
**T.C.**

**KTO Karatay Üniversitesi**

**Fen Bilimleri Enstitüsü**

ELEKTRİK VE BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI

TEZLİ YÜKSEK LİSANS PROGRAMI

# SANAL ÖZEL AĞLARDA VERİ GÜVENLİĞİ

Seyit BÖGE

KONYA

Ocak 2018

# SANAL ÖZEL AĞLARDA VERİ GÜVENLİĞİ

Seyit BÖGE

KTO Karatay Üniversitesi Fen Bilimleri Enstitüsü

Elektrik ve Bilgisayar Mühendisliği Ana Bilim Dalı

Yüksek Lisans Programı

Yüksek Lisans Tezi

KONYA

Ocak 2018

Fen Bilimleri Enstitü Onayı

Prof. Dr. Hüseyin Bekir YILDIZ

Fen Bilimleri Enstitüsü Müdürü

Bu tezli yüksek lisans tezinin yapılması gereken bütün gerekliliklerinin yerine getirdiğini onaylıyorum.

Yrd. Doç. Dr. Hüseyin Oktay ALTUN

Anabilim Dalı Başkanı

Seyit BÖGE tarafından hazırlanan "SANAL ÖZEL AĞLARDA VERİ GÜVENLİĞİ" başlıklı bu çalışma08/01/2018 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jüri tarafından tezli yüksek lisans tezi olarak kabul edilmiştir.

Yrd. Doç. Dr. Ali ÖZTÜRK

Tez Danışmanı

Jüri Üyeleri

Başkan: Prof. Dr. Novruz ALLAHVERDİ.....

Üye: Yrd. Doç. Dr. Ali ÖZTÜRK .....

Üye: Yrd. Doç. Dr. Mesut GÜNDÜZ.....

## TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu bildirir aksi bir durumda aleyhime doğabilecek tüm hak ve kayıplarını kabullendiğimi beyan ederim.

08/01/2018

Seyit BÖGE

# ÖZET

SANAL ÖZEL AĞLARDA VERİ GÜVENLİĞİ

Seyit BÖGE

Yüksek Lisans- Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Yrd. Doç. Dr. Ali ÖZTÜRK

Ocak 2018

Ağ güvenliği, günümüz dünyasının en önemli meselelerinden biri haline gelmiştir. İnternetin yaygınlaşması ile beraber kurumlar ve şirketler, ağlar üzerinden önemli mahrem bilgiler paylaşmaktadırlar. Erişim izni olmayan üçüncü kişilerin eline geçmesi halinde ciddi zararlara yol açabilecek olan bu bilgilerin korunması oldukça kritiktir. Dahası, artan siber saldırılarla birlikte kurumsal veya özel ağlar ciddi tehdit altındadır. Özellikle kurumsal ağlar ulusal güvenlik açısından kritik önemde olduğu için, ağların güvenlik önlemlerinin arttırılması hayati önem arz etmektedir. Bu tez çalışmasında, günümüzde en çok kullanılan ağ teknolojilerinin başında gelen Sanal özel ağlardaki veri iletişiminin, güvenli bir şekilde yapılması için gerekli protokol, donanım ve teknolojilerin incelenmesi ve alınması gereken önlemler araştırılmıştır.

**Anahtar Kelimeler:** Sanal özel ağ, Veri güvenliği, Şifreleme, Tünelleme, Doğrulama

**ABSTRACT**

Seyit BÖGE

DATA SECURİTY ON VİRTUAL PRİVATE NETWORKS

M.Sc. Electrical and Computer Engineering

Ass.Prof. Dr. Ali ÖZTÜRK

January 2018

Network security has become one of the most important issues in today's world. Along with the widespread use of the Internet, corporations and companies share important confidential information over networks. The protection of this information, which may lead to serious harm if third-parties have access to it, is vital. Moreover, with increased cyber attacks, corporate or private networks are under serious threat. Increasing the security of networks is of vital importance, because corporate networks are especially critical to national security. In this thesis study, necessary protocols, equipment, technologies and necessary precautions have been investigated in order to make data communication in virtual private networks, which is one of the most used network technologies today, to be done safely.

**Keywords:** Virtual private network, Data security, Encryption, Tunneling, Verification

## TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Yrd. Doç. Dr. Ali ÖZTÜRK'e ve kıymetli tecrübelerinden faydalandığım KTO Karatay Üniversitesi Elektrik ve Bilgisayar Mühendisliği Bölümü öğretim üyelerine teşekkürü bir borç bilirim.

Seyit BÖGE

Ocak-2018

İÇİNDEKİLER

# TABLO LİSTESİ

## ŞEKİLLERİN LİSTESİ

## KISALTMALAR

| Kısaltmalar | Açıklama |
|---|---|
| AAA | Authentication Authorization Accounting |
| AES | Advance Encryption Standart |
| AH | Authentication Header |
| CHAP | Challenge-Handshake Authentication Protocol |
| CCP | Compression Control Protocol |
| CA | Certificate authority |
| DES | Data Encryption Standart |
| EAP | Extensible Authentication Protocol |
| GRE | Generic Routing Encapsulation |
| DH | Diffie-Hellman |
| DEA | Data Encryption Algorithm |
| IETF | Internet Engineering Task Force |
| IPSEC | IP Security |
| L2TP | Layer 2 Tunneling Protocol |
| MAC | Message Authentication Code |
| NAT | Network Address Translation |
| PAP | Password Authentication Protocol |
| ESP | Encapsulating Security Payload |
| L2FP | Layer 2 Forwarding Protocol |
| ISP | Internet service provider |
| MD5 | Message-Digest algorithm 5 |
| NAS | Network Access Server |
| PSK | Pre-Shared Key |
| RADIUS | Remote Authentication Dial-In User Service |
| PEAP | Protected Extensible Authentication Protocol |
| IKE | Internet Key Exchange |
| HA | Home Agent |
| HTTPS | Secure Hypertext Transfer Protocol |
| ISDN | Integrated Services Digital Network |
| IPv4 | İnternet Protokol Versiyon 4 |
| MPPE | Microsoft Point-to-Point Encryption |
| RSA | Rivest-Shamir-Adleman |
| TTLS | Tunneled Transport Layer Security |
| UDP | User Datagram Protocol |
| LCP | Link Control Protocol |
| PPP | Point to Point Protocol |

| | |
|---|---|
| FA | Foreign Agent |
| IP | Internet Protocol |
| TLS | Transport Layer Security |
| VPN | Virtual Private Network |
| TACACS | Terminal Access Controller Access Control System |
| RAS | Remote Access Server |
| IPv6 | İnternet Protokol Versiyon 6 |
| LAN | Local Area Network |
| MS-CHAP | Microsoft version of the Challenge-Handshake Authentication Protocol |
| SSTP | Secure Socket Tunneling Protocol |
| WAN | Wide Area Network |
| SLIP | Serial Line IP |
| PPTP | Point to Point Tunnel Protocol |
| SHA | Secure Hash Algorithm |
| NCP | Network Control Protocol |
| NPS | Network Policy Server |
| OSI | Open Systems Interconnection |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |

# 1. GİRİŞ

Ağ terimi; 1962 yılında farklı konumlardaki bilgisayarlar arası iletişim isteği ile ortaya çıkmıştır. İlk kez 1965 yılında iki bilgisayar arasında yapılan haberleşme ile uygulanmaya başlamıştır. Amerikan donanması tarafından kullanılan Advanced Research Project Agency Network (ARPANET) projesi kapsamında 1969 yılında 4 bilgisayarın birbirleri ile iletişim kurmasıyla günümüzdeki internet' in temelleri atılmıştır. ARPANET projesinin uygulanması sonucu ortaya çıkan TCP/IP ile internet, 1983 yılında deneysel olmaktan çıkmış günlük hayatta yerini almaya başlamıştır. TCP/IP ile eş zamanlı olarak Uluslararası Standart Organizasyonu (ISO) yaptığı çalışmalarla (Open Systems Interconnect – OSI) Açık Sistemler Bağlantı Modeli ortaya çıkmıştır.

İnternetin yaygınlaşması ve güvenlik ihlallerinin artması sonucunda, 1996 yılında Microsoft tarafından Noktadan noktaya tünel protokolü (PPTP) geliştirilerek günümüzdeki sanal özel ağların temeli atılmış oldu.

Günümüzde büyük firmalar ve gizliliğe önem veren bazı bireysel kullanıcılar sanal özel ağları kullanmaktadır. Sanal özel ağın temel amacı iki nokta arasındaki iletişimde gizliliği ve güvenliği sağlamaktır. Tez çalışmamda sanal özel ağlardaki veri güvenlik önlemleri incelenip yeni öneriler sunulması hedeflenmektedir.

Bu çalışmanın 1. Kısmında sanal özel ağlara giriş yapılmış 2. Kısımda ise sanal özel ağlarda veri güvenliği hakkında literatür taraması yapılmıştır. 3. Kısımda sanal özel ağın ne olduğu, nasıl çalıştığı ve ağ çeşitleri incelenmiştir. 4. kısımda ise sanal özel ağların temeli olan Kapsülleme (Encapsulation), Doğrulama (Authentication) ve Şifreleme (Encryption) unsurları araştırılmıştır. 5. kısımda ise sanal özel ağlarda kullanılan protokoller ve yöntemler incelenmiştir. 6. Kısımda sanal özel ağlarda veri güvenliğine yönelik araştırma yapılmış ve konu ile ilgili testler yapılmıştır. 7. Kısımda elde edilen veriler karşılaştırılmış ve sonuçlar tartışılmıştır.

## 2. LİTERATÜR TARAMASI

Son yıllarda ağ güvenliği üzerine yapılan çok sayıda çalışma bulunmaktadır. Ortaya çıkan yeni tehditlere karşı alınacak önlemlerin anlatıldığı çalışmalar savunma tekniklerinin güncel tutulmasına yardımcı olmaktadır.

Süheyla EKİZ tarafından yapılan çalışmada kablosuz yerel alan ağı uygulamaların hava alanları, kafeler, oteller, evler gibi çeşitli ortamlarda fazlası ile kullanıldığı, kablosuz iletişimin en büyük sorunu olan güvenli iletişimin Sanal Özel Ağ kullanımı ile giderilebileceği belirtilmektedir. Sanal Özel Ağ protokollerinden IPSec tünel protokolü ile kablosuz iletişim güvenliğinin performansını ölçmektedir. IPSec protokolü ile birim zamanda gönderilen veri miktarı, paket kaybı ve gecikme değerleri incelenmiştir. Sonuç kısmında Sanal Özel Ağ'ın kablosuz ağlar üzerinde kullanılmasının performans düşüşüne sebep olduğu gözlemlenmiştir. [1]

Zeynep YÜKSEL tarafından yapılan çalışmada ağ güvenliğini ilgilendiren her türlü bileşen incelenmiş ve güvenlik duvarı ile VPN ve NAT uygulamaları incelenmiştir. Tezde genel işaretleşme kavramları, modülasyon teknikleri ve iletim ortamları, yerel alan ağlarında TCP/IP ve katman güvenliği incelenmiştir. Bilgisayar ağının güvenliğini ilgilendiren her türlü bileşenin yönetimi ile ilgili güvenlik politikaları, güvenlik duvarı mimarileri ve bileşenleri araştırılıp ağ cihazları üzerinde nasıl önlemler alınabileceği irdelenmiş ve güvenliğin bir bütün olarak incelenmesinin gerekliliği vurgulanmıştır. Sonuç kısmında ise ağ güvenliğinin önemi vurgulanmıştır. [2]

İlker SÖGÜT tarafından yapılan çalışmada MPLS yöntemi kullanılarak sanal özel ağ kurulumu incelenmektedir, çalışma ile alanlar arası sanal özel ağ kurulmuş ve etiketleme yöntemi ile iletişime geçilmiştir. Geliştirilen yöntem ile alanlar arası sanal özel ağ yapılandırılmasında MPLS kullanılarak bilinen yönlendirme protokollerinin yaşadığı sorunlara çözüm üretilmektedir. Yapılan çalışma sonunda, uygulama olarak hazırlanan ağ topolojisinde alanlar arası sanal özel ağ için her bir yönlendiricide yönlendirme tablosundaki her ağ tanımı için bir etiket üretilmiştir Böylece oluşturulan özel sanal ağ arasında çok protokollü etiket anahtarlama kullanılarak yönlendirme

gerçekleştirilmiştir ve özel sanal ağ yapısı tezin konusunda belirlenen şekilde gerçekleştirilmiştir. [3]

Fuat DEMİR tarafından yapılan çalışmada SSL VPN, IPSec Uzak Erişim VPN ve IPSec Uçtan Uca VPN çeşitlerini Cisco 5500 serisi güvenlik duvarı kullanılarak konfigürasyonlarının yapılışı anlatılmıştır. Bu üç tip sanal özel ağ üzerinden, Windows işletim sistemi kullanan bir istemciden, uzak ağda bulunan bir web sunucusuna erişim yapılmıştır. Aynı şifreleme ve paket bütünlüğü algoritması kullanılarak, istemcinin uzak yerel ağdaki web sunucusuna erişim süresi ölçülmüş ve özel sanal ağ tipleri erişim hızı açısından değerlendirilmiştir. Çalışmada SSL ile IPSec teknolojileri ile sanal özel ağlarda yaygın olarak kullanılan şifreleme yöntemleri de karşılaştırılmıştır. [4]

Nurdoğan AYDOĞDU tarafından yapılan çalışmada sistemlerinde sabit parola ya da token ile üretilen pin kodu girişi algoritmasının kaynak sağlayıcı firmadan çalınması ihtimali üzerine bu yönteme ek olarak kullanıcı tarafından oluşturulan dört haneli pin oluşturulması güvenliği arttırma konusunda ek önlem olarak görülmektedir. Token cihazının ürettiği kod ile beraber sisteme ilk girişte kullanıcının kendi belirleyeceği (yalnızca kullanıcının kendi bileceği) dört hane ön pin oluşturarak sonraki denemesinde ve ileride bundan sonraki tüm sistem erişiminde kullanacağı bu basit güvenlik geliştirmesi ile pin + token kodu = güvenli giriş kodu ile sisteme güvenli bir şekilde erişilebilmesi planlanmaktadır. [5]

Yunus Emre SEYYAR tarafından yapılan çalışmada “Siteden siteye sanal özel ağ” topolojisi GNS3 benzetim uygulaması kullanılarak hazırlanmıştır. Hazırlanan topolojilere Vmware sanal uygulaması kullanılarak sanal bilgisayarlar ile çalışır hale getirilmiştir. Her iki uygulamada da cihaz maliyetleri açısından da fark olmadığı görülmüştür. Ancak performansları detaylı incelendiğinde, dinamik çok noktalı sanal özel ağ yapılandırmasının sanal özel ağ yapılandırmasından daha kolay ve az olması nedeni ile genel ağ trafiğini rahatlattığı gözlenmiştir. Sonuç olarak çok noktaya sahip kullanıcılar için siteden siteye sanal özel ağ uygulamasından ziyade çok noktalı sanal özel ağ uygulamasının faydalı olacağı sonucuna varılmıştır. [6]

Taha ALJADIR tarafından yapılan çalışmada bilgisayar ağlarına karşı çeşitli saldırı türleri için sistem güvenlik sorunlarının belirlenmesi üzerinde durulmaktadır. Çalışmada siteden siteye VPN ile uzaktan erişim ve VPN' in saldırılara karşı tutumu incelenmektedir. SSL ve PPTP olmak üzere 2 çeşit VPN ağı kurulup farklı saldırı türleri uygulanarak güvenlik açıkları gözlemlenmiştir. Bu protokollerin güvenlik açıkları için öneriler geliştirilmiştir. [7]

Mouath SALIM tarafından yapılan çalışmada Uzaktan Erişimli Bilgisayar İletişiminin Analizi ve Uygulanması üzerinde durulmuştur. Çalışmada sanal özel ağlar hakkında genel bilgiler incelenmiştir. Ağ kurulum yöntemleri hakkında bilgi verilmiş ve bu yöntemler ile uzaktan erişimli Sanal Özel ağ protokollerinin (PPTP, SSL ve 2TP/IPSec) üç farklı tipi VMware ve GNS3 araçları ile kullanımı sanal olarak sağlanmıştır. Bu protokollerin benzer koşullar altında yapılan ölçüm testleri ile performansları test edilmiştir. [8]

Shaneel Narayan ve arkadaşları tarafından yapılan çalışmada Windows 2003 işletim sistemi üzerinde sanal özel ağ protokollerinin performansı değerlendirilmiştir. Çalışmada IPSec, PPTP ve SSL tünel protokollerinin bant genişliği ve CPU kullanım süreleri ölçülmüş ve VPN sunucusunun, CPU performansı seçilecek tünel protokolüne bağlı olarak değiştiği gözlemlenmiştir. [9]

Yongguang Zhang tarafından yapılan çalışmada kablosuz ağlarda TCP performans artışı için çok katmanlı ip güvenlik protokollünün uygulaması gösterilmiş ve Ipsec ve ML-Ipsec protokollerinin işlem gecikme hızları, CPU yükü ve bant genişliği yüklerinin karşılaştırılarak performansları test edilmiştir. [10]

Diaa Salama Abd Elminaam ve arkadaşları tarafından yapılan çalışmada simetrik şifreleme algoritmalarının performansı değerlendirilmektedir. Çalışmada simetrik şifreleme algoritmalarının farklı boyutlardaki paketlerin şifreleme süreleri, algoritmaların saniyede şifreleye bildikleri veri miktarları ve saniye başına çözebildikleri şifre boyutları test edilmiştir. [11]

Zhao Aqun ve arkadaşları tarafından yapılan çalışmada sanal özel ağ protokol özellikleri araştırılmış, protokollerin artıları ve eksileri tespit edilmiştir. Tünel protokolleri konfigürasyonları ve kurulumu anlatılmıştır. Tünel protokollerinin yönetimi ve bakımı hakkında öneriler sunmaktadır. [12]

Yukarıdaki çalışmalarda Sanal özel ağların güvenliğini sağlamak için farklı yöntemler mevcuttur. Bu çalışmanın amacı ise sanal özel ağlardaki veri güvenliği için SSTP protokolü kullanılarak SSL-TLS üzerinden veri akşının sağlanması ve bu protokollerin veri güvenliğine sağladığı katkıların araştırılıp, protokoller üzerinde yapılan test sonuçları ile kullanılması gereken yöntemlerin belirlenmesini sağlamaktır.

## 3. SANAL ÖZEL AĞ

Sanal Özel Ağ (VPN) fiziksel bağlantısı olmayan iki nokta arasında uzaktan erişim yoluyla bağlantı sağlayarak sanal bir ağ kurulması ve aynı konumdaymış gibi veri alışverişi yapılmasını sağlar. Geniş Alan Ağı kurma yöntemlerinden biri olan VPN, internet altyapısı kullandığın için maliyeti en düşük Geniş Alan Ağı çözümüdür.

VPN sayesinde sanal ağa bağlanan bir cihaz fiziki olarak o konumda bulunuyormuş gibi o ağın fonksiyonel, güvenlik ve yönetim özelliklerini kullanır. Bu teknoloji sayesinde büyük firmalar veya şube sayısı çok olan kuruluşlar, kendi aralarında doküman alışverişi, stok takibi, sipariş bilgileri gibi birçok veriyi güvenli ve en ucuz yöntem ile kullanabilmektedir.

VPN hattı güvensiz bir hat üzerinden yapılan bağlantıları güvenli hale getirir. Herhangi bir sanal özel ağ üzerinden iletişime geçtiğinizde sizin bağlantınızı şifreleyerek kimliğinizin gizlenmesini sağlar. VPN ağlarındaki veri transferleri şifrelenerek yapıldığı için 3. şahıslar veriyi görseler bile içeriğini anlayamazlar.


**Şekil 1** Basit VPN Bağlantısı [13]

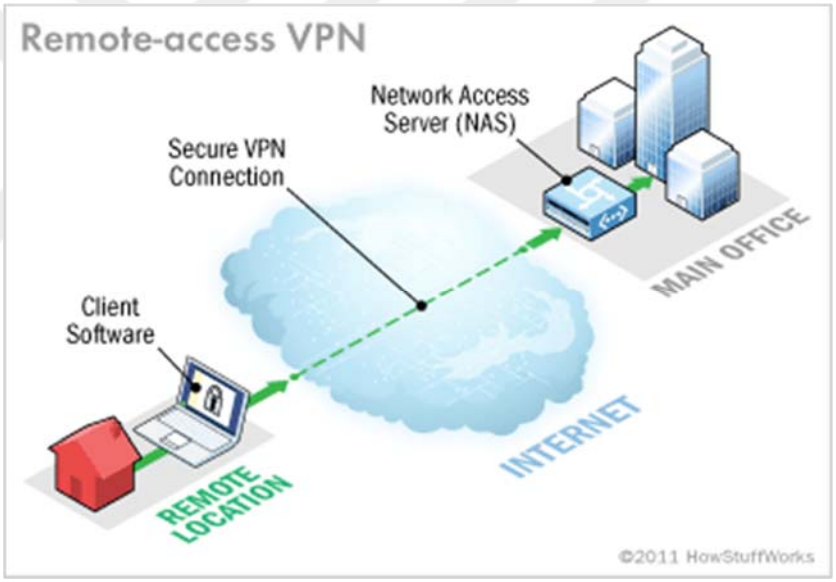
VPN ağlarına bağlı iken VPN sunucusunun bulunduğu konumdaki adli ve idari kontrollere tabi olunmaktadır. Örneğin ülkemizde yasaklı olan bir site VPN sunucusunun bulunduğu ABD de yasaklı değilse ağa bağlı iken yasaklı siteye girebilme imkânı tanımaktadır.

