Lab – Balanceamento de carga de aplicações TCP com NAT

Tópicos

1. Compreender o funcionamento do NAT
2. Analisar e identificar estabelecimento de ligações via NAT
3. Implementar o NAT com redundância de ligações a servidores aplicacionais
4. Efetuar troubleshooting das configurações efetuadas.

1. Cenário prático

A Figura 1 ilustra uma rede onde se pretende distribuir a carga das ligações TCP provenientes da rede 192.168.1.0/24 aos servidores 10.1.1.10 e 10.1.1.11, ambos com a máscara de rede 255.255.255.0. O balanceamento de carga será efectuado através do endereço virtual 10.1.1.100/24.

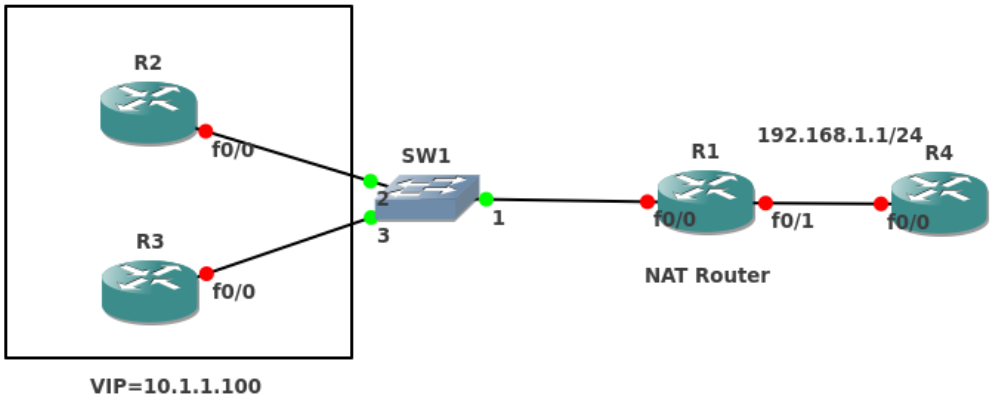

Figura 1 –Cenário prático de NAT com balanceamento de carga entre os servidores.

2. Atividades

1. Implemente no GNS3 o cenário apresentado na figura, contemplando o endereçamento proposto.
2. Configure o NAT com *TCP Load distribuition* por forma a assegurar que as ligações Telnet (e apenas estas) são balanceadas pelo router de NAT, através do endereço virtual 10.1.1.100.

3. Efetue teste de comunicação e valide os resultados. Para o efeito, proceda a várias ligações de telnet a partir da rede 192.168.1.1 e confirme que são distribuídas pelos dois servidores de telnet.
4. Efectue as alterações necessárias para assegurar o balanceamento de carga das ligações HTTP ao servidor Web em execução dos routers.

Relembram-se os passos gerais que deverão ser executados para a configuração de NAT num router:

1. Configurar a *pool* de endereços de NAT a serem usados em modo rotativo (*rotary*).
2. Definir o tipo *inside* e *outside* a cada uma das interfaces, conforme assegurem a entrada ou a saída de pacotes entre as redes envolvidas no NAT.
3. Definir ACL para assegurar que as ligações telnet para o endereço virtual são mapeadas na *pool* do NAT.
4. Associar pool definida em 2) à ACL definida em 3). Para tal, recorra ao comando `ip nat inside destination`.
5. Definir `ip alias` para o endereço IP virtual e para o porto do serviço, neste caso o porto TCP 80.

3. Exercício complementar

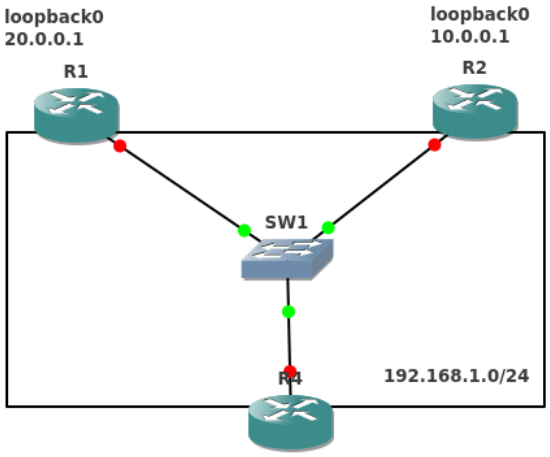

Figura 2 –Cenário prático com o efeito da mensagem ICMP Redirect.

No cenário apresentado na Figura 2, o gateway do router R4 é o router R1, que está configurado com o IP 192.168.1.1/24. Este router tem uma rota por omissão para a interface `loopback0` e uma rota para a rede 10.0.0.0/24, onde está o router R2. Esta rota tem como próximo salto o router R2 (192.168.1.2), na mesma rede de R1 e do R4. Todo tráfego enviado pelo router R4 é encaminhado pelo router R1.

Quando R4 tenta comunicar com a interface de loopback de R2 (10.0.0.1), o tráfego é enviado para R1. Neste caso, R1 verifica (pela tabela de encaminhamento) que a rota para a rede 10.0.0.0/24 é efectuada através de 192.168.1.2. Então R1 envia o tráfego para R2 e envia uma mensagem `ICMP Redirect` para o router R4.

O `ICMP Redirect` é activado por omissão nos routers Cisco (menos nas interfaces configuradas com HSRP). O comando `no ip redirects` desactiva o `ICMP Redirect` na interface desejada.

Pretende-se neste cenário efetuar as seguintes configurações:

1. Desenhar no GNS3 a topologia de rede ilustrada na figura.
2. Configurar o protocolo de encaminhamento RIP em R1 e R2. Verificar se cada router tem, na sua tabela de encaminhamento, as redes da interface de *loopback0* do router vizinho.
3. No router R4 efectuar um `ping` ao IP da interface `loopback0` do router R2.
4. Em cada um dos routers, na respetiva interface `fastethernet 0/0`, desactivar o `ICMP redirect` (encontra-se activo por omissão).
5. Limpar a tabela de encaminhamento do router R4. Para isso, pode usar o comando `no ip route` ou desativar a interface de rede e reactivá-la de seguida.

No router R4, efectuar um novo ping ao IP do loopback de R2. Verifique a tabela de encaminhamento, no router R4 e discuta as alterações verificadas.

4. Documentos de apoio

- Reference guide e tutoriais da Cisco:
  http://www.cisco.com/cisco/web/psa/reference.html

  https://sites.google.com/site/amitsciscozone/home/nat/tcp-load-distribution-using-rotary-nat