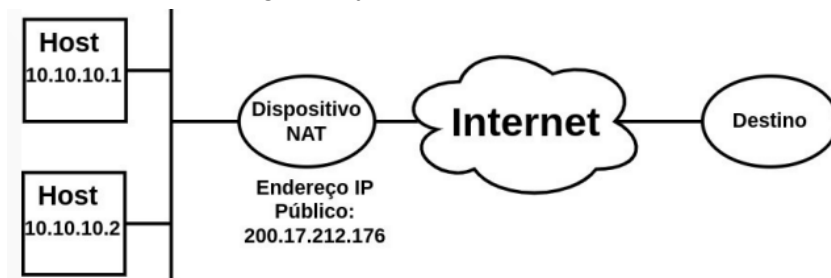


Redes 2

NAT, IPv6 & História

- NAT
 - Camada de Rede
 - Network Address Translation
 - Endereços inválidos/não-roteáveis
 - Muito usados para identificação de hosts internos
 - O NAT surgiu no mesmo contexto de ameaça de exaustão de endereços que ameaçou a Internet nos anos 90
 - Na época, surgiram: IPv6, CIDR e NAT
 - Na verdade, o NAT foi além: solução de segurança
 - Mesmo em uma Internet inteiramente IPv6, o NAT vai continuar sendo usado
 - Espaços de endereçamento
 - Endereços públicos ou válidos
 - Endereços privados ou inválidos: não roteáveis, estão presentes em toda a Internet
 - A IANA definiu 3 faixas de endereços privados: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
 - Os hosts internos de uma rede podem ter assinalados endereços inválidos
 - Para permitir que se comuniquem na Internet, usamos um dispositivo NAT
 - Funciona como um gateway entre a rede interna e a Internet



- TODOS os dispositivos da rede interna usam o mesmo endereço válido do dispositivo NAT
- A comunicação de/para a Internet com NAT
 - NAPT - Network Address PORT Translation
 - Toda comunicação NAT inicia no host interno
 - O Dispositivo NAT quando percebe uma nova comunicação (pelos endereços/porta pares origem/destino), ele cria uma Sessão NAT, identificada por uma porta
 - Portas nesse caso não são usadas para comunicação de processos
 - Todo pacote, antes de sair para a Internet tem
 - Endereço IP válido do NAT
 - Porta que identifica a sessão NAT
 - Todo pacote que chega da Internet, o dispositivo NAT faz a busca na tabela de sessões, substitui endereço IP/porta e retransmite na rede interna
- Campos de uma Sessão NAT
 1. Tipo da Sessão: UDP, TCP ou ICMP (eventualmente outro)
 2. Estado da Conexão TCP
 3. ip_local do host que iniciou a comunicação

4. porta_local do processo interno
 5. ip_destino, porta_destino
 6. porta_NAT utilizada para identificar a sessão NAT e para comunicação externa
 7. ip_externo sendo usado (quando existe mais de um endereço válido)
 8. temporizador: permite identificar sessões silenciosas
- Como toda conexão começa interna para externa = segurança