AĞ GÜVENLİĞİ VE GÜVENLİK DUVARINDA VPN UYGULAMASI

N. Özlem ÜNVERDİ [1] **Zeynep YÜKSEL [2]**

Elektronik ve Haberleşme Mühendisliği Bölümü
Elektrik-Elektronik Fakültesi
Yıldız Teknik Üniversitesi, 34349, Beşiktaş, İstanbul

[1] e-posta: unverdi@yildiz.edu.tr [2] e-posta: zeynoyuksel@gmail.com

Anahtar sözcükler : Ağ Güvenliği, VPN, Uzak Erişim

ÖZET

Bu çalışmada, dünya çapında hızla yaygınlık kazanan güvenlik duvarı ile örnek bir özel sanal ağ uygulaması (VPN - Virtual Private Networks) incelenmiştir. VPN teknolojisinde bilginin korunarak iletilmesi analiz edilmiş ve ASDM kullanarak Uzak Erişim VPN uygulaması yapılandırılmıştır.

1. GİRİŞ

Kurumsal ağ kaynaklarının iç ve dış tehditlere karşı korunması, günümüzde iç ağ / dış ağ ayrımının yapılması söz konusu olmadan, kurumdaki herhangi bir kişiye herhangi bir yerden erişebilmek anlamında genişlemiştir. Ancak, bu gelişime paralel olarak, güvenlik uzmanları da ağlarına karşı olan tehditlerle başa çıkabilmek için daha karmaşık güvenlik politikaları uygulamak zorunda kalmaktadır. Bu tehditlerin en başta geleni, önemli ağ kaynaklarını Internet'ten veya yerel ağdan gelebilecek muhtemel saldırılara karşı korumaktır.

Dağınık yapıdaki özel iletişim ağlarının üzerinde bulunan bilgilerin, kamu iletişim ağı altyapısını kullanarak paylaşılması sırasında, kamu iletişim ağı üzerinden geçen bilgilerin üçüncü kişiler tarafından deşifre edilmesinin engellenmesi gerekir. VPN (Virtual Private Networks), bu sorunu ortadan kaldırmak için geliştirilmiş bir sistemdir. VPN sayesinde, özel iletişim ağına ait uzaktaki kullanıcıların, güvenilir olmayan kamu iletişim ağları üzerinden, kendi iletişim ağları ile serbestçe ve güvenilir bir şekilde haberleşmesi sağlanır [1,2].

Bu çalışmada, iletişim teknolojisindeki son gelişmeler içinde yer alan VPN'in çalışma akışı ve güvenlik duvarı mantığı ışığında konuyla ilgili özel sanal ağ uygulaması yapılmıştır. Çalışmanın 2. Bölümü'nde, VPN'in temel özellikleri incelenmiş ve güvenlik yapılandırılması açıklanmıştır. 3. Bölüm'de, ASDM kullanarak Uzak Erişim VPN konfigüre edilmiş ve 4. Bölüm'de, elde edilen sonuçlar değerlendirilerek yorumlanmıştır.

2. VPN SİSTEMLERİNDE BİLGİNİN KORUNMASI

Bu bölümde, ağdaki güvenlik mekanizması irdelenmiştir.

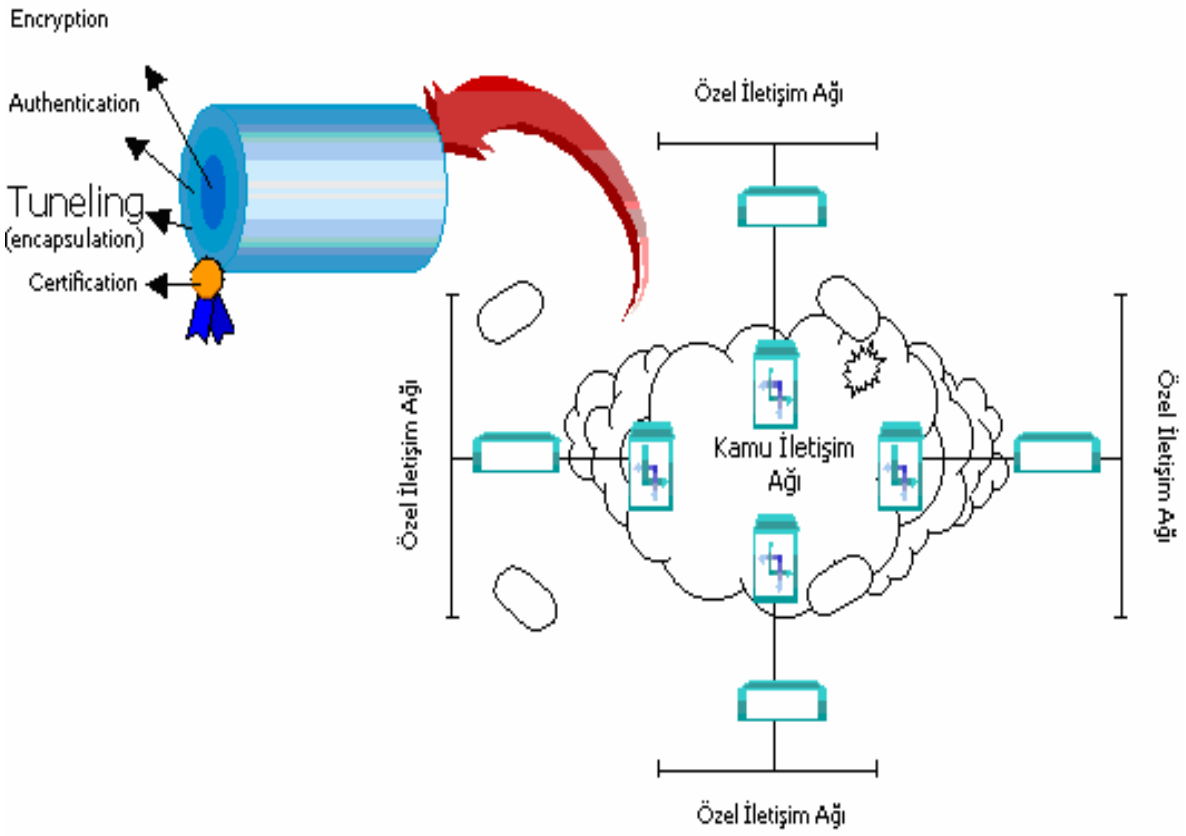
2.1 VPN SİSTEMLERİNDE GÜVENLİK SEVİYELERİ

VPN kurabilmek için özel iletişim ağı ile kamu iletişim ağı arasına çeşitli üreticilerin VPN donanım ve yazılımlarının konulması gerekir. Dolayısıyla, kullanıcılardan birisi, uzakta bulunan bir ağdaki kullanıcı ile haberleşmek istediğinde, kullanıcının haberleşme paketleri, önce kendi özel iletişim ağında bulunan VPN sistemine gelir, ardından kamu iletişim ağı üzerinde uzaktaki haberleşmek istediği kullanıcının özel iletişim ağını koruyan VPN sistemine gider ve buradan da kullanıcıya ulaşır. Özel iletişim ağları arasında, her ağda bulunan VPN sistemleri kendi aralarında *sanal tüneller* oluşturur. VPN sistemleri, özel bilgileri taşıyan haberleşme paketlerinin korunmasını, kendi aralarında yarattıkları sanal tüneller sayesinde sağlar.

VPN sistemlerinde dört seviyeye kadar güvenlik sağlanabilir. Bu seviyeler, Sertifikasyon, Şifreleme, Tanımlama - Sorgulama ve Tünelleme'dir [2]:

- **Sertifikasyon :** Tüm iletişim ağı içerisinde bulunan VPN sistemleri aynı sertifikasyon ismini taşımalıdır. Bu isme sahip olmayan VPN sistemine diğer VPN sistemleri tarafından güvenilmeyecek ve bağlantı kurulmayacaktır.

- **Şifreleme :** Özel iletişim ağından kamu iletişim ağına paketler iletilmeden önce şifrelenir. Şekil-1'den de anlaşılacağı gibi, herkese açık olan kamu iletişim ağında paketler başkaları tarafından incelense bile içeriğinin anlaşılması mümkün değildir. Şifreleme belli kurallarla yapılır ve bu kurallar anahtar kod ile belirlenir.



Şekil-1 VPN'in genel yapısı.

Bu kod, VPN sistemleri arasında belli aralıklarla sürekli olarak değişir. Bu sayede bu kodun öğrenilmesi mümkün olmaz.

- **Tanımlama - Sorgulama :** Şifrelenmiş paketler, aynı zamanda şifreleme işlemini yapan kaynak VPN sisteminin imzasını taşır. Bu imzanın konulmasının, gönderilen veya alınan mesajın güvenilir olduğunun garantiye alınması ve gönderen kişinin kimliğinin ortaya çıkarılması olmak üzere iki amacı vardır.

- **Tünelleme :** VPN sistemleri, şifrelenmiş haberleşme paketlerini, diğer VPN sistemlerine güvenliğin olmadığı kamu iletişim ağları üzerindeki sanal tüneller içerisinden yollar. Bu tüneller, gönderen ve alan VPN sistemlerinin IP adreslerinden oluşur. Gönderilen bilgi, bu paketler içerisine *yeni bilgi ekleme yöntemi* ile konulur. Gerçek gönderen ve alan kullanıcıların IP adresleri, bu sayede saklanmış olur.

2.2 VPN TİPLERİ

Teknolojide dört tür VPN'den yararlanılır:

- **Siteden Siteye VPN'ler :** İnternet gibi bir ağ üzerinden çeşitli şifreleme metodları ile uzaktaki ofislerin, merkezdeki ofislere güvenli bir şekilde bağlantısını sağlar.

- **Uzak Erişim VPN'ler :** Modem kullanıcıları ve uzak kullanıcılar gibi gezici kullanıcıların, şirket içi ağlarına İnternet üzerinden şifreli ve güvenli bir şekilde bağlantısını sağlar.

- **VPN – İstemciler :** Merkezdeki VPN, donanım, yazılım, kablosuz istemci çözümleri ile cihazlara bağlanarak güvenli bir şekilde şirket içi ağa ulaşma imkanını sağlar.

- **Servis Sağlayıcı VPN'ler :** MPLS tabanlı VPN ağları, Frame Relay ve ATM'in güvenlik ve servis kalitesini, IP'nin de ölçeklenebilirlik özelliklerini aynı anda kullanıcıya sunar. MPLS, IP yönlendirme yapan bir omurga üzerinde çalışır ve verilen servisle ilgili kararlar omurganın uç noktalarında ek bir işlem yükü gerektirmeden yapılabilir. MPLS - VPN, aynı zamanda Frame Relay'de ve ATM'de yapılması gereken karmaşık protokol ve adres dönüşümlerini ortadan kaldırır [1-3]. Frame Relay ve ATM ağlarında güvenliğin sağlanması için gereken dört öge olan adres alanı ayrılması, yönlendirmenin tamamen bağımsız yapılması, saldırılara karşı dirençli olması ve IP Spoofing'e karşı dirençli olması özellikleri, MPLS'de de sağlanır. Bu anlamda, ikinci ve üçüncü seviye arasında çalışan bir protokol olarak düşünülebilen MPLS, en az Frame Relay ve ATM kadar güvenilirdir [2, 3].

3. ASDM KULLANILARAK UZAK ERİŞİM VPN KONFİGÜRASYONU

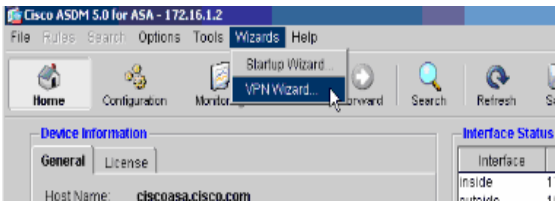
Bu çalışmada, güvenlik duvarı üzerinde ASDM kullanarak Uzak Erişim VPN yapılandırılmıştır. Uzak erişim konfigürasyonu, Cisco VPN Client'ların yüklendiği mobil kullanıcılar için güvenli uzak erişim sağlar. Uzak Erişim VPN, uzak kullanıcılara ve merkezi ağ kaynaklarına güvenli bir şekilde erişime imkan tanır.

Güvenlik uygulamalarının yapılandırılmasında ve VPN'lerin güvenli yönetimindeki ana kavramlar, gruplar ve kullanıcılardır. Bunlar, VPN kullanımı ve kullanıcı erişimi için tanımlanan özellikleri belirtir. Bir grup, tek bir varlık gibi davranan kullanıcılardan oluşur. Kullanıcılar, *group policy*lerden özelliklerini alır. Tünel grupları, spesifik bağlantılar için group policy tanımlar. Eğer bir kullanıcıya şahsi group policy atanmazsa bağlantılar için group policy uygulanır.

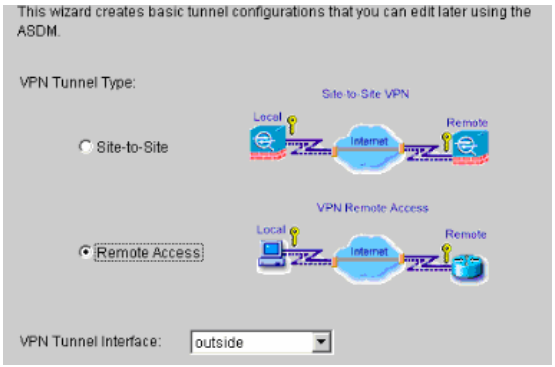
The Internet Security Association and Key Management Protocol (ISAKMP), IPSec Security Association'ın nasıl yapılandırıldığına razı olan host'ların hemfikir olduğu IKE olarak adlandırılan bir müzakere protokolüdür. Her ISAKMP müzakeresi, Phase 1 ve Phase 2 olmak üzere iki bölüme ayrılır. Phase 1, ISAKMP müzakere mesajları için korunan ilk tüneli, Phase 2 ise, güvenli bağlantı boyunca seyahat eden veriyi koruyan tünelleri yaratır [4].

3.1 ASDM KULLANILARAK REMOTE VPN KONFİGÜRASYONU

- Şekil-2'de görüldüğü üzere ana pencereden Wizards > VPN Wizard seçilir.



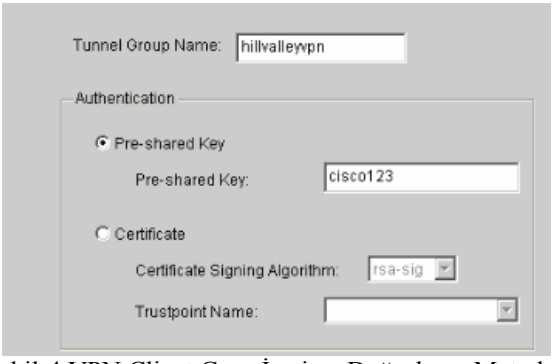
Şekil-2 ASDM ana sayfasından VPN Wizard seçimi.



Şekil-3 Uzak Erişim VPN.

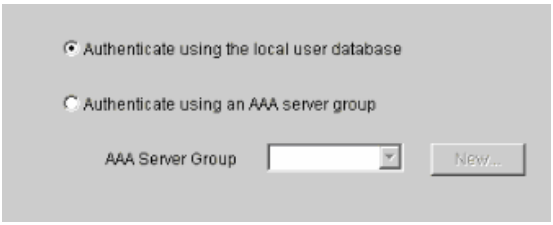
- Günümüzde gezici kullanıcıların artması nedeniyle yoğunlaşan şirket içi ağlarına İnternet üzerinden güvenli erişimi sağlayan Uzak Erişim VPN (Remote Access) çeşidi, Şekil-3'de görüldüğü gibi seçilir.

- Kullanılan güvenlik cihazı, ortak erişim parametreleri ile temellendirilen uzak erişim tünellerinin gruplandırılmasına izin verir. Şekil-4'de gösterildiği gibi, tünel grup ismi için bir ad girilir ve doğrulama bilgisi tanımlanır. Bu çalışmada **Pre-shared Key** seçilmiştir.

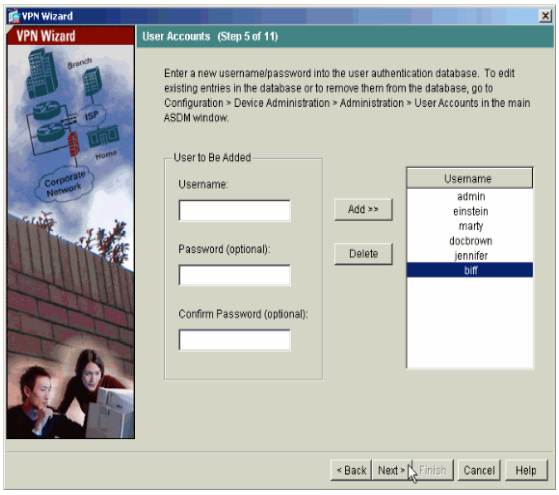


Şekil-4 VPN Client Grup İsmi ve Doğrulama Metodu.

- Şekil-5'de, uzak kullanıcıların, yerel kullanıcı veritabanına veya harici AAA server grubuna doğrulanması için hangi doğrulamanın kullanılacağının seçimi yer almaktadır. Burada, yerel kullanıcı veritabanı kullanılarak doğrulama seçilmiştir.



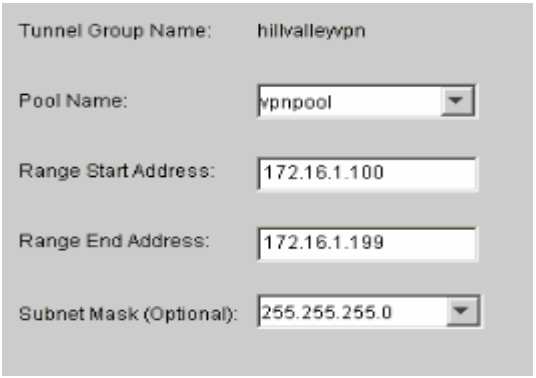
Şekil-5 Client doğrulama.



Şekil-6 Kullanıcı hesapları.

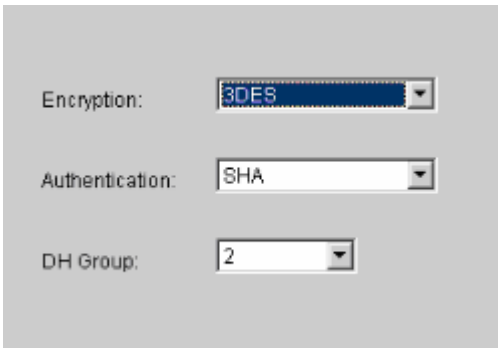
- Şekil-6'da görüldüğü gibi, gerekirse yerel veritabanına kullanıcılar ilave edilir.

- Uzak VPN Client'lar bağlandığında, dinamik olarak adres ataması için yerel adres havuzunun tanımlanması, Şekil-7'de yer almaktadır.



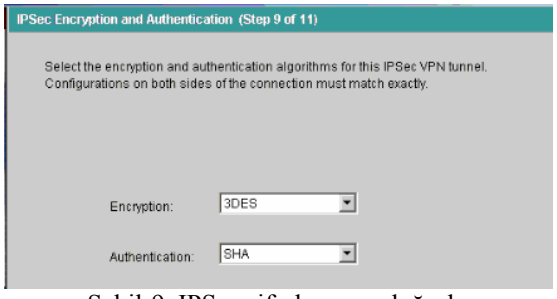
Şekil-7 Adres havuzu.

- Şekil-8'de IKE (Internet Key Exchange) için parametrelerin tanımlanması görülmektedir.



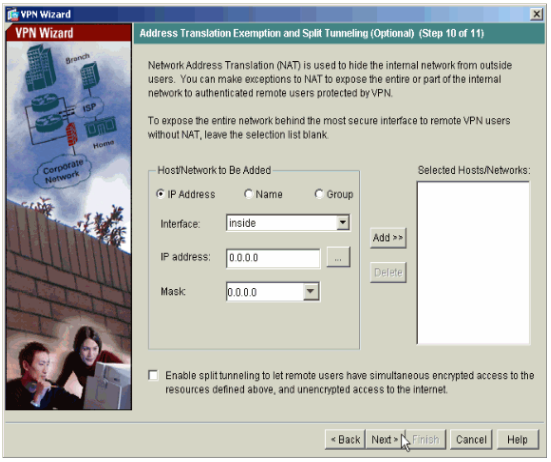
Şekil-8 IKE Policy.