VPN çalışma mantığı temel olarak bilgisayarın fiziksel olarak bulunduğu yerden bağlanacağı ağa dış dünyadan yalıtılmış kriptolu tünel açarak veri alışverişini bu tünel aracılığı ile yapmaktadır. Güvenli sanal ağlar iki makine, bir makine ve bir ağ veya iki ağ arasında oluşturulur. İki çeşit VPN bağlantısı vardır; uzaktan erişim (Remote Access) ve siteden siteye (site to site).

### 3.1. VPN Bağlanti Çeşitleri

#### 3.1.1 Uzaktan Erişim (Remote Access)

Uzaktan erişim VPN bireysel kullanıcılara uzaktaki bir bilgisayar ağı ile güvenli bağlantı kurmak için izin verir. Bu kullanıcılar bu ağdaki güvenli kaynaklara doğrudan ağ sunucularına bağlanmış gibi erişebilirler.




**Şekil 2** Uzaktan Erişim VPN Bağlantısı [14]

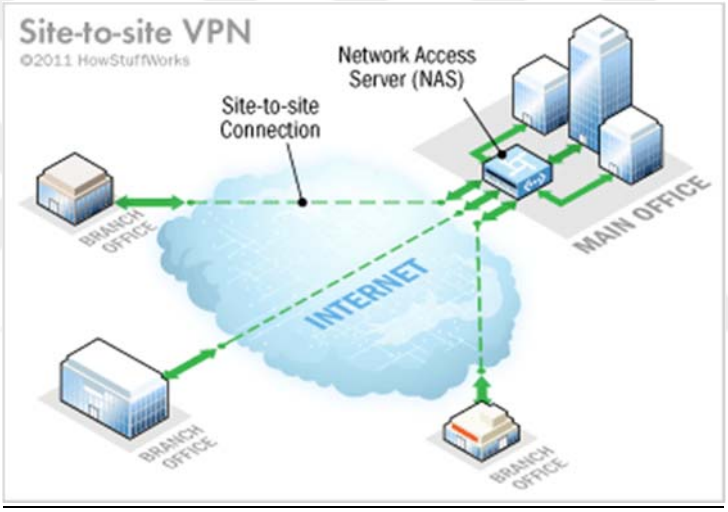
Uzaktan erişim VPN' de iki bileşen gereklidir. Birincisi, bir medya ağ geçidi veya uzaktan erişim sunucusu (RAS) olarak da adlandırılan bir ağ erişim sunucusudur. Ağ Erişim Sunucusu (NAS), kullanıcının VPN' de oturum açmak için geçerli kimlik bilgilerini sağlamasını şart koşar. Kullanıcının kimlik bilgilerini doğrulamak için NAS, kendi kimlik doğrulama işlemini veya ağda çalışan ayrı bir kimlik doğrulama sunucusunu kullanır.

Uzaktan erişim VPN'lerin diğer gerekli bileşeni istemci yazılımıdır. Diğer bir deyişle, VPN'leri bilgisayarlarından kullanmak isteyen çalışanlar için, bu bilgisayarlarda VPN

ile bağlantı kurulabilen ve bunları koruyabilen bir yazılım gerektirir. İstemci yazılımı, kullanıcının İnternet adresiyle belirlediği bir NAS' a tünelli bağlantı kurar. Yazılım ayrıca, bağlantıyı güvenli tutmak için gereken şifrelemeyi yönetir. [14]

### 3.1.2 Siteden Siteye (Site to Site)

Herhangi bir konumda bulunan istemci ile farklı bir noktada bulunan sunucu ile kurulan VPN bağlantı şekline siteden siteye bağlantı denir. Siteden siteye VPN, şirketin ağını genişleterek bir yerdeki bilgisayar kaynaklarını başka yerlerde çalışanların kullanımına açar. Siteden siteye VPN'e örnek olarak dünya çapında şubesi bulunan bir şirket gösterilebilir.




**Şekil 3** Siteden Siteye VPN Bağlantısı [14]

Siteden Siteye VPN'lerin iki türü vardır:

Intranet tabanlı: Bir şirket tek bir özel ağa katılmak isteyen bir veya daha fazla uzak konuma sahipse, her bir ayrı LAN'ı tek bir WAN'a bağlamak için bir intranet VPN oluşturabilirler.

Extranet tabanlı: Bir şirket başka bir şirketle (bir ortak, tedarikçi veya müşteri gibi) yakın bir ilişki içeriyorsa, bu şirketlerin LAN'larını birbirine bağlayan bir extranet VPN oluşturabilir. Bu extranet VPN, şirketlerin ayrı bir intranet'e erişimini engelleyerek güvenli, paylaşımlı bir ağ ortamında birlikte çalışmasına olanak tanır.

Siteler arası VPN'in amacı, uzaktan erişim VPN'in amacından farklı olsa da aynı yazılım ve ekipmanlardan bazılarını kullanabilir. İdeal olarak, bir siteler arası VPN, her bir bilgisayarın VPN istemci yazılımını uzaktan erişim VPN'de olduğu gibi çalışması gereğini ortadan kaldırmalıdır.

Sunucularında özel ekipman ve büyük ölçekli şifreleme kullanan bir şirket, birçok sabit noktayı internet gibi genel bir ağa bağlayabilir. Her site aynı kamu ağı için yalnızca yerel bir bağlantıya ihtiyaç duyar ve böylece uzun özel kiralık hatlarda tasarruf sağlar. Siteden Siteye VPN'ler ayrıca intranet veya extranet olarak sınıflandırılabilir. Aynı şirketin ofisleri arasında inşa edilmiş bir siteler arası VPN' nin bir intranet VPN, şirketin ortağına veya müşterisine bağlanması için yapılmış bir VPN' e extranet VPN adı verilir.

# 4. SANAL ÖZEL AĞ GÜVENLİĞİ

## 4.1. Kapsülleme

VPN ağında veriler bir üstbilgi ile kapsüllenir. Bu üst bilgi, verilerin geçiş ağı sırasında çapraz geçmelerine izin verecek bilgileri içerir. Paketin başlıklarının önüne yeni başlıklar ekleyerek, taşındığı ağdaki olası izleyicilerden gizlenmesini sağlar. Bunun sonucunda, yönlendiriciler sadece sonradan eklenen başlıkları görür ve onlara göre paketi yönlendirir.

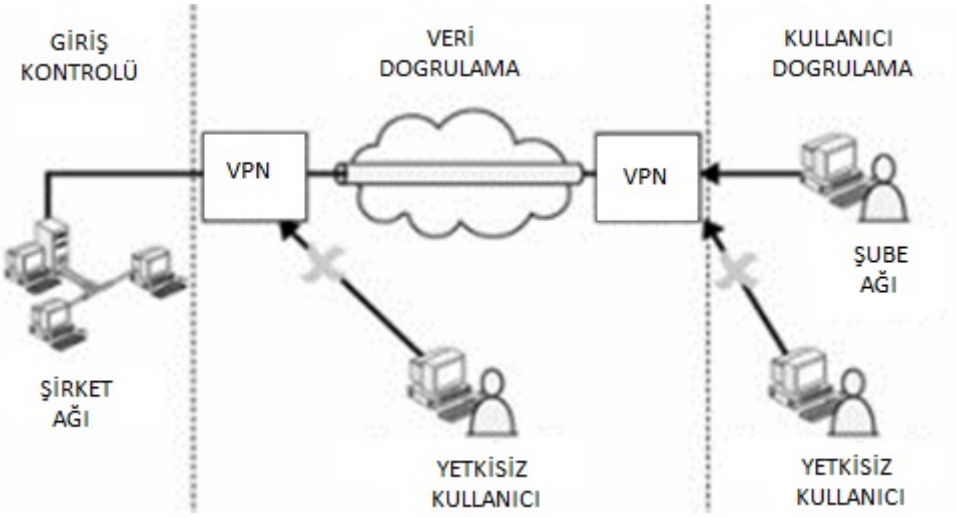
Tünelleme, sunucu uygulamasında gerçekleşecek şekilde tasarlanmıştır. Gelen paketler yeni bir TCP/IP paketinin içine gömülür ve alıcı sunucusuna gönderilir. Kapsülleme işlemi tamamlandığında yeni paketin boyu eski pakete göre iki başlık boyu kadar büyük olacaktır. Yeni paketin Ethernet başlığında, kaynak sunucusunun ve ağ geçidinin MAC adresi bulunur. Ipv4 başlığında ise yine sunucuların IP adresleri bulunur ve toplam sınama değeri tekrar hesaplanır. TCP başlığının da sunucularla senkronize çalışabilecekleri şekilde düzenlenmesi gerekir. Orijinal paket ise Ipv4 ve TCP başlıklarıyla beraber yeni paketin veri kısmını oluşturur.

Virtual Private Network, aynı özel ağda bulunmayan bir veya birden fazla ağ cihazı arasından güvenli bir şifreleme metodu kullanarak kapsüllenmiş veri akışı yapar. Bu kapsülleme özelliği aslında tünelleme olarak da bilinmektedir.

Güvenli şifreleme metodunun amacı, verilerin özel ya da kamusal alandaki diğer ağ cihazlarından gizlenmesidir. VPN'nin asıl amacı kullanıcı internet akışını başka bir ağa aktararak kullanıcı kimliğini gizlemektir. Bu sayede kullanıcıların kimlikleri bilinmeksizin İnternet'te gezinmeleri sağlanmaktadır. [5]

## 4.2. Doğrulama

VPN sisteminde iki tip doğrulama kontrolü vardır. Birincisi kim, nereye ve nasıl erişmek istiyor? İkincisi ise erişim sırasında başkaları bu bilgileri temin etmiş olabilir mi? Bu soruları incelediğimizde Sabit Hatlar ile VPN Sistemleri arasındaki en önemli fark ortaya çıkmış olmaktadır. Hatta diğer birçok sistem ile karşılaştırıldığında daha az maliyetli olduğundan yerel güvenlik çözümleri arasında sabit bağlantılar içerisinde başkasının verileri dinleyerek elde etme ihtimaline karşı VPN çözümü uygulanmaktadır.




**Şekil 4** Doğrulama Yapısı

### 4.2.1 Kimlik Doğrulama

Bazı güvenlik gerekçeleri nedeniyle her kullanıcının VPN ile uzaktan kurumsal verilerinize erişmesini istemeyebilirsiniz. Bu noktada devreye kimlik doğrulama sistemi girmektedir. Bu güvenlik önlemi sayesinde kullanıcıların yetkisine göre ulaşabileceği verileri belirlenmektedir. Gerçek erişim yetkisini sahip kullanıcının kendisine verilen yetkiler doğrultusunda bağlanmasını sağlamak için Kimlik Doğrulama servisleri kullanılır. Örneğin muhasebe biriminde çalışan a kullanıcısı sistemde bulunan personel bilgilerine erişmesi için yetkisinin olup olmadığı kontrol edilir yetkisi var ise bilgilere ulaşması sağlanır.

### 4.2.2 Paket Doğrulaması

Şifreleme, mesajın içeriğini anlamsız kelimelere çevirerek 3. şahısların mesaj içeriğini görmelerini engeller fakat aktarılan mesajın içeriğinin değişip değiştirilmediğini kontrol edemez. Mesajın aktarılması sırasında devreye doğrulama sistemi girmektedir. Doğrulama, mesajın karşı tarafa aktarımı esnasında değiştirilip değiştirilmediğini kontrol eden sistemdir.

VPN sistemlerde doğrulamayı IPSec'in "Internet Key Exchange protokolü (IKE)" kısmı yerine getirmektedir. IKE, iki IPSec ucu arasında güvenlik hizmetleri konusunda, ilişkilendirilmiş oldukları oturum doğrulaması ve kripto anahtarlarında uzlaşılmasını sağlar. [15]

### 4.3. Veri Şifreleme

Verilerin güvenli bir şekilde yollanması ve karşı taraftan alınabilmesi için kriptografi bilimi aracılığıyla geliştirilen çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları kullanılmaktadır. Kriptoloji algoritmalarından en yaygın kullanılanı ise şifreleme algoritmalarıdır. Şifreleme algoritması şifrelenecek metni ve şifreleme anahtarını girdi olarak alır ve veriyi anlamsız bir hale getirir. Çözümleme algoritması ise şifreleme algoritmasının ters yönünde çalışır. Kriptografi de şifreleme için kullanılan anahtarın özellikleri ve çeşidine göre temel olarak iki çeşit şifreleme algoritması bulunmaktadır. [16]

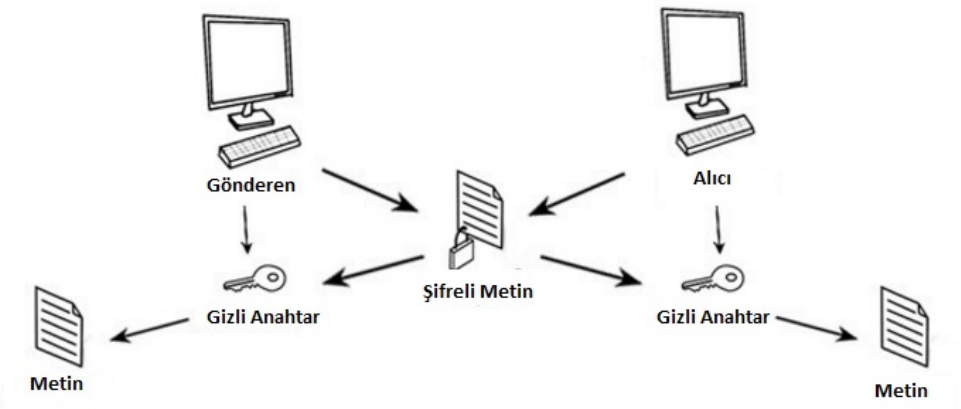
Şifreleme algoritmaları anahtar kullanma yöntemlerine göre genel olarak iki Kategoriye ayrılmaktadır. Bunlar:

- Gizli anahtarlı (Simetrik) şifreleme algoritmaları

- Açık anahtarlı (Asimetrik) şifreleme algoritmaları

#### 4.3.1 Simetrik (Gizli Anahtarlı) Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları şifreleme ve şifre çözme işlemleri için tek bir gizli anahtar kullanmaktadır. Bu durum veri şifreleme için matematiksel açıdan daha az problem çıkaran bir yaklaşımdır ve çok kullanılan bir yöntemdir. Bu tip algoritmalarda şifreleme işlemi gerçekleştirildikten sonra şifreli metni alıcıya gönderirken şifreli metinle birlikte gizli anahtarı da alıcıya güvenli bir şekilde göndermek gerekmektedir. Simetrik şifreleme algoritmaları çok hızlı bir şekilde şifreleme ve şifre çözme işlemlerini gerçekleştirebilmektedir [17].




**Şekil 5:** Gizli Anahtarlı Şifreleme

#### 4.3.1.1 DES (Data Encrytion Standard)

DES, güvenli veri transferi için, verilerin şifrelenmesi ve şifrelenen verinin orijinal haline dönüştürmek için geliştirilmiş bir şifreleme standardıdır. DES temeli blok şifrelemeye dayanmaktadır. Şifrelenecek veri parçalara ayrılarak her parçayı ayrı ayrı şifreler. Bu şifreleme blokları 64 bit uzunluğundadır. DES 64 bit uzunluğunda anahtar kullanmaktadır. DES ile şifrelenmiş veriyi açmak için şifreli veri ve şifreleme anahtarı ile yapılmaktadır. [18]

Günümüzde bilgisayarların güçlenmesi sonucu, büyük işlemleri kısa sürede yapması sonucu DES şifrelerinin çözümü kolaylaşmıştır. Bu durumu önlemek için 3DES algoritması geliştirilmiştir. Bu algoritma 128 bit anahtar uzunluğu kullandığı için DES'e göre daha güvenlidir.

#### 4.3.1.2. AES (Advanced Encrytion Standard)

DES şifreleme algoritmasının saldırılara karşı yetersiz kalması sonucunda AES protokolünün ortaya çıkmasına neden olmuştur. AES protokolü Joan Daemen ve Vincent Rijmen tarafından veri güvenliği sağlanması amacıyla geliştirilmiştir. Gelişmiş Şifreleme Standardı 128, 192, 256 bit anahtar uzunluğuna sahiptir. [19]

AES protokolü şifreleme işlemi için verileri, dizilere bölerek başlamaktadır. Şifrelemenin başlangıcı düz metne ait durum matrisi ile anahtara ait durum matrisinin birleşimiyle yapılır. AES şifreleme işleminde kullandığı anahtarı şifre çözme

işleminde de kullanmaktadır. Şifrelemede kullanılan algoritma için anahtar uzunluğuna göre döngü sayısı atar. Bu döngü sayısı arttıkça veri güvenliği de artmaktadır. Yani anahtar boyutu arttıkça veri güvenliği de aynı oranda artmaktadır.

### 4.3.2. Asimetrik (Açık Anahtarlı) Şifreleme Algoritmaları

Açık anahtarlı şifreleme algoritmaları simetrik şifreleme algoritmalarından radikal bir farklılık göstermektedir. Bu tip şifreleme algoritmaları açık (public) ve özel (private) anahtar olmak üzere iki ayrı anahtar kullanmaktadır. Asimetrik algoritmalar da denilen açık anahtarlı algoritmalarda şifreleme için kullanılan anahtar ile şifre çözme için kullanılan anahtar birbirinden farklıdır. Anahtar çiftlerini üreten algoritmaların matematiksel özelliklerinden dolayı açık-özel anahtar çiftleri her kişi için farklıdır, diğer bir deyişle her kullanıcının açık-özel anahtar çifti yalnızca o kullanıcıya özeldir. Ayrıca şifre çözüm anahtarı (en azından makul bir zaman dilimi içerisinde) şifre anahtarından hesaplanamaz. Bu algoritmalara açık anahtarlı algoritmalar denmesinin sebebi şifre anahtarının halka (kamuya/genel kullanıma) açık olmasıdır. Yabancı bir iletiyi şifrelemek için şifreleme anahtarını kullanabilir, ancak sadece ilgili şifre çözüm anahtarına sahip kişi iletinin şifresini çözebilir. Bu sistemde, şifre anahtarına genellikle açık anahtar adı verilmektedir. Şifre çözüm anahtarı da genellikle özel anahtar olarak adlandırılmaktadır. Özel anahtar kimi zaman gizli anahtar olarak da adlandırılır, ancak simetrik algoritmalarla karışmaması için bu terim genelde kullanılmamaktadır. [17]


**Şekil 6:** Açık Anahtarlı Şifreleme

#### 4.3.2.1. DH (Diffie-Helman)

1976 yılında Diffie ve Helman tarafından bulunmuş ilk asimetrik şifreleme algoritmasıdır. DH iki katılımcının öncesinde herhangi bir bilgi alışverişi yapmadan güvenli olmayan bir kanal vasıtasıyla (güvenli bir şekilde) ortak bir şifrede karar kılmalarına yarayan bir protokoldür. Algoritma anahtar değişimi ile asıl amacı, iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır. Diffie–Hellman algoritması oluşturularak simetrik şifreleme algoritmaları için büyük problemi olan gizli anahtarı koruma ve dağıtım büyük ölçüde aşılmıştır. Bununla birlikte Diffie-hellman algoritması sadece ortak gizli anahtarı belirlemekte kullanılmaktadır. [16]

Diffie-hellman algoritması için sayısal örnek; Ortak anahtarı oluşturmak için öncelikle p sayısını p=541 ve g sayısını g=2 seçelim. A kişisi kendi gizli anahtarı olan a sayısını, a=137 ve B kişisi kendi gizli anahtarı olan b sayısını, b=193 olarak belirlesin.

$c = g^a \pmod p = 2^{137} \pmod{541} = 208$

$d = g^b \pmod p = 2^{193} \pmod{541} = 195$

A ve B ortak anahtar k'yi hesaplar,

$k = d^a = c^b = (g^b)^a \pmod{541} = (2^{137})^{193} = 486$

Bu örnek için 486 sayısı her iki taraf için de açık olarak paylaşılmayan, ancak paylaşılan açık anahtarlarla hesaplanan özel bir anahtardır.

Burada, A ile B'nin hattını dinleyen üçüncü bir kişi, örnekteki, g, p, c ve d sayılarını öğrenebilir. Ancak a ve b özel sayıları hat üzerinden paylaşılmadığından bu sayıları öğrenemez. Üçüncü kişi k anahtarını bulmak için,

$d^a \pmod p = c^b \pmod p = k$

eşitliğini çözmek zorundadır. [4]

#### 4.3.2.2. RSA (Rivest-Shamir-Adleman)

RSA, güvenliği tam sayıları çarpanlarına ayrımanın algoritmik zorluğuna dayanan bir tür Açık anahtarlı şifreleme yöntemidir. 1978'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunmuştur. Bir RSA kullanıcısı iki büyük asal sayının çarpımını üretir ve seçtiği diğer bir değerle birlikte ortak anahtar olarak ilan eder. Seçilen asal çarpanları ise saklar. Ortak anahtarı kullanan biri herhangi bir mesajı şifreleyebilir, ancak şu anki yöntemlerle eğer ortak anahtar yeterince büyükse sadece asal çarpanları bilen kişi bu mesajı çözebilir. RSA şifrelemeyi kırmanın çarpanlara ayırma problemini kırmak kadar zor olup olmadığı hala kesinleşmemiş bir problemdir.

RSA algoritması anahtar üretimi, şifreleme ve şifre çözme olmak üzere 3 basamaktan oluşmaktadır. [21]

### 4.3.3. Anahtarsız Algoritmalar

Simetrik ve asimetrik şifrelemelerin haricinde girdi olarak anahtar kullanmayan algoritmalar da bulunmaktadır. Bu algoritmalar genel olarak bir sistemde yalnız olarak kullanılmazlar. Sistemde bulunan simetrik ve asimetrik diğer algoritmalara yardımcı olmak için yapılmışlardır. Özet fonksiyonu (Hash Functions) adı verilen algoritma en çok tercih edilendir. Bütünlük denetiminde ve güvenli şifre saklama işlemlerinde oldukça kullanılır. Bununla birlikte sayısal imza uygulamalarında asimetirik şifreleme kullanmak uygulamanın oldukça yavaş çalışmasına neden olmaktadır. Bu yüzden bu tür uygulamalarda özet fonkisyonları da kullanmak hız problemini azaltmaktadır. [20]

#### 4.3.3.1. MD5 (Message-Digest algorithm 5)

Algoritma 1991 yılında Ron Rivest tarafından MD4 algoritması yerine geliştirilmiştir. MD5 günümüzde en çok kullanılan şifreleme özet fonksiyonlarından biridir. Algoritmanın güvenlik açıkları nedeni ile kullanımı azalmaya başlamaktadır. Algoritmaya verilen verinin boyutundan bağımsız olarak, 128-bit özet değeri vermektedir. MD5 sadece mesaj doğrulama işi yapmaktadır veri şifreleme özelliği bulunmamaktadır. Algoritmadan çıkan 128 bitlik mesaj özet değeri ile verinin aktarım sırasında değişikliğe uğrayıp uğramadığı kontrol edilir.

#### 4.3.3.2. SHA (Secure Hash Algorithms)

Güvenli karma algoritmaları ailesi içinde, bu araçların daha iyi dijital güvenlik sağlamak için kurulmuş birkaç örneği vardır. Birincisi, SHA-0, 1993 yılında geliştirildi. Halefi gibi, SHA-1, SHA-0 16-bit karma özelliğine sahiptir.

Sonraki güvenli karma algoritması, SHA-2, sırasıyla 256-bit ve 512-bit teknolojileri ile iki fonksiyon kümesini içerir. Ayrıca, kimlerin siber güvenlik için yeni bir algoritma tasarlayabileceğini görmek için kalabalık kaynak yarışmasından geliştirilen SHA-3 veya "Keccak" olarak bilinen en üst düzey bir güvenli hash algoritması da vardır.

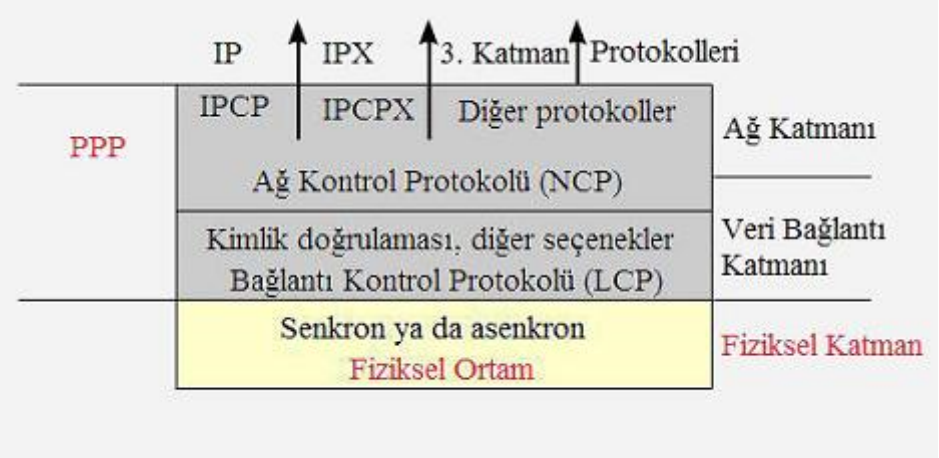
Bu güvenli hash algoritmalarının hepsi, hassas verileri güvenli tutmak ve farklı saldırı türlerini önlemek için yeni şifreleme standartlarının bir parçasıdır. Bunların bir kısmı Ulusal Güvenlik Ajansı gibi kurumlar tarafından geliştirilmiş olmasına ve bazıları bağımsız geliştiriciler tarafından geliştirilmiş olmasına rağmen, hepsi belirli veri tabanı ve ağ senaryolarında verileri koruyan karma şifrelemenin genel işlevleri ile ilişkili olup, dijital çağda siber güvenliği geliştirmeye yardımcı olmaktadır. [22]

# 5. SANAL ÖZEL AĞ PROTOKOLLERİ

## 5.1. Noktadan Noktaya Protokolü (PPP)

Veri Bağlama Katmanı protokolü olan PPP, iki nokta arasında çift yönlü iletişim sağlamaktadır. PPP Protokolü, SLIP protokolünün sıkıştırma ve düzenleme özelliklerinin geliştirilmesi sonucu ortaya çıkmıştır. Her iki protokol de modem veya başka bir ağ cihazı ile seri bağlantı kurabilir. Bu protokollerden PPP standart bir İnternet protokolü iken, SLIP protokolü standart bir protokol değildir. PPP protokolünün veri sıkıştırma, kimlik denetleme, adresleme ve hata düzeltme özellikleri ile günümüzde kullanımı devam etmektedir. PPP, SLIP' in tersine asenkron hatlara ek olarak senkron hatlar ile de çalışmaktadır.

PPP, Bağlantı Kontrol Protokolü ve Ağ Kontrol Protokolü olmak üzere iki alt protokolden oluşmaktadır.




**Şekil 7:** PPP Yapısı. [27]

### 5.1.1. Bağlantı Kontrol Protokolü (LCP)

PPP bağlantılarının kurulması, yapılandırması ve test edilmesi Bağlantı Kontrol Protokolü (LCP) tarafından sağlanır.

LCP protokolü:

- Bağlı cihazın kimliğini denetler ve cihazı kabul eder veya reddeder
- İletim için kabul edilebilir paket boyutunu belirler

- Yapılandırmada hatalar arar
- Gereksinimler parametreleri aşarsa bağlantıyı sonlandırabilir

LCP paketinin bağlantı kabul edilebilirliğini belirleyene kadar aygıtlar bir ağ üzerinden veri iletmek için PPP kullanamaz, ancak LCP paketleri PPP paketlerine gömülür ve bu nedenle LCP yeniden yapılandırmadan önce bir temel PPP bağlantısı kurulmalıdır. PPP paketleri üzerindeki LCP, kontrol kodu 0xC021'e sahiptir ve bilgi alanı, dört alana (Code, ID, Length ve Data) sahip olan LCP paketini içerir. [27]

### 5.1.2. Ağ Kontrol Protokolü (NCP)

Günümüzde ağ protokollerinin kullanımı sonucu birçok problem meydana gelmektedir. PPP ile bu ağ protokollerinin kullanımı mevcut sorunları daha da içinden çıkılmaz hale getirmektedir. PPP bu problemleri çözmek için ağ kontrol protokollerini kullanır. PPP ile kullanılan bağlantı üzerinde birden çok ağ katmanı protokolünün çalışmasına olanak sağlar. Çalışan her Ağ katmanı protokolü için, PPP ayrı bir NCP kullanır.

### 5.1.3. PPP Bağlantı Kurma

**Bağlı olmama durumu (Dead Link):** Bu durum, iki nokta arasında kurulan bağlantının herhangi bir sorundan dolayı kopması sonucu yada taraflardan birinin bağlantıyı sonlandırması ile ortaya çıkan durumdur. [28]

**Bağlantının kurulması durumu (Link Establishment):** Bu durum, iki nokta arasındaki kurulacak bağlantının başarı ile kurulduğunu, bağlantı onayı istenip istenmemesine göre bir sonraki adıma geçişin yapıldığı bölümdür

**Bağlantı onayı (Authenticate):** Bu kısım ise isteğe bağlıdır. PPP' nin doğrulama özelliği açık ise bağlantı yapmak isteyen kullanıcıların kimlikleri kontrol edilir. Kullanıcının bağlantı izni var ise bir sonraki adıma geçilir.

**Bağlantının sonlandırılması (Link Termination Phase):** Bu bölümde ise iki nokta arasında sağlanan bağlantı herhangi bir hata olması, kimlik doğrulama ihlali veya herhangi bir tarafın bağlantıyı sonlandırmayı istemesi durumunda bağlantıyı sonlandıran kısımdır.

### 5.1.4. PPP Kimlik Doğrulama Yöntemleri

PPP'nin Kimlik Doğrulama Aşamasında kullanılan PAP (Şifre Doğrulama Protokolü) ve CHAP (Sorun Çözme Kimlik Doğrulaması Protokolü) olmak üzere iki farklı kimlik doğrulama yöntemi bulunmaktadır.

#### 5.1.4.1. Şifre Doğrulama Protokülü (PAP-Password Authentication Protocol)

PAP çok basit bir kimlik doğrulama protokolüdür. Sunucuya erişmek isteyen istemci, kullanıcı adını ve şifresini açık metin olarak gönderir. Sunucu, kullanıcı adı ve parolanın geçerliliğini kontrol eder ve bağlantı kabul eder veya reddeder. Buna iki yönlü el sıkışma denir. PAP çift yönlü el sıkışma işleminde, kullanıcı adı ve parola ilk iletide gönderilir.

Daha fazla güvenlik gerektiren sistemler için, üçüncü taraf olarak PAP yeterli değildir, bu bağlantıya kolayca erişerek parolayı kolayca alabilir ve sistem kaynaklarına erişebilir. [29]

#### 5.1.4.2. Sorun Çözme Kimlik Doğrulaması Protokolü (CHAP)

CHAP, istemcilerin kimliğini periyodik olarak doğrulamak için kullanılan bir kimlik doğrulama protokolüdür. CHAP, kullanıcıların kimliğini doğrulamak için internet erişim sağlayıcıları tarafından kullanılır.

CHAP 3 yollu bir el sıkışma prosedürü kullanarak istemcinin kimliğini doğrular.

Kimlik doğrulama aracı (genellikle bir ağ sunucusu) istemciye bir "sorun" mesajı gönderir. Bu mesajlar rastgele bir sayı ve bir kimlik değeri içerir.

İstemci, bu mesajı, bir karma değerini hesaplamak için paylaşılan bir şifre ile (genellikle kullanıcı adı ve şifresi) birlikte kullanır.

Kimlik doğrulayıcı, yanıtı beklenen karma değerin kendi hesaplamasına karşı denetler. Değerler eşleşirse, kimlik doğrulama kabul edilir; aksi halde bağlantı sonlandırılmalıdır. Bu yöntem, bağlantı kurulduktan sonra rastgele aralıklarla tekrarlanabilir.

Bu protokolü kullanarak, kullanıcı adı ve şifre, bilgisayar korsanlarına veya diğer davetsiz misafirlere karşı şifrelenmiş bir biçimde iletilir. [30]

### 5.2. Noktadan Noktaya Tünel Protokolü (PPTP)

OSI modelinin 2. Katmanında çalışan bir istemci-sunucu tasarımı kullanan, TCP / IP tabanlı veri ağlarında sanal özel ağ oluşturarak uzak bir istemciden uzak bir sunucuya verilerin güvenli bir şekilde aktarılmasını sağlayan bir ağ protokolüdür. Bir PPTP tüneli, 1723 TCP bağlantı noktasını kullanarak iletişimi sağlar.

Günümüzde PPTP'nin en popüler ve yaygın olarak kullanılan VPN protokollerinden biri olmasının birçok nedeni vardır. PPTP Windows tarafından desteklenen ilk VPN protokolü olması ve 1995'ten buyana her Microsoft Windows işletim sistemi bu protokolü desteklemesi en büyük etkenlerden birisidir. Windows dışında, Linux ve OS X gibi işletim sistemleri de bu protokolü desteklemeye başladı. Günümüzde hemen hemen her masaüstü ve mobil platform PPTP'yi desteklemektedir.

Genellikle, her PPTP dağıtımında üç bilgisayar vardır:

- Bir PPTP istemcisi
- Bir ağ erişim sunucusu
- Bir PPTP sunucusu

PPTP, kimlik doğrulama, şifreleme ve PPP'yi kullanır. Bu protokol, LAN veya WAN üzerinden güvenli iletişim sağlayan bir tünel oluşturarak verileri şifreler ve paket haline getirir. Bu verilerin, şifrelenme, kimlik doğrulama ve kapsüllenmeyi kullandığı için, verileri internet gibi kamu ağları üzerinden bile iletmek güvenlidir. PPTP'nin kullandığı iki tünel yöntemi vardır.

Kullanıcı tarafından başlatılan tünel tipine gönüllü tünel oluşturma, sunucu tarafından başlatılan tünel tine zorunlu tünelleme denir. Gönüllü Tünel, köprüler, yönlendiriciler gibi ağ aygıtları gerektirmez. Öte yandan, Zorunlu Tünel, yönlendiriciler tarafından desteklenmeli ve sunucu tarafından başlatılmalıdır.

Ağ üzerinde aktarım gerçekleştirdiğinde PPP çerçeveleri, IP datagramları içerisinde kapsüller.

Tünel yönetimi için GRE (Generic Routing Encapsulation) (Genel Yönlendirme Kapsülleme) değiştirilmiş sürümünü kullanmaktadır. Aynı zamanda kapsüllenen PPP çerçeveleri sıkıştırılabilir ve şifrelenebilir.

PPTP tüneli kurulduktan sonra, kullanıcı verileri istemci ve PPTP sunucusu arasında iletilir. Veriler, PPP paketleri içeren IP datagramlarında iletilir. IP veri birimleri,

Internet Genel Yönlendirme Kapsülleme (GRE) protokolünün değiştirilmiş bir sürümünü kullanarak oluşturulmuştur. IP teslimat başlığı, datagramın İnternet'i dolaştırması için gerekli bilgileri sağlar. GRE başlığı, IP veri ağında PPP paketini kapsüllemek için kullanılır. PPP paketi RAS tarafından oluşturulur. PPP paketi şifreli olduğu için anlaşılmaz bir blokdur. IP datagramı engellense bile, verilerin şifresini çözmek neredeyse imkânsızdır.

PPTP filtrelemesi, özel ağdaki PPTP sunucusu, kimliği doğrulanmış kullanıcılardan yalnızca PPTP paketlerini kabul eder ve yönlendirir. Bu önlem, diğer paketlerin PPTP sunucusuna ve ağa girmesini engeller. [23]

PPTP Aşamaları

PPTP protokolü ile oluşturulan iletişim aşağıdaki 3 aşamadan oluşur.

*1-PPP Bağlantısı ve İletişim*: bağlantı kurmak ve veri paketlerini şifrelemek için PPP protokolünü kullanır.

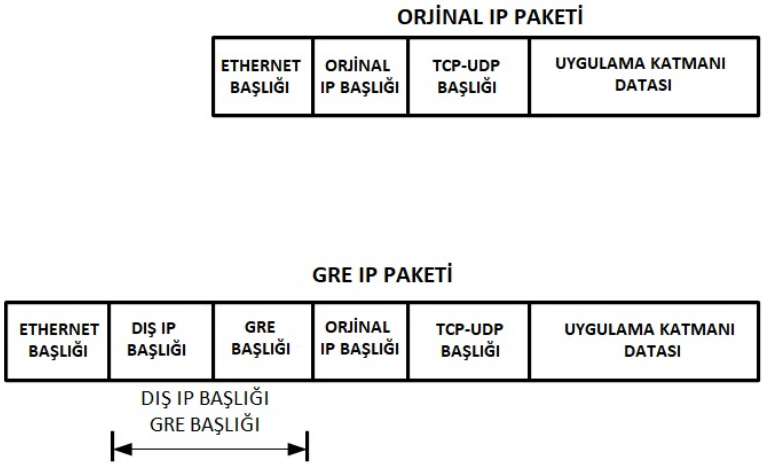
*2-PPTP Denetim Bağlantısı*: PPTP istemcisinden Internet üzerindeki bir PPTP sunucusuna bir denetim bağlantısı oluşturur.

*3-PPTP Veri Tünelleme*: PPTP tüneli üzerinden PPTP sunucusuna gönderilen şifreli PPP paketlerini içeren veri dizelerini oluşturur.

### 5.2.1. Genel Yönlendirme Kapsülleme (GRE-Generic Routing Encapsulation)

Genel yönlendirme kapsülleme (GRE), bir ağ üzerinden IP paketlerini taşımak için kullanılan IP kapsülleme protokolüdür. Genel yönlendirme kapsüllemesi (GRE) başlangıçta Cisco tarafından geliştirildi, ancak daha sonra endüstri standardı haline geldi. GRE, IP de dahil olmak üzere herhangi bir Katman 3 protokolünü tünelleyebilir. GRE 'de, bir IP datagramı başka bir IP veri ağında tünellenir (kapsüllenir).

GRE'nin bir avantajı, genel IPv4 internet üzerinden ayrılmış özel IPv4 ağları arasında IP paketlerinin yönlendirilmesine izin vermesidir. GRE, IPv4 yayınını ve çok noktaya yayın trafiğini kapsüllemeyi de desteklemektedir. GRE tünelleri güvenli değildir, çünkü Genel yönlendirme kapsüllemesi veri yükünü şifrelemez. Gerçek zamanlı olarak ağ güvenliğini sağlamak için IPSec gibi diğer güvenli tünel protokolleriyle birlikte kullanılır. [31]




**Şekil 8:** GRE Kapsüllemesi

### 5.2.2. Microsoft Karşılıklı Kimlik Doğrulama Protokolü (MS-CHAP)

MS-CHAP, şifre bilgilerini endüstri standardı MD5 tek yönlü şifreleme yöntemini kullanarak bir PPP bağlantısı üzerinden iletmeden önce şifreleyen Challenge Handshake Authentication Protocol'a (CHAP) benzer. MS-CHAP, Microsoft'un CHAP sürümünü; CHAP'tan aşağıdaki şekillerde farklılık gösterir:

- MS-CHAP kimlik sorma tepki paketi, Windows platformları için özel olarak tasarlanmış bir biçimde yer almaktadır.
- MS-CHAP, CHAP'in yaptığı şekilde düz metin veya geri dönüşümlü şifrelenmiş parolalar gerektirmez. Bunun yerine, RAS sunucusu, zorlama yanıtı doğrulamak için parola MD4 karmasını kullanır.

Hem istemci hem de kimlik doğrulama sunucusu, veri şifrelemesi için bağımsız başlangıç tuşları üretir. Örneğin, Windows NT RAS sunucusu ve Windows çevirmeli ağ istemcisi arasında bir PPP oturumu oluşturmak için, istemci önce RAS sunucusundan kimlik doğrulama isteğinde bulunur. RAS sunucusu daha sonra istemciye bir oturum tanımlayıcısından ve zorlama dizgesi adı verilen keyfi bir karakter dizesinden oluşan bir soruyu gönderir. İstemci, kullanıcı adına, parola, oturum tanımlayıcısı ve sorun dizesinin tek yönlü şifrelemesinden oluşan bir yanıt gönderir. RAS sunucusu yanıtı inceler ve istemcinin kimlik doğrulamasını belirler. [32]

### 5.2.3. Microsoft Noktadan Noktaya Şifreleme (MPPE)

Microsoft Noktadan Noktaya Şifreleme (MPPE), Noktadan Noktaya İletişim Kuralı (PPP) tabanlı çevirmeli bağlantılar veya Noktadan Noktaya Tünel Protokolü (PPTP) sanal özel ağ (VPN) bağlantılarındaki verileri şifreler. 128-bit anahtar (güçlü), 56-bit anahtar ve 40-bit anahtar (standart) MPPE şifreleme şemaları desteklenmektedir. MPPE, VPN istemcisi ve VPN sunucusu arasındaki PPTP bağlantısı için veri güvenliği sağlar.

MPPE tek başına veri sıkıştırmaz veya genişletmez, ancak protokol genellikle PPP veya VPN bağlantılarında verileri sıkıştıran Microsoft Noktadan Noktaya Sıkıştırma ile birlikte kullanılır.

MPPE anlaşması, PPP'nin bir alt protokolü olan Sıkıştırma Kontrol Protokolü'nde (CCP) gerçekleşir. Bu, bir sıkıştırma protokolü olduğuna dair yanlış inançlara neden olabilir. [35]

### 5.2.4. Genişletilebilir Kimlik Doğrulama Protokolü (EAP)

Genişletilebilir Kimlik Doğrulama Protokolü (EAP), kimlik doğrulama protokolünün kendisi yerine, kimlik doğrulama protokollerini taşımak için bir çerçeve olarak düşünülür. EAP, çevirmeli bağlantı ve VPN bağlantılarını doğrulamak için ve ayrıca IEEE 802.1X ile birlikte Yerel Alan Ağı (LAN) bağlantı noktalarını doğrulamak için kullanılabilir.

EAP 'de, kimlik doğrulama belgesi isteyen tarafa kimliği doğrulayıcı, kimliği doğrulanan tarafa da istemci adı verilir. EAP, dört paket türünü tanımlar: istek, yanıt, başarı ve başarısızlık. İstek paketleri kimliği doğrulayan tarafından verilir ve istek sahibi tarafından bir yanıt paketi istemektedir. Kimlik doğrulama işlemini tamamlamak için herhangi bir sayıdaki istek-yanıt değişimi kullanılabilir. Kimlik doğrulama başarılı olursa, başvuru sahibine bir başarı paketi gönderilir; değilse bir hata paketi gönderilir.

#### 5.2.4.1. EAP Türleri TLS, TTLS ve PEAP

TLS EAP türü, verileri şifrelemek için kullanılabilecek anahtarların kimlik doğrulamasında ve görüşülmesinde açık anahtar şifrelemesini kullanan Aktarım Katmanı Güvenliği (TLS) protokolünü temel alır. TLS ayrıca HTTPS'yi güvence altına almak için kullanılan protokoldür. Temel fark, HTTPS'nin TCP üzerinden taşınması ve EAP TLS'in istemci ve EAP sunucusu arasındaki EAP oturumu üzerinden taşınmasıdır. HTTPS'deki gibi, istekte bulunan yerel olarak depolanan bir kök sertifika kullanarak sunucunun kimliğini doğrulamaktadır. Bununla birlikte, çoğu HTTPS işleminden farklı olarak, EAP TLS istemciyi sunucuya doğrulamak için bir kullanıcı sertifikası kullanır.

Bu, TLS'in yalnızca kullanıcı sertifikaları yayınlayan bir Sertifika Yetkilisi (CA) olan kuruluşlar tarafından kullanılabileceği anlamına gelir; Bu nedenle, mükemmel bir güvenlik sunmasına rağmen yaygın şekilde konuşlandırılamaz. Bunun yerine, iki başka EAP türü olan Korumalı EAP (PEAP) ve Tünel TLS (TTLS) bu soruna geçici bir çözüm getirmektedir. Bu türlerin her ikisi de sunucu kimlik doğrulaması ve şifreleme için TLS kullanır, ancak istemci ile sunucu arasında TLS şifrelemesi ile korunan ikinci bir kimlik doğrulama protokolünü kullanarak kullanıcı sertifikalarına duyulan gereksinimden kaçınılmalıdır. Bu, kullanıcının düz metin kimlik bilgilerinin TLS tarafından korunduğu geleneksel HTTPS kimlik doğrulamasına çok benzemektedir. Türler arasındaki en büyük fark, PEAP'in yalnızca diğer EAP türlerini koruyabilmesidir; oysa TTLS hemen hemen tüm kimlik doğrulama protokollerini koruyabilir. [36]

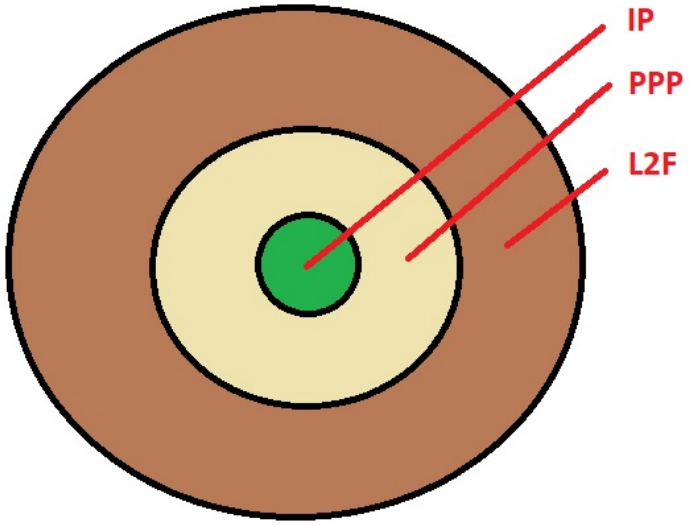
### 5.3. Katman 2 Tünel Protokolü (L2TP)

İkinci katman tünelleme Protokolü, Cisco tarafından geliştirilmiş protokol trafiğinin şifrelenmesi ve sonrada noktadan noktaya veri transferi teslimini destekleyen bir tünelleme protokolüdür. Kendi içinde hiçbir gizlilik ya da şifreleme içermez; tunnel yapısı ile bilgi transferi sağlayan ipsec protokolünden faydalanır. UDP 500 portunu kullandığı için güvenlik duvarı ile bazen sorunlar yaşayabilmektedir. L2TP, PPTP ve L2F'nin birleşmesi ile oluşmuş ve bu iki protokolün en iyi özelliklerini kendisinde toplamıştır. L2TP, şifreleme için İnternet Protokolü (IPSec) güvenliği ESP (Encapsulating Security Payload) kullanır.

L2TP paketlerinin kapsüllenmesi iki katmandan oluşmaktadır. Birinci katman, PPP çerçevesi L2TP ve UDP üstbilgisiyle kapsüllenir. İkinci katman ise IPSec kimlik doğrulama altbilgisi ve IP üstbilgisiyle kapsüllenir. IP üstbilgisinde VPN server IP adresi bulunmaktadır.

### 5.4. Katman 2 Yönlendirme Protokolü (L2F)

L2F protokolü, Cisco, Nortel ve Shiva firmaları tarafından geliştirilmiş, geliştirici bağımlı bir protokoldür. L2F protokolü, RAS ve ağ yönlendiricileri gibi ağ bağlantı cihazları arasında tünel kurulumunu sağlamaktadır. PPTP tarafından desteklenen birçok protokol L2F tarafından da desteklenmektedir, fakat PPTP bir yazılım çözümü iken L2F bir donanım çözümüdür. PPTP, ağ katmanında yalnızca IP'yi desteklerken, L2F protokolü ise PPTP'nin desteklemediği ağ katmanı protokollerinide desteklemektedir. L2F kapsülleme için GRE'yi kullanmaz. L2F tüneli kurulur iken, taraflar, birbirlerinin güvenilirliği için CHAP/PAP kullanılır. [37]

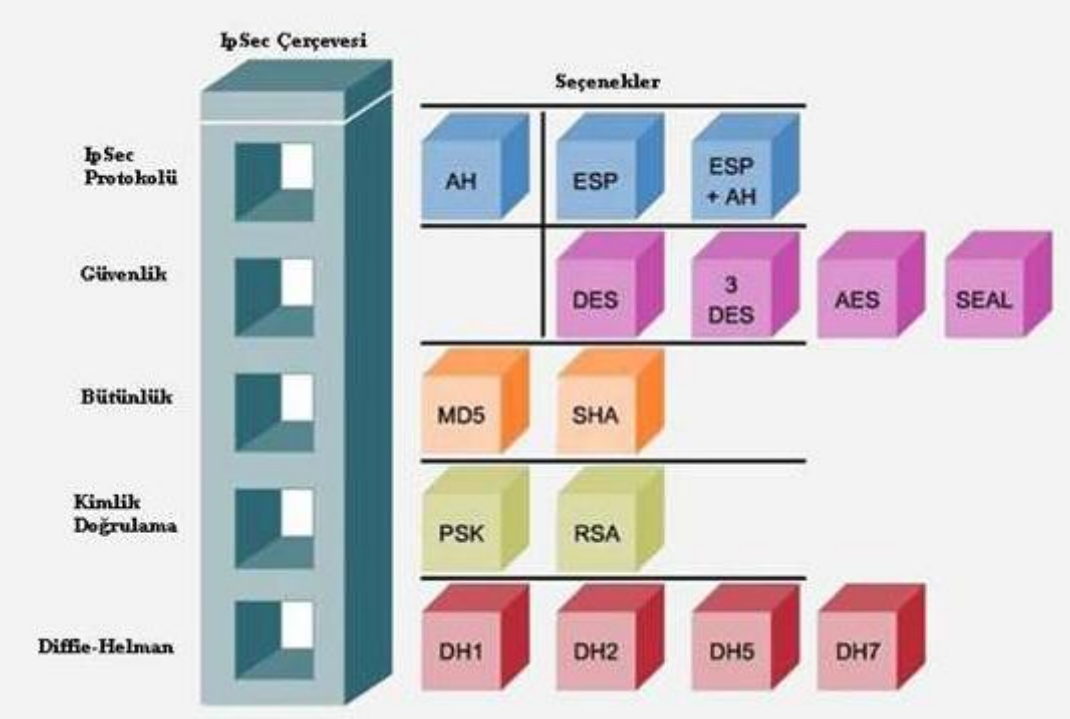



**Şekil 9:** L2F Yapısı

### 5.5. İnternet Protokolü Güvenliği (IPSec)

IPSec, şifreleme ve güvenlik özellikleri sayesinde, IP protokolünün güvenliğini sağlamak için IETF tarafından geliştirilmiş bir şifreleme ve güvenlik protokolüdür. IPSec ağ katmanında çalışarak uygulamalardan bağımsız bir şekilde verileri şifreler ve şifreleme sonrası oluşturduğu başlık ile verinin güvenli bir şekilde İnternette yolculuk edebilmesini sağlar.

IPSec protokolü uygulama katmanında çalıştığı için diğer güvenlik protokollerinden daha esnek ve üstün performans sağlamaktadır.




**Şekil 10:** IPSec çerçevesi [24]

IPSec 5 bölümden meydana gelmektedir.

- İlk bölüm IPSec yer alır. ESP ve AH protokolleri bulunur.
- İkinci bölümde ise güvenlik ve gizlilik şifreleme algoritmaları yer alır.
- Üçüncü bölümde, MD5 veya SHA algoritmaları ile doğrulama yapılmaktadır.
- Dördüncü bölümde PSK ve RSA gibi kimlik doğrulama denetimlerini yapılır.
- Son bölümde ise Diffie-Hellman algoritmaları yer alır.

### 5.5.1. IPSec Protokolleri

#### 5.5.1.1. Kimlik Denetimi Başlığı (AH)

Kimlik Doğrulama Üstbilgisi (AH) protokolü, veri kökenli kimlik doğrulama, veri bütünlüğü ve tekrar koruma sağlar. Bununla birlikte, AH veri gizliliğini sağlamaz, bu da tüm verilerinizin açık olarak gönderildiğini gösterir.

AH, MD5 gibi bir ileti doğrulama kodunun ürettiği sağlama toplamıyla veri bütünlüğünü sağlar. Veri kökenli kimlik doğrulamasını sağlamak için AH, kimlik doğrulama için kullandığı algoritmada gizli bir paylaşım anahtarı içerir. Çalma korumasını sağlamak için, AH, AH başlığı içerisinde bir sıra numarası alanı kullanır. Burada dikkati çeken nokta, bu üç farklı işlevin birlikte toplanması ve kimlik doğrulama olarak geçmesidir. En basit ifadeyle, AH, verilerinizin son hedefe giden yolda değiştirilmemesini sağlar.

AH, mümkün olduğunca IP datagramının çoğunu doğrulamakla birlikte, IP başlığındaki bazı alanların değerleri alıcı tarafından tahmin edilemez. AH değiştirilebilir alanlar olarak bilinen bu alanları korumaz. Bununla birlikte, AH her zaman IP paketinin yükünü korur.

Çoğu durumda, veriler yalnızca kimlik doğrulaması gerektirir. Encapsulating Security Payload (ESP) protokolü kimlik doğrulama yapabilirken, AH, ESP'de olduğu gibi sistem performansını etkilemez. AH'yi kullanmanın diğer bir avantajı, AH'nin tüm veri ağacının kimliğini doğrulamasıdır. Bununla birlikte, ESP önde gelen IP başlığını veya ESP başlığından önce gelen diğer bilgileri doğrulamaz.

AH iki şekilde uygulayabilir: aktarma modu veya tünel modu. Aktarım modunda, veri ağının IP başlığı en dışındaki IP üstbilgisidir ve onu AH başlığı ve ardından veri ağının yükü takip eder. AH değiştirilebilir alanlar haricinde tüm veri ağacının kimliğini doğrulamaktadır. Bununla birlikte, veri dizisinde bulunan bilgiler net olarak taşınır ve bu nedenle dinlemeye tabi tutulur. Aktarım modu, tünel modundan daha az işlem gerektirir, ancak fazla güvenlik sağlamaz.

Tünel modu, yeni bir IP başlığı oluşturur ve bunu veri ağının en dıştaki IP başlığı olarak kullanır. AH başlığı yeni IP başlığını takip eder. Orijinal datagram (hem IP başlığı hem de orijinal yük) en sonda yer alır. AH tüm datagramın kimliğini doğrular,

bu da yanıt veren sistemin veri grubunun geçiş halindeyken değişip değişmediğini algılayabildiği anlamına gelir.

Bir güvenlik ilişkisinin her iki biti de bir ağ geçidi olduğunda tünel modunu kullanın. Tünel modunda, en dıştaki IP üstbilgisindeki kaynak ve hedef adreslerin, orijinal IP başlığında olanlar ile aynı olması gerekmez. Örneğin, iki güvenlik geçidi birbirine bağlanan ağlar arasındaki tüm trafiğin kimliğini doğrulamak için AH tünelini çalıştırabilir.

Tünel modunu kullanmanın temel avantajı, tünel modunun, kapsüllenmiş IP veri ağını tamamen koruduğudur. Buna ek olarak, tünel modu özel adresleri kullanmayı mümkün kılar. [25]

#### 5.5.1.2. Kapsüllenen Güvenlik Yükü (ESP)

ESP, IPSec bağlantılarının kurulması esnasında izinsiz girişleri engelleyerek, ağ dinleme işlemlerinde güvenlik sağlar. Sistemde açık bulunan portları, kontrol ederek zararlı yazılımların sisteme zarar vermesini engeller.

ESP iki şekilde uygulanabilir: aktarım modu veya tünel modu. Aktarım modunda, ESP başlığı orijinal IP veri ağının IP başlığını takip eder. Veri dizisi zaten bir IPSec üstbilgisi varsa, ESP üstbilgisi önce gelir. ESP römorku ve isteğe bağlı kimlik doğrulama verileri yükü takip eder.

Aktarım modu, IP başlığını kimlik doğrulaması yapmaz veya şifrelemez; bu, veri dizisi geçiş halindeyken adres bilgilerini potansiyel saldırganlara gösterebilir. Aktarım modu, tünel modundan daha az işlem gerektirir, ancak fazla güvenlik sağlamaz. Çoğu durumda, ana bilgisayarlar taşıma modunda ESP kullanır.

Tünel modu, yeni bir IP üstbilgisi oluşturur ve onu veri paketinin en dışındaki IP başlığı olarak kullanır, ardından ESP başlığı ve daha sonra orijinal veri birimi (hem IP başlığı hem de orijinal yükü) izler. ESP römorku ve isteğe bağlı kimlik doğrulama verileri yüke eklenir. Hem şifreleme hem de kimlik doğrulama kullanıldığında, ESP orijinal veri ağını tamamen korur, buna karşın ESP paketi için yük miktarı verisi ve ESP yeni IP üstbilgisini korumaz. [26]

### 5.6. Güvenli Yuva Tünel Protokolü (SSTP)

Güvenli Yuva Tünel Protokolü (SSTP), trafiklerin PPTP ve L2TP / IPSec trafiğini engelleyen güvenlik duvarlarından geçmesine izin veren tünel protokolüdür. SSTP, HTTPS protokolünün SSL kanalı üzerinden PPP trafiğini kapsüllemesi için bir mekanizma sağlar. PPP'nin kullanılması, EAP-TLS gibi güçlü kimlik doğrulama yöntemleri için destek sağlar. HTTPS kullanımı, TCP 443 bağlantı noktası üzerinden akar ve bu bağlantı genellikle Web erişimi için kullanılan bir bağlantı noktasıdır. Güvenli Yuva Katmanı (SSL), gelişmiş anahtar görüşmesi, şifreleme ve bütünlük denetimi ile taşıma düzeyinde güvenlik sağlar. [32]

SSTP, parolalar, akıllı kartlar, sertifika tabanlı ve "Bir Zamanlı Parola" kimlik doğrulaması gibi birden çok kimlik doğrulama yöntemini destekler. SSTP, kimlik doğrulama ve yetkilendirmede NPS (Ağ İlkesi Sunucusu) kullanılarak istemci sağlığı kontrolü için NAP desteğini entegre etmiştir. [33]

Bu protokol Linux, RouterOS ve SEIL işletim sitemleri için de mevcut olmasına rağmen çoğunlukla Windows tarafından kullanılıyor. SSL el sıkışma gerçekleştiğinde, istemci SSL sertifikası kullanarak sunucuyu doğrular. Başlık 32 bitten oluşur. İlk sekiz bit protokol versiyonuna karşılık gelir, 9-15 bit rezerve edilmiştir, 16. veri (0) veya kontrol paketi (1) olan paketin olup olmadığını belirleyen kontrol bitidir, bitler 17-20 de ayrılmıştır ve Son 12 bit, paket uzunluğunu gösterir. [34]

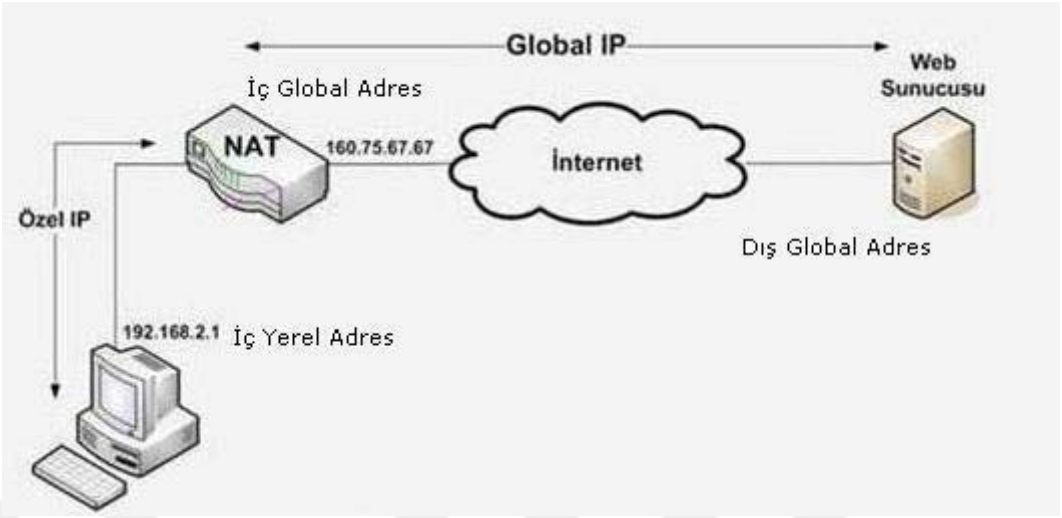
SSTP Çalışma Prensibi

1. SSTP istemcisi, istemcideki dinamik olarak ayrılan bir TCP bağlantı noktası ile sunucu üzerindeki TCP bağlantı noktası 443 arasında SSTP sunucusu ile bir TCP bağlantısı kurar.
2. SSTP istemcisi, istemcinin SSTP sunucusuyla bir SSL oturumu oluşturmak istediğini belirten bir SSL İstemcisi-Merhaba iletisi gönderir.
3. SSTP sunucusu, bilgisayar sertifikasını SSTP istemcisine gönderir.
4. SSTP istemcisi, bilgisayar sertifikasını doğrular, SSL oturumunun şifreleme yöntemini belirler, bir SSL oturum anahtarı oluşturur ve daha sonra SSTP sunucusunun sertifikasının genel anahtarı ile şifreler.

5. SSTP istemcisi SSL oturum anahtarının şifreli biçimini SSTP sunucusuna gönderir.
6. SSTP sunucusu, şifreli SSL oturum anahtarı, bilgisayar sertifikasının özel anahtarı ile çözer. SSTP istemcisi ile SSTP sunucusu arasındaki gelecekte yapılacak olan tüm iletişim anlaşmalı şifreleme yöntemi ve SSL oturum anahtarı ile şifrelenir.
7. SSTP istemcisi, SSTP sunucusuna SSL üzerinden bir HTTP istek iletisi gönderir.
8. SSTP istemcisi, SSTP sunucusu ile bir SSTP tüneli müzakere eder.
9. SSTP istemcisi, SSTP sunucusuyla PPP bağlantısını görüşür. Bu müzakere, kullanıcının kimlik bilgilerini bir PPP kimlik doğrulama yöntemi ile doğrulamak ve IPv4 veya IPv6 trafiği için ayarları yapılandırmak için kullanılır.
10. SSTP istemcisi, PPP bağlantısı üzerinden IPv4 veya IPv6 trafiği göndermeye başlar.

### 5.7. Ağ Adresi Dönüştürme (NAT)

İnternet kullanımı hızla arttığı için IP adresleri (Internet Protocol) sayıca yetersiz kalmaya başlamıştır. Sayı sorununu çözmek için IPv6 protokolü geliştirilmiş, ancak günümüzde kullanımı yaygınlaşmadığı için IPv4 protokolü kullanımı devam etmektedir. IPv4 sürümünün dağıtabileceği IP adresi yetersiz kaldığı için Ağ Adresi Dönüştürme Protokolü (NAT) geliştirilmiştir. NAT kuruma veya kuruluşa ait tek bir dış IP adresini, o kurumdaki bilgisayarlara dağıtarak kurumda bulunan tüm bilgisayarların internette tek bir IP adresi ile çıkışını sağlamaktadır. NAT protokolü ile ağ güvenliğini ve ağa bağlı cihazları yönetme imkânı sağlar.




**Şekil 11:** NAT Yapısı. [38]

NAT, ağ güvenliğinin çok önemli bir parçasıdır. Bir kuruluşta kullanılan genel adreslerin sayısını korur ve güvenlik duvarının her iki tarafındaki kaynaklara erişimi daha sıkı kontrol etmeyi sağlar.

Temel olarak bir NAT yönlendiricisi NAT tablosu adı verilen bir tablo yardımıyla IP çevirme işlemini gerçekleştirir. Kullanıcının bilgisayarında özel IP adresleri aralığından bir adres bulunur. Buradan yerel ağın içinde olmayan bir adrese gitmek için bir talep gelince, NAT yönlendiricisi daha önceden kullanıcının ayarladığı NAT tablosuna bakarak, özel IP adresini genel bir IP adresine çevirir ve bu şekilde dış ağlara ya da İnternete çıkılmış olur. Yönlendiricinin çeviri yaparak değiştirdiği bu IP, kullanıcının İnternetteki bilinen IP'sidir. Aynı şekilde dış ağlardan bu bilinen IP'ye doğru bir istek gelince, yönlendirici tablosuna bakarak bu IP'yi kullanıcın özel IP adresine yönlendirir ve paketi kullanıcının bilgisayarına gönderir. [39]

### 5.7.1. Sabit NAT

Sabit NAT ağda kullanılan yerel IP adresinin internette kullanılacak olan genel IP adresine birebir çevrilmesidir. NAT tablosu sistem yöneticisi tarafından oluşturularak yerel IP adresleri ile genel IP adresleri bu tabloya işlenir. NAT tablosunda olmayan yerel IP internete çıkamaz.

### 5.7.2. Dinamik NAT

Dinamik NAT türünde özel IP adres bloğu, genel IP adres blokları ile NAT yönlendiricisi tarafından otomatik olarak eşleştirilmesidir. Sabit NAT türünden farkı eşleştirmenin yönlendirici tarafından yapılmasıdır. Örneğin elimizde bulunan 10 adet özel IP adresi bulunmaktadır, 10 adet de genel IP adresi bulunmaktadır. Bu adresler yönlendirici tarafından otomatik eşleştirildikten sonra dış ağlara bağlantı sağlanıyor. İlk önce eşleşen IP adresi internete ilk olarak çıkar. Yeterli sayıda genel IP adresi varsa hepsi eşleştirilir. Eğer yeterli sayıda IP adresi yoksa sıra ile eşleştirme yapılır. Bağlantı sona erdiğinde ise NAT tablosundaki kayıtlar silinir.

### 5.7.3. Aşırı Yükleme NAT

Aşırı Yükleme NAT ile genel IP adresine eklenecek port numarası ile yerel ağdaki IP adresine port numarası yardımı ile bağlantı sağlanır. Sistemin çalışmasına Örnek olarak bir kuruma ait 100 bilgisayar var ve bu kurumun sadece 1 adet dış ip adresi bulunmaktadır. Kurumun içerisinde mail sunucusu, dosya sunucusu gibi sunucular bulunmaktadır. Kurum çalışanlarından birisi evinden dosya sunucusuna bağlanmak istediğinde kurumun ip adresini yazdığında ağa bağlanmış olur fakat hangi bilgisayara bağlanacağını bilmez bu kısımda devreye router girer. Router bizim hangi bilgisayara bağlanacağımızı port numarası ile belirleyebilmektedir. Kurumun ağında bulunan her bilgisayara bir port numarası atanabilmektedir. Bu yöntem az sayıda ip adresi bulunan ağlar için adreslerin daha verimli kullanılmasını sağlamaktadır.

### 5.7.4. Değerlendirme

**Avantajları**

- Az sayıda dış IP adresi kullanılarak daha çok kullanıcının internete bağlanmasını sağlamaktadır.
- IPv4'te bulunan IP yetersizliği sorunu azaltılmıştır.
- Yerel ağdaki kullanıcıların dış ağlara yönlendirici tarafından çevrilmiş IP'lerle bağlanması sonucunda etkili bir güvenlik sistemi sağlanmış olur.
- Özel IP adresleri sayesinde yerel ağdaki IP adresleri ve ağ topolojisi korunmaktadır.

- NAT genel ağa olan bağlantıların esneklik derecesini artırır. Çoklu IP havuzları, yedek IP havuzları ve yük dengeleme havuzları güvenilir bir ağ bağlantısı sağlamak için uygulanabilirler.
- NAT tablosu değiştirilerek yerel ağ kullanıcılarının özel IP adresleri maliyetsiz bir şekilde kontrol edilir.

**Dezavantajları**

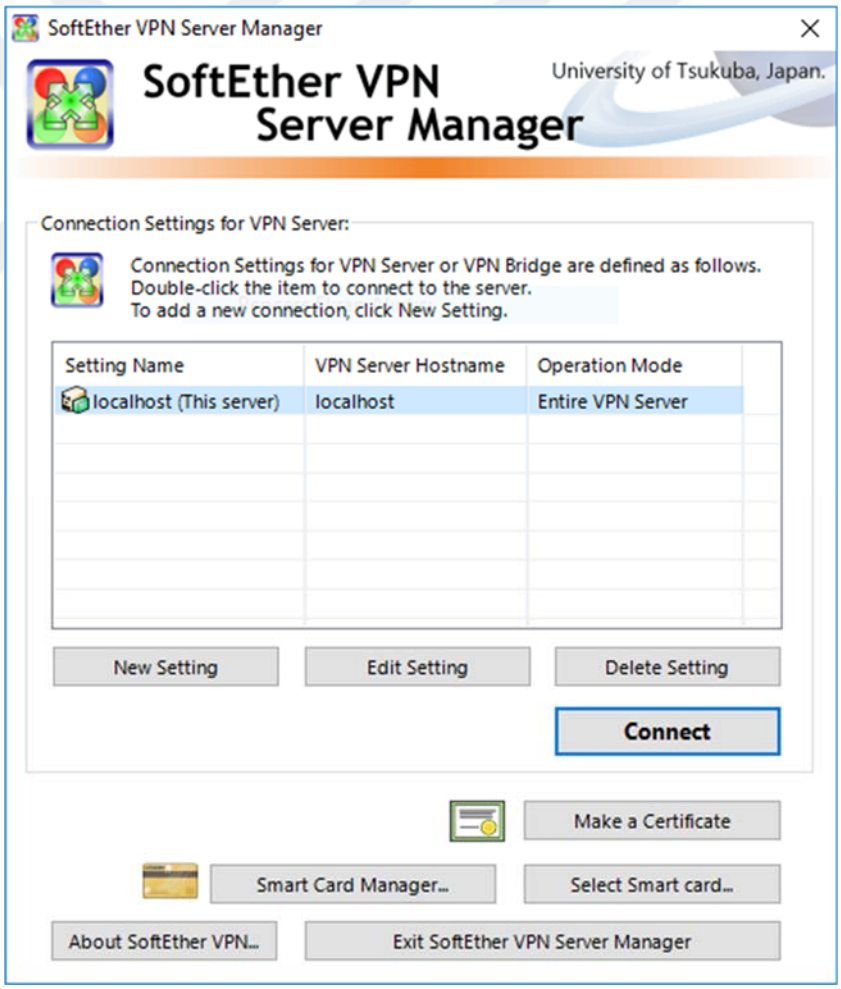
- IP adresi ve port numaraları değişikliği sonucu bazı uygulamalar çalışmayabilir.
- Az sayıda genel IP adresi ile dış bağlantı sağlandığından dolayı IP takibi zorlaşır.
- NAT lar tünel protokollerinin kullanımını karmaşıklaştırır.

## 6. GÜVENLİ SANAL ÖZEL AĞ OLUŞTURMA VE DENEYSEL SONUÇLAR

Bu çalışmada, Daiyuu Nobori' nin Tsukuba Üniversitesi'ndeki master araştırması için geliştirilen açık kaynaklı, çapraz platformlu, birden çok protokolü destekleyebilen VPN istemci ve sunucu yazılımı olan SoftEther uygulaması kullanılmıştır. Bu yazılım, SSL VPN, L2TP / IPSec, OpenVPN ve SSTP gibi VPN protokolleri tek bir VPN sunucusunda sağlayabilmektedir.

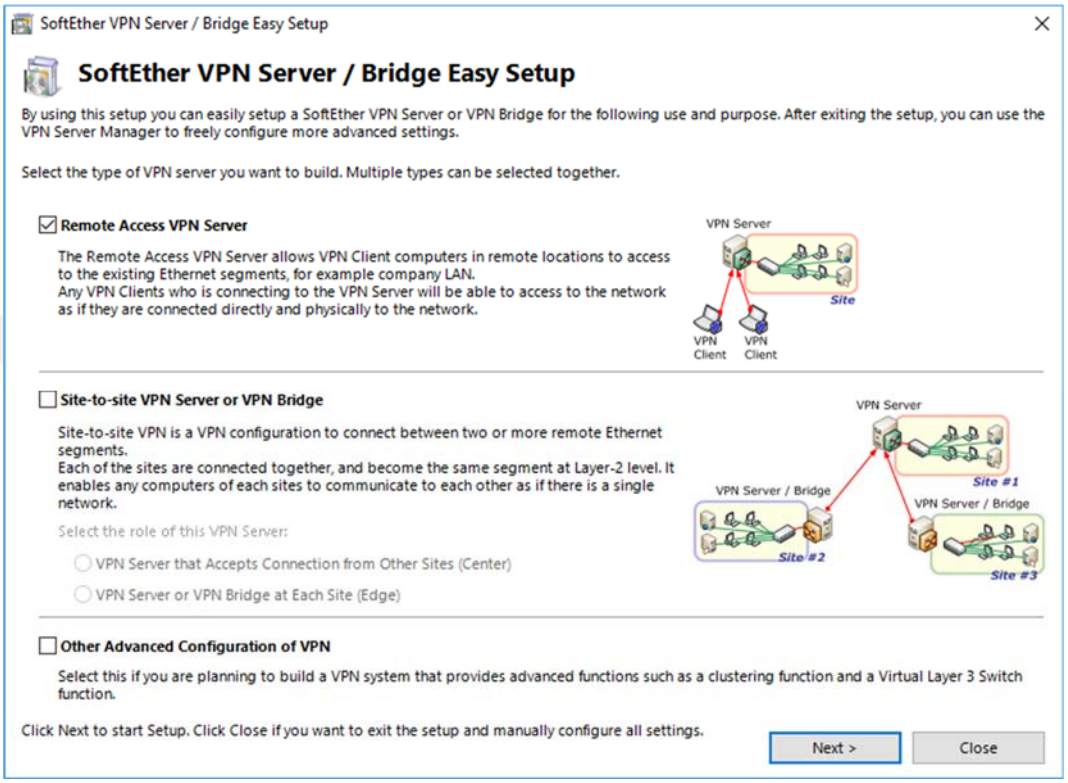
SoftEther uygulaması ile VPN Server Kurulumu yapılıp, istemci üzerinden testler yaparak veri güvenliğini arttırmak için alınması gereken önlemler belirtilmiştir.

Aşağıda bir VPN Server kurulumu için gereken adımlar verilmiştir.



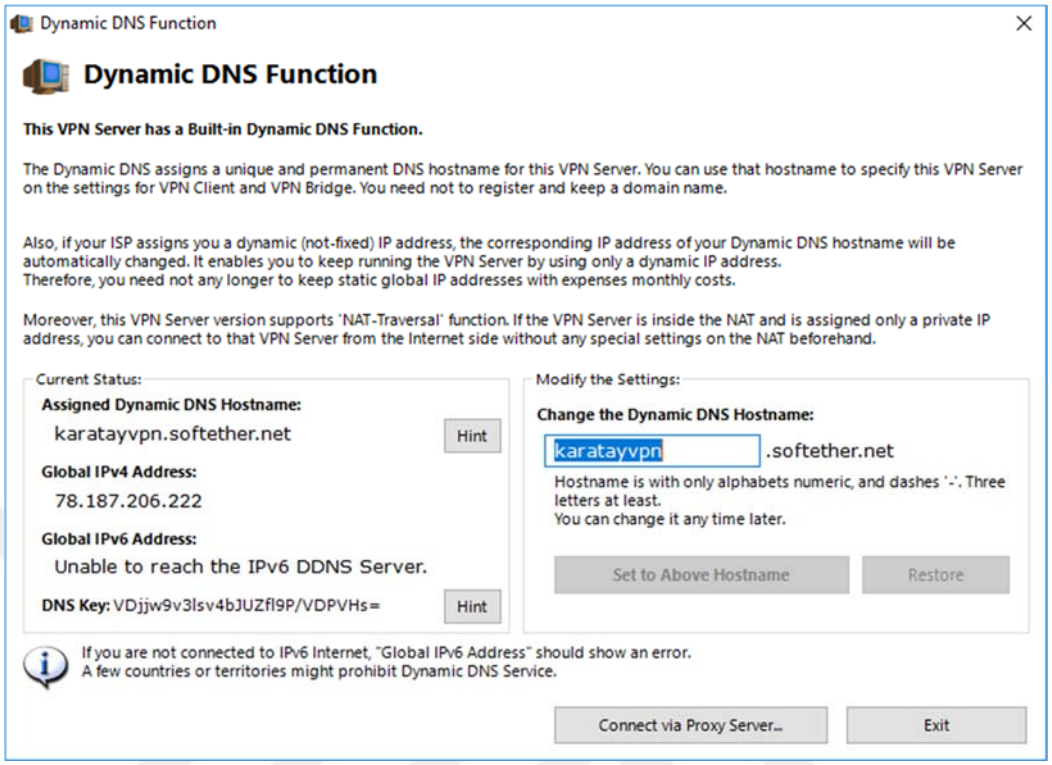

**Şekil 12:** VPN Server Listeleri

Şekil 13'te verilen ekranda VPN Server seçeneği işaretlenir. Çünkü evden veya başka şubesi bulunmayan kurumlar için router veya benzeri aletler olmadan direk VPN sunucuya bağlanma imkânı verdiği için en uygun seçenektir.



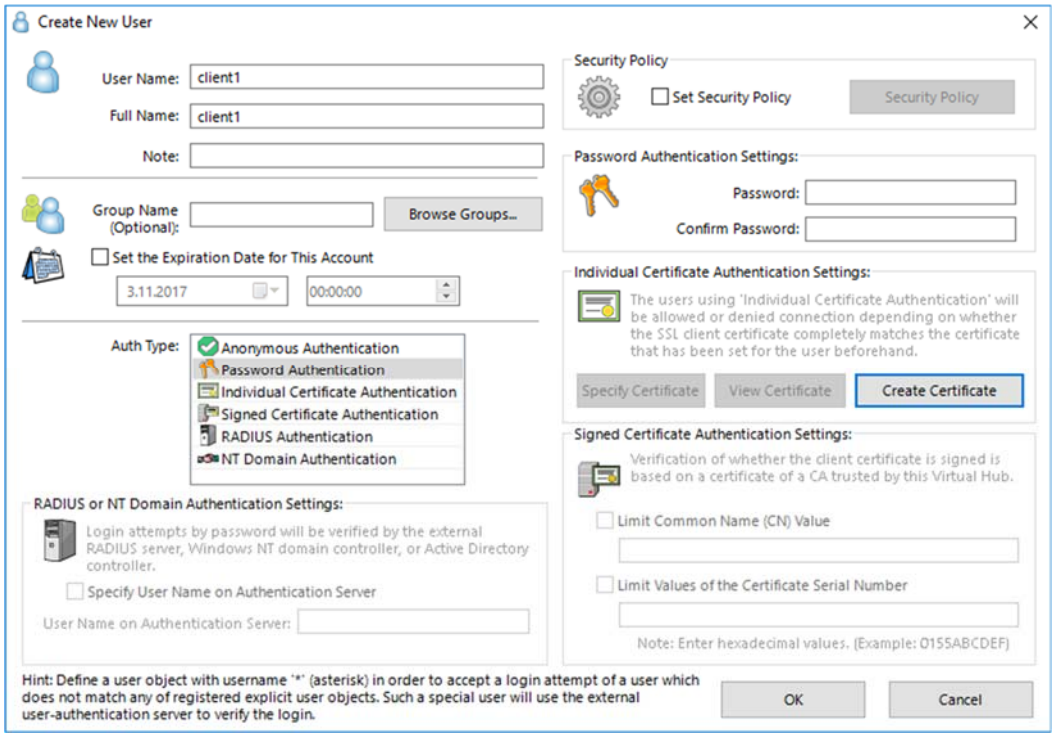

**Şekil 13:** VPN Server Tipi Seçimi

Bu kısımda remote access VPN server seçeneğini işaretlenir. Çünkü evden veya başka şubesi bulunmayan kurumlar için router veya benzeri aletler olmadan direk VPN server' a bağlanma imkânı verdiğinden bizim için en uygun seçenektir.




**Şekil 14:** VPN Server DNS Ayarları.

Şekil 14'te VPN sunucusuna bağlanılabilmek için gerekli ayarlamalar yapılır.




**Şekil 15:** VPN Server Kullanıcı Ayarları.

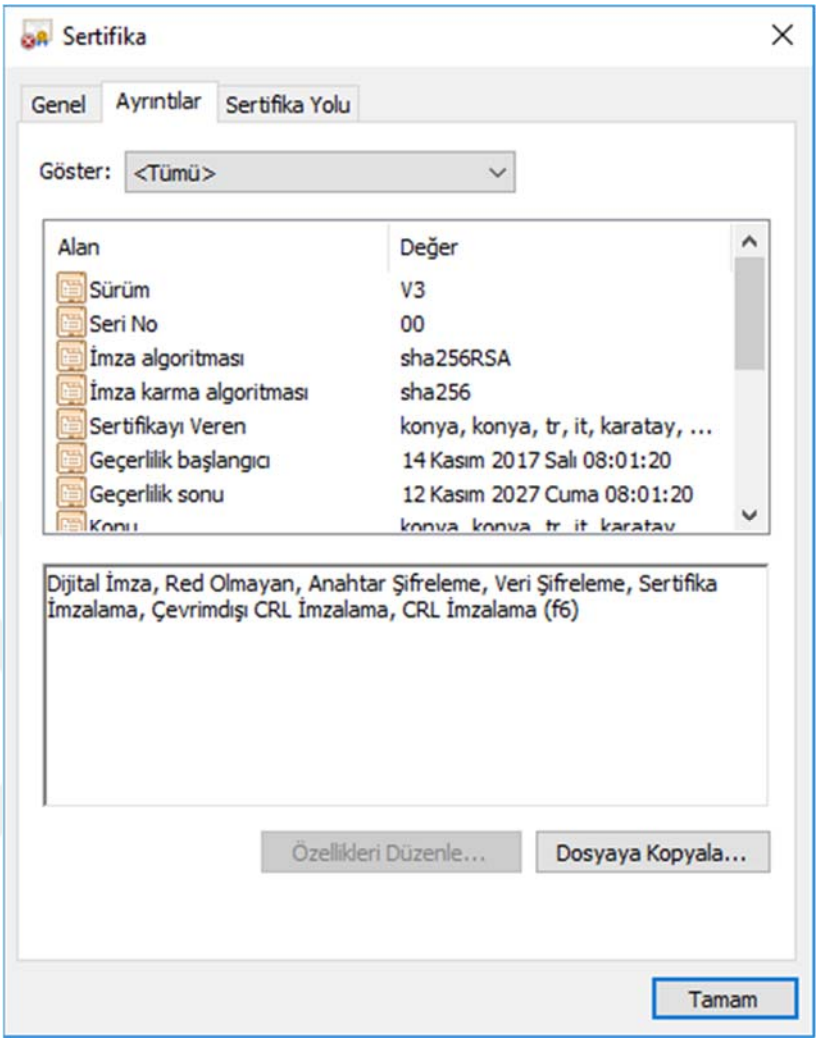
Şekil 15'te verilen ekranda yapılacak ayarlar sanal özel ağ kurulumunun en önemli aşamasını oluşturmaktadır. VPN sunucumuza bağlanacak kullanıcıların ne tür güvenlik önlemlerine tabi tutulacağı bu kısımdan ayarlanır. Genellikle sunuculara bağlanmak için çeşitli kullanıcı doğrulama yöntemleri vardır. Bunlardan en çok kullanılan yöntem ise kullanıcı adı ve şifre ile doğrulama; bu yöntem ile kullanıcının sisteme bağlanabilmesi için sunucu tarafından kullanıcıya verilen id ve şifre ile sisteme girişi sağlanmaktadır. Bu yöntem uygulamada basit ve hızlı olmasına karşın güvenlik yönünden dezavantajları bulunmaktadır. Zayıf şifrelerin kullanılması, kimlik hırsızlığı ve veri ihlallerinin artması sonucunda kullanıcı adı – parola ile doğrulama artık yeterli bir güvenlik denetimi olmadığını göstermektedir. Günümüzde iki faktörlü kimlik doğrulama ile kurumların hassas verilerini koruması zorunlu bir hale gelmiştir.

Bir başka yöntem ise Radius kimlik doğrulama güvenlik sistemidir. Sisteme bağlanacak olan kullanıcıların id – şifreleri Radius sunucuna gönderilir ve sisteme girme yetkileri kontrol edilir. Kullanıcıların erişim süreleri, raporlama ve yetkilendirme gibi işlemlerini de yapmasına karşın güvenlik yönünden zayıf kalmaktadır.

Sertifika tabanlı kimlik doğrulama yöntemi, bir sunucuya Internet üzerinden güvenli bağlantılar oluşturmak için kullanılabilir. Bu yöntem ile yetkisiz erişimler önlenir ve mevcut güvenliği geliştirir. Ek bir donanım (ör. token) gerektirmediği ve her büyüklükteki kuruluşlara uygulanabilir olduğu için uygun maliyetlidir.

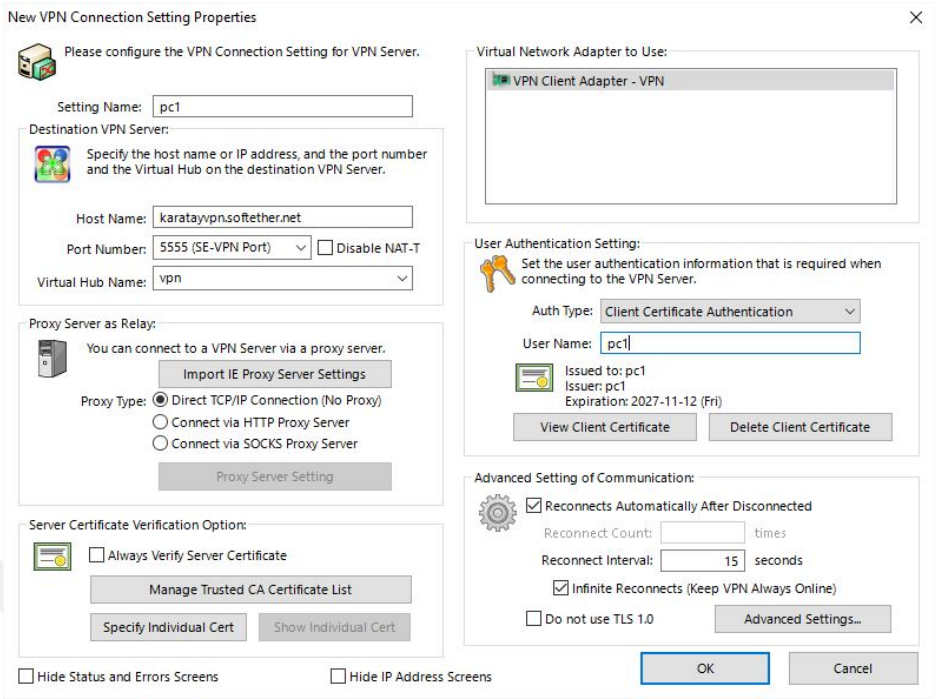
Sertifika tarafından kullanılan açık anahtar ne kadar iyi seçilir ise Kimlik doğrulamanın kalitesi, güvenilirliği ve performansı aynı oranda artmaktadır. Çünkü veriler açık anahtar ile şifrelenip özel anahtar ile açılacağı için verinin şifrelenmesi ne kadar güçlü ise güvenlik o derece yüksektir.

İki çeşit sertifika bulunmaktadır. Bunlardan ilki yerel kaynaklar tarafından üretilen sadece üretilen sistem için güvenli sayılan, özel üretim Sertifikalar. İkincisi ise CA tarafından üretilen küresel ölçekte güvenilir sayılan sertifikalardır.



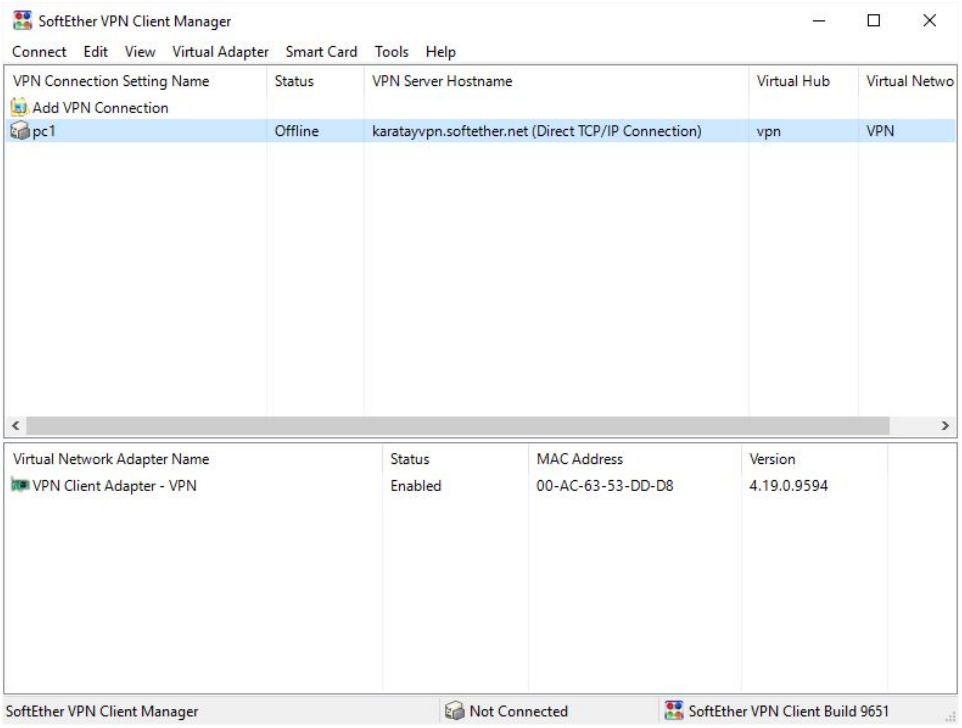

**Şekil 16:** VPN Server Tarafından Oluşturulmuş Özel Doğrulama Sertifikası.

VPN sunucusunu başarılı bir şekilde oluşturduktan ve gerekli ayarlamaları yaptıktan sonra, sunucuya bir bilgisayarı bağlayarak aşağıdaki test işlemleri gerçekleştirilmiştir. İlk olarak sunucu bilgileri girilerek bağlantı sağlanmıştır.



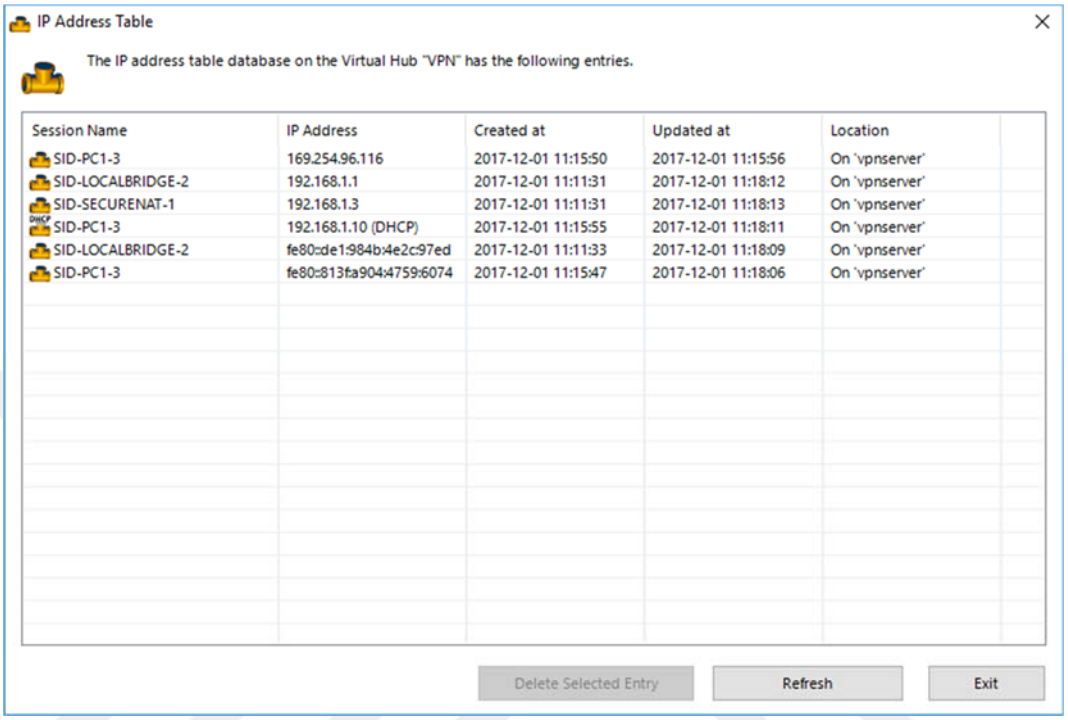

**Şekil 17:** VPN Sunucusuna Bağlantı Ayarları

Bağlantı için 5555 nolu port seçilmiştir. Sunucu tarafından üretilen sertifika ile kullanıcı doğrulaması sağlanmıştır.




**Şekil 18:** VPN Sunucusuna Bağlantı Kısmı

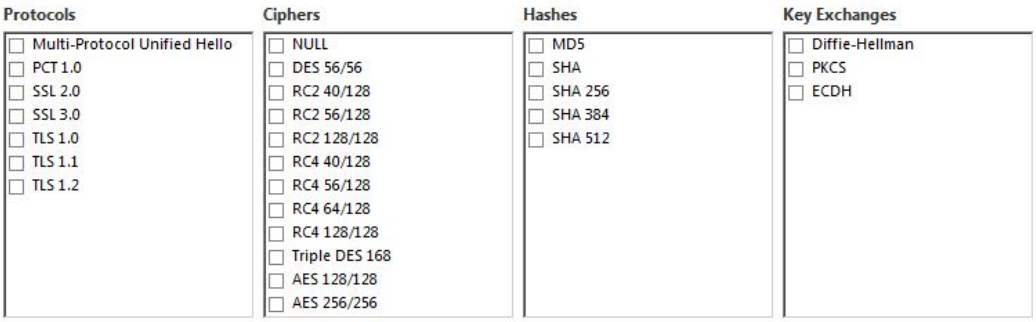
Sunucu eklendikten sonra bağlantı kurulmuştur. Bağlantının sorunsuz bir şekilde sağlandığı ve client' in sunucu ile aynı ip bloğunda olduğu Şekil 19'da görülmektedir.




**Şekil 19:** VPN Ip Tablosu

TLS / SSL Şifreleme paketleri, bir dizi şifreleme algoritmasıdır. Bir TLS / SSL şifreleme paketi, aşağıdaki görevler için bir algoritma belirler.

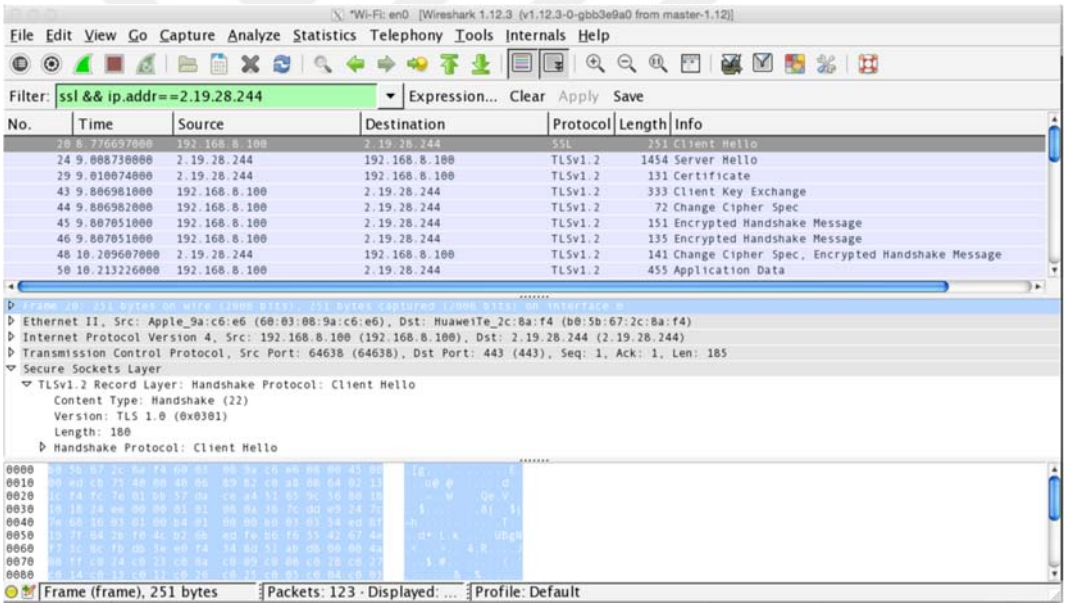
- Anahtar değişimi
- Toplu şifreleme
- Mesaj doğrulama




**Şekil 20:** SSL-TLS Protokolleri

Anahtar değişimi algoritmaları, paylaşılan anahtarlar oluşturmak için gereken bilgileri korur. Toplu şifreleme algoritmaları, istemciler ve sunucular arasında değiş tokuş edilen mesajları şifreler. Bu algoritmalar simetriktir ve büyük miktarda veri için iyi performans gösterir. Mesaj doğrulama algoritmaları, bir mesajın bütünlüğünü sağlayan mesaj hash' lerini ve imzaları üretir.

Güvenlik noktasında hem TLS hem de SSL hemen hemen eşit seviyede güvenlik sunar. Bu noktadaki tek fark SSL bağlantıları güvenlik ile başlar ve doğrudan güvenli iletişime geçer, TLS bağlantıları ise sunucuya gönderilen güvenli olmayan bir "merhaba" mesajı ile başlar ve istemci ile sunucu arasındaki handshake (el sıkışma) gerçekleştikten sonra güvenli bağlantı kurulur. Eğer TLS el sıkışması gerçekleşemezse bağlantı asla kurulmaz.

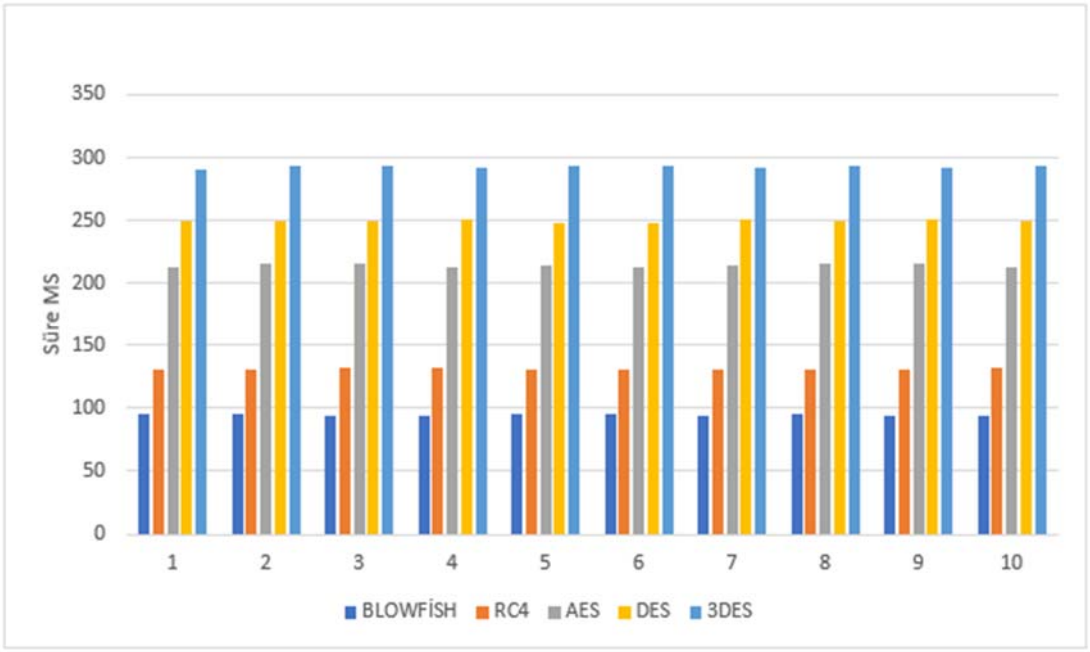



**Şekil 21:** TLS El Sıkışması

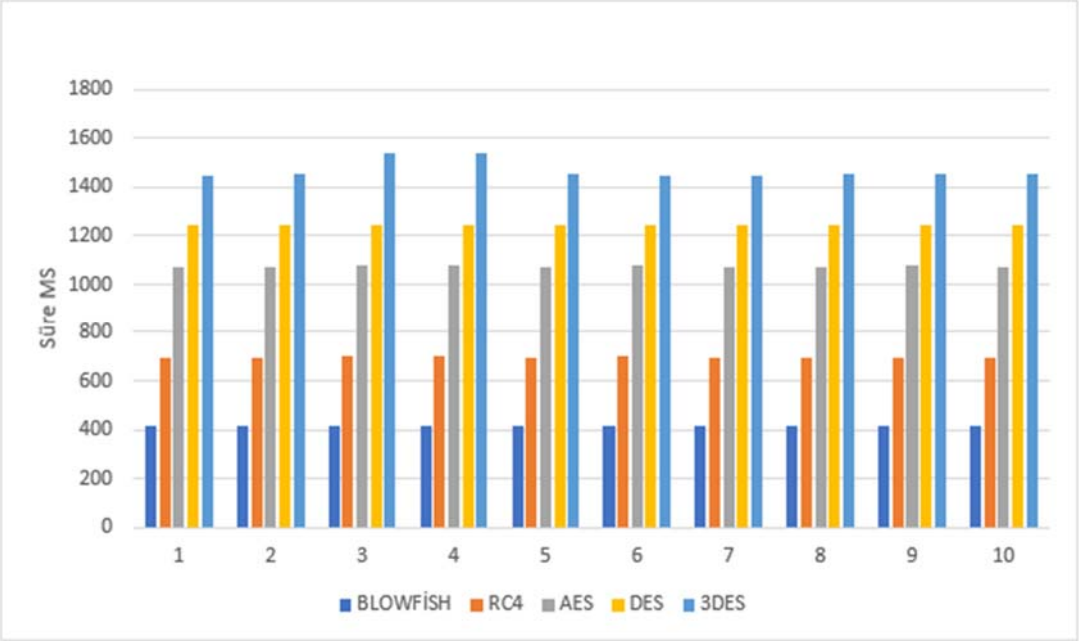
RC4 algoritması bugün hala TLS' de kullanılan en eski şifrelemelerden biridir. Bir akış şifresi olan RC4, küçük sistemlerde performans yönünden oldukça faydalı olmaktadır, ancak hızlı olmasına karşın güvenlik yönünden zayıf kalmaktadır.

En çok kullanılan algoritma ise AES dir. AES, 128, 192 ve 256 bitlik 3 çeşidi vardır. Şu an 128 bit en yaygın kullanılanı, günümüzde 128 bitin yeterli güvenliği sağladığı 256 bit için gerekli maliyete gerek olmadığı görüşü yaygındır.

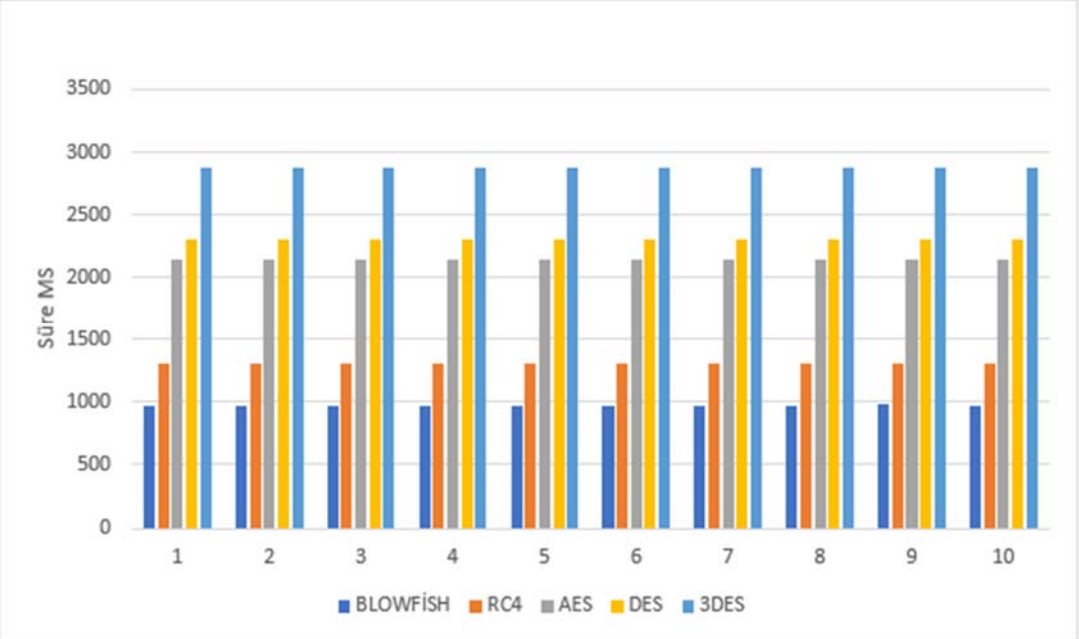
TripleDES veya 3DES, Windows XP için geliştirilen eski bir şifredir. AES kadar güçlü olmadığı için 3DES'in AES'in arkasına simetrik şifre tercihi şeklinde yerleştirilmesi önerilir. Aşağıda 1, 5, 10 MB'lık bir veri dosyasının farklı şifreleme algoritmaları tarafından şifrelenme süreleri verilmiştir.




**Şekil 22:** 1 MB Veri Dosyası Şifreleme Süreleri.




**Şekil 23:** 5 MB Veri Dosyası Şifreleme Süreleri.



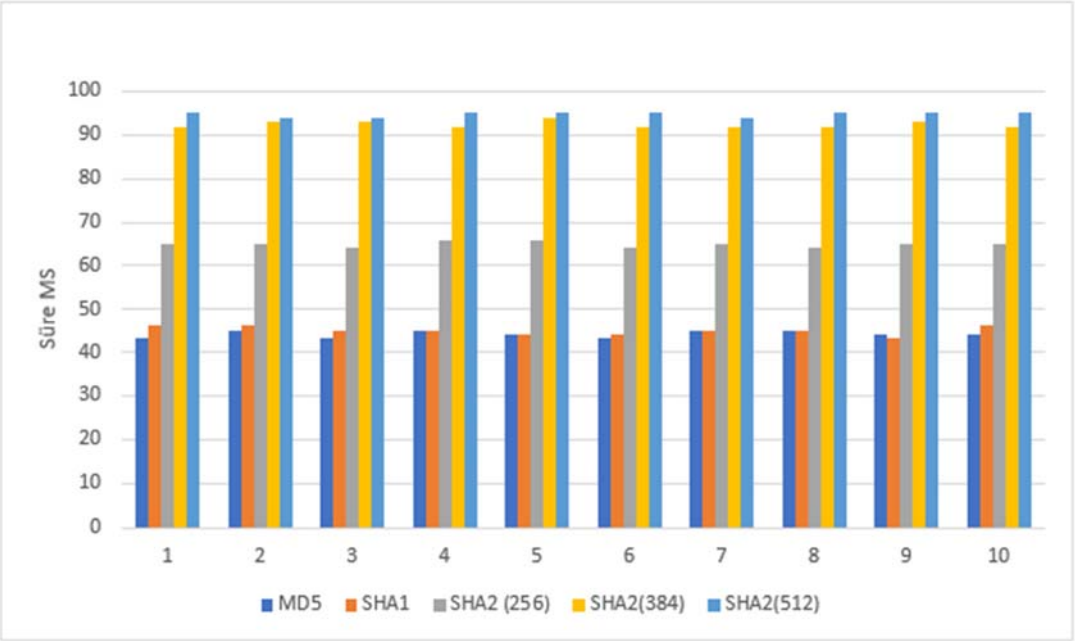

**Şekil 24:** 10 MB Veri Dosyası Şifreleme Süreleri.

Şekil 22, 23, 24'de 1, 5, ve 10 MB'lık veriler üzerinde yapılan ölçümlerde dalgalanmalar olmasına karşın algoritmaların sıralaması değişmemektedir. Ölçüm sonuçlarına göre en iyi performansı Blowfish algoritması vermektedir. Bu algoritmayı sırasıyla RC4, AES, DES ve 3DES algoritmarı izlemektedir.

Özetleme (Hash) Algoritmaları, Tek Yönlü Algoritmalar olarak bilinir. Tek yönlü algoritma ile şifrelenen veri tekrar orijinal haline dönmesi mümkün değildir. Şifreleme algoritmaları üretilen sonucu tekrar orijinal haline çevirebilmektedir. Hash algoritmaları ise üretilen sonuç orijinal haline dönüştürülemez. Bu algoritmaların veri güvenliğine katkısı, iki nokta arasındaki veri transferi sırasında gönderen kişi dosyanın hash kodunu alır, alıcı dosyayı aldığında tekrar hash kodunu alır ve ilk hash kodu ile karşılaştır kodlar aynı ise transfer sırasında dosya 3 kişiler tarafından değiştirilmemiştir. 1 gb lık bir veri dosyası içinden sadece tek bir harf bile değiştirilse hash kodu da değişir.

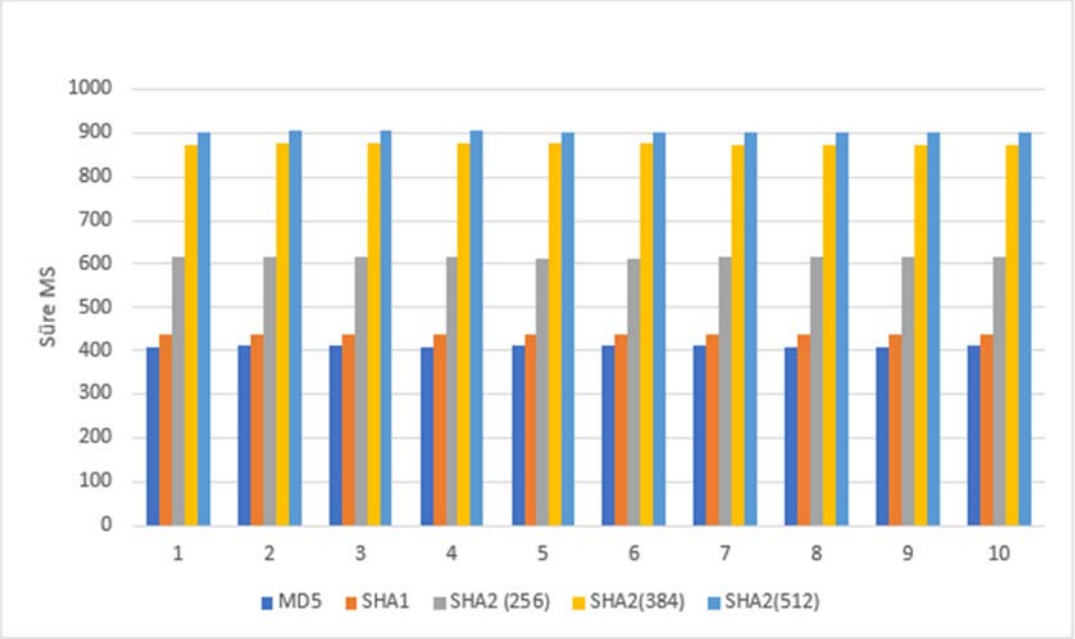
MD5 son yıllarda güvenilirliğini kaybetmektedir. MD5 in yerini SHA algoritmaları almaktadır. Bit sayısı arttıkça o algoritma daha güvenlidir (aynı algoritma ailesinde olmak kaydıyla). SHA1 160 bit uzunluğunda çıkış vermektedir. SHA2 ise 256,384 ve 512 bit uzunluğunda çıkış verebilmektedir. Bu bilgiler ışığında SHA2, SHA1 den daha iyi koruma sağladığı söylenebilir.

Aşağıda 1, 5, 10 MB'lık bir veri dosyası için farklı algoritmalar ile Hash kodu üretim süreleri verilmiştir.




**Şekil 25:** 1 MB Veri Dosyası Hash Kodu Üretme Süreleri.


**Şekil 26:** 5 MB Veri Dosyası Hash Kodu Üretme Süreleri.




**Şekil 27:** 10 MB Veri Dosyası Hash Kodu Üretme Süreleri.

Şekil 25, 26, 27'de 5 farklı özetleme (hash) algoritmaları üzerinde 1, 5 ve 10 MB'lık veri dosyaları ile ölçüm yapılmıştır. Yapılan ölçümlere göre en iyi performansı MD5 algoritması vermiştir. Bu algoritmayı sırasıyla SHA1, SHA2(256), SHA2(384) ve SHA2(512) algoritmaları takip etmektedir.

SSL ve TLS' de, şifreleme paketleri güvenli iletişimin nasıl gerçekleştiğini tanımlar. Çeşitlilik yoluyla güvenlik elde etme fikri ile çeşitli yapı taşlarından oluşurlar. Şifreleme setleri yukarıdaki değinilen konuların bir arada kullanılması ile meydana gelmektedir. Şifreleme seti yapısı Şekil 28'de verilmiştir.


**Şekil 28:** Şifreleme Seti Yapısı.

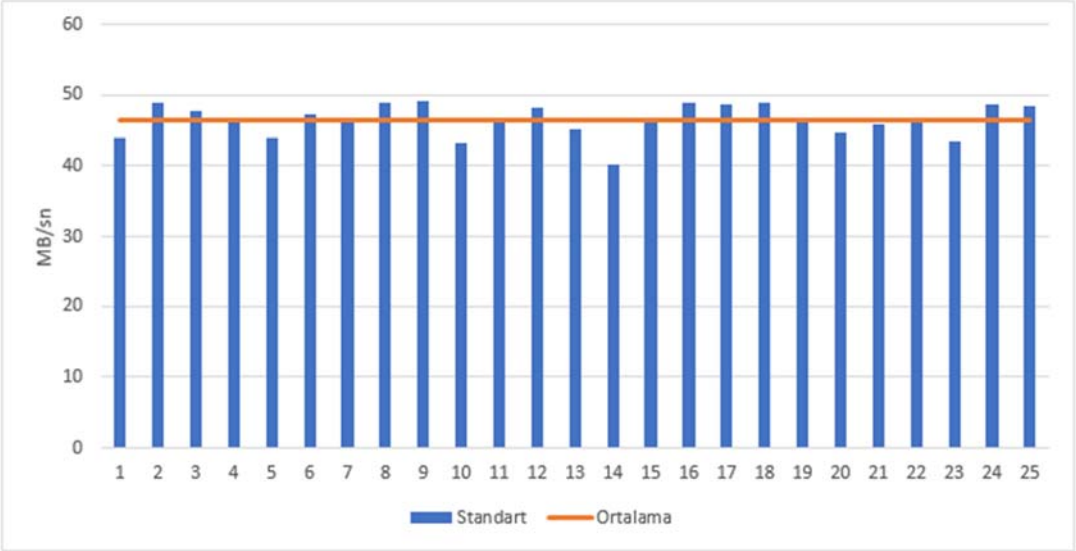
# 7.TARTIŞMA VE KARŞILAŞTIMALAR

## 7.1. Tünel protokollerinin karşılaştırılması

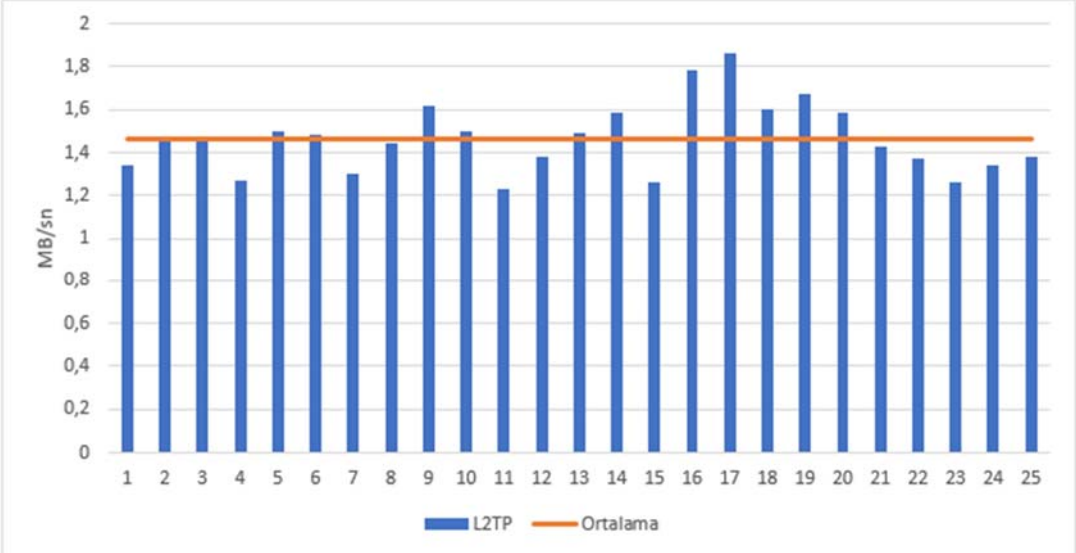
Noktadan Noktaya Tünel Protokolü, sanal özel ağlar için standart protokol olmuştur. Windows tarafından desteklenen ilk VPN protokolü olduğu için birçok platform tarafından desteklenmektedir ve kurulumu çok kolaydır. Protokolün az hesaplama yaparak çalışması mevcut protokoller içinde en hızlılarından biri olmasını sağlamaktadır. Veri iletişimi 128 bitlik şifreleme ile yapılsa da ciddi güvenlik açıkları bulunmaktadır.

Katman 2 Tünel Protokolü, diğer VPN protokollerinden farklı olarak, trafik akışına herhangi bir gizlilik veya şifreleme sağlamaz. Bu nedenle, genellikle verilerin aktarılmadan önce şifrelenmesi ve kullanıcılara gizlilik ve güvenlik sağlanması için IPSec olarak bilinen bir protokol paketi ile uygulanır. Günümüzdeki çoğu platform L2TP / IPSec protokolünü desteklemektedir. Protokolün kurulumu PPTP kadar hızlı ve kolay olmasına rağmen UDP 500 portunu kullanması nedeni ile bazı güvenlik duvarları tarafından sorun çıkabilmektedir. IPSec şifrelemelerinde önemli bir güvenlik açığı bulunmamaktadır ve düzgün bir şekilde uygulandığında güvenliği sağlayabilmektedir. Protokol ile veriler iki kez kapsüllendiğinden çalışması hızı diğerlerine göre düşüktür.

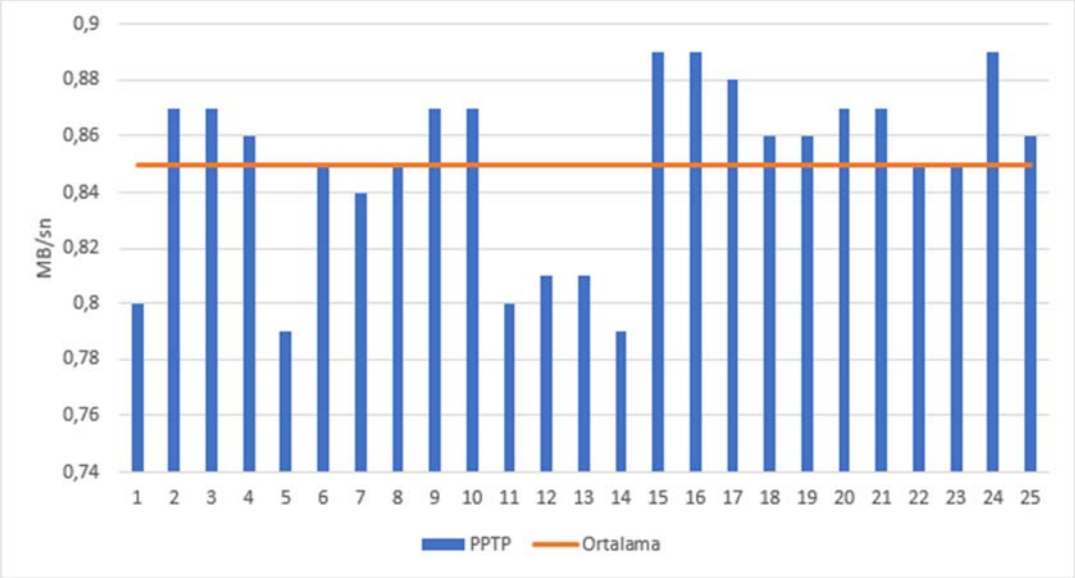
Güvenli Soket Tünel Protokolü, Windows ve Linux tarafından desteklenmektedir. SSL ve TLS kullandığı için güvenlik duvarı sorunları çıkartmaz. Ağırlıkla Windows' a özgü bir protokol olduğu için istikrarlı ve kullanımı kolaydır. SSTP parolalar, akıllı kartlar, sertifika tabanlı birden çok kimlik doğrulama yöntemini desteklediği için güvenlik konusunda gayet başarılıdır.



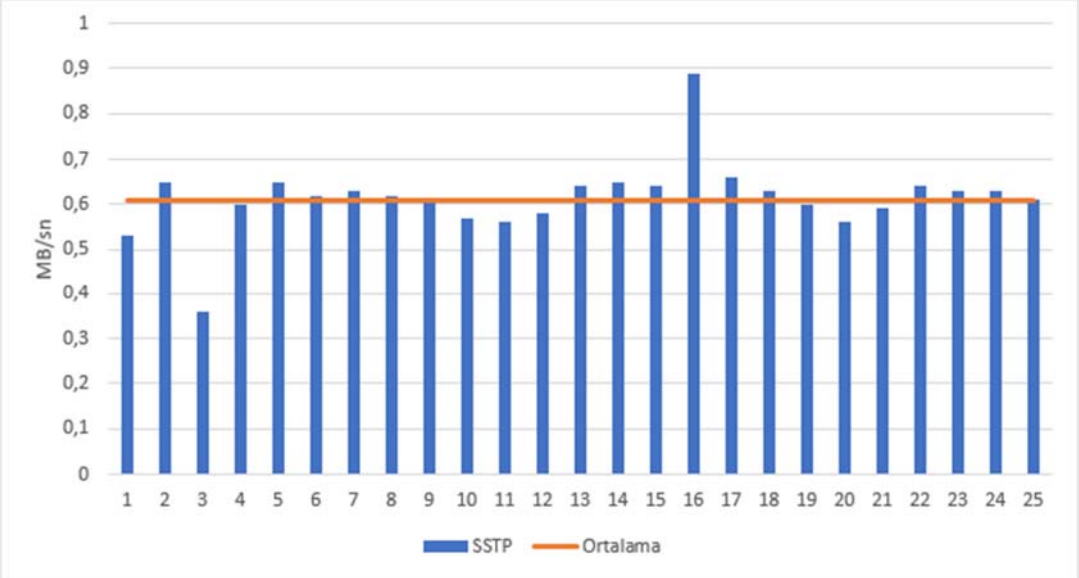

**Şekil 29:** Standart Bağlantı İndirme (Download) Hızı MB\sn.




**Şekil 30:** L2TP Bağlantı İndirme (Download) Hızı MB\sn.




**Şekil 31:** PPTP Bağlantı İndirme (Download) Hızı MB\sn.




**Şekil 32:** SSTP Bağlantı İndirme (Download) Hızı MB\sn.

| | Ortalama (25 Deneme) | Standart Sapma (25 Deneme) |
|---|---|---|
| Standart | 46,54 | 2,274 |
| L2TP | 1,46 | 0,163 |
| PPTP | 0,85 | 0,032 |
| SSTP | 0,61 | 0,083 |

**Tablo 1:** Tünel Protokollerinin Ortalama ve Standart Sapma Değerleri MB/sn.

Şekil 29, 30, 31 ve 32 de 4 farklı tünel protokolü üzerinde yapılan hız testinde normal bağlantı sırasında elde edilen bağlantı hızı, tünel protokolleri kullanıldığında yaklaşık % 98 civarında düşüş yaşamaktadır. Tünel protokolleri üzerinde 25 defa hız ölçümü yapılmış ve en iyi performansı L2TP vermiştir. Bu protokolü sırası ile PPTP ve SSTP takip etmektedir. Yapılan ölçümlerde PPTP'nin hız olarak L2TP'nin arkasında kalmasına karşın bağlantı hızlarındaki standart sapmanın en az yaşandığı protokol olmuştur.

Sonuç olarak PPTP' nin eski ve güvenlik açıkları olduğu için, L2TP/IPSec' in ise güvenlik duvarı ile sorunları ve yavaş çalışmasından dolayı bu protokollerin yerine, daha istikrarlı olması ve güvenlik açıklarının daha az olması nedeni ile SSTP'nin kullanılması veri güvenliği için daha yararlı olacağı sonucuna varılmıştır.

### 7.2. SSL ve TLS Sürümlerinin incelenmesi

SSL / TLS ailesinde SSL v2, SSL v3, TLS v1.0, TLS v1.1 ve TLS v1.2 olmak üzere 5 tane protokol bulunmaktadır.

- SSL v2 ve SSL v3 eski sürüm olması ve güvenlik açıkları bulunmasından dolayı günümüzde çok az sayıda kullanılmaktadır.
- TLS v1.0, eski bir protokol olmasından dolayı kullanımı uygun değildir, fakat bazı eski uygulamaların yeni sürümleri desteklememesinden dolayı bu sürümün kullanıldığı yerler bulunmaktadır.
- TLS v1.1 ve TLS v1.2 de bilinen güvenlik sorunu bulunmamaktadır, ancak TLS v1.2 modern şifreleme algoritmaları sağlamaktadır.

TLS v1.2 Modern kimliği doğrulanmış şifrelemeyi (AEAD olarak da bilinir) sunan tek sürüm olduğundan TLS v1.2 sürümünü kullanmamız gerekmektedir. Bazı firmalar yakın gelecekte TLS v1.0 sürümünden desteklerini çekeceklerini açıklamışlarıdır. Eski sürümlerin kullanımının bırakılması ve yeni sürümlere doğru yönelinmesi veri güvenliği açısından oldukça önemlidir.

### 7.3. Sertifika ve Özel Anahtarların incelenmesi

TLS de güvenlik ilk olarak şifreleme kimliği ile başlar. Saldırıların önlenmesi için güçlü bir özel anahtar ve güçlü bir sertifika kullanmamız gerekmektedir.

Sertifika güvenliği, sertifikayı imzalamak için kullanılan özel anahtarın gücüne ve imzada kullanılan karma işlevin gücüne bağlıdır. Sanal özel ağlarda kullanıcıların sunucuya bağlantıları için sertifika ile bağlantılarının sağlanması, sertifika sahibi olmayanların sisteme erişmesini engeller ve veri güvenliğine katkı sağlayabilmektedir.

Çoğu web site için 2048 bitlik RSA özel anahtarı yeterli güvenlik sağlayabilmesi, RSA' nın yaygın olarak desteklenmesi ile varsayılan seçenek halini almıştır. 2048 bitlik bir RSA özel anahtarı yaklaşık olarak 112 bitlik bir güvenlik sağlayabilmektedir. 128 bitlik güvenlik için 3072 bitlik RSA özel anahtarı kullanmamız gerekmektedir, buda performansta düşüşe neden olmaktadır. 256 bitlik ECDSA ise 3072 bitlik bir RSA ile aynı güvenliği sağlamaktadır. ECDSA algoritması RSA ya göre az anahtar uzunluğu ile aynı güvenliği sağlayabilmektedir. ECDSA algoritması kullanılarak sistem kaynakları daha az kullanılarak aynı güvenliği sağlamsı ve yeni bir algoritma olması nedeni ile özel anahtar olarak bu algoritmanın kullanılması daha yararlı olacağı düşünülmektedir.

Tablo 3'de Eliptik Eğri Dijital İmza Algoritması (ECDSA) ile RSA algoritmasının özel anahtar uzunlukları ve sağladıkları güvenlik değerleri verilmiştir.

| Algoritma | Anahtar Uzunluğu (bit) | Güvenlik (bit) |
|---|---|---|
| RSA | 1024 | 80 |
| RSA | 2048 | 112 |
| RSA | 3072 | 128 |
| RSA | 15360 | 256 |
| ECDSA | 163 | 80 |
| ECDSA | 224 | 112 |
| ECDSA | 256 | 125 |
| ECDSA | 521 | 256 |

**Tablo 2:** RSA ve ECDSA Algoritmaları Anahtar Uzunlukları

### 7.4. Şifreleme Algoritmalarının Karşılaştırılması

Simetrik şifreleme algoritmaları verileri şifrelemek ve şifre çözmek için gizli bir anahtar kullanmaktadır. Algoritma İşlemleri basit olduğu için kısa sürede sonuç vermektedir. Bu nedenle çok fazla donanım ihtiyacı duymamaktadır. Basit elektronik cihazlarda kullanımı iyi sonuçlar vermektedir. Bu algoritmaların bit sayıları düşük olduğu için anahtar boyları daha az yer kaplar. Anahtarların dağıtımı zordur ve kapasiteleri sınırlıdır. Bu dezavantajları nedeni ile güvenlik konusunda sıkıntı oluşturmaktadır.

Asimetrik şifreleme algoritmalarında 2 farklı anahtar kullanıldığı için şifrelerin kırılması simetrik algoritmalara göre biraz daha zordur. Kimlik doğrulama, bütünlük ve gizlilik ilkelerini sağlayabilmektedir. Kullanıcılar anahtarları kendileri belirleyebildikleri için esneklik sağlamaktadır. Şifreleme için kullanılan özel anahtarların alıcıya aktarılması gerekli değildir. Şifreleme işlemleri iki anahtar ile yapıldığından inkâr etme sorununu ortadan kaldırmaktadır. Asimetrik şifreleme algoritmalarında şifreler uzun olduğu için sistemin yavaş çalışmasına neden olur. Anahtarlar boyu ne kadar uzun olursa bit sayıları da aynı oranda yükselir.

Sonuç olarak asimetrik algoritmaların güvenliğini sağlayabilmek için çok büyük asal sayılar kullanılması hem zaman açısından çok büyük problemleri beraberinde getirmekle birlikte donanımsal yapılara uyum sağlaması çok zor olmaktadır. Şifreleme algoritmalarının performansı ve güvenliğini, Şifrelerin kırılabilmesi için harcanan zaman, verileri şifreleme ve şifre çözme işlemleri için kullanılan zaman ve bu işlemler için gerekli bellek alanı verileri, algoritmanın kurulacak sisteme uygunluğu belirler. Asimetrik şifreleme algoritmalarının dezavantajlarının çok olması nedeni ile simetrik şifreleme algoritmalarının sistem kaynaklarını daha az kullanması ve günümüzde yaygın kullanımından dolayı asimetrik algoritmalara göre daha iyi olduğu düşünülmektedir.

### 7.5. Anahtar Değişimi Algoritmalarının İncelenmesi

Anahtar değişimi algoritmaları için genellikle Diffie-Hellman anahtar değişimi (DH) ve eliptik eğri varyantı ECDHE kullanılır. Başka anahtar değişimi algoritmaları da vardır, ancak genelde güvenlik açıkları bulunduğundan kullanımları yaygın değildir. RSA anahtar değişimi ise çok popüler olmasına karşın ileri gizlilik sağlamamaktadır.

2015'te bir grup araştırmacı DH' ye karşı Logjam saldırısı ile daha düşük mukavemetli DH anahtar alışverişlerinin (örneğin 768 bit) kolaylıkla bozulabileceğini keşfetti. Veri güvenliği sağlayabilmek için, DH anahtar değişimini seçilirse, bunu en az 2048 bit güvenlik ile yapılandırılması gerekmektedir. Bazı eski istemciler bu seviyedeki gücü destekleyememektedir. Performans nedenleriyle, çoğu sunucu daha güçlü ve daha hızlı olan ECDHE' yi tercih etmektedir.

### 7.6. Özetleme (Hash) Algoritmalarının İncelenmesi

Özetleme (Hash) algoritmaları veri güvenliği konusunda bize oldukça yardımı bulunmaktadır. Karşı tarafa giden bir dosyanın değişip değişmediği açılıp açılmadığını bu algoritmalar sayesinde öğrenebilmekteyiz. Günümüzde MD5 algoritması eski olduğu ve güvenlik açıklarının bulunmasından dolayı yerini SHA algoritmalarına bırakmaktadır. 256 bitlik bir SHA algoritması mevcut sistem için güvenli olduğu düşünülmektedir.

### 7.7. Çok Fazla Güvenliği Önleme

Güvenli bağlantılar kurmak için kullanılan algoritma ve protokollerde, çok kısa bir anahtar kullanmak güvensizdir, ancak çok uzun bir anahtar kullanılması "çok fazla" güvenlik ve yavaş çalışma ile sonuçlanacaktır. Çoğu web sitesi için 2048 bitten daha güçlü RSA anahtarlarını ve 256 bitten daha güçlü ECDSA anahtarlarını kullanmak CPU güç kaybıdır ve kullanıcı deneyimini etkileyebilir. Benzer şekilde, anahtar alışverişlerinde DHE için 2048 bit ve ECDHE için 256 biti aşan güçlere çıkmanın çok az faydası vardır. Sonuç olarak çok fazla güvenlik önlemi her zaman iyi sonuç getirmeyebilir. Protokol ve algoritmalar seçilirken o zamanki şartlar ve genel kullanım durumuna göre yeterli bir güvenlik önlemi alınmalıdır.

# 8. SONUÇ

Günümüzde hayatımızın hemen her yerinde bulunan internetin, günden güne hayatımızdaki önemi iyice artmaktadır. Artık bankacılık işlemlerinden devlet dairelerindeki işlemlere birçok alanda internet kullanılmaktadır. Hayatımıza bu denli giren internet kötü niyetli kişilerin iştahını kabartmaktadır. Kişisel ve kurumsal bilgilerimizi 3. Şahıslara karşı korumak için güvenlik önlemleri geliştirilmektedir. Bu güvenlilik önlemlerinin en popüleri ise sanal özel ağlardır. Ülkemizde devlet daireleri ve özel şirketler şubeleri ile olan veri transferi için VPN hizmetini kullanmaktadır. Hayatımızın hemen hemen her yerinde ihtiyaç duyduğumuz internette güvenli bir şekilde işlerimizi halletmek ve veri mahremiyetimizi korumamız gerekmektedir.

Bu çalışmada Softether uygulaması ile sanal özel ağ kurulup, kurulum aşamaları ve konfigürasyonları adım adım anlatılmıştır. Kurulan sanal özel ağ üzerinde tünel protokolleri test edilmiştir. Test sonucunda indirme hızında L2TP en iyi sonucu vermiş ve bu protokolü PPTP ve SSTP takip etmiştir. Yükleme hızı için yapılan test sonucunda sıralama PPTP, L2TP ve SSTP olarak gözlemlenmiştir. İndirme testinde ilk sırada olan L2TP protokolü yükleme testinde 2 sıraya düşmüştür. Bunun nedeni ise L2TP de veriler iki kez kapsüllendiği için çalışma hızını düşürmektedir. Test sonuçları ve yapılan araştırmalar neticesinde SSTP protokolü diğerlerine göre daha istikrarlı çalışması ve veri güvenliği için güncel teknolojileri kullanmasından dolayı bu protokolün kullanılması sonucuna varılmıştır.

SSTP protokolünde iletişim SSL-TLS üzerinden yapılmaktadır. SSL-TLS' in 5 adet sürümü bulunmaktadır. Bu sürümler için yapılan araştırmada SSL'e ait 2 sürümün güvenlik açıkları olduğu ve kullanımının azaldığı, TLS'e ait 3 sürümün ise v1.0'ın güncelliğini yitirdiği, v1.1 ve v1.2 sürümlerinin bilinen güvenlik açıklarının olmaması ve güncel teknoloji kullanmasından dolayı, TLS v1.1 ve TLS v1.2'nin kullanılması veri güvenliği açısından verimli olacağı tespit edilmiştir.

SSL-TLS güvenlik için şifreleme setleri kullanır. Şifreleme setleri çeşitli algoritma ve protokol konfigürasyonları ile meydana gelir. Şifreleme setlerinde standart olarak anahtar değişim algoritması, sertifika anahtarı, veri şifreleme algoritması ve özetleme algoritmasından meydana gelir. Çalışmamda anahtar değişim algoritmaları üzerinde

yapılan araştırmada DH ve ECDHE algoritmaları günümüz şartlarında yeterli güvenliği sağladığı, Diffie-Hellman algoritmasının Eliptik eğri varyantı, Diffie-Hellman algoritmasına karşı yaklaşık 10 kat daha iyi sonuç verdiği ve donanım bileşenlerine fazla yük getirmeden yeterli güvenliği sağladığı gözlemlenmiştir. Sertifika anahtarı içinde benzer durum söz konusudur. ECDSA'nın RSA ya göre daha iyi performans gösterdiği gözlemlenmiştir. Şifreleme algoritmalarında ise simetrik şifreleme algoritmalarının asimetrik şifreleme algoritmalarına göre sistem kaynaklarını fazla kullanmadan yeterli güvenliği sağlaması nedeni ile simetrik şifreleme algoritmaları üzerinde yapılan testlere göre en iyi süreyi Blowfish algoritması vermesine karşı yeterli güvenlik sunamamaktadır. AES algoritması hem süre yönünden hemde güvenlik yönünden iyi sonuç vermesi ve günümüzde yaygın olarak kullanılmasından dolayı bu algoritmanın veri şifrelemede kullanılması sonucuna varılmıştır.

Sonuç olarak bu tez çalışmasında, sanal özel ağlardaki veri güvenliği için gerekli donanım, yazılım ve yöntemlerin neler olduğu, bu araçların kullanılmasının veri güvenliği açısından nasıl bir fayda sağlayacağı uygulamalı olarak anlatılmıştır.

## KAYNAKLAR

[1] Süheyla İKİZ, 2006, Performance Parameters Of Wıreless Vırtual Prıvate Network, Y. Lisans tezi, Orta Doğu Teknik Üniversitesi Fen Bilimleri Enstitüsü, Ankara

[2] Zeynep YÜKSEL, 2007, Ağ Güvenliği ve Güvenlik Duvarında VPN ve NAT Uygulamaları, Y. Lisans tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul

[3] İlker SÖGÜT, 2009, Çok Protokollü Etiket Anahtarlama (Mpls) Kullanılarak Çok Alanlı Sanal Özel Ağ (VPN) Kurulumu, Y. Lisans tezi, Muğla Üniversitesi Fen Bilimleri Enstitüsü, Muğla

[4] Fuat DEMİR, 2010, Güvenli Veri İletişiminde Kullanılan VPN Tiplerinin Uygulaması ve Performans Analizi, Y. Lisans tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul

[5] Nurdoğan AYDOĞDU, 2014, Sanal Özel Ağ (VPN) Bağlantı Mantığı (VPN Teknolojisi) ve Token Güvenliğinin Pin Kodu İle Arttırılması, Y. Lisans tezi, Beykent Üniversitesi Fen Bilimleri Enstitüsü, İstanbul

[6] Yunus Emre SEYYAR, 2013, Siteden Siteye Sanal Özel Ağ ve Dinamik Çok Noktalı Sanal Özel Ağ Karşılaştırmalı İncelenmesi, Y. Lisans tezi, Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü, Kırıkkale

[7] Taha ALJADIR, 2015, Measurement Of System Securıty Issues Of Prıvate Computer Networks For Dıfferent Types Of Attacks, Y. Lisans tezi, Çankaya Üniversitesi Fen Bilimleri Enstitüsü, Ankara

[8] Mouath SALIM, 2015, Analysıs And Implementatıon Of Remote Access Computer Communıcatıon, Y. Lisans tezi, Çankaya Üniversitesi Fen Bilimleri Enstitüsü, Ankara

[9] Shaneel Narayan, Samad S. Kolahi, Kris Brooking, Simon de Vere, Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment, UNITEC New Zealand

[10] Yongguang Zhang, A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks, IEEE

[11] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader and Mohiy Mohamed Hadhoud, Evaluating The Performance of Symmetric Encryption Algorithms, International Journal of Network Security, Vol.10, No.3, PP.213–219, May 2010

[12] Zhao Aqun, Yuan Yuan, Ji Yi, Gu Guanqun, Research on tunneling techniques in virtual private networks, 21-25 Aug. 2000

[13] "What Is VPN And Why Would I Need It" erişim adresi: http://www.VPNmonitor.eu erişim tarihi Mayıs 2017

[14] "How VPNs Work" erişim adresi: http://computer.howstuffworks.com/VPN.htm, erişim tarihi Mayıs 2017

[15] Ahmet Musa KÖSALI, 2013, VPN Teknikleri ve Uygulamaları, Y. Lisans tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya

[16] "Şifreleme Yöntemleri", erişim adresi: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/şifreleme-yöntemleri, erişim tarihi Mayıs 2017

[17] Selçuk-Teknik Dergisi, Cilt 9, Sayı:1-2010, Simetrik Ve Asimetrik Şifreleme Algoritmalarının karşılaştırılması

[18] "DES (Veri Şifreleme Standardı, Data Encryption Standard)" erişim adresi: http://bilgisayarkavramlari.sadievrenseker.com/2008/03/13/des-veri-sifreleme-standardi-data-encryption-standard/, erişim tarihi Haziran 2017

[19] "AES Algoritmasının Yapısı" erişim adresi: http://cryptographicprocessor.weebly.com/project-schedule.html, erişim tarihi Haziran 2017

[20] "Kriptografi - 2. Bölüm", erişim adresi: http://blog.btrisk.com/2014/04/kriptografi-2-bolum.html, erişim tarihi Haziran 2017

[21] “RSA Algoritması ve Uygulaması”, erişim adresi: https://blog.tolgaakkapulu.com/rsa-algoritmasi-ve-uygulamasi.php, erişim tarihi Haziran 2017

[22] “Secure Hash Algorithm (SHA)”, erişim adresi: https://www.techopedia.com/definition/10328/secure-hash-algorithm-sha, erişim tarihi Haziran 2017

[23] “Understanding PPTP”, erişim adresi: https://technet.microsoft.com/en-us/library/cc768084.aspx, erişim tarihi Haziran 2017

[24] “IPSec VPN (Internet Protocol Security – İnternet Protokolü Güvenliği)”, erişim adresi: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/IPSec-VPN-(internet-protocol-security-internet-protokolü-güvenliği), erişim tarihi Haziran 2017

[25]”Authentication Header”, erişim adresi: https://www.ibm.com/support/knowledgecenter/en/ssw_i5_54/rzaja/rzajaahheader.htm , erişim tarihi: Haziran 2017

[26] ” Encapsulating Security Payload”, erişim adresi: https://www.ibm.com/support/knowledgecenter/en/ssw_i5_54/rzaja/rzajaesp.htm, erişim tarihi: Temmuz 2017

[27] “Point to Point Protocol (Noktadan Noktaya Protokolü)” erişim adresi: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/point-to-point-protocol-(noktadan-noktaya-protokolü): Temmuz 2017

[28] “The Point-to-Point Protocol (PPP)” erişim adresi: https://tools.ietf.org/html/rfc1661, erişim tarihi: Temmuz 2017

[29] “Point to Point Protocol (PPP) Tutorial” erişim adresi: http://www.9tut.com/point-to-point-protocol-ppp-tutorial erişim tarihi: Temmuz 2017

[30] “CHAP” erişim adresi: http://www.telecomabc.com/c/chap.html erişim tarihi: Temmuz 2017

[31] “What is GRE (Generic Routing Encapsulation)” erişim adresi: http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-gre-generic-routing-encapsulation.php, erişim tarihi: Temmuz 2017

[32] “SSTP Remote Access Step-by-Step Guide: Deployment” erişim adresi: https://technet.microsoft.com/en-us/library/cc731352.aspx erişim tarihi: Temmuz 2017

[33] “SSTP (Secure Socket Tunneling Protocol)” erişim adresi: http://en.bmstu.wiki/SSTP_(Secure_Socket_Tunneling_Protocol), erişim tarihi: Temmuz 2017

[34] “Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)” erişim adresi: http://www.thenetworkencyclopedia.com/entry/microsoft-challenge-handshake-authentication-protocol-ms-chap, erişim tarihi: Ağustos 2017

[35] “Microsoft Point-to-Point Encryption” erişim adresi: https://en.wikipedia.org/wiki/Microsoft_Point-to-Point_Encryption erişim tarihi: Ağustos 2017

[36] “Extensible authentication protocol” erişim adresi: https://community.jisc.ac.uk/library/advisory-services/extensible-authentication-protocol erişim tarihi: Ağustos 2017

[37] “VPN Teknolojisi” erişim adresi: http://tuncaybas.com/?p=250 erişim tarihi: Ağustos 2017

[38] “NAT (Network Address Translation) nedir? ” erişim adresi: http://www.beyaz.net/tr/dokumanlar/nat-network-address-translation-nedir.html, erişim tarihi: Ağustos 2017

[39] “NAT (Network Address Translation - Ağ Adresi Çeviricisi)” erişim adresi: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/nat-(network-address-translation---ağ-adresi-çeviricisi), erişim tarihi: Ağustos 2017

# ÖZGEÇMİŞ

**Kişisel Bilgiler**


| | |
|---|---|
| **Soyadı, adı** | : BÖGE Seyit |
| **Uyruğu** | : T.C. |
| **Doğum tarihi ve yeri** | : 20.03.1991 Aksaray Medeni hali : Evli |
| **Telefon** | : 0 (551) 233 61 01 |
| **Faks** | : 0 (382) 215 36 98 |
| **e-mail** | : seyitboge@gmail.com |


**Eğitim**

| **Derece** | **Eğitim Birimi** | **Mezuniyet tarihi** |
|---|---|---|
| Lisans | Ahmet Yesevi Üniversitesi / Bil. Müh. | 2014 |

**İş Deneyimi**

| **Yıl** | **Yer** | **Görev** |
|---|---|---|
| 2010- | İçişleri Bakanlığı | Bilgisayar Mühendisi |

**Yabancı Dil**

İngilizce