Ficha 02 – Introdução ao NAT

Ano Letivo de 2023/2024

1 – Introdução

Nesta ficha iremos introduzir a utilização de NAT, a qual se tornou particularmente importante desde que o crescimento da Internet levou a que existisse escassez de endereçamento IPv4. Para isso, iremos utilizar o GNS3 na máquina virtual fornecida na disciplina. Os princípios básicos da configuração de NAT e o cenário de rede a utilizar são descritos nos pontos abaixo.

Avaliação da Ficha

- Esta Ficha vale **1 valor** (em 20).
- As respostas à ficha devem ser submetidas no Moodle até 25/fev.

2 – Funcionamento do SNAT (Source NAT) e DNAT (Destination NAT)

O NAT (*Network Address Translation*) permite mapear endereços IP nas comunicações entre diferentes redes, através da alteração do endereço de origem ou destino no cabeçalho dos pacotes IP, durante a sua passagem por um *router*. Na realidade, o NAT implementa várias técnicas, algumas das quais com designação que varia de fabricante para fabricante. Uma das técnicas mais úteis é a do SNAT (ou Source NAT), utilizado na prática nas comunicações entre redes com endereços IP privados e a Internet, onde forçosamente se usam endereços IP públicos. O funcionamento do SNAT é ilustrado na Figura 1.

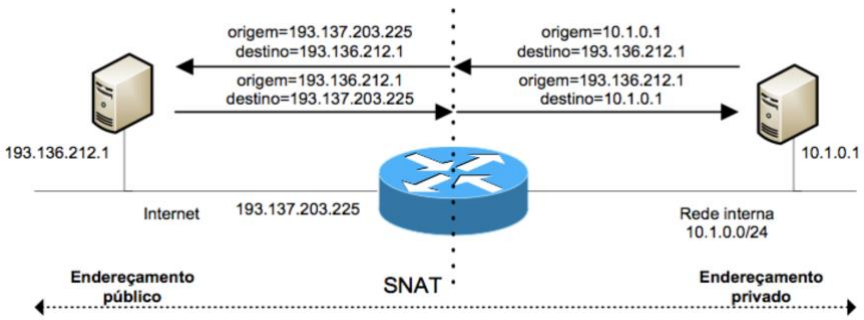

Figura 1 – Exemplo de funcionamento do NAT (SNAT)

Como é possível ver na Figura 1, neste cenário o NAT utiliza o endereço externo do *router* (neste exemplo o endereço 193.137.203.225) como endereço de origem para as comunicações com origem na rede interna (a rede 10.1.0.0/24). Para este efeito, o NAT recorre a portos diferentes para distinguir as várias comunicações sujeitas a NAT, para as quais armazena a correspondência entre portos internos e externos numa tabela de translação de endereços.

Por sua vez, o DNAT (Destination NAT) permite a translação do endereço de destino dos pacotes IP. O funcionamento do DNAT encontra-se ilustrado na Figura 2, sendo que no exemplo as comunicações com origem no exterior e destinadas ao endereço de destino 193.137.203.225 (o endereço IP da interface de ligação do router ao exterior) é alterado para o endereço 10.1.0.1, para que a ligação seja efetivamente redirecionada para a máquina da rede interna.

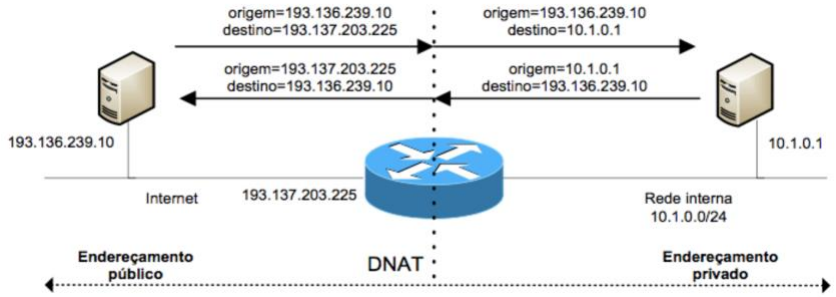

Figura 2 - Funcionamento do DNAT (DNAT)

Como é visível no exemplo, o DNAT permite, desta forma, expor ao exterior serviços que estejam disponíveis em servidores na rede interna (com endereçamento privado), com recurso ao endereço externo do router. A seguir descrevem-se os fundamentos em relação à configuração dos mecanismos de DNAT e SNAT em routers Cisco.

