یا ذا الامن والامان

امنیت داده و شبکه

امنیت لایه IP

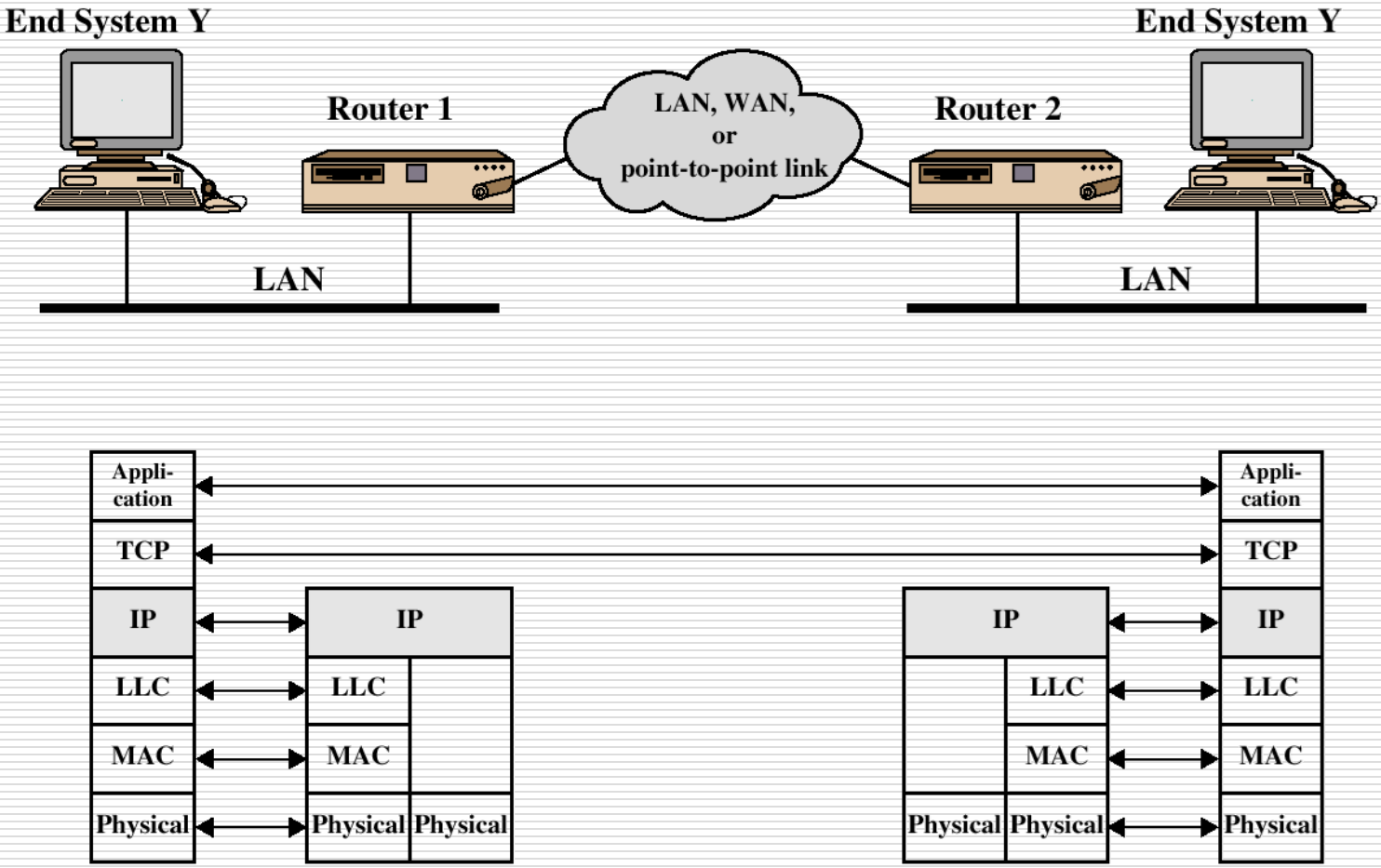
مرتضی امینی - نیمسال دوم ۱۴۰۰-۱۳۹۹

مرکز امنیت داده و شبکه شریف
http://dnsl.ce.sharif.edu

فهرست مطالب

- مقدمه
- معماری IPSec
- پروتکل AH
- پروتکل ESP
- ترکیب SAها
- مدیریت کلید

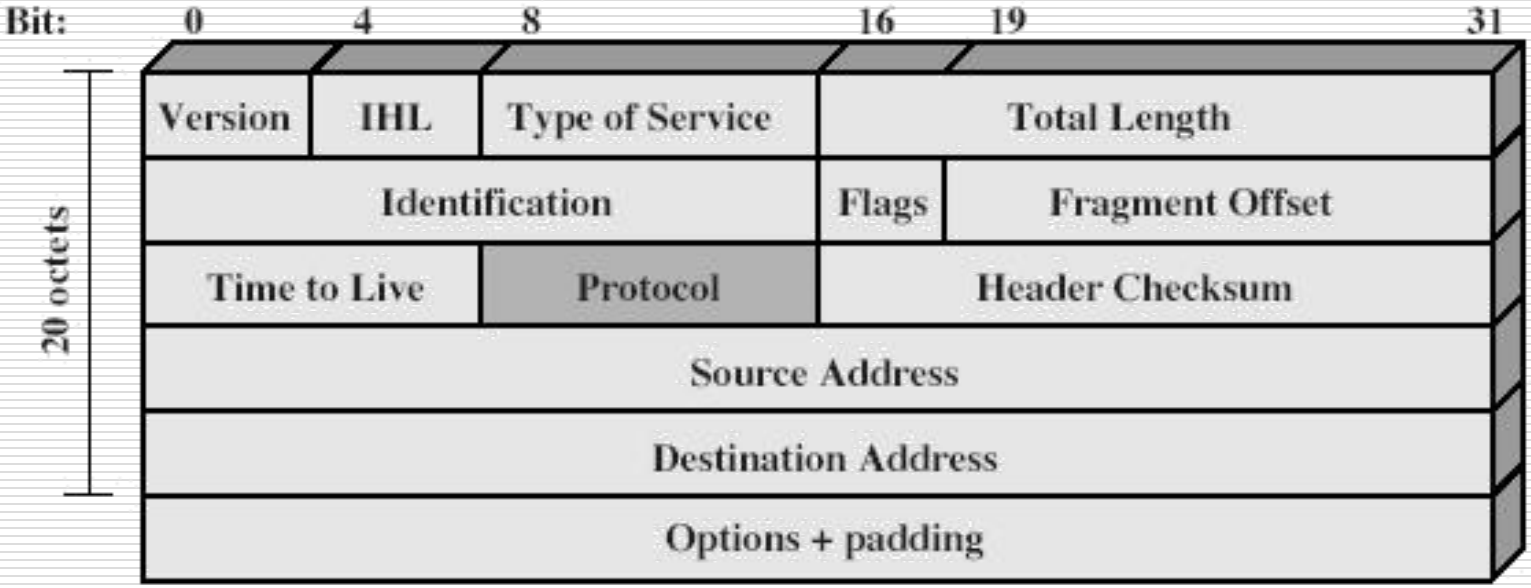
مقدمه – مثالی از TCP/IP



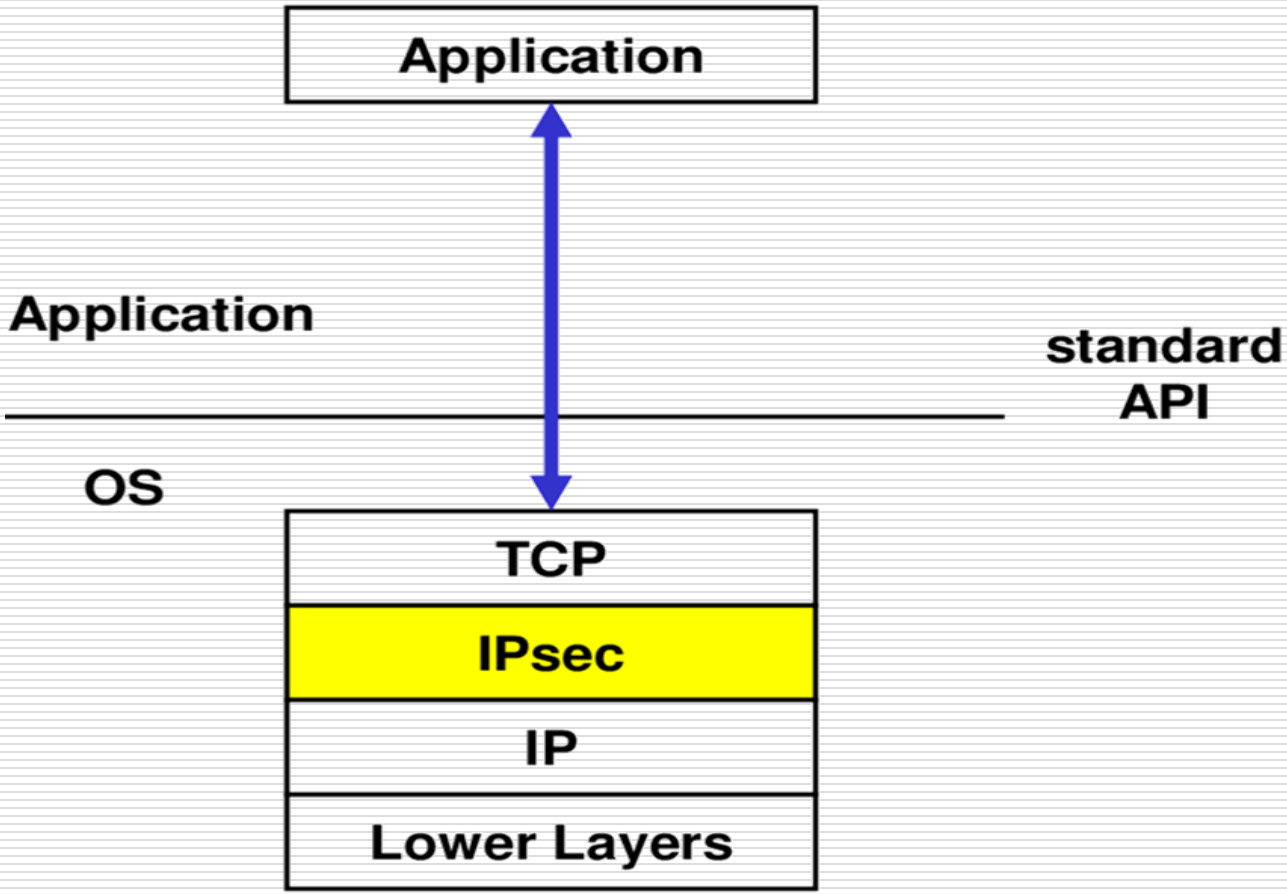
مقدمه

- راه‌حل‌های امنیتی وابسته به کاربرد (تاکنون)
  - S/MIME و PGP: امنیت پست الکترونیکی
  - Kerberos: امنیت بین کاربر-کارگزار (احراز اصالت)
  - SSL: معمولا ایجاد یک کانال امن در وب (تقریبا مستقل از کاربرد است)
- نیاز به امنیت در سطح IP و مستقل از کاربرد
  - محرمانگی محتوای بسته‌های IP
  - احراز اصالت فرستنده و گیرنده بسته‌ها

IPV4 – مقدمه


Bit:
0
4
8
16
19
31
20 octets
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + padding

