# Güvenlik Duvarları ve Tüneller

# Konular

- Temel Kavramlar ve İlkeler
- Kriptografik Yapı Taşları
- Kullanıcı Kimlik Doğrulaması - Parolalar, Biyometri ve Alternatifler
- Kimlik Doğrulama Protokolleri ve Anahtar Kurulumu
- İşletim Sistemi Güvenliği ve Erişim Denetimi
- Yazılım Güvenliği - İstismarlar ve Ayrıcalık Arttırma
- Kötü Amaçlı Yazılımlar
- Açık Anahtar Sertifika Yönetimi ve Kullanım Durumları
- Web ve Tarayıcı Güvenliği
- Güvenlik Duvarları ve Tüneller
- Saldırı Tespiti ve Ağ Tabanlı Saldırılar

# Temel Ağ Kavramları ve Ön Bilgiler

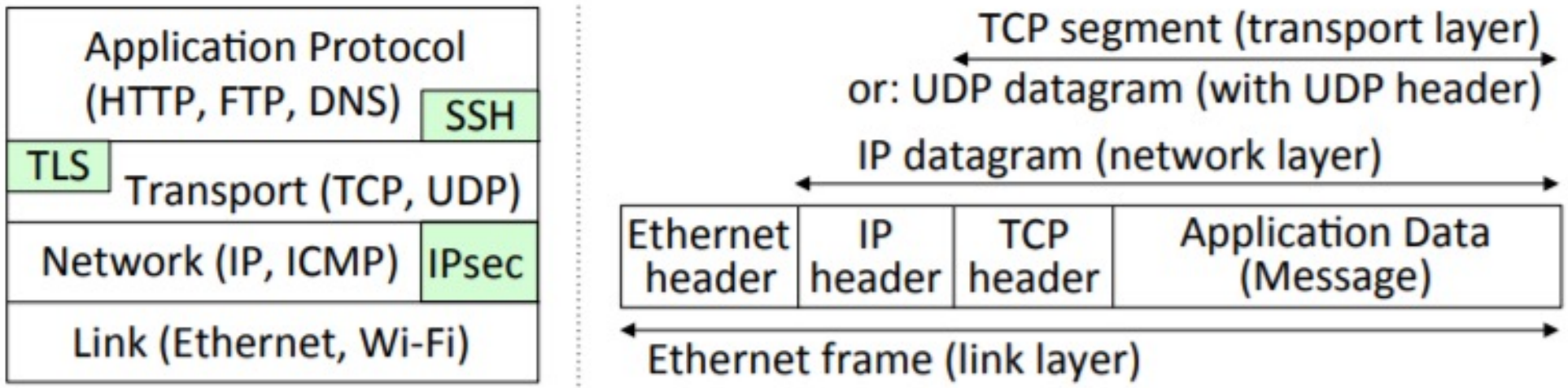


Figure 10.10: Network protocol stack (TCP/IP model) and encapsulation. In the seven-layer OSI model, between Application (7) and Transport are Presentation and Session layers, and Link is Data Link, above Physical (1). Wi-Fi denotes IEEE 802.11 wireless.

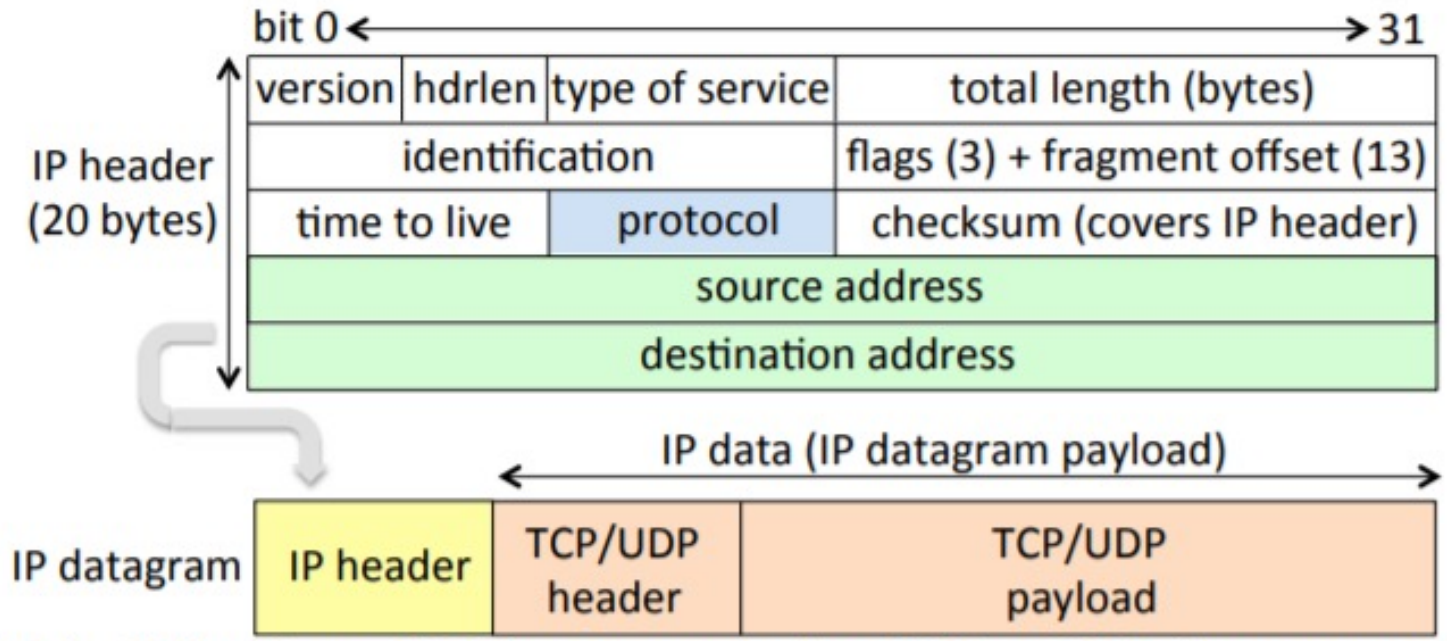


Figure 10.14: IP header and IP datagram carrying TCP or UDP datagram payload. The `identification` field is used in datagram fragmentation and reassembly. TTL (time to live) upper-bounds the number of routers a packet can transit; each router decrements it by one. The IP header checksum is verified (and recalculated, e.g., after TTL updates) at each hop. `Protocol` values of interest are TCP, UDP, ICMP, IP, ESP, AH. `hdrlen` (internal header length, in 32-bit words) is 5 unless an IP `options` field (not shown) is present. The TCP/UDP data part is where Application data is carried, including user data.

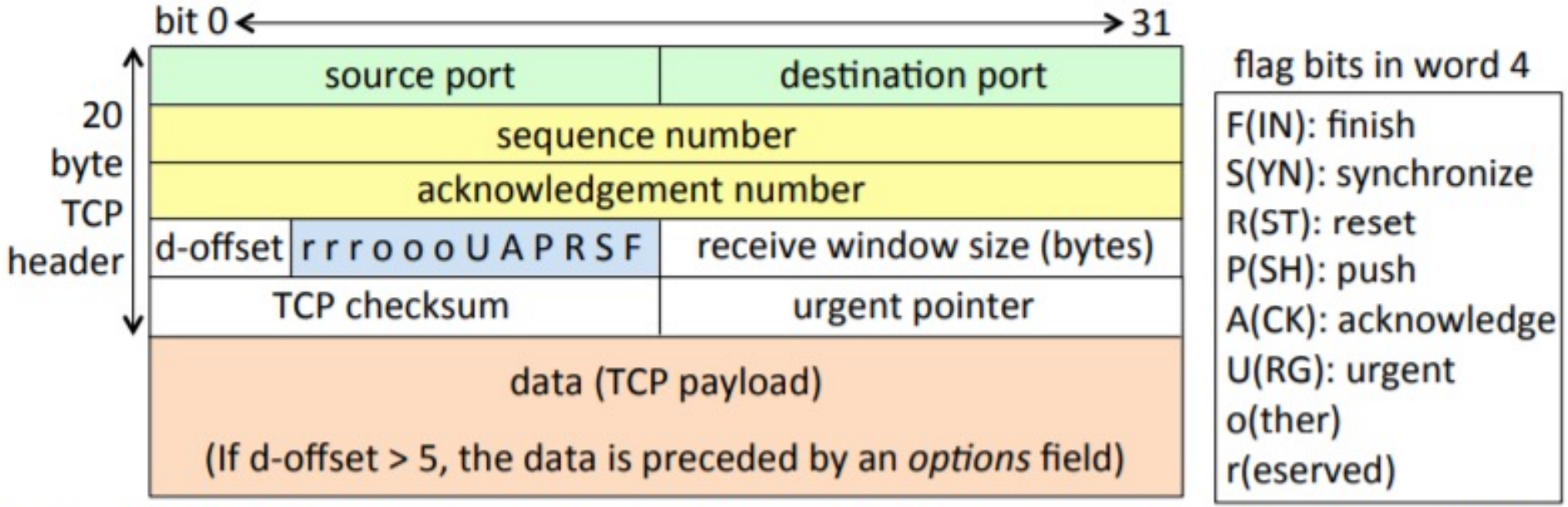


Figure 10.15: TCP header. The 4-bit data offset (`d-offset`) specifies the number of 32-bit words preceding the data. A flag bit of 1 is set (on); 0 is off. Other flag bits beyond our scope are NS (ECN-nonce), CWR (congestion window reduced), and ECE (ECN-echo). The `window_size` advertises how many bytes the receiver will accept, relative to the byte specified in `acknowledgement_number`; values larger than $2^{16} - 1$ bytes are possible by pre-negotiating a window scale option.

# Giriş

- Bu bölüm, güvenlik duvarlarından başlar ve daha sonra uzak kullanıcıların ve aralarında mesafe olan eşlerin ağ iletişimini güvence altına almak için tamamlayıcı teknolojileri konu edinir.
- Sınır-temelli savunma (perimeter-based defense) yöntemleri tartışılır.
- şifrelenmiş tüneller
- sanal özel ağlar (VPN'ler)
- SSH
- IPsec

# Güvenlik Duvarları

- İki temel kategoriye ayrılır:

1. Paket filtreleri
2. Vekil (Proxy) Güvenlik Duvarları

# Paket Filtre Ateş Duvarları

- Bir ağ güvenliği güvenlik duvarı, iki ağ veya bir ağ ve bir cihaz arasında veri geçişine izin verebilen veya reddeden ve isteğe bağlı olarak değiştirebilen erişim kontrolü işlevi sağlayan bir ağ geçididir.
- Tasarım amacı, trafiğin her iki yönde de güvenlik duvarını atlatamamasıdır - bu nedenle teoride, paketler TAM ARACILIK (İ4) sürecinden geçer.
- Ateş Duvarı (Güvenlik Duvarı - Firewall) terimi, İ5 (İZOLASYONLU BÖLMELER) ilkesine uygun olarak, yangın durumunda hasarı izole etmek ve yayılmasını önlemek için tasarlanmış yangına dayanıklı kapılardan gelir. (ateş tuğlası?)
- Ağ güvenlik duvarları en yaygın olarak sınır-temelli savunmalarda hizmet eder ve güvenilir bir özel (dahili) ağı, güvenilmeyen bir genel (harici) ağdan (ör. İnternet) korur.

# Ağ Güvenlik Duvarı (Temel Model)

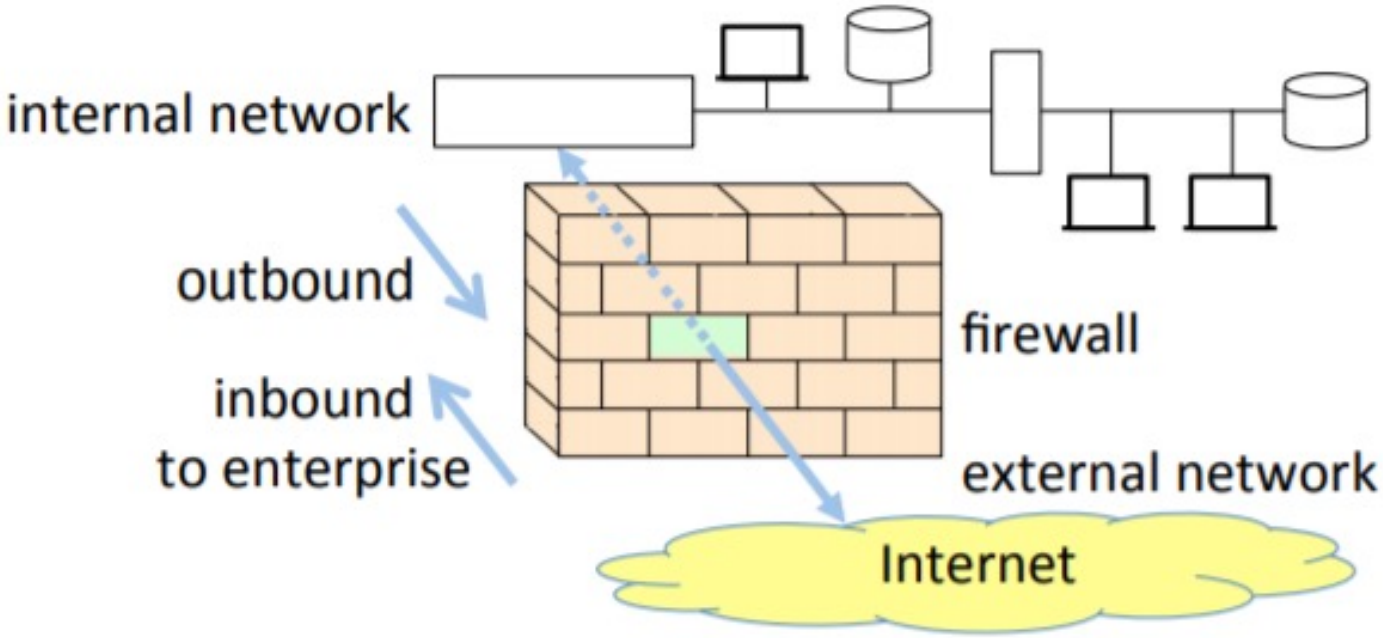


Figure 10.1: Network firewall (basic model).

# Paket Filtreleme Kuralları

- Bir paket filtre güvenlik duvarı, bir yönetici tarafından yapılandırılır.
- <Koşul, eylem> biçiminde bir kural listesi içerir.
- Bir "ilk eşleştirme kuralı" güvenlik duvarında, bir paket için gerçekleştirilen eylem, koşulu karşılanan ilk kural tarafından belirtilen eylemdir.
- Temel eylemler şunlardır:
  1. İZİN VER (paketin geçmesine izin ver
  2. DÜŞÜR (sessizce paketi atın — tip-1 reddetme)
  3. REDDET (geçirme ama aynı zamanda kaynağı bilgilendirmeye çalış — tip-2 reddetme).

     Bir TCP RST (sıfırlama) paketi gönderilmesine veya UDP için bir ICMP "ulaşılamaz hedef" hata koduna neden olabilir.

# Paket Filtreleme Kuralları (2)

- Ek olarak, ikinci bir eylem, örneğin syslog genel sistem günlük kaydı hizmetini kullanarak paketi günlüğe kaydetmektir.
- Verimlilik için, çoğu paket filtresi eşleştirme kuralı beş TCP / IP başlık alanına (src addr, src port, dst addr, dst port, prot) ve eğer ICMP ise ICMP türü ve kodunu temel alır.
- Bazen diğer başlık alanları (paket boyutu, bayraklar) da kullanılır.
- Daha karmaşık kurallar ve akıllı paket filtreleme, yük (payload) verilerini, örneğin URL'e dayalı bir izin verme veya reddetme kararını içerebilir - ancak uygulama yüklerinin incelenmesi genellikle paket filtrelerinin kapsamının dışındadır.

# Durumsuz ve Durumlu Güvenlik Duvarları

- Basit bir durumsuz paket filtresinde, her paket diğerlerinden bağımsız olarak işlenir (önceki paketlere bağımlı olmaksızın).
- Bunun aksine, durumlu bir paket filtresi, daha sonraki paketlerin işlenmesinde kullanılmak üzere paketler işlenirken seçilen ayrıntıları izler.
- Durum ayrıntıları bir güvenlik duvarı durum tablosunda tutulur. Bu genellikle TCP bağlantı durumlarının izlenmesi anlamına gelir; Oluşturulan veya devam eden bağlantı kurulumlarına karşılık gelen kaynaklara sahip paketler, yeni kaynaklardan farklı şekilde ele alınır.

| Rule #, Action | | Path | Source | | Destination | | Protocol | Extra field | Comments |
|---|---|---|---|---|---|---|---|---|---|
| | | | addr | port | addr | port | | | |
| 1 | NO | in | us | * | * | * | * | | ingress and egress |
| 2 | NO | out | them | * | * | * | * | | filtering (Sect. 11.3) |
| 3 | NO | in | black | * | * | * | * | | blacklist bad servers |
| 4 | OK | in | them | high | GW | 25 | TCP | | inbound mail... |
| 5 | OK | out | GW | 25 | them | high | TCP | ACK | ...our responses out |
| 6 | OK | out | GW | high | them | 25 | TCP | | SMTP mail out... |
| 7 | OK | in | them | 25 | GW | high | TCP | ACK | ...inbound response |
| 8 | OK | out | us | high | them | 80 | TCP | | HTTP request out... |
| 9 | OK | in | them | 80 | us | high | TCP | ACK | ...allow responses |
| A | NO | in | them | * | us | 80 | TCP | | no inbound requests |
| B | OK | out | GW | 53 | them | 53 | UDP | | our DNS queries |
| C | OK | in | them | * | GW | 53 | UDP | | DNS queries to us... |
| D | OK | out | GW | 53 | them | * | UDP | | ...responses from us |
| E | OK | in | them | – | us | – | ICMP | 8 | pings to us... |
| F | OK | out | us | – | them | – | ICMP | 0 | ...our responses |
| G | OK | out | us | – | them | – | ICMP | 8 | our pings out... |
| H | OK | in | them | – | us | – | ICMP | 0 | ...responses to us |
| Z | NO | * | * | * | * | * | * | | default deny |

Table 10.1: Packet-filtering rule examples (illustrative, for discussion). Notation: NO (deny packet), OK (allow packet), in/out (inbound/outbound packet direction), us/them (internal/external addresses; products specify explicit ranges), * (any value matches), high (port above 1023, unprivileged), black (list of blacklisted addresses, e.g., spam servers), ACK (ACK bit set), GW (our enterprise gateway mail server/DNS server). For ICMP rules, values (8, 0) refer to ICMP message types; recall that ICMP does not use ports.

# Sorular

- Varsayılan-olarak-Reddet (Default-Deny) kural kümesi mi kullanalım, Varsayılan-olarak-Kabul-et (Default-Accept) mi? (İ2: SAFE-DEFAULTS)
- Güvenlik duvarları ile bir kurumun İnternet güvenlik politikası arasında nasıl bir ilişki bulunur?
- Güvenlik duvarlarının yetersizlikleri nelerdir?
- Bu yetersizliklerine rağmen güvenlik duvarları yine de yararlı olarak addedilebilir mi?
- Dedicated firewalls vs. Hybrid appliances (ör. UTM) ?
- Kişisel veya Dağıtık Güvenlik Duvarları ?

# Vekil (Proxy) Güvenlik Duvarları

- Paket filtre dışında vekil olarak isimlendirilebilen iki farklı türden güvenlik duvarı daha vardır:

1. Devre seviyesinde Vekil (Circuit-level Proxy): bağlantıları genel olarak tek bir vekil noktası üzerinden aktarır; ana amaç önce bağlantıya izin veya red kararını vermek ve ardından verileri aktarmaktır.
2. Uygulama seviyesinde Filtre (Application-level Filters): önceden belirlenmiş ve yetki verilmiş bir dizi uygulama için birden çok özel işlemci aracılığıyla uygulamaya-özgü işlemler gerçekleştirir.

# Devre-seviyesinde Vekil (Proxy) Güvenlik Duvarı

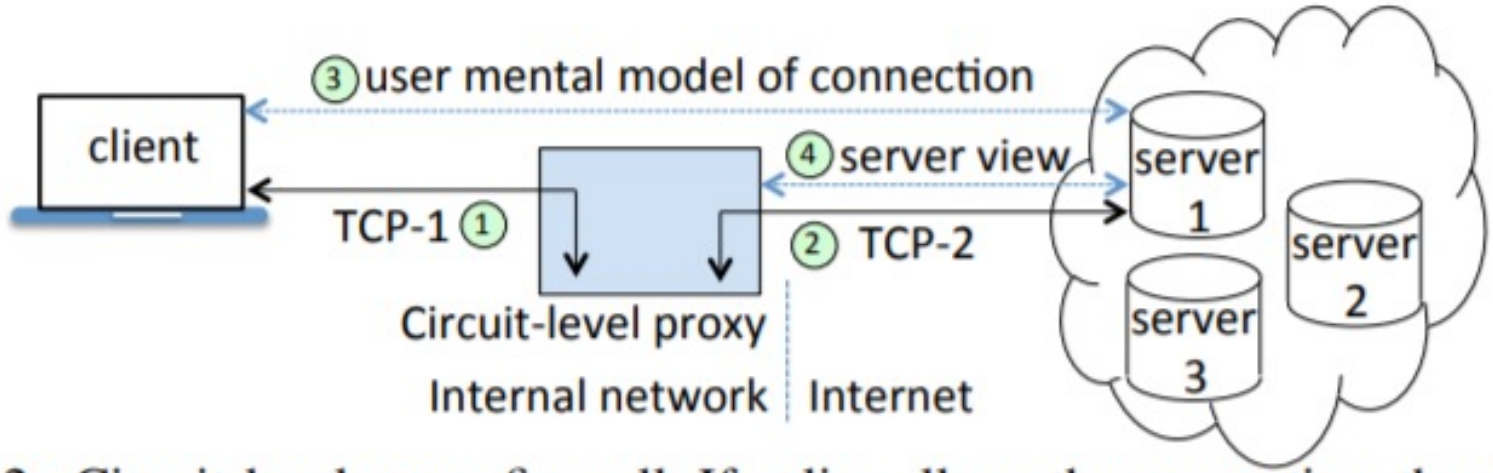


Figure 10.2: Circuit-level proxy firewall. If policy allows the connection, the circuit-level proxy establishes a virtual circuit that fulfills the user view of the connection. Technically, it receives packets on one TCP connection (TCP-1), with packet reassembly as usual, and retransmits using a second TCP connection (TCP-2) to the target server (server 1). From the server viewpoint, the connection is to the proxy, not the end-user client.

# Uygulama-seviyesinde Filtre

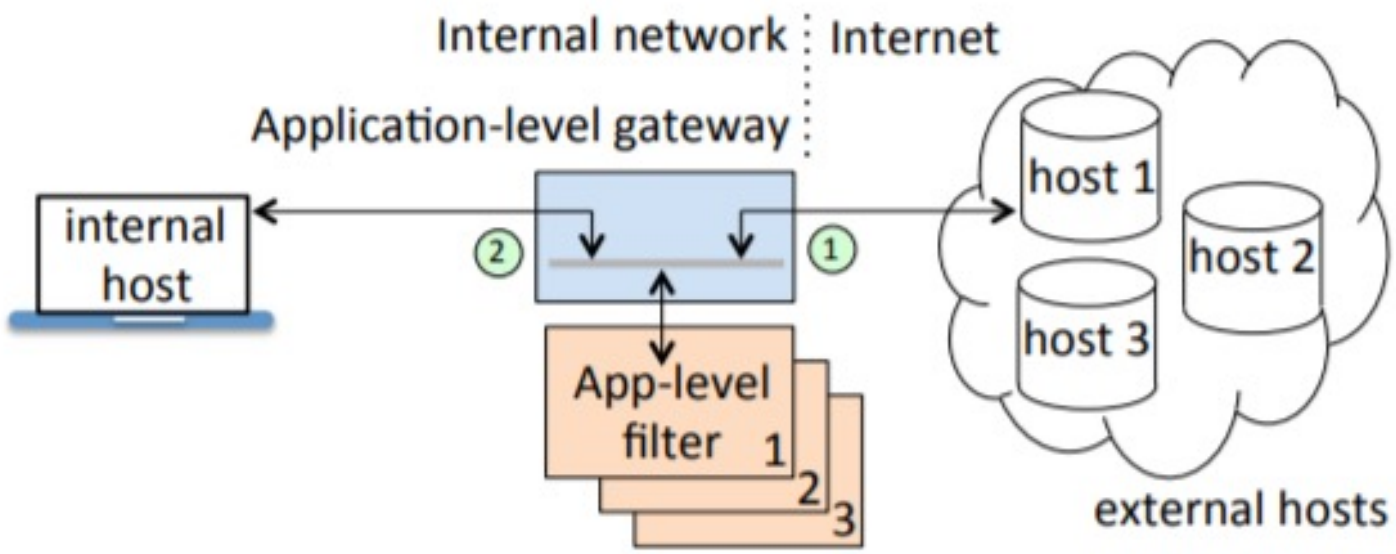


Figure 10.3: Application-level gateway filters. The application-level gateway selects the appropriate filter for application-specific filtering of data packets.

# Kurumsal Güvenlik Duvarı Mimarileri

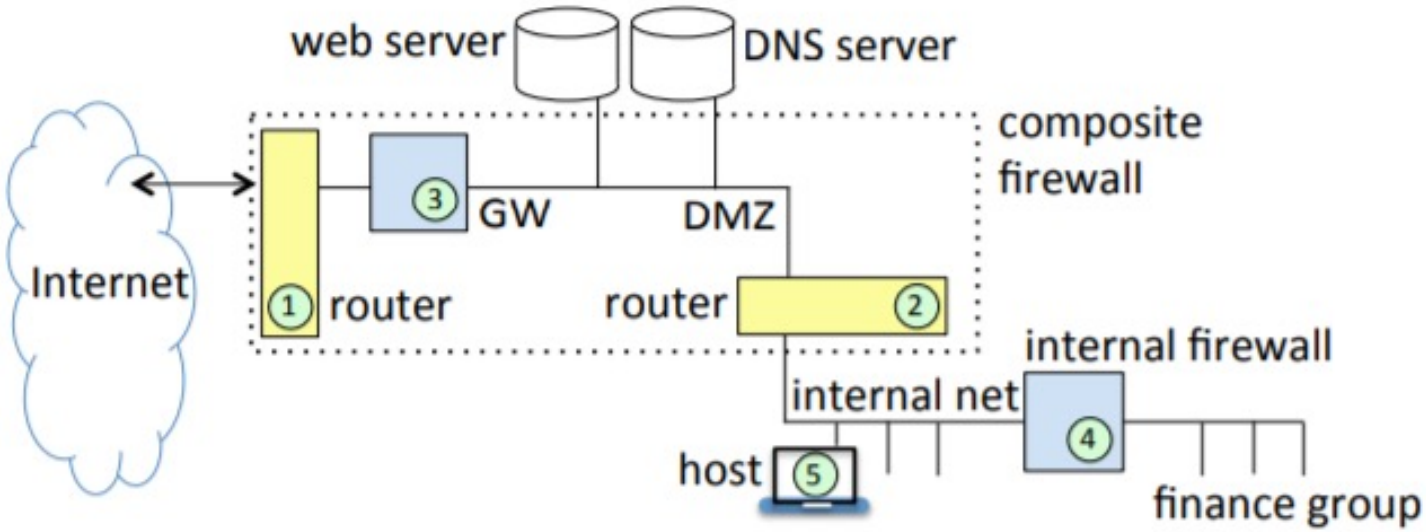


Figure 10.4: Firewall architecture including DMZ. The gateway firewall (3) is a bastion host. An internal host (5) connects to Internet services by proxying through GW, and might be allowed to make outgoing connections (only) through the exterior router (1), bypassing GW, for a reduced set of packet-filtered protocols, depending on policy.

# SSH (Secure Shell)

- SSH'den önce, uzaktan oturum açma (rlogin, telnet), ve ilgili Unix uzaktan erişim komutları (rsh, rcp, rexec) ve dosya aktarımı (ftp), ağ üzerinden verileri ve parolaları açıktan gönderiyor idi.
- SSH ve SSH kullanarak oluşturulan yardımcı programlar daha güvenli alternatifler olarak tasarlandı (gizlilik, doğruluk, kimlik doğrulama sağlayacak şekilde).
- Güvenilir paket aktarımı için TCP'yi kullanan SSH, hem uzak hizmetlere oturum açmak için gönderilen parolaları hem de kimlik doğrulama sonrası devam eden TCP bağlantılarını koruyan taşıma katmanında bir güvenlik tüneli sağlar.
- SSH ile, uzak bir ana bilgisayarda bulunan herhangi bir programın güvenlik tüneli üzerinden çalıştırılabilmesi mümkün olur.

# SSH Tüneli üzerinden Uzak Kabuk

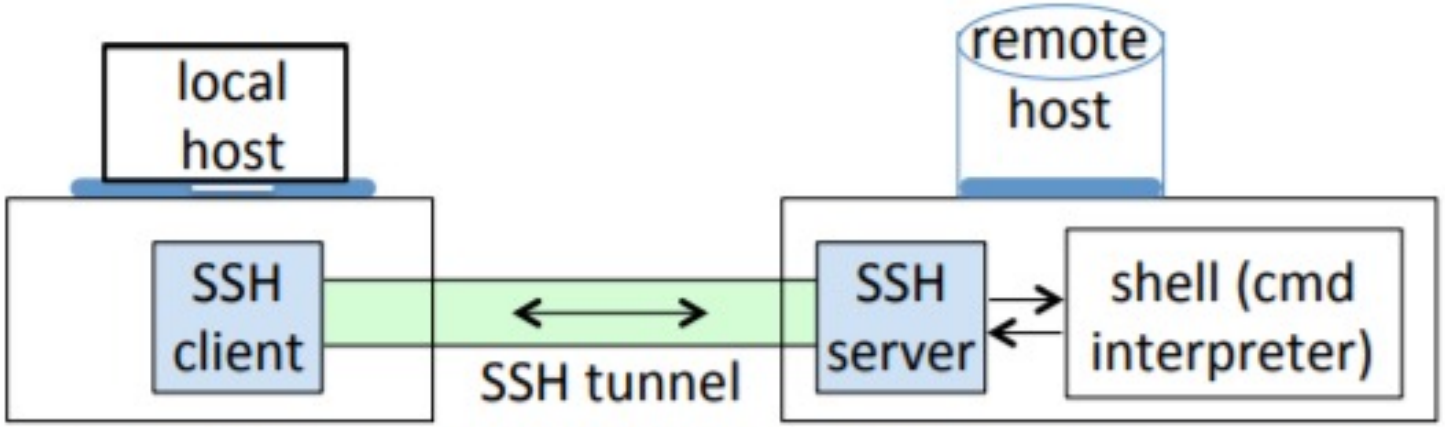


Figure 10.5: Remote shell through an SSH tunnel, providing authenticated encryption.

# SSH Protokolleri

SSH üç parçadan oluşur:

1. Taşıma katmanı protokolü: sunucu kimlik doğrulama, şifreleme, bütünlük koruma.
2. Kullanıcı kimlik doğrulama protokolü:
   - İstemci parolası (veya tek-kullanımlık parolalar)
   - Kerberos
   - İstemci açık-anahtar
3. Bağlantı protokolü: Tek bir tünelin birden fazla amaç için kullanılmasını sağlar (mantıksal kanallar) (çoklama).

# Şifreli Tüneller ve VPN'ler

- Normal TCP/IP paketleri düz metindir. Tüm paket içeriği (başlık ve yük) paket akışına erişimi olan tüm partiler (yönlendiriciler, anahtarlar, geçitler, vb.) tarafından görülebilir.
- Koruma için fikirlerden biri gönderici tarafta tüm paketin şifrelenmesidir. Fakat, bu protokolleri çalışmaz kılar: başlık bilgilerinin okunması imkansız olur.
- Bu sebeple paket başlıkları da şifrelenecek ise bu pkaetin başka bir paket içerisine konumlandırılması gerekir. Alternatif olarak, paketin sadece yük kısmı korunabilir.
- Tünelleme kavramı kapsülleme (encapsulation) ile doğrudan ilgilidir: Bir protokol (başlık ve yük) diğer birinin yükü olur.
- Tünelleme için yaygın olarak kullanılan iki protokol SSH ve Ipsec'dir.
- Tünel kurulduktan sonra uygulamalar ve kullanıcılar başka bir değişikliğe gerek duymadan güvenli hale gelirler.
- Tünellerin bir diğer uygulaması da Sanal Özel Ağlardır (VPN).

# Şifreli Tünel Kavramı

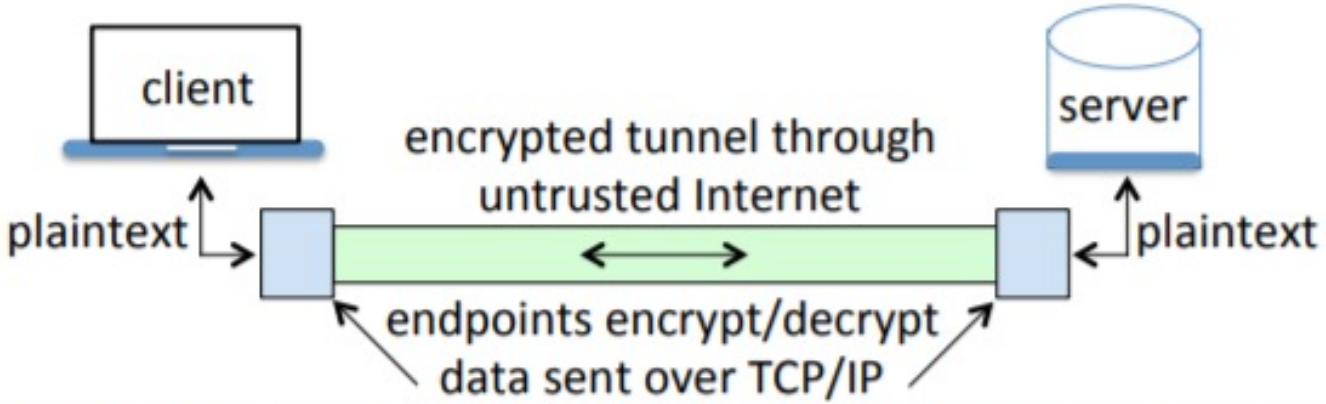


Figure 10.8: Encrypted tunnel (concept). To avoid breaking pre-existing protocols, the tunneling protocol must preserve packet header data used for routing and middlebox (i.e., non-endpoint) processing.

# VPN Tasarımı ve Mimarileri

| VPN design | VPN architecture | Notes and use cases |
|---|---|---|
| transport mode | host-to-host VPN | provides end-to-end security<br>(VPN endpoints are final destination) |
| tunnel mode | network-to-network | network gateways add/remove VPN security<br>(no VPN protection internal to gateway) |
| | host-to-network | for remote host access to enterprise<br>(in-host gateway adds/removes VPN security) |

Table 10.3: VPN designs and architectures. See Fig. 10.9 for illustrations.

# VPN Tasarımları

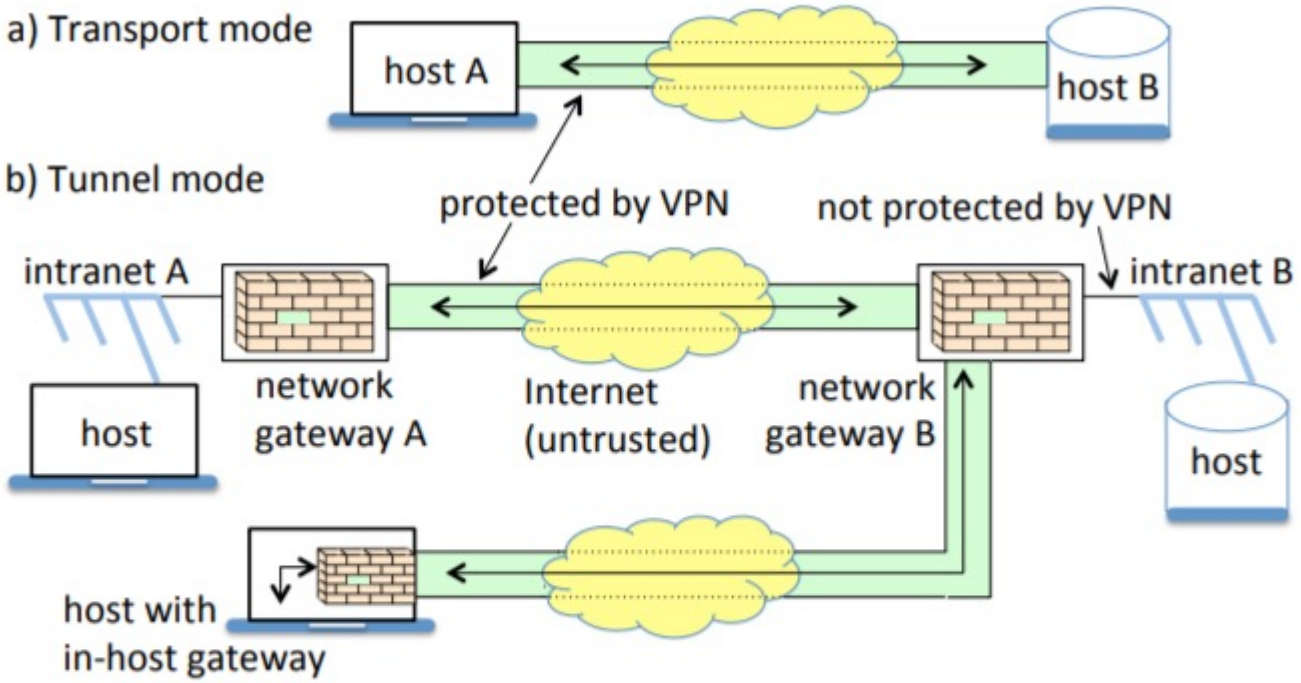


Figure 10.9: VPN designs. (a) Transport mode is host to host (single hosts), still delivering a payload via an encrypted tunnel in the sense of Fig. 10.8. (b) Tunnel mode involves network gateways. In the in-host gateway case, one end has a within-host final hop. Intranet A, on the enterprise side of a gateway, is an internal enterprise network. Intranet B may be a second enterprise network, or a remote employee's home network.

# Şifreli Tünellerin Kısıtlamaları?

# IPsec

- TLS ve SSH’den farklı olarak IPsec protokolü ağ katmanında bir güvenlik servisi sunar. Bu sayede tüm taşıma ve uygulama katmanı protokolleri otomatik olarak korunur.
- VPN’ler için IPsec üç protokol ileçok geniş bir yelpazede güvenlik servisleri sunar:

1. IKE (Internet Key Exchange)
2. AH (Authentication Header)
3. ESP (Encapsulating Security Payload)

# IPsec Authentication Header

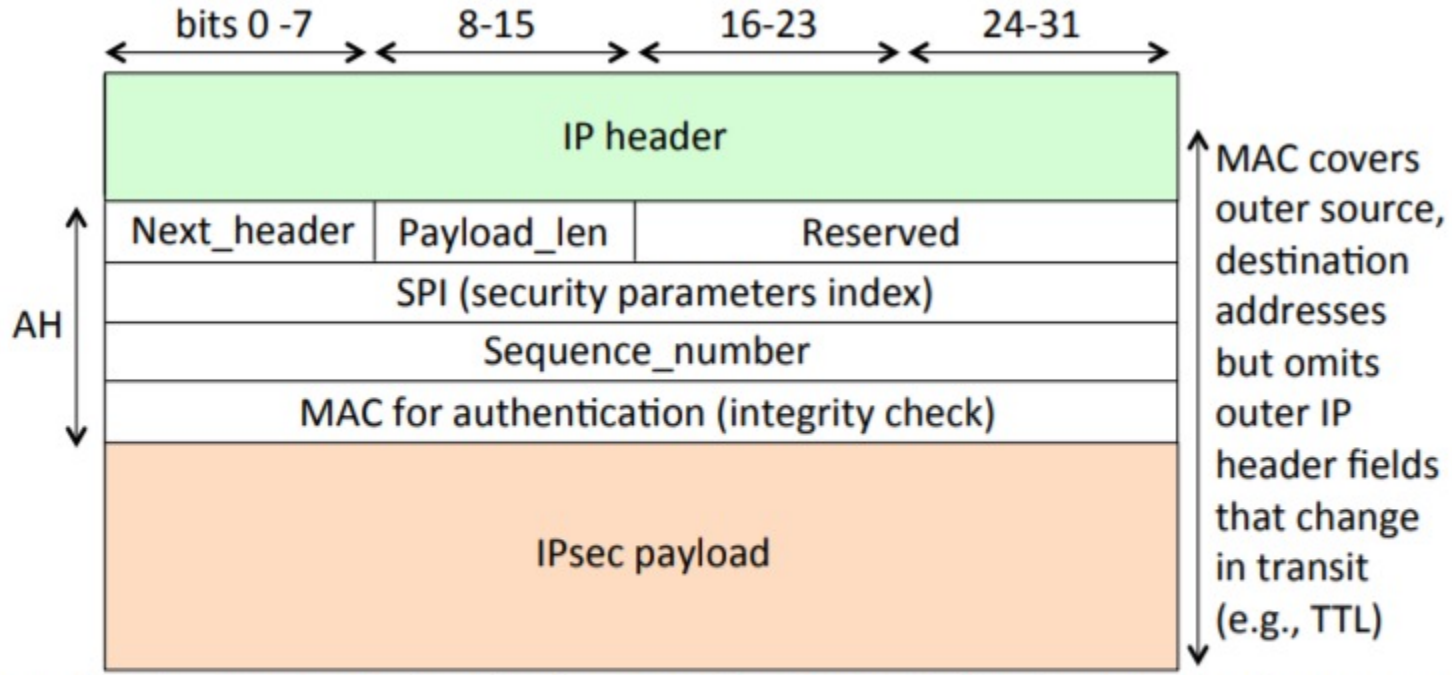


Figure 10.11: IPsec Authentication Header (AH) field view, for both transport and tunnel modes. `Next_header` identifies the protocol of the AH payload (e.g., TCP=6). `Payload_len` is used to calculate the length of the AH header. `SPI` identifies the Security Association. `Sequence_number` allows replay protection (if enabled).

# IPsec Encapsulating Security Payload

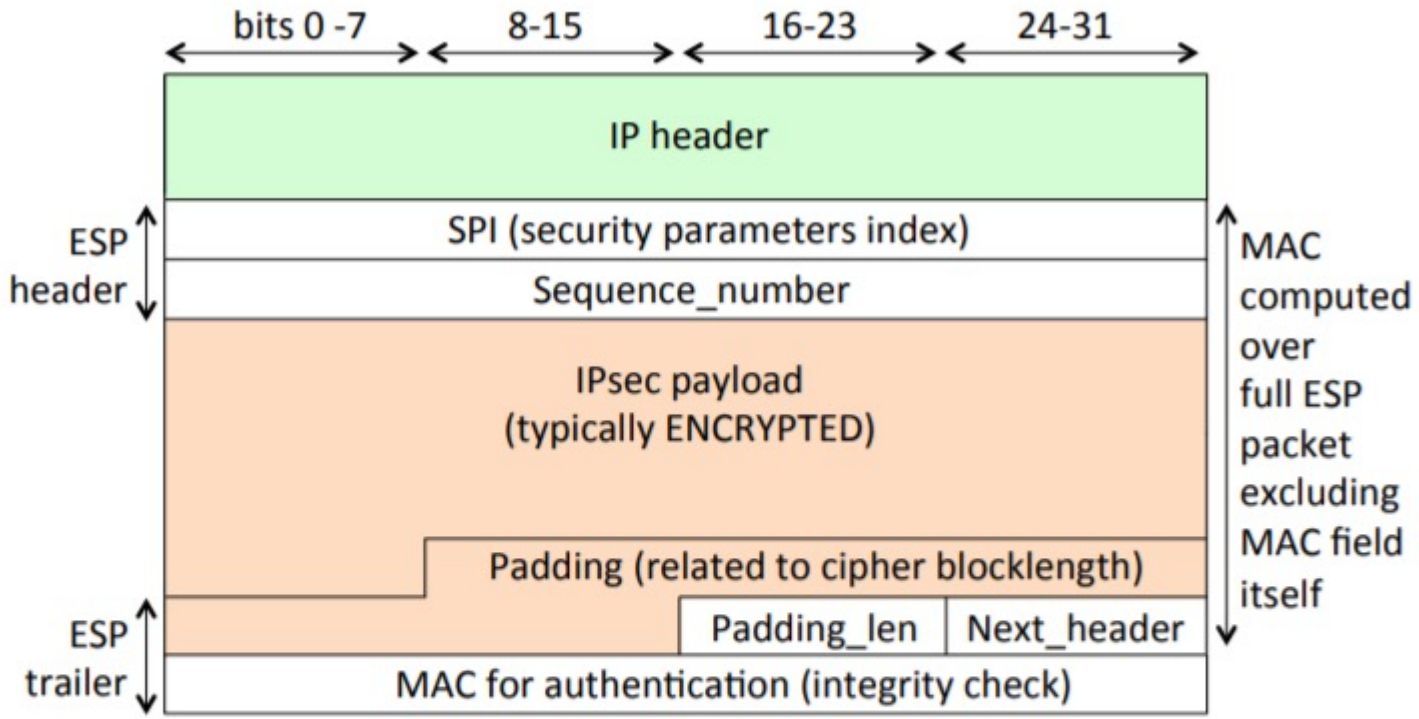


Figure 10.12: IPsec Encapsulating Security Payload (ESP) field view, for both transport and tunnel modes. `SPI` identifies the Security Association. `Sequence_number` allows replay protection (if enabled). `Next_header` (which may include a crypto IV or Initialization Vector) indicates the type of data in the ENCRYPTED field. A payload length field is not needed, as the ESP header is fixed at two 32-bit words, and the length of the IPsec payload (which is the same as that of the original payload) is specified in the IP header.

# IPsec Taşıma Modu ve Tünel Modu

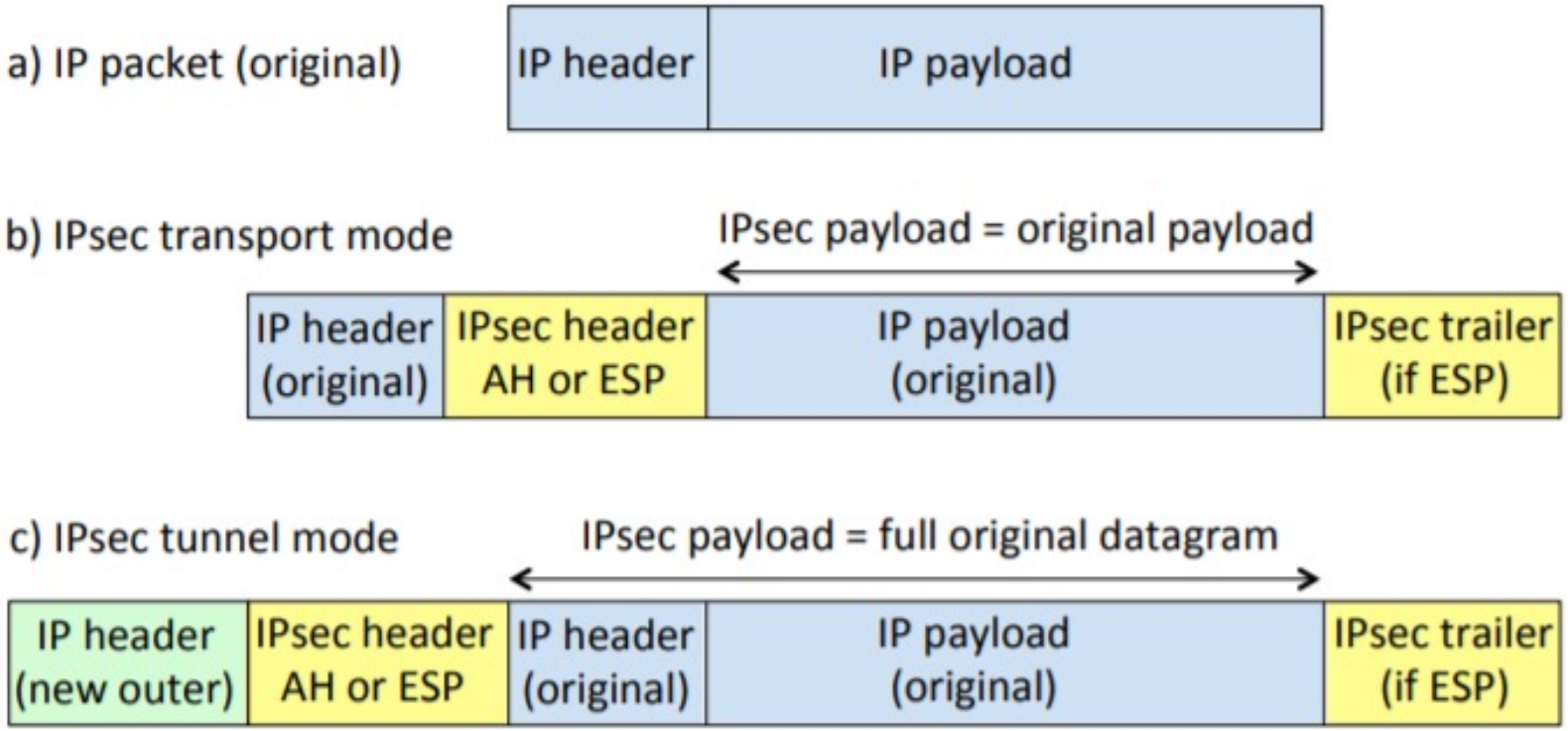


Figure 10.13: IPsec transport mode vs. tunnel mode (structural views).

# IPSec - Tartışma

- Ağ katmanında değişiklik gerektirdiği için TLS veya SSH'ye göre daha karmaşıktır ve uzmanlık gerektirir.
- IPsec politikaları ile tüm paketlerin VPN üzerinden gitmemesi sağlanabilir (politika tabanlı paket filtreleme).
- NAT ile IPSec'in uyumsuzluğu. Niye?