IPv6 Geçiş Yöntemleri Güvenlik Analizi

Emre Yüce[1] *Yavuz Gökırmak*[2] *Onur Bektaş*[3] *Serkan Orcan*[4]

TÜBİTAK ULAKBİM, ANKARA

[1]e-posta: emre@ulakbim.gov.tr [2]e-posta: yavuzg@ulakbim.gov.tr
[3]e-posta: onur@ulakbim.gov.tr [4]e-posta: serkan@ulakbim.gov.tr

Özet

Gelişen internet altyapısı ile birlikte yeni İnternet Protokolüne geçiş bir zorunluluk olarak gözükmektedir. Bu geçiş aşamasında kullanıcıların ve servis sağlayıcıların olumsuz etkilenmemesi için IPv6 geçiş yöntemleri ve oluşabilecek güvenlik problemleri derinlemesine incelenmelidir. Bu çalışma, geçiş yöntemleri ve ilgili güvenlik gözlemlerini içermektedir.
Anahtar Kelimeler:IPv6, geçiş yöntemleri, ağ güvenliği

1. GİRİŞ

IP (Internet Protocol), birbirine bağlı ağ cihazlarının (istemciler, sunucular, yönlendiriciler vs.) aralarında veri iletimini sağlayan temel iletişim protokolüdür. Günümüzde yaygın olarak kullanılan versiyonu IPv4 1981 yılında tanımlanmıştır. [1] 80'li yılların sonlarına doğru IPv4 protokolünün, internet altyapısının gelişimini engelleyecek eksiklikler içerdiği anlaşılmış ve yeni bir protokol üzerinde çalışılmaya başlanmıştır. Bu eksikliklerin başında mevcut IPv4 adreslerinin tükenmesi gelmektedir. IPv6, bu eksiklikleri gidermek amacıyla 1998 yılında önerilmiştir. [2]

Her iki protokol de geçiş süresi boyunca uzun bir müddet kullanımda olacaktır. Bu geçiş sürecinden kullanıcı ve servis sağlayıcıların olumsuz yönde etkilenmemeleri için çeşitli geçiş yöntemleri önerilmiştir. [3]

Bu makale, önerilen geçiş yöntemlerinin kısa tanımlarını ve ilgili güvenlik gözlemlerini içermektedir. Makalenin devamında; ikinci bölümde geçiş yöntemleri ve güvenlik gözlemleri sunulmuştur, üçüncü bölümde ise sonuç ve gelecek çalışmalar ile ilgili bilgiler yer almaktadır.

2. GEÇİŞ YÖNTEMLERİ VE GÜVENLİK GÖZLEMLERİ

Önerilen geçiş yöntemleri ikili yığın, tünelleme ve çeviri olmak üzere üç başlık altında toplanabilir. Önerilen yöntemler arasında her ağa uygulanabilir genel geçer bir geçiş yöntemi mevcut değildir. Ağ yöneticilerinin bu geçiş yöntemlerini analiz etmeleri ve kendi ağlarına uygun olan bir veya birden fazla geçiş yöntemini ağlarına uygulamaları gerekmektedir. Buna ek olarak ağ yöneticilerinin bu geçiş yöntemlerinin kullanımı ile oluşabilecek güvenlik açıklarının farkında olmaları ve bu açıklara karşı önlem almaları gerekmektedir.
Ağ yönlendiricileri ve güvenlik donanımında (ateş duvarı, saldırı tespit sistemi vs.), IPv6 desteği olmaması, ağın IPv6 tabanlı bir saldırıya maruz kalmayacağı anlamına gelmemektedir. Günümüzde kullanılan birçok işletim sistemi kurulumda IPv6 desteği ile gelmektedir. Bu istemciye, IPv4 içinde IPv6 tüneli ile IPv6 uygulama tabanlı bir saldırı gerçekleştiren bir saldırganın ağdaki güvenlik elemanlarını aşabileceği gösterilmiştir. [4]

Bu sebeple ağdaki yönlendirici ve güvenlik elemanlarına IPv6 desteği sağlanmalıdır. Bu destekle birlikte ağdaki trafiğin izlenebilmesi, karşılıklı açılan tünellerin kontrol altında tutulabilmesi güvenli bir IPv6 ağı oluşturabilmek için şarttır.

