بسم الله الرحمن الرحيم

وزارت ارتباطات و فناوری اطلاعات
معاونت فناوری اطلاعات

راهنمای نرم‌افزارهای سازمانی آزاد/ متن باز (امنیت)

طرح تدوین طرح جامعه فناوری اطلاعات کشور
(کد پروژه: ITMP-40812001-043-4)

مجری طرح:	مهندس عبدالمجید ریاضی، معاون فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات
ناظر طرح:	دکتر علی ناصری، عضو هیئت علمی دانشگاه امام حسین (ع) و مدیر کل امور زیر بنایی فناوری اطلاعات، وزارت ارتباطات و فناوری اطلاعات
مجری پروژه:	مرکز تحقیقات مخابرات ایران
ناظر پروژه:	دکتر حمیدرضا ربیعی، عضو هیئت علمی دانشگاه صنعتی شریف
مؤلفان:	بهروز رحمتی، مهدی امیری کردستانی، محمود تقی زاده

سال ۱۳۸۷

سرشناسه:	ریاضی،عبدالمجید، مجری طرح
عنوان و نام پدیدآور:	راهنمای نرم افزارهای سازمانی آزاد/متن باز(امنیت): طرح تدوین طرح جامع فناوری اطلاعات کشور (ITMP-40812004043-4) ؛ مجری طرح عبدالمجید ریاضی؛ ناظر طرح علی ناصری؛ مؤلفان بهروز رحمتی، مهدی امیری کردستانی، محمود تقی زاده؛ مجری پروژه مرکز تحقیقات مخابرات ایران؛ ناظر پروژه حمید رضا ربیعی؛ [برای وزارت ارتباطات و فناوری اطلاعات].
مشخصات نشر:	تهران: جهان جام جم، ۱۳۸۷.
مشخصات ظاهری:	۲۲۸ ص. مصور، جدول، نمودار.
شابک:	978-964-8625-882
وضعیت فهرست نویسی:	فیپا
یادداشت:	کتابنامه : ص [۲۲۳-۲۲۴]
موضوع:	نرم افزار متن باز.
موضوع:	حفاظت اطلاعات
موضوع:	کامپیوترها، ایمنی اطلاعات
موضوع:	فایروال (ایمن سازی کامپیوتر)
شناسه افزوده:	رحمتی، بهروز،۱۳۵۵
شناسه افزوده:	امیری کردستانی، مهدی، ۱۳۵۹
شناسه افزوده:	تقی زاده، محمود، ۱۳۵۳
شناسه افزوده:	ناصری، علی، ۱۳۴۸
شناسه افزوده:	ربیعی، حمیدرضا، ۱۳۴۰
شناسه افزوده:	مرکز تحقیقات مخابرات ایران.
شناسه افزوده:	ایران. وزارت ارتباطات و فناوری اطلاعات. معاونت فناوری اطلاعات.
رده بندی کنگره:	QA۷۶/۷۶/آ۴ ر۹۳ ۱۳۸۷
رده بندی دیویی:	۰۰۵/۳
شماره کتابشناسی ملی:	۱۲۱۱۳۷۸

راهنمای نرم افزارهای سازمانی آزاد/متن باز (امنیت)

مؤلفان: بهروز رحمتی، مهدی امیری کردستانی، محمود تقی زاده
حروفچینی و صفحه بندی:زهرا محبی متین
ویراستار محتوایی: محمدمهدی نظام آبادی
مسوول فنی: عاطفه قوامی فر
گرافیست: ناصر اسماعیلی
لیتوگرافی: بهنورپرداز
چاپ: نگرش
نوبت چاپ: اول
شمارگان:۲۰۰۰
سال انتشار:۱۳۸۷
ناشر: موسسه انتشارات جهان جام جم
نشانی: تهران- جنت آباد-خ گلزارغربی-کوچه شهید محسنی بعد- پلاک ۱۳- تلفکس: ۴۴۸۲۹۲۳۱

پیشگفتار

زندگی بشر از عصر تولید انبوه به عصر ارتباطات و اطلاعات ارتقاء یافته و حرکت تکاملی کشورهای جهان به سوی جوامع اطلاعاتی و دانش بنیان، کلیه فرایندها و فعالیت‌های اقتصادی، فرهنگی، صنعتی، سیاسی و روابط اجتماعی را تحت تاثیر قرار داده است.

چارچوب ساختاری تشکیل دهنده این عصر را تولید، پردازش، انتقال و مدیریت اطلاعات و ارتباطات به منظور ایجاد پایگاه‌های دانش و معرفت فردی، گروهی، سازمانی و کشور تشکیل می‌دهد و لذا فناوری اطلاعات را که شامل فناوری‌های بکارگرفته شده در فرایند مذکور می‌باشد برای جوامع بشری به عنوان عامل حیاتی و تعیین کننده مطرح ساخته است.

در دنیای امروز اطلاعات نه تنها به عنوان یکی از منابع و دارایی‌های اصلی سازمان‌ها شناخته می‌شود بلکه درحکم وسیله و ابزاری برای مدیریت اثر بخش بر سایر منابع و دارایی‌های سازمان (منابع مالی، نیروی انسانی وغیره) نیز محسوب می‌شود و لذا از اهمیت و ارزش ویژه‌ای برخوردار گشته است. اما این ارزش تنها در صورتی محقق و دست یافتنی خواهد بود که اطلاعات بتوانند در زمان مناسب، با کیفیت مطلوب و امنیت قابل قبول در اختیار افراد مناسب قرارگیرد و ارتباطات به صورت مطلوب و بهینه در سازمان برقرار گردد. از این رو است که فناوری اطلاعات که زمینه‌ساز انتقال، جابجایی، بکارگیری و مدیریت موثر اطلاعات در کشورها می‌باشد، از اهمیتی حیاتی برخوردار گشته است.لذا در راستای چشم‌انداز بیست ساله جمهوری اسلامی ایران مبنی بر تحقق جامعه‌ای توسعه یافته، متناسب با مقتضیات فرهنگی، متکی بر اصول اخلاقی و ارزش‌های اسلامی، حفظ هویت ایرانی اسلامی با تاکید بر مردم سالاری دینی و عدالت اجتماعی، آزادی‌های مشروع، حفظ کرامت و حقوق انسان‌ها و برخوردار از دانش پیشرفته از یک طرف، و تاثیر عمیق فناوری اطلاعات و ارتباطات بر ابعاد مختلف زندگی بشر و بالاخص نقش حیاتی و حساس آن درجنبه‌های فرهنگی، اقتصادی، امنیتی، اجتماعی و سیاسی از طرف دیگر وزارت ارتباطات و فناوری اطلاعات را برآن داشت که جهت برنامه‌ریزی کلان توسعه فناوری اطلاعات اقدام به پیشنهاد طرح تدوین طرح جامع فناوری اطلاعات کشور به سازمان مدیریت و برنامه‌ریزی نماید که بعد از بررسی کارشناسی طی موافقتنامه‌ای به امضاء طرفین (وزارت ارتباطات و فناوری اطلاعات و سازمان مدیریت و برنامه‌ریزی) رسید این موافقتنامه شامل ۵ پروژه اصلی؛ تدوین طرح کلان فناوری اطلاعات،

تدوین برنامه اجرایی وظایف وزارت در حوزه امنیت (افتا)، ایجاد بانک اطلاعاتی وضعیت فناوری اطلاعات، تدوین چارچوب کاربردهای فناوری اطلاعات در کشور، تهیه و پیش‌نویس لوایح و مقررات حقوقی است که هر کدام حاوی زیر بخش‌های مختلف می‌باشند.

امید است انجام فعالیت‌های مندرج در این طرح بتواند زمینه توسعه و ارتقاء صنعت و خدمات فناوری اطلاعات در کشور را مهیا سازد. این کتاب نتیجه حاصل یکی از فعالیت‌های طرح می‌باشد که با همت کارشناسان فناوری اطلاعات به سرانجام رسیده است.

عبدالمجید ریاضی

مجری طرح تدوین طرح جامع فناوری اطلاعات

مقدمه

نفوذ فناوری اطلاعات در حوزه‌های مختلف تحول عظیمی در نحوه زندگی بشر ایجاد نموده است. بسترها و ابزارهای لازم برای ورود فناوری اطلاعات به عرصه‌های گوناگون نقش تعیین کننده‌ای در میزان اثر بخشی این فناوری در آن عرصه ایفا می‌کنند. زیر ساخت‌های ارتباطی، سیستم‌های سخت افزاری، نرم‌افزارهای مختلف و تجهیزات امنیتی همه و همه از جمله الزامات استفاده از فناوری اطلاعات به شمار می‌روند. همه گیر شدن استفاده از این فناوری از یک طرف و ارئه ابزارهای عملیاتی گوناگون توسط محققین و برنامه نویسان از طرف دیگر لزوم ارائه ابزارهای یکپارچه و در اصطلاح در سطح سازمان را آشکار ساخته است. این مسئله سبب گردیده است تا مجموعه‌های استفاده کننده از فناوری اطلاعات برای رسیدن به راندمان بالاتر و ارائه خدمات با کیفیت تر عمدتاً در پی راهکارهای یکپارچه و در سطح سازمان باشند.

امنیت با توجه به دارا بودن نقش کلیدی در تداوم حیات هر سیستم رایانه‌ای از اهمیت ویژه‌ای برخوردار است و نرم‌افزارهای امنیتی متن‌باز با توجه به ویژگی‌ها و قابلیت های منحصر به فرد مورد توجه بسیاری از محققین قرارگرفته است. هدف اصلی کتاب حاضر ارتقاء سطح دانش موجود در کشور در زمینه نرم‌افزارهای امنیتی آزاد/ متن‌باز بوده است که با توجه به روند جهانی در این حوزه لازم است مورد توجه بیشتری قرارگیرد.

برای ورود به بحث نرم‌افزارهای امنیتی متن باز در فصل اول انواع تهدیدات اینترنتی و استراتژی‌های موجود برای مقابله با آنها آورده شده است. در فصل دوم دو مقوله فایروال و فیلترینگ به عنوان دو ابزار کلیدی در ایمن سازی تبادل اطلاعات به تفصیل مورد مطالعه قرار گرفته‌اند. در بخش نخست این فصل، انواع فایروال به همراه معماری‌های مختلف آن مورد بررسی قرار گرفته و در ادامه چند نمونه از فایروال‌های متن باز معرفی و نحوه عملکرد آنها توضیح داده شده است. در بخش دوم ویژگی‌های انواع مختلف سیستم‌های فیلترینگ محتوا، معماری آنها و نهایتاً نمونه‌های متن باز آن مطالعه شده‌اند. سیستم‌های تشخیص نفوذ به عنوان یکی از ابزارهای محوری در تأمین امنیت سیستم‌های رایانه‌ای موضوع اصلی فصل سوم هستند. در این فصل پس از معرفی انواع سیستم‌های تشخیص نفوذ، چندین نمونه از انواع متن باز آن مورد بررسی قرار گرفته‌اند. فصل آخر کتاب به موضوع نرم‌افزارهای آنتی ویروس پرداخته است و برنامه ClamAV را به عنوان یکی از آنتی ویروس‌های متن باز معتبر مورد بررسی دقیق قرارداده است.

امید است کتاب حاضر با توجه به اهمیت بحث نرم‌افزارهای آزاد / متن‌باز بتواند نقشی هرچند اندک در ارتقاء سطح دانش این حوزه در کشور داشته باشد.

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فهرست مطالب

عنوان **صفحه**

فصل اول– تهدیدهای اینترنتی

۱–۱– انواع تهدیدهای اینترنتی

تهدیدهای امنیتی مربوط به شبکه را از جهات مختلف می‌توان دسته‌بندی کرد. یک نوع دسته‌بندی این حملات براساس لایه عملکرد حمله یا تهدید است. بر این اساس مطابق با لایه‌های پروتکل TCP/IP انواع حملات وجود خواهد داشت. حمله در هر لایه نیز خود دسته‌بندی‌های مختلفی می‌تواند داشته باشد که در ادامه بعضی از آنها آورده شده‌اند. اکثر این تهدیدها به خاطر ضعف تکنولوژی و طراحی پروتکل به وجود آمده است. بعضی از مخاطرات امنیتی نیز ناشی از پیاده‌سازی‌های غلط و عدم رعایت نکات امنیتی در پیاده‌سازی به وجود می‌آیند.

تهدیدهای امنیتی رایج در لایه ۲ شبکه:

- دسترسی غیرمجاز
- حملات از کار انداختن سرویس
- استراق‌سمع (که امکان فراهم شدن انجام حملات دیگر نظیر نفوذ به سیستم را می‌دهد)
- تغییر محتویات بسته‌ها
- تحلیل ترافیک شبکه

تهدیدهای امنیتی رایج در لایه ۳ شبکه:

- حملات از کار انداختن سرویس
- حملات مربوط به پروتکل‌های روتینگ
- تحلیل ترافیک شبکه / استخراج ساختار شبکه / دسترسی غیرمجاز
- جعل آدرس بسته

تهدیدهای امنیتی رایج در لایه‌های بالاتر:

- حملات از کار انداختی سرویس
- حملات DNS
- حملات برنامه‌های تحت وب

تهدیدهای امنیتی رایج در سطح سیستم عامل:

- حملات مربوط به برنامه‌های کاربردی نظیر دیتابیس یا برنامه‌های کاربردی تحت وب
- از کار انداختن سرویس
- آلوده شدن سیستم عامل به ویروس
- نفوذ به سیستم عامل از طریق باگ‌های امنیتی سیستم عامل و یا برنامه‌های کاربردی
- نفوذ به سیستم از طریق حدس کلمه رمز

۱-۲- توضیح و تعریف بعضی از انواع حملات

۱-۲-۱- حمله از کار انداختن سرویس

به دسته‌ای از حملات و تهدیدها گفته می‌شود که منجربه از کار افتادن سرویسی در شبکه شود.

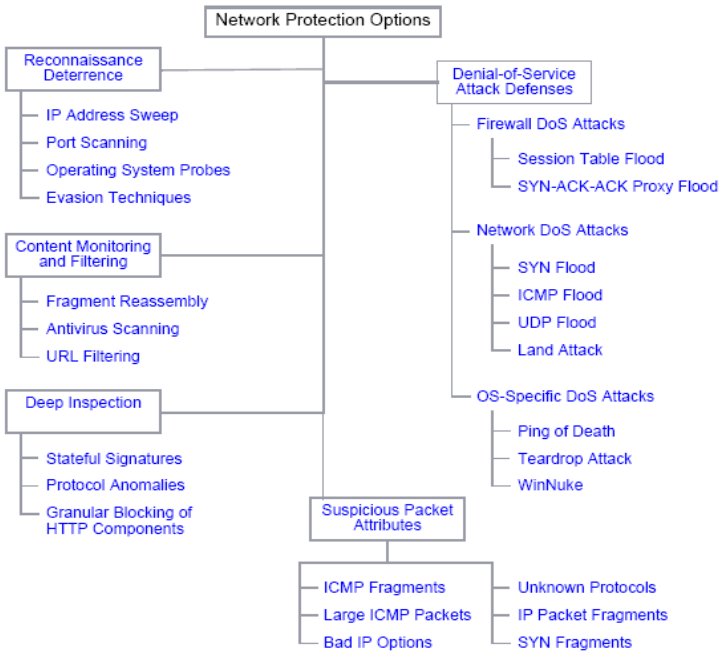
۱-۲-۲- حمله دسترسی غیر مجاز

هر حمله‌ای که منجر به دسترسی مهاجم به اطلاعات یا بخشی از اطلاعات به صورت غیرمجاز شود. برای مثال با انجام عملیات شنود ترافیک شبکه (در صورتی که رمز نشده باشد) مهاجم می‌تواند به اطلاعات دسترسی داشته باشد که این یک تهدید از نوع دسترسی غیرمجاز خواهد بود.

۱-۲-۳- تغییر داده ها

در مواردی مهاجم ممکن است بدون آنکه بتواند محتویات داده‌ها را پردازش کند، داده‌های جعلی و غلط وارد شبکه کند و یا داده‌های اصلی را تغییر دهد. برای مثال یک ویروس معمولاً فایل‌های اصلی را به صورت غیرمجاز تغییر می‌دهد.

هدف از این قسمت آن است که ضمن آنالیز بعضی از حملات شناخته شده؛ روش جلوگیری از این حملات در فایروال توضیح داده شود. ذکر دو نکته در اینجا ضروری است. اول آنکه لزوما روش مقابله با یک حمله منحصر به فرد نیست و در ثانی تمامی انواع حملات را نمی‌توان صرفاً با استفاده از یک فایروال پوشش داد.



شکل ۱-۱: محافظت از شبکه در برابر انواع حملات

به‌طور کلی هر حمله در دو مرحله جداگانه انجام می‌گیرد. در مرحلهٔ اول، حمله کننده به جمع‌آوری اطلاعات می‌پردازد و در مرحلهٔ دوم او آغاز به حمله می‌کند.

۱-۲-۴- اقدامات شناسایی

- شبکه را map کرده و همچنین مشخص شود که چه دستگاه‌هایی فعال هستند (IP address sweep).
- تشخیص اینکه چه پورتی برروی دستگاه‌ها فعال است (پوییدن پورت‌ها).
- شناسایی سیستم عامل، که از این طریق ضعف‌های سیستم عامل آشکار می‌شود.
- شروع کردن حمله
- پنهان کردن اصل و منشا حمله
- اقدام به حمله
- از بین بردن یا پنهان کردن مدارک

۱-۲-۵- جلوگیری از شناسایی

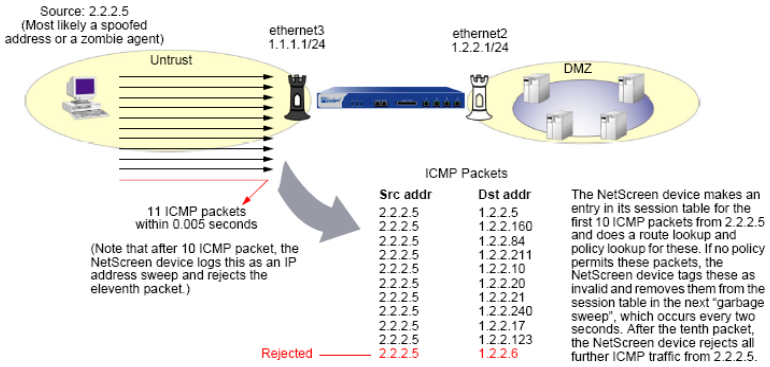
هنگامی که حمله کننده‌ها در ابتدا لایه‌های شبکه هدف خود را شناسایی کنند، بهتر می‌توانند برنامه حملهٔ خود را برنامه‌ریزی کنند (چه آدرس‌های IP بالا و فعال می‌باشند). نقاط ورودی ممکن(چه شماره پورتی فعال است) و وضعیت قربانیان (چه سیستم عاملی برروی دستگاه‌های فعال، در حال اجرا است). برای بدست آوردن این اطلاعات حمله کننده باید عملیات شناسایی را انجای دهد. برای جلوگیری از تلاشهای حمله کننده‌ها در جهت شناسایی شبکه‌های محافظت شده و کسب اطلاعات با ارزش در مورد منابع شبکه چندین راه حل وجود دارد.

- جاروب کردن آدرس‌های IP
- پوییدن پورت‌ها
- شناسایی شبکه با استفاده از انتخاب‌های IP
- کاوش و بررسی سیستم‌های عامل
- نشاندن فلگ‌های FIN و SYN
- فلگ FIN بدون فلگ ACK
- سرآیندهای TCP بدون نشاندن فلگ
- تکنیک‌های حلیه و گریززنی
- پوییدن FIN
- فلگ‌های NON-SYN
- کلاهبرداری IP (IP Spoofing)
- انتخاب‌های مسیریابی منبع IP

۱-۲-۵-۱- جاروب کردن آدرس‌های IP

جاروب کردن یک آدرس هنگامی رخ می‌دهد که یک آدرس IP، تعداد ۱۰ بسته ICMP به سمت دستگاه‌های متفاوت در عرض یک زمان مشخص (۵۰۰۰ میکروثانیه به صورت پیش‌فرض) می‌فرستد. هدف از این طرح فرستادن بسته‌های ICMP به‌طور نوعی echo request به سمت دستگاه‌های متفاوت به امید اینکه حداقل یک دستگاه پاسخ می‌دهد. بدین ترتیب یک آدرس برای هدف بودن شناسایی می‌شود. برخی از تجهیزات امنیتی مانند Netscreen عبور

ترافیک ICMP به سمت ۱۰ آدرس در مدت زمان کمتر از 0.005 ثانیه را به‌عنوان الگوی حمله شناسایی می‌کنند و ترافیک به سمت آدرس یازدهم را قطع می‌کند.



شکل ۱-۲: اسکن افقی آدرس‌ها

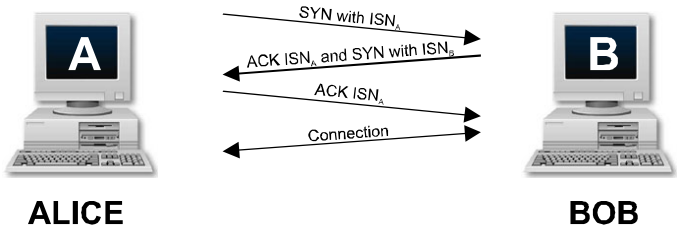
۱-۲-۵-۲- پویدن پورت‌ها

پویش پورت زمانی رخ می‌دهد که یک آدرس IP بسته‌های IP شامل قطعات ICP SYN به سمت ۱۰ پورت متفاوت از یک IP مقصد در عرض فاصله‌های زمانی از پیش تعریف شده می‌فرستد. هدف از این طرح پویش سرویس‌های قابل دسترس برروی یک دستگاه می‌باشد در صورت شناسایی یک پورت باز، سرویس که باید به عنوان هدف در نظر گرفته شود، برای حمله کننده شناسایی می‌شود.

برقراری ارتباط بین دو پروسه روی دو ماشین، اتصال‌گرا[1] است و قبل از مبادله هرگونه داده باید یک ارتباط (اتصال) TCP به روش دست تکانی سه مرحله‌ای[2] برقرار شود. به شکل (۱-۳) دقت کنید. ماشین Alice اقدام به برقراری ارتباط TCP با ماشین Bob می‌نماید. بدین منظور بسته‌ای با تنظیم SYN=1 و ISNA=X ارسال می‌شود؛ x عددی تصادفی است و براساس آن ترتیب صحیح بسته‌ها حفظ می‌شود. اگر در سمت مقابل پروسه‌ای به شماره پورت مورد نظر گوش بدهد در پاسخ به این تقاضا بسته‌ای با مشخصات ACK=1 و SYN=1 و ISNB ارسال می‌کند. ISNB نیز عددی تصادفی است و ترتیب صحیح بسته‌های سمت مقابل را تضمین

[1] Connection Oriented
[2] Way Handshake

می‌کند. پس از ارسال نهائی یک بسته با مشخصات ACK=1 وSYN=1 و Ack. N. = ISNB پروسه‌های طرفین، قادر به مبادله داده خواهند بود.



شکل ۱-۳: مکانیزم دست تکانی سه مرحله‌ای (3-Way Handshake)

بسته‌هایی که از Alice به Bob ارسال می‌شوند با شماره ترتیب ISNA شروع می‌شوند و بالعکس بسته‌های Bob به Alice با شماره ترتیب ISNB آغاز می‌شوند. در خلال مبادله داده‌ها، هرگاه بسته‌ای در مسیر گم یا خراب شود، گیرنده با اعلام شماره آن در فیلد Ack . No تقاضای ارسال مجدد آنرا می‌نماید. با این مقدمه تکنیک‌های پویش و کشف پورت‌های باز را تشریح می‌کنیم.

مکانیزم پویش مودبانه (PoliteScan)

در این مکانیزم، نرم‌افزار "پویشگر پورت" سعی می‌کند یک ارتباط کامل و سه مرحله‌ای TCP با یک شماره پورت خاص برقرار نماید. اگر این اتصال برقرار شود، بنابراین پورت مربوطه کاملاً باز است. بدلیل آنکه نرم‌افزار پویشگر در یک روال طبیعی و معمول سعی در برقراری یک ارتباط TCP می‌کند، احتمال آنکه ماشین هدف دچار مشکل و اختلال شود وجود ندارد. مراحل عملیاتی که در "پویش مودبانه" انجام می‌شود به ترتیب زیر است :

- یک بسته SYN به سمت ماشین هدف ارسال می‌شود.
- پویشگر مدت زمان مشخصی انتظار می‌کشد تا پاسخ SYN-ACK برگردد. اگر چنین پاسخی برگردد، بنابراین پورت مربوطه باز است؛ در غیر اینصورت ممکن است پورت باز نباشد.
- اگر پورت باز بود و جواب SYN-ACK برگشت مرحله سوم از دست تکانی سه مرحله‌ای با بسته ACK تکمیل می‌شود.

- حال ارتباط TCP برقرار است و باید مودبانه خـتم شـود زیـرا هـدف، مبادلـه داده نبوده و فقط یک بررسی و آزمایش بوده است. پویشگر بلافاصـله ایـن ارتبـاط را بـا ارسال بسته FIN=1 ختم می‌نماید.
- عدم بازگشت پاسخ در مرحله دوم، این یقین را حاصل نمی‌کند که آن پورت بسـته است
- . زمانی می‌توان مطمئن شد که پورت مورد نظر بسته است که در پاسـخ بـه بسـته SYN-ACK یکی از دو پیغام زیر برگردد.
- بسته RESET (RST=1) به جای بسته ACK باز گردد.
- بسته ICMP Port unreachable به جای بسته ACK باز گردد.

این نوع پویش و جستجو اگرچه برای استفاده صلح جویانه و اهداف مدیریت شبکه بسیار مناسب است ولی به دو دلیل نفوذگر از این روش استقبال نمی‌کند:

۱- بسیاری از سرویس دهنده‌ها به محض تکمیل شدن مراحل دست تکانی سه مرحله‌ای و برقراری یک ارتباط TCP ، مشخصات آن را در فایلی درج (log) می‌کنند ؛ لذا بسادگی آدرس نفوذگر کشف خواهد شد. دقت کنید که در برقراری ارتباط TCP ، نفوذگر نمی‌تواند از آدرس‌های دروغین (IP Spoofing) استفاده کند زیرا در این صورت قطعاً هیچ پاسخی مبنی بر باز یا بسته بودن پورت دریافت نخواهد کرد؛ (چون بسته پاسخ برای آدرس جعلی ارسال خواهد شد.) بدین ترتیب نفوذگر مجبور است از آدرس IP حقیقی استفاده کند که درج شدن این آدرس در فایل ثبت عملکرد (log file)، هویت او را آشکار خواهد کرد.

۲- تکمیل سه مرحله دست تکانی و خاتمه دادن به ارتباط TCP برای نفوذگر بسیار وقت‌گیر است، زیرا باید به ازای هر پورت مورد آزمایش، این عملیات از نو تکرار شود و چون تعداد پورت‌ها نسبتاً زیاد است وقت بسیار زیادی از نفوذگر خواهد گرفت. (دقت کنید زمانی که نرم‌افزار پویشگر پس از ارسال بسته SYN باید منتظر بماند تا پاسخ SYN ACK برگردد نسبتاً زیاد است؛ در حد چند ثانیه). به دلایل فوق نفوذگر از روش‌های مخفیانه تر و سریع‌تری بهره می‌گیرد.

پویش مخفیانه(TCP SYN Scan)

در این مکانیزم، مراحل زیر دنبال می‌شود :

- یک بسته SYN به سمت ماشین هدف ارسال می‌شود.
- پویشگر، مدت زمان مشخصی انتظار می‌کشد تا بسته SYN-ACK باز گردد. بازگشت چنین بسته‌ای نشان می‌دهد که پورت باز است.
- در صورت برگشت بسته SYN-ACK ، پویشگر بلافاصله بسته RESET را ارسال می کند قبل از آنکه هیچ ارتباطی برقرار شود.

در حقیقت بدین روش فقط دو مرحله از دست تکانی سه مرحله‌ای انجام می شود. بدین ترتیب نفوذگر در یک حاشیه امنیت قرار می‌گیرد زیرا مشخصات یک ارتباط نیمه کاره در فایل ثبت عملکرد (log file) درج نخواهد شد و در ضمن نیمه کاره بودن ارتباط، سرعت عمل پویش را بسیار زیاد می‌کند.

اگر پورت مورد نظر بسته باشد ممکن است در پاسخ به بسته SYN، بسته RESET و یا پیغام ICMP Port unreachable باز گردد. در صورت دریافت چنین بسته‌هایی می توان اطمینان یافت که پورت بسته است .

البته باید این نکته را اشاره کرد که مسیریاب‌هایی که به فایروال مجهز هستند قادرند ورود بسته‌های SYN را ردیابی و ثبت نمایند.

دلیل آنکه پویشگر پس از دریافت بسته SYN ACK سریعاً بسته RESET می فرستد آن است که هدف موردنظر به انتظار تکمیل مراحل بعدی ارتباط TCP نماند. البته در یک نوع حمله به سیستم از ارسال سیل آسای بسته SYN جهت مختل کردن و درهم شکستن هدف استفاده می شود ولی فعلاً هدف پویشگر، بررسی پورت‌های باز است نه مختل کردن هدف.

پویش به روش نقض اصول پروتکل

در دو روش قبلی، عمل پویش پورت با ارسال بسته SYN و انتظار برای دریافت بسته SYN ACK انجام می‌شود. در مکانیزم پویش به روش "نقض اصول پروتکل" در اولین مرحله ، بسته‌ای ارسال می‌شود که متعارف و معمول نیست! بسته‌ای که در شرایط طبیعی هیچگاه ارسال نخواهد شد. در زیر برخی از این بسته‌های نا متعارف که اصول پروتکل TCP را نقض می‌کنند معرفی شده‌اند:

TCP FIN Scan : به طور متعارف بسته TCP FIN برای خاتمه دادن به یک ارتباط TCP ارسال می‌شود و هیچگاه چنین بسته‌ای بدون مقدمه و پیش از برقراری یک ارتباط TCP ارسال نخواهد شد. در روش پویش TCP FIN Scan ، بدون مقدمه یک بسته FIN از طرف پویشگر به سمت یک شماره پورت از ماشین هدف ارسال می‌شود. اگر پورت مورد نظر بسته باشد بر طبق اصول پروتکل TCP باید یک بسته RESET برگردد ولی اگر پورت باز باشد هیچ پاسخی دریافت نخواهد شد. پس برنامه پویشگر با دریافت بسته RESET از بسته بودن آن پورت اطمینان حاصل می‌کند ولی در صورتی که چیزی دریافت نکند احتمال باز بودن آن پورت بالاست. بنابراین بر خلاف دو روش قبل برگشتن پاسخ در این روش به معنای بسته بودن پورت مربوطه است ولیکن عدم بازگشت بسته، به معنای باز بودن احتمالی آن پورت می‌باشد.

Null Scan : در این مکانیزم، برنامه پویشگر بدون آنکه ارتباط TCP با مقصد برقرار کرده باشد، یک بستهTCP با شماره پورت مشخص برای یک پورت خاص ارسال می‌کند. ویژگی این بسته آن است که هیچیک از بیت‌های SYN ، FIN و ACK آن 1 نیست. این بسته طبق تعریف پروتکل TCP هیچ معنای خاصی ندارد و اگر پورت مربوطه باز باشد، بسته حذف می‌شود و هیچ پاسخی برنخواهد گشت، در حالی که اگر پورت مربوطه بسته باشد در پاسخ بسته RESET برمی‌گردد. بنابراین عدم بازگشت بسته به معنای باز بودن پورت و برگشت بسته RESET نشان‌دهنده بسته بودن پورت می‌باشد.

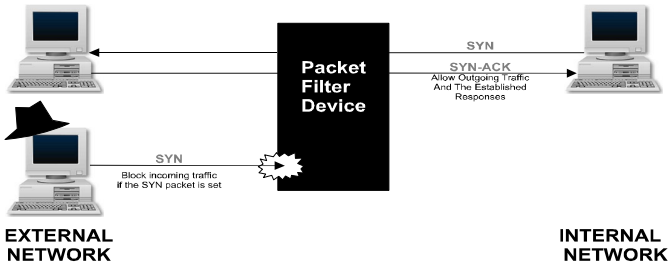
Xmas Tree : در این مکانیزم، پویشگر بسته‌ای را به یک پورت در ماشین هدف ارسال می‌کند که در آن تمام بیت‌های FIN ، URG و PUSH با مقدار 1 تنظیم شده است. این بسته نیز هیچ معنای خاصی ندارد و در مقصد قطعاً حذف خواهد شد. بنابراین اگر پورت مربوطه باز باشد هیچ پاسخی باز نمی‌گردد ولی اگر این بسته به سمت یک پورت بسته ارسال شود، در پاسخ بسته RESET ارسال می‌شود.

این سه مکانیزم به جز در ماشین‌های با سیستم عامل ویندوز، در سایر سیستم‌های عامل به خوبی کار می‌کند و جواب صحیحی خواهد داد؛ ولیکن در سری سیستم عامل‌های ویندوز (9x,NT,2000) استفاده از این سه روش کارآیی ندارد زیرا برخلاف اصول پروتکل TCP، در Windows هرگاه بسته‌ای غیرمتعارف دریافت شود چه پورت باز باشد و چه بسته در جواب RESET باز خواهد گشت.

پویش به روش TCP ACK Scan

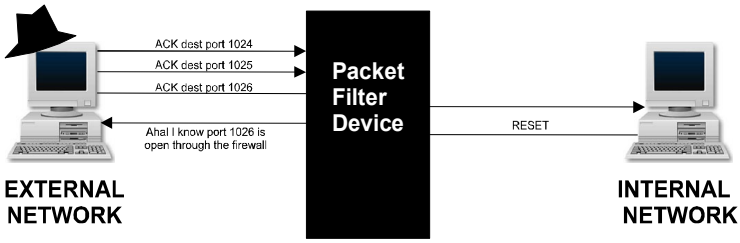
همانند سه مکانیزم قبلی، در مکانیزم TCP ACK Scan برای پویش یک پورت از ارسال غیرمتعارف بسته ACK به سمت یک هدف استفاده می‌شود. یعنی بدون مقدمه یک بسته SYN ACK، به سوی یک پورت در ماشین هدف ارسال می‌شود. (به‌طور معمول و متعارف این بسته در پاسخ به بسته SYN فرستاده می‌شود.) حال وقتی این بسته به یک پورت باز ارسال می‌شود، چون ماشین منتظر دریافت چنین بسته‌ای نبوده است، آن را حذف می‌کند لذا عدم بازگشت پاسخ نشانگر آنست که احتمالاً آن پورت باز است ولیکن اگر پورت مربوطه بسته باشد در پاسخ بسته RESET برمی‌گردد. پویش به روش TCP ACK Scan یک امتیاز بسیار مهم نسبت به بقیه روش‌ها دارد و آن هم امکان عبور چنین بسته‌ای از فایروال یا مسیریاب‌های فیلتر کننده می‌باشد.

به‌طور معمول از یک شبکه داخلی که هیچ گونه سرویسی را به خارج از شبکه نمی‌دهد بوسیله فایروال حراست می‌شود؛ فایروال اجازه ورود هیچ‌گونه بسته SYN را به درون شبکه نمی‌دهد. یعنی چون قرار نیست هیچ سرویسی به بیرون از شبکه داده شود لذا ورود بسته‌های SYN که اولین مرحله از برقراری یک ارتباط TCP و سرویس‌گیری محسوب می‌شود، موردی ندارد و باید حذف شود. بدین نحو در مکانیزم‌های پویش Polite Scan و TCP SYN Scan بسته‌های SYN قادر نخواهند بود از فایروال عبور کنند و بالطبع این مکانیزم‌ها برای آگاهی از باز یا بسته بودن پورت‌ها عملاً ناتوان خواهند بود. هرچند دیوارهای آتش، بسته‌های SYN وارد شده از خارج را حذف می‌کنند ولی بسته‌های SYN ACK از فایروال عبور داده خواهد شد زیرا بسته‌های SYN ACK در پاسخ به بسته‌های SYN که از درون به بیرون ارسال شده، به شبکه وارد می‌شوند تا مرحله دوم از دست تکانی سه مرحله‌ای کامل شود. شکل (۱-۴) این مفهوم را نشان می‌دهد در این شکل فایروال مانع ورود بسته SYN به درون شبکه می‌شود در حالی که ورود بسته SYN ACK مجاز است.



شکل ۱-۴: ممانعت از ورود بستهٔ SYN به درون شبکه/ صدور مجوز ورود SYN-ACK

دقت کنید که وقتی یک ماشین داخلی می‌خواهد به یک سایت وب دسترسی داشته باشد قاعدتاً یک شماره پورت بزرگتر از ۱۰۲۴ انتخاب کرده و اقدام به ارسال یک بسته SYN به سمت پورت ۸۰ از سرویس دهنده می‌کند و منتظر بسته SYN ACK می‌شود. بنابراین ورود بسته SYN ACK از پورت ۸۰ به سمت پورتی با شماره بالاتر از ۱۰۲۴ کاملاً طبیعی و مجاز است. با استفاده از همین مفهوم نفوذگر قادر است پورت‌های باز یک ماشین را پویش نماید. در شکل (۱-۵) چگونگی پویش پورت‌های باز از میان فایروال به تصویر کشیده شده است.



شکل ۱-۵: پویش پورت‌های باز از میان فایروال با مکانیزم SYN-ACK

اگر در پاسخ به بسته SYN ACK پاسخ RESET برگردد نشان می‌دهد که آن پورت باز است. زیرا پروسه‌ای که به آن شماره پورت گوش می‌داده، انتظار دریافت بسته SYN ACK نداشته است؛ لذا تعجب خود را از دریافت چنین بسته‌ای با ارسال بسته RESET اعلام می‌کند.

اگر در پاسخ به بسته‌های SYN ACK پاسخی برنگردد نمی‌توان از باز بودن و بسته بودن پورت اطمینان حاصل کرد به همین دلیل ابزارهای پویش پورت (همانند Nmap) اگر در یک مدت زمان معین، پاسخی دریافت نکنند آن پورت را فیلتر شده[1] در نظر می‌گیرند یعنی فرض

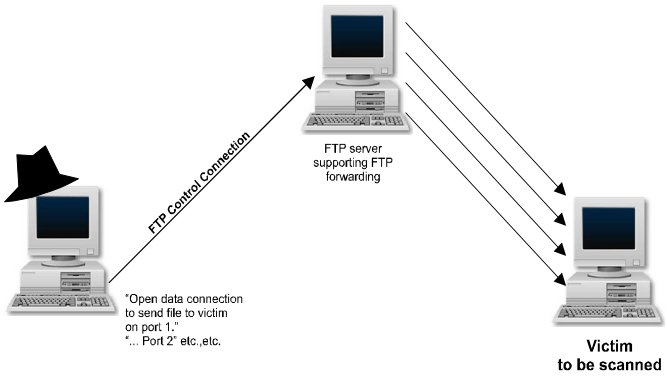
[1] Filtered

می‌شود که آن بسته توسط مسیریاب یا فایروال شده است مگر آنکه بوسیله تکنیک‌های دیگر خلاف آن ثابت شود.

پویش به روش FTP Bounce Scan

یک نفوذگر تمایل دارد که در حین پویش یک شبکه و جستجوی پورت‌های باز، هویتش ناشناس بماند و آدرسIP او کشف نشود. یکی از مکانیزم‌هائی که نفوذگر برای پویش مخفیانه به کار می‌گیرد قابلیتی است که سرویس دهنده‌های قدیمی FTP در اختیار کاربران می‌گذاشتند. بدین ترتیب که کاربران می‌توانستند ضمن برقراری ارتباط TCP با سرویس‌دهنده و ایجاد یک نشست، تقاضا بدهند تا یک فایل از آن سرویس‌دهنده به یک ماشین ثالث منتقل شود. یعنی در حقیقت یک کاربر دارای خط انتقال کم ظرفیت می‌توانست از سرویس‌دهنده‌های سریع (دارای خطوط با پهنای بالا) بخواهد تا یک فایل را به ماشینی دیگر در شبکه منتقل نماید تا این انتقال با سرعت بیشتری انجام شود. این امکان اگر چه راحتی کاربران را فراهم می‌کند ولیکن به نفوذگر امکان می‌دهد تا پویش پورت‌های باز یک ماشین را از طریق سرویس‌دهنده FTP انجام بدهد.

با استفاده از این قابلیت، نفوذگر یک ارتباط TCP با سرویس‌دهنده FTP برقرار می‌کند و از آن می‌خواهد تا با یک شماره پورت مشخص در ماشین هدف ارتباط برقرار نماید. (به‌منظور انتقال فایل) اگر پورت موردنظر برروی ماشین هدف باز نباشد، سرویس دهنده FTP به نفوذگر گزارش می‌دهد که پورت مربوطه بسته است و قادر به برقراری ارتباط نیست؛ اما اگر پورت مربوطه باز باشد، سرویس‌دهنده به نفوذگر گزارش می‌دهد که پورت مورد نظر او باز است ولی قادر به مبادله داده طبق پروتکل FTP نیست. این همان چیزی است که نفوذگر می‌خواهد بداند. حال نفوذگر پورت‌های بعدی را امتحان می‌کند. وقتی که ماشین هدف، مشخصات ماشین پویشگر را ذخیره و درج می‌نماید در حقیقت مشخصات سرویس‌دهنده FTP را درج کرده، در حالی که یک واسطه و کاملاً بی‌گناه است. بنابراین هویت نفوذگر مخفی خواهد ماند. تنها از طریق بررسی فایل مراجعات به سرویس دهنده FTP می‌توان نفوذگر را شناسائی کرد. شکل (۱-۶) مکانیزم این نوع پویش را نشان می‌دهد.



شکل۱-۶: مکانیزم FTP Bounce Scan

به این قابلیت در سرویس‌دهنده FTP ، File-Forwarding گفته می‌شود که بدلیل همین نوع مشکلات، امروزه در اکثر سرویس دهنده‌های FTP از آن حمایت نمی‌شود. اگر در شبکه خود سرویس‌دهنده FTP نصب کرده‌اید مطمئن شوید که چنین قابلیتی را عرضه نمی‌کند چرا که می‌تواند قربانی توطئه نفوذگران قرار بگیرد. اگر می‌خواهید از وجود یا عدم وجود این قابلیت در سرویس دهنده FTP خود مطمئن شوید از نرم‌افزاری که توسط گروه CERT در دانشگاه کارنگی ملون نوشته شده است، استفاده کنید:

http:// www. Cert. org/advisories/CA-1997-27.html

۱-۲-۵-۳- بهره گیری از بسته‌های UDP

مکانیزم‌هائی که تا اینجا بررسی کردیم مبتنی‌بر پروتکلTCP و اصول دست تکانی سه مرحله‌ای بودند و فقط پورت‌های باز از نوع TCP را پویش و جستجو می‌کردند. برخلاف پروتکل TCP، در پروتکل UDP،" دست تکانی سه مرحله‌ای"، فیلد شماره ترتیب[1]و بیت‌های کنترلی[2] وجود ندارد. بسته‌ها ممکن است اصلاً به مقصد نرسند یا خارج از ترتیب به مقصد برسند. چون UDPیک پروتکل "بدون اتصال" است.

به دلیل سادگی بیش از اندازه پروتکل UDP، گزینه‌های بسیار کمی برای جستجوی پورت‌های باز UDP وجود دارد. وقتی از طریقTCP پویش پورت‌های باز انجام می شود برگشت

[1] Sequence Number
[2] Code Bits

بسته‌های مفیدی همانند SYN ACK یا RESET می‌تواند تکلیف باز یا بسته بودن پورت را مشخص نماید در حالی که در UDP چنین بسته‌هایی مبادله نخواهد شد.

برای پویش پورت‌های باز UDP، نرم‌افزاری مثل Nmap دنباله ای از بسته‌های UDP را برای پورت‌های مختلف هدف ارسال می‌نماید. اگر در پاسخ به یک بسته UDP پیغام ICMP Port unreachable برگردد می‌توان اطمینان حاصل کرد که آن پورت یقیناً بسته است. در غیر اینصورت هیچ چیزی را نمی‌توان در مورد آن پورت ثابت کرد، به همین دلیل نرم‌افزاری مثل Nmap فرض می‌کند آن پورت باز است. (هرچند هیچ اطمینانی به باز بودن آن نیست.)

بهترین مکانیزم برای پویش پورت‌های UDP آنست که از بین شماره پورت‌هایی که بسته بودن آنها محرز نشده است، پورت‌های مشهوری مثل پورت ۵۳ (مربوط به DNS) را با ارسال بسته‌های تقاضا بررسی کرد. مثلاً اگر نرم‌افزار Nmap پورت 7070 را (به دلیل عدم دریافت پیغام بسته بودن) باز کرد، می‌توان حدس زد که این پورت مربوط به سرویس‌دهنده Real Audio & Video است . با آن شماره پورت مبتنی‌بر پروتکل خاص آن سرویس‌دهنده، محاوره کرد تا از باز بودن آن اطمینان حاصل شود .

۱-۲-۵-۴-عمل Ping بدون بهره گیری از ICMP

بگونه‌ای که اشاره شد عمل Ping به‌منظور کشف ماشین‌های فعال در یک شبکه انجام می‌شود. از آنجایی که عمل Ping از پروتکلICMP بهره می‌گیرد برخی از ماشین‌های فعال به‌منظور پنهان ماندن از چشم ابزارهای پویشگر، پروتکلICMP را غیرفعال می‌نمایند. لذا Ping کردن این ماشین‌ها هیچ سودی ندارد. ابزارهائی مثل Nmap، هنگامی که عملPing نتیجه نمی‌دهد با ارسال یک‌سری از بسته‌های TCP کاملا بی-هدف به سمت آن ماشین، فعال بودن آنرا بررسی می‌کنند. هدف از این کار پویش پورت‌های باز نیست بلکه هر نوع بسته بازگشتی مثل SYN ACK یا RESET حاکی از فعال بودن آن ماشین است .

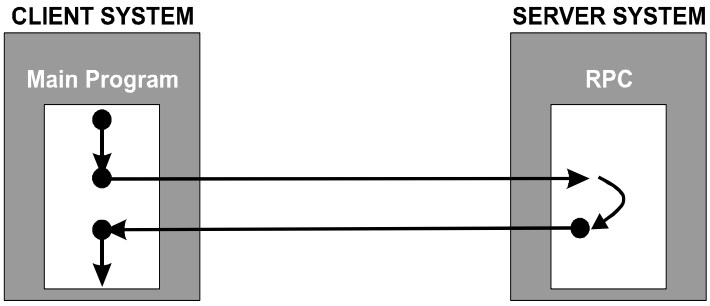
استفاده از این قابلیت باعث خواهد شد که در موقع غیرفعال بودن ICMP روی یک ماشین، آن ماشین از دید نفوذگر پنهان نماند.

شناسایی برنامه‌هایRPC نامطمئن (Romote Procedure Call)

تمام روش‌های پویش و جستجوی پورت‌های باز، مبتنی بر پروتکل‌های ICMP و TCP هستند. یکی از قابلیت‌های دیگر نرم‌افزار Nmap پویش سرویس

RPC (Romote Procedure Call) برروی ماشین‌های شبکه است سرویس RPC روشی برای توسعه سیستم‌ها و سرویس دهنده‌های توزیع شده در شبکه محسوب می‌شود.

با استفاده از این سرویس، برنامه نویس می‌تواند در بخشی از برنامه خود یک روال را از روی یک سرویس دهنده RPC در شبکه، فراخوانی کند و منتظر بماند تا نتیجه این فراخوانی بازگردد . یعنی بخشی از کد اجرائی برروی سرویس‌دهنده RPC اجرا می‌شود. شکل (۱-۷) این مفهوم را نشان می‌دهد.



شکل ۱-۷: فراخوانی یک برنامهٔ RPC

بسیاری از شرکت‌های توسعه نرم‌افزار، برنامه‌های کاربردی بسیار وسیعی را مبتنی‌بر سرویس RPC عرضه کرده اند. سرویس‌های شناخته شده RPC عبارتنداز :

- Rstatd : سرویسی که آمار مربوط به کارآئی[1] هسته سرویس‌دهنده را ارائه می‌دهد .
- Rwalld : سرویسی که اجازه می‌دهد به کاربران حاضر در سیستم، پیام‌هایی ارسال شود.
- Rup : سرویسی که زمان فعلی و متوسط بار سرویس دهنده را عرضه می‌کند.

متاسفانه بسیاری از سرویس‌های RPC با نقاط ضعف فراوان عرضه شده‌اند. دانستن سرویس‌های RPC ارائه شده توسط یک ماشین، اطلاعات مفیدی برای نفوذگر محسوب می‌شود. نرم‌افزار پویشگر برای کشف سرویس‌های RPC، یک‌سری دستورات پوچ RPC (Null RPC Command)، به سمت پورت‌های باز یک ماشین ارسال می‌کند. پاسخی که از این پورت‌ها باز خواهد گشت تعیین کننده نوع سرویس RPC اجرا شده بر روی آن ماشین است.

[1] Performance

اگر یک سرویس‌دهندهRPC روی یک ماشین کشف شد، نفوذگر سعی می‌کند با رخنه در آن، ماشین مربوطه را تحت کنترل خود در آورد. روش رخنه در سرویس‌دهنده RPC، ارسال کدهای Exploit به منظور در هم شکستن پشته و در اختیار گرفتن کنترل آن است.

۱-۲-۶- تنظیم زیرکانه شماره پورت مبداءبرای پویش موفق

برای آنکه شانس عبور بسته‌هائی که توسط نرم‌افزار پویشگر تولید می‌شود از مسیریاب و فایروال یک شبکه افزایش یابد، نفوذگر سعی می‌کند شماره پورت مبداء بسته‌های TCP و UDP ارسالی خود را به نحو زیرکانه و دقیقی تنظیم نماید.

نرم‌افزار پویشگر پورت، یکسری از بسته‌های متوالی TCP یا UDP به آدرس پورت‌های مختلف از ماشین هدف ارسال می‌نماید تا تعیین کند کدام پورت باز و کدام پورت بسته و غیرفعال است. لذا فیلد Destination Port از بسته ارسالی تعیین کننده شماره پورتی است که قرار است تحت بررسی و آزمایش قرار بگیرد .

فیلد Source Port از هر بسته ارسال شده به سمت هدف، پارامتر تعیین کننده‌ای برای فیلترها و فایروال است. بسیاری از فیلتر کننده‌ها جهت اعطای مجوز عبور به یک بسته TCP، شرایطی را برای Source Port تعیین کرده‌اند. هدف نفوذگر آنست که بسته‌های ارسالی به سمت ماشین هدف از فیلتر عبور نمایند؛ یعنی به همان صورتی که بسته‌های معمولی و مجاز از فایروال یا فیلتر عبور می‌کنند بسته‌های TCP ارسالی به سمت ماشین هدف نیز از فیلتر عبور نمایند.

نفوذگر به دقت شماره پورت‌هائی را که اگر در فیلد Source Port از یک بستهTCP تنظیم شود قادر به عبور از فایروال خواهد بود، می‌شناسد. به‌عنوان مثال معمولی‌ترین شماره پورت، TCP 80 است. بسته‌ای که با این شماره پورت به سمت ماشین هدف ارسال شود شانس زیادی برای عبور از فیلترها و دیوارهای آتش دارد چرا که به نظر می‌رسد این بسته از طرف یک سرویس دهنده وب ارسال شده و ناشی از تقاضای قبلی آن ماشین بوده است؛ در اینجا فیلتر به ناچار بسته را عبور خواهد داد. یعنی نفوذگر برای به اشتباه انداختن فیلتر، بستهTCP را با مشخصات زیر ارسال می‌نماید .

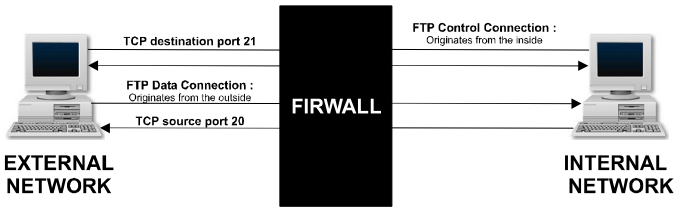
- جعلی Source Port = 80
- شماره پورت مورد آزمایش = Destination Port

- مشخصه یک بسته SYN-ACK ACK Bit = 1

یکی دیگر از شماره پورت‌های مشهور که شانس عبور زیادی از فیلتر دارد، پورت TCP 25 است که به طور معمول از طرف سرویس دهنده نامه الکترونیکی یا SMTP تولید می‌شود.

پورت TCP شماره ۲۰ نیز شانس عبور از فیلتر را دارد؛ زیرا این پورت متعلق به سرویس دهنده FTP است.

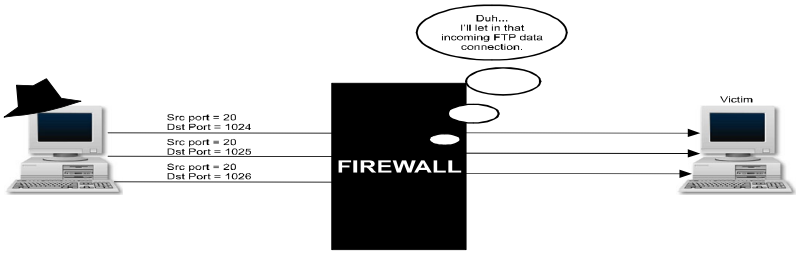
به گونه‌ای که در شکل (۱-۸) یک نشستFTP ، منوط به برقراری دو ارتباط مجزای TCP است که هر یک کانال نامیده می‌شود. ارتباط TCP با پورت شماره ۲۱ از سرویس‌دهنده جهت مبادله فرامین FTP (کانال فرمان) و ارتباطTCP با پورت شماره ۲۰ از سرویس‌دهنده FTP جهت مبادله فایل(کانال داده).



شکل ۱-۸: برقراری یک نشست FTP با ایجاد دو ارتباط TCP

کانال فرمان از سمت برنامه مشتری به سرویس‌دهنده FTP باز می‌شود و جهت عملیاتی نظیر ورود (Log in) تقاضای فایل، فهرست‌گیری و ... کاربرد دارد. پس از باز شدن این کانال و به‌منظور مبادله داده‌های فایل، سرویس‌دهنده FTP یک ارتباط مستقل TCP بین شماره پورت ۲۰ خود و شماره پورت پیشنهاد شده از مشتری برقرار می‌نماید.

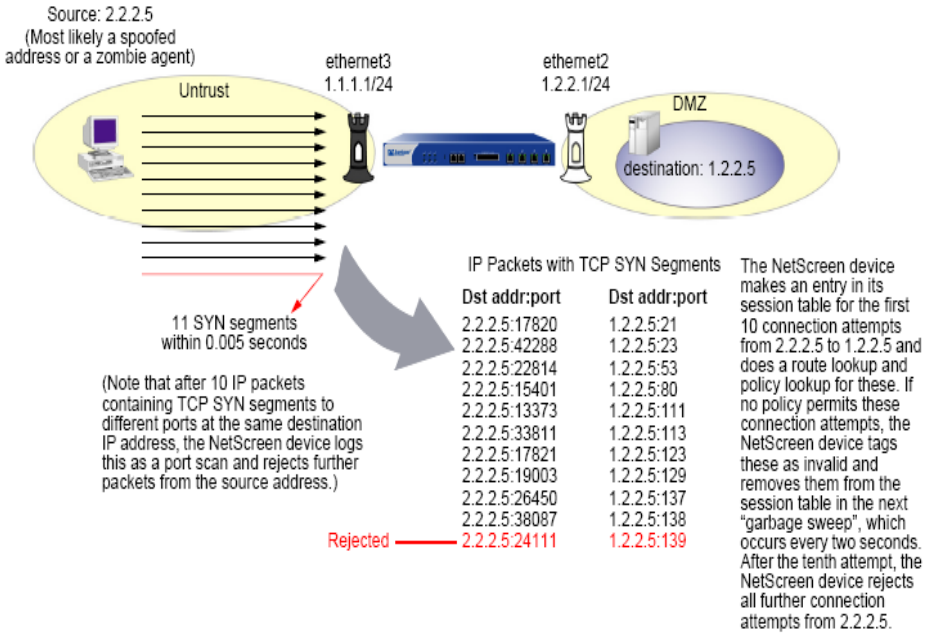
با این توضیح هر سرویس دهنده FTP خارجی باید اجازه داشته باشد تا یک ارتباط TCP از بیرون به درون یک شبکه برقرار نماید و بالطبع فایروال یا فیلتر باید مجوز عبور برای بسته-های TCP با مشخصه Source Port = 20، صادر نماید.



شکل ۱-۹: مکانیزم پویش پورت‌های باز با استفاده از کانال باز FTP Port 20

نفوذگر از همین نکته استفاده می‌کند و بسته‌های TCP خود را به منظور پویش پورت‌های باز با شماره پورت Source Port = 20 ارسال می‌کند و لاجرم دیوارهای آتش معمولی و فیلترها آنها را عبور می‌دهند برای ارسال بسته‌های UDP نیز بهترین شماره‌ای که می‌توان به عنوان Source Port استفاده کرد، پورت ۵۳ (متعلق به سرویس دهنده DNS) است زیرا ورود بسته‌های DNS به درون هر شبکه تقریباً الزامی و اجباری می باشد.

نرم‌افزار Nmap این امکان را فراهم آورده تا بتوان هر شماره پورت دلخواه برای بسته‌های TCP یا Source Port UDP انتخاب کرد .



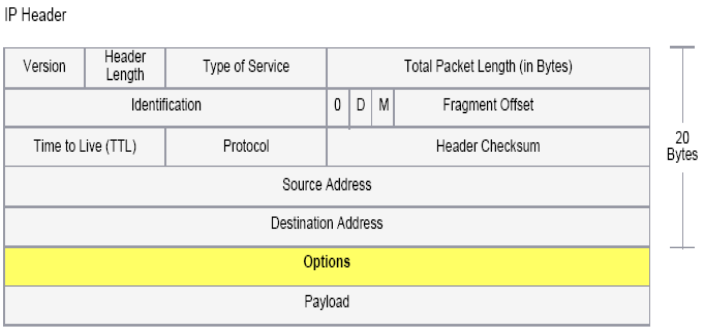
شکل ۱-۱۰: اسکن عمودی آدرس‌ها

۱-۲-۷- شناسایی شبکه با استفاده از انتخاب‌های IP

استاندارد پروتکل اینترنت Internet protocol، RFC 791 دارای یک مجموعه از انتخاب‌هایی است که کنترل مسیرهای ویژه، ابزار تشخیص و امنیت را به عهده دارد. این گزینه‌های انتخابی بعد از آدرس مقصد در یک فرآیند بسته IP وجود دارند. RFC 791 تصدیق می‌کند که این انتخاب‌ها برای بسیاری از ارتباطات معروف غیرضروری هستند و در حقیقت آنها به ندرت در

سرآیند بسته‌های IP استفاده می‌شوند. در زیر برخی از انتخاب‌های معروف که یک حمله کننده می‌تواند برای شناسایی یا برخی از اهداف مظنون استفاده کند آورده شده است.

- **ثبت مسیر:** آدرس‌های IP تجهیزات شبکه در طور عبور بسته‌های IP را ثبت می‌کند. بدین ترتیب برخی از تجهیزات امنیتی بسته‌هایی که IP Option آنها 7 است و قابلیت ثبت مسیر را دارند را شناسایی می‌کنند.
- **Time lamp:** زمانی که تجهیزات شبکه‌ای بسته‌های IP را در طول مسیر از نقطه آغاز تا مقصد دریافت می‌کند را ثبت می‌کند. برخی از تجهیزات امنیتی بسته‌هایی که قابلیت ثبت زمانی را دارند شناسایی می‌کند.
- **Security:** ایجاد روشی است برای دستگاه‌ها جهت ارسال امنیت، پارامترهای TCC و کدهای بکارگیری و ایجاد محدودیت مطابق با نیازهای DOD برخی از تجهیزات امنیتی بسته‌هایی که این خصوصیت در آنها تنظیم شده است را کشف و ضبط می‌کنند.
- **Stream ID:** روشی است برای شناختن SAT NET Stream برای شبکه‌هایی که از مفهوم Stream نمی‌شناسند و پشتیبانی نمی‌کنند. به همین ترتیب این ویژگی نیز توسط برخی از تجهیزات امنیتی قابل شناسایی است.



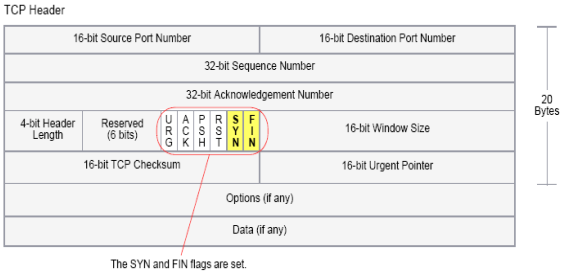
شکل ۱-۱۱: IP Header

۱-۲-۸-کاوش در جهت سیستم عامل‌ها

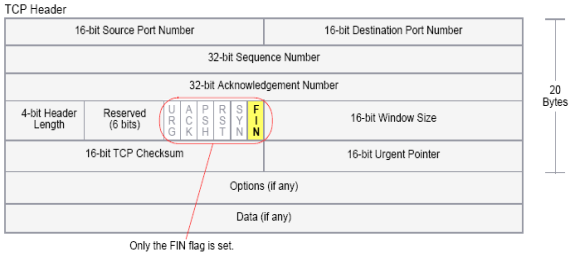
قبل از انجام هرگونه سوءاستفاده‌ای، ممکن است برخی حمله کننده‌ها سعی در شناسایی نوع سیستم عامل سیستم هدف کنند. با علم به نوع سیستم عامل او بهتر می‌تواند تصمیم بگیرد از چه حمله‌ای باید استفاده کند و از کدام آسیب‌پذیری بهره‌برداری کند.

۱-۲-۹- نشاندن فلگ‌های SYN و FIN

در حالت نرمال فلگ‌های کنترلی SYN و FIN در سرآیندهای TCP ست نشده‌اند. فلگ SYN برای همزمان کردن دنباله بسته‌ها جهت برقراری یک ارتباط TCP به کار می‌رود. فلگ FIN برای اتمام انتقال داده‌ها جهت پایان دادن به یک ارتباط TCP به کار می‌رود. استفاده از آنها در یک زمان غیرممکن و نادرست است. سرآیند TCP با فلگ SYN و FIN نشانده شده نشان‌دهنده رفتار غیرعادی TCP است که بسته به نوع سیستم عامل موجب پاسخ‌های متفاوتی از جانب گیرنده می‌شود. یک حمله کننده با ارسال یک بسته با فلگ‌های SYN و FIN ست شده نوع سیستم عامل سیستم هدف را مشخص می‌کند و با شناخت نوع سیستم عامل حمله کننده با استفاده از آسیب‌پذیری‌های معروف آن نوع سیستم عامل، به حمله‌های بعدی می‌پردازد.



شکل ۱-۱۲: یک بسته TCP با فلگهای SYN و FIN ست شده



شکل ۱-۱۳: یک بسته TCP با فلگ FIN ست شده

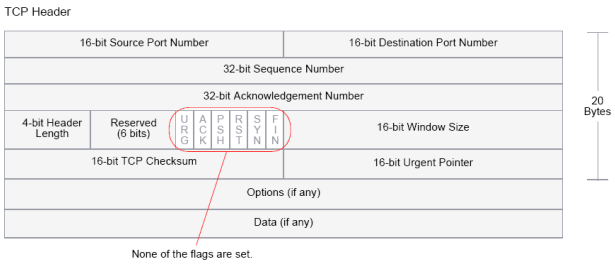
۱-۲-۹-۱- فلگ FIN، بدون فلگ ACK

قطعات TCP با فلگ کنترلی FIN ست شده (برای پایان بخشیدن به یک ارتباط) معمولاً دارای فلگ ACK ست شده نیز می‌باشد (برای تصدیق دریافت بستهٔ قبلی). از آنجایی که فلگ FIN ست شده و فلگ ACK ست نشده در یک سرآیند TCP یک رفتار غیرعادی TCP را

نشان می‌دهد، یک پاسخ یکسان و یکنواختی برای آن وجود ندارد. سیستم‌عامل ممکن است با ارسال یک قطعه TCP با فلگ RST ست شده پاسخ دهد. سیستم‌عامل دیگری ممکن است کاملاً از آن بسته صرفه‌نظر کنند. نوع پاسخ سیستم‌عامل می‌تواند به‌عنوان کلیدی در تشخیص سیستم‌عامل برای حمله کننده‌ها باشد. در بسیاری از تجهیزات امنیتی با تشخیص بسته‌هایی که فلگ FIN آنها ست شده و فلگ ACK آنها در سرآیند TCP ست نشده باشد، مانع از عبور آنها می‌شود.

۱–۲–۹–۲– سرآیند بدون هیچ فلگ ست شده

یک قطعه سرآیند TCP نرمال، حداقل یک فلگ کنترلی ست شده دارد. یک بسته TCP بدون هیچ نوع فلگ ست شده می‌تواند به عنوان یک رفتار غیرعادی تلقی شود. از آنجایی که سیستم عامل‌های مختلف پاسخ‌های متفاوتی به چنین رفتارهای غیرمتعارف می‌دهند، نوع پاسخ (یا عدم هرگونه پاسخ) از سوی دستگاه هدف می‌تواند به عنوان کلیدی در تشخیص نوع سیستم عامل در حال اجرا روی دستگاه باشد.



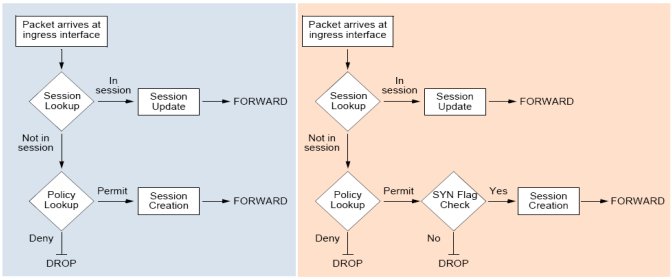
شکل ۱-۱۴: یک بسته TCP بدون هیچ نوع فلگ ست شده

۱–۲–۱۰– تکنیک‌های حیله‌زنی

هنگام جمع‌آوری اطلاعات یا انجام یک حمله، به طور معمول حمله‌کننده از شناسایی خود توسط سیستم‌ها جلوگیری می‌کند گرچه برخی آدرس‌های IP و پویش پورت‌ها به سادگی قابل کشف هستند، بسیاری از حمله کننده‌ها از روش‌هایی استفاده می‌کنند تا بتوانند فعالیت‌های خود را پنهان کنند نظیر استفاده از تکنیک‌های پویش FIN به جای پویش SYN. حمله کننده‌ها می‌دانند غالب فایروال‌ها و برنامه‌های کشف نفوذ حملات را کشف می‌کنند که نشان دهنده پیشرفت در تکنیک‌های بهره‌برداری سوء و شناسایی سیستم‌ها از طرف حمله کننده‌ها می‌باشد.

۱-۲-۱۰-۱- پویش FIN

پویش FIN با ارسال بسته TCP همراه با فلگ FIN ست شده سعی در تحریک یک پاسخ و در نتیجه کشف یک دستگاه فعال و با یک پورت فعال روی یک سیستم منجر می‌شود. ممکن است یک حمله کننده این روش را نسبت به جاروب یک آدرس با استفاده از بسته‌های ICMP یا پویش یک آدرس با قطعات SYN به کار ببرد چرا که دو روش اخیر توسط بسیاری از فایروال‌ها شناخته شده است و در برابر آنها محافظت می‌شود اما لزوماً همهٔ آنها پویش FIN را هنوز نمی‌شناسند.

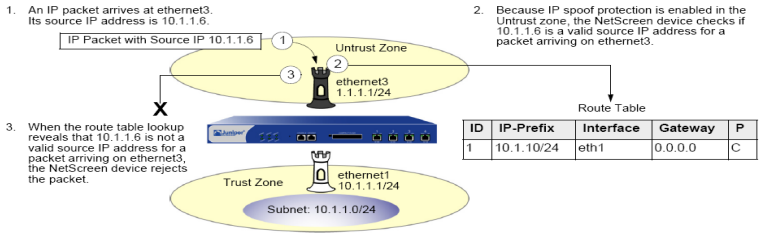


شکل ۱-۱۵: پویش FIN

۱-۲-۱۰-۲- جعل IP (IP Spoofing)

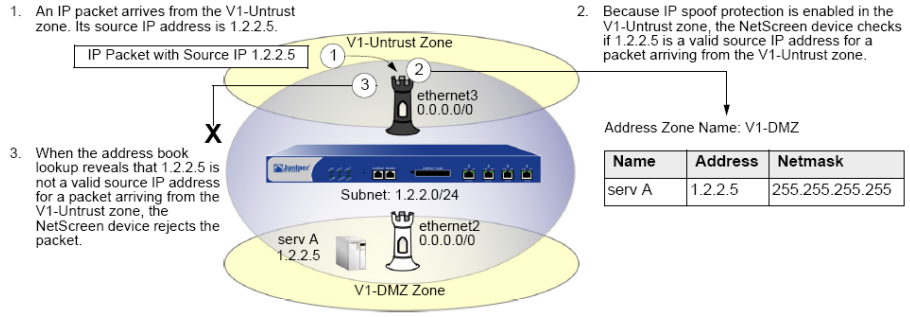
یک روش در درسترسی پیدا کردن به یک ناحیه محدود شده در شبکه، عوض کردن آدرس مبدا در سرآیند بسته است. طوری که به نظر می‌رسد بسته از یک مبدا قابل اعتماد سرچشمه گرفته است. نام این تکنیک جعل IP است.

با این نظر که فایروال در لایهٔ ۳ کار می‌کند (NAT-Route mode) یا لایهٔ ۲ (Transparent mode) از دو روش مجزا برای کشف بسته‌هایی که جعل IP انجام داده‌اند استفاده می‌کند.



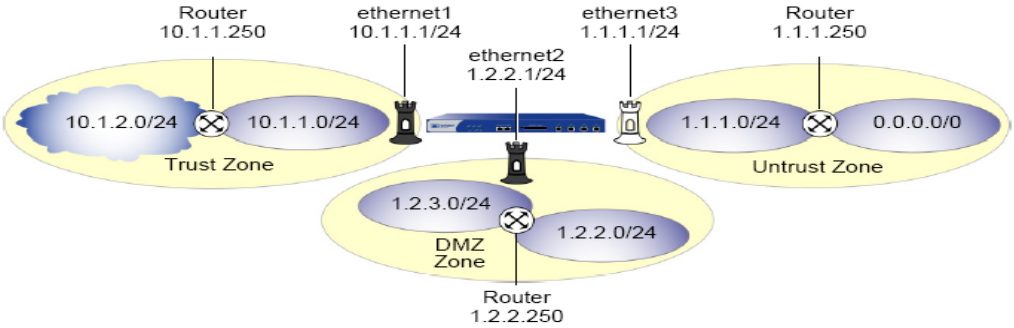
شکل ۱-۱۶: جعل IP

لایهٔ ۳- هنگامی که یک اینترفیس فایروال در مد NAT یا Route کار می‌کند، مکانیزم کشف جعل IP بر مبنای جداول مسیریابی استوار است. به طور مثال اگر بسته‌ای با آدرس مبدا 10.1.1.6 از اینترفیس ۳ وارد شود ولی در جدول مسیریابی فایروال مسیری وجود داشته باشد که 10.1.1.0/29 از اینترفیس ۱ وارد می‌شود، مکانیزم جعل IP یادآور می‌شود که این بسته از طریق اینترفیس غیرمعتبری وارد شده است و فایروال این بسته را به دور می‌اندازد.



شکل ۱-۱۷: جعل IP در لایه ۳

لایهٔ ۲- زمانی که اینترفیس‌ها در فایروال در مد Transparent کار می‌کنند، مکانیزم تست جعل IP از ورودی‌های دفترچه آدرس‌ها استفاده می‌کند. به‌طور مثال یک آدرس برای server به صورت 1.2.2.5/32 در ناحیه VI-DM7 تعریف می‌شود. اگر بسته‌ای با آدرس IP مبدا 1.2.2.5/32 از یک اینترفیس ناحیه VI-untrust وارد فایروال شود مکانیزم جعل IP پیغام می‌دهد بسته با آدرس مبدا 1.2.2.5 از یک اینترفیس غیرمعتبر وارد شده است.



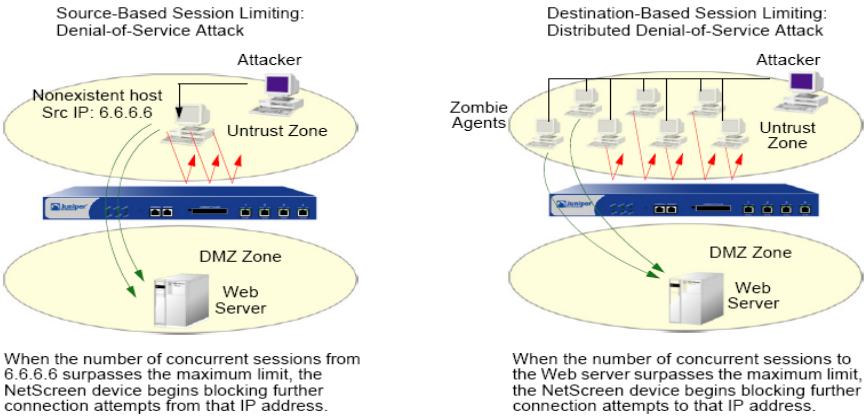
شکل ۱-۱۸: جعل IP در لایه ۲

۱-۲-۱۱- حملات Dos فایروال

اگر یک مهاجم وجود یک فایروال را در شبکه کشف کند، ممکن است دست به حمله انکار از خدمت (Dos) برعلیه فایروال بزند. حمله Dos موفقیت آمیز علیه فایروال به اندازه حمله Dos علیه شبکه‌ها می‌باشد. این بخش دو روش که مهاجمان از آن برای پرکردن جداول جلسات در فایروال استفاده می‌کنند که در نهایت منجر به یک حمله Dos می‌شود را بررسی می‌کند.

۱-۲-۱۱-۱- Session table Flood

یک حمله Dos موفقیت‌آمیز قربانی خود را با سیل ترافیک غیرضروری اشباع می‌کند طوری که دیگر توانایی پردازش درخواست‌های قانونی را هم ندارد. برای حملات Dos چند فرم متفاوت وجود دارد. SYN Flood, ACK-SYN Flood و UDP Flood و ICMP Flood و غیره. ولی همهٔ آنها در جستجوی یک هدف هستند پرکردن جداول جلسات برقرار شده قربانی خود. هنگامی که جدول جلسات پر شده باشد دستگاه قادر به ایجاد هیچ جلسه جدیدی نمی‌باشد و تمام درخواست‌های ارتباطی جدید را رد می‌کند توانایی دفاع یک فایروال در برابر این نوع حملات بسیار با اهمیت است.



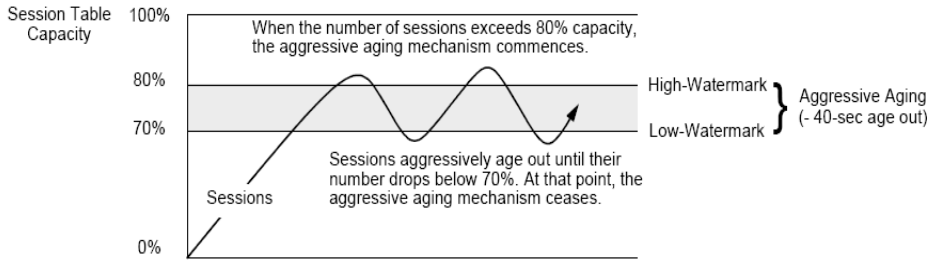
شکل ۱-۱۹: حمله Dos – Session table Flood

۱-۲-۱۱-۲- محدودیت‌های ایجاد جلسات برمبنای آدرس مقصد و مبداء

علاوه بر محدود کردن تعداد جلسات همزمان برگرفته از یک آدرس مبدا، همچنین می‌توان تعداد جلسات همزمان به یک آدرس مقصد را نیز محدود کرد. یکی از مزایای تنظیم محدودیت براساس آدرس مبدا جلوگیری از حملهٔ ویروس Nimda (در حقیقت هم ویروس و هم کرم می‌باشد)است. این ویروس پس از آلوده کردن یک سرور شروع به تولید حجم بسیار وسیعی ترافیک می‌کند. ازآنجایی که کلیه ترافیک تولید شده توسط ویروس از یک آدرس IP نشات می‌گیرد. محدودیت تعداد جلسات براساس مبدا قادر به کاهش این تخریب می‌باشد. مزیت دیگر ایجاد محدودیت تعداد جلسات بر اساس مبدا کاهش تلاش‌های صورت گرفته در جهت پرکردن جدول جلسات یک فایروال از سمت یک آدرس IP می‌باشد. با این وجود بسیاری از مهاجمان با کمک گرفتن چند دستگاه اقدام به حملات گسترده انکار از خدمات Dos می‌کند. در حملات Dos ترافیک خرابکار از صدها دستگاه، شبیه Zombie agent، که تحت کنترل یک مهاجم هستند نشأت می‌گیرد. علاوه بر شناسایی SYN, UDP, ICMP flood تنظیم محدودیت تعداد جلسات براساس مقصد، تعداد درخواست‌های ارتباط همزمان، بدون توجه به آدرس مبدا به یک تعداد قابل قبول محدود می‌کند. این تعداد قابل قبول بسته به نوع فایروال و ظرفیت جدول جلسات آن دارد.

Aggressive Aging –۳–۱۱–۲–۱

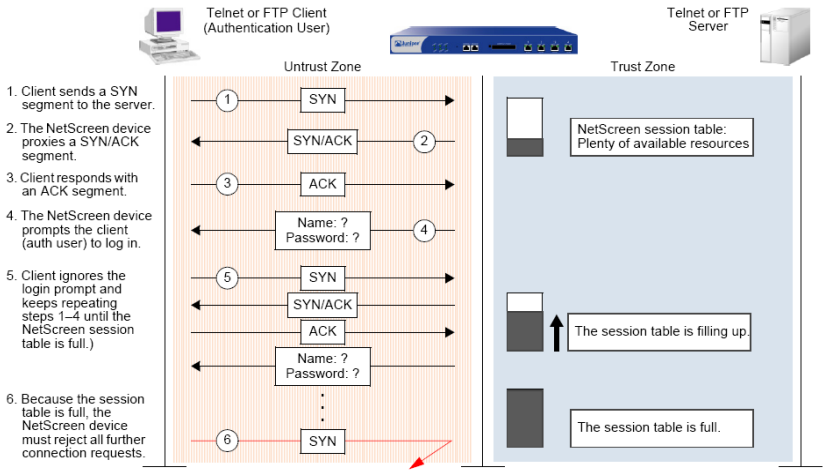
به صورت پیش‌فرض جلسهٔ آغازسازی TCP موسوم به 3-Way handshake پس از ۲۰ ثانیه، در صورت غیرفعال بودن صرفنظر می‌شود. بعد از اینکه جلسه TCP برقرار شد مقدار time out به ۳۰ دقیقه تغییر می‌کند. برای جلسات UDP و HTTP مقدار time out به ترتیب ۱ دقیقه و ۵ دقیقه می‌باشد. شمارنده time out جلسات، پس از آغازسازی جلسه در صورت فعال بودن هر ۱۰ ثانیه refresh می‌شود. اگر یک جلسه بیش از ۱۰ ثانیه به صورت غیراستفاده باقی بماند. شمارنده time out شروع به کاهش می‌کند.



شکل ۱-۲۰: Aggressive Aging

SYN ACK-ACK Proxy flood –۴–۱۱–۲–۱

هنگامی که یک کاربر به صورت مکانیزم تصدیق هویت یک ارتباط FTP یا Telnet را آغازسازی می‌کند. یک بسته SYN به سمت سرور FTP یا Telnet می‌فرستد. دستگاه فایروال بسته SYN را دریافت کرده و یک ورودی در جدول جلسه خود ایجاد می‌کند. و به صورت پراکسی یک بسته SYN-ACK به سمت کاربر می‌فرستد. سپس کاربر با بستهٔ ACK به آن جواب می‌دهد. بنابراین در این نقطه برقراری ارتباط اولیه موسوم به 3-way handshake کامل می‌شود فایروال یک اعلان Login به سمت کاربرمی‌فرستد. اگر کاربر با قصد خرابکاری، Login نکند و به جای آن جلسات SYN ACK به صورت پشت‌سرهم درست کند، جدول جلسات پر شده و دستگاه حتی به کاربران عادی و قانونی نیز قادر به ارائه سرویس نخواهد بود.



شکل ۱-۲۱: نحوه برخورد فایروال با SYN-ACK-ACK Proxy flood

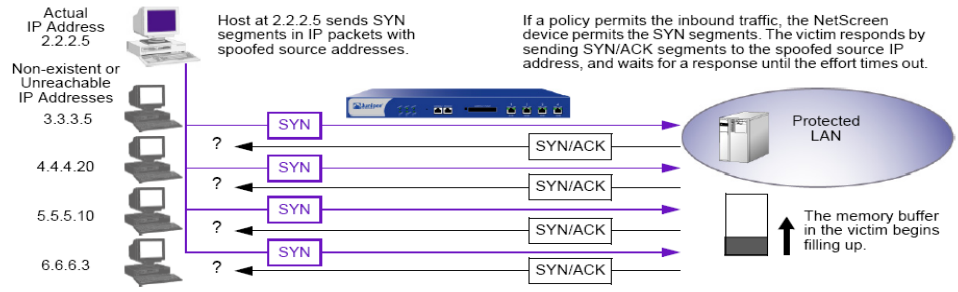
۱-۲-۱۲- حملات Dos شبکه

حملات انکار از خدمت (Dos) یک یا چند منابع شبکه را مورد هدف قرار می‌دهند. این حملات با بمباران کردن شبکه با استفاده از بسته‌های ICMP,UDP و یا SYN و یا خرد کردن تعدادی بسته‌های SYN انجام می‌گیرد. بسته به اهداف مهاجمان و میزان موفقیت آنها در جمع‌آوری داده‌ها و اطلاعات ممکن است مهاجم یک دستگاه خاص مانند روتر و یا سرور را مورد حمله قرار داده و یا رنجی از دستگاه‌ها را در عرض شبکه هدف گیرد. و یک از رویکردهای فوق پتانسیل از بین بردن ارائه سرویس توسط یک دستگاه یا شبکه را دارد.

۱-۲-۱۲-۱- بمباران SYN

بمباران SYN هنگامی رخ می‌دهد که یک دستگاه توسط قطعات SYN شروع به درخواست ارتباط ناتمام می‌کند به‌طوری که دیگر پردازشی برای درخواست‌های ارتباط قانونی باقی نمی‌ماند.

دو دستگاه با یک تبادل سه‌گانه قطعات TCP موسوم 3way handshake یک ارتباط TCP را برقرار می‌کنند. A یک بستهٔ SYN به B می‌فرستد. B با بسته SYN/ACK به آن پاسخ می‌دهد و در نهایت A با قطعهٔ ACK پاسخ می‌دهد. در حملهٔ بمباران SYN دستگاه A یک بستهٔ SYN را با آدرس مبداهای جعلی یا آدرس غیرقابل دسترس به سمت دستگاه B می‌فرستد. دستگاه B با قطعهٔ SYN/ACK به این آدرس‌ها پاسخ می‌دهد و سپس منتظر پاسخ بستهٔ ACK از طرف مقابل می‌ماند. از آنجایی که قطعات SYN/ACK به آدرس‌های IP غیرقابل دسترسی فرستاده می‌شود، هرگز به این درخواست‌ها پاسخ داده نمی‌شود و سرانجام time out می‌شود. با بمباران کردن یک دستگاه با ارتباطات TCP ناتمام، مهاجم سرانجام بافر حافظهٔ قربانی را پر می‌کند. هنگامی که این بافر پر می‌شود، دیگر دستگاه قادر به پاسخگویی درخواست‌های جدید نیست این بمباران ممکن است به سیستم‌عامل قربانی، آسیب جدی برساند. بدین ترتیب مهاجم، عملیات طبیعی قربانی را غیرفعال می‌کند.



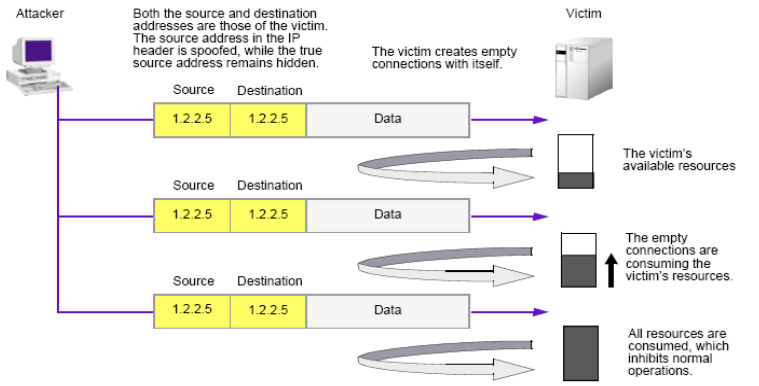
شکل ۱-۲۲: بمباران SYN

۱-۲-۱۲-۲- حفاظت در برابر بمباران SYN

فایروال‌ها تعداد درخواست‌های بسته‌های SYN که در یک ثانیه حق عبور دارند را محدود می‌کند آستانهٔ حمله را می‌توان با تعریف تعداد ارتباطات برحسب آدرس مقصد و پورت و یا تنها آدرس مقصد و یا آدرس مبدا مشخص کرد. هنگامی که تعداد بسته‌های SYN در یک ثانیه از هر یک از این آستانه‌ها گذر کند، بسته به نوع فایروال‌ها، ۲ نوع برخورد متفاوت می‌شود. یا اینکه درخواست‌های اضافه drop می‌شوند و یا اینکه فایروال مانند یک پراکسی عمل کرده و با بستهٔ SYN/ACK به درخواست کننده پاسخ می‌دهد و سپس درخواست ناتمام را در یک صف ارتباطی ذخیره می‌کند. این ارتباط ناتمام تا زمان کامل شدن ارتباط و یا time out شدن درخواست در صف باقی می‌ماند.

۱-۲-۱۲-۳- حملهٔ Land

ترکیبی از یک حملهٔ SYN با جعل آدرس IP است. بدین ترتیب که یک مهاجم بسته‌های SYN شامل آدرس IP مبدا و مقصد یکسان (آدرس IP قربانی) به سمت قربانی می‌فرستد. سیستم دریافت کننده با ارسال بسته‌های SYN ACK به خودش پاسخ می‌دهد طوری که اتصالات خالی ایجاد می‌شود و تا زمان time out به طول می‌انجامد. بمباران کردن یک سیستم با ایجاد چنین اتصالات خالی یک حملهٔ Dos را موجب می‌شود.



شکل ۱-۲۳: حمله Land

۱-۲-۱۳- حملات Dos ویژهٔ سیستم عامل

اگر یک مهاجم علاوه‌بر شناسایی آدرس IP و شماره پورت پاسخ دهنده یک دستگاه فعال سیستم عامل آن را نیز شناسایی کند، می‌تواند حملات بیشتر و متنوع تری علیه قربانی سازمان‌دهی کند. حملاتی که در این قسمت به آن می‌پردازیم به راحتی و با تلاش حداقل می‌توانند یک سیستم را فلج کنند. دستگاه فایروال مورد استفاده در شبکه باید بتواند جلوی این حملات را بگیرد.

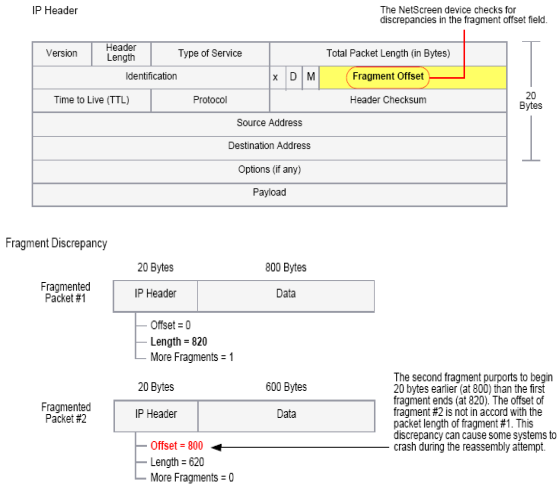
۱-۲-۱۳-۱- Ping of Death

حداکثر اندازهٔ مجاز بسته‌های IP، 65535 بایت می‌باشد شامل سرآیند بسته که به طور نوعی اندازه آن ۲۰ بایت می‌باشد. ICMP echo request یک بستهٔ IP با سرآیند کاذب است که 8 بایت طول دارد. بنابراین حداکثر اندازهٔ مجاز ناحیهٔ داده درICMP echo request، 65507 بایت (65,535-20-8=65,507) می‌باشد.

بسیاری از محیط‌های پیاده‌سازی ping به کاربراجازه می‌دهند تا اندازه یک بسته را بزرگتر از 85507 بایت در نظر گیرند. بسته‌های ICMP بزرگتر از مقدار مجاز موجب پاسخ‌های غیرعادی سیستم نظیر انکار از خدمت، crash کردن، freeze شدن و یا reboot شدن سیستم شود.

۱-۲-۱۳-۲- حمله Teardrop

حملهٔ teardrop از سوار کردن دوبارهٔ بسته‌های IP قطعه قطعه شده بهره برداری سوء می‌کند. در سرآیند IP، یکی از فیلدها، فیلد افست هر قطعه می‌باشد. این فیلد توالی بسته‌ها را مشخص می‌کند به عبارتی موقعیت یک قطعه را نسبت به بسته کلی قطعه نشده نشان می‌دهد. هنگامی که مجموع افست‌ها و اندازه یک بسته قطعه شده با بستهٔ قطعه بعدی متفاوت باشد بسته‌ها overlap کرده و کارگزاری که قصد دوباره‌سازی این بسته‌ها را دارد Crash خواهد کرد. مخصوصاً این آسیب‌پذیری در سیستم عامل‌های قدیمی مشهورتر می‌باشد.



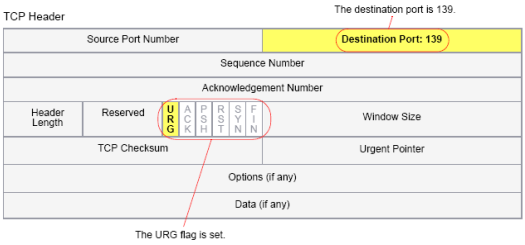
شکل ۱-۲۴: حمله Teardrop

۱-۲-۱۳-۳- حمله winnuke

یک حملهٔ Dos است که هر کامپیوتر بر روی اینترنت که دارای سیستم عامل Windows باشد را هدف قرار می‌دهد. مهاجم یک بستهٔ TCP (معمولاً Net BIOS پورت و 13 با فلگ (URG) ست شده به سمت یک دستگاه با یک ارتباط برقرار شده می‌فرستد. این موجب Overlap شدن قطعه Net BIOS شده و باعث Crash شدن تمام سیستم‌هایی که سیستم عامل آنها ویندوز است می‌شود. بعد از reboot شدن ماشین قربانی پیغام زیر نمایش داده می‌شود. که نشان می‌دهد که یک حمله اتفاق افتاده است.

An exception OE has occurred at 0028:{address} in VXD MSTCP (01)+ 000041AE. This was called from 0028:{address} in VXD NDIS (01)+
0000860. if maybe possible to continue normally.
Press any key to attempt to continue.

Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.
Press any key to continue.



شکل ۱-۲۵: حمله winnuke

۱-۳- استراتژی‌های مقابله با حمله

در این قسمت بعضی از استراتژی‌های معروف مقابله با حمله مورد بررسی قرار داده شده است.

۱-۳-۱- استراتژی حداقل رده دسترسی

یک استراتژی امنیتی مبتنی‌بر مفهوم فراهم کردن حداقل محاسن و مزایا است، و یک استراتژی اندیشمندانه است که اجازه نمی‌دهد هر جزء از سیستم ماوراء وظایف و عملکردش، کاری را انجام دهد. استفاده از این استراتژی باعث به حداقل رساندن میزان در معرض قرارگیری مؤلفه‌های سیستم می‌شود، در این استراتژی امکان حملات محدود می‌شود زیرا اگرچه هکر به درون اجزاء سیستم رخنه می‌کند لیکن یک حداقل امکاناتی را دسترسی پیدا می‌کند.

به لحاظ اینکه شما بیشترین هزینه امنیتی را صرف بهترین اجزاء سیستم می‌کنید و نه صرف اجزاء معمولی‌تر، لذا این استراتژی یک استراتژی کم‌هزینه و به صرف محسوب می‌گردد. جزیی که دارای حق‌تقدم بالاست نظیر مدیر سیستم دارای امنیت بالا و سنگین‌تری از یک جزء با حق تقدم کمتر می‌باشد.

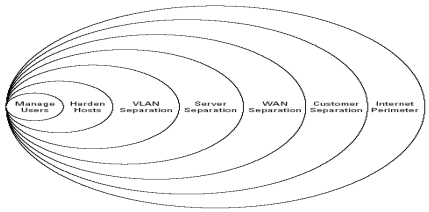
یک مثال از چنین استراتژی امنیت گروهی از صورتحساب‌ها در سیستم عامل یونیکس و Windows NT می‌باشد، در چنین سیستم عامل‌هایی، گروه‌های کاربر مختلفی ایجاد می‌شوند که به هر کدام از آنها یک حق تقدمی اختصاص داده می‌شود، لذا شما می‌توانید گروه‌های کاری

با حق تقدم‌های متفاوت داشته باشید و نیز یک صورتحساب کاربر در یک زمان می‌تواند به چندین گروه تعلق داشته باشد.

۱-۳-۲- استراتژی دفاع در عمق

استراتژیی است که در آن سیستم با استفاده از یک مکانیزم امنیتی چند لایه، ایمن می‌گردد. تمرکز دفاع در عمق، روی ایمن نمودن لینک‌های شبکه، انتقال، کاربرد و لایه‌های شبکه می‌باشد تا آن را برای هکرها غیرقابل نفوذ و غیرشکننده بنماید، در این استراتژی، انواع مختلف فناوری‌ها و مکانیزم‌ها بکار گرفته می‌شود تا از ورود و نفوذ هکرهای خارج از سیستم جلوگیری شود.

در این استراتژی هدف اصلی ترساندن مهاجمین از هرگونه تلاش برای نفوذ به سیستم می‌باشد که در این راستا ترکیبی از مکانیزم‌ها نظیر مکانیزم امنیت محیطی و فیزیکی امنیت شبکه، امنیت رایانه و همچنین امنیت انسان در محل زیرساختارها است که مهاجم احساس می‌کند که نفوذ غیرممکن و لذا هرگونه تلاش در این جهت بی‌حاصل و در ضمن فوق العاده هزینه‌بر می‌باشد، در استراتژی دفاع در عمق شما بایستی از طرح‌های پشتیبان نظیر طرح A، طرح B و طرح C که یکدیگر را پشتیبانی می‌نمایند، مطمئن باشید.



شکل ۱-۲۶: دفاع در عمق

۱-۳-۳- استراتژی گلوگاهی

یک استراتژی جهت برقراری یک گلوگاه عمدی بین شبکه محلی و اینترنت می‌باشد. این گلوگاه را Chock Point گویند و یک کانال نفوذ را بقدری باریک می‌نماید که حمله مهاجم به آن مشکل می‌گردد. نظریه پشتیبان این استراتژی نظارت آسان بر گلوگاه است، این نظریه پهنای باند مخابراتی سیستم را کاهش نمی‌دهد، لیکن تعداد نقاط دسترسی به شبکه را محدود می‌کند .

برای مثال شما می‌توانید تنها یک گیت وی بین شبکه محلیتان و اینترنت داشته باشید، بعبارتی شما می‌توانید یک فایروال روی گیت وی نصب نمائید که در نظارت و کنترل ترافیک شبکه کمک نماید. در این استراتژی لازم است از عدم وجود درهای پشتی[1] برای شبکه و همچنین اینکه گیت وی تنها نقطه دسترسی صحیح برای شبکه می‌باشد، مطمئن شویم .

۱–۳–۴– استراتژی ضعیف ترین لینک

در این استراتژی سیستم مورد تحلیل کامل قرار گرفته و نقاط ضعف آن نمایان می‌گردد، قدم بعدی حذف نقاط ضعف آشکار شده می‌باشد. در یک شبکه پیچیده حذف مؤلفه‌های داخلی خاصی بدلیل تاثیری که نبود آن مؤلفه خاص بر کل شبکه می‌تواند داشته باشد دشوار است. اینگونه مؤلفه‌ها می‌توانند ضعیف‌ترین زنجیره‌ها در شبکه باشند. از آنجائیکه اجزاء مذکور مهم می‌باشند ممکن است حذف همگی آنها با هم دشوار باشد. بهترین کاری که می‌توان انجام داد این است که سعی شود آسیب‌پذیری مؤلفه را با بکارگیری اقداماتی که در زمان تشخیص آسیب‌پذیری پیشنهاد گردید، تقلیل داد. چنانچه یک مؤلفه داخلی هنوز امنیت شبکه را علیرغم همه این اقدامات به خطر اندازد بسیار مهم است که توجه خاصی به آن شود، توصیه ای که راهبرد این استراتژی می‌نماید این است که فعالیت‌های ضعیف‌ترین لینک‌ها را در شبکه، مورد نظارت دقیق قرار دهد، زیرا که این نظارت از برای سلامت و امنیت شبکه بسیار حائز اهمیت است، بنیان نهادن یک دفاع خوب برای ضعیف‌ترین لینک‌ها یک واجب عینی است.

۱–۳–۵– استراتژی ایمن از خرابی

موضوع ایمن از خرابی عبارت است از یک استراتژی امنیت مبتنی‌بر مفهـــوم (Failovers). در یک شبکه پیچیده نمی‌توان انتظار داشت که مؤلفه‌های داخلی شبکه همواره سلامت و فعال بوده باشند و لذا همیشه ایده خوبی مبنی‌بر داشتن طرح و نقشه‌ای جهت بهبود خرابی‌ها وجود داشته باشد، درون یک شبکه حتی اگر چنانچه مؤلفه‌ای با کیفیت بالا که هیچگاه خراب نگردد وجود داشته باشد، باز احتمال دارد که برق اصلی محرکه آن مؤلفه قطع شود، موضوع (Fail – Safe) چنین فرض می‌کند، مؤلفه‌ها خراب خواهند شد، اگر واقعاً آنها خراب شوند، نبایست امنیت شبکه را به خطر اندازند و نه وضعیت کاری سیستم را. بایستی در درون یک سیستم

[1] Back door

برای مؤلفه‌های عمده آن (Failover) طراحی شود. این مولفه‌ها عبارتنداز: سرورهایی که از امنیت پیرامونی استفاده می‌کنند، گیت‌وی‌های شبکه، سرویس‌های DNS و Post، پایگاه‌های داده‌ای، سرورهای کاربردی، سرورهای وب و برق.

فصل دوم– فایروال و فیلترینگ

فایروال‌ها یکی از مؤثرترین و مهمترین روش‌های افزایش " مصونیت شبکه " هستند و قادرند تا حد زیادی از دسترسی غیر مجاز دنیای بیرون به منابع داخلی جلوگیری کنند. فایروال، محلی برای ایست بازرسی بسته‌های اطلاعاتی است، به گونه‌ای که بسته‌ها براساس قواعد امنیتی و حفاظتی، کنترل شده و سپس مجوز عبور یا عدم عبور صادر می‌شود. فایروال‌ها اگر چه که از بروز مشکلات مختلف برای شبکه داخلی جلوگیری می‌کنند، اما بدون عیب و اشکال نیستند. فایروال‌ها، مانند خندق پیرامون قلعه‌های باستانی، عمل می‌کنند. خندق دور قلعه باعث می‌شود، نفوذ به قلعه مشکل باشد. با وجود خندق‌ها، افراد خرابکار ماهر همیشه قادرند با شنا یا از طریق دیگر، از خندق و سایر موانع عبور کرده و در یک فرصت مناسب وارد قلعه شوند. اما با این وجود همچنان از خندق‌ها برای حفاظت قلعه‌ها و از فایروال‌ها برای حفاظت شبکه‌های داخلی، استفاده می‌شود. با توجه به مثال، اگرچه در حالات خاصی فایروال نفوذپذیر است و خرابکاران قادرند از آن عبور کنند، اما با این حال این ابزار از عبور بسیاری از خرابکاران جلوگیری می‌کند و موثرترین ابزار در کنترل دسترسی خارجی به شبکه به محسوب می‌شود. در صورتی که هیچ خندق یا مانع دیگری وجود نداشته باشد، ورود افراد غیرمجاز به قلعه بسیار آسانتر خواهد بود و طبعاً مهمترین علت استفاده از فایروال‌ها، افزایش ضریب اطمینان و کاهش نفوذهای موفق است.

در هر حال یک فایروال قادر است در جهت بالا رفتن سطح امنیتی شبکه اقدامات مفیدی را انجام دهد. در این مستند مواردی که یک فایروال قادر است انجام دهد و به امنیت شبکه کمک کند را مورد بررسی قرار می‌دهیم و سپس به بررسی نرم‌افزارهای متن‌باز معروف در زمینه فایروال‌ها می‌پردازیم و بهترین گزینه‌ها را معرفی می‌کنیم. اگرچه بهترین نرم‌افزار فایروال بطور عام معنی نمی‌دهد و همه پارامترها نسبت به شرایط کاری سنجیده شده است.

توجه کنید که هیچ مدیر سیستم یا شبکه‌ای به سادگی و بی‌درنگ اقدام به برپایی یک فایروال بدون تحلیل کامل مجموعه و شناخت کامل فایروال نمی‌کند. از این رو شناخت انواع فایروال کمک به‌سزایی به مدیران ارشد در انتخاب و استفاده از فایروال‌ها خواهد کرد. نرم‌افزارها و یا دستگاه‌های مخصوص فایروال‌ها، معمولا هم در لایه یک دستگاه کامپیوتر به‌صورت یک برنامه نرم‌افزاری (Personal Firewall یا Host Firewall) و هم در لایه‌ی کلان یک شبکه بزرگ موجود هستند و در این مستند سعی شده به هر دو موضوع اشاره شود.

۲-۱- مفاهیم اولیه

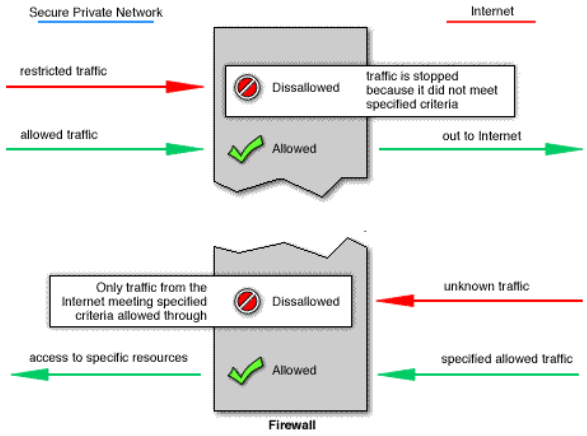
فایروال وسیله‌ای برای کنترل عبور و مرور بسته‌ها با هدف فراهم آوردن امنیت برای یک شبکه و یا حتی یک کامپیوتر شخصی است. معمولاً برای محافظت از ورود بسته‌های غیر مجاز به داخل شبکه از این سیستم استفاده می‌شود. فایروال‌ها به صورت سخت‌افزار و یا نرم‌افزار ارائه می‌گردند. مدل‌های متنوعی از این محصول وجود دارد که بر حسب اندازه شبکه و نوع کنترل‌های مورد نیاز می‌توان از آنها استفاده کرد. فایروال‌های نرم‌افزاری برای حفاظت یک کامپیوتر(فایروال شخصی) و یا یک شبکه به کار برده می‌شوند در حالیکه از فایروال‌های سخت‌افزاری برای محافظت یک شبکه استفاده می‌شود. فایروال‌ها در مدل‌های متعددی ارائه می‌شوند از یک سیستم ساده فیلتر بسته تا ابزارهای پیشرفته با قابلیت‌های مختلف نظیر ترجمه آدرس و پورت، تشخیص و جلوگیری از نفوذ، کنترل بسته از نظر وجود ویروس و کدهای مخرب و نیز امکان کنترل محتوای وب‌سایت‌ها. فایروال‌ها لزوماً برای حفاظت از شبکه‌های بزرگ استفاده نمی‌شوند و امروزه برای محافظت از کاربران خانگی که با خطوط پرسرعت به اینترنت متصل هستند نیز کاربرد دارد. فایروال‌ها برای محافظت از شبکه‌های کامپیوتری در مقابل خطرات ناشی از ضعف پروتکل TCP/IP و نیز ضعف پیاده‌سازی آنها بکار برده می‌شود.

فایروال‌ها در شکل‌های مختلفی ارائه می‌شوند؛ یک روتر مرزی سازمان با قابلیت فیلترینگ بسته‌ها نیز یک فایروال است. همان‌طور که ممکن است یک فایروال علاوه بر قابلیت فیلترینگ بسته‌ها بتواند ضعفهای متعدد پروتکل TCP/IP را نیز پوشش دهد. فایروال‌های پیشرفته محتویات بسته‌ها را نیز مورد بررسی و تحلیل قرار می‌دهند و بر اساس سیاست‌های امنیتی سازمان ممکن است بر این اساس جلوی عبور برخی از بسته‌ها گرفته شود. مثلاً می‌توان نوع فایل‌هایی را که می‌توان از طریق اینترنت دانلود کرد را محدود ساخت.

تعریف ساده: فایروال یک ابزار یا گروهی از ابزارها (نرم‌افزار/ سخت‌افزار) است که به ما کمک می‌کند سیاست‌های امنیتی برای مقابله با تهدیدهای ناشی از ترافیک شبکه را پیاده‌سازی کنیم. گذاشتن فایروال بین هر دو شبکه امکان کنترل تردد بسته‌ها بین آن دو شبکه را بوجود می‌آورد. در عمل معمولاً یکی از این شبکه‌ها، شبکه محلی سازمان و دیگری شبکه‌اینترنت است. البته یک فایروال می‌تواند چندین تردد و ترافیک شبکه مجزا را کنترل کند. هدف ما در این قسمت آن است که فایروال‌های نرم‌افزاری متن باز که امکان تبدیل‌شدن آنها به یک

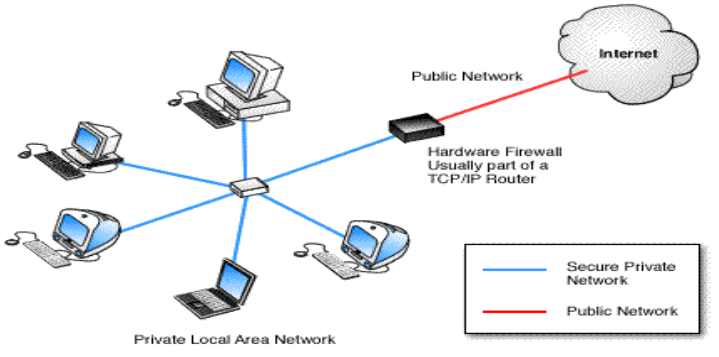
فایروال حرفه‌ای برای حفاظت یک شبکه وجود دارد را بررسی کنیم. در شکل زیر عملکرد کلی یک فایروال نشان داده شده است.

همان‌طور که در شکل ساده (۲-۱) مشخص است فایروال بسته‌ها را مورد وارسی قرار داده و بر اساس قواعد تعریف شده جلوی عبور بعضی از این بسته‌های(مخرب) را می‌گیرد.



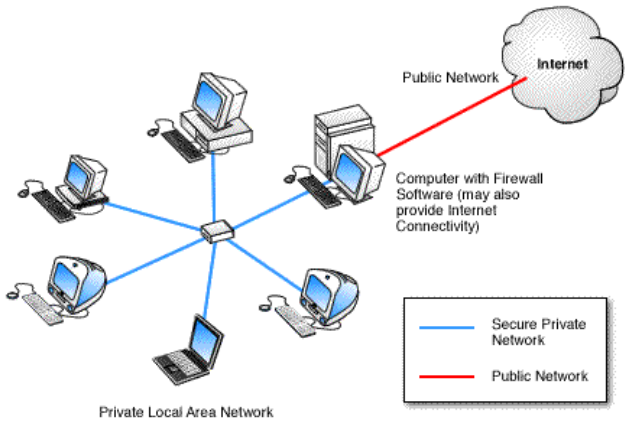
شکل ۲-۱: بررسی بسته‌های اطلاعاتی توسط فایروال

فایروال می‌تواند به صورت یک سخت‌افزار و یا یک نرم‌افزار ارائه گردد. معمولاً فایروال‌های سخت‌افزاری از قدرت، سرعت و عملکرد بهتری برخوردار هستند و این به آن علّت است که نرم‌افزار امنیتی فایروال به خوبی با سخت‌افزار مناسب تطبیق داده شده است. فایروال‌های نرم‌افزاری چون روی یک سخت‌افزار عمومی نصب می‌شوند پایداری و سرعت یک فایروال سخت‌افزاری‌را نخواهند داشت.



شکل ۲-۲: فایروال سخت‌افزاری در یک شبکه

در شکل (۲-۳) نحوه قرار گیری یک فایروال سخت‌افزاری و یک فایروال نرم‌افزاری شبکه‌ای در شکل مشخص شده است. فایروال‌های سخت‌افزاری همگی برای حفاظت یک شبکه به کاربرده می‌شوند ولی فایروال نرم‌افزاری ممکن است برای محافظت از فقط یک کامپیوتر به کار برده شود که در این حالت به آن فایروال شخصی گفته می‌شود.



شکل ۲-۳: نحوه قرار گیری یک فایروال سخت‌افزاری و یک فایروال نرم‌افزاری در یک شبکه

۲-۱-۱- تاریخچه

اگر چه تکنولوژی فایروال‌ها جوان است و به تازگی شکل گرفته، اما این تکنولوژی بسیار سریع رشد کرده و در کمتر از بیست سال تحولات زیادی را پشت سر گذاشته است.

اولین نسل از فایروال‌ها در حدود سال ۱۹۸۵ به‌وجود آمدند و فایروال‌های پالایش‌گر بسته[1] نام گرفتند. ایده اصلی آنها از امکانات نرم‌افزاری گرفته شده بود که متعلق به شرکت Cisco بود و تحت عنوان IOS (Internetworking Operation system) شناخته می‌شد. اولین مقاله در ارتباط با فرآیند غربال کردن[2] که توسط این نوع فایروال‌ها مورد استفاده قرار می‌گرفت در سال ۱۹۸۸ منتشر شد.

در سال ۱۹۸۹ آزمایشگاه شرکت AT&T برای اولین بار نسل دوم فایروال‌ها که در آینده فایروال‌ها سطح مدار[3] لقب گرفتند را به‌وجود آوردند. در همان سال آنها همچنین اولین مدل

[1] Packet filter firewalls
[2] Screening Process
[3] Circuit level firewalls

عملی[1] از نسل سوم فایروال‌ها یعنی فایروال‌های لایه کاربرد[2] را پیاده‌سازی کردند اما نه هیچ مقاله‌ای در این ارتباط منتشر شد و نه محصولی بر اساس این مدل به بازار عرضه گشت.

در اواخر سال ۱۹۸۹ و اوایل دهه ۹۰ تحقیقات مختلف و پراکنده‌ای در سطح کشور آمریکا برروی نسل سوم فایروال‌ها انجام شد و بالاخره نتایج این تحقیقات به صورت جداگانه در سال‌های ۱۹۹۰ و ۱۹۹۱ توسط Gene Spafford از دانشگاه Bill Cheswick,Purdue از لابراتوار Bell شرکت AT&T و Marcus Ranum انتشار یافتند. در سال ۱۹۹۱ تحقیقات Marcus Ranum بیشترین توجه را به خودش معطوف کرد و باعث به‌وجود آمدن Bastion hostهایی که سرویس proxy را اجرا می‌کردند شد. نتایج این تحقیقات به سرعت در اولین محصول تجاری شکل عینی یافت و به کار گرفته شد. این محصول که SEAL نام داشت توسط شرکت DEC عرضه شد.

در اواخر سال۱۹۹۱، Bill Cheswick و Steve Bellovin تحقیقاتی را در ارتباط با پالایش کردن بسته‌ها به صورت پویا (Dynamic) شروع کردند و بر این اساس محصولی داخلی را در لابراتوار Bell پیاده‌سازی کردند که البته هرگز به بیرون عرضه نشد. در سال ۱۹۹۲، Bob Barden و Annette DeSchon در مؤسسه USC's Information Science Institute تحقیقاتی را بر روی نسل چهارم فایروال‌ها تحت عنوان فایروال‌های پالایش‌گر بسته پویا[3] برای سیستمی با نام Visas به طور جداگانه شروع کردند و در نهایت نرم‌افزار Check Point، اولین محصول تجاری بر پایه معماری نسل چهارم فایروال‌ها، در سال ۱۹۹۴ به بازار عرضه شد.

در سال ۱۹۹۶، Scott Wiegel طرحی را برای نسل پنجم فایروال‌ها با عنوان Kernel Proxy ارائه داد. فایروال Cisco Centri که در سال ۱۹۹۷ پیاده سازی شد اولین محصول تجاری بر اساس معماری این نسل بود.

در سال‌های اخیر نیاز به سیستم‌های امنیتی که پرسرعت و در عین حال قابل گسترش، قابل نگهداری و انعطاف‌پذیر باشند باعث شده است شرکت‌های فعال در زمینه امنیت در تکاپوی یافتن راه حل‌هایی مناسب و کاربردی برای پاسخگویی به این نیازها باشند.

---

[1] Working Model
[2] Application layer firewalls
[3] Dynamic packet filter firewalls

۲-۱-۲- تعریف فایروال

فایروال سیستمی است بین کاربران یک شبکه محلی و یک شبکه بیرونی (مثل اینترنت) که ضمن نظارت بر دسترسی‌ها، در تمام سطوح، ورود و خروج اطلاعات را تحت نظر دارد. بر خلاف تصور عموم کاربری این نرم‌افزارها صرفاً در جهت فیلترینگ سایت‌ها نیست. برای آشنایی بیشتر با نرم‌افزارهای فایروال، آشنایی با طرز کار آنها شاید مفیدترین راه باشد.

انجمن NCSA (Network Computer Security Association) تعریف زیر را از فایروال ارائه داده است." فایروال، یک سیستم یا ترکیبی از چندین سیستم است که یک سری محدودیت را بین دو یا چند شبکه اعمال می‌کند." در واقع یک فایروال با محدود کردن دسترسی بین دو شبکه سعی می‌کند یکی را از دیگری محافظت کند. عموماً فایروال‌ها به منظور محافظت شبکه خصوصی که به یک شبکه عمومی یا مشترک متصل است به کار گرفته می‌شوند. فایروال‌ها یک نقطه محدود کننده را بین دو شبکه ایجاد می‌کند.

عملکرد فایروال‌ها را می‌توان در سه جمله خلاصه کرد:

- آنها افراد را موقع ورود در یک نقطه کاملاً کنترل شده محدود می‌سازند.
- آنها از نزدیک شدن خرابکاران به منابع داخلی جلوگیری می‌کنند.
- آنها افراد را موقع خروج در یک نقطه کاملاً کنترل شده محدود می‌سازند.

در واقع این نقطه کاملاً کنترل شده در مثال قلعه‌های باستانی همان پل متحرکی است که تنها در مواقع ورود و خروج افراد مشخص بر روی خندق قرار می‌گیرد و در دیگر موارد بسته است و در نقش درب قلعه عمل می‌کند. فایروال اغلب در نقطه‌ای که شبکه داخلی به شبکه خارجی متصل است قرار داده می‌شود. تمام ترافیکی که از سمت شبکه خارجی به شبکه داخلی وارد می‌شود و یا از شبکه داخلی به سمت شبکه خارجی، خارج می‌شود از فایروال عبور می‌کند؛ به همین علت فایروال فرصت و موقعیت مناسبی را داراست که تشخیص دهد آیا ترافیک عبوری مورد پذیرش هست یا خیر. اینکه چه ترافیکی مورد پذیرش هست به سیاست امنیتی[1] شبکه باز می‌گردد. سیاست‌های امنیتی تعیین می‌کنند که چه نوع ترافیک‌هایی مجوز ورود و یا خروج را دارا هستند.

[1] Security Policy

به طور مختصر می‌توان گفت بسته‌های TCP/IP قبل و پس از ورود به شبکه وارد فایروال می‌شوند و منتظر می‌مانند تا طبق معیارهای امنیتی خاصی پردازش شوند. حاصل این پردازش احتمال وقوع سه حالت است : ۱- اجازه عبور بسته صادر می‌شود. ۲- بسته حذف می‌شود. ۳ - بسته حذف می‌شود و پیام مناسبی به مبدا ارسال بسته فرستاده می‌شود. همان‌طور که همه جا ایست بازرسی وقت‌گیر است فایروال نیز می‌تواند به عنوان یک گلوگاه باعث بالا رفتن ترافیک، تاخیر، ازدحام و بن‌بست شود.

با تمام گفته‌های فوق در واقع می‌توان گفت یک فایروال:

- یک جداساز است.
- یک محدودساز[1] است.
- یک آنالیز کننده[2] است.

یک فایروال ممکن است مسیریابی با چند لیست کنترل دسترسی باشد؛ نرم‌افزاری که روی یک PC یا یک سیستم Unix اجرا می‌شود باشد؛ و یا یک جعبه سخت‌افزاری اختصاصی باشد.

انواع پیچیده‌تر فایروال‌ها به صورت ترکیبی از چندین سیستم و راه حل‌های Multi-computer و Multi-router پیاده‌سازی می‌شوند. شبکه‌های مختلف بسته به نیازهای امنیتی مختلف و هزینه‌ای که برای تأمین امنیت در نظر گرفته‌اند از فایروال‌ها مختلف و روش‌های پیاده‌سازی مختلف آنها استفاده می‌کنند.

۲-۱-۳- معماری TCP/IP و عملکرد فایروال

فایروال سیستمی است بین کاربران یک شبکه محلی و یک شبکه بیرونی (مثل اینترنت). از آنجا که معماری TCP/IP به صورت لایه به لایه است (شامل ۴ لایه: فیزیکی، شبکه، انتقال و کاربردی) و هر بسته برای ارسال یا دریافت باید از هر ۴ لایه عبور کند، بنابراین برای حفاظت باید فیلدهای مربوطه در هر لایه مورد بررسی قرار گیرند. بیشترین اهمیت در لایه‌های شبکه، انتقال و کاربرد است چون فیلد مربوط به لایه فیزیکی منحصر به فرد نیست و در طول مسیر عوض می‌شود، پس به یک فایروال چند لایه نیاز داریم.

---

[1] Restrictor
[2] Analyzer

سیاست امنیتی یک شبکه مجموعه‌ای از قواعد حفاظتی است که بنابر ماهیت شبکه در یکی از سه لایه فایروال تعریف می‌شوند. کارهایی که در هر لایه از فایروال انجام می‌شود عبارت است از:

- تعیین بسته‌های ممنوع (سیاه) و حذف آنها یا ارسال آنها به سیستم‌های مخصوص ردیابی (لایه اول فایروال).
- بستن برخی از پورت‌ها متعلق به برخی سرویس‌ها مثلTelnet، FTP و غیره. (لایه دوم فایروال).
- تحلیل برآیند متن یک صفحه وب یا نامه الکترونیکی یا عملکردهای مشابه (لایه سوم فایروال).

در لایه اول فیلدهای سرآیند بسته IP مورد تحلیل قرار می‌گیرد که شرح آنها در ادامه آمده است.

آدرس مبدأ: برخی از ماشین‌های داخل یا خارج شبکه حق ارسال بسته را ندارند، بنابراین بسته‌های آنها به محض ورود به فایروال حذف می‌شود.

آدرس مقصد: برخی از ماشین‌های داخل یا خارج شبکه حق دریافت بسته را ندارند، بنابراین بسته‌های آنها به محض ورود به فایروال حذف می‌شود. آدرس‌های IP غیرمجاز و مجاز برای ارسال و دریافت، توسط مدیران مشخص می‌شود.

شماره شناسایی یک دیتاگرام تکه به تکه شده: بسته‌هایی که تکه به تکه شده‌اند یا متعلق به یک دیتا گرام خاص هستند حذف می‌شوند.

زمان حیات بسته: بسته‌هایی که بیش از تعداد مشخصی مسیریاب را طی کرده‌اند حذف می‌شوند.

بقیه فیلدها: براساس صلاحدید مدیر فایروال قابل بررسی‌اند.

بهترین خصوصیت لایه اول سادگی و سرعت آن است چرا که در این لایه بسته‌ها به صورت مستقل از هم بررسی می‌شوند و نیازی به بررسی لایه‌های قبلی و بعدی نیست. به همین دلیل امروزه مسیریاب‌هایی با قابلیت انجام وظایف لایه اول فایروال عرضه شده‌اند که با دریافت بسته آنها را غربال کرده و به بسته‌های غیرمجاز اجازه عبور نمی‌دهند. با توجه به سرعت این لایه هر چه قوانین سختگیرانه‌تری برای عبور بسته‌ها از این لایه وضع شود بسته‌های مشکوک بیشتری حذف می‌شوند و حجم پردازش کمتری به لایه‌های بالاتر اعمال می‌شود.

در لایه دوم فیلدهای سرآیند لایه انتقال بررسی می‌شوند که شرح آنها در ادامه آمده است.

شماره پورت پروسه مبدأ و مقصد: با توجه به این مسئله که شماره پورت‌های استاندارد شناخته شده‌اند ممکن است مدیر فایروال بخواهد مثلاً سرویس FTP فقط برای کاربران داخل شبکه وجود داشته باشد، بنابراین فایروال بسته‌های TCP با شماره پورت ۲۰ و ۲۱ که قصد ورود یا خروج از شبکه را داشته باشند حذف می‌کند و یا پورت ۲۳ که مخصوص Telnet است اغلب بسته است. یعنی بسته‌هایی که پورت مقصدشان ۲۳ است حذف می‌شوند.

کدهای کنترلی: فایروال با بررسی این کدها به ماهیت بسته پی می‌برد و سیاست‌های لازم برای حفاظت را اعمال می‌کند. مثلاً ممکن است فایروال طوری تنظیم شده باشد که بسته‌های ورودی با SYN=1 را حذف کند. بنابراین هیچ ارتباط TCP از بیرون با شبکه برقرار نمی‌شود.

فیلد شماره ترتیب و Acknowledgement: بنابر قواعد تعریف شده توسط مدیر شبکه قابل بررسی‌اند. در این لایه فایروال با بررسی تقاضای ارتباط با لایه TCP، تقاضاهای غیرمجاز را حذف می‌کند. در این مرحله فایروال نیاز به جدولی از شماره پورت‌های غیرمجاز دارد. هر چه قوانین سخت گیرانه تری برای عبور بسته‌ها از این لایه وضع شود و پورت‌های بیشتری بسته شوند بسته‌های مشکوک بیشتری حذف می‌شوند و حجم پردازش کمتری به لایه سوم اعمال می‌شود.

در لایه سوم حفاظت براساس نوع سرویس و برنامه کاربردی صورت می‌گیرد: در این لایه برای هر برنامه کاربردی یک سری پردازش‌های مجزا صورت می‌گیرد. بنابراین در این مرحله حجم پردازش‌ها زیاد است. مثلاً فرض کنید برخی از اطلاعات پست الکترونیکی شما محرمانه است و شما نگران فاش شدن آنها هستید. در اینجا فایروال به کمک شما می‌آید و برخی آدرس‌های الکترونیکی مشکوک را بلوکه می‌کند، در متون نامه‌ها به دنبال برخی کلمات حساس می‌گردد و متون رمز گذاری شده ای که نتواند ترجمه کند را حذف می‌کند.

۲-۱-۴- توانایی‌ها و ناتوانی‌های فایروال‌ها

۲-۱-۴-۱- توانایی‌های فایروال ها

یک فایروال می‌تواند اجرای تصمیمات امنیتی را در یک نقطه متمرکز کند. همان‌طورکه‌گفته شد، فایروال یک نقطه محدود کننده بین دو شبکه است. تمام ترافیک به داخل و از خارج باید از این نقطه باریک عبور کند و راه دیگری برای عبور ترافیک وجود ندارد.

بدین‌ترتیب فایروال قابلیت اعمال کنترل شدیدی را دارا خواهد بود و می‌تواند با اعمال ابزار مختلف تأمین‌کننده امنیت در این نقطه سطح قابل قبولی از امنیت را تضمین کند. در واقع چون همه چیز در یک کانال ارتباطی قابل کنترل است می‌توان تصمیمات مختلفی را در ارتباط با امنیت شبکه گرفت و به اجرا در آوردن آنها را در یک نقطه متمرکز ساخت.

یک فایروال می‌تواند سیاست امنیتی شبکه را به اجرا در آورد. می‌دانیم سرویس‌های مختلفی در شبکه‌ها وجود دارند و با گسترش اینترنت تنوع و تعداد آنها بسیار افزایش یافته است. اغلب این سرویس‌ها ناامن هستند و هنگام استفاده و ارائه آنها باید دقت کرد. سیاست امنیتی شبکه‌های مختلف تعیین می‌کند که چه سرویس‌هایی در شبکه ارائه می‌شود و چه افرادی مجازند از این سرویس‌ها استفاده کنند. فایروال‌ها قادرند با پاسبانی و کنترل سرویس‌های مختلف تنها به سرویس‌های مجاز تعریف شده در سیاست امنیتی اجازه عبور دهند و بدین ترتیب سیاست امنیتی شبکه را به اجرا درآورند. سیاست‌های امنیتی نهایتاً به تعدادی قوانین اجرایی تبدیل می‌شوند که فایروال‌ها قادر خواهند بود تعداد زیادی از آنها را اجرا کنند. فایروال‌ها ممکن است سرویس‌های خطرناک و ناامن و را با اعمال محدودیت تنها در شبکه داخلی اجازه دهند.

سیاست‌های امنیتی مختلفی قابل اتخاذ هستند. مدیران یک شبکه ممکن است تنها به یک سیستم داخلی اجازه دهند. با دنیای بیرون در ارتباط باشد، در این صورت فایروال تنها ترافیک متعلق به آن سیستم را از خود عبور خواهد داد.

ذکر این نکته ضروری است که پیاده‌سازی‌های مختلف از فایروال‌ها توانایی‌های متفاوت در به اجرا در آوردن سیاست‌های امنیتی دارند و بنابراین با استفاده از برخی از فایروال‌ها ممکن است نتوان برخی از سیاست‌ها را به اجرا در آورد.

یک فایروال می‌تواند فعالیت‌های مهم را ثبت کند؛ توضیح این که به علت این که تمام ترافیک از فایروال عبور می‌کند، فایروال یک مکان مناسب برای ثبت مجموعه‌های مختلف از فعالیت‌هاست. به عنوان تنها نقطه دسترسی، فایروال می‌تواند ثبت کند که چه اتفاقاتی بین شبکه محافظت شده و شبکه بیرونی رخ می‌دهند. با دسته بندی این اطلاعات می‌توان به نتایج خوبی در ارتباط با استفاده از شبکه، تهاجم‌های در حال شکل‌گیری، مزاحمان و متخلفان داخلی و خارجی و غیره دست یافت.

یک فایروال قادر است سطوح مختلفی از امنیت را برای بخش‌های مختلف پیاده‌سازی کند؛ به این معنی که از فایروال‌ها گاهی برای جدا نگه داشتن یک بخش از بخش‌های دیگر استفاده می‌شود. این حالت زمانی اتفاق می‌افتد که یک بخش از شبکه بیشتر از بخش‌های دیگر حساس باشد و نیازمند امنیت بیشتری باشد. بدین ترتیب با استفاده از فایروال‌ها می‌توان بخش‌های مختلف با سطوح امنیتی مختلف را ایجاد نمود. این مسأله باعث می‌شود بروز مشکلات امنیتی نتواند تمام سرتاسر شبکه را تحت تأثیر قرار دهد و برخی بخش‌های مهمتر و حساس‌تر مصون بمانند. فایروال‌ها در مجموع قادرند شبکه را در برابر تهدیدات مختلف تا حد زیادی مورد محافظت قرار دهند، اما آنها راه حل امنیتی کامل و بدون عیبی نیستند. برخی از خطرات و مشکلات از کنترل فایروال خارج هستند و برای مقابله با آنها باید از روش‌هایی مانند ایجاد مکانیزم‌های قوی امنیت فیزیکی، " مصونیت میزبان" و آموزش کاربران و مدیران و غیره استفاده کرد.

۲-۱-۴-۲- ناتوانی‌های فایروال ها

یک فایروال نمی‌تواند شبکه و منابع آن را از خرابکاران داخلی محافظت‌کند. فایروال ممکن است بتواند از اینکه اطلاعات مفید سازمان از طریق خط ارتباطی شبکه به بیرون انتقال یابند جلوگیری کند اما هنگامی که این اطلاعات از خط ارتباطی عبور نمی‌کنند نمی‌تواند هیچ‌کاری انجام دهد. کاربری ممکن است با استفاده از یک دیسک، لوح فشرده و یا تعدادی ورقه که آنها را در کیفش قرار می‌دهد اطلاعات حساس سازمان را به بیرون انتقال دهد. در مقابله با این نوع کاربران (که ممکن است اطلاعات داخل را عمداً و یا سهواً از روی غفلت افشا کنند)، فایروال‌ها ناتوان هستند و هیچ‌کاری از دستشان ساخته نیست. برخی از افراد داخلی سطوح دسترسی بالایی را در شبکه دارا هستند و مجازند به منابع مختلف در شبکه دسترسی داشته باشند، این افراد قادر خواهند بود سخت‌افزارها را خراب کنند، نرم‌افزارها و برنامه‌های مختلف را دچار مشکل‌کنند، به طور ماهرانه‌ای برنامه‌ها را تغییر دهند، سطوح دسترسی‌ها را دستکاری کنند و... . واقعیت این است که فایروال‌ها در مقابله با این مشکلات کاری نمی‌توانند انجام دهند. یک فایروال نمی‌تواند از بروز تمام مشکلات امنیتی جلوگیری‌کند: فایروال برای مقابله با خطرات شناخته شده طراحی شده است. مدیران شبکه با شناختی که از حملات و خطرات مختلف دارند و با تصویب تعدادی قوانین و اجرای آنها توسط فایروال سعی می‌کنند از بروز آنها

جلوگیری کنند، اما روز به روز حملات و مشکلات امنیتی جدیدی به وجود می‌آیند و فایروال نمی‌تواند به طور خودکار با این خطرات مقابله کند. فایروال نیز مانند تجهیزات دیگر توسط مدیر سیستم پیکربندی می‌شود و پیرو دستوراتی است که مدیر می‌دهد. یک پیکربندی خوب تا حدودی قادر خواهد بود از خطرات جدید نیز جلوگیری‌کند. در این پیکربندی هیچ ترافیکی عبور داده نمی‌شود غیر از ترافیک مربوط به تعداد بسیار اندکی سرویس مطمئن. خرابکاران به طور مرتب راه‌های جدیدی برای نفوذ و خراب کاری پیدا می‌کنند. آنها یا از سرویس‌های مطمئن شناخته شده سوء استفاده می‌کنند و یا مشکلاتی که تا کنون برای کسی رخ نداده (و بنابراین هیچ کس راجع به آنها چیزی نمی‌داند و به همین دلیل در هیچ فایروالی در نظر گرفته نشده) را به کار می‌بندند. یک فایروال را نمی‌توان یک بار پیکربندی کرد و انتظار داشت برای همیشه شبکه را از هر خطری مورد محافظت قرار دهد.

یک فایروال معمولاً نمی‌تواند از ورود همه ویروس‌ها جلوگیری کند. اغلب فایروال‌ها بخش‌های مربوط به آدرس مبدأ و آدرس مقصد و شماره پورت مبدأ و مقصد شبکه‌های ورودی را مورد بازرسی قرار می‌دهند و به جزئیات داده توجهی ندارند. پیاده‌سازی بخش تشخیص ویروس و بررسی کامل داده بسته‌ها در فایروال‌ها زیاد منوط به مکانیزم عملکرد ویروس می‌باشد. انواع بسیار زیادی از ویروس‌ها وجود دارند و روش‌های زیادی برای آنکه ویروس خودش را در داخل داده مخفی‌کند وجود دارد. تشخیص ویروس در یک بسته تصادفی از داده‌ای که از فایروال عبور می‌کند بسیار مشکل است. برای تشخیص ویروس در بسته‌ها نیازمندی‌های زیر وجود دارد:

- تشخیص این مطلب که بخش داده بسته بخشی از یک برنامه است.
- مشخص کردن این‌که یک برنامه مجاز چگونه است و چه ویژگی‌هایی دارد.
- تشخیص این که تفاوتی بین این برنامه و مدل برنامه‌های بدون مشکل و مجاز وجود دارد و بنابراین برنامه یک ویروس است اغلب فایروال‌ها ماشین‌هایی از انواع مختلف و با فرمت‌های اجرایی مختلف را مورد محافظت قرار می‌دهند.

یک برنامه ممکن است یک برنامه کامپایل شده قابل اجرا و یا یک اسکریپت[1] باشد. علاوه بر این، بسیاری از برنامه‌ها قبل از اینکه انتقال یابند به شکل یک پکیج[2] در می‌آیند و به خوبی

[1] Script
[2] Package

فشرده سازی می‌شوند. این مسایل باعث می‌شود پیچیدگی مسأله تشخیص ویروس‌ها بالاتر رود و پیاده‌سازی آن مشکل باشد. با این همه باز هم نمی‌توان تمامی منابع دیگر انتقال ویروس‌ها را کنترل کرد. بسیاری از برنامه‌ها ممکن است از طریق مودم‌های اشخاصی که به اینترنت متصل هستند و از فایروال رد نمی‌شوند download شوند و یا با یک دیسکت از محل سکونت به شبکه داخلی سازمان انتقال یابند و ... روش عملی تر مقابله با ویروس‌ها استفاده از نرم‌افزارهای host-base virus protection است. آموزش کاربران و آگاه کردن آنها از خطرات ویروس‌ها نیز می‌تواند مؤثر باشد.

۲-۱-۵- ویژگی‌های یک فایروال قوی

مشخصه‌های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

توانایی ثبت و اخطار :ثبت وقایع یکی از مشخصه‌های بسیار مهم یک فایروال به شمار می‌شود و به مدیران شبکه این امکان را می‌دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می‌تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می‌تواند براحتی به بخش‌های مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

بازدید حجم بالایی از بسته‌های اطلاعات: یکی از تست‌های یک فایروال، توانایی آن در بازدید حجم بالایی از بسته‌های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده‌ای که یک فایروال می‌تواند کنترل کند برای شبکه‌های مختلف متفاوت است اما یک فایروال قطعا نباید به گلوگاه شبکه تحت حفاظت تبدیل شود. عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیت‌ها از طرف سرعت پردازنده و بهینه سازی کد نرم‌افزار بر کارایی فایروال تحمیل می‌شوند. عامل محدود کننده دیگر می‌تواند کارت‌های واسط (کارت شبکه) باشد که بر روی فایروال نصب می‌شوند. فایروالی که بعضی کارها مانند صدور اخطار، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم‌افزارهای دیگر می‌سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

سادگی پیکربندی: سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است. در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه‌ها می‌شود به

پیکربندی غلط فایروال بر می‌گردد. لذا پیکربندی سریع و ساده یک فایروال، امکان بروز خطا را کم می‌کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزاری که بتواند سیاست‌های امنیتی را به پیکربندی ترجمه کند، برای یک فایروال بسیار مهم است.

امنیت و افزونگی فایروال: امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند ، قطعا اجازه ورود هکرها و مهاجمان را به سایر بخش‌های شبکه نیز خواهد داد.

امنیت در دو بخش از فایروال ، تامین کننده امنیت فایروال و شبکه است:

الف- امنیت سیستم عامل فایروال: اگر نرم‌افزار فایروال بر روی سیستم عامل جداگانه ای کار می‌کند، نقاط ضعف امنیتی سیستم عامل، می‌تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و به‌روز رسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی: یک فایروال باید مکانیزم‌های امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روش‌ها می‌تواند رمزنگاری را همراه با روش‌های مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

۲-۱-۵-۱- ترجمه آدرس شبکه‌ای

NAT روشی برای پنهان کردن چهارچوب آدرس دهی شبکه‌ای است که پشت یک فایروال قرار گرفته است. با استفاده از آن می‌توان یک مدل آدرس دهی اختیاری را در پشت فایروال به کار گرفت، بدون اینکه به توانایی کاربران شبکه در اتصال به منابع آنسوی شبکه لطمه وارد شود. کاربرد اصلی NAT محدود کردن تعداد آدرس‌های IP عمومی برای اهداف اقتصادی یا امنیتی است.

در عمومی ترین حالت، NAT شبکه داخلی را با آدرس‌های خصوصی(۱۰.۰.۰.۰ تا ۱۰.۲۵۵.۲۵۵.۲۵۵، ۱۷۲.۱۶.۰.۰ تا ۱۷۲.۱۶.۲۵۵.۲۵۵ ویا ۱۹۲.۱۶۸.۰.۰ تا ۱۹۲.۱۶۸.۲۵۵.۲۵۵) آدرس دهی میکند. این آدرس‌ها که روی اینترنت غیر قابل مسیریابی هستند و تنها در یک شبکه داخلی معتبرند، در RFC 1918 لیست شده‌اند. این الگوی آدرس دهی برای کامپیوترهایی که تنها میخواهند از منابع درونی شبکه مانند سرویس دهنده‌های فایل یا چاپگر استفاده کنند، به خوبی کار می‌کند. مسیریاب‌های درون شبکه بدون هیچ

مشکلی می‌توانند بسته‌های با آدرس خصوصی را درون شبکه هدایت کنند. اما برای دسترسی به منابع روی اینترنت، این کامپیوتر باید یک آدرس IP عمومی برای برگرداندن پاسخ درخواست به آنها داشته باشند. ارتباط بین آدرس‌های غیر معتبر درونی با آدرس‌های معتبر عمومی به عهده‌ی NAT است. ترجمه آدرس شبکه‌ای (NAT)با سه روش امکان پذیر است:

- ***ترجمه ایستا***[1] : هر یک از سیستم‌های داخلی شبکه اختصاصی دارای یک آدرس متناظر و قابل مسیریابی خارجی است که به آن اختصاص داده شده است. در این روش حفظ قابلیت اعطای حقوق دسترسی تحت کنترل، به کاربران خارجی امکان پذیر است. سیستم خارجی می‌تواند به سرویس دهنده داخلی دسترسی پیدا کرده و فایروال تبدیل آدرس‌ها را (از داخل به خارج یا خارج به داخل) به عهده دارد.
- ***ترجمه پنهان***[2] : کلیه آدرس‌های IP داخلی پشت یک آدرس IP پنهان می‌شوند. ضعف اصلی این پیکربندی آن است که امکان دسترسی کاربران خارجی به منابع داخل شبکه اختصاصی وجود ندارد، زیرا همه آدرس‌های داخلی به یک آدرس تبدیل (MAP) می‌شوند. در این حالت فایروال از آدرس کانال ارتباطی خارجی خود به عنوان جایگزین آدرس همه ماشین‌های شبکه اختصاصی استفاده می‌کند. این کار باعث کاهش انعطاف پذیری سیستم می‌گردد.
- ***ترجمه آدرس درگاه***[3] : این روش با تفاوت‌هایی مشابه روش NAT پنهان است. در این روش نیازی به استفاده از آدرسIP کانال خارجی فایروال نمی‌باشد و دسترسی به منابع آن سوی فایروال به صورت انتخابی و از طریق ارسال اتصال‌های ورودی به درگاه‌های خاصی از ماشین‌های از پیش تعیین شده انجام می‌شود.

مزایای ترجمه آدرس شبکه‌ای

نیازی به پیکربندی خاص در سمت سرویس گیرنده داخلی وجود ندارد، مگر اینکه قرار بر پیکربندی مسیریابی به صورت نرمال باشد. فقط لازم است کاربران از آدرس IP دروازه ارتباطی[4] آگاه باشند.

---

[1] Static NAT
[2] Hiding NAT
[3] Port Address Translation
[4] Gateway

با استفاده از آدرس‌های خصوصی برای کامپیوترهای شبکه داخلی، وضع سیاست‌های امنیتی برای فایروال امن تر و کاراتر می‌شود. زیرا به آسانی می‌توان برای آدرس‌های IP خارجی سیاست‌های امنیتی سختگیرانه‌تری نسبت به آدرس‌های خصوصی اعمال کرد. همچنین می‌توان شرح وقایع(log) با جزئیات بیشتری برای نشست‌های تولید شده توسط IPهای خارجی ثبت کرد.

معایب ترجمه آدرس شبکه‌ای

اغلب قابلیت‌های فایروال و NAT به خوبی از هم تفکیک نمی‌شوند. فایروال یک کنترل دسترسی طبقه بندی شده برای شبکه به وجود می‌آورد و دارای حالت خرابی کاملا روشن است. فایروال‌ها برای محدود کردن ترافیک شبکه طراحی شده‌اند در حالی که NAT تنها آدرس‌ها را ترجمه میکند. در بیشتر حالات فایروال به تنهایی تمام نیازمندی‌های امنیتی شبکه را فراهم میکند.

NAT دارای "حالت عدم موفقیت[1] دقیقاً تعریف شده‌ای نیست. اگر دستگاهی نادرست پیکره بندی شده باشد یا به طور غیر قابل پیش بینی از کار بیفتد، هیچ تضمینی وجود ندارد که میزبان‌های داخلی در دسترس مهاجمین خارجی نباشند. همچنین با داشتن آدرس MAC میزبان نهایی، NAT بدون هیچ سوالی بسته را ارسال میکند.

بر خلاف باور عمومی، NAT الزاماً هویت میزبان‌های پشت خودش را پنهان نمیکند. با تحلیل غیر فعال[2] پروتکل‌های TCP/IP و لایه کاربرد، بدست آوردن اطلاعات با جزئیات زیاد از شبکه داخلی ممکن است. اختلاف در مقدار اولیه شماره ترتیب در سرآیند TCP، انتخاب‌های IP و شناسه‌های IP (IP IDs) برای شمردن میزبان‌های درون شبکه بیش از حد کافیست!

ازآنجا که NAT تنها در لایه IP کار میکند، کاربر می‌تواند از بسته‌های با طول عمر(TTL) کم استفاده کند و اطلاعات کافی درباره معماری و زیرساخت‌های شبکه داخلی به دست آورد.

به جز گزینه " Allow This Type of Traffic" گزینه امنیتی دیگری وجود ندارد. درصورتی که سرویس گیرنده‌ای از طریق یک پروتکل مجاز ارتباط برقرار کرد، هر کاری در

[1] Failure Mode
[2] Passive

چهارچوب پروتکل امکان پذیر است. روشی برای استفاده از پروتکل‌های خاص که از تکنیک بازگشت اتصال استفاده می‌کنند وجود ندارد.

اثرات جانبی

جدا از مشکلات امنیتی، استفاده از NAT محدودیت‌هایی برای شبکه به وجود می‌آورد. بخشی از این محدودیت‌ها عبارتند از:

عیب یابی و تحقیق در باره‌ی حوادث امنیتی در شبکه را دشوارتر می‌کند. زیرا تعداد متعددی میزبان از یک آدرس IP عمومی استفاده میکنند و برنامه‌ای مثل UMNet's Hackfinder که از سرآیند بسته‌ها در روترهای مرزی برای کشف حمله استفاده میکند، از کار میافتد.

راه حل "Port forwarding" که برای ارتباط دو میزبان که هر دو پشت NAT قرار دارند به کار میرود، محدودیت‌هایی به وجود می‌آورد. مثلاً به ازای پورت‌های معروف مانند (Web)80، در کل شبکه تنها یک سرویس می‌توان قرار داد که به وضوح انعطاف پذیری شبکه را کاهش می‌دهد.

پروتکل‌های دوطرفه مثل FTP , IRC و SSH بدون پیاده سازی صریح در NAT قابل اجرا نیستند.

NAT گزینه‌های پیکره بندی VPNرا به شدت کاهش می‌دهد. مثلاً برای استفاده تنها بخشی از شبکه از VPN باید از نوع خاصی از NAT به نام (NAT traversal) NAT-T استفاده کرد.

به طور خلاصه، باید توجه داشت که NAT علاوه بر محدودیت‌هایی که به وجود می‌آورد، به هیچ وجه نیازهای امنیتی شبکه را برآورده نمیکند و استفاده از آن بدون فایروال توصیه نمی‌شود.

۲-۱-۵-۲- مدیریت‌ومونیتورینگ

باید بپذیریم که حتی بهترین فایروال‌ها و سیستم‌های امنیتی در معرض مشکلات و ضعف-های امنیتی هستند. چیزی به اسم شبکه کامل امن وجود ندارد. ضعیف‌ترین حلقه امنیتی در هر راهکار امنیتی، انسان‌هایی هستند که مسئولیت تنظیم و مدیریت سیستم با آنهاست. حلقه ضعیف بعدی عدم پیکربندی صحیح تجهیزات است. سادگی در مدیریت سیستم از اصول است

چرا که پیچیدگی زیاد خود باعث بروز مشکلات امنیتی می‌شود. به عنوان مثال اگر شما مجبور باشید برای کنترل یک ترافیک بیش از ۱۰ دستور مختلف را اجرا کنید به زودی فایروال شما لبریز از قوانین مختلفی خواهد شد که درک آن برای هر متخصص امنیت سخت و غیرممکن می‌شود. چنین وضعیتی نهایتاً منجر به فراموش کردن برخی نکات مهم در پیکربندی خواهد شد. سیستم مدیریت فایروال باید دارای ساختار لایه‌ای مناسب باشد و لذا روش‌های گوناگون کار سیاست‌گذاری را ساده و قابل فهم کند.

۲-۲- انواع فایروال ها

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم، انجام می‌دهند، اما روش انجام کار توسط انواع مختلف، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می‌شود. بر این اساس فایروال‌ها را به ۵ گروه تقسیم می‌کنند.

۲-۲-۱- فایروال‌های سطح مدار

این فایروال‌ها به عنوان یک تکرار کننده برای ارتباطات TCP عمل می‌کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می‌کنند و خود به جای آن رایانه به پاسخگویی اولیه می‌پردازند. تنها پس از برقراری ارتباط است که اجازه می‌دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته‌های داده‌ای مرتبط اجازه عبور می‌دهند. این نوع از فایروال‌ها هیچ داده درون بسته‌های اطلاعات را مورد بررسی قرار نمی‌دهند و لذا سرعت خوبی دارند. ضمناً امکان ایجاد محدودیت بر روی سایر پروتکل‌ها (غیر از TCP) را نیز نمی‌دهند.

۲-۲-۲- فایروال‌های پروکسی سرور

فایروال‌های پروکسی سرور به بررسی بسته‌های اطلاعات در لایه کاربرد می‌پردازند. یک پروکسی سرور درخواست ارائه شده توسط برنامه‌های کاربردی پشتش را قطع می‌کند و خود به جای آنها درخواست را ارسال می‌کند. نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه‌های کاربردی ارسال می‌کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه‌های کاربردی خارجی امنیت بالایی را تأمین می‌کند. از آنجایی که این فایروال‌ها پروتکل‌های سطح کاربرد را می‌شناسند، لذا می‌توانند بر مبنای این پروتکل‌ها محدودیت‌هایی را ایجاد کنند. همچنین آنها می‌توانند با بررسی محتوای بسته‌های داده‌ای به ایجاد محدودیت‌های

لازم بپردازند. البته این سطح بررسی می‌تواند به کندی این فایروال‌ها بیانجامد. همچنین از آنجایی که این فایروال‌ها باید ترافیک ورودی و اطلاعات برنامه‌های کاربردی کاربر انتهایی را پردازش کنند، کارایی آنها بیشتر کاهش می‌یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتواند این فایروال‌ها را به کار بگیرد. هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد.

۲-۲-۳- فیلترهای Nonstateful Packet

این فیلترها روش کار ساده‌ای دارند. آنها بر مسیر یک شبکه می‌نشینند و با استفاده از مجموعه‌ای از قواعد، به بعضی بسته‌ها اجازه عبور می‌دهند و بعضی دیگر را بلوکه می‌کنند. این تصمیم‌ها با توجه به اطلاعات آدرس دهی موجود در پروتکل‌های لایه شبکه مانند IP و در بعضی موارد با توجه به اطلاعات موجود در پروتکل‌های لایه انتقال مانند سرآیندهای TCP و UDP اتخاذ می‌شود. این فیلترها زمانی می‌توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویس‌های مورد نیاز شبکه جهت محافظت داشته باشند. همچنین این فیلترها می‌توانند سریع باشند چون همانند پروکسی‌ها عمل نمی‌کنند و اطلاعاتی درباره پروتکل‌های لایه کاربرد ندارند.

۲-۲-۴- فیلترهای Stateful Packet

این فیلترها بسیار باهوش تر از فیلترهای ساده هستند. آنها تقریباً تمامی ترافیک ورودی را بلوکه می‌کنند اما می‌توانند به ماشین‌های پشتشان اجازه بدهند تا به پاسخگویی بپردازند. آنها این کار را با نگهداری رکورد اتصالاتی که ماشین‌های پشتشان در لایه انتقال ایجاد می‌کنند، انجام می‌دهند. این فیلترها، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه‌های مدرن هستند. این فیلترها می‌توانند ردپای اطلاعات مختلف را از طریق بسته‌هایی که در حال عبور هستند، ثبت کنند. برای مثال شماره پورت‌های TCP و UDP مبدا و مقصد، شماره ترتیب TCP و پرچم‌های TCP. بسیاری از فیلترهای جدید Stateful می‌توانند پروتکل‌های لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می‌توانند اعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکل‌ها انجام دهند.

۲-۲-۵- فایروال‌های شخصی

فایروال‌های شخصی، فایروال‌هایی هستند که بر روی رایانه‌های شخصی نصب می‌شوند. آنها برای مقابله با حملات شبکه‌ای طراحی شده‌اند. معمولاً از برنامه‌های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط این برنامه‌ها اجازه می‌دهند که به کار بپردازند. نصب یک فایروال شخصی بر روی یک PC بسیار مفید است زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می‌دهد. از طرف دیگر از آنجایی که امروزه بسیاری از حملات از درون شبکه حفاظت شده انجام می‌شوند، فایروال شبکه نمی‌تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفید خواهد بود. معمولا نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست.

۲-۲-۶- انواع فایروال‌های مرسوم در بازار

۲-۲-۶-۱- فایروال‌های سخت‌افزاری

فایروال‌های سخت‌افزاری عبارتند از یک کامپیوتر ویژه به همراه مجموعه‌ای از برنامه‌های نهفته که قابلیت‌های متنوع و کاربردی را به همراه یک یا چند واسط کاربری ارائه می‌دهند. دستگاه‌های سخت‌افزاری ویژه برای فایروال معمولاً در داخل خود یا از برنامه‌های متن‌باز استفاده می‌کنند و یا دارای برنامه‌های ویژه و متن بسته مخصوص به خود هستند. در هر دو صورت، دستگاه کامپیوتر مورد استفاده، معمولاً یک کامپیوتر ساده است که جهت تامین نیازهای نرم‌افزاری بهینه شده است و سخت‌افزار بدون استفاده (مانند کارت گرافیک) در آنها وجود ندارد. در بسیاری موارد این کامپیوترها به لحاظ ساختارهای داخلی آنچنان اختلاف چندانی با یک کامپیوتر معمولی ندارند، ولی این دستگاه‌ها معمولاً طول عمر کارکرد طولانی‌تری نسبت به سایر کامپیوترهای عمومی و موجود در بازار دارند و عموماً قطعات الکترونیکی و فیزیکی که در کامپیوترهای معمولی بیشتر در معرض آسیب و خرابی هستند (مانند دیسک سخت) در این دستگاه‌ها کمتر به چشم می‌خورد و از تکنیک‌های مشابه که طول عمر بیشتری دارند (مانند Flash)، برای جایگزین کردن قطعات آسیب پذیر، استفاده می‌شود.

معمولاً در کاربردهای شبکه که احتیاج به محاسبات ریاضی و مقایسه فراوان وجود دارد، از پردازنده‌های RISC استفاده می‌شود. این پردازنده‌ها، سرعت محاسبات ریاضی و مقایسه بسیار سریع‌تری نسبت به پردازنده‌های همه منظوره CISC دارند و بسیار ساده‌تر و ارزانتر از سری

CISC هستند، از این رو کلاً این پردازنده‌ها برای کاربردهای خاص مانند یک دستگاه مسیریاب یا فایروال بسیار مناسب می‌باشند.

در بعضی از فایروال‌های سخت‌افزاری از نرم‌افزارهای متن‌باز استفاده می‌شود. نرم‌افزارهای متن‌باز مورد استفاده در فایروال‌های سخت‌افزاری، غالباً برنامه‌هایی هستند که در کامپیوترهای معمولی هم قابل استفاده هستند و تعدادی از این برنامه‌ها در قسمت‌های آتی معرفی شده‌اند. با ترکیب این برنامه‌ها و سخت‌افزار مناسب می‌توان فایروال‌های سخت‌افزاری تولید کرد. اگرچه استفاده از کامپیوترهای معمولی به جای دستگاه‌های تعبیه شده با پذیرفتن ضریب خطای سخت‌افزاری نسبتاً بالا و صرف هزینه سخت‌افزار گرانتر همراه است، ولی در صورت انتخاب اصولی و کارشناسانه متخصصین سخت‌افزار، این کامپیوترها به همراه نرم‌افزارهای مناسب می‌توانند تنها جایگزین برای فایروال‌ها سخت‌افزاری گران قیمت و متن‌بسته خارجی باشند.

۲-۲-۶-۲- فایروال‌های نرم‌افزاری متن باز

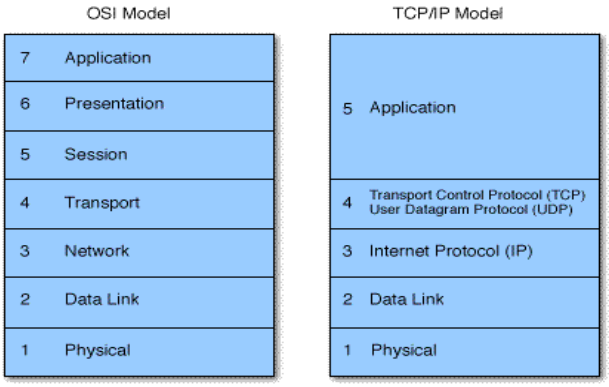
معمولاً تولید کنندگان فایروال‌ها، عمدتاً محصولات خود را به‌صورت یک سیستم‌کامل (Appliance) ارائه می‌کنند و از نرم‌افزارهای مخصوص استفاده می‌کنند، ولی همان‌طور که گفته شد، در بعضی از فایروال‌ها تجاری منجمله فایروال‌های سخت‌افزاری، از برنامه‌های متن‌باز استفاده می‌شود. معروفترین و شناخته شده‌ترین برنامه‌هایی که برای تولید فایروال‌ها در سطح جهانی استفاده می‌شوند عبارتند از iptables، ipchains، ipfwadm، ipfilter، pf و ipfw . این برنامه‌ها عمدتاً در داخل سیستم‌عامل‌های متن‌باز وجود دارند و در برخی موارد جزئی از بدنه خود سیستم‌عامل محسوب می‌شوند، از این رو استفاده صحیح از این برنامه‌ها مستلزم شناخت کامل خود سیستم‌عامل نیز می‌شود.

برنامه‌های ذکر شده فوق در سیستم‌عامل‌ها، عمدتا جزو ابزارهای عمومی کنترل و تنظیم بسته‌های IP شبکه و تولید فایروال محسوب می‌شوند و در فعالیت و اعمال تنظیم‌های متنوع مانند فیلتر کردن و حذف کردن بسته‌های IP، ایجاد تغییرهای گوناگون در اطلاعات سرآمد بسته IP و بسیاری موارد دیگر که به تفصیل در ادامه آمده است، کاربرد دارند. با توجه به اینکه این برنامه‌ها همگی تنظیم‌پذیر هستند و به طور عمومی برای کنترل و مدیریت قدرتمند بسته‌هایIP طراحی شده‌اند، با تنظیم صحیح این برنامه‌ها، می‌توان از آنها به عنوان فایروال‌های گوناگون و متنوع برای خود کامپیوتر یا شبکه استفاده کرد. برای مثال با قرار دادن یک

کامپیوتر با دو کارت شبکه به صورت Bridge در مسیر اصلی اطلاعات کل شبکه و با تنظیم صحیح این برنامه‌ها و حذف ترافیک و نفوذهای ناخواسته و رعایت سایر موارد ضروری دیگر، می‌توان از آن کامپیوتر به عنوان یک فایروال برای کل شبکه استفاده کرد.

۲-۲-۷- انواع فایروال‌ها براساس لایه شبکه کنترل کننده بسته

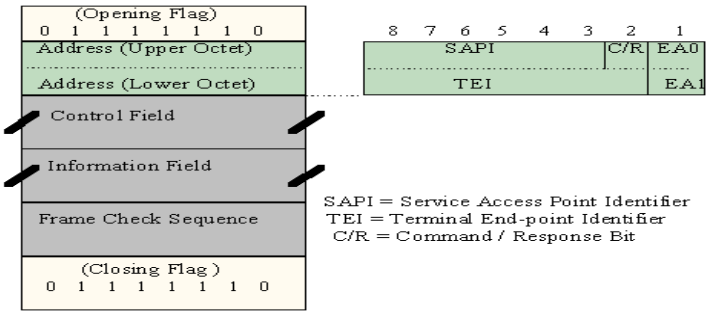
بسته به اینکه عمل کنترل بسته در کدام لایه شبکه انجام شود فایروال‌ها را به دسته‌های مختلفی تقسیم می‌کنند.(در شکل (۲-۴) تطابق لایه‌های پروتکل TCP/IP و OSI نشان‌داده‌شده‌است.)



شکل ۲-۴: تطابق لایه‌های پروتکل TCP/IP و OSI

۲-۲-۷-۱- فایروال در سطح فریم

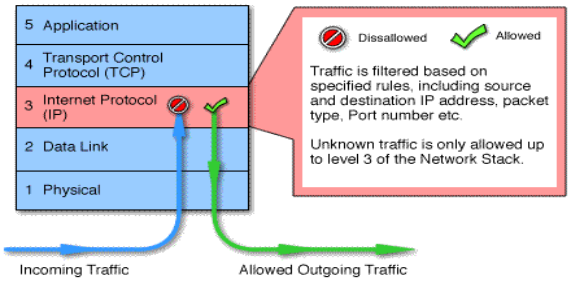
سیستمی که قادر باشد عملیات کنترل عبور و مرور فریم‌ها در لایه دسترسی را انجام دهد یک فایروال لایه ۲ است. به عنوان مثال بعضی از سوئیچ‌های شبکه در این دسته قرار می‌گیرند. در اینجا بر اساس پارامترهای یک فریم نظیر آدرس فرستنده، آدرس گیرنده، نوع پروتکل حمل شونده و.... کنترل‌هایی انجام می‌شود. اکثر فایروال‌های تجاری فاقد امکانات کامل برای کنترل فیلدهای یک فریم هستند. معمولاً فقط امکان فیلترکردن بر اساس آدرس MAC در فایروال قرار داده می‌شود.



شکل ۲-۵: فایروال در سطح فریم

۲-۲-۷-۲- فایروال در سطح بسته

عمومی‌ترین شکل فایروال نوع صافی بسته است این نوع فایروال‌ها اساساً یک روتر هستند. این فایروال‌ها عموماً در لایه سه (لایه شبکه) عمل می‌کنند (و گاهاً در لایه۴). در شکل(۲-۶) لایه‌هایی که این فایروال‌ها در آن عمل می‌کنند، نشان داده شده است. روترهای سیسکو با قابلیت تعریف ACL بارزترین مثال یک فایروال صافی بسته هستند.



شکل ۲-۶: فایروال در سطح بسته

چون یک فایروال صافی بسته در لایه شبکه عمل می‌کند بنابراین می‌تواند بر اساس فیلدهای زیر عمل کنترل و بازرسی بسته را انجام دهد: آدرس فرستنده، آدرس گیرنده، نوع پروتکل فیلدهای خاص مربوط به پروتکل مثلاً شماره پورت در پروتکل TCP یا نوع بسته ICMP. یک فایروال صافی بسته از یک یا چند لیست از قوانین برای کنترل تردد بسته‌های شبکه استفاده می‌کند. معمولاً مجموعه این قوانین در محل ورود یا خروج بسته یعنی بر روی اینترفیس‌ها فعال می‌شود.

چون این گونه فایروال‌ها فقط سرآیند بسته را مورد بررسی و پردازش قرار می‌دهند از سرعت بالایی برخوردار هستند. با توجه به خصوصیات اینگونه فایروال‌ها، معمولاً آنها را در مرز یک شبکه مورد استفاده قرار می‌دهند.

معایب فایروال‌های صافی بسته

چون این فایروال‌ها فقط در لایه سه و چهار عمل می‌کنند محدودیت‌ها و نواقص زیر در آنها وجود دارد.

اینگونه فایروال‌ها نمی‌توانند جلوی تهدیدها و مشکلات لایه کاربرد را بگیرند. چون این فایروال‌ها اصلاً محتویات بسته را مورد وارسی قرار نمی‌دهند نمی‌توانند داده‌های خامی که مربوط به برنامه‌های کاربردی است را پردازش و جلوی خطرات احتمالی را بگیرند. مثلاً نمی‌توانند جلوی ویروس‌ها، کرم‌های اینترنتی و یا فایل‌های مخرب را بگیرند.

چون این فایروال‌ها در سطح لایه کاربرد عمل نمی‌کنند نمی‌توان عملیات احراز هویت کاربر را در آنها انجام داد. احراز هویت کاربر به فایروال اجازه می‌دهد تا با نشان دادن یک Prompt از کاربر نام شناسه و رمز عبور را بپرسد. عدم وجود مکانیزم احراز هویت به این معنی است که تنها راه اعمال سیاست بر اساس آدرس فرستنده است که به راحتی قابل جعل است.

تنها فیلدهایی که این فایروال با آن سرو کار دارد فیلدهای پروتکل IP است و بنابراین نمی‌توانند اطلاعات مفید دیگری ثبت و برای آنالیز بعدی در اختیار قرار دهد.

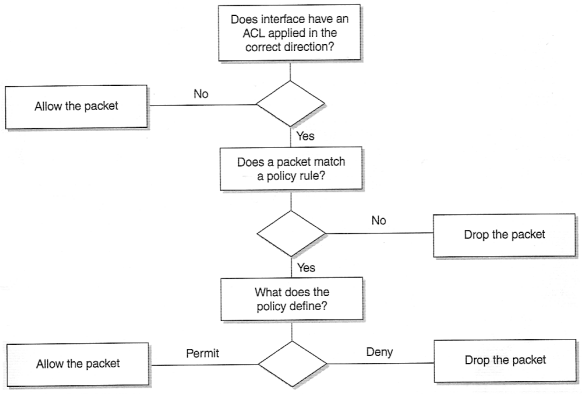
پروتکل TCP/IP به طور ذاتی نواقص و مشکلات امنیتی با خود دارد که یک فایروال لایه سه و چهار نمی‌تواند آن نواقص را پوشش دهد. مثلاً یکی از این نواقص ip spoofing یا جعل IP است که باعث می‌شود مهاجم بتواند از طریق تغییر آدرس خود فایروال را دور بزند. مثال دیگر حمله syn Flooding است که یک فایروال لایه سه نمی‌تواند در مقابل این حمله کاری انجام دهد.

معمولاً فایروال‌های صافی بسته فاقد ابزارهای مناسب برای پیکربندی آسان هستند حداکثر تنظیمات از طریق خط فرمان صورت می‌گیرد. در صورتی که تعداد قوانین از حد معینی تجاوز کند مدیریت فایروال بسیار سخت می‌شود.

با توجه به نواقص مطرح شده، معمولاً نمی‌تواند صرفاً با تکیه بر یک فایروال صافی بسته امنیت شبکه را تامین کرد.

مکانیزم فیلترینگ در فایروال صافی بسته

فرایند فیلترینگ بسته در فایروال صافی بسته بسیار ساده است (شکل۲-۷). اولین قدم آن است که آیا در اینترفیس ورودی/ خروجی فیلتری وجود دارد یا خیر؟ اگر بسته‌ای در حال خروج از اینترفیس باشد و فیلتری برای بسته‌های خروجی وجود نداشته باشد و یا در هنگام ورود بسته اگر فیلتری برای ورود بسته‌ها نداشته باشیم بسته بدون تغییر عبور داده می‌شود. اگر بر روی اینترفیس فیلتری تعریف شده باشد، در قدم دوم قوانین آن فیلتر با فیلترهای بسته مطابقت داده می‌شوند در صورتی که بسته با یکی از آن قوانین تطبیق داشته باشد طبقه دستور آن قاعده با بسته برخورد می‌شود (طبق سیاست تعریف شده).



شکل ۲-۷: فرایند فیلترینگ بسته در فایروال صافی

روش تطبیق بسته با قوانین در فایروال‌های مختلف فرق می‌کند. در برخی از آنها قوانین به ترتیب بررسی می‌شوند(مثلاً فایروال لینوکس) و برخی دیگر دقیق‌ترین حالت تطابق مورد استفاده قرار می‌گیرد(فایروال BSD). شکل (۲-۸) مثالی از از جدول قوانین است.

action	src	port	dest	port	flags	comment
allow	*	*	MAILGATE	25		inbound mail access
allow	*	*	MAILGATE	53	UDP	access to our DNS
allow	SECONDARY	*	MAILGATE	53		secondary nameserver access
allow	*	*	MAILGATE	23		incoming telnet access
allow	NTP.OUTSIDE	123	NTP.INSIDE	123	UDP	external time source
allow	INSIDE-NET	*	*	*		outgoing TCP packets are OK
allow	*	*	INSIDE-NET	*	ACK	return ACK packets are OK
block	*	*	*	*		nothing else is OK
block	*	*	*	*	UDP	block other UDP, too

Figure 9.6: Some filtering rules for a small company. Rules without explicit protocol flags refer to TCP.

شکل ۲-۸: مثالی از قوانین تطبیق بسته

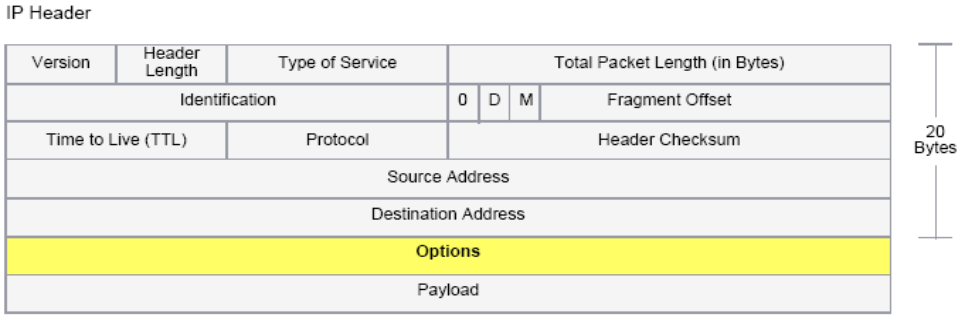
اگر بسته با هیچکدام از قواعد تعریف شده تطبیق نداشت، طبق سیاست کلی فایروال با آن برخورد می‌شود. در اکثر فایروال‌ها سیاست کلی، Drop کردن بسته است. می‌توان فرض کرد خط زیر در انتهای تمامی جداول موجود است.

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	*default*

شکل ۲-۹: خط انتهای تمامی جداول تطبیق بسته

در شکل (۲-۱۰) فیلدهای یک بسته ip نشان داده شده است. یک فایروال صافی بسته ایده‌ال باید روی تمامی این فیلدها کنترل داشته باشد. متاسفانه اکثر این‌گونه فایروال‌ها این امکان را ندارند و تنها امکان کنترل و نظارت بر بعضی از فیلدها توسط آنها وجود دارد.

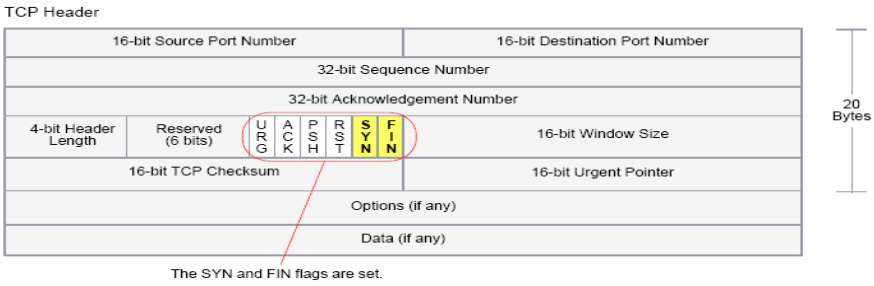
در قسمت بعد بعضی از حملات شناخته شده لایه ip مورد بررسی قرار گرفته‌اند. در صورتیکه یک فایروال بتواند روی تمامی فیلدهای یک بسته ip کنترل و نظارت داشته باشد جلوی خیلی از این حملات را می‌توان گرفت. متاسفانه اکثر فایروال‌های بسته‌صافی فقط روی بعضی از فیلدهای ip امکان کنترل و نظارت دارند.



شکل ۲-۱۰: فیلدهای یک بسته IP

علاوه بر فیلدهای بسته ip یک فایروال بسته‌صافی باید بتواند روی فیلدهای مربوط به پروتکل‌های سطح بالاتر نظیر TCP و UDP نیز کنترل و نظارت داشته باشد. در شکل(۲-۱۱) ساختار یک بسته TCP نشان داده شده است. معمولاً فایروال‌های صافی بسته قادر نیستند روی تمام فیلدهای خاص این پروتکل کنترل و نظارت داشته باشند.

به عنوان یک مثال در نوعی از حملات مربوط به پویش شبکه پرچم‌های FIN, SYN هر دو روشن هستند. این حالت غیر طبیعی و نادرست است. یک فایروال بسته‌صافی باید قادر باشد این مسئله را تشخیص داده و جلوی عبور بسته را بگیرد.

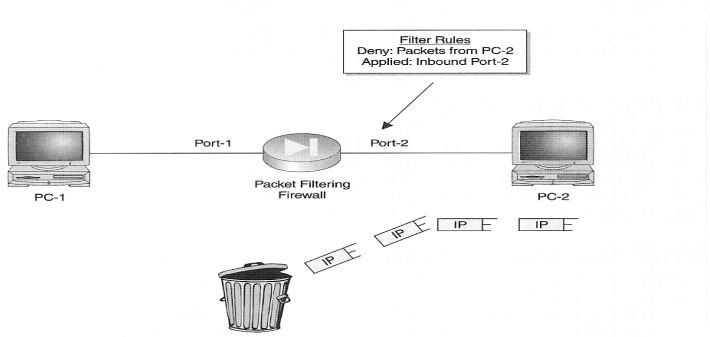


شکل ۲-۱۱: ست بودن پرچمهای FIN, SYN در یک بسته IP

۲-۲-۷-۳- فایروال حالتمند

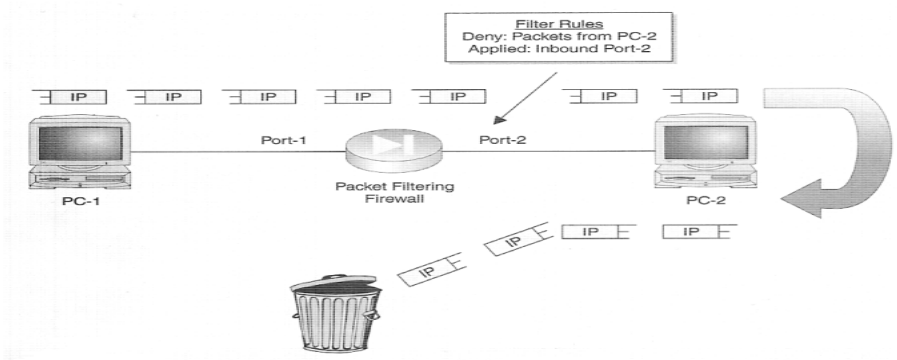
عملکرد این فایروال بسیار شبیه فایروال صافی بسته است و مثل این فایروال در لایه ۳ و ۴ عمل می‌کند. با این تفاوت که بر خلاف فایروال صافی بسته که هر بسته را مستقل از بسته بعدی پردازش می‌کند، این گونه فایروال‌ها در جدولی وضعیت هر اتصال یا نشست را مثبت کرده و به نوعی روی جریان اتصال عمل می‌کنند به جای آنکه هر بسته را مستقلاً مورد بررسی قرار دهند.

تفاوت اصلی عملکرد فایروال حالتمند با فایروال صافی بسته، آن است که این نوع فایروال‌ها وضعیت اتصال‌های برقرارشده را در خود نگاهداری می‌کنند. یک فایروال صافی بسته در هنگام بررسی یک بسته به هیچوجه به این مسئله فکر نمی‌کند که آیا این بسته به بسته‌های قبلی این اتصال ربط دارد یا خیر.



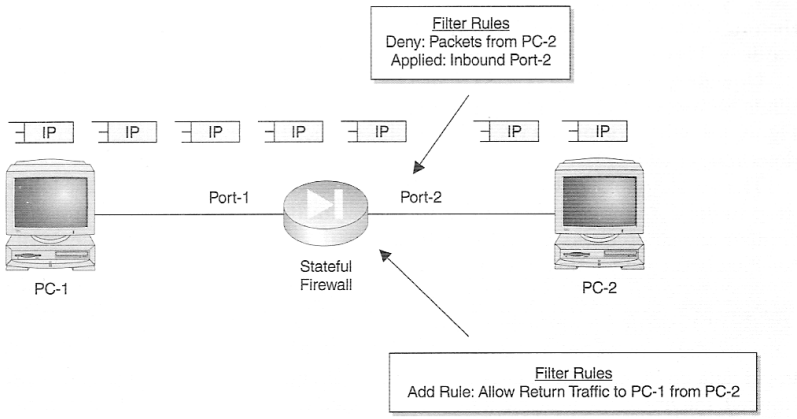
شکل ۲-۱۲: تعریف ارتباط در فایروال (اجازه ارتباط PC1 با PC2 و عدم اجازه ارتباط به PC2)

فرض کنید می‌خواهیم به PC1 اجازه دهیم با PC2 ارتباط برقرار کند ولی نمی‌خواهیم PC2 توانایی برقراری ارتباط را داشته باشد. در یک فایروال صافی بسته این کار به آسانی امکان‌پذیر نیست. ما باید قانونی وضع کنیم که اگر در بسته‌ای، آدرس مبدا آن PC2 بود آن بسته Block شود متاسفانه این کار باعث می‌شود که حتی PC1 نیز دیگر نتواند به PC2 ارتباط برقرار کند چون با Block کردن بسته‌های با مبدا PC2 عملاً امکان دریافت جواب بسته‌ها توسط PC1 نیز از بین خواهد گرفت.

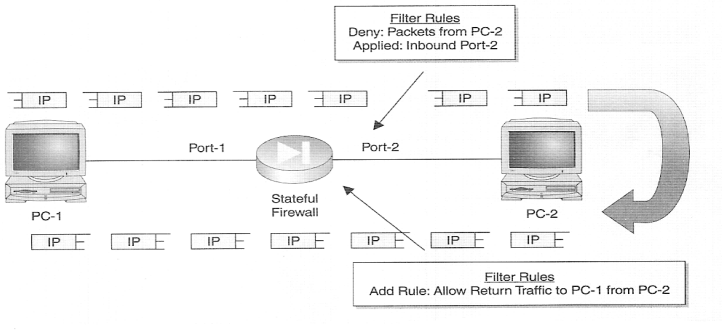


شکل ۲-۱۳: تعریف ارتباط در فایروال (عدم ارتباط با PC2 به علت نادرست بودن قوانین)

همین مثال را در فایروال حالتمند در نظر بگیرید: هنگامیکه بسته‌ای از PC1 به PC2 ارسال شد به طور اتوماتیک امکان برگشت جواب آن بسته نیز به وجود می‌آید. یعنی ارتباط PC1 با PC2 با وجود آنکه همان قانون فوق را روی اینترفیس اعمال کرده‌ایم، برقرار خواهد شد. در این حال اگر PC2 بخواهد شروع کننده یک اتصال جدید باشد چون در فایروال حالتمند، وضعیتی برای این اتصال وجود ندارد و با توجه به قانونی را تمام بسته‌های با آدرس فرستنده PC2 را block می‌کند، این ارتباط ناموفق خواهد بود.

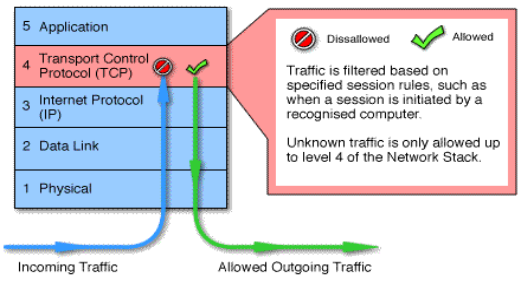


شکل ۲-۱۴: تعریف ارتباط در فایروال حالتمند (اجازه ارتباط PC1 با PC2 و عدم اجازه ارتباط به PC2)



شکل ۲-۱۵: تعریف ارتباط در فایروال حالتمند (برقراری ارتباط)

فایروال حالتمند به این دلیل قادر است این کار را انجام دهد که وضعیت اتصالها را در خود نگهداری می‌کند.



شکل ۲-۱۶: نگهداری وضعیت اتصالها در فایروال حالتمند

بحث نگهداری حالت در پروتکل‌های مختلف فرق می‌کند. در این قسمت به بررسی حالت‌های مختلف یک اتصال TCP پرداخته شده است. طبیعی است که یک فایروال حالتمند باید قادر باشد تمامی این حالت‌ها را بشناسد. بعضی از حملات نظیر حمله SYN FLOOD توسط فایروال‌های حالتمند قابل تشخیص است. در این حمله تعداد زیادی اتصال TCP در وضعیت SYN SENT و یا SYN RCVD به وجود می‌آید (در حالت طبیعی یک اتصال TCP بلافاصله از این حالت به حالت ESTABLISHED می‌رود) در این حالت فایروال حالتمند با تشخیص این حالت غیر طبیعی جلوی عبور بسته‌های مخرب را می‌گیرد.

حالت در بسته‌های TCP

CLOSED: حالت بدون وضعیتی است که قبل از ایجاد اتصال وجود دارد.

LISTEN: یک ماشین منتظر دریافت بسته و تشکیل یک اتصال جدید از طرف دیگر است.

SYN SENT: کسیکه می‌خواهد با یک نفر دیگر ارتباط TCP برقرار کند ابتدا یک بسته SYN به سمت نفر دیگر ارسال می‌کند بعد از ارسال بسته SYN به حالت SYN SENT می‌رود.

SYN-RCVD: ماشین دوم بعد از دریافت بسته SYN به این حالت می‌رود.

ESTABLISHED: بعد از اتمام مذاکره برای ایجاد اتصال و رد و بدل شدن ACKها اتصال به این حالت خواهد رفت.

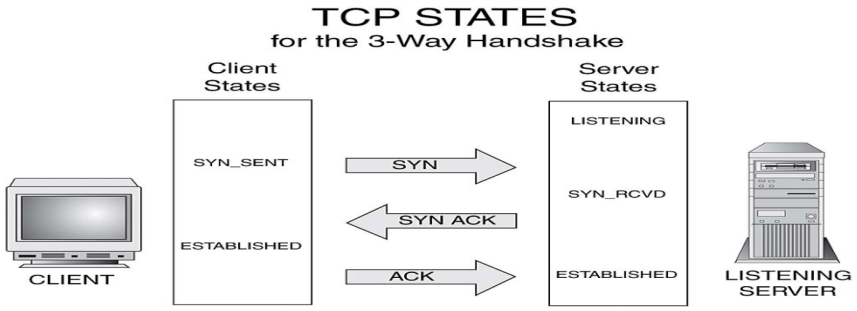
CLOSE-WAIT: بعد از دریافت بسته FIN و ارسال ACK اتصال به این حالت خواهد رفت.

FIN-WAIT : کسیکه یک بسته FIN به طرف دیگر ارسال کرده و ACK آن را هم دریافت کرده در این حالت خواهد بود.

LAST ACK: وضعیت ماشینی است که آخرین FIN را برای ختم اتصال به نفریکه اولین FIN را فرستاده است می‌فرستد و منتظر دریافت ACK نهایی از آن خواهد بود.

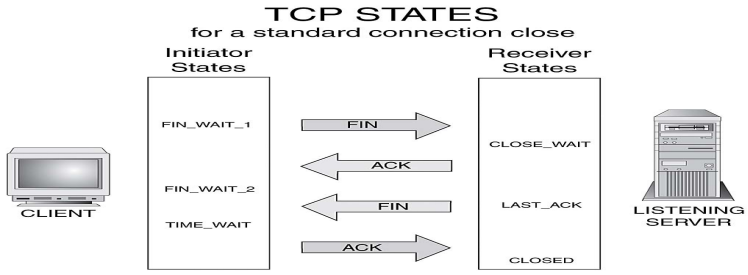
TIME-WAIT: وضعیت ماشینی است که آخرین FIN را برای ختم اتصال دریافت کرده و ACK آن را ارسال نموده است. چون مطمئن نیست که آخرین ACK به گیرنده برسد مجبور است مدتی را منتظر بماند و بعد اتصال را خاتمه دهد.

CLOSING: این وضعیت هنگامی رخ می‌دهد که هر دو نفر باهم اتصال را ببندند.



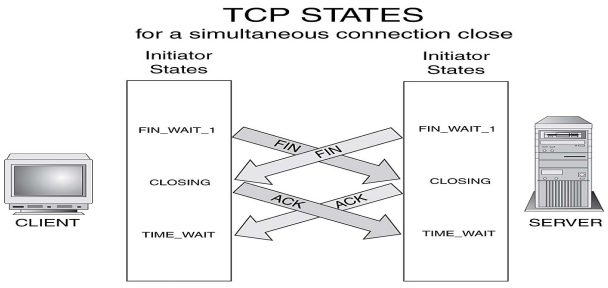
شکل ۲-۱۷: نحوه ساخته شدن یک اتصال TCP

در شکل (۲-۱۷) نحوه ساخته شدن یک اتصال TCP را مشاهده می‌کنید. وضعیت‌های میانی اتصال نیز در شکل مشخص شده است. در شکل (۲-۱۸) نیز حالت استاندارد بسته شدن یک اتصال TCP نشان داده شده است. وضعیت‌های میانی نیز در شکل مشخص شده است.



شکل ۲-۱۸: حالت استاندارد بسته شدن یک اتصال TCP

شکل (۲-۱۹) ختم اتصال را در حالتی نشان می‌دهد که هر دو نفر باهم اتصال را می‌بندند.



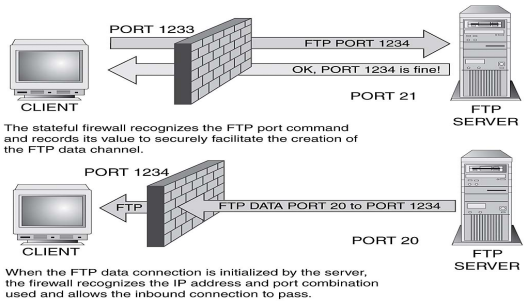
شکل ۲-۱۹: ختم اتصال یک اتصال TCP

- حالت در بسته‌های UDP
- حالت در بسته‌های ICMP
- حالت در پروتکل‌های لایه کاربرد

FTP MultiMedia HTTP and Stat

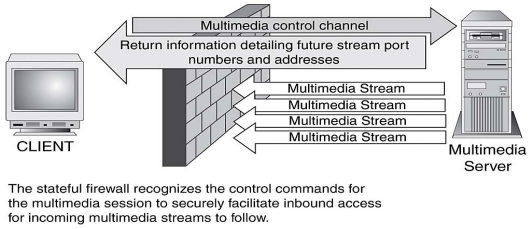
در شکل زیر بحث نگاهداری حالت در پروتکل FTP نشان داده شده است. مکانیزم و روش عملکرد پروتکل FTP به این صورت است که ابتدا سرویس گیرنده به پورت ۲۱ سرویس‌دهنده متصل می‌شود. به این اتصال، اتصال کنترلی گفته می‌شود. وقتی که سرویس‌گیرنده تقاضای انتقال یک فایل را با دستور get و یا put می‌دهد یک اتصال جدید ساخته خواهد شد. این اتصال جدید معمولا از طرف سرویس دهنده به سرویس گیرنده صورت می‌گیرد (حالت active) برای اینکه این اتصال ایجاد شود سرویس‌گیرنده شماره پورتی که از طریق آن آمادگی دریافت و یا ارسال فایل را دارد به سرویس دهنده اعلام می‌کند (شکل ۲-۲۰).

یک فایروال حالتمندکه پروتکل FTP را نیز می‌شناسد به طور اتوماتیک اجازه عبور این اتصال جدید را خواهد داد.



شکل ۲-۲۰: نگاهداری حالت در پروتکل FTP در یک فایروال حالتمند

در شکل (۲-۲۱) رفتار فایروال حالتمند در برخورد با یک پروتکل انتقال داده‌های چندرسانه‌ای نشان داده شده است. این پروتکل‌ها نیز یک اتصال کنترلی و یک اتصال برای انتقال داده دارند که فایروال باید به طور اتوماتیک اجازه ایجاد اتصال جدید را در خود ایجاد کند.



شکل ۲-۲۱: رفتار فایروال حالتمند در برخورد با یک پروتکل انتقال داده‌های چندرسانه‌ای

مزایای فایروال حالتمند

همان‌طور که در قسمت‌های قبلی دیدید، امنیت فایروال حالتمند از فایروال صافی بسته بیشتر است. زیرا فایروال حالتمند، اطلاعات مربوط به وضعیت اتصال را نگهداری می‌کند و به پاسخهای فرستاده شده به مبداء مجاز، اجازه می‌دهد که از مقصد به مبداء بازگردند. به همین خاطر گفته می‌شود که فایروال‌های حالتمند از اطلاعات لایه‌ی ۴ با خبرند. بدلیل این ویژگی پیشرفته یعنی آگاهی از ارتباطات، می‌توان به فایروال حالتمند، فایروال مافوق صافی بسته نیز گفت. همچنین بر خلاف فایروال‌های صافی بسته، فایروال حالتمند مجبور نیست به تمام درگاه‌های با شماره‌ی بالا اجازه عبوردهد تا این پردازه صورت گیرد، بنابراین راه حل بسیار امن‌تری است. در یک فایروال صافی بسته برای اینکه پروتکل‌های پیچیده نظیر ftp و rstsp بتوانند کار کنند، مجبور هستیم پورت‌های زیادی را باز بگذاریم که این خود یک مشکل امنیتی خواهد بود.

یکی دیگر از مزایای فایروال حالتمند آن است که این فایروال‌ها می‌توانند بسیار سریع‌تر از فایروال‌های صافی بسته عمل کنند. هر چند ممکن است به نظر آید که فایروال‌های صافی بسته به دلیل پردازش کم خود سربار کمی دارند و باید سرعت بالاتری داشته باشند. تصور کنید که بیش از ۱۰۰ قاعده در فایروال تعریف شده باشد. در یک فایروال صافی‌بسته چون هیچ اطلاعی راجع به اتصال نگهداری نمی‌شود مادام که اتصال برقرار است هر بسته‌ای که از فایروال عبور می‌کند باید با تمامی این قواعد تطبیق داده شود. (حال آنکه این پردازشها تکراری هستند و قبلا برای بسته مشابه انجام شده‌اند). در یک فایروال حالتمند بعد از اولین بررسی و بعد از تشکیل اتصال سایر بسته‌ها با قواعد تطبیق داده نمی‌شوند. در واقع هر بسته‌ای که مربوط به یک اتصال باشد بدون کنترل عبور داده می‌شود

معایب فایروال حالتمند

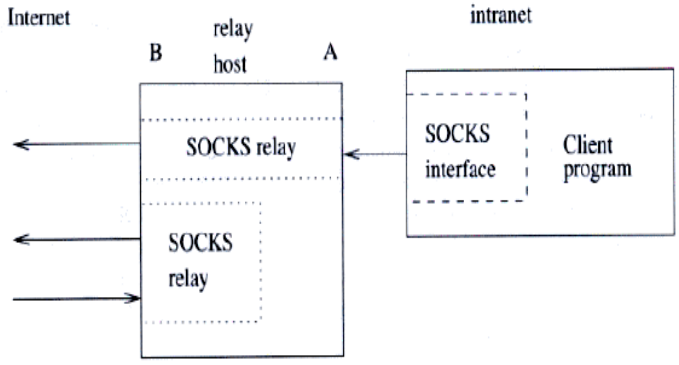
فایروال‌های حالتمند نیز مانند تمام راه حل‌های امنیتی دیگر معایبی دارند از جمله این که مجبور به پردازش بیشتر و نگهداری اطلاعات بیشتری هستند. فرض کنید که شما شبکه بسیار بزرگی با ۲۰۰۰۰ کاربر داشته باشید که در هر لحظه ۵۰۰۰ ارتباط فعال با اینترنت داشته باشند. فایروال حالتمند باید تمام این ارتباطات را در جدول وضعیتش اضافه و نگهداری کند، که در مقایسه با فایروال صافی بسته که ممکن است تنها یک فهرست کوچک از دستورات

مربوط به سیاست فیلتر کردن داشته باشد، نیاز به پردازش و حافظه‌ی بسیار بیشتری دارد. بخاطر پردازش‌های اضافی و نیاز به حافظه، فایروال‌های حالتمند از فایروال‌های صافی بسته گرانترند.

۲-۲-۷-۴- فایروال‌های درسطح مسیر

فایروال‌های در سطح مسیر در لایه TCP کار می‌کنند. ارتباطات TCP از طریق کامپیوتری رله می‌شوند که در واقع همانند یک سیم عمل میکنند. کامپیوتر رله، برنامه ای را اجرا میکند که بایت‌های بین دو ارتباط را کپی میکند و ممکن است اطلاعاتی را نیز ضبط کند. در واقع هنگامی که مشتری بخواهد به سرور متصل شود، به یک میزبان رله متصل می‌شود و گاهی اطلاعات اتصال مقصد را نیز از طریق یک پروتکل ساده فراهم میکند. در عوض میزبان رله به سرور متصل می‌شود. بنابر این عموماً نام و IP مشتری از دید سرور پنهان میماند. این فایروال‌ها همچنین می‌توانند بین دو شبکه که IP شراکتی ندارند، پل بزنند.

رله‌های در سطح مسیر در حالت کلی برای ایجاد ارتباطات خاص بین شبکه‌های مجزا به کار میروند. شکل (۲-۲۲) یک شکل بندی خاص را نشان می‌دهد:



شکل ۲-۲۲: رله‌های در سطح مسیر برای ایجاد ارتباطات خاص بین شبکه‌های مجزا

در بعضی حالات یک ارتباط در سطح مسیر به طور خودکار، به عنوان بخشی از معماری فایروال تشکیل می‌شود. گاهی یک سرویس TCP خاص باید از یک میزبان خارجی به یک پایگاه داده خارجی رله شود. مثالهایی از این برنامه‌ها با نام عمومی TCPRELAY روی اینترنت موجود است.

دربقیه حالات رله پس از اتصال نیاز دارد که مقصد مورد نظر را بداند. در این حالت پروتکل کوچکی بین مشتری و دروازه وجود دارد. این پروتکل سرویس و مقصد پروتکل را توصیف میکند. فایروال نیز پیغام‌های خطا را در صورت وجود برمی‌گرداند. این سرویس برای اولین بار توسط David & Michelle Koblas در قالب SOCKS پیاده سازی شده است. امروزه این برنامه به طور گسترده توسط کاربران اینترنت مورد استفاده قرار گرفته است.

SOCKS

نسخه‌ی ۵ این برنامه در RFC 1928 تعریف شده است. در این RFC، SOCKS اینگونه معرفی شده است:

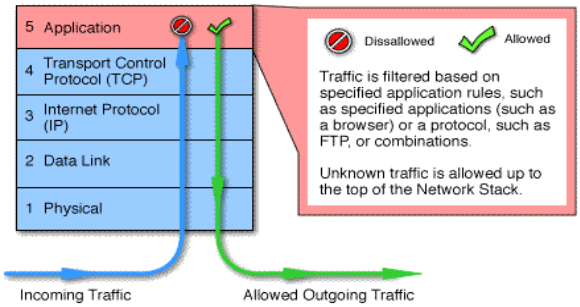
پروتکل توصیف شده در اینجا برای فراهم آوردن چارچوبی برای برنامه‌های کاربردی مشتری- سرور در هر دو حوزه TCP وUDP طراحی شده است تا استفاده راحت و امن از سرویس‌های فایروال‌های شبکه ممکن باشد. این پروتکل در واقع یک زیرلایه میانی بین لایه‌های کاربرد و لایه انتقال است و سرویس‌های لایه شبکه را فراهم نمی‌کند. SOCKS از بخش‌های زیر تشکیل شده است:

- سرور SOCKS: که روی یک فایروال مبتنی بر UNIX اجرا می‌شود.
- کتابخانه مشتریان SOCKS: که روی یک میزبان داخلی تحت پوشش فایروال اجرا می‌شود.
- SOCKS-ified Applications: نسخه‌های سازگار با SOCKS بسیاری از برنامه‌های کاربردی مشتریان مانند FTP و TELNET.

هنگامی که یک مشتری بر پایه TCP می‌خواهد ارتباط با گره‌ای برقرار کند که تنها از طریق FireWall در دسترس است، باید یک ارتباط با پورت مناسب SOCKS روی سرور SOCKS برقرار کند. سرویس SOCKS روی پورت ۱۰۸۰ واقع است. اگر درخواست اتصال موفقیت‌آمیز باشد، مشتری بر سر روش احراز هویت مذاکره می‌کند، احراز هویت می‌کند و سپس یک درخواست رله می‌فرستد. سرور درخواست را بررسی کرده، یا یک ارتباط مناسب برقرار می‌کند و یا درخواست را رد می‌کند. ارتباط UDP نیز همینگونه اداره می‌شود. درواقع یک ارتباط TCP برای احراز هویت کاربری که می‌خواهد قطعه UDP ارسال و دریافت کند، باز می‌شود. قطعات UDP تا هنگامی که این اتصال TCP باز است، جابه جا می‌شوند.

۲-۲-۷-۵- فایروال‌های درسطح کاربرد (دروازه نرم‌افزاری)

این فایروال‌ها در سطح لایه کاربرد عمل می‌کنند. و محتویات بسته‌ها را مطابق با پروتکل‌های لایه کاربرد مورد بررسی قرار می‌دهند.



شکل ۲-۲۳: فایروال در سطح کاربرد (Proxy)

معمولاً در فایروال دروازه نرم‌افزاری، کاربر باید برای هر نشست قبل از اینکه فایروال اجازه دسترسی به سرویس را به آن بدهد، احراز هویت کند. بسیاری از فایروال‌های دروازه نرم‌افزاری سیستم احراز هویت کاربران را برای انواع خاصی از نرم‌افزارهای کاربردی و بقیه برای انواع زیادی از آن‌ها فراهم می‌کنند. به گروه اول اغلب فایروال‌های صرفاً پروکسی گفته می‌شود. در زیر نمونه‌هایی از فایروال‌های نرم‌افزاری آورده شده است:

Email proxy
Web proxy
FTP proxy
Telnet proxy
DNS proxy
Finger proxy
LDAP proxy
Usenet News proxy

روش‌های احراز هویت

زمانیکه از دروازه نرم‌افزاری استفاده می‌شود ابتدا کاربر، ارتباطی را مانند ارتباط FTP، با فایروال نرم‌افزاری برقرار می‌کند، سپس فایروال دروازه نرم‌افزاری دسترسی کاربر را تایید می‌کند. این روال احراز هویت به وسیله نرم‌افزاری در لایه ۷ مدل مرجع OSI صورت می‌گیرد و می‌تواند با هر کدام از سازوکارهای احراز هویت زیر انجام شود:

- نام کاربری و رمز عبور

- احراز هویت با استفاده از آدرس مبداء
- احراز هویت با استفاده از Token Card مبتنی بر سخت‌افزار/نرم‌افزار
- احراز هویت بیومتریک

اساساً، هر روش احراز هویتی که برای دسترسی به منابع شبکه استفاده شود، می‌تواند توسط دروازه نرم‌افزاری برای انجام احراز هویت کاربر مورد استفاده قرار گیرد. یکی از نقاط ضعف فایروال‌های صافی بسته و حالتمند این است که آن‌ها تنها در لایه شبکه/انتقال عمل می‌کنند و بهمین دلیل احراز هویت آن‌ها فقط بر پایه آدرس مبداء و مقصد و نوع ارتباط می‌تواند صورت گیرد (یعنی نمی‌توانند شخصی را که درخواست ارتباط می‌فرستد تشخیص دهند). بازرسی صرف آدرس مبداء و مقصد، این دو فایروال را در معرض خطر جعل IP و نقاب‌گذاری قرار می‌دهد. دروازه نرم‌افزاری علاوه بر کنترل آدرس مبداء و مقصد دستگاه، به اطلاعات مربوط به شخص درخواست کننده‌ی دسترسی به نرم‌افزار کاربردی نیز نگاه می‌کند و این کار خطر حمله‌ی جعل IP کمتری را متوجه آن می‌کند. مثال ساده زمانی است که دو کاربر از یک دستگاه برای درخواست دسترسی به یک نرم‌افزار کاربردی استفاده می‌کنند. اگر دسترسی بر پایه‌ی اطلاعات احراز هویت صورت گیرد، ممکن است یکی از آنها اجازه دسترسی داشته باشد در صورتیکه دیگری مجاز نباشد.

در ادامه یک دید کلی از روش‌های احراز هویت که معمولاً توسط دروازه‌های نرم‌افزاری استفاده می‌شوند، ارائه خواهد شد.

احراز هویت از طریق نام کاربری و رمز عبور. در این روش، نام کاربری و رمز عبور متناظر با آن از کاربر خواسته می‌شود، سپس این اطلاعات با اطلاعات موجود در بانک اطلاعاتی نام کاربری درونی متعلق به دروازه‌ی نرم‌افزاری و یا یک بانک اطلاعاتی بیرونی، مانند ساختار دایرکتوری NDS در Netware، یا بانک اطلاعاتی Oracle و یا بانک اطلاعاتی سرویس امنیتی، مقایسه می‌شود.

احراز هویت با استفاده از آدرس مبداء. در این روش، دروازه‌ی نرم‌افزاری آدرس مبداء را با فهرست آدرس‌های مبداء مجاز مقایسه می‌کند. دروازه‌ی نرم‌افزاری ممکن است چندین فهرست داشته باشد.

احراز هویت با استفاده از Token Card. در این روش، کاربر از یک کارت مخصوص که کلیدی به آن اختصاص داده شده است استفاده می‌کند. این کلید با سرویس‌دهنده‌ی

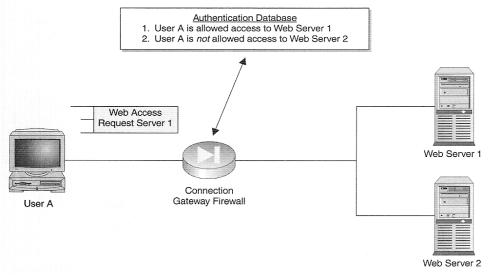
Token Card هماهنگ شده است. کاربر، کلیدی را که بر روی کارت نشان داده شده است (که تنها برای مدت کوتاهی معتبر است) وارد می‌نماید و دروازه‌ی نرم‌افزاری آن را برای تایید اعتبار به سرویس‌دهنده‌ی Token Card می‌فرستد.

احراز هویت بیومتریک. در روش بیومتریک، برخی از اطلاعات فیزیکی کاربر مانند اثر انگشت، پویش شبکیه‌ی چشم، موج صوتی صدای کاربر و یا سازوکارهای دیگری که برای هر فرد منحصر به فرد است، مورد استفاده قرار می‌گیرد. فایروال‌های دروازه‌ی نرم‌افزاری در یکی از دو گروه زیر قرار می‌گیرند:

Connection و Cut-Through (این اصطلاح خاص فایروال‌های PIX متعلق به شرکت سیسکو است و ممکن است در فایروال‌های دیگر اصطلاح دیگری برای این منظور استفاده شود.) مسئله اصلی آن است که در این روش فقط عملیات هویت شناسی در لایه ۷ انجام شده و سپس اتصال اصلی در همان لایه اصلی خود برقرار می‌شود.) این دو گروه در قسمت‌های بعدی همراه با چگونگی عملکردشان و مزایا و معایب آنها توضیح داده شده‌اند.

فایروال دروازه‌ی نوع Connection

دروازه‌ی نرم‌افزاری نوع Connection، کاربر را مجبور می‌کند تا یک ارتباط نرم‌افزاری با فایروال دروازه‌ی نرم‌افزاری ایجاد کند. سپس همان‌طور که در شکل زیر نشان داده شده است، کاربر را نه تنها بر اساس شناسه‌ی کاربر بلکه بر اساس اینکه آیا کاربر اجازه‌ی دسترسی به نرم‌افزار کاربردی در مقصد درخواست شده را دارد یا نه نیز، احراز هویت می‌کند.



شکل ۲-۲۴: فایروال دروازه‌ی نوع Connection

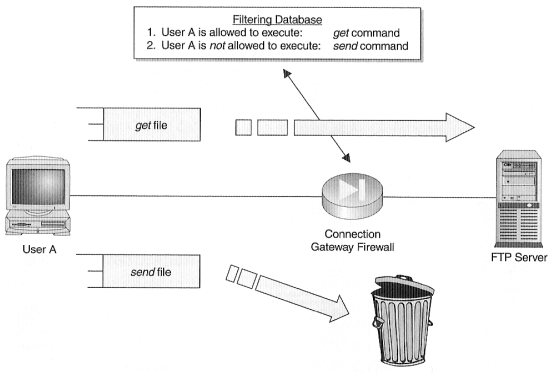
اگر کاربر مجاز باشد، دروازه‌ی نرم‌افزاری نوع Connection ارتباط جدیدی را به سمت مقصد ایجاد می‌کند که مانند یک پروکسی بین ارتباط اولیه‌ی کاربر و ارتباطی که دروازه‌ی نرم‌افزاری به سمت مقصد ایجاد کرده است، عمل می‌کند. در این مثال، در واقع دو ارتباط

وجود دارد و دروازه، مسئول مدیریت انتقال اطلاعات بین دو ارتباط مجزاست. اگر کاربر مجاز نباشد، ارتباط بین کاربر و دروازه‌ی نرم‌افزاری قطع می‌شود.

مزایای فایروال‌های دروازه‌ی نرم‌افزاری نوع Connection عبارتند از توانایی ثبت وقایع با جزئیات زیاد و فیلتر کردن داده‌ی نرم‌افزاری. به این دلیل که دروازه‌ی نوع Connection همواره اطلاعات را در لایه‌ی ۷ مدل مرجع OSI پردازش می‌کند، در مقایسه با فایروال‌های صافی بسته و حالتمند، توانایی بسیار بیشتری برای ثبت تمام داده‌ها در تعامل داده دارد، زیرا آنها اطلاعات را تنها در لایه‌ی ۳ و یا شاید لایه‌ی ۴ پردازش می‌کنند. هر دستور و بطور کلی هر ضربه‌ای که توسط کاربر به صفحه کلید وارد شود توسط دروازه‌ی نوع Connection قابل رویت است.

همچنین، برخلاف فایروال‌هایی که تنها در لایه‌ی ۳ و ۴ کار می‌کنند، چون فایروال دروازه‌ی نوع Connection تمام داده‌ی رد و بدل شده بین کاربر و پردازه‌ی نرم‌افزار کاربردی را می‌بیند، می‌تواند محتوای داده‌ی اصلی را فیلتر کند. این عمل ممکن است از دستورات معین اجرایی استفاده کند و یا به منابع معینی دسترسی داشته باشد. مثلاً، کاربری که به سرویس وب دسترسی دارد را می‌توان با استفاده از قوانین فیلتر کردن در دروازه‌ی نرم‌افزاری طوری محدود کرد که تنها به صفحه‌های وب معینی دسترسی داشته باشد. و یا در مورد دریافت‌های اینترنتی، برخی کاربران ممکن است اجازه‌ی دسترسی به برنامه‌های Java و اسکریپت‌های ActiveX را داشته باشند و بقیه مجاز نباشند. نمونه‌ی دیگر می‌تواند کاربرهایی که به یک سرویس‌دهنده‌ی FTP دسترسی دارند باشد که ممکن است در نوع ساختار دایرکتوری‌هایی که مجاز به دسترسی به آنها هستند، محدودیت داشته باشند. به این دلیل که فایروال دروازه‌ی نوع Connection تمام داده‌های رد و بدل شده بین کاربر و روال بسته‌ی نرم‌افزاری را می‌بیند، می‌توان در سیاست فیلتر کردن بسیار خلاق بود.

شکل زیر مثالی از فایروال دروازه‌ی نوع Connection که برای دسترسی به FTP بکار رفته است را نشان می‌دهد.



شکل ۲-۲۵: فایروال دروازه‌ی نوع Connection که برای دسترسی به FTP

در این مثال، اگر کاربر A دستور get را برای دریافت فایل از سرویس‌دهنده‌ی FTP صادر کند، با وجود فایروال دروازه‌ی نرم‌افزاری مجاز است که آن را اجرا کند. اما اگر کاربر بخواهد فایلی را با دستور send در سرویس‌دهنده‌ی FTP قرار دهد، فایروال دروازه‌ی نرم‌افزاری جلوی این دستور را می‌گیرد و آنرا دور می‌اندازد. علیرغم تمام مزایایی که برای این روش ذکر شد، فایروال‌های دروازه‌ی نرم‌افزاری معایبی نیز دارند:

- در پردازش داده بسیار کندند. چونکه دروازه‌های نرم‌افزاری باید برای هر دو ارتباط ترافیک را در هر هفت لایه‌ی مدل مرجع OSI مدیریت کنند، مثلاً ترافیک را بین دو ارتباط Bridge کنند، به همین دلیل بسیار کند بوده، دارای مشکلات جدی در مقیاس‌پذیری می‌باشند. هر چه تعداد کاربر بیشتری از دروازه‌ی نرم‌افزاری استفاده کند، ارتباط کندتر خواهد شد.

- معمولاً به نرم‌افزارهای کاربردی معین و یا به مجموعه‌ی کوچکی از آنها محدودند. اکثر دروازه‌های نرم‌افزاری نوع Connection ی که شرکت‌های تجاری ایجاد می‌کنند مختص به یک نرم‌افزار کاربردی خاص هستند: معمولاً با یک نوع نرم‌افزار مثل سرویس‌های وب، telnet یا FTP کار می‌کنند. بنابراین، اگر برای مثال احتیاج به این نوع امنیت برای هر دو ترافیک وب و telnet دارید، بطور معمول باید دو نوع مختلف از دروازه‌ی نرم‌افزاری را بخرید: یکی برای telnet و یکی برای ارتباطات وب. برخی محصولات دروازه‌ی نرم‌افزاری

نوع Connection قابلیت کار با بیش از یک نوع نرم‌افزار کاربردی را دارند، اما حتی بـرای آنها هم تعداد نرم‌افزارها بسیار محدود است مثلاً دو یا سه نرم‌افزار.

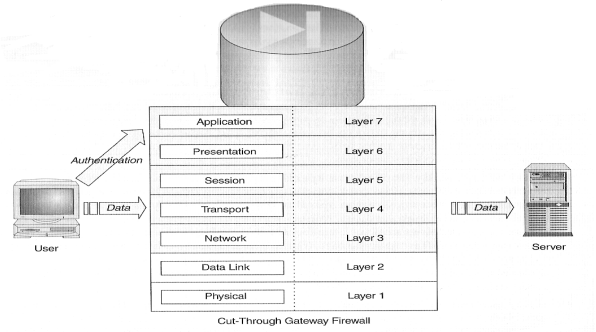
- بعضی اوقات به نرم‌افزار خاصی برای بارگذاری شدن بر روی سیستم گیرنـده نیـاز دارنـد. مشکل دیگری که بسیاری از محصولات دروازه‌ی نرم‌افزاری نوع Connection دارند ایـن است که یا نیاز دارند که خود شما نرم‌افزار کاربردی خاصی را بر روی دستگاه‌تان نصب و پیکربندی کنید و یا حداقل نرم‌افزارهای کاربردی موجود را پیکربندی مجدد کنید.

فایروال دروازه‌ی نوع Cut-Through

در این نوع، اولین پردازش بسیار شبیه به آن چیزی است که در فایروال دروازه‌ی نوع Connection بود: ابتدا کاربر برای دروازه‌ی نرم‌افزاری احراز هویت می‌کند، اما اگر کاربر موفق شود، فایروال دروازه یکی از دو سازوکار زیر را برای تکمیل ارتباط انجام می‌دهد:

- به خود کاربر اجازه‌ی تکمیل ارتباط را می‌دهد.
- دروازه نیمه‌ی دیگر ارتباط را می‌سازد و آنرا به نیمه‌ی اول متصّل می‌کند.

برخلاف فایروال دروازه‌ی نوع Connection که همیشه ترافیک کاربر را در لایه‌ی کاربرد پردازش می‌کند (زیرا بعنوان یک Bridge بین دو ارتباط عمل می‌کند). با هر کدام از این دو روش، تنها یک ارتباط وجود دارد که دروازه‌ی نوع Cut-through می‌تواند در لایه‌ی ۳ یا ۴ فایروال دروازه آنرا پردازش کند. شکل زیر مثالی در این مورد را نشان می‌دهد.



شکل ۲-۲۶: فایروال دروازه‌ی نوع Cut-Through

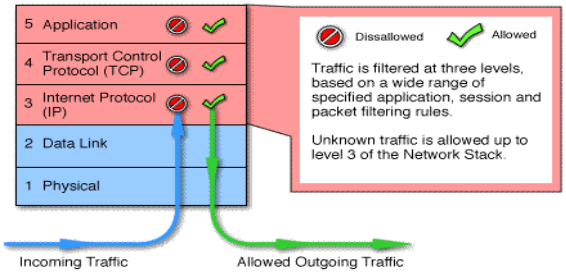
فایروال‌های دروازه‌ی نوع Cut-through بر نوع Connection برتری‌هایی دارد. یکی از مهمترین آنها این است که با وجود این که روال احراز هویت در لایه‌ی ۷ انجام می‌گیرد،

ترافیک متعاقب بین کاربر و سرویس در لایه‌ی ۳ و ۴ پردازش می‌شود که جریان خروجی را تقویت می‌کند.

علاوه بر این، بدلیل اینکه فایروال دروازه‌ی نرم‌افزاری تنها مسئول اداره‌ی قسمت احراز هویت است، برخلاف فایروال دروازه نوع Connection می‌تواند انواع زیادی از نرم‌افزارهای کاربردی را مدیریت کند و محدودیتی ندارد. همچنین، چون تعداد زیادی از نرم‌افزارهای کاربردی قابلیت کار با روش‌های دسترسی متداول، مانند خط فرمان و یا GUI، را دارند، این فایروال نوعی از احراز هویت را بکار می‌گیرد که معمولاً تغییر نرم‌افزارهای کاربردی موجود کاربر مورد نیاز نیست. بعنوان مثال، فایروال Cisco PIX برای telnet ، FTP و ارتباطات HTTP از دروازه‌ی نوع Cut-through استفاده می‌کند و برای تمامی اینها هیچ نیازی به تغییر نرم‌افزارهای کاربردی کاربر نیست.

باوجود تمامی برتری‌ها ذکر شده، فایروال دروازه‌ی نرم‌افزاری معایبی نیز دارد. جاییکه از این فایروال‌در جریان خروجی استفاده شود خاصیت فیلتر کردن خود را از دست می‌دهد و به این دلیل که تنها در مدت انجام عملیات احراز هویت با لایه‌ی کاربرد سروکار دارد، نمی‌تواند اطلاعات این لایه را فیلتر کند (تنها توانایی فیلتر کردن اطلاعات لایه‌ی ۳ و ۴ مدل مرجع OSI را دارد.) و چون تنها با لایه‌های ۴ و زیر آن برخورد دارد، توانایی ضبط جزئیات اطلاعاتی را که فایروال دروازه‌ی نوع Connection در ثبت وقایع خود دارد، ندارد.

فایروال‌هایی که کنترل‌هایی را در مورد محتویات فایل‌ها انجام می‌دهند. نظیر آنتی ویروسها و.... را فایروال‌های در سطح فایل و فایروال‌هایی که ترکیبی از فایروال‌ها در سطوح مختلف هستند، فایروال‌های ترکیبی می‌نامند.



شکل ۲-۲۷: فایروال ترکیبی

در جدول(۲-۱) نمونه‌هایی از هر نوع فایروال آورده شده‌اند.

جدول ۲-۱: مثالهایی از انواع فایروال

	Packet Level Protection	Session Level Protection	Application Level Protection	File Level Protection
Examples	Packet filtering (router ACLs or stateless firewalls)	Stateful inspection firewalls	Intrusion prevention systems (IPS) and proxy firewalls	Gateway antivirus
Mechanism	Examine packet header	Examine packet header and control fields	Examine application fields	Examine files inside application traffic
Protocol and Application Coverage	N.A. packet level	Large	Medium	Small (email, web and file transfers)
Protection Provided	Client-to-server and server-to-client	Client-to-server and server-to-client	Mainly client-to-server	Mainly server-to-client
Relative Performance	High	High	Medium	Low

۲-۳- موقعیت یابی برای فایروال

محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن ، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از :

موقعیت و محل نصب از لحاظ توپولوژی

معمولا مناسب به نظر می‌رسد که فایروال را در درگاه ورودی/خروجی شبکه خصوصی نصب کنیم. این امر به ایجاد بهترین پوشش امنیتی برای شبکه خصوصی با کمک فایروال از یک طرف و جداسازی شبکه خصوصی از شبکه عمومی از طرف دیگر کمک می‌کند.

قابلیت دسترسی و نواحی امنیتی

اگر سرورهایی وجود دارند که باید برای شبکه عمومی در دسترس باشند، بهتر است آنها را بعد از فایروال و در ناحیه DMZ قرار دهید. قرار دادن این سرورها در شبکه خصوصی و تنظیم فایروال جهت صدور اجازه به کاربران خارجی برای دسترسی به این سرورها برابر خواهد بود با هک شدن شبکه داخلی. چون شما خود مسیر هکرها را در فایروال باز کرده‌اید. در حالی که با استفاده از ناحیه DMZ، سرورهای قابل دسترسی برای شبکه عمومی از شبکه خصوصی شما بطور فیزیکی جدا هستند، لذا اگر هکرها بتوانند به نحوی به این سرورها نفوذ کنند بازهم فایروال را پیش روی خود دارند.

مسیریابی نامتقارن

بیشتر فایروال‌های مدرن سعی می‌کنند اطلاعات مربوط به اتصالات مختلفی را که از طریق آنها شبکه داخلی را به شبکه عمومی وصل کرده است، نگهداری کنند. این اطلاعات کمک می‌کنند تا تنها بسته‌های اطلاعاتی مجاز به شبکه خصوصی وارد شوند. در نتیجه حائز اهمیت است که نقطه ورود و خروج تمامی اطلاعات به/از شبکه خصوصی از طریق یک فایروال باشد.

فایروال‌های لایه‌ای

در شبکه‌های با درجه امنیتی بالا بهتر است دو یا چند فایروال در مسیر قرار گیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می‌دهد. معمولا بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم‌افزاری یا حفره امنیتی در یکی از آنها، سایرین بتوانند امنیت شبکه را تامین کنند.

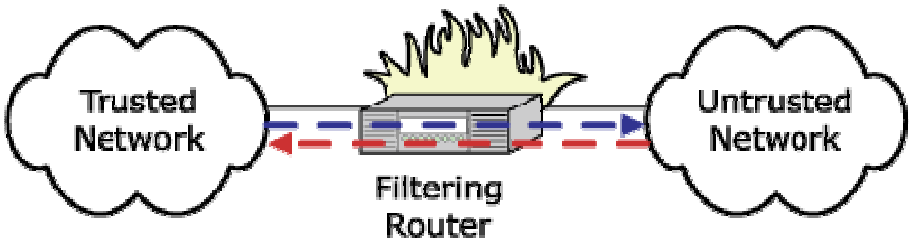
۲-۴- معماری فایروال ها

Personal Firewall -۱-۴-۲

فایروال شخصی در واقع فایروالی است که بر روی یک کامپیوتر شخصی (یا سرور) برای محافظت از آن کامپیوتر نصب می‌شود. فایروال‌های شخصی همگی نرم‌افزاری هستند و عمدتا برای سیستم عامل‌های ویندوزی طراحی شده‌اند. این فایروال‌ها طیف زیادی از حملات اینترنتی را پوشش می‌دهند. اکثر این فایروال‌ها همراه با بسته‌های آنتی ویروس ارائه می‌شوند. با توجه به اینکه حوزه حفاظت اینگونه فایروال‌ها فقط یک کامپیوتر است ممکن است به نظر برسد که توانایی اینگونه فایروال‌ها زیاد نیست و یا از اهمیت کمی برخوردار هستند. ولی در واقع اینگونه فایروال‌ها از اهمیت به سزایی در برقراری امنیت ایفا می‌کنند. فراموش نکنیم که فایروال‌ها و سیستم‌های محافظتی نمی‌توانند در مقابل داده‌های رمز شده و یا حملاتی که اصلاً از فایروال عبور نمی‌کنند واکنشی نشان دهند. یک فایروال شخصی این محدودیتها را ندارد. در واقع اگر به استراتژی دفاع در عمق توجه داشته باشیم یکی از مهمترین مراحل امن سازی استفاده از فایروال شخصی است. اینگونه فایروال‌ها معمولاً تمامی ویژگی‌های یک فایروال لایه کاربرد را دارا هستند و اکثراً همراه با یک بسته آنتی ویروس ارائه می‌گردند.

Packet Filtering Router –۲–۴–۲

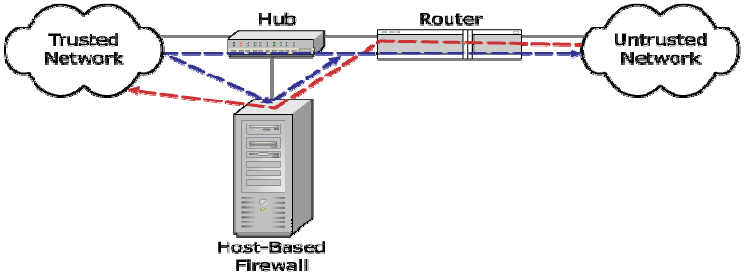
روترهای مرزی سازمان عموماً در نقش یک صافی بسته به عنوان اولین خاکریز دفاعی در برابر حملات تلقی می‌شوند. در مورد مزایا و معایب فایروال‌های صافی‌بسته قبلاً صحبت شده است.



شکل ۲-۲۸: Packet Filtering Router

Screened Host (Host-Based) –۳–۴–۲

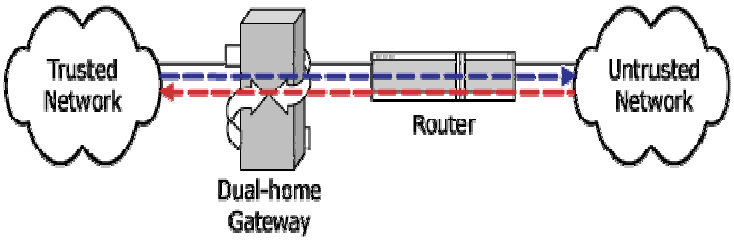
این سیستم، یک کامپیوتر با سیستم عامل معمولی همراه با نرم‌افزار مونیتورینگ است، فقط بسته‌ها را مونیتور می‌کند و در مسیر عبور بسته‌ها قرار نمی‌گیرد. اکثر سیستم‌های تشخیص نفوذ و نیز بعضی از سیستم‌های فیلترینگ محتوا از این معماری استفاده می‌کنند.



شکل ۲-۲۹: فایروال Host Based

Dual-home Gateway –۴–۴–۲

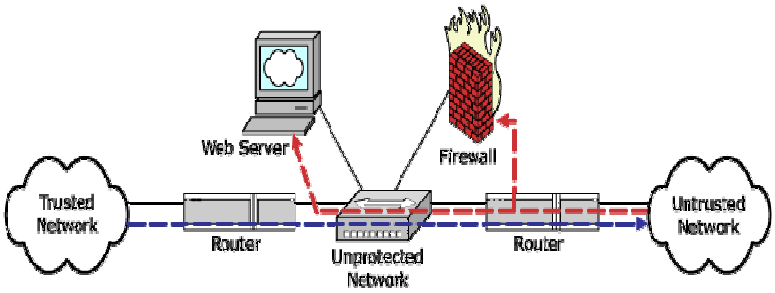
یک کامپیوتر با سیستم عامل معمولی همراه با نرم‌افزار فایروالینگ که در مسیر عبور بسته‌ها قرار می‌گیرد. معمولاً این سیستم‌ها به صورت روتر در مدار قرار می‌گیرند هرچند مدل‌های جدید اکثراً می‌توانند به صورت Bridge نیز در شبکه قرار گیرند.



شکل ۲-۳۰: Dual-Home Gateway

۲-۴-۵- Screened Subnet or Demilitarized Zone (DMZ)

فایروال‌های حرفه‌ای کل شبکه را به بیش از دو زیر شبکه تقسیم می‌کنند و برای هر زیرشبکه ملاحضات خاص امنیتی را در نظر می‌گیرند. معمولاً ناحیه سرورها به سیستم مونیتورینگ و تشخیص نفود نیز مجهز می‌شود.



شکل۲-۳۱: تقسیم بندی شبکه توسط فایروال

۲-۴-۶- Firewall Appliance

این سیستم‌ها ترکیب سخت‌افزار و نرم‌افزار ویژه فایروالینگ هستند که به طور ویژه برای انجام عملیات فایروالینگ بهینه سازی شده‌اند. در فایروال‌های حرفه‌ای بسیاری از عملیات نظارتی و کنترلی با استفاده از سخت‌افزارهای ویژه انجام می‌شود.

۲-۵- معیارهای انتخاب فایروال

یکی از تصمیم‌های مشکل برای هر مدیرشبکه انتخاب فایروال است به منظور انتخاب درست باید انواع فایروال‌ها و تواناییهای آنها را بشناسیم و بر اساس نیازها و هزینه مناسب بتوانیم بهترین انتخاب را انجام دهیم. برخی از فایروال‌های حرفه‌ای قابلیت‌هایی بسیار فراتر از

نیازهای امنیتی یک سازمان را در خود دارند و برخی دیگر فاقد برخی از نیازمندیهای اصلی هستند.

۲-۵-۱- معیارهای ارزیابی

انواع زیادی از محصول‌های فایروال و VPN با امکانات و قابلیت‌های گوناگون در بازار ارائه می‌شود که تصمیم‌گیری درباره انتخاب صحیح محصول مطابق با نیازهای سازمان را با مشکل مواجه می‌سازد. در این بخش برای کمک به مدیران و کارشناسان فنی جهت مقایسه محصول‌ها، معیارهای انتخاب دسته بندی و خلاصه شده‌اند.

۲-۵-۱-۱- امنیت بالا

اولین وظیفه‌ای که از یک فایروال انتظار می‌رود برقراری امنیت در شبکه است. برخی از امکاناتی که فایروال باید در این زمینه ارائه کند عبارتند از: کنترل دسترسی، هویت شناسی کاربر[1]، محافظت در برابر حملات، رمز نگاری به منظور تامین محرمانگی داده و افراز شبکه برای محصورسازی حمله و جلوگیری از گسترش آن. علاوه‌بر فراهم کردن امنیت برای شبکه داخلی, خود فایروال نیز باید بتواند از خود به خوبی محافظت کند. فایروال خط مقدم شبکه داخلی در برابر شبکه خارجی و حملات بیرونی است. بنابراین امنیت خود فایروال نیز باید مورد توجه قرار گیرد. برای این منظور راه‌حل‌های مختلفی برای محافظت از فایروال ارائه شده است. یکی از بهترین روش‌ها استفاده از سیستم عامل‌های خاص منظوره است که در این صورت نفوذ کردن به آن مشکلتر شده و نمی‌توان از روش‌های حمله و نفوذ به سیستم‌های دیگر، برای نفوذ به فایروال استفاده کرد.

۲-۵-۱-۲- کارآیی قابل پیش بینی

با توجه به این که فایروال در مسیر تمام ترافیک ورودی و خروجی شبکه قرار دارد، کارایی آن از اهمیت زیادی برخوردار است. اگر فایروال نتواند نیازمندی‌های کارایی شبکه را حفظ کند، تبدیل به گلوگاه شده و ارزش خود را از دست خواهد داد. فایروال باید ترافیک را به طور کارا پردازش نموده و کارایی بالا و قابل پیش بینی ارائه دهد. این کارایی باید برای بسته‌های کوچک

[1] User Authentication

و هم بسته‌های بزرگ قابل تحمل باشد. همچنین تاخیر را کمینه کرده و تعداد اتصال‌های همزمان و تونل‌های VPN همزمان مورد نیاز را برآورده کند.

۲-۵-۱-۳- تحمل پذیری بالای خطا به منظور تضمین دائمی دسترس پذیری

یکی از موارد مهم در انتخاب فایروال حداکثر پایداری و حداقل خرابی می‌باشد. به علت آن که فایروال نقطه تماس شبکه داخلی با بیرون است، در صورت از کار افتادگی فایروال، کلیه ارتباطات با بیرون شبکه قطع خواهد شد. برای این منظور فایروال باید از قابلیت‌های تحمل پذیری خطا برای جبران خطاها و پوشش آنها استفاده کند.

به طور معمول تحمل‌پذیری خطا با استفاده از افزونگی چه در سطح قطعات و چه در سطح سیستم انجام می‌شود که این افزونگی متناسب با سطح تحمل‌پذیری خطا و هزینه صرف شده است. در سطح سیستم از چند فایروال در کنار هم استفاده می‌شود که در صورت خرابی یکی، دیگری به کار ادامه دهد.

باید توجه داشت که راهکار مورد نظر باید در تمام سطوح افزونگی فراهم کند به طوری که سازمان بتواند هر سطح از دسترس‌پذیری را برای هر قطعه از شبکه متناسب با نیازمندی‌های دسترس‌پذیری و هزینه انتخاب و اعمال کند. خود ابزار نیز باید افزونگی قطعات را پشتیبانی کند.

۲-۵-۱-۴- نصب و استقرار سریع و ساده

مدیران IT، شبکه و امنیت انتظار دارند که سرویس‌های مورد نیاز همیشه بر پا باشند. از این رو باید فایروال یا دیگر ابزارها سریع و ساده نصب شده و بلافاصله قابل بهره برداری باشند. از نظر قابلیت استفاده باید ساده بوده و نیازی به دانش امنیتی بالا نداشته باشد. به روز رسانی‌ها باید به راحتی بدون نگرانی از بابت بر هم زدن پیکر بندی قبلی یا ایجاد رخنه‌های جدید قابل اعمال باشند. به عنوان مثال نباید نگران آن بود که ترمیم (Patch) اعمال شده به سیستم عامل روی برنامه‌های دیگر یا بستر شبکه تاثیر بگذارد. فایروال باید به گونه‌ای طراحی شود که با اجزای دیگر به راحتی کار کرده تا پیچیدگی را کاهش داده و نصب را آسان سازد.

۲-۵-۱-۵- سادگی استفاده و مدیریت

هزینه‌های واقعی یک راهکار تنها در هزینه اولیه نیست بلکه باید هزینه‌های مدیریت و نگهداری را نیز به آن افزود. علاوه بر آن باید تعامل ساده‌ای با مدیر شبکه داشته، به نحوی که بتوان سیاست‌های امنیتی را به راحتی اعمال نمود. باید توجه داشت که یکی از دلایل بروز رخنه‌های امنیتی پیچیدگی در مدیریت و پیکربندی بوده و در صورت پیچیدگی استفاده، امکان بروز رخنههای امنیتی بالا خواهد رفت. همچنین مشکلات فنی باید به سادگی قابل رفع باشند و از پشتیبانی قوی فنی برخوردار باشد. سازمان‌ها مایل به صرف وقت برای نگهداری و رفع مشکل نیستند و خواهان صرف کمترین هزینه و زمان برای مدیریت هستند.

۲-۵-۱-۶- پشتیبانی قوی

باید توجه داشت که محصول‌های امنیتی به دلیل نیاز به دانش فنی بالا و پیچیدگی‌های پیکربندی ممکن است با مشکلات مختلفی در چرخه حیات (نصب، پیکربندی عملیات) مواجه شوند. علاوه بر آن به علت نقش حیاتی فایروال در برقراری سرویس‌های سازمان، بروز مشکلات در آن می‌تواند هزینه گزافی را به دنبال داشته باشد. بنابراین پشتیانی قوی با استفاده از کادرهای فنی متخصص و دوره دیده یکی از نیازهای اساسی در تهیه فایروال می‌باشد. فروشنده باید گزینه‌های مختلفی مانند پشتیبانی از راه دور و از طریق شبکه ویا خط Dialup در اختیار خریدار قرار دهد. نکته دیگر در نحوه پشتیبانی سروکار داشتن با فروشندگان مختلف است. ممکن است فایروال از ماجول‌های مختلفی از طرف شرکت‌های مختلف تشکیل شده باشد که ناچار از مراجعه به هر یک از آنها می‌باشید. علاوه بر آن اعتبار و سابقه ارائه کننده از اهمیت زیادی برخوردار است.

۲-۵-۲- چک لیست

برای این که نسبت به کیفیت فایروال انتخابی خود مطمئن شوید، پرسش‌های زیر را پاسخ دهید.

امنیت بالا

- آیا فایروال حالتمند[1] است؟

[1] Stateful

- آیا فایروال می‌تواند در برابر حملات (مانند DoS و DDOS) حفاظت کند؟
- آیا فایروال می‌تواند در برابر حملات لایه کاربرد حفاظت کند؟
- آیا سیستم قادر است URLهای مخرب را شناسایی و متوقف کند؟
- فایروال از چه نوع هویت شناسی پشتیبانی می‌کند؟
- آیا فایروال می‌تواند کاربران را با استفاده از پایگاه داده فعلی کاربران هویت شناسی کند؟
- آیا سیستم قابلیت تقسیم شبکه به نواحی مختلف امنیتی را دارد؟
- آیا VPN بر اساس IPSec کار می‌کند (برای سازگاری با VPNهای دیگر)؟
- محصول چه تأییدیه‌های امنیتی دارد؟ (این گزینه خیلی مهم است. در واقع شرکتهای معتبری وجود دارند که کارشان ارزیابی فایروال است و اگر فایروالی بتواند تستهای آنها را با موفقیت بگذراند، تأییدیه را دریافت میکند.)
- محصول چگونه حمله را محصور کرده و از گسترش آن جلوگیری می‌کند؟
- آیا فایروال و VPN دارای مدیریت یکسان از یک کنسول مشترک هستند؟
- آیا از اطلاعات یکدیگر استفاده می‌کنند؟
- آیا سیاست فایروال به ترافیک VPN اعمال می‌شود؟
- چگونه سیستم خود را در برابر آسیب پذیری‌های بالقوه محافظت می‌کند؟
- آیا محصول می‌تواند برای برآورده کردن سطوح مختلف امنیت از سایتهای کوچک تا بزرگ گسترش یابد؟ (آیا فایروال می‌تواند نیازهای آتی سازمان را بعد از گسترش شبکه تأمین کند؟)
- آیا فایروال می‌تواند با سیستم‌های دیگر از قبیل URL Filter, Virus Scanner کار کند؟

شبکه‌های خصوصی

- آیا برای ایجاد شبکه خصوصی از پروتکل ipsec استفاده می‌کند؟
- آیا از پروتکل IKE برای تبادل کلید استفاده می‌کند؟
- آیا از روش‌های قوی رمزنگاری پشتیبانی می‌کند؟
- آیا از روش‌های قوی هویت شناسی پشتیبانی می‌کند؟

ترکیب فایروال و شبکه خصوصی

- آیا پیکربندی فایروال و شبکه خصوصی به طور متمرکز و باهم انجام می‌شود؟
- آیا سیستم از یک سیستم عامل مخصوص و محکم و امن شده استفاده می‌کند؟
- آیا سیستم قابلیت استفاده در محیطهای گوناگون با تعداد کاربران متفاوت را دارد؟

کارایی قابل پیش بینی

- آیا فروشنده تضمین می‌کند که بعد از نصب فایروال هیچ گونه افت کارایی در شبکه به وجود نیاید؟
- فایروال برای بهینه سازی پردازش ترافیک چه میکند؟
- فایروال چگونه نرخ صعودی اتصالها را برای جلوگیری از حمله DoS راهبری میکند؟
- فایروال برای کارآیی بالا از چه معماری استفاده میکند؟
- فایروال چگونه اتصالهای همزمان را برای جلوگیری از قطعی یا کندی، راهبری میکند؟ (مشاهده شده است که بعضی از فایروال‌های حرفه‌ای نیز پس از افزایش تعداد اتصالهای همزمان، دچار افت کارایی شدیدی شده‌اند.)
- فایروال چگونه بدون کاهش کارایی، از قابلیت‌های اضافه پشتیبانی می‌کند؟
- فایروال چگونه برقراری اتصالها و تونلهای VPN را شتاب می‌دهد؟
- فایروال چگونه تاخیر را برای کاربردهای بی‌درنگ(مانند VOIP) به حداقل می‌رساند؟

ارائه سرویس با تحمل خطای بالا برای تضمین دسترس پذیری دائمی

- آیا فایروال پیکربندی HA (High Availability) را برای کاهش احتمال خرابی پشتیبانی میکند؟
- آیا محصول می‌تواند از پروتکل‌های مسیر یابی پویا نظیر RIP, OSPF, IGRP پشتیبانی کند؟
- آیا فایروال از مسیرهای اضافه پشتیبانی میکند؟ چگونه (اتصال به چند ISP، خط پشتیبان Dial) ؟
- چه امکانات افزونگی در پیکربندی VPN وجود دارد؟

- چه مکانیزمهایی برای حداقل کردن زمان بازسازی پس از خرابی و حداکثر نمودن زمان Uptime وجود دارد؟

نصب و استقرار سریع و ساده

- آیا راهکار به صورت Appliance (برای سادگی نصب) است؟
- آیا گزینه‌های مختلف برای نصب وپیکربندی وجود دارد؟
- آیا محصول از پیکربندی خط فرمان، تحت وب و مبتنی بر سیاست[1] پشتیبانی می‌کند؟
- برای استقرار سریع پشتیبانی از چه امکانات شبکه‌ای استفاده می‌شود؟
- ترمیم‌ها[2] و به روز رسانی‌ها چگونه اعمال می‌شوند؟

سادگی استفاده و مدیریت

- میزان سادگی مدیریت محصول چقدر است؟
- آیا از روش‌های مختلف قرارگیری فایروال در شبکه حمایت می‌کند؟
- آیا از پروتکل‌های دینامیک مسیریابی حمایت می‌کند؟
- تغییرات در یک شبکه توزیع شده با چه سرعتی قابل اعمال هستند؟
- آیا روش‌های مختلفی برای تعامل و مدیریت سیستم وجود دارد؟
- پس از قطعی یک اتصال، چه میزان مداخله دستی لازم است؟
- رفع عیوب احتمالی تا چه میزان ساده است؟
- میزان سادگی اضافه کردن یک شبکه به VPNچقدر است؟
- پیکربندیهای پیچیده VPN مانند همبندی‌های Hybrid Full-Mesh، Hub و Spoke چقدر ساده است؟
- آیا سیاست‌های فایروال به آسانی و بدون پیکربندیهای اضافه، قابل اعمال به ترافیک VPN است؟
- آیا نرم‌افزارهای جانبی برای تنظیم فایروال وجود دارد؟

---

[1] Policy-based
[2] Patches

- آیا از VLAN پشتیبانی می‌کند؟
- آیا ویزاردهای راحت و ساده برای تنظیم اولیه سیستم وجود دارد؟
- آیا امکانات خوبی برای مونیتور کردن بسته‌ها و قوانین فایروال و نیز تونلهای شبکه خصوصی دارد؟

پشتیبانی

- آیا گزینه‌های پشتیبانی گسترده ای وجود دارد؟
- آیا امکان پشتیبانی از راه دور با استفاده از شبکه اینترنت و خط Dialup وجود دارد؟
- آیا فروشنده نسخه‌هایی از فایروال را برای ارزیابی در اختیار شما قرار می‌دهد؟
- زیرساخت پشتیبانی چقدر پیچیده است؟ آیا شما باید با چند فروشنده و پروانه‌های متعدد سروکار داشته باشید؟
- اعتبار و سابقه شرکت ارائه کننده چقدر است؟ آیا شرکت محصولهای دیگری نیز با پشتیبانی قوی ارائه میکند؟ آیا مشتریان قبلی شرکت از سرویس‌های آن راضی بوده‌اند؟
- آیا برای به روزرسانی سیستم هزینه اضافی باید پرداخت شود یا این سرویس به صورت مجانی ارائه می‌شود؟

۲-۶- معرفی نرم‌افزارهای متن باز فایروال

۲-۶-۱- معرفی نرم‌افزارهای سیستم عامل Linux و نرم‌افزار iptables

نرم‌افزارها و بسته‌های نرم‌افزاری متعددی برای ساخت و برپایی یک فایروال در محیط سیستم عامل Linux وجود دارد که تمامی آنها بر پایه مکانیزم Packet Filtering که جزیی از امکانات امنیتی در هسته اصلی سیستم عامل Linux می‌باشد ، عمل می‌کنند.

تا کنون ۳ مجموعه Packet Filter به‌صورت پیش فرض در هسته سیستم‌عامل Linux وجود داشته‌اند. اولین مجموعه نرم‌افزار ipfwadm است که با استفاده کد اولیه نرم‌افزار IPFW از سیستم‌عامل FreeBSD شکل گرفت و تکمیل یافت. نرم‌افزار ipfwadm پس از مدتی به نرم‌افزار ipchains در نسخه ۲.۲ هسته سیستم عامل Linux رشد یافت و در حال حاضر آخرین

نسخه نرم‌افزاری از این مجموعه iptables می‌باشد. تمامی این سه مجموعه جزئی از هسته سیستم عامل Linux بوده‌اند و به‌صورت ماژول‌های آماده به نصب (Loadable kernel modules) در هسته سیستم عامل Linux قرار می‌گیرند.

اغلب فایروال‌ها در Linux ، یک رابط کاربر نهایی برای بسته‌های نرم‌افزاری ipchains و iptables می‌باشند که به‌صورت یک یا چند اسکریپت نوشته شده و در هنگام بوت شدن سیستم و یا هر زمان دیگر اجرا شده و مجموعه قوانین کنترلی را بر روی سیستم عامل اعمال می‌کند. بعضی از فایروال‌ها هم دارای واسط‌های رابط کاربری می‌باشند که به‌صورت نمایی، می‌توان در آنها قوانین مورد نظر را تنظیم کرد.

از نسخه ۲.۴ هسته سیستم عامل Linux به بعد ، مجموعه نرم‌افزارهای امنیتی و Packet Filtering در Linux تحت عنوان Netfilter نامیده شد که تا کنون از آن در جهت راهکارهای امنیتی در سیستم عامل Linux استفاده می‌شود. کاربردها و امکانات Netfilter که بسته iptables جزء اصلی آن است به حدی بالا و قدرتمند است که بسیاری آنرا با لیست‌های دسترسی دستگاهای Cisco مقایسه می‌کنند. در زیر نگاهی اجمالی به نحوه عملکرد و مکانیزمهای موجود در Netfilter اشاره می‌شود:

مجموعه Netfilter در Linux بر پایه سه رکن اصلی می‌باشد که جهت حفظ مفاهیم فنی ، از ترجمه تحت الفظی کلمات خودداری شده است: مجموعه Rules ، مجموعه Chains و مجموعه Tables. در ادامه به توضیح این سه رکن پرداخته شده است.

۲-۶-۱-۱- مفاهیم Rules

پائین‌ترین مرحله در Netfilter ، Ruleها می‌باشند. با مشخص کردن Rule در حقیقت مشخص می‌شود که هدف عملیات Filtering یا Manipulation (دستکاری packetها) است؛ که البته اعمال تغییرات و دستکاری packetها روش‌های متفاوتی دارد. اصولا یک Rule از ۴ بخش تشکیل شده است:

- بخش Table مربوطه که این rule به آن تعلق دارد. در صورتیکه هیچ نام table ای ذکر نشود netfilter به صورت خودکار آنرا عضو table ای به نام filter که عنوانش بیانگر وظیفه آن می‌باشد، قرار می‌دهد.

- بخش Chain مربوطه که این rule به آن تعلق دارد. مثلاً این rule در هنگام ورود packet باید اعمال شود(INPUT)؛ یا در هنگامی که تصمیم به فرستادن packet به جای دیگری گرفته می‌شود(FORWARD) و یا هنگامیکه می‌خواهد از Device خروجی شبکه خارج شود(OUTPUT). البته در tableهای مختلف مراتب مختلفی وجود دارد و مواردی که در اینجا ذکر شد مربوط به filter می‌باشد.
- ساختار Filter کردن یا دستکاری در Packet. مثلاً اینکه چه قوانینی برای تصمیم‌گیری در مورد اینکه آیا یک packet باید filter بشود یا نه. این قوانین بر اساس خصوصیات متعددی می‌تواند باشد که از جمله آنها به source address و destination address و شماره درگاه ورودی یا خروجی (Port) و غیره می‌توان اشاره کرد که خود حاوی مجموعه قوانین و مکانیزمهای کامل و مفصلی می‌باشد.
- نتیجه rule. به این معنی که در صورتیکه در بخش ساختار مشخص شد که باید عملی برروی این packet انجام شود، این عمل چیست. مثلاً در بحش filter مهمترین عمل DROP یا ACCEPT می‌باشد. در بعضی موارد هدف فقط تهیه LOG از Packetها بوده و هیچگونه عمل اضافی روی آنها انجام نمی‌شود. بسته به موقعیت و table ای که در آن قرار دارد و همچنین chain مورد استفاده، می‌توان کنترل‌های مختلفی روی بسته‌های اطلاعات اعمال کرد.

۲-۶-۱-۲- مفاهیم Chain

قوانین و ruleهای ساده و ابتدایی به راحتی می‌توانند در Chainهای پیش فرض موجود قرار گیرند. تعدادی از chainها به صورت پیش فرض همیشه در اختیار مدیر شبکه قرار دارند، مانند INPUT و OUTPUT. این chainهای پیش فرض می‌توانند دارای یک نتیجه عمل پیش فرض نیز باشند، که در صورتیکه در هیچ یک از ruleهای آن chain صدق نکردند ، سیستم بداند در حالت عادی باید چه عملی را بر روی این packetها انجام دهد.

همچنین برای مدیریت فیلترها و فایروال‌ها و در بعضی موارد routeهای حجیم و زیاد، می‌توان برای آسانتر شدن کار chainهای دلخواه ایجاد کرده و آنها را به سیستم اضافه کرد. این

chainها می‌توانند خودشان شامل یک سری rule باشند که به عنوان نتیجه عمل یک یا چند rule، در chainهای پیش فرض قرار می‌گیرند.

۲-۶-۱-۳- مفاهیم Tables

به جهت ساده‌تر کردن مدیریت ruleها و منطقی کردن عمل filtering و manipulating بر روی بسته‌های اطلاعات tableها طراحی شده‌اند؛ که مجموعه ruleها در آن قرار می‌گیرند. به‌طور کلی ۳ table در حالت استاندارد در netfilter وجود داردکه عبارتند از:

table ای به نام filter که برای packet filtering استفاده می‌شود.این table، همان قسمتی است که برای درست کردن یک فایروال به آن نیاز است. همچنین این table ، table پیش فرضی است که در صورت ذکر نکردن نام هیچ table ای ruleهای فایروال در آن قرار می‌گیرند.

table ای به نام nat که وظیفه آن ترجمه packetها است. به این معنی که می‌توان در این table مقصد و یا منبع packet را به آدرس‌های دیگری تغییر داده و آنها را مدیریت نمود. IP Masquerading که بسیار مشهور بوده و کاربرد بالایی دارد و برای ایجاد دسترسی IPهای Invalid به شبکه استفاده می‌شود، در این قسمت قرار دارد.

table ای به نام mangle که شامل ruleها و chainهایی است که خواص دیگری از packet را تغییر داده و یا اینکه آنها را علامت‌گذاری می‌کنند که توسط برنامه دیگری و در زمان دیگری استفاده شوند. این table کاربرد چندانی برای استفاده در موارد ساده و معمولی ندارد. اما برای application layer filtering فوق العاده مهم و توانمند می‌باشد.

اکثر مدیران شبکه‌ها بر این باورند که امکاناتی که Netfilter در Linux برای انجام Firewalling و Translation در اختیار قرار می‌دهد، حتی از PIX که محصولی خاص در امنیت Cisco می‌باشد متنوع‌تر است. اما تنها ضعفی که در سرویس‌های Netfilter در نسخه هسته ۲.۴ در لینوکس وجود دارد این است که مدیریت آن بسیار مشکل است و امکان بروز اشتباه در آن بسیار زیاد است. این سرویس از نظر کیفیت، قابلیت و تنوع، تقریباً بی‌رقیب می‌باشد. معمولا قیمت سخت‌افزارهای تجاری آماده مانند Cisco و نرم‌افزارهای آنها بسیار بالا است و نیازمند کسب امتیاز استفاده[1] از شرکت سازنده می‌باشند. فایروال‌های تجاری به هنگام مواجهه با حجم

[1] License

بالای انتقال اطلاعات، نیازمند سخت‌افزارهای بسیار قوی و گران می‌باشند در حالیکه این مشکل در ابزارهای متن باز که مبتنی بر سیستم‌عامل‌های متن‌باز هستند، با سخت‌افزارهایی متداول در بازار مانند سخت‌افزارهای PC سازگار هستند به مشکل تهیه سخت‌افزار وجود ندارد.

با استفاده از یکی از ماژول‌های Netfilter به راحتی می‌توان دسترسی کاربران و اجزای شبکه را بر اساس نوع سیستم عامل محدود نمود. به عنوان مثال می‌توان اجازه استفاده از پورت X را فقط به کاربران سیستم عامل ویندوز در شبکه داد و یا مواردی اینچنین را برای انواع مختلفی از سیستم عامل‌ها اعمال نمود. با استفاده از این ماژول به راحتی می‌توانید با ruleای مانند زیر دسترسی کاربران ویندوز به ICMP را محدود نمود.

iptables -A INPUT -p icmp- m osf-- genre Windows -j REJECT

کارایی این ابزار برای مدیران شبکه که خواهان مبارزه با ویروس‌ها و Wormهای ویندوز هستند بسیار بالا می‌باشد. مثلاً می‌بایست پورت مربوط به TFTP را برای ویندوز مسدود نمود؛ چون بعضی از Wormها از طریق این پورت کار می‌کنند، اما اگر این کار را برای همه کاربران انجام دهید، دیگر کسی هم که واقعاً می‌خواهد از TFTP استفاده کند نمی‌تواند از آن استفاده کند. سیستم عامل‌هایی را که بر اساس آنها می‌توان Ruleهای امنیتی را تعریف کرد عبارتند از: Linux, FreeBSD, NetBSD, OpenBSD, Windows . معادل این دستور در سیستم عامل BSD و نرم‌افزار ipfw و سیستم‌عامل OpenBSD نیز وجود دارد، ولی تمامی پارامترهای این Module در iptables را ندارد.

از نسخه ۲.۴ هسته Linux به بعد، پیشرفت امکانات Networking در Linux بسیار چشمگیر بوده و سرعت و کارایی آن بسیار بالاتر از سایر رقبای خود شده است. یکی از این موارد که Netfilter در آن از سایر نرم‌افزارهای مشابه متمایز است، قدرت این نرم‌افزار در NAT می‌باشد که امکانات متنوعی را ارائه می‌کند. پیاده سازی NAT در Cisco کمی پیچیده بوده و در عین حال نیازمند منابع سخت‌افزاری مناسب می‌باشد که در صورت حجم بالای عملیات نیازمند RAM و CPU قدرتمند می‌باشد. بعلاوه یکی از دیگر مزیت‌های NAT در Linux وجود ماژول‌های زیاد برای برنامه‌ها و پروتکل‌های مختلف می‌باشد، که در حالت عادی در سیستم‌های NAT شده، کار نمی‌کنند. این ماژول‌ها همگی در نرم‌افزار Netfilter و هسته سیستم‌عامل لینوکس وجود دارند و قابل اضافه کردن و فعال شدن هستند. از جمله مهمترین این ماژول‌ها ، وجود ماژول H323 برای پشتیبانی از پروتکل H.323 در محیط NAT شده می‌باشد که در

حالت عادی این پروتکل به علت ماهیت دوطرفه بودن آن، در محیط NAT شده کار نمی‌کند. از جمله برنامه‌هایی که از این پروتکل استفاده می‌کنند Net meeting و بسیاری از Voice Chat وVideo Chat هستند.

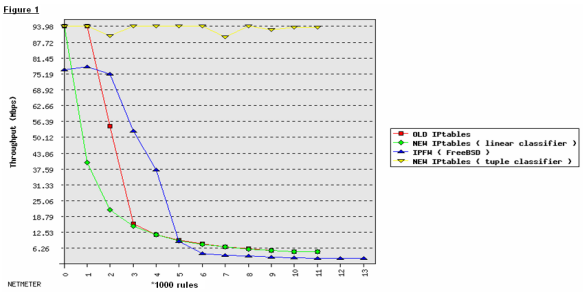
۲-۶-۱-۴- مزایا و معایب iptables و برنامه‌های دیگر برای سیستم عاملLinux

نرم‌افزار iptables به علت تنوع امکانات و ویژگی‌های گسترده‌ای که دارد، برترین نرم‌افزار Packet Filtering متن‌باز در حال حاضر محسوب می‌شود. اشکال این نرم‌افزار کاهش چشمگیر سرعت عملکرد آن با افزایش تعداد ruleها است. سرعت این نرم‌افزار با افزایش هر ۱۰۰۰ عدد rule، به صورت تصاعدی نصف می‌شود. برای حل این مشکل نرم‌افزارهای زیر به وجود آمده‌اند.

نرم‌افزار nf-hipac مشابه iptables برای Packet Filter استفاده می‌شود و از ساختار درختهای دودویی (binary tree) برای ذخیره سازی و ارزیابی ruleها استفاده می‌کند. رابط کاربری این برنامه بسیار شبیه به برنامه iptables است و می‌توان از امکانات برنامه nf-hopac در کنار برنامه iptables استفاده کرد. سرعت برنامه nf-hipac برای چندین هزار rule مانند برنامه iptables برای بیست rule می‌باشد.

نرم‌افزار Compact Filter یا به اختصار CF مانند iptables یک بسته Packet Filter دیگر برای سیستم‌عامل لینوکس است. این نرم‌افزار بسیار ساده‌تر و سریع‌تر از برنامه iptables عمل می‌کند ولی در عوض کارایی و قابلیت‌های کمتری نسبت به iptables دارد. این برنامه ruleها را در محیط کاربری (User Space) تولید و به‌صورت بهینه و فشرده به هسته سیستم منتقل می‌کند.

نرم‌افزار iptables with classifiers با روشی نوین به نام tuple classifier امکانات نوین به برنامه iptables اضافه می‌کند که سرعت نرم‌افزار iptables را به میزان قابل توجهی افزایش می‌دهد.



شکل ۲-۳۲: مقایسه میزان عرض باند خروجی

در شکل(۲-۳۲) مقایسه میزان عرض باند خروجی (Throughput) بر حسب تعداد rule در یکصد هزار، در نرم‌افزار iptables عادی (OLD Iptables)، نسخه نوین با امکانات Linear Classifier و نسخه نوین دیگر با امکانات Tuple Classifier و نرم‌افزار IPFW در سیستم‌عامل FreeBSD با یکدیگر مقایسه شده‌اند. برای کسب اطلاعات بیشتر در ارتباط با شرایط مقایسه به سایت iptables with classifiers در http://www.geocities.com/hamidreza_jm مراجعه فرمایید.

نرم‌افزار ipset مشابه نرم‌افزارهای فوق، به عنوان یک جایگزین برای iptables نیست و فقط روش‌های نوین برای ذخیره سازی ruleها و روش‌های کنترل نوین برای iptables می‌باشد که سرعت عملکرد برنامه iptables را به میزان قابل توجهی افزایش می‌دهد.

همان‌طور که گفته شد، نرم‌افزار iptables غنی‌ترین برنامه متن‌باز در زمینه Packet Filter است و جوابگوی بسیاری از نیازها خواهد بود. در صورتیکه تعداد ruleها زیاد شوند (بیش از ۱۰۰) و عرض باند عبوری از فایروال زیاد و با اهمیت باشد، می‌توان از ترکیب این نرم‌افزار با نرم‌افزارهای فوق استفاده کرد و فایروال بهتری ساخت.

۲-۶-۲- معرفی نرم‌افزارهای سیستم عامل FreeBSD و نرم‌افزار IPFW

سیستم‌عامل FreeBSD دارای سه برنامه متداول برای برپایی فایروال می‌باشد. این ابزارها عبارتند از برنامه IPFilter که در این سیستم‌عامل به نام IPF شناخته می‌شود، برنامه IPFirewall که در این سیستم‌عامل به نام IPFW شناخته می‌شود و برنامه فیلترینگ بسته‌ها در سیستم‌عامل OpenBSD که به سیستم‌عامل FreeBSD هم منتقل شده است و با نام PF شناخته می‌شود. غیر از این ابزارها، سیستم‌عامل FreeBSD دارای دو ابزار برای کنترل پهنای باند و ترافیک شبکه دارد که این برنامه‌ها عبارتند از برنامه dummynet و برنامه altq. وجود سه برنامه مختلف در سیستم‌عامل FreeBSD برای برپایی فایروال به علت اختلاف نیازهای اولیه برای طراحی فایروال در شبکه‌های مختلف و متفاوت می‌باشد. این برنامه‌ها هریک دارای قابلیت‌های مختلف و کارایی متفاوتی می‌باشند. آقای ژوزف باربیش نویسنده فصل ۲۶ کتاب FreeBSD Handbook (مبحث Firewallها) که معتبر ترین کتاب در زمینه سیستم‌عامل FreeBSD است، برنامه IPFilter را نسبت به برنامه‌های دیگر فایروال در این سیستم‌عامل

ترجیح می‌دهد و علت آن را سادگی دستورات State Full این ابزار در محیط NAT و وجود یک FTP Proxy در داخل این برنامه عنوان می‌کند. دقت شود که نرم‌افزار IPFilter مستقل از سیستم عامل FreeBSD است و بر روی اکثر نسخه‌های BSD و همچنین نسخه‌هایی از Linux و Solaris قابل اجرا و استفاده است. از آنجا که برنامه IPFilter ویژه سیستم‌عامل FreeBSD نیست، از توضیح این برنامه در این قسمت صرف نظر می‌کنیم و در ادامه به این برنامه خواهیم پرداخت.

همان‌طور که گفته شد، برنامه PF از سیستم‌عامل OpenBSD به سیستم‌عامل FreeBSD منتقل شده است. در صورتیکه هدف از استفاده از سیستم‌عامل FreeBSD وجود برنامه PF باشد، بهتر است از سیستم‌عامل OpenBSD که نسخه به‌روزتر این برنامه را دارد، استفاده شود. در اینجا، تشریح مفصل‌تر برنامه PF در بخش معرفی برنامه‌های سیستم‌عامل OpenBSD ارائه شده است.

برنامه IPFIREWALL یا IPFW یکی دیگر از ابزارهای فیلترینگ بسته‌های اطلاعاتی (Packet Filtering) می‌باشد که توانایی برپایی فایروال و کنترل ترافیک شبکه‌ها را به کمک برنامه dummynet دارد. برنامه IPFW منحصر به سیستم‌عامل FreeBSD است و مادر بسیاری از برنامه‌های Packet Filter دیگر مانند برنامه IPTables در لینوکس می‌باشد. در حال حاضر نسخه‌های چندانی از این برنامه به صورت اولیه در سیستم‌عامل‌های دیگر وجود ندارد و نسخه‌های منتقل شده همه مانند IPTables کاملا ارتقاء و تکامل یافته‌اند تا جایی که دیگر با IPFW قابل مقایسه نیستند. شایان ذکر است نسخه‌ای از این برنامه به سیستم‌عامل ویندوز نیز منتقل شده که از آدرس wipfw.sourceforge.net قابل دریافت می‌باشد.

برنامه IPFW از stateless rules و تکنولوژی Rule Coding برای پیاده سازی منطق Stateful ساده استفاده می‌کند. استفاده از امکانات خاص برنامه IPFW احتیاج به دانش فنی بسیار زیادی مانند درک بخش سرآمد پروتکل‌ها در معماری TCP/IP دارد.

برنامه IPFW شامل ترکیب هفت جزء نرم‌افزاری است که امکانات و توانمندی‌های گوناگون را به این برنامه می‌دهند. مهمترین جزء، امکانات Packet Filter و امکانات محاسبه آن است. امکانات دیگر مانند Logging ، امکان divert که امکان انتقال و ترجمه آدرس‌ها (NAT) را به‌وجود می‌آورد، برنامه dummynet که امکان کنترل ترافیک و پهنای باند را به‌وجود می‌آورد، امکان fwd rule ، امکان برقراری پل (Bridge) و امکان ipstealth می‌باشد.

۲-۶-۳- معرفی نرم‌افزارهای سیستم عامل OpenBSD و نرم‌افزار PF

نرم‌افزار Packet Filter که به طور مختصر PF نامیده می‌شود، سیستم فیلترینگ و فایروال در سیستم‌عامل OpenBSD است که به بسیاری از سیستم‌عامل‌های دیگر مانند FreeBSD، NetBSD و DragonFlyBSD نیز منتقل شده است. نسخه‌هایی از این برنامه حتی برای ویندوز نیز وجود دارد که البته قابلیت‌های بسیار کمتری دارند. این برنامه توسط Daniel Hartmeier نگارش شده و جایگزین برنامه IPFilter بوده است. علت جایگزین کردن برنامه IPFilter، منع شدن تیم توسعه دهندگان OpenBSD از توسعه و تغییر در کد اولیه این برنامه بوده است. نرم‌افزار PF دارای الگوی دستوری شبیه به IPFilter است و در حال حاضر این نرم‌افزار مزایای مختلفی نسبت به IPFilter اولیه دارد. این نرم‌افزار قدرت ترجمه آدرس‌های اینترنتی (NAT) و QOS را به خوبی دارد که کد مربوط به QOS از برنامه ALTQ به این برنامه منتقل شده است.

برنامه PF سه کاربرد اولیه دارد: ۱- نرمال کردن بسته‌های اینترنتی (Packets) ۲- فیلتر کردن بسته‌ها (Filtering) ۳- ترجمه‌ها (Translations). بجز کاربردهای اولیه این برنامه می‌توان کاربردهای زیر را نیز به این برنامه اضافه کرد: ۱- تسکین حملات DOS (Denial of Service Mitigation) ۲- امکان Redundancy در فایروال‌ها (Firewall Redundancy) ۳- تقسیم بار (Load Balancing).

۲-۶-۳-۱- قابلیت نرمال کردن بسته‌های اینترنتی در برنامه PF

نرمال کردن بسته‌های اینترنتی (Packets) شامل موارد زیر است:

- نرمال کردن محتوای بسته‌ها (Packet Content) و رفع ابهامات
- روال جمع آوری بسته‌های fragment شده در پروتکل IP (IP fragment reassembly)
- نرمال کردن آدرس‌های اینترنتی (IP normalization)

نرمال کردن پروتکل TCP (TCP normalization) شامل :

- استفاده غلط از ترکیب پرچمهای TCP/IP (Illegal flag combinations)
- گزینه‌های پروتکل TCP (TCP options)
- حفاظت در مقابل سلسله شماره‌های پیچیده (Protect Against Wrapped Sequence Numbers)

- تاکید برای استفاده از حداقل TTL (Enforce minimum TTL)

۲-۶-۳-۲- امکانات فیلترینگ در برنامه PF

قابلیت‌های فیلترینگ این برنامه به شرح زیر هستند:

ویژگی‌های قابل فیلتر کردن (Filterable Attributes):

- بر اساس واسط ارتباطی (Interface)
- جهت ارتباط (Direction)
- پروتکل بسته (Protocol)
- آدرس فرستنده و یا گیرنده (Source/destination address)
- فیلد TOS
- بر اساس Fragments
- بر اساس گزینه‌های پروتکل IP (IP Options)
- بسته‌های علامت خورده (Tagging)
- پورت ارسال یا دریافت در پروتکل TCP و UDP (Source/destination port)
- کد و نوع ICMP
- پرچم‌های پروتکل TCP (TCP flags)
- OS منبع (Source OS)
- قوانین Stateful (Stateful Rules)
- بخش Tables
- بخش Anchors

۲-۶-۳-۳- انواع ترجمه در برنامه PF

قابلیت‌های ترجمه این برنامه به شرح زیر هستند:

- ترجمه آدرس منبع یا nat (source address translation)
- ترجمه آدرس مقصد یا rdr (destination address translation)
- ترجمه آدرس دو طرفه یا binat (bidirectional address translation)

۲-۶-۳-۴- مقابله و تسکین حملات DOS در برنامه PF

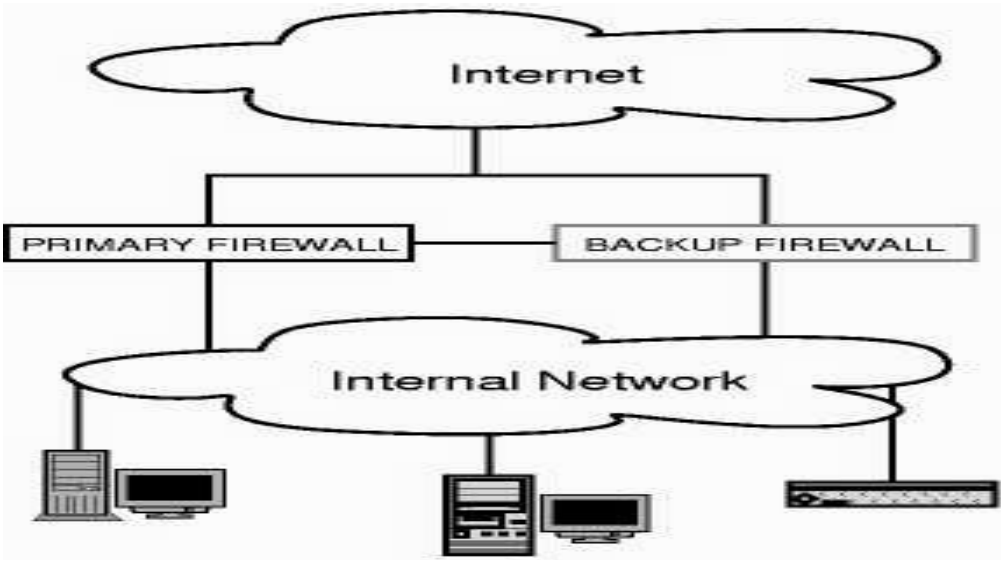
تسکین حملات DOS (Denial of Service Mitigation):

- قابلیت synproxy برنامه PF اعلان آمادگی (handshake) سه طرفه TCP را کامل و نظارت می‌کند. این باعث حفاظت در مقابل spoofed TCP SYN floods خواهد شد.
- قابلیت تنظیم Timeout برای stateها و سایر موارد.
- قابلیت‌های max-src-states به مفهوم محدود کردن تعداد همزمان وضعیت‌های (State) یک آدرس اینترنتی و max-src-nodes به مفهوم محدود کردن تعداد آدرس‌های اینترنتی که همزمان می‌توانند تولید وضعیت (State) کنند.
- قابلیت ALTQ برای اعمال محدودیت در میزان عرض باند با اعمال دسته بندی‌ها و اولویت بندی‌های مختلف است.
- قابلیت بر طرف کردن تراکم صف ورودی (Input queue congestion handling) در حالیکه کامپیوتر زیر بار سنگین حمله DOS باشد، بسته‌های اینترنتی Stateful عبور می‌کنند و بسته‌های Stateless از بین می‌روند. در این حالت ماشین همچنان در دسترس خواهد بود.

۲-۶-۳-۵- امکان Redundancy در فایروال‌ها با برنامه PF

امکان Redundancy در فایروال‌ها (Firewall Redundancy) به معنی وجود دو فایروال همزمان است. در این مدل، هر گاه فایروال‌های اصلی (Master Firewall) به دلایل مختلف مانند اختلال برق، از کار افتاد، فایروال آماده به خدمت (Standby Firewall) به سرعت و به‌صورت اتوماتیک جایگزین فایروال اول می‌شود. به کمک برنامه CARP و pfsync می‌توان از دو دستگاه فایروال برای Redundant کردن استفاده کرد. ابزار CARP برنامه‌ای است که به گروهی از کامپیوترها امکان استفاده از یک آدرس اینترنتی IP را فراهم می‌کند. در مدل برنامه CARP یک کامپیوتر به صورت کامپیوتر اصلی (Master) و یک یا چند کامپیوتر به صورت آماده به خدمت(Backup or Standby) قرار می‌گیرند. کامپیوتر اصلی همواره حضور خود را به کامپیوترهای آماده به خدمت اعلام می‌کند. در صورتیکه یک کامپیوتر آماده به خدمت در یک

زمان مشخص، اعلام آمادگی دستگاه اصلی را نبیند، خود به خود با همان آدرس اینترنتی (IP) کامپیوتر اصلی شروع به کار می‌کند.



شکل ۲-۳۳: Redundancy در فایروال‌ها

برنامه pfsync نیز برای اعلام وضعیت برنامه PF می‌باشد. این برنامه می‌تواند وضعیت برنامه PF را به صورت Broadcast به شبکه محلی ارسال کند. ترکیب برنامه pfsync و CARP می‌تواند امکان رفع اشکال را در سیستم فایروال را به کمک دو دستگاه فراهم کند.

۲-۶-۳-۶- تقسیم بار ترافیک به کمک برنامه PF

به کمک برنامه PF می‌توان از الگوریتم‌های تقسیم بار (Load Balancing) به منظورهای زیر استفاده کرد:

- ترجمه آدرس (NAT) و ارسال ترافیک خروجی یک شبکه به چندین ارائه دهنده (Gateway).
- تقسیم بار ورودی یک سرور به چند سرور.
- تقسیم بار خروجی به چند Gateway (در صورت عدم وجود BGP).

۲-۶-۴- معرفی نرم‌افزار IPFilter

تا کنون سه برنامه iptables، IPFirewall و PF معرفی و عنوان شده‌اند. اکنون به معرفی برنامه IPFilter یا به اختصار IPF می‌پردازیم. برنامه IPF توسط آقای دارن رید نگارش شده است و یک برنامه قابل انتقال به انواع سیستم‌عامل‌ها است. این برنامه می‌تواند به صورت یک ماژول خارجی یا در قلب هسته سیستم‌عامل باشد ولی نویسنده برنامه توصیه کرده تا در صورت امکان به‌صورت یک ماژول از این برنامه استفاده شود. آخرین نسخه از این برنامه 4.1.15 در تاریخ November 3, 2006 ارائه شده و توسعه این برنامه بسیار سریع است. این برنامه به‌صورت پیش فرض در سیستم‌عامل‌های زیر حضور دارد:

FreeBSD-current (post 2.2): http://www.freebsd.org/
NetBSD-current (post 1.2): http://www.netbsd.org/
xMach: http://www.xmach.org/
Solaris 10: http://www.sun.com/solaris
Open Solaris: http://www.opensolaris.org/
AIX 5.3 ML05: http://www.ibm.com/aix

همچنین در سیستم‌عامل‌های زیر قابل استفاده است:

Solaris/Solaris-x86 2.3 - 9
SunOS 4.1.4 - 4.1.4
NetBSD 1.0 - 1.4
FreeBSD 2.0.0 - 2.2.8
BSD/OS-1.1 - 4
IRIX 6.2, 6.5
OpenBSD 2.0 - 3.5
Linux 2.4 - 2.6
HP-UX 11.00 (IPFilter 4.0alpha)
Tru64 5.1a

۲-۶-۴-۱- اجزای برنامه IPF

برنامه IPF با مجموعه دستورات زیر قابل کنترل است:

- برنامه ipf: این برنامه، دستورات را از ورودی استاندارد یا فایل دریافت و به هسته منتقل می‌کند.
- برنامه ipfstat: این برنامه، وضعیت برنامه IPF را نمایش می‌دهد.
- برنامه ipftest: این برنامه دستورات IPF را از یک فایل خوانده و نمونه‌ای از بسته‌ها را به این دستورات اعلام می‌کند تا نتیجه دستورات مشخص شود.

- برنامه ipmon: اطلاعات را از دستگاه خروجی خوانده و نمایش یا ذخیره در فایل و یا ثبت در Syslog می‌کند.
- برنامه ipsend: بسته‌های اطلاعاتی اختیاری تولید می‌کند.
- برنامه ipresend: اطلاعات مجموعه‌ای از بسته‌ها را از فایل خوانده و ارسال می‌کند.
- برنامه iptest: شامل مجموعه‌ای از برنامه‌ها برای روتین‌های آزمایشی است.
- برنامه ipnat: مانند برنامه ipf دستورات را از ورودی استاندارد یا فایل خوانده و به جدول nat در هسته اضافه می‌کند.

۲-۷- ویژگی‌های سیستم فیلترینگ محتوا

برخی از فایروال‌ها یا خود دارای سیستم فیلترینگ محتوا هستند و یا اینکه قادرند از طریق پروتکلهای استاندارد با این‌گونه سیستم‌ها ارتباط برقرار کنند. این قابلیت به فایروال اجازه می‌دهد که محتویات بسته‌های مربوط به ارائه کاربر را مورد بررسی و آنالیز قرار دهد.

یک نمونه کاربرد این سیستم، کنترل محتویات emailها از نظر وجود ویروس و یا هرگونه داده خطرناک دیگر است. مثال دیگر کنترل و جلوگیری از دانلود شدن محتویات خطرناک نظیر java appletها و Activex به داخل سازمان است.

یکی از محدودیت‌های سیستم‌های فیلترینگ آن است که برای اینکه بتوان عملیات بررسی و کنترل را انجام داد حتماً باید داده‌ها به صورت Clear و رمزنشده باشند.

۲-۷-۱- فیلترینگ محتوا چیست؟

یک فیلتر محتوا ترکیبی از یک یا چند نرم‌افزار است که مانع از دسترسی کاربران به داده‌های خاصی روی اینترنت می‌شود. این فرایند از دو جزء تشکیل شده است:

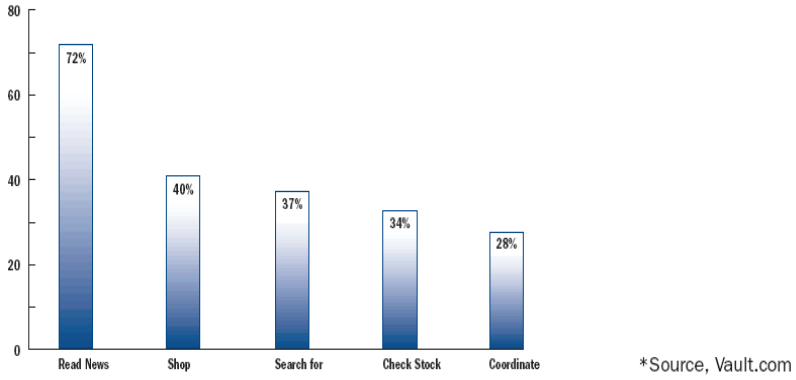
- Rating: مقداری است که برای دسته‌بندی سایت‌ها بر اساس محتویات آنها به کار می‌رود. این مقدار ممکن است در خیلی از نرم افزاهای فیلترینگ فقط دو ارزش مجاز و غیر مجاز داشته باشد و یا در بعضی از نرم‌افزارهای فیلترینگ مبتنی بر PICS ممکن است ارزشهای مختلف دیگری نیز داشته باشد.
- Filtering: نرم‌افزار فیلترینگ هر درخواست کاربر را مورد وارسی قرار می‌دهد تا مشخص شود آیا کاربر حق دسترسی به آن را دارد یا خیر. اگر سایت در دسته غیر

مجازها باشد و یا در سیستم PICS مقدار مورد نظر را نداشته باشد یک پیـام خطـا به کاربر نشان داده می‌شود.

۲-۷-۲- چرا باید فیلترینگ محتوا داشته باشیم؟

استفاده از سیستم‌های فیلترینگ محتوا هم از نظر امنیتی ضروری است تا از ورود داده‌های مخرب و خطرناک به داخل شبکه محلی و یا کامپیوتر شخصی مقابله شود و هم از نظر اقتصادی برای سازمان‌هایی که به کارمندان خود اجازه دسترسی به اینترنت را داده‌اند مفید است تا مانع از وبگردی و اتلاف وقت کارمندان خود شوند و هم برای خانواده‌هایی که به حفظ حریم خانواده خود اهمیت می‌دهند کمک می‌کند تا کودکان خود را در مقابل محتویات غیر اخلاقی اینترنت محافظت کنند. البته در هر صورت جلوگیری از عبور و مرور ترافیکهای غیر ضروری و غیر مفید باعث صرفه‌جویی در مصرف پهنای باند و کاهش هزینه‌های مربوط به آن و نیز افزایش سرعت برنامه‌های کاربردی مفید خواهد شد. فیلترینگ به عنوان بازدارنده عمل می‌کند ولی در بعضی از موارد ما به سیستم‌های مونیتورینگ محتوا نیاز داریم. اکثر سیستم‌های فیلترینگ محتوا قابلیت مونیتورینگ را نیز دارند.

امروزه در کشورهای پیشرفته حدود ۳۰ درصد از کارمندان در محیط کار به اینترنت دسترسی دارند. طبیعی است رعایت اخلاق کاری و نیز ملاحضات اقتصادی باعث توجه مدیران اینگونه شرکت‌ها و سازمان‌ها به کنترل دسترسی افراد به اینترنت خواهد شد. مهمترین و اصلی‌ترین راهکار استفاده از سیستم محدودیت دسترسی به سایت‌های مشخص بوده است. طبق بررسی‌های انجام شده حدود ۷۰ درصد از دسترسی‌های غیر مجاز به سایت‌های غیر اخلاقی و جنسی در ساعت‌های کاری بوده است. حدود ۳۰ تا ۴۰ درصد کاربران به سایت‌هایی دسترسی دارند که اصلاً ربطی به کار آنها ندارد. دسترسی به محتویاتی نظیر موسیقی و فیلم در اینترنت که روز به روز در حال افزایش است علاوه بر اتلاف وقت، مقدار زیادی از پهنای باند مفید سازمان را نیز اشغال می‌کند. در شکل زیر میزان و نحوه استفاده از اینترنت توسط کارمندان تشریح شده است. ۸۰ درصد کارمندان در بررسی‌ها اذعان داشته‌اند که در هنگام کار از اینترنت برای استفاده‌های شخصی استفاده کرده‌اند.



شکل ۲-۳۴: میزان و نحوه استفاده از اینترنت توسط کارمندان

متاسفانه تنها راه دسترسی به اینترنت استفاده از یک برنامه مرورگر و سایت‌های اینترنتی نیستند. امروزه برنامه‌های متعددی نظیر messengerها و نامه‌های الکترونیکی و پیوست‌های آنها و برنامه‌های متعدد p2p وجود دارند که استفاده از آنها رواج پیدا کرده است. بررسی آماری توسط CSI نشان می‌دهد که تنها ۲۰ درصد از استفاده‌های غیر مجاز مربوط به دسترسی به سایتهای غیر مجاز است و ۸۰ درصد از تخلفات مربوط به استفاده از سایر برنامه‌های کاربردی است. در شکل زیر خطرات استفاده از برنامه‌های کاربردی مختلف دیگر نشان داده شده است.

Misuse	Description
General	• 30% of Web surfing is not work related
Hacking	• 75% of the companies cited employee as a likely source of hacking attacks. While 45% of business had reported unauthorized access by insiders. (*CSI/FBI Computer Crime and Security Survey, 2003*)
IMv	• More than 43 million users misuse IM at the workplace (*IDC, 2003*)
P2P	• 45% of the executable files downloaded through popular P2P network Kazaa contain malicious code (*TrueSecure, 2004*)
Legal	• A company can be liable to $150k per pirated work for allowing employees to use company network to download copyrighted material (*RIAA, 2003*) • 27% of fortune 500 companies have battled sexual harassment claims stemming from employee misuse. (*American Management Association*)
Porn	• 70% of the pornography is downloaded between 9am to 5pm (*SexTracker*)
Streaming Media	• 77% of online listening to Internet Radio on week days take place between 9am to 5pm, pacific time (*Arbitron, 2004*) • 44% of corporate employees actively use streaming media. (*NielsenNetRatings*)

Source: Vijay Gawde, ITSecurity.com, *http://www.itsecurity.com/papers/gawde1.htm*

شکل ۲-۳۵: خطرات استفاده از برنامه‌های کاربردی مختلف هنگام استفاده از اینترنت توسط کارمندان

۲-۷-۳- فیلترینگ محتوا در اینترنت

امروزه تعداد بسیار زیادی از کارمندان در گوشه کنار دنیا در ساعات کاری online هستند. همچنان که کسب وکار در حال پیشرفت است، خطوط پرسرعت اینترنتی و دسترسی‌های Dialup در حال افزایش است از طرفی تجارت الکترونیک در حال همه گیر شدن است لذا قابلیت دسترسی به اینترنت به عنوان یک نیاز حتمی تلقی می‌شود. استفاده نابجا از اینترنت مانند بازی‌های اینترنتی، سایت‌های قمار، هرزه نگاری از جمله مواردی است که مسئولین سازمان‌ها را به این فکر انداخته است که در صدد جلوگیری از دسترسی به برخی سایت‌ها شوند. از طرفی دیگر اطلاعات محرمانه سازمان‌ها می‌تواند از طریق ایمیل‌های شخصی در خطر باشد.

اکثر سازمان‌ها به این نتیجه رسیده‌اند که کارمندان وقت بسیاری را صرف استفاده‌های غیرکاری از اینترنت می‌کنند و پهنای باند زیادی از شبکه را اشغال کرده و مانع از کارایی مفید می‌شوند. از این رو نیاز به فیلترینگ اینترنت برای افزایش کارایی کسب وکارروز به روز برای سازمان‌ها حیاتی تر خواهد بود.

۲-۷-۴- لزوم سیاست گذاری در دسترسی به وب

چه کسی؟ چه وقت؟ چه سایتهایی؟ چه فعالیت‌هایی؟ چه عواقبی؟ روی چه سرویس هایی؟

فیلترینگ محتوا روی سرویس‌های مختلف و با اهداف مختلف قابل انجام است. از مهمترین اهداف فیلترینگ محتوا مقابله با فایل‌های مخرب و خطرناک و نیز مقابله با داده‌های عمدتاً غیر اخلاقی است. در این قسمت ما تمرکز خود را روی موضوع فیلترینگ سایت‌های اینترنتی (URL Filtering) و با هدف کنترل سایت‌های غیر اخلاقی معطوف می‌کنیم. در این بررسی به تکنیکهای مختلف دسته‌بندی سایت‌ها و روش‌های مختلف فیلترینگ خواهیم پرداخت.

اتکا به سیستم فیلترینگ سایت‌های اینترنتی برای مقابله با تهدیدهای رایج استفاده از شبکه به هیچ وجه کافی نیست. سیستم مونیتورینگ و فیلترینگ محتوا باید در کنار سیستم فیلترینگ سایت‌ها به کار برده شود. در واقع حداقل سرویس‌هایی که باید از نظر محتوایی مونیتور و فیلتر شوند عبارتند از :

روی سرویس www

- بررسی و تطابق urlهای درخواستی با بانک اطلاعاتی
- بررسی و کنترل محتویات وب از نظر وجود کلمات کلیدی خاص
- بررسی و کنترل محتویات وب از نظر وجود کُدها و داده‌های مخرب و ویروس‌ها
- تشخیص محتویات وب روی تمامی پورت‌ها

روی سرویس mail

- بررسی و تطابق آدرس فرستنده نامه با بانک اطلاعاتی
- بررسی و کنترل محتویات نامه از نظر وجود کُدها و داده‌های مخرب و ویروس‌ها
- مقابله با نامه‌های ناخواسته
- مقابله با نامه‌هایی با محتویات غیر اخلاقی و غیر مجاز

روی سرویس messengerها

- بررسی و تطابق آدرس فرستنده نامه با بانک اطلاعاتی
- بررسی و کنترل محتویات متن‌ها وفایل‌های جابجا شده از نظر وجود کُدها و داده‌های مخرب و ویروس‌ها
- مقابله با مبادله پیام‌ها و فایل‌های غیر اخلاقی و غیر مجاز
- تشخیص نوع پروتکل messenger روی پورت‌های مختلف

روی سرویس p2p ها

- بررسی و تطابق آدرس سرورهای مجاز
- تشخیص پروتکل مورد استفاده با بررسی ترافیک تمامی پورت‌ها
- بررسی و کنترل محتویات فایل‌ها از نظر وجود کُدها و داده‌های مخرب و ویروس‌ها
- بررسی و کنترل کلمات جستجو
- مقابله با فایل‌های با محتویات غیر اخلاقی و غیر مجاز

۲-۷-۵- روش‌های اِعمال فیلترینگ URL

فیلترینگ استاتیک

- بر اساس لیستی از آدرس سایتها
- بر اساس ip و پورت
- بر اساس کلمات کلیدی در هنگام جستجو
- بر اساس کلمات کلیدی در متن

فیلترینگ دینامیک

- بر اساس پردازش محتوای صفحه و لینکها
- بر اساس پردازش تصاویر
- استفاده از مکانیزم PICS

ویژگی‌های یک سیستم فیلترینگ

- سرعت به روز رسانی پایگاه داده
- پشتیبانی از پروتکل‌های مختلف
- عدم تاثیر در کارایی شبکه

۲-۷-۵-۱- مکانیزم مونیتورینگ و فیلترینگ محتوا

در این قسمت به بررسی مفهومی site blocking و مونیتورینگ و فیلترینگ محتوا پرداخته می‌شود ضمن آنکه به لزوم استفاده از مونیتورینگ و فیلترینگ محتوا در کنار site blocking اشاره خواهد شد.

مونیتورینگ و فیلترینگ محتوا یعنی توانایی مونیتور کردن و فیلتر کردن محتویات اینترنت و Chat roomها و Messengerها و نامه‌های الکترونیکی و پیوست‌های آنها. سیستم‌های مونیتورینگ و فیلترینگ محتوا ضمن بررسی اطلاعات ارسالی به اینترنت و یا دریافتی از آن و مقایسه آن با یک کتابخانه از کلمات کلیدی و عبارات در مورد تردد آن تصمیم‌گیری می‌کنند. این تصمیم‌گیری ممکن است منجر به اجازه عبور و یا عدم اجازه عبور و یا صرفاً ثبت درخواست و یا ترکیبی از این موارد باشد. معمولاً در این سیستم‌ها با نصب یک agent روی

ایستگاه‌های کاری دسترسی کاربر به سایت‌های غیر مجاز شناسایی شده و در سرور اصلی به طور کامل به عنوان یک نقض قانون توسط کاربر ثبت می‌شود که بعداً در قسمت گزارش‌گیری از آن استفاده خواهد شد.

استفاده از یک کتابخانه از کلمات کلیدی اجازه می‌دهد که صرفاً روی محتویاتی که ممکن است ناقض قانون استفاده از اینترنت در سازمان است متمرکز شویم. برای مثال مسائل جنسی ترمینولوژی خاص خود را دارد. در یک سیستم مونیتورینگ/فیلترینگ محتوا اجاز عبور کلماتی که با مباحث پزشکی و علمی مشترک است را می‌دهد بدون آنکه سیستم نقض قانون آن رخدادی را ثبت کند. برای مثال کلمه "breast" کلمه‌ای است که در هر دو دسته‌بندی جای می‌گیرد. استفاده از سیستم کلمات کلیدی حتی به سیستم اجازه می‌دهد جلوی خروج داده‌های مهم و محرمانه از سازمان را بگیرد. روش انجام این کار تعریف کلمات کلیدی نشان‌دهنده اطلاعات محرمانه شرکت و سپس فعال شدن سیستم در صورت کشف محتویاتی با چنین کلمات کلیدی است.

سیسیتم فیلترینگ محتوا روی تمامی محتویات اینترنت عمل می‌کند و نه صرفا روی وب‌سایت‌ها. با توجه به اینکه این سیستم با سیستم‌عامل کاربر نیز در ارتباط است (از طریق agent) می‌تواند تمامی انواع محتویات موجود در سیستم را نیز با کتابخانه کلمات کلیدی مقایسه کند.

استفاده از سیسیتم مونیتورینگ/فیلترینگ محتوا برزگترین حفره امنیتی هر شبکه‌ای را پوشش می‌دهد. این سیستم با مونیتور کردن ترافیک می‌تواند ضمن تشخیص خروج اطلاعات محرمانه سازمان، جلوی انجام این کار را نیز بگیرد.

استفاده از این سیستم موجب آموزش کاربر در رعایت سیاست مورد قبول سازمان خواهد شد. این سیستم باعث تغییر رفتار کاربران و تطبیق آنها با سیاست‌های سازمان خواهد شد.

این سیستم با تشخیص نقض قانون‌های انجام شده توسط کاربران و ثبت تمامی اطلاعات (زمان/ نام/ تصویر کامپیوتر در لحظه رخداد نقض قانون) نشان دهنده این نقض قانون، اطلاعات قانونی مورد نیاز سازمان را نیز فراهم می‌کند.

مونیتورینگ و فیلترینگ محتوا سیستم مرکزی اطلاع رسانی سراسری در مورد نحوه استفاده صحیح از منابع شبکه را به وجود می‌آورد. با استفاده از این سیستم می‌توان کاربران را از قوانین و نحوه استفاده از شبکه آگاه کرد.

استفاده از این سیستم‌ها برای فیلتر کردن محتویاتی غیر از محتویات جنسی سخت است چرا که کاربر باید ترمینولوژی مورد نظر را تعریف و در کتابخانه کلمات کلیدی سیستم اضافه کند. اِعمال و نصب agent روی تعداد زیادی کامپیوتر نیاز به امکانات خاصی دارد.

۲-۷-۶- نحوه عملکرد سیستم Site Blocking

برنامه‌های کاربردی مختلفی که برای فیلترینگ سایت‌ها وجود دارند عمدتاً بر اساس تکنولوژی Pass-Through عمل می‌کنند. در این روش تمامی درخواست‌های دسترسی به اینترنت باید از یک نقطه– مثلاً یک فایروال یا پروکسی و یا یک Cache–سرور عبور کند. سپس این سیستم هر درخواست وب را مورد واررسی قرار می‌دهد و بر اساس مکانیزم‌های مشخص اجازه عبور یا عدم عبور درخواست را تعیین می‌کند. معمولاً در اینگونه سیستم‌ها تمامی درخواست‌ها ثبت می‌شوند. معمولاً این سیستم‌ها برای اِعمال سیاست فیلترینگ از یک پایگاه داده با ۴ یا ۵ میلیون آدرس که در دسته‌بندی‌های مختلف قرار داده شده‌اند کار می‌کند. بسته به نوع سیستم تعداد این دسته‌بندی‌ها بین ۲۰ تا ۷۰ می‌باشد.

برای هر دسته از کاربران یا گروه‌های کاری سیستم می‌تواند اجازه دسترسی به یک دسته بندی مشخص را به طور کامل بدهد و یا کلاً اجازه دسترسی به آن دسته‌بندی را سلب کند. بعضی از سیستم‌های فیلترینگ امکان دسترسی محدود را نیز می‌دهند. این محدودیت معمولاً بر اساس زمان و مدت استفاده است. سایت‌های جدیدی که دراینترنت هستند به صورت روزانه و به طور اتوماتیک به این پایگاه داده اضافه می‌شوند.

۲-۷-۶-۱- مزایا و معایب استفاده از مکانیزم Site Blocking

این روش یک راه موثر برای جلوگیری از دسترسی کاربران به سایتهای مشخص غیر مجاز اینترنتی است.

تخمین زده می‌شود که به طور هفتگی بین ۳ تا ۵ میلیون وب سایت جدید ایجاد و یا تغییر داده می‌شوند. که این در واقع به معنی عدم امکان داشتن یک پایگاه داده دقیق و صحیح از سایت‌ها می‌باشد. در واقع این ادعا که پایگاه داده‌های موجود دقتی بالای ۹۰ درصد دارند با توجه به نرخ رشد و تغییر وب سایت‌ها ادعای ضعیفی می‌باشد. سایت‌های تولید کننده محتویات غیر اخلاقی روزانه چندین هزار سایت جدید ایجاد می‌کنند و چون سیاست کاری سیستم‌های Site Blocking بستن سایت‌هایی است که در لیست خود دارند بسیاری از

سایت‌های جدید از چشم آنها دور می‌ماند. استفاده کاربران از موتورهای جستجو این مسئله را حادتر کرده و این ضعف سیستم‌های مبتنی بر لیست را بیش از پیش نمایان می‌کند.

مکانیزم Site Blocking ممکن است سایتهای خوب را نیز ببندد. این مکانیزم عمدتاً روی درخواست‌های http است و در سایر برنامه‌های کاربردی نظیر Messengerها و نامه‌های الکترونیکی تاثیری ندارد. استفاده از مکانیزم Site Blocking به طور ضمنی به این معنی است که اگر کاربران بتوانند سایتی را ببینند آن سایت مجاز خواهد بود و دیدن آن سایت هیچ اشکالی ندارد.

اگر فیلترینگ مبتنی بر کلمات کلیدی موجود در سایت را نداشته باشیم، مکانیزم Site Blocking عملاً با استفاده از موتورهای جستجو بلااستفاده خواهد بود. چرا که کاربر با جستجو محتوای مورد نظر خود در سایت جستجو به هر آنچه که می‌خواهد دسترسی خواهد داشت. عملاً تنها کاری که یک سیستم Site Blocking در این حالت می‌تواند انجام دهد آن است که کل سایت‌های جستجو را مسدود کند و یا از مکانیزم کمکی کلمات کلیدی استفاده کند.

۲-۷-۷- سیستم‌های فیلترینگ

بعضی از سیستم‌های فیلترینگ به صورت مستقل عمل می‌کنند (برای کار کردن به هیچ سیستم دیگری نیاز ندارند) و برخی دیگر با استفاده از پروتکل‌های خاص ارتباطی تمامی اطلاعات مربوط به Rating سایت‌ها را از اینترنت و از طریق سرورهای خاص به دست می‌آورند. بعضی از سیستم‌های فیلترینگ سایت امکانات محدودی نیز برای فیلتر کردن پروتکل‌های دیگر نظیر پروتکل گروه‌های خبری دارند.

۲-۷-۸- سیستم‌های مستقل فیلترینگ

یک سیستم مستقل فیلترینگ یک راهکار کامل فیلترینگ است که توسط یک شرکت ارائه می‌شود. این سیستم‌ها بر اساس سیاست و بانک اطلاعاتی فراهم شده توسط شرکت سازنده دسترسی کاربران را کنترل می‌کنند. اگر دسته بندی انجام شده در نرم‌افزار برای کاربر مفید نباشد کاربر مجبور است کل سیستم را با یک سیستم دیگر تعویض کند. در سیستم‌هایی که بر

اساس یک پروتکل کار می‌کنند کاربر می‌تواند سرور دیگری که روش Rating آن متفاوت است را انتخاب کند.

اکثر سیستم‌های فیلترینگ تنها بر اساس لیست کلمات کلیدی و لیست سایت‌های مشخص عملیات خود را انجام می‌دهند. لیست سایت‌ها شامل آدرس سایت‌هایی است که مشخصاً باید Block شوند و یا مشخصاً دسترسی به آنها آزاد است. این لیست توسط شرکت سازنده تامین می‌شود. معمولاً شرکت سازنده سایتهای اینترنت را در دسته‌بندیهای مختلف قرار داده و در قالب یک لیست به همراه نرم‌افزار فیلتر خود ارائه می‌کند.

سیاست شرکت‌های سازنده فیلترینگ در مورد ارائه اطلاعات لیست سایت‌ها یکسان نیست. متاسفانه اکثر شرکت‌ها به کاربران اجازه نمی‌دهند که لیست تهیه شده آن شرکت را ببینند. در واقع مالکیت معنوی این لیست متعلق به آن شرکت است. بعضی از شرکت‌ها جزئیاتی از نحوه تهیه لیست خود ارائه می‌کنند و برخی حتی اجازه می‌دهند که آدرس‌های جدیدی توسط کاربر به لیست موجود اضافه شود.

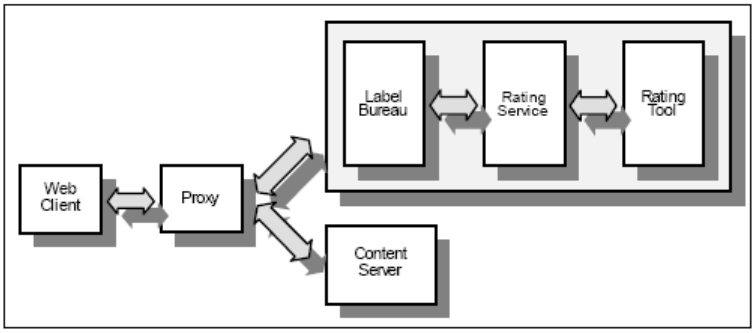
در مورد روش مشخص کردن دسته‌بندی‌های غیر مجاز نیز سیاست یکسانی وجود ندارد. در بعضی از نرم‌افزارها صرفاً می‌توان یک دسته‌بندی را مجاز یا غیر مجاز اعلام کرد و در برخی دیگر یک دسته‌بندی خود دارای درجات مختلفی می‌باشد که می‌توان درجه خاصی از یک دسته‌بندی را فیلتر کرد.

روش استفاده از کلمات کلیدی نیز به این صورت است که در صورت وجود کلمات کلیدی خاص در آدرس سایت و یا محتوای سایت، آن سایت بسته خواهد شد.

تخمین زده می‌شود که به طور هفتگی بین ۳ تا ۵ میلیون وب سایت جدید ایجاد و یا تغییر داده می‌شوند. که این در واقع به معنی عدم امکان داشتن یک پایگاه داده دقیق و صحیح از سایت‌ها می‌باشد. در واقع این ادعا که پایگاه داده‌های موجود دقتی بالای ۹۰ درصد دارند با توجه به نرخ رشد و تغییر وب سایت‌ها ادعای ضعیفی می‌باشد.

مهمترین مشکل روش استفاده از کلمات کلیدی آن است که عدم توجه به مفهوم متن و صرفاً تکیه به وجود یک کلمه در متن باعث دسته بندی غیر دقیق و غلط بسیار از سایت‌ها خواهد شد. استفاده از کلمات کلیدی یک روش غیر دقیق است که ممکن است باعث مسدود شدن سایت‌های مجاز و باز ماندن سایت‌های غیر مجاز شود.

مشکل دوم آن است که در این روش تصاویر پردازش نمی‌شوند. چون در حال حاضر روشی برای جستجوی متن در یک تصویر وجود ندارد. این مسئله باعث می‌شود که بسیاری از سایت‌ها که صرفاً حاوی تصاویر هستند با این روش دسته‌بندی نشوند.



شکل ۲-۳۶: انتخاب محتوای اینترنتی

۲-۷-۹- فناوری PICS

سکویی برای انتخاب محتوای اینترنتی (PICS) توسط کنسرسیوم W3 – اهرم راهنمای World Wide Web – توسعه داده شده است که به عنوان یک پروتکل در تبادل اطلاعات دسته بندی شده به کار می‌رود. Paul Resnick – پروفسور دانشگاه میشیگان و خالق PICS، این فناوری را در مقاله Scientific American در سال ۱۹۹۷ توضیح داده است. بعد از آن کنسرسیوم World Wide Web انستیتو فناوری ماساچوست مجموعه‌ای از استانداردهای تکنیکی تحت عنوان PICS (سکویی برای انتخاب محتوای اینترنتی) را توسعه داده است، تا اینکه کاربران بتوانند به صورت الکترونیکی تعاریف و توضیحات فعالیت‌های دیجیتال را در یک فرم ساده و قابل خواندن برای کامپیوتر گسترش دهند. کامپیوترها این متمم‌ها را در پس زمینه پردازش کرده و به صورت اتوماتیک کاربران را از دسترسی به موارد غیرمفید ایزوله کرده و توجه آنها را به سوی سایت‌های ویژه‌ای هدایت می‌کنند.

هدف اصلی از PICS این بوده است که به والدین و معلمان اجازه می‌دهد تا مواردی که آنها احساس می‌کردند برای کودکان مضر وغیرمفید است را مسدود کنند، علاوه بر سانسور آنچه که توزیع شده است – مانند بسیاری از موسسات قانونگذار که سعی در انجام چنین کاری دارند. PICS به کاربران کمک می‌کند تا آنچه را که دریافت می‌کنند کنترل کنند. دو عنصر در به

کارگیری عملی PICS نقش دارند. سیستم دسته بندی شده و نرم‌افزارهایی که از این سیستم‌های دسته بندی شده جهت فیلتر محتوا استفاده می‌کنند.

۲-۷-۹-۱- تفاوت فیلترینگ بر اساس PICS با سیستم‌های مستقل

محصولات فیلترینگ مستقل عموما شامل لیستی از سایت‌ها هستند که باید فیلتر شوند. مشتریان این نوع محصولات باید از تصمیمات فیلترینگ که توسط سازنده این نرم‌افزارها ارائه می‌شود استفاده کنند. نرم‌افزارهای مبتنی بر PICS از یک رویکرد آلترناتیو دیگر برای فیلترینگ براساس اشتراک گذاری اطلاعات دسته بندی شده استفاده می‌کنند. به جای استفاده از لیست سایت‌های بلاک شده و کلمات کلیدی جستجو، برنامه‌هایی که از PICS استفاده می‌کنند از سیستم‌های دسته بندی استاندارد شده جهت تعیین اینکه کدام سایت باید بلاک شود بهره می‌برند. کاربران نرم‌افزارهای مبتنی بر PICS توانایی انتخاب اینکه از کدام سیستم دسته بندی به صورت دلخواه استفاده کنند را دارا خواهند بود.

به عنوان یک استاندارد باز می‌توان PICS را در رنج وسیعی از برنامه‌های کاربردی به کار برد. علاوه بر ایجاد سازوکاری در بلاک کردن محتویات غیرمفید برای کودکان، ممکن است در تشریح محتوا بر حسب محتوای آموزشی، پتانسیل خشونت و دگر معیارهایی که سایت‌های اینترنتی را درجه بندی می‌کنند به کار گرفته شود. در بسیاری از موارد برنامه‌هایی که از PICS استفاده می‌کنند بسیار انعطاف پذیرتر از نرم‌افزارهای فیلترینگ مستقل هستند. کاربران نرم‌افزارهای PICS مجبور به تبعیت از داوری‌های سازنده این نرم‌افزارها نیستند.

۲-۷-۹-۲- سیستم‌های دسته بندی چه هستند؟

سیستم دسته بندی یک سری از مقوله‌ها و درجه بندی‌ها هستند که در غالب آن مقوله‌ها به طبقه‌بندی محتویات می‌پردازند. مقوله‌هایی که به کار می‌رود توسط توسعه دهندگان سیستم‌های دسته بندی انتخاب می‌شود و ممکن است شامل موضوعاتی نظیر "محتویات جنسی"، "نژاد" و "تنهایی" باشد. هر یک ازاین مقوله‌ها باید در سطوح متفاوت محتوا نظیر "رمانتیک، نه سکس"، "فعالیت آشکار سکسی" و یا در جایی بین این دو تشریح شوند. دسته بندی توضیحی از برخی محتوای اینترنتی ویژه است که از ترم‌ها و لغات برخی از سیستم‌های دسته بندی استفاده می‌کنند.

۲-۷-۹-۳- توسعه سیستم‌های دسته بندی

توسعه دهندگان PICS و کنسرسیوم W3، PICS را به عنوان یک استاندارد باز تشکیل داده‌اند. بنابراین هر کس می‌تواند یک سیستم دسته بندی درست کند. فرد یا گروهی از افراد می‌توانند با تعریف مقوله‌ها و توصیف درجه‌بندی بین آن مقوله‌ها، سیستم‌های دسته بندی را توسعه دهند. هنگامی که یک سیستم دسته‌بندی توسعه داده شد، باید برای کاربران و منتشران به صورت عموم در آید.

۲-۷-۹-۴- دسته بندی سایت‌ها

استاندارد PICS دو رویکرد برای دسته بندی کردن سایت‌ها دارد:

- خود دسته بندی[1]: انتشاردهندگان وب سایت محتویات صفحات وب خود را ارزیابی کرده و اطلاعات دسته بندی PICS را به طور مستقیم در صفحات وب خود قرار می‌دهند. این ارزیابی از طریق وب توسط توسعه دهندگان سرویس‌های دسته بندی اصلی انجام می‌شود.
- دسته بندی طرف ثالث[2]: افراد شخص ثالث می‌توانند از سیستم‌های دسته بندی PICS برای ارزیابی وب سایت‌ها استفاده کرده و دسته بندی خودشان را برای این سایت‌ها انتشار دهند. گروه‌های آموزشی ، گروه‌های مذهبی یا افراد حقیقی می‌توانند سایت‌ها را دسته بندی کرده و این دسته بندی‌ها را روی اینترنت جهت دسترسی همگان منتشر کنند.

۲-۷-۱۰- طرز استفاده از PICS

برای استفاده از PICS، کاربران شروع به پیکربندی مرورگرهای خود یا نرم‌افزارهای PICS برای استفاده از سیستم‌های دسته بندی (مانند ICRA یا SafeSurf) می‌کنند. هنگامی که سیستم دسته بندی انتخاب شده باشد، کاربران باید هر یک از مقوله‌ها را به منظور انتخاب یک سطح مناسب از اطلاعات آزمایش کنند. در عمل، این بدان معنی است که هر یک از کاربران تا چه حد و سطحی قصد اعمال فیلترینگ را دارند. به عنوان مثال انتخاب یک سیستم دسته

[1] Self-Rating
[2] Third-party

بندی برای برهنگی شامل "هیچکدام"، "آرایش آشکار"، "برهنگی جزیی"، "برهنگی تمام رخ" و "آشکار" خواهد بود.

هنگامی که این موارد انتخاب شد، نرم‌افزار مرورگر از آنها برای فیلتر کردن سایت‌ها استفاده می‌کند. هنگانی که از طرف کاربریک سایت اینترنت درخواست می‌شود، مرورگر دسته بندی سایت را با انتخاب‌های کاربر مقایسه می‌کند.

اگر سایت مورد نظر در درجه بندی قرار داشته باشد و با پارامترهای انتخاب شده کاربر همخوانی داشته باشد، آن صفحه به صورت نرمال نمایش داده خواهد شد. اگر دسته بندی سایت خارج از آن پارامترها قرار گرفته باشد (شاید سایت در دسته بندی "برهنگی تمام رخ" قرار گرفته، در حالی که کاربر "برهنگی جزیی" را انتخاب کرده باشد) دسترسی به آن سایت ممنوع خواهد شد و برای کاربر پیغامی فرستاده می‌شود مبنی بر اینکه دسترسی به سایت بلاک شده است.

از آنجایی که هم اکنون بسیاری از سایت‌ها دسته بندی نشده‌اند. غالب نرم‌افزارها امکانی برای کاربران به وجود می‌آورند که سایت‌هایی که در دسته بندی PICS قرار ندارند را بلاک کند. به منظور جلوگیری از دسترسی خردسالان و کودکان در تغییر دسته بندی‌ها و یا غیرفعال کردن PICS، غالب مرورگرها را می‌توان طوری پیکربندی کرد که قبل از غیرفعال کردن PICS احتیاج به وارد کردن رمز کلمه عبور باشد.

۲-۸- معماری سیستم‌های فیلترینگ متمرکز

به طور کلی سیستم‌های فیلترینگ به ۴ گروه دسته بندی می‌شوند.

- فیلترینگ بر مبنای ایستگاه‌های کاری
- سیستم‌های فیلترینگ Pass by
- سیستم‌های فیلترینگ Pass Through
- فیلترهای پراکسی

۲-۸-۱- فیلترینگ بر مبنای ایستگاه‌های کاری

در فیلترینگ بر مبنای ایستگاه کاری، کاربر بایستی نرم‌افزار فیلترینگ را بر روی دستگاه ایسگاه کاری خود نصب کند. این نرم‌افزار دسترسی‌های HTTP و دیگر ترافیک‌ها را بریده و آن

را فیلتر می‌کند. این سیستم در محیط‌های خانگی در جاهایی که تعداد ایستگاه‌های کاری کم است خوب کار می‌کند، اما در حالت کلی این ابزارها در محیط‌های کسب و کار مناسب نیستند.

نصب نرم‌افزار ویژه روی صدها و یا حتی هزاران ماشین بسیار پرهزینه است. از طرفی چون نرم‌افزار روی ایستگاه کاری اجرا می‌شود و توسط کاربر کنترل می‌شود، به راحتی قابل غیر فعال کردن و بایپس توسط کاربر می‌باشد.

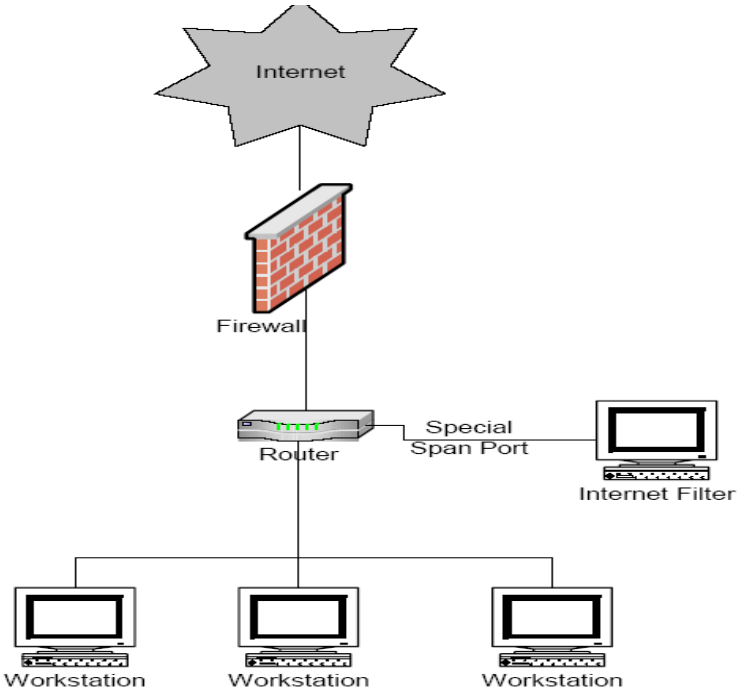
۲-۸-۲- سیستم‌های فیلترینگ Pass by

در این معماری هنگامی که یک بسته به سمت اینترنت فرستاده می‌شود. سیستم فیلترینگ آن را کشف کرده و به سمت سیستم طبقه بندی جهت تصمیم‌گیری رد یا عبور بسته را می‌گیرد. اگر تصمیم به بلاک کردن بسته گرفته شود، سیستم فیلترینگ بسته ویژه‌ای به سمت ایستگاه کاری می‌فرستد و سپس ارتباط را قطع کرده و خاتمه می‌دهد.

تنظیمات زمان در استفاده از این نوع فیلترینگ وب بسیار حساس می‌باشد. بین زمانی که درخواست به سمت بیرون می‌رود و اولین پاسخ از کارگزار وب بر می‌گردد مراحل زیر به ترتیب اتفاق می‌افتد.

- سیستم کشف کننده باید ترافیک مورد نظر را شناسایی کند.
- سیستم کشف کننده باید یک درخواست رد یا عبور بسته به سمت سیستم طبقه بندی بفرستد.
- سیستم طبقه بندی کننده باید درخواست‌ها را طبقه بندی کرده و بر اساس آن تصمیم اتخاذ کند.
- نتیجه این تصمیم گیری باید به سیستم کشف فرستاده شود.
- اگر درخواست رد شده باشد باید TCP RESET به سمت ایستگاه کاری فرستاده شود.
- نصب سیستم کشف کننده معمولا با پیکربندی دوباره مسیریاب‌ها و فایروال همراه خواهد بود و اگر تغییرات به درستی انجام نپذیرد ممکن است کل شبکه در وضعیت ریسک به سر ببرد.

یکی از مزیت‌های این سیستم فیلترینگ این است که اگر سیستم فیلترینگ عمل نکند و یا به عبارتی مشکلی در آن به وجود آمده باشد، شبکه Stop نخواهد شد. کلیه کاربران همچنان می‌توانند از اینترنت استفاده کنند و تنها بلاک کردن سایت‌های ممنوع عمل نمی‌کند.

