امنیت تجارت الکترونیک

فصل دوازدهم:
امنیت لایه اینترنت

تهیه و تنظیم: دکتر آرش حبیبی لشکری
منبع: کتاب "اصول امنیت برای تجارت الکترونیکی"

اولین نسخه: دی 1393
بروزرسانی: فروردین 1396

فهرست

- فیلتر کردن بسته ای
- فیلتر کردن براساس آدرسهای شبکه
- فیلتر کردن بر اساس آدرس‌های شبکه و شماره‌های پورت
- مشکلات FTP
- مشکلات TCP
- برگردان آدرس شبکه (NAT)
- امنیت IP (IPSec)
- مدل تشخیص نفوذ شبکه

مقدمه

اولین مکانیزم امنیتی در لایه اینترنت در سیستم‌های دیوارآتش برپایه فیلترکردن بسته‌ها به کارگرفته شده است

لزوم این امر، استفاده گسترده از احرازهویت‌ها بر اساس آدرس‌های IP بود، که به یکی از جدیترین آسیبپذیریهای مجموعه TCP/IP مبدل گردید.

یک مفهوم کامل امنیتی IP با آمدن IPsec شکل گرفت که متاسفانه بدلیل اینکه نیازمند تغییرات زیادی در سیستم عامل بود، هنوز هم به خوبی متدوال نشده است.

پروتکلهای پشتیبان در مجموعه TCP/IP نیز از مشکلات امنیتی رنج میبرند. باتوجه به مشکل احرازهویت برپایه آدرس‌های IPو نامهای میزبان، چنین نتیجه میگیریم که DNS بطور خاصی حیاتی است.

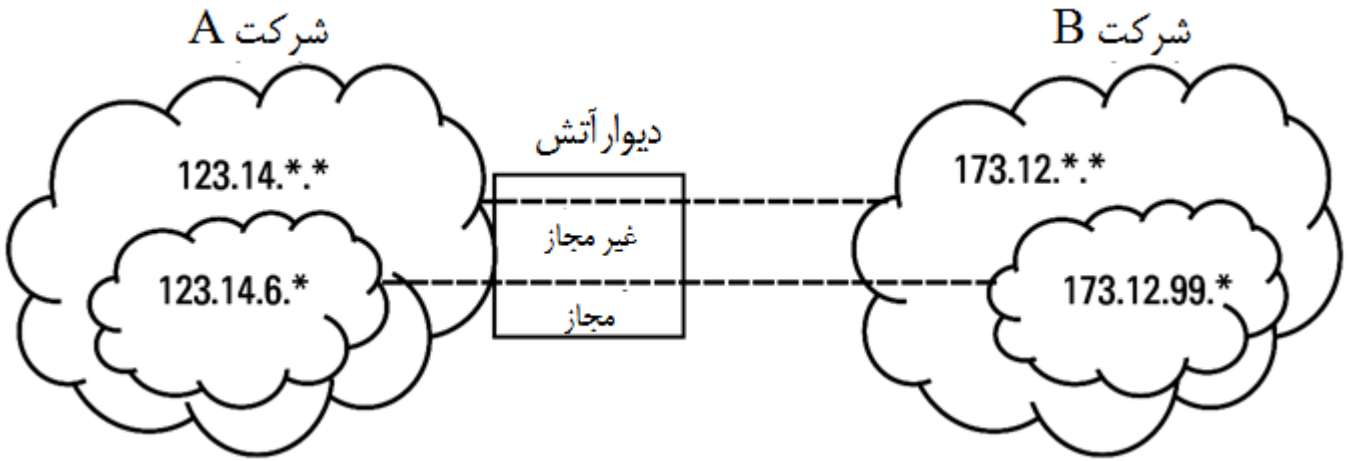
در پایان، برای کنار آمدن با رشد مداوم تعداد حملات شبکه ای، نیاز به یک مکانیزم منعطف برای حفاظت سریع از یک شبکه داخلی احساس میشود

فیلتر کردن بسته ای

- اولین دیوارهای آتش، مسیریاب هایی بودند که قابلیت فیلترکردن ترافیکها را بر اساس فیلدهای سربارهای IP داشتند.
- آنها به صورت سخت‌افزاری پیاده سازی شده بودند، بنابراین اولین فیلترها بصورت جفتهای ماسک/مقدار داده شدند (هگزادسیمال).
- نسل بعدی فیلترها با زبانهای ساده فیلترینگ ارائه شد، اما هنوز برای یک مدیر دانستن نحو آن زبان موردنیاز بود.
- آخرین ابزارهای مدیریت، فرمهای مبتنی بر وب بودند که - حداقل از نقطه نظر نحوی - پرکردن آنها ساده بود.

فیلتر کردن براساس آدرسهای شبکه

قانون	آدرس IP مبدا	آدرس IP مقصد	عکس العمل
1	173.12.99.*	123.14.6.*	مجاز
2	173.12.*.*	123.14.*.*	غیرمجاز
3	123.14.6.*	173.12.99.*	مجاز
4	123.14.*.*	173.12.*.*	غیرمجاز
5	*.*.*.*	*.*.*.*	غیرمجاز



فیلتر کردن بر اساس آدرس‌های شبکه و شماره‌های پورت

عکس العمل	پورت مقصد	پورت مبدا	آدرس IP مقصد	آدرس IP مبدا	نوع	اتصال	قانون
مجاز	25	>=1024	داخلی	خارجی	TCP	داخلی	1
مجاز	>=1024	25	خارجی	داخلی	TCP	داخلی	2
مجاز	25	>=1024	خارجی	داخلی	TCP	خارجی	3
مجاز	>=1024	25	داخلی	خارجی	TCP	خارجی	4
غیرمجاز	همه	همه	*.*.*.*	*.*.*.*	همه	همه	5

مشکلات تکه تکه شدن در لایه IP

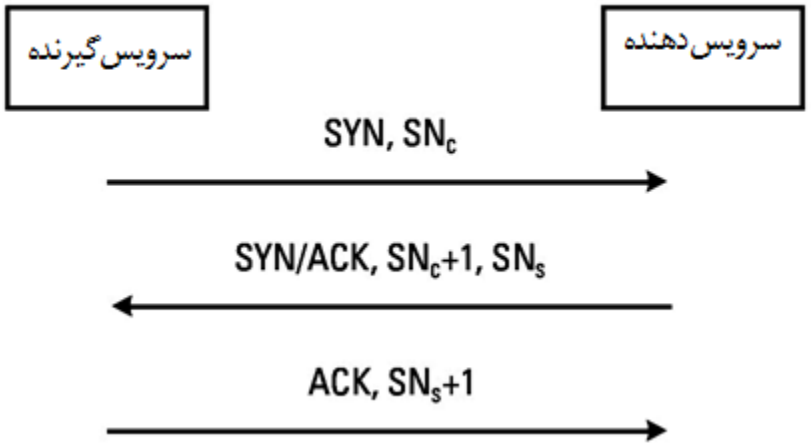
مجوعه فعالیتهای اضافه شده در هر ارتباط

فعالیت	سرویس	مقصد	منبع
احرازهویت کاربر	FTP	123.14.6.23	*.*.*.*

مشکلات FTP

قانون	اتصال	نوع	آدرس IP مبدا	آدرس IP مقصد	پورت مبدا	پورت مقصد	پرچم	عکس العمل
1	داخلی	TCP	خارجی	داخلی	20	>=1024		مجاز
2	داخلی	TCP	داخلی	خارجی	>=1024	20	ACK	مجاز
3	خارجی	داخلی	داخلی	خارجی	>=1024	21		مجاز
4	خارجی	TCP	خارجی	داخلی	21	>=1024	ACK	مجاز
5	همه	همه	*.*.*.*	*.*.*.*	همه	همه		غیرمجاز

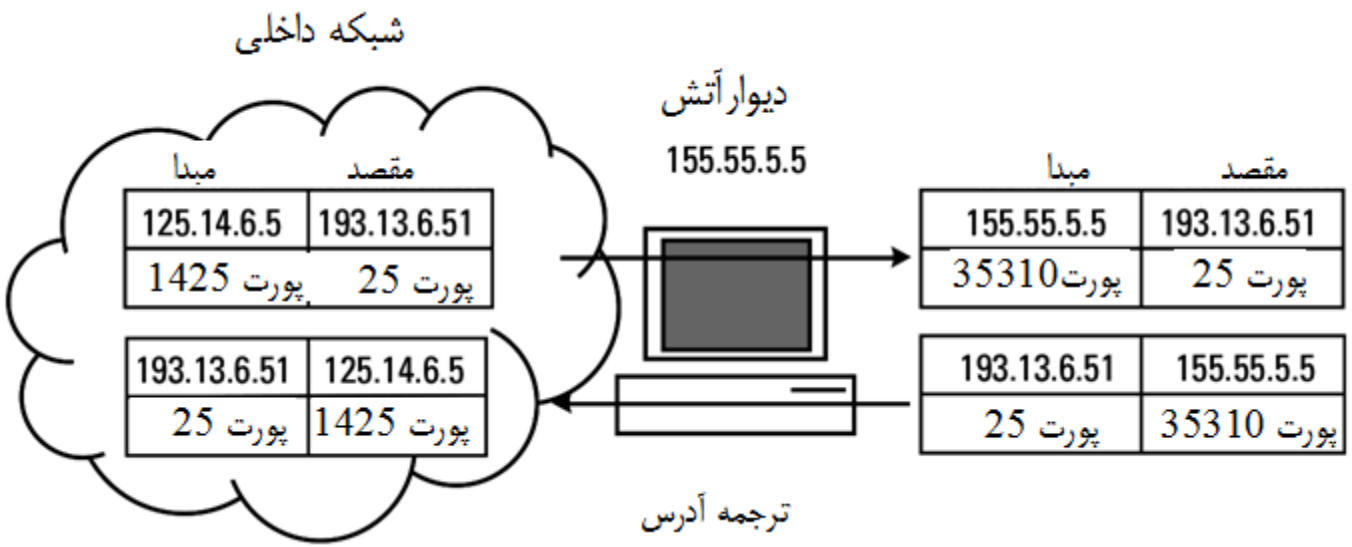
مشکلات TCP



حمله SYN Flood یا سیلاب SYN در TCP

پیش‌بینی شماره توالی در TCP

برگردان آدرس شبکه (NAT)



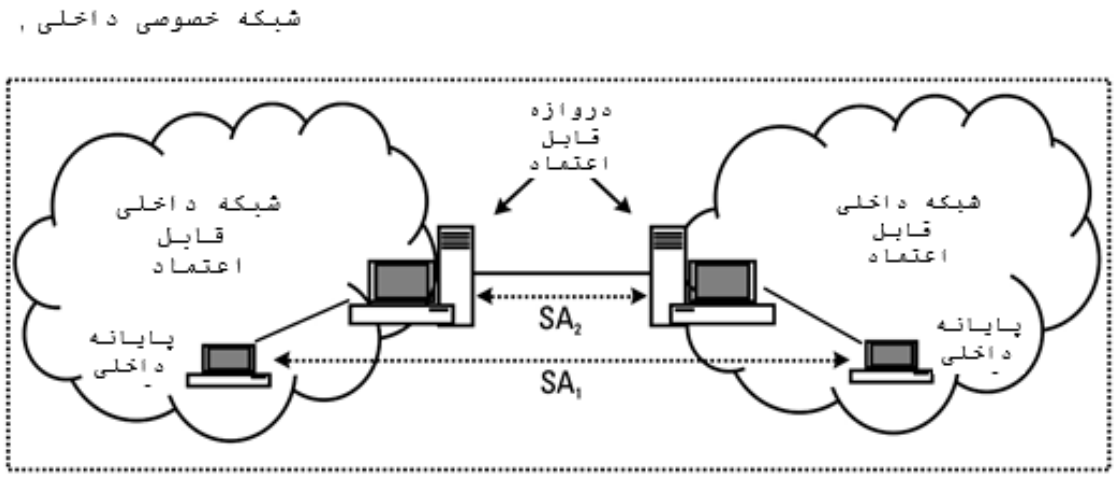
امنیت IP (IPsec)

IPSEC نامی‌رایج برای تعمیمات امنیتی پروتکل IPاست. سرویس‌های امنیتی IP عبارت‌اند از:

- پشتیبانی کنترل دسترسی غیر مستقیم؛ یکپارچگی غیراتصال‌گرا؛ احراز هویت اصلیت داده؛ حفاظت در برابر بازپخش/مرتب سازی مجدد بسته‌های IP؛ محرمانگی؛ محرمانگی چرخه ترافیک محدودشده؛

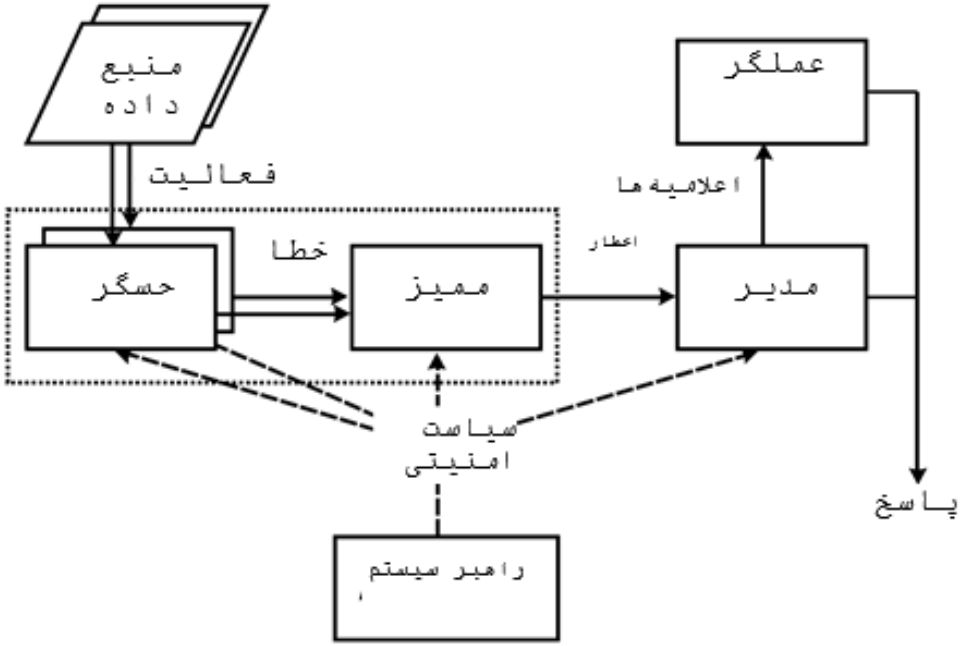
بخشهای اساسی معماری امنیتی IP عبارت‌اند از:

- پروتکل‌های امنیتی (AH، ESP)؛
- الگوریتمهایی برای احراز هویت و رمز نگاری؛
- مدیریت کلید (IKE)؛
- مشارکتهای امنیتی



مدل تشخیص نفوذ شبکه

روش‌های مبتنی بر قانون و روش‌های آماری



خلاصه: فیلتر کردن بسته ای، فیلتر کردن براساس آدرسهای شبکه، فیلتر کردن بر اساس آدرس‌های شبکه و شماره‌های پورت، مشکلات FTP، مشکلات TCP، برگردان آدرس شبکه (NAT)، امنیت IP (IPSec)، مدل تشخیص نفوذ شبکه

جلسه بعدی: امنیت لایه انتقال

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.