دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکدهٔ مهندسی کامپیوتر و فنآوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

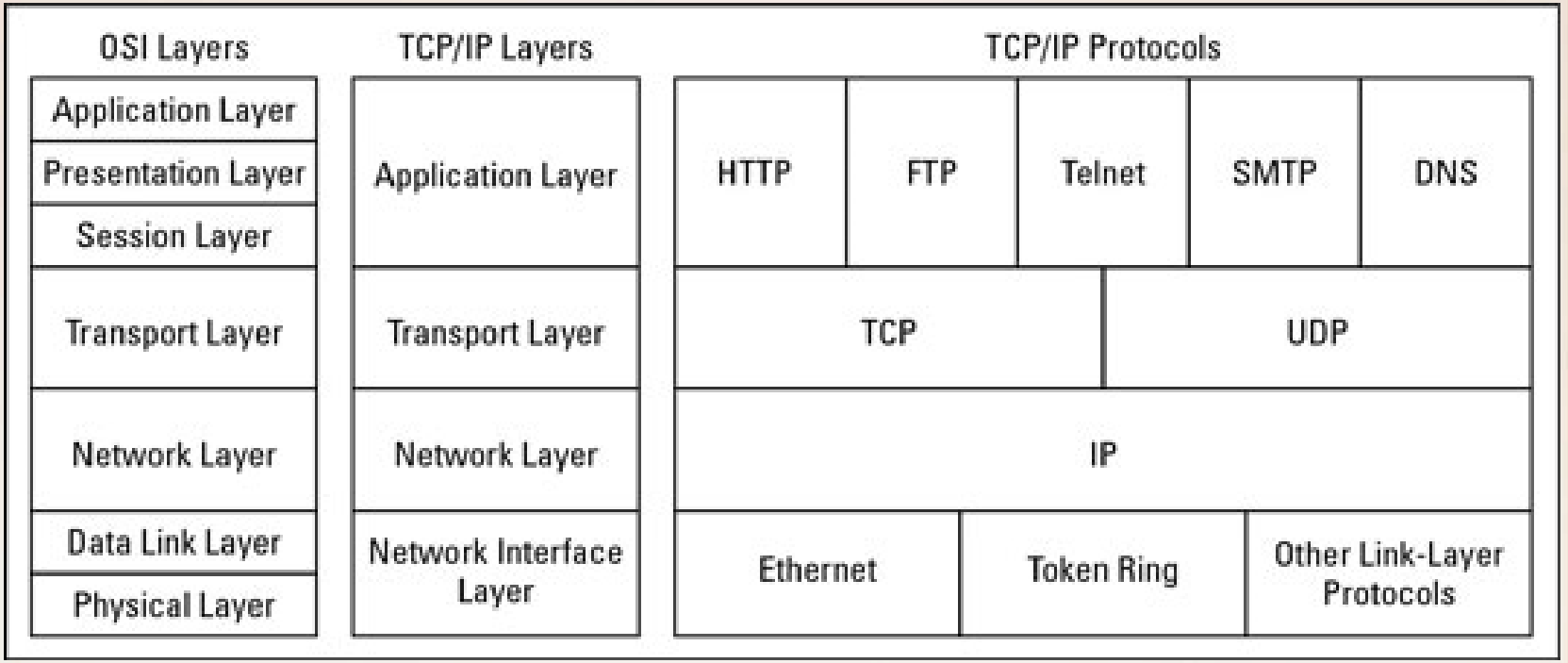
IPsec

نستوه طاهری جوان

nastooh@aut.ac.ir

روش های برقراری امنیت در اینترنت

- یادآوری: معماری لایه ای در اینترنت



nastooh@aut.ac.ir

روش های برقراری امنیت در اینترنت

- ✓ یادآوری: مولفه های امنیتی مرور شده

  - Confidentiality
  - Data Integrity
  - Non-Repudiation
  - Authentication

nastooh@aut.ac.ir

روش های برقراری امنیت در اینترنت

- ✓ رویکردها
  - امنیت انتها به انتها در سطح برنامه کاربردی
    - رمزنگاری در برنامه های کاربردی، مانند PGP و SET
  - امنیت انتها به انتها در سطح لایهٔ انتقال
    - مزیت: درگیر نشدن برنامه های کاربردی، مانند TLS و SSL
  - **امنیت در لایهٔ شبکه**
    - انجام رمزنگاری و احراز هویت در لایهٔ شبکه، مانند IPsec
  - امنیت در لایهٔ پیوند داده
    - رمزنگاری در سطح فریم ها، مانند WPA و WEP ،L2TP
  - امنیت در لایهٔ فیزیکی
    - استفاده از محافظت های فیزیکی در شبکه های سیمی یا چنل-هاپینگ در بیسیم

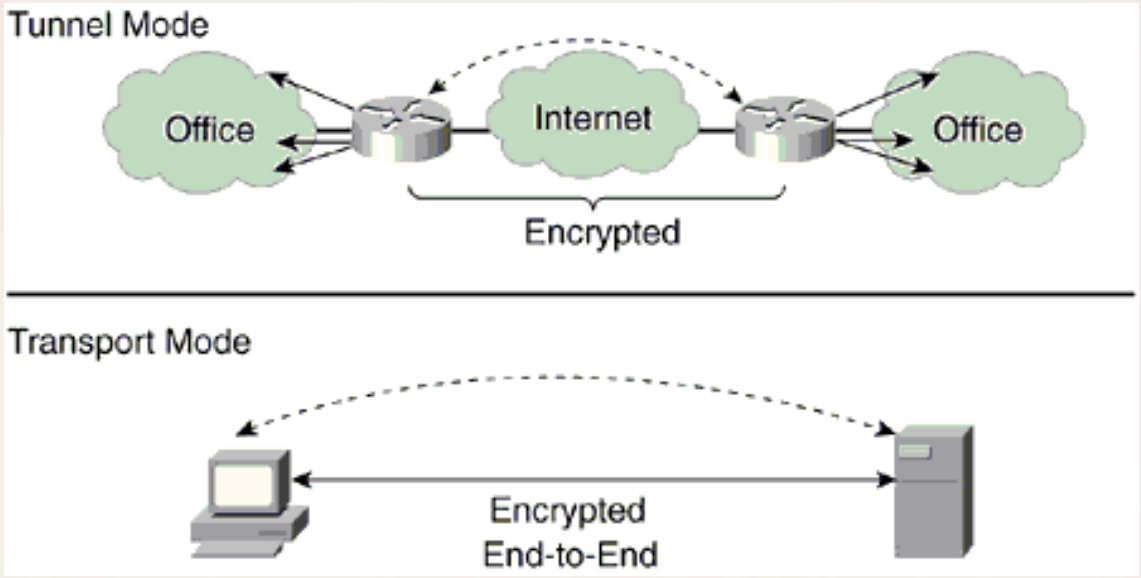
IPsec

- ✓ کلیات پروتکل IPsec
  - یک چهارچوب برای ارائهٔ خدمات چندگانه شامل:
    1. رمزنگاری داده ها
    2. تضمین صحت داده ها
    3. جلوگیری از حملات تکرار
  - نیاز به برقراری یک اتصال بین مبدا و مقصد
    - به آن Security Association گویند
    - برای ارتباط دوطرفه به دو SA نیاز داریم.
    - هر SA یک ID منحصر به فرد دارد و همهٔ بسته های یک اتصال آن را حمل می کنند.
    - هر SA از یک کلید مشترک برای رمزنگاری متقارن استفاده می کند.
  - IPsec هر پروتکلی که بر روی IP قرار دارد را در بر میگیرد.
    - برای برنامه های کاربردی شفاف است.

nastooh@aut.ac.ir

IPsec

- ✓ حالت های IPsec
  - ○ حالت انتقال
    - ایجاد دو SA مستقیم بین دو ماشین
  - ○ حالت تونل
    - اتصال دوشبکه به کمک دروازه ها

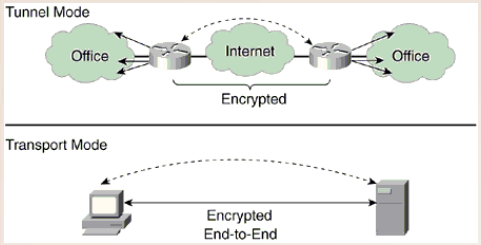


nastooh@aut.ac.ir

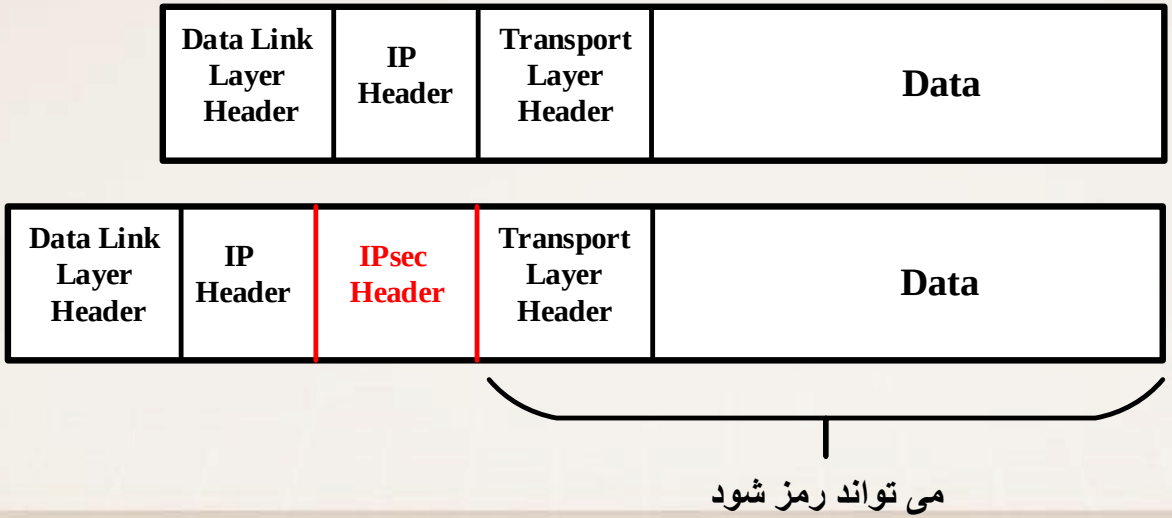
IPsec

✓ حالت **انتقال** در IPsec

- به بسته های IP یک سرآیند اضافی به نام IPsec اضافه می شود.
  - سرآیند IPsec شامل فیلدهای زیر است:
    - شناسهٔ SA
    - شماره ترتیب بسته
    - امضای دیجیتال بسته



- اختیاری: در صورت تمایل کل بسته نیز رمز شده و به عنوان بدنهٔ بستهٔ IPsec ارسال می شود.



nastooh@aut.ac.ir

IPsec

- ✓ حالت **انتقال** در IPsec
  - ○ با کمک پروتکل AH (Authentication Header)
    - سرویسهای ارائه شده در این حالت:
      - ➢ احراز هویت مبدا
      - ➢ جامعیت داده
      - ➢ جلوگیری از ارسال مجدد بسته ها
    - نیاز به سِت کردن کلید بین مبدا و مقصد دارد. (چگونه؟)

Data Link Layer Header	IP Header	AH Header	Transport Layer Header	Data

nastooh@aut.ac.ir

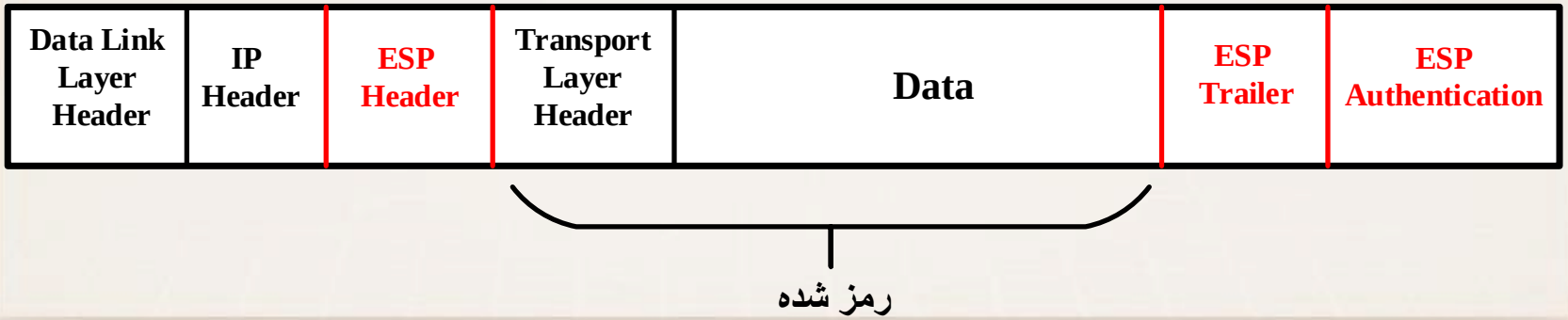
IPsec

- ✓ حالت **انتقال** در IPsec
  - سرآیند پروتکل AH
    - پروتکل لایه بعد
    - طول داده
    - SPI: مشخصهٔ SA
    - شناسه ترتیبی بسته
    - ICV: به کمک HMAC یک خلاصه از داده و سرآیند IP

Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	*Next Header*								*Payload Len*								*Reserved*															
32	*Security Parameters Index (SPI)*																															
64	*Sequence Number*																															
96	*Integrity Check Value (ICV)*																															

IPsec

- ✓ حالت **انتقال** در IPsec
  - ○ به کمک پروتکل ESP (Encapsulating Security Payload)
    - سرویس های ارائه شده در این حالت:
      - **محرمانگی**
      - احراز هویت مبدا
      - جامعیت داده
      - جلوگیری از ارسال مجدد بسته ها
    - نیاز به سِت کردن کلید بین مبدا و مقصد.
    - داده و سرآیند لایهٔ انتقال رمز می شوند. (با روشهایی مانند DES و AES)



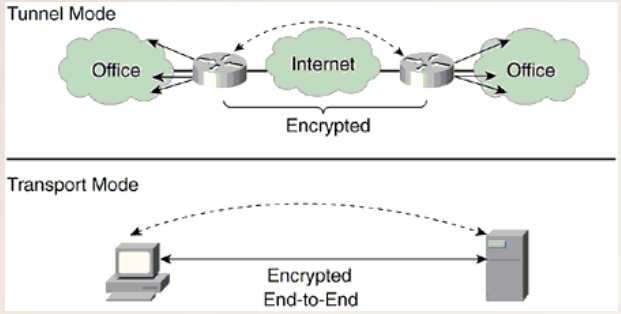
nastooh@aut.ac.ir

IPsec

- ✓ حالت **انتقال** در IPsec
  - فیلدهای سرآیند ESP
    - شناسهٔ SA
    - شناسهٔ ترتیبی بسته
  - فیلدهای پی آیند ESP
    - تنظیم طول داده (برای استفاده رمزنگاری های بلوکی)
    - پروتکل لایه بعدی
  - فیلد .ESP Auth
    - خلاصهٔ داده به کمک HMAC

IPsec

- حالت **تونل** در IPsec
  - بستهٔ دادهٔ IP پس از اضافه شدن سرآیند IPsec دوباره در قالب یک بستهٔ IP جدید در شبکه روانه می شود!



Data Link Layer Header	IP Header	Transport Layer Header	Data

Data Link Layer Header	New IP Header	IPsec Header	IP Header	Transport Layer Header	Data

می تواند رمز شود

IPsec

- ✓ حالت **تونل** در IPsec
  - ○ با کمک پروتکل AH
    - سرآیند AH همانند حالت انتقال

شکل گویا!

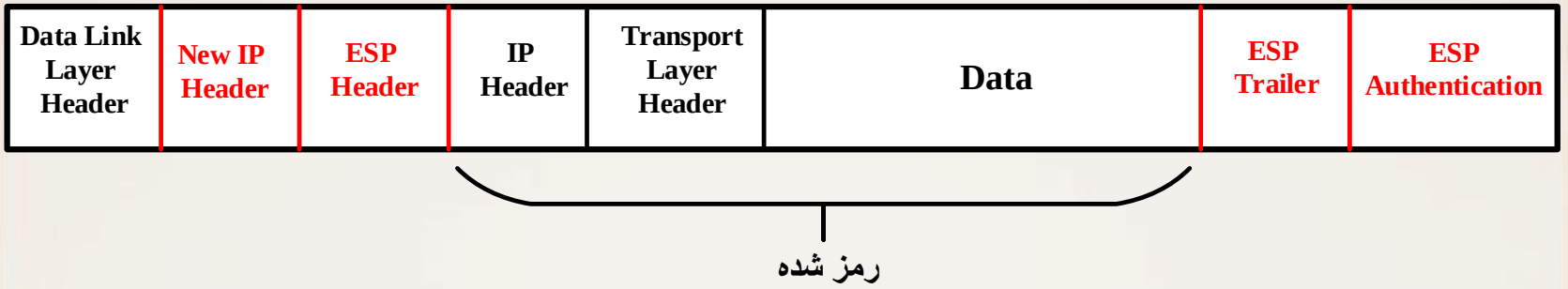
Data Link Layer Header	New IP Header	AH Header	IP Header	Transport Layer Header	Data

nastooh@aut.ac.ir

IPsec

- ✓ حالت **تونل** در IPsec
  - ○ با کمک پروتکل ESP
    - سرآیند و پی آیند ESP همانند حالت انتقال

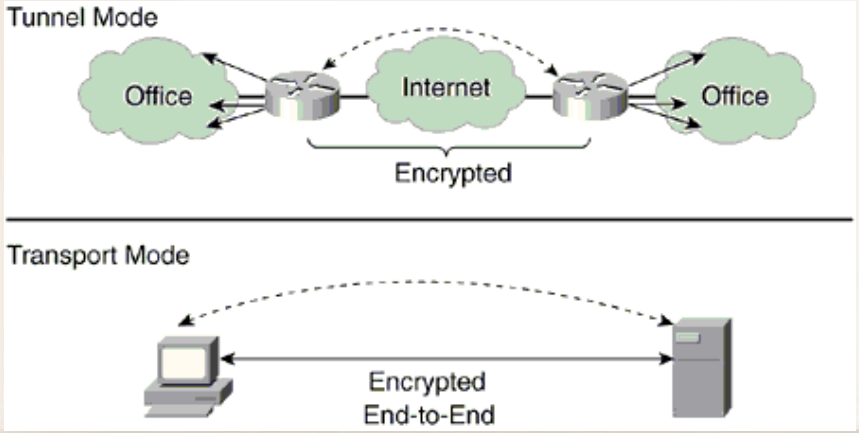
شکل گویا!



nastooh@aut.ac.ir

IPsec

- ✓ جمع بندی IPsec
  - چهار حالت دارد:
    - حالت انتقال با پروتکل AH
      - کاربرد: عموما برای بررسی اصالت داده (بدون محرمانگی) استفاده می شود.
    - حالت انتقال با پروتکل ESP
      - کاربرد: هم حفظ اصالت داده و هم محرمانگی
    - حالت تونل با پروتکل AH
      - کاربرد عملی ندارد!
    - حالت تونل با پروتکل ESP
      - کاربرد عمده: VPN



nastooh@aut.ac.ir

IPsec

- ✓ مسالهٔ تبادل کلید در IPsec
  - در IPsec هر SA نیاز به دو کلید دارد، یکی برای AH و یکی برای ESP
    - یعنی هر ارتباط دوطرفه به چهار کلید نیاز دارد
  - کلید ها را می توان به دو صورت ست کرد:
    - دستی
    - خودکار

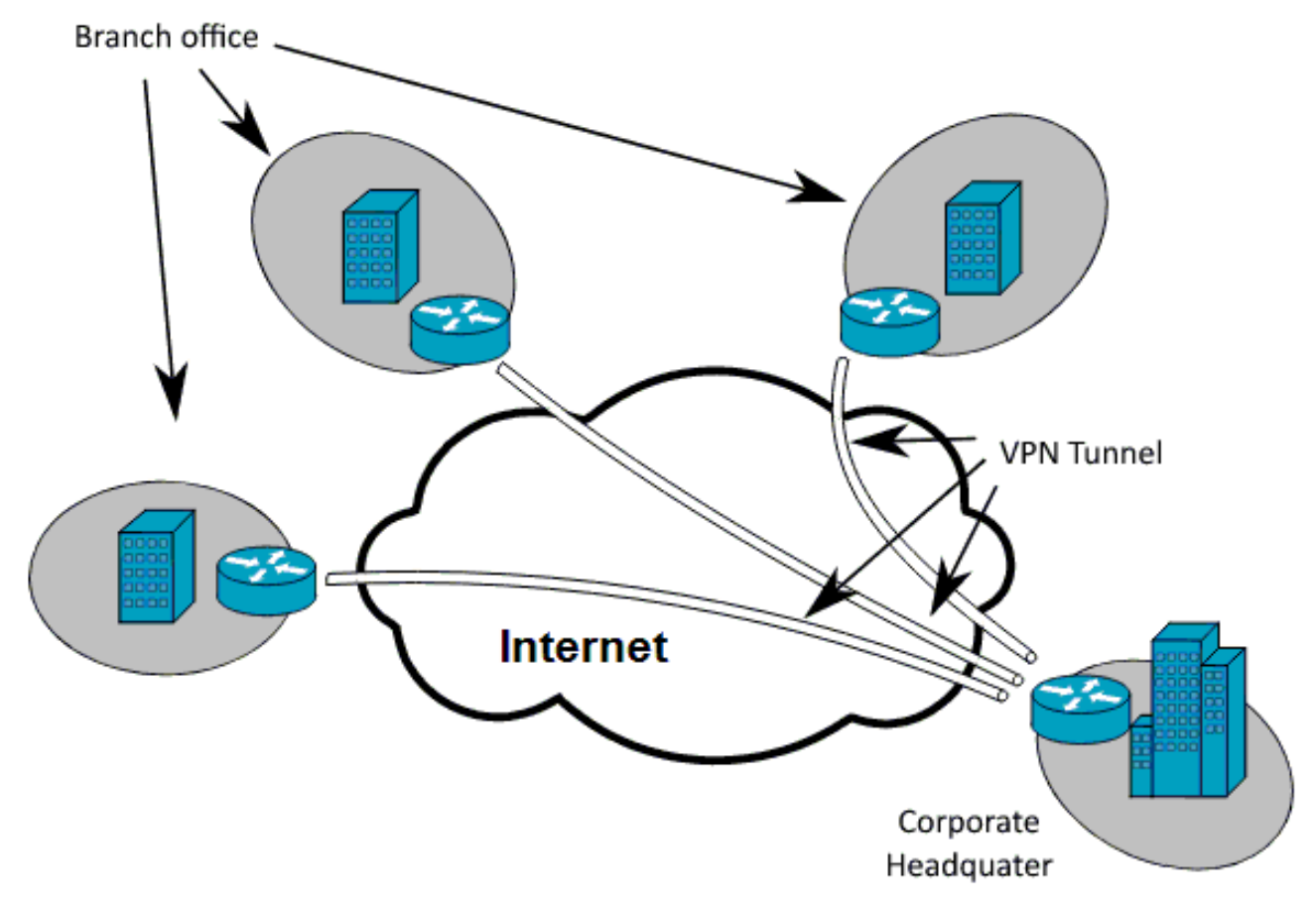
IPsec

- ✓ مسالهٔ تبادل کلید در IPsec
  - تبادل **خودکار** در IPsec هر SA نیاز به دو کلید دارد، یکی برای AH و یکی برای ESP
    - یعنی هر ارتباط دوطرفه به چهار کلید نیاز دارد
  - در حالت خودکار از پروتکل ISAKMP/Oakley استفاده می شود.
    - مبتنی بر دیفی-هلمن به صورت بهبود یافته.
    - قدری کند.
    - نیاز به اصلاحات و تغییرات دارد.

nastooh@aut.ac.ir

VPN

VPN (Virtual Private Network) ✓



nastooh@aut.ac.ir

VPN

- ✓ پیاده سازی VPN
  - عموما مسیریابهای مرزی (یا دیواره های آتش مرزی) در شبکه ها یک تونل بین هم برقرار می کنند.
  - در این حالت ارتباطات شبکه های داخلی ارتباطی با VPN ندارند.

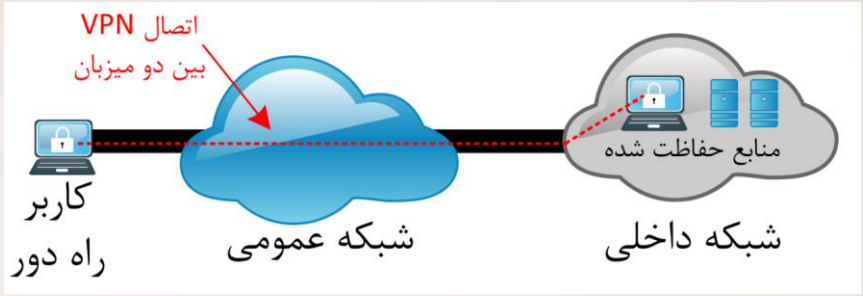
  - انواع VPN
    - H2H
    - H2N
    - N2N

nastooh@aut.ac.ir

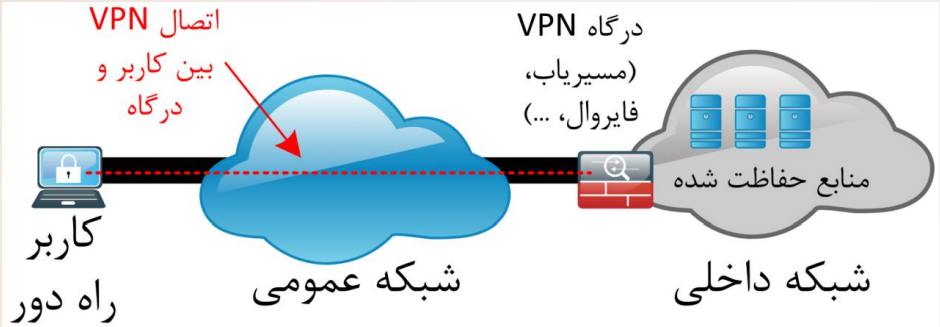
VPN

✓ انواع VPN

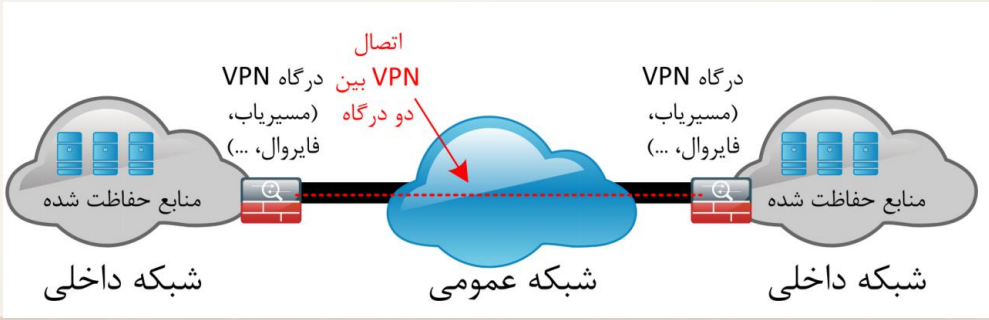
مدل H2H



مدل H2N



مدل N2N



nastooh@aut.ac.ir

VPN

- پیاده سازی VPN
  - VPN لزوما با IPsec پیاده سازی نمی شود.
  - مدلهای دیگری از پیاده سازی وی پی ان هست مانند:
  - L2TP
  - MPLS
  - PPTP
  - SSTP
  - OpenVPN
  - VPN-Q

منابع

[1] William Stallings, “Cryptography and Network Security,” 7th ed.

nastooh@aut.ac.ir

پایان

nastooh@aut.ac.ir