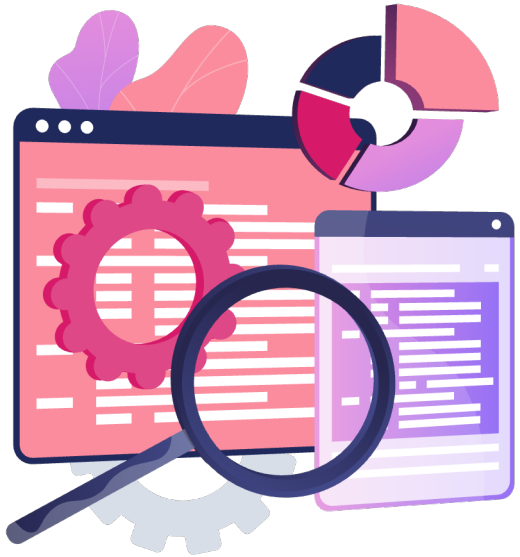
CHAPTER 7

CHECK POINT NAT

YOU DESERVE THE BEST SECURITY

Learning Objectives

- Discuss how NAT (Network Address Translation) affects traffic.
- Describe how to configure manual and automatic NAT.



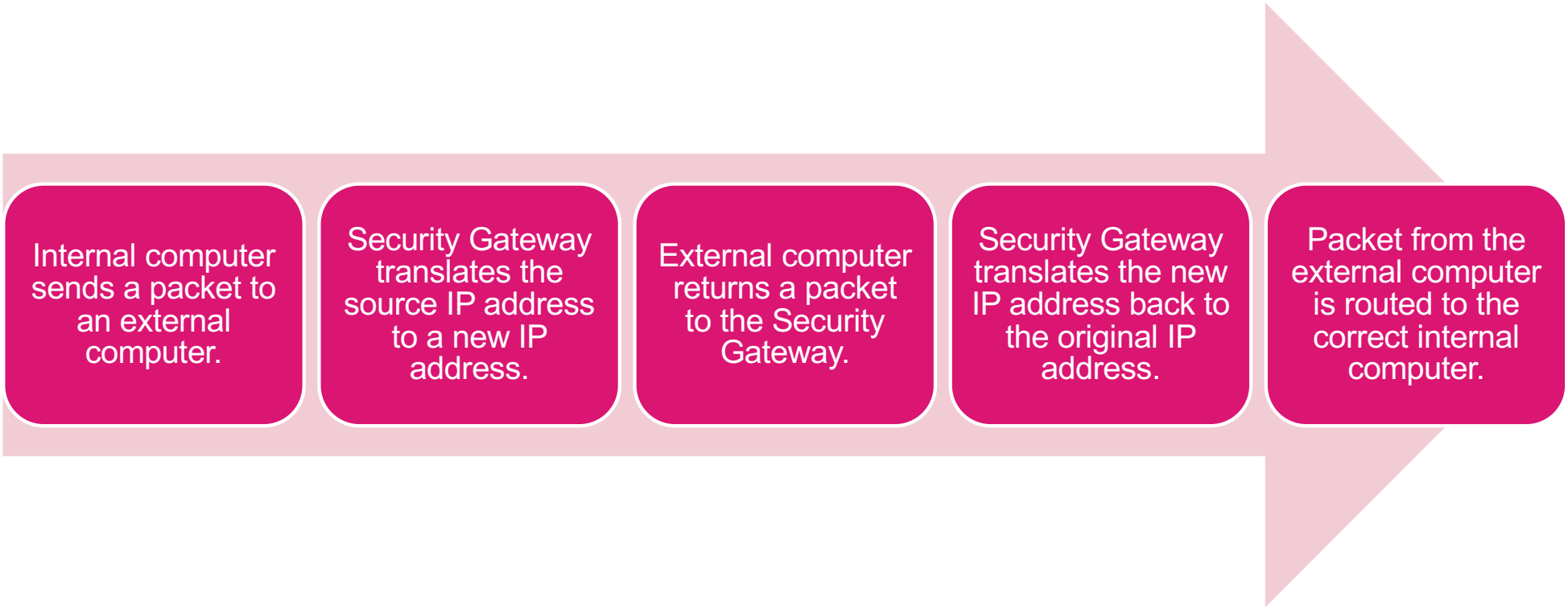
Check Point NAT Overview

NAT is a method of mapping an IP address to another IP address.

From IETF:

A method by which IP addresses are mapped from one realm to another in an attempt to provide transparent routing to hosts.