İlerleyen bölümlerde geçiş yöntemlerine özgü karşılaşılabilecek saldırı türleri ve bu geçiş yöntemleri ile birlikte oluşabilecek güvenlik açıkları incelenmiştir.

2.1. İkili Yığın

İkili yığın geçiş yönteminde her iki protokol de aynı anda desteklenmektedir. Bu yöntemi kullanan cihazlar hem IPv4 adresi hem de IPv6 adresi almaktadır. Tünelleme ve çeviri yöntemlerinde ağın belirli noktalarında her iki protokolü de destekleyen ağ elemanlarına duyulan ihtiyaç bu yöntemin kullanılması ile aşılmaktadır.

İkili yığın yöntemi kullanan cihazlar her iki protokol için de geçerli olan saldırılara maruz kalabilir. Bu yöntemde güvenlik donanımları ve yönlendiriciler her iki protokol için yeniden düzenlenmelidir. Buna ek olarak "IPv6 İkili Yığın Geçiş Yönteminde Uygulamaların Saldırı Altında Performans Analizi" adlı çalışmada ikili yığın geçiş yöntemini kullanan sunucuların, yalın IPv4 ve yalın IPv6 kullanan

sunuculara göre DOS saldırısından daha fazla etkilendiği gösterilmiştir. [5]

İki protokolün aynı anda desteklenmesine yönelik olarak yapılan bir çalışmada, ikili yığın ağlarda solucan yayılımı gibi diğer bir güvenlik tehdidinin yalın IPv4 ve yalın IPv6 destekli ağlara göre daha yüksek olabileceğine yönelik bulgular elde edilmiştir. [6]

2.2. Tünelleme

Tünelleme geçiş yönteminde, bir protokole ait trafik diğer protokol paketleri ile sarmalanarak taşınmaktadır. Bu sayede aynı protokolü kullanan iki uç, diğer protokol üzerinden haberleşebilmektedir. Tünelin uç noktalarında sarmalama ve sarmalamayı açma işlemlerini gerçekleştirmek için ikili yığın yöntemini kullanan tünel uç noktaları yer almaktadır.

Tünelleme yönteminde, kurulan tünellerin kontrol altında tutulması ve tünellenmiş trafiğin filtrelenmesi güvenli bir ağ oluşturmak için önem taşımaktadır. Ağ yöneticisinin IPv6 desteği vermediği bir ağda tünel açarak IPv6 bağlantısı gerçekleştiren istemciler bulunabilmektedir. Tünelleme kullanılarak IPv6 desteği verildiği durumlarda ise -tünellenmiş trafiğin filterelenmesi mümkün olmadığı için [7]- trafiğin paket sarmalaması açıldıktan sonra o protokol için geçerli kurallar ile filtrelenmesi gerekmektedir.

Tünelleme yöntemlerinde uç noktaları için IPv4 adresi doğrulaması dışında kimlik doğrulaması yapılmaması da önemli bir güvenlik açığıdır. IPv4 adresini taklit eden bir saldırganın böyle bir tünele dışarıdan paket sokması mümkün gözükmektedir. [8]

Literatürde çeşitli tünelleme yöntemleri önerilmiştir; elle ayarlanmış tünelleme, Tunnel Brokers, 6to4, ISATAP, Teredo. İlerleyen bölümlerde bu tünelleme yöntemleri ile ilgili güvenlik gözlemleri yer almaktadır.

2.2.1. Elle Ayarlanmış Tünelleme

Elle ayarlanmış tünelleme yönteminde [3] tünel uç noktalarındaki cihazlar, tünel bitiş noktası ile ilgili bilgileri (IPv4 adresi, IPv6 adresi vb.) içermektedir. Her cihazın bu bilgileri içerir şekilde ayarlanması ve değişiklik olduğunda güncellenmesi beraberinde kurulum ve yönetim problemleri getirmektedir.

Tünel kurulumunun elle yapılandırılması, filtreleme, günlük bilgisinin alınması benzeri güvenlik tedbirlerinin alınmasını kolaylaştırmakta ve servis dışı bırakma saldırısı riskini azaltmaktadır. Benzer durum otomatik ayarlanmış tünelleme yöntemlerinde bulunmamaktadır.

2.2.2. Tunnel Broker

Tunnel Broker [9] yönteminde, elle ayarlanmış tünellemeden farklı olarak, tünel uç noktası tünel bilgilerini Tunnel Broker sunucusundan çalıştırılabilir bir betik şeklinde indirir. Tunnel Broker sunucusu, tünel ağ geçidini istemci ve kurulacak tünel hakkında bilgilendirir. İstemci, indirdiği betiği kullanarak tünel ağ geçidi üzerinden tünel kurulumunu gerçekleştirir.

Tünel Broker yönteminde;

- İstemci ve Tunnel Broker sunucusu
- Tunnel Broker sunucusu ve tünel ağ geçidi
- Tunnel Broker sunucusu ve DNS sunucusu

arasındaki iletişim güvenli bir şekilde sağlanmalıdır. [9]

Bu önlemlere ek olarak, kötü niyetli bir kullanıcı çok sayıda tünel açma isteği ile tünel ağ geçidine servis dışı bırakma saldırısı gerçekleştirebilir. Bu saldırının engellenmesi için ağda bir kullanıcının açabileceği tünel sayısı sınırlandırılabilir.

2.2.3. Otomatik Tünelleme

Otomatik tünelleme [10] ilk önerilen yöntemlerden bir tanesidir. Bu yöntemde, IPv4 uyumlu IPv6 adresleri otomatik tünellemeyi gerçekleştirecek ikili yığın destekleyen uçlara atanmaktadır. Bu uçlar IPv6 adresini ve IPv6 adresinin içine gömülmüş IPv4 adresini kullanmaktadır. Bu yöntem yeni önerilen geçiş yöntemleri dökümanlarında yerini 6to4 ve ISATAP yöntemlerine bırakmıştır.

2.2.4. 6to4

6to4 geçiş yöntemi [11]; yönlendiriciden yönlendiriciye kullanılan otomatik tünelleme yöntemidir. Bu yöntemi kullanan sistemler, IANA [12] tarafından atanmış 2002::/16 önekini kullanmaktadır. Bu yöntem sayesinde ayrık IPv6 ağları, mevcut IPv4 altyapısını kullanarak haberleşebilirler. Bu yöntemi kullanan ayrık IPv6 ağındaki bir istemci, önek olarak 2002:V4ADDR::/48 adresini kullanır. V4ADDR ayrık IPv6 ağında, ağ dışına bağlantıyı sağlayan uç noktadaki yönlendiricinin IPv4 adresidir.

6to4 kullanan ağlar kendi aralarında herhangi ek bir ayarlamaya gerek kalmadan haberleşebilir. 6to4 yöntemini kullanan bir ağın, 6to4 kullanmayan bir IPv6 ağına bağlanması için nakledici yönlendirici (relay router) kullanması gerekmektedir. Nakledici yönlendirici bir tane 6to4 ara yüzü, bir tane de IPv6 ara yüzü içeren bir yönlendiricidir.

6to4 yönteminde her iki protokol seviyesinde de IP güvenliği kullanımı performans kaybına yol açacağı önerilmemektedir. [11] Örneğin IPv6 paketi şifrelenmiş

ise trafik analizi bir tehdit olarak görülmediği durumlarda IPv4 paketinin de şifrelenmesi gerekli görülmemektedir.

Sahte IPv6 adresi kullanımının engellenmesi için, kaynak adres tabanlı filtreleme uygulanabilir. Aynı şekilde 2002:V4ADDR::/48 adres yapısına uymayan adreslerden gelen paketler sarmalayıcı ve sarmalamayı açan uçlar tarafından düşürülmelidir.