Configuração de SNAT nos *routers* Cisco

Tal como seria de esperar, os routers Cisco suportam a configuração do NAT nos seus vários modos de utilização, entre os quais o SNAT e DNAT (descritos anteriormente). O exemplo seguinte ilustra a configuração do SNAT para translação de endereços da rede 10.5.0.0/24 (endereços privados) para a rede externa (gama de endereços oficiais 193.137.203.0/24), recorrendo para o efeito ao endereço 193.137.203.1, o endereço da interface externa utilizado no modo "overload". O modo "overload" significa que o NAT recorre a diferentes portas para diferenciar as várias ligações.

```
router# config terminal
router(config)# access-list 30 permit 10.5.0.0 0.0.0.255
router(config)# ip nat inside source list 30 interface Ethernet0 overload
router(config)# interface FastEthernet0
router(config-if)# ip address 10.5.0.1 255.255.255.0
router(config-if)# ip nat inside
router(config-if)# exit
router(config)# interface Ethernet0
router(config-if)# ip address 193.137.203.1 255.255.255.0
router(config-if)# ip nat outside
router(config-if)# end
```

Conforme o exemplo anterior ilustra, as interfaces nas quais o NAT opera são declaradas como "inside" e "outside". A primeira é a interface de ligação à rede interna, na qual é utilizada a gama de endereços privados, sendo a externa a interface "outside". O comando "access-list" permite definir a gama de endereços aos quais a operação de NAT irá aplicar-se, no exemplo a toda a rede 10.5.0.0/24 (de notar a utilização de "0.0.0.255", para identificar a totalidade da gama desta rede).

Configuração de DNAT nos *routers* Cisco

Os routers Cisco suportam igualmente a configuração de NAT no modo DNAT, descrito anteriormente. Neste modo, é necessário identificar as comunicações a sujeitar a DNAT (para as quais o endereço de destino deve ser alterado), para que sejam redirecionadas para o servidor da rede interna. Uma das formas de configurar DNAT nos routers Cisco consiste no redireccionamento de portos específicos, para ligações efetuadas ao IP da interface do router que liga às redes exteriores. Considere o seguinte exemplo, que ilustra esta forma de configuração.

```
router# config terminal
router(config)# ip nat inside source static tcp 10.5.0.200 80 193.137.203.1 80
router(config)# interface FastEthernet0
router(config-if)# ip address 10.5.0.1 255.255.255.0
router(config-if)# ip nat inside
router(config-if)# exit
router(config)# interface Ethernet0
router(config-if)# ip address 193.137.203.1 255.255.255.0
router(config-if)# ip nat outside
router(config-if)# end
```

No exemplo anterior, utiliza-se DNAT para redirecionar ligações efetuadas ao porto 80 do endereço 193.137.203.1 (da interface externa ou 'outside' do router) para o mesmo IP na máquina 10.5.0.200 da rede interna.

3 – Cenário de Rede a configurar no GNS3

Considere o cenário seguinte, que ilustra 3 redes interligadas através de vários *routers*. O endereçamento de cada uma das redes é apresentado na figura.

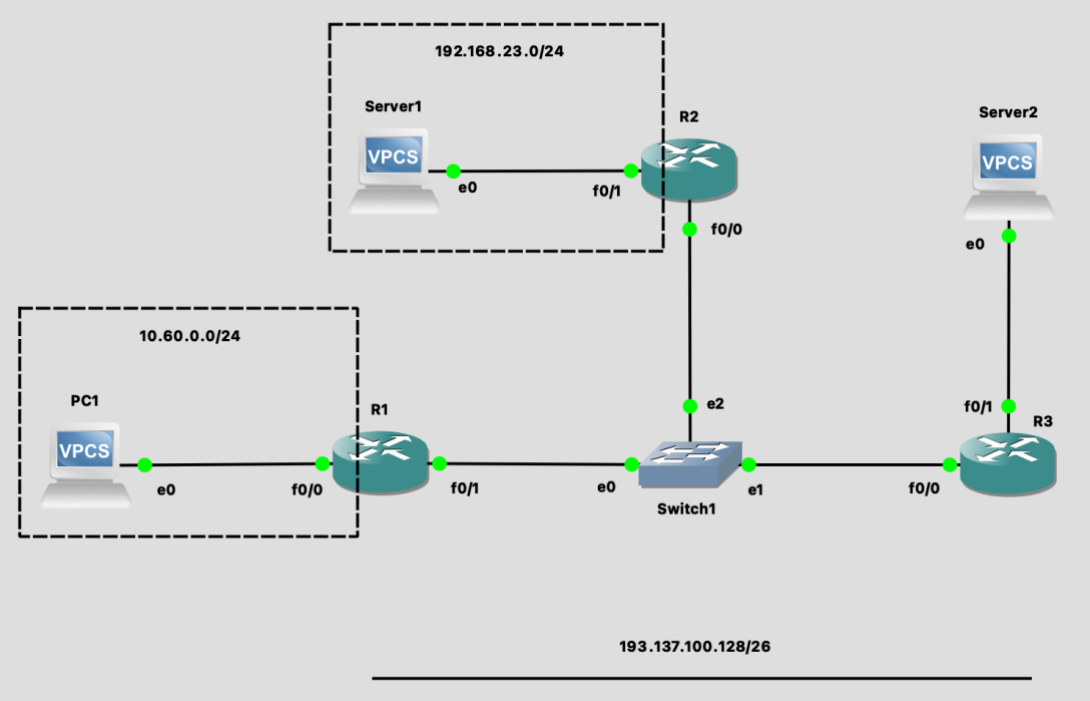

Figura 3 - Cenário de Rede

O objetivo da ficha é garantir conectividade total do PC e dos servidores indicados, a qual deve ser conseguida seguindo as seguintes indicações:

a) Em primeiro lugar, deve considerar as redes existentes e dividir a sub-rede 193.137.100.128/26 em duas sub-redes de igual tamanho. A primeira será utilizada para interligar os routers, a segunda para a rede do Server 2.

