Guião4 – NATs

Ex1-

Primeiro montamos a rede de acordo com a imagem, associamos os endereços IP aos respetivos PCs e às respetivas interfaces (fi 1/0 e fi 1/1) do router da rede privada e da rede pública.

Depois criamos uma net pool chamada “PISCINA”.

Depois definimos qual a rede privada e qual a pública configurando o router.

F1/0 -> inside -> privada

F1/1 -> outside -> pública

2-

Depois, definimos as gateways necessárias para fazer pings entre PC1, PC2 e PCB. Observamos que quando tentamos fazer ping de PC1->PCB há comunicação, mas se fizermos logo a seguir ping PC2->PCB já é unreachable, i.e., não há comunicação.

A seguir usamos o seguinte comando e verificamos que esta é a tabela de IP NAT translations, que mostra qual o IP da rede pública que corresponde a cada IP que dá NAT a um endereço IP privado. Esta tabela é para ele “se lembrar” de qual foi a troca de IPs feita.

R1#show ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 192.1.1.21:2255 192.168.1.1:2255 192.1.1.45:2255 192.1.1.45:2255

icmp 192.1.1.21:2511 192.168.1.1:2511 192.1.1.45:2511 192.1.1.45:2511

icmp 192.1.1.21:2767 192.168.1.1:2767 192.1.1.45:2767 192.1.1.45:2767

icmp 192.1.1.21:3023 192.168.1.1:3023 192.1.1.45:3023 192.1.1.45:3023

icmp 192.1.1.21:3279 192.168.1.1:3279 192.1.1.45:3279 192.1.1.45:3279

--- 192.1.1.21 192.168.1.1 --- ---

3-

A seguir fizemos clear da tabela, ao dar “show” já não aparece a tabela. Depois fez-se ping PC2->PCB e observamos que na tabela do NAT translations, o PC2 usou o endereço pool público:

Pro Inside global Inside local Outside local Outside global  
--- 192.1.1.21 192.168.1.2 --- ---

4-

Configuramos o tempo que os valores vão ser guardados na tabela anteriormente referida para 60s, a seguir fizemos clear e fizemos um ping e observamos que a rede privada usou o NAT para aceder à rede pública.

Consegue-se dar ping do PC1 para o 192.1.1.40, mas se for feito, imediatamente a seguir, do PC2 não irá funcionar. Se o PC2 for o primeiro a dar ping, irá funcionar no PC2 mas não no PC1.

Não dá para dar ping aos dois PC´S ao mesmo tempo porque apenas têm NAT e um único endereço disponível.

5- Agora queremos que o PC1 e o PC2 possam comunicar (ao mesmo tempo) com PCs da rede pública sem necessidade de fazer mais NAT-Pools, para isto são adicionamos portos à NAT, pois é com os portos que agora se consegue fazer ter uma distinção entre os PCs.

Tivemos de tirar um modo em que a NAT se encontrava fazendo “no ip nat inside source list 2 pool PISCINA”, fizemos o comando e assim ficou overload, i.e., assim verificamos a comunicação entre PC1 e PC2 ao mesmo tempo e PCB.

6- Declaramos os portos para PC1 e PC2 através de conexões UDP e TCP para com um PC que se encontra na rede pública, com o uso de comandos como “ping 192.1.1.40 -3 -p 22” no PC1/PC2, onde é definido o tipo de conexão (2->UDP; 3-> TCP) e no final o número de porto que se deseja utilizar. Com a uso destes portos se podem comunicar PCs da rede pública com a privada mesmo só havendo uma pool na NAT.

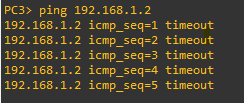
UDP- mais rápido/menos seguro.

Serve para partilhar vídeos/áudios com um grande número de utilizadores.

TCP- menos rápido/mais seguro por haver handshake.

Serve para haver uma comunicação confiável entre utilizadores e servidores.

7- Tentou-se dar ping do PCA para PC1 sem sucesso, pois um PC duma rede pública não tem forma de aceder a uma rede privada.



8- Recorreu-se à criação de um novo endereço IP (192.1.1.201) para o PCA conseguir comunicar com o PC1. Para isto criou-se uma ligação direta no Router (uma espécie de tradução de IPs) que define que se um PC da rede pública quiser aceder à rede privada, então usará o IP 192.1.1.201.

Observou-se no Wireshark que os pacotes foram do PCA para o Router e o IP que deu reply no Router foi o 192.1.1.201, depois esta comunicação continuou do Router até o PC1 e verificou-se que os PCs conseguiram comunicar.

9- Usaram-se os comandos para criar um servidor DHCP privado no router que permite atribuir IPs no intervalo de 192.168.1.99 a 192.168.1.200 de forma dinâmica.

DDORA -> Discover Offer Request

Acknoledge -> É o servidor a dizer OK

10-