Laboratuvar Raporu 6

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Özlem Kayıkcı

152120191043

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İçindekiler

2 Giriş

Wireshark NAT Lab, ağı analiz etmek ve ağ trafiğini incelemek için kullanılan bir laboratuvar ortamı olmakla birlikte bu laboratuvar, Network Address Translation (NAT) yönteminin çalışma prensiplerini ve etkileşimlerini anlamak için tasarlanmış bir uygulama sürecini kapsamaktadır. NAT, özellikle IP adreslerinin tükenmeye başladığı durumlarda kullanılan bir ağ yönlendirme tekniği olarak; bir ağdaki cihazların yerel IP adreslerini (private IP) genel IP adresleriyle (public IP) eşleştirerek, ağ trafiğini yönlendirmek ve paylaşmak için bir aracı görevi görmektedir. Bu şekilde de birden fazla yerel cihazın aynı genel IP adresini kullanarak internete erişimini sağlar.

Bu laboratuvar, aşağıdaki gibi bazı hedeflere ulaşma konusunda yardımcı olmuştur:

1. NAT işleyişini anlamak adına laboratuvar ortamında gerçekleşen veri trafiği üzerinden NAT işleyişini gözlemleyerek, iç ve dış ağlar arasındaki adres dönüşümlerini anlaşılmaktadır. Bu sayede NAT'ın nasıl çalıştığını ve paketlerin nasıl yönlendirildiğini öğrenildi.

2. Port yönlendirmesi (port forwarding) analizi: NAT ortamında belirli bir portun yönlendirilmesi durumunda, gelen paketlerin nasıl iç ağdaki belirli bir cihaza yönlendirildiğini incelendi.

3. Ağ trafiği analizi: laboratuvar ortamında yakalanan veri trafiğini analiz ederek, iç ve dış ağ arasında iletilen paketlerin içeriğini, protokollerini ve diğer ağ katmanı bilgilerini incelendi. Bu da son olarak, ağ güvenliği, hata ayıklama ve ağ performansı optimizasyonu gibi alanlarda fayda sağlayabilmektedir.

3 Laboratuvar Uygulaması

3.1 NAT Measurement Scenario

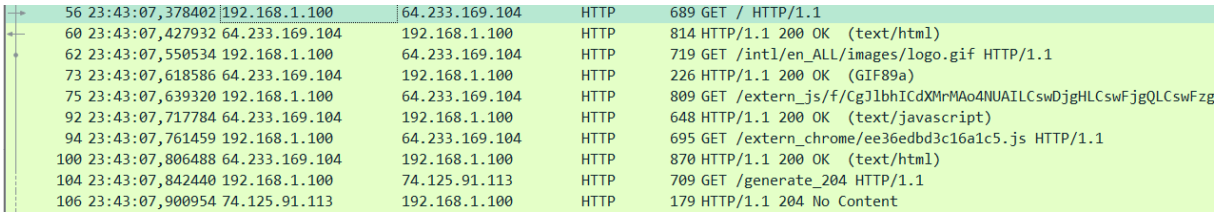
3.1.1 1.soru

1. What is the IP address of the client?

Client IP adresi 192.168.1.100 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

3.1.2 2.soru

2. The client actually communicates with several different Google servers in order to implement "safe browsing." (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression "http && ip.addr == 64.233.169.104" (without quotes) into the Filter: field in Wireshark .



56	23:43:07,378402	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1
60	23:43:07,427932	64.233.169.104	192.168.1.100	HTTP	814 HTTP/1.1 200 OK (text/html)
62	23:43:07,550534	192.168.1.100	64.233.169.104	HTTP	719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	23:43:07,618586	64.233.169.104	192.168.1.100	HTTP	226 HTTP/1.1 200 OK (GIF89a)
75	23:43:07,639320	192.168.1.100	64.233.169.104	HTTP	809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzg
92	23:43:07,717784	64.233.169.104	192.168.1.100	HTTP	648 HTTP/1.1 200 OK (text/javascript)
94	23:43:07,761459	192.168.1.100	64.233.169.104	HTTP	695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100	23:43:07,806488	64.233.169.104	192.168.1.100	HTTP	870 HTTP/1.1 200 OK (text/html)
104	23:43:07,842440	192.168.1.100	74.125.91.113	HTTP	709 GET /generate_204 HTTP/1.1
106	23:43:07,900954	74.125.91.113	192.168.1.100	HTTP	179 HTTP/1.1 204 No Content

3.1.3 3.soru

3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

Source IP adresi 192.168.1.100 , 4335ve Destination IP adresi 64.233.169.104 , 80 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

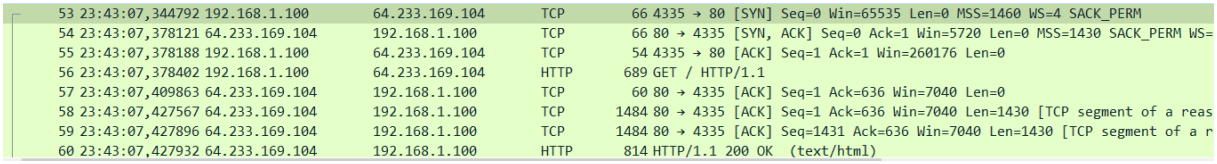
3.1.4 4.soru

4. At what time4 is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

Time değeri 7.158798, Source IP adresi 64.233.168.104 , 80 ve Destination IP adresi 192.168.1.100 , 4335 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

3.1.5 5.soru

5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter "tcp", only TCP segments will be displayed by Wireshark)



53 ve 54 numaralı segmentlerde; 53 numaralı segment için, Time değeri 7.344792 Source IP adresi (TCP SYN olarak): 192.168.1.100 ve de Destination IP adresi (TCP SYN olarak): 64.233.169.104 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

54 numaralı segment için, Time değeri 7.378121 ,Source IP adresi (ACK) 64.233.169.104 ve de Destination IP adresi (ACK) 192.168.1.100 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

3.1.6 6.soru

6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

85.segmentte, Zaman (NAT_ISP_side izleme dosyasında): 7.800232 , Source IP adresi 71.192.34.104 ve Destination IP adresi 64.233.169.104 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

3.soruyla 6.soru arasındaki fark source IP adreslerinin farklı olmasıdır, 3.soruda adres 192.168.1.100 iken 6.soruda ise 71.192.34.104 olarak gözlemlenmiştir.

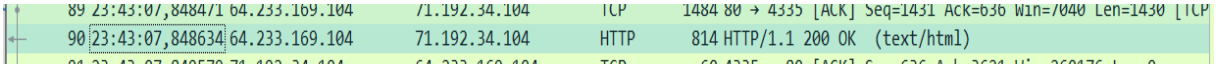
3.1.7 7.soru

7. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

Source IP adresinin değişmesi, checksum'ın içerdiği değerler dolayısıyla checksum değerinde değişim olmuştur.Onun dışındaki alanlarda herhangi bir değişiklik yoktur.

3.1.8 8.soru

8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

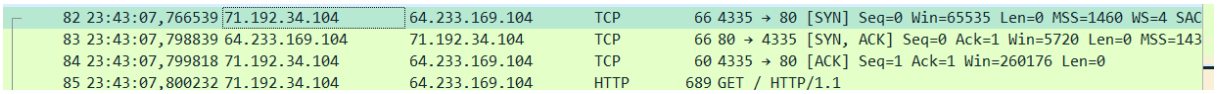


Time değeri 7.848634, Source IP adresi 64.233.169.104 ve Destination IP adresi 71.192.34.104 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

4.soruyla 8.soru arasındaki fark destination IP adreslerinin farklı olmasıdır, 4.soruda adres 192.168.1.100 iken 6.soruda ise 71.192.34.104 olarak gözlemlenmiştir.

3.1.9 9.soru

9. In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?



82 ve 83. Segmentler incelendiğinde, 82. Segment için Time değeri (TCP SYN) 7.766539 ve Source IP adresi (TCP SYN) 71.192.34.104 , Destination IP adresi (TCP SYN) 64.233.16.104 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

83. Segment için Time değeri (TCP ACK) 7.98839 ve Source IP adresi (TCP ACK) 64.233.169.104 , Destination IP adresi (TCP ACK): 71.192.34.104 olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

Aralarındaki benzer ve farklılıklar için, SYN paketi için soruce IP adresi değişmiştir, ACK paketi için destination IP adresi değişmiştir. Port numaraları aynıdır.

3.1.10 10.soru

10. Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

NAT Translation Table	
WAN	LAN
71.192.34.104, 4335	192.168.1.100, 4335

3.1.11 Extra Credit

Extra Credit: The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and write a half page explanation of the purpose of each of these messages.

1.573215 zamanındaki GET isteği için:

Bu belirli GET isteği, istemcinin Google sunucusuna karşı başka bağlantıları temsil eder ve üzerinde çalışılan HTTP GET, 200 OK istek/yanıtından farklıdır. Bu istek, istemcinin sunucuyla bağlantı kurması ve bir oturumu başlatması amacını taşır. İstemci, sunucudan belirli bir kaynağı veya web sayfasını almak için bir GET isteği gönderir, Bu mesaj genellikle istenen kaynak hakkında bilgiler içerir, örneğin URL'si, protokolü ve başlıkları gibi. Google sunucusu, bu isteği aldığında onu işler ve buna uygun şekilde yanıt verir.Bu GET isteğinin amacı, bir web sitesinin ana sayfasını yüklemek, belirli bir dosyayı almak veya Google sunucusuyla başka bir etkileşimi başlatmak olabilir. İstemci ve sunucu arasındaki iletişim ve veri alışverişi, bu başlangıç GET isteği tarafından kolaylaştırılır ve etkileşimin temelini oluşturmktadır.

7.573305 zamanındaki GET isteği için:

7.573305 zamanındaki ikinci GET isteği, istemci ve Google sunucusu arasındaki ek bir etkileşimi temsil etmektedir. Verilen zaman aralığına dayanarak, bu isteğin başlangıç isteği ve sonrasındaki yanıtın ardından gerçekleştiği anlaşılabilir.Bu belirli GET isteğinin amacı, izlenen trace dosyasının ve kullanılan web uygulamasının belirli bağlamına bağlı olarak değişebilir. Bu takip isteğinin ardından yapılabilecek bazı olası nedenler, web sayfasını doğru şekilde render etmek için gereken resimler, betikler veya stil dosyaları gibi ek kaynakları almak olabilir. Ayrıca, sunucudan gerçek zamanlı güncellemeler veya kullanıcıya özgü veriler gibi dinamik içeriklerin alınması da söz konusu olabilir.Bu istek, web uygulamalarının dinamik yapısını gösterir, burada sunucudan çeşitli kaynakları almak ve sorunsuz bir kullanıcı deneyimi sağlamak için sunucuya birden fazla istek gönderilir.Genel olarak, NAT_home_side trace dosyasındaki bu iki ek GET isteği, bağlantı kurma, web kaynaklarını almak ve istemci

ile Google sunucusu arasındaki iletişimi sağlama amacını taşır. Verilen web uygulaması veya senaryo içindeki belirli bağlama ve isteklerin içeriğini anlamak, bu mesajların kesin amacı ve işlevi hakkında daha fazla bilgi sağlar.

4 Kaynakça

- Wireshark Lab: NAT v8.0 Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross