IPSEC

İnternet Protokol Güvenliği

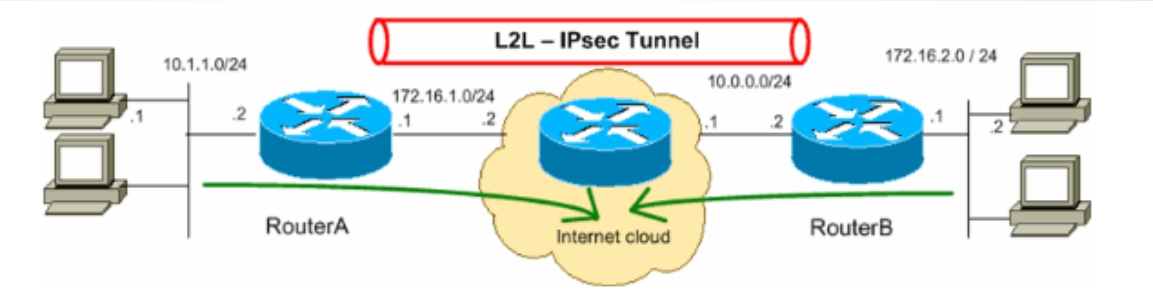
İçerik

Kısaltmalar

- AH: Authentication Header
- ESP: Encapsulating Security Payload
- SA: Security Association
- SAD: Security Association Database
- SPD: Security Policy Database
- IKE: Internet Key Exchange
- SPI: Security Parameter Index
- ICV: Integrity Check Value
- PA: Packet Accelerator

IPSEC NEDİR?

- Günümüzde network üzerinden veri alışverişi yapmanın doğurduğu pek çok güvenlik sorunu bulunmaktadır. “SYN flood”, “ICMP flood”, “teardrop attack” gibi DDOS atakları, “source spoofing” ve “playback attack” gibi pek çok kolay uygulanabilir metot ile kullanıcılar tehdit edilmektedir. Bu sorunu minimum seviyeye indirebilmek için “untrusted network” olarak nitelendirilen ağlar için IPsec protokolü kullanılmaktadır.
- IPsec, IP protokolü tabanlı çalışan haberleşme sistemlerinde peer’lar arasında tüneller oluşturarak IP paketlerinin authenticate ve/veya encrypt edilerek güvenliğinin sağlanması üzerine bir protokoldür.



IPsec Kullanım Nedenleri

- IPsec, IP protokolü tabanlı çalışan sistemlere firewall özelliği kazandırmaktadır. IPsec protokolü ile inbound ve outbound trafikte hangi paketlerin IPsec özelliği taşıyacağı (IPsec konfigürasyon bilgisine bağlı olarak), hangi paketlerin discard edileceği ya da hangi paketlerin bypass edileceği (IP datagramının herhangi bir değişikliğe uğramaması) belirlenmektedir. Genel olarak IPsec'in kullanım amaçları ve getirilerini aşağıdaki gibi listeleyebiliriz:
- IP paketlerinin source'unu verify etmek (authentication)
- Eski paketlerin tekrarını önlemek (anti-replay)
- Paketler için integrity ve/veya gizlilik sağlamak (data integrity/data encryption)

IPsec Security Protokolleri

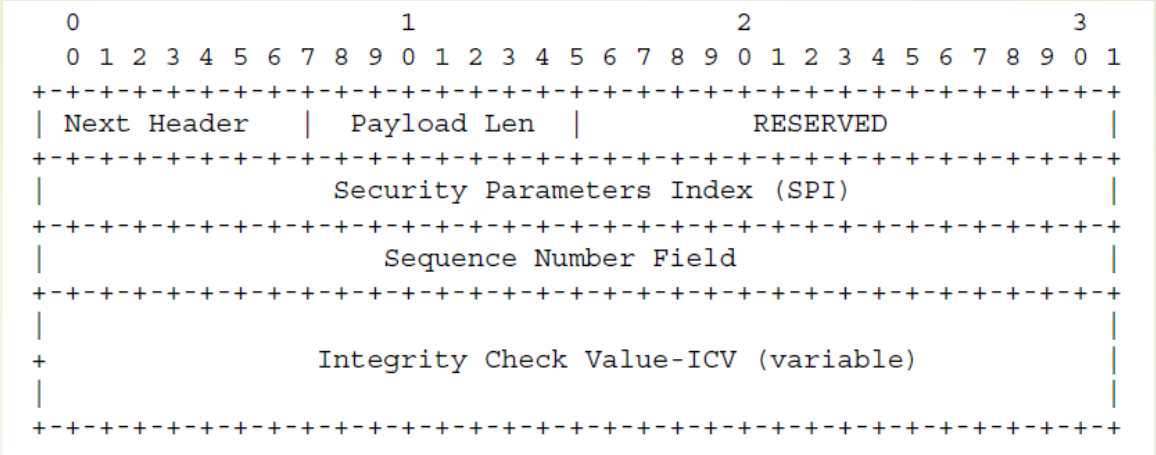
- Kullanılan protokole bağlı olarak, IP paketleri authenticate ya da encrypt edilebilmektedir. IPsec'te kullanılan protokoller, Authentication Header (AH) ve Encapsulating Security Payload (ESP) olmak üzere ikiye ayrılır.

AH Protokolü

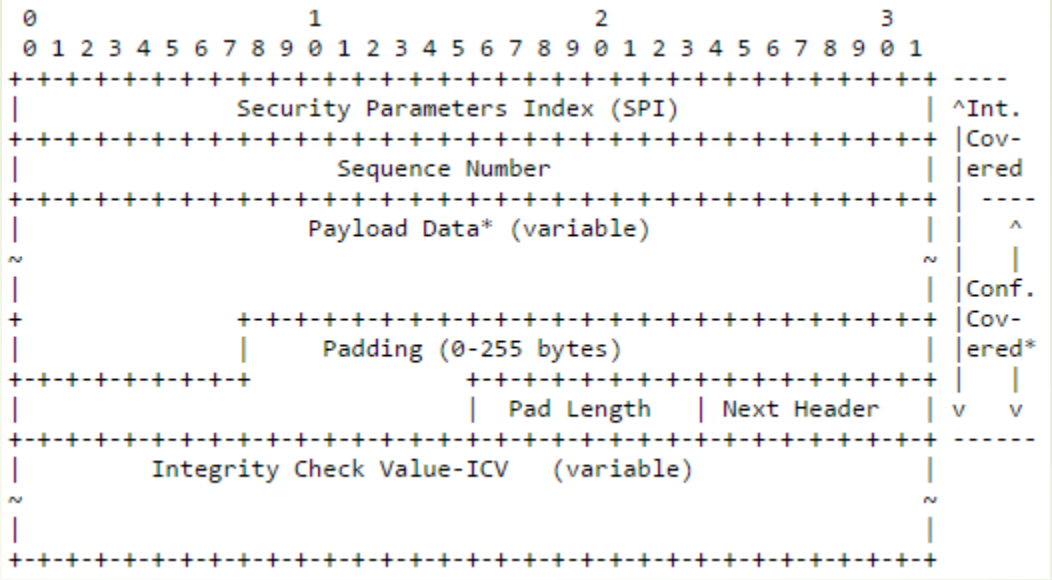
- AH protokolü, IP paketlerine data origin authentication, data integrity ve anti-replay koruması sağlamaktadır. IP paketi encrypt edilmediği için data gizliliği sağlamamaktadır. AH protokolü, datayı okunabilir ancak modifiye edilemez kılar.

ESP Protokolü

- ESP, IP paketlerine data origin authentication, data integrity, anti-replay koruması ve AH'tan farklı olarak data gizlilik sağlamaktadır. ESP protokolü ile IP paketinin belirli bir kısmı encrypt edilerek data gizliliği sağlanmaktadır.