2.2.5. 6over4

6over4 [13], harici tünel kullanmadan IPv4 ağı üzerinden IPv6 iletimi olarak tanımlanmaktadır. Bu yöntem ayrık IPv6 istemcilerini, IPv4 çoklu gönderim (multicast) özelliğini kullanarak birbirine bağlamaktadır. Bu yöntemde elle ayarlanmış tünellere veya IPv4 uyumlu IPv6 adreslerine ihtiyaç duyulmamaktadır. IPv4 ağlarındaki çoklu gönderim desteği ve kullanımı yaygın olmadığı için 6over4 yöntemi yaygınlaşmamıştır.

2.2.6. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) [14], 6over4 yöntemi yerine önerilmiştir. ISATAP yönteminde de, 6over4 yöntemine benzer bir yapıda IPv4 alt yapısı ağ için sanal bir bağlantı olarak kullanılır. Ancak farklı olarak IPv4 çoklu gönderim alt yapısını kullanmadığı için bağlantı çoklu gönderim içermeyen çoklu erişim (NBMA Non-Broadcast Multiple Access) olarak adlandırılır. 6over4 yönteminde olduğu gibi makinenin IPv4 adresi, ağda tanımlayıcı olarak kullanılır ve IPv6 adresinin son 32 biti olarak kullanılır. Adresin elle ve otomatik olarak ayarlanmasını destekler.

ISATAP yönlendiricilerinin doğru yapılandırılması, bu yöntemi kullanan ağlarda önem teşkil etmektedir. Literatürde ISATAP yönlendiricilerinin LINUX işletim sisteminde yapılandırılmasını inceleyen bir çalışma yer almaktadır. [15]

ISATAP yöntemini kullanan bir ağda, ISATAP sunucuları sadece iç ağdaki istemcilerden gelen isteklere cevap vermelidir. Bu IPv4 ateş duvarı kuralları kullanarak gerçekleştirilebilir. Buna ek olarak ağdaki uç yönlendiriciler gelen ve giden trafik için 41 numaralı protokole sadece bilinen tünel uçları için izin vermelidir. Bu sayede sadece ISATAP sunucuları değil, ağ içindeki istemciler de korunmaktadır. ISATAP sunucu listesi DNS, DHCP gibi otomatik bir şekilde sunuluyorsa, bu liste de korunmalıdır. IPv6 ağlarında yerel ağdaki keşif mesajları için uygulanan güvenlik önlemleri ISATAP yöntemini kullanan ağlarda da uygulanmalıdır [16].

2.2.7. Teredo

Teredo [17] NAT arkasına yerleştirilmiş IPv4 istemcilerinin, IPv6 ağına bağlanmalarını sağlayan otomatik tünelleme yöntemidir. İstemciden istemciye modeli ile çalışan bu yöntemde, bir veya daha fazla NAT arkasına yerleştirilmiş, ikili yığın kullanan istemci, IPv6 paketlerini IPv4 tabanlı UDP mesajlarına sarmalayarak gönderir. Teredo servisi Teredo sunucusu ve Teredo nakledici yönlendirici (relay) olmak üzere iki elemandan oluşmaktadır. Teredo sunucusu bilinen bir UDP portunu (3544), Teredo istemcilerin gelecek istekler için dinler.

Teredo sunucusu, istemcilerden gelen istekleri dinler ve bu isteklere IPv6 adresi ile cevap verir. Teredo sunucusu IPv4 ile sarmalanmış IPv6 paketlerini, Teredo nakledici yönlendiricisine (relay) iletir. Teredo sunucusu aynı zamanda Teredo nakledici yönlendiricisinden (relay) gelen IPv6 paketlerinin, ilgili IPv4 istemcisinin bağlantı sağlayan UDP portuna iletilmesini sağlar. Teredo nakledici sunucusu sadece IPv6 yönlendirici gibi çalışır; Teredo sunucusundan gelen IPv6 paketlerini IPv6 ağına, IPv6 ağından gelen paketleri de Teredo sunucusuna iletir.

