IPSec

IP Güvenlik Mimarisi

IPSec, IPv4 ve IPv6 için, yüksek kaliteli, kriptografi tabanlı güvenlik sağlamak üzere tasarlanmıştır. Sunulan güvenlik hizmetleri kümesi, erişim denetimi, bağlantıya yönelik olmayan doğruluk, veri kaynağı doğrulaması, tekrarlama saldırılarına karşı koruma, gizlilik *(Kriptolama)* ve sınırlı trafik akış güvenliğini içerir. Bu hizmetler IP ve üst katmanlar için yine IP katmanında sağlanır.

IPsec bir sistemin gerekli güvenlik protokollerini seçmesine, hizmetler için kullanacağı protokolleri belirlemesine ve kriptografik anahtarların konumlandırılmasına olanak tanıyarak, talep edilen hizmetlerin sunulmasını sağlar. IPSec bir çift uç arasında birden fazla yolun korunması için kullanılabileceği gibi, bu koruma iki güvenlik geçidi arasında veya bir geçit ve uç arasında da sağlanabilir. "Güvenlik Geçidi" IPSec protokolünü destekleyen firewall veya yönlendirici gibi bir ara sistemi ifade eder.

IP üzerinde güvenlik hizmetleri, Internet Güvenlik İlişkilendirmesi ve Anahtar Yönetimi Protokolü *(Internet Security Association and Key Management Protocol, ISAKMP)* ve Internet Anahtar Alış Veriş Protokolünü *(Internet Key Exchange, IKE)* içeren kriptografik anahtar yönetimi işlemleri ve protokolleri aracılığında iki güvenlik protokolü yoluyla - Doğrulama Başlığı *(Authentication Header, AH)* ve Kapsüllenmiş Güvenli Veri Yükü *(Encapsulating Security Payload, ESP)* - sağlanır.

AH başlığı, IP başlığından hemen sonra gelir ve verinin kriptografik özetini ve kimliğini içerir. AH, IP başlığının kaynak ve al›c adreslerini korur.

ESP başlığı veri yükünü kriptolanmasına olanak tanıyarak veri güvenliğini ve gizliliğini sağlar. ESP, DES, 3DES ve Blowfish gibi simetrik kriptolama algoritmaları ile çalışır. IPSec'in kullanılabilmesi için, her iki ucun aynı protokolü, kriptolama algoritmalar›n› ve anahtarlar›n›kullanmas gereklidir.

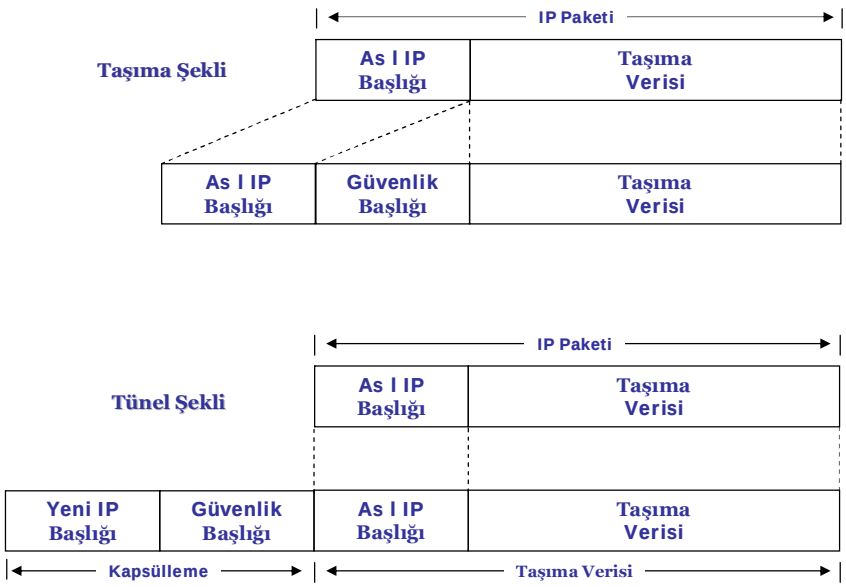
IKE, iki IPSec ucu arasında güvenlik hizmetleri konusunda, ilişkilendirilmiş oldukları oturum doğrulaması ve kripto anahtarlarında uzlaşılmasını sağlar.

Güvenlik İlişkilendirmeleri

Güvenlik İlişkilendirmesi *(Security Associattion, SA)* kavram , IP güvenlik mimarisinin temelidir. Bir SA, paketleri kimin gönderdiği, paketlerin nereye gittiği ve yük olarak ne taşındığı hakkında veri paketlerine uygulanması gereken güvenlik tedbirlerini tan›mlar. Bir SA taraf ndan sunulan güvenlik hizmetleri kümesi, güvenlik protokolüne, bu protokolün seçeneklerine ve SA'nın hangi çalışma şeklinde işletildiğine dayan›r. SA'lar için, güvenlik yöneticisi taraf›ndan verilen güvenlik politikalar na dayalı olarak, IPSec'in bir ya da daha fazla güvenlik hizmeti kullanılacağı zaman, haberleşen uçlar arasında dinamik uzlaşı gerçekleştirilebilir. Başka bir yaklaşım, nadir olarak kullan›lsa da, SA'lar statik olarak tan›mlanmas›d r.

Bir SA, üç parametre ile benzersiz olarak tan›mlan›r; bir al›c IP adresi, bir güvenlik protokolü tan›mlay›c›s ve bir Güvenlik Parametre Indeksi *(Security Parameter Index, SPI)*. Al›c› IP adresi, SA için al›c››ucun IP adresidir. SPI, genellikle SA'n n al›c› ucu taraf ndan seçilen, sadece o uçta yerel anlam› olan 32 bitlik bir say›d r. Güvenlik protokolü tan›mlay›c›s ise AH *(51)* veya ESP *(50)* için protokol numaras›d r.

Kaynak IP adresinin SA'yı tanımlamak için kullanılmadığına dikkat edilmelidir. Bu, SA'n›n, iki uç veya geçit aras nda tek bir yönde veri iletimi için yapılmış bir hizmet anlaşması olmasından kaynaklanır. Bunun sonucu olarak eğer iki uç arasında IPSec kullanılarak iki yönlü veri iletimi gerçekleştirilecekse, her biri bir yön için, iki adet SA'n›n tan›mlanmas gerekir.



Şekil 1. Taşıma ve Tünel Şekilleri

SA iki çalışma şeklinde işletilir; taşıma ve tünel çalışma şekli. Taşıma çalışma şekli birincil olarak üst katman *(TCP ve UDP gibi)* protokollerinin korunmas için tasar-

lanmıştır. Tünel çalışma şeklinde ise bir IP paketi başka bir IP paketinin taşıma verisi olmaktadır. Bu yöntemde içerdeki IP paketi, başlığı ile birlikte kriptolanmakta, dış başlık ise bu kriptolanmış paketin ağ üzerinde, yönlendirilmiş olduğu ağa ulaştırılmasını sağlamaktadır. Uçlar hem taşıma ve hem de tünel çalışma şekillerinde işletilebilirken, güvenlik geçitleri sadece tünel çalışma şeklinde yapılandırılabilirler *(Geçit uç rolünü üstlendiğinde her iki çalışma şeklini de destekleyebilir)*.

Yukarıdaki şekilde, her iki çalışma şekli için IP paket yapıları gösterilmektedir. Taşıma şeklinde asıl IP başlığı hemen hemen bozulmaz; IP taşıma verisi ve başlığı arasında bir güvenlik başlığı eklenir. Tünel çalışma şeklinde asıl IP paketi, kapsülleyen IP paketinin taşıma verisi olur; kapsülleyen IP paketi başlığı ve taşıma verisi arasına taşıma şeklinde olduğu gibi bir güvenlik başlığı eklenir.

Bir SA, AH veya ESP güvenliği sunan tek yönlü bir kanal olarak düşünülebilir. Her SA bu güvenlik yöntemlerinden sadece birini sunabileceğine dikkat edilmelidir. Eğer hem AH ve hem de ESP korumas bir veri dizisine uygulanacaksa iki SA kurulmalı ve sürdürülmelidir. Benzeri şekilde iki uç veya güvenlik geçidi arasında iki yönlü bir haberleşme kanalının güvenliği sağlanacağı zaman her biri bir yön için iki SA gereklidir.

Güvenlik Veritabanl ›

Bir IPSec ucunda iki veri taban› tutulur; Güvenlik Politikas› Veritaban *(Security Policy Database, SPD)* ve Güvenlik İlişkilendirmesi Veritabanı *(Security Association Database, SAD)*. Bir politika yöneticisi, uçtan dışarı ve içeri doğru tüm veri trafiği için güvenlik ihtiyaçlarını karşılayan bir güvenlik politikası kümesi düzenler. Bu politikalar SPD'ler içinde tutulur ve IP paketlerinin işlenmesinin yönetilmesi ve ihtiyaç duyuldukça SA'lar›n kurulmas› için kullan›l r. Tüm SA'lar SAD'lar içinde, SA'lar n parametreleri ile birlikte kaydedilir.

Güvenlik Politikas› Veritab ›

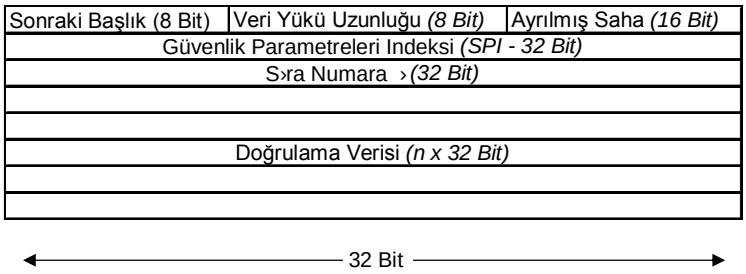
SPD, ne tür hizmetlerin sunulacağını tanımlayan politikalarla kurulur; hangi adreslere standart güvenlikte IPSec uygulanacağı, hangi adreslere yönelen trafiğin IPSec uygulanmadan geçirileceği belirlenir.

Sağlanan koruma SPD tarafından tanımlanan gereksinimlere dayanır. Bu gereksinimler kullan›c› veya bir sistem yöneticisi taraf›ndan belirlenir ve bak›m gerçekleştirilir. Genel olarak, SPD'deki girişler doğrultusunda, IP ve taşıma katmanı başlık bilgisine eşleştirilen IP paketleri üç işlem şeklinden birine göre seçilerek işlenirler. Her paket ya IPSec'e göre işlenir, göz ardı edilir veya IPSec güvenlik hizmetleri uygulanmadan geçişine izin verilir.

Güvenlik İlişkilendirmesi Veritab ›

SAD, SPD ile belirlenen her SA ile ilişkilendirilen parametreleri içerir.

Doğrulama Başlığı



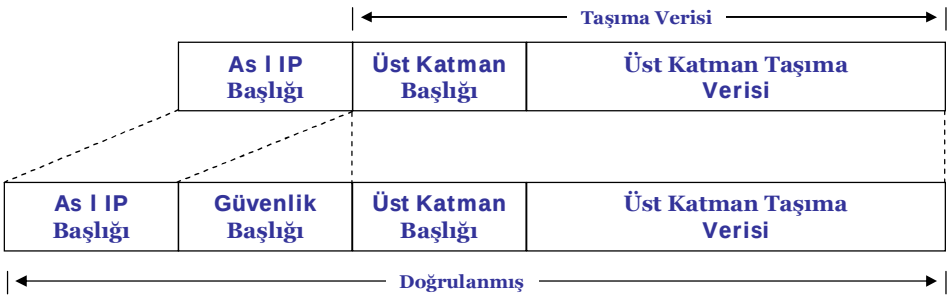
Şekil 2. Doğrulama Başlığı *(AH)* Şekli

IPSec Doğrulama Başlığı *(Authentication Header, AH)* protokolü paket başına doğrulamayı sağlamak için kullanılır. Bu IP taşıma yükü için *(Üst katman protokol başlığı ve verisi)* veri doğruluğu, veri kaynağı ve mümkün oldukça IP başlığının doğrulanmasıdır. Hangi kriptolama algoritmasının kullanıldığı ve anahtarlamanın nasıl gerçekleştirildiğine bağlı olarak AH, ayrıca hizmet kaynağının kimlik reddini engellemeyi de sağlayabilir. Son olarak AH, tekrarlama saldırılarına karşı da koruma sağlar.

Doğrulama için AH tarafından kullanılan temel yöntem doğrulama başlığıdır. Doğrulama başlığı, yeni bir IP başlığını takiben ya da asıl IP başlığı biraz değiştirilerek elde edilen başlığı takiben eklenerek yeni bir IP paketi oluşturulur. Doğrulama başlığını oluşturan altı saha yukarıdaki şekilde gösterilmektedir.

- **Sonraki Başlık:** Sekiz bitlik bu sahada, AH'den hemen sonraki protokol başlığı türü belirtilir.
- **Veri Yükü Uzunluğu:** Sekiz bitlik bu saha 32 bitlik gruplar halinde AH'nin uzunluğunu belirtir.
- **Ayrılmış Saha:** Gelecekteki kullanım için ayrılmıştır ve değeri sıfıra ayarlanmıştır.
- **Güvenlik Parametreleri İndeksi:** Al›c IP adresi ile birlikte 32 bitlik bu saha SA'y› tan›mlar. SPI, SA'n›n kurulmas ›üzerine belirlenen rasgele bir say d r. S - f r değeri SA'nın henüz kurulmadığını belirtirken, 1-255 değerleri gelecekteki kullanımlar için ayrılmıştır.
- **S›ra Numaras :** 32 bitlik bu saha, paketin dizideki konumunu belirtir. SA kurulduğunda saha değeri sıfıra ayarlanır ve paketler gönderildikçe birer birer art - rılır. Eğer tekrarlama saldırısı koruması etkin ise, bu değerin döngüye girmesine izin verilmez. Tüm sıra numarası değerleri kullanıldığında, yeni bir SA ve dolay›s›yla bir anahtar kullan lmal d r.
- **Doğrulama Verisi:** Bu saha, karşılık gelen SA'da belirtilen doğrulama algoritması ve kripto anahtarı kullanılarak üretilmiş Doğruluk Kontrolü Değerini *(Integrity Check Value, ICV)* içerir. Bu sahasının uzunluğu sabit değildir ve kullanılan algoritma tanımına bağlıdır. Gönderen taraf bu veriyi IP paketini gön-

dermeden önce hesaplar, alıcı da alımı gerçekleştirdikten sonra doğrulamasını sağlar.

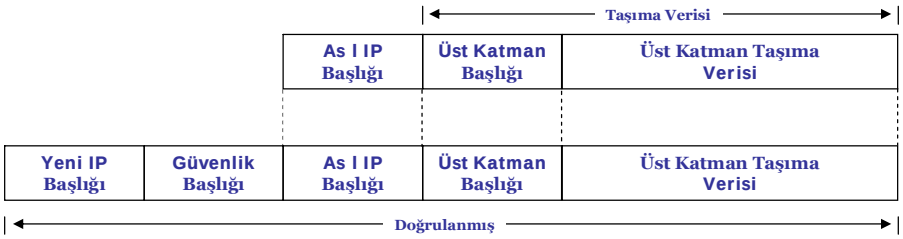


Şekil 3. AH Taşıma Şekli

Taşıma Şekli

Taşıma şeklinde, yukarıdaki şekilde gösterildiği gibi, asıl IP başlığı yeni IP paketinin başlığı olarak muhafaza edilir ve IP başlığı ile asıl taşıma verisi arasına doğrulama başlığı eklenir.

Taşıma şeklinde, asıl IP paketine çok az miktarda eklenti yapıldığından bir avantaj mevcuttur. Ancak yeni IP paketinin başlığı olarak asıl IP başlığı kullanıldığından yalnızca son uçlar AH taşıma şeklini kullanabilirler. Bu sınırlama eğer karşılık lı IPSec uçları başka cihazların yerine işlem görüyorsa kabul edilebilir. Başka bir problemde, içeriğin korunması için tedbirler alınsa da, ağ üzerinde bir gözlemci, paket say›s›ndan ve türünden bir tak m bilgiler edinebilir.



Şekil 4. AH Tünel Şekli

Tünel Şekli

Tünel şeklinde, yukarıdaki şekilde gösterildiği gibi yeni IP paketi için yeni bir IP başlığı oluşturulur, asıl ve yeni IP başlığı arasına doğrulama başlığı eklenir. Asıl IP paketi değişmeden muhafaza edilir, yani IP paketi ile kapsüllenir. Bu yolla doğrulama, doğrulama başlığı ve yeni IP başlığının değiştirilemez sahalar dahil olmak üzere tüm asıl IP paketi üzerinde gerçekleştirilmiş olur. Ancak bu ek başlık bilgilerinin eklenmesi ve ayıklanması için daha fazla işlem gücü gerekir. Asıl IP paketi değiştirilmeden tutulur ve son al›c ile kaynak adresini içerir. Yeni IP paket başlığının kay-

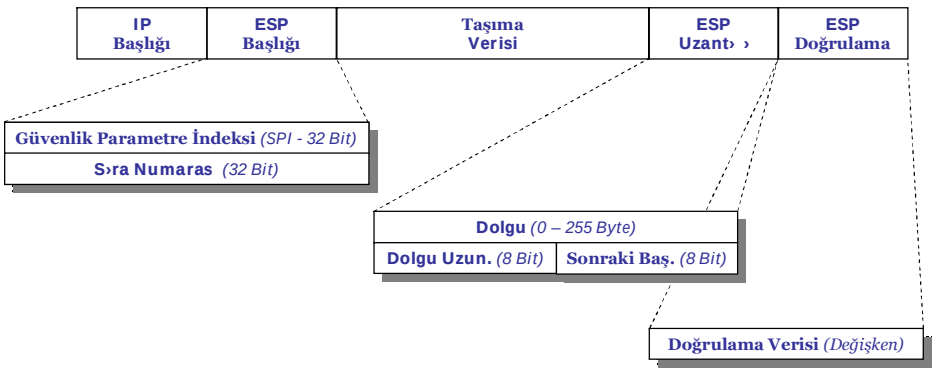
nak ve alıcı adresleri, yeni paketin yol alacağı iki IPSec ucunun adresleri olacaktır. Sonuç olarak tünel şekli SA'nın son uçları veya güvenlik geçitleri arasında kullan - labilir. Eğer SA uçlar arasında ise, yeni paketin alıcı ve kaynak adresleri genellikle aynı kalır. AH'nin uçlar arasında tünel şeklinde kullanılmasının tipik sebebi asıl paketin tamamen doğrulanması ihtiyacıdır.

Eğer SA güvenlik geçitleri arasında ise kaynak ve alıcı adresleri, güvenlik geçitlerinin IP adresleri, yeni IP paketinde al›c› ve kaynak adresleri olarak kullan›lacakt r. Tünel şekli ağlar arasında, doğrulanmış tüneller aracılığı ile trafik konsolidasyonu sağlamaktadır. Ayrıca asıl IP paketleri yeni IP paketlerinin veri yükü olarak gömüldüğünden ve ağlar arasında farklı trafikler birbirleri ile çoğullandığından trafik analizi güçleştirilmektedir.

AH algoritması bağımsız olduğundan ihtiyaç duyulan güvenlik seviyesine göre bir algoritmanın işletilmesi mümkündür. Şu anda seçenekler arasında HMAC *(Hash'lenmiş Mesaj Doğrulama Kodu)*, MD5 veya HMAC SHA-1 bulunmaktad r. Seçime bağlı olarak, seçilmişse, AH, alıcı sıra numaralarını kontrol ettiğinden, tekrarlama sald›r›lar na *(Man-in-the-middle)* karşı korumsa sağlar. AH, alıcı adresi istisnası dışında, üst katman verisi dahil olmak üzere paketin tümünü doğrular. AH yalnız başına kullanılabileceği gibi, daha üst seviye bir güvenlik sağlanması için ESP ile birlikte de kullan labilir.

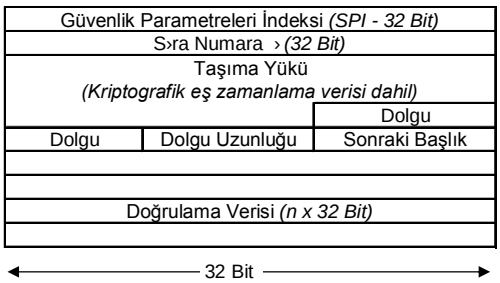
Kapsülleyen Güvenlik Veri Yükü (ESP)

IPSec ESP protokolü IP paketleri için, doğrulama, kriptolama ile veri gizliliği ve seçime bağlı olarak tekrarlama saldırılarına karşı koruma sağlar.



Şekil 5. ESP başlığı, uzantısı ve doğrulama başlığı şekilleri

AH'de olduğu gibi, bu hizmetlerin sunulması için IP paketinin içine ek sahalar eklenir ve bu sahalar AH'dekilerle ayn anlama sahiptirler. Ancak AH'nin aksine bu sahalar IP paketi boyunca dağıtılırlar. Bunlardan bir kısmı, yukarıdaki şekilde gösterildiği gibi, ESP başlığını, bir kısmı ESP uzantısı, geri kalanı ise ESP doğrulama segmenini oluştururlar.

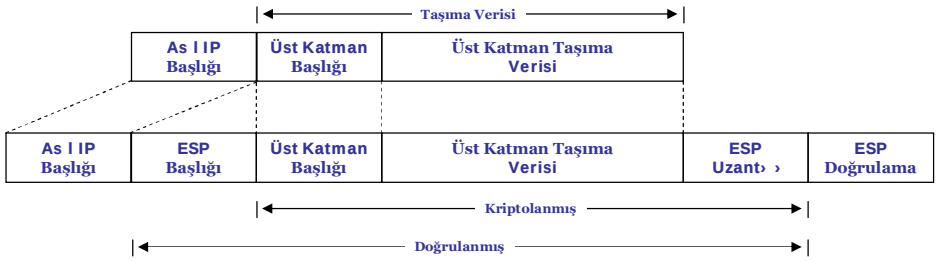


Şekil 6. ESP Şekli

ESP başlığı, çalışma şekline bağlı olarak, yeni bir IP veya biraz değiştirilmiş asıl IP paket başlığını takip eder. ESP uzantısı asıl IP paketinin sonunda yer alır ve onu ESP doğrulama segmeni takip eder. Eğer doğrulama uygulanmamışsa, ESP doğrulama segmeni eklenmez. Eğer kriptolama uygulanmışsa ESP başlığının sonunda, ESP uzantısının sonuna kadar olan bölüm kriptolanır.

ESP şekli, şekil 31.11'de gösterilmektedir. ESP başlığı, uzantısı ve doğrulama segmenindeki sahalar AH'dekine benzerdir. Aslında SPI, sıra numarası, sonraki başlık ve doğrulama verisi AH protokolünde tanımlandığı gibidir. Ek sahalar aşağıda açıklanmaktadır:

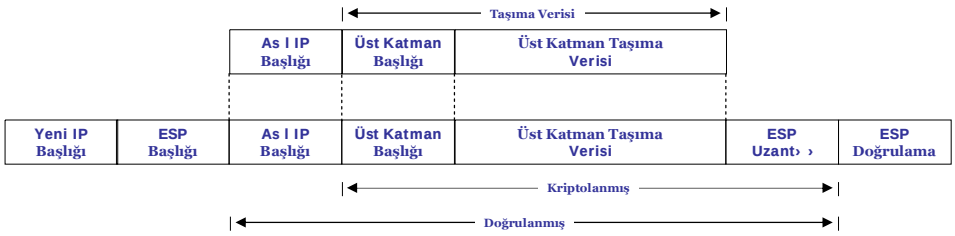
- **Taşıma Yükü:** Bu saha paket tarafından taşınan asıl veridir ve türü Sonraki Başlık sahasında belirtilir. Kriptolama algoritması tarafından ihtiyaç duyulan herhangi bir kripto eşzamanlama verisi, örneğin Başlangıç Vektörü *(Initialization Vector, IV)*, bu sahada taşınabilir. Bir kriptolama algoritması böyle bir belirtmeye ihtiyaç duyuyorsa, paket başına eşzamanlama verisi, bu veri için, uzunluk, yapı ve konumu belirtmelidir.
- **Dolgu:** Dolgu sahası 0-255 arasında rasgele olarak üretilmiş veriyi içerir ve birçok amaç için kullanılabilir:
    - Bazı kripto algoritmaları, kriptolanacak verinin belirli sayıda Byte'ın katı olmasını gerektirir; bu durumda *(Veri yükü ve Sonraki Başlık sahası dahil)* kriptolanacak bloğun algoritmanın gerektirdiği uzunluğu getirilmesi için bu saha kullanılır.
    - Dolgu, kullanılan algoritmadan ilgisiz olmak üzere, ESP paket şeklinin gerektirdiği gibi, kriptolanmış veri yükünün 32 bitlik sınırda sonlandırılması için gerekebilir.
    - Kısmi trafik akışı güvenliği sağlamak amacı ile, veri yükünün asıl uzunluğunu saklamak için de dolgu kullanılabilir.
- **Dolgu Uzunluğu:** Bu saha, kendinden hemen önce gelen dolgu Byte' sayısını belirtir. Geçerli değerler 0-255 arasındadır ve sıfır değeri dolgu Byte'ı kullanılmadığını gösterir. Bu saha zorunlu olarak bulunması gereken bir sahadır.



Şekil 7. ESP Taşıma Şekli

Taşıma Şekli

Yukarıdaki şekilde, IP başlığı ve veri yükü arasına ESP başlığı ve paket sonuna, gerekli ise, ESP uzantısı ile ESP doğrulama segmeninin eklenmesiyle, asıl IP paketinden yeni IP paketinin nasıl inşa edildiği gösterilmektedir. Eğer asıl IP paketi IPSec güvenlik başlıklarına sahip ise, yeni ESP başlığı bunlardan önce konumlandırılır. Çünkü, asıl IP başlığı kullanıldığından, IP paketinin kaynak ve alıcı adresleri değiştirilemez. Bu yüzden, ESP taşıma şekli, AH taşıma şeklinde olduğu gibi, sadece uçlar aras›nda kullan labilir.



Şekil 8. ESP Tünel Şekli

Tünel Şekli

Tünel şeklinde tüm asıl IP paketi yeni bir IP paketi içinde kapsüllenir. Yukarıdaki şekilde yeni IP ve ESP başlığının asıl paket başına, ESP uzantısı ve doğrulama segmeninin ise paket sonuna nasıl eklendiği gösterilmektedir. Eğer tünel uçlar arasında ise, kaynak ve alıcı adresleri, asıl IP paketindekilerle aynı olabilir. Eğer tünel iki güvenlik geçidi arasında ise, yeni IP başlığındaki adresler, geçit adreslerini yans - tacaktır. ESP'nin tünel şeklinde çalıştırılması, iki geçit arasındaki geçiş trafiğinin hem güvenliğini ve hem de doğrulamasını sağlayacaktır.

ESP ayrıca kullanılacak kriptolama algoritmasından bağımsız çalışacak şekilde tasarlanmıştır; seçenekler arasında DES, 3DES, RC5, Blowfish, Idea ve Cast bulunmaktad r ve yenileri de eklenmektedir.

Tablo 1. AH ve ESP başlıkları tarafından sunulan güvenlik hizmetlerinin karşılaştırılması

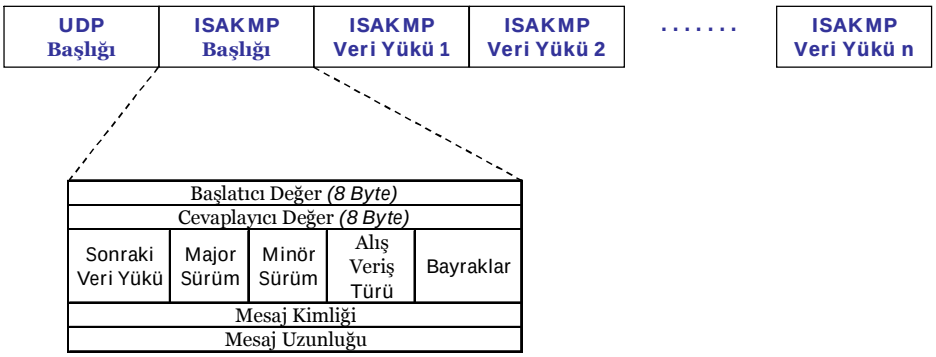
	Veri Kaynağı Doğrulaması	Veri Doğruluğu	Tekrarlama Saldırısı Korum	Veri Güvenliği
AH	Evet	Evet	Evet	Hayır
ESP	Evet	Evet	Evet	Evet

Internet Anahtar Alış Verişi (Internet Key Exchange, IKE)

IPSec AH ve ESP protokolleri, IPSec cihazları arasında uzlaşılan SA'lar üzerine veri güvenliği hizmetlerinin nasıl verileceğini tanımlamalarına rağmen, aslında bu SA'lar üzerinde nasıl bir şekilde uzlaşılacağını açıklamazlar. SA'lar sistem yöneticileri tarafından elle yapılandırılacaklar gibi, IKE gibi bir anahtar yönetimi protokolü ile de dinamik olarak uzlaşı sağlanabilir. IKE, Internet Güvenliği İlişkilendirmesi ve Anahtar Yönetimi Protokolü *(Internet Security Association and Key Management Protocol, ISAKMP)* tarafından belirlenen bir taslak yapıya dayanır. IKE, kendi iki yöntemi ile birlikte, Oakley ve SKEME'nin *(Güvenli Anahtar Alış Veriş Mekanizmas , Secure Key Exchange Mechanism)* bazı bölümlerini kullanır.

ISAKMP

ISAKMP, haberleşilen bir ucun doğrulanması, SA'lar oluşturulması ve yönetilmesi, anahtar oluşturma teknikleri ve tehdit *(DoS ve tekrarlama saldırıları gibi)* riskinin azaltılması ile ilgili işlevleri tanımlar. Tüm bunlar Internet ortamında güvenli bir haberleşmenin kurulması *(IPSec veya başka bir güvenlik protokolü ile)* ve sürdürülmesi için gereklidir. Bu işlemler herhangi belirli bir algoritma, anahtar üretim yöntemi ve güvenlik protokolü ile bağdaştırılmamıştır.



Şekil 9. ISAKMP Mesaj Şekli

Bir ISAKMP mesajı, bir UDP paketinin içinde *(Port 500)* bir ISAKMP başlığı ve bir ya da birbirine bağlı birkaç ISAKMP veri yükünden oluşur. Bu yapı yukarıdaki şekilde gösterilmektedir. Başlatıcı Değer *(Initiator Cookie)* ve Cevaplayıcı Değer *(Responder Cookie)*, ISAKMP işlemcisini tıkayarak bir DoS saldırısı gerçekleştirilmesini engellemek için ISAKMP tarafından üretilen özel değerlerdir. Bu değerler

geçersiz mesajların göz ardı edilmesi ile koruma sağlarlar. Bu iki değer ayrıca iki ISAKMP ucu arasında güvenlik ilişkilendirmesini belirtmek için de, uzlaşı başarı ile tamamland›ktan sonra, kullan›lmaktad r.

ISAKMP, SA uzlaşısında iki aşama tanımlar. İlk aşamada iki ISAKMP ucu arasında uzlaşı gerçekleştirilir. Bu aşamada, uçlar arasında daha sonra yapılacak haberleşmenin nasıl güvenlik altına alınacağı konusunda anlaşılarak, bir ISAKMP güvenlik ilişkilendirmesi kurulur. Bir ISAKMP SA'sı, IPSec SA'sı ile karıştırılmamalıdır. Bir ISAKMP SA'sı iki yönlüdür ve IPSec trafiğine uygulanmaz. İkinci aşamada diğer güvenlik protokolleri *(Örneğin IPSec; ancak teorik olarak ISAKMP diğer güvenlik protokolleri için de kullan labilir)* için SA'lar, ISAKMP uçları arasında uzlaşı gerçekleştirilir. Uzlaşan taraflar arasındaki haberleşme kanalı hali hazırda güvenlik alt - na alındığından diğer uzlaşı adımları daha hızlı geçilebilir.

Oakley

Oakley Diffie-Hellman anahtar alış veriş yöntemini kullanan bir anahtar belirleme protokolüdür. Oakley, PFS'yi destekler *(Perfect Forward Secrecy)*; bir haberleşmeyi koruyan bir anahtar veya daha önce anahtar üretmek için kullanılmış materyal başka anahtarlar›n hesaplanmas› için kullan lmaz.

Diffie-Hellman (DH) Tekniği

Diffie-Hellman tekniği *(İsmini mucitleri Whitfield Diffie ve Martin Hellman'dan almaktad r)* haberleşen iki tarafın paylaşılan bir anahtar üzerinde anlaşmasına olanak tan›yan, bir kamusal kriptolama algoritmas›d›r. DH iki taraf aras nda kamusal bilgi alış verişi ile başlar. Her uç kendi gizli bilgisi ve karşı tarafın kamusal bilgisini birleştirerek paylaşılmış gizli bir değer üretir.

SKEME

SKEME, birçok güvenlik modelini destekleyen oldukça taşınabilir bir protokoldür. SKEME, gereksiz sistem karmaşıklığına yol açmadan güvenlik ve performans ölçütlerinde birçok seçenek sunar. Söz konusu protokol, kamusal anahtar tabanl anahtar alış verişi, anahtar dağıtım merkezleri veya elle kurulumu destekler ve hızlı ve güvenli anahtar yenilemesini sağlar. SKEME ayrıca seçime bağlı olarak etkin kriptografik parametrelerin uzlaşılması, değiştirilebilmesi için PFS'i desteklediği gibi anonimlik ve kimlik reddi gibi konularda da bir araç olarak kullan labilir. IKE protokolleri, iki aşamadan birinde çalışan değişik alış veriş yöntemleri sunarlar. Birinci aşamada ISAKMP SA kurulur ve paylaşılmış gizli anahtarlar türetilir. İkinci aşamada IPSec ve diğer güvenlik protokollerine ilişkin güvenlik hizmetlerinde uzlaşı gerçekleştirilir ve taze anahtarlama materyali oluşturulur. Üç temel çalışma şekli bulunmaktadır: Birinci aşamada ana ve etkin, ikinci aşamada ise hızlı çalışma şekli.

- **Ana çalışma şekli**, iki IPSec ucu arasında, uçların doğrulanması ve anahtarlama materyali uzlaşısının tamamlanması için altı farklı mesajın alış verişini kullanır. Bu uzlaşı gerekli ise PFS'i sağlayacak ve ilk iki mesajın alış verişinden sonra takiben haberleşme koruma alt›na al›nacakt r.

- **Etkin çalışma şekli**, yalnızca üç mesajla uçları doğrular fakat PFS sağlamaz. Ayrıca SA uzlaşısı etkin çalışma şeklinde sınırlandırılmıştır.
- **Hızlı çalışma şekli**, tünel kurulduktan sonra kriptolama amaçl taze anahtarlama materyalinin üretilmesi için kullanılır; uçları doğrulamaz. Takiben haberleşme verisinin kriptolanmas› için yeni anahtar verisi kullan›l r.