

Tổng Kết Kiến Thức NAT CHO CÁC THÀNH VIÊN CCNA

1. Cấu hình PAT NAT

Trong cấu hình PAT (Port Address Translation), nhiều địa chỉ IP nội bộ (Inside Local) có thể chia sẻ một địa chỉ IP công cộng duy nhất (Inside Global) bằng cách phân biệt qua các cổng nguồn. Đây là dạng NAT phổ biến nhất trong môi trường doanh nghiệp nhỏ hoặc hộ gia đình kết nối Internet qua một địa chỉ IP duy nhất.

Cấu hình bao gồm các bước chính:

- Định nghĩa cổng nội bộ và cổng ngoại vi (ip nat inside và ip nat outside).
- Thiết lập pool địa chỉ IP công cộng nếu không dùng địa chỉ cụ thể.
- Sử dụng lệnh `ip nat inside source list <ACL> interface <outside interface> overload` để bật PAT.

PAT sử dụng "overload" để ánh xạ nhiều IP nội sang một IP ngoại dựa vào số hiệu cổng TCP/UDP.

2. NAT động không dùng PAT

NAT động (Dynamic NAT) ánh xạ các địa chỉ IP nội bộ với một tập hợp các địa chỉ IP công cộng một cách linh động, nhưng không sử dụng "overload" như PAT.

Quy trình:

- Định nghĩa dãy địa chỉ IP công cộng dùng cho NAT bằng `ip nat pool`.
- Dùng ACL để xác định các địa chỉ IP nội bộ cần NAT.
- Dùng lệnh `ip nat inside source list <ACL> pool <pool-name>` để liên kết ACL và pool.

Khác với PAT, NAT động yêu cầu số lượng địa chỉ IP công cộng phải tương ứng với số lượng địa chỉ IP nội bộ đồng thời truy cập ra ngoài.

3. Cấu hình NAT tĩnh

NAT tĩnh (Static NAT) thiết lập ánh xạ một-một giữa một địa chỉ IP nội bộ với một địa chỉ IP công cộng.

Cấu hình gồm các bước:

- Xác định các cổng `ip nat inside` và `ip nat outside`.
- Dùng lệnh `ip nat inside source static <inside-local-ip> <inside-global-ip>` để ánh xạ địa chỉ IP cụ thể.

Static NAT phù hợp với các dịch vụ cần truy cập từ bên ngoài như Web server, Mail server nội bộ. Ưu điểm là luôn ánh xạ cố định nhưng nhược điểm là tốn IP công cộng.

4. NAT và PAT trong mạng

Phân tích cơ chế hoạt động của NAT nói chung và PAT nói riêng khi gói tin đi từ bên trong ra bên ngoài mạng:

- NAT động: Khi một gói tin từ máy nội bộ đi ra ngoài, router kiểm tra xem có trùng điều kiện ACL không. Nếu có, sẽ lấy một IP từ pool và thêm vào bảng NAT để ánh xạ.
- PAT: Nếu sử dụng overload, sẽ ánh xạ cùng một địa chỉ IP công cộng nhưng phân biệt theo số hiệu cổng.

Điểm khác biệt:

- NAT tĩnh: ánh xạ cố định 1-1.
- NAT động: ánh xạ động 1-1 với giới hạn số lượng IP công cộng.
- PAT: ánh xạ nhiều-một bằng cách dùng số hiệu cổng.

PAT thường được dùng nhất vì hiệu quả sử dụng địa chỉ IP công cộng tốt hơn.