Teredo yöntemi, IKE (Internet Key Exchange) [18], AH (Authentication Header) [19], ESP (Encapsulation Security Payload) [20] gibi IPSec (Internet Protocol Security) [21] servislerinin kullanımına imkân sağlamaktadır. Buna karşın Teredo geçiş yönteminin kullanımı beraberinde dikkat edilmesi gereken güvenlik problemleri de getirmektedir. [22] Bu problemler RFC 4380'de [17] 4 başlık altında incelenmiştir: NAT yapısında delik açma, ortadaki adam saldırısı için Teredo servisini kullanmak, Teredo servisini servis dışı bırakma saldırısı, Teredo servisini kullanmayan uçlara servis dışı bırakma saldırısı.

Teredo yöntemi kullanan bir ağda, UDP paketine sarmalanmış IPv6 paketleri NAT servisi veren makine üzerinde bulunan ateş duvarı uygulamasını aşabilir. Böyle bir durumda yerel kullanıma açık tüm servisler, IPv6 ağındaki saldırganlar için potansiyel hedef haline gelebilir. Bu şekilde oluşabilecek bir açık, paket sarmalaması açıldıktan sonra kullanılacak IPv6 destekli bir ateş duvarı (örn: istemci bilgisayarındaki bir ateş duvarı uygulaması) veya IPSec kullanımı ile kapanabilir.

Teredo yöntemi kullanan ağlara yönelik uygulanabilecek diğer bir saldırı, Teredo istemcisinin yönlendirici talebini kesip, sahte bir yönlendirici ilanı ile cevap vermek ve istemciye yanlış bir adres sağlamak olarak geçmektedir. [17] Saldırgan bu noktada istemciyi ulaşılamaz bir adrese yönlendirerek servis dışı bırakma saldırısına maruz bırakabilir veya istemci için nakledici

yönlendirici olarak gözükür ve istemcinin tüm trafiğini izleyebilir. İkinci seçenek ile saldırgan ortadaki adam saldırısı gerçekleştirmiş olacaktır. Bu saldırıya karşı IPv6 güvenlik uygulaması IPSec, sadece IPv6 başlıkları için şifreleme ve kimlik doğrulama sağladığı ve IPv4 ve UDP başlıkları için ek bir güvenlik getirmediği için koruma sağlayamamaktadır. Bu saldırıya karşın Teredo istemcisinin giden IPv6 paketlerini IPSec kullanarak şifrelemesi, sahte IPv6 paketlerinin gönderilmesini ve trafiğin takip edilmesini engelleyecektir.

2.3. Çeviri

Çeviri başlığı altında incelenen yöntemlerde paket formatı bir protokol formatından diğer protokol formatına çevrilir ve bu sayede farklı protokoller kullanan iki uygulama aralarında haberleşebilir. Fakat bu yöntem internetin uçtan uca yapısını bozmaktadır. İkili yığın ya da tünelleme yöntemi kullanan ağlarda paket bir uçtan bir uca değiştirilmeden iletilmektedir. Çeviri yönteminde ise paket başlıkları değiştirildiği için bir protokol tarafından desteklenip, diğeri tarafından desteklenmeyen özelliklerin kullanılamaması söz konusudur. Örneğin bu yöntemde uçtan uca IPSec kullanarak şifreleme ve doğrulama uygulamalarında problemler çıkmaktadır.

2.3.1. SIIT (Stateless IP/ICMP Translation Algorithm)

Ağ katmanında protokol yığınına yerleştirilen çeviriciler "başlık çevirici" olarak adlandırılmaktadır. Bu çeviriciler IPv4 başlıklarını IPv6 başlıklarına ve tersine çevirme işlemini gerçekleştirmektedir. Bu çeviricilere bir örnek SIIT (Stateless IP/ICMP Translation Algorithm) [23] yöntemidir.

SIIT yöntemi ile IPv6 kullanımından doğabilecek mevcut güvenlik zafiyetlerine ek bir güvenlik açığı gelmemektedir. [23] Ancak bu yöntemin kullanıldığı ağlarda IPv6 ile desteği zorunlu hale gelen IPSec kullanımına birtakım kısıtlamalar gelmektedir. IPSec özelliklerinden AH, IPv4 tanımlama alanını içerecek şekilde tanımlanmıştır. Çevirme fonksiyonunun tanımlama alanını her zaman düzgün şekilde çevirmesi mümkün olamamaktadır. Böyle bir durumda paketi alan IPv6 uç noktası da tanımlama başlığını (AH) hesaplayamamaktadır. Dolayısıyla AH özelliği, çeviri yöntemi kullanan ağlarda kullanılamamaktadır. IPSec ile gelen bir diğer özellik olan ESP kullanımı başlık bilgisine bağlı olmadığı için çeviri yöntemi kullanan ağlarda uygulanabilmektedir. ESP tünel modunda IPv6 ucu paketi gönderirken IPv4 başlığı oluşturması ve paketi aldığında da bu başlığı kaldırması gerekliliği, ESP transport modunun kullanımını daha kolay kılmaktadır.

2.3.2. NAT-PT ve NAPT-PT Yöntemleri

NAT-PT [24] (Network Address Translation with Protocol Translation) yöntemi ise iki farklı protokol arasındaki haberleşmeyi bir paketi diğer protokolun paketine çevirerek yapmaktadır. IPv4 protokolunde kullanılan NAT uygulamasına benzer şekilde, NAT-PT yönteminin NAT kısmı özel veya global IPv4 adreslerini IPv6 adreslerine; aynı şekilde IPv6 adreslerini IPv4 adreslerine çevirir. PT kısmı ise paket başlıklarının bir protokolden diğer protokole çevrilmesi ile ilgilidir. NAT-PT yönteminde çevrilen paketlere atanan adresler bir adres havuzundan seçilmektedir.

NAPT-PT (Network Address Port Translation with Package Translation) [24] yöntemi IPv6 uçlarının, bir tane IPv4 adresi kullanarak haberleşmesini sağlamaktadır. Bu yöntem belli sayıda portu dinamik olarak alıcı NAPT-PT ucundaki soketlere eşleştirmektedir.

NAT-PT yönteminde uçtan uca güvenlik sağlamak mümkün olmamaktadır. Yalın IPv6 kullanan bir uç, bir IPv4 ucuna bağlantı kurmak istediğinde, ESP ve AH gibi IPSec özellikleri ve TCP/UDP/ICMP kontrol değerleri için kullanılan geçerli kaynak ve hedef adreslerini içeren bir paket gönderir. Ancak NAT-PT IPv6 ucunun adresini, IPv6 adresi ile herhangi bir ilişkisi olmayan bir IPv4 adresine çevirmektedir. Dolayısıyla alıcı IPv4 ucu, gönderen ucun gerçek IPv6 adresine ulaşamamakta ve gelen paketi doğrulayamamaktadır.

Literatürde NAT-PT yöntemi detaylı incelemesi yapılmış ve bu yöntemin önerilen geçiş yöntemleri arasından kaldırılmasının gerekliliği belirtilmiştir. [25]

3. SONUÇ

Yeni nesil Internet Protokolü IPv6'ya geçiş için her ağın kullanacağı yöntemler farklılık göstermektedir. Ağ yöneticileri geçiş yöntemlerini ve ilgili güvenlik gözlemlerini analiz etmeli ve kendi ağlarına uygun geçiş yöntemi veya yöntemlerini seçmelidir. Bu makalede, önerilmiş ve yaygın olarak bilinen geçiş yöntemleri ve bu yöntemlerin uygulanması halinde güvenlik açığı oluşturmamak için dikkat edilmesi gereken noktalar belirtilmiştir.

Teşekkür

Bu çalışma Türkiye çapında IPv6 altyapısı oluşturmak ve Türkiye'nin IPv6 protokolüne geçişini planlamak amacıyla TÜBİTAK – ULAKBİM'in yönetici, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi'nin yürütücü, Bilgi Teknolojileri ve İletişim Kurumu'nun müşteri kurum olarak katıldığı "Ulusal IPv6 Protokol

Altyapısı Tasarımı ve Geçişi Projesi" kapsamında gerçekleştirilmiştir. [26] Bu proje TÜBİTAK tarafından desteklenmektedir.

