İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

GÜVENLİ VERİ İLETİMİNDE KULLANILAN VPN TİPLERİNİN UYGULAMASI VE PERFORMANS ANALİZİ

YÜKSEK LİSANS TEZİ

Müh. Fuat DEMİR

Anabilim Dalı : Elektronik ve Haberleşme Mühendisliği

Programı : Telekomünikasyon Mühendisliği

Tez Danışmanı: Prof. Dr. Ahmet Hamdi KAYRAN

AĞUSTOS 2010

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

GÜVENLİ VERİ İLETİMİNDE KULLANILAN VPN TİPLERİNİN UYGULAMASI VE PERFORMANS ANALİZİ

YÜKSEK LİSANS TEZİ
Fuat DEMİR
(504051343)

Tezin Enstitüye Verildiği Tarih : 13 Ağustos 2010
Tezin Savunulduğu Tarih : 17 Ağustos 2010

Tez Danışmanı : Prof. Dr. Ahmet Hamdi KAYRAN (İTÜ)
Diğer Jüri Üyeleri : Prof. Dr. Mehmet Ertuğrul ÇELEBİ (İTÜ)
Yrd. Doç. Dr. Mustafa Ersel KAMAŞAK (İTÜ)

AĞUSTOS 2010

Eşime ve oğluma,

ÖNSÖZ

Yüksek lisans çalışmam boyunca bilgi ve tecrübesinden faydalandığım değerli hocam Prof. Dr. Ahmet Hamdi KAYRAN'a,

Bugünlere gelmemde en büyük rol sahibi olan ve her zaman yanımda olan anne ve babama,

Desteğini esirgemeyen eşime ve bu dönemde dünyaya gelen oğluma,

Teşekkürlerimi, sevgi ve saygılarımı sunarım.

Ağustos 2010 Fuat DEMİR

İÇİNDEKİLER

Sayfa

KISALTMALAR

3DES : Triple Data Encryption Standart
ADSL : Asymmetric Digital Subscriber Line
AES : Advanced Encryption Standart
AH : Authentication Header
ARPANET : Advanced Research Project Agency Network
ASA : Adaptive Security Appliance
ASDM : Adaptive Security Device Manager
ATM : Asenkron İletim Modu
CA : Certificate Authority
CLI : Command Line Interface
CVPN : Client Virtual Private Network
DES : Data Encryption Standart
DH : Diffie-Hellman
DSA : Dijital İmza Algoritması
ESP : Encapsulated Security Payload
HMAC : Hash-based Message Authentication Code
HTTP : Hyper Text Transfer Protocol
HTTPS : Hyper Text Transfer Protocol Secure
ICV : Integrity Checksum Value
IETF : Internet Engineering Task Force
IKE : Internet Key Exchange
IP : Internet Protocol
IPSec : IP Security
ISAKMP : Internet Security Association and Key Management Protocol
ISO : Uluslararası Standart Organizasyonu
KEA : Anahtar Değişim Algoritması
L2L : LAN-to-LAN
L2TP : Layer 2 Tunneling Protocol
LAN : Local Area Network
MAN : Metropolitan Area Network
MD5 : Message-Digest Algorithm 5
NAT : Network Address Translation
OSI : Open Systems Interconnect
PSK : Pre Shared Key
RSA : Rivest-Shamir-Adelman
SA : Security Association
SHA : Secure Hash Algorithm
SPI : Security Parameter Index
SSL : Secure Socket Layer
TCP/IP : Transmission Control Protocol/Internet Protocol
TFTP : Trivial File Transfer Protocol
UDP : User Datagram Protocol

URL **:** Uniform Resource Locator
VPN **:** Virtual Private Network
WAN **:** Wide Area Network
XAUTH **:** Extra Authentication

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

GÜVENLİ VERİ İLETİMİNDE KULLANILAN VPN TİPLERİNİN UYGULAMASI VE PERFORMANS ANALİZİ

ÖZET

Özel sanal ağ, bilgisayar haberleşmesinde kullanılan ve bilgisayar ağları üzerinden güvenli veri iletimini sağlamak için ortaya çıkmış bir kavramdır. Önceleri çok geniş olmayan yerel ağ içindeki veri alışverişinde ön planda olmayan bilgi güvenliği, ağlar arası haberleşme ihtiyacı ile önem kazanmıştır. İnternet'in de bugünkü halini alması ve halen büyümeye devam etmesi ile kötü amaçlı kişilerin ve yazılımların artması, veri gizliliğini kritik noktalara getirmiştir.

İki uç nokta arasında, internet servis sağlayıcı tarafından sağlanan, üçüncü bir kişinin giremeyeceği temiz kanallar ile sağlanmaya çalışılan bilgi güvenliği problemi maliyet açısından ve ölçeklenebilirlik açısından getirdiği dezavantaj sebebiyle, özel sanal ağ kullanımı giderek artmıştır.

Özel sanal ağlar, bir istemciden uzak bir sunucuya ya da bir ağdan uzak bir ağa, karşılıklı olarak, verinin bir noktadan şifrelenerek karşı tarafa gönderilmesi, karşı tarafında şifrelenmiş verinin deşifre edilerek gerçek veriye ulaşılması mantığına dayanmaktadır. Şifreleme ve şifre çözme işlemi için gerekli anahtarların paylaşılması, şifreleme algoritmaları ve paket doğrulanması gibi bir çok parametre özel sanal ağ için anahtar kavramlardır.

Tüm özel sanal ağlar en az bir tarafta özel sanal ağ geçidi olarak kullanılacak bir donanıma ihtiyaç duyar. Bu çalışmada kullanılan ağ geçidi Cisco 5500 serisi güvenlik duvarıdır. Özel sanal ağ tiplerinden SSL VPN, IPSec CVPN ve IPSec L2L VPN Cisco ağ geçidi üzerinde ve istemci tarafındaki uygulamaları gösterilmiştir. Bu üç tip özel sanal 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.

APPLICATION AND PERFORMANCE ANALYSIS OF VPN TYPES USED SECURE DATA TRANSFER

SUMMARY

Virtual private network, is a term that used in computer networking terminology which provides a secure data transfer between network devices. Communication needs between network devices, increased the importance of information security which is not a major parameter in local networks. Internet which is the biggest network today, raises the level of importance of security to the critical point.

Information security which is being provided by clear channels between two endpoints has some disadvantages like its cost and scalabilitiy. Therefore usage of virtual private network is getting more popular.

Virtual private network is set from a client to a server or from a network to another network by encrypting and sending the data from one point to the remote point and decrypting the encrypted data on the remote site. Exchange of the keys for encrypting and decrypting the data, encryption algorithms, packet authentication are the key terms in virtual private networks.

All virtual private networks need a hardware as a VPN gateway at least in one site. In this work, Cisco 5500 series firewall is used as VPN gateway. VPN types of SSL VPN, IPSec CVPN and IPSec L2L VPN is configured on Cisco 5500 series firewall and client site device. In addition to this, connection from a client computer which has a Windows operationg system, is established to a web server located on remote site with these three types of VPN. By using the same encryption and packet integrity algorithms as parameters, access durations to remotely located web server are measured and three VPN types are compared with their access speeds.

1. GİRİŞ

Bilgisayar günümüzde en çok kullanılan cihazların başında gelmektedir. İlk bilgisayarlar, şu an evde ve ofiste kullanılan bilgisayarlara göre çok daha büyüklerdi ve onluk sayı tabanında işlem yapabiliyorlardı (ENIAC - 1946). İhtiyaçlar doğrultusunda teknolojinin gelişimi ile geliştirilen işlemci bellek ve kartlar ile bilgisayar boyutları küçüldü ve kullanımı yaygınlaştı. Başka bir bilgisayardaki veriye erişme isteği ile 1962 yılında ortaya çıkan ilk "Ağ" kavramı, 1965 yılında iki bilgisayarın ilk kez birbiriyle haberleşmesi ile ortaya çıkmış oldu. Amerikan donanmasında kullanılan ilk proje ARPANET (Advanced Research Project Agency Network) ile 1969 yılında dört bilgisayarın birbiri ile iletişim kurmasıyla internet'in temelleri atılmış oldu. Bu proje ile ortaya çıkan TCP/IP (Transmission Control Protocol/Internet Protocol) ile internet 1983 yılında deneysel olmaktan çıkmıştır. TCP/IP ile eş zamanlı olarak Uluslararası Standart Organizasyonu (ISO) yaptığı çalışmalarla ilerleyen yıllarda iletişim protokolleri standartlarını oluşturmaya başlamıştır. Bu çalışmalarla Açık Sistemler Bağlantı Modeli (Open Systems Interconnect – OSI) ortaya çıkmıştır.

1.1 Elektronik Güvenlik

Bilgisayarlar ve internet, iletişim teknolojisini geliştirirken, bilginin güvenliği ihtiyacını da en üst seviyeye çıkarmıştır. İlk olarak askeri bilgilerin gizlenme amacıyla ortaya çıkan kriptografi (veri şifrelenmesi), artık günümüzde internet üzerinden yapılan neredeyse her işlem için zorunlu hale gelmiştir. Kriptografi, gizlilik ve kimlik doğrulama güvenlik problemlerinin matematiksel çalışma alanıdır [1]. Elektronik güvenlik, bu noktada, tüm sistemi, kullanıcıdan, ağ yapısına, ağ yapısından yazılıma kadar bir bütün olarak görerek, verinin iletim yolu boyunca, gizli, bütünlüğü bozulmadan ve doğrulanmış olmasını gerekli kılar.

1.2 Güvenlik Prensipleri

Bilişim güvenliğinin birçok boyutu olmasına karşın, temel olarak üç prensipten söz edilebilir: Gizlilik, Veri Bütünlüğü ve Süreklilik.

1.2.1 Gizlilik (Confidentiality)

Gizlilik, bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir [2]. Gizlilik, hem kalıcı ortamlarda (disk, tape, vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar, yetkileri olmayan verilere birçok yolla erişebilirler: Parola dosyalarının çalınması, sosyal mühendislik, bilgisayar başında çalışan bir kullanıcının, ona fark ettirmeden özel bir bilgisini ele geçirme (parolasını girerken gözetleme gibi). Bunun yanında trafik analizinin, yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir.

1.2.2 Veri bütünlüğü (Data integrity)

Bu hizmetin amacı, veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır. Bu hizmeti, geri dönüşümü olan ve olmayan şekilde verebiliriz. Şöyle ki; alıcıda iki tür bütünlük sınaması yapılabilir: Bozulma Sınaması ya da Düzeltme Sınaması. Bozulma Sınaması ile verinin göndericiden alıcıya ulaştırılması sırasında değiştirilip değiştirilmediğinin sezilmesi hedeflenmiştir. Düzeltme Sınaması'nda ise, Bozulma Sınaması'na ek olarak eğer veride değişiklik sezildiyse bunu göndericiden çıktığı haline döndürmek hedeflenmektedir.

1.2.3 Süreklilik (Availability)

Bilişim sistemleri, kendilerinden beklenen işleri gerçekleştirirken, hedeflenen bir başarım (performance) vardır. Bu başarım sayesinde müşteri memnuniyeti artar, elektronik işe geçiş süreci hızlanır. Süreklilik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarım düşürücü tehditlere karşı korumayı hedefler.Süreklilik hizmeti sayesinde, kullanıcılar, erişim yetkileri dahilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilirler.

Sistem sürekliliği, yalnızca kötü amaçlı bir bilgisayar korsanının, sistem başarımını düşürmeye yönelik bir saldırısı sonucu zedelenmez. Bilgisayar yazılımlarındaki hatalar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması, ortam şartlarındaki değişimler (nem, ısı, yıldırım düşmesi, topraklama eksikliği) gibi faktörler de sistem sürekliliğini etkileyebilir. Aşağıda, yukarıdaki üç temel prensibe ek olarak ikinci planda değerlendirilebilecek izlenebilirlik, kimlik sınaması, güvenilirlik ve inkâr edememe prensiplerinden bahsedilmiştir.

1.2.4 İzlenebilirlik (Accountability)

Bu hizmetin hedefi sistemde gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır. Burada olay dendiğinde, bilgisayar sistemi ya da ağı üzerinde olan herhangi bir faaliyeti anlayabiliriz. Bir sistemde olabilecek olaylara, kullanıcının parolasını yazarak sisteme girmesi, bir web sayfasına bağlanmak, e-posta almak göndermek ya da anlık mesajlaşma uygulamaları ile mesaj yollamak gibi örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin örüntülerine rastlanırsa ya da bulanık mantık kullanılarak daha önce rastlanmayan ve saldırı olasılığı yüksek bir aktivite tespit edilirse alarm mesajları üretilerek sistem yöneticileri uyarılır.

1.2.5 Kimlik doğrulama (Authentication)

Ağ güvenliği açısından önemli gereksinimlerden biri de alıcı ve göndericinin birbirlerini doğrulama için güvenli bir metod sağlamasıdır [3]. Alıcı, göndericinin iddia ettiği kişi olduğundan emin olmalıdır. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik doğrulama, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik doğrulama sistemleri yaygın olarak kullanmaya başlanmıştır.

1.2.6 Güvenilirlik (Reliability)

Sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir deyiş ile güvenilirlik, sistemden ne yapmasını bekliyorsak, sistemin de eksiksiz ve fazlasız olarak bunu yapması ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir.

1.2.7 İnkar edememe (Non-repudiation)

Bu hizmet sayesinde, ne gönderici alıcıya bir mesajı gönderdiğini ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır ve gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır. Bu hizmetler, zaman içinde bilgisayar sistemlerine karşı ortaya çıkmış tehditler ve yaşanmış olaylar sonucunda ortaya konmuştur. Yani her bir hizmet, belli bir grup potansiyel tehdide karşı sistemi korumaya yöneliktir, denilebilir.

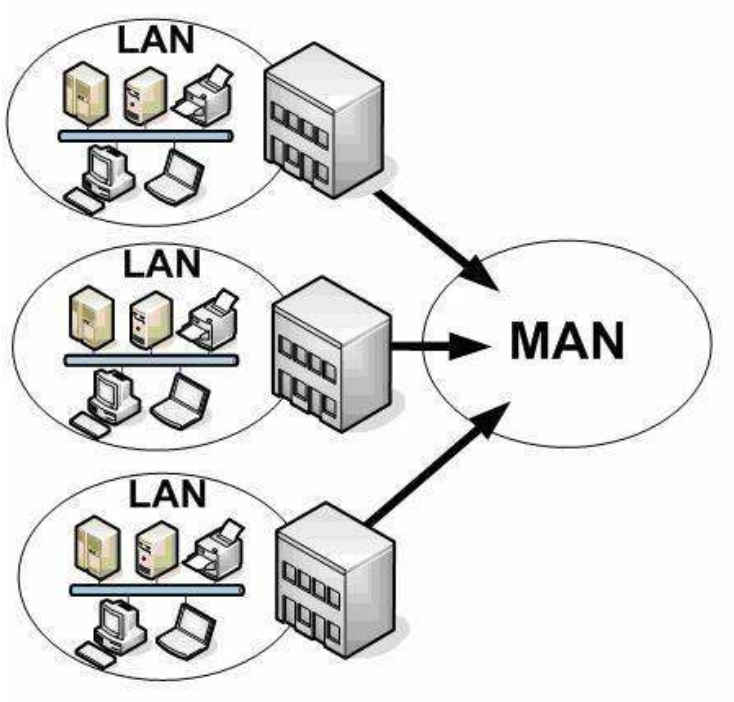
1.3 Bilgisayar Ağları

Bilgisayar ağlarını genel olarak üç sınıfa ayırmak mümkündür.

- Yerel Alan Ağları (LAN)
- Metropolitan Alan Ağları (MAN)
- Geniş Alan Ağları (WAN)

1.3.1 Yerel alan ağları (LAN)

Genel olarak tek bir binada yada bir yerleşke içersinde kurulan bilgisayar ağını tanımlar.



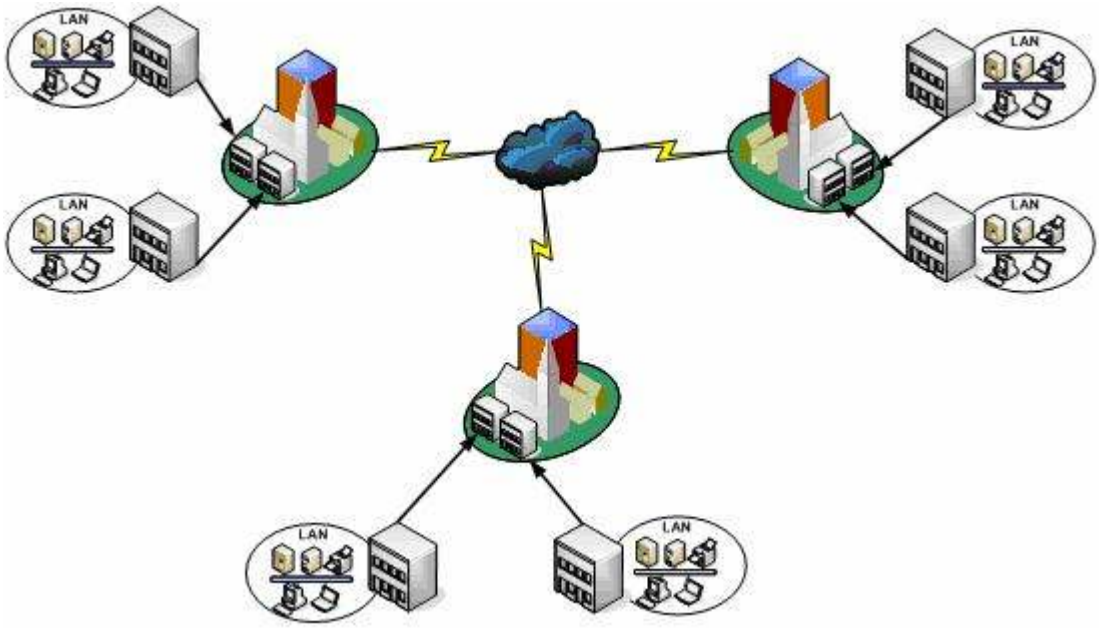
Şekil 1.1 : Yerel Alan Ağı (LAN) ve Metropolitan Alan Ağı (MAN)

1.3.2 Metropolitan alan ağları (MAN)

Daha geniş bir ağ grubunu kapsamaktadır. Metropolitan adı ile anılmasının sebebi bir şehrin tamamını veya büyük bir kısmını kapsıyor olmasındandır.

1.3.3 Geniş alan ağları (WAN)

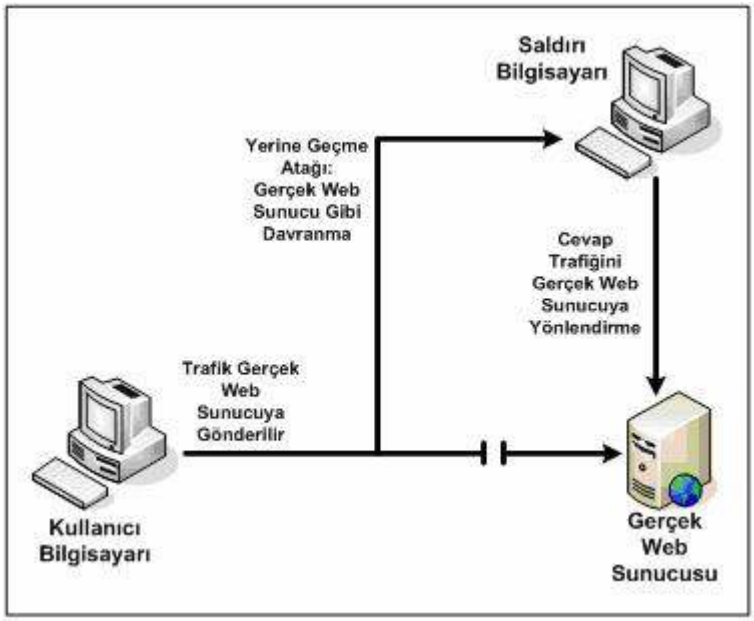
Geniş alan ağları metropolitan alan ağları birbirine bağlayan ağların genel adıdır. Bu ağlar şehirleri hatta ülkeleri birbirine bağlayan ağlardır. İnternet bir geniş alan ağı olarak verilebilecek en güzel örnektir [4].



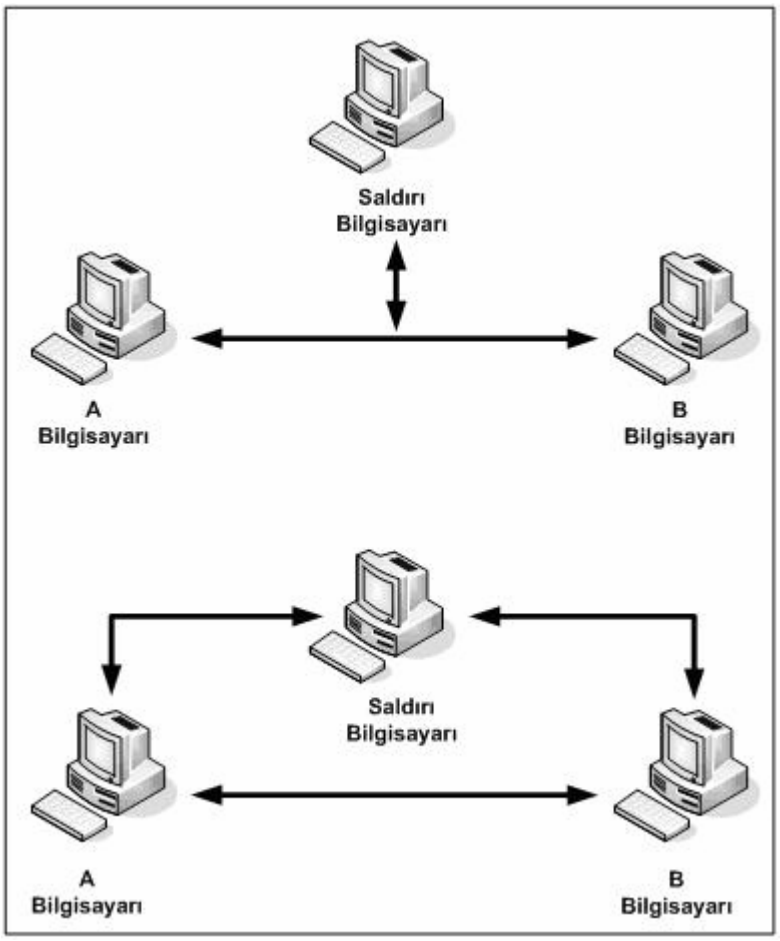
Şekil 1.2 : Geniş Alan Ağı (LAN)

2. VPN VE VPN TİPLERİ

VPN'ler (Özel Sanal Ağlar) bir ağ üzerinden gönderilen verinin güvenlik problemini çözme amaçlı geliştirilmiştir. Aynı zamanda VPN'ler özel ağ kurmak için kiralık hatlara ekonomik bir alternatif olarak ortaya çıkmıştır [5]. İki nokta arasında yapılan açık (şifrelenmemiş) veri alışverişi, verinin izlediği yol boyunca, aradaki ya da uç noktalardaki herhangi biri tarafından kolaylıkla görülebilir ve saldırı gerçekleştirebilir. Yapılan saldırılar, dinleme (Eavesdropping) ve yerine geçme (Masquerading) şeklinde gerçekleştirilebilir. Kötü niyetli bir kullanıcı, şifrelenmemiş paketi dinleyerek, kullanıcı adı ve şifre gibi bilgileri, verinin iletim yolunda, gerçek kullanıcıya sezdirmeden alarak, gerçek kullanıcının eriştiği sistemlere erişebilir. Yerine geçme yöntemi ile ise, kötü niyetli kullanıcı çeşitli yöntemlerle, kendisini, veri iletim yolunda gerçek sunucu ya da istemci gibi göstermek suretiyle saldırı gerçekleştirebilir. Örneğin, elektronik posta adreslerine gönderilen iletilerde, saldırgan, istemciyi banka internet adresi yerine, banka internet sitesinin birebir kopyası olan bir internet sayfası hazırlamak suretiyle, kendisine ait olan bir sunucuya yönlendirerek, istemcinin kullanıcı adı ve şifre bilgilerini kendi sunucusuna kaydeder.



Şekil 2.1 : Oturum Cevaplama Atağı



Şekil 2.2 : Oturum Dinleme Atağı

2.1 VPN Tanımı

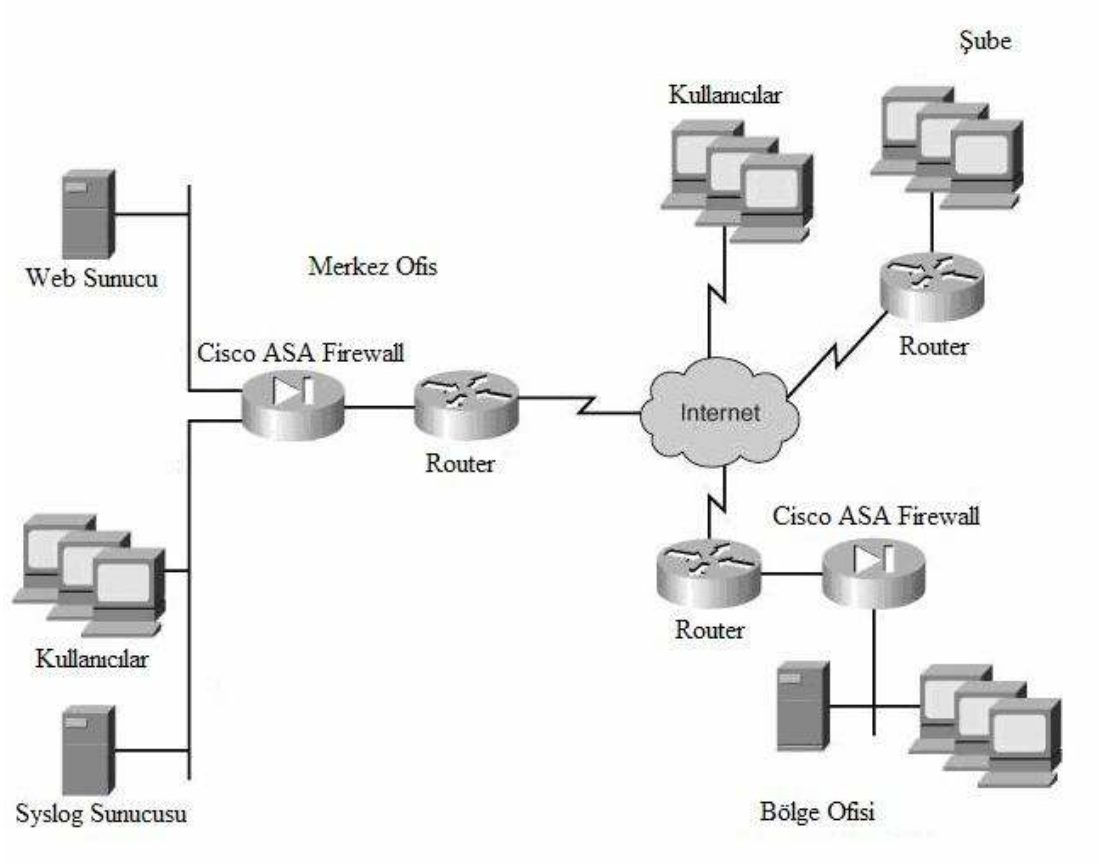
VPN yani özel sanal ağ, tanım olarak, verinin şifrelenerek bir tünel içinden gönderilmesidir. Bu sayede VPN, yukarda bahsedilen saldırı tiplerini önlemede, öncül olarak kullanılmaktadır.

2.2 VPN Bağlantı Modları

VPN temel olarak verinin şifrelenmesi ve sarmalanması (encapsulation) ilkesine dayanır. VPN tipleri de bu işlemlerin yapıldığı noktaya göre temel anlamda ikiye ayrılmaktadır. Bu modlar, taşıma modu ve tünel modudur.

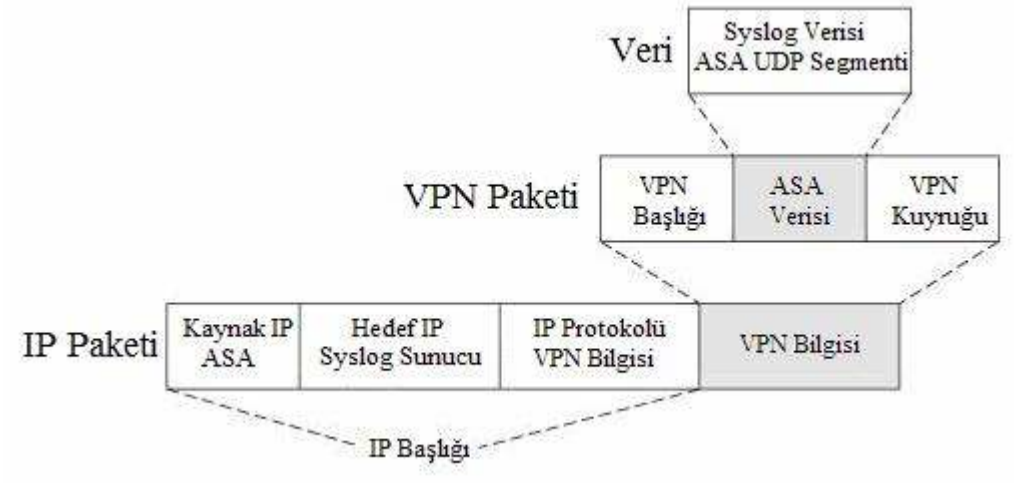
2.2.1 Taşıma modu

Bu mod, cihazdan-cihaza yapılan VPN modudur. Taşıma Modunda VPN bağlantısı, kaynak ile hedef cihazın gerçek IP'leri ile yapılır. VPN üzerinden gönderilecek IP paketi, cihaz üzerinde yapılır. Bu da gerçek IP kullanmayı mecbur kılar.



Şekil 2.3 : Taşıma ve Tünel Modu [6]

Yukarıdaki şekilde bölgesel ofis tarafındaki ASA cihazı üzerindeki syslog mesajları, merkez ofis tarafındaki Syslog Server cihazında gönderilmek isteniyor. Bu durumda Transport Mode ile yapılan sarma (encapsulation) aşağıdaki gibi olmaktadır.

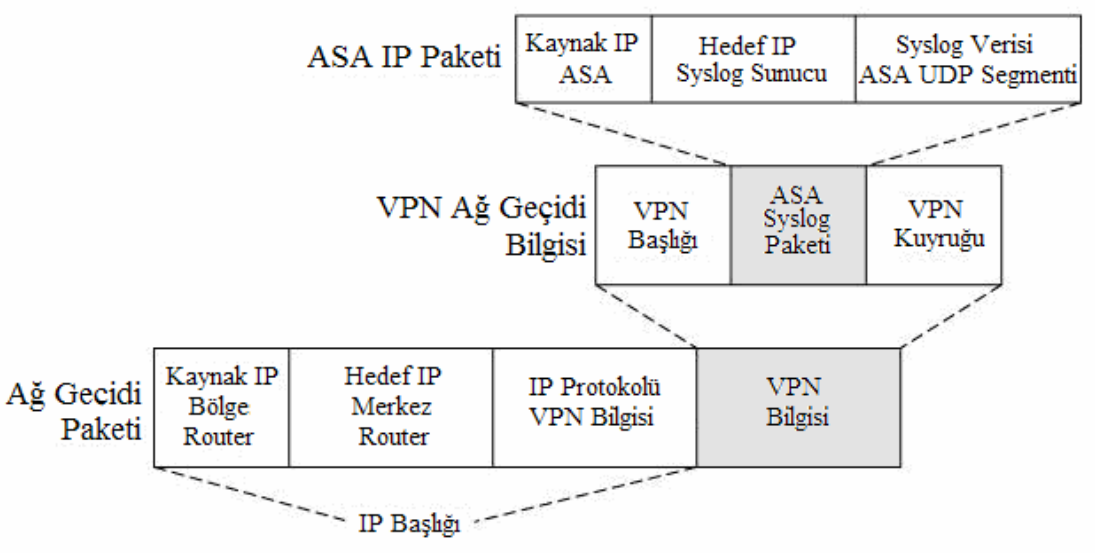


Şekil 2.4 : Taşıma Modu Paket Yapısı [6]

Burada evasdropping denilen internet üzerinden geçen paketleri dinleme anlamına gelen saldırı ile kaynak ve hedef cihazın IP'leri açıkça sezilebilir.

2.2.2 Tünel modu

Tünel Modu, Taşıma modundan farklı olarak, VPN'i cihazdan-cihaza değil, bir ağdan başka bir ağa güvenli iletim için kullanılmak üzere oluşturulan bir moddur. Bu modda yukarıdaki örnekteki sağlanmakta istenen iletişim için sarmalaması aşağıdaki gibi olmaktadır. IP Paketi, bütün olarak, VPN paketine dönüştürülür ve VPN sonlandırıcı cihazın IP başlığı eklenerek karşı tarafa iletilir.



Şekil 2.5 : Tünel Modu Paket Yapısı [6]

2.3 VPN Tipleri

VPN Tiplerini 4 başlıkta toplayabiliriz.

- Uçtan Uca VPNler – Site-to-Site VPNs
- Uzak Erişim VPNler – Remote Access VPNs
- Güvenlik Duvarı VPNler – Firewall VPNs
- Kullanıcıdan Kullanıcıya VPNler – User-to-User VPNs

2.3.1 Uçtan uca VPN (Site-to-site VPN)

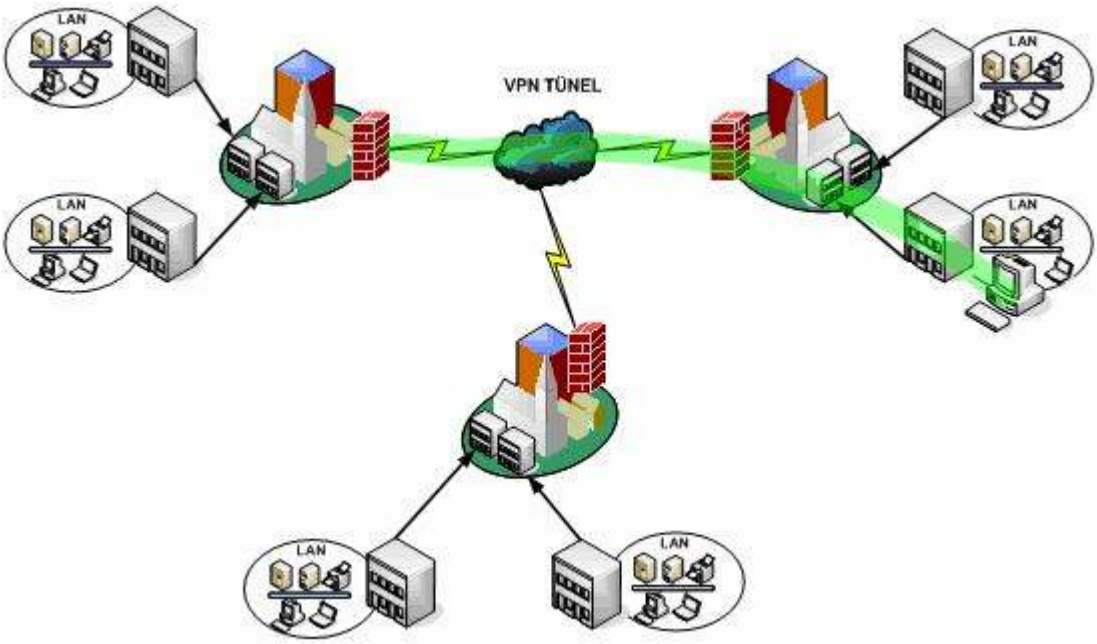
Uçtan-Uca VPN bağlantılar, VPN uç cihazları arasında, tünel modu kullanarak, güvenli iletişimi sağlar.

Uçtan-Uca VPN genel olarak L2L (LAN-to-LAN) olarak da bilinir.

L2L ile her bir lokasyondaki VPN sonlandırıcı cihaz, karşılıklı olarak iletilen trafiğin korunmasını sağlamaktadır.

2.3.2 Uzak erişim VPN (Remote Access VPN)

Uzak erişim VPN bağlantılar daha çok düşük bant genişliği olan kullanıcılar için kullanılan bir VPN tipidir. Uzak erişim VPN tipinde Tünel Modu kullanılır.



Şekil 2.6 : Uzak Erişim VPN

2.3.3 Güvenlik duvarı VPN (Firewall VPN)

Güvenlik Duvarı VPN'ler temelde L2L ve uzaktan erişim VPNlerin ilave olarak güvenlik ve firewall fonksiyonlarının ilave edilmiş hali olarak düşünülebilir. Bu tipteki VPNler genellikle VPN'in bir ucundaki cihazın bağlı olduğu şirketin güvenlik politikası gereği genişletilmiş bir güvenliğe ve firewall fonksiyonlarına ihtiyaç duyması durumunda kullanılır. Firewall fonksiyonları ve genişletilmiş güvenlikten kasıt;

- Stateful (korumalı) filtreleme
- Uygulama katmanında filtreleme
- Adres transfer politikaları

2.3.4 Kullanıcıdan kullanıcıya VPN (User-to-User VPN)

Kullanıcıdan kullanıcıya VPNler, Taşıma Modu kullanır.

Her iki taraftaki cihaz, bir güvenlik duvarı ile bir syslog sunucu, bir yönlendirici ile bir TFTP (Kolay Dosya Transfer Protokolü) server veya bir yönlendiriciye telnet ile bağlanan bir kullanıcı olabilir.

2.4 VPN Kategorileri

VPN bir bilgisayar ağında kullanımı üç farklı kategoride incelenir.

- İntranet
- Extranet
- İnternet

2.4.1 İntranet

Bir intranet VPN bağlantısı bir firmanın kaynakları arasında altyapıyı kullanarak yaptığı bağlantıyı ifade eder.

Taşıyıcı mod bağlantısı ile şirket altyapısı içindeki iki cihaz arasındaki VPN (bir yönlendiricinin bir syslog sunucusuna gönderdiği trafik.), Tünel mod ile bir şirketin farklı lokasyonlarda bulunan iki veya daha fazla şubesi arasındaki özel Frame Relay veya ATM (Asenkron İletim Modu) ağı ile kurulan VPN intranet VPN'lere örnektir.

2.4.2 Extranet

Bir extranet VPN, aralarında anlaşma bulunan iki farklı şirketi birbirine olan bağlantısını ifade eder.

Genel olarak L2L tipteki bağlantılar olmaktadır, ancak diğer tiplerde de olabilir.

2.4.3 İnternet

Internet VPN, iki cihazı birbirine bağlamak için internet omurgasını kullandığı kategori olarak tanımlanır.

2.5 VPN Bileşenleri

VPN uygulamalarının bazı bileşenleri aşağıdaki gibi sıralanabilir.

- Kimlik Doğrulama
- Sarma metodu (Encapsulation)
- Veri şifreleme
- Paket bütünlüğü
- Anahtar Yönetimi
- Uygulama ve Protokol desteği
- Adres Yönetimi

Bu bileşenlerin hepsinin tüm VPN uygulamalarında olması şart değildir.

2.5.1 Kimlik doğrulama

Bir cihaz yada bir lokal ağın VPN kurmadan önce VPN kurmaya yetkili olup olmadığının doğrulanması gerekir. Genel olarak 2 doğrulama kategorisi vardır.

- Cihaz
- Kullanıcı

2.5.1.1 Cihaz için kimlik doğrulama

Cihaz için kimlik doğrulama, VPN ağına bağlanmak isteyen VPN sonlandırıcılar için kimlik doğrulaması yapar. Bunun için iki yol vardır.

- Önceden paylaşılmış olan anahtar / anahtarlar (PSK - pre-shared key)
- Dijital İmza / Dijital Sertifika

Önceden paylaşılmış anahtarlar, daha çok küçük VPN ortamları için uygundur. Bir yada daha fazla anahtar cihazları kimlik doğrulaması için kullanılır. Bir çok ağ yöneticisi, bu kimlik doğrulama metodunu, dijital sertifikaya oranla daha çok tercih eder.

Önceden paylaşılmış anahtarlar, kolay uygulanmasının yanı sıra genişleyen ağlar için ek konfigurasyon gerektirmesi sonucu bir dezavantaj sağlar.

Dijital sertifikalar, geniş VPN uygulamaları için uygundur. Merkez bir cihaz tarafından barındırılan sertifikalara, Certificate Authority (CA) denir ki CA VPN cihazların kimlik doğrulamasında kullanılır.

Topolojiye yeni bir VPN cihazı eklendiğinde, bu cihaz için, bu cihazın kaydını içeren bir sertifika üretilir. Bu da CA tarafından tutulur. Diğer VPN cihazlar, başka bir cihazın kimliğini doğrulamak için CA'ye erişebilirler. Burada da görüldüğü üzere, VPN'deki herhangi bir cihaz bağlanmak istediği cihazın kimlik doğrulama bilgisini lokal olarak saklamak zorunda değildir.

2.5.1.2 Kullanıcı için kimlik doğrulama

Cihaz için kimlik doğrulamadaki problem, önceden paylaşılan anahtarlar gibi, kimlik doğrulama bilgisinin lokal cihazda tutulmasıdır. Bu durum, güvenli yerlerde, örneğin bir servis sağlayıcının veri merkezindeki cihazlar için çok büyük problem teşkil etmez ancak, kişisel bilgisayarlar ve dizüstü bilgisayarlarda bulunan kimlik doğulama bilgileri güvenlik açığı oluşturmaktadır.

Bu sebeple VPN uygulamaları için kullanıcı için kimlik doğrulama gibi yeni bir kimlik doğrulama katmanı eklenmiştir.

Bu tip kimlik doğrulamada kullanıcı bir kullanıcı adı ve şifre ile VPN'e bağlanır.

2.5.2 Sarma metodu (Encapsulation Method)

Sarma metodu, veri gibi kullanıcı bilgilerinin ağ üzerinde nasıl sarmalanıp iletileceği ile ilgilidir. Başka bir ifade ile içeriğin formatının ne olacağına karar verilir. Sarmalama işlemi

- VPN başlık ve kuyruk bilgisinde bulunan alanlar
- Alanların diziliş sırası
- Alanların büyüklüğü

İle ilgilidir.

Sarmalama metodu bazı güvenlik duvarı ve adres çevirme (NAT : Network Address Translation) durumlarında daha çok önem kazanmaktadır.

2.5.3 Veri şifreleme

Veri şifreleme, internet üzerinde yol alan paketlerin okunmasını önlemek için gereklidir.

Temel olarak, kullanıcı verisini bir şifreleme algoritmasına koyarak verinin anlaşılmaz olmasını sağlar.

Karşı taraf, gönderici tarafın kullandığı algoritmayı ve anahtar kelimeyi kullanarak veriyi deşifre eder ve kullanıcı vericisi güvenli olarak taşınmış olur.

En çok kullanılan veri şifreleme algoritmaları

- DES (Data Encryption Standart) (56 bitlik anahtar)
- 3DES (Triple Data Encryption Standart) (168 bitlik anahtar)
- AES (Advanced Encryption Standart) (128 – 192 ve 256 bitlik anahtar)

2.5.4 Paket bütünlüğü

Veri şifreleme, cihaz işlemcisini yoran bir bileşendir. Bir VPN sonlandırıcı cihazın şifreleme yapması onu spoofing saldırılar denilen saldırı metodunun hedefi haline getirebilir. Spoofing, bir istemcinin, IP adresini karşı tarafa olduğundan farklı göstermesidir.

Bu yüzden bazı VPN uygulamaları paket bütünlüğü (paket kimlik doğrulaması) kontrolü sağlamaktadır. Paket bütünlüğü kontrolü pakete bir imza eklemesi ile yapılır. Bu imza, karşılıklı paylaşılan anahtarlara bir takım işlemler sonucu oluşturulan bir çıktıdır.

3. VPN TEKNOLOJİSİ

3.1 Anahtarlar

Anahtar genel olarak kullanıldığı terim anlamıyla, başkasının erişmek istemediği size ait olan bir varlığı korumaya yönelik kilitlemek için kullanılan aletin adıdır.

Bilgisayar ağı güvenliğinde kullanılan anahtar farklı işlemler için kullanılmaktadır.

Bunlar,

- Şifrelemek
- Paket bütünlüğünü sağlamak
- Kimlik Doğrulamak

Anahtarlama iki farklı çeşit ile gerçeklenir.

- Simetrik
- Asimetrik

3.1.1 Simetrik anahtarlar

Simetrik anahtarlar bilgi saklamak için karşılıklı aynı ve tek bir anahtarın kullanıldığı anahtarlama algoritmasıdır. Şifreleme işlemlerini gerçekleştirdikten sonra şifreli metni alıcıya gönderirken şifreli metinle birlikte gizli anahtarı da alıcıya güvenli bir şekilde göndermesi gerekmektedir. Karşılıklı aynı anahtar kullanıldığı için temelde basit bir yöntem olup çok hızlı işlem gerçeklenir [7].

3.1.2 Asimetrik anahtarlar

Asimetrik anahtarlamada kullanılan iki tip anahtar vardır

- Özel Anahtar
- Genel Anahtar

Özel anahtar gizli bir anahtardır ve kimseyle paylaşılmaz. Genel anahtar diğer cihazlarla paylaşılan bir anahtardır. Bu iki anahtar için rasgele bir seçim yapılamaz. Bunun yerine özel bir algoritma kullanılır çünkü her iki anahtar arasında güvenliği ve kimlik doğrulamayı sağlamak için özel bir ilişki mevcuttur.

Asimetrik anahtarlar iki temel güvenlik fonksiyonunu gerçeklemek için kullanılır.

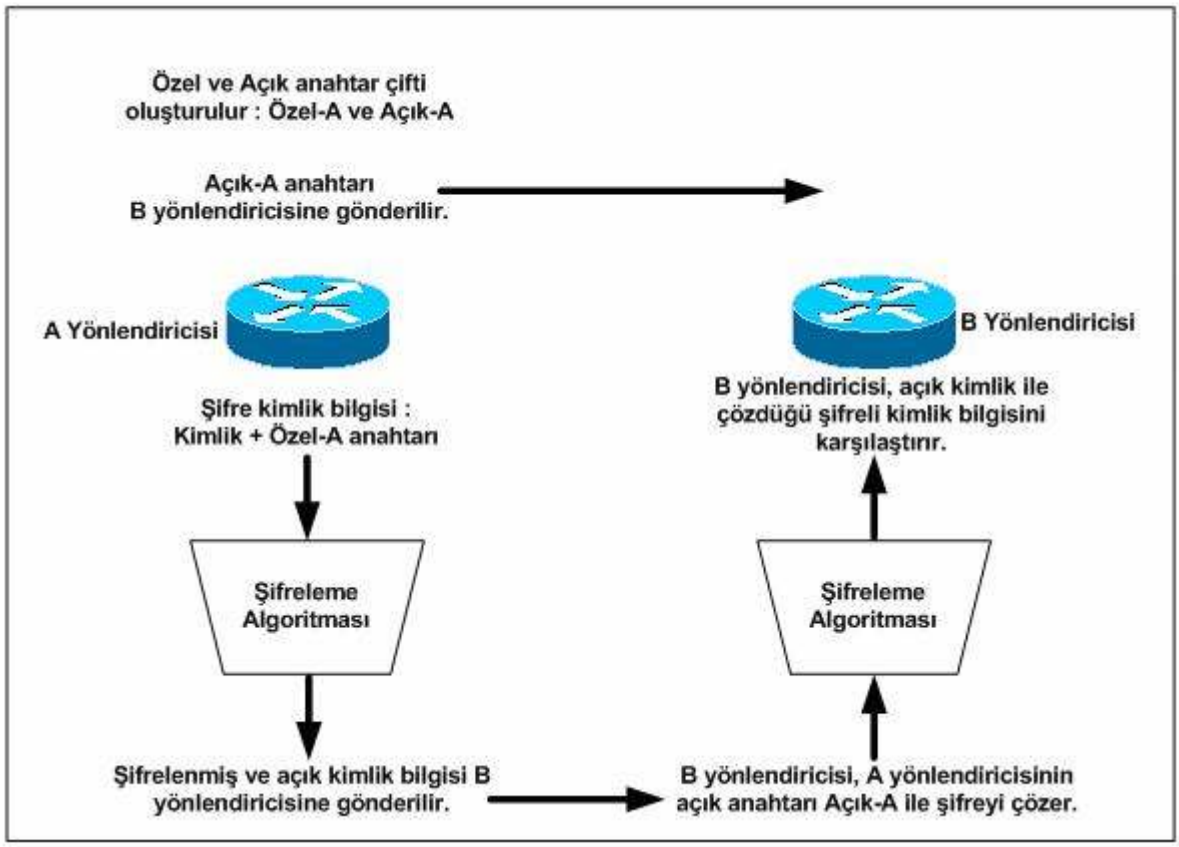
- Şifreleme
- Kimlik Doğrulama

3.1.2.1 Asimetrik anahtarlama ve şifreleme

Asimetrik anahtarlar veri şifrelemesinde kullanılabilir. Bunun için şifrelemeyi yapacak cihaz önce bir çift özel ve genel anahtar (private/public key) üretir. Örnek olarak iki yönlendirici arasında veri şifreleneceğini düşünelim. İlk olarak A yönlendiricisi ile B yönlendiricisi birbirlerine genel birer anahtar üreterek paylaşırlar. B yönlendiricisi, A yönlendiricisine göndereceği veriyi genel (public) anahtar ile şifreler ve gönderir. Asimetrik anahtarlamada, sadece ilgili özel anahtar veriyi açmak için kullanılır. Bu sebeple A yönlendiricisi aldığı şifreli veriyi kendi ürettiği özel anahtar ile açar. Aynı durum tam tersi yönde de gerçeklenir. A yönlendiricisi de B yönlendiricisinden aldığı genel anahtar ile veriyi şifreleyerek B yönlendiricisine gönderir. B yönlendiricisi de kendi özel anahtarı ile veriyi açar. Her iki cihazda sadece genel anahtarları birbirine gönderirken, özel anahtarlar hiç bir zaman paylaşılmaz. Bu sebeple genel anahtarı ve şifrelenmiş veri paketini, ağ üzerinden geçen paketleri kopyalayan biri alsa bile, veriyi açacak (decryption) özel anahtar olmadığı için, özel bilgiye ulaşamaz [8].

3.1.2.2 Asimetrik anahtarlama ve kimlik doğrulama

Şifrelemenin yanı sıra, asimetrik anahtarların bir diğer kullanımı kimlik doğrulamasıdır. Aşağıdaki şekilde asimetrik anahtarlamanın kimlik doğrulamasında kullanımı gösterilmiştir.



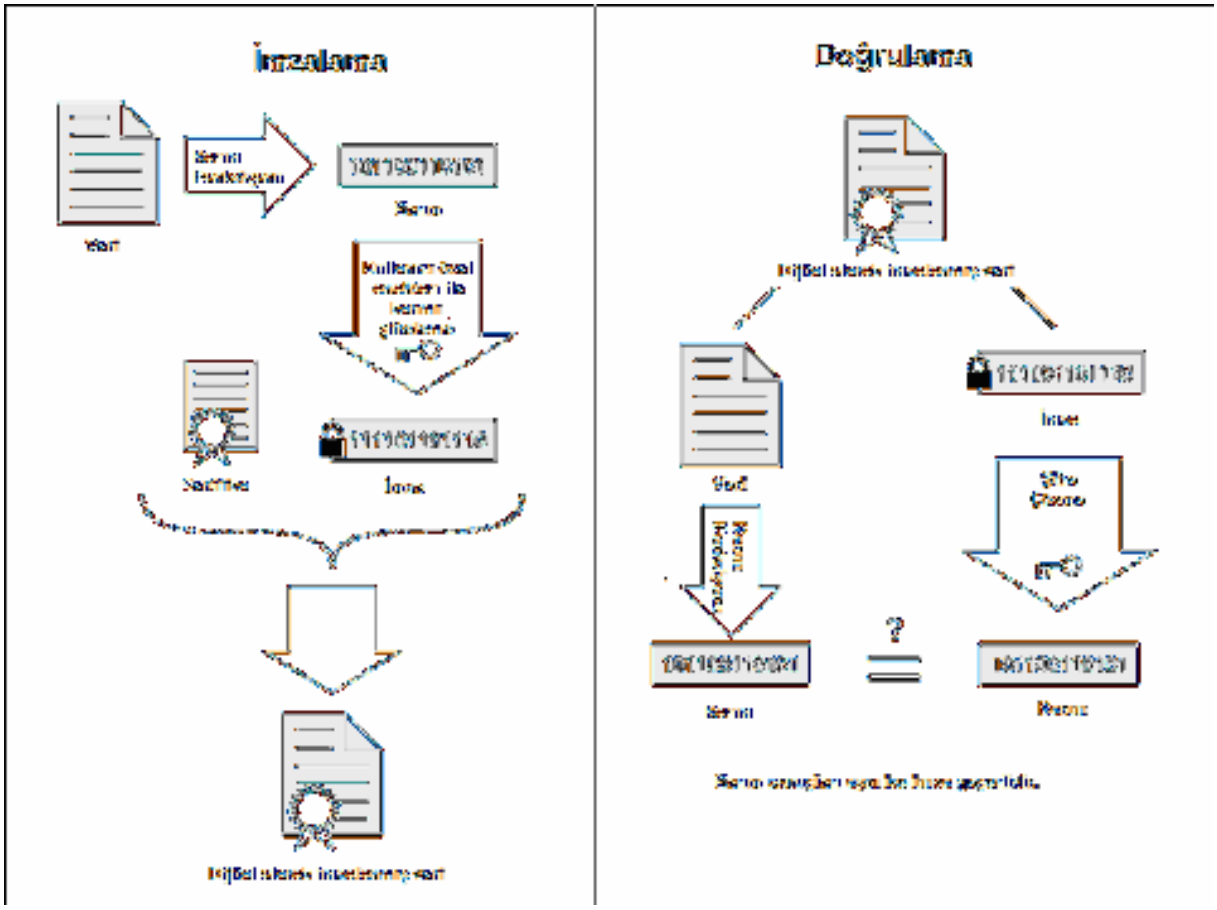
Şekil 3.1 : Asimetrik Anahtarlar ile Kimlik Doğrulama

Şekilde görüldüğü üzere,

- A yönlendiricisi genel ve özel anahtar çiftini oluşturur.
- A yönlendiricisi açık anahtarını B yönlendiricisi ile paylaşır.
- A yönlendiricisi kendi kimlik bilgisini kendi özel şifresi ile şifreler
- A yönlendiricisi kendi kimlik bilgisi ile şifreli kimlik bilgisini B yönlendiricisine gönderir.
- B yönlendiricisi şifrelenmiş kimlik bilgisini açar ve A yönlendiricisinin gönderdiği şifrelenmemiş kimlik bilgisi ile karşılaştırır.
- Eğer her iki kimlik bilgisi birbirinin aynısı ise, B yönlendiricisi, şifreleme işlemini A yönlendiricisinden yaptığından emin olur.

Bu örnekteki özel anahtar, şifrelemede olduğu gibi paylaşılmaz. Genel (public) anahtar karşı tarafla paylaşılır ve karşı tarafın kimlik doğrulaması için kullanılır.

Özel anahtarla şifrelenen bu kimlik bilgisine, bilinen adı ile dijital imza denir. Dijital imzanın doğruluğu imzanın içeriği, alıcıya iletilen mesaj ve açık anahtar kullanılarak kanıtlanır [9].



Şekil 3.2 : Dijital İmza ile Kimlik Doğrulama

3.1.2.3 Asimetrik anahtarlama çeşitleri

- **RSA genel anahtarlama :** En yaygın olarak kullanılan açık anahtarlama kripto sistemi Rivest, Shamir ve Adelman tarafından bulunmuştur [10]. RSA anahtarlama, kimlik doğrulamada kullanılan dijital imza oluşturmada ve şifrelemede kullanılır. RSA anahtarlama, sertifikalarda bulunan dijital imzalarla kullanılır. 512, 768, 1024 bit ve daha yüksek büyüklükte anahtarlamayı destekler.
- **Dijital imza algoritması (DSA) :** RSA'ya benzer şekilde sertifikalar için dijital imza oluşturmada kullanılır. Ancak şifreleme fonksiyonları için kullanılmaz.

- **Diffie-Hellman (DH) :** Bu anahtarlama, IPSec VPN'lerde kullanılan, IKE (internet anahtar değişimi) protokolü tarafından, anahtarlama bilgisi ve anahtarları IPSec cihazları arasında paylaşırken kullanılır.
- **KEA (Anahtar değişim algoritması) :** DH anahtarlama metodunun gelişmiş versiyonu olarak değerlendirilir.

3.1.2.4 Asimetrik anahtarlamanın avantajları ve dezavantajları

Asimetrik anahtarlamanın, simetrik anahtarlamaya bir çok üstünlüğü vardır. Öncelikle, çok büyük asal sayılar kullanılarak oluşturulduğu için simetrik anahtarlara göre koruma prosesi çok daha güvenlidir. Bilindiği gibi asal sayı kendinden ve birden başka bir sayıya bölünemeyen sayıdır. İki büyük asal sayı çarpılarak ve ilave bilgiler eklenerek, genel ve özel anahtarlar oluşturulur.

Bu güne kadar asimetrik anahtarla şifrelemeyi makul bir sürede kıracak bir metod yoktur. Örnek olarak, 34,555 ve 88,333 asal sayıları çarpıldığında elde edilen 3,052,346,815 sayısının hangi iki sayının çarpımından oluştuğunu bulmak ömür boyu sürebilir. Veriyi deşifre etmek, özel ve genel anahtarları bilmeyi gerektirdiğinden, özel anahtarların paylaşılmaması sebebiyle, veri hiçbir şekilde deşifre edilemez.

Bütün bunlar göz önüne alındığında asimetrik anahtarlama bir çok algoritma asimetrik anahtarlamayı kullanır. Ancak, asimetrik anahtarlama, simetrik algoritmaya göre yaklaşık 1500 kat yavaştır. Bu sebeple, veri şifrelerken, gecikme, işleme koyma süresi öncelikli unsur ise, simetrik anahtarlama tercih edilmelidir [6].

3.1.2.5 RSA anahtarlama için veri şifreleme örneği

RSA üç adımda gerçeklenir. Birinci fazda özel ve genel anahtarlar oluşturulur. İkinci fazda veri şifrelenir. Üçüncü fazda şifrelenmiş metin açık metine dönüştürülür [11-14].

RSA faz 1 : Özel ve genel anahtarları belirleme

Özel ve Genel anahtarları hesaplamak için her iki taraf da aşağıdaki adımları gerçekleştirir.

1. İki tane büyük asal sayı seçilir (Bunlara P ve Q diyelim)
2. P ve Q'nun çarpımından N elde edilir.

3. F(n) fonksiyonu olarak (P-1)(Q-1) hesaplanır.
4. N ile 1 arasında öyle bir E sayısı seçilir ki EBOB(e, F(n)) = 1 olsun. Açık anahtar {E,n} olarak belirlenir.
5. E.D ≡ 1 (mod F(n)) eşitliğini sağlayacak bir D sayısı hesaplanır. Özel (gizli) anahtar {D,n} olarak belirlenir.

RSA faz 2 : Veriyi şifreleme

M mesajını RSA ile şifrelemek için Mesaj boyu 1<M<N-1 olacak şekilde mesaj boyutu belirlenir ve M Mesajı

$C = M^E$ (Mod N) olarak C şifrelenmiş metin (chiphertext) oluşturulur ve alıcıya gönderilir.

RSA faz 3 : Şifrelenmiş veriyi çözme

Şifreli metini deşifre etmek için aşağıdaki formül uygulanır

C^D (Mod N) = M

Burada M mesajı gönderen tarafından şifrelenen düz metindir.

RSA örneği

İki asal sayı ele alınsın. Bu asal sayılar 3 ve 11 olsun.

N = P.Q = 3.11 = 33

F(n) = (P-1).(Q-1) = 2.10 = 20

E sayısı olarak 3'ü seçelim. (EBOB(3,20) = 1)

D.E ≡ 1 (mod F(n)) eşitliğinden D.3 ≡ 1 (Mod 20) eşitliğinden D=7 olarak hesaplanır.

Bu durumda açık anahtar = (N,E) = (33,3)

Gizli anahtar = (N,D) = (33,7) olur.

Diyelim ki M=7 mesajı şifrelenmek isteniyor olsun.

$C = M^E$ Mod N = 7^3 Mod 33 = 343 Mod 33 = 13

Böylece açık metin 7 için şifreli metin 13 olur.

Şifrelenmiş veriyi açmak için elimizde bulunan C şifreli metin, D ve N değerleri ile formülü uygularsak

$M = C^D \text{ Mod } N = 13^7 \text{ Mod } 33 = 7$ olarak bulunur.

Aşağıda M mesajının 0 ile 32 arasındaki değerlerinin şifreli metin değerleri görülmektedir.

m 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

c 0 1 8 27 31 26 18 13 17 3 10 11 12 19 5 9 4

m 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

c 29 24 28 14 21 22 23 30 16 20 15 7 2 6 25 32

3.2 Şifreleme

Şifreleme, verinin iletimi boyunca şifrelemede kullanılan anahtarlar bilinmeden açılması mümkün olmayan biçime getirilmesi prosesidir.

3.2.1 Şifreleme işlemi

Şifreleme işlemi, kullanılan simetrik ve asimetrik anahtarlama metoduna göre değişir. Simetrik anahtarlamada karşılıklı kullanılan aynı anahtar ile şifreleme ve şifre çözme işlemi gerçekleştirilir. Asimetrik anahtarlamada ise paylaşılan genel anahtarlar ile şifrelenen veri, ancak paylaşılmayan özel anahtar ile açılabilir.

Asimetrik anahtarlama, şifreleme ve şifreyi çözme açısından simetrik anahtarlamaya göre yavaş olduğu için daha çok kimlik doğrulama için kullanılır. Şifreleme işlemi için ise simetrik anahtarlama yöntemi daha yaygın olarak kullanılır.

3.2.2 Şifreleme algoritmaları

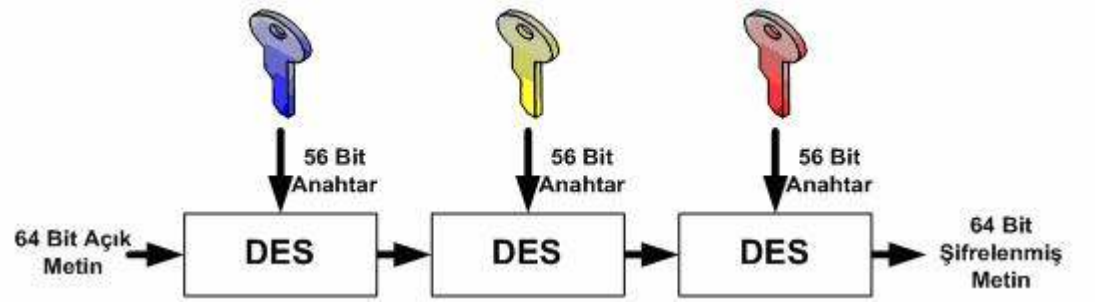
En çok bilinen simetrik şifreleme algoritmaları,

- DES ve 3DES
- AES
- Blowfish

3.2.2.1 DES ve 3DES algoritmaları

Data şifreleme standardı (DES) : DES, 1977 yılında Uluslararası Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilmiştir. 64-bitlik bir anahtarlama yapısı kullanır ancak bunun 8-bitlik bölümü hata kontrolü için kullanılır. Bu sebeple efektif olarak 56-bitlik bir anahtarlama yapısı kullanır. Bu da 7 karakter demektir. 1970'li yıllarda kırılamaz gibi görünen 7 karakterlik şifreler, günümüz simetrik anahtarlama yapısında çok zayıf kalmaktadır.

Üç DES (3DES) : 3DES, DES algoritmasının 3 kez farklı anahtar ile oluşturulan yapısıdır. Uygulanan 3 anahtar aynı olması durumunda DES yerine kullanılabilir [15]. DES 56-bitlik anahtarlama kullandığı için, 3DES, 168-bitlik bir anahtarlama yapısı kullanmaktadır. 3DES, DES'e göre çok daha güçlü olmasına rağmen daha yavaştır.



Şekil 3.3 : 3DES

3.2.2.2 AES algoritması

AES yine NIST tarafından 2002 yılında 3DES'in yerine oluşturulmuş bir standarttır. 3DES'ten daha güçlü ve daha hızlı bir şifreleme algoritmasıdır. Kriptografi araştırmacıları Dr. Joan Daemen ve Dr. Vincent Rijmen tarafından geliştirildiğinden, Rijndael adı ile de bilinir [16].

3.2.2.3 Blowfish algoritması

1993 yılında DES algoritmasının yerini alması için tasarlanmış şifreleme algoritmasıdır.

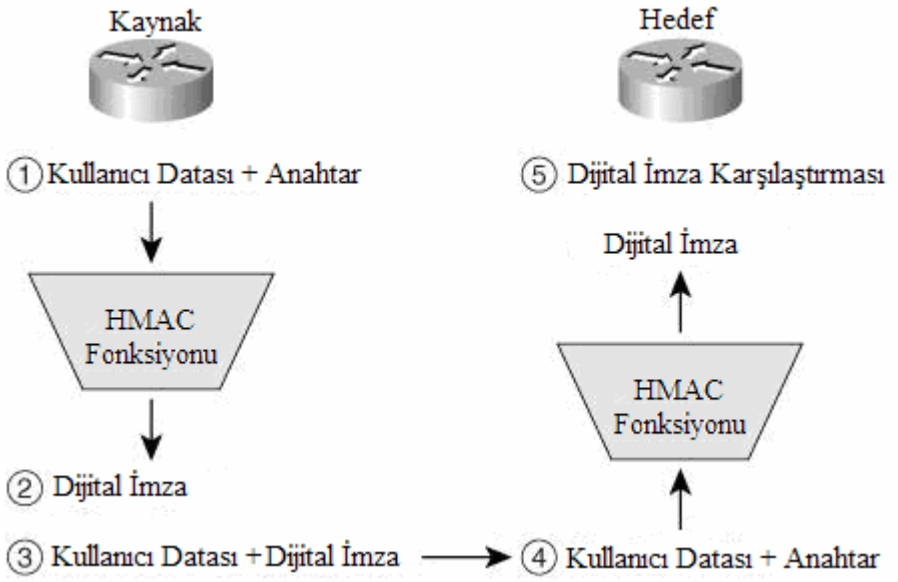
3.3 Paket Kimlik Doğrulama

Alınan paketin doğrulanması verinin doğru kaynaktan gelip gelmediği ve verinin değişikliğe uğrayıp uğramadığı ile ilişkilidir.

Sağlama (hashing) fonksiyonları, kullanıcı verisini ya da paketi gibi değişken uzunluklu veri paketini alarak dijital imza üretmede kullanılırlar. Sistem çıkışı her zaman sabit uzunlukta bir veridir. Sağlama fonksiyonuna aynı giriş uygulandığı sürece çıkış da hep aynıdır, değişmez.

Sağlama mesajı kimlik doğrulama kodları (HMAC) fonksiyonları sağlama fonksiyonlarının bir alt kümesi olarak değerlendirilir. HMAC fonksiyonları veri paketlerinin kimlik doğrulama problemlerini ortadan kaldırmak için geliştirilmiştir. HMAC fonksiyonları dijital imza yada parmak izi ile adlandırılan çıktıyı üretirken paylaşılmış simetrik anahtar kullanırlar.

HMAC fonksiyonları ile aynı veri ve aynı gizli anahtar kullanıldığı sürece oluşturulan imza hep aynıdır. Kullanılan veri yada gizli anahtarlardan biri değişirse imza da değişir.



Şekil 3.4 : Paket Kimlik Doğrulama [6]

- Kaynak cihaz kullanıcı verisi ve anahtarı HMAC fonksiyonuna sokmaktadır.
- HMAC fonksiyonunun çıkış bir dijital imza ya da parmak izidir.
- Kaynak cihaz HMAC fonksiyonuna girdi olarak verdiği orijinal data ile dijital imzayı hedef cihaza gönderir.
- Hedef cihaz dijital imzayı doğrulamak için aynı işlemi gerçekleştirir. Kaynak cihaz tarafından gönderilen veri ile önceden paylaşılan anahtar ile aynı HMAC fonksiyonuna sokar ve bir dijital imza elde eder.

- Hedef cihaz, elde ettiği dijital imza ile kaynak cihaz tarafından gönderilen dijital imzayı karşılaştırır. Eğer dijital imzalar aynı ise, gönderilen verinin ancak önceden paylaştığı anahtarı kullanan kaynak cihaz tarafından gönderildiği doğrulanır ve veri kabul edilir. Eğer dijital imzalar farklı ise, verinin, izlediği yol boyunca, bir saldırgan tarafından, ya da herhangi bir şekilde değiştirildiği anlamı taşır ve veri reddedilir.

Bir çok VPN uygulamasında HMAC fonksiyonları kullanılmaktadır. IPSec Kimlik doğrulama başlığı (AH - Authentication Header) ve Sarmalama Güvenlik Verisi (ESP - Encapsulation Security Payload) HMAC kullanmaktadır. En çok kullanılan iki HMAC fonksiyonları MD5 ve SHA'dır.

3.3.1 MD5 HMAC fonksiyonu

MD5 (Mesaj Digest) HMAC fonksiyonu 1994 yılında Ronald Rivest tarafından geliştirilmiş bir fonksiyondur. MD5 128-bit uzunluğunda bir imza üretir. SHA HMAC fonksiyonuna göre daha az güvenli ama daha hızlıdır.

3.3.2 SHA HMAC fonksiyonu

SHA (Güvenli Sağlama Algoritması), NIST tarafından geliştirilmiş bir algoritmadır. Orijinal SHA algoritmasının ilk versiyonu 1994 yılında SHA-1 olarak ortaya çıkmıştır. SHA-1, 160-bitlik bir imza ürettiğinden MD5'e göre daha güvenli ancak daha yavaştır.

2005 yılında belirli grupların çalışmaları sonucunda, ilk önce MD5'de bir süre sonra da SHA-1'de farklı verilerden aynı imzanın üretilebileceği ortaya atılmıştır. VPN uygulamalarının çok fazla etkilenmediği bu durum diğer uygulamalarda daha büyük problemlere yol açacağı düşünüldüğünden SHA algoritmasının 256-bitlik ve 512-bitlik versiyonları için çalışmalar yürütülmektedir.

3.4 IPSec (İnternet protokol güvenliği)

IPSec (Internet Protokol Güvenliği), cihazlar arasındaki trafiğin nasıl korunacağını belirten IETF tarafından geliştirilmiş bir standarttır. Güvenlik ağ geçitleri ya da kullanıcı cihazları arasında IP trafiğini koruma amaçlı bir dizi protokoller kullanır [17].

IPSec 3 ana özellik sağlamaktadır:

- Kimlik Denetimi Başlığı olarak adlandırılan Kimlik-Denetimi özelliği
- Sarmalanmış güvenlik yükü (ESP) olarak adlandırılan kimlik denetimi ve de şifreleme özelliği,
- Anahtar değiş-tokuş özelliği

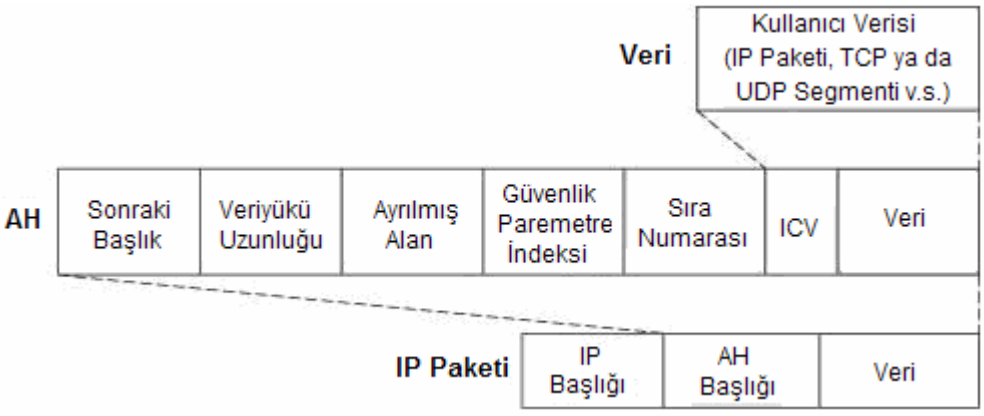
Özel Sanal Ağlar için kimlik denetimi ve şifreleme istenen özelliklerdir, çünkü yetkisi olmayan kullanıcıların özel ağların içine girmemesinin garantilenmesi ve internet üzerinden hattı gizlice dinleyenlerin özel sanal ağlar üzerinden gönderilen mesajları deşifre etmemesi gerekmektedir. IPSec kaynak için kimlik denetimi, veri içeriği kontrolü ve de veri bütünlüğünün güvenliğini sağlamaktadır

3.4.1 IPSec Protokolleri

IPSec de IP datagramlarının korunması iki protokol sayesinde sağlanır. Bunlar Kimlik Denetimi Başlığı (AH) ve Sarmalanmış edilmiş güvenlik veri yüküdür (ESP). AH temel olarak veri içeriğinin kontrolü ve kullanıcı kimlik denetimi gibi özellikleri barındırır. ESP, AH ile benzer özellikleri taşır ve opsiyon olarak verinin şifrelenerek güvenli bir şekilde iletilmesini sağlar.

3.4.1.1 AH (Kimlik denetim başlığı)

Kimlik denetim başlığı protokolü, veri içeriği kontrolü ve veri kullanıcı kimlik denetimi gibi temel güvenlik fonksiyonlarını barındırır.



Şekil 3.5 : AH Paket Yapısı [6]

Sonraki Başlık : Bu alan, verinin hangi sarmalama (encapsulation) protokolünü kullandığını belirtir. (TCP için protokol numarası 6, UDP için17 gibi)

Veri yükü Uzunluğu : Bu alan AH başlığının uzunluğunu belirler.

Ayrılmış Alan: Bu alan ayrılmış ancak kullanılmayan bir alandır.

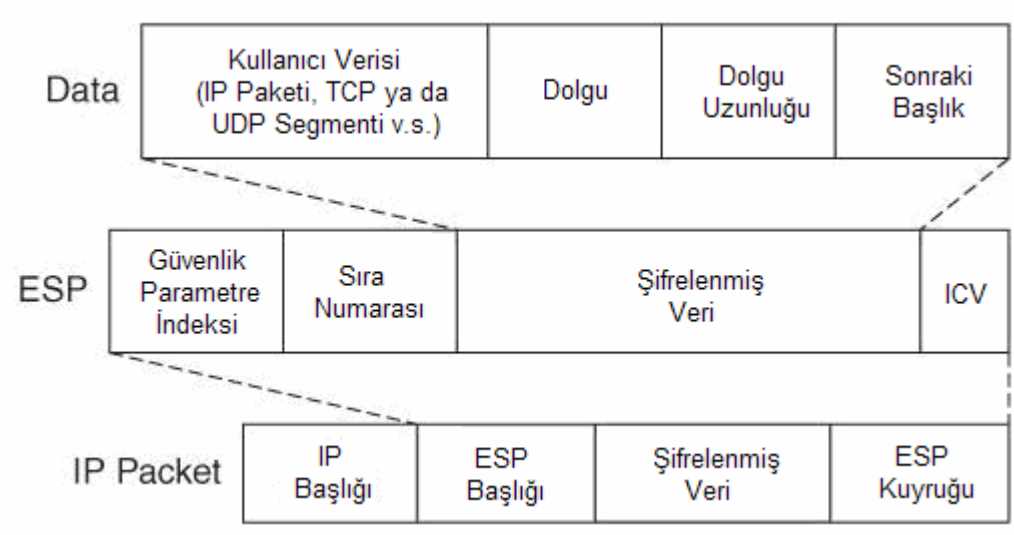
Güvenlik Parametre İndeksi (SPI) : Bu alan uzak cihaza yapılan bağlantıya verilen eşsiz bir nümerik değerdir. Bu numara sayesinde çift taraflı oluşturulan farklı bağlantılar birbirinden ayrılmaktadır. 4 byte uzunluğunda bir alandır.

Sıra Numarası : Bu alan verinin alış verişi sırasındaki her bir pakete verilen ve o pakete özgü sıra numarasıdır.

Bütünlük Kontrol Değeri (ICV) : Bu alan kimlik doğrulaması bilgisinin tutulduğu alan yani MD5 ya da SHA-1 HMAC fonksiyonu ile üretilen dijital imzadır.

3.4.1.2 ESP (Sarmalanmış Güvenlik Veri yükü)

Sarmalanmış güvenlik veri yükü (ESP), kimlik denetim başlığının (AH) sağladığı servis tiplerini sağlamakla beraber, verinin şifrelenmesini de sağlar. Ayrıca ESP'nin veri kimlik doğrulama ve bütünlük servisi, sadece ESP başlığı ve veri yükünü kapsar IP başlığını kapsamaz. Bu sebeple, herhangi bir sebeple IP başlığında yapılan değişiklik ESP tarafından algılanamazken AH buna izin vermez [11]. Elbette bu IP paket başlığının değiştirilmesi gereken durumlarda, örneğin ağ adres çevirimi (NAT) yapılması gereken durumlarda bir avantaj sağlamaktadır.



Şekil 3.6 : ESP Paket Yapısı [6]

3.4.2 Güvenlik bağlantıları (Security Association)

Karşılıklı olarak kurulacak IPSec VPN yapısı kurulmadan önce kullanılacak kimlik doğrulama ve şifreleme algoritmaları gibi parametreler üzerinde anlaşma sağlanması gerekmektedir.

Güvenlik bağlantıları her iki tarafın haberleşmeye başlaması için güvenlik ayarlarının kurulması aşamasında yapılan anlaşmayı ifade eder.

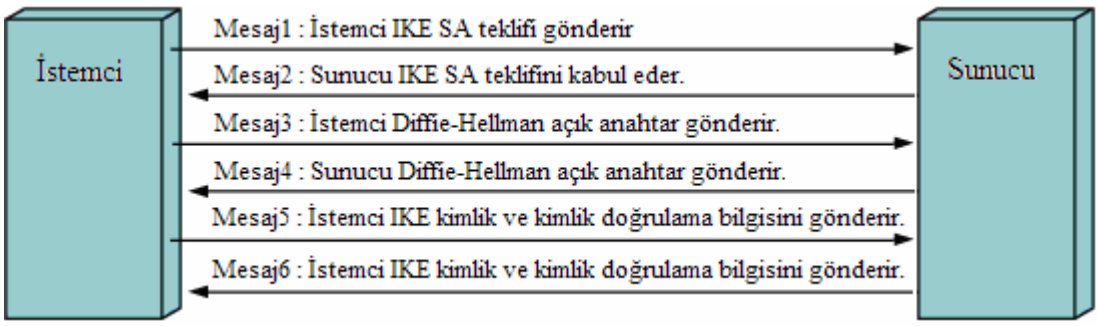
Güvenlik bağlantıları tek yönlüdür. Bunun anlamı güvenlik parametrelerinin tanımlanması aşamasında ağ geçidine giren ve çıkan trafik olmak üzere iki ayrı güvenlik bağlantısı oluşturulur. Güvenlik bağlantıları, IPSec protokolünü kullanarak bağlantı yapan cihazda küçük bir veritabanında saklanmaktadır. Her bir güvenlik bağlantısı, AH ve ESP paketleri içersinde tanımlı olan Güvenlik Parametre İndeksi (SPI) ile eşleştirerek, doğru güvenlik bağlantısını bulur.

Güvenlik bağlantılarının kurulmasında anahtar değişimini yapan ve yöneten protokole IKE (Internet Key Exchange) denir.

IKE bu görevi yapabilmek için iki protokol kullanır.

ISAKMP: Açılımı Internet Security Association and Key Management Protocol olan ISAKMP security associationların (SA) oluşturulması, kararlaştırılması, değiştirilmesi ve silinmesinden sorumludur. Şifreleme, kimlik doğrulama ve veri bütünlüğü algoritmalarından hangileri VPN bağlantımızda kullanılacağı ISAKMP protokolü ile belirlenir. Veri iletişiminin transport mod mu yoksa tünel mod mu olacağına bu protokol ile karar verilir. ISAKMP protokolü ile anahtar değişimi yapılmaz.

Oakley: Oakley protokolü IKE protokolü içindeki anahtar değişiminden sorumlu protokoldür. Anahtar oluşturulması ve paylaşılması için Diffie-Hellman tekniğini kullanır.



Şekil 3.7 : Güvenlik Bağlantıları (SA)

3.4.3 Diffie-Hellman algoritması

Diffie-Hellman (DH) algoritması VPN uygulamalarında, internet gibi güvenli olmayan ortamlar üzerinde, güvenli bir şekilde, DES, 3DES, AES, SHA ve MD5 gibi simetrik anahtarlama kullanan algoritmaların anahtar paylaşımı için kullanılan algoritmadır. Asimetrik bir anahtarlama yöntemini kullanır. DH, açık anahtar şifreleme sistemini kullandığı için, açık anahtar değişim metodu olarak da bilinir.

Diffie-Hellman açık anahtar değişimi algoritması, 1976 yılında geliştirilen ve açık olarak kullanıma sunulan günümüzdeki yaygın olarak kullanılan ilk anahtar paylaşım metodudur.

Diffie-Hellman ortak gizli anahtar oluşturma güvenilirliği çok büyük asal sayılar seçmeye dayanmaktadır [18].

Ali (A) ve Banu (B) , birbirleri ile açık olarak paylaşmadıkları ortak bir anahtar belirleyecek olsunlar.

Yeterince büyük bir p asal sayısı ile p'de asal kök olan g sayısı her iki kişi tarafından bilinsin. Buna göre,

A, $0 \leq a \leq p\text{-}2$ eşitsizliğini sağlayan ve tesadüfi olan bir a sayısı seçer. $c = g^a \pmod p$ yı hesaplar ve B'ye gönderir.

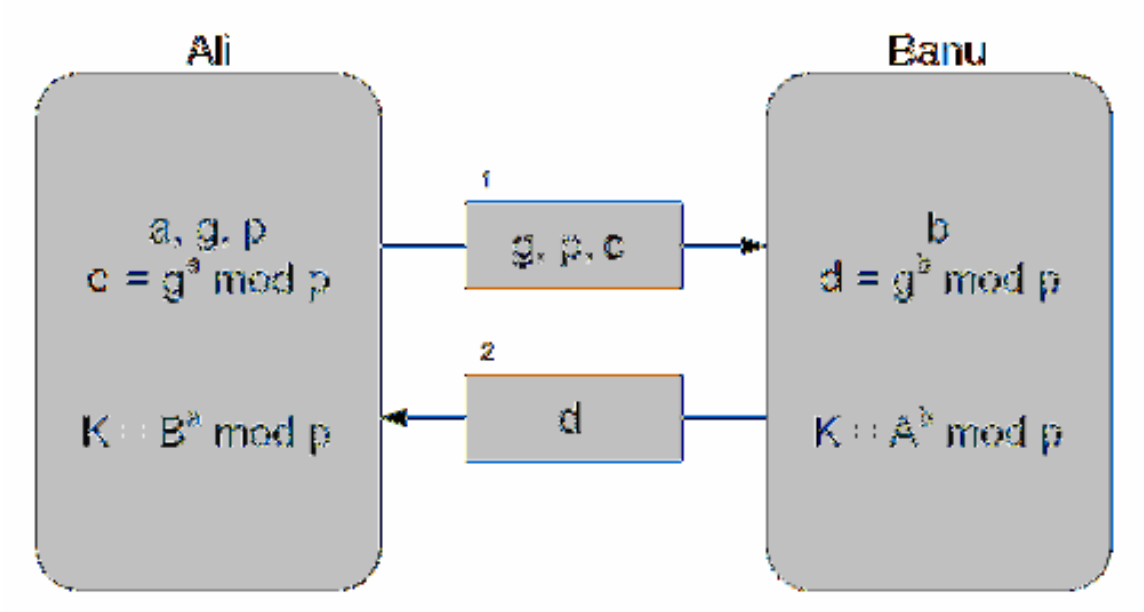
B, $0 \leq b \leq p\text{-}2$ eşitsizliğini sağlayan ve tesadüfi olan bir b sayısı seçer. $d = g^b \pmod p$ yı hesaplar ve bunu A'ya gönderir.

A, ortak anahtar k' yı şu şekilde hesaplar:

$$k = d^a = (g^b)^a \pmod p$$

B, ortak anahtar k' yı şu şekilde hesaplar:

$$k = c^b = (g^a)^b \pmod p$$



Şekil 3.8 : Diffie-Hellman Anahtar Değişimi Yöntemi

3.4.3.1 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.

3.4.4 İnternet anahtar değişim (IKE) fazları

IKE işleyişi 2 faza ayrılmıştır.

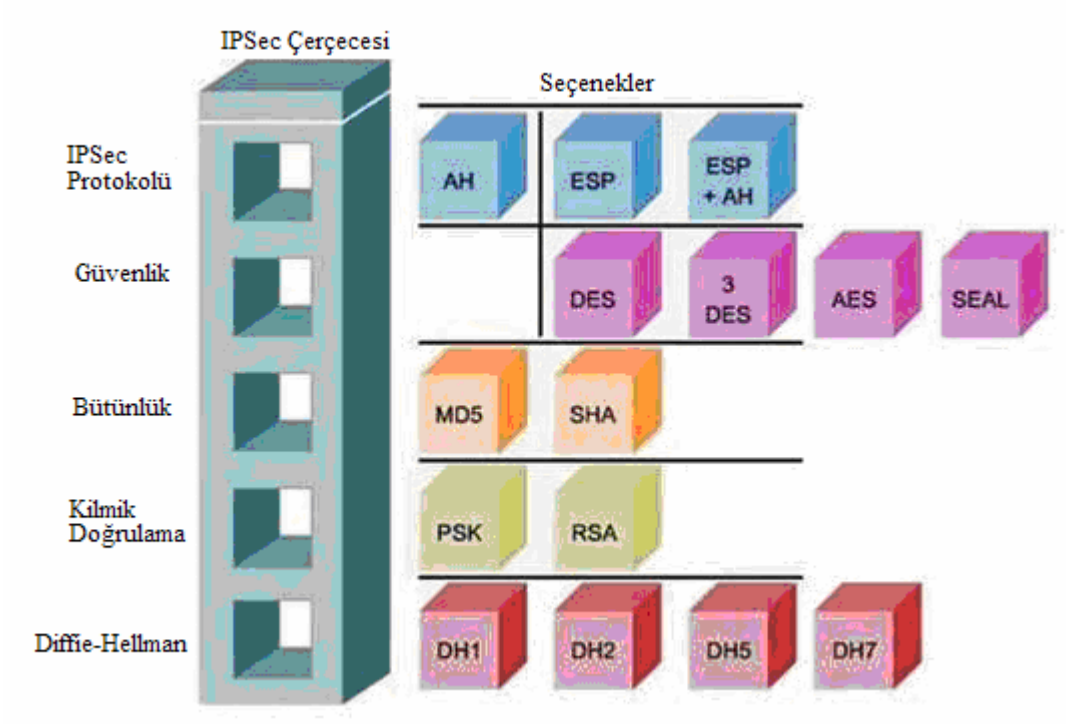
IKE faz 1: IKE Faz 1, anahtar değişiminin nasıl korunacağına karar vermek için gerçekleşen fazdır. İki şekilde gerçekleştirilebilir.

Ana Mod : Ana Modda, üç aşamada anlaşma gerçekleşir. İlk aşama, kimlik doğrulama yöntemi, ikinci aşama, Diffie-Hellman ile anahtar oluşturulması, üçüncü aşama ise kimlik doğrulama yöntemidir.

Agresif Mod : Agresif Modda, Ana Mod'a oranla daha az paket değişimi olur ve ilk pakette, Diffie-Hellman açık anahtarı, kimlik bilgisi gibi bilgiler gönderilir.

IKE faz 1.5: Opsiyonel bir ara fazdır. Her IPSec VPN bağlantısında bulunmaz. Bu fazda XAUTH (Extended Authentication) adı verilen bir kimlik doğrulama yapılır. XAUTH, Cisco VPN Client uygulaması gibi son kullanıcı VPN bağlantılarında, kullanıcının kimlik doğrulamasından sorumludur.

IKE faz 2: IKE Faz 2, IPSec paketlerinin nasıl korunacağını belirleyen fazdır. Güvenilirlik için DES, 3DES, ve AES gibi şifreleme algoritmaları, doğrulama için de SHA1 ve MD5 gibi yöntemleri kullanır.



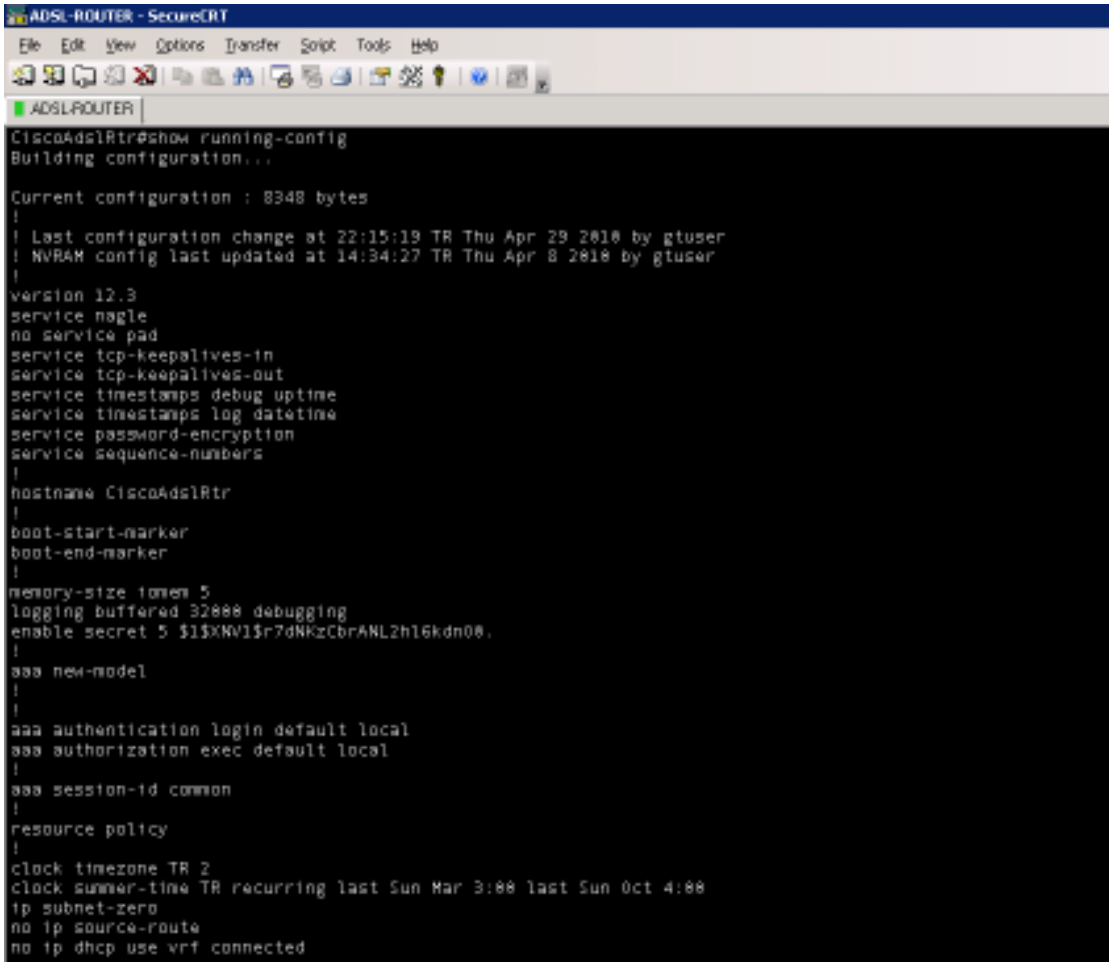
Şekil 3.9 : IPSec Çerçevesi [19]

4. VPN UYGULAMALARI

VPN uygulamalarında VPN Ağ Geçidi olarak, Cisco 5500 Serisinden ASA 5540 Güvenlik duvarı kullanılmıştır.

Cisco serisi cihazlar iki şekilde yönetilmektedir. Bunlardan birincisi, Komut Satırı Arabirimi (CLI – Command Line Interface), ikincisi ise Adaptif Güvenlik Cihazı Yönetimi (ASDM – Adaptive Security Device Manager).

Komut Satırı Arabirimine, konsol ile, ya da tanımlı olan arabirimden telnet ya da ssh protokolü ile erişilebilir.



Şekil 4.1 : Cisco Komut Satırı Ara yüzü

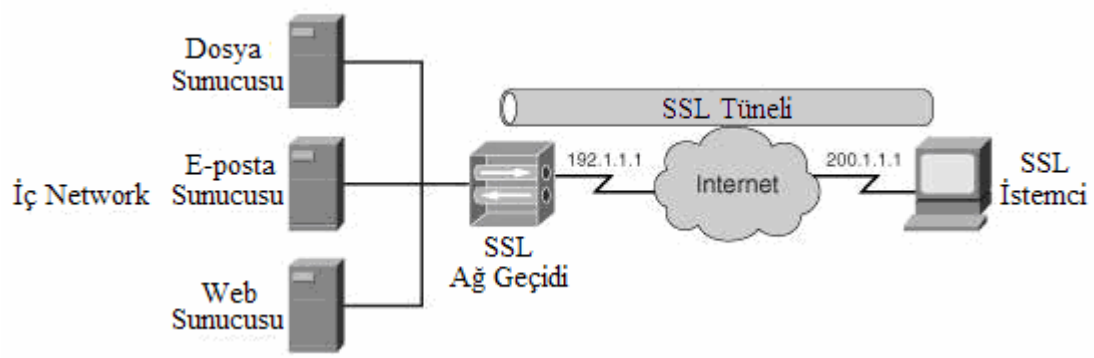
Adaptif Güvenlik Cihazı Yönetimi, Cisco cihazlarının grafiksel ara yüzü olan yönetim uygulamasıdır. Komut Satırı Arabiriminde girilen komutların görsel olarak tanımlanmasını sağlar.

Şekil 4.2 : Cisco Adaptif Güvenlik Cihazı Yönetimi Ara yüzü

4.1 SSL VPN Uygulaması (Web VPN)

4.1.1 SSL VPN nedir?

SSL VPN (Secure Socket Layer Virtual Private Network) web tarayıcılar üzerinde https protokolü ile erişilebilen ve SSL teknolojisini kullanan bir VPN çeşididir. Web tabanlı VPN çeşitlerinde kullanılan SSL protokolü günümüzde standart olarak değerlendirilebilir [20]. Kullanıcı bazlı olması SSL VPN'in en büyük avantajlarından biridir. Kullanıcı tarafında herhangi bir donanıma ihtiyaç duymadan güvenli bir şekilde uzak sistemlere bağlanmayı sağlar.



Şekil 4.3 : SSL VPN Tüneli

4.1.2 SSL VPN bileşenleri

SSL VPN için iki bileşen vardır. Bunlar;

- SSL istemcisi
- SSL ağ geçidi

4.1.2.1 SSL istemci

SSL VPN kullanmak, istemci tarafında herhangi bir donanım ya da yazılıma ihtiyaç duymasa da işletim sistemi ve üzerinde yüklü eklentiler açısından uzak sistemin desteklediği versiyonlara uyumlu olmak zorundadır.

SSL VPN ile istemci web tarayıcı tabanlı ve web tarayıcı tabanlı olmayan uygulamaları çalıştırabilirler.

4.1.2.2 SSL ağ geçidi

SSL VPN uygulamasında önemli bileşen ağ geçididir. Bu anlamda incelenecek olan ürün pazarda öncü üreticilerin başında gelen Cisco'nun ASA 5500 serisi güvenlik duvarlarıdır.

4.1.3 SSL VPN uygulaması

CVPN uygulamasında ağ geçidi olarak Cisco 5500 serisi güvenlik duvarı kullanılmıştır. Güvenlik duvarının internet tarafında ve lokal ağda olmak üzere iki adet ağ arabirim kartına IP adresi konfigurasyonu yapılmıştır. Güvenlik duvarı arkasında bir web sunucu bulunmakta ve istemci, Windows işletim sistemine sahip bilgisayarının web tarayıcısından internet üzerinden güvenlik duvarı ile SSL VPN kurarak, ağ geçidinin konfigürasyonunda tanımlı ve sadece lokalden erişilebilen web sayfasını görüntülemek istemektedir.

4.1.4 Ağ geçidi konfigürasyonu

İnternet ortamında bir istemcinin güvenli bir şekilde, SSL VPN ağ geçidi olarak Cisco ASA 5500 serisi güvenlik duvarı kullanılan uzak sistemde web tabanlı bir uygulamaya erişmek ihtiyacını karşılamak için, Cisco ASA 5500 serisi cihaz üzerinde bulunan işletim sistemi versiyonu 7.2 ve daha yüksek bir versiyon olmalıdır.

İstemci tarafında Internet Explorer, Mozilla gibi bir web tarayıcı bulunmalı ve istemci ile cihaz arasındaki yol boyunca TCP 443 portu engellenmemiş olmalıdır.

Cisco SSL VPN çözümü ile istemci uzak sistemlerdeki aşağıdaki kaynaklara erişebilir.

Cisco terminolojisinde SSL VPN "Web VPN" olarak adlandırılmaktadır.

- Mail Sunucusu
- HTTP ve HTTPS lokal web sunuculara
- Windows dosya erişimi
- Citrix sunuculara

Ağ geçidi üzerinde aşağıdaki konfigurasyon yapılmalıdır.

Web VPN için grup politikası tanımlamak ve erişim izinlerini belirtmek için,

Cisco güvenlik duvarı üzerinde aşağıdaki tanımlamalarla grup politikası belirlenerek bir isim verilir. Bu politika ayarları içersinde erişimin webwpn olacağı belirtilir ve webvpn ile erişen kullanıcıların ne tip haklara sahip olacağı belirlenir. Dosya erişimi, paylaşılan dosyaları görüntüleme gibi izinler tanımlanabilir.

Ciscoasa(config)#group-policy WEBVPN internal

Ciscoasa(config)# group-policy WEBVPN attributes

Ciscoasa(config-group-policy)#vpn-tunnel-protocol webvpn

Ayrıca URL (Uniform Resource Locator - Birörnek Kaynak konumlayıcı) listesinin belirlenmesi de bu konfigurasyon altında yapılmaktadır.

Url Liste Örneği :

OrnekUrlListe.xml dosyası aşağıdaki gibi kaydedilmelidir.

<url-list>

<bookmark>

<title><![CDATA[HTTP BOOKMARK]]></title>

<method><![CDATA[get]]></method>

<favorite><![CDATA[yes]]></favorite>

<url><![CDATA[http://10.129.3.77:8080]]></url>

<subtitle><![CDATA[ISM_Server]]></subtitle>

<thumbnail><![CDATA[]]></thumbnail>

<smart-tunnel><![CDATA[no]]></smart-tunnel>

</bookmark>

</url-list>

Oluşturulan birörnek kaynak konumlayıcı xml formatı ile kaydedilir. Cisco 5500 serisi güvenlik duvarına TFTP (Küçük dosya transfer protokolü) protokolü ile aşağıdaki komut çalıştırılarak gönderilir.

Ciscoasa(config)#import webvpn url-list WEBVPNURL tftp://10.0.0.77/OrnekUrlListesi.xml

OrnekUrlListesi.xml olarak kaydedilen dosya güvenlik duvarında WEBVPNURL adı ile saklanır. Bu dosyayı ilgili grubun yer imi kısa yolunda göstermek için grup politikası içine eklenir.

Ciscoasa(config-group-policy)#webvpn

Ciscoasa(config-group-webvpn)#url-list value WEBVPNURL

Güvenlik duvarı üzerinde ağ geçidinin http servisini açmak ve internetten gelen https isteklerini karşılamak için, Cisco güvenlik duvarı üzerinde başlangıçta kapalı olan http ve https protokollerinin açılması gerekmektedir. Bunun için aşağıdaki komutlar çalıştırılır.

Ciscoasa(config)#http server enable

Ciscoasa(config)#http redirect outside 80

Web VPN parametreleri için, Cisco güvenlik duvarı üzerinde http ve https protokolleri WEB VPN dışında da kullanıldığı için, WEB VPN'in kendisinin de aktif edilmesi gereklidir.

Ciscoasa(config)#webvpn

Ciscoasa(config-webvpn)#enable outside

Ciscoasa(config-webvpn)#tunnel-group-list enable

Tünel grup tanımlanır ve önceden tanımlanan grup politikası bu tünel grup politikasına atanır.

Ciscoasa(config)#tunnel-group DefaultWEBVPNGroup general-attributes

Ciscoasa(config-tunnel-group)#default-group-policy WEBVPN

Kullanıcı tanımlamak için,

Ciscoasa(config)#username fuatd password 53QNetqK.Kqqfshe encrypted

SSL şifreleme algoritması aşağıdaki komutla seçilebilir.

Ciscoasa(config)#ssl encryption 3des-sha1

Bu uygulama için 3DES şifreleme ve SHA1 karım (hash) algoritması kullanılmıştır. Bu güvenlik çiftinin yanı sıra aşağıdaki seçenekler de kullanılabilir.

Ciscoasa(config)# ssl encryption ?

configure mode commands/options:

3des-sha1 Indicate use of 3des-sha1 for ssl encryption

aes128-sha1 Indicate use of aes128-sha1 for ssl encryption

aes256-sha1 Indicate use of aes256-sha1 for ssl encryption

des-sha1 Indicate use of des-sha1 for ssl encryption

null-sha1 Indicate use of null-sha1 for ssl encryption (NOTE: Data is NOT encrypted if this cipher is chosen)

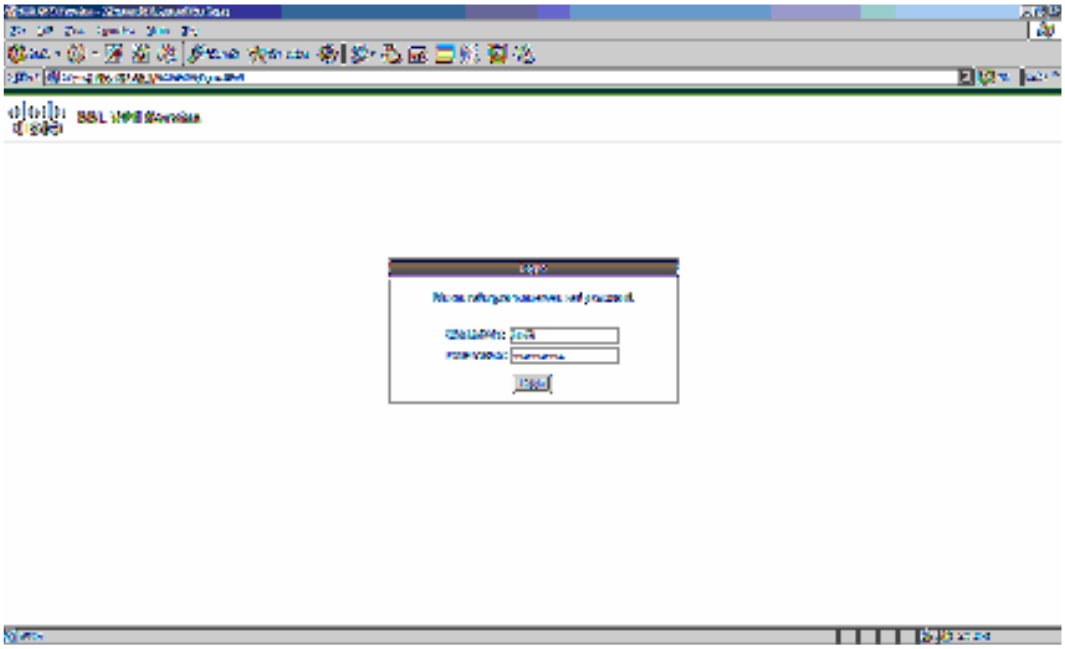
rc4-md5 Indicate use of rc4-md5 for ssl encryption

rc4-sha1 Indicate use of rc4-sha1 for ssl encryption

4.1.5 İstemci konfigürasyonu

SSL Ağ geçidi üzerindeki bu konfigurasyonun ardından, istemci aşağıdaki gibi web tarayıcısına ağ geçidinin internet adresini yazarak erişebilir.

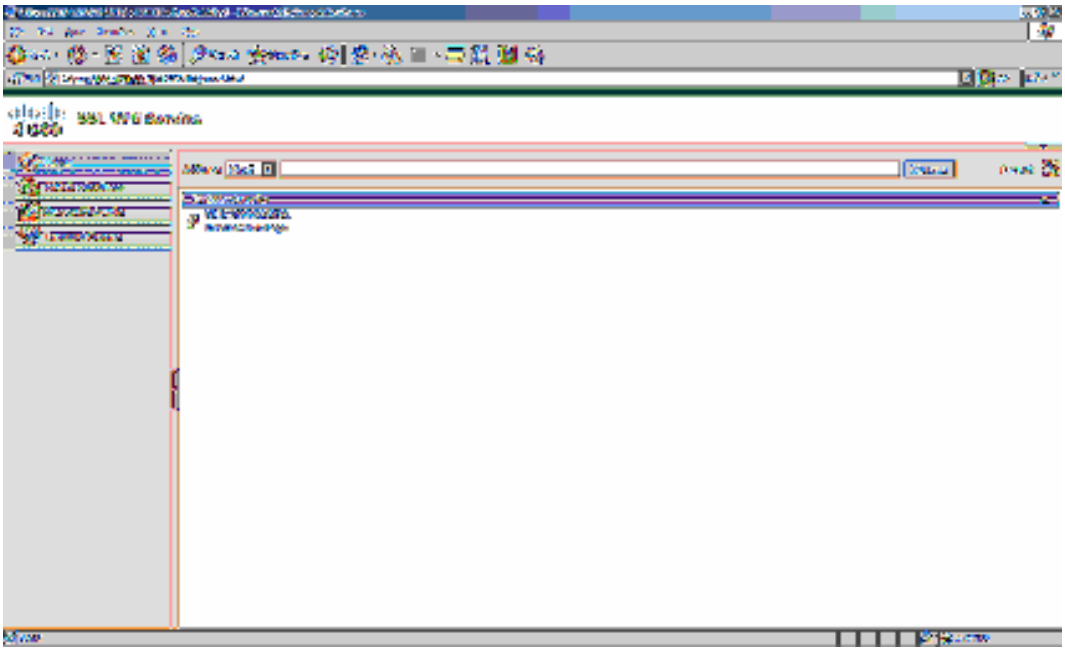
https://[ASA 5500 Güvenlik Duvarının internet adresi]



Şekil 4.4 : SSL VPN Bağlantısı

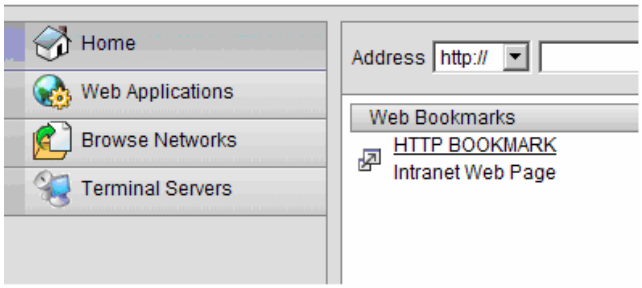
Web tarayıcısında SSL VPN servisi için konfigurasyonda girilen kullanıcı adı ve şifre bilgileri girilerek kimlik doğrulaması geçilir.

Cisco SSL VPN ara yüzü şekildeki gibidir.



Şekil 4.5 : SSL VPN Ara yüzü

Adres kısmına erişilmek istenen sunucunun protokol bilgisi seçilir ve sunucu adı ya da IP adresi yazılarak erişilir. Ya da eklenmiş bir URL listesi varsa bu liste şekildeki yer imi olarak görünür. OrnekUrlListe.xml ismi ile kaydedilip WEBVPNURL adı ile güvenlik duvarı üzerinde sakladığımız yer imi kısa yolu şekildeki gibi görünür.



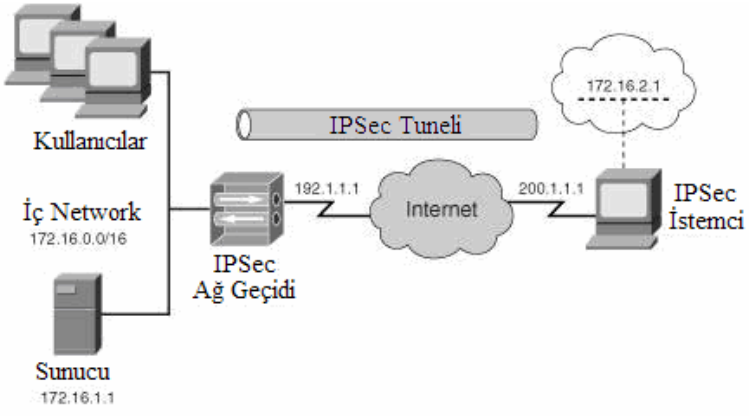
Şekil 4.6 : SSL VPN Web Yerimi

Açılan sayfa internet üzerinden herkese kapalı olan, ancak hedef bilgisayar yerel ağındaki istemciler tarafından erişilebilen bir web sayfasıdır.

4.2 Client VPN – CVPN (IPSec Uzak Erişim VPN)

4.2.1 Client VPN nedir ?

CVPN, istemci tarafındaki Microsoft Windows, Linux ve MAC tabanlı işletim sistemlerinde çalışabilen, uzak cihaza, istemci tarafında kurulan bir uygulama kullanarak bağlanabilen bir VPN çeşididir. IPSec Uzak Bağlantı olarak da bilinir. IPSec uzak erişim VPN için, IPSec ağ geçidi tarafında yapılan konfigurasyona ilave olarak, istemci tarafında da ilgili üretici firmanın ürettiği yazılımın, istemcinin işletim sistemine uygun olan versiyonu kurulum ve konfigurasyonu da gereklidir.



Şekil 4.7 : IPSec Client VPN Tüneli

Burada IPSec uzak bağlantı VPN örnek topolojisi gösterilmiştir. Burada, istemci, erişmek istediği hedef bilgisayar ağının biz uzantısı olarak yer almaktadır. Uygulama ile IPSec ağ geçidi tarafından istemciye bir IP atanarak, hedef ağın bir parçası olması sağlanmıştır.

4.2.2 CVPN uygulaması

CVPN uygulamasında ağ geçidi olarak Cisco 5500 serisi güvenlik duvarı kullanılmıştır. Güvenlik duvarının internet tarafında ve lokal ağda olmak üzere iki adet ağ arabirim kartına IP konfigurasyonu yapılmıştır.

Güvenlik duvarı arkasında bir web sunucu bulunmakta ve istemci, Windows işletim sistemine sahip bilgisayara CVPN uygulamasını kurup, internet üzerinden ağ geçidi ile VPN kurarak, bu web sunucusunun yayınladığı ve sadece lokale açık olan sayfasını görüntülemek istemektedir.

4.2.2.1 Ağ geçidi konfigürasyonu

IPSec uzak erişim VPN bağlantısı için ağ geçidi olarak kullanılan Cisco 5540 ağ geçidinde aşağıdaki konfigurasyonlar yapılır.

Grup politikası tanımlanır ve isim verilir. Bu isim, istemci konfigürasyonunda kullanılacak olan isimdir.

Ciscoasa(config)#group-policy admin internal

Bu grup için tanımlanacak niteliklerin belirlenmesi için alt grup tanımlamalarına geçilir.

Ciscoasa(config)#group-policy admin attributes

Eş zamanlı bağlantı sayısını belirtmek için aşağıdaki şekilde komut girilir.

Ciscoasa(config-group-policy)#vpn-simultaneous-logins 3

CVPN ile istemci bilgisayarına ip adresi ile birlikte etki alanı isim sunucu (DNS - domain name server) adresi de atanır.

Etki alanı isim sunucusu, isimlerin IP adreslerine oranla akılda tutulması daha kolay olduğundan isimleri IP adreslerine çeviren bir sunucudur.

Örneğin, www.itu.edu.tr etki alanı adı için IP adresi 160.75.2.110'dir. Bu etki alanını, IP adresine çeviren etki alanı isim sunucusudur. İnternette etki alanları isim sunucuları hiyerarşik bir yapıda olduğundan, bir etki alanında çözümlenemeyen etki alanı, bir başka etki alanı isim sunucusuna sorulmak suretiyle çözülerek istemciye iletilir. Yerel ağlarda ise, etki alanı isim sunucusu o yerel ağa özeldir. Aşağıdaki konfigurasyon satırında da 10.10.10.100 ve 10.10.10.101 adresli etki alanı sunucuları, istemcinin bilgisayarında, uzak ağdaki yerel etki alanlarını IP adreslerine çevirmede kullanılır.

Ciscoasa(config-group-policy)#dns-server value 10.10.10.100 10.10.10.101

CVPN ile uzak sisteme bağlandıktan sonra, paket alışverişi olmaması durumunda VPN'in ağ geçidi tarafından kopartılmaması istenirse aşağıdaki komut girilir.

Ciscoasa(config-group-policy)#vpn-idle-timeout none

Split-tunneling kavramı, bir VPN kullanıcısının, aynı fiziksel ağ bağlantısını kullanarak, internete ve uzak yerel ya da geniş alan ağına aynı anda bağlanmasını ifade eder.

CVPN üzerinde grup politikası ayarlarında split tünel politikası aşağıdaki şekilde konfigure edilirse, istemci bilgisayarında, kullanıcı hem internete hem de erişim listesi ile belirlenen uzak yerel ağ listesine aynı anda erişebilir.

Ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified

İstemcilerin alacağı adres havuzu belirlenir.

Ciscoasa(config)#ip local pool clientvpnpool 10.128.113.33-10.128.113.63

İstemci bilgisayara aktarılan ağ listesi ile tanımlanan izinler access-list ile belirlenir.

Access-list, Cisco cihazları üzerinde temel olarak bir IP paketinin kaynak IP, kaynak bağlantı noktası (port), hedef IP ve hedef port izinlerini tanımlamak için kullanılan ve yukarıdan aşağıya doğru sıra ile işlenen listelerdir.

Grup politikasında bu ağ listesi ve izinlerin hangi access-list ile yapılacağı belirtilir. Grup politikasında bu erişim listesini (access-list) belirtmeden önce access-list tanımlanmalıdır.

Ciscoasa(config)#access-list clientvpnaccess line 1 extended permit ip 172.16.0.0 255.240.0.0 10.128.113.32 255.255.255.224

Ciscoasa(config)#access-list clientvpnaccess line 2 extended permit ip 192.168.0.0 255.255.0.0 10.128.113.32 255.255.255.224

Ciscoasa(config)#access-list clientvpnaccess line 3 extended permit ip 10.0.0.0 255.0.0.0 10.128.113.32 255.255.255.224

Tanımlanan access-list grup politikasında tanımlanır.

Ciscoasa(config-group-policy)#split-tunnel-network-list value clientvpnaccess

ISAKMP parametreleri belirlenir.

Ciscoasa(config)#crypto isakmp policy 65535

Ciscoasa(config-isakmp-policy)#authentication pre-share

Ciscoasa(config-isakmp-policy)#encryption aes

Ciscoasa(config-isakmp-policy)#hash sha

IPSec parametreleri belirlenir.

Ciscoasa(config)#crypto ipsec transform set rtpset esp-3des esp-sha-hmac

Ciscoasa(config)#crypto map rtptrans 500 ipsec-isakmp dynamic rtpmap

Tanımlanan iletim seti, kurulacak VPN internet tarafında olacağı için, internete doğru olan arabirimde aktif edilir. Ayrıca CVPN için dinamik bir kripto haritası oluşturulur.

Ciscoasa(config)#crypto map rtptrans interface outside

Ciscoasa(config)#crypto dynamic-map rtpmap 10 set transform-set rtpset

CVPN için bir tünel grup oluşturulur ve tip olarak IPSec uzak erişim tipi seçilir (ipsec-ra)

Ciscoasa(config)#tunnel-group HitClientVPN type ipsec-ra

Tünel grup menüsü altında genel tanımlamalar belirlenir. Bu tanımlamalarda, bu tünel grubu altından bağlanacak kullanıcılara hangi adres havuzundan IP adresi verileceği belirlenir. Yine bu tünel gruba giren kullanıcıları hangi grup politikasına tabi olacağı belirtilir. Bu tünel grup için de önceden paylaşılmış anahtar tanımlanır.

Ciscoasa(config)#tunnel-group HitClientVPN general-attributes

Ciscoasa(config-tunnel-group)#address-pool clientvpnpool

Ciscoasa(config-tunnel-group)#default-group-policy HitClientVpn

Ciscoasa(config)#tunnel-group HitClientVPN ipsec-attributes

Ciscoasa(config-tunnel-group)#pre-shared-key q3h$5%/9Lgf#

Lokal kullanıcı tanımı aşağıdaki gibi yapılır.

Ciscoasa(config)#username fuatd password 53QNetqK.Kqqfshe encrypted

4.2.2.2 İstemci konfigürasyonu

IPSec uzak erişim VPN için kullanılan Cisco Client VPN uygulaması, Windows, Linux ve MAC işletim sistemlerinde çalıştırılabilir.

Bu çalışmada, Cisco Client VPN uygulaması Windows işletim sistemi üzerine kurulumu ve konfigurasyonu ele alınacaktır.

Kullanıcı bilgisayarına üretici firma Cisco tarafından üretilen ve yayınlanan CVPN yazılımı Windows ortamında kurulduktan sonra, güvenlik duvarı üzerinde yapılan konfigurasyon ile eşleşen bir konfigurasyon yapılarak uzak sisteme bağlanılabilir.

CVPN uygulaması çalıştırıldığında şekildeki ekran açılır.

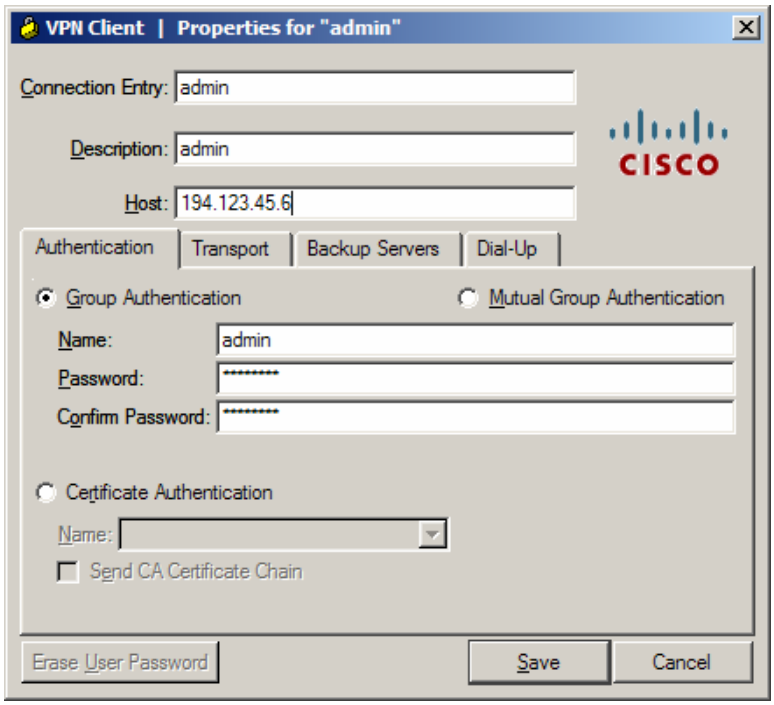
Uzak sisteme bağlantı için girilecek parametreler için yeni bir bağlantı satırı eklenir.

“Connection Entry” kısmına, bu erişim için bir isim verilir.

“Description” alanına bir açıklama girilir.

“Host” alanına, erişilmek istenen ağ geçidinin IP adresi yazılır.

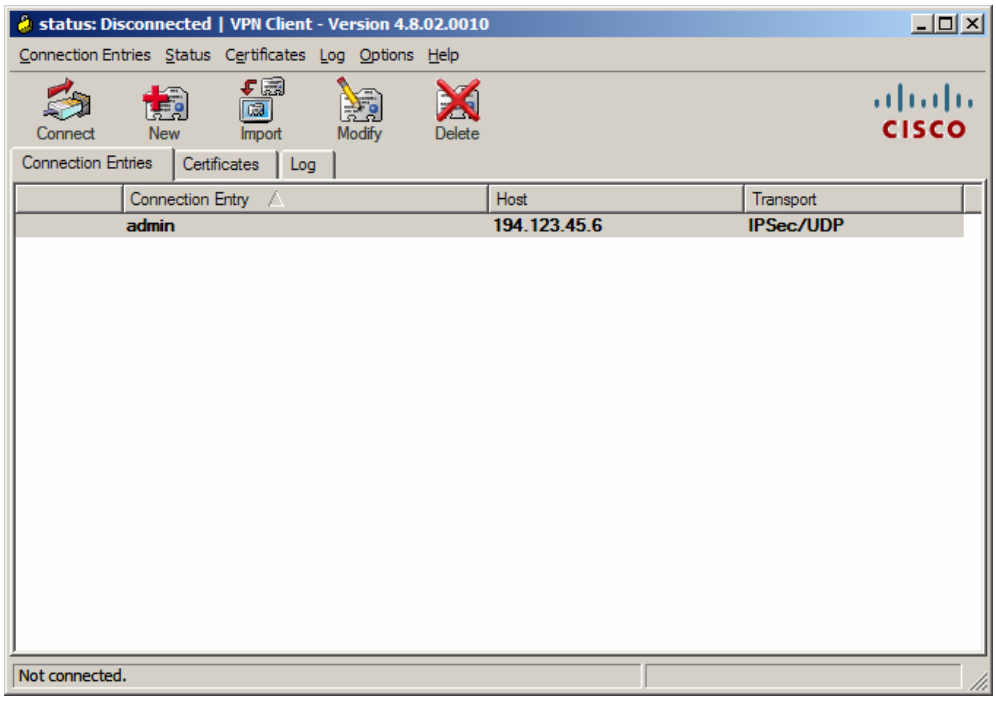
Bu uygulamada grup kimlik doğrulaması yapıldığından, “Group Authentication” seçilerek “Name” alanına, ağ geçidinde tanımlanan tünel grup politikasının adı verilir. “Password” ve “Confirm Password” alanlarına yine tünel grup politikasında tanımlanan önceden paylaştırılmış anahtar girilir.



Şekil 4.8 : CVPN Konfigurasyonu Kimlik Doğrulama

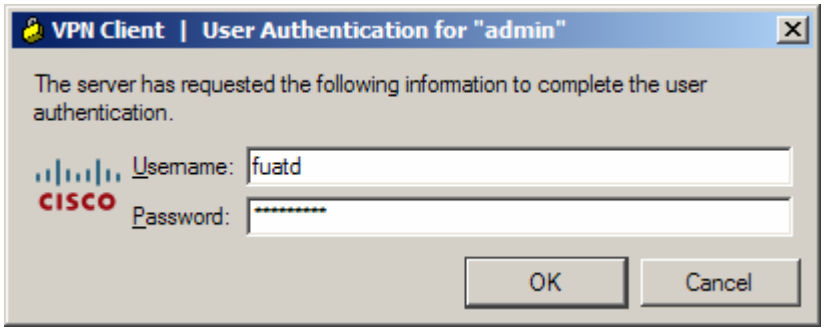
"Transport" alanında, ağ geçidi tarafından başlangıç ayarları olarak gelen IPSec paketinin UDP ile sarmalanması seçeneği işaretlenir. "Save" butonu ile bağlantı ayarlarımızı kaydetmiş oluruz.

Uygulamanın ekranında görünen kaydettiğimiz bağlantı satırı aşağıdaki gibi görünür.



Şekil 4.9 : CVPN Kayıtlı Konfigurasyonlar

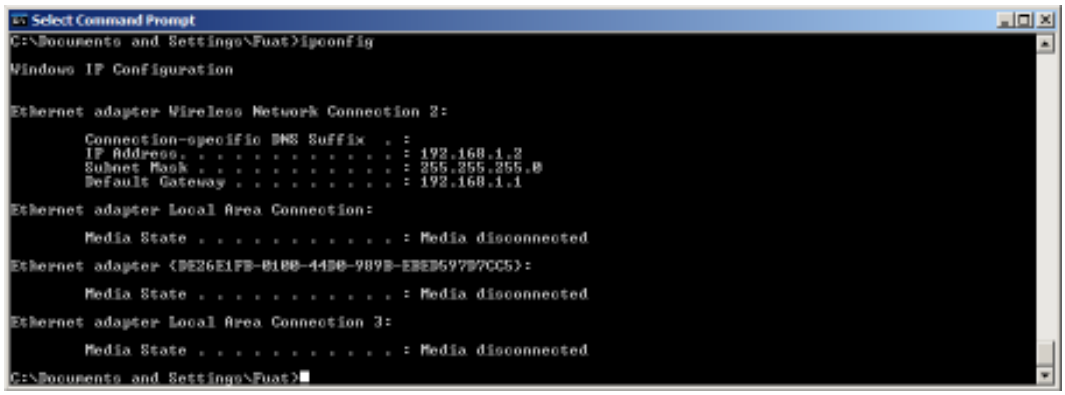
Bu bağlantı satırına çift tıklandığında ya da seçilip üst menüdeki “Connect” butonuna basıldığında kimlik doğrulama ekranı gelir. Bu ekran önceden bahsedilen ekstra kimlik doğrulamanın (XAUTH) yapıldığı nokta yani IKE faz 1.5’dur.



Şekil 4.10 : CVPN Kimlik Bilgileri Girme Ekranı

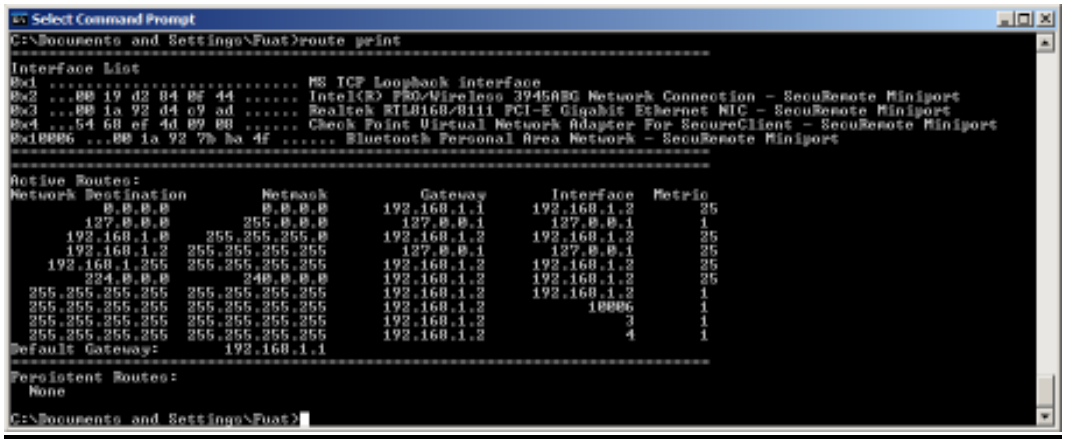
Ağ geçidinde oluşturduğumuz kimlik bilgileri girildiğinde CVPN bağlantısı tamamlanmış olur ve Windows ekranının sol altında önceden açık olan kilit simgesi kilitli hale gelir.

IPSec uzak bağlantı uygulaması Cisco Client VPN çalıştırılmadan önce istemci bilgisayarında, bağlantı arabirim ve arabirim IP adresi ve IP yönlendirme tablosu aşağıdaki gibi olmaktadır.



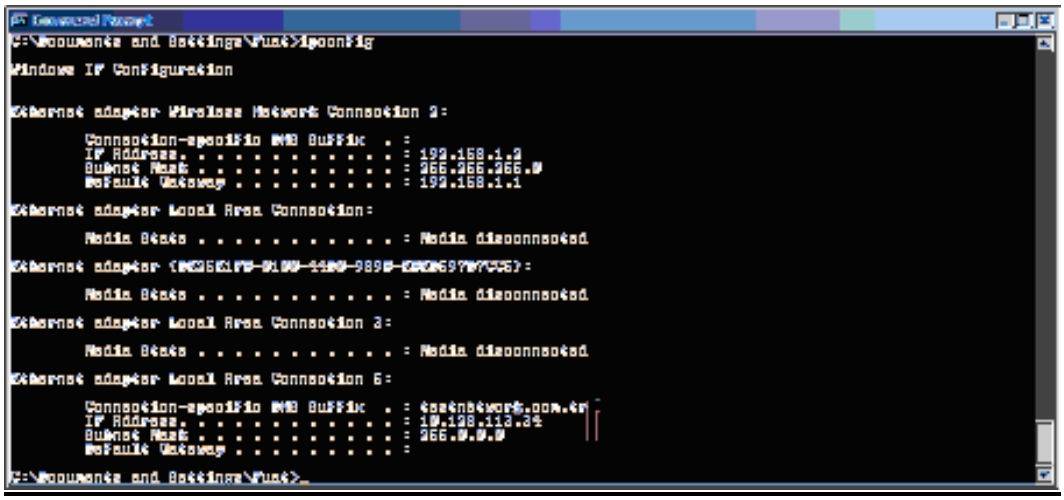
Şekil 4.11 : CVPN Bağlantı Öncesinde IP Adres Konfigurasyonu

İstemci bilgisayarı üzerinden çıkan paketler, bir sonraki noktaya, kendi üzerinde tanımlı olan yönlendirme tablosuna göre gider. Aşağıda, istemci bilgisayarı üzerindeki yönlendirme tablosu görülmektedir.



Şekil 4.12 : CVPN Bağlantı Öncesinde IP Yönlendirme Tablosu

Cisco client VPN uygulaması ile IP uzak erişim bağlantısı yapıldıktan sonra istemci bilgisayarında, bağlantı arabirim ve arabirim IP adresi ve IP yönlendirme tablosu aşağıdaki gibi olmaktadır.

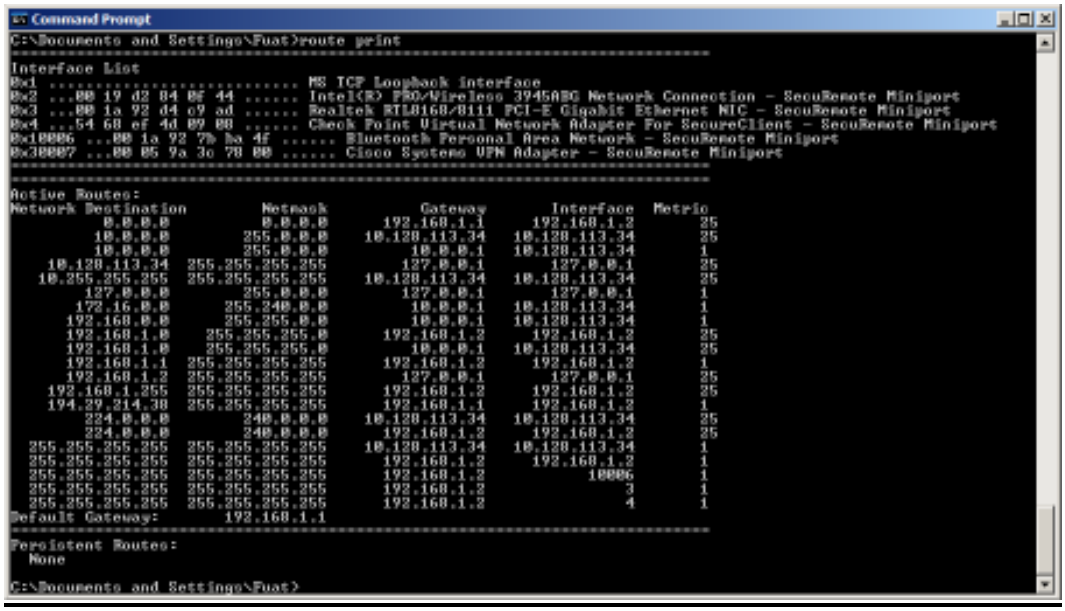


Şekil 4.13 : CVPN Bağlantı Sonrası IP Adres Konfigurasyonu

Görüldüğü gibi, arabirim listesine, “Cisco Systems VPN Adapter” eklenmiştir. Bu sanal arabirim ile birlikte, Cisco 5500 ağ geçidi üzerindeki tanımlamalarla, istemci bilgisayarına aktarılan IP adresi ve yönlendirme tablosu da değişmiştir.

İstemci bilgisayarı, 192.168.1.2 ip adresine sahip iken, “Cisco Systems VPN Adapter” ile eklenen sanal arabirimine de, Cisco 5500 ağ geçidi tarafından 10.128.113.34 IP adresi verilmiştir. Böylece, istemci bilgisayarında iki adet IP adresi olmuştur.

İstemci bilgisayarı üzerindeki yönlendirme tablosuna da yeni ip adresi için ilave ağ yönlendirmeleri eklenmiştir.



Şekil 4.14 : CVPN Bağlantı Sonrası IP Yönlendirme Tablosu

Bağlantı kurulduktan sonra, ağ geçidi Cisco ASA 5500 serisi güvenlik duvarı üzerinde aşağıdaki komut çalıştırılarak o an açık olan uzak bağlantı oturumları görülebilir.

Ciscoasa#sh vpn-sessiondb remote

Session Type: IPsec

Username : fuatd Index : 57414

Assigned IP : 10.128.113.34 Public IP : 212.156.184.142

Protocol : IKE IPsecOverNatT

License : IPsec

Encryption : 3DES Hashing : SHA1

Bytes Tx : 153641 Bytes Rx : 56759

Group Policy : admin Tunnel Group : admin

Login Time : 19:25:39 TR Sat Apr 24 2010

Duration : 0h:18m:22s

NAC Result : Unknown

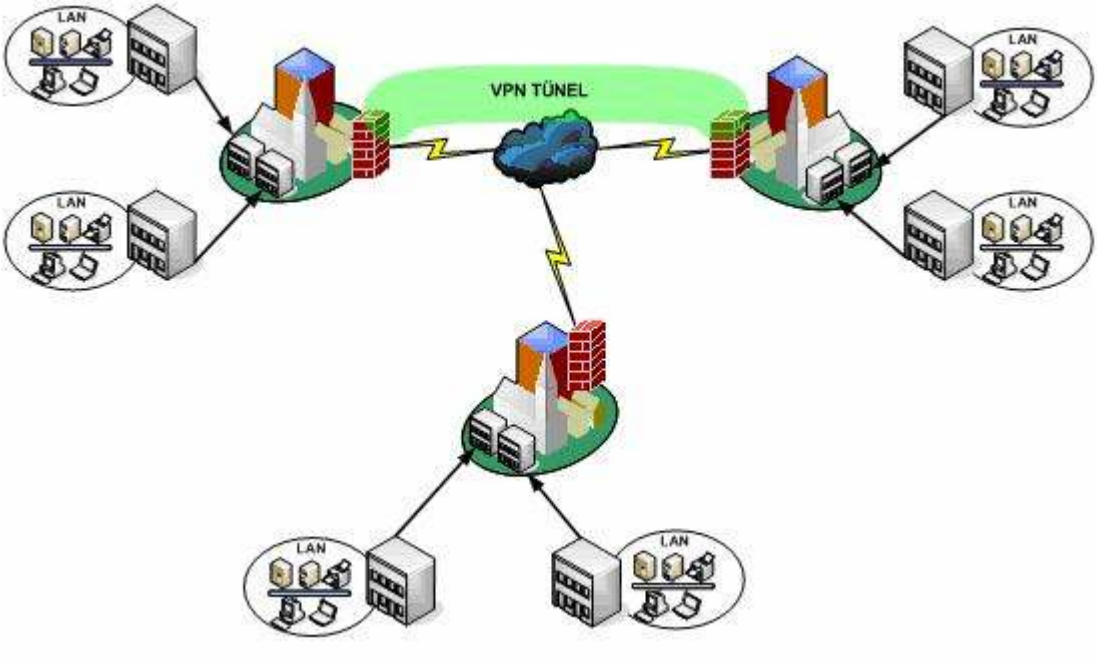
VLAN Mapping : N/A VLAN : none

CVPN bağlantısı kurulduktan sonra uzak ağın intranetindeki web sayfasına web tarayıcısına web sunucusunun adresi yazılarak erişilebilir.

4.3 Uçtan Uca VPN (Site To Site VPN)

4.3.1 Uçtan uca VPN nedir ?

Uçtan uca VPN, her iki uç noktada birer VPN sonlandırıcı cihazın olduğu ve bu VPN sonlandırıcı ağ geçitlerinin arkasında bulunan en az bir sunucunun birbiri ya da birbirleriyle güvenli bir şekilde haberleşmesini sağlayan VPN çeşididir.



Şekil 4.15 : Uçtan Uca VPN Topolojisi

4.3.2 Uçtan uca VPN uygulaması

Uçtan uca VPN uygulamasında iki ağ geçidinin arkasındaki cihaz ya da cihazlar tek yönlü ya da çift yönlü güvenli iletim kanalı üzerinden birbirleriyle haberleşebilmektedirler. Bu uygulamada, birinci ağ geçidi Cisco ASA 5500 serisi güvenlik duvarı, ikinci ağ geçidi Cisco 850 serisi ADSL yönlendirici olarak seçilmiştir. Cihazların biri internet tarafında diğeri lokalde ikişer adet ağ arabirim kartlarına IP adresi konfigurasyonu yapılmıştır.

4.3.2.1 Birinci ağ geçidi konfigurasyonu

Birinci Ağ geçidi olarak seçilen Cisco 5500 serisi ağ geçidi için uçtan uca VPN konfigurasyonu aşağıdaki gibi yapılmaktadır.

ISAKMP protokolü internet tarafındaki arabirimde aktive edilir.

Ciscoasa(config)#crypto isakmp enable outside

ISAKMP konfigurasyonu yapılır.

Ciscoasa(config)#crypto isakmp policy 10

Ciscoasa(config-isakmp-policy)#authentication pre-share

Ciscoasa(config-isakmp-policy)#encryption aes

Ciscoasa(config-isakmp-policy)#hash sha

İletim seti tanımlanır. Bu iletim setine isim verilir ve şifreleme ve kimlik doğrulama algoritmaları belirlenir.

Ciscoasa(config)#crypto ipsec transform-set myset esp-aes esp-sha-hmac

Erişim listeleri tanımlanarak ağ geçidi arkasında hangi cihazların erişim yapacağı belirlenir. Burada erişimin yönüne bakılmaksızın, ağ geçidinin arkasındaki ağ her zaman kaynak adres olarak karşı taraftaki ağ geçidinin arkasındaki ağ her zaman hedef adres olarak tanımlanır.

Ciscoasa(config)#access-list sitetositeacl extended permit ip 10.0.0.0 255.0.0.0 192.168.0.0 255.255.255.0

Burada 10.0.0.0 255.0.0.0 ağı, birinci ağ geçidinin arkasında, 192.168.0.0 255.255.255.0 ağı, ikinci ağ geçidi arkasındadır.

Tünel grup tanımlanır. VPN yapılacak ağ geçidi tanımlanır. Önceden paylaşılmış anahtar burada belirlenir.

Ciscoasa(config)#tunnel-group 10.20.20.1 type ipsec-l2l

Ciscoasa(config)#tunnel-group 10.20.20.1 ipsec-attributes

Ciscoasa(config-tunnel-group)#pre-shared-key P@rtn3rNetw0rk

IPSec faz 2 için kripto haritası denen parametreler ve eşlemeler yapılır.

Kripto haritasının hangi arabirime uygulanacağı belirlenir ve isim verilir. “outside” arabirimi internet yönüne bakan arabirimdir.

Ciscoasa(config)#crypto map mymap interface outside

Kripto haritasının tanımlandığı arabirim altında bir öncelik numarası vererek, hangi erişim listesinin uçtan uca VPN'in içine alınacağı ağları kapsadığı belirtilir. Buna o VPN için ilgili trafik adı verilir.

Ciscoasa(config)#crypto map mymap 10 match address sitesiteacl

İkici ağ geçidinin internet adresi VPN yapılacak cihaz olarak tanımlanır ve IPSec faz 2 parametre kümesi seçilir.

Ciscoasa(config)#crypto map mymap 10 set peer 212.185.51.135

Ciscoasa(config)#crypto map mymap 10 set transform-set myset

4.3.2.2 İkinci ağ geçidi konfigurasyonu

Cisco 850 serisi ADSL yönlendiricisi kullanılan ikinci ağ geçidinde birinci ağ geçidine özel olan isimler değişiklik gösterebilir. Bunun dışında tanımlı olan birinci ağ geçidi adresi değiştirilir.

CiscoAdslRtr(config)#crypto isakmp policy 10

CiscoAdslRtr(config-isakmp)#hash md5

CiscoAdslRtr(config-isakmp)#authentication pre-share

CiscoAdslRtr(config)#crypto isakmp key 1qaz2wsx address 194.123.45.6

CiscoAdslRtr(config)#crypto ipsec transform-set mytransset esp-3des esp-sha-hmac

CiscoAdslRtr(config)#crypto map mycryptomap 10 ipsec-isakmp

CiscoAdslRtr(config- crypto-map)#set peer 194.123.45.6

CiscoAdslRtr(config-crypto-map)#set transform-set mytransset

CiscoAdslRtr(config-crypto-map)#match address sitetositeacl

Ayrıca, birini ağ geçidinde yazılan erişim listesi, kaynak ağ adresi hedef ağ adresine, hedef ağ adresi de kaynak ağ adresine yazılacak şekilde tersten yazılır.

CiscoAdslRtr(config)#access-list sitetositeacl extended permit ip 192.168.0.0 0.0.0.255 10.0.0.0 0.255.255.255

Bunlar dışında tanımlı olan, IPSec faz1 ve faz 2 ayarları, önceden paylaşılmış anahtarlar birebir aynı olmalıdır.

4.3.2.3 Uçtan uca erişim

Uçtan uca VPN'de erişim yapan istemci, SSL VPN'deki gibi karşı taraftaki ağ geçidine bağlanıp herhangi bir kimlik doğrulaması yapmaksızın ve IPSec Uzak Erişim (CVPN) gibi bilgisayarına herhangi bir uygulama yüklemeksizin, erişeceği sunucu sanki kendi lokalindeymiş gibi direk olarak bağlantı gerçekleştirebilir. Çünkü, her türlü kimlik doğrulama, şifreleme, paket bütünlüğü gibi işlemleri ağ geçitleri kendi aralarında yapmakta ve istemci ve sunucuya bunu yansıtmamaktadır. İstemci ve sunucu sadece, karşı tarafa göndereceği paketleri kendi ağ geçidine yönlendirmekle yükümlüdür.

Birinci ağ geçidi Cisco 5500 serisi güvenlik duvarı üzerinde "show isakmp sa" komutu ile faz 1 in oluşup oluşmadı kontrol edilebilir.

Ciscoasa#show isakmp sa

1 IKE Peer: 212.185.51.135

Type : L2L Role : initiator

Rekey : no State : MM_ACTIVE

İkinci ağ geçidi Cisco 850 serisi cihazı üzerinde "show crypto isakmp sa" komutu ile faz 1 in oluşup oluşmadığı kontrol edilebilir.

CiscoAdslRtr#show crypto isakmp sa

dst srcstate conn-idslot status

212.185.51.135192.123.45.6QM_IDLE11 0ACTIVE

IPSec Uçtan uca VPN yöntemi ile karşı taraftaki web sunucuya bağlantıda aynı CVPN yöntemindeki gibi kullanıcı direk olarak web tarayıcısına erişmek istediği sunucunun yerel adresini yazarak erişebilir.

Faz 2 nin oluşup VPN üzerinden veri alışverişinin başlayıp başlamadığının kontrolü Cisco 5500 güvenlik duvarı üzerinde "show ipsec sa peer <peer ip address>" komutu ile yapılır.

ASA-VPNGW# sh ipsec sa pe 212.185.51.135

peer address: 212.185.51.135

Crypto map tag: rtpmap, seq num: 10, local addr: 194.123.45.6

access-list sitetositeacl extended permit ip 10.0.0.0 255.0.0.0 192.168.0.0 255.255.255.0

local ident (addr/mask/prot/port): (10.0.0.100/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/0/0)

current_peer: 212.185.51.135

#pkts encaps: 118452, #pkts encrypt: 118452, #pkts digest: 118452

#pkts decaps: 114994, #pkts decrypt: 114994, #pkts verify: 114994

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 118452, #pkts comp failed: 0, #pkts decomp failed: 0

#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

#send errors: 0, #recv errors: 0

local crypto endpt.: 194.123.45.6, remote crypto endpt.: 212.185.51.135

path mtu 2000, ipsec overhead 58, media mtu 1500

current outbound spi: 750ACE3D

inbound esp sas:

spi: 0xA6E4FDB6 (2800025014)

transform: esp-3des esp-sha-hmac no compression

in use settings ={L2L, Tunnel, }

slot: 0, conn_id: 3764224, crypto-map: rtpmap

sa timing: remaining key lifetime (kB/sec): (4374000/3217)

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

outbound esp sas:

spi: 0x750ACE3D (1963642429)

transform: esp-3des esp-sha-hmac no compression

in use settings ={L2L, Tunnel, }

slot: 0, conn_id: 3764224, crypto-map: rtpmap

sa timing: remaining key lifetime (kB/sec): (4374000/3217)

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

4.4 Konu Üzerinde Yapılan Çalışmalar

VPN uygulamaları ile yapılan çalışmalardan 2002 yılında IEEE uluslararası konferansında Samir Al-Khayatt, Siraj A.Shaikh, Babak Akhgar ve Jawed Siddiqi tarafından yayınlanan VPN tünelleme modelleri üzerine yapılan çalışmada, Windows ve Novell sistemleri ayrı ayrı kullanılarak kurulan IPSec uçtan uca VPN ile dosya transfer protokolü ile dosya transferi sırasındaki bantgenişliği ölçümlemesi yapılmıştır. Aynı ölçümler IPSec uçtan uca VPN tünel yokken de yapılmış ölçümler karşılaştırılmıştır. Elde edilen neticede bilgisayar ağı üzerinde VPN performansı kullanılan donanım ve yazılıma göre değişiklik gösterdiği sonucuna varılmıştır.

Aamer Nadeem ile Dr M. Younus Javed tarafından yapılan ve 2005 yılında IEEE Bilgi ve Haberleşme Teknolojileri konferansında yayınlanan makalelerinde şifreleme algoritmalarının şifreleme hızlarını iki farklı donanım üzerinde karşılaştırmışlardır. Elde edilen sonuçlarda Blowfish algoritması en hızlı şifreleme yapan algoritma olarak ortaya çıkmıştır. 3DES algoritması da en yavaş algoritma olarak ölçülmüştür.

Bu çalışmada ise uzak sisteme güvenli bir şekilde erişmeyi sağlayacak olan farklı VPN tiplerinin performansı, aynı şifreleme ve karım fonksiyonları kullanılarak, farklı boyuttaki web sayfalarını görüntüleme süreleri ölçülerek karşılaştırılmıştır.

5. KARŞILAŞTIRMA VE ANALİZ

Bilgisayar ağı güvenliğinin sağlanması, bilgisayar ağı üzerinden iletişim performansına olumsuz yönde etki eder. Ancak bu yük bugün kullanılan yoğun uygulamaların getirdiği yükten sadece biridir [21]. Bu sebeple uygulaması yapılan VPN çeşitleri performans açısından birbirleri ile karşılaştırılmıştır.

5.1 SSL ve IPSec Karşılaştırması

Uzak sisteme internet üzerinden güvenli bir şekilde bağlanmayı sağlayan Özel Sanal Ağ yönteminde kullanılan SSL ve IPSec teknolojilerinin çeşitli açılardan karşılaştırılması aşağıdaki tabloda verilmiştir [6].

Çizelge 5.1 : SSL IPSec Karşılaştırma Tablosu

Bileşen	**SSL**	**IPsec**
Bağlantı Tipi	Uzak Erişim (Remote Access)	Uzak erişim ve Uçtan Uca (Site-to-Site ve Remote Acc.)
Cihaz Kimlik Doğrulaması	Dijital Sertifika desteği	Önceden paylaşım anahtarlar, RSA ve dijital sertifika
Kullanıcı Kimlik Doğrulaması	Desteklenir	IPSec kimlik doğrulamayı XAUTH üzerinden L2TP/IPSec kullanılması durumunda yapar. Burada L2TP kimlik doğrulamadan sorumlu protokoldür.
Koruma	Sadece TCP veri yükü koruması	İletim modunda veri paketi koruması yapılırken, tünel modunda tüm IP paketi korunur.
Şifreleme	RC2, RC4, IDEA, DES, 3DES, and AES; ancak Bazı web browserlar sadece RC4, DES, ve 3DES destekler.	IPSec DES, 3DES, and AES şifreleme algoritmalarını destekler.
Mesaj Bütünlüğü	TCP desteklidir.	MD5 ve SHA-1 HMAC fonksiyonları ile yapılır.
Uygulamak için gerekenler	SSL, Java/ActiveX yüklü bir web browsera ihtiyaç duyar. Bir çok işletim sistemi tarafından desteklenir.	IPSec, bir IPSec kullanıcısına yada işletim sisteminin bu iş için tanımlanmış uygulamasına ihtiyaç duyar. Üretici firmanın desteklediği işletim sistemleri desteklenir.
Şeffaflık	SSL herhangi bir adres ya da port değişikliği yapan bir cihaz üzerinden geçen oturumda sorunsuz bir şekilde çalışmaktadır.	IPSec adres değişikliği yapan cihaz üzerinde AH ile, port değişikliği yapan cihaz üzerinde de ESP ile problem yaşatabilir. Ancak genelde, güvenlik duvarında varsayılan ayarlarda IPSec paketi geçmesine izin verilmez.
İnternet Servis Sağlayıcı Problemleri	SSL internet ortamında çok kullanıldığından internet servis sağlayıcılar bu tip trafiği kesmezler.	Bazı internet servis sağlayıcılar IPSec trafiğine izin vermek için kullanıcılardan ekstra ücret talep etmektedirler. Bu problem Cisco cihazları için özel bir çözüm olan IPSec paketini TCP ya da UDP paketi ile sarmalama ile giderilebilir. Ancak bu da veri iletimine ilave bir yük demektir.

5.2 Şifreleme Algoritmalarının Karşılaştırılması

Çizelge 5.2 : Şifreleme Algoritmalarını Karşılaştırma Tablosu

Faktörler	**AES**	**3DES**	**DES**
Anahtar Uzunluğu	128, 192 veya 256 Bit	112 veya 168 Bit	56 Bit
Şifreleme Tipi	Blok	Blok	Blok
Blok Uzunluğu	128, 192 ya da 256 Bit	64 Bit	64 Bit
Buluş Yılı	2000	1987	1977
Anahtar çeşitliliği	$2^{128}, 2^{192}, 2^{256}$	$2^{112}, 2^{168}$	2^{56}
Saniyede 50 Milyon Anahtar Deneyerek Anahtarı Bulma Süresi	128 Bitlik anahtar için $5x10^{21}$ Yıl.	112 Bitlik Anahtar için 800 Yıl.	56 Bitlik Anahtar için 400 Yıl

5.3 Farklı Tip VPN Çeşitleri İle İntranet Web Sayfasına Bağlanma Süreleri

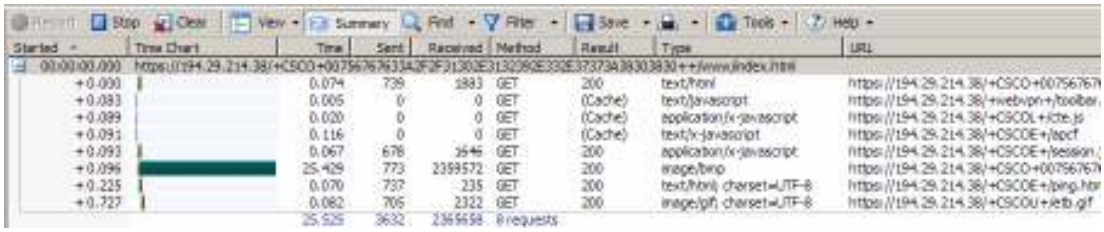
5.3.1 Yöntem

Bu çalışmada istemci tarafında 1 Mbps ADSL hattı kullanıldı. Yine istemci tarafında, Cisco 850 Serisi ADSL modem, Windows XP işletim sistemi, Intel Core2 Duo 1.83Ghz işlemcili 2048 MB RAM kapasiteli bir bilgisayar kullanıldı. Uygulaması yapılan SSL VPN, CVPN ve Uçtan Uca VPN (S2S VPN) VPN çeşitleri ile uzak bilgisayar ağındaki bir web sunucusuna bağlanıldı. Her VPN çeşidi ile 2.5 MB ve 10 MB büyüklüğündeki iki sayfa görüntülendi ve görüntülenme süreleri, her bir VPN çeşidi ve web sayfası boyutu ile 50 kez ölçüldü. Ölçümler, internet tarayıcısına bir eklenti olarak yüklenen HttpWatch programı ile yapıldı. 3 VPN ve 2 farklı boyuttaki web sayfası için toplam 300 ölçüm yapıldı. Her bir ölçüm grubu için ortalama yanıt süreleri ve standart sapmalar hesaplandı.

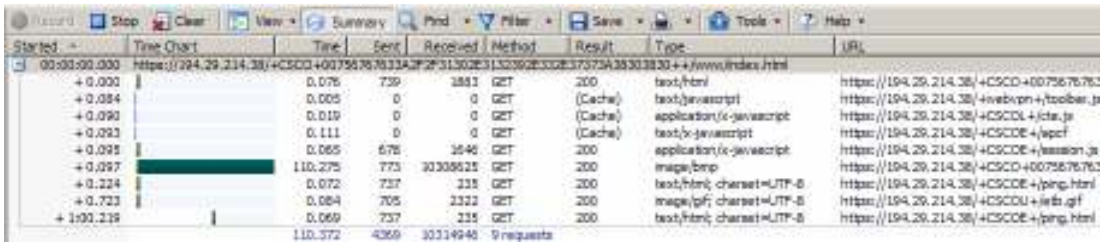
5.3.2 SSL VPN ile intranet web sayfasına bağlanma süresi

SSL VPN bağlantısı için konfigure edilen ağ geçidine erişildikten sonra, intranet web sayfasında erişildi.

İstemci ile ağ geçidi arasında SSL tüneli kurulduktan sonra tanımlanan yer imi üzerinden sırası ile 2.5 MB ve 10 MB büyüklüğündeki web sayfaları çağırıldı.

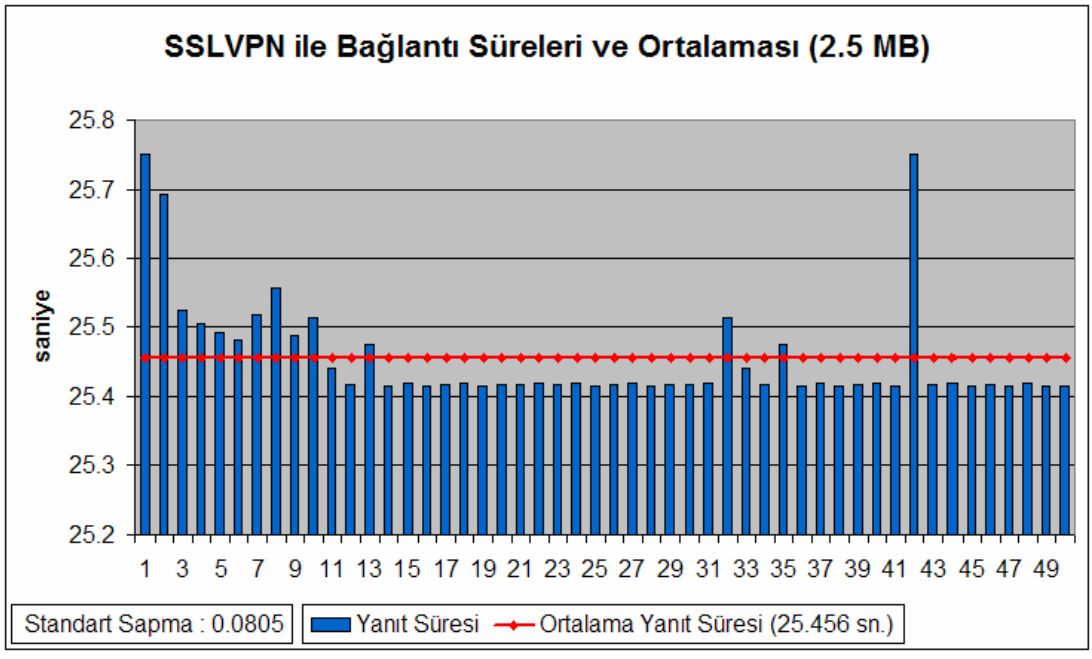


Şekil 5.1 : SSL VPN ile 2.5 MB'lık Web Sayfasının Görüntülenme Süresi



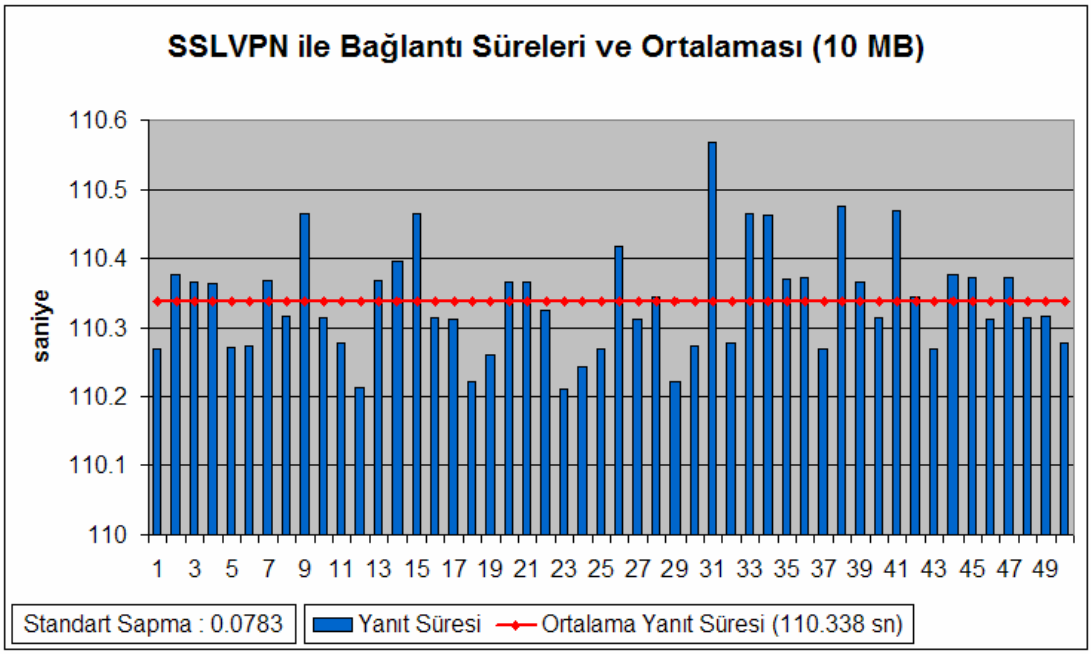
Şekil 5.2 : SSL VPN ile 10 MB'lık Web Sayfasının Görüntülenme Süresi

Yapılan erişimler her bir web sayfası için 50'şer kez tekrarlandı. 2.5 MB'lık web sayfasının ortalama görüntüleme süresi 25.456 sn. olarak ölçüldü. Standart sapma 0.0805 olarak hesaplandı.



Şekil 5.3 : SSL VPN ile Çağrılan Web Sayfası Yanıt Süreleri (2.5 MB)

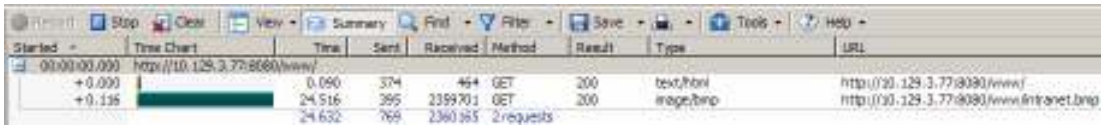
Aynı ölçümler 10 MB'lık web sayfası için tekrarlandı. Bu kez ortalama görüntüleme süresi 110.338 sn. olarak ölçüldü. Standart sapma 0.0783 olarak hesaplandı.