Example Flow Using NAT



Translation Methods

Static NAT:

- One-to-one relationship between private and public IP addresses.
- Useful for servers or hosts that require a consistent address accessible from the Internet.

Hide NAT:

- Many-to-one translation that hides many source IP addresses behind one or a few IP addresses.
- Useful when fewer IP addresses are available.

For protocols where the port number cannot be changed, Hide NAT cannot be used.

To distinguish between connections, the source port of the connection must be also changed. For this process, port allocation with the Global NAT (GNAT) feature is used.

GNAT is discussed in the CCTE course. For further information, see SecureKnowledge article sk26202 - Changing the kernel global parameters for Check Point Security Gateway.

Check Point NAT Rules

- Two types of NAT rules:
  - Automatic
  - Manual
- Part of the NAT Policy.
- Generally viewed and configured with SmartConsole.

Automatic NAT Rules

Automatic NAT Rules

In most cases, the NAT Policy is automatically populated with the necessary rules.

The Security Gateway creates the rules automatically, based on the defined network object proper.

Manual NAT Rules - Example Uses

- Specified IP addresses (destination and source) or services (ports)
- Static NAT in only one direction
- Translation of source and destination IP addresses in the same packet
- Translation of services (destination ports)
- Translation of IP addresses for dynamic objects

When using manual NAT rules, Proxy ARP is required.

Rule Enforcement

Manual Rule Enforcement:

- First manual NAT rule that matches connection is enforced.

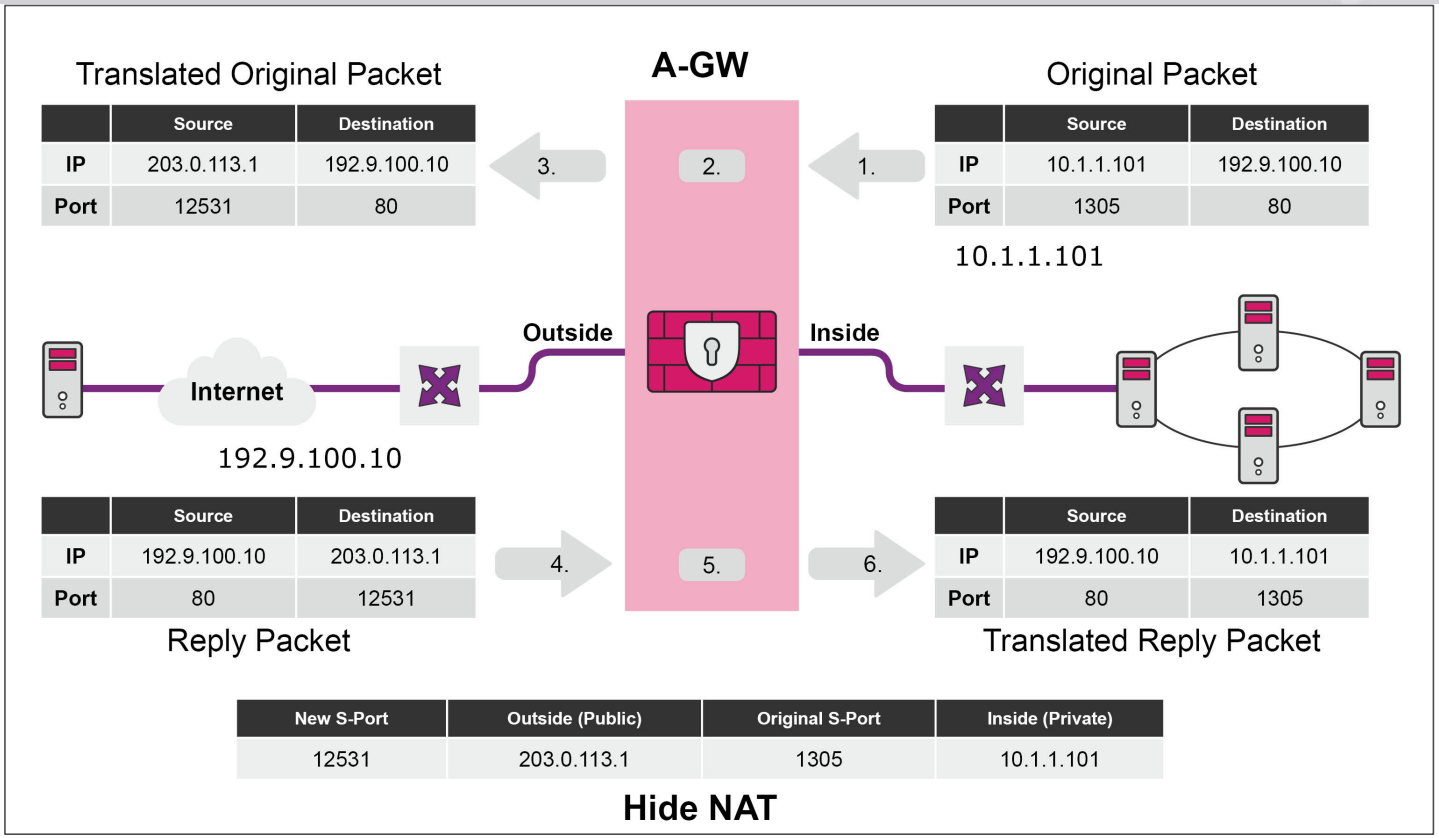
Automatic Rule Enforcement:

- Two automatic NAT rules that match a connection can be enforced:
  - One rule for the source
  - One rule for the destination.

You can enable automatic NAT rules for these SmartConsole objects:

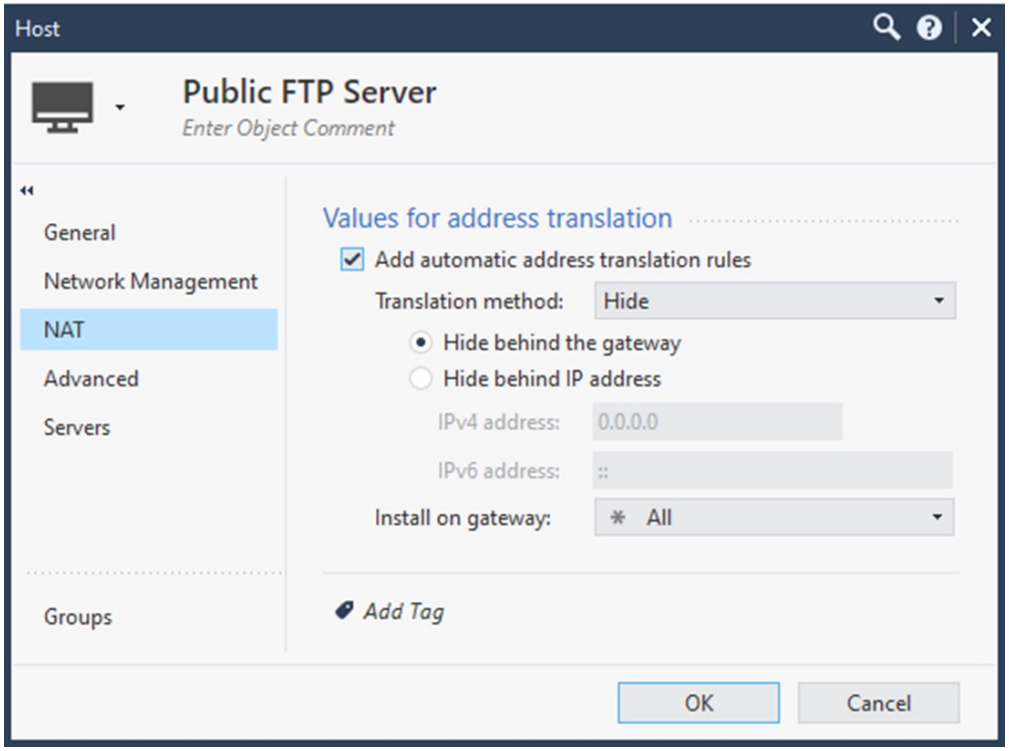
- Security Gateways
- Hosts
- Networks
- Address Ranges

Hide NAT



Translation occurs on the server side.