- IPSec için parametreler tanımlanır. Tünelin her iki yakasındaki konfigürasyonlar tam olarak eşleşir; ancak, Cisco VPN Client otomatik olarak kendisi için düzgün konfigürasyonu seçer. Bu nedenle, PC kullanıcıları üzerinde IKE konfigürasyonu gerekli değildir. Şekil-9'da IPSec şifreleme ve doğrulama izlenmektedir.



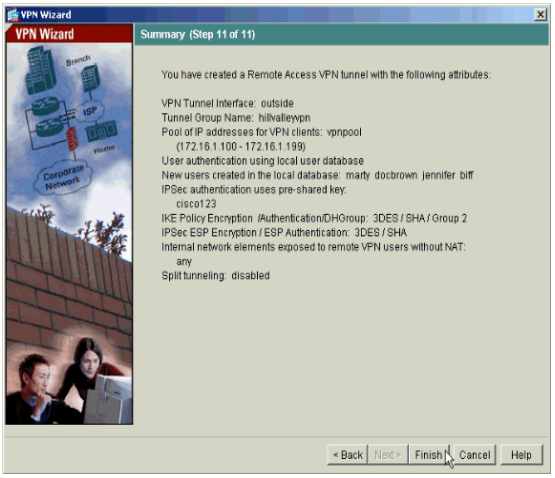
Şekil-9 IPSec şifreleme ve doğrulama.

NAT (Network Address Translator, Ağ Adresi Çeviricisi), dış kullanıcılardan iç ağı saklamak için kullanılır. Bu liste boş bırakılırsa, uzak VPN kullanıcılarının, güvenlik duvarının iç ağına erişimlerine olanak tanınır. Şekil-10'daki pencerede görüldüğü gibi, trafiği şifreleyen *split tunneling*'e imkan sağlanır. Split tunneling kullanılmadığında, uzak VPN kullanıcılarından gelen tüm trafik, güvenlik duvarı üzerinden geçer. Bu durum, çok fazla bant genişliği ve işlemci yoğunluğuna neden olur.



Şekil-10 NAT.

- Şekil-11'deki pencere yapılmış işlemlerin özetini göstermektedir. Finish'e tıklanarak konfigürasyon tamamlanır [4, 5].



Şekil-11 Remote Access VPN işlemini tamamlama.

4. SONUÇ

Bu çalışmada, güvenlik duvarında uzak erişim VPN kullanıcılarının ağ erişiminin sınırlandırılması ele alınmıştır. Güvenlik duvarı üzerinde Uzak Erişim VPN yapılandırılarak mobil kullanıcılar için güvenli uzak erişim sağlanmıştır. Bu çalışma ile, mobil kullanıcılara ait verilerin, İnternet üzerinden güvenli bir şekilde bir noktadan diğerine aktarılırken şifrelenmesi sağlanmıştır. Uygulamada görüldüğü gibi, bu sistem sayesinde, VPN

teknolojisi ile verilerin çalınması veya değiştirilmesi mümkün değildir.

VPN, herkese açık bir ağ olan İnternet üzerinden verilerin güvenli bir şekilde iletilmesine olanak tanıdığı için, şirketlerin, ofislerini birbirine ya da mobil kullanıcılarını merkeze bağlamak için kendi ağ omurgalarını kurmasına gerek kalmaz. Bu durum da, iletişim maliyetlerinin düşürülmesini sağlar.

KAYNAKLAR

[1] *Internetworking & TCP/IP*, Armada Eğitim Merkezi, İstanbul, 2002.

[2] Çölkesen R., Örencik B., *Bilgisaycar Haberleşmesi ve Ağ Teknolojileri*, Papatya Yayıncılık, İstanbul, 2003.

[3] Akbulut N., Koçak B., *TCP/IP & Networking*, Turkcell, İstanbul, 2002.

[4] *Configuration Examples and TechNotes:* http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_configuration_examples_list.html

[5] Yüksel Z., *Ağ Güvenliği ve Güvenlik Duvarında VPN ve NAT Uygulamaları*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 2007.