آشنایی با مبانی امنیت شبکه

تعریف اطلاعات: دانشی است که از طریق تحقیق، آموزش، مطالعه، اخبار و حقایق موجود بدست می‌آید. یا به عبارتی اطلاعات داده‌های پردازش شده می‌باشد.

تعریف امنیت: رهائی از هر گونه خطر و حملات احتمالی و برقراری ایمنی و رهائی از ترس یا نگرانی را امنیت گویند.

تعریف امنیت اطلاعات: عبارتی است که به اقدامات پیشگیرانه اطلاق می‌شود. به طوریکه این اقدامات قادر است از اطلاعات و قابلیت‌هایمان نگهداری نماید و ما به کمک آنها می‌توانیم اطلاعات را در برابر حملات خارجی و بهره‌برداری غیرمجاز محافظت نماییم. به عبارت بهتر امنیت اطلاعات فرآیندی است جهت حفظ اطلاعات از دسترسی غیرمجاز، افشا کردن، خراب کردن، تغییر دادن و یا از بین بردن آنهاست.

تاریخچهٔ امنیت: فهمیدن روند رشد امنیت اطلاعات از این جهت حائز اهمیت است که می‌توانیم احتیاجات امروز خود را بهتر درک کرده و مطابق با نیازهای فعلی خود ساختار امنیتی مناسبی بسازیم. موارد مطرح در این خصوص عبارتند از:

۱- امنیت فیزیکی: اولین شکل اطلاعاتی که بشر آنها را نگهداری می‌کرد به شکل فیزیکی بود به طوریکه در ابتدا این اطلاعات را در جاهایی ثبت می‌کردند و سپس اطلاعات ثبت شده را پنهان می‌ساختند، همچنین به منظور انتقال این اطلاعات از پیک‌هایی استفاده می‌شد و با توجه به نوع عملکرد در این روش دو خطر مهم و اصلی در این ساختار وجود داشت.

الف) اطلاعات پس از سرقت به طور کامل قابل استفاده بود.

ب) مالک اصلی اطلاعات به اطلاعات خود دسترسی نداشته است. (نسخه پشتیبانی وجود نداشت)

۲- امنیت مخابراتی: با توجه به نقص اصلی که در امنیت فیزیک وجود داشت و اطلاعات هنگام جابه‌جایی قابل استفاده و یادگیری توسط دشمن بود از بسترهای مخابراتی برای انتقال اطلاعات استفاده می‌شد و در ضمن اطلاعات را در هنگام انتقال به شکل رمز در می‌آوردند تا اگر پیام در مسیر انتقال سرقت شد قابل استفاده و بهره‌برداری نباشد.

۳- امنیت تشعشع: معمولاً سیگنالهای الکتریکی و الکترونیکی که در ساختار مخابراتی استفاده می‌شود و همچنین تجهیزاتی که به منظور رمزگشایی و رمزنگاری پیام‌های مخابراتی استفاده می‌شود دارای تشعشعاتی الکترونیکی هستند. به کمک ابزارهای پیشرفته می‌توان تشعشعات را دریافت و اطلاعات اصلی را از بین آنها استخراج نمود. به دلیل وجود این مشکلات سرفصل جدیدی به عنوان امنیت تشعشع مطرح گردید که به کمک مکانیزم‌هایی تشعشعات موجود در سیستم‌های مخابراتی را کنترل نماییم تا اطلاعات اصلی در اختیار کاربران غیرمجاز قرار نگیرد.

۴- امنیت کامپیوتر: با ورود کامپیوترها به بخش‌های مختلف سازمان‌ها و انجام کارهای محاسباتی مختلف مبحث

امنیت کامپیوترها مطرح گردید. کشورهایی که از کامپیوتر به عنوان تجهیزات اصلی سازمان استفاده می‌کردند به منظور رعایت امنیت طرح طبقه‌بندی اطلاعات را مطرح نمودند که با این طرح افراد مختلف در سازمان فقط به اطلاعاتی دسترسی داشتند که متناسب با کار ویژهٔ خودشان بود و امکان دسترسی به اطلاعات سطوح بالاتر باید با مجوز مقام ارشد سازمان انجام می‌گرفت.

۵- امنیت شبکه: با ایجاد شبکه‌ها و ارتباط کامپیوترها به یکدیگر مفاهیم جدید امنیتی مطرح گردید که در مباحث قبلی پیش‌بینی نشده بود. در این ساختار جدید چند و یا چندین هزار کامپیوتر به هم متصل شده و با سرعت‌های زیادی در حال تبادل اطلاعات می‌باشند که پیاده‌سازی امنیت در این بستر نیاز به طرح‌های کامل‌تری داشت. به همین دلیل در کشورهای پیش‌رو طرح امنیتی ویژه‌ای برای شبکه‌های کامپیوتری طراحی گردید که در آنها به مباحث مربوط به امنیت کامپیوترها هم پرداخته شده بود.

حمله (Attack)

تعریف حمله: راه‌هایی که خواسته یا ناخواسته از طریق سیستم یا اشخاص سبب از بین رفتن اطلاعات، دسترسی به اطلاعات و یا خسارت زدن به منابع اطلاعاتی باشد را حمله می‌گویند. حملات بر اساس نوع عملکرد و چگونگی رخ دادن آنها به انواع زیر تقسیم می‌شوند:

۱- حمله دسترسی: در این نوع حمله مهاجم سعی خواهد کرد به اطلاعاتی دسترسی پیدا کند که مجاز به استفاده آنها نبوده است. این نوع حملات معمولاً برای بدست آوردن اطلاعات محرمانه صورت می‌پذیرد. و اصل اطلاعات نیز دچار تغییر نمی‌شود و انواع آن عبارتند از:

الف) جاسوسی: در این روش مهاجم در بین اطلاعات به جستجو پرداخته به امید آنکه اطلاعات مهم و قابل توجهی در بین آنها یافت می‌شود.

ب) استراق سمع یا شنود: در این روش مهاجم به طور غیرمجاز به اطلاعاتی که از کانال ارتباطی عبور می‌کند دسترسی یافته و از آن استفاده می‌کند. (مهاجم با اصل اطلاعات کاری ندارد)

ج) حائل شدن یا واسطه شدن: برخلاف روش قبلی این نوع حمله یک حمله فعال در مقابل اطلاعات است و مهاجم خود را در مسیر عبور اطلاعات قرار داده و قبل از رسیدن اطلاعات به مقصد از آنها سوء استفاده می‌کند و پس از آن ممکن است اجازهٔ عبور آن اطلاعات داده شود.

۲- حمله دستکاری: در این نوع حمله مهاجم سعی می‌کند اطلاعاتی را تغییر دهد که مجاز به انجام این تغییرات نمی‌باشد. در این حمله صحت و تمامیت اطلاعات از بین می‌رود و مهاجم از طریق کانال ارتباطی و یا از طریق اطلاعات اصلی ساختار و کیفیت اصلی اطلاعات را تغییر می‌دهد. این نوع حمله دارای اقسامی است که عبارتند از:

الف) تغییر اطلاعات

ب) حذف اطلاعات

ج) اضافه کردن اطلاعات

۳- حمله جلوگیری از سرویس: در این نوع حمله کاربر مجاز نمی‌تواند از منابع موجود و در اختیار (اطلاعات و قابلیت‌های سیستم) استفاده نماید. در این نوع حمله به مهاجم اجازه دسترسی و تغییر اطلاعات اصلی معمولاً داده نمی‌شود. ولی از سرویس‌دهی به کاربران مجاز جلوگیری می‌کند. هدف مهاجم در این نوع حمله معمولاً خرابکاری است، انواع عبارتند از:

الف) جلوگیری از سرویس با حمله به برنامه کاربردی: در این نوع حمله نرم‌افزارهایی که اطلاعات اصلی را پردازش می‌نمایند هدف حلمه قرار می‌گیرند و بدین ترتیب این برنامه‌ها دیگر توانایی پردازش اطلاعات و نمایش آن به کاربران را نخواهند داشت.

ب) جلوگیری از سرویس با حمله به کانال ارتباطی: مهاجم در این نوع حمله کانال ارتباطی را متوقف می‌سازد به طوری که هیچ راه ورود و خروجی وجود نخواهد داشت.

ج) جلوگیری از سرویس با حمله به کل سیستم: این نوع حمله باعث خواهد شد سیستم به همراه تمامی برنامه‌های کاربردی آن و اطلاعاتی که این برنامه‌ها با آن کار می‌کنند غیرقابل استفاده گردد.

۴- تکذیب و انکار: این حمله باعث می‌شود تا اطلاعات به صورت نادرست و غیر واقعی ارائه شود و یا اینکه وقوع یک واقعه حقیقی و عملیاتی که انجام شده است انکار شود. انواع آن عبارتند از:

الف) ماسک زدن: در این نوع حلمه مهاجم سعی می‌کند هویت شخص یا سیستم دیگری را جعل کند.