Hide NAT Configuration

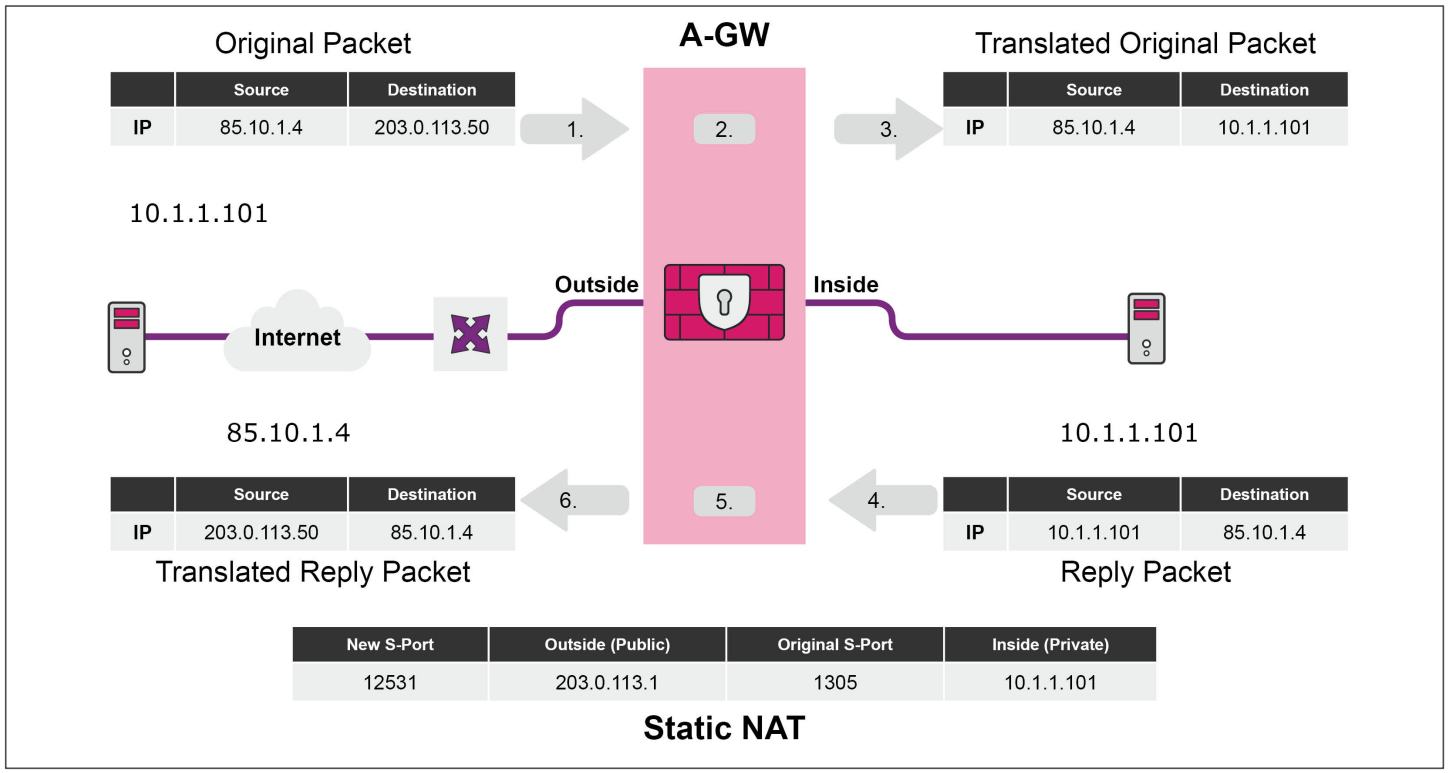


Configured by manually creating rules in the NAT policy or by enabling NAT on the desired network object.

Configuring Hide NAT Rules

- Two rules are created automatically.
  - The first rule prevents the translation of packets traveling from the translated object to itself.
  - The second rule instructs the Security Gateway to translate packets whose source IP address is part of the company's network. This rule translates packets from private addresses to the IP address of the exiting interface of the Security Gateway.
- Modify IP address information associated with traffic packets as they pass through Security Gateway.

Static NAT



Assigned to a server that needs to be accessed directly from outside the Security Gateway.

Configuring Static NAT Rules

- Configuring a Security Gateway to perform Static NAT for a host is like to configuring a Security Gateway to perform Hide NAT using another externally accessible IP address.
- Configuring an object for automatic creation of Static NAT rules adds two rules to the Address Translation policy. Both rules are translating rules.
  - For routing to work properly, Translate to IP Address configuration must be on the same subnet as the Security Gateway's IP address.
  - When Automatic NAT rule creation is used, it makes the necessary adjustments to the ARP configuration.

