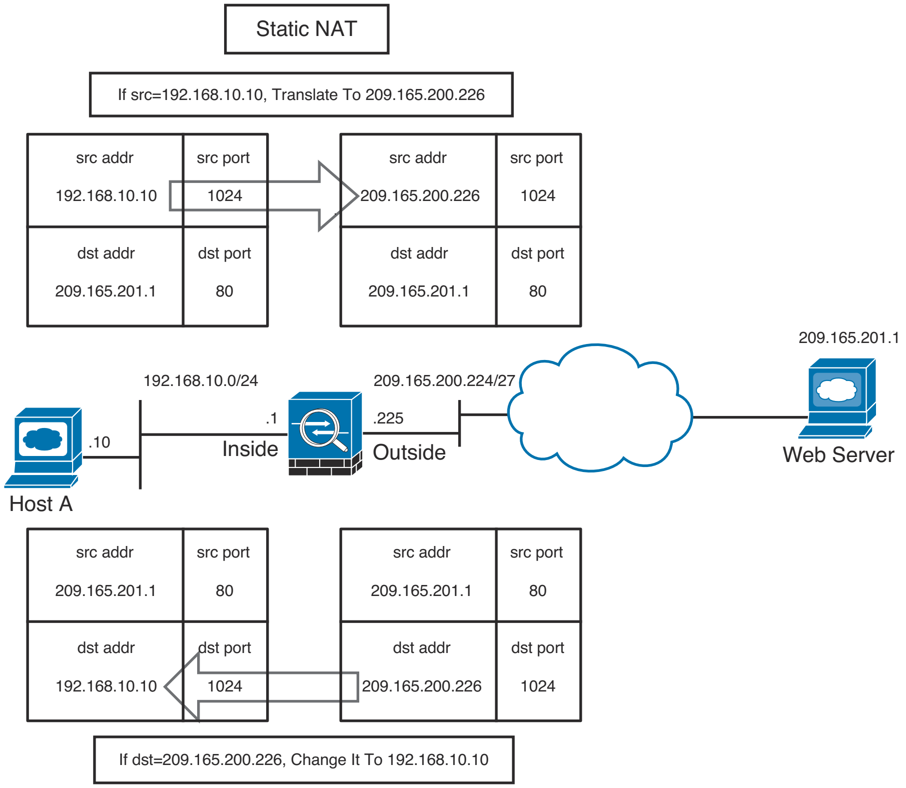


Figure 10-1 *Inside Network Address Translation*

Optionally, the hosts on the lower security–level interface can be translated when traffic is destined for a host on the higher security–level interface. This method, known as *outside NAT*, is useful when you want a host on the outside network to appear as one of the internal IP addresses. In Figure 10-2, a host on the outside network, 209.165.201.1, sends traffic to a host on the inside network, 192.168.10.10, by using its global IP address as the destination address. Cisco ASA converts the source IP address to 192.168.10.100 while changing the destination IP address to 192.168.10.10. Because both the source and destination IP addresses are changing, this is also known as *bidirectional NAT.*

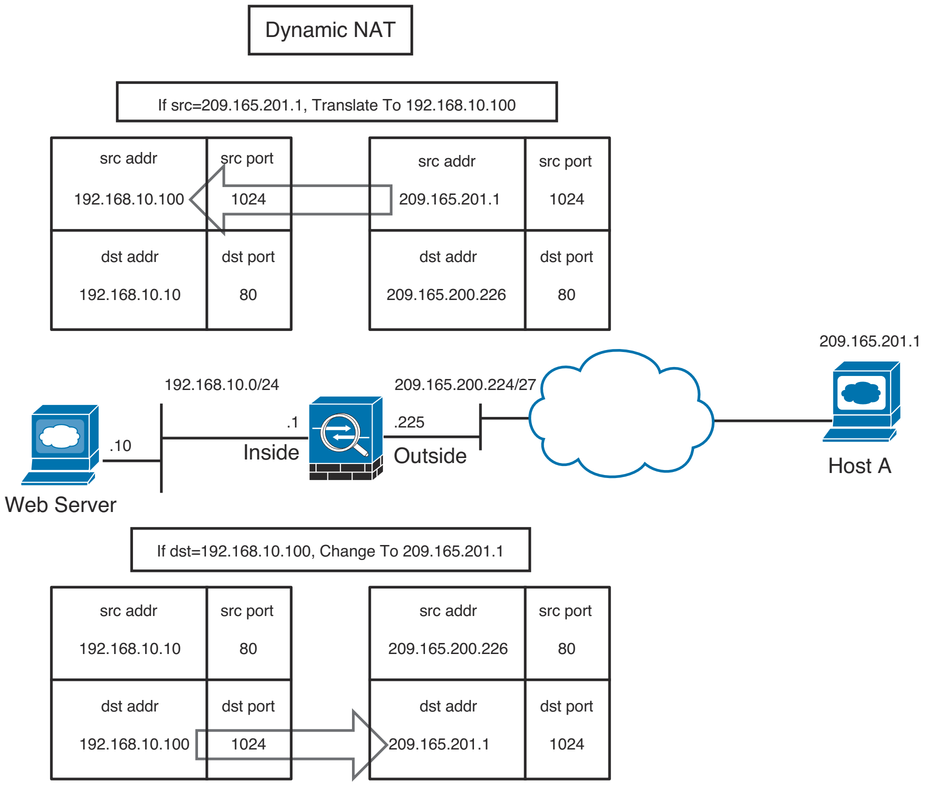


Figure 10-2 *Outside Network Address Translation*

Note If the packets are denied by the interface ACLs, the security appliance does not build the corresponding address translation table entry.

Port Address Translation

Port Address Translation (PAT) defines a many-to-one address mapping when a packet passes through the security appliance and matches criteria for translation. The security appliance creates the translation table by looking at the Layer 4 information in the header to distinguish between the inside hosts using the same global IP address.

Figure 10-3 illustrates an appliance set up for PAT for the inside network of 192.168.10.0/24. However, only one global address is available for translation. If two inside hosts, 192.168.10.10 and 192.168.10.20, require connectivity to an outside host, 209.165.201.1, the security appliance builds the translation table by evaluating the Layer 4 header information. In this case, because both inside hosts have the same source port number, the security appliance assigns a random source port number to keep both entries unique from each other. This way, when the response from the web server returns to the security appliance, the security appliance knows which inside host to forward the packets.

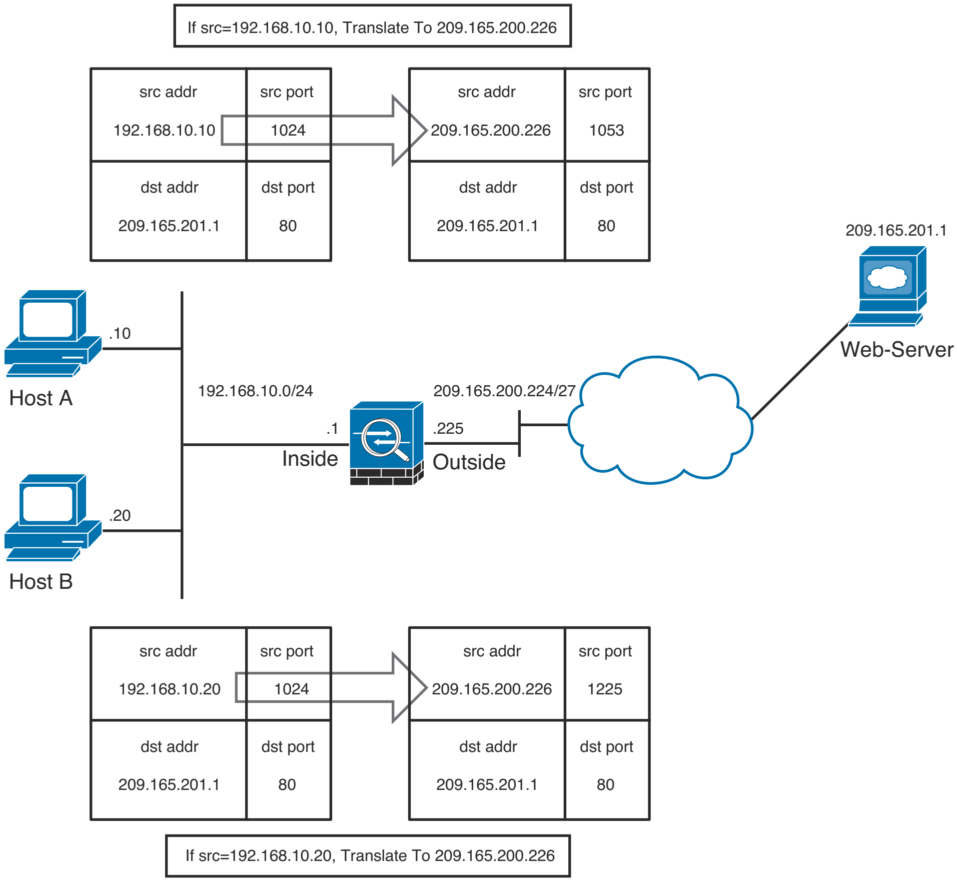


Figure 10-3 *Port Address Translation*

Address Translation Methods

Cisco ASA supports the following four methods to translate an address:

- Static NAT/PAT
- Dynamic NAT/PAT
- Policy NAT/PAT
- Identity NAT

Static NAT/PAT

Static NAT defines a fixed translation of an inside host or subnet address to a global routable address or subnet. The security appliance uses the one-to-one methodology by