

قواعد IP security با مقررات امنیت در این زمینه اطلاعات ارسالی در این‌ها

بلاسی و صورت خودکار امن می‌شود. Application ها بدون اینده کارم

بباید امن می‌شود

امنیت شبکه متمرکز می‌شود، به عبارت دیگر سرویس‌های مانند دسترسی،

کلیدها، الگوریتم‌ها هم بصورت متمرکز مدیریت می‌شوند

~~کارهای امنیتی~~

- IP security تعیین می‌کند که: (۱) اعلان حضور میزبان جدید

(۲) اعلان حضور یک میزبان که این میزبان ارتباطات همسایگی را با میزبان

دیگر حفظ می‌کند (۳) به‌طور کلی تغییر میزبان‌ها (۴) به‌صورت مازی

میزبان

- کارمدهای IP security به اتصال شعب سازمانها، شبکه‌ها به یکدیگر

(۲) اتصال و ارتباط از راه دور (۳) ارتقاء امنیت تجارت الکترونیکی

(۴) مقررات اتصال اینترنت و اینترنت از طریق ابزار هویتی و محرمانگی

- سرویس‌های Ip security :

Authentication ~~Authentication~~ ①

۱۴ رمزنگاری

۱۵ مدیریت کلیدها

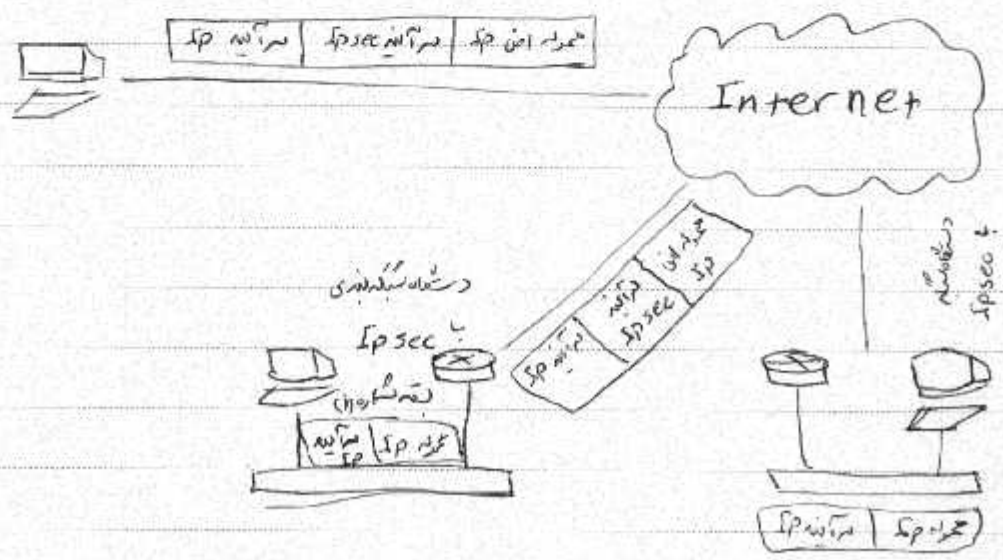
- همان‌طور که میدانید یکی از کارهای مهم در سرویس‌های Ip security ایجاد امنیت است،

در این سرویس بسته‌های ارسالی از طرف یک client بصورت بسته شماره‌گذاری می‌شوند

وقتی این بسته به Router می‌رسد گیرنده می‌تواند بسته‌های بدست‌آمده را بررسی کند

در انتی‌دیت رد و بدل می‌شود که مهم‌ترین آن رمزنگاری است، این بسته در صورت مقصد

دوباره رمزگشایی می‌شود (دکامپرس) و گویی سرور محلی داده می‌شود



پروتکل‌های امنیت IP و AH (۱) و ESP (۲)

Authentication (۱) header و Integrity (۲) header اضافه می‌کند. IP امن می‌شود که از آن

برای افزایش امنیت استفاده می‌شود، البته این صند فقط از هویت و انجام می‌دهد و

نه هم‌زمان داده را

Encapsulation security payload : هیچ صندلی به آن اضافه نمی‌شود بلکه فقط رمزنگاری

کتابه‌ها را انجام می‌دهد، البته از هویت و نیز انجام می‌دهد، در این صورت کل محتوای

کتابه IP رمزنگاری و صندهای سرآیند و دنباله نیز لمس می‌شوند

از جمله از الگوریتم‌هایی که برای رمزنگاری، صندهای داده (payload) و سرآیند و دنباله

توسط سرآیند ESP استفاده می‌شود الگوریتم‌های DES، RC5

و 3DES