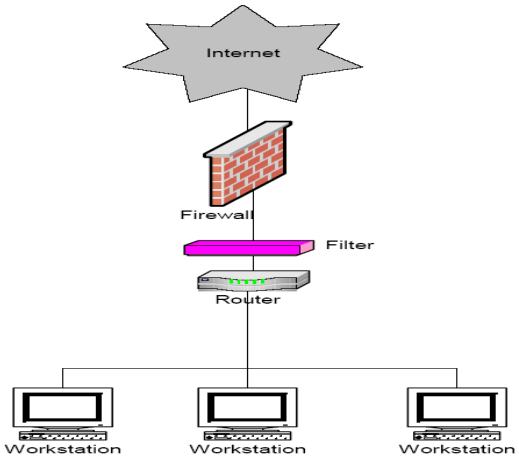


شکل ۲-۳۷: سیستم‌های فیلترینگ Pass by

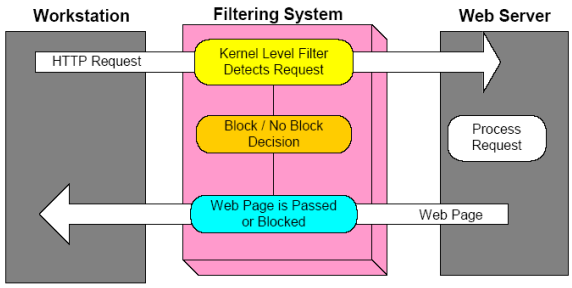
۲-۸-۳- سیستم‌های فیلترینگ Pass Through

سیستم فیلترینگ In-line بین شبکه سازمانی و اینترنت مستقر می‌شود. این سیستم طوری مکان داده می‌شود که از دید ایستگاه‌های کاری به صورت شفاف یا ترانسپرنت دیده می‌شود. از آنجا که سیستم هر بسته‌ای را می‌بیند می‌تواند هر یک از آنها را بازبینی کند و برای اعمال فیلترینگ تصمیم گیری کند. فیلترینگ می‌تواند در سطح کاربر و یا در سطح کرنل اعمال شود. در فیلترینگ سطح کاربر تحلیل ترافیک توسط یک برنامه سطح کاربر انجام می‌شود. این بدان معنی است که هر بسته باید از چند لایه کد جهت عبور از سیستم گذر کند.

فیلترهای In-Line مقدار ۱۰۰٪ ترافیک شبکه را اداره می‌کنند. چرا که هر بسته‌ای از طریق سیستم فیلترینگ عبور می‌کند. همچنین هر بسته، صرف‌نظر از اینکه از چه پورتی استفاده می‌کند توسط سیستم فیلترینگ بازبینی و برای عبور یا رد آن تصمیم‌گیری می‌شود.



شکل ۲-۳۸: سیستم‌های فیلترینگ Pass Through



شکل ۲-۳۹: سیستم‌های فیلترینگ Pass Through

این معماری شبیه رویکرد فیلترینگ Pass by بوده با این تفاوت که در برابر بار زیاد قصور نمی‌کند. ترافیکی که از کارگزار وب وارد می‌شود قبل از این که تصمیم گیری جهت رد یا عبور ترافیک اتخاذ شود، تا زمان تصمیم‌گیری برای آن ترافیک تاخیر داده خواهد شد. بنابراین سیستم قادر به پاسخ گویی حتی در برابر بارهای خیلی زیاد هم خواهد بود.

۲-۸-۴- فیلترهای پراکسی

وب پراکسی به عنوان یک سرویس تبادل متقابل بین ایستگاه‌های کاری و کارگزار وب عمل می‌کند. در حالت نرمال مرورگر وب به صورت مستقیم سراغ کارگزار وب می‌رود. هنگامی که از یک پراکسی استفاده می‌شود مرورگر از پراکسی برای واکشی صفحه وب استفاده می‌کند. پراکسی این درخواست را فیلتر می‌کند و بر اساس این که این درخواست باید رد یا عبور داده شود آن را پردازش می‌کند.

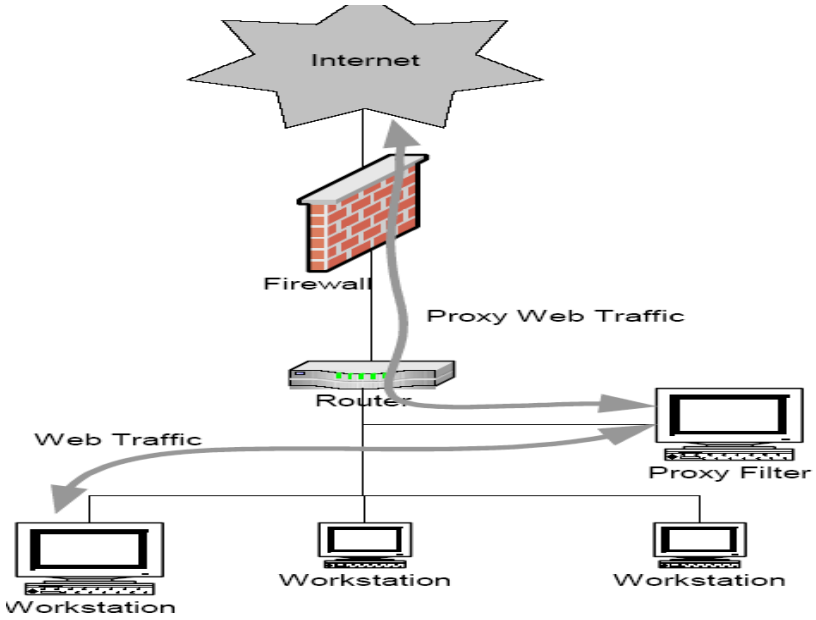
فیلترهای پراکسی تنها زمانی عمل می‌کنند که تمام کاربران شبکه مجاب به استفاده سیستم فیلترینگ به عنوان پراکسی باشند. برای اینکه از دسترسی ایستگاه‌های کاری به کاگزارهای وب خارجی جلوگیری شود باید در قوانین فایروال اصلاحاتی در جهت بلاک کردن این درخواست‌ها استفاده شود.

فیلترینگ پراکسی تاخیر قابل ملاحظه‌ای در ترافیک شبکه ایجاد می‌کند. هر بسته ای که از ایستگاه کاری به سمت کارگزار وب می‌رود بایستی توسط پراکسی دوباره نوشته شود طوری که به نظر می‌رسد مبدا این بسته پراکسی می‌باشد. به همین ترتیب هر پاسخی که از کارگزار وب به سمت ایستگاه کاری می‌رود باید دوباره توسط پراکسی بسته بندی شود.

هر بسته ای که از یک ایستگاه کاری به سمت اینترنت می‌رود باید مراحل زیر را طی کند:

- ارسال توسط ایستگاه کاری
- دریافت توسط درایور شبکه برای پورت شبکه داخلی
- انتقال داده‌ها از سطح کرنل به سطح کاربر
- سوییچ به سطح کاربر
- دوباره نویسی آدرس بسته
- سوییچ به سطح کرنل
- انتقال داده از سطح کاربر به سطح کرنل
- انتقال داده توسط درایور دستگاه برای پورت خارجی شبکه

یکی از مشکلات این معماری این است که اگر کارگزار پراکسی خاموش و یا به عبارتی down شود، کلیه ترافیک عبوری از سیستم Stop خواهد شد. بنابراین قصور و یا کوتاهی در سیستم منجر به قصور در شبکه می‌شود.



شکل ۲-۴۰: سیستم‌های فیلترینگ پراکسی

۲-۸-۴-۱- پروتکل تطبیق محتوای اینترنتی (ICAP)

ICAP(Internet Content Adaptation Protocol) پروتکلی است که برای فرستادن محتوای خاص بر مبنای پروتکل HTTP به یک کارگزار مشخص استفاده می‌شود. در نتیجه به منظور آزاد ساختن منابع سیستم و استانداردسازی ارتباط طراحی شده است. به عنوان مثال کارگزاری که تنها عمل ترجمه به یک زبان را انجام می‌دهد بسیار کارامدتر از کارگزار استاندارد وبی بوده که ممکن است علاوه بر وظیفه فوق چند کار دیگر هم انجام می‌دهد.

ICAP بر روی سیستم‌های نظیر پراکسی و کش به منظور کمک در ارائه سرویس‌های با ارزش افزوده[1] متمرکز شده است. در دل هسته این پردازش یک کش وجود دارد که تمام تراکنش‌های کلاینت را به مانند پراکسی از طزیق کارگزار ICAP/Web پردازش می‌کند. این نوع کارگزارهای ICAP بر روی فرایند و تابع خاصی متمرکز هستند. مانند الحاق تبلیغات[2]، پویش ویروس ها[3] ترجمه محتوا، ترجمه زبان و یا فیلترینگ محتوا را می‌توان نام برد. ارسال

[1] Value-added
[2] Advertising Insertion
[3] Virus Scanning

سرویس‌های با ارزش افزوده از کارگزار وب به کارگزارهای ICAP به این دو کارگزار اجازه مقیاس پذیری با توجه به توان عملیاتی HTTP را می‌دهد.

ICAP به زبان بسیار ساده یک پروتکل HTTP کوچک بر مبنای " صدا زدن رویه کاری از دور " می‌باشد. به عبارت دیگر ICAP به کلاینت‌ها اجازه می‌دهد تا پیغام‌های بر اساس HTTP (HTML) خود را، (محتوا)، به یک کارگزار ICAP برای انجام عملیات تطبیق ارسال دارند. تطبیق به انجام سرویس‌های با ارزش افزوده (کنترل کامل و دقیق محتوا) برای درخواست/ پاسخ یک کلاینت اطلاق می‌شود.

۲-۸-۵- دلیل به وجود آمدن ICAP چیست؟

یکی از مشکلاتی که در اینترنت در قدم‌های ابتدایی رشد وجود دارد اینست که توانایی مقیاس پذیری ترافیک، پهنای باند، سرویس ها، دسترسی‌ها وغیره وجود ندارد. متاسفانه این نوع سرویس‌های با ارزش افزوده، منابع سیستم نظیر پهنای باند و زمان پردازش کارگزارها را هدر می‌دهند.

سرویس‌های امروزی تقریبا روی APIهای مناسبی اجرا می‌شوند که بر اساس برنامه کسب و کار خاص ساخته می‌شوند. این APIها گاهی وقت‌ها غیر قابل اعتماد هستند. چرا که آنها هم گام با رشد کسب و کار اینترتی شرکت طراحی نشده‌اند. علاوه بر این اعمال تغییرات بر روی APIها بسیار هزینه ساز بوده و یا اینکه هر سرویس جدید نیاز به یک API اضافی دارد.

تعداد زیاد سرویس‌های ارائه شده دسترسی به یک سایت و تراکنش با کسب و کار را کند و گاهی وقت‌ها Overload می‌کند. هر کدام از این سرویس‌ها از روی برنامه‌های خاصی مستقر بر روی کارگزار اجرا می‌شوند که منجر به لختی سیستم می‌شود.

این سرویس‌ها شامل دسترسی، تصدیق هویت، پایگاه داده‌های اطلاعات مشتریان، تجارت الکترونیک، ترجمه زبان، فیلترینگ محتوا، پویش ویروس‌ها، الحاق تبلیغات و بسیاری از موارد دیگر را شامل می‌شود. همه این‌ها منجر به زمان عکس العمل زیاد وکاهش اعتماد به کارگزار می‌شود.

۲-۸-۶- مزایای ICAP

ICAP بر روی تجهیزات قابل دسترس و موجود امروزی قابل استفاده می‌باشد. به عنوان نمونه اگر Netcache (یک نوع پراکسی) از قبل نصب شده باشد، جز به کارگزار(های) ICAP به تجهیزات دیگری نیاز نمی‌باشد.

ICAP بر مبنای HTTP است در نتیجه دسترسی از طریق در گاه‌های امنیتی که تنها به ترافیک پورت ۸۰ اجازه عبور می‌دهند را امکان پذیر می‌کند.

ICAP یک پروتکل متن باز است و به هر کارگزار یا برنامه کاربردی اجازه به کارگیری آن را می‌دهد. از زمان استفاده از کدهای Apache پیاده سازی ICAP بسیار آسان شده است. ISPها و سازمان‌های بزرگ می‌توانند از پشتیبانان و برنامه‌نویسان متفاوت در تهیه برنامه‌های کاربردی با ارزش افزوده مناسب استفاده کنند.

ICAP ، سرویس‌های با ارزش افزوده را به سمت کارگزارهای ICAP ، offload می‌کند و بدین ترتیب منابع کارگزارهای وب را آزاد می‌سازد و این عمل در نهایت زمان دسترسی به سایت را کاهش می‌دهد.

ICAP ، پیاده سازی ، قابلیت اعتماد و مقیاس پذیری سرویس‌های با ارزش افزوده را ساده می‌کند.

۲-۸-۷- سرویس‌هایی که ICAP ارائه می‌دهد

۲-۸-۷-۱- پویش ویروس‌ها

این مورد قابلیتی است که محتویات جدید را به صورت "on-the-fly" از وجود ویروس چک می‌کند و محتویات کش را پس از ویروس چک مهیا می‌سازد. در روش سنتی هر Object یا شی پتانسیل چند بار پویش ویروس را دارد و بدین ترتیب یکی از دلایل هدر دادن منابع خواهد بود.

هیچ روش قدیمی"on-the-fly" برای پویش ویروس‌ها به صورت پریودیک وجود ندارد. پویش "on the fly" ویروس‌ها در ICAP به شی‌های یک بار پویش شده قدیمی غیر آلوده، اجازه کش شدن را می‌دهد و بدین ترتیب منابع سیستم را آزاد می‌کند.

۲-۸-۷-۲- ترجمه زبان نشانه گذاری

این مورد قابلیتی است که به دستگاه‌های به اصطلاح Non–HTML نظیر تلفن‌های سلولی اجازه می‌دهد تا با دستگاه‌های HTML نظیر کامپیوترهای شخصی ارتباط برقرار سازند. این مورد اساس یک پل ارتباطی ترجمه WAP/XML/HTML می‌باشد.

روش سنتی: استفاده از یک دروازه اختصاصی جهت ترجمه از یک زبان دستگاه ویژه به HTML و برعکس. این روش تمام انتقال‌ها را به یک مجموعه در گا ها به عنوان نقطه ای از حضور در اینترنت محدود می‌سازد.

یک کش کلیه درخواست‌های کاربر را به یک کارگزار مترجم ICAP ، آدرس دهی می‌کند و کپی‌های کش شده Objectهای مختلف را در خود برای پاسخ سریع‌تر به کاربر نگهداری می‌کند.

۲-۸-۷-۳- الحاق آگهی

این قابلیتی است که بر اساس آن آگهی‌های تبلیغاتی وارد صفحات وب می‌شوند و یا بر اساس اولویت‌های مشتری (هنگامی که کاربر یک درخواست ویژه از یک وب سایت مانند موتورهای جستجوگر می‌فرستد) صفحات جدید تولید می‌شوند.

روش سنتی: در روش‌های سنتی وارد کردن آگهی‌های تبلیغاتی به صفحات وب یا بر خود وب سایت اصلی بوده (Hosting Provider) و یا خود سایت برای تبلیغات مستقیم در جایی Sign up می‌کند.

از مزایای استفاده از ICAP در تزریق آگهی‌های تبلیغاتی این است که این تبلیغات متناسب با عوالی نظیر آدرس IP کارگزار پراکسی، کلمات کلیدی ورودی یا اطلاعات جمع آوری شده برای هر مشتری متفاوت خواهد بود.

۲-۸-۷-۴- ترجمه زبان انسان

این مورد قابلیتی است که محتوای تگ‌های HTML را از یک زبان به زبان دیگر ترجمه می‌کند.

روش سنتی: برنامه‌های توسعه یافته وسنگین API که بر روی ماشین‌های کلاینت یا کارگزارهای وب در حال اجرا هستند برای انجام این کار استفاده می‌شده‌اند.

درخواست‌های به خصوص به کارگزارهای ICAP ویژه، از طریق Redirect کردن درخواست‌ها توسط کارگزارهای پراکسی منتقل و ترجمه می‌شوند.

۲-۸-۷-۵- فیلترینگ محتوا

این قابلیتی است که درخواست‌های محدود شده و یا غیر مجاز را به سایت‌ها و صفحات دیگر Redirect می‌کند.

روش سنتی: توسط کارگزارهای پراکسی از طریق تنظیم دستی اطلاعات ورودی یا کسب اطلاعات و دانلود پایگاه داده‌های نام سایت‌ها از فروشنده سایت‌های فیلتر شده انجام می‌شود.

تحت ICAP فیلترینگ محتوا بسیار گسترده تر از نگاه مشتری است. با استفاده از ICAP محتویات دینامیک هم می‌توانند فیلتر شوند و از سوی دیگر قابلیت مدیریت سرویس‌ها به صورت برون سپاری وجود دارد. علاوه بر آن کارگزارهای فیلترینگ ICAP می‌توانند خارج از سایت مشتری مستقر شوند.

۲-۸-۷-۶- فشرده سازی داده‌ها

قابلیتی است برای فشرده کردن صفحات HTML و شی‌ها از کارگزار اصلی آن.

روش سنتی: هیچگونه فشرده سازی در سطح صفحات HTML و فشرده سازی دستی برای شی‌های گسترده انجام نمی‌گیرد.

در غالب به کارگیری ICAP، کارگزارهای اصلی قابلیت فشرده سازی دارند و بدین صورت پهنای باند زیادی ذخیره می‌شود.

۲-۸-۸- سیاست‌های ICAP

به طور عموم ICAP به سوالاتی نظیر چه زمانی، چه کسی، یا چرا برای کنترل کامل محتوا استفاده نمی‌کند و تنها به منظور آماده ساختن محتوا برای یک کارگزار که عملیات تطابق را انجام می‌دهد به کار می‌رود. به عنوان مثال اگر ICAP ابزاری برای مجوز ترجمه / تطابق محتوا باشد، شما همچنان به یک موتور تطابق (کارگزار ICAP) جهت تصمیم گیری در سوالاتی نظیر چه زمان، چه کسی یا چرا، نیاز خواهید داشت.

۲-۸-۹- معماری ICAP

ICAP چگونه معماری شده است؟ از آنجایی که سرویس‌های بسیاری از این پروتکل جهت ارایه خدمات کمک می‌گیرند به یک طرح و ساختار ماجولار، ساده و " آسان در پیاده سازی " نیاز است. همچنین این پروتکل باید بتواند با روش‌های موجود ارتباط برقرار کرده و با تجهیزات شبکه‌ای نصب شده استاندارد و برنامه‌های کاربردی موجود سازگاری کامل داشته باشد.

وب سایت‌های تجاری شامل مجموعه‌ای از تجارت الکترونیک، فایل، کارگزارهای FTP و پایگاه داده‌ها می‌باشد. همچنین برقراری ارتباط تنها از طریق HTTP محدود نمی‌شود. دامنه وسیعی از ترافیک لایه ۷ بر پایه http می‌باشد. پراکسی‌های ICAP از یک http post که درآن درخواست کلاینت و پاسخ کارگزار اصلی در اولین قسمت از بدنه HTML کپسوله شده، استفاده می‌کند.

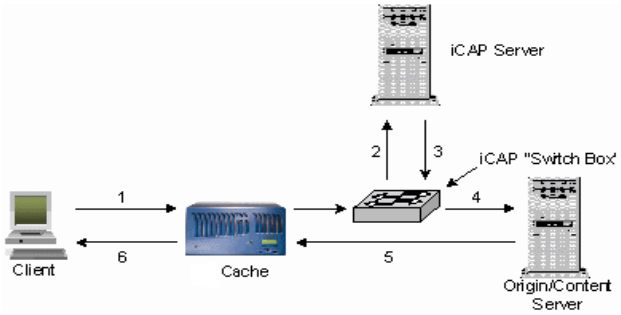
با استفاده از یکی از ۴ تکنیک تطابق زیر، ICAP قادر به تسهیل کلیه تطابق محتوای ممکن خواهد بود. در هر مورد یک کش (Forward Proxy) به عنوان نقطه مرکزی در پردازش گروهی ICAP و پاسخ نهایی به کلاینت عمل می‌کند. کارگزار کش قادر به کش کردن قسمتی از ICAP بدون نیاز به کپی و پردازش دوباره درخواست‌ها می‌باشد.

۲-۸-۹-۱- تغییر درخواست‌ها

درخواست‌های کلاینت به سمت یک کارگزارICAP، Redirect می‌شود و ICAP درخواست‌ها را تغییر داده و به کارگزارهای مقصد می‌فرستد.

در این مدل کلاینت جهت آوردن صفحه وب یک درخواست به سمت کارگزار مورد نظر می‌فرستد. این درخواست با دخالت کارگزار پراکسی (کش) به سمت یک کارگزار ICAP ارسال می‌دارد.

کارگزار ICAP پیغام را تغییر داده و آن را به کارگزار پراکسی برمی‌گرداند. کارگزار پراکسی پیغام تغییر داده شده را دریافت کرده و آن را به سمت کارگزار مقصدی که مورد درخواست کلاینت می‌باشد می‌فرستد. درخواست توسط کارگزار مقصد اجرا شده و پاسخ به سمت کلاینت بر گردانده می‌شود.



شکل ۲-۴۱: تغییر درخواست

مثال: فیلترینگ محتوا. کلاینت یک درخواست برای یک صفحه وب می‌فرستد. کارگزار پراکسی این درخواست را به سمت کارگزار ICAP، redirect می‌کند. کارگزار ICAP درخواست HTML را تجزیه کرده و فیلترینگ بر اساس URL را با مقایسه URL درخواستی با لیستی از URLهای غیر مجاز، انجام می‌دهد. اگر URL در لیست غیرمجاز وجود داشته باشد، درخواست کلاینت به درخواست یک پیغام خطا از طرف کارگزار مقصد و یا از طرف کارگزار پراکسی (کش) تغییر داده می‌شود. این پیغام خطا به سمت کلاینت فرستاده می‌شود. اگر URL کارگزار مقصد غیر مجاز نباشد، کارگزارICAP درخواست را از طریق کارگزار پراکسی به سمت کارگزار مقصد می‌فرستد.

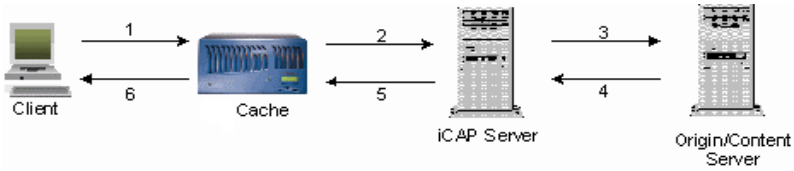
۲-۸-۹-۲- رضایت (ارضا) درخواست

درخواست کلاینت‌ها به سمت یک کارگزار ICAP جهت تغییر در درخواست فرستاده می‌شود و سپس از طرف آن به سمت کارگزار اصلی می‌رود. درخواست تغییر داده شده مستقیما و بدون بازگشت به پراکسی به سمت کارگزار اصلی فرستاده می‌شود.

در این حالت کلاینت یک درخواست به سمت کارگزار اصلی می‌فرستد. این درخواست با دخالت کارگزار پراکسی (کش) به سمت کارگزار ICAP فرستاده می‌شود. کارگزار ICAP این پیغام را تغییر داده و به طور مستقیم و بدون بازگشت به پراکسی به سمت کارگزار اصلی یا اینترنتی جهت اجرا می‌فرستد. پس از پردازش درخواست، کارگزار اصلی جواب را از طریق کارگزار ICAP و کارگزار پراکسی به سمت کلاینت می‌فرستد.

مثال: شبیه آنچه که در فیلترینگ محتوای مثال فوق آورده شده، با تغییر و اصلاح درخواست، فرآیند عوض می‌شود. درخواست کلاینت همچنان توسط کارگزار ICAP بازرسی

می‌شود، اگر محتوا معتبر نباشد کارگزار ICAP یک پاسخ خطا از طریق کارگزار پراکسی به کلاینت می‌فرستد و از ارسال درخواست به کارگزار اینترنتی مورد نظر کلاینت صرفنظر می‌کند. اگر کلاینت مجاز به دسترسی به سایت مورد نظر خود باشد، کارگزار ICAP محتوا و شی‌های خواسته شده را از کارگزار اینترتی واکشی کرده و آن را برای کلاینت مهیا می‌سازد.



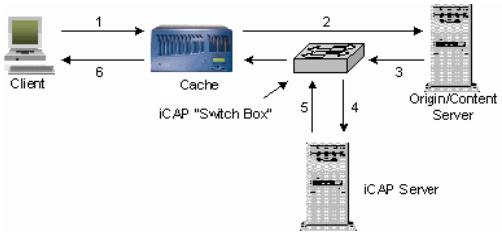
شکل ۲-۴۲: ارضا درخواست

۲-۸-۹-۳- تغییر پاسخ

درخواست کلاینت توسط کارگزار اصلی یا همان سایت مورد نظر پردازش می‌شود، اما پاسخ درخواست از طرف کارگزار اصلی به سمت کارگزار اصلی به سمت کارگزار ICAP، جهت تغییر و تحویل به کلاینت Redirect می‌شود.

در این حالت کلاینت درخواست را به سمت کارگزار اصلی می‌فرستد این درخواست همچنان که انتظار می‌رود توسط کارگزار اصلی پردازش و انجام می‌شود. پاسخ توسط کارگزار پراکسی به کارگزار ICAP، برگردانده می‌شود. کارگزار ICAP تغییرات لازم را در پاسخ انجام داده و آن را از طریق کارگزار پراکسی به کلاینت تحویل می‌دهد.

مثال: برگردان یا ترجمه درگاه (فرمت بندی HTML). مانند درخواستی که از طریق تلفن‌های سلولی به پروفایل‌های سهام یک شرکت می‌رود. درخواست به طور مستقیم به کارگزار اصلی فرستاده می‌شود. پاسخ تولید شده توسط کارگزار اصلی به سمت کارگزار ICAP جهت تغییر در پاسخ به منظور نمایش صحیح محتوا در تلفن‌های سلولی، برگردانده[1] می‌شود.



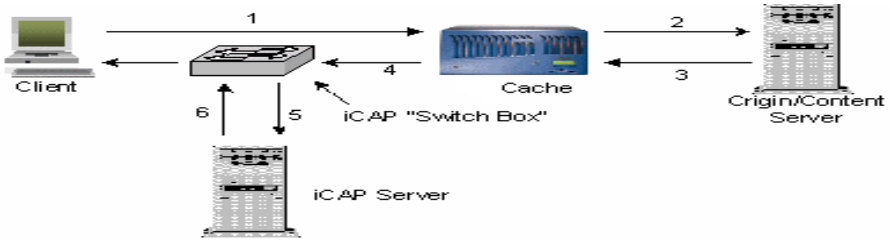
شکل ۲-۴۳: تغییر در پاسخ

[1] Redirect

۲-۸-۹-۴- تغییر و اصلاح نتیجه

درخواست کلاینت‌ها توسط کارگزار اصلی پردازش، و پاسخ تولید شده برای کارگزار ICAP جهت تغییر و اصلاح برگردانده می‌شود. این حالت با تغییر و اصلاح پاسخ فرق دارد و از طرفی دیگرکارگزار ICAP قبل از کارگزار پراکسی (کش) قرار دارد. در این حالت، کلاینت درخواست را به سمت سایت اصلی می‌فرستد و این درخواست توسط سایت مورد نظر(کارگزار اصلی) پردازش و انجام می‌شود. پاسخ به ترتیب ابتدا به سمت کارگزار پراکسی سپس به سمت کارگزار ICAP فرستاده می‌شود. کارگزار ICAP پاسخ را اصلاح کرده و از طریق پراکسی پاسخ اصلاح شده را به سمت کلاینت می‌فرستد. برتری و مزیت این روش نسبت به روش تغییر واصلاح پاسخ این است که کارگزار ICAP در لایه پایین‌تر از کارگزار پراکسی قرار داشته و پراکسی می‌تواند شی‌ها و محتواهایی که به کلاینت تحویل می‌شود را کش کند.

مثال: الحاق تبلیغات. کلاینت یک درخواست به یک صفحه وب می‌فرستد و کارگزار پراکسی این درخواست را به کارگزار سایت درخواست شده ارسال می‌کند. کارگزار اصلی درخواست را انجام داده و پاسخ را به کارگزار پراکسی تحویل می‌دهد. پراکسی شی‌ها و محتوا را کش کرده و پاسخ را به سمت کارگزار ICAP می‌فرستد. کارگزار ICAP پاسخ HTML را تجزیه و بررسی کرده و عمل پروفایل هر کلاینت را انجام می‌دهد. کارگزار ICAP تبلیغات مناسب را وارد این صفحات کرده و پاسخ را به سمت کلاینت ارسال می‌دارد.



شکل ۲-۴۴: تغییر و اصلاح نتیجه

۲-۸-۱۰- جزییات پروتکل

ICAP از طریق جلسات TCP ارتباط برقرار می‌کند. کارگزار ICAP به صورت غیر فعال به تمام درخواست‌های Redirect شده از سوی کارگزارهای وب گوش می‌دهند و همچنین فرمت کلیه پیغام‌های ICAP مطابق با RFC822 می‌باشد.

شرکت Network Appliance اولین تولید کننده ICAP Client و ICAP Server می‌باشد که می‌توان آن را روی پلتفرم‌های ویندوز یا لینوکس به صورت جداگانه کامپایل کرد.

محصولات شرکت Trend Micro برای کارکردن با کارگزار پراکسی Net Cache طراحی شده است. بسته‌های امنیت وب Trend Micro نسخه ICAP ، در سر راه دروازه‌های اینترنتی برای پویش کلیه ترافیک HTTP از ویروسها و کلیه محتوای خرابکار، نصب می‌شود. ترافیک وب از کش به سمت کارگزار ICAP به‌منظور اطمینان از محتوای مطمئن (پویش ویروسها)، فرستاده می‌شود.

محصولات شرکت Symantec موتور پویش Symantec، یک کارگزار TCP/IP و اینترفیسی است که از برنامه‌های جانبی جهت همکاری در پویش محتوا استفاده می‌کند. این محصول سرویس پویش محتوای سریع ، مقیاس‌پذیر و قابل اعتماد برای محافظت از ویروس‌ها، اسپای‌ها و دیگر محتوای ناخواسته را در یک پویش ساده انجام می‌دهد. موتور پویش سیمانتک از طریق ICAP با بسیاری از دستگاه‌ها و برنامه‌های کاربردی نظیر Blue Coat ProxySG ، NetCache و Cisco ACNS ارتباط برقرار خواهد کرد.

شرکت Webwasher در فیلترینگ محتوا محصولات و فن آوری‌هایی را گسترش می‌دهد که باروری و سودمندی اینترنت را ارتقا می‌دهند. Webwasher.com AG سرویس‌های با ارزش افزوده را با به‌کارگیری ICAP توسعه می‌دهد. برنامه‌های کاربردی که در آن از ICAP پشتیبانی می‌شود. با کمک این محصول یک ابزار قدرتمند برای فیلترینگ محتوای هوشمند از URLها و آدرس‌های IP و سرآیند و بدنه صفحات وب را تشکیل می‌شود که می‌تواند بسیاری از سیاست‌های امنیتی شرکت را پوشش دهد.

شرکت Zack Systems با Network Appliance در سپتامبر ۲۰۰۰ به عنوان قسمتی از ابتکار وخلق ICAP شریک بوده است. شرکت Zack پلتفرم پراکسی خود را از طریق ICAP با کارگزار کش محصول Network Appliance در ایجاد یک محصول با ارزش افزوده یکی کرده است. Zack محصول کش Network Appliance را با توسعه برنامه‌های کاربردی نظیر ویرایش محتوا (اضافه کردن، استخراج کردن و تغییردادن)، جمع آوری داده‌های متراکم و وارد کردن تبلیغات ارتقا داده است.

۲-۹- معرفی نرم‌افزارهای متن باز فیلترینگ

فیلترینگ محتوا[1]، یک ابزار برای مسدود کردن و یا باز گذاشتن سایت‌های اینترنتی و محتوای آنان از دسترس یک کاربر، گروهی از کاربران و یا کلیه کاربران می‌باشد.

ابزارهای فیلترینگی که بر اساس آدرس وب سایت (URL) عمل می‌کنند، عموماً لیست بلند بالایی از وب‌سایتها را مسدود می‌کنند و چنانچه کاربری قصد ورود به آن سایتها را داشته باشد؛ با پیغام‌هایی از قبیل " ورود شما به این سایت غیرقانونی است." و ... مواجه می‌شود.

از آنجاییکه وب‌سایت‌ها به سرعت، محل و آدرس خود را تغییر داده و حتی موتورهای جستجوی قوی مثل Google، AltaVista و Yahoo نیز از نیمی از این تغییر آدرس‌ها بی‌خبر هستند. لذا فیلترینگ بر اساس URL با تغییر آدرس سایت‌ها و همچنین اضافه شدن روزانه سایت‌هایی با محتوای ممنوعه، سخت‌تر می‌شود. بنابراین فیلترینگ جامع و وسیع فقط با استفاده از URLها ممکن نیست. چیزی که مورد نیاز است ابزاری است که بتواند هر صفحه‌ای را که به آن دسترسی داریم از لحاظ محتوا کنترل کرده و چنانچه دارای موضوعات مناسبی نیستند؛ آنها را مسدود می‌کند. این ابزار " فیلترینگ محتوا " نام دارد.

۲-۹-۱- معرفی اجمالی برنامه DansGuardian

یکی از انواع فیلترهای متن‌باز محتوا، ابزاری به نام DansGuardian است. برنامه DansGuardian یک فیلتر محتوای متن باز وب است که بر روی سیستم‌عامل‌های Linux، FreeBSD، OpenBSD، NetBSD، Mac OS X، HP-UX و Solaris اجرا می‌شود. این ابزار محتوای واقعی صفحات را بر مبنای روش‌های متنوعی شامل Phrase Matching (فیلترینگ بر مبنای عبارت‌های داخل متن) و URL Filtering (فیلترینگ بر مبنای آدرس وب سایت)، فیلتر می‌کند. برنامه DansGuardian مانند اکثر فیلترهای موجود، فقط بر اساس لیستی از آدرس‌های سایت‌های ممنوعه عملکرد فیلترینگ را انجام نمی‌دهد. برنامه DansGuardian به گونه‌ای طراحی شده است که کاملاً انعطاف پذیر باشد و به شما این امکان را بدهد که فیلترینگ را دقیقاً بر اساس خواسته‌های خود تنظیم کنید.

---

[1] Content Filtering

شکل ۲-۴۵:آرم برنامه DansGuardian

روش‌های فیلترینگ برنامه DansGuardian بسیار متنوع هستند و این برنامه به استفاده از یکی روش‌های Phrase Matching، File Extension Matching، MIME Type Matching، PICS Filtering و URL/Domain Blocking، POST Filtering محدود نمی‌شود و می‌تواند از همه این روش‌ها در آن واحد استفاده کند که در ادامه به شرح مهمترین این روش‌ها پرداخته شده است.

- روش Phrase Matching: عموماً صفحاتی را که دارای عبارتهای ناخواسته هستند جستجو می‌کند و آنها را مسدود می‌نماید.
- روش POST Filtering: به شما اجازه می‌دهد که بار گذاری (upload) بر روی وب را محدود و یا مسدود نمائید.
- روش URL/Domain Filtering: قادر به کار کردن با لیست‌های بزرگ ممنوعه از وب‌سایت‌ها بوده و از SquidGuard سریعتر است.

برنامه DansGuardian به همراه یک برنامه Anti Virus، توانایی اسکن ویروس‌ها را به صورت بلادرنگ برخوردار است. این برنامه همچنین می‌تواند به هر اندازه‌ای که شما می‌خواهید برای کاربران سخت‌گیر و محدود کننده و یا راحت باشد. تنظیمات پیش فرض آن به گونه‌ای است که در یک مدرسه ابتدایی لازم است؛ اما به شما این امکان را می‌دهد که آن را به گونه دلخواه خود تنظیم کنید. بطور کلی تمامی بخش‌های برنامه DansGuardian و لیست‌های سیاه این برنامه قابل تنظیم است. یک ویژگی قابل تنظیم دیگر این برنامه لیست Domain، User و Source IPهای استثنا است که قادرند از لیست‌های سیاه عبور و بدون محدودیت از اینترنت استفاده کنند. این برنامه همچنین به خوبی از SSL Tunneling پشتیبانی می‌کند.

لازم به ذکر است که برنامه DansGuardian برای اجرا به برنامه Squid و یا یک برنامه Caching Proxy Server مشابه موجود در شبکه محلی نیاز دارد و توانایی کار با برنامه‌های

پروکسی غیر از برنامه Squid را داراست. برای نمونه قادر به کار با برنامه Oops است. قابلیت‌های این برنامه به شرح زیر هستند:

- به طور قابل ملاحظه‌ای ارزانتر از برنامه IGear است که یکی از بهترین ابزارهای فیلترینگ تجاری می‌باشد.
- قابلیت مسدود کردن تبلیغات با استفاده از لیست URLهای تبلیغاتی که باید مسدود شوند را داراست.
- قابلیت فیلتر کردن صفحات html و text را برای محتواهای غیرقانونی و غیر اخلاقی دارد.
- از یک سیستم پیشرفته وزن گذاری عبارت‌ها (phrase weighting system) برای کاهش مسدود کردن‌های اضافی و یا مسدود کردن‌های ناقص استفاده می‌کند.
- قابلیت فیلتر کردن وب‌سایت‌ها را بر اساس سیستم PICS (Platform for Internet Content Selection) دارد.
- قابلیت فیلتر کردن را با توجه به MIME typeها و پسوندهای فایل داراست.
- فیلترینگ از طریق URL همانند لیست‌های سیاه در برنامه SquidGuard است.
- فیلترینگ از طریق URL در آن دارای قابلیت فیلتر کردن درخواست‌های مربوط به https است.
- قابلیت کار کردن در حالت ' white list ' را دارد که در آن همه سایت‌ها به جز سایتهایی که در لیست قرار دارند مسدود می‌شوند.
- قابلیت مسدود کردن کلیه URLهای مبتنی بر IP را دارد.
- قابلیت مسدود کردن سایت‌ها را حتی در زمانی که کاربران قصد ورود به سایت را از طریق آدرس IP دارند، داراست.
- فایل log را در یک قالب بسیار ساده و خوانا ایجاد می‌کند.
- فایل log را در قالب CSV برای Import آسان به بانک اطلاعاتی ایجاد می‌کند. (در صورت تمایل)
- قابلیت log گرفتن از Usernameها را با استفاده از احراز هویت Proxy دارد.
- توانایی غیرفعال کردن فیلترینگ را برای سایت‌های خاص، و برخی از کاربران دارد.

- قابلیت محدود و یا مسدود کردن بارگذاری(Upload) بر روی وب را دارد. (برای مثال حجم Attachmentها در وب سایت Hotmail)
- قابلیت مسدود کردن IPهای منبع خاص را دارد.
- قابلیت کار کردن در حالت مخفی را دارد، به گونه‌ای که توانایی مانیتور کردن کاربران را بدون آنکه متوجه شوند دارید.
- از الگوریتم هوشمندی برای یافتن عبارات غیرمجاز سایت‌ها که در کدهای Html مخلوط شده‌اند، استفاده می‌کند.
- از کاراکتر ستهای Big5، Unicode و top-bit برای جستجوی عبارت‌های غیرمجاز استفاده می‌کند.
- DansGuardian 2.4 بیشتر از ۶ برابر از DansGuardian 1.x.x سریعتر است.
- URL filtering در آن به طور قابل ملاحظه‌ای از SquidGuard سریعتر است.
- کاملاً پیاده‌سازی شده با زبان C++ که می‌تواند در GCC3 کامپایل شود.
- قابلیت کار کردن با Squid و Oops را به طور کامل دارد.
- از Compressed Html پشتیبانی می‌کند.
- می‌تواند تنها به یک IP خاص نظارت داشته باشد.

۲-۹-۲- معرفی اجمالی برنامه SquidGuard

برنامه SquidGuard یک برنامه بسیار سریع، قابل تنظیم و قدیمی برای فیلتر کردن و بازنویسی URL در برنامه معروف Squid است. قابلیت‌های این برنامه به شرح زیر هستند:

- محدود کردن گروهی از کاربران به دسترسی محدود فقط به برخی از URLها.
- بستن کلی بعضی از URLها مانند URLهای سایت‌های غیر مجاز برای گروهی از کاربران.
- بستن کلی URLهایی که با قوانین Regular Expressions سازگار می‌شوند.
- بستن کلی بعضی از URLهایی که بر اساس IPهای دامنه‌های غیر مجاز می‌باشند.
- ارسال صفحه‌های مبنی بر CGI به کاربران برای URLهای مسدود شده.
- ارسال کاربران تعریف نشده در سیستم به صفحه‌های ثبت کاربران.

- بازنویسی آدرس فایل‌های متداول جهت دانلود فایل به آدرس‌های محلی در سیستم.
- بازنویسی آدرس فایل‌های تبلیغاتی مانند فایل‌های متحرک GIF به آدرس فایل‌های محلی.
- امکان تعریف دسترسی‌های مختلف بر اساس ساعات روزانه، روزهای هفته و تاریخ.
- امکان تعریف دسترسی‌های مختلف برای گروه‌های کاربران مختلف.

از جمله مهمترین نقاط ضعف برنامه SquidGuard می‌توان به موارد زیر اشاره نمود:

- بازنویسی متن داخل صفحات.
- بازنویسی و حذف انواع اسکریپت‌های داخل صفحات

شکل ۲-۴۶: آرم برنامه SquidGuard

برنامه SquidGuard بسیار بهینه طراحی شده است و در یک کامپیوتر 500 MHz، پردازش ۱۰۰،۰۰۰ درخواست وب را در ۲۰۰۰۰۰ آدرس URL لیست شده غیر مجاز، در حدود ۱۰ ثانیه انجام می‌دهد. همچنین کد متن این برنامه بسیار قابل انتقال است و در اکثر سیستم‌عامل‌های مشابه UNIX مانند Linux ، FreeBSD، AIX و Solaris قابل استفاده است.

از برنامه SquidGuard برای فیلترینگ در یک سازمان کوچک مانند شرکت، مدرسه و دانشگاه و حتی یک ISP کوچک می‌توان استفاده کرد. دقت شود که از این برنامه برای فیلتر کردن واقعی محتوای صفحات نمی‌توان استفاده کرد.

۲-۹-۳- معرفی اجمالی برنامه Internet Junk Buster

برنامه Internet Junk Buster یا به اختصار IJB، یک برنامه پروکسی به همراه قابلیت فیلتر کردن URL است. هدف اصلی این برنامه افزایش Privacy یا حریم خصوصی کاربر است. این برنامه به تنهایی یا با استفاده از برنامه معروف Squid قابل استفاده است.

The Internet
JUNKBUSTER

شکل ۲-۴۷: آرم Internet Junk Buster

قابلیت‌های این برنامه به شرح زیر هستند:

- بستن کلی بعضی از URLها مانند URLهای سایتهای غیر مجاز بر اساس لیست سیاه این برنامه.
- حذف Cookieهای نا خواسته.
- حذف Headerهای اضافی بین برنامه مرورگر وب و سرور وب.
- برنامه IJB دارای لیسانس GPL است و به صورت شخصی یا در به صورت یک سرور برای گروهی از کاربران قابل استفاده است.

۲-۹-۴- معرفی اجمالی برنامه Privoxy

برنامه Privoxy یک برنامه پروکسی بسیار کامل است که امکانات زیر را دارا می‌باشد:

- قدرت فیلترینگ بسیار پیشرفته و کامل.
- تغییر محتوای صفحات وب، مانند تغییر متن داخل صفحه.
- مدیریت کامل Cookieها.
- کنترل دسترسی و دستیابی آدرس‌ها.
- حذف تبلیغات ناخواسته.
- حذف Bannerهای تبلیغاتی.
- حذف پنجره‌های اضافی (Pop Ups).

برنامه Privoxy با استفاده از کد برنامه Internet Junk Buster توسعه و طراحی شده است و دارای لیسانس GPL است. این برنامه به‌صورت شخصی و یا گروهی قابل استفاده است.

۲-۱۰- آیا فایروال تمام مشکلات امنیتی را از بین می برد؟

طبیعی است که جواب این سوال منفی است. فایروال تنها جزئی از راه حل امنیتی است و برقراری امنیت کامل مستلزم رعایت نکات بسیار مهمی است. حتی فایروال به تنهایی نمی‌تواند از تمامی تهدیدهای شبکه‌ای جلوگیری کند. در ادامه بعضی از نقاط ضعف یک فایروال ذکر شده است.

- عدم امکان مقابله با حملاتی که از فایروال عبور نمی‌کنند.
- عدم امکان مقابله به خطرات ناشی از اشتباهات عمدی/غیر عمدی مدیران سیستم.

- عدم امکان مقابله با خطرات غیر مربوط به شبکه نظیر کپی غیر قانونی داده‌ها.
- عدم امکان مقابله صددرصد در مقابل ویروسها و کرمهای اینترنتی (این بدان معنی است که برای محافظت در مقابل ویروسها صرفاً نمی‌توان به یک فایروال اکتفا کرد و استفاده از نرم‌افزار حرفه‌ای آنتی ویروس ضروری است.)

معمولاً فایروال‌ها نمی‌توانند بسته‌های فشرده شرده و یا رمز شده را مورد واررسی قرار دهند و اگر کاربر اجازه تردد چنیین بسته‌هایی را داده باشد فایروال در مقابل طیