



# IP Güvenliđi

**Dr. Fatih KALEMKUŞ**

*Kafkas Üniversitesi*



# Giriş

- IP GÜVENLİĞİNE GENEL BAKIŞ
- IP GÜVENLİK MİMARİSİ
- KİMLİK DOĞRULAMA BAŞLIĞI
- GÜVENLİK YÜKÜNÜ SARMA
- GÜVENLİK İLİŞKİLENDİRMELERİNİ BİRLEŞTİRME
- ANAHTAR YÖNETİMİ

*Dr. Fatih KALEMKUŞ*



# IP Güvenliğine Genel Bakış

Standart İnternet iletişim protokolü tamamen korunmasızdır ve ana bilgisayarların iletimdeki veriyi incelemesine veya değiştirmesine olanak tanır. Sisteme IPsec eklemek, güçlü şifreleme, bütünlük, kimlik doğrulama ve tekrar oynatma koruması sağlayarak bu sınırlamayı çözecektir.

*Dr. Fatih KALEMKUŞ*



# Hangi Güvenlik Sorunu?

Günümüz İnterneti öncelikli olarak şunlardan oluşur:

- Genel
- Güvenilmeyen
- Güvenilmez IP ağları

Bu doğal güvenlik eksikliği nedeniyle, İnternet çeşitli tehdit türlerine maruz kalmaktadır...

*Dr. Fatih KALEMKUŞ*



# İnternet Tehditleri

- Veri bütünlüğü Bir paketin içeriği kazara veya bilerek değiştirilebilir.
- Kimlik sahtekarlığı (Identity spoofing) Bir IP paketinin kökeni taklit edilebilir.
- Tekrar saldırılarına karşı koruma (Anti-reply attacks) Yetkisiz veriler yeniden iletilebilir.
- Gizlilik kaybı Bir paketin içeriği aktarım sırasında incelenebilir.

*Dr. Fatih KALEMKUŞ*



# Hangi Seviyede Güvenlik?

- Application Layer: Uygulama Katmanı
  - Transport Layer: Taşıma Katmanı
  - Network Layer: Ağ Katmanı
  - Data Link Layer: Veri Bağlantı Katmanı
- PGP, Kerberos, SSH, etc. : PGP, Kerberos, SSH, vb.
  - Transport Layer Security (TLS): Taşıma Katmanı Güvenliği (TLS)
  - IP Security: IP Güvenliği
  - Hardware encryption: Donanım şifreleme

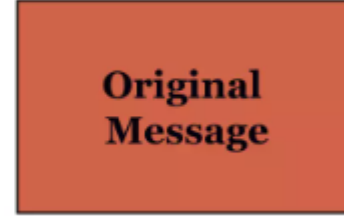
*Dr. Fatih KALEMKUŞ*



# Hangi Seviyede Güvenlik?

Encapsulation of Data for Network Delivery: Ağ Teslimi İçin Veri Kapsüllemesi

Application Layer



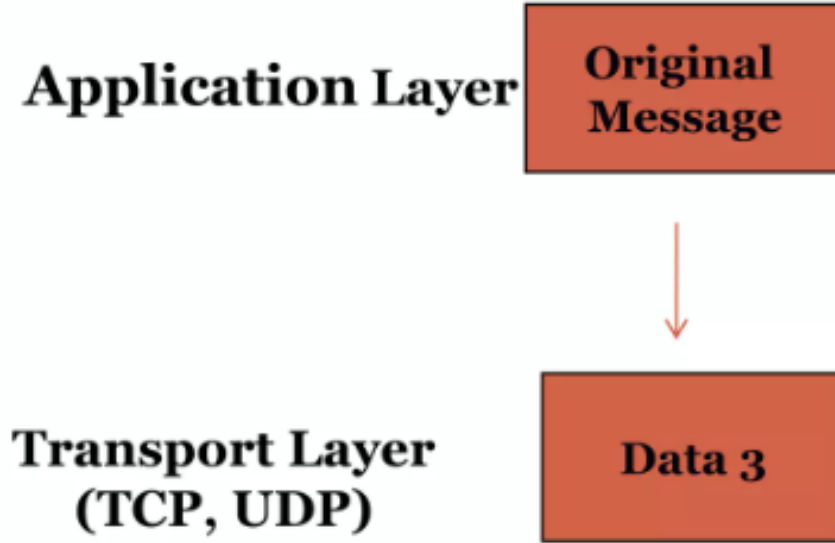
Application Layer: Uygulama Katmanı

Original Message: Orijinal Mesaj

*Dr. Fatih KALEMKUŞ*

# Hangi Seviyede Güvenlik?

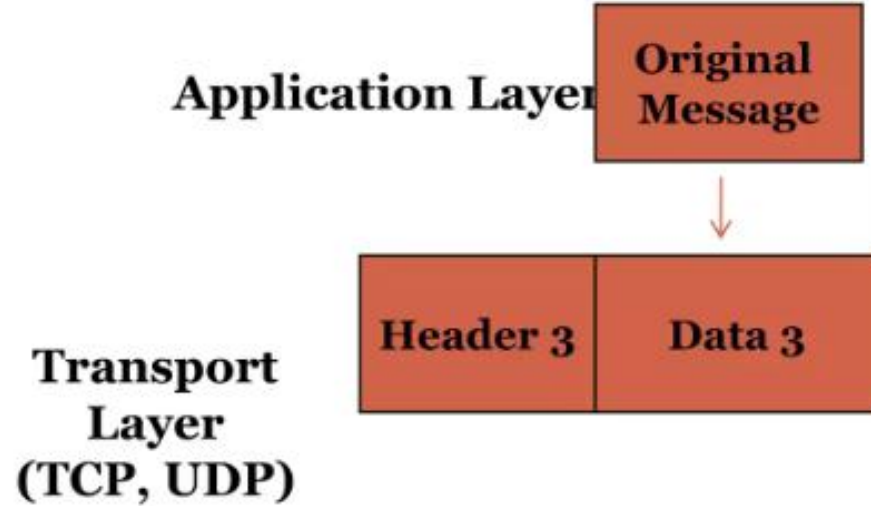
Encapsulation of Data for Network Delivery: Ağ Teslimi İçin Veri Kapsüllemesi



- Application Layer: Uygulama Katmanı
- Transport Layer: Taşıma Katmanı

# Hangi Seviyede Güvenlik?

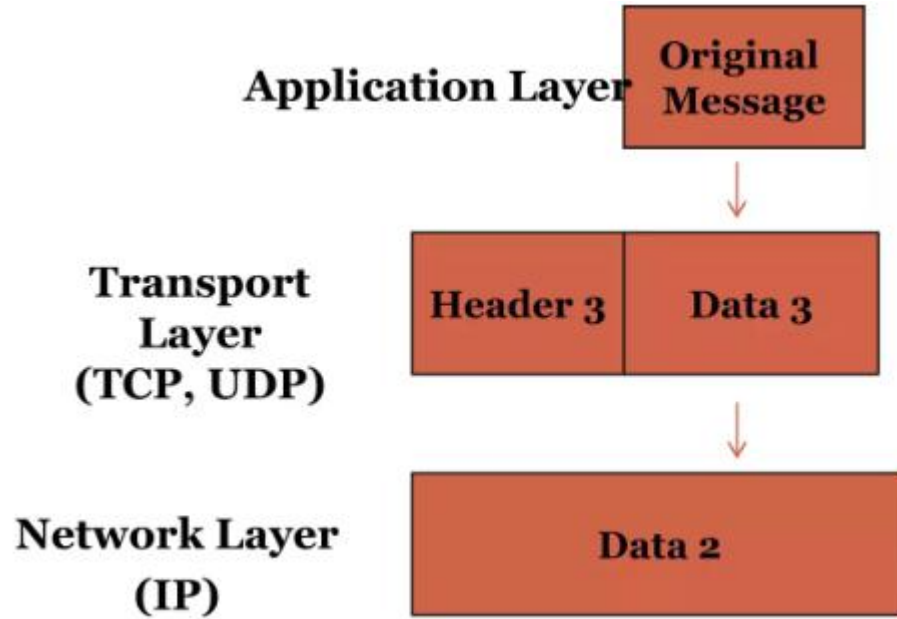
Encapsulation of Data for Network Delivery: Ağ Teslimi İçin Veri Kapsüllemesi



- Application Layer: Uygulama Katmanı
- Transport Layer: Taşıma Katmanı

# Hangi Seviyede Güvenlik?

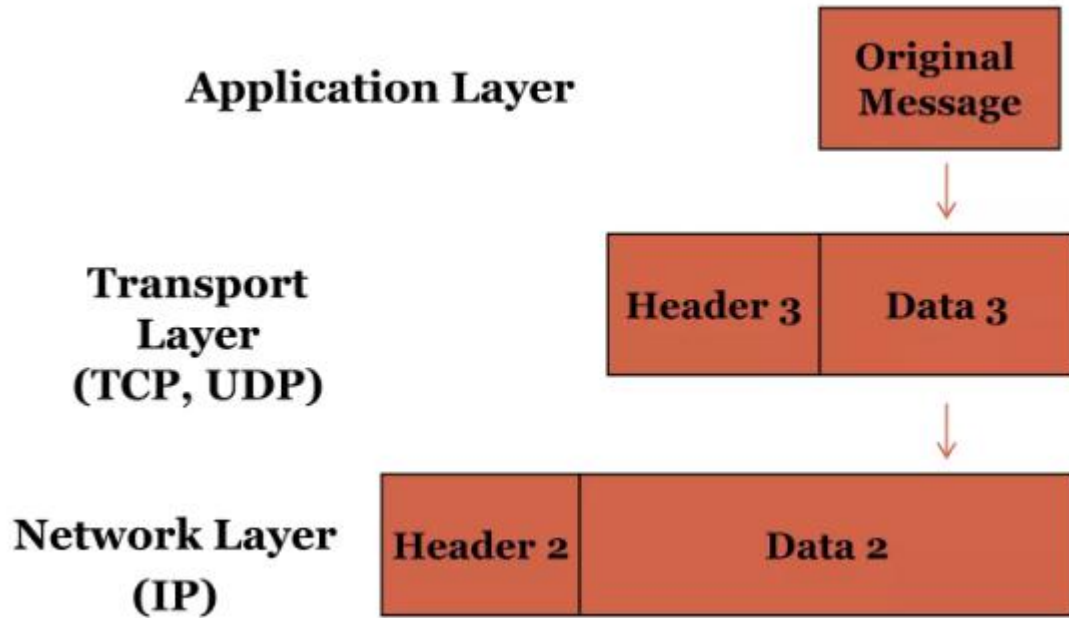
Encapsulation of Data for Network Delivery: Ağ Teslimi İçin Veri Kapsüllemesi



- Application Layer: Uygulama Katmanı
- Transport Layer: Taşıma Katmanı
- Network Layer (IP): Ağ Katmanı (IP)

# Hangi Seviyede Güvenlik?

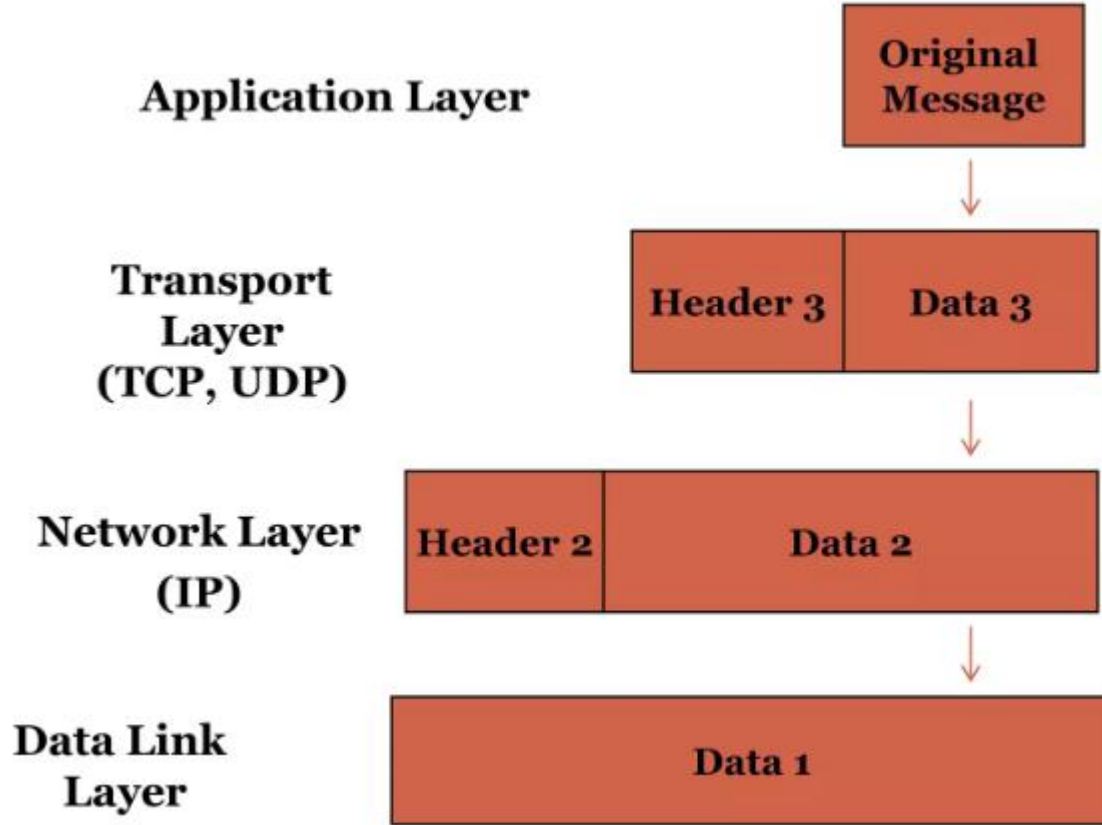
Encapsulation of Data for Network Delivery: Ağ Teslimi İçin Veri Kapsüllemesi



- Application Layer: Uygulama Katmanı
- Transport Layer: Taşıma Katmanı
- Network Layer (IP): Ağ Katmanı (IP)

# Hangi Seviyede Güvenlik?

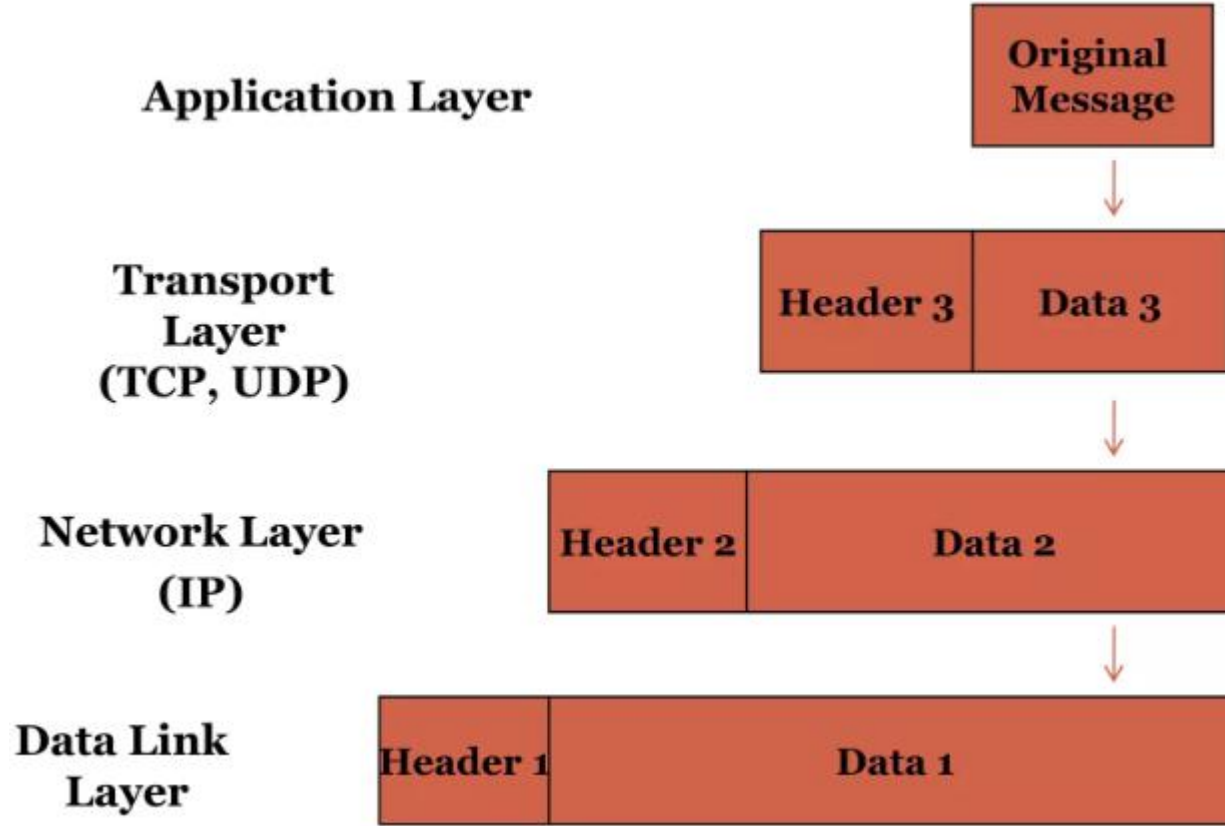
Encapsulation of Data for Network Delivery: Ağ Teslimi İçin Veri Kapsüllemesi



- Application Layer: Uygulama Katmanı
- Transport Layer: Taşıma Katmanı
- Network Layer (IP): Ağ Katmanı (IP)
- Data Link Layer: Veri Bağlantı Katmanı

# Hangi Seviyede Güvenlik?

Encapsulation of Data for Network Delivery: Ağ Teslimi İçin Veri Kapsüllemesi



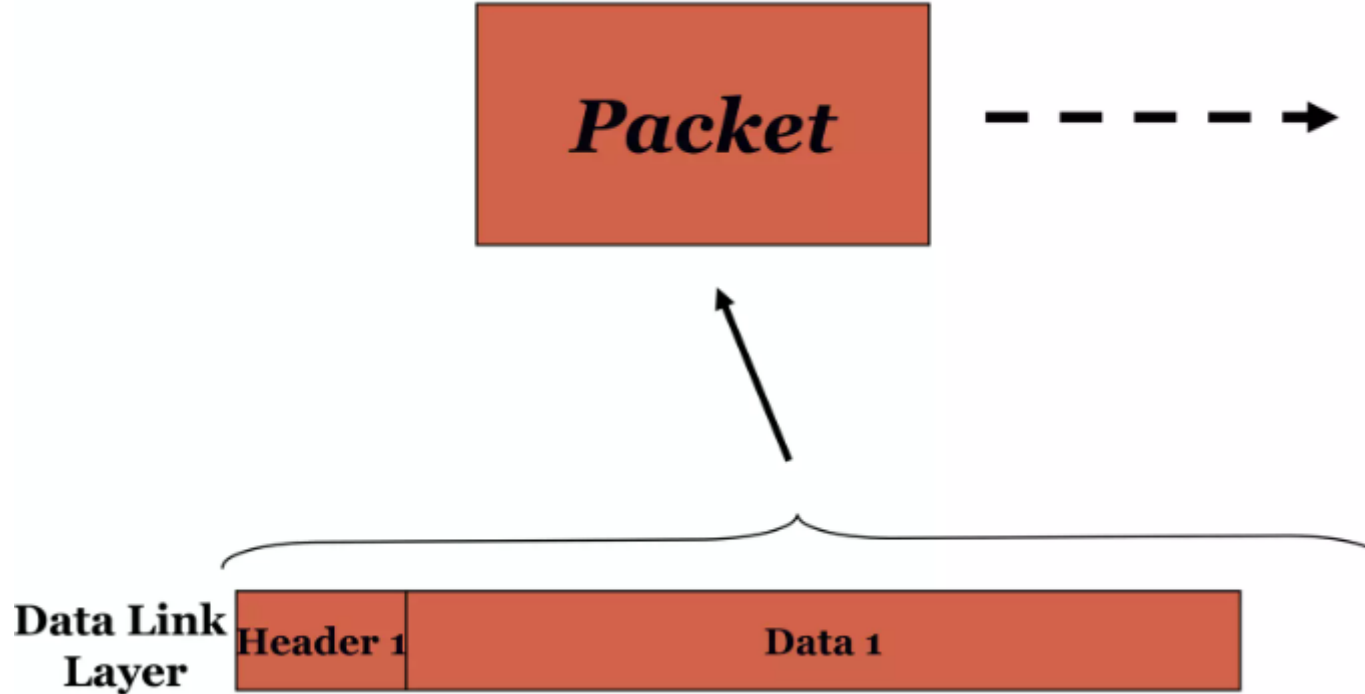
- Application Layer: Uygulama Katmanı
- Transport Layer: Taşıma Katmanı
- Network Layer (IP): Ağ Katmanı (IP)
- Data Link Layer: Veri Bağlantı Katmanı

*Dr. Fatih KALEMKUŞ*

# Hangi Seviyede Güvenlik?

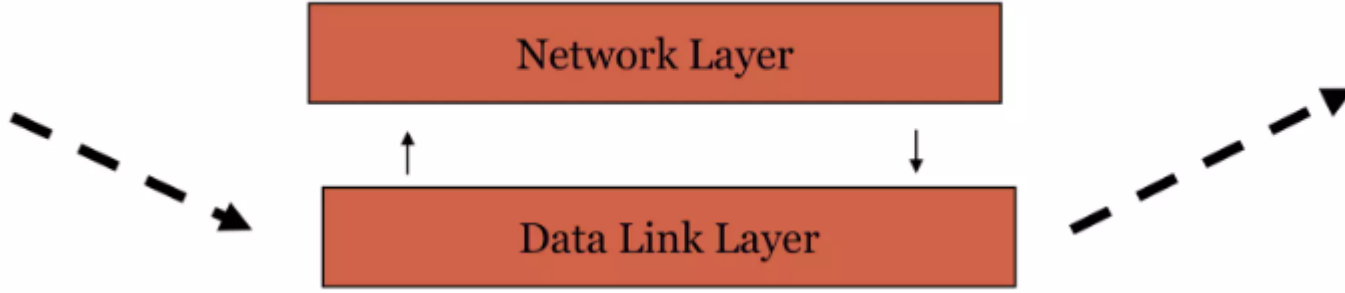
"A Ana Bilgisayarı Tarafından Gönderilen Paket"

- Data Link Layer: Veri Bağlantı Katmanı



*Dr. Fatik KALEMKUŞ*

# Router (Ara Yönlendirici) Tarafından Alınan Paket



- Network Layer (IP): Ağ Katmanı (IP)
- Data Link Layer: Veri Bağlantı Katmanı



# Ağ Tesliminden Verinin Çözümlemesi

- Data Link Layer: Veri Bağlantı Katmanı



*Dr. Fatih KALEMKUŞ*



# Ağ Tesliminden Verinin Çözümlemesi

- Data Link Layer: Veri Bağlantı Katmanı

**Data Link  
Layer**

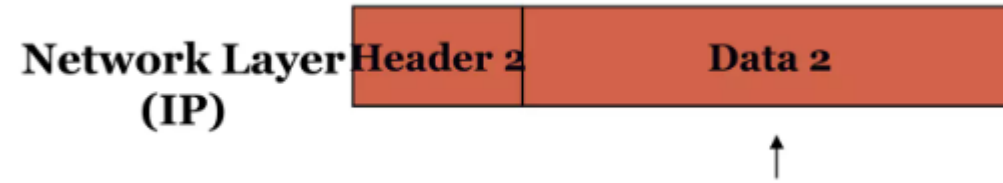


*Dr. Fatih KALEMKUŞ*



# Ağ Tesliminden Verinin Çözülmesi

- Network Layer (IP): Ağ Katmanı (IP)



*Dr. Fatih KALEMKUŞ*



# Ağ Tesliminden Verinin Çözümlemesi

- Network Layer (IP): Ağ Katmanı (IP)

**Network Layer  
(IP)**



*Dr. Fatih KALEMKUŞ*



# Ağ Tesliminden Verinin Çözülmesi

- Transport Layer: Taşıma Katmanı



*Dr. Fatih KALEMKUŞ*



# Ağ Tesliminden Verinin Çözümlemesi

- Transport Layer: Taşıma Katmanı

**Transport Layer  
(TCP, UDP)**

**Data 3**

*Dr. Fatih KALEMKUŞ*



# Ağ Tesliminden Verinin Çözülmesi

- Application Layer: Uygulama Katmanı



*Dr. Fatih KALEMKUŞ*



# IP Güvenliđi

IP düzeyi güvenliđi üç işlevsel alanı kapsar:

- Kimlik Doğrulama
- Gizlilik
- Anahtar yönetimi

*Dr. Fatih KALEMKUŞ*

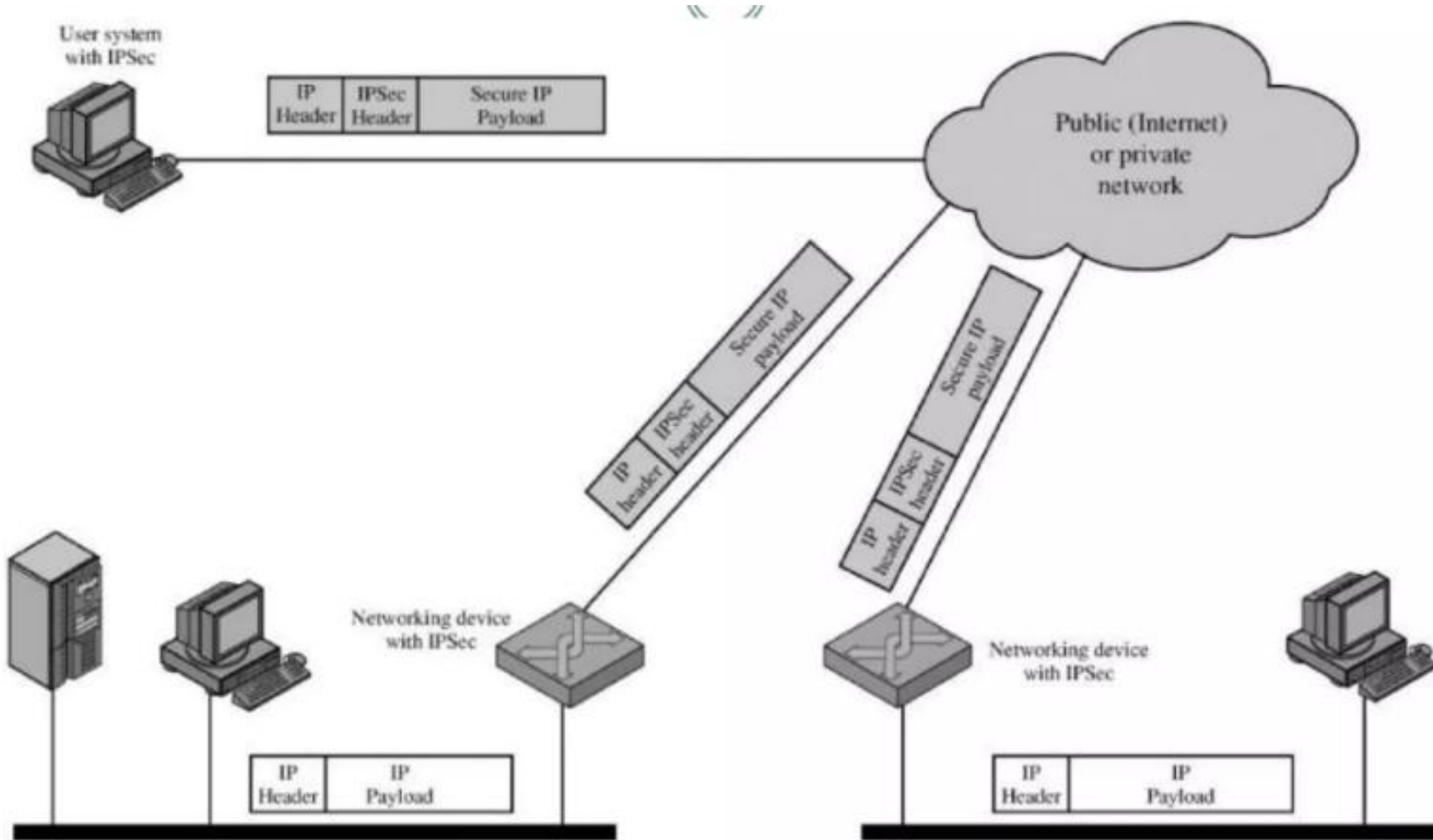


# IP Güvenliđi

- **Kimlik Doğrulama:** Kimlik doğrulama mekanizması, alınan paketin tanımlanmış kaynak tarafından gönderildiđini garanti eder. Ayrıca, paketin iletim sırasında deđiştirilmediđinden emin olur.
- **Gizlilik:** Gizlilik özelliđi, iletişim kuran düđümlerin mesajları şifrelemesini sağlayarak üçüncü tarafların gizlice dinlemesini engeller.
- **Anahtar Yönetimi:** Anahtarların güvenli bir şekilde deđişimini ele alır.

*Dr. Fatih KALEMKUŞ*

# IP Güvenlik Senaryosu





# IP Güvenlik Uygulamaları

- İnternet üzerinden güvenli şube ofisi bağlantısı.
- İnternet üzerinden güvenli uzaktan erişim.
- İş ortaklarıyla extranet ve intranet bağlantısı kurma.
- Elektronik ticaret güvenliğini artırma.

*Dr. Fatih KALEMKUŞ*



# IPSec'in Faydaları

- Sınırı geçen tüm trafiğe uygulanabilecek bir güvenlik duvarı veya yönlendiricide uygulandığında güçlü güvenlik sağlar.
- Dışarıdan gelen tüm trafik IP kullanmak zorundaysa ve güvenlik duvarı İnternet'ten kuruluşa tek giriş yoluysa, IPsec atlatmaya karşı dayanıklıdır.
- Ulaştırma katmanının altında olduğundan, uygulamalara karşı şeffaftır.
- Son kullanıcılara karşı şeffaf olabilir.
- Gerekirse bireysel kullanıcılar için güvenlik sağlayabilir.

*Dr. Fatih KALEMKUŞ*

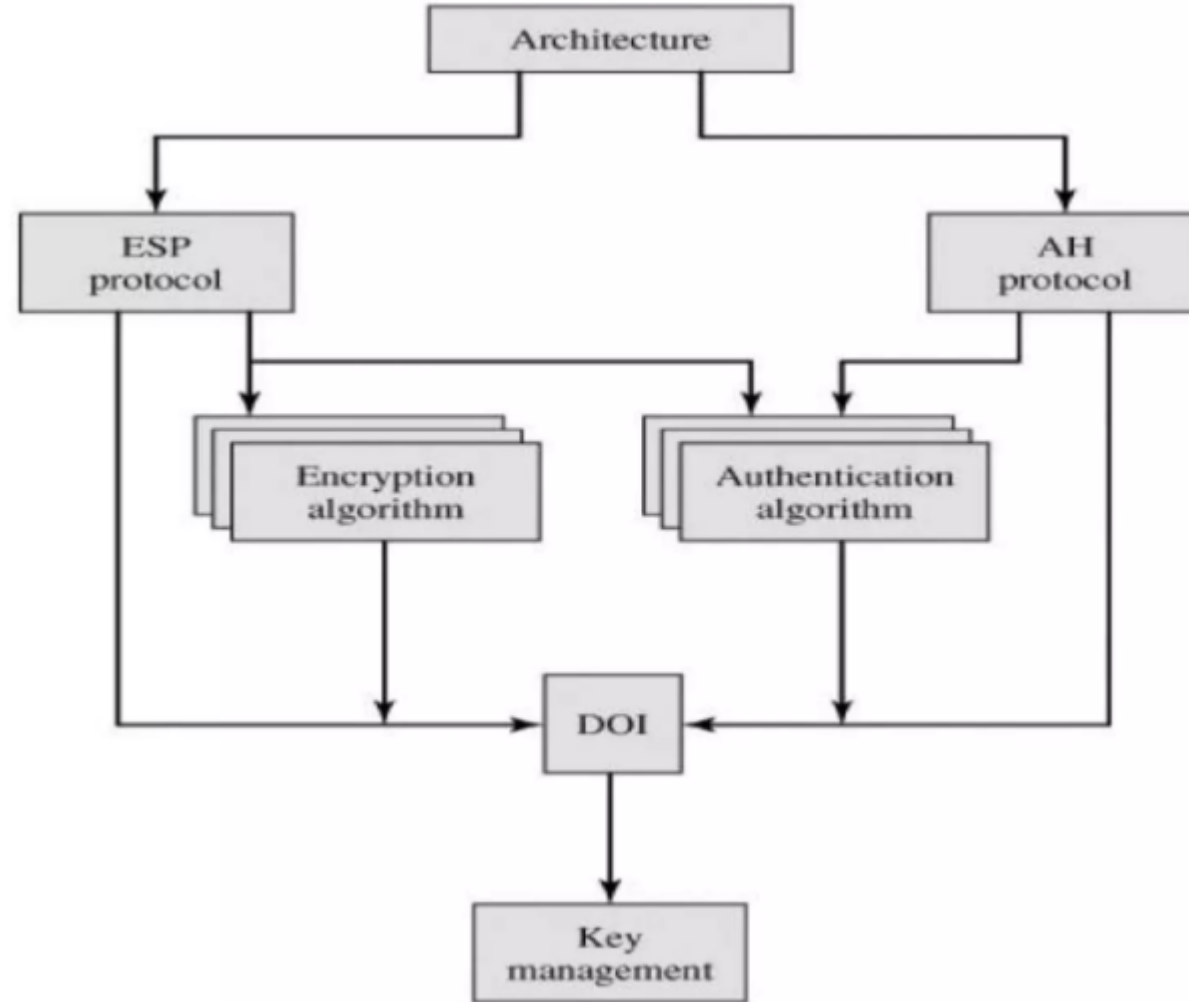


# IPSec Dokümanları

- **Mimari** – IPsec teknolojisini tanımlayan genel kavram güvenlik gereksinimlerini, tanımları ve mekanizmaları kapsar.
- **Kimlik Doğrulama Başlığı (AH)** – Mesaj kimlik doğrulaması sağlamak için bir uzantı başlığı. Güncel spesifikasyon RFC 4302'dir.
- **Kapsülleme Güvenlik Yüğü** – Şifreleme veya birleşik şifreleme/kimlik doğrulama sağlamak için kullanılan bir kapsülleme başlığı ve sonu içerir. Güncel spesifikasyon RFC 4303'tür.
- **İnternet Anahtar Değişimi (IKE)** – IPsec ile kullanılacak anahtar yönetimi şemalarını açıklayan bir belge koleksiyonu.
- **Kriptografik algoritmalar** – Şifreleme, mesaj kimlik doğrulaması, sözde rasgele fonksiyonlar ve kriptografik anahtar değişimi için kriptografik algoritmaları tanımlayan ve açıklayan geniş bir belge setini içerir.
- **Yorum Alanı** – Diğer belgelerin birbiriyle ilişkilendirilmesi için gereken değerleri içerir. Bunlar, onaylanmış şifreleme ve kimlik doğrulama algoritmaları için tanımlayıcıların yanı sıra anahtar ömrü gibi operasyonel parametreleri de içerir.

*Dr. Fatih KALEMKUŞ*

# IPSec Dokümanlarına Genel Bakış





# IPSec Güvenlik Hizmetleri

- Bağlantısız bütünlük Alınan trafiğin değiştirilmediğinin güvencesi. Bütünlük, tekrar saldırısı önleme savunmalarını içerir.
- Veri kaynağı kimlik doğrulaması Trafiğin yasal bir taraf veya taraflarca gönderildiğinin güvencesi.
- Gizlilik (şifreleme) Kullanıcının trafiğinin yetkisiz taraflarca incelenmediğinin güvencesi.
- Erişim kontrolü Bir kaynağın yetkisiz kullanımının önlenmesi.
- Sınırlı trafik akışı gizliliği

*Dr. Fatih KALEMKUŞ*



# Güvenlik İlişkileri

- Bir gönderici ile alıcı arasında, üzerinde taşınan trafiğe güvenlik hizmetleri sağlayan tek yönlü bir ilişki.

Bir güvenlik ilişkisi üç parametre ile benzersiz şekilde tanımlanır:

- **Güvenlik Parametreleri Dizini (SPI):** Bu SA'ya atanan ve yalnızca yerel önemi olan bir bit dizisi. SPI, AH ve ESP başlıklarında taşınır ve alıcı sistemin, alınan bir paketin işleneceği SA'yı seçmesini sağlar.
- **IP Hedef Adresi:** Şu anda yalnızca unicast adreslere izin verilmektedir; bu, bir son kullanıcı sistemi veya bir güvenlik duvarı ya da yönlendirici gibi bir ağ sistemi olabilen SA'nın hedef uç noktasının adresidir.
- **Güvenlik Protokol Tanımlayıcı:** Bu, ilişkinin bir AH mi yoksa ESP güvenlik ilişkisi mi olduğunu gösterir.

*Dr. Fatih KALEMKUŞ*



# Güvenlik İlişkisi Parametreleri

Güvenlik İlişkisi Veritabanı, her SA ile ilişkili parametreleri tanımlar. Bir güvenlik ilişkisi normalde aşağıdaki parametrelerle tanımlanır:

- **Sıra Numarası Sayacı:** AH veya ESP başlıklarındaki Sıra Numarası alanını oluşturmak için kullanılan 32-bitlik bir değer.
- **Sıra Sayacı Taşması:** Sıra Numarası Sayacının taşmasının denetlenebilir bir olay oluşturup oluşturmaması ve bu SA üzerindeki paketlerin daha fazla iletimini engelleyip engellememesi gerektiğini belirten bir bayrak (tüm uygulamalar için gereklidir).
- **Tekrar Oynatma Önleme Penceresi (Anti-Replay Window):** Gelen bir AH veya ESP paketinin bir tekrar oynatma olup olmadığını belirlemek için kullanılır.
- **AH Bilgileri:** AH ile kullanılan doğrulama algoritması, anahtarlar, anahtar ömrü ve ilgili parametreler (AH uygulamaları için gereklidir).

*Dr. Fatih KALEMKUŞ*



# Güvenlik İlişkisi Parametreleri

- **ESP Bilgileri:** ESP ile kullanılan şifreleme ve kimlik doğrulama algoritması, anahtarlar, başlatma değerleri, anahtar ömürleri ve ilgili parametreler (ESP uygulamaları için gereklidir).
- **Bu Güvenlik İlişkisinin Ömrü:** Bir SA'nın yeni bir SA (ve yeni bir SPI) ile değiştirilmesi veya sonlandırılması gereken bir zaman aralığı veya bayt sayısı, ayrıca bu eylemlerden hangisinin gerçekleşmesi gerektiğinin bir göstergesi (tüm uygulamalar için gereklidir).
- **IPSec Protokol Modu:** Tünel, taşıma veya joker karakter (tüm uygulamalar için gereklidir).
- **Yol MTU:** Gözlemlenen herhangi bir yol maksimum iletim birimi (parçalanma olmadan iletilebilecek bir paketin maksimum boyutu) ve eskime değişkenleri (tüm uygulamalar için gereklidir).

*Dr. Fatih KALEMKUŞ*



# Güvenlik İlişkisi Seçicileri

IP trafiğinin belirli SA'larla (veya IPSec'i atlamasına izin verilen trafik durumunda hiçbir SA ile) ilişkilendirildiği araç, nominal Güvenlik Politikası Veritabanı (SPD)'dir.

Aşağıdaki seçiciler bir SPD girdisini belirler:

- **Hedef IP Adresi:** Bu, tek bir IP adresi, numaralandırılmış bir liste veya adres aralığı ya da bir joker (maske) adresi olabilir. Son ikisi, aynı SA'yı paylaşan birden fazla hedef sistemi (örn. bir güvenlik duvarının arkasında) desteklemek için gereklidir.
- **Kaynak IP Adresi:** Bu, tek bir IP adresi, numaralandırılmış bir liste veya adres aralığı ya da bir joker (maske) adresi olabilir. Son ikisi, aynı SA'yı paylaşan birden fazla kaynak sistemi (örn. bir güvenlik duvarının arkasında) desteklemek için gereklidir.
- **UserID:** İşletim sisteminden bir kullanıcı tanımlayıcısıdır. Bu, IP veya üst katman başlıklarında bir alan değildir ancak IPSec kullanıcının çalıştığı aynı işletim sisteminde çalışıyorsa kullanılabilir.

*Dr. Fatih KALEMKUŞ*



# Güvenlik İlişkisi Seçicileri

- **Veri Hassasiyet Seviyesi:** Bilgi akış güvenliği sağlayan sistemler için kullanılır (örn., Gizli veya Sınıflandırılmamış).
- **Taşıma Katmanı Protokolü:** IPv4 Protokolü veya IPv6 Sonraki Başlık alanından elde edilir. Bu, tek bir protokol numarası, bir protokol numaraları listesi veya bir protokol numaraları aralığı olabilir.
- **Kaynak ve Hedef Bağlantı Noktaları:** Bunlar, tek tek TCP veya UDP bağlantı noktası değerleri, numaralandırılmış bir bağlantı noktaları listesi veya bir joker bağlantı noktası olabilir.

*Dr. Fatih KALEMKUŞ*



# IPSec Çalışma Modları

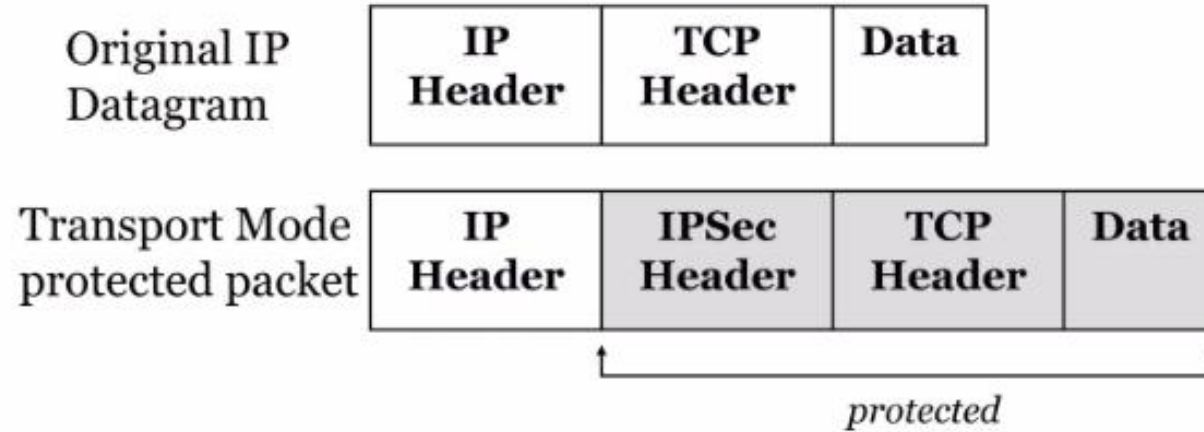
Hem AH hem de ESP iki kullanım modunu destekler:

- **Taşıma modu** – Öncelikle üst katman protokolleri için koruma sağlar. Taşıma modundaki ESP, IP yükünü şifreler ve isteğe bağlı olarak doğrular, ancak IP başlığını şifrelemez. AH, IP yükünü ve IP başlığının seçilen kısımlarını doğrular.
- **Tünel modu** – Tüm IP paketine koruma sağlar. AH veya ESP alanları IP paketine eklendikten sonra, tüm paket artık güvenlik alanları, yeni bir dış IP başlığına sahip yeni bir dış paketin yükü olarak işlem görür.

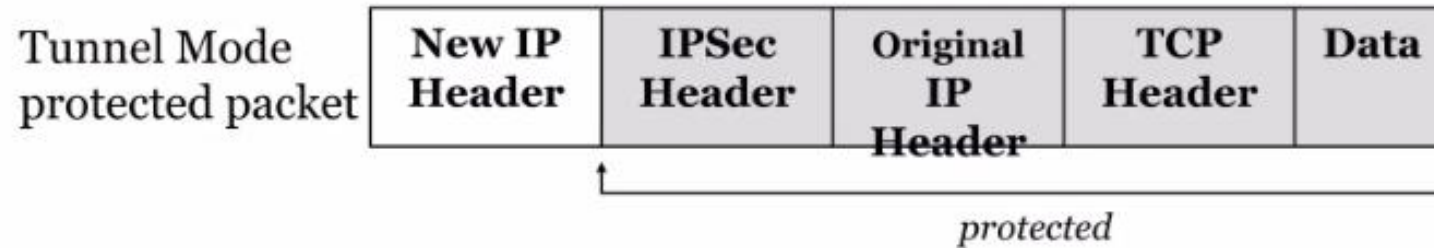
*Dr. Fatih KALEMKUŞ*

# IPSec Çalışma Modları

- Transport Mode: protect the upper layer protocols



- Tunnel Mode: protect the entire IP payload





# Taşıma Modu ve Tünel Modu İşlevleri

## Taşıma modu ve Tünel modu işlevleri

	Taşıma Modu SA	Tünel Modu SA
AH	IP yükünü ve IP başlığının seçilen kısımlarını ve IPv6 uzantı başlıklarını doğrular.	Tüm iç IP paketini artı dış IP başlığının seçilen kısımlarını doğrular.
ESP	IP yükünü ve herhangi bir IPv6 uzantı başlığını şifreler.	İç IP paketini şifreler.
Doğrulamalı ESP	IP yükünü ve herhangi bir IPv6 uzantı başlığını şifreler. IP yükünü doğrular ancak IP başlığını doğrulamaz.	İç IP paketini şifreler. İç IP paketini doğrular.

*Dr. Fatih KALEMKUŞ*



# Doğrulama Başlığı (Authentication Header)

- IP paketlerinin veri bütünlüğü ve kimlik doğrulaması için destek sağlar.
- Kimlik doğrulama, bir mesaj doğrulama kodu (MAC) kullanımına dayanır, bu nedenle iki taraf gizli bir anahtar paylaşmalıdır.

*Dr. Fatih KALEMKUŞ*



# Doğrulama Başlığı (Authentication Header)

Doğrulama Başlığı aşağıdaki alanlardan oluşur:

- **Sonraki Başlık (8 bit):** Bu başlığı hemen takip eden başlığın türünü tanımlar.
- **Yük Uzunluğu (8 bit):** Doğrulama Başlığının 32-bit kelimeler cinsinden uzunluğu, eksi 2.
- **Ayrılmış (16 bit):** Gelecekteki kullanım için.
- **Güvenlik Parametreleri Dizini (32 bit):** Bir güvenlik ilişkisini tanımlar.
  - **Sıra Numarası (32 bit):** Monotonik olarak artan bir sayaç değeri.
- **Doğrulama Verisi (değişken):** Bütünlük Kontrol Değerini (ICV) veya MAC'i içeren değişken uzunlukta bir alan (32-bit kelimelerin tam sayısı olmalıdır).

*Dr. Fatih KALEMKUŞ*

# Doğrulama Başlığı (Authentication Header)

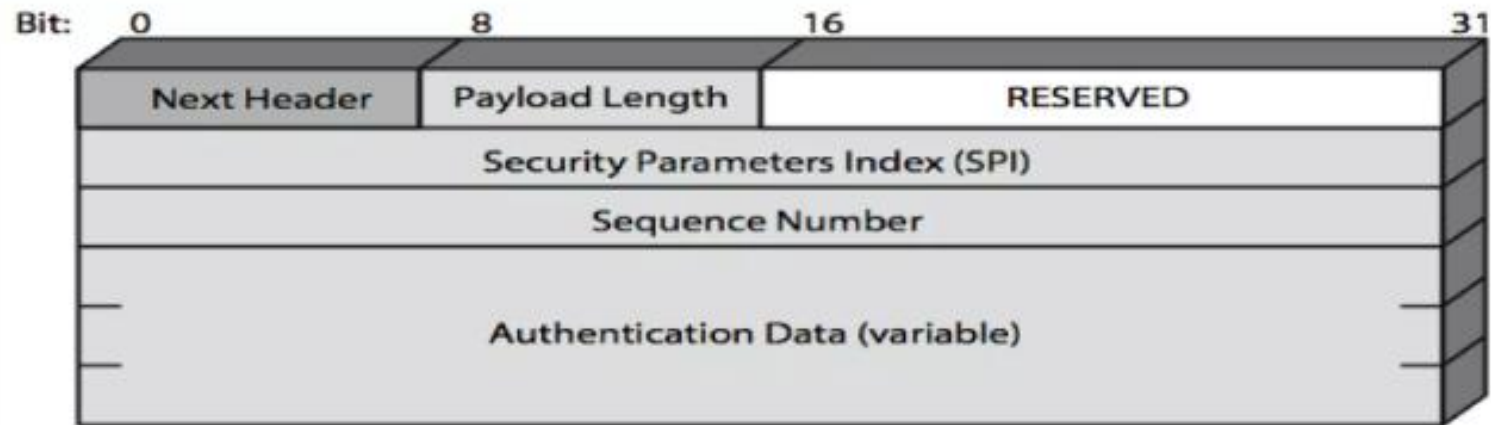


Figure 16.3 IPsec Authentication Header



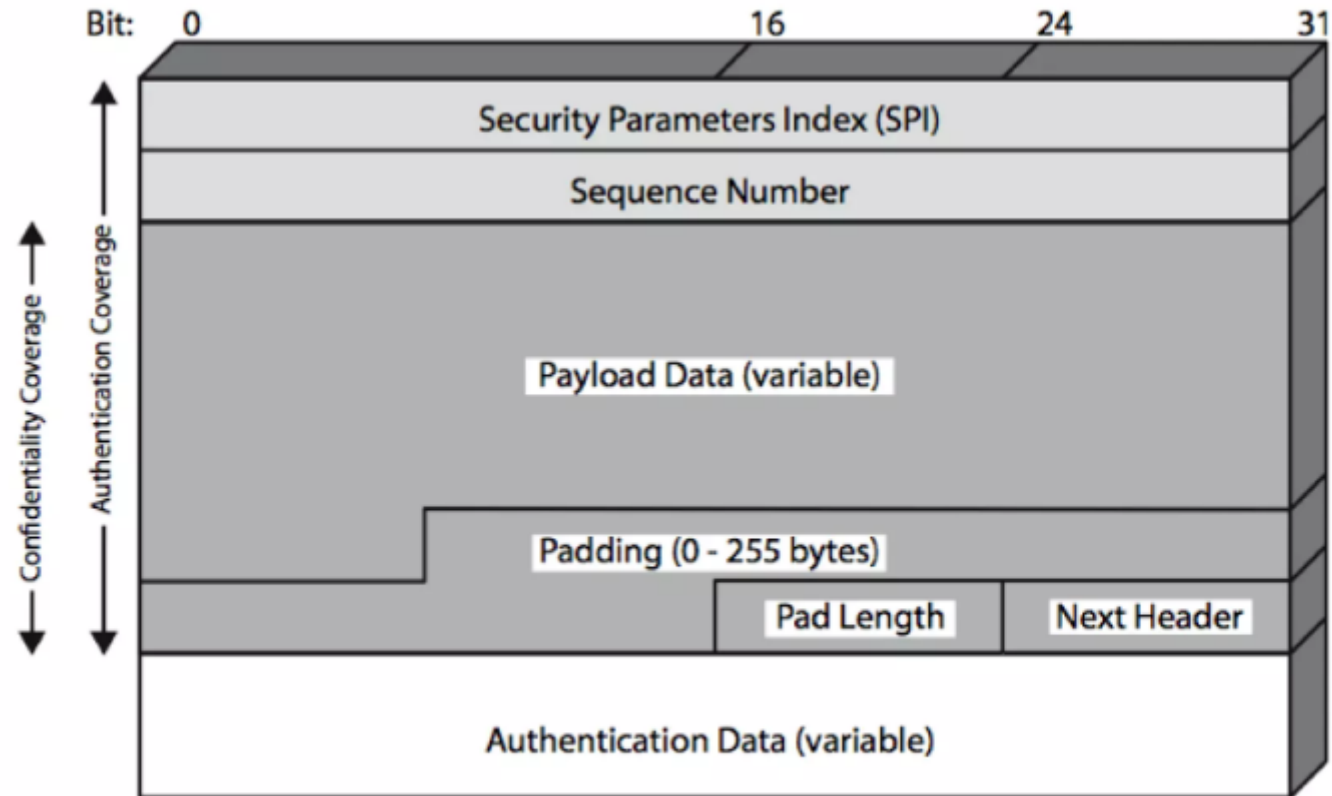
# Encapsulating Security Payload (ESP)

## Kapsülleme Güvenlik Yüğü (ESP)

- mesaj içeriđi gizliliđi ve sınırlı trafik akışı gizliliđi sağlar
- isteđe bađlı olarak AH ile aynı dođrulama hizmetlerini sağlayabilir
- mesaj dođrulama ESP tarafından sağlandıđı için AH'nin kullanımı önerilmemektedir (deprecated)
- çeşitli şifreleri, modları, doldurmayı (padding) destekler
  - DES, Üçlü-DES, RC5, IDEA, CAST vb. içerir
  - CBC ve diđer modlar
  - blok boyutunu, alanları, trafik akışı için doldurma (padding) gereklidir

*Dr. Fatih KALEMKUŞ*

# Encapsulating Security Payload (ESP)



**Fig-1. ESP Format**



# Encapsulating Security Payload (ESP)

**Güvenlik Parametreleri Dizini (32 bit):** Bir güvenlik ilişkisini tanımlar

**Sıra Numarası (32 bit):** Monotonik olarak artan bir sayaç değeridir; bu, tekrar oynatmaya karşı bir işlev sağlar

**Yük Verisi (değişken):** Şifreleme ile korunan bir taşıma katmanı segmenti (taşıma modu) veya IP paketi (tünel modu)

**Doldurma (0–255 bayt):** Çeşitli nedenlerle

**Doldurma Uzunluğu (8 bit):** Bu alanın hemen önündeki doldurma baytlarının sayısını gösterir

**Sonraki Başlık (8 bit):** Yük veri alanında bulunan veri türünü, o yükteki ilk başlığı tanımlayarak belirtir

**Bütünlük Kontrol Değeri (değişken):** ESP paketinden Kimlik Doğrulama Veri alanı çıkarılarak hesaplanan Bütünlük Kontrol Değerini içeren, değişken uzunluklu bir alan

*Dr. Fatih KALEMKUŞ*



# Anti-Replay Service

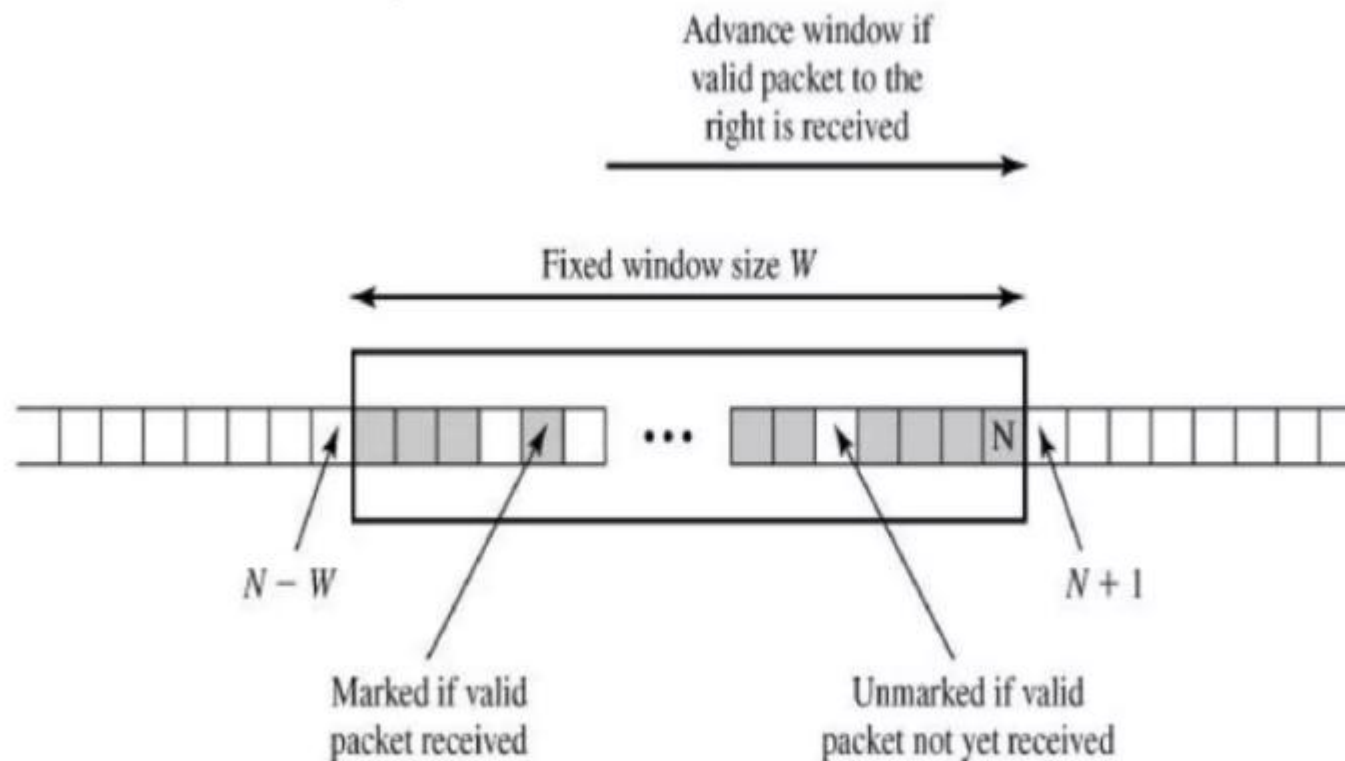
## Tekrar Oynatma Önleme Hizmeti

- Tekrar oynatma saldırısı, bir saldırganın doğrulanmış bir paketin kopyasını ele geçirip daha sonra onu hedeflenen varış noktasına ilettiği bir saldırı türüdür. Tekrarlanan, doğrulanmış IP paketlerinin alınması hizmeti bir şekilde aksatabilir veya başka istenmeyen sonuçlara yol açabilir.
- Sıra Numarası alanı bu tür saldırıları engellemek için tasarlanmıştır.
- Yeni bir SA (Güvenlik ilişkisi) kurulduğunda, gönderici bir sıra numarası sayacını 0'a başlatır.
- Eğer tekrar oynatma önleme etkinse (varsayılan), gönderici sıra numarasının  $2^{32} - 1$ 'den sıfıra geri dönmesine izin vermemelidir. Aksi takdirde, aynı sıra numarasına sahip birden fazla geçerli paket olacaktır. Eğer  $2^{32} - 1$  sınırı aşırsa, gönderici bu SA'yı sonlandırmalı ve yeni bir anahtarla yeni bir SA üzerinde anlaşma sağlamalıdır.

*Dr. Fatih KALEMKUŞ*

# Anti-Replay Service

with a default of  $W = 64$



**Fig-2. Antireplay Mechanism**

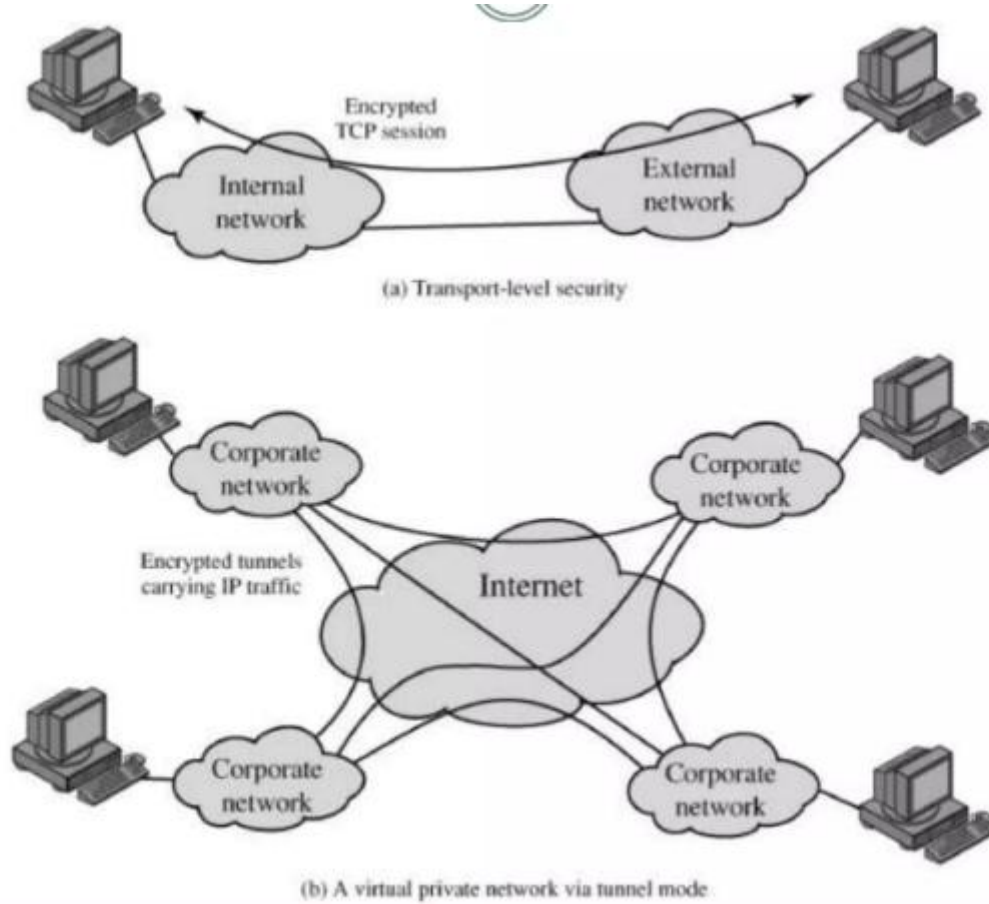


# Taşıma Modu ve Tünel Modu ESP Karşılaştırması

- Taşıma modu, IP verilerini şifrelemek ve isteğe bağlı olarak doğrulamak için kullanılır.
  - veriler korunur ancak başlık açık bırakılır
  - trafik analizi yapılabilir ancak verimlidir
  - ESP ana bilgisayardan ana bilgisayara trafik için iyidir
- Tünel modu, tüm IP paketini şifreler.
  - sonraki atlama için yeni başlık ekler
  - VPN'ler ve ağ geçidinden ağ geçidine güvenlik için iyidir

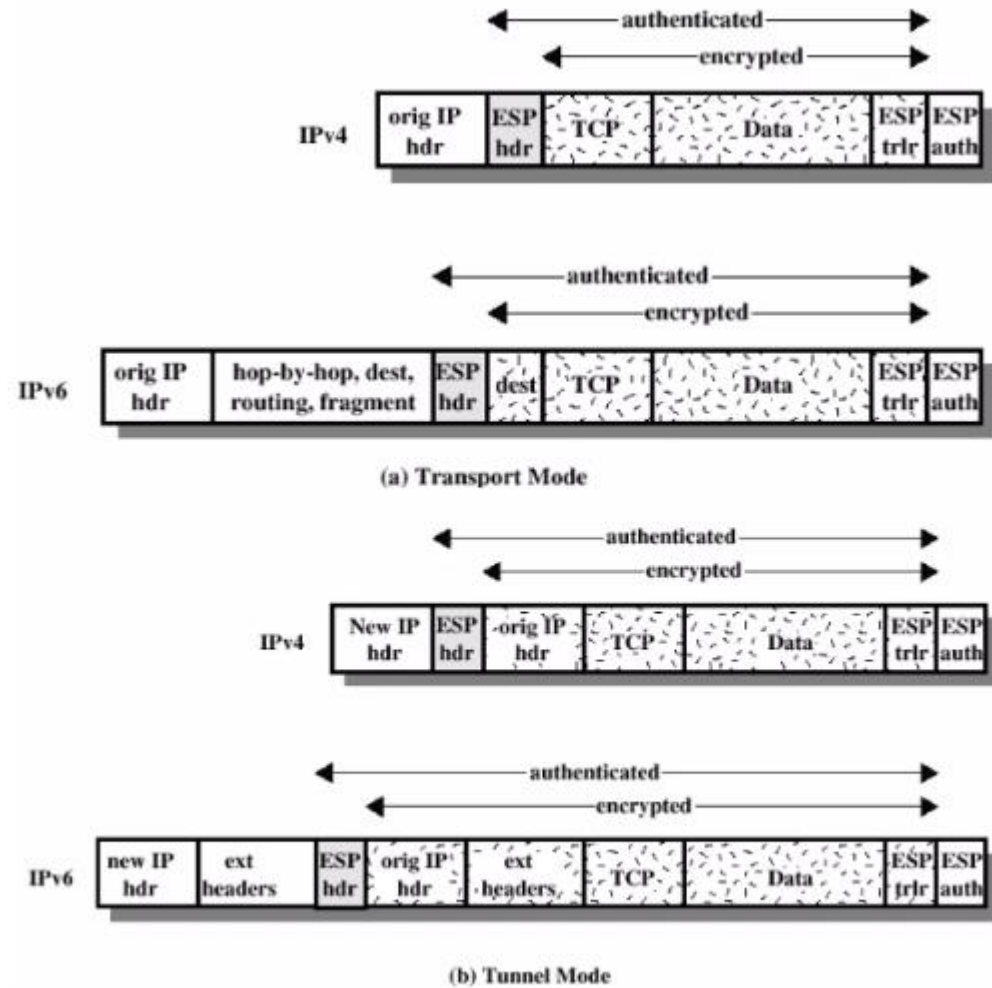
*Dr. Fatih KALEMKUŞ*

# Taşıma Modu ve Tünel Modu ESP Karşılaştırması



**Fig-3. Transport-Mode vs. Tunnel-Mode Encryption**

# Taşıma Modu ve Tünel Modu ESP Karşılaştırması



**Fig-4. Scope of ESP Encryption and Authentication**



# Güvenlik İlişkilendirmelerini Birleştirme

- SA'lar (Güvenlik İlişkilendirmeleri) ya AH (Kimlik Doğrulama Başlığı) ya da ESP (Kapsülle Birleştiren Güvenlik Yüğü) uygulayabilir.
- Her ikisini de uygulamak için SA'ları birleştirmek gerekir:
  - bir güvenlik ilişkilendirme paketi oluşturulur
  - farklı veya aynı uç noktalarda sonlanabilir
  - şu yöntemlerle birleştirilir:
    - taşıma yakınlığı (transport adjacency)
    - yinelenen tünelleme (iterated tunneling)
- Kimlik doğrulama ve şifreleme sırası sorunu vardır.

*Dr. Fatih KALEMKUŞ*



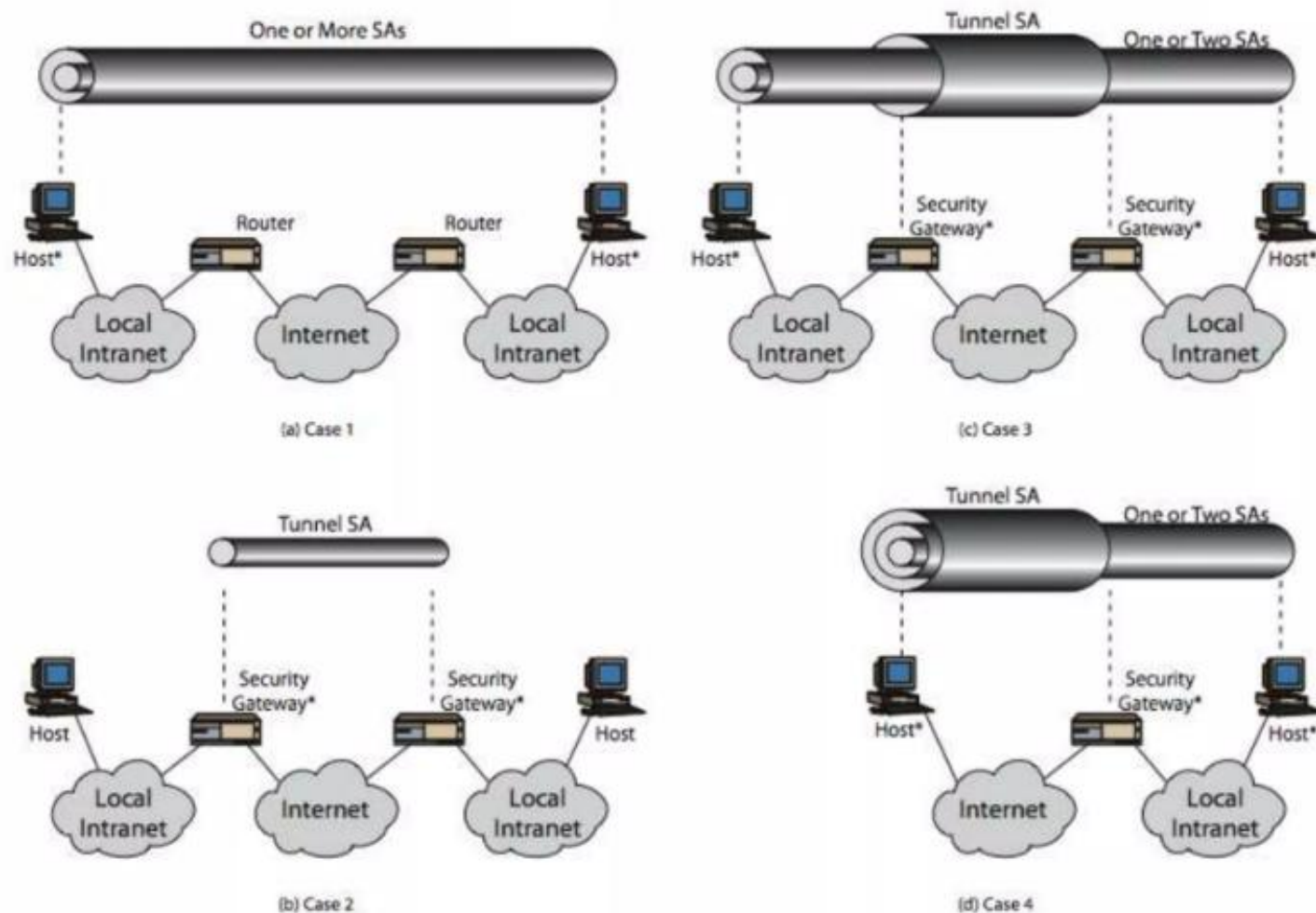
# Kimlik Doğrulama ve Gizlilik Birleşimi

Ana bilgisayarlar arasında hem gizliliği hem de kimlik doğrulamayı içeren IP paketi iletimi:

1. **Kimlik Doğrulama Seçeneği ile ESP:** Taşıma modu ESP veya Tünel modu ESP kullanarak şifrelemeden sonra kimlik doğrulama.
2. **Taşıma Yakınlığı:** Şifrelemeden sonra Kimlik Doğrulamayı uygulamanın başka bir yolu.
  - İçteki bir ESP SA (Güvenlik ilişkisi) ve dıştaki bir AH (Kimlik Doğrulama Başlığı) SA olan iki paketlenmiş taşıma SA'sını kullanın.
  - Burada ESP kimlik doğrulama seçeneği olmadan kullanılır.
  - **Avantaj:** Kimlik doğrulama, kaynak ve hedef IP adresleri de dahil olmak üzere daha fazla alanı kapsar.
  - **Dezavantaj:** İki SA'nın ek yükü, tek bir SA'ya kıyasla.
3. **Taşıma-Tünel Paketi:** Şifrelemeden önce kimlik doğrulama.
  - İçteki bir AH taşıma SA'sı ve dıştaki bir ESP tünel SA'sından oluşan bir paket kullanın.
  - **Avantajlar:**
    - a) Mesajı yakalamak ve kimlik doğrulama verilerini tespit edilmeden değiştirmek imkansızdır.
    - b) Mesajla birlikte kimlik doğrulama bilgileri, daha sonraki referanslar için hedefte saklanabilir.

*Dr. Fatih KALEMKUŞ*

# Güvenlik İlişkilendirmelerinin Temel Kombinasyonları



**Fig-5. Basic Combinations of Security Associations**



# Anahtar Yönetimi

## IPSec Anahtar Yönetimi

- Anahtar üretimini ve dağıtımını yönetir.
- Genellikle 2 anahtar çiftine ihtiyaç duyar:
  - AH ve ESP için yön başına 2 tane
- Manuel anahtar yönetimi:
  - Sistem yöneticisi her sistemi manuel olarak yapılandırır.
- Otomatik anahtar yönetimi:
  - Büyük sistemlerde SA'lar (Güvenlik İlişkilendirmeleri) için isteğe bağlı anahtar oluşturma için otomatik sistem.
  - Oakley ve ISAKMP öğeleri içerir.

# Sorular

---



*Dr. Fatih KALEMKUŞ*



TEŞEKKÜRLER

*Dr. Fatik KALEMKUŞ*

# Kaynakça

Cryptography and Network Security Principles and Practices, 4th Ed - William Stallings