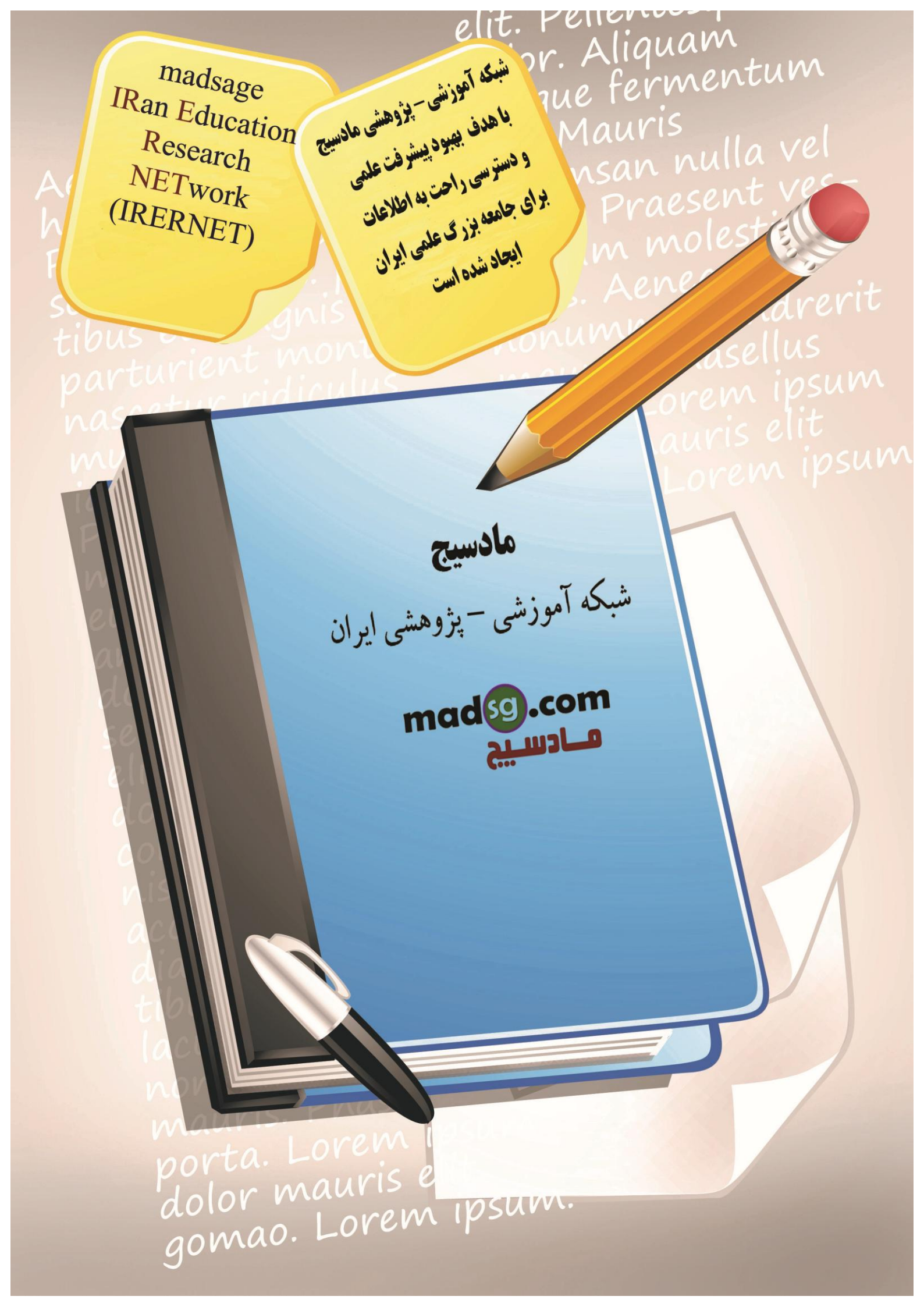

madsage
IRan Education
Research
NETwork
(IRERNET)
شبکه آموزشی-پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است
مادسیج
شبکه آموزشی - پژوهشی ایران
madsg.com
مادسیج

یا ذاالامن والامان

امنیت داده و شبکه

امنیت IP

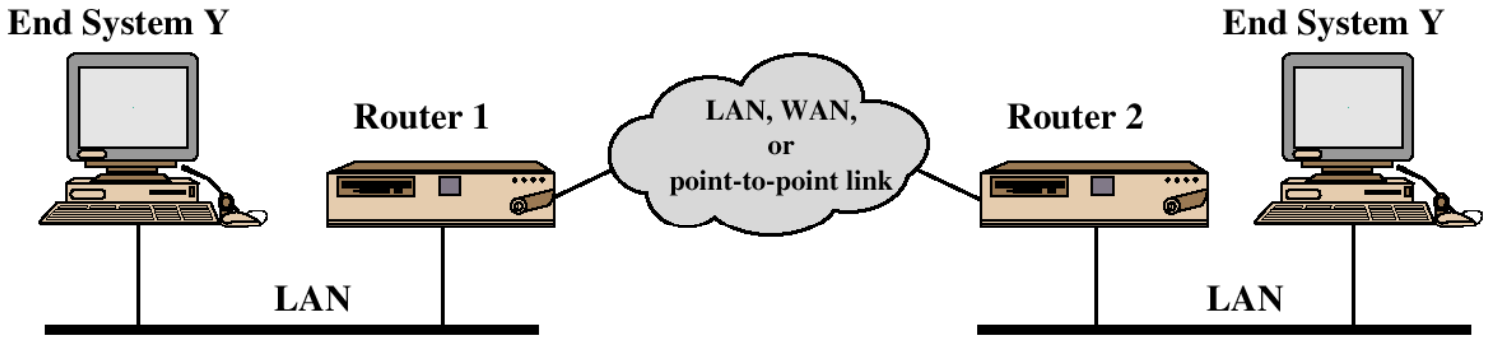
مرتضی امینی - نیمسال اول ۹۱-۹۰

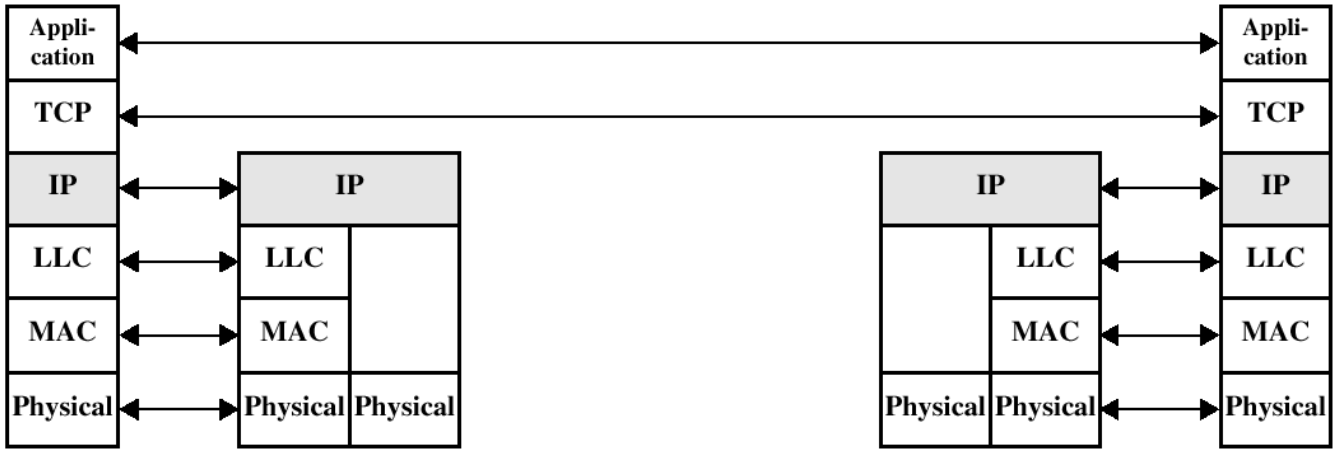
مرکز امنیت داده و شبکه شریف
http://dnsl.ce.sharif.edu

فهرست مطالب

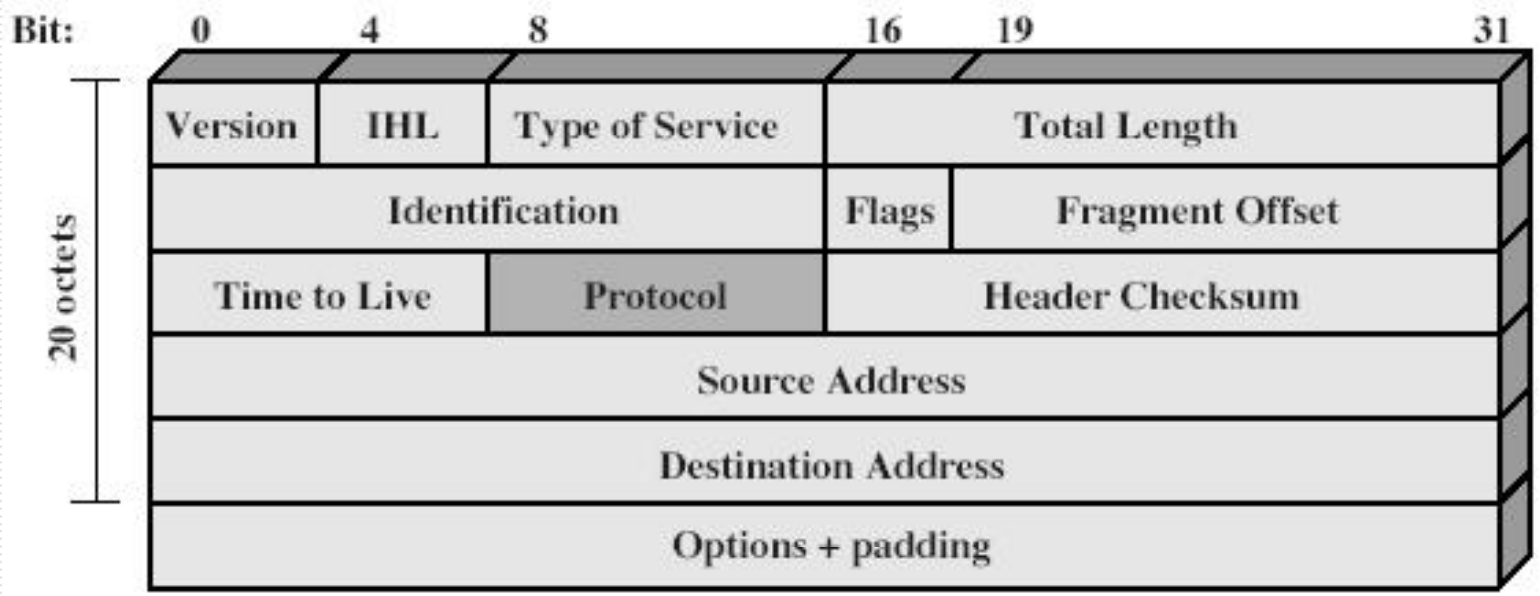
- مقدمه
- معماری IPSec
- پروتکل AH
- پروتکل ESP
- ترکیب SAها
- مدیریت کلید

مقدمه – مثالی از TCP / IP





IPV4


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

مقدمه

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

مقدمه

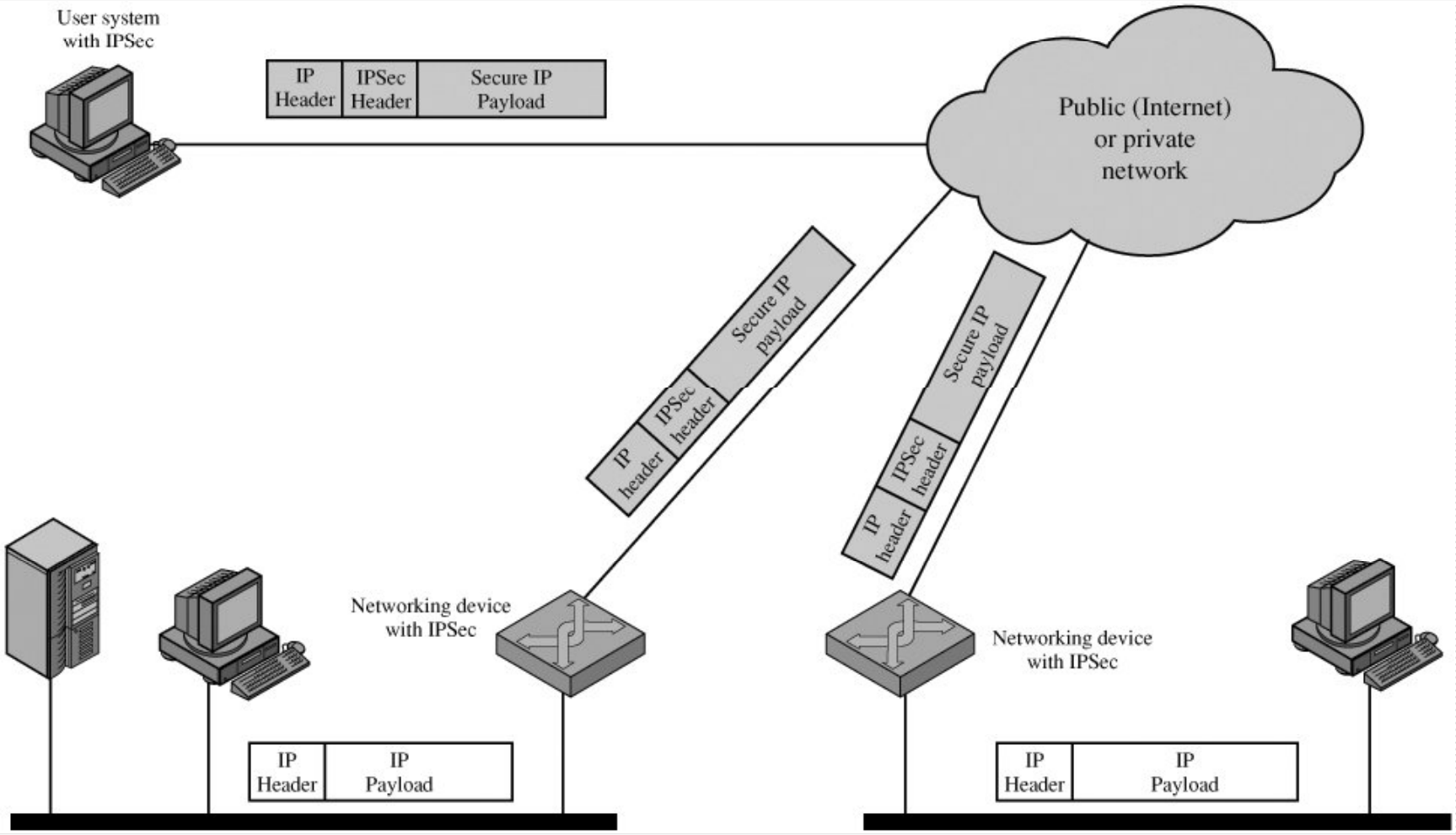
- IPSec یک پروتکل تنها نیست بلکه مجموعه‌ای از الگوریتم‌های امنیتی است که چارچوبی کلی را برای برقراری یک ارتباط امن فراهم می نماید.
- سرویس‌های امنیتی فراهم شده توسط IPSec
  - احراز اصالت (به همراه کنترل صحت داده‌ها)
  - محرمانگی بسته‌ها
  - مدیریت کلید (تبادل امن کلید)

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
- به وجود آوردن خدمات امنیتی برای کاربردهای دیگر (مثل تجارت الکترونیکی)

نمونه‌ای از کاربرد IPSec



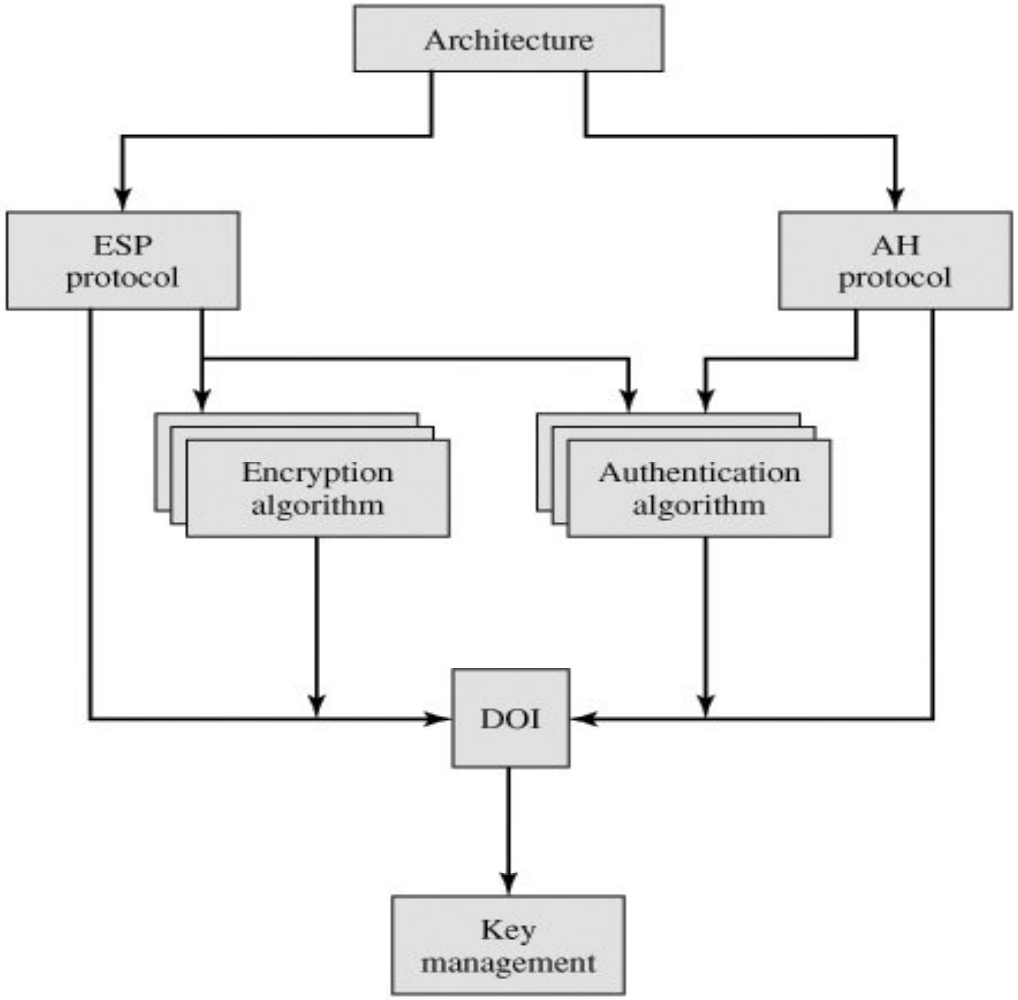
مقدمه

- مزایای استفاده از IPSec
  - تامین امنیت قوی بین داخل و خارج LAN در صورت بکارگیری در مسیریابها و حفاظ ها (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
- الزامی در IPv6 و اختیاری در IPv4
- 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:
  - کنترل دسترسی
  - 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)

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

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:**
- یک SA بصورت یکتا با ۳ پارامتر 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

مُدهای انتقال بسته در IPSec

- در هر دوی AH و ESP دو مُد انتقال 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) مثل کارگزار/کارفرما استفاده می‌شود.
- ESP : رمزنگاری (ضروری) و صحت (اختیاری) محتوای بسته
- AH : صحت محتوای بسته و قسمتهای انتخاب شده سرآیند بسته

مُد تونل در IPSec

مُد تونل

- مورد استفاده در ارتباط Gateway به Gateway.
- هیچ مسیریاب (router) میانی قادر به تشخیص سرآیند داخلی نیست.

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

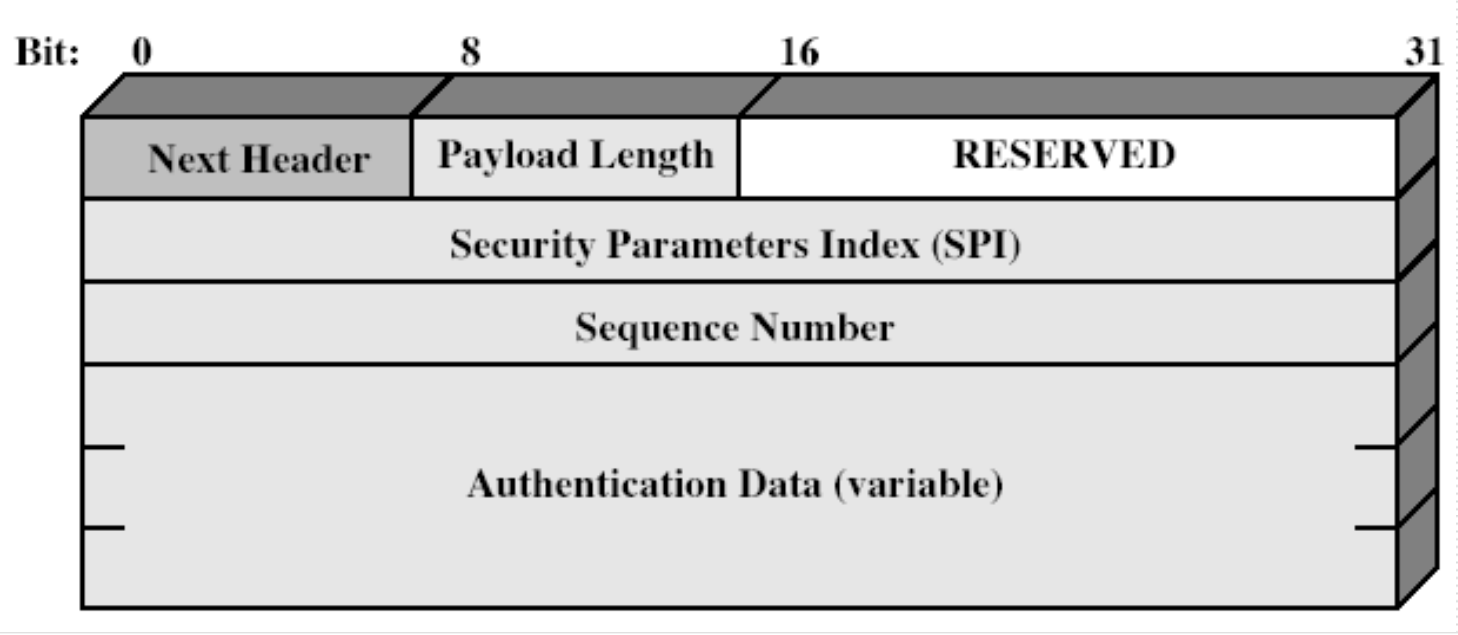
فهرست مطالب

- 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-MD5-96 یا HMAC-SHA-1-96
    - 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 HMAC
  - HMAC-MD5 یا HMAC-SHA-1
- 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)