ب) تکذیب یک واقعه: در این نوع حمله مهاجم یک واقعه‌ای را که اتفاق افتاده و مجموعه فعالیت‌هایی که انجام شده و ثبت گردیده است را انکار می‌نماید.

سرویس مقابله / نوع حمله	محرمانه‌سازی	تمامیت	فراهمی	مجوزسنجی
دسترسی	✓	—	—	✓
دستکاری	✓	✓	✓	✓
جلوگیری از سرویس (Dos)	—	—	✓	—
انکار	✓	✓	—	✓

سرویس‌های مقابله با حملات: مجموعه سرویس‌هایی که برای خنثی کردن حملات احتمالی به اطلاعات یک سازمان وجود دارد سرویس‌های مقابله با حملات یا سرویس‌های امنیتی گفته می‌شود. در این سرویس‌ها مکانیزم‌هایی توصیه می‌شود که به کمک آنها راه‌های نفوذگری و حمله مسدود می‌گردد که با توجه به این روش‌ها چهار راه مقابله با حملات ارائه می‌گردد:

۱- محرمانه‌سازی: در این سرویس امکاناتی فراهم می‌شود که به کمک آنها فقط کاربرانی اجازه دسترسی به اطلاعات را دارند که مجاز به استفاده می‌باشند برخی از روش‌های این سرویس عبارتند از: الف) محرمانه‌سازی اطلاعات به هنگام ارسال و مخابره: در این روش اطلاعات قبل از اینکه بر روی کانال ارتباطی قرار گیرد به صورت رمز درآمده و سپس ارسال می‌گردد. ب) محرمانه‌سازی جریان ترافیک: همان‌طور که می‌دانیم با استفاده از اطلاعات ترافیکی بین دو نقطه تا حدودی می‌توان سازمانی که این دو Node در آن وجود دارند را شناسایی کرد چرا که اطلاعات مبادله شده شامل بخشی از اطلاعات سازمان می‌باشد. لذا سرویس محرمانه‌سازی در جریان ترافیک با اصل اطلاعات که ذخیره یا ارسال می‌شود کاری ندارد بلکه به نوع و شکل مبادله اطلاعات بین دو نقطه می‌پردازد.

نکته: با استفاده از سرویس محرمانه‌سازی می‌توان حمله دسترسی را خنثی نمود. اما این سرویس به تنهایی قادر به حل همه مشکلات امنیتی نیست.

۲- سرویس تمامیت: این سرویس برای صحت و کامل بودن اطلاعات ایجاد شده است و کاربر می‌تواند از تمامیت اطلاعات و درست بودن آنها اطمینان حاصل نماید و مطمئن باشد.که این اطلاعات توسط افراد غیرمجاز دستکاری نشده است. این سرویس قادر است از موفقیت حملات تکذیب و دستکاری اطلاعات جلوگیری نماید و با وجود آن تغییرات غیرمجاز چه در مبدأ، مقصد و زمان انتقال کشف خواهد شد. با ترکیب این سرویس با سرویس‌های دیگر حتی تغییراتی که خارج از سازمان به روی اطلاعات انجام می‌شود قابل کشف و پیگیری خواهد بود.

۳- سرویس فراهمی: این سرویس باعث می‌شود اطلاعات همیشه در دسترس بوده و قابل استفاده باشد. مکانیزم‌های این سرویس به کاربران اجازه می‌دهد در کوتاهترین زمان به اطلاعات اصلی و یا برنامه کاربردی دستری پیدا نمایند. همچنین در خصوص کانال‌های ارتباطی نیز راه‌هایی پیشنهاد می‌شود که اطلاعات مورد درخواست کاربران در نهایت توسط ایشان دریافت شود. برخی از این روش‌ها عبارتند از:

الف) استفاده از نسخه پشتیبان: در این روش به هنگام تخریب عمومی و یا از بین رفتن اطلاعات سازمان اطلاعات اصلی به شکل نسخه‌های پشتیبان در مکان‌های امنی نگهداری می‌شود و پس از بروز اشکالی در سیستم و یا از بین رفتن اطلاعات می‌توان آن را به حالت صحیح اولیه بازگرداند. همانگونه که مشخص است بازیابی اطلاعات در این روش به مدت زمانی نیاز دارد.

ب) روش غلبه بر خطا: در این روش بروز خطا و اشکال به‌طور خودکار تشخیص داده شده و پس از آن اطلاعات صحیح به شکل اولیه خود بازسازی می‌گردد. در این روش زمانی برای بازسازی اطلاعات ظاهراً صرف نمی‌شود و کاربران خارج از سرویس بودن سرویس‌دهنده را حس نمی‌کنند. این روش به دلیل استفاده از تجهیزات سخت‌افزاری نسبت به روش‌های قبلی هزینه‌های بیشتری را نیاز دارد.

نکته: سرویس فراهمی باعث می‌شود بتوانیم در مقابله با حملات Dos مقاومت نماییم. اگر چه راهی برای پیشگیری از حملات Dos وجود ندارد. اما این سرویس باعث کاهش اثرات ناشی از آن می‌شود و می‌توان سیستم را در اسرع وقت به حالت اولیه برگرداند.

۴- سرویس مجوزسنجی: این سرویس سخت‌ترین بخش امنیت است چرا که بدون اضافه کردن ارزشی به سیستم پیچیدگی آن را اضافه می‌نماید و به نسبت هزینه‌ها بالا می‌رود و کاربری مشکل می‌شود. البته این سرویس به خودی خود قادر به محافظت کامل در برابر حملات نمی‌باشد بلکه معمولاً به منظور بالا بردن امنیت به همراه سرویس‌های دیگر استفاده می‌شود و خود شامل دو بخش اصلی است.

الف) هویت سنجی: در این بخش مشخص می‌شود فردی که قصد انجام کاری را دارد همان شخصی است که ادعا می‌کند و هویت فرد با توجه به اطلاعات ارائه شده سنجیده می‌شود.

ب) اعتبار سنجی: در این بخش ادعای فرد ثابت شده و اعتبار آن بررسی می‌شود و معمولاً این روش‌ها با استفاده از موارد زیر انجام می‌گیرد:

۱- بر پایهٔ آنچه شخص می‌داند مثل Passwoed
۲- بر پایهٔ آنچه شخص دارد و مالک آن است مانند کارت‌های اعتباری
۳- بر پایهٔ آنچه شخص هست مانند اثر انگشت یا قرنیه چشم

سیاست‌های امنیتی

تعریف: اعلامیه‌ای است رسمی شامل مجموعه عواملی که می‌بایست توسط تمامی کاربران که به نوعی با سرمایه‌های اطلاعاتی و تکنولوژیکی سازمانی و شبکه آن در ارتباط هستند اجرا گردد. این سیاست‌ها باید به گونه‌ای تدوین شود که تمامی کاربران (مدیران، کارشناسان و کارکنای که به نوعی در امور سازمان دخیل هستند) مرتبط باشد در واقع ضمانت اجرایی یک سیاست امنیتی همین نکته است.

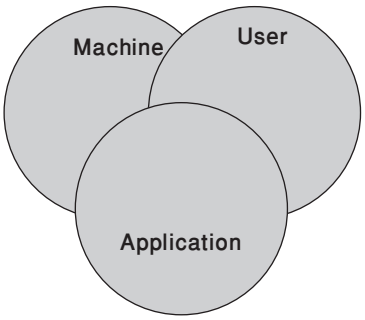
اهداف سیاست امنیتی:

- دادن آگاهی لازم به تمامی کاربران، مسئولین و افراد مرتبط با سازمان در خصوص چگونگی بکارگیری صحیح از تجهیزات موجود جهت حفظ و سیاست از سرمایه‌های اطلاعاتی.
- ارائه راه‌حل‌های اصولی و تبعیت از آن برای پیکربندی صحیح و تست آسیب‌پذیری ابزارها، سیستم و برنامه کاربردی موجود که هر یک از این موارد در غالب سیاست‌های امنیتی باید توسط تمامی کاربران ارائه شود.

معمولاً سیاست‌های امنیتی در سه سطح ارائه می‌گردد:

- کاربران
- برنامه کاربردی
- تجهیزات

در واقع سیاست‌های امنیتی به همه این سطوح و وجه اشتراکشان تأثیرگذار است.



پارامترهای لازم‌الاجرای سیاست‌های امنیتی:

یک سیاست امنیتی در صورتی پذیرفته می‌شود و قابل اجراست که پارامترهایی را در هر یک از سطوح فوق مهیا نماید که برخی از این موارد عبارتند از:

۱- مشخص بودن چهارچوب سیاست امنیتی که در این بخش موارد زیر حائز اهمیت است:
الف) چه ابزاری و با چه عملکردهایی مورد نیاز است؟
ب) در مقابل کارهای مخرب از طرف کاربران و نفوذگران چه رفتاری را باید اتخاذ نمود.

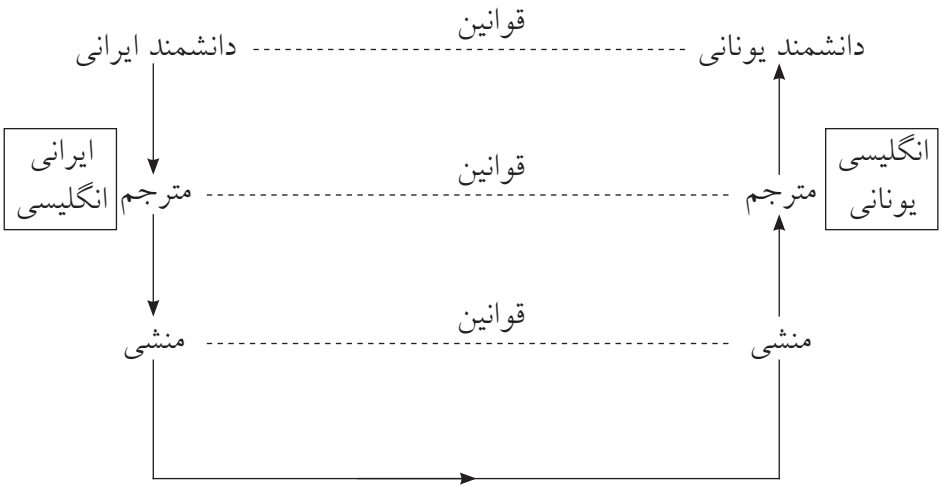
ج) چه کارهایی را کاربران مجاز به انجام آن می‌باشند و برای انجام چه کارهایی مجاز نیستند و...

۲- به چه کسی و یا چه چیزی و به چه میزان باید اطمینان نمود؟
۳- در نظر گرفتن دیدگاه‌های افراد مختلف که در سازمان حضور دارند در رابطه با چگونگی برقرای سیاستهای لازم.
۴- چه کسی یا چه کسانی در مقابل سیاست‌های اعمال شده مسئولیت دارند و وظایف آنها چگونه است؟
۵- مشخص کردن فرآیند طراحی سیاست‌های امنیتی

نکته: سیاست‌های امنیتی بر اساس ساختار، قوانین و امکانات یک سازمان تعیین می‌شود. بنابراین طبیعی است که هر سازمان سیاست‌های امنیتی خاص خود را داشته باشد.

ویژگی‌های سیاست امنیتی:
۱- به گونه‌ای طراحی شود که امکان پیاده‌سازی عملی آن در سطوح مختلف وجود داشته باشد.
۲- محدودهٔ مسئولیت کاربران، مدیران شبکه، مدیران عملیاتی و کلیه کارکنان سازمان باید در یک سیاست امنیتی خوب به صورت شفاف مشخص شده باشد.
۳- سیاست‌های امنیتی باید قابل ارتقاء، و انعطاف‌پذیر باشد تا در مقابل تغییرات دچار اشکال نشود.

*** ملزومات اولیه سیاست‌های امنیتی:**
۱- سیاست‌ها باید مختصر و مفید و قابل فهم برای تمامی کاربران سیستم باشد.
۲- سیاست امنیتی باید به گونه‌ای طراحی شود که موازنه منطقی بین حفاظت، سرعت و هزینه‌ها ایجاد نماید.
۳- دلایل احتیاج به این سیاست امنیتی به‌طور صریح و روشن بیان گردد.
۴- چگونگی برخورد با متخلفین که از چارچوب سیاست‌های تعیین شده خارج می‌شوند به‌طور دقیق و روشن بیان گردد.



پروتکل‌های شبکه:

برای تحلیل و فهم روش‌هایی که یک نفوذگر با بکارگیری آنها به شبکه حمله می‌کند باید یک دانش پایه از تکنولوژی‌های شبکه داشته باشیم تا مکانیزم‌های حملات را بهتر درک نماییم. در این راستا آشنایی با مجموعه قوانین و مقررات موجود در شبکه‌ها مفید خواهد بود.

با توجه به مثال ارائه شده (شکل بالا) برای جلوگیری از طراحی شبکه‌ها به صورت سلیقه‌ای و به‌تبع آن پیچیده‌تر شدن ارتباطات شبکه‌ای سازمان جهانی استاندارد مدل ۷ لایه‌ای را برای ارتباطات شبکه‌ای ارائه نمود که این لایه‌ها عبارتند از:

۱- Physical (فیزیکی)
۲- Data Link (اتصال داده)
۳- Network (شبکه)
۴- Transport (انتقال)
۵- Session (جلسه)
۶- Presentation (نمایش یا ارائه)
۷- Application (کاربرد)

مسائل و مشکلات طراحی شبکه‌ها:

برای طراحی مجموعه قوانین یک شبکه کامپیوتری مسائل و مشکلات بسیار گسترده و متنوعی وجود دارد که برای دست یافتن به یک ارتباط مطمئن و قابل اعتماد بین دو ماشین باید به گونه‌ای حل شود. این مسائل و مشکلات همگی از یک جنس نیستند و منشأ و راه‌حل مشابهی نیز ندارند.

برخی از آنها توسط سخت‌افزار و بخشی دیگر با تکنیک‌های نرم‌افزاری قابل حل است. برخی از این مسائل و مشکلات عبارتند از:

۱- چگونگی ارسال و دریافت بیت‌های اطلاعات که آیا به صورت سیگنال الکتریکی، الکترومغناطیسی و یا نوری باشد که معمولاً با توجه به کانال ارتباطی یکی از این روش‌ها انتخاب می‌شود.

۲- ماهیت انتقال اطلاعات چگونه باشد که در این بخش سه روش مختلف مطرح می‌گردد. الف) ارتباط یک‌طرفه مانند رادیو و تلویزیون ب) ارتباط دوطرفه غیرهم زمان مانند بی‌سیم ج) ارتباط دوطرفه همزمان مانند خطوط تلفن.

۳- مسألهٔ خطا و وجود Noise در کانال‌های ارتباطی بدین معناست که ممکن است در حین ارسال داده‌ها روی کانال فیزیکی بخشی از بیت‌ها دچار خرابی شوند. بنابراین باید خطای موجود تشخیص داده شده و اصلاح شود و در صورت عدم امکان اصلاح مجدداً ارسال گردد.

۴- با توجه به اینکه در شبکه‌ها ممکن است مسیرهای گوناگونی بین مبدأ و مقصد وجود داشته باشد پیدا کردن بهترین مسیر و هدایت بسته‌ها به سمت مقصد از کارهای مهم و پیچیده محسوب می‌شود.

۵- ممکن است گیرنده به دلایلی نتواند با سرعتی که فرستنده اطلاعات را ارسال می‌کند آنها را دریافت نماید. بنابراین تکنیک‌ها و روش‌های هماهنگی بین فرستنده و گیرنده از کارهای مهم به حساب می‌آید.

۶- با توجه به اینکه ماشین‌های بسیاری به عنوان فرستنده و یا گیرنده در یک شبکه وجود دارند حل کردن مشکلات ازدحام، تداخل، تصادم، حائز اهمیت است.

اصول طراحی قوانین شبکه‌ها (پروتکل)

۱- هر لایه وظیفه مخصوص به خود را دارد و لایه‌ها بر اساس ماهیت کاریشان ایجاد می‌شوند.
۲- وظیفه هر لایه باید با توجه به قراردادها و استانداردهای جهانی مشخص شود.
۳- تعداد لایه‌ها نباید آنقدر زیاد باشد که تمایز لایه‌ها با توجه به سرویس‌های آنها مشکل شود و نه آنقدر کم باشد که وظیفه و خدمات یک لایه پیچیده و نامشخص گردد.
۴- هر لایه به لایه بالاتر سرویس می‌دهد و به جزئیات لایه‌های زیرین توجهی ندارد.
۵- مرزهای هر لایه به گونه‌ای انتخاب شود که جریان اطلاعات بین لایه‌ها حداقل باشد.

وظایف لایه‌های مختلف پروتکل OSI:

۱- لایه فیزیکی(Physical): وظیفه اصلی در این لایه انتقال بیت‌ها به صورت سیگنال‌های الکتریکی و ارسال آن بر روی کانال ارتباطی است. واحد اطلاعات در این لایه بیت است و برخی از پارامترهایی که در این لایه مد نظر قرار می‌گیرند عبارتند از: الف) ظرفیت کانال ارتباطی. ب) نرخ انتقال اطلاعات...

