به نام خدا

دانشکده مهندسی برق،
دانشگاه صنعتی شریف

مبانی رمزنگاری و امنیت شبکه

امنیت IP

IP Security

مهتاب میرمحسنی

نیم‌سال دوم (بهار) ۹۸-۹۹

امنیت IP

- خدمات امنیتی بر اساس کاربرد
  - ایمیل: S/MIME, PGP
  - کلاینت/سرور: Kerberos
  - دسترسی به وب: SSL

- برخی نیازهای امنیتی در سطح لایه IP هستند
  - شبکه IP امن که امکان دسترسی به سایت‌های غیرمجاز را نمی‌دهد و بسته‌های ارسالی را رمز و دریافتی را احراز اصالت می‌کند
  - تامین امنیت برای تمامی کاربردها (برخی ممکن است امنیت را پیاده‌سازی نکرده باشند)

امنیت IP

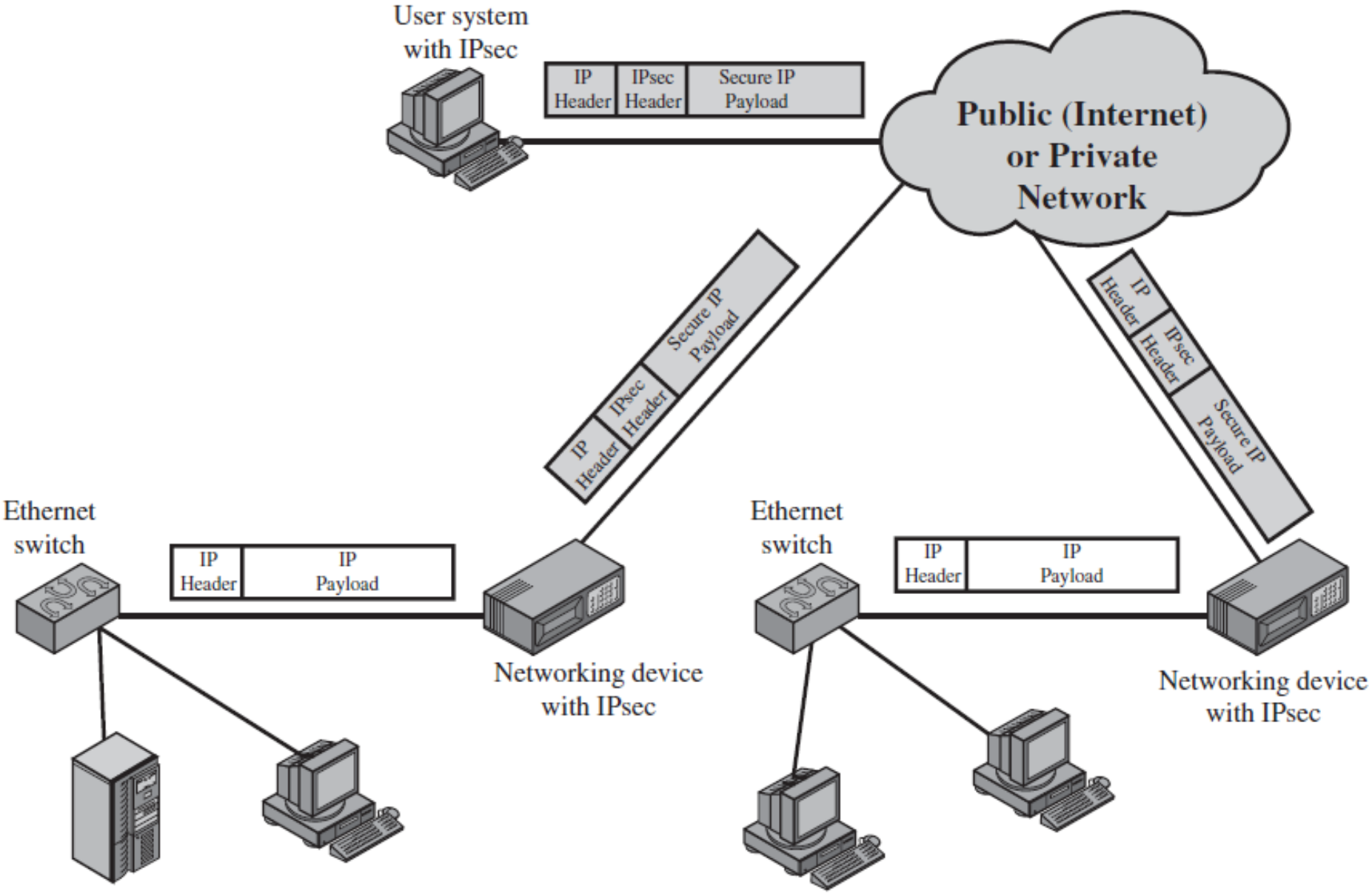
- IPsec
- ۳ قابلیت زیر را دارد:
  - احراز اصالت پیام و منبع (فرستنده بسته مطابق با سرآیند است)
  - محرمانگی
  - مدیریت کلید (مبادله امن کلیدها)

- پیاده‌سازی امنیت در IPv6 الزامی است
  - قابل پیاده‌سازی در IPv4 نیز است
  - برخی استانداردها نیز مطرح شده است

کاربردهای IPsec

- ایجاد شبکه خصوصی مجازی (VPN) در اینترنت یا WAN توسط یک شرکت یا سازمان
  - نیاز به شبکه خصوصی را کاهش می‌دهد (کاهش هزینه)
  - امکان اتصال کارمندان از راه دور با استفاده از پروتکل IPsec به این شبکه نیز وجود دارد
- امکان ایجاد ارتباط امن میان چندین سازمان
- افزایش میزان امنیت در کاربردهایی که امنیت در لایه کاربرد را پیاده‌سازی کرده‌اند
  - به ویژه در کاربردهای تجارت الکترونیکی

یک سناریو از استفاده IPsec



خدمات IPsec

- خدمات امنیتی در سطح IP با انتخاب پروتکل‌های امنیتی لازم، الگوریتم‌ها، کلیدها
  - کنترل دسترسی (Access control)
  - یکپارچگی در ارتباط بدون اتصال (Connectionless integrity)
  - احراز اصالت منبع (Data origin authentication)
  - رد بسته‌های تکراری (Rejection of replayed packets)
  - محرمانگی (رمزنگاری)
  - محرمانگی شار ترافیک به صورت محدود (Limited traffic flow confidentiality)
- ۲ پروتکل مهم
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

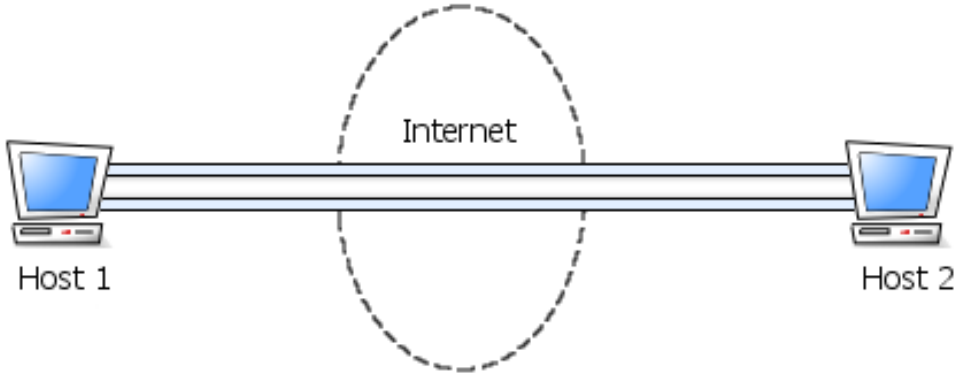
سبک‌های IPsec

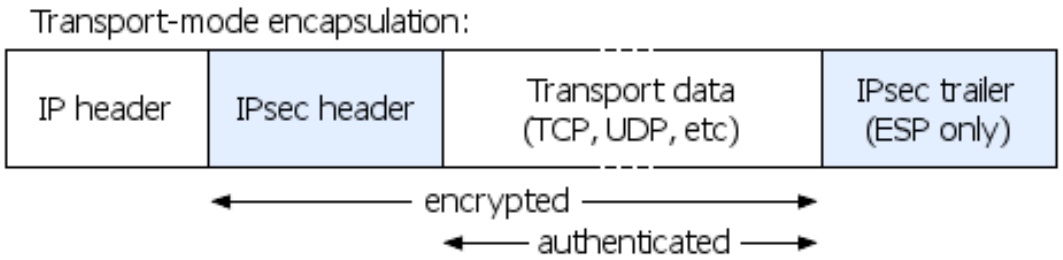
هر دو پروتکل امنیتی AH و ESP از دو سبک زیر پشتیبانی می‌کنند:

- سبک انتقال (Transport Mode)
  - امنیت برای پروتکل‌های لایه بالاتر
  - تغییرات روی محتوای بسته صورت می‌گیرد
- سبک تونل (Tunnel Mode)
  - امنیت بر روی کل بسته IP
  - تغییرات روی محتوای بسته + سرآیند صورت می‌گیرد ← بسته جدید

سبک انتقال (Transport Mode)

- محتوا (payload) بسته IP تغییر می‌یابد
- مناسب برای ارتباط انتها-به-انتها میان دو میزبان
  - کلاینت/سرور یا دو ایستگاه کاری
- ESP: رمزنگاری (الزامی) و احراز اصالت (اختیاری) محتوای بسته IP (بدون سرآیند)
- AH: احراز اصالت محتوای بسته IP و بخش‌هایی از سرآیند IP



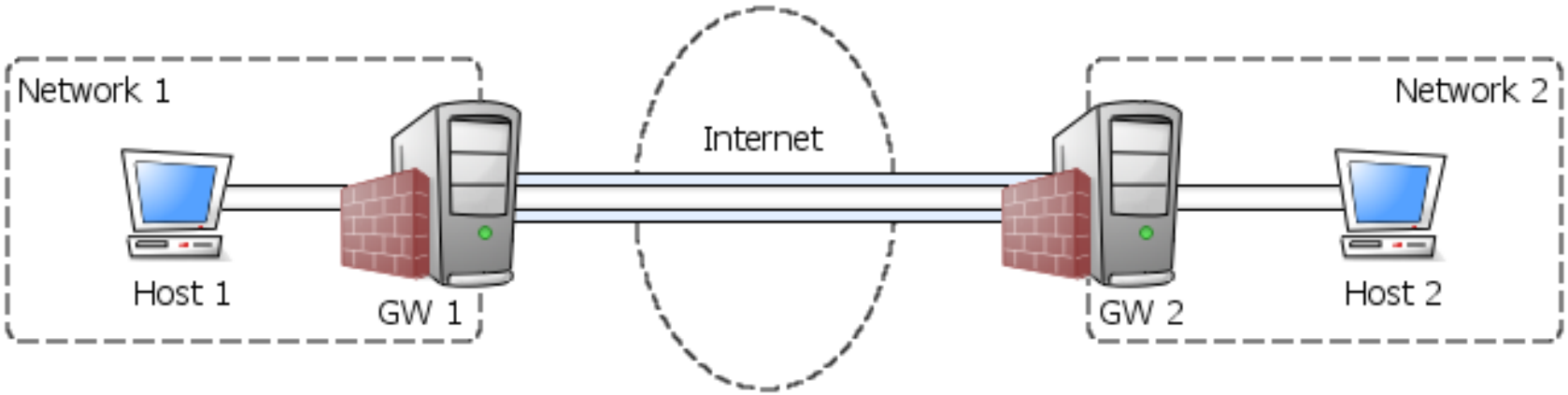


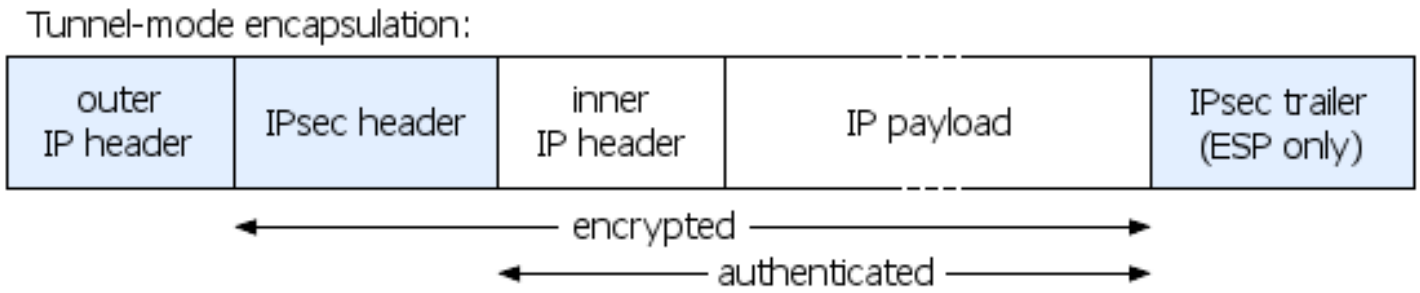
سبک تونل (Tunnel Mode)

- امنیت بر روی کل بسته IP
- پس از افزودن بخش‌های AH یا ESP به بسته IP، تمامی بسته (به همراه بخش‌های امنیتی) به عنوان محتوای (payload) یک بسته جدید IP در نظر گرفته می‌شود ← بسته جدید با سرآیند جدید
  - بسته درونی در یک تونل منتقل می‌شود و مسیریاب‌های میانی قادر به تشخیص سرآیند آن نیستند
  - افزایش امنیت: آدرس‌های IP بسته جدید ممکن است متفاوت باشد (بسته به محل اجرای IPsec)
- کاربرد در ارتباطی که حداقل یکی از طرفین دروازه (gateway) باشد
  - مثلا مسیریاب یا دیوار آتش

سبک تونل (Tunnel Mode)

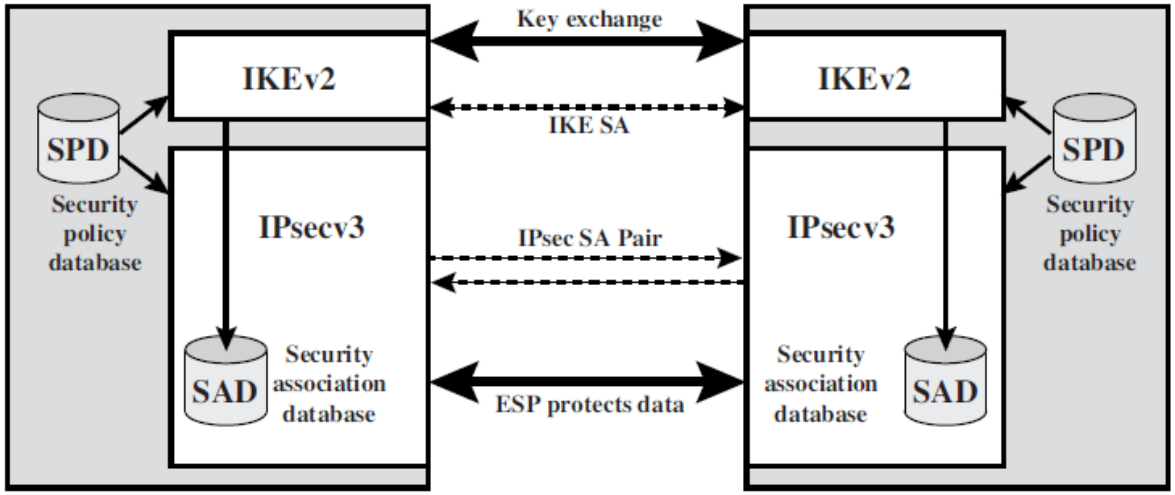
- ESP: رمزنگاری (الزامی) و احراز اصالت (اختیاری) کل بسته IP درونی (شامل سرآیند)
- AH: احراز اصالت کل بسته IP درونی (شامل سرآیند) و بخش‌هایی از سرآیند بسته IP بیرونی





خط‌مشی امنیتی IP

- خط‌مشی اعمالی به هر بسته IP بر اساس دو پایگاه داده
  - پایگاه داده پیمان امنیتی: security association database (SAD)
  - پایگاه داده خط‌مشی امنیتی: security policy database (SPD)
- پیمان امنیتی: security association (SA)
  - یک ارتباط یک طرفه میان فرستنده و گیرنده برای ایجاد ترافیک امن (متعلق به AH یا ESP)
  - برای ایجاد ارتباط همتا-به-همتا نیاز به دو SA داریم



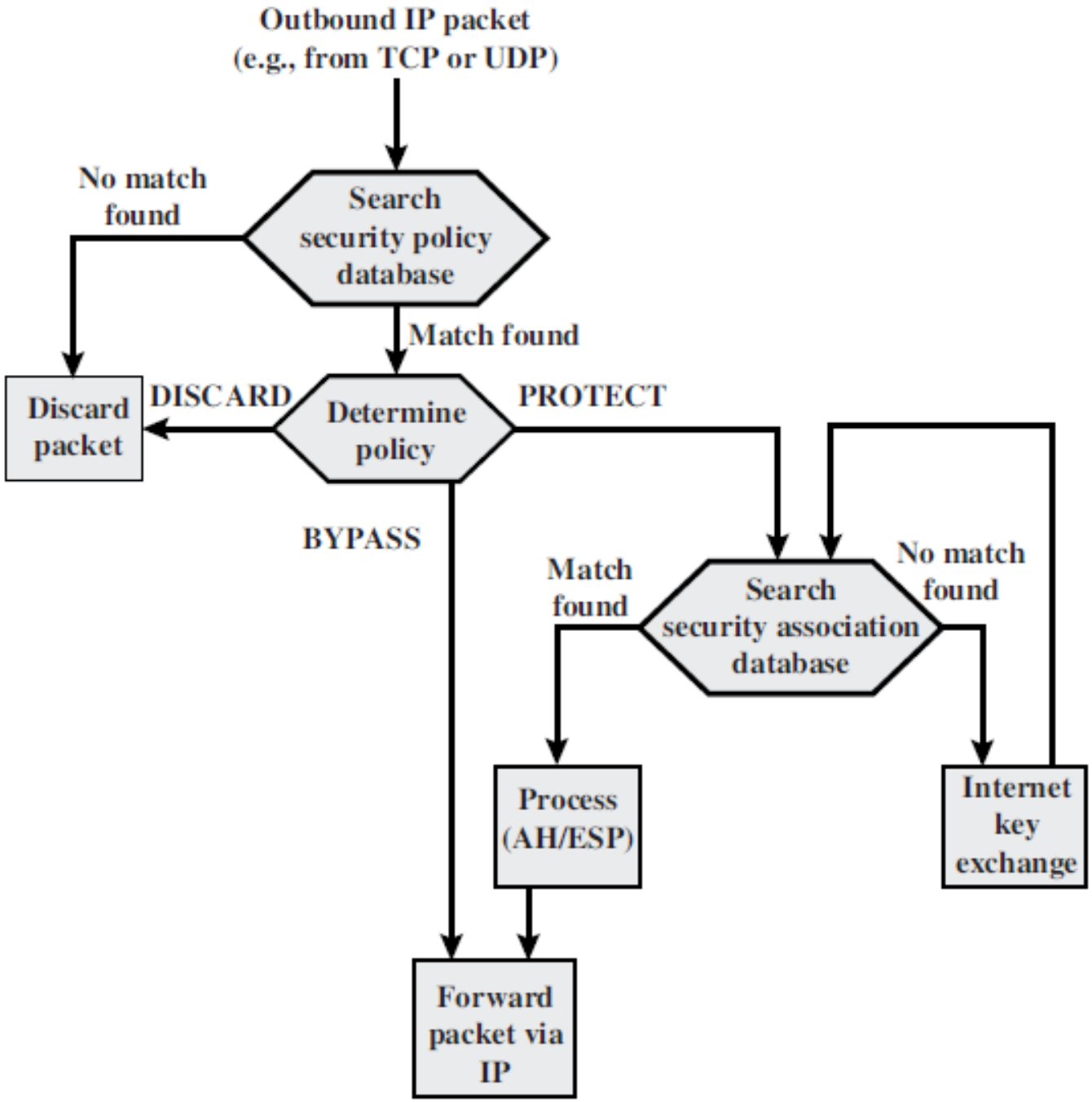
پارامترها:

- Security Parameters Index (SPI): گیرنده بفهمد که بسته متعلق به کدام SA است
- IP Destination Address
- Security Protocol Identifier: AH یا ESP

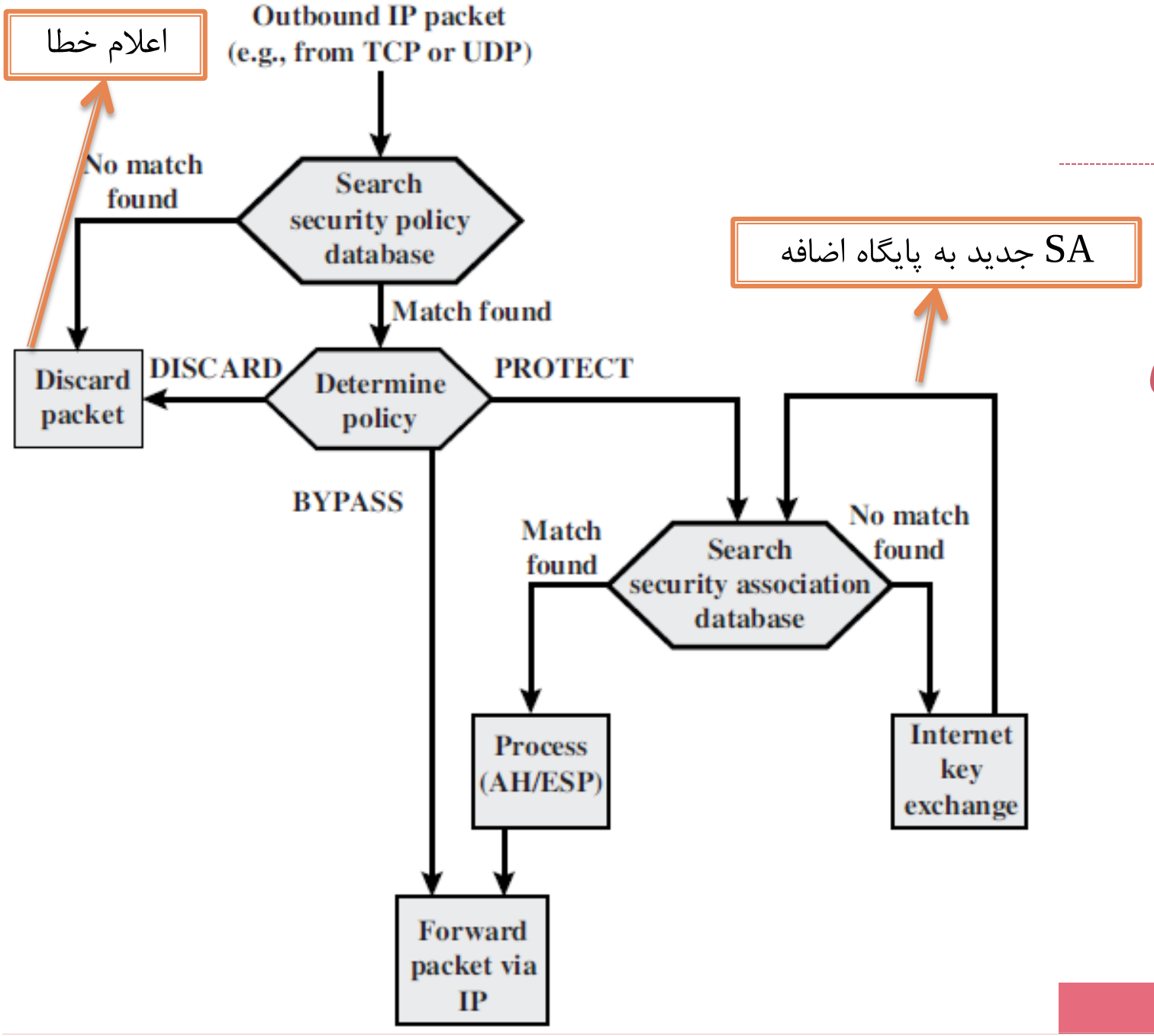
پایگاه داده خط‌مشی امنیتی: security policy database (SPD)

- کدام SA و به چه صورت به ترافیک IP پاسخ دهد
- با مقدار انتخابگر در سرآیند بسته IP، SA مورد نظر در پایگاه داده SPD مشخص می‌شود (در صورت وجود)
  - Local IP Address، Remote IP Address، Next Layer Protocol، Name، Local and Remote Ports
- سپس پردازش IPsec (AH یا ESP) بر روی آن بسته اعمال می‌شود

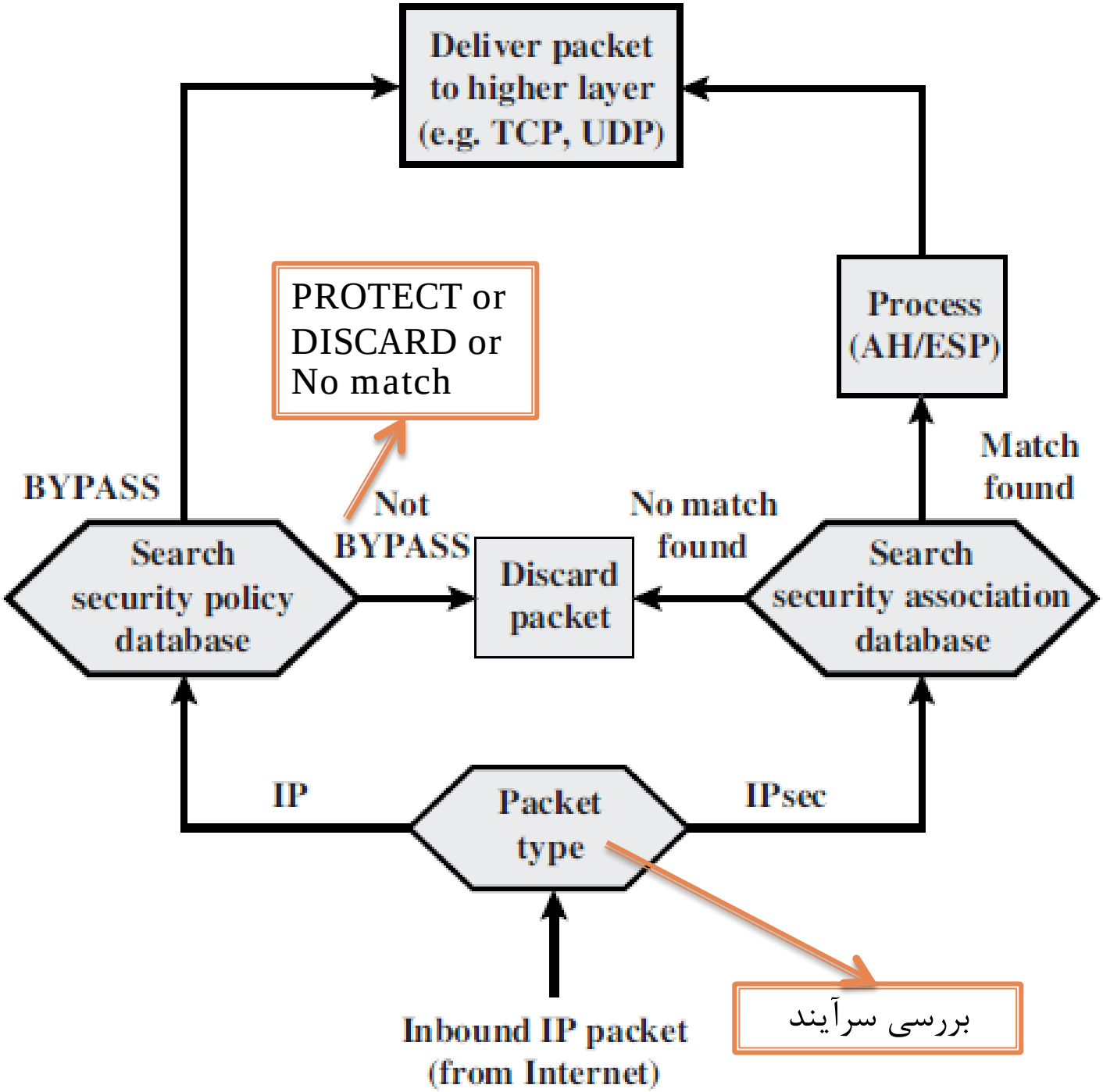
بسته‌های ارسالی



بسته‌های ارسالی

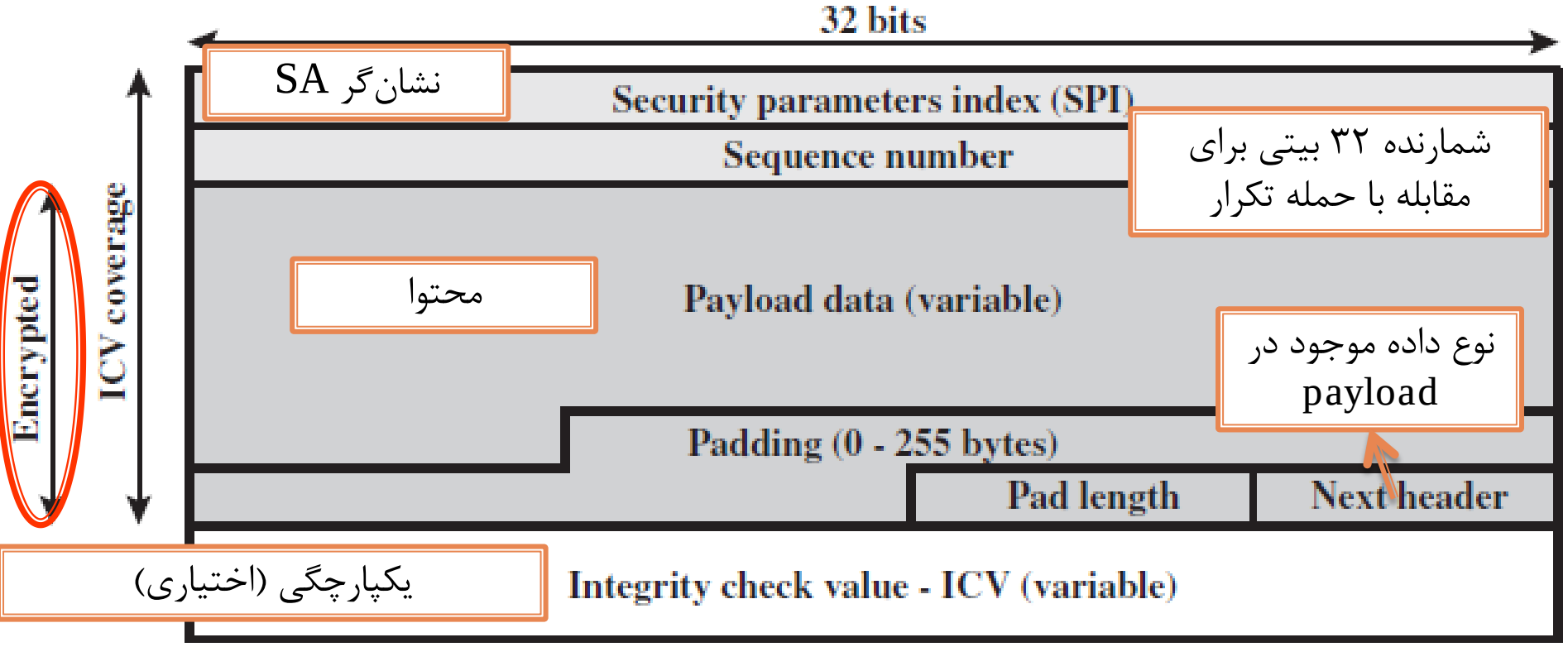


بسته‌های دریافتی

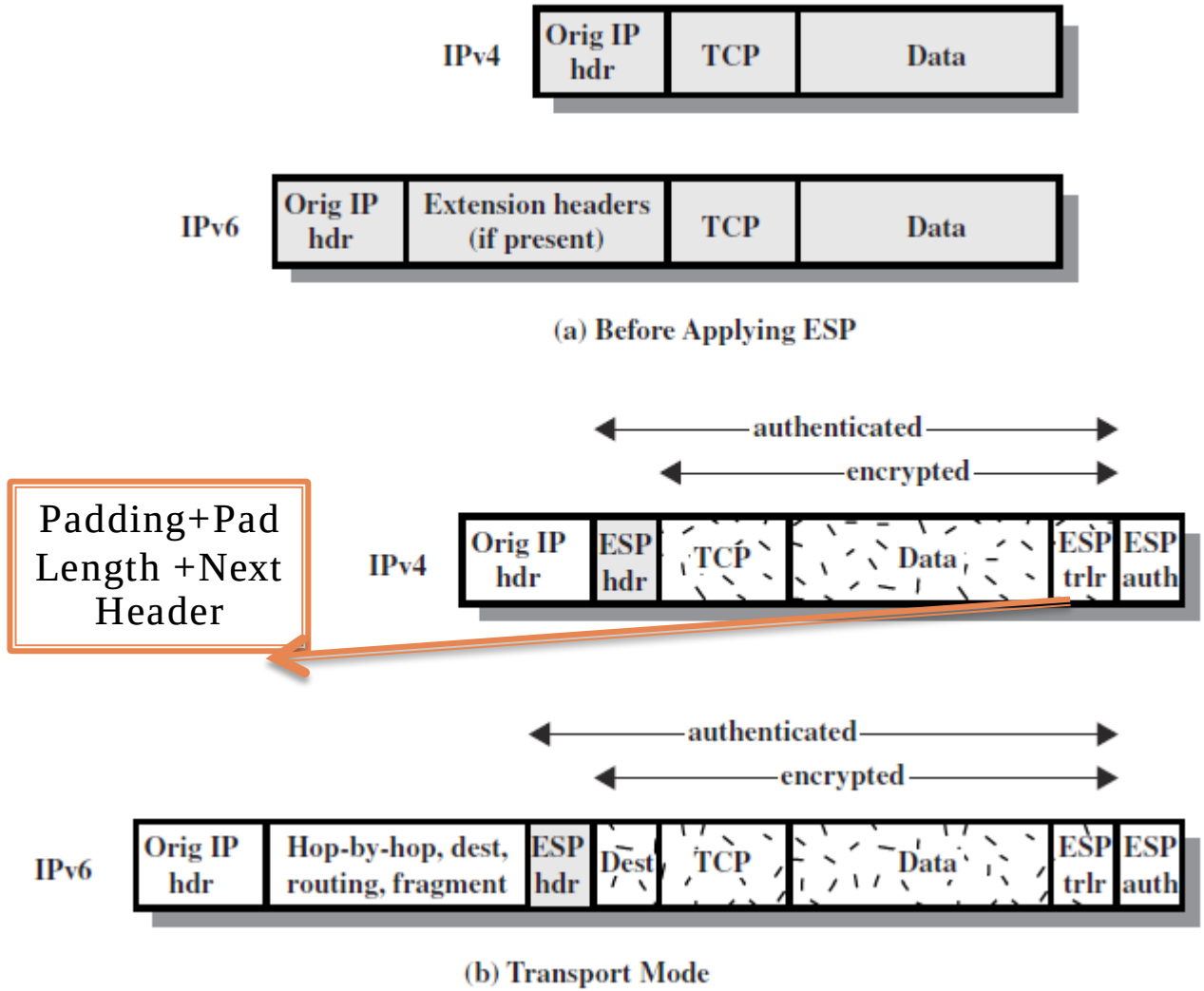


Encapsulating Security Payload (ESP)

- محرمانگی، احراز اصالت منبع، یکپارچگی در ارتباط بدون اتصال، خدمت ضد تکرار، محرمانگی شار ترافیک به صورت محدود
  - در زمان ایجاد SA انتخاب می‌شوند



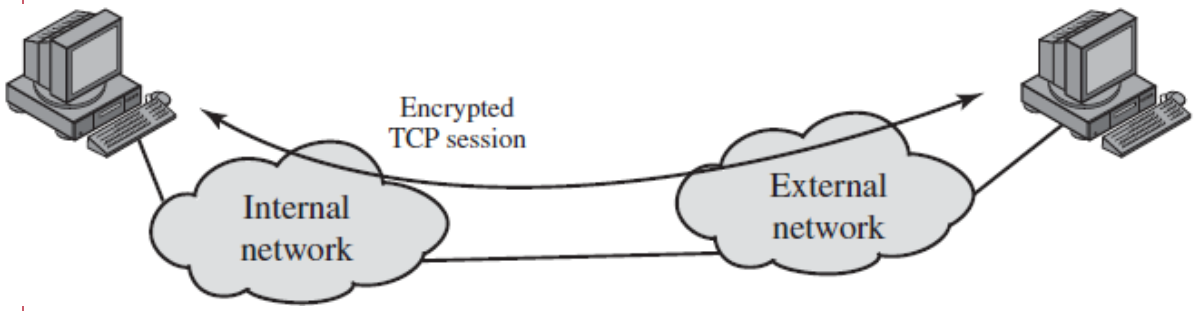
سبک انتقال در ESP
Transport mode ESP

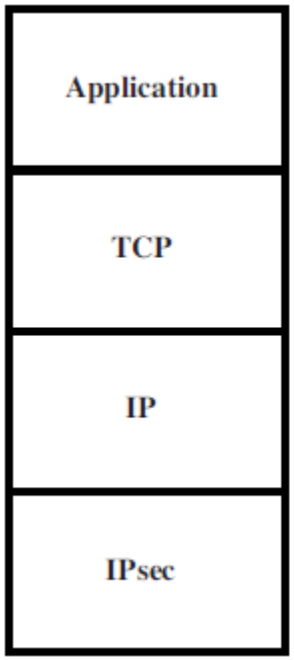


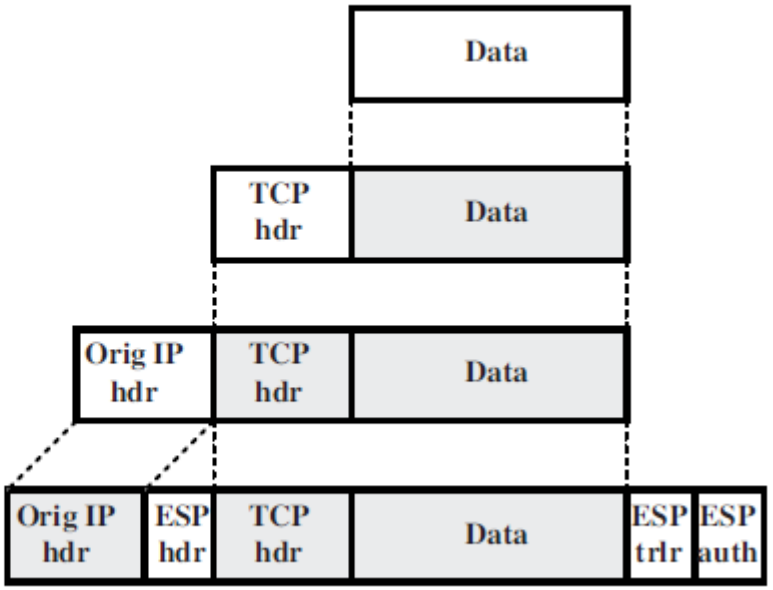
- مسیریاب‌های میانی سرآیندها (IP و ESP) را بررسی می‌کنند ولی نیازی به رمزگشایی ندارند
- گیرنده انتهایی با استفاده از SPI در سرآیند ESP رمزگشایی می‌کند
- تحلیل ترافیک بسته‌های ارسالی ممکن است

سبک انتقال در ESP

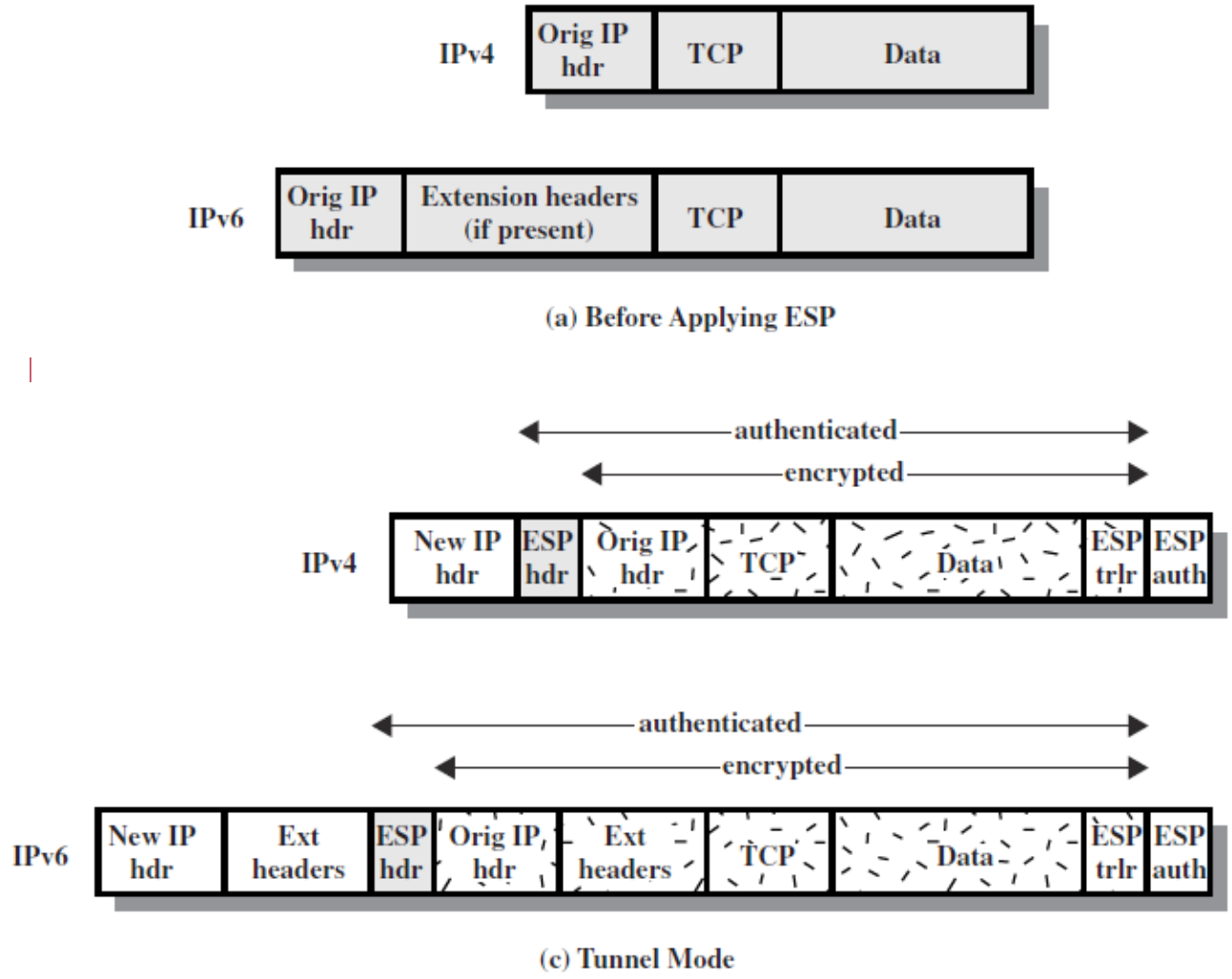
- مناسب برای ارتباط میزبان‌ها





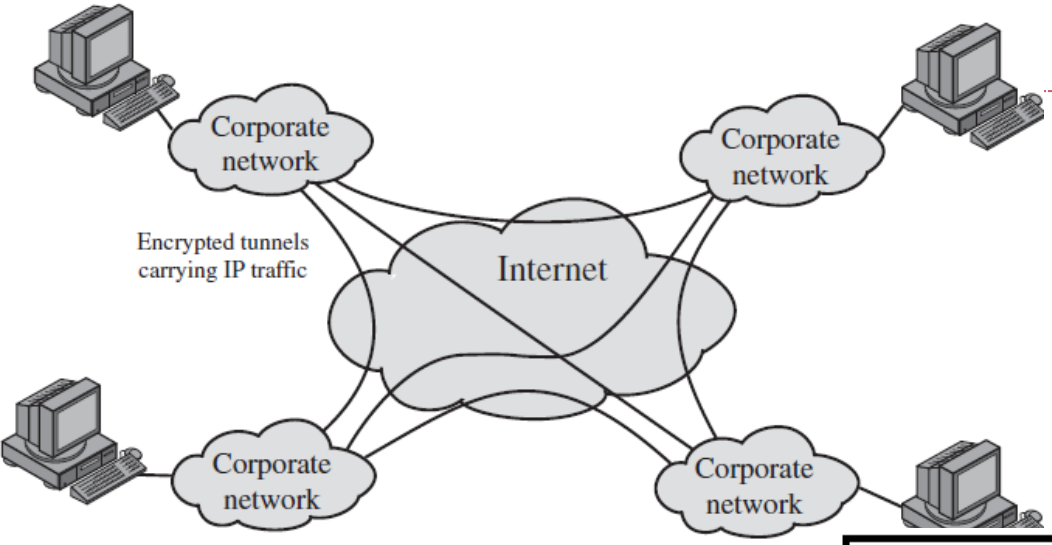


سبک تونل در ESP



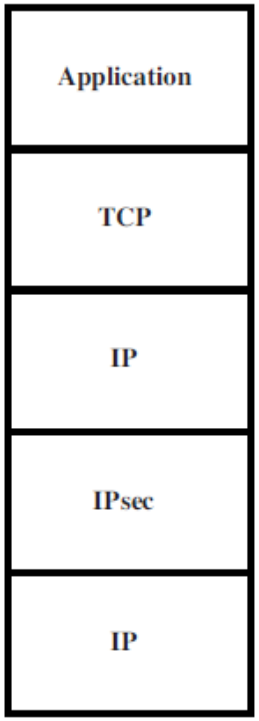
- اضافه کردن سرآیند جدید
- لفافه بندی بسته قبلی (encapsulating)
- مسیریاب‌های میانی از سرآیند جدید استفاده می‌کنند
- مقابله با حمله تحلیل ترافیک
- پس از رسیدن به دروازه مقصد، رمزگشایی شده و مسیریابی از روی سرآیند اصلی تا گیرنده انتهایی صورت می‌گیرد

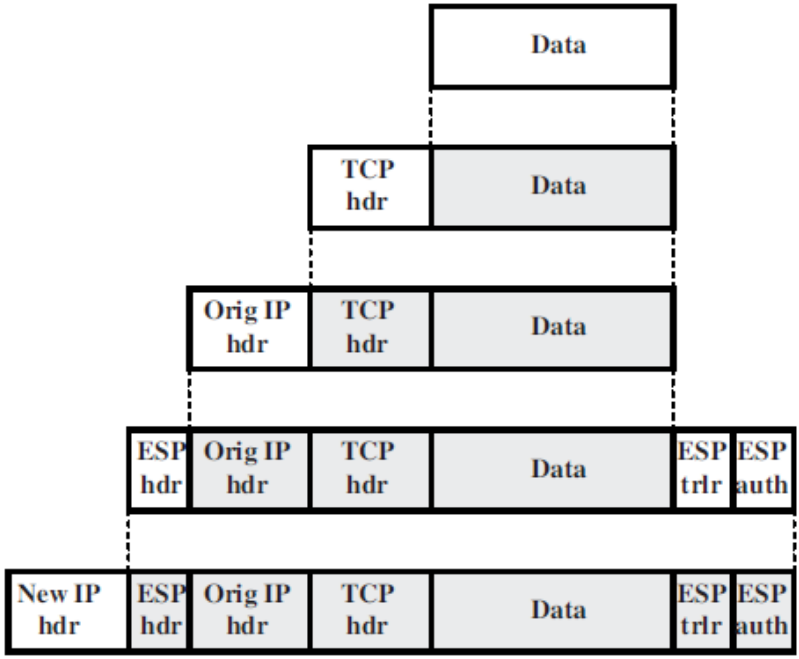
سبک تونل در ESP



(b) A virtual private network via tunnel mode

- ارتباط دروازه-به-دروازه
- ایجاد شبکه خصوصی مجازی (VPN)





ترکیب SAها

- ترکیب SAها بر روی یک بسته ← bundle
  - هر SA، تنها یکی از AH یا ESP را پیاده‌سازی می‌کند (ترکیب برای استفاده از هر دو)
  - ممکن است خدمت درخواستی یک ترافیک میان میزبان‌ها و یا دروازه‌ها متفاوت باشد
- به ۲ روش:
- Transport Adjacency
  - اعمال IPsec در گیرنده انتهایی
  - چند SA در سبک انتقال (تونل لازم نیست): یک لایه
- Iterated Tunneling
  - چند لایه از پروتکل‌های امنیتی با سبک تونل (تو در تو)
  - مبدا و مقصد هر تونل می‌توانند متفاوت باشند

مدیریت کلید در IPsec

- نیاز به ۴ کلید مخفی: محرمانگی و یکپارچگی (ارسال و دریافت)
- مستندات از ۲ روش پشتیبانی می‌کنند:
  - دستی: قابل استفاده در سیستم‌های کوچک و محیط‌های نسبتاً ایستا
  - خودکار: تولید کلید خودکار بر حسب تقاضا برای SAها
    - پروتکل ISAKMP/Oakley (Internet Security Association and Key Management Protocol) ← IKEv1 و IKEv2
- پروتکل Oakley
  - بر اساس توزیع کلید دیفی-هلمن (با امنیت بیشتر)
- پروتکل ISAKMP
  - تعریف ساختارهای بسته‌ها و پیام‌ها
  - در اصل پروتکلی را معین نمی‌کند

پروتکل Oakley
مقابله با حمله انسداد (Clogging)

- مهاجم با جعل آدرس یک فرستنده قانونی، درخواست مکرر مبادله کلید DH را می‌دهد
  - با توجه به حجم پردازشی، منابع قربانی تلف می‌شود
- هر یک از طرفین در ابتدا یک عدد تصادفی (کلوچک) می‌فرستد
- طرف مقابل دریافت آن را با ارسال ack تایید می‌کند
- این کلوچک باید در پیام اولیه DH تکرار شود
  - در غیر این صورت درخواست مبادله کلید پذیرفته نمی‌شود
- با توجه به آدرس جعلی، مهاجم ack را دریافت نمی‌کند و نمی‌تواند درخواست بدهد

الگوریتم‌های رمزنگاری
RFC 4308

- جهت ایجاد شبکه خصوصی مجازی (VPN)

IKEv1

IPsecv3+IKEv2
قوی‌تر

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC (128-bit key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC (128-bit key)
IKE PRF	HMAC-SHA1	AES-XCBC-PRF-128
IKE Integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH group	1024-bit MODP	2048-bit MODP

الگوریتم‌های رمزنگاری
RFC 6379

- سازگار با United States National Security Agency

	GCM-128	GCM-256	GMAC-128	GMAC-256
ESP encryption/Integrity	AES-GCM (128-bit key)	AES-GCM (256-bit key)	Null	Null
ESP integrity	Null	Null	AES-GMAC (128-bit key)	AES-GMAC (256-bit key)
IKE encryption	AES-CBC (128-bit key)	AES-CBC (256-bit key)	AES-CBC (128-bit key)	AES-CBC (256-bit key)
IKE PRF	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
IKE Integrity	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
IKE DH group	256-bit random ECP	384-bit random ECP	256-bit random ECP	384-bit random ECP