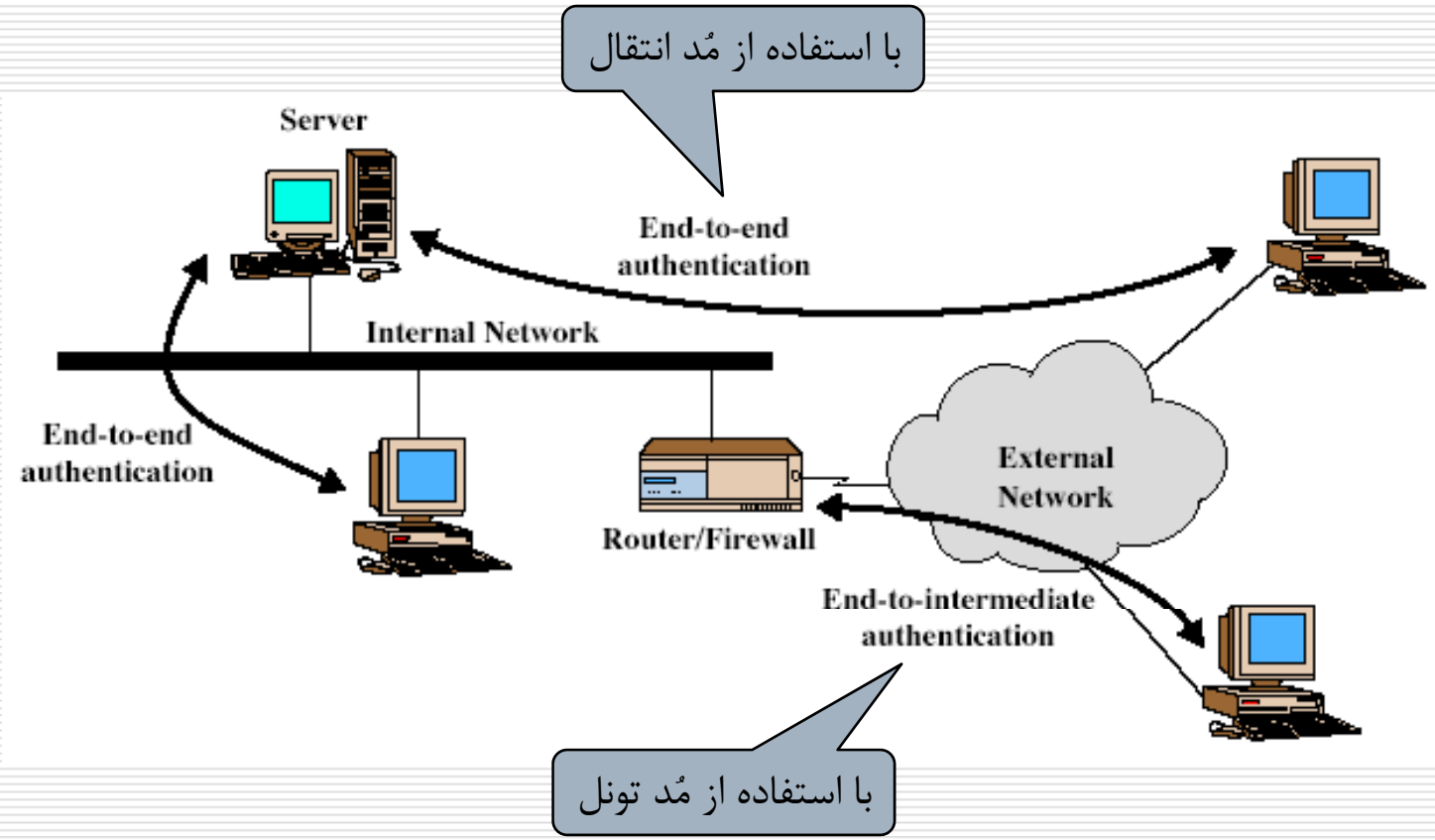
Authentication Header (AH)

- مُدهای انتقال و تونل در AH:

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

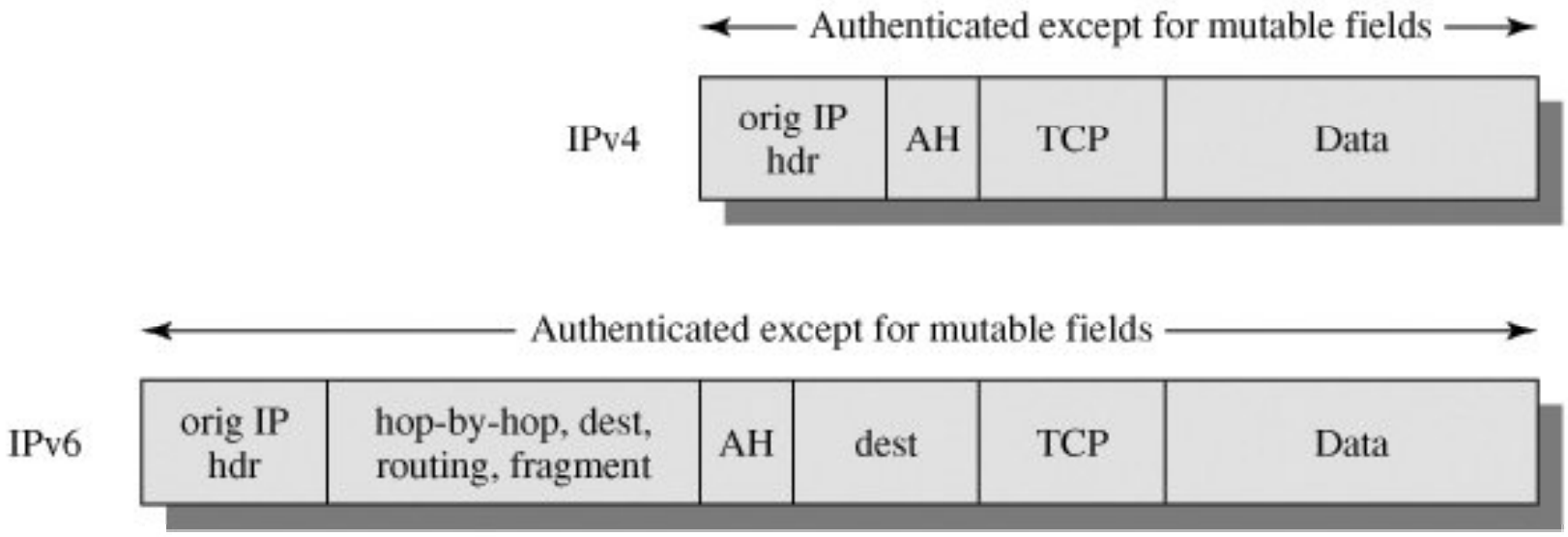
  - مُد تونل (Tunnel): برای احراز اصالت بین کاربر و حفاظ (firewall)

انواع احراز اصالت با AH



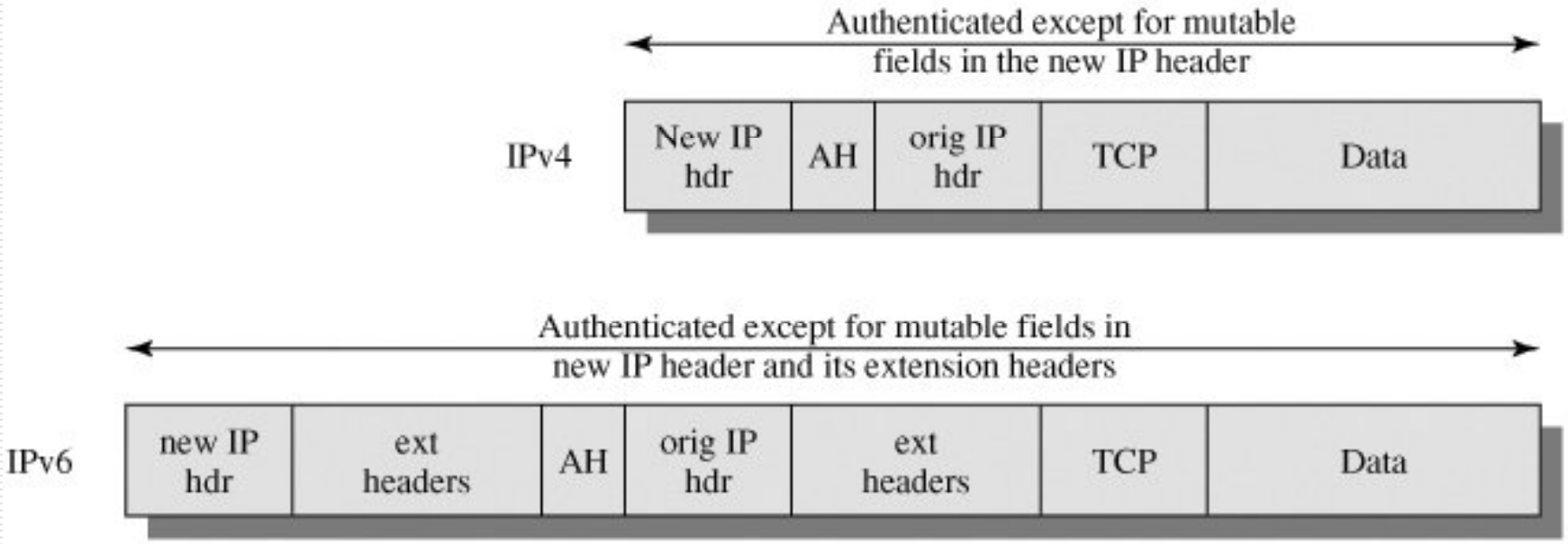
محدوده احراز اصالت AH

- مُد انتقال



محدوده احراز اصالت AH

- مُد تونل



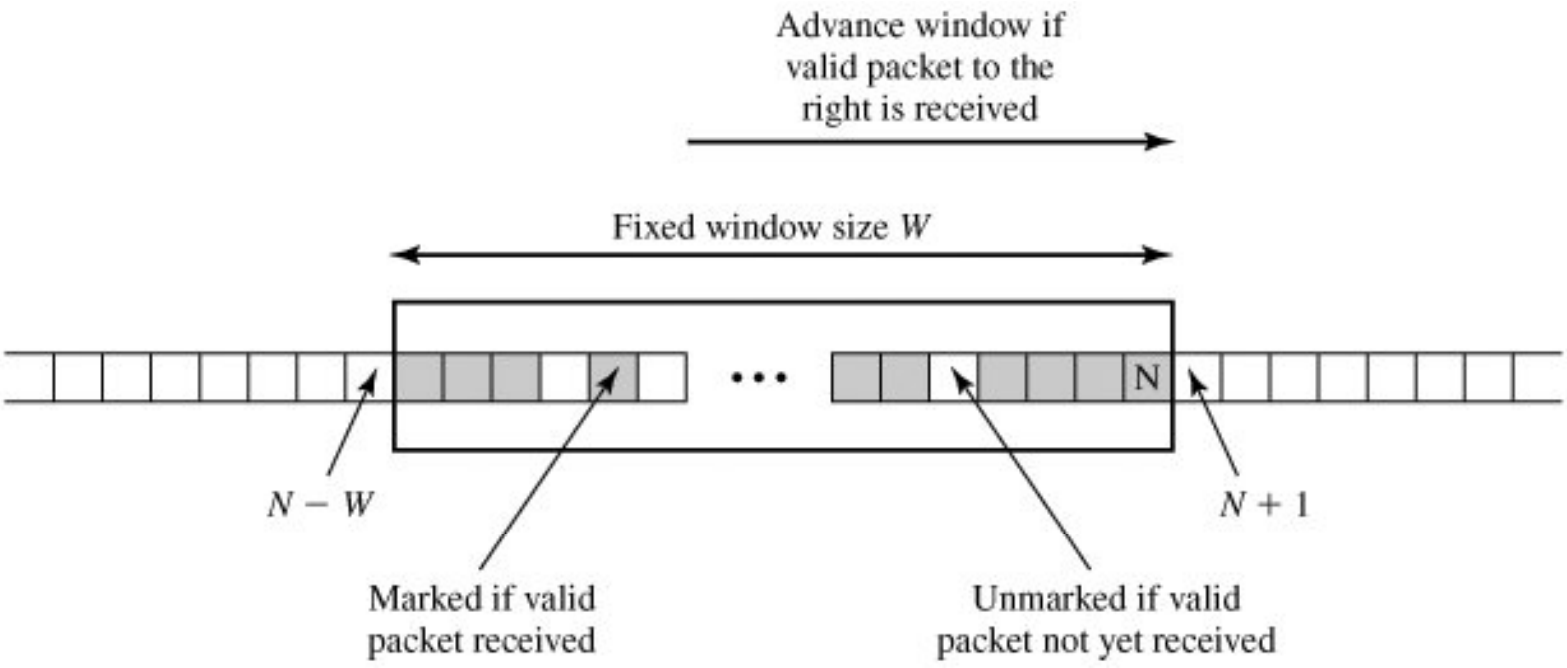
مقابله با حمله تکرار در AH

- 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 می شود.
  - 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 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

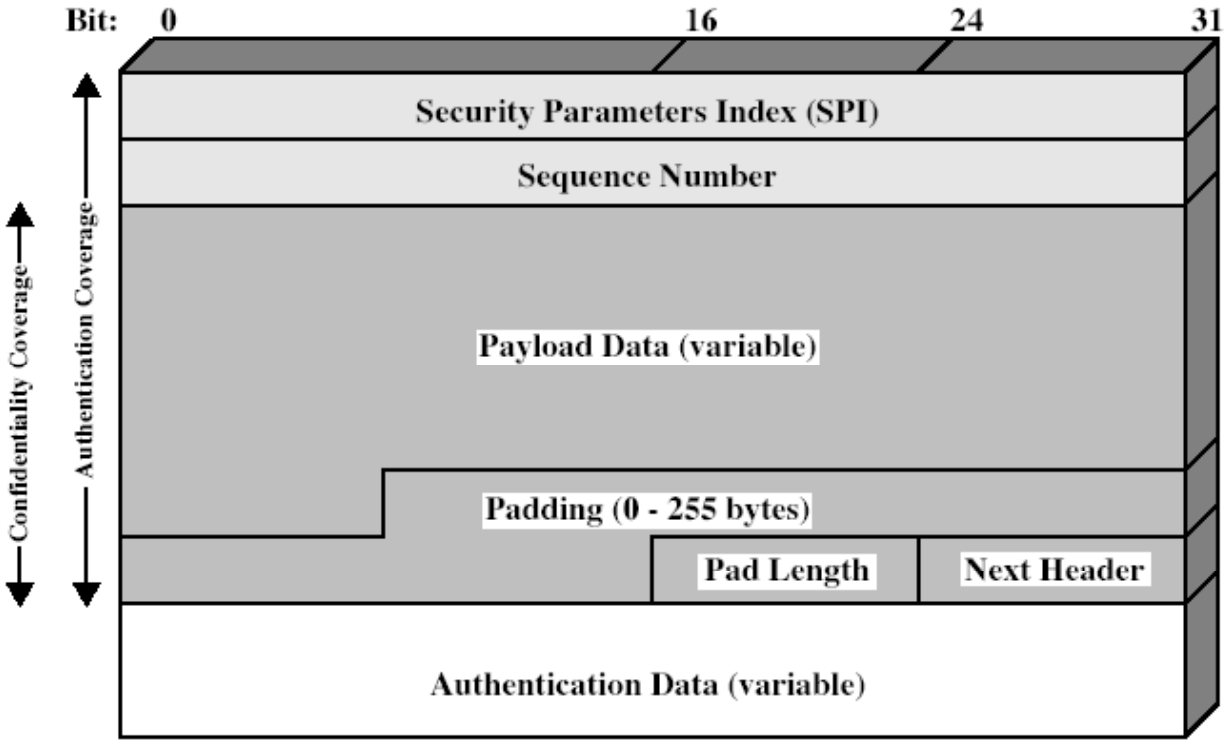
- پشتیبانی از محرمانگی داده و تا حدی محرمانگی ترافیک
- امکان احراز اصالت (مشابه AH)
- استفاده از الگوریتم DES در مد CBC (امکان استفاده از 3-DES, RC5, IDEA, 3-IDEA, CAST و Blowfish نیز وجود دارد).

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)

Encapsulating Security Payload (ESP)



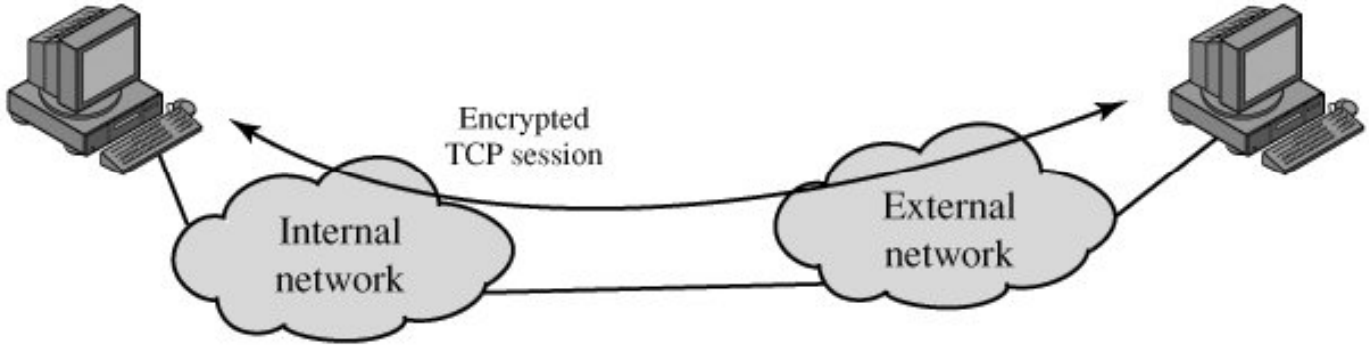
مُد انتقال در ESP

مُد انتقال

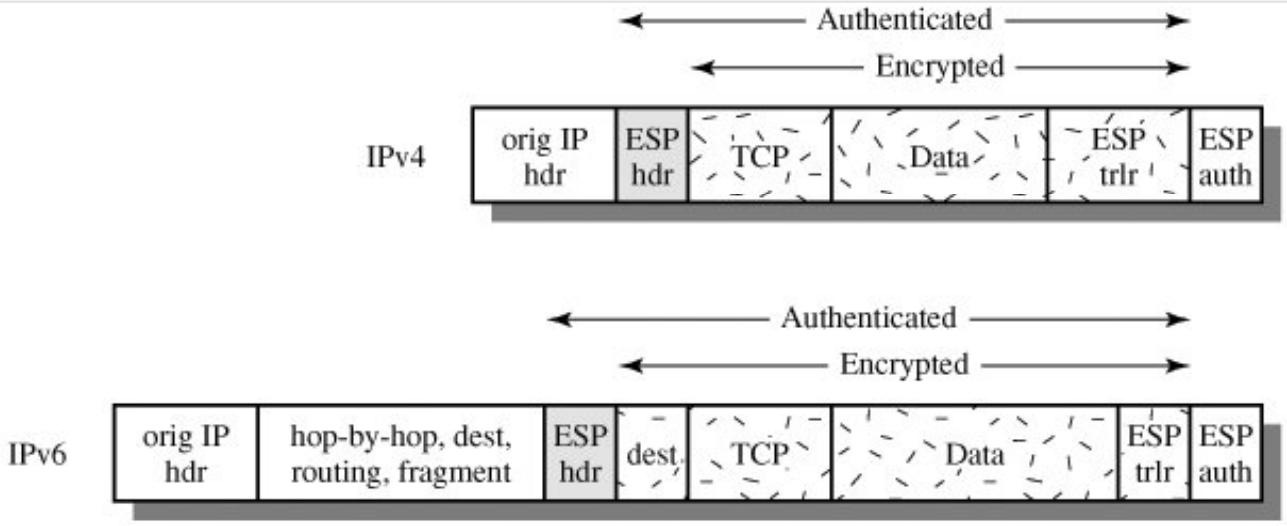
- تضمین محرمانگی بین hostها
- رمزنگاری بسته داده، دنباله ESP و اضافه شدن MAC درصورت انتخاب احراز اصالت توسط مبداء
- تعیین مسیر توسط مسیریابهای میانی با استفاده از سرآیندهای اصلی (که رمز نشده‌اند)
- چک کردن سرآیند IP توسط مقصد و واگشایی رمز باقیمانده پیام
- امکان آنالیز ترافیک

مُد انتقال در ESP

- برای ارتباط بین میزبان‌ها



- محدوده ESP



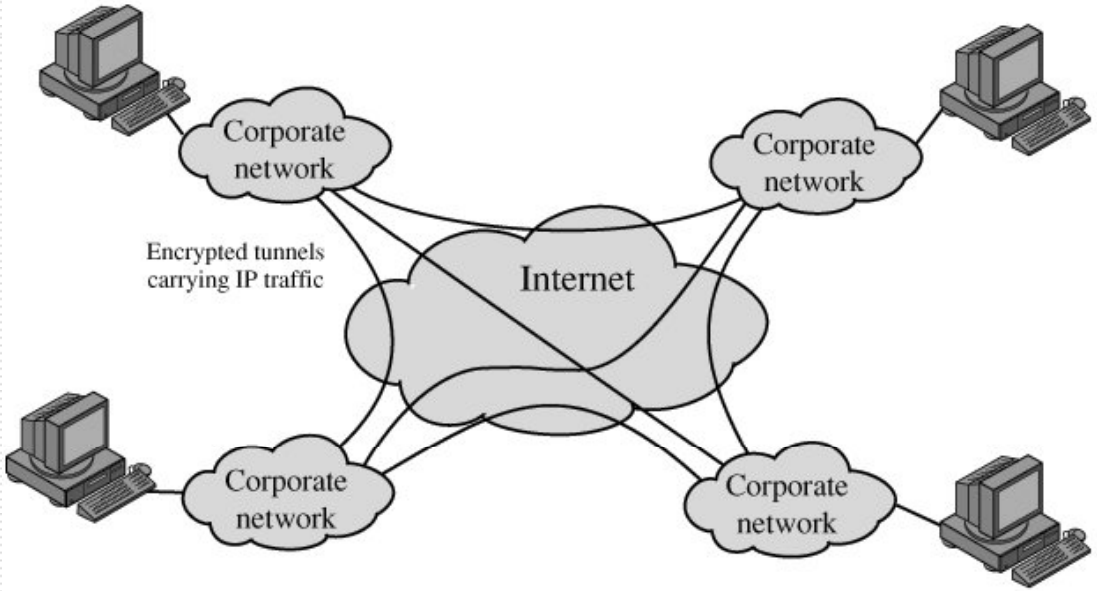
ESP trailer =
Padding, Pad Length, and Next Header Fields

مُد تونل در ESP

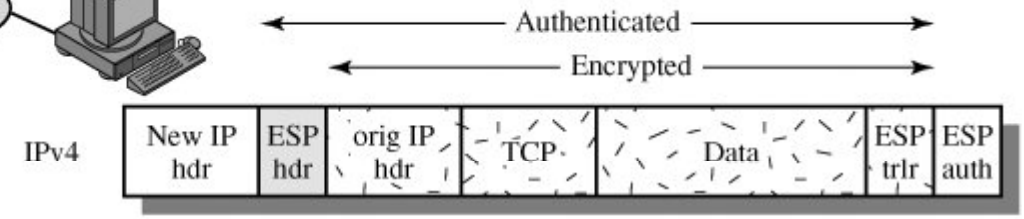
مُد تونل

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

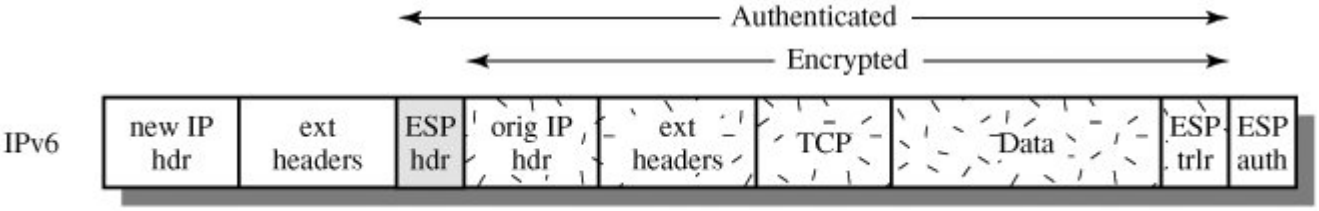
مُد تونل در ESP



- شبکه خصوصی مجازی (VPN)



- ESP محدوده در مُـد 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
  - پیاده سازی IPSec توسط host های متناظر
  - پیاده سازی IPSec توسط gateway ها
  - ترکیب دو حالت بالا

ترکیب SAها

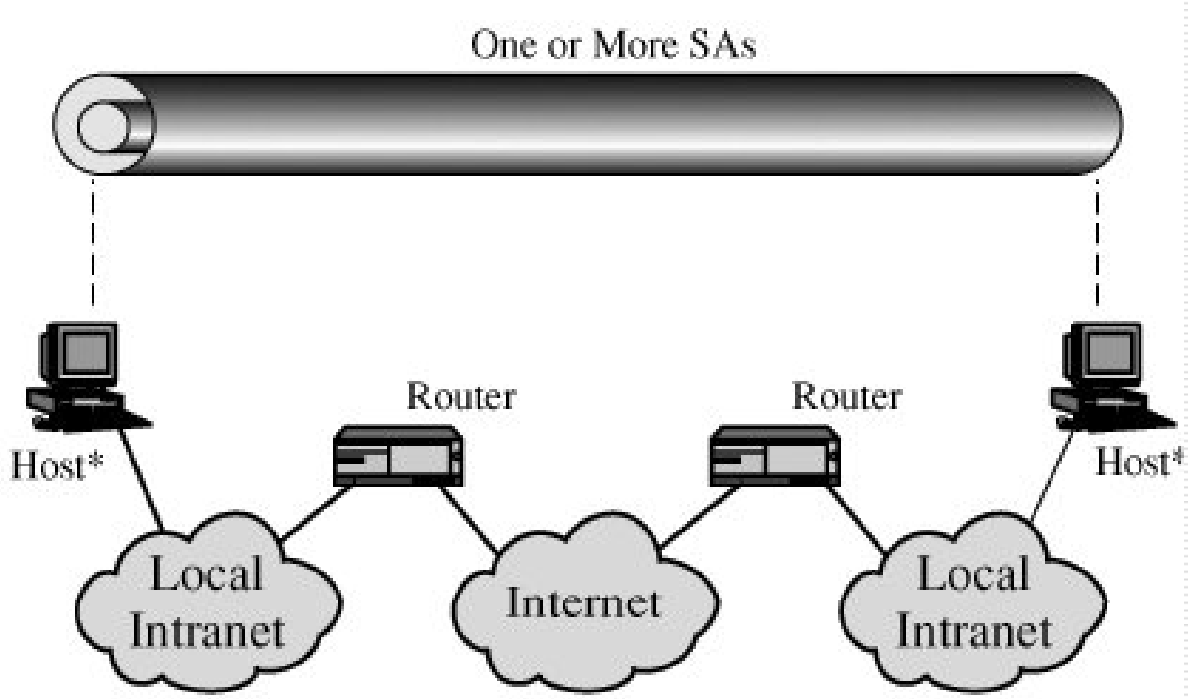
- ترتیبی از SAها که باید بر روی یک بسته اِعمال شوند، bundle نامیده می شوند.
- SAها در یک bundle به دو طریق قابل ترکیب هستند:
  - Transport Adjacency
    - اِعمال چند SA در مُد انتقال به بسته
    - صرفاً یک سطح از ترکیب را برای AH و ESP فراهم می‌نماید.
  - Iterated Tunneling
    - ایجاد چند لایه امنیتی 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

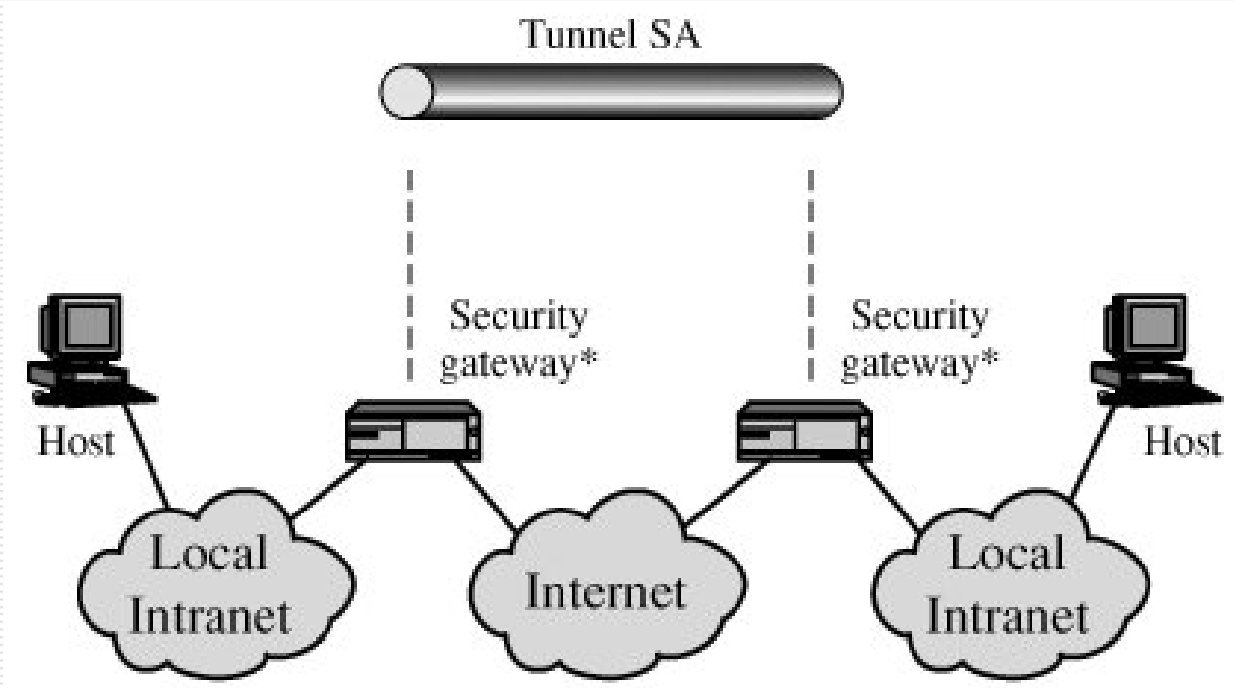
ترکیب SAها: حالت ۱

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



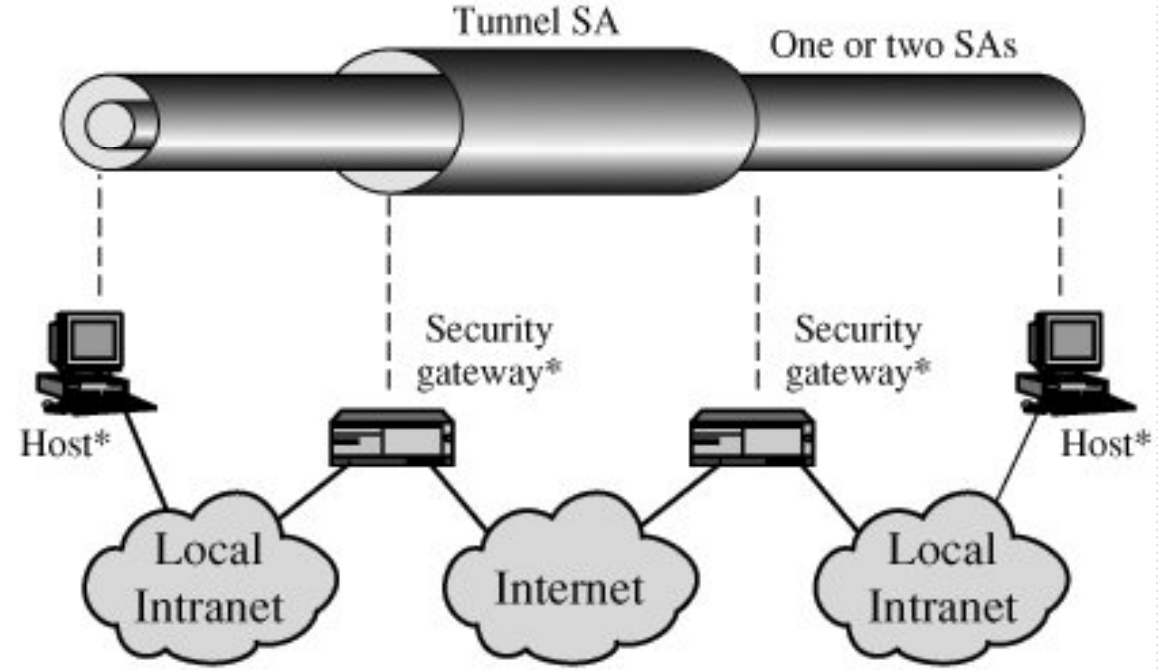
ترکیب SAها: حالت ۲

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



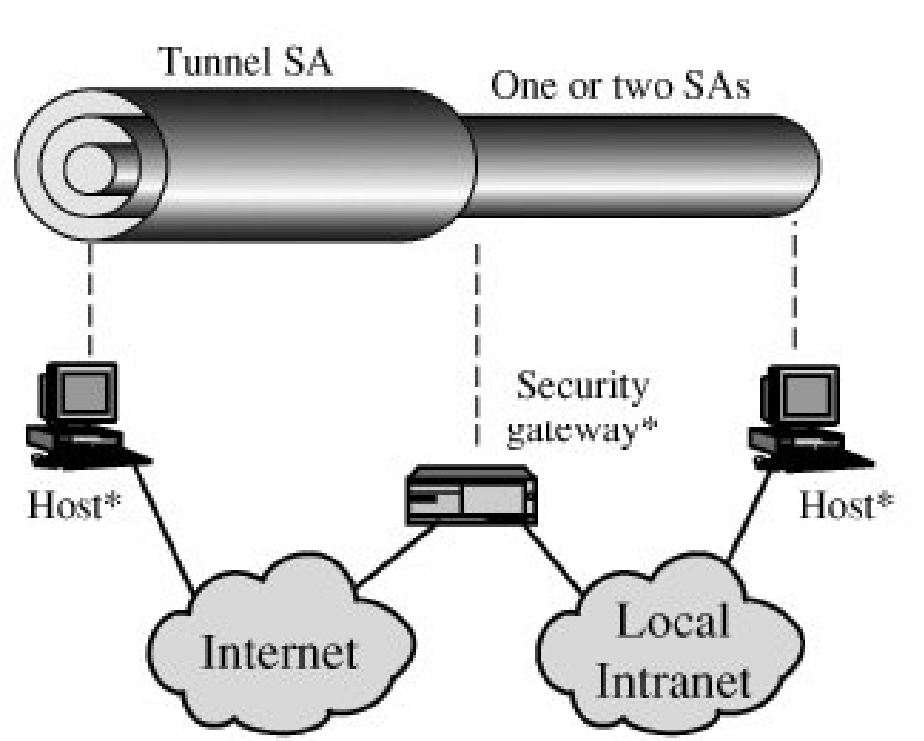
ترکیب SAها: حالت ۳

- 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 ISAKMP/Oakley نامیده می شود.

Internet Security Association and Key Management Protocol

مدیریت کلید

- مدیریت کلید خودکار به نام ISAKMP/Oakley معروف است و شامل دو پروتکل است:
  - پروتکل تعیین کلید Oakley
    - فرم توسعه یافته پروتکل Diffie-Hellman که ضعفهای آن را برطرف کرده است.
  - پروتکل مدیریت کلید و SA در اینترنت (ISAKMP)
    - تعریف رویه‌ها و قالب بسته‌ها برای برقراری، مذاکره، تغییر یا حذف SA

پروتکل Oakley

- خصوصیات پروتکل Oakley
  - مقابله با حمله Clogging در DH: منابع قربانی با درخواستهای مکرر تبادل کلید تلف می‌شود.
    - با استفاده از تعریف مفهومی تحت عنوان کوکی (Cookie) مشکل این حمله را برطرف می کند.
  - مقابله با حمله مرد میانی در DH:
    - احراز اصالت در تبادل کلید DH
  - مقابله با حمله تکرار:
    - با استفاده از نانس با حمله‌های تکرار مقابله می‌کند.

پروتکل Oakley

- مقابله با حمله Clogging
  - استفاده از کوکی (توسط هر یک از طرفین) به صورت زیر:
    - ارسال عدد تصادفی کوکی توسط هریک از طرفین ارتباط
    - ارسال ack توسط طرف دیگر
    - نیاز به ارسال ack توسط مبدأ در اولین پیام DH
  - اگر مهاجم از آدرس جعلی برای ارسال کوکی استفاده کرده باشد، چون ack را دریافت نمی‌کند، نمی تواند DH را آغاز نماید.
  - باید تولید و وارسی کوکی کم هزینه باشد تا حملات اتلاف منابع ممکن نباشد.

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

پایان

مرکز امنیت داده و شبکه شریف

http://dnsl.ce.sharif.edu

پست الکترونیکی

m_amini@ce.sharif.edu

شبکه آموزشی- پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

madsg.com

مادسیج

IRan Education & Research NETwork
(IRERNET)