4. KAYNAKÇA

[1] J. Postel, *INTERNET PROTOCOL*, RFC 0791, Eylül 1981

[2] S. Deering ve R. Hinden, *Internet Protocol, Version 6, (IPv6) Specification*, RFC 2460, Aralık 1998

[3] R. Gilligan, E. Nordmark, *"Basic Transition Mechanisms for IPv6 Hosts and Routers"*, RFC 4213, Ekim 2005

[4] Emre Yüce, A Case Study on the Security of IPv6 Transition Methods, Eylül 2009

[5] B. Çalışkan ve O. Bektaş, *IPv6 İkili Yığın Geçiş Yönteminde Uygulamaların Saldırı Altında Performans Analizi*, 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Aralık 2008. Sayfa 145-150

[6] Zheng, Q., Liu, T., Guan, X., Qu, Y., ve Wang, N. , *A new worm exploiting IPv4-IPv6 dual-stack networks,* In Proceedings of the 2007 ACM Workshop on Recurring Malcode (Alexandria, Virginia, USA, November 02 - 02, 2007). WORM '07. ACM, New York, NY, 9-15. DOI= http://doi.acm.org/10.1145/1314389.1314392

[7] J. Hoagland, S. Krishnan ve D. Thaler. *Security Concerns With IP Tunneling,* draft-ietf-v6ops-tunnel-security-concerns-01, Ekim 2008

[8] Colitti L., Di Battista G., Patrignani M., *"IPv6-in-IPv4 Tunnel Discovery: Methods and Experimental Results,",* Network and Service Management, IEEE Transactions on , vol.1, no.1, pp.30-38, Nisan 2004

[9] A. Durand, P. Fasano, I. Guardini, D. Lento, *"IPv6 Tunnel Broker"*, IETF Request for Comments 3053, Ocak 2001.

[10] R. Gilligan ve E. Nordmark, *Transition Mechanisms for IPv6 Hosts and Routers*, IETF Request for Comments 1933, Nisan 1996

[11] B. Carpenter, K. Moore, *"Connection of IPv6 Domains via IPv4 Clouds"*, IETF Request for Comments 3056, Şubat 2001

[12] Internet Assigned Numbers Authority, http://www.iana.org/

[13] B. Carpenter, C. Jung, *"Transmission of IPv6 over IPv4 Domains without Explicit Tunnels"*, IETF Request for Comments 2529, Mart 1999.

[14] F. Templin, T. Gleeson, D. Thaler, *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*, Request for Comments 5214, Mart 2008

[15] Sang-Do Lee; Myung-Ki Shin; Hyoung-Jun Kim, *"The implementation of ISATAP router"*, Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference , vol.2, no., pp.3 pp.-1163, 20-22 Şubat

[16] Editor: Martin Dunmore, *An IPv6 Deployment Guide*, 6net

[17] C. Huitema, Microsoft, *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*, Request for Comments 4380, Şubat 2006

[18] D. Harkins, D. Carrel, *The Internet Key Exchange (IKE)*, Request for Comments 2409, Kasım 1998

[19] Atkinson, R., *"IP Authentication Header"*, Request for Comments 2402, Kasım 1998

[20] Atkinson, R., *"IP Encapsulating Security Payload (ESP)"*, Request for Comments 2406, Kasım 1998

[21] S Kent, R Atkinson, *"Security Architecture for the Internet Protocol",* Request for Comments 2401, Kasım 1998

[22] Dr. James Hoagland, *The Teredo Protocol: Tunneling Past Network Security and Other Security Implications*, Symantec

[23] E. Nordmark, *"Stateless IP/ICMP Translation Algorithm (SIIT)"*, IETF Request for Comments 2765, Şubat 2000

[24] G. Tsirtsis, P. Srisuresh, *"Network Address Translation - Protocol Translation (NAT-PT)"*, IETF Request for Comments 2766, Şubat 2000.

[25] C. Aoun, E. Davies, *Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status*, Request for Comments 4966, Temmuz 2007

[26] TÜBİTAK - ULAKBİM, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi, *Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi*, http://www.ipv6.net.tr/