۲- اتصال داده یا پیوند داده (Data Link): در این لایه با استفاده از مکانیزم‌های کشف و کنترل خطا فرآیندی صورت می‌گیرد تا اطلاعات بدون خطا و مطمئن به مقصد برسد. در این لایه اشکالات کشف شده اصلاح می‌گردد و در صورتیکه نتوان اطلاعات را اصلاح نمود تدابیری اتخاذ می‌گردد تا اطلاعات مجدداً ارسال شود. همچنین یکی دیگر از وظایف این لایه کنترل جریان ترافیک است و سعی می‌شود هماهنگی بین فرستنده سریع و گیرندهٔ کُند بوجود آید. واحد اطلاعاتی در این لایه Frame است.

۳- لایه شبکه(Network): از آنجایی که بین دو ماشین در شبکه مسیرهای گوناگونی وجود دارد این لایه وظیفه دارد مسیر هدایت اطلاعات به مقصد درست را تعیین نماید. در این لایه تدابیری اندیشیده می‌شود تا از ازدحام و تداخل جلوگیری شود. واحد اطلاعاتی در این لایه Packet است.

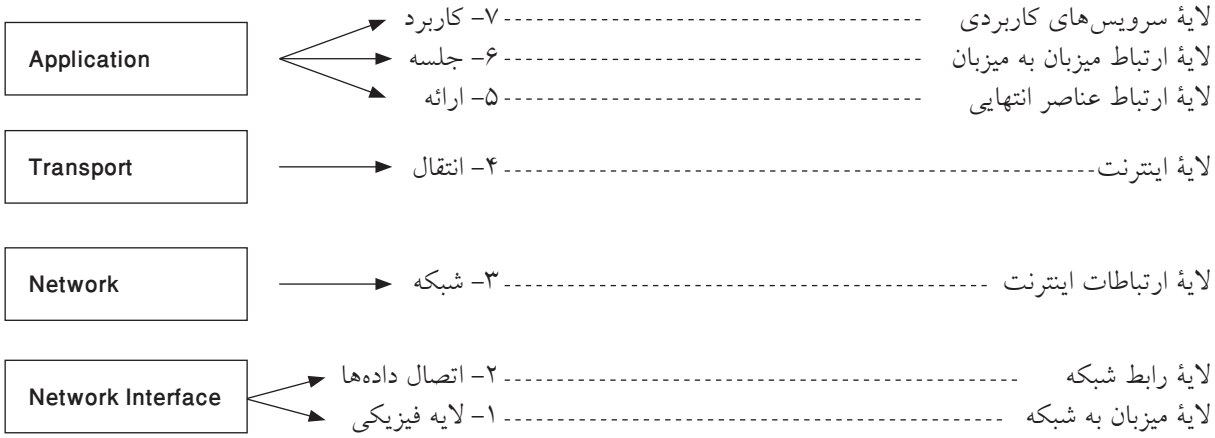
۴- لایه انتقال(Transport): در این لایه بر اساس خدمات لایه‌های زیرین یک سرویس انتقال بسیار مطمئن (اتصال‌گرا) ارائه می‌شود. همچنین تقسیم پیامهای بزرگ به بسته‌های اطلاعاتی کوچک‌تر و بازسازی بسته‌های اطلاعاتی و تشکیل یک پیام کامل، از وظایف این لایه محسوب می‌شود. واحد اطلاعاتی در این لایه قطعه (Secment) است.

۵- لایه جلسه (Session): وظیفهٔ این لایه فراهم آوردن شرایط یک نشست (مانند ورود به سیستم از راه دور، احراز هویت طرفین و مواردی این چنینی) می‌باشد. برخی از این وظایف عبارتند از: برقراری و مدیریت یک جلسه یا نشست، مشخص نمودن اعتبار پیامها و اتمام جلسات و...

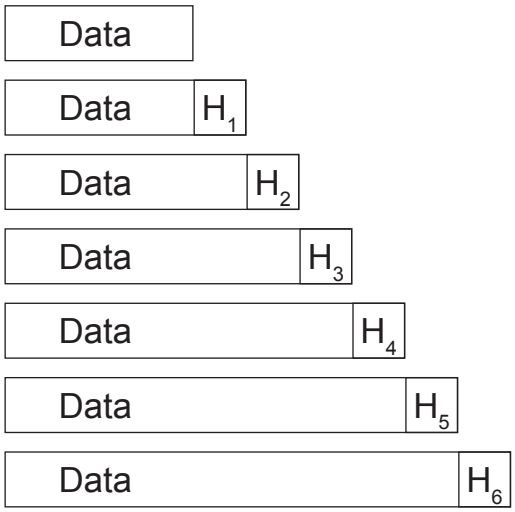
۶- لایه نمایش یا ارائه (Presentation): در این لایه وظایفی مانند فشرده‌سازی فایل‌ها، رمزگشایی و رمزنگاری اطلاعات، تبدیل کدهای مختلف به یکدیگر و به عبارتی تمامی کارهایی که مربوط به چگونگی نمایش اطلاعات می‌باشد، در این لایه انجام می‌شود.

۷- **لایه کاربرد (Application):** در این لایه استاندارد مبادله پیام بین نرم‌افزارهایی که در اختیار کاربر بوده و به نحوی با شبکه در ارتباط هستند تعریف می‌شوند. این لایه شامل استانداردهایی نظیر: انتقال نامه‌های الکترونیکی، دسترسی به بانک‌های اطلاعاتی از راه دور، مدیریت شبکه و مواردی این چنینی می‌باشد.

اسامی دیگر لایه‌های TCP/IP

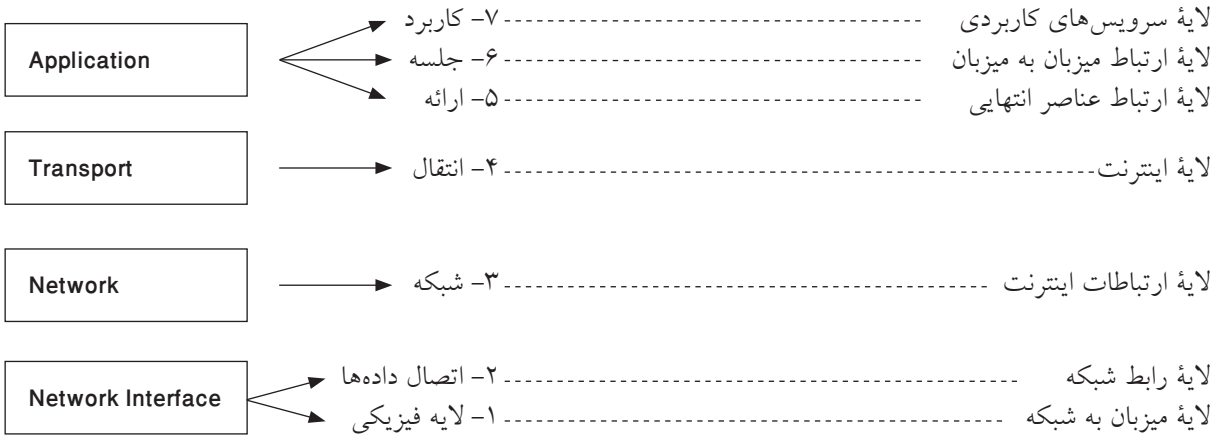


TCP/IP
Transmission Control Protocol / Internet Protocol



پروتکل TCP/IP: این مدل در کتاب‌های استاندارد دارای ۴ لایه می‌باشد که امروزه با توجه به مباحث امنیتی و تفکیک وظایف برخی از این پروتکل‌ها به تعداد این لایه‌ها اضافه گردیده است.

ارتباط مدل OSI با TCP/IP:



وظایف پروتکل TCP/IP:

۱- لایهٔ میزبان به شبکه (Network Interface): در این لایه استانداردهای سخت‌افزاری - نرم‌افزاری (راه‌اندازها یا Drivers) و پروتکل‌های شبکه تعریف می‌شود. این لایه با مسائل فیزیکی، الکتریکی، مخابراتی، چگونگی عملکرد رابطه‌های شبکه (کارت شبکه) و موارد این چنینی درگیر است. همچنین با توجه به اینکه شبکه‌های مختلف استانداردهای مختلفی را رعایت می‌کنند (چه از لحاظ سخت‌افزاری و چه از لحاظ نرم‌افزاری) این لایه وظیفه دارد هماهنگی بین این شبکه‌های متفاوت را انجام دهد. پروتکل‌های لایه اول می‌توانند مبتنی بر ارسال بیت یا بایت باشد.

۲- لایهٔ شبکه (Network): مهم‌ترین وظیفهٔ این لایه عبارتست از هدایت بسته‌ها از مبدأ تا مقصد که بدین منظور در این لایه چندین پروتکل در کنار هم وظیفهٔ مسیریابی و تحویل بسته‌های اطلاعاتی از مبدأ تا مقصد را انجام می‌دهد. مهم‌ترین پروتکل این لایه پروتکل IP است. مکانیزم‌های موجود در این لایه بر اساس ساختار بدون اتصال می‌باشد یعنی ارسال یک بسته بر روی شبکه عبور از مسیر خاصی را تضمین نمی‌کند. یعنی اگر دو بسته متوالی برای یک مقصد یکسان ارسال شود هیچ تضمینی در به ترتیب رسیدن آنها وجود ندارد. چرا که ممکن است این بسته‌ها از مسیرهای متفاوتی به سمت مقصد خود حرکت نمایند. ضمناً در این لایه سرویسی به منظور سالم رسیدن یا نرسیدن اطلاعات به مقصد وجود ندارد به همین دلیل این سرویس‌ها نامطمئن هستند و قاعدتاً لایه‌های بالاتر وظایف این چنینی را برعهده خواهند داشت. (Connection less)

۳- لایهٔ انتقال(Transport): این لایه ارتباط ماشین‌های انتهایی را برقرار می‌کند و با سرویس‌هایی که ارائه می‌نماید یک ارتباط اتصال‌گرا و مطمئن برقرار خواهد شد. (Connection Oriented)

نکته: منظور از اتصال‌گرا و بدون اتصال مانند مخابرات و پست است. در این لایه سرویس‌های پیش‌بینی شده است که فرستنده از رسیدن یا عدم رسیدن درست بسته به مقصد با خبر شود.

۴- لایهٔ کاربرد (Application): در این لایه بر اساس خدمات لایه‌های زیرین سرویس‌های سطح بالایی برای ایجاد برنامه‌های کاربردی ارائه می‌شود که این خدمات در غالب پروتکل‌های استانداردی همانند موارد زیر در اختیار کاربران قرار می‌گیرد.

- پروتکل انتقال فایل یا FTP
- سرویس مدیریت پست الکترونیکی.
- پروتکل انتقال صفحات فوق متنی یا HTTP
- و...

Firewall

FireWall: تکنولوژی دیوار آتش در دهۀ اول ۱۹۹۵ با دیوارهای آتش ساده به دنیای IT معرفی و عرضه شد. با توسعۀ فضای مجازی جدید FireWallها نیز پیشرفت چشمگیری در جهت تأمین امنیت برای کاربران شبکه فراهم نمود.

تعریف Firewall: سیستمی است که سیاست‌های کنترل دسترسی یا ACL (Access Control List) را بین دو شبکه اجرا کرده و بر چگونگی انجام این کار نظارت دارد. همچنین Firewallها را می‌توان جهت ایزوله نمودن یک شبکه منفرد از شبکه‌های دیگر (اینترنت یا زیر شبکه‌های داخلی) استفاده نمود. در حقیقت Firewall محلی است برای ایست و بازرسی بسته‌های اطلاعاتی (مانند ایست و بازرسی فرودگاه) به گونه‌ای که این اطلاعات بر اساس تابعی از قوانین امنیتی که در سیاست‌های امنیتی پیش‌بینی شده است پردازش شده و صرفاً بر طبق آن قوانین اجازۀ عبور و یا جلوگیری کردن از اطلاعات صادر می‌شود.

وظایف Firewall:

فایروال‌های بسته‌های ورودی به شبکه و یا خروجی از شبکه را بر اساس IP مبدأ و IP مقصد و نوع پروتکل، شماره پورت مبدأ، شماره پورت مقصد، نوع برنامه کاربردی و برخی اطلاعات سرآیندهای بسته‌ها را مورد بازرسی و کنترل قرار می‌دهند و با توجه به نوع سیاست امنیتی سه حالت مختلف برای ترافیک عبوری بسته‌ها در نظر می‌گیرند:

۱- **Allow Mode:** تمام بسته‌ها اجازه عبور دارند.

۲- **Restrict Mode:** تنها اجازه عبور به بسته‌هایی داده می‌شود که اجازه عبور داشته باشند و همچنین برای بسته‌هایی که اجازه عبور نداشتند پیامی ارسال می‌شود.

۳- **Block Mode:** تمامی بسته‌ها بلوک می‌شوند و اجازه عبور دریافت نخواهند کرد.

نکاتی در خصوص فایروال‌ها:

۱- باتوجه به اینکه امروزه در هر سازمان و شبکه مربوط به آن مباحث امنیت از اهمیت ویژه‌ای برخوردارند وجود فایروال برای تأمین امنیت و به عنوان یکی از مهمترین استانداردهای امنیتی برای هر سازمان و کاربری لازم و اجباری می‌باشد.

۲- با توجه به نوع وظیفه و نوع عملکردی که فایروال‌ها بر عهده دارند این سیستم همواره به عنوان یک گلوگاه در شبکه محسوب می شود چراکه باعث بالا رفتن ترافیک، تأخیر در انتقال اطلاعات، ازدحام و در شرایط بدتر نهایتاً تبدیل به بن‌بست می‌شود با این توضیحات تأخیر در فایروال‌ها اجتناب‌ناپذیر است و باید در پیاده‌سازی آن تعادلی بین سرعت و امنیت ایجاد کرد.

قابلیت‌های اضافه در فایروال‌های جدید:

فایروال‌های امروزی علاوه بر وظایف اصلی که برعهده دارند قادر به پشتیبانی از ویژگیهای بیشتر امنیتی نیز می‌باشند برخی از این ویژگیها عبارتند از:

۱- **Nat** (Network Address Translation): این ویژگی اجازه استفاده از آدرس‌های IP خصوصی را در شبکه می‌دهد و کامپیوترهای موجود در شبکه با تعداد کمی آدرس IP عمومی به شبکه بزرگتری مانند اینترنت متصل می‌شوند این ویژگی باعث مخفی نمودن آدرس‌های IP شبکه داخلی شده و از دید کاربر خارجی پنهان می‌ماند.

۲- **Port Forwarding:** قابلیتی است که امکان دسترسی کاربران خارجی به سرورهای عمومی شبکه داخلی با آدرس IP خصوصی را فراهم می‌کند.

۳- **Virus Checking:** فایروال‌ها توانایی این را خواهند داشت که اجازه عبور بسته‌های اطلاعاتی را که حامل داده‌های آلوده می‌باشند را ندهد.
۴- **URL Screening:** با استفاده از این قابلیت می‌توان بر اساس سیاستهای امنیتی که برای سازمان پیش‌بینی شده است دسترسی به برخی از سایت‌های موجود در اینترنت را محدود نمود.
۵- **Remote Management:** با استفاده از این ویژگی کنترل و نظارت بر اساس سیاستهای امنیتی را می‌توان از راه دور انجام داد.
۶- **VPN** (Virtural Private Network): استفاده از قابلیت‌های ارتباطی و امنیتی بین دو شبکه داخلی به کمک این مکانیزم ایجاد می‌شود و فایروال‌های امروزی توانایی برپایی VPN را به کاربران خود می‌دهند.
۷- و موارد دیگر...

مزایا و معایب استفاده از فایروال:

مزیت‌ها:

۱- فایروال‌ها وسیله‌ای هستند که می‌توان سیاست امنیتی مورد نظر را به کمک آنها در ساختار سازمان اعمال نمود تا این سیاستها در تمامی شبکه سازمان گسترش یافته و اجرایی شود.
۲- از فایروال‌ها برای محدود نمودن دسترسی کاربران به سرویس‌های موجود به شبکه نیز استفاده می‌شود. به عنوان مثال می‌توان با تنظیماتی در فایروال اجازه استفاده از سرویس FTP به برخی از کاربران داده شود و به برخی دیگر داده نشود.
۳- فایروال‌ها قابلیت ثبت تمامی وقایع جاری شبکه را در Log fileها فراهم خواهند کرد و با بررسی دقیق این فایل‌ها می‌توان نسبت به حملات جاری و یا حملات احتمالی روش‌های پیشگیری لازم به کار گرفته شوند.

معایب:

۱- کارآیی این سیستم‌ها وابسته به قوانین موجود در سیاست امنیتی است و در مقابل قوانین پیکربندی و مدیریت که برخی از مسائل اساسی را در نظر نگرفته‌اند بسیار آسیب‌پذیر خواهد بود.
۲- این سیستم‌ها برای متوقف کردن حملاتی که بر علیه پورتهای باز صورت می‌گیرد، توانایی مقابله ندارد.

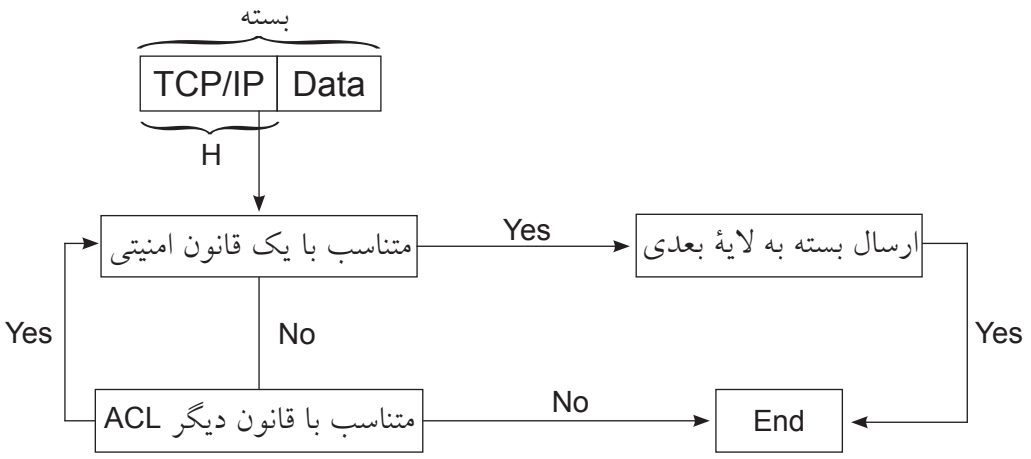
انواع Firewall از لحاظ نوع عملکرد:

- **Packet Filtering** (فیلتر عمومی)
- **Statefull Incpection** (بازرسی هوشمند)
- **Application Gateway / Proxy** (دروازه برنامه کاربردی)

معمولاً بر اساس نوع کاری که Firewallها در لایه‌های مختلف بر روی سرآیندها انجام می‌دهند. دارای عملکردهای متفاوتی می‌باشند و بر اساس این عملکرد و همچنین تعداد لایه‌هایی که در پروتکل TCP/IP مورد ارزیابی قرار می‌دهند به سه دسته تقسیم می‌شوند.

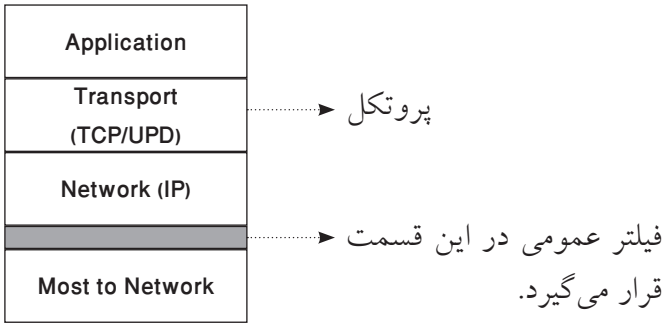
۱- **Packet Filtering:** این فایروال‌ها به عنوان اولین فایروال‌های مطرح برای تأمین امنیت شبکه معرفی و عرضه

شده‌اند. فایروال‌های اینگونه معمولاً بر روی فیلدهای سرآیند پروتکل IP و برخی از فیلدهای سرآیند پروتکل TCP مطابق شکل زیر عمل می‌کند.



موارد مطرح در این فایروال‌ها عبارتند از:

۱- آدرس IP مبدأ بسته یا Packet
۲- آدرس IP مقصد بسته یا Packet
۳- نوع پروتکل ارتباطی
۴- شماره Port (درگاه) مبدأ بسته
۵- شماره Port (درگاه) مقصد بسته
۶- و موارد این چنین...



نکته ۱: با توجه به نوع عملکرد این نوع فایروال‌ها بهتر است از آنها در کنار فایروال‌های دیگر استفاده نمود تا کارآیی بالا رفته و بازدهی شبکه بیشتر شود.

نکته ۲: به طور کلی فایروال‌های Packet Filtering برای محیط‌هایی که فاکتور سرعت ارجحیت دارد و نیاز به ثبت رخدادهای موجود در شبکه Logfile نمی‌باشد پیشنهاد می‌گردد.

نکته ۳: این نوع فایروال‌ها یکی از بهترین ابزارهای موجود برای ایمن نمودن شبکه در نقاط مرزی و ارتباطی با سایر شبکه‌هاست. همچنین به منظور محدود نمودن ارتباطات زیرشبکه‌های داخلی و اجرای سیاست‌های ACL (Access Control List) و انتقال ترافیک عبوری به سایر فایروال‌ها از این نوع فایروال‌ها استفاده می‌شود.

معایب و مزایای Packet Filtering:

معایب

۱- به دلیل عدم نظارت بر لایه‌های بالاتر توانایی مقابله با انواع مختلف حمله‌ها که در این لایه‌ها صورت می‌گیرد را ندارد به عنوان مثال توانایی Block نمودن دستورات اجرایی که در متن بسته‌ها گنجانده می‌شود را

ندارد.

۲- به دلیل محدود بودن تعداد فیلدهای کنترلی اطلاعات درست و کاملی در خصوص موارد مشکوک که باید جلوگیری شود بدست نمی‌آید.

۳- تأئید اعتبار کاربران به علت فقدان اطلاعات لازم (که البته در لایه‌های بالاتر وجود دارد) بصورت پیشرفته صورت نمی‌گیرد.

۴- در مقابل حملاتی که ناشی از ضعف پروتکل‌های IP و TCP است عاجز و ناتوان است، چرا که بر اساس اطلاعاتی که این پروتکل‌ها تولید می‌کنند کار می‌کند.

مزیت‌ها:

۱- Over Head یا سربار کمتری نسبت به سایر فایروال‌ها دارد از این‌رو سریعتر از آنها بوده و باعث افت کارآیی شبکه نمی‌شود.

۲- نسبت به سایر فایروال‌ها ارزانتر است.

۳- نظارت و مدیریت ترافیک شبکه را بر اساس آدرس‌های IP مبدأ و مقصد به خوبی اجرا می‌نماید.

۲- Stateful Inspection: این فایروال‌ها قادرند مشخصات ترافیکی خروجی از شبکه را برای مدتی حفظ نمایند و بر اساس پردازش آنها مجوز عبور لازم صادر کند با وجود این نوع فایروال‌ها بسته‌هایی که با ظاهر مجاز می‌خواهند به درون شبکه نفوذ کنند از بسته‌های واقعی تمیز داده می‌شوند مکانیزم‌های موجود در این نوع فایروال‌ها این‌گونه عمل می‌کند که ترافیک خروجی برای چند ثانیه در حافظه‌های موجود نگهداری کرده پس از پردازش اطلاعات موجود تصمیم می‌گیرند که آیا یک بسته اجازه عبور دارد یا خیر.

مزیت:

۱- تمرکز این فایروال بر روی لایه‌های Transport و Internet می‌باشد بنابراین نسبت به فایروال‌های مبتنی بر پراکسی سریعتر است.

۲- مستقل از برنامه کاربردی بوده و کار نظارت و بررسی خود را انجام می‌دهد.

۳- نسبت به فایروال‌های قبلی جزئیات بیشتری را بررسی و کنترل می‌نماید و فیلدهای کنترلی بیشتری در این نوع فایروال‌ها وجود دارد.

معایب:

۱- به دلیل نگهداری ترافیک خروجی (حتی برای چند میلی ثانیه) دارای تأخیر بوده و نسبت به فایروال‌های Packet filtering کندتر عمل می‌کند.

۲- به منظور نگهداری ترافیک خروجی به حافظه‌های زیاد نیاز داشته در نتیجه هزینه بر خواهد بود.

۳- Application Gateway / Proxy: با استفاده از این فایروال‌ها هیچ نشست مستقیم (Session) و رو در روی بین مبدأ و مقصد شکل نمی‌گیرد. بلکه ارتباط این دو Node به وسیله یک ماشین واسط برقرار می‌شود که این واسطه بر روی داده‌های در حال مبادله در طول نشست کنترل و نظارت خواهد داشت همانگونه که مشخص است این نوع فایروال به حافظه نسبتاً زیاد و پردازشگرهای بسیار سریع نیاز دارند.

مزیت‌ها:

۱- ارتباط در این نوع فایروال صرفاً از طریق پراکسی صورت می‌گیرد بنابراین سیستم‌های هدف از دید کاربران خارجی پنهان خواهد بود.

۲- علاوه بر فیلدهای سرآیند پروتکل‌های مختلف توانایی بررسی و کنترل محتوای داده‌ای مانند محتوای نامه‌های الکترونیکی و صفحات وب را نیز دارا می‌باشند.

۳- با استفاده از این نوع فایروال‌ها می‌توان حملاتی که از طرف کاربران داخلی صورت می‌گیرد خنثی نمود.

۴- قابلیت محدود نمودن دسترسی کاربران با اعمال فرآیند تأیید اعتبار به ازای هر سرویس و منبعی را دارا می‌باشد.

۵- امکان پویش و جستجوی فایل‌های آلوده و ویروس‌ها را داشته و امکاناتی برای حذف آنها ارائه می‌دهد.

۶- امکان بلوکه نمودن سرویس‌های برنامه‌های کاربردی خاص به عنوان مثال جلوگیری کردن از ارسال و دریافت پیام توسط برنامه‌های کاربردی مربوطه.

۷- امکان بلوکه نمودن دستورات اجرای خاص در برنامه‌های کاربردی.

۸- کنترل و نظارت خاص به ازای هر کاربر شبکه و بلوکه نمودن اجرای برخی از برنامه‌های آنها.

معایب:

۱- برای Applicationهای مختلف مانند پست الکترونیکی و موارد این چنینی نیاز به پراکسی مجازی می‌باشد.

۲- به دلیل عدم انعطاف‌پذیری برای برنامه‌های کاربردی جدید هیچ نظارت و کنترلی در این فایروال‌ها قابل اعمال نمی‌باشد و نمی‌توان آنها را برای Applicationهای جدید مجددا پیکربندی کرد.

۳- زمان بیشتری برای کنترل ترافیک صرف می‌نماید بنابراین تأخیر داشته و برای کاربردهایی که به پهنای باند بالایی نیاز دارند مناسب نمی‌باشند.

۴- به دلیل اینکه تمامی نشست‌های برقرار شده در ارتباط شبکه‌ای می‌باید کنترل و مدیریت شود غالباً این فایروال‌های به عنوان گلوگاه شبکه محسوب می‌شود و هر گونه تغییر و اشکال در پیکربندی آن کل شبکه را دچار بحران خواهد کرد.

۵- هزینه‌های این نوع فایروال‌ها به دلیل داشتن CPU یا پردازشگرهای سریع و حافظهٔ زیاد دارای هزینه‌های بالایی هستند.

مدیریت ریسک یا خطرپذیری (Risk management):

معمولاً هدف از امنیت مدیریت خطرپذیری است چنانچه مخاطرات امنیتی که متوجه سرمایه‌های اطلاعاتی یک سازمان است به شایستگی و درستی شناسایی یا درک نشود پیرو آن هنگام بروز خطا از منابع کافی استفاده نمی‌گردد و یا برعکس از منابع موجود بیش از اندازه استفاده می‌شود. نکته قابل توجه این است که با توجه به توضیحات بالا مدیریت خطرپذیری باعث ارزش‌گذاری سرمایه‌های اطلاعاتی می‌شود.

خطرپذیری یا ریسک چیست: امکان از دست دادن چیزی که نیاز به حفاظت دارد.

اجزای ریسک یا خطرپذیری:

۱- **آسیب‌پذیری:** پتانسیل و نیروی بالقوه‌ای که باعث می‌گردد سیستم اطلاعاتی ما مورد حمله قرار گیرد و انواع آن عبارتند از:

الف) آسیب‌پذیری سطح بالا: در این نوع آسیب‌پذیری با داشتن اطلاعات کمی می‌توان به تمامی سیستم دسترسی داشته و به گونه‌ای کنترل کل سیستم را به‌دست گرفت.

ب) آسیب‌پذیری سطح پایین: در این نوع آسیب‌پذیری مهاجم با در اختیار داشتن منابع و تجهیزات کافی و دسترسی به عوامل انسانی لازم اطلاعاتی را به‌دست آورد که از اهمیت بالایی برخوردار نیستند.

۲- **تهدید:** اقدام یا واقعه‌ای که بتواند امنیت محیطی سیستم مورد نظر را دچار آسیب کرده و باعث بروز اشکال در بخش‌های مختلف سیستم اطلاعتی گردد.

اجزای تهدید:

الف) هدف ب) مزدور ج) رخداد

الف) هدف: بخشی از سیستم‌های اطلاعاتی که مورد حمله قرار می‌گیرند هدف محسوب می‌شوند و معمولاً در ساختارهای اطلاعاتی که راههایی را برای مقابله با حملات پیش‌بینی نموده‌اند هدف همان سرویس‌های مقابله با حملات می‌باشد. به عنوان مثال اگر محرمانه‌سازی هدف قرار گیرد انگیزهٔ آن افشای اطلاعات برای افراد یا سازمان‌هایی است که مجاز به استفاده از این اطلاعات نیستند در این موارد مهاجم می‌خواهد چیزی را بداند که در حالت عادی از او دریغ می‌شود اگر تمامیت هدف باشد انگیزه تغییر اطلاعات و مهاجم به دنبال راهی برای دستکاری اطلاعات خواهد بود و یا اگر فراهمی هدف باشد انگیزه تغییر و جلوگیری از سرویس‌دهی اگر مجوز سنجی هدف باشد انگیزه از آن باز داشتن سازمان از بازسازی وقایع گذشته و تداخل در احراز هویت کاربران مجاز می‌باشد.

نکته: به عنوان هدف تهدید معمولاً سرویس‌های مقابله با حملات به تنهایی مورد حمله قرار نمی‌گیرند به عنوان مثال مهاجم مجوزسنجی را هدف قرار می‌دهد تا مقدمات لازم برای حمله به سرویس‌های دیگر فراهم گردد.

ب) مزدور: کسی است که برای آسیب‌رساندن به سازمان تهدید ایجاد می‌کند و دارای سه مشخصهٔ اصلی است: ۱- انگیزه ۲- دانش ۳- دسترسی، اجزای دسترسی: الف) دسترسی مستقیم ب) دسترسی غیرمستقیم. به عنوان مثال برق سرور را دستکاری می‌کنند تا اطلاعات سرور از بین برود. در سیستم‌های اطلاعاتی دانش مزدور عبارت است از: کلمه عبور کاربران، ID کاربران، محل قرار گرفتن فایل‌های اطلاعاتی، لیست اسامی پرسنل، آدرس Node شبکه و موارد دیگر...

انگیزه عبارتند از: کینه توزی، مبارزه‌طلبی، رقابت و...

نکته: بعضی از مزدورانی که برای سیستم‌های اطلاعاتی تهدید ایجاد می‌کنند عبارتند از: پرسنل سازمان، کارکنان اخراجی، نفوذگران و هکران، رقبای تجاری، مشتریان، بازدیدکنندگان و موارد دیگر...

ج) رخداد یا Event: از جمله روش‌های هستند که مزدوران تهدید کننده از طریق آن به سرمایه‌های اطلاعاتی سازمان صدمه می‌رسانند. برخی از رویدادها عبارتند از: سوء استفاده از دسترسی مجاز به اطلاعات، تغییر دادن اطلاعات از روی بدخواهی، تغییر اطلاعات به دلیل بروز حوادث، دسترسی غیر مجاز به اطلاعات، استراق سمع از طریق ارتباطات خارجی و داخلی، سرقت تجهیزات و سخت‌افزارهای به کار گرفته شده و موارد دیگر...

همانطور که می‌دانیم خطرپذیری یا ریسک از ترکیب تهدید و آسیب‌پذیری نتیجه می‌شود و با توجه به تعاریفی که برای این دو ارائه شد می‌توان سه سطح زیر را برای خطرپذیری در نظر گرفت:

۱- ریسک کم: که در این سطح آسیب‌پذیری را برای سازمان مطرح می‌کنند که احتمال وقوع آن بسیار کم می‌باشد و با این احتمال بروز پایین در صورت رخداد مشکلات چندانی ایجاد نخواهد کرد.

۲- ریسک متوسط یا سطح خطرپذیری متوسط: در این سطح اطلاعات، سیستم‌ها و برنامه‌های کاربردی سازمان در تمام حوضه‌های محرمانه‌سازی، تمامیت، فراهمی و مجوزسنجی آسیب‌پذیرند احتمال بروز خطرات در این سطح در حد متوسط بوده و هر گونه تلاش در جهت این آسیب‌پذیری به نفع سازمان خواهد بود.

۳- ریسک زیاد: در این حالت اطلاعات و سیستم‌ها و فرمان‌های کاربردی سازمان باز در حوضه‌های محرمانه‌سازی تمامیت، فراهمی و مجوزسنجی در معرض خطر واقعی قرار دارند و لازم است نسبت به رفع این آسیب‌پذیری بلافاصله اقدامات لازم انجام شود در غیر این صورت ضررهای جبران ناپذیری را سازمان متحمل خواهد شد.

شناسایی و مدیریت خطرپذیری در سازمان: به منظور مدیریت خطرپذیری در سازمان با توجه به تعریف خطرپذیری ابتدا باید آسیب‌پذیریهایی که متوجه سازمان است شناسایی شده همچنین تهدیدهای موجود بررسی و شناخته شوند تا بتوان برای جلوگیری این مخاطرات اقدامات متقابل لازم را انجام دهیم.

شناسایی تهدیدات: بررسی و شناسایی تهدیدها اغلب جزئیات زیادی داشته و کاری است بسیار مشکل معمولاً در تلاش برای شناسایی تهدیدات موجود اولین کاندیدهای مطرح رقبا هستند نکته قابل توجه این است که در این

تهدید درست تهدیدکننده خود را از دید دیگران مخفی نگه می‌دارد و خود را تا زمان واقعه نشان نمی‌دهد به هر حال یک راه جایگزین در این حوضه شناسایی تهدیدات هدف‌دار است تهدید هدفمند تهدیدی است که مهاجم با امکان دسترسی معلوم، انگیزهٔ لازم کار معلومی را علیه هدف معلوم انجام می‌دهد و یا تهدیدات را به صورت کلی در نظر بگیریم و به همه و همه چیز مظنون باشیم.

شناسایی آسیب‌پذیری: این شناسایی با تعیین چگونگی و موقعیت دسترسی به اطلاعات سازمان صورت می‌پذیرد. برخی از این موارد عبارتند از: ۱- دسترسی فیزیکی به امکانات و تجهیزات ۲- ارتباطات شبکه‌ای ۳- دسترسی به اطلاعات و مدیریت از راه دور ۴- ارتباط و اتصال به شرکت‌ها و سازمانهای دیگر ۵- نقاط دسترسی کاربران به ساختار ارتباطی و اطلاعاتی ۶- موارد دیگر

اقدامات متقابل: نمی‌توان آسیب‌پذیری را در یک محیط آزمایشگاهی ارزیابی و شناسایی نمود مسیرها و روش‌هایی که امکان حمله از آنها وجود دارد باید در محیط واقعی آزمایش شوند و به هنگام شناخت آسیب‌پذیریها اقدامات و کارهای خنثی کننده در برابر حملات انجام دهیم برخی از این اقدامات عبارتند از: نصب و راه‌اندازی فایروال، نصب و راه‌اندازی نرم‌افزارهای آنتی‌ویروس، بازرسی و کنترل‌های فیزیکی، پیاده کردن سیستم‌های هویت‌سنجی و اعتبارسنجی کارآمد، استفاده از کارتهای هوشمند برای دسترسی به امکانات و تجهیزات، کنترل دسترسی به فایل‌ها و اطلاعات سازمان، آموزش پرسنل سازمان در خصوص مباحث امنیتی

IDS (Intrusion Detection System):

تشخیص هر گونه تلاش در جهت نفوذ به سیستم‌های اطلاعاتی که تحت نظارت و حفاظت بوده و دارای مکانیزم امنیتی است.

IT یک سیستمی است که در آن سعی می‌شود هویت مهاجم مشخص گردد و به هنگام تهاجم موفق، مکانیزم‌هایی دارد که مدیر سیستم را مطلع می‌سازد. همچنین نسبت به فعالیت‌هایی که در سیستم انجام می‌شود حساس بوده و اعمالی که به منظور آماده‌سازی برای حملهٔ اصلی انجام می‌شود را تشخیص می‌دهد. مثال واقعی سیستم‌های IDS مانند: نگهبان ساختمان، دزدگیر ماشین، زنگ خطر بانک‌ها و...

نکته: IDS هر گونه تلاش و سعی در جهت وارد شدن به برنامه‌های کاربردی نرم‌افزاری، بانک‌های اطلاعاتی، شبکه‌های کامپیوتری و موارد این چنینی که به دلایلی تحت حفاظت قرار دارند، شناسایی کرده و تشخیص می‌دهد.

انواع IDS:

H_IDS
N_IDS
P_IDS
AP_IDS
Hybrid_IDS

H_IDS: این نوع IDS موظف است logfileهای موجود در سیستم را بررسی کرده (البته در سیستم عامل‌های مختلف، logfileهای متفاوتی وجود دارد) تا اطلاعاتی را که مشخص کننده نوعی فعالیت غیرعادی می‌باشد یافته و پردازش نماید و با توجه به تنظیماتی که انجام شده است و عدم تطابق بین سیاست‌های مد نظر به مدیر سیستم هشدار دهد. IDSهای جدیدتر در یک حوزه توانایی این را داشته که سیستم‌های تحت حمایت خود را حتی از لحاظ دستکاری نیز کنترل نماید.

مزایا و معایب H_IDS:

مزایا:

۱- تا مادامی که مهاجم در حال انجام فعالیت است پیغام‌هایی تولید می‌کند و ترافیک حمله‌ای که به سیستم شده است را گُم نخواهد کرد.

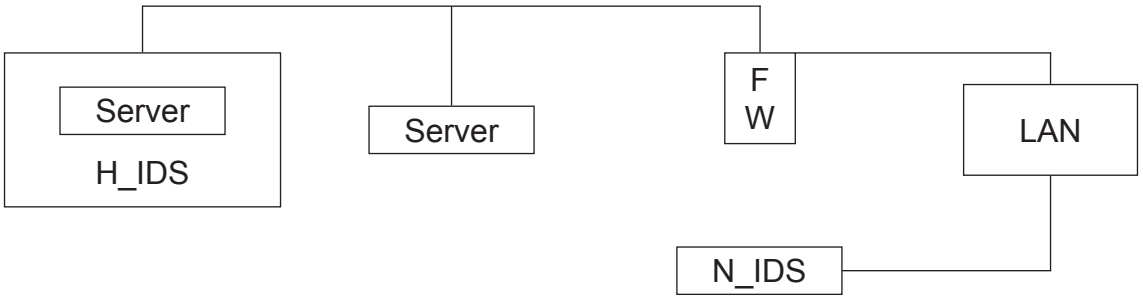
۲- این IDSها با بررس پیام‌های تولید شده و نشانه‌های دیگر موجود در سیستم می‌توانند موفقیت و یا عدم موفقیت حمله را تشخیص دهند.

معایب:

۱- در این IDSها مهاجم توانمند می‌تواند مجموعه کارها و فرآیندهای IDS را شناسایی کرده و آنها را غیرفعال نماید.

۲- این نوع IDSها فقط در مواردی اعلام خطر می‌کنند که محتویات logfileها با قوانین امنیتی مطابقت داشته باشد.

:N_IDS



به صورت فرآیند نرم‌افزاری است که باید بر روی سخت‌افزار به خصوصی نصب و راه‌اندازی شود. این نوع IDSها کارت شبکه را که روی این سیستم‌ها نصب می‌شود به حالت بی‌قید و شرط برده و تمامی ترافیک شبکه را به سمت N_IDS عبور می‌دهد بدون توجه به اینکه این اطلاعات برای این سیستم ارسال شده است یا خیر پس از پردازش اطلاعات مورد نظر و مقایسهٔ آنها با قواعد و قوانین موجود در صورت کشف حمله یک Event (رخداد) ایجاد و ثبت می‌گردد.

نکته: معمول‌ترین روش پیکربندی N_IDS استفاده از دو کارت شبکه است یکی از این کارت‌ها جهت مشاهده و کنترل شبکه به کار می‌رود به شکلی که این کارت آدرس IP ندارد. به همین دلیل اطلاعات ارسال شده ورودی پاسخ نمی‌دهد. کارت دوم به منظور ارتباط با مدیر سیستم و ارسال اخطارهای امنیتی به کار گرفته می‌شود.

مزایا و معایب N_IDS:

مزایا:

۱- این نوع IDS را می‌توان به طور کامل در شبکه مشخص نمود به طوری که مهاجم متوجه نخواهد شد که تحت کنترل است.

۲- با این نوع IDSها می‌توان نظارت و کنترل ترافیک تعداد زیادی از سیستم‌ها را انجام داد.

معایب:

۱- فقط زمانی اعلام خطر می‌کند که اعمالی خلاف قوانین و مقررات امنیتی انجام شده باشد.

۲- به دلیل نوع انجام فعالیت‌ها در این IDS نیاز به پهنای باند بالایی دارد بنابراین ممکن است بخشی از ترافیک از بین برود.

۳- قادر به بررسی ترافیک رمز شده نمی‌باشد و همچنین توانایی اعلام موفقیت حملات را ندارد.

نکته: در استفاده از انواع IDSها نمی‌توان گفت کدامیک بهتر است ولی معمولاً N_IDSها مقرون به صرفه‌ترند. چرا که ترافیک تعداد زیادی از کامپیوترها را می‌توان به کمک آنها کنترل نمود. اما در سازمان‌هایی که نگرانی در مورد کاربران داخلی مجاز بیشتر از مهاجمان خارجی است. H_IDS مناسب‌تر است.