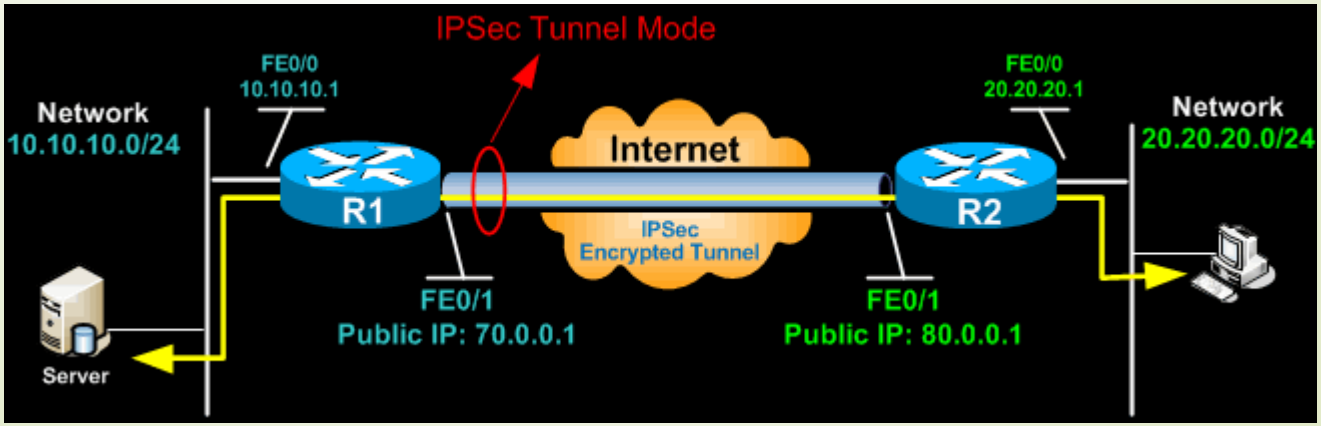
- Next Header: 8 bitlik bir alandır. AH Header'ını takip eden headerın tipini belirtir.
- Payload Len: Bu 8 bitlik alan, AH Header'ının uzunluğunu tutar.
- RESERVED: 16 bitlik reserved alandır.
- Security Parameter Index (SPI): 32 bitlik bir alandır. Inbound paketlerin hangi Security Association'a ait olduğu bilgisini tutar.
- Sequence Number Field: 32 bitlik bir alan olup aynı Security Association'a bağlı her paket için ardışık olarak artar.
- Integrity Check Value (ICV): Sabit bir boyutu olmamakla beraber 32 bitin katı olmalıdır (IPv4 ve IPv6). Bu alan her paket için data bütünlüğünün kontrolü için ICV değerini taşımaktadır.



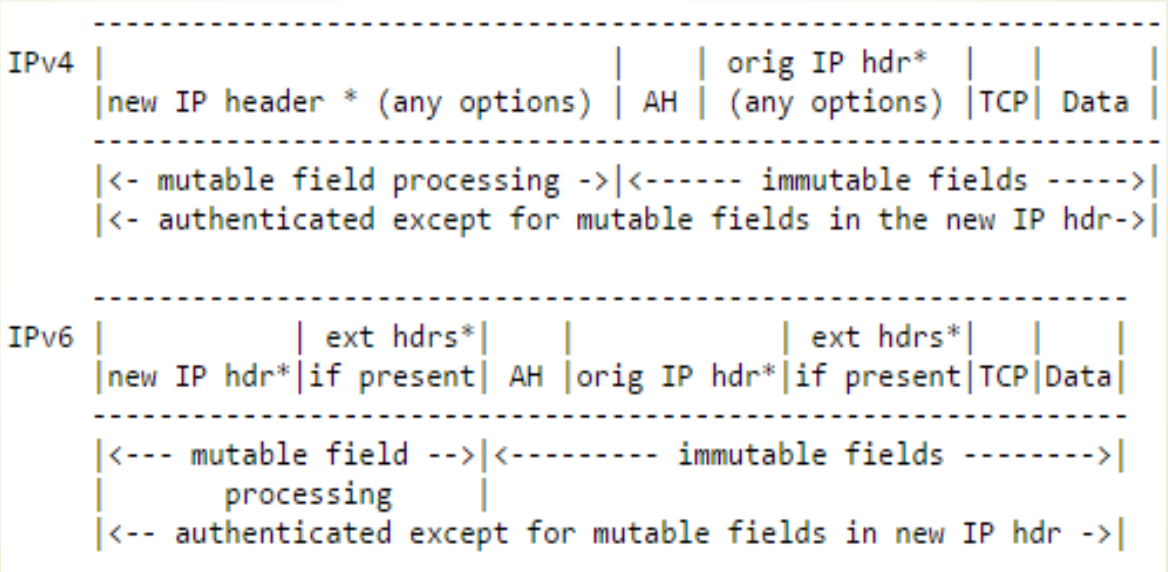
- SPI: 32 bitlik bir alandır. Inbound paketlerin hangi Security Association'a ait olduğu bilgisini tutar..
- Sequence Number: 32 bitlik bir alan olup aynı Security Association'a bağlı her paket için ardışık olarak artar.
- Initialization Vector: (IV) İlk 8 byte her encryption algoritması için sabittir. Sonrasında encryption algoritmasına gore değişken boyutlarda IV eklenir.
- Payload Data: ESP Header'ın uzunluğunu tutar.
- Padding: 0 – 255 byte arası padding yapılabilmektedir.
- Pad Length: Bu alanın boyutu 32 bitin katı olmalıdır.
- Next Header: 8 bitlik bir alandır. ESP Header'ını takip eden headerın tipini belirtir.
- Integrity Check Value: Sabit bir boyutu olmamakla beraber 32 bitin katı olmalıdır (IPv4 ve IPv6).

IPsec Modları

- IPsec, iki farklı modda konfigure edilebilir. Bu modlar "Tunnel Mode" ve "Transport Mode" 'dur. Her bir mod, ESP ve/veya AH protokolüne uygulanabilmektedir
- Tunnel Mode'un Transport Mode'dan farkı ise IP header'ının gizlenmesidir. Tunnel Mode ile orjinal paketin IP header'ı da encrypt edilebilirken Transport Mode'da sadece payload encrypt edilmektedir.

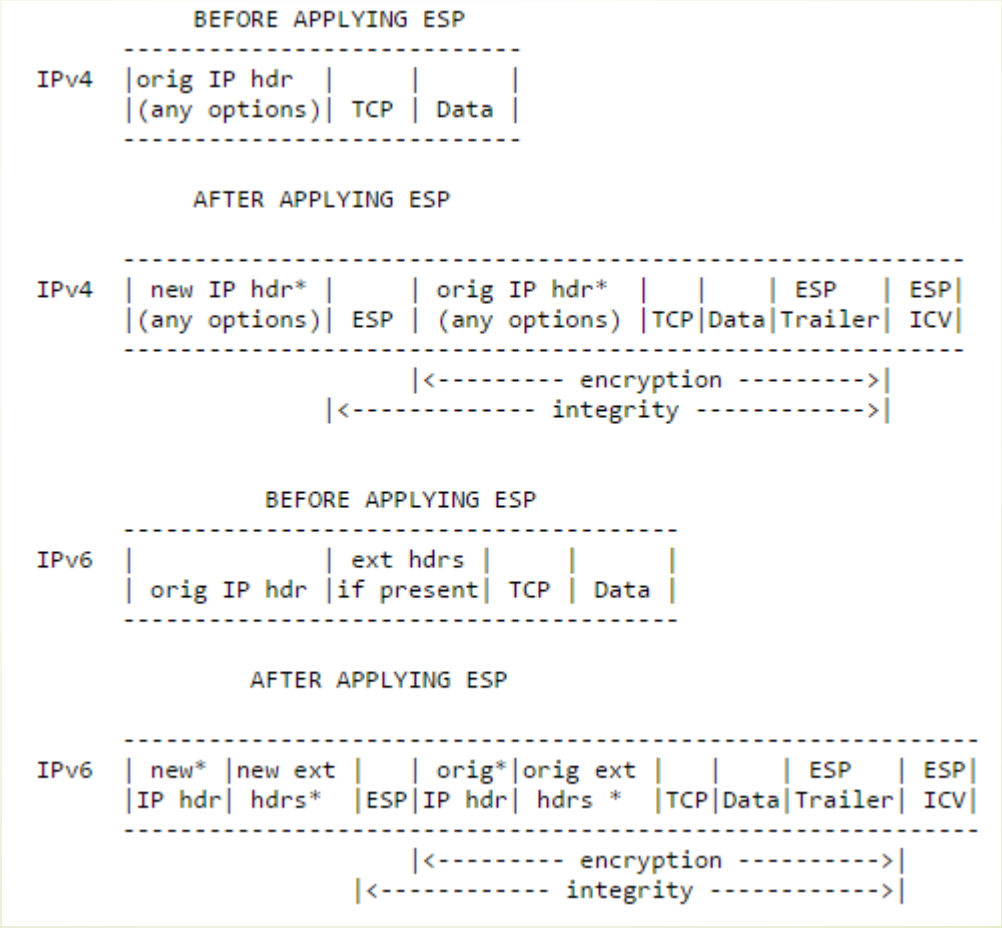


AH Protokolü ile Tunnel Mode'da Inner IP Header'ı ile Outer IP Header'ı arasına AH Header'ı gelmektedir. Bu konfigürasyonda paket, Şekil de görüldüğü üzere Outer IP Header'ından itibaren authenticate edilmektedir.



AH Tunnel Mode

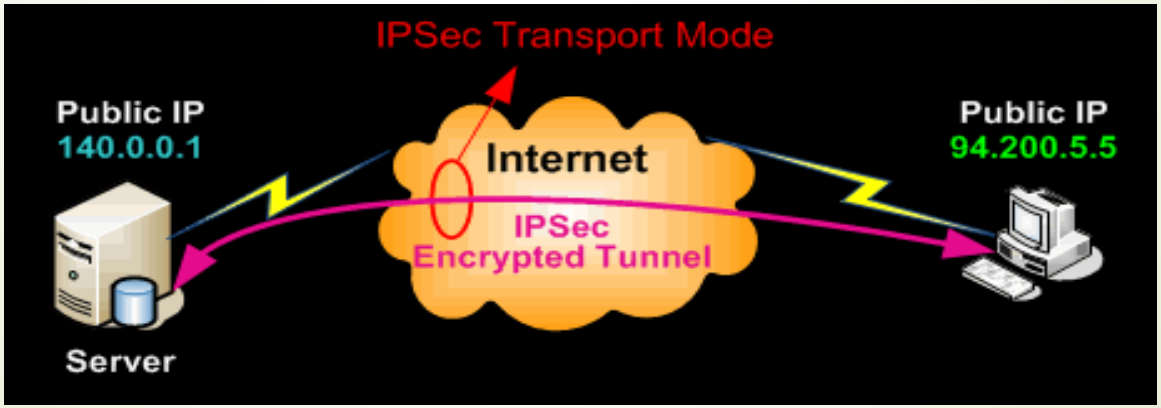
- ESP Protokolü ile Tunnel Mode'da Inner IP Header'ı ile Outer IP Header'ı arasına ESP Header'ı gelmektedir. Bu konfigürasyonda paket, Şekil de görüldüğü üzere ESP Header'ından itibaren authenticate, Inner IP Header'ından itibaren encrypt edilmektedir.



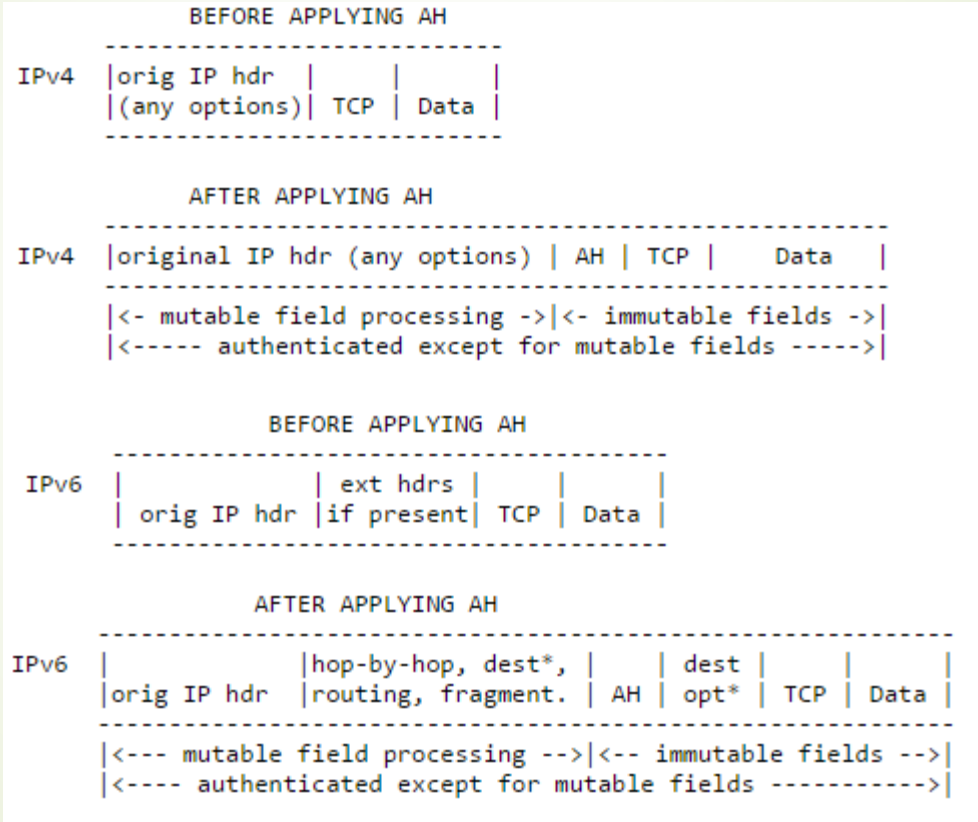
ESP Tunnel Mode

Transport Mode

- Transport Mode, sadece payload'u encrypt etmektedir, IP Header'ı üzerinde herhangi bir kriptolama işlemi yapılmamaktadır.

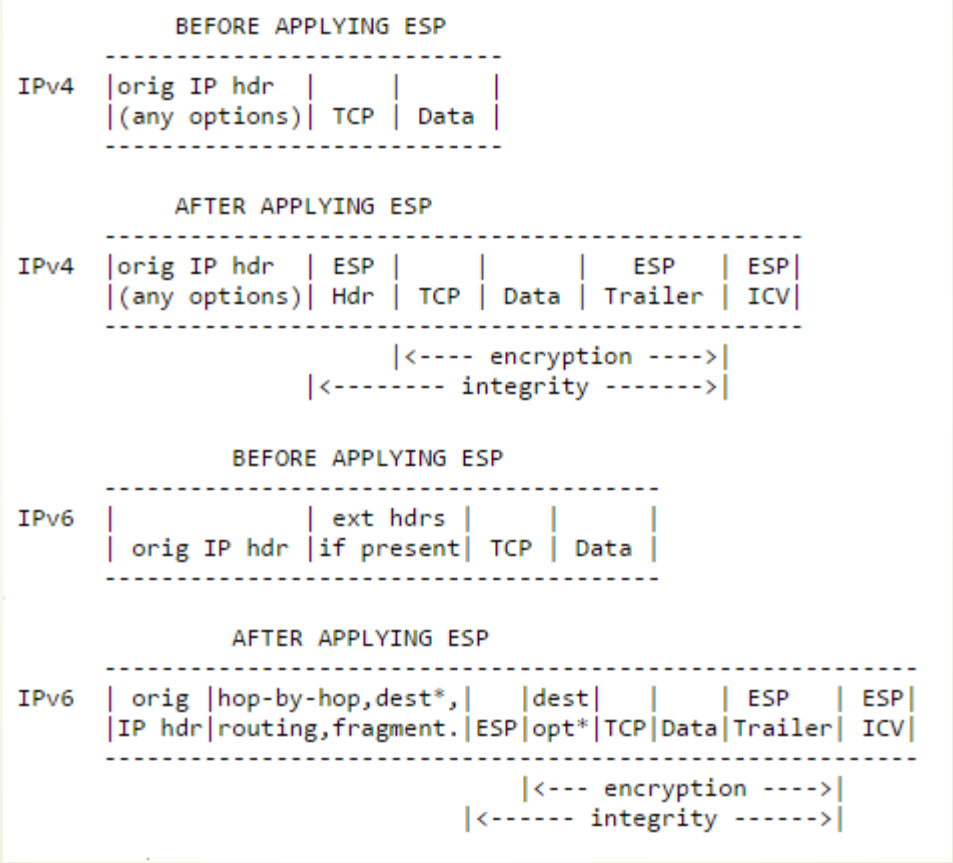


- AH Protokolü ile Transport Mode'da IP Header'ın ardına AH Header'ı gelmektedir. Bu konfigürasyonda paket, Şekil 4'te görüldüğü üzere IP Header'ından itibaren authenticate edilmektedir.

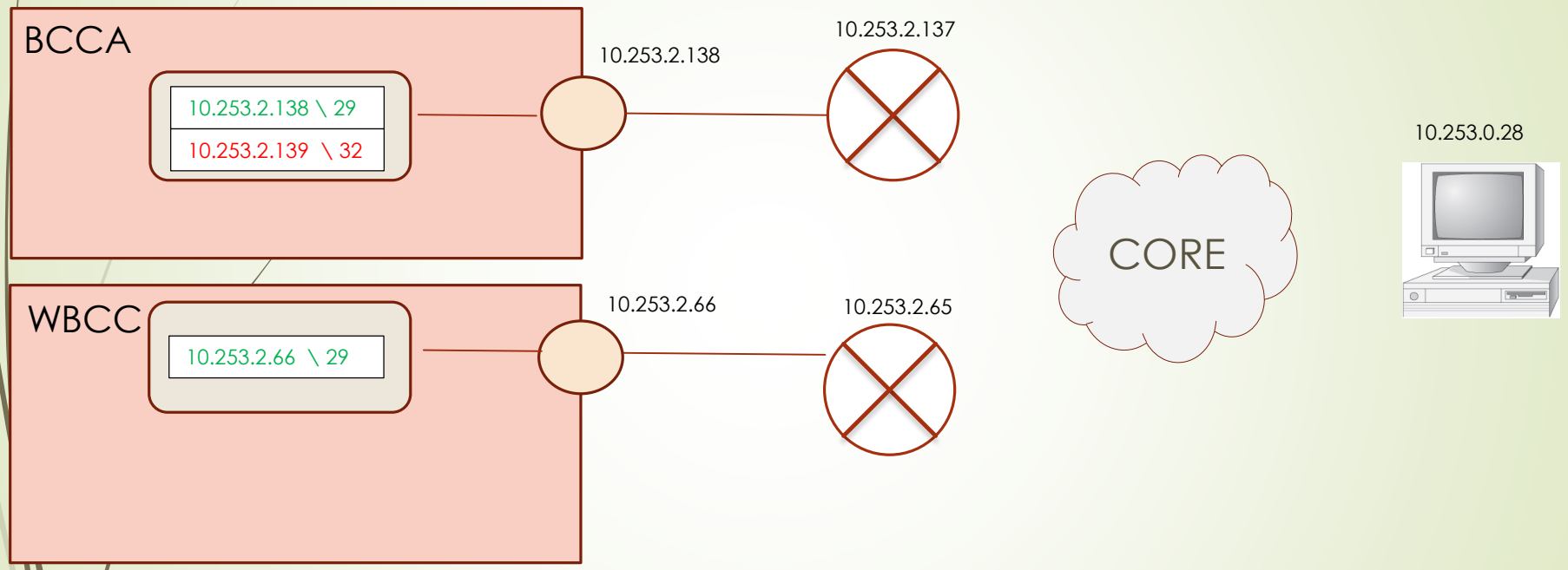


AH Transport Mode

- ESP Protokolü ile Tunnel Mode'da IP Header'ın ardına ESP Header'ı gelmektedir. Bu konfigürasyonda paket, Şekil de görüldüğü üzere ESP Header'ından itibaren authenticate, IP Header payload'ından itibaren encrypt edilmektedir.



ESP Transport Mode



Not: Her network cihazı için 3 menü ve bir terminal ekranı vardır.

I P v 4 I N T E R F A C E A D M I N I S T R A T I O N

Card Id : BCCA

Id	**IF Type**	**Ip Addr**	**\P**	**NEXT HOP**
00	BCCA	10.253.2.138	\29	10.253.2.137
01	IPSEC_INN	10.253.2.139	\32	-

I P v 4 P O L I C Y D A T A B A S E A D M I N I S T R A T I O N

Card Id : BCCA Policy Id : 0 / 59

IF Index : 1 Process Info: PROTECT Setup : MANUAL

S_Tunnel: 10.253.2.138 D_Tunnel: 10.253.2.66 NextHop: 10.253.2.137

TRAFFIC FLOW:

Idx	**Src Ip**	**\P**	**Dst Ip**	**\P**
00	10.253.2.139	\32	-	\-

qqqqqqqq I P v 4 M A N U A L S E C U R I T Y A S S O C I A T I O N qqqqqqq

Card Id	**:**	**BCCA**	**SA Index**	**:**	**0**
IF Id	:	0	SrcTunnel IP:		10.253.2.138
DstTunnel IP:		10.253.2.66	Direction	:	BOTH
Protocol	:	ESP	Mode	:	TUNNEL

OUTBOUND

SPI	:	1234			
AUTH KEY	:	12345678912345678912	AUTH TYPE	:	HMAC_SHA1
ENC KEY	:	1234567891234567	ENC TYPE	:	AES_CBC

INBOUND

SPI	:	1234			
AUTH KEY	:	12345678912345678912	AUTH TYPE	:	HMAC_SHA1
ENC KEY	:	1234567891234567	ENC TYPE	:	AES_CBC

ÖNEMLİ

Bu projeler lisansüstü öğrencilerinin hazırladığı çalışmalar olup tüm sorumluluk hazırlayan öğrencilere aittir. Öğrenciler hazırladığı projeye göre not almışlardır.