



یاد‌الامن والامان

امنیت داده و شبکه

امنیت لایه IP

مرتضی امینی - سیدمهدی خرازی

نیمسال اول ۱۴۰۴-۱۴۰۳



فهرست مطالب

مقدمه

IPSec معماری

AH پروتکل

ESP پروتکل

ترکیب SAها

مدیریت کلید



فهرست مطالب

□ مقدمه

□ معماری IPSec

□ پروتکل AH

□ پروتکل ESP

□ ترکیب SAها

□ مدیریت کلید



مقدمه – معرفی IPSec

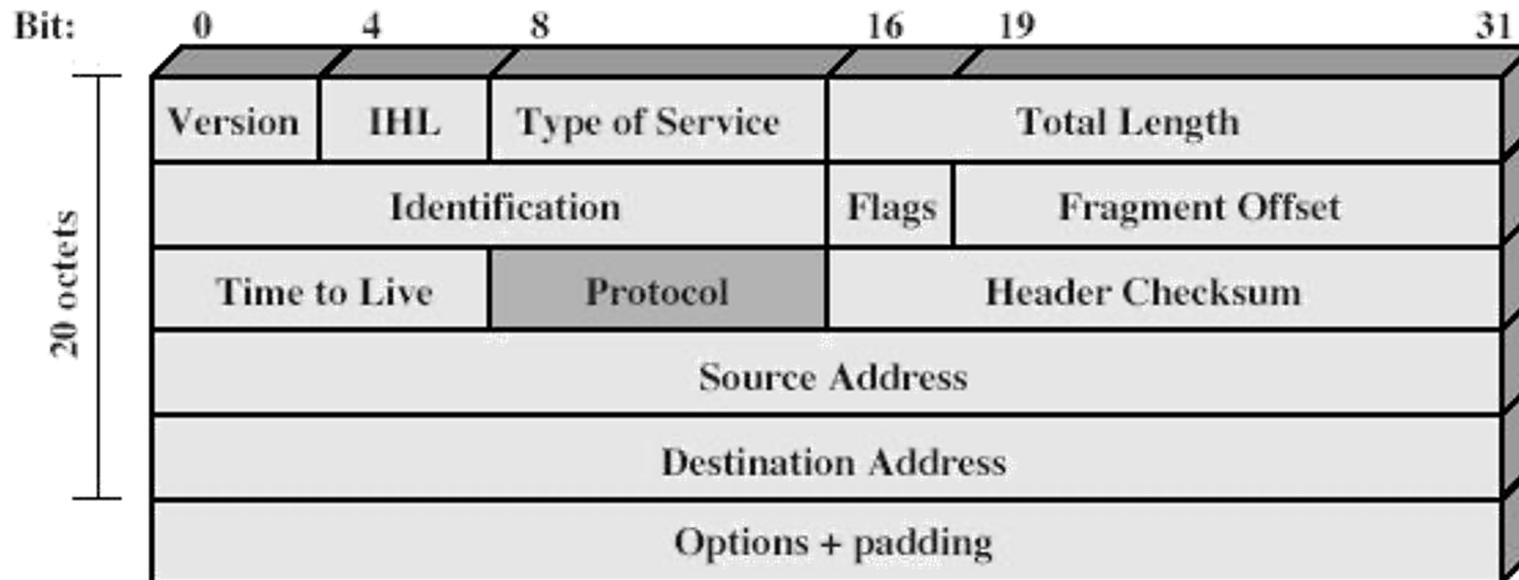
IPSec یک پروتکل تنها نیست بلکه مجموعه‌ای از الگوریتم‌های امنیتی است که چارچوبی کلی را برای برقراری یک ارتباط امن در لایه IP فراهم می‌نماید.

سرвис‌های امنیتی فراهم شده توسط IPSec

- احراز اصالت (به همراه کنترل صحت داده‌ها)
- محرومگی بسته‌ها / ترافیک
- مدیریت کلید (تبادل امن کلید)

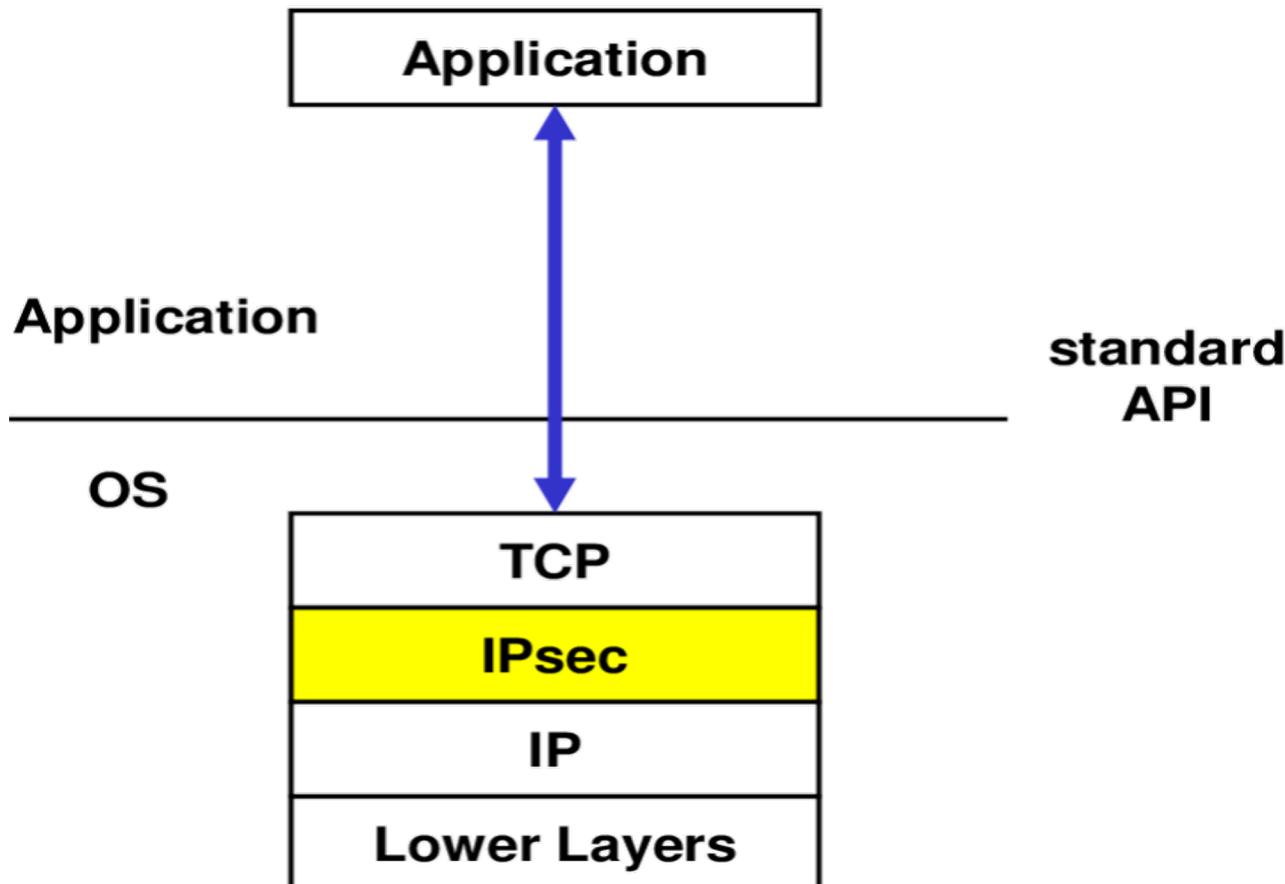


IPV4 – مقدمه





IPSec برای امنیت در لایه IP



(C) 2007, D.I. Manfred Lindner



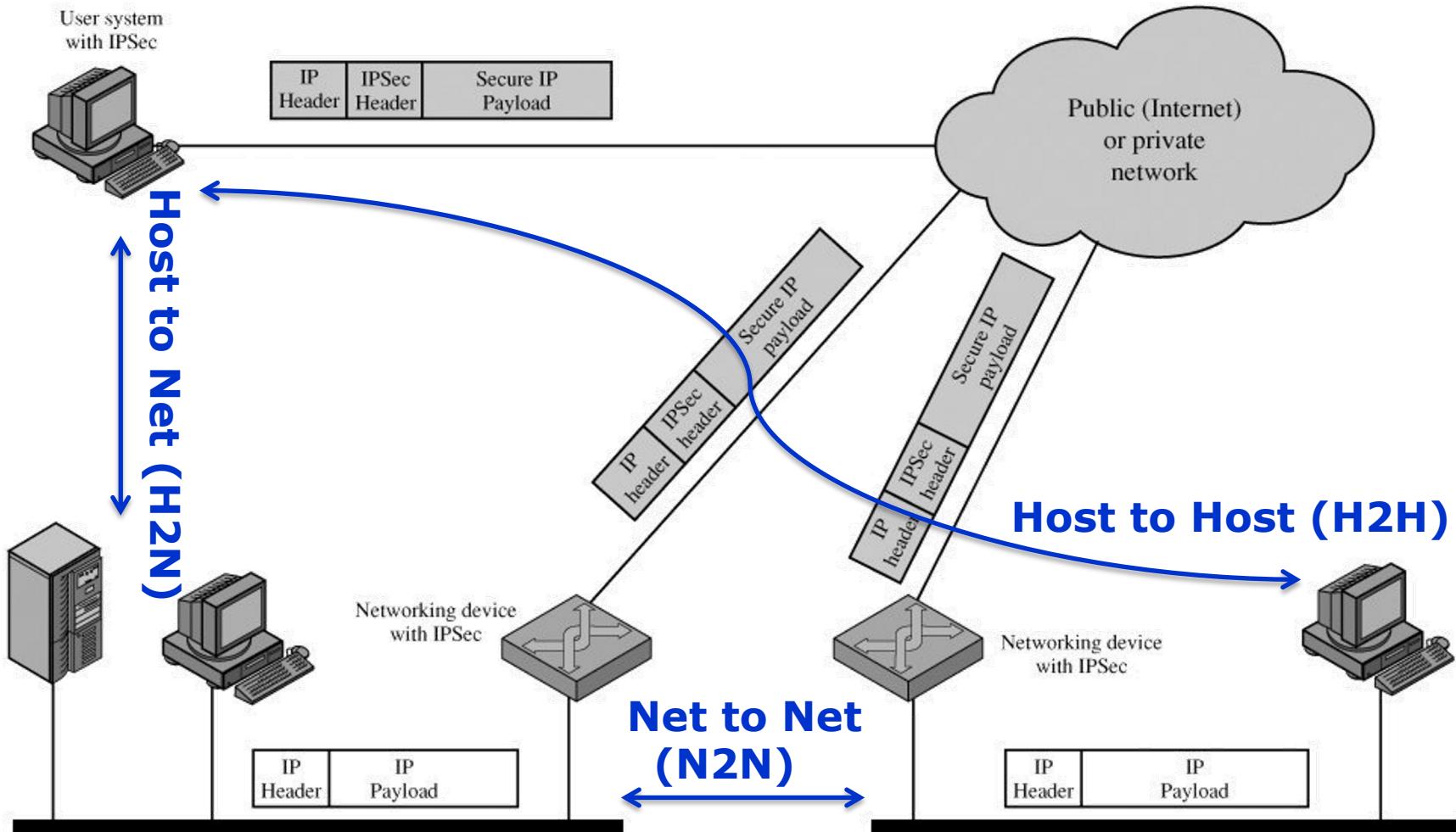
کاربرد IPSec

□ نمونه کاربردهای IPSec

- ایجاد شبکه خصوصی مجازی (VPN) برای شعبه‌های مختلف یک سازمان از طریق اینترنت
- دسترسی امن کارمندان شرکت به منابع شبکه از طریق اینترنت
- امکان ارتباط امن بین چند سازمان
- تامین امنیت برای کاربردهای دیگر (مثل تجارت الکترونیکی)



نمونه‌ای از کاربرد IPSec





فهرست مطالب

مقدمه

IPSec معماری

AH پروتکل

ESP پروتکل

ترکیب SAها

مدیریت کلید



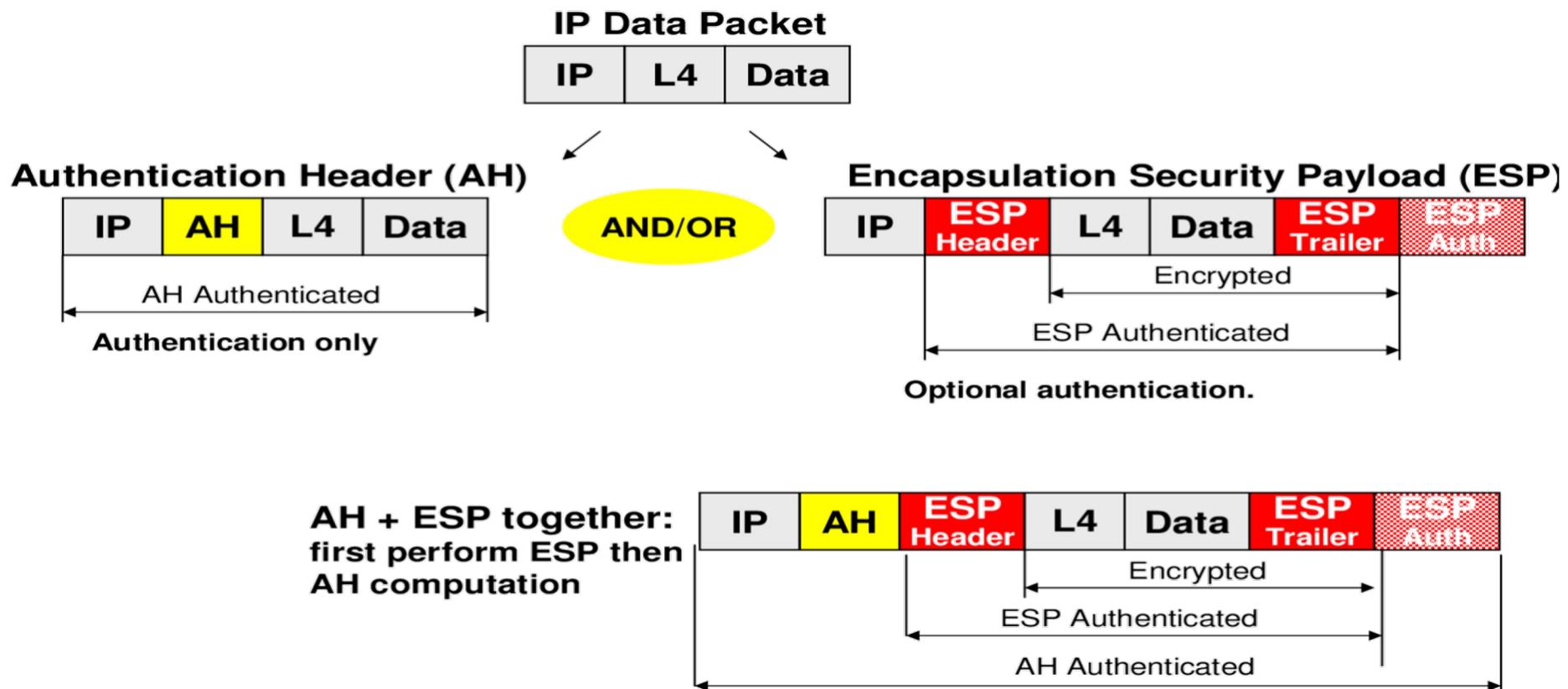
سرویس‌های IPSEC

- همه سرویس‌ها با دو پروتکل زیر ارائه می‌شوند:
- Authentication Header (AH)
 - Encapsulating Security Payload (ESP)

ESP (encryption plus authentication)	ESP (encryption only)	AH	
✓		✓	صحت
✓		✓	احراز اصالت منبع داده
✓	✓	✓	رد بسته‌های بازارسال شده
✓	✓		محرومانگی بسته‌ها
✓	✓		محرومانگی جریان ترافیک



سرآیندهای IPsec





مُدّهای انتقال بسته در IPSec

□ در هر دوی AH و ESP دو مُد ارسال بسته وجود دارد:

■ مُد انتقال (Transport Mode)

□ محاسبه MAC و یا رمزنگاری تنها روی **محتوای بسته** بدون درنظرگیری

یا تغییر سرآیند IP

■ مُد تونل (Tunnel Mode)

□ محاسبه MAC و یا رمزنگاری روی **کل بسته IP (سرآیند+Payload)**

و ارسال حاصل در قالب یک بسته جدید



قابلیت های مُدهای انتقال و توپل

مُد توپل	مُد انتقال	
احراز اصالت کل بسته IP داخلی به انضمام بخشهايی از سرآيند IP بسته بیرونی	احراز بخش دادهای IP و بخشهايی از سرآيند IP	AH
رمز کل بسته IP داخلی	رمز بخش دادهای IP که به دنبال سرآيند ESP قرار دارد.	ESP
رمز کل بسته IP داخلی. احراز اصالت بسته IP داخلی	رمز بخش دادهای IP که به دنبال سرآيند ESP قرار دارد. احراز اصالت بخش دادهای IP و نه سرآيند آن.	ESP with Authentication



مجمع امنیتی

- **تعريف:** مجمع امنیتی (Security Association) یک مفهوم کلیدی در مکانیزم‌های احراز اصالت و محترمانگی برای IP بوده و یک رابطه یک طرفه بین فرستنده و گیرنده بسته ایجاد می‌کند.
- SA در IP به نوعی معادل Connection در TCP است.



مجمع امنیتی

- ویژگیها:
- ماهیت یک SA با ۳ پارامتر اصلی زیر مشخص می‌شود:
- (SPI) Security Parameters Index : یک رشته بیتی نسبت داده شده به SA
- IP Destination Address : آدرس مقصد نهایی SA
- Security Protocol Identifier : بیانگر تعلق SA به ESP یا AH



فهرست مطالب

مقدمه

معماری IPSec

پروتکل AH

پروتکل ESP

ترکیب SAها

مدیریت کلید



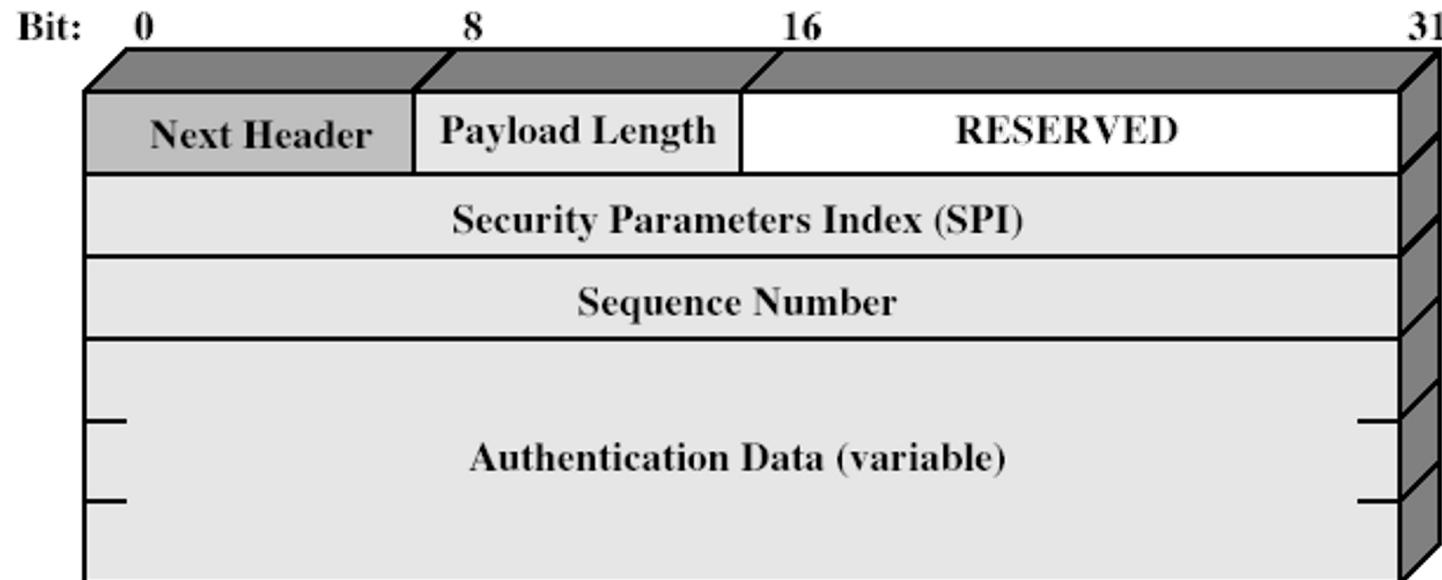
Authentication Header (AH)

Authentication Header □

- تضمین صحت و احراز اصالت بسته‌های IP
- تامین سرویس صحت داده‌ها با استفاده از MAC
... / AES-XCBC-MAC-96 / HMAC-SHA-1-96 □
- برای اطلاع از جزئیات الگوریتم‌ها مراجعه شود به RFC8221
- به مقدار فیلد MAC در AH، مقدار کنترل صحت (ICV) گفته می‌شود.
- طرفین نیاز به توافق روی یک کلید مشترک متقارن دارند.



Authentication Header (AH)





Authentication Header (AH)

□ فیلد های AH

- نوع سرآیند بعدی موجود در بسته Next Header (8 بیت)
- بیانگر طول AH (با واحد کلمه ۳۲ PayLoad Length بیتی) منهای ۲
- رزرو شده برای استفاده های آینده Reserved (16 بیت)
- برای تعیین SPI مربوط به SA (32 بیت) Sec. Param. Index
- شمارنده Sequence Number (32 بیت)
- در برگیرنده Authentication Data (متغیر) ICV (Integrity Check Value) یا MAC



Authentication Header (AH)

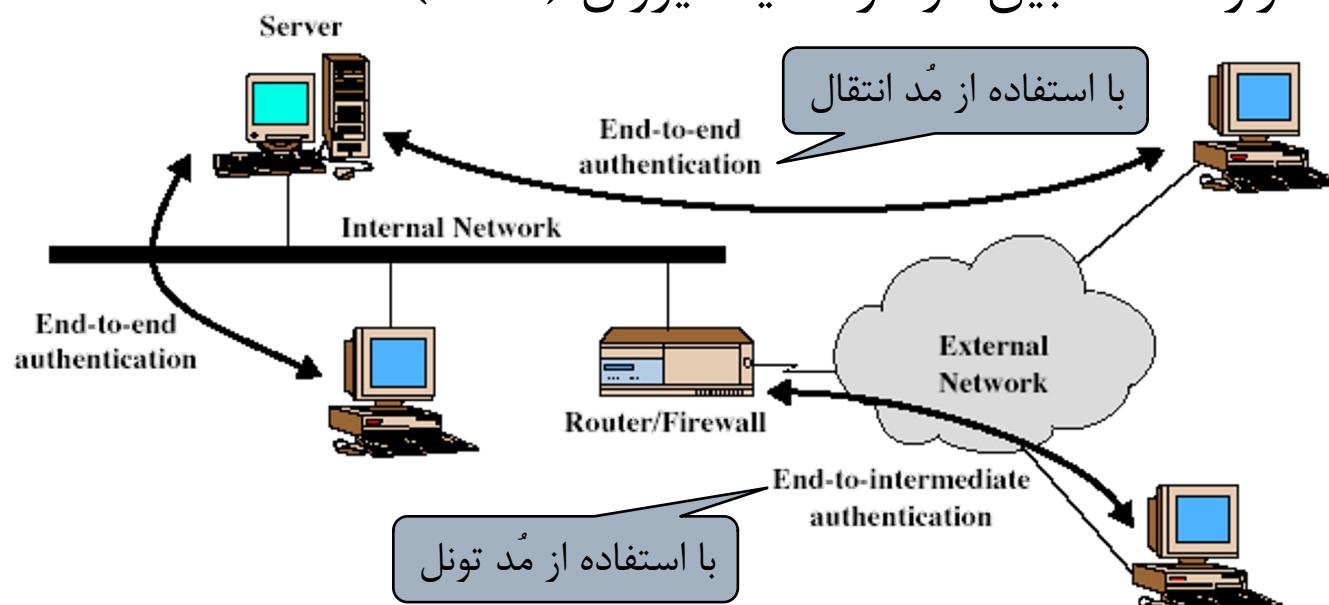
□ محاسبه MAC

- طول پیش فرض ۹۶ بیت (۳ تا ۳۲ بیتی)
- اولین ۹۶ بیت خروجی الگوریتم تولید MAC
- محاسبه MAC روی مقادیر زیر انجام می‌گیرد:
 - سرآیند نامتغیر IP، سرآیند نامتغیر AH و محتوای بسته
 - قسمتهایی از سرآیند که احتمالاً در انتقال تغییر می‌کنند (مانند TTL)، در محاسبه MAC صفر منظور می‌شوند.
- آدرس‌های فرستنده و گیرنده نیز در محاسبه MAC دخیل هستند
(جهت جلوگیری از حمله جعل IP)

Authentication Header (AH)

□ مُدهای انتقال و تونل در AH

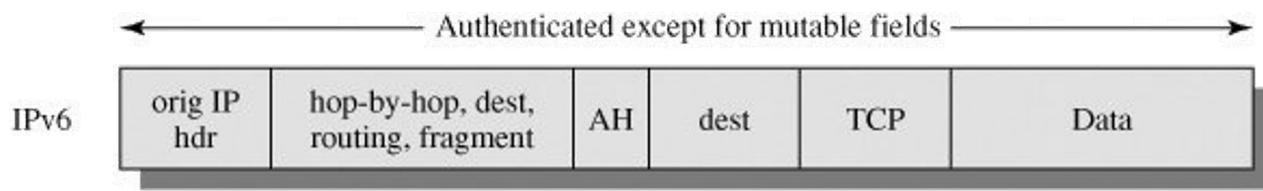
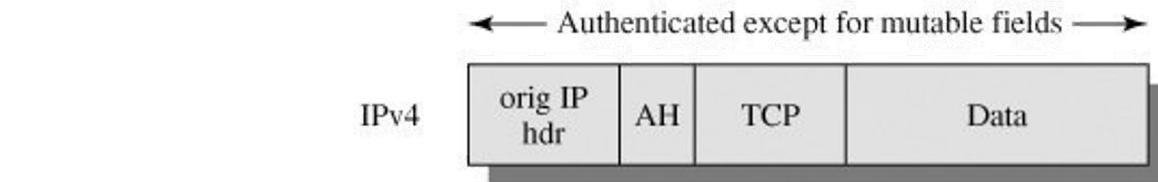
- **مُد انتقال (Transport):** برای احراز اصالت مستقیم بین کامپیوتر کاربر و کارگزار (H2H) (H2N)
- **مُد تونل (Tunnel):** برای احراز اصالت بین کاربر و درگاه یا فایروال (N2N) و یا احراز اصالت بین دو درگاه یا فایروال (N2N)



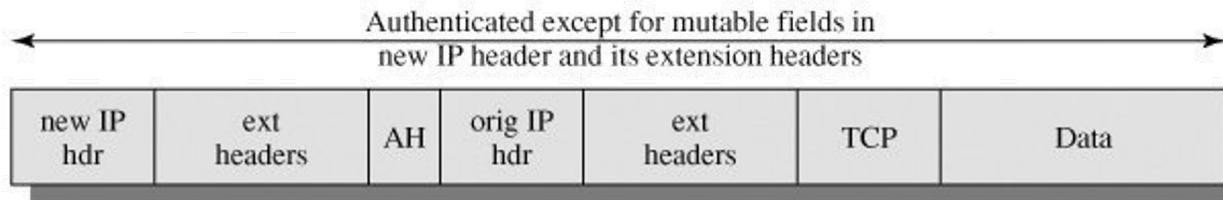
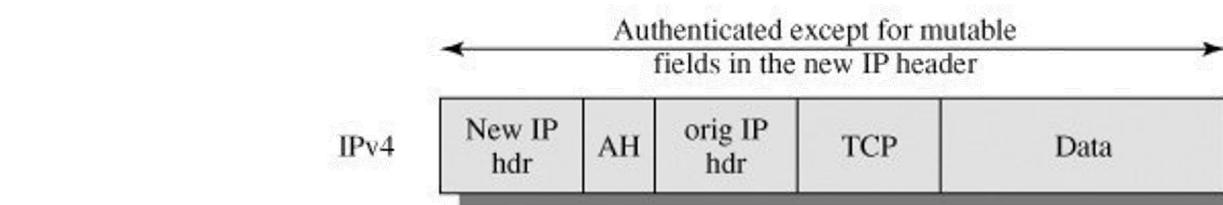


محدوده احراز اصالت AH

مُد انتقال □



مُد تونل □





مقابله با حمله تکرار در AH

□ روشن مقابله با حمله تکرار (Replay)

- اختصاص یک **شمارنده** با مقدار صفر به هر SA
- افزایش شمارنده به ازای هر بسته جدید که با این SA فرستاده می‌شود.
- درنظرگرفتن یک **پنجره** به اندازه پیش فرض $W = 64$
- لبه سمت راست پنجره به بزرگترین شماره بسته رسیده و تاییدشده از نظر صحت اختصاص می‌یابد.

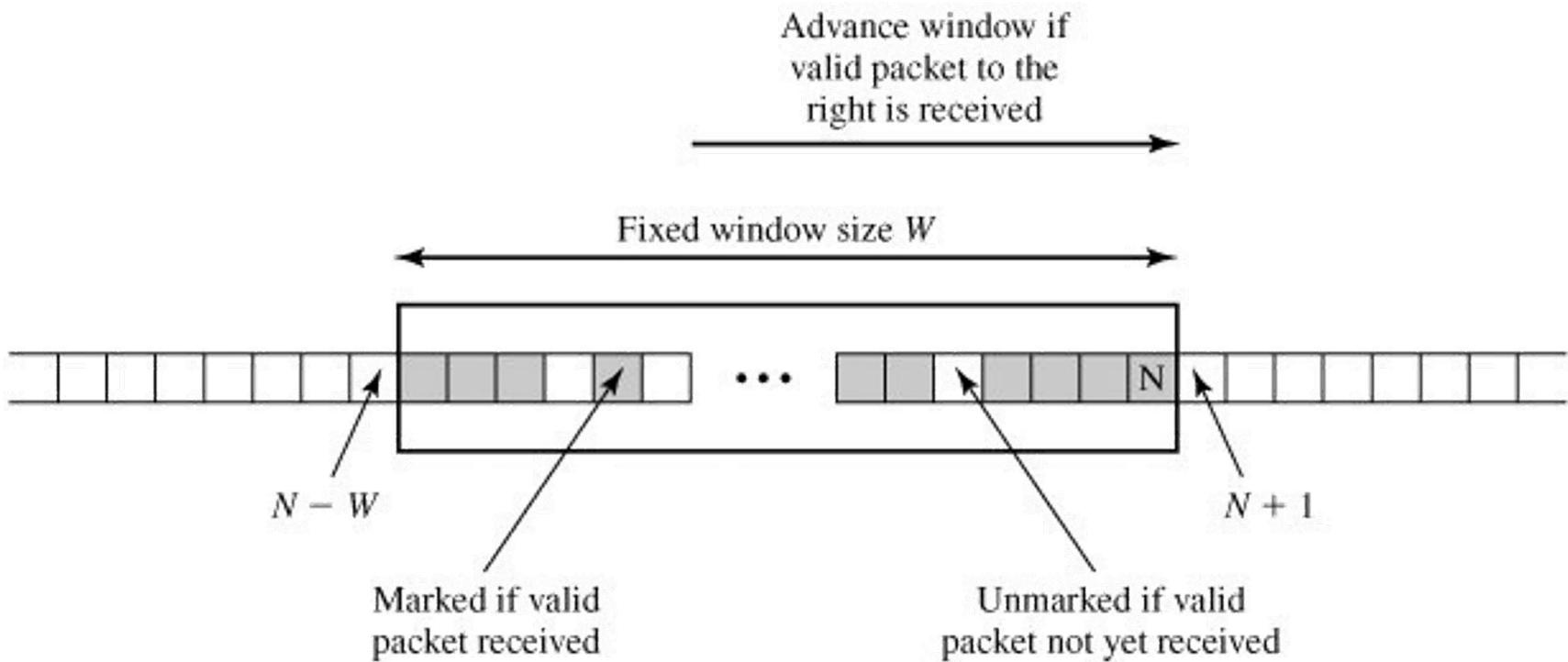


مقابله با حمله تکرار در AH

- مکانیزم برخورد با بسته جدید در پنجره
 - بسته داخل محدوده پنجره
 - محاسبه MAC و علامت زدن خانه متناظر در پنجره در صورت احراز اصالت
- بسته خارج از محدوده سمت راست پنجره
 - محاسبه MAC، احراز اصالت و شیفت پنجره به سمت راست، به طوری که خانه متناظر، سمت راست لبه پنجره را نشان دهد.
- بسته خارج از محدوده سمت چپ پنجره / عدم احراز اصالت / تکراری
 - دور انداخته می شود!



مقابله با حمله تکرار در AH





فهرست مطالب

مقدمه

معماری IPSec

پروتکل AH

پروتکل ESP

ترکیب SAها

مدیریت کلید

Encapsulating Security Payload (ESP)



□ ویژگیها

- پشتیبانی از محرمانگی داده و تا حدی محرمانگی ترافیک
- محرمانگی با استفاده از یکی از الگوریتم‌های تعیین شده مانند 3DES-CBC، AES-CTR، AES-CBC و ...
- امکان احراز اصالت (مشابه AH)
- برای اطلاع از جزئیات الگوریتم‌ها مراجعه شود به RFC8221

Encapsulating Security Payload (ESP)

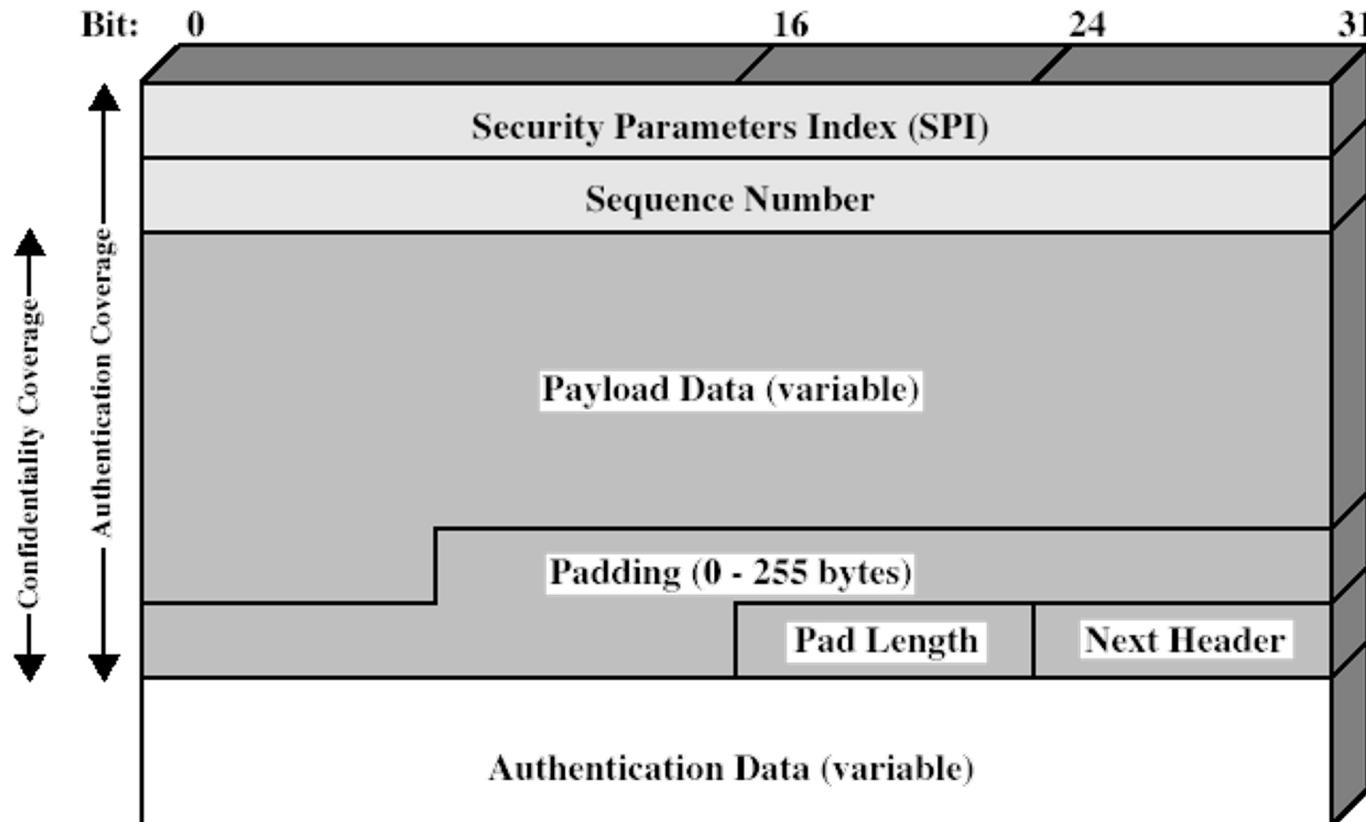


فیلدهای ESP

- SA : شناسه SPI
- شمارنده برای جلوگیری از حمله تکرار مشابه Sequence Number
- AH
- محتوای بسته که رمز می‌شود Payload
- بیتهای اضافی Padding
- طول فیلد بالا Pad Length
- نوع داده موجود در Next Header Payload Data
- مقدار MAC محاسبه شده (بدون در نظر گرفتن خود فیلد)- صرفاً از روی بخش داده‌ای و سرآیند ESP محاسبه می‌شود و وابسته به سرآیند IP نیست. Authentication Data



Encapsulating Security Payload (ESP)





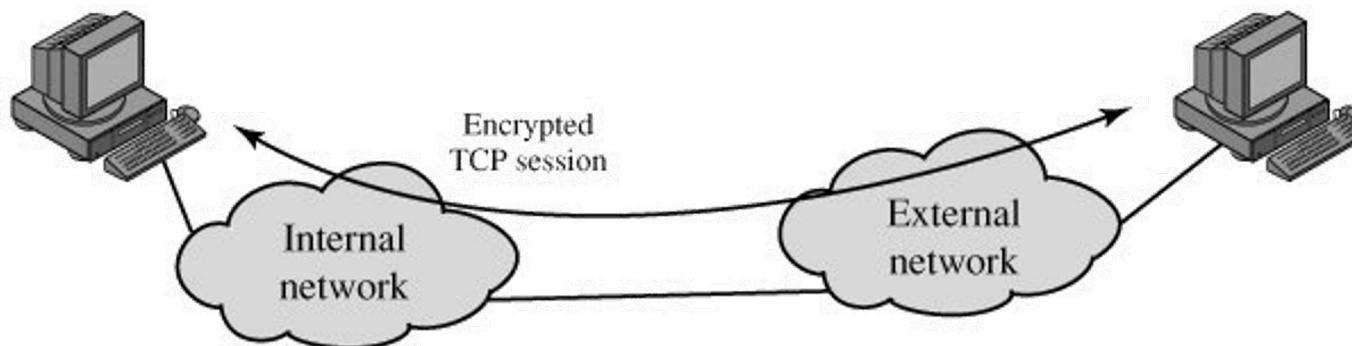
مُد انتقال در ESP

□ مُد انتقال

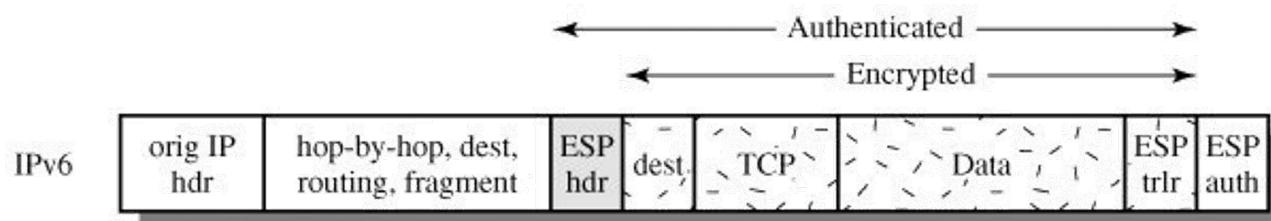
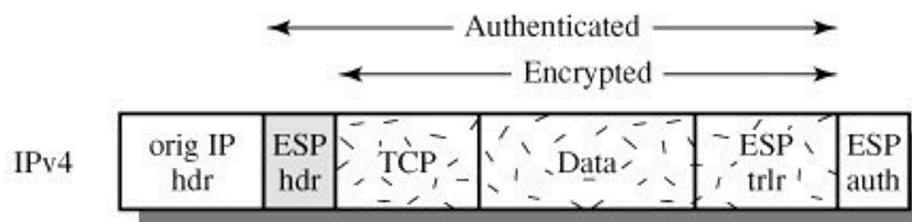
- تضمین محرومگی بین hostها
- رمزنگاری بسته داده، دنباله MAC و اضافه شدن ESP در صورت انتخاب احراز اصالت توسط مبداء
- تعیین مسیر توسط مسیریابهای میانی با استفاده از سرآیندهای اصلی (که رمز نشده‌اند)
- چک کردن سرآیند IP توسط مقصد و واگشایی رمز با قیمانده پیام
- امکان تحلیل ترافیک

مُد انتقال در ESP

□ برای ارتباط بین میزبان‌ها (H2H)



□ **ESP محدوده**



ESP trailer =
Padding, Pad Length,
and Next Header Fields



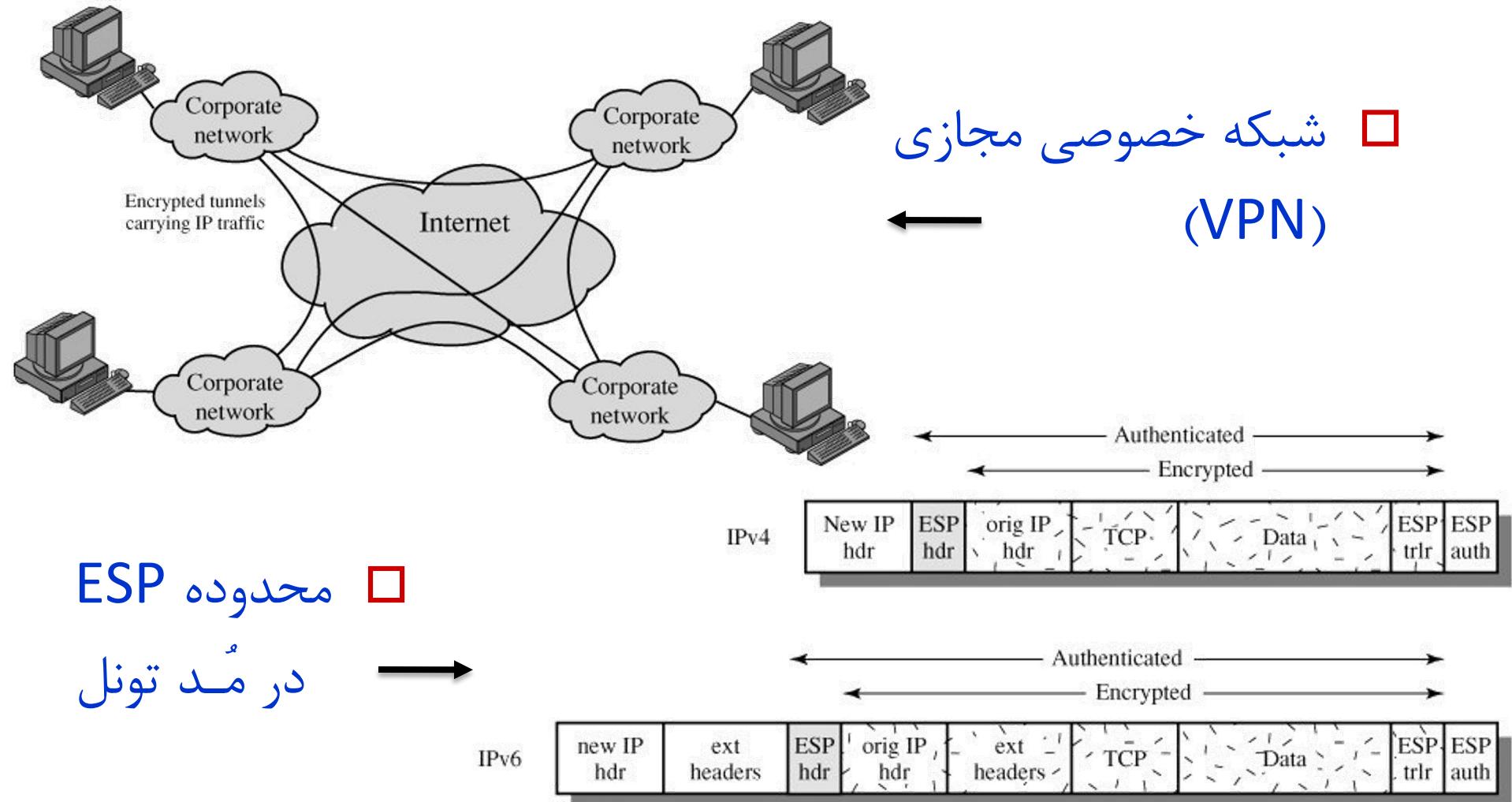
مُد تونل در ESP

□ مُد تونل

- اضافه شدن آدرس مبداء و مقصد دروازه‌های خروجی فرستنده و گیرنده، سرآیند ESP و دنباله ESP و قسمت مربوط به MAC در صورت نیاز (برای احراز اصالت)
- انجام مسیریابی در مسیریاب‌های میانی از روی آدرس‌های جدید
- رسیدن بسته به فایروال شبکه مقصد و مسیریابی از روی آدرس IP قبلی (مربوط به بسته اصلی) تا گره نهايی
- مُد تونل IPSec يکی از روش‌های ايجاد شبکه‌های خصوصی مجازی (VPN) است.



مُد تونل در ESP





فهرست مطالب

مقدمه

معماری IPSec

پروتکل AH

پروتکل ESP

ترکیب SAها

مدیریت کلید



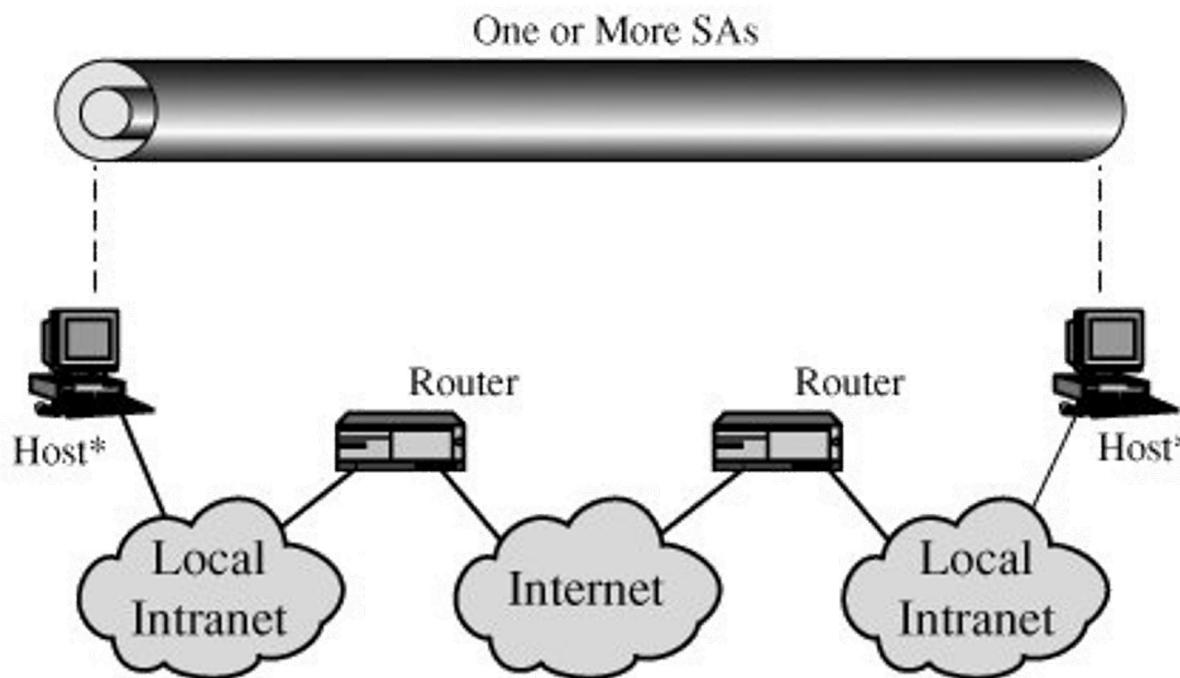
ترکیب SA ها

- با توجه به اینکه هر SA تنها یکی از سرویس‌های AH یا ESP را پیاده‌سازی کرده است، برای استفاده از هر دو سرویس باید آنها را باهم ترکیب کرد.
- ترکیب‌های مختلف
 - پیاده‌سازی IPSec توسط host های متناظر
 - پیاده‌سازی IPSec توسط gateway ها
 - ترکیب دو حالت بالا



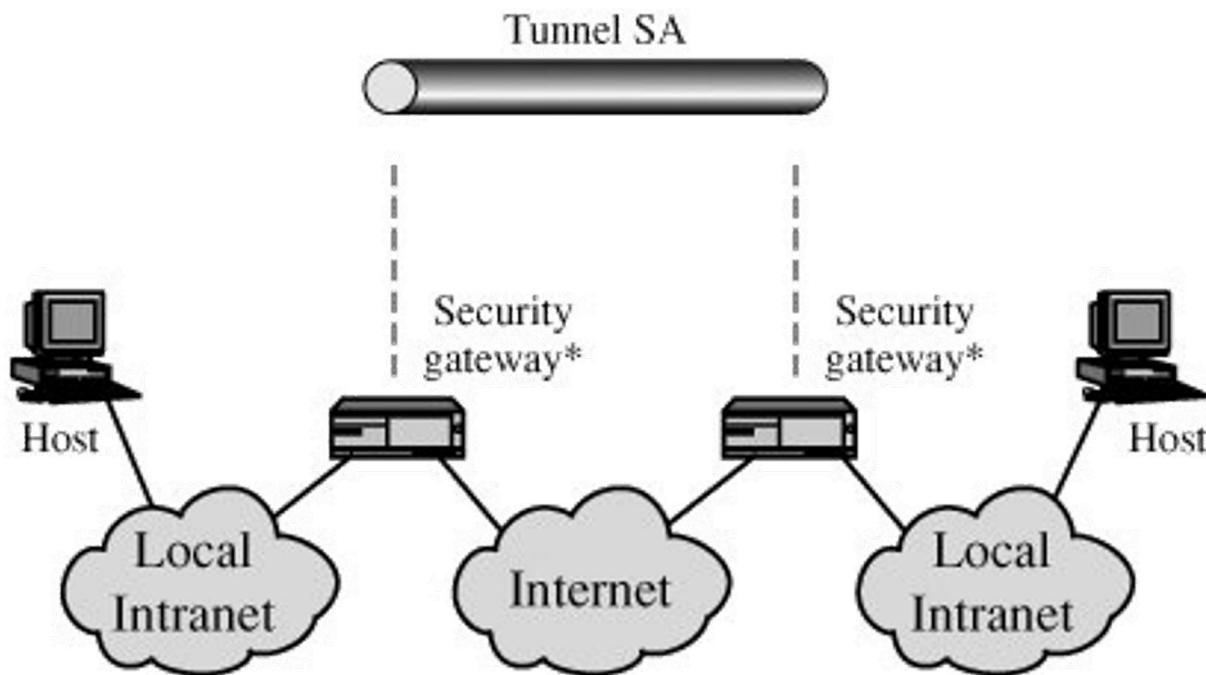
ترکیب SAها: نمونه ۱

- پیاده سازی IPSec به صورت انتهای-به-انتهای
- امکان استفاده از هر یک از ترکیبات ممکن از انواع SAها



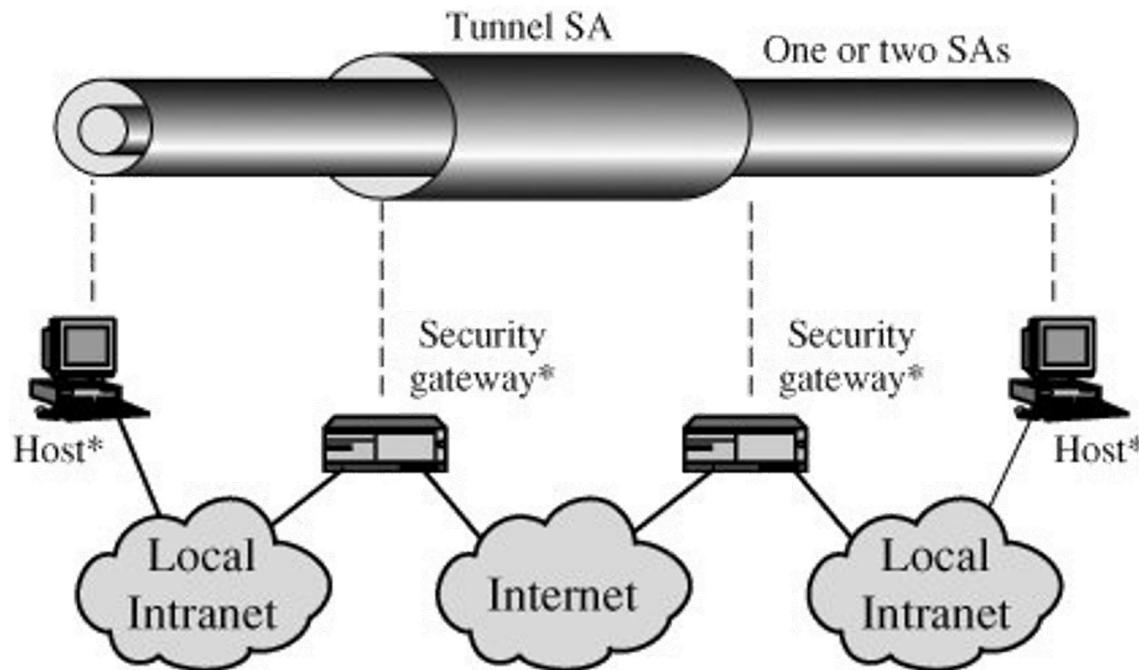
ترکیب SA‌ها: نمونه ۲

- برقراری تونل آمن بین دروازه‌ها: شبکه خصوصی مجازی
- ایجاد تونل در یکی از مدهای ESP و AH با Auth.



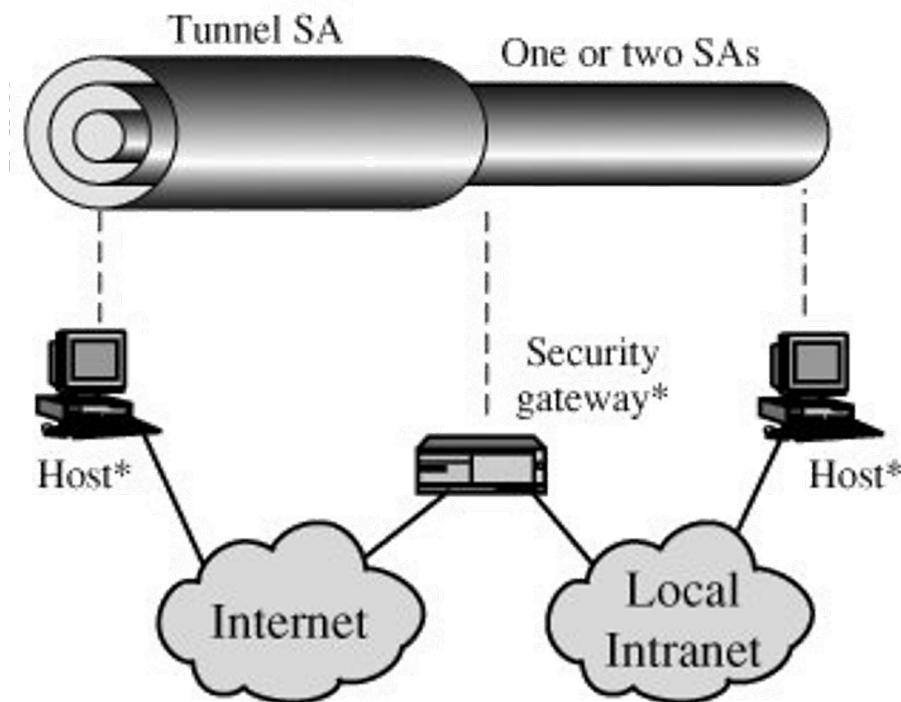
ترکیب SA‌ها: نمونه ۳

- ترکیب دو حالت ۱ و ۲
- اگر تونل بین دروازه‌ها از نوع ESP باشد، به طور محدود محرمانگی ترافیک نیز فراهم می‌گردد.



ترکیب SA‌ها: نمونه ۴

- برای اتصال یک میزبان بیرونی به یک سیستم شبکه داخلی
- ایجاد تونل تا دروازه شبکه داخلی، ترکیب چند SA





فهرست مطالب

مقدمه

معماری IPSec

پروتکل AH

پروتکل ESP

ترکیب SAها

مدیریت کلید



مدیریت کلید

- عموما به ۴ کلید سری، دو تا برای AH و دو تا برای ESP (در دو جهت) نیازمندیم.

- برای تولید و توزیع این کلیدها به یک مکانیزم مدیریت کلید نیازمندیم.



مدیریت کلید

□ مدیریت کلید دستی: تنها در سیستم های ایستا و کوچک قابل استفاده است.

□ مدیریت کلید خودکار:

■ پروتکل اتوماتیک و پیش فرض مدیریت و توزیع کلید IPSec اصطلاحا IKE(ISAKMP/Oakley) نامیده می شود.

Internet Security Association
and Key Management Protocol

■ دارای دو نسخه استاندارد **IKEv2** و **IKEv1** است.

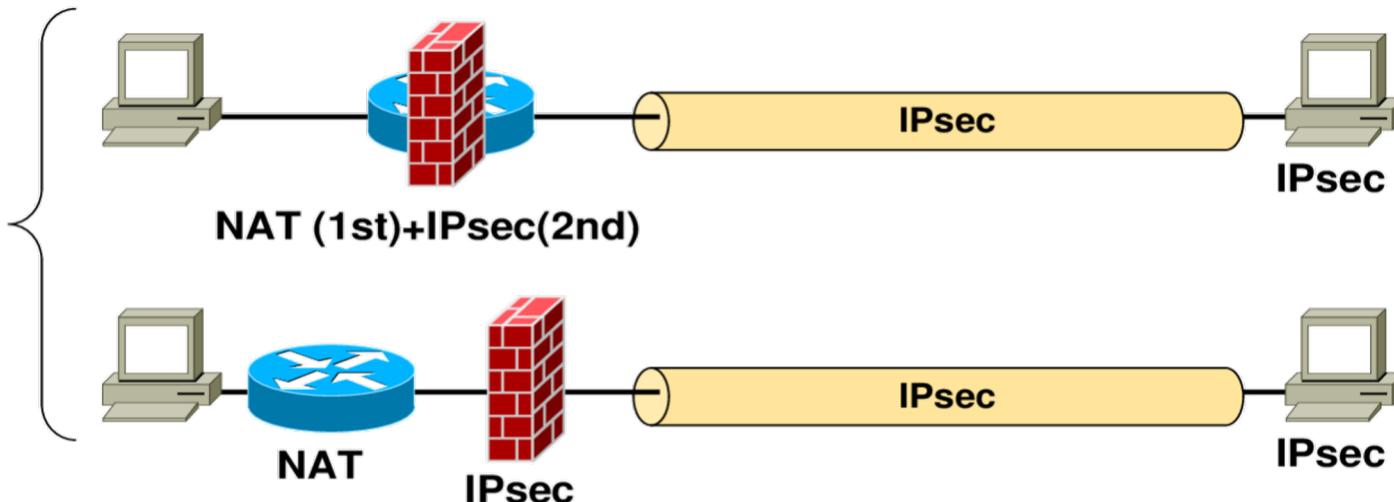
■ در حال حاضر استفاده از **IKEv1** به دلیل مشکلات امنیتی توصیه نمی شود.



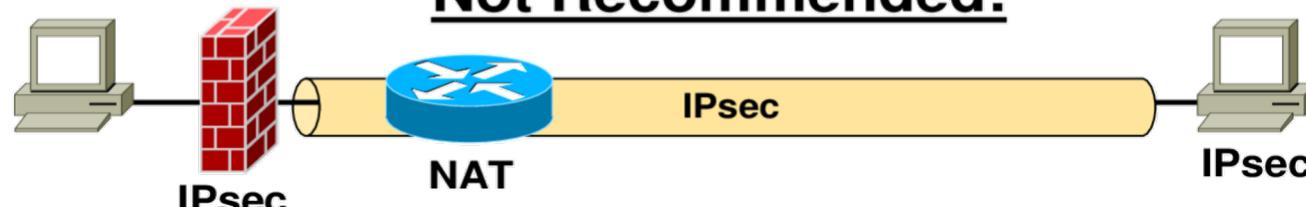
مشکل با IPsec و NAT

ترتیب استفاده از IPsec و NAT □

Recommended



Not Recommended:



(C) 2007, D.I. Manfred Lindner



مشکل NAT بعد از IPSec

□ در AH

- در محاسبه HMAC، سرآیند IP مدنظر قرار می‌گیرد.
- بنابراین نمی‌توان بعد از محاسبه AH، با NAT تغییر آدرس داد.

□ در ESP

- **در مُد انتقال:** در محاسبه HMAC، سرآیند IP را در نظر نمی‌گیرد ولی سرآیند TCP/UDP را در محاسبه لحاظ می‌کند.
 - چون در TCP Checksum (بخشی از سرآیند TCP)، آدرس‌های IP مبدا و مقصد لحاظ می‌شود و در NAT این مقدار باید مجدداً محاسبه شود ولی با اعمال ESP رمز شده. برای جلوگیری از مشکل، باید وارسی TCP Checksum در سمت گیرنده را خاموش کرد.
 - ترجمه پورت (PAT) امکان‌پذیر نیست!

- **در مُد تونل:** مشکلی با انجام NAT بعد از محاسبه ESP ندارد، چرا که سرآیند IP بسته بیرونی نه رمز می‌شود و نه احراز اصالت (کنترل صحت) می‌شود.



پایان

پست الکترونیکی

amini@sharif.edu

kharrazi@sharif.edu