sunset
LEARNING
INSTITUTE
Authorized Training That Optimizes Your Network...
And Advances Your Career

Network Address Translation (NAT) and Port Address Translation (PAT) on Cisco ASA Software between Version 8.2 and 8.3 and Later

By Tuan Nguyen, a Sunset Learning Institute Cisco Specialized Instructor

Cisco ASA Software Version 8.2 and earlier versions use NAT and PAT configurations that have existed since the Cisco PIX Firewall and can be very complex. With the capabilities that were introduced with the Cisco ASA security appliance, the earlier NAT and PAT configurations became cumbersome and difficult to organize. For example, the newer Cisco ASA security appliances can support up to 1024 virtual interfaces (VLANs) with many security levels, which make the NAT and PAT configurations of Cisco ASA Software Version 8.2 and earlier difficult to manage.

Cisco ASA Software Version 8.3 and later versions use an object-oriented configuration to overcome the earlier configuration constraints. By creating an object for every host, translated address, and service that is used in translations, it is easier to understand how the NAT and PAT configurations are used. With Cisco ASA Software Version 8.3 and later, you can configure translations as network objects that are added to the configuration (auto NAT). You can also configure a complete translation definition using a single CLI command. You are no longer required to link NAT commands into one or more GLOBAL commands. As a result, the NAT and PAT configurations are easier to manage and should result in fewer configuration errors.

Some significant changes have occurred with NAT and PAT in Cisco ASA Software Version 8.3 and later:

- NAT control is no longer an available option. If a connection cannot find a translation, the connection is still allowed, according to all other access policies.

- In Cisco ASA Software Version 8.2 and earlier, when multiple address pools or multiple PAT addresses were defined for a translation, the appliance would hash through the lowest IP address range (or PAT address) until all options for that range (or PAT address) were exhausted before moving to the next range or address. The behavior for NAT and PAT is currently the same as for Cisco ASA Software Version 8.3 and later; all one-to-one dynamic mappings are exhausted first, then the global PAT IPs are completely exhausted before moving to the next PAT IP address.

- There is an “any” option that you can use when defining input and output interfaces in the NAT configuration. The ANY keyword enables you to create a configuration that is used for all interfaces that are configured in a single line, as opposed to a line of configurations for every interface that the translation will use, resulting in a more user-friendly configuration.

- You can configure translations as network objects that are added to the configuration (auto NAT). Using auto NAT simplifies the configuration when only one translation policy is needed for a host.

- A major enhancement to the Cisco ASA Software Version 8.3 configuration is how the security appliance matches translated hosts in other parts of the configuration. Before Cisco ASA Software Version 8.3, the administrator needed to know every translation that a host might have to every possible output interface. The translated IP address needed to be used in various configuration options that were applied to that interface, such as access control list (ACL), Cisco Modular Policy Framework (MPF), Cisco ASA Botnet Traffic Filter, authentication, authorization, and accounting (AAA) cut-through-proxy, and Web Cache Communications Protocol (WCCP) filters. Cisco ASA Software Version 8.3 and later versions match the original (real) address of the host, making it easier to understand, modify, and create the policies that are applied to the interface.