BÖLÜM 4

SANAL ÖZEL AĞ

ANAHTAR KAVRAMLAR

Sanal Özel Ağ, Şifreleme Fonksiyonları, Bütünlük Fonksiyonları, Kimlik Doğrulama Algoritmaları, Ipsec, VPN Türleri, VPN'in Avantajları

ÖĞRENME HEDEFLERİ

1. VPN teknolojisine neden ihtiyaç duyulduğunu açıklar
2. VPN'in çalışma prensibini açıklar
3. VPN yapısında kullanılan kriptografik algoritmaları açıklar
4. Simetrik ve asimetrik şifreleme algoritmalarına örnekler verir
5. Hash fonksiyonlarının amacını açıklar
6. IPsec çerçevesini açıklar
7. VPN türlerini bilir
8. VPN türlerinin kullanım amacını açıklar

DÖRDÜNCÜ BÖLÜM

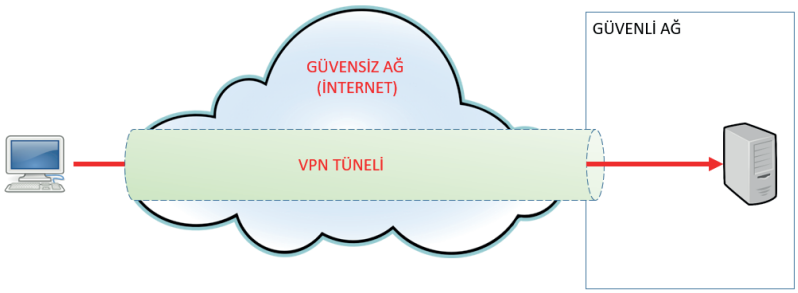
GİRİŞ

Bilgisayar ağlarının devasa bir koleksiyonu olan İnternet, genelde güvensiz bir ortam olarak düşünülür. Kurumlar veya bireyler, siber güvenlik ilkelerini uygulamadıkları taktirde, bu güvensiz ortam üzerinden IP paketleri aracılığıyla taşınan veriler güvende değildir. Bu durumda veriler potansiyel olarak üçüncü taraflarca okunabilir ve değiştirilebilir. Bu nedenle özellikle hassas verilerin güvenliğinin sağlanması gerekir.

Siber güvenliğin üç temel unsuru, gizlilik, bütünlük ve kullanılabilirliktir. İster sabit bir diskte saklanan durağan veriler olsun, ister ağdan akan hareket halindeki veriler olsun, verilerin güvenliğinin sağlanması bu üç temel unsura bağlıdır. Yani veriler internet ortamındaki IP paketleri içerisinde akışı esnasında şifrelenmesi (gizlilik), verinin değişip değişmediğinin belirlenmesi (bütünlük) ve verilerin kaynağının doğrulanması siber güvenliğin gerektirdiği bir ihtiyaçtır.

İnternet ve ağ ortamında hareket eden veriler IP paketlerinin içerisinde belirli boyutlarda yükler olarak taşınırlar. IP ise tasarımı gereği güvenli bir protokol değildir. Yani şifreleme, kimlik doğrulama ve bütünlük tasarım olarak IP protokolünde yoktur. Bu nedenle IP'nin güvenli bir şekilde taşınabilmesi için geliştirilen çeşitli yöntemlerden biri **Sanal Özel Ağ (Virutal Private Network - VPN)** kullanmaktır.

VPN teknolojisinde iletişim kuran taraflar arasında *tünel* olarak adlandırılan özel kanallar kullanılır. Şekil 1'de basit bir VPN tüneli yapısı gösterilmektedir.



Şekil 1. VPN Tünelinin yapısı

VPN tüneli, internet trafiğini şifreleyerek ve güvenli bir şekilde ileterek, kullanıcıya veya kuruma güvenli bir şekilde veri iletim imkânı sunar(P. Ferguson & Huston, 1998).

VPN, çeşitli kriptografik algoritmalar ve teknikler kullanılarak, IP'de tasarımsal olarak var olmayan özelliklerin sonradan eklenmesini sağlayan bir teknoloji kümesidir(Ezra ve diğerleri, 2022). VPN sayesinde IP paketlerinin içerikleri (yükleri) desteklenen çeşitli kriptografik algoritmalar aracılığıyla şifrelenebilir. Benzer şekilde verilerin değişip değişmediğini doğrulamak için bütünlük sağlayıcı kriptografik algoritmalar VPN yapısında kullanılır. Yine VPN yapısında kimlik doğrulama ve inkâr edilememezlik sağlayan kriptografik fonksiyonlar kullanılabilir. Bu nedenle bu bölümde öncelikle VPN için son derece önemli olan kriptografik algoritmalar kısaca açıklanacaktır.

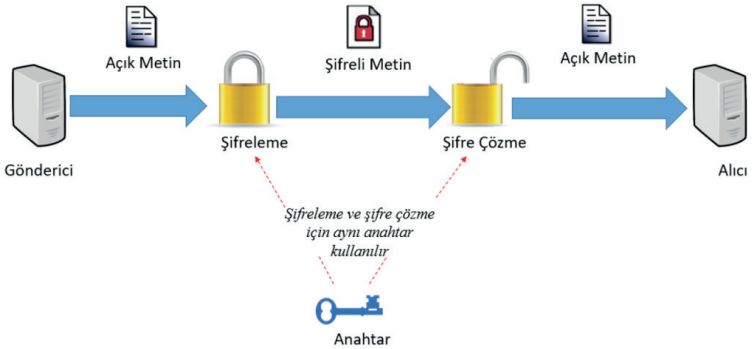
1. KRİPTOGRAFİK ALGORİTMALAR

VPN yapısında kullanılan kriptografik algoritmalar, internet trafiğini şifrelemek ve güvenli bir şekilde iletmek için kritik bir rol oynar. Bu algoritmalar, kullanıcı verilerini koruyarak gizliliği sağlamak, veri bütünlüğünü korumak ve güvenli bir iletişim kanalı oluşturmak amacıyla özenle seçilir ve konfigüre edilir.

2. ŞİFRELEME ALGORİTMALARI

Şifreleme algoritmaları veri gizliliğini sağlayan kriptografik matematiksel fonksiyonlardır. Şifreleme, verileri anahtar (key) denen bir veri ile dönüştürerek, yalnızca doğru anahtara sahip olan kişilerin veya sistemlerin verileri okuyabilmesini sağlar. Bir şifreleme algoritması, metni veya veriyi şifrelerken belirli bir anahtarla birlikte matematiksel operasyonları uygular. Şifreleme, bilgisayarlar arası iletişimden veri depolamaya, çevrimiçi bankacılıktan dosya şifrelemeye kadar birçok farklı uygulamada kullanılır. Şifreleme, hassas verilerin güvenliğini sağlamak için temel bir araçtır ve kritik bir öneme sahiptir.

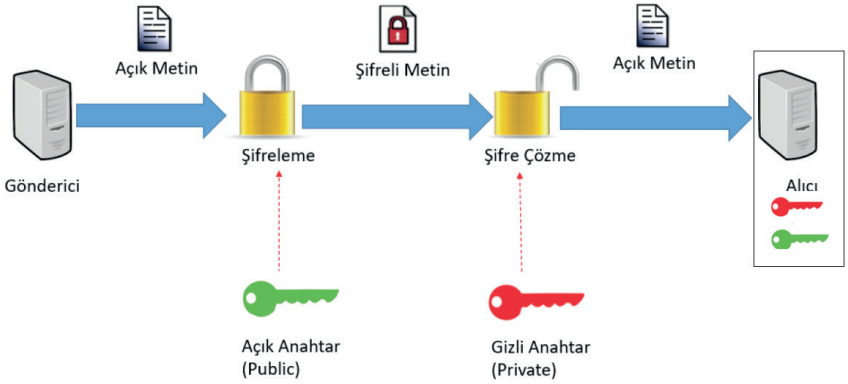
Genelde simetrik ve asimetrik olmak üzere iki tür şifreleme algoritması bulunur. Simetrik şifrelemede veriyi şifrelemek ve şifreyi çözmek için aynı anahtar kullanılır(Alenezi ve diğerleri, 2020) (Şekil 2).



Şekil 2. Simetrik şifreleme

Simetrik şifrelemede kullanılan anahtar, gönderici ve alıcı tarafından bilinmelidir. Bu anahtar sadece bu iki taraf arasında paylaşılır ve gizli kalır. Bu nedenle bu tür anahtarlara *gizli anahtar* denir.

Asimetrik şifrelemede ise veriyi şifrelemek ve deşifre etmek için birbiri ile matematiksel ilişkili bir anahtar çifti kullanılır. Bu anahtar çiftinden şifrelemeyi sağlayan anahtara açık anahtar (public key), şifre çözmeyi sağlayan anahtara ise gizli anahtar (private key) denir. Şekil 3'te asimetrik anahtar yapısı gösterilmektedir.



Şekil 3. Asimetrik şifreleme

Açık anahtar, veriyi şifrelemek isteyen herkes ile açık bir şekilde paylaşılabilir. Açık anahtar şifre çözme için kullanılamayacağı için, anahtara sahip farklı kişiler olsa bile şifrelenmiş veri çözümlenemez. Şifre çözme için kullanılan anahtar ise sadece bir tarafta ve paylaşılmadan gizli olarak tutulur. Böylece açık anahtara sahip olan herkes birbirlerinin verilerini deşifre edemeden güvenli bir şekilde gönderebilir. Şifre çözme işlemi sadece gizli anahtara sahip tarafça yapılır.

Simetrik ve asimetrik şifreleme, VPN yapısında farklı amaçlar doğrultusunda kullanılır. Simetrik şifreleme hızlı olduğu için genelde IP paketlerinin şifrelenmesinde kullanılırken, asimetrik şifreme kimlik doğrulama sürecinde anahtar değişimi için kullanılır. VPN yapısında yaygın olarak kullanılan simetrik şifreleme algoritmaları şunlardır:

Veri Şifreleme Standardı (DES) : Verileri şifrelemek için kullanılan eski bir simetrik şifreleme algoritmasıdır. DES, Amerika Birleşik Devletleri Ulusal Standartlar Enstitüsü (NIST) tarafından 1977 yılında yayınlanmıştır ve daha sonraki yıllarda daha güvenli şifreleme algoritmalarıyla yer değiştirmiştir. DES, 64-bit bloklar halinde çalışır ve 56-bitlik bir anahtar kullanır. Yani, şifrelenecek metin 64-bitlik bloklara bölünür ve bu bloklar aynı anahtar kullanılarak şifrelenir. Dezavantajı, 56-bitlik anahtarın günümüz standartlarında yeterince güvenli olmamasıdır; modern bilgisayar gücü, kısa anahtarları daha hızlı kırabilir.

Bu nedenle, DES günümüzde genellikle daha güçlü ve güvenli şifreleme algoritmalarına yerini bırakmıştır. Ancak DES, şifreleme tarihinde önemli bir dönemeç olarak kabul edilir ve simetrik şifreleme alanında temel bir anlayışı temsil eder.

Gelişmiş Şifreleme Standardı (AES) : Verileri şifrelemek için kullanılan güçlü ve yaygın bir simetrik şifreleme algoritmasıdır. AES, DES gibi eski şifreleme standartlarını yerine geçmek üzere 2001 yılında Amerika Birleşik Devletleri Ulusal Standartlar Enstitüsü tarafından belirlenmiştir(Su ve diğerleri., 2019).

AES, 128-bit, 192-bit ve 256-bit olmak üzere üç farklı anahtar uzunluğunu destekler. Bu, daha güçlü şifreleme seçeneklerini sunar ve şifrelenmiş verilerin daha güvenli hale getirilmesine olanak tanır(Muttaqin & Rahmadoni, 2020). AES,

bilgisayarlar arası iletişimden dosya şifrelemeye kadar bir dizi uygulamada kullanılır ve günümüzde genellikle standart şifreleme ihtiyaçlarını karşılamak için tercih edilen bir algoritmadır. AES, hızlı ve etkili bir şekilde çalışırken güçlü güvenlik sağlar. Bu özellikleri nedeniyle, VPN, veri depolama ve diğer birçok uygulama için yaygın olarak kullanılır. AES, bilgisayar güvenliği açısından kritik bir rol oynar ve dünya genelinde birçok şifreleme uygulamasında standart olarak kabul edilir(Mouha ve diğerleri, 2021).

VPN'lerde sıkça kullanılan asimetrik şifreleme algoritmalarından bazıları aşağıda özetle açıklanmıştır.

RSA (Rivest-Shamir-Adleman): RSA, genel anahtar altyapısını kullanan en yaygın asimetrik şifreleme algoritmalarından biridir. Anahtar değişiminde ve dijital imzalarda sıklıkla kullanılır(Obaid, 2020).

Diffie-Hellman Anahtar Değişimi: Diffie-Hellman (DH) anahtar değişimi protokolü, iki taraf arasında güvenli bir şekilde ortak bir anahtar oluşturmak için kullanılır(Purohit ve diğerleri, 2020). Bu anahtar daha sonra simetrik şifreleme anahtarlarını güvenli bir şekilde değiştirmek için kullanılabilir.

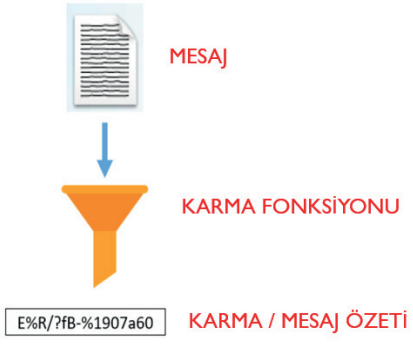
Eliptik Eğri Kriptografisi (ECC): ECC, daha küçük anahtar uzunluklarıyla güçlü şifreleme sağlayabilen bir asimetrik şifreleme algoritmasıdır(Miller, 1985). ECC, daha düşük hesaplama gücü ve daha az bant genişliği kullanımıyla özellikle mobil cihazlar için idealdir.

Bu algoritmalar, VPN'lerde güvenli anahtar değişimi ve dijital imzalama için kullanılır. VPN sağlayıcıları genellikle kullanıcılara güvenli bir anahtar değişimi için uygun algoritmaları seçmelerini sağlar ve genellikle güvenlik standartlarına ve kullanım senaryolarına bağlı olarak uygun olan algoritmaları belirler.

3. BÜTÜNLÜK ALGORİTMALARI

Bütünlük (integrity) algoritmaları, verilerin bütünlüğünü sağlamak için VPN yapısında kullanılır. Bu algoritmalar, verilerin iletim sırasında değiştirilip değiştirilmediğini doğrular. Verilerin güvenli bir şekilde iletilmesi esnasında, verilerin bütünlüğü sağlanarak, verilerin izinsiz değiştirilmesi veya bozulması önlenir.

Veri bütünlüğünü sağlamak için *hash* (bazen karma veya özet olarak da adlandırılır) fonksiyonları kullanılır (Şekil 3).



Şekil 4. Hash algoritmalarının çalışma mantığı

Kriptografi alanında hash fonksiyonu, bir girdiyi (mesaj, veri veya dosya) hash değeri veya mesaj özeti (message digest) olarak bilinen sabit boyutlu bir karakter dizisine dönüştürme işlemidir. Bu dönüşüm, girdi verisine matematiksel bir algoritma uygulanarak elde edilir. Karma işlemin sonucu, orijinal mesajın sabit uzunluktaki bir parmak izi olarak düşünülebilir. Bu nedenle bazen bir mesaj özeti olarak da adlandırılır.

En yaygın kullanılan bütünlük algoritmaları şunlardır:

HMAC (Hash-based Message Authentication Code): HMAC, bir hash fonksiyonu (örneğin, SHA-256) kullanarak verilere özel bir doğrulama kodu ekler. Bu işlem hem bütünlüğü doğrular hem de verinin doğruluğunu sağlar.

SHA-2 (Secure Hash Algorithm 2): SHA-2 ailesi, 224, 256, 384, 512 bitlik hash fonksiyonları içerir. Özellikle SHA-256 ve SHA-512, genellikle bütünlük doğrulaması için kullanılır(Gupta & Kumar, 2014).

MD5 (Message Digest Algorithm 5): MD5, 128-bit hash değeri üreten eski bir hash fonksiyonudur(Yong-Xia & Ge, 2010). Ancak, günümüzde güvenlik açıkları nedeniyle önerilmez(Gupta & Kumar, 2014).

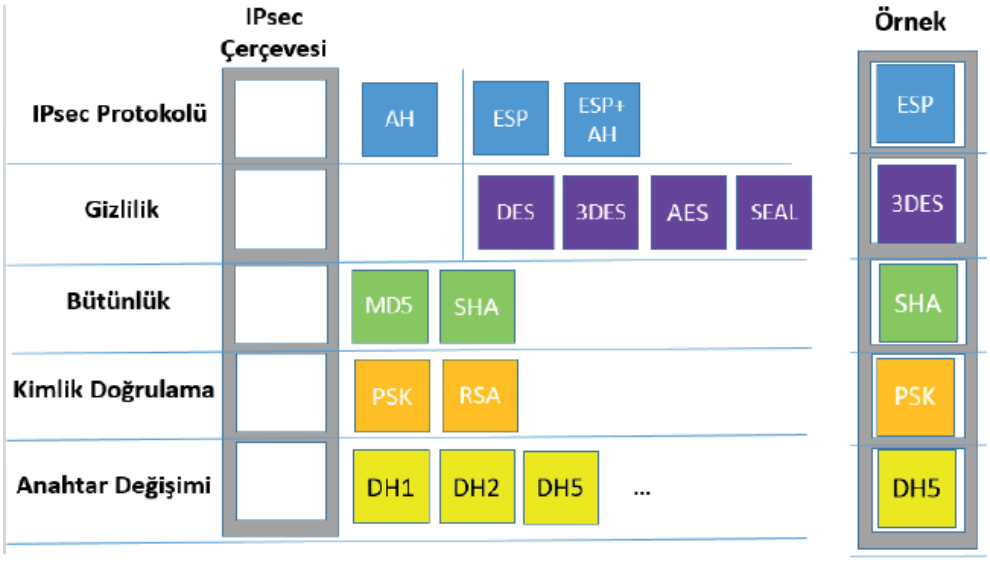
Bu algoritmalar, verilerin bütünlüğünü doğrulamak için kullanılır. Hangi algoritmanın tercih edileceği, kullanım senaryosuna ve güvenlik gereksinimlerine bağlı olarak değişebilir. Daha yüksek güvenlik seviyeleri gerektiren durumlarda HMAC ve SHA-2 gibi güçlü ve güvenilir algoritmalar tercih edilir.

4. IPsec ÇERÇEVESİ

IPsec (Internet Protocol Security), internet üzerinden veri iletimini güvenli hale getirmek için kullanılan bir güvenlik çerçevesidir (framework) (N. Ferguson & Schneier, 1999). IPsec, veri bütünlüğünü doğrulama, verileri şifreleme ve kimlik doğrulama gibi güvenlik hizmetlerini sağlayarak internet trafiğini korur. IPsec, genellikle VPN bağlantılarında, uzaktan erişimde, güvenli ağ bağlantılarında ve sanal özel ağlarda (VLAN) kullanılır.

IPsec, IP paketlerini şifreleyerek ve/veya doğrulayarak iletim sırasında verilerin gizliliğini ve bütünlüğünü sağlar. Ayrıca, IPsec, veri iletimi sırasında paketleri kimlik doğrulama sürecinden geçirerek güvenilirliği artırır. Bu şekilde, internet üzerinden veri iletimi güvenli hale gelir ve izinsiz erişim, veri değişiklikleri veya veri manipülasyonu gibi tehditlere karşı koruma sağlanır.

IPsec, iki ana bileşenden oluşur: AH (Authentication Header) ve ESP (Encapsulating Security Payload)(Madson & Glenn, 1998). AH, veri bütünlüğünü doğrularken, ESP, verileri şifreleyerek ve/veya doğrulayarak güvenlik sağlar. IPsec, özellikle şirket içi ağlardan uzaktan erişime kadar bir dizi uygulama senaryosunda güvenli iletişim sağlamak için kullanılır.



Şekil 5. IPsec çerçevesi ve örnek poliçe

Şekil 5'te gösterilen IPsec çerçevesi, IP'nin güvenli transferi için gereken gizlilik, bütünlük ve kimlik doğrulama gibi ek özellikleri sağlar. Şekil 5'deki örnekte desteklenen ek özellikler ile bir poliçe oluşturulur. Böylece bu poliçeyi destekleyen taraflarla güvenli VPN bağlantısı kurulabilir.

5. VPN TÜRLERİ

İnternet üzerinde güvenli bir şekilde veri iletimi sağlamak için kullanılan VPN'ler, farklı kullanım senaryolarına uygun olarak farklı türlerde olabilir. Yaygın olarak kullanılan VPN türlerinin bazıları aşağıda tanımlanmıştır.

Uzaktan Erişim VPN (Remote Access VPN): Uzaktan erişim VPN'leri, uzak kullanıcıların güvenli bir şekilde şirket içi ağa veya başka bir özel ağa erişmesine olanak tanır. Bu tür VPN'ler, evden çalışan personel veya seyahat eden çalışanlar gibi uzaktan çalışan kullanıcılar için idealdir.

Remote Access VPN'in çalışma şekli aşağıda adımlar halinde ifade edilmiştir.

• *Kimlik Doğrulama*: Uzaktan erişim VPN'i kullanıcılardan kimlik doğrulama bilgilerini (kullanıcı adı, şifre, vb.) talep eder. Bu adım, doğru kullanıcıların sisteme giriş yapmasını sağlar.

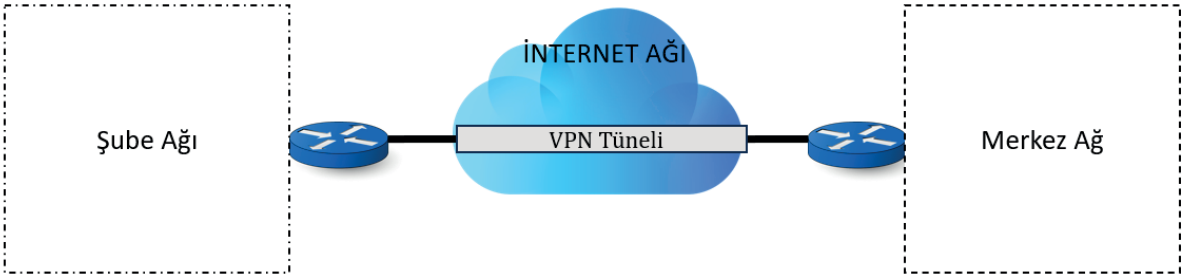
• *Şifreleme*: Kullanıcının bilgisayarındaki VPN istemcisi, şirket içi ağa giden veriyi şifreler. Bu şifreleme, verilerin güvenli bir şekilde iletilmesini sağlar. Genellikle SSL/TLS veya IPSec protokolleri kullanılarak şifreleme gerçekleştirilir.

• *Uzaktan Bağlantı Kurma*: Kullanıcı, VPN istemcisini kullanarak uzaktan şirket içi ağa bağlanır. Bağlantı, genellikle internet üzerinden yapılır. VPN istemcisi, kullanıcının cihazı ve şirket içi ağ arasında güvenli bir tünel oluşturur.

• *Tünel Oluşturma*: Şirket içi ağdaki VPN sunucusu, uzaktaki kullanıcıya özel bir ağ tüneli oluşturur. Bu tünel, kullanıcının verilerinin şifrelenmiş bir şekilde şirket içi ağa iletilmesini sağlar.

• *Güvenli Erişim*: Uzaktan erişim VPN'i ile kullanıcılar, şirket içi ağda bulunan kaynaklara (dosyalar, yazıcılar, veritabanları, uygulamalar vb.) güvenli bir şekilde erişebilir. Bu erişim, sanki kullanıcı şirket içi ağda fiziksel olarak bulunuyormuş gibi sağlanır.

Site-to-Site VPN: Site-to-Site VPN'ler, iki veya daha fazla şirket içi ağı arasında güvenli bir bağlantı sağlar. Bu tür VPN'ler, genellikle şirketler veya uzak şubeler arası güvenli veri paylaşımı gerektiğinde kullanılır(Santoso et al., 2021). Şekil 5'te Site-to-Site VPN örneği gösterilmiştir.



Şekil 6. Site-to-Site VPN örneği

Site-to-Site VPN yapısında, uzak iki ağın güvensiz bir ortamda tünel kurularak güvenli iletişim yapması sağlanır. VPN yapılandırması her iki ağın sınır cihazlarında yapılır. Bu sayede ağ içerisinde yer alan kullanıcıların herhangi bir yapılandırma yapmasına gerek kalmaz(Rathore et

al., 2009). Ayrıca çoğu durumda son kullanıcılar VPN'in varlığından haberi olmaz.

Site-to-Site VPN'in çalışma şekli aşağıda adımlar halinde verilmiştir.

• *Noktadan Noktaya Bağlantı*: Farklı konumlardaki şirket içi ağlar, internet üzerinden noktadan noktaya (site-to-site) bağlantı kurarlar. Bu bağlantılar genellikle internet bağlantıları üzerinden gerçekleştirilir.

• *Tünel Oluşturma*: Şirket içi ağlardaki VPN cihazları (genellikle VPN gateway'ler olarak adlandırılır), şifreli bir tünel oluşturur. Bu tünel, şifrelenmiş verilerin güvenli bir şekilde iletilmesini sağlar. Genellikle IPSec protokolü kullanılarak şifreleme yapılır.

• *Güvenli Veri İletimi*: Veriler, şifrelenmiş tünelden geçerek güvenli bir şekilde diğer şirket içi ağına iletilir. Bu şifreleme, verilerin güvenliği ve gizliliği için önemlidir.

• *Farklı Kaynaklara Erişim*: Bağlı şirket içi ağlar, birbirlerine ait kaynaklara (dosyalar, sunucular, yazıcılar, uygulamalar vb.) güvenli bir şekilde erişebilirler. Bu durum, farklı ofisler veya şirket içi departmanlar arasında işbirliği ve veri paylaşımını mümkün kılar(Dhall et al., 2012).

Extranet VPN: Extranet VPN'ler, farklı şirketler veya organizasyonlar arasında güvenli veri paylaşımını mümkün kılar. Extranet VPN'ler, iş ortakları veya tedarikçiler gibi harici kullanıcılarla güvenli bir şekilde bilgi paylaşımını destekler.

Intranet VPN: Intranet VPN'ler, aynı şirket veya organizasyonun farklı fiziksel konumları arasında güvenli bir ağ bağlantısı oluşturur. Bu tür VPN'ler, farklı ofisler veya departmanlar arasında güvenli veri paylaşımını sağlamak için kullanılır.

Mobile VPN: Mobile VPN'ler, hareket halindeki kullanıcılara güvenli bir şekilde bağlanma imkanı sağlar(Shneyderman & Casati, 2003). Bu tür VPN'ler, mobil cihazlar (cep telefonları, tabletler) üzerinden güvenli bir internet erişimi sağlayarak kullanıcıların güvenli bir şekilde gezinmesini sağlar.

SSL VPN (Secure Sockets Layer Virtual Private Network): SSL VPN internet üzerinden güvenli bir şekilde uzaktan erişim sağlamak için kullanılan bir VPN türüdür. SSL VPN, SSL/TLS (Secure Sockets Layer/Transport Layer Security) protokollerini kullanarak güvenli şifreleme ve kimlik doğrulama sağlar. Bu şekilde, kullanıcılar şirket içi ağa veya kaynaklara güvenli bir şekilde erişebilirler.

SSL VPN, genellikle web tarayıcıları üzerinden erişim sağlama imkânı sunar. Bu, kullanıcıların özel bir VPN istemcisi yerine sadece bir web tarayıcısı ile güvenli erişime sahip olmalarını sağlar. Kullanıcılar, güvenli bir SSL bağlantısı aracılığıyla özel şirket kaynaklarına, dosya sunucularına, veritabanlarına veya web uygulamalarına erişebilir.

SSL VPN, kullanıcıların herhangi bir yerden ve herhangi bir cihazdan (bilgisayar, tablet, cep telefonu) güvenli bir şekilde şirket içi ağlarına veya kaynaklarına erişmelerini sağlayarak mobil çalışma ve uzaktan erişim için ideal bir çözümdür.

Her bir VPN türü, farklı kullanım senaryolarına ve güvenlik gereksinimlerine uygun olarak seçilir ve yapılandırılır.

5.1. VPN'in Avantajları

VPN, internet üzerindeki veri iletimini şifreleyerek güvenli bir şekilde IP iletişimi sağlar. Bu, verilerin izinsiz erişim veya manipülasyondan korunmasını sağlanır. Ayrıca VPN, kullanıcılara ve kurumlara güvenliğin haricinde bir dizi avantaj da sunar. Bu avantajlar aşağıda özetle ifade edilmiştir.

Uzaktan Erişim: Uzaktan erişim VPN'leri, çalışanların veya uzaktan kullanıcıların şirket içi ağa

güvenli bir şekilde erişmesini sağlar. Bu, uzaktan çalışma olanaklarını artırır.

Gizlilik ve Anonimlik: VPN, kullanıcıların çevrimiçi aktivitelerini gizleyerek ve gerçek IP adreslerini gizleyerek anonim kalmasını sağlar.

Verimlilik ve Güvenlik: VPN, şirket içi çalışanlar veya uzaktan kullanıcılar için güvenli bir şekilde veri paylaşımını sağlar. Bu, işbirliğini artırır ve verimliliği destekler.

Açık WiFi Ağlarında Güvenlik: VPN, açık veya kamu WiFi ağlarında güvenli bir bağlantı sağlayarak kullanıcıları siber saldırılardan korur.

Daha Fazla Gizlilik Kontrolü: Kurumsal VPN'ler, şirket içi verilerin kontrol edilmesi ve izlenmesi için ek araçlar sağlayarak gizliliği artırır.

Maliyet Tasarrufu: VPN, özel ağ kiralama maliyetinden tasarruf sağlar. Uzaktan çalışanlar veya uzak ofisler arasındaki güvenli iletişim için ekstra maliyetli hatlar gerekmez.

Bu avantajlar, VPN'lerin kullanımını yaygınlaştırmış ve çeşitli sektörlerde güvenli iletişim ihtiyaçlarını karşılamak için önemli bir araç haline getirmiştir.

BÖLÜM ÖZETİ

Bu bölümde, VPN teknolojisinin temel prensiplerini, kriptografik algoritmaları ve çeşitli VPN türleri ele alınmıştır. VPN, internet üzerinde veri iletimini güvenli hale getirmek için kullanılan bir teknolojidir. Temel amaçlarından biri, verilerin güvenli bir şekilde iletilmesini sağlamak, gizliliği korumak, bütünlüğü doğrulamak ve kimlik doğrulamayı gerçekleştirmektir. VPN'ler, farklı kullanım senaryolarına uygun olarak farklı türlerde olabilir. Uzaktan erişim VPN'leri, uzak kullanıcıların güvenli bir şekilde şirket içi ağa veya başka bir özel ağa erişmesine olanak tanır. Site-to-Site VPN'ler, iki veya daha fazla şirket içi ağı arasında güvenli bir bağlantı sağlar. Extranet VPN'ler, farklı şirketler veya organizasyonlar arasında güvenli veri paylaşımını mümkün kılar. Intranet VPN'ler, aynı şirket veya organizasyonun farklı fiziksel konumları arasında güvenli bir ağ bağlantısı oluşturur. Mobile VPN'ler, hareket halindeki kullanıcılara güvenli bir şekilde bağlanma imkânı sağlar. SSL VPN ise internet üzerinden güvenli bir şekilde uzaktan erişim sağlamak için kullanılan bir VPN türüdür. VPN kullanmanın avantajları arasında uzaktan erişim imkânı gizlilik ve anonimlik, verimlilik ve güvenlik, açık WiFi ağlarında güvenlik, daha fazla gizlilik kontrolü ve maliyet tasarrufu yer alır. VPN, açık WiFi ağlarında güvenli bir bağlantı sağlayarak kullanıcıları siber saldırılardan korurken, aynı zamanda şirket içi verilerin güvenli bir şekilde paylaşılmasını ve iş birliğini destekler. VPN teknolojisi, günümüzde birçok organizasyon ve birey için temel bir güvenlik önlemi olarak önemli bir rol oynamaktadır.

GÖZDEN GEÇİRELİM

1. **Siber güvenliğin temel unsurları nelerdir?**
   a) Yalnızca gizlilik
   b) Bütünlük, gizlilik ve kullanılabilirlik
   c) Yalnızca bütünlük
   d) Bütünlük ve güvenilirlik

2. **VPN nedir?**
   a) Veritabanı Yönetim Sistemi
   b) Virüs Programı
   c) Sanal Özel Ağ
   d) İnternet Tarayıcısı

3. **Simetrik şifreleme ile ilgili doğru bir ifade hangisidir?**
   a) Aynı anahtar kullanılır veriyi şifrelemek ve çözmek için
   b) Farklı anahtarlar kullanılır veriyi şifrelemek ve çözmek için
   c) Açık anahtar kullanılır
   d) Şifreleme kullanılmaz

4. **SHA-2 hangi türde bir kriptografik algoritmadır?**
   a) Hash Fonksiyonu
   b) Asimetrik Şifreleme
   c) Simetrik Şifreleme
   d) Kimlik Doğrulama Protokolü

5. **IPsec'in ana bileşenleri nelerdir?**
   a) SHA ve AES
   b) AH ve ESP
   c) SSL ve TLS
   d) DNS ve DHCP

6. **Site-to-Site VPN ne tür bir VPN bağlantısını tanımlar?**
   a) Uzaktan Erişim VPN
   b) Şirket İçi VPN
   c) Farklı şirket içi ağlar arasında güvenli bağlantı
   d) Mobil VPN

7. **SSL VPN hangi protokolleri kullanarak güvenli şifreleme ve kimlik doğrulama sağlar?**
   a) IPSec
   b) SSL/TLS
   c) HMAC
   d) RSA

8. **Hangisi VPN'in avantajlarından biridir?**
   a) Maliyet artışı
   b) Kullanıcıların gerçek IP adreslerini açığa çıkarır
   c) Açık WiFi ağlarında güvenliği azaltır
   d) Uzaktan erişim ve gizlilik sağlar

9. Bütünlük algoritmaları hangi amaçla kullanılır?

a) Verileri şifrelemek
b) Verilerin bütünlüğünü sağlamak
c) Kimlik doğrulamak
d) Ağ trafiğini yönlendirmek

10. Hangisi asimetrik şifreleme algoritmalarından biri değildir?

a) RSA
b) Diffie-Hellman Anahtar Değişimi
c) AES
d) Eliptik Eğri Kriptografisi (ECC)

Yanıt Anahtarı: 1-B, 2-C, 3-A, 4-A, 5-B, 6-C, 7-B, 8-D, 9-B, 10-C

Kaynakça

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), 256–272.

Dhall, H., Dhall, D., Batra, S., & Rani, P. (2012). Implementation of IPSec protocol. *2012 Second International Conference on Advanced Computing \& Communication Technologies*, 176–181.

Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2022). Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021*, 309–319.

Ferguson, N., & Schneier, B. (1999). *A cryptographic evaluation of IPsec*.

Ferguson, P., & Huston, G. (1998). *What is a VPN?*

Gupta, P., & Kumar, S. (2014). A comparative analysis of SHA and MD5 algorithm. *Architecture*, *1*(5).

Madson, C., & Glenn, R. (1998). *The use of HMAC-MD5-96 within ESP and AH*.

Miller, V. S. (1985). Use of elliptic curves in cryptography. *Conference on the Theory and Application of Cryptographic Techniques*, 417–426.

Mouha, N., Dworkin, M., & others. (2021). Review of the advanced encryption standard. *Technical Report, National Institute of Standards and Technology*.

Muttaqin, K., & Rahmadoni, J. (2020). Analysis and design of file security system AES (advanced encryption standard) cryptography based. *Journal of Applied Engineering and Technological Science (JAETS)*, *1*(2), 113–123.

Obaid, T. S. (2020). Study a public key in RSA algorithm. *European Journal of Engineering and Technology Research*, *5*(4), 395–398.

Purohit, K., Kumar, A., Upadhyay, M., & Kumar, K. (2020). Symmetric key generation and distribution using Diffie-Hellman algorithm. In *Soft Computing: Theories and Applications: Proceedings of SoCTA 2019* (pp. 135–141). Springer.

Rathore, M. S., Razzaq, A., Hidell, M., & Sjödin, P. (2009). *Site-to-Site VPN Technologies: A Survey*.

Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN Site To Site Implementation Using Protocol L2TP And IPSec. *TEKNOKOM*, *4*(1), 30–36.

Shneyderman, A., & Casati, A. (2003). *Mobile VPN: delivering advanced services in next generation wireless systems*. John Wiley \& Sons.

Su, N., Zhang, Y., & Li, M. (2019). Research on data encryption standard based on aes algorithm in internet of things environment. *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2071–2075.

Yong-Xia, Z., & Ge, Z. (2010). MD5 research. *2010 Second International Conference on Multimedia and Information Technology*, *2*, 271–273.

Okuma Listesi

Kaya ve İ. Türkoğlu , "Simetrik ve Asimetrik Şifreleme Algoritmalarının Performans Karşılaştırılması", *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, c. 35, sayı. 2, ss. 891-900, Eyl. 2023, doi:10.35234/fumbd.1296228

Yerlikaya, T. , Gençoğlu, H. , Emir, M. K. , Çankaya, M. & Buluş, E. (2011). RSA ŞİFRELEME ALGORİTMASI VE ARİTMETİK MODÜL UYGULAMASI . İstanbul Aydın Üniversitesi Dergisi , 3 (9) , 95-104 . Retrieved from https://dergipark.org.tr/tr/pub/iaud/issue/30054/324501

Beşkirli, A. , Özdemir, D. & Beşkirli, M. (2019). Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme . Avrupa Bilim ve Teknoloji Dergisi , Özel Sayı 2019 , 284-291 . DOI: 10.31590/ejosat.638090

T. Yerlikaya ve N. İşçimen , "ASİMETRİK ŞİFRELEMEDE ASAL SAYILAR VE GÜVENLİK", Trakya Üniversitesi Mühendislik Bilimleri Dergisi, c. 24, sayı. 1, ss. 11-18, Tem. 2023, doi:10.59314/tujes.1303091

Çelik, S. (2021). Kuantum Kriptolojisi ve Siber Güvenlik . Bilişim Teknolojileri Dergisi , 14 (1) , 53-64 . DOI: 10.17671/gazibtd.733309