IPSec برای امنیت در لایه IP



(C) 2007, D.I. Manfred Lindner

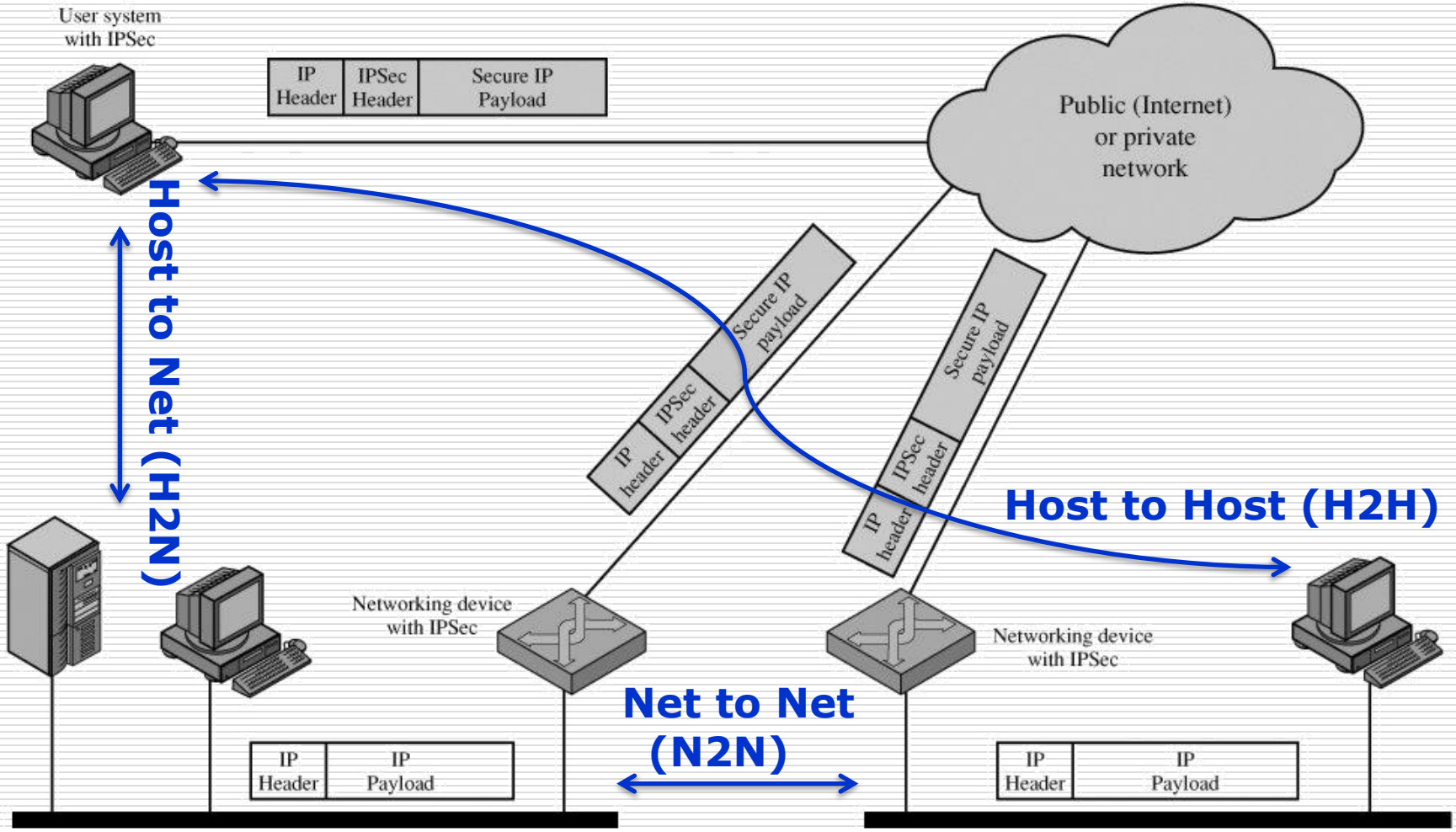
معرفی IPSec

- IPSec یک پروتکل تنها نیست بلکه مجموعه‌ای از الگوریتم‌های امنیتی است که چارچوبی کلی را برای برقراری یک ارتباط امن فراهم می نماید.
- سرویس‌های امنیتی فراهم شده توسط IPSec
  - احراز اصالت (به همراه کنترل صحت داده‌ها)
  - محرمانگی بسته‌ها
  - مدیریت کلید (تبادل امن کلید)

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



مقدمه

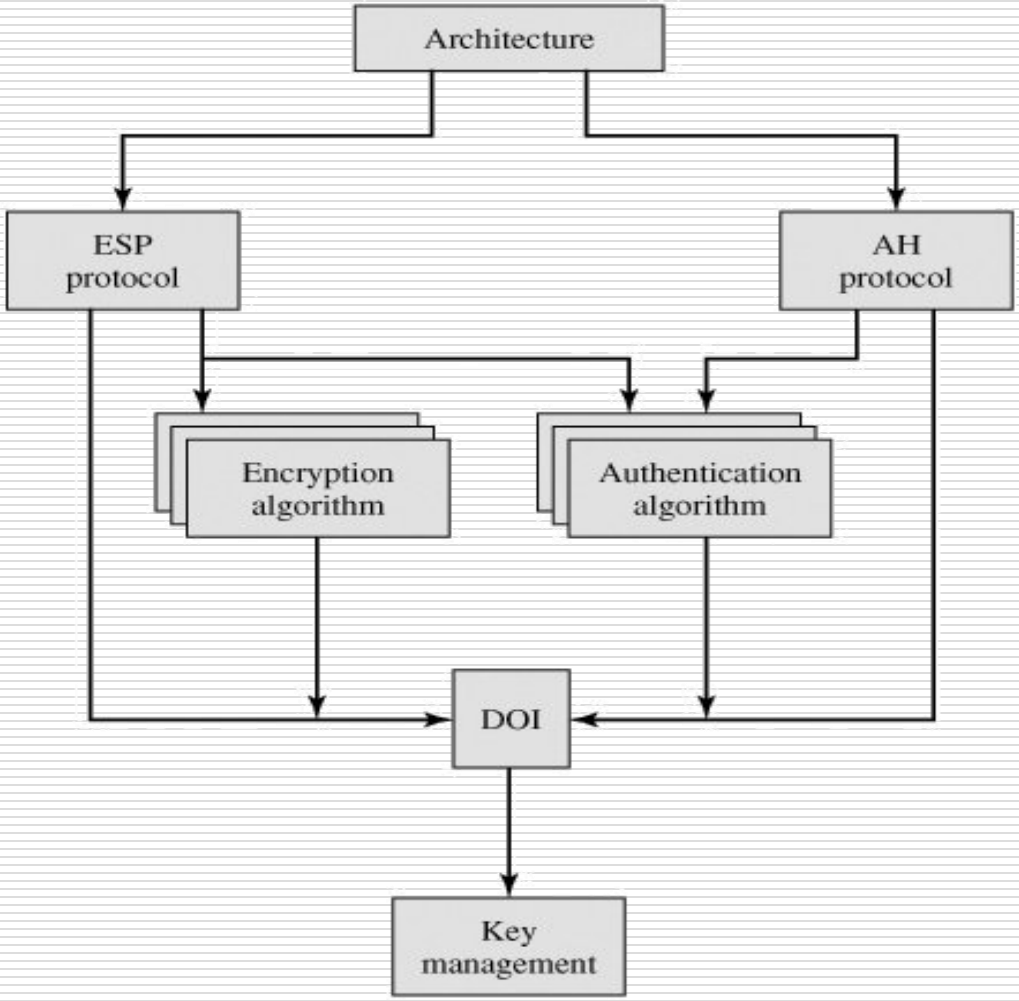
- مزایای استفاده از IPSec

- تامین امنیت قوی بین داخل و خارج LAN در صورت به کارگیری آن در مسیریابها و حفاظ‌ها (Firewallها)
  - عدم سربار رمزنگاری در نقاط انتهایی
  - پنهانی از نظر کاربران
- پنهانی از دید برنامه‌های کاربردی لایه‌های بالاتر (IPSec زیر لایه انتقال عمل می‌نماید)
- ایجاد ارتباط امن بین کارکنان سازمان از خارج به داخل

ویژگیهای IPSec

- دارای توصیف نسبتا مشکل
- پیاده‌سازی آن در IPv6 الزامی و در IPv4 اختیاری است.
- پروتکل IPSec در سرآیندهای توسعه یافته و بعد از سرآیند اصلی IP پیاده‌سازی می‌شود.
- مستندات IPSec بسیار حجیم بوده و به صورت زیر دسته‌بندی شده است:
  - معماری (Architecture)
  - Encapsulating Security Payload (ESP) : رمزنگاری بسته‌ها (احراز اصالت به صورت اختیاری)
  - Authentication Header (AH) : احراز اصالت بسته‌ها
  - مدیریت کلید: تبادل امن کلیدها
  - الگوریتم‌های رمزنگاری و احراز اصالت

ساختار مستندات IPSec



فهرست مطالب

- مقدمه
- معماری IPSec
- پروتکل AH
- پروتکل ESP
- ترکیب SAها
- مدیریت کلید

سرویس‌های IPSec

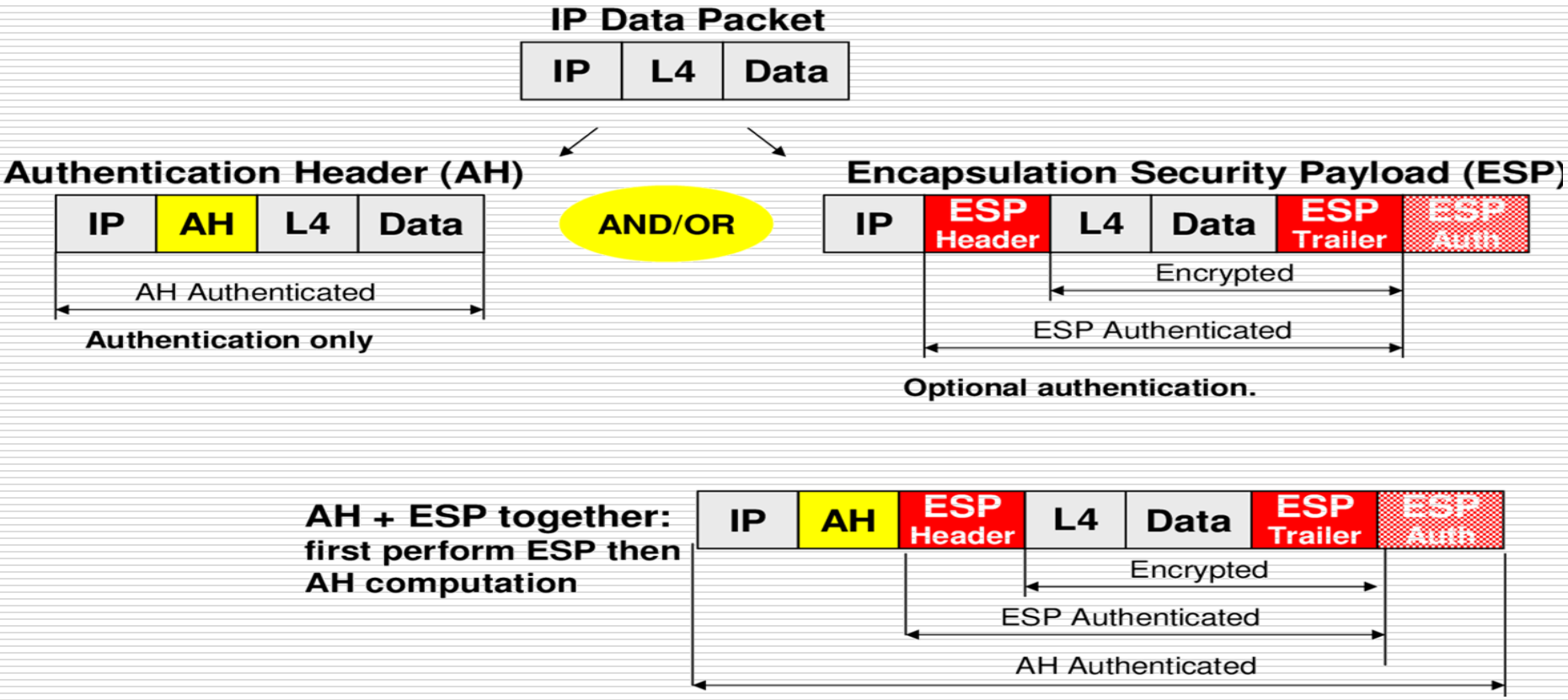
- سرویس‌های ارائه شده:
  - تضمین صحت داده‌ها در ارتباط Connectionless
  - احراز اصالت منبع داده‌ها (Data Origin)
  - تشخیص بسته‌های بازارسال شده و رد آنها (مقابله با حملات تکرار)
  - محرمانگی بسته‌ها
  - محرمانگی جریان ترافیک

سرویس‌های IPSec

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

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

سرآیندهای IPSec



(C) 2007, D.I. Manfred Lindner

مُدهای انتقال بسته در IPSec

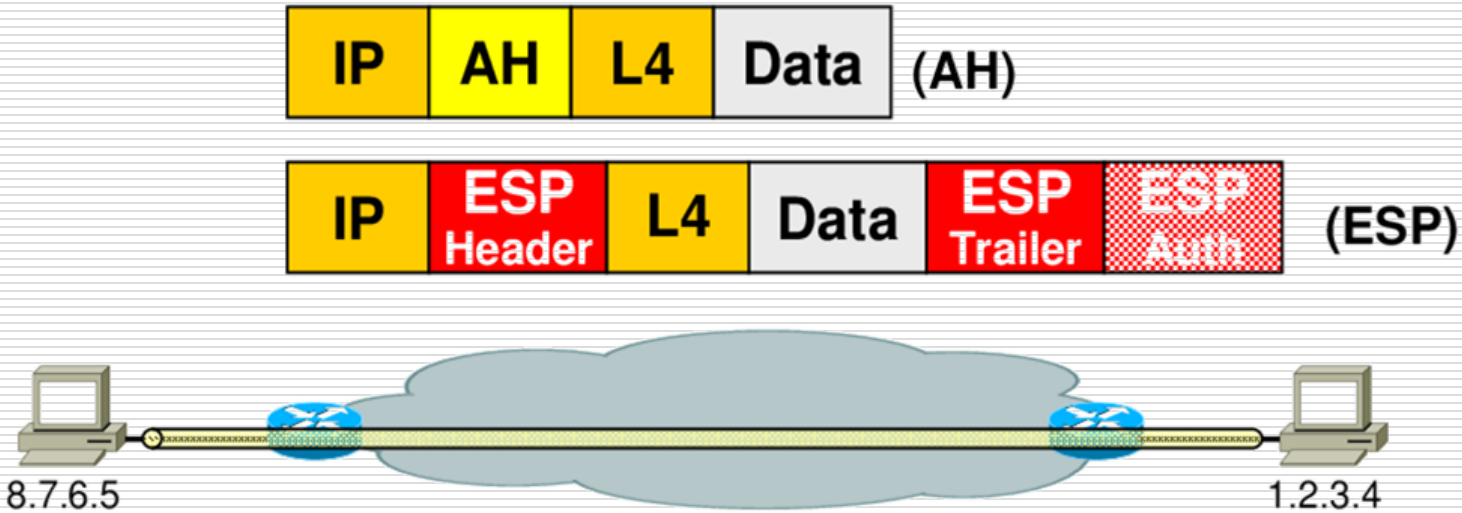
- در هر دوی AH و ESP دو مُد ارسال بسته وجود دارد:
  - مُد انتقال (Transport Mode)
    - تغییرات تنها روی محتوای بسته صورت می گیرد، بدون تغییر سرآیند IP
  - مُد تونل (Tunnel Mode)
    - اعمال تغییرات روی کل بسته IP (سرآیند+Payload) و فرستادن نتیجه به عنوان یک بسته جدید

مُد انتقال در IPSec

مُد انتقال

- در کاربردهای انتها به انتها (end-to-end) یا میزبان به میزبان (H2H) مثل کارگزار/کارفرما استفاده می‌شود.
- ESP : رمزنگاری (ضروری) و صحت (اختیاری) محتوای بسته
- AH : صحت محتوا و سرآیند بسته (به غیر از بخشهای متغیر در گذار بسته از شبکه)

مُد انتقال در IPSec



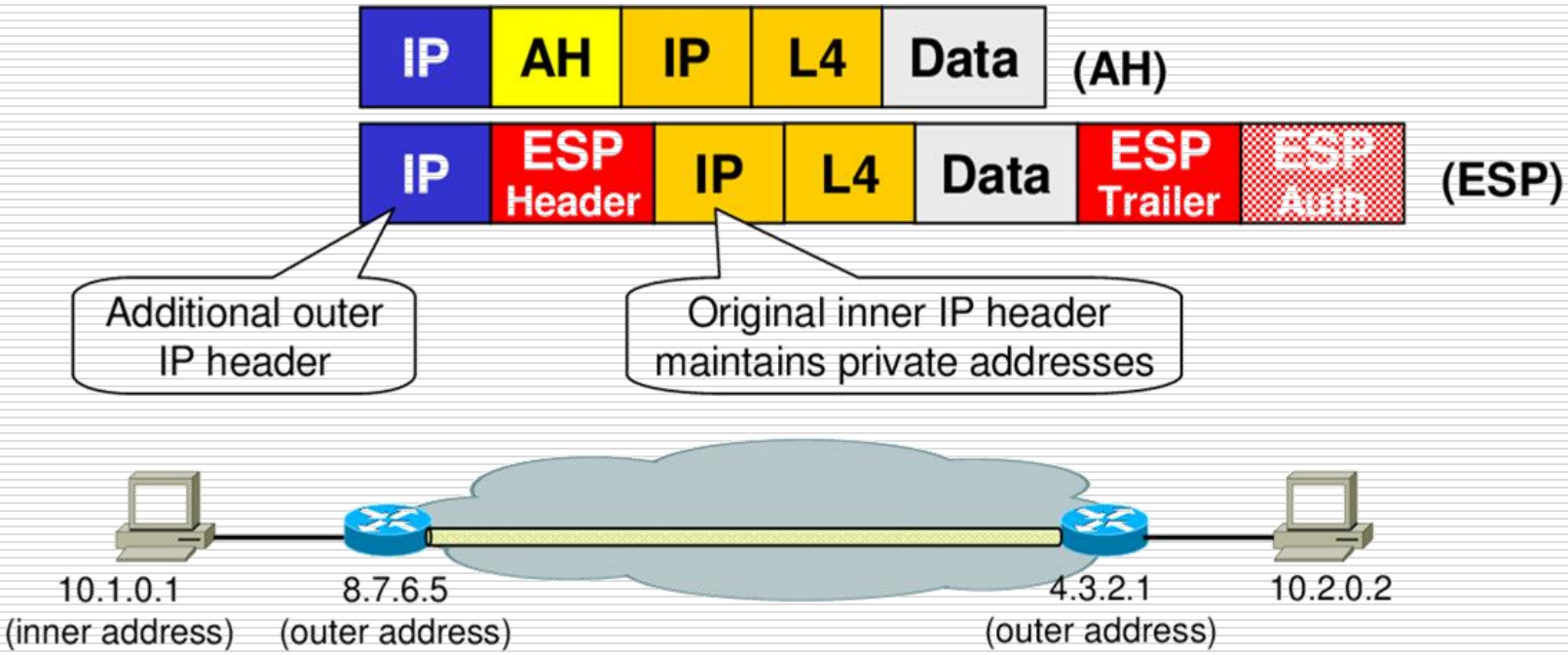
(C) 2007, D.I. Manfred Lindner

مُد تونل در IPSec

مُد تونل

- مورد استفاده در ارتباط Gateway به Gateway یا شبکه به شبکه (N2N) و همچنین میزبان به شبکه (H2N).
- هیچ مسیریاب (router) میانی قادر به تشخیص سرآیند داخلی نیست.

مُد تونل در IPSec



(C) 2007, D.I. Manfred Lindner

قابلیت های مُدهای انتقال و تونل

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

مجمع امنیتی

- **تعریف:** مجمع امنیتی(Security Association) یک مفهوم کلیدی در مکانیزم‌های احراز اصالت و محرمانگی 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:
  - Security Parameters Index (SPI): یک رشته بیتی نسبت داده شده به SA
  - IP Destination Address : آدرس مقصد نهایی SA
  - Security Protocol Identifier : بیانگر تعلق SA به AH یا ESP

مجمع امنیتی

پارامترهای SA

- Sequence Number Counter: شماره سریال بسته‌ها
- Sequence Counter Overflow: نشانگر سرریز در شمارنده
- Anti Replay Window: استفاده برای مشخص کردن تکراری بودن بسته دریافتی
- AH Information: الگوریتم احراز اصالت، کلیدها و طول عمر آنها و ...
- ESP Information: الگوریتم رمز و احراز اصالت، کلیدها و طول عمر آنها، مقادیر اولیه و ...
- SA Lifetime: طول عمر SA
- IPSec Protocol Mode: یک از مُدهای انتقال و تونل
- Maximum Transmission Unit: هرگونه مقدار MTU (حداکثر واحد قابل انتقال) مشاهده شده در مسیر

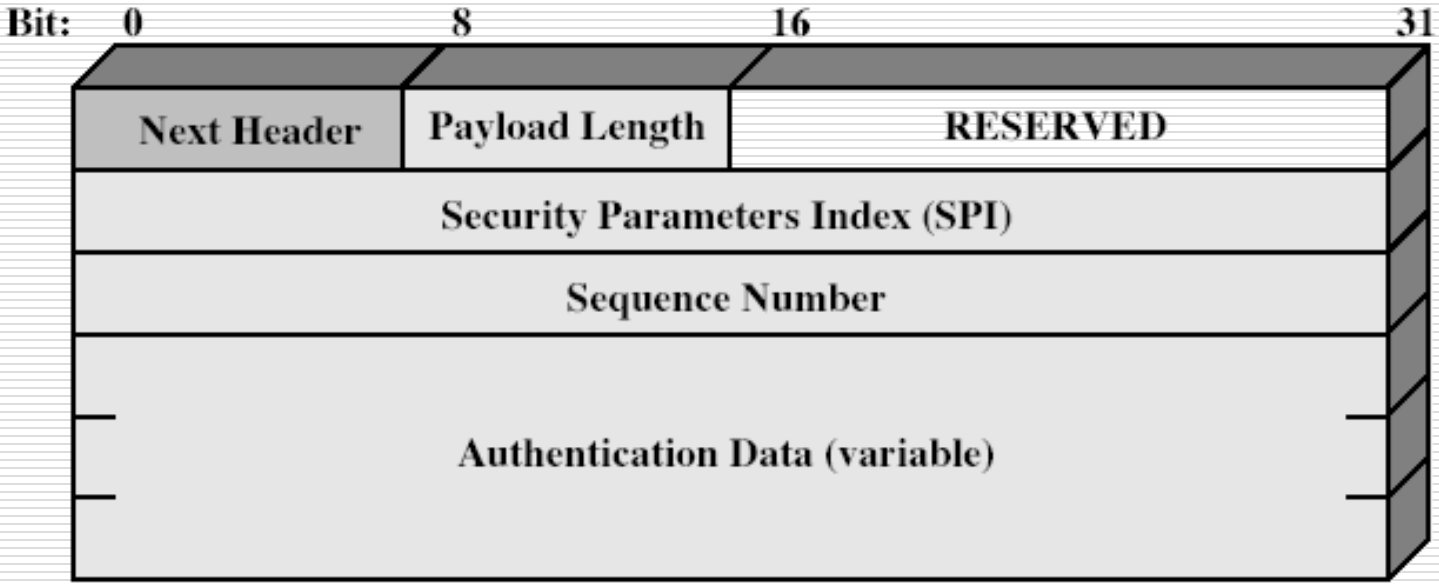
فهرست مطالب

- 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
    - HMAC-SHA-1-96 / AES-XCBC-MAC-96 / ...
    - برای اطلاع از جزییات 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)

- **فیلدهای AH:**
  - Next Header (۸ بیت): نوع سرآیند بعدی موجود در بسته
  - PayLoad Length (۸ بیت): بیانگر طول AH (با واحد کلمه ۳۲ بیتی) منهای ۲
  - Reserved (۱۶ بیت): رزرو شده برای استفاده‌های آینده
  - Sec. Param. Index (۳۲ بیت): برای تعیین SPI مربوط به SA
  - Sequence Number (۳۲ بیت): شمارنده
  - Authentication Data (متغیر): دربرگیرنده MAC یا ICV (Integrity Check Value)

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 احتمالا 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)

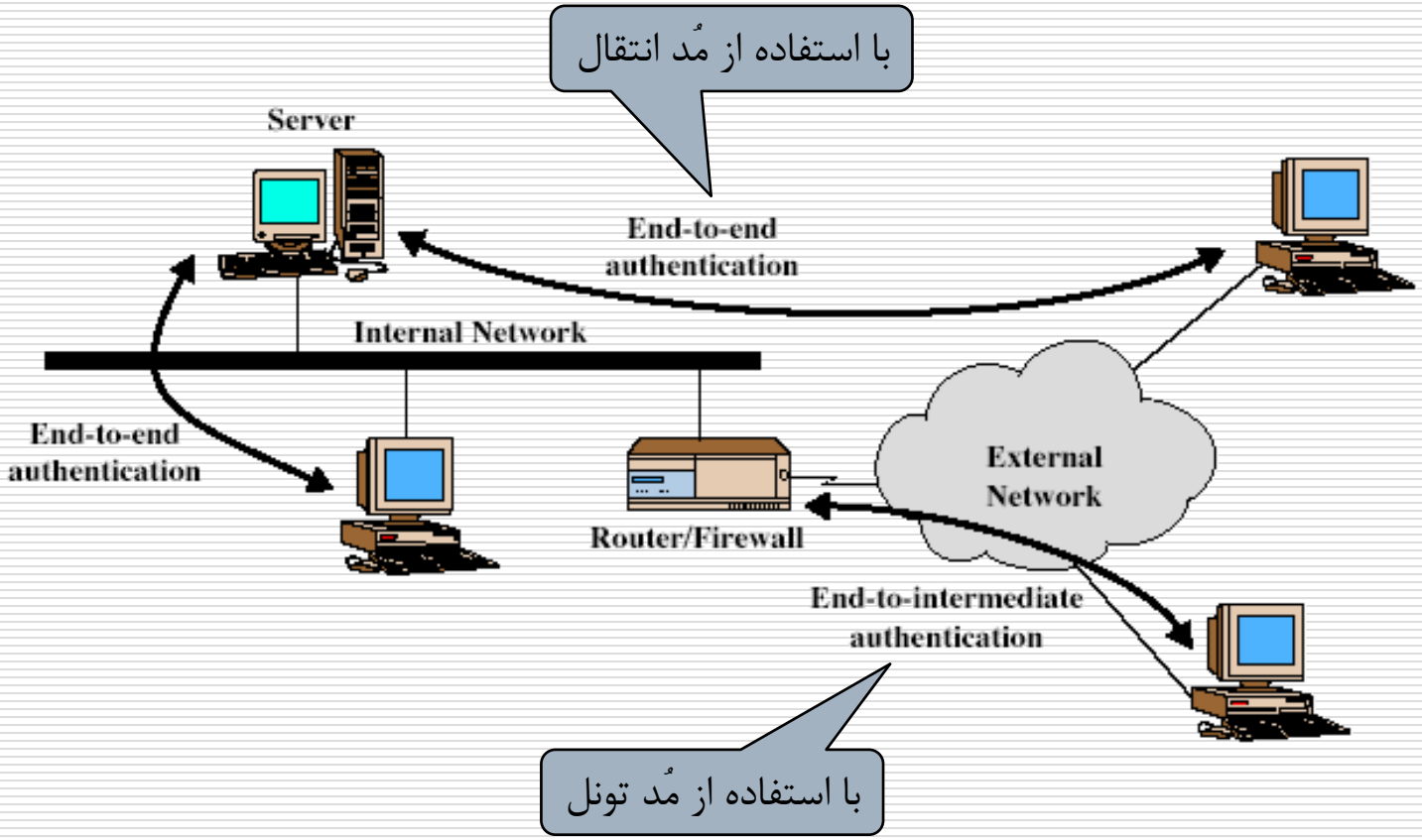
Authentication Header (AH)

- مُدهای انتقال و تونل در AH:

  - **مُد انتقال (Transport):** برای احراز اصالت مستقیم بین کامپیوتر کاربر و کارگزار (H2H)

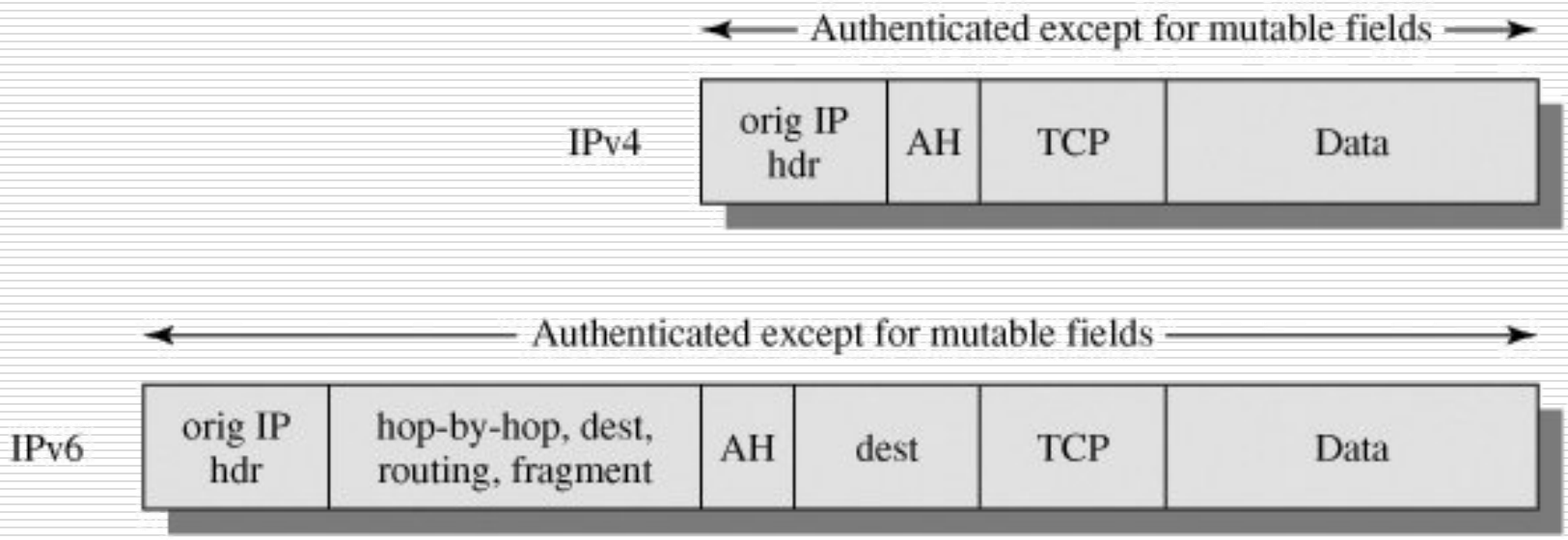
  - **مُد تونل (Tunnel):** برای احراز اصالت بین کاربر و درگاه یا فایروال (H2N) و یا احراز اصالت بین دو درگاه یا فایروال (N2N)

انواع احراز اصالت با AH



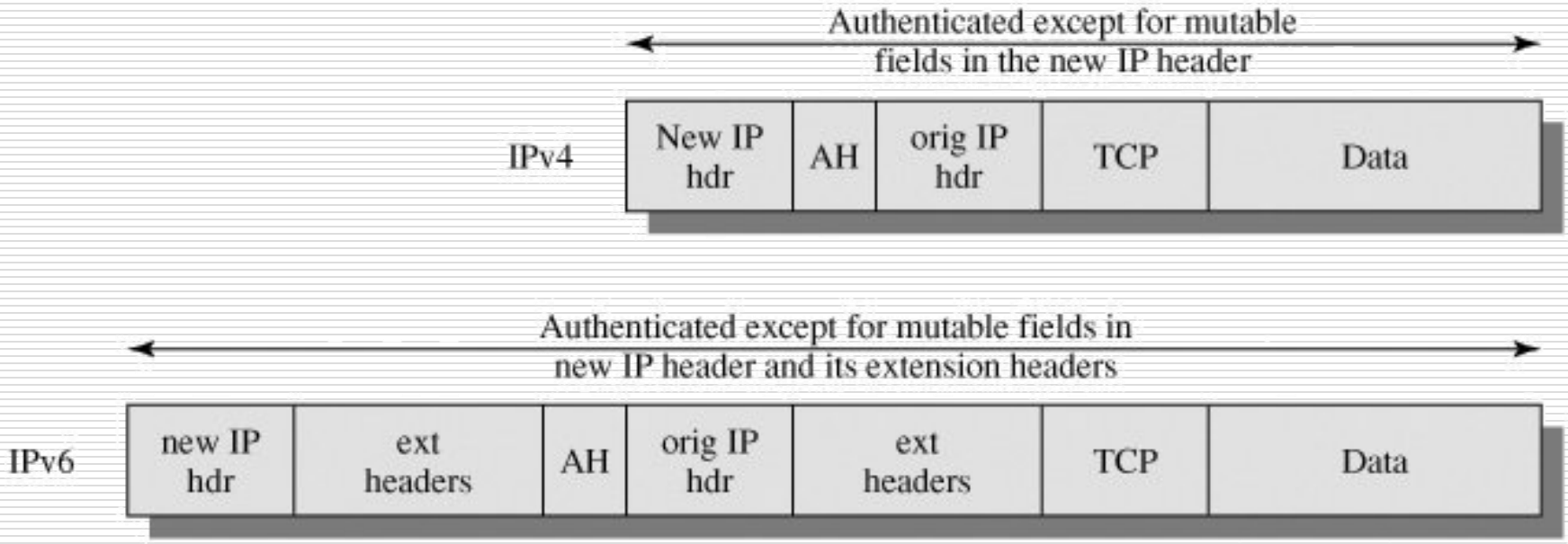
محدوده احراز اصالت AH

- مُد انتقال



محدوده احراز اصالت AH

- مُد تونل



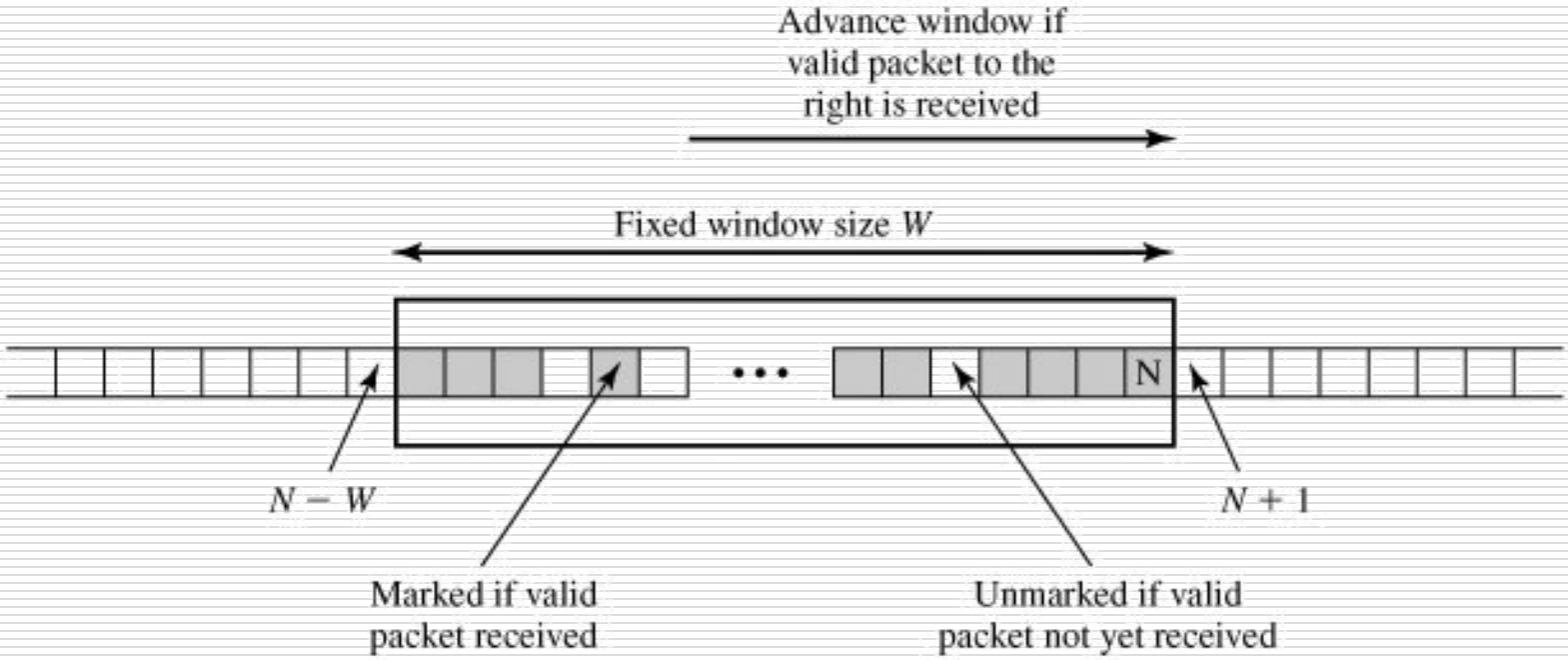
مقابله با حمله تکرار در AH

- روش 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.
  - اگر شمارنده به مقدار $2^{32}-1$ برسد، باید از یک SA جدید با کلید جدید استفاده کرد.
  - درنظرگرفتن یک پنجره به اندازه پیش فرض W =۶۴
  - 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 جدید و داخل محدوده پنجره
    - محاسبه MAC و علامت زدن خانه متناظر در پنجره در صورت احراز اصالت
  - بسته خارج از محدوده پنجره (سمت راست)
    - محاسبه MAC، احراز اصالت و شیفت پنجره به سمت راست، به طوری که خانه متناظر، سمت راست لبه پنجره را نشان دهد.
  - بسته جدید خارج از محدوده پنجره (سمت چپ) یا عدم احراز اصالت آن
    - دور انداخته می‌شود!

مقابله با حمله تکرار در AH



فهرست مطالب

- مقدمه
- معماری IPSec
- پروتکل AH
- **پروتکل ESP**
- ترکیب SAها
- مدیریت کلید

Encapsulating Security Payload (ESP)

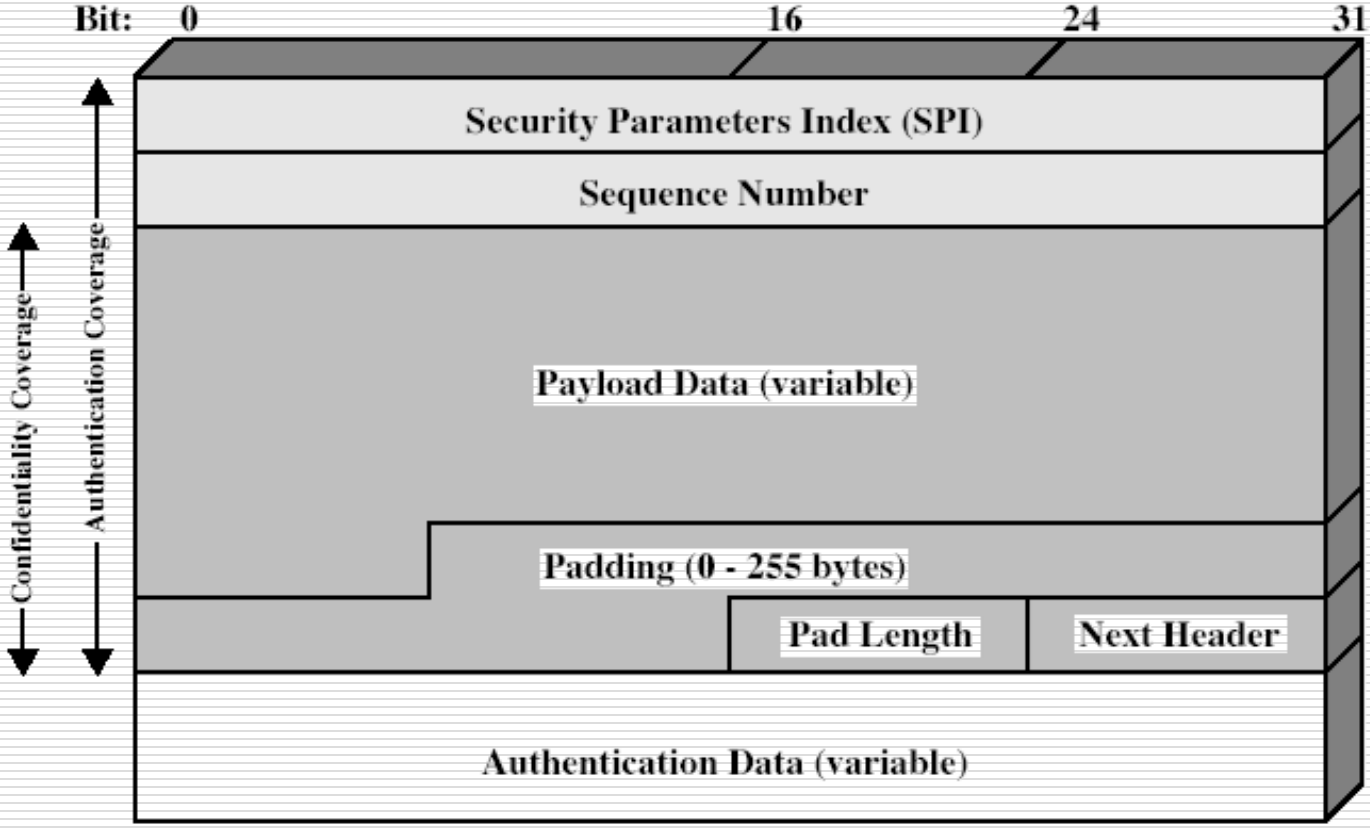
ویژگیها

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

Encapsulating Security Payload (ESP)

- فیلدهای ESP
  - SPI : شناسه SA
  - Sequence Number : شمارنده برای جلوگیری از حمله تکرار مشابه AH
  - Payload : محتوای بسته که رمز می‌شود
  - Padding : بیتهای اضافی
  - Pad Length : طول فیلد بالا
  - Next Header : نوع داده موجود در Payload Data
  - Authentication 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.

Encapsulating Security Payload (ESP)



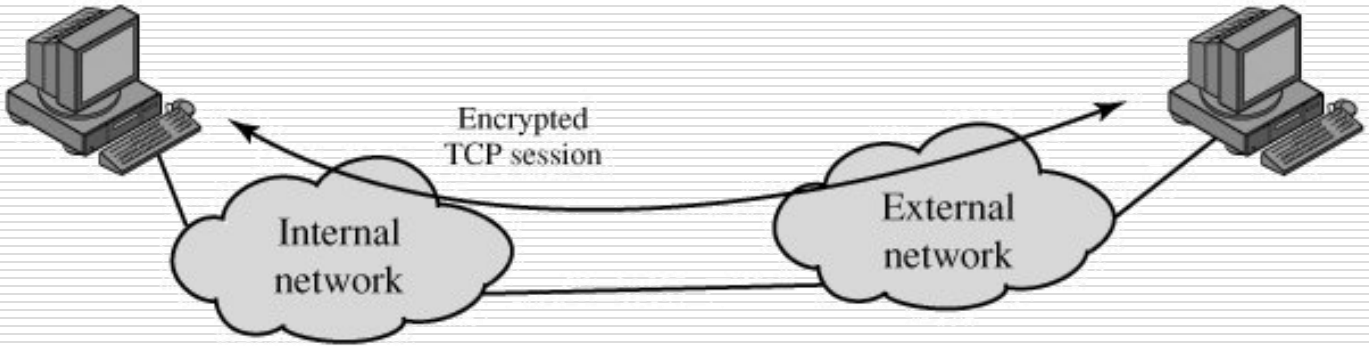
مُد انتقال در ESP

مُد انتقال

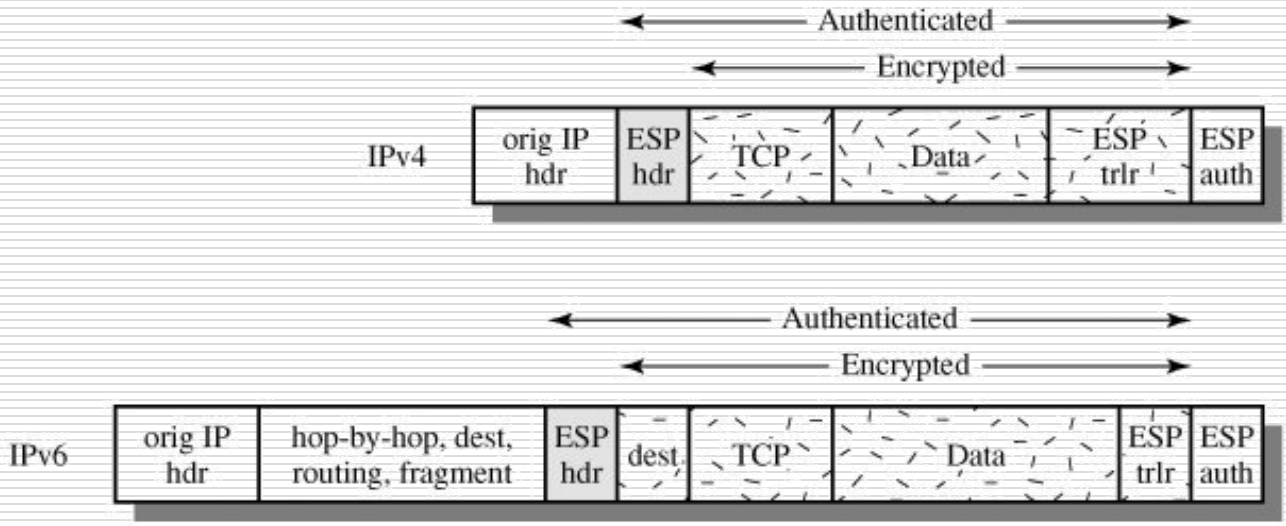
- تضمین محرمانگی بین hostها
- رمزنگاری بسته داده، دنباله ESP و اضافه شدن MAC درصورت انتخاب احراز اصالت توسط مبداء
- تعیین مسیر توسط مسیریابهای میانی با استفاده از سرآیندهای اصلی (که رمز نشده‌اند)
- چک کردن سرآیند IP توسط مقصد و واگشایی رمز باقیمانده پیام
- امکان آنالیز ترافیک

مُد انتقال در ESP

- برای ارتباط بین میزبان‌ها (H2H)



- محدوده ESP



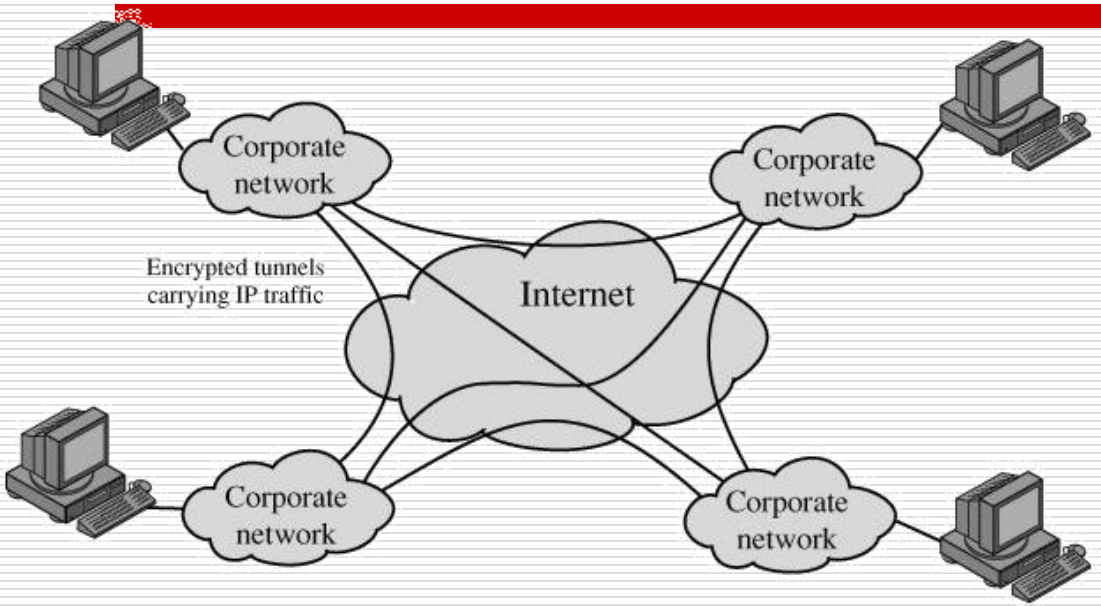
ESP trailer =
Padding, Pad Length, and Next Header Fields

مُد تونل در ESP

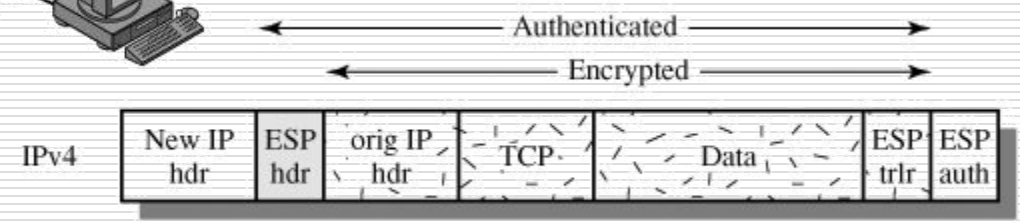
مُد تونل

- 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 نهایی
- مُد تونل IPSec یکی از روش‌های ایجاد شبکه‌های خصوصی مجازی (VPN) است.

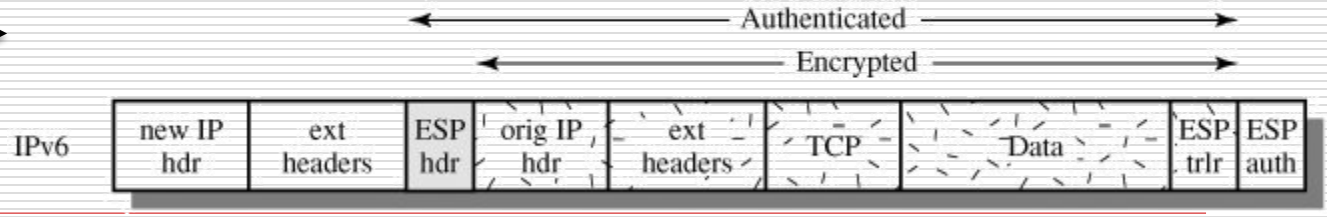
مُد تونل در ESP



- شبکه خصوصی مجازی (VPN)



- محدوده ESP در مُد تونل



فهرست مطالب

- مقدمه
- معماری IPSec
- پروتکل AH
- پروتکل ESP
- **ترکیب SAها**
- مدیریت کلید

ترکیب SAها

- 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

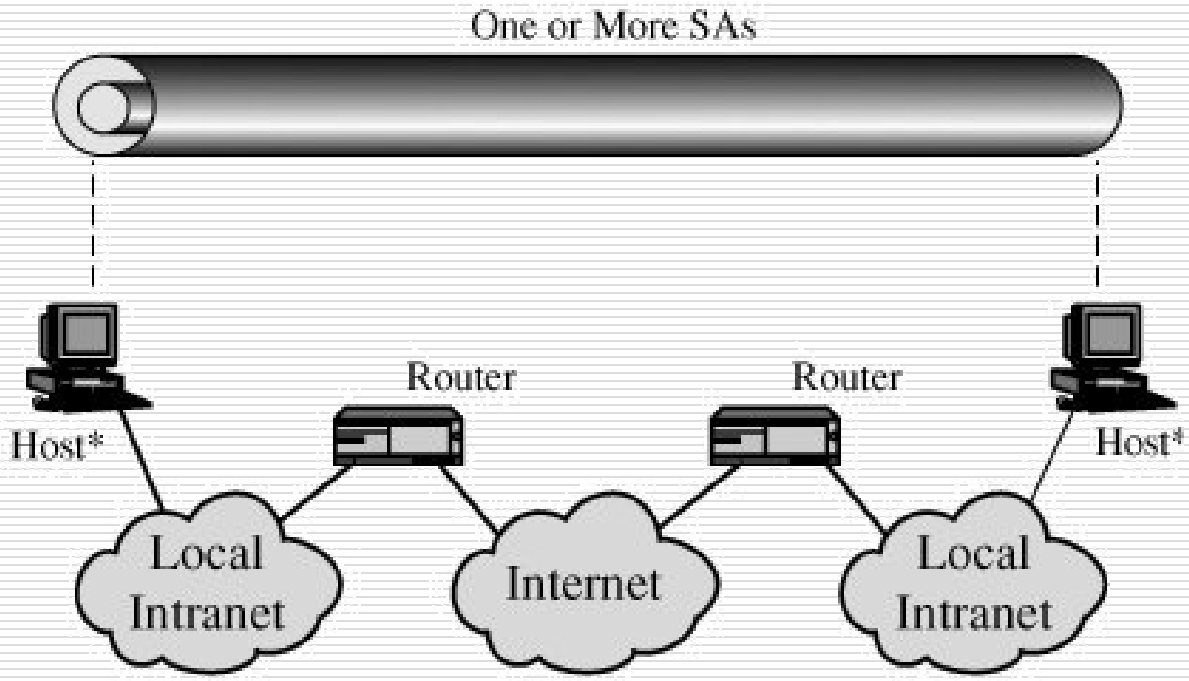
- ترتیبی از SAها که باید بر روی یک بسته اِعمال شوند، bundle نامیده می شوند.
- SAها در یک bundle به دو طریق قابل ترکیب هستند:
  - Transport Adjacency
    - اِعمال چند SA در مُد انتقال به بسته
    - صرفاً یک سطح از ترکیب را برای AH و ESP فراهم می‌نماید.
  - Iterated Tunneling
    - ایجاد چند لایه امنیتی با تونل‌های تو در تو
    - مبدا و مقصد هر تونل می‌تواند در سایتهای مختلفی از مسیر باشد.

ترکیب SAها

- امکان داشتن **احراز اصالت و محرمانگی به صورت توأم** از طریق:
  - ESP with Authentication Option: احراز اصالت محتوای رمزشده
    - مُد انتقال: عدم حفاظت سرآیند IP
    - مُد تونل: حفاظت کل بسته داخلی
  - Transport Adjacency: اِعمال ESP و سپس AH بر روی آن در مُد انتقال
    - حفاظت از سرآیند IP و سرآیند ESP، حفظ محرمانگی بسته
  - Transport-Tunnel Bundle: اِعمال AH در مُد انتقال و سپس ESP در مُد تونل
    - احراز اصالت داده و سرآیند IP (به غیر از فیلدهای متغیر)
    - محرمانگی کل بسته و امضای آن

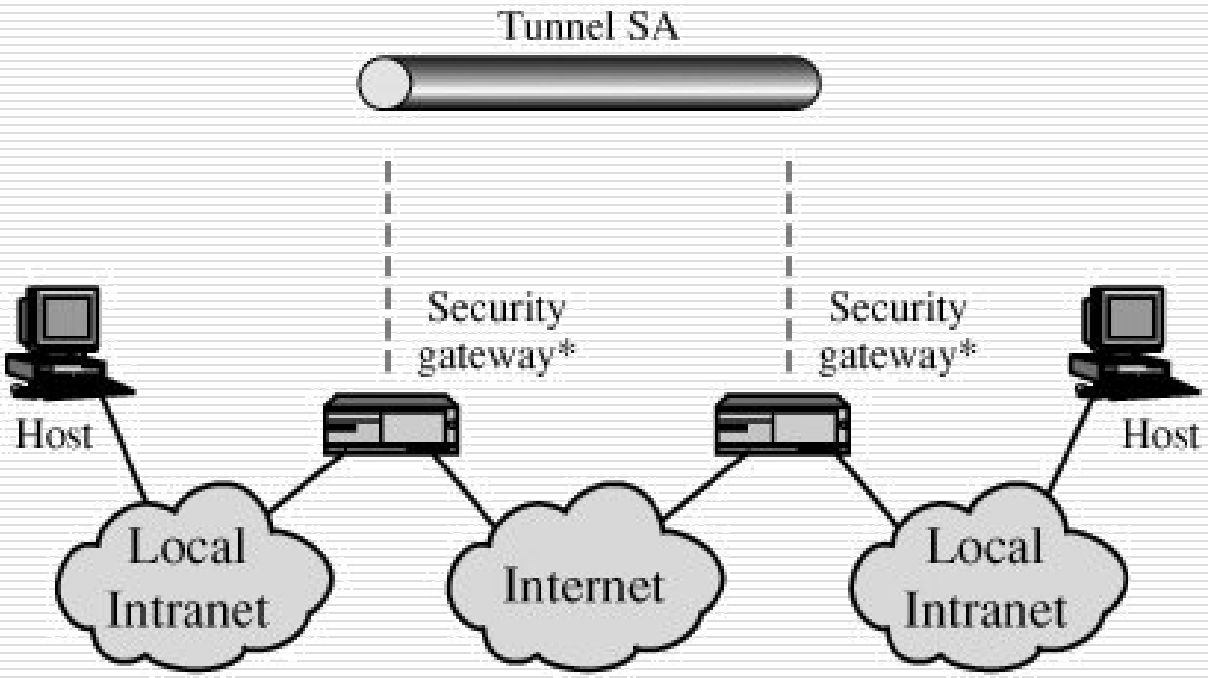
ترکیب SAها: حالت ۱

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



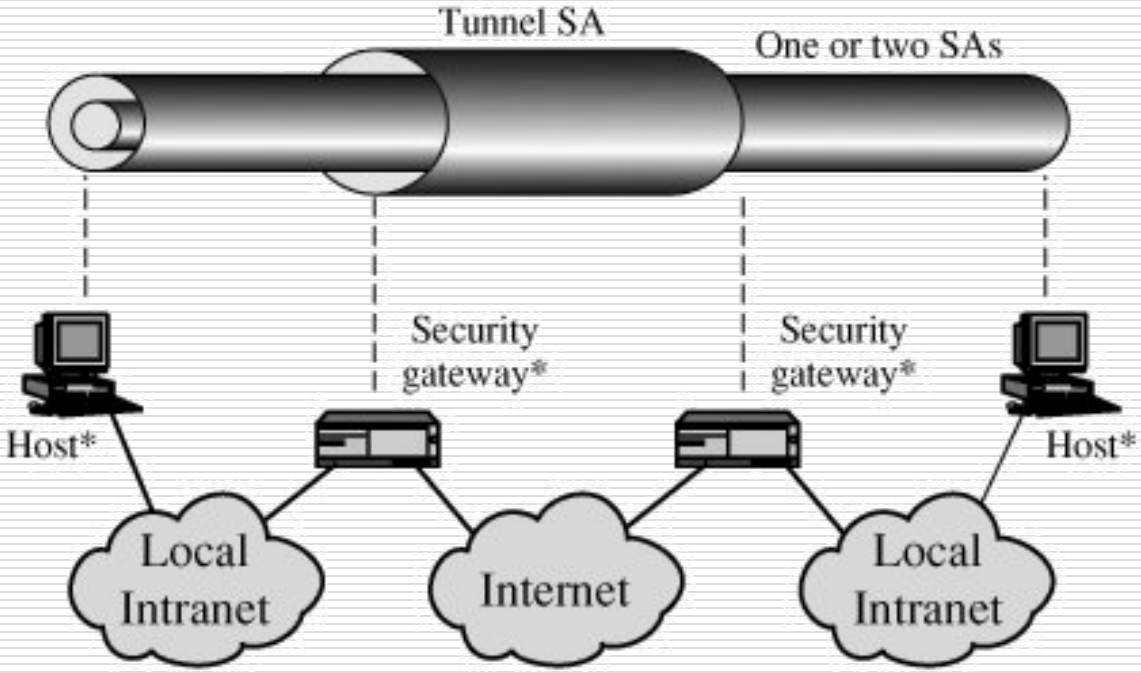
ترکیب SAها: حالت ۲

- برقراری تونل اَمن بین دروازه‌ها: شبکه خصوصی مجازی
- ایجاد تونل در یکی از مُدهای AH، ESP و یا ESP with Auth.



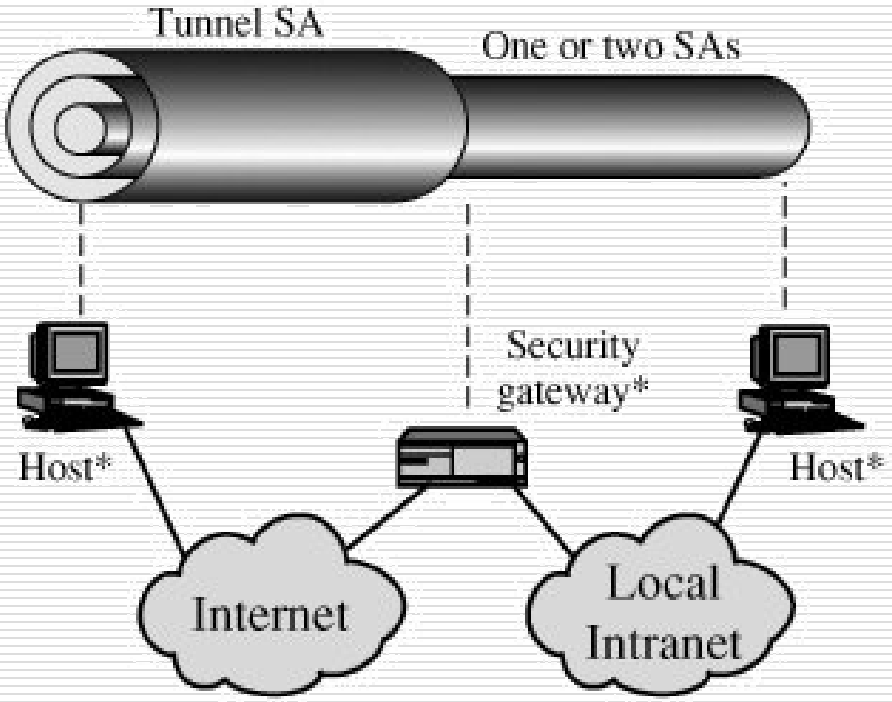
ترکیب SAها: حالت ۳

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



ترکیب SAها: حالت 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 **IKEv1** و **IKEv2** است.

IKEv1

- طراحی نه فقط برای IPSec، بلکه برای انواع پروتکلهایی که به تبادل کلید نیاز داشتند.
  - به شدت عام و پیچیده؛ پر از مشکلات امنیتی!
  - استاندارد شده در سه RFC (۲۴۰۷ الی ۲۴۰۹) در سال ۱۹۹۸
  - به حدی پیچیده که حتی پیاده‌سازان (سیسکو، مایکروسافت، ...) نتوانستند برداشت واحدی از استاندارد داشته باشند!
  - نقض غرض! هدف استاندارد، یکسان‌سازی برداشتها بود.
- در دنیای واقع فقط برای IPSec مورد استفاده قرار گرفت.

وضعیت IKEv1 در حال حاضر

- اگرچه IKEv2 در سال ۲۰۰۵ استاندارد شد، ولی IKEv1 در حال حاضر به طور گسترده‌تری مورد استفاده است.
  - ویندوزهای XP و ۲۰۰۳ به قبل فقط IKEv1
  - IOS سیسکو نسخه ۱۲ به قبل فقط IKEv1 (فعلاً فقط نسخه ۱۵ از IKEv2 پشتیبانی می‌کند)
  - لازم است با IKEv1 آشنایی داشته باشیم.

دو پروتکل مورد استفاده در IKEv1

- **ISAKMP:** Internet Security Association and Key Management Protocol
  - ☜ چارچوب کلی (بستر) پروتکل تبادل کلید
- Oakley + SKEME (Secure Key Exchange Mechanism)
  - ☜ پروتکل واقعی تبادل کلید

ISAKMP (آیساکمپ)

- تعریف شده در RFC 2408
- چارچوبی برای احراز هویت و تبادل کلید فراهم می‌آورد، ولی سازوکار را تعریف نمی‌کند.
- به عبارت دیگر، ISAKMP می‌تواند بستری باشد که روی آن انواع پروتکلهای احراز هویت و تبادل کلید اجرا شوند.

پروتکل ISAKMP

- تعریف رویه‌ها و قالب بسته‌ها برای برقراری، مذاکره، تغییر یا حذف SA
- قالب بسته‌های ISAKMP
  - یک پیام ISAKMP شامل سرآیند و یک نوع بخش داده‌ای برای تبادل داده‌های مربوط به تولید کلید و احراز اصالت است.
- رویه‌ها
  - شامل مجموعه‌ای از تعامل‌های (پروتکل‌های) از قبل تعریف شده برای امور مختلف

انواع بخش داده ای در ISAKMP

Type	Description
Security Association (SA)	Used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place.
Proposal (P)	Used during SA negotiation; indicates protocol to be used and number of transforms.
Transform (T)	Used during SA negotiation; indicates transform and related SA attributes.
Key Exchange (KE)	Supports a variety of key exchange techniques.
Identification (ID)	Used to exchange identification information.
Certificate (CERT)	Used to transport certificates and other certificate- related information.
Certificate Request (CR)	Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities.
Hash (HASH)	Contains data generated by a hash function.
Signature (SIG)	Contains data generated by a digital signature function.
Nonce (NONCE)	Contains a nonce.
Notification (N)	Used to transmit notification data, such as an error condition.
Delete (D)	Indicates an SA that is no longer valid.

انواع تعاملات در ISAKMP

- Base Exchange: تبادل کلید و احراز اصالت بدون گمنامی.
- Identity Protection Exchange: توسعه تعامل پایه با حفاظت از شناسه طرفین و گمنامی آنها.
- Authentication Only Exchange: صرفاً احراز اصالت دوطرفه بدون تبادل کلید.
- Aggressive Exchange: کاهش تعداد پیامهای تبادلی بدون گمنامی.
- Informational Exchange: ارسال یکطرفه اطلاعات برای مدیریت SA.

Oakley + SKEME

- **Oakley** (اُکلی) و **SKEME** (اسکیم) دو خانواده از پروتکلهای احراز هویت و تبادل کلید هستند (هر دو برگرفته از پروتکل STS که مبتنی بر Diffie-Hellman است)
- IKEv1 از بخشی از Oakley و بخشی از SKEME استفاده می‌کند.
  - بیشتر متمایل به Oakley
  - SKEME فقط برای احراز هویت مبتنی بر رمزنگاری کلید عمومی و فرآیند تجدید کلید سریع مورد استفاده قرار می‌گیرد.

پروتکل Oakley

- فرم توسعه یافته پروتکل Diffie-Hellman که ضعفهای آن را برطرف کرده است.

- **خصوصیات پروتکل Oakley**

  - **مقابله با حمله مرد میانی در DH:**

    - احراز اصالت در تبادل کلید DH با استفاده از Preshared Key، یا Digital Signature

پروتکل Oakley

- خصوصیات پروتکل **Oakley** (ادامه)

  - **مقابله با حمله تکرار:**

    - با استفاده از نانس با حمله‌های تکرار مقابله می‌کند.

  - **مقابله با حمله Clogging در DH:** اجرای DH بسیار سنگین است، و ایجاد تعداد زیادی اتصال توسط مهاجم سبب نوعی حمله منع خدمت (DoS) به نام Clogging می‌شود.

    - با استفاده از تعریف مفهومی تحت عنوان کوکی (Cookie) مشکل این حمله را برطرف می کند.

پروتکل Oakley

مقابله با حمله Clogging

- استفاده از **کوکی** (توسط هر یک از طرفین) به صورت زیر:
  - شروع پروتکل با ارسال درخواست از سوی یکی از طرفین ارتباط
  - ارسال کوکی توسط طرف دیگر
  - نیاز به ارسال کوکی توسط مبدأ در اولین پیام DH
- اگر مهاجم از آدرس جعلی برای ارسال کوکی استفاده کرده باشد، چون کوکی را دریافت نمی‌کند، نمی‌تواند DH را آغاز نماید.
- باید تولید و وارسی کوکی کم هزینه باشد تا حملات اتلاف منابع ممکن نباشد.

پروتکل Oakley

- **مقابله با حمله Clogging** (ادامه)
  - برای جلوگیری از نیاز به ذخیره‌سازی کوکی، می‌توان کوکی را تابعی از مقادیر زیر (با اعمال یک تابع درهم‌ساز) در نظر گرفت. در اینصورت فقط نیاز به یک مقدار سری محلی برای وارسی تمام درخواستهای تبادل کلید است.
    - آدرس IP مبدا و مقصد
    - آدرس پورت مبدا و مقصد
    - مقدار سری محلی

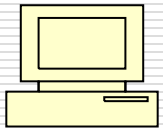
$$\textbf{Cookie= H(}\text{SrcIP, DstIP, SrcPort, DstPort, } S_{local}\textbf{)}$$

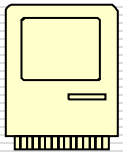
پروتکل Oakley

- مقابله با حمله **Clogging** (ادامه)

آغازکننده ارتباط

کارگزار





I Want to talk →

← Cookie

Cookie= H(SrcIP, DstIP, SrcPort, DstPort, S**)**

Cookie, Start rest of the protocol →

Cookie= H(SrcIP, DstIP, SrcPort, DstPort, S**)?**

اگر برقرار است ادامه بده

فازهای IKEv1

- **فاز اول:**
  - انجام احراز اصالت دوطرفه و تبادل کلید نشست IKE
  - برپاسازی Main SA یا IKE SA
- **فاز دوم:**
  - برپاسازی IPSec SAهای مورد نیاز با استفاده از کلید نشست حاصل از فاز اول

- چرا دو فاز؟
  - احراز اصالت دوطرفه هزینه‌بر است و برای برپاسازی چند SA مختلف، فقط یکبار انجام آن کافی است.
- جزئیات فازها بر حسب نوع تعامل انتخاب شده (بر اساس ISAKMP) متفاوت است.

سبکهای مورد استفاده در IKEv1

- **فاز ۱:** دو سبک
  - سبک اصلی (Main Mode)
    - شامل ۶ پیام (سه زوج پیام)
    - حافظ گمنامی (Anonymity) طرفین (Identity Protection)
  - سبک هجومی (Aggressive Mode)
    - شامل ۳ پیام؛ بدون گمنامی

- **فاز ۲:** یک سبک
  - سبک سریع (Quick Mode): شامل ۳ پیام

پیام‌های سبک اصلی (Main)

- **زوج پیام ۱:** تبادل سیاستهای IKEv1 پیکربندی شده روی هر ابزار
  - شامل ارسال Security Parameter Index (SPI) توسط هر طرف به عنوان شناسه SA
- **زوج پیام ۲:** تبادل DH
- **زوج پیام ۳:** احراز هویت ISAKMP
  - طرفین یکدیگر را با استفاده از کلید مشترک (PSK) یا کلید عمومی طرف مقابل احراز هویت می‌کنند.

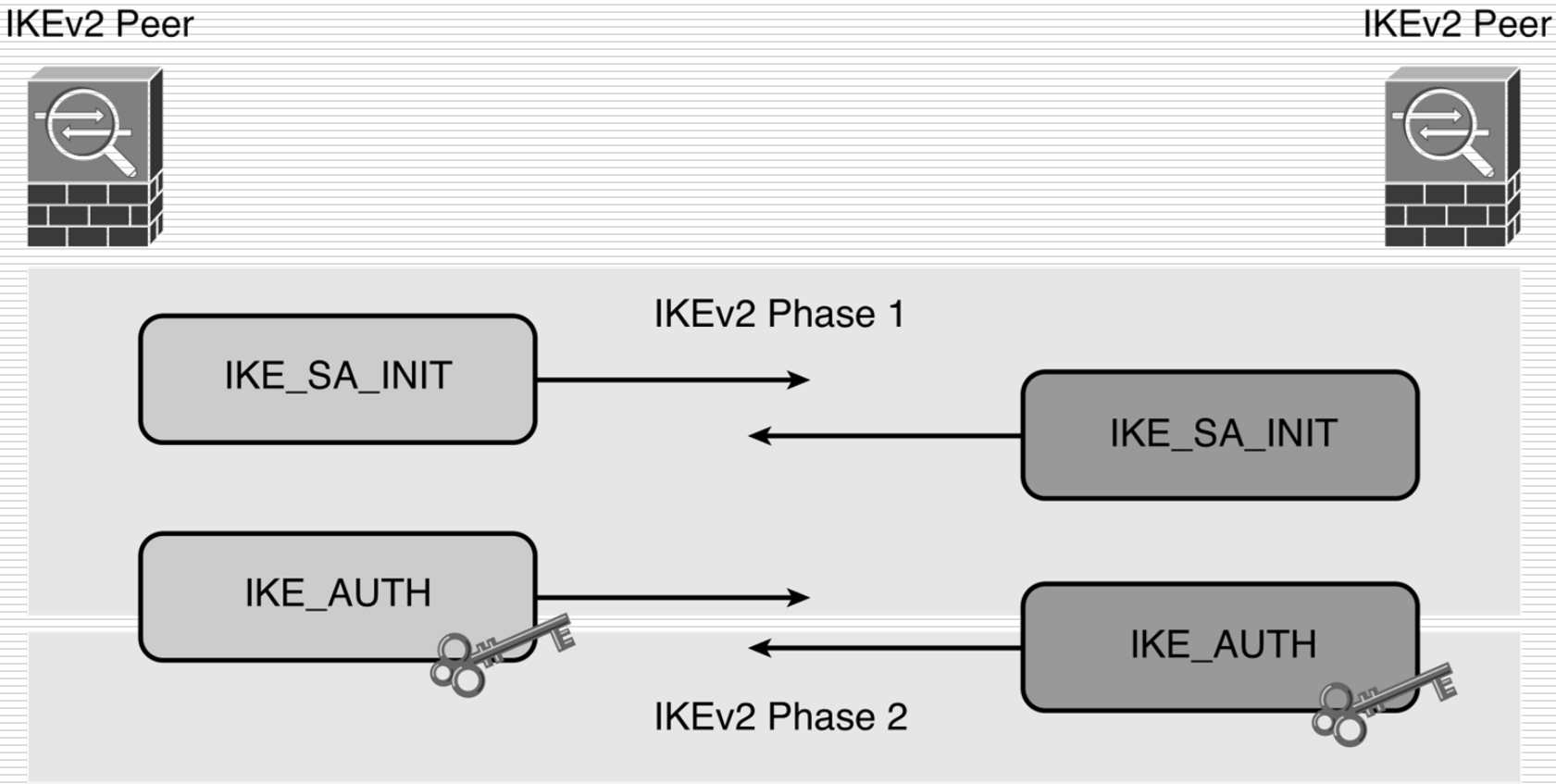
پیام‌های سبک هجومی (Aggressive)

- **پیام ۱:** هویت طرف اول، SPI، پیام نخست DH، سیاستهای IKEv1
- **پیام ۲:** هویت طرف دوم، SPI، پیام دوم DH، سیاستهای IKEv1، امضا/MAC برای احراز هویت
- **پیام ۳:** SPI، امضا/MAC برای احراز هویت

IKEv2

- IKEv2 برای ساده و کارآمدسازی IKEv1 ایجاد شد. به علاوه، امنیت IKEv1 را در مواردی بهبود بخشید.
  - **نسخه اولیه:** سال ۲۰۰۵ (RFC 5996)
  - **آخرین به‌روز رسانی:** سال ۲۰۱۴ (RFC 7296)
- IKEv1 حداقل ۶ پیام و حداکثر ۹ پیام برای تبادل کلید دارد.
- Main mode = 6 + 3 (Quick mode)
- Aggressive mode = 3 + 3 (Quick mode)
- IKEv2 فقط از دو زوج (= ۴) پیام بهره می‌گیرد.

فازها و پیامهای IKEv2



زیر پروتکل IKE_SA_INIT (فاز ۱)

- تبادل پارامترهای مختلف
  - تبادل پارامترهای امنیتی و الگوریتمهای امنیتی (رمزنگاری و صحت)
  - تبادل مقادیر مربوط به پروتکل Diffie-Hellman
  - تبادل نانس و SPI

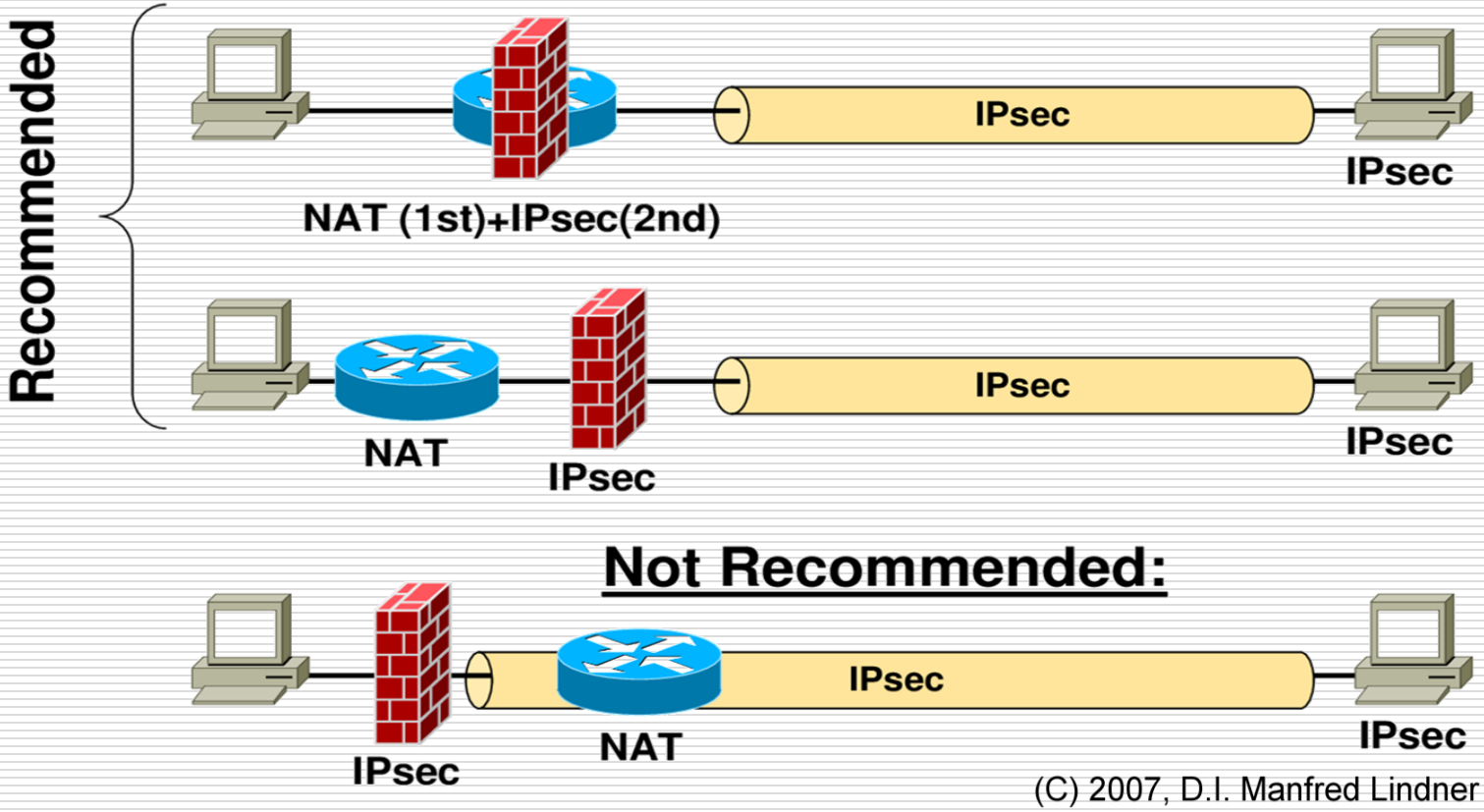
- پس از این تبادلات، طرفین روی مقدار SKEYSEED توافق می‌کنند.
  - یک بذر برای تولید کلیدهای رمزنگاری نشست

زیر پروتکل IKE_AUTH (فازهای ۱ و ۲)

- روی IKE_SA ایجاد شده توسط IKE_SA_INIT عمل می‌کند.
- **هدف ۱:** احراز هویت طرفین
  - به کمک کلید متقارن (PSK)، کلید عمومی (گواهی دیجیتال) یا Extensible Authentication Protocol (EAP)
- **هدف ۲:** تبادل پروتکلهای رمزگذاری، احراز هویت و صحت برای ایجاد نخستین SA جهت به‌کارگیری در AH/ESP
- **توجه:** بر خلاف IKEv1، پروتکل IKE_AUTH قابلیت گمنامی ندارد و هویت طرفین برای شبکه عمومی آشکار می‌شود.

مشکل IPSec با NAT

- ترتیب استفاده از NAT و IPSec



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 مجددا محاسبه شود ولی با اِعمال 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

مرکز امنیت شبکه شریف

http://dnsl.ce.sharif.edu

پست الکترونیکی

amini@sharif.edu