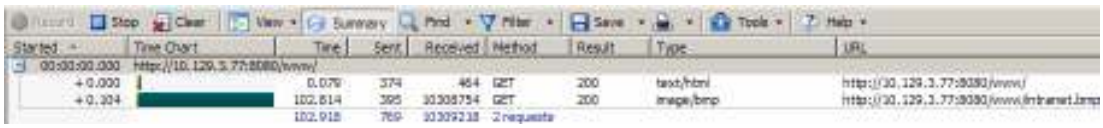
Şekil 5.4 : SSL VPN ile Çağrılan Web Sayfası Yanıt Süreleri (10 MB)

5.3.3 CVPN ile intranet web sayfasına bağlanma süresi

SSL VPN bağlantısı için konfigure edilen ağ geçidine erişildikten sonra, intranet web sayfasında erişildi. İstemci ile ağ geçidi arasında uzak erişim tüneli kurulduktan sırası ile 2.5 MB ve 10 MB büyüklüğündeki web sayfaları çağırıldı.

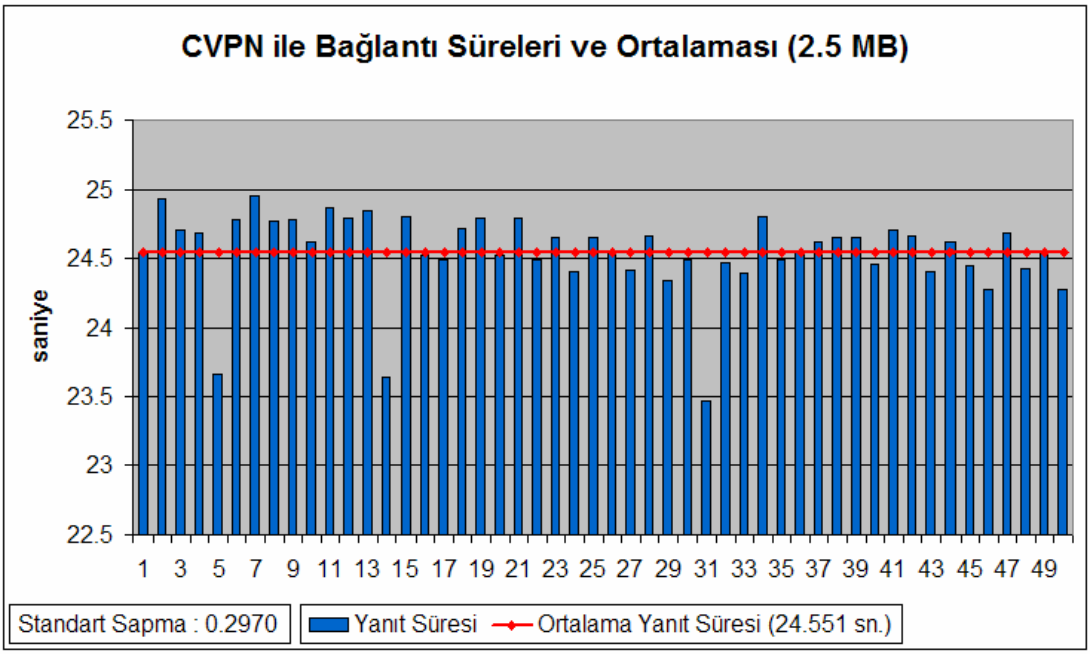


Şekil 5.5 : CVPN ile 2.5 MB'lık Web Sayfasının Görüntülenme Süresi



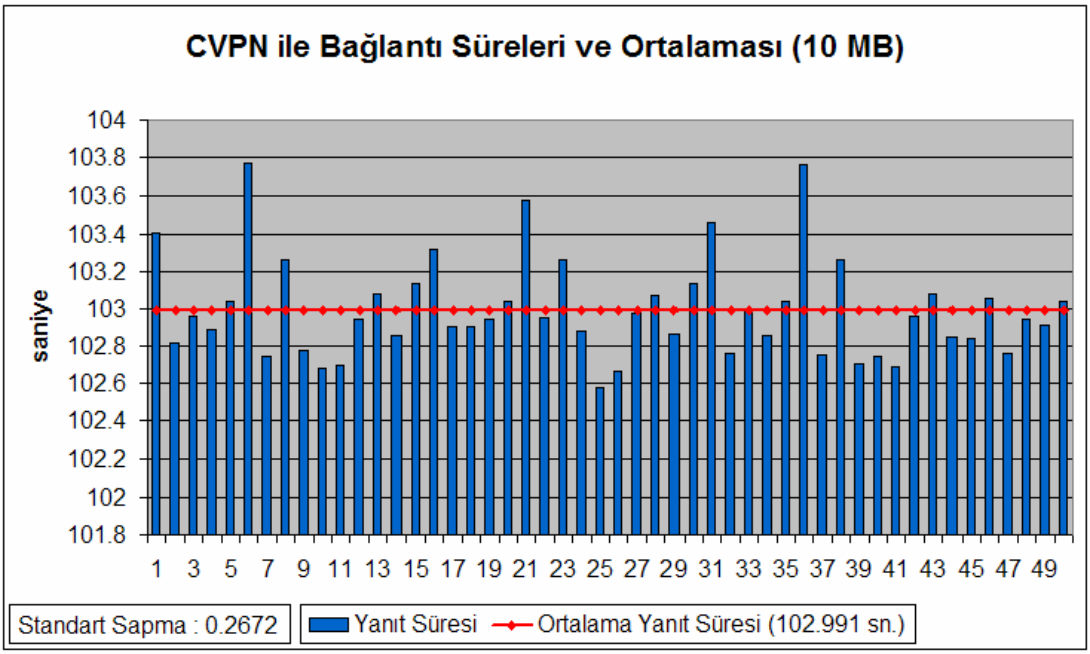
Şekil 5.6 : CVPN ile 10 MB'lık Web Sayfasının Görüntülenme Süresi

Yapılan erişimler her bir web sayfası için 50'şer kez tekrarlandı. 2.5 MB'lık web sayfasının ortalama görüntüleme süresi 24.551 sn. olarak ölçüldü. Standart sapma 0.2970 olarak hesaplandı.



Şekil 5.7 : CVPN ile Çağrılan Web Sayfası Yanıt Süreleri (2.5 MB)

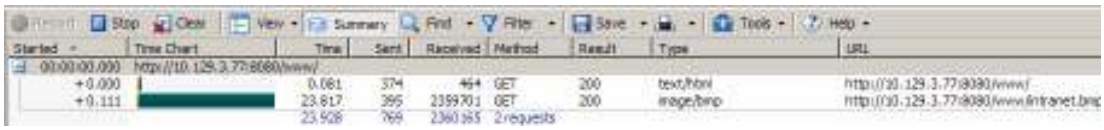
Aynı ölçümler 10 MB'lık web sayfası için tekrarlandı. Bu kez ortalama görüntüleme süresi 102.991 sn. olarak ölçüldü. Standart sapma 0.2672 olarak hesaplandı.



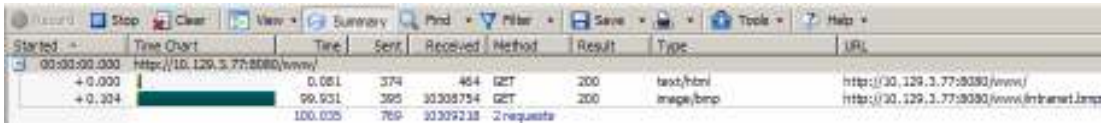
Şekil 5.8 : CVPN ile Çağrılan Web Sayfası Yanıt Süreleri (10 MB)

5.3.4 Uçtan Uca VPN ile intranet web sayfasına bağlanma süresi

SSL VPN bağlantısı için konfigure edilen ağ geçidine erişildikten sonra, intranet web sayfasında erişildi. İstemci ile ağ geçidi arasında uçtan uca IPSec tüneli kurulduktan sırası ile 2.5 MB ve 10 MB büyüklüğündeki web sayfaları çağırıldı.

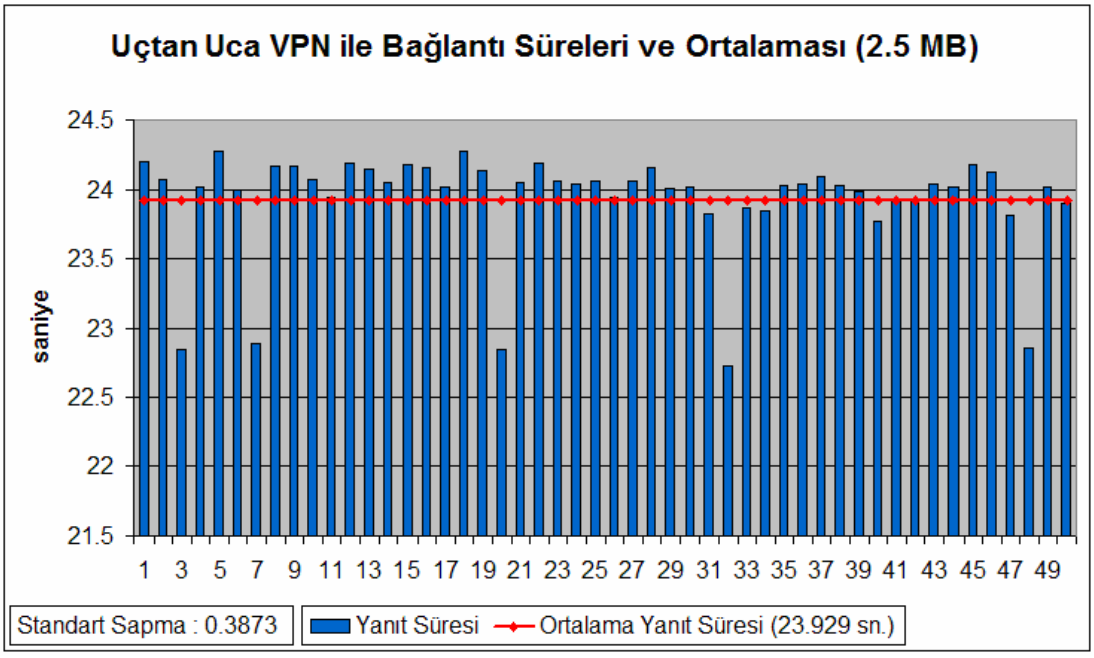


Şekil 5.9 : Uçtan Uca ile 2.5 MB'lık Web Sayfasının Görüntülenme Süresi



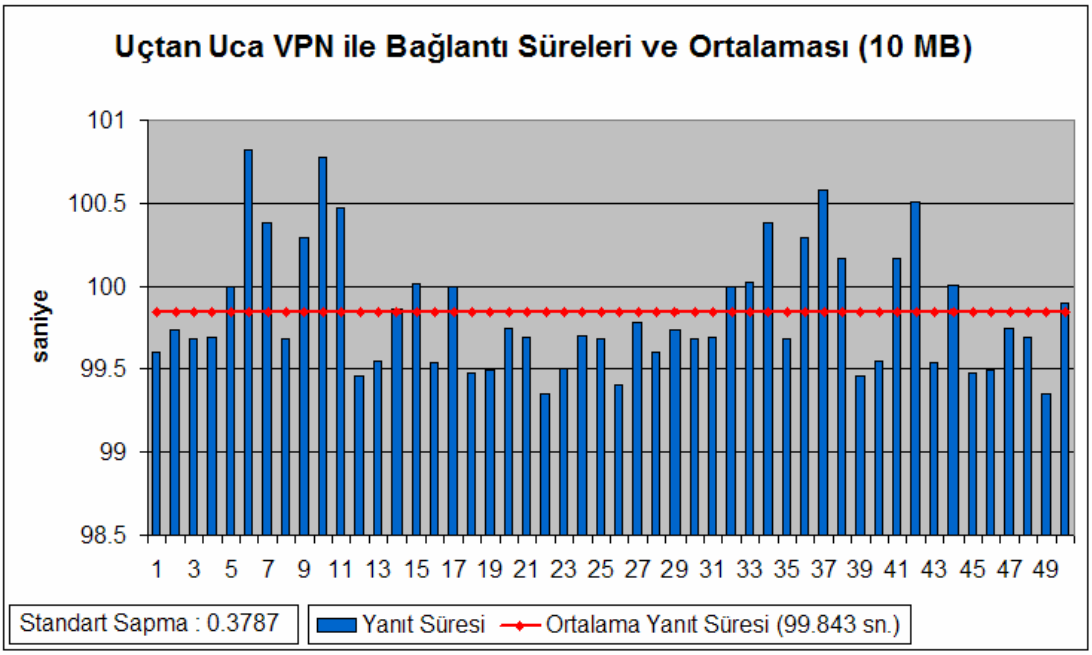
Şekil 5.10 : Uçtan Uca ile 10 MB'lık Web Sayfasının Görüntülenme Süresi

Yapılan erişimler her bir web sayfası için 50'şer kez tekrarlandı. 2.5 MB'lık web sayfasının ortalama görüntüleme süresi 23.929 sn. olarak ölçüldü. Standart sapma 0.3873 olarak hesaplandı.



Şekil 5.11 : Uçtan Uca ile Çağrılan Web Sayfası Yanıt Süreleri (2.5 MB)

Aynı ölçümler 10 MB'lık web sayfası için tekrarlandı. Bu kez ortalama görüntüleme süresi 99.843 sn. olarak ölçüldü. Standart sapma 0.3787 olarak hesaplandı.



Şekil 5.12 : Uçtan Uca ile Çağrılan Web Sayfası Yanıt Süreleri (10 MB)

6. SONUÇ

Giderek büyüyen internet ile iletişim altyapısı da büyümekte ve bilgisayar haberleşmesinin sağlandığı ağ yapısı da daha karmaşık hale gelmektedir. İnternet, getirdiği birçok avantajın yanında, kötü niyetli kullanıcılar sebebiyle, bilgi güvenliğinin öneminin en üst düzeyde olduğu bir platform olmuştur.

Güvenlik duvarları farklı güvenlik seviyesindeki bölgelerin kontrollü erişimini sağlamakla görevli bilgisayar ağı cihazlarıdır.

Küçük, orta ve büyük ölçekli kurum ve kuruluşlar, bilgi güvenliğinin önemli olduğu veri alışverişi ihtiyaçlarını, internetin güvenli olmaması sebebiyle internet servis sağlayıcılar tarafından kendilerine ayrılmış özel hatlar ile sağlamaktadır. Ancak bu hatların yüksek maliyetli olması, güvenlik ve ölçeklenebilirliğin olmaması Özel Sanal Ağ (VPN) kavramını ortaya çıkarmıştır. Özel sanal ağ ile, güvenli olmayan internet ortamında, veri alışverişi, sanal bir ağ ile güvenli şekilde yapılmaktadır.

Güvenlik duvarında sonlandırılabilen özel sanal ağların, SSL VPN, IPSec Uzak Erişim VPN ve IPSec Uçtan Uca VPN olanları internet ortamında en az bir istemciden uzak sisteme bağlanmayı sağlayan çeşitleridir. Bunlardan SSL VPN, istemci tarafındaki bilgisayarda yazılıma ihtiyaç duymadan karşı tarafa güvenli bir şekilde bağlantı kurabilir. IPSec Uzak Erişim VPN, istemci bilgisayarında karşı taraftaki ağ geçidine özel bir uygulamayı yüklemek ve konfigürasyonunu yapmak sureti ile VPN bağlantısını kurar. IPSec Uçtan uca VPN ise, sanal ağ kurmak için istemci tarafında IPSec destekleyen bir donanıma ihtiyaç duymaktadır.

Bu çalışmada, bu üç VPN çeşidinin Cisco 5500 serisi güvenlik duvarında konfigürasyonları adım adım anlatılmıştır. İstemci tarafında Windows işletim sistemi üzerinde SSL VPN ile karşı tarafta tanımlanan, internet üzerinden açık olarak erişilemeyen bir yerel web sunucusuna erişim sağlanması gösterilmiştir. IPSec Uzak Erişim VPN için, istemci tarafındaki bilgisayara Cisco Client VPN (CVPN) uygulaması yüklenmiş ve konfigürasyonu yapılmıştır. CVPN ile de karşı taraftaki yerel web sunucusuna erişim sağlanarak sanal ağın kurulduğu gösterilmiştir.

IPSec Uçtan uca VPN uygulamasında, istemci tarafında Cisco 850 serisi ADSL yönlendirici kullanılmıştır. Bu yönlendirici IPSec uzak erişim için konfigürasyon yapılarak, karşı taraftaki Cisco 5500 güvenlik duvarı ile Uçtan Uca IPSec VPN bağlantısı kurulmuştur. Bu VPN üzerinden de Cisco 850 serisi yönlendirici arkasında bulunan kullanıcının, Cisco 5500 serisi güvenlik duvarı arkasındaki yerel ağda bulunan web sunucusuna eriştiği gösterilmiştir.

Çalışmada aynı zamanda SSL ile IPSec teknolojileri ile Özel sanal ağlarda yaygın olarak kullanılan şifreleme yöntemleri de karşılaştırılmıştır.

Yine bu çalışmada her üç VPN tipi için, aynı şifreleme algoritmaları ve aynı hat kullanıldığı durumda hangi VPN tipinin http protokolü ile bir web sayfasının çağırılmasında daha hızlı olduğunun tespitine çalışılmıştır. Karşı tarafta erişilen web sunucusunun görüntülenme zamanları web tarayıcısına kurulan bir yazılımla ölçülmüş ve karşılaştırma yapılmıştır. Elde edilen sonuçlarda, SSL VPN yöntemi ile web sayfasına erişim süresi IPSec Uçtan Uca VPN ile IPSec Uzak Erişim VPN (CVPN) yöntemlerine göre daha uzun çıkmıştır. 2.5 MB boyutundaki web sayfası SSL VPN ile ortalama 25.5 sn. civarında görüntülenirken, CVPN ile bu süre 24.5 sn. Uçtan Uca VPN ile 24 sn. olarak ölçülmüştür. 10 MB boyutundaki web sayfası ise SSL VPN ile ortalama 110 sn. civarında görüntülenirken, CVPN ile bu süre 103 sn. Uçtan Uca VPN ile 100 sn. olarak kaydedilmiştir. Ölçümlerde Uçtan uca VPN çözümünde en düşük süre kaydedilmesi, şifreleme ve sarım işlemlerinin VPN ağ geçidi üzerinde yapılmasından kaynaklanmaktadır. Yapılan ölçümlerin standart sapmaları ise her iki boyuttaki web sayfasına erişimde SSL VPN yönteminde 1'in altında iken diğer yöntemlerde daha yüksek değerlerde hesaplanmıştır.

SSL VPN yöntemi, istemci tarafında herhangi bir yazılım donanıma ihtiyaç duymaması bir avantaj gibi görünse de, şifreleme işlemi web tarayıcı üzerinde SSL yöntemi ile yapıldığından http protokolünün kullanıldığı web sayfalarını çağırmadaki süresi, IPSec VPN'lere göre daha yüksek çıkmıştır. IPSec Uçtan Uca VPN yöntemi IPSec CVPN yöntemine göre 10 MB boyutunda daha net ortaya çıkan hızlı yanıt süresi, şifreleme ve şifre çözme işlemlerinin kullanılan ağ geçidi cihazında yapmasının bir sonucu olarak kaydedilmiştir.

KAYNAKLAR

[1] **Diffie W., Helmann M.E., Kasım,** 1976**,** New Directions in Cryptography, Information Theory, IEEE Transactions on Volume: 22 , Issue: 6

[2] **Ernesto Rassi, Subbarao V. Wunnava,** 2002, Data Encryption Performance and Evaluation Schemes, SoutheastCon, 2002. Proceedings IEEE

[3] **Popek, G. J., Kline, C. S.,** "Encryption and Secure Computers Networks", ACM Computer Surveys, 28 (1): 335-356 (1979)

[4] **Bülent Örencik, Rıfat Çölkesen,** 2002: Bilgisayar Haberleşmesi ve Ağ Teknolojileri, Papatya Yayıncılık, 2002

[5] **Sampalli Srinivas, Wei Qu,** IPSec Based Secure Wireless Virtual Private Networks, 2002, MILCOM 2002. Proceedings IEEE Volume: 2

[6] **Richard Deal,** 2005: The Complete Cisco VPN Configuration Guide, Cisco Press

[7] **Tarık Yerlikaya, Ercan Buluş, Nusret Buluş,** 2006, Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri, Akademik Bilişim Konferansları

[8] **Vijay Bollapragada, Mohamed Khalid, Scott Wainner**, 2005, IPSec VPN Design, Cisco Press

[9] **Aslan, G. B.,** 1999, Sayısal İmza Sistemlerinin İncelenmesi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü, İstanbul, p. 58

[10] **Salomaa, A.,** 1990, Public-Key Cryptography", ***Springer Verlag***, New York

[11] **Url-1** <*http://www.cisco.com*>*,* alındığı tarih 15.03.2010

[12] **Url-2** < *http://technet.microsoft.com*>*,* alındığı tarih 29.03.2010

[13] **Url-3** < *http://www.di-mgt.com.au*>*,* alındığı tarih 02.04.2010

[14] **Url-4** <*http://williamstallings.com*>, alındığı tarih, 10.04.2010

[15] **Aamer Nadeem, Dr M. Younus Javed**, 2005, A Performance Comparison of Data Encryption Algorithms, Information and Communication Technologies, 2005. ICICT 2005. p. 84 - 89

[16] **Stallings, William**, 1999, Cryptography and Network Security, Prentice Hall

[17] **Mark Lewis,** 2006: Comparing, Designing, and Deploying VPNs, Cisco Press

[18] **Scott C., Wolfe P., Erwin M.**, 1999, Virtual Private Networks, O'Reilly & Associations Inc. , Sebastopol, O'Reilly 1999

[19] **Url-5** <*http://bidb.itu.edu.tr*>, alındığı tarih, 10.05.2010

[20] **Jaha A.A., Shatwan F.B., Ashibani M.**, 2008, Proper Virtual Private Network (VPN) Solution. Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. The Second International Conference, p. 309 - 314

[21] **Shaikh, S.A., Al-Khayatt, S., Akhgar, B., Siddiqi, J.** 2002: A Study of Encrypted, Tunneling Models in Virtual Private Networks, Information Technology: Coding and Computing, 2002. Proceedings. International Conference, p. 139-143

ÖZGEÇMİŞ

Ad Soyad: Fuat Demir

Doğum Yeri ve Tarihi: 15 Mart 1981 KÜTAHYA

Lisans Üniversite: İstanbul Teknik Üniversitesi Elektronik ve Haberleşme Müh.

Fuat Demir, 15 Mart 1981'de Kütahya'da doğdu. İlk, orta ve lise yıllarını 1987-1999 yılları arasında Kütahya'da tamamladı. 2004 yılında İstanbul Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümünden mezun oldu. 2005 yılında İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü Telekomünikasyon Mühendisliği Yüksek Lisans programına kabul edildi.