Proxy ARP for Manual NAT

- Technique by which a proxy server on a given network answers the Address Resolution Protocol (ARP) queries for an IP address that is not on that network.
- The proxy is aware of the location of the destination and offers its own MAC address as the destination.
- Traffic directed to the proxy address is typically routed by the proxy to the intended destination using another interface or tunnel.

https://en.wikipedia.org/wiki/Proxy_ARP

Proxy ARP Configuration

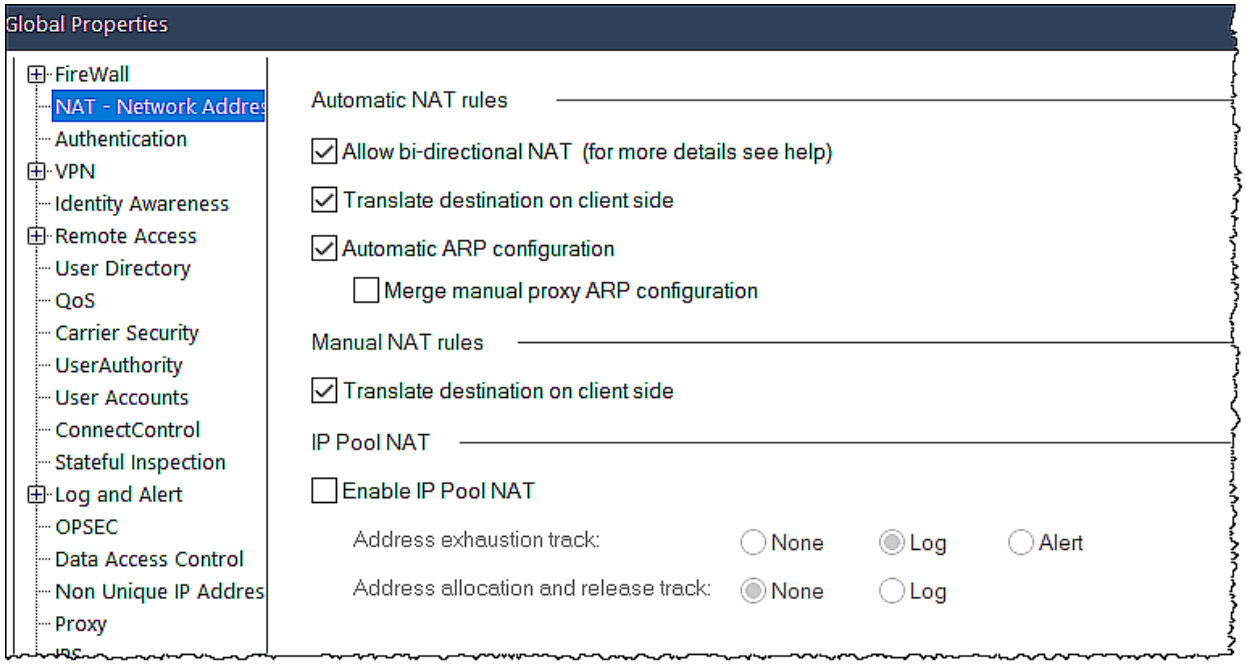
- Two-part process:
  1. Configure Layer 2-to-Layer 3 matching on Security Gateway / each cluster member.
  2. Create relevant Manual NAT rules and install the policy.

Layer 2-to-Layer 3 matching is used to match IP addresses of the relevant hosts on the Internal network (where the hosts are located) to the MAC address of the Security Gateway on the External network (where the IP addresses of these hosts should be published).

Check Point supports the Automatic Creation of Proxy ARP for Manual NAT rules on the Security Gateway. This streamlines the process.

See sk114395 - Automatic creation of Proxy ARP for Manual NAT rules on Security Gateway.

NAT Global Properties



Influence how NAT is handled by a Security Gateway.

Automatic NAT Rules

- Allow Bi-directional NAT:
  - Applies to automatic NAT rules in the NAT Rule Base.
  - Allows two automatic NAT rules to match a connection.
- Translate Destination on Client Side:
  - Applies to packets originating at the client with the server as the destination.

Automatic NAT Rules (Continued)

- Automatic ARP Configuration:
  - Ensures that ARP requests are answered by the Check Point Security Gateway.
- Merge Manual Proxy ARP:
  - Merges the automatic and manual ARP configurations.

Manual NAT Rules

- Firewall rulebase rule that handles connections from the Internet to the object on which NAT is performed - Use the real (untranslated) address for the NATed object.
- Connections that are not sent to a security server - Use the NATed (fake) address for the NATed object.

Review Questions

1. List the two types of rules that Check Point NAT supports for address translation.
2. What is the difference between Hide NAT and Static NAT?

Lab 7A

Configuring Network Address Translation Policy