b) Os equipamentos devem ter um endereço IP na rede em que se encontram. Por convenção, utilize o primeiro endereço da rede para computadores e o último para routers.

c) Adicione todas as rotas de encaminhamento que considere necessárias, sempre tendo em conta que não existe encaminhamento direto entre redes de domínio privado (192.168.23.0/24 e 10.60.0.0/24) e redes de domínio público (as duas sub-redes com base na 193.137.100.128/26).

d) Tendo em conta a limitação no encaminhamento da alínea anterior, configure as regras de SNAT e DNAT que considere necessárias. Considere que os servidores (Server 1 e Server 2) estão à escuta de ligações de clientes no porto TCP 443.

4 – Simulação no GNS3

Para simular o cenário proposto no GNS3, terá de criar e configurar todos os equipamentos e interligações necessárias, de acordo com o que foi pedido na secção anterior e com as notas seguintes:

- Crie e configure todos os equipamentos ativos de rede.
- Crie as ligações de rede entre os equipamentos tal como estão indicadas na Fig.3. Respeite as ligações entre as portas tal como estão indicadas.
- Todos os *routers* devem usar a imagem de um *router* Cisco2691 (imagem fornecida).
- Use apenas encaminhamento (rotas) estático para configurar as rotas nos *routers*.
- Use apenas endereços IP estáticos.

5 – Validação

De forma a validar o cenário construído, poderá estabelecer comunicações TCP a partir de um VPC com o comando:

ping <*ip_address*> -P 6 – p 443

No qual **<*ip_address*>** deve ser substituído pelo IP de destino, ***-P*** indica o protocolo TCP e ***-p*** o porto ao qual nos pretendemos ligar. Os VPCs já se encontram à escuta de um conjunto de portos, e irão aceitar a ligação no porto 443. A Fig.4 ilustra uma ligação TCP bem-sucedida a partir do VPC, recorrendo ao comando "ping".

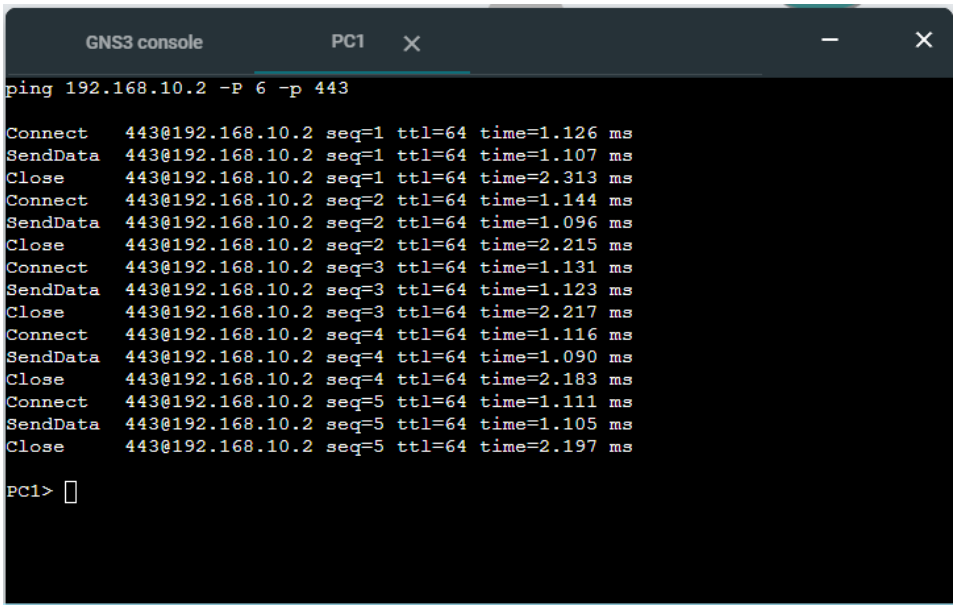

Figura 4 – Exemplo de comunicação TCP com um VPC

Deverá ainda recorrer ao Wireshark para visualizar o tráfego realizado, e aí deverá visualizar que tanto os endereços IP de destino (DNAT) como de origem (SNAT) são substituídos por outros endereços IP que serão reconhecidos nas respetivas redes de destino. Para isso, visualize o tráfego em pontos separados do cenário de rede: antes de ser aplicado o NAT, e depois de ser aplicado o NAT.