Laboratorul 7 – Protocolul NAT

În acest laborator se va investiga comportamentul protocolului NAT(Network Address Translation). Acest laborator va fi diferit de celelalte, unde s-a capturat un trace la un singur punct "măsurat" cu Wireshark. Deoarece vrem să capturăm pachete atât la intrarea cât și la ieșirea dispozitivului NAT, va trebui să capturăm pachete la două locații. De asemenea, datorită faptului că mulți studenți nu au acces ușor la un dispozitiv NAT sau la două computere, acest laborator nu va putea fi executat cu ușurință ("live") de către un student. Din acest motiv, veți folosi trace-uri Wireshark deja capturate.

Setup

În acest laborator, vom captura pachete făcând o simplă cerere "web request" de la un PC, la un server www.google.com.

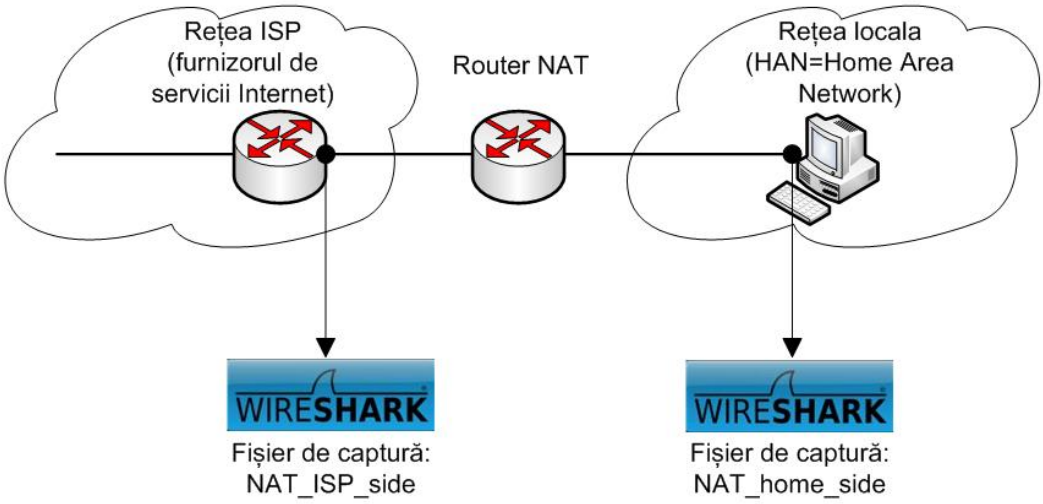

Figura 1 - Legătura dintre rețeaua ISP și rețeaua proprie (home network)

Avem scenariul din Figura 1. Vom folosi fișierul NAT_home_side de pe platforma e-learning. Deoarece ne interesează și pachetele trimise de router-ul NAT în ISP, vom colecta încă un trace de la un PC (neprezentat), folosind legătura de la home router către rețeaua ISP-ului, așa cum se vede în figura de mai sus. Hub-ul desenat pe partea ISP a router-ului este folosit pentru a folosi link-ul dintre router-ul NAT și router-ul de la primul hop din ISP. Fișierul trace capturat pe partea ISP a home router-ului este numit NAT_ISP_side.

Deschideți fișierul NAT_home_side și răspundeți la următoarele întrebări. Puteți folosi un filtru Wireshark pentru a vedea doar cadre care conțin mesaje HTTP.

1. Care este adresa IP a clientului?
2. De fapt clientul comunică cu mai multe servere Google diferite pentru a implementa "safe browsing". Serverul principal Google care are pagina principală Google, are adresa IP 64.233.169.104. Pentru a afișa doar cadrele care conțin mesaje HTTP care sunt trimise la / de la acest server Google, scrieți "http&&ip.addr==64.233.169.104" la filtrul Wireshark.
3. Priviți acum mesajul HTTP GET trimis de la client la serverul Google (al cărui IP este 64.233.169.104) la momentul 7.102967. Care sunt adresele IP și porturile TCP ale sursei și destinației pe datagrama IP care transportă acest HTTP GET?
4. La care moment este recepționat mesajul corespunzător 200 OK HTTP de la serverul Google? Care sunt adresele IP și porturile TCP ale sursei și destinației pe datagrama IP care transportă mesajul 200 OK HTTP?
5. Știm că înainte ca o comanda GET să poată fi trimisă unui server HTTP, TCP trebuie întâi să seteze o conexiune folosind "three-way SYN/ACK handshake". La care moment este trimis, de la client către server, segmentul TCP SYN care setează conexiunea folosită de GET la momentul 7.102967 ? Care sunt adresele IP și porturile TCP ale sursei și destinației pentru acest segment TCP SYN ? Care sunt adresele IP și porturile TCP ale sursei și destinației pe datagrama IP ale ACK-ului trimis ca răspuns lui SYN ? La ce moment este acest ACK recepționat la client? (Aici trebuie sa scrieți "tcp" la filtru).

În cele ce urmează vom privi doar cele 2 mesaje HTTP (GET și 200 OK) și segmentele SYN și ACK de mai sus. Scopul nostru este să localizăm aceste mesaje HTTP și două segmente TCP în fișierul trace (NAT_ISP_side) capturat pe link-ul dintre router și ISP. Cadrele capturate au fost deja forward-ate prin router-ul NAT, de unde rezultă că anumite adrese IP și porturi se vor fi schimbat datorită translației NAT.

Deschideți NAT_ISP_side. *Observați ca "timestamp-urile" din acest fișier și din NAT_home_side nu sunt sincronizate deoarece capturile pachetelor la cele două locații din figura de mai sus nu au fost pornite simultan.* Ar trebui ca timestamp-urile unui pachet capturat la link-ul ISP sa fie mai mic decât timestamp-ul pachetului capturat la PC.

6. În fișierul NAT_ISP_side, mesajul HTTP GET a fost trimis de la client către Google la 7.102967 (unde t = 7.102967 este timpul când mesajul a fost trimis, după cum a fost înregistrat în trace-ul NAT_home_side). La care moment apare mesajul în trace-ul NAT_ISP_side ? Care sunt adresele IP și porturile TCP ale sursei și destinației pe datagrama IP care transportă acest HTTP GET (după cum s-a înregistrat în trace-ul NAT_ISP_side) ? Care dintre aceste câmpuri sunt aceleași și care sunt diferite, față de răspunsul din întrebarea 3. ?

7. Este vreun câmp din mesajul HTTP GET schimbat ? Care dintre câmpurile următoare din datagrama IP este schimbat: Version, Header Length, Flags, Checksum? Justificați răspunsurile.

8. În trace-ul NAT_ISP_side, la care moment a fost recepționat mesajul 200 OK HTTP de la serverul Google? Care dintre aceste câmpuri sunt la fel, și care sunt diferite față de răspunsul de la întrebarea 4 ?

9. În fișierul NAT_ISP_side, la care moment a fost capturat segmentul client-to-server TCP SYN și segmentul server-to-client TCP ACK corespunzătoare segmentelor din întrebarea 5? Care sunt adresele IP și porturile TCP ale sursei și destinației pentru aceste segmente? Care dintre aceste câmpuri sunt la fel și care sunt diferite față de răspunsul la întrebarea 5?

10. Folosindu-va de răspunsurile de la întrebările 1-8, completați tabela de translație NAT pentru conexiunea HTTP din întrebările de mai sus.

Bonus:

Trace-urile investigate mai sus au conexiuni adiționale la serverele Google de mai sus și dincolo de mesajele HTTP GET, 200 OK cerere/răspuns studiate mai sus. De exemplu, în trace-ul NAT_home_side, alegeți mesajul GET client-to-server la timpul 1.573215 și GET la 7.573305. La ce sunt folosite aceste mesaje HTTP ? Explicați răspunsul în jumătate de pagina.

Configurarea NAT

Protocolul NAT translatează adresele interne ne-rutabile în adrese IP publice rutabile. Acesta are un beneficiu suplimentar, deoarece oferă un grad de intimitate și securitate unei rețele, prin ascunderea adresei IP interne de rețelele din afară. În această activitate, veți configura dinamic și static NAT.

1. Porniți Cisco Packet Tracer și deschideți fișierul NAT_Config.

2. Tabela de dirijare:

Dispozitivul	Interfața	Adresa IP	Masca
R1	Fa 0/1	192.168.10.1	255.255.255.0
	S 0/0/0	10.1.1.1	255.255.255.252
R3	Fa 0/1	192.168.30.1	255.255.255.0
	S 0/0/1	10.2.2.2	255.255.255.252
R2	Fa 0/0	192.168.20.1	255.255.255.0
	S 0/0/0	10.1.1.2	255.255.255.252
	S 0/0/1	10.2.2.1	255.255.255.252
	S 0/1/0	209.165.200.225	255.255.255.224
PC1	NIC	192.168.10.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0
Outside Host	NIC	209.165.201.14	255.255.255.240
Public Web Server	NIC	209.165.201.30	255.255.255.240

Tabelul 1 – Tabela de dirijare

3. Configurați routere-le și dispozitivele terminale cu datele din tabela de dirijare.

4. Pentru a defini adresele interne, în urma translatării în adrese publice în procesul NAT, creați un standard ACL (Access Control List) numit **R2NAT**. Această listă este utilizată în paşii de configurare NAT care vor urma.

R2(config)#**ip access-list standard R2NAT**
R2(config-std-nacl)# **permit 192.168.10.0 0.0.0.255**
R2(config-std-nacl)# **permit 192.168.20.0 0.0.0.255**
R2(config-std-nacl)# **permit 192.168.30.0 0.0.0.255**

5. Configurați NAT static pentru server-ul „Inside Web Server”. Acest server trebuie să aibă o adresă IP publică care nu se va schimba niciodată, pentru a putea fi accesat din afara rețelei. Configurarea adresei NAT static permite server-ului web de a putea fi configurat cu o adresă internă privată. Apoi, procesul NAT va mapa întotdeauna pachetele utilizând adresa publică a serverului la adresa privată.

R2(config)#**ip nat inside source static 192.168.20.254 209.165.202.131**

6. Definiți intervalul de adrese și configurați NAT dinamic. Introduceți următoarele comenzi pentru a configura intervalul de adrese publice, care sunt mapate dinamic gazdelor interne.

R2(config)#**ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask 255.255.255.252**

Această primă comandă definește intervalul de adrese publice care sunt mapate la adresele interne. Enumerați aceste adrese.

R2(config)#**ip nat inside source list R2NAT pool R2POOL overload**

Cea de a doua comandă instruiește procesul NAT de a mapa adresele din interval în adresele definite în lista creată la punctul 4.

7. Configurați interfețele router-ului R2 pentru a aplica NAT. În modul de configurare al interfețelor pe router-ul R2, configurați fiecare dintre interfețe folosind comanda **ip nat** {**inside | outside**}. Identificați ce interfețe se vor configura cu comanda **ip nat inside** și care cu comanda **ip nat outside.**

8. Configurați router-ul ISP cu o rută statică la router-ul R2 folosind următoarea comandă:

ISP(config)#**ip route 209.165.202.128 255.255.255.224 serial0/0/0**

9. Testați conectivitatea prin utilizarea comenzii **ping** de la oricare gazdă internă la serverul „Public Web Server” sau dispozitivul terminal „Outside Host”. Intrați în modul simulare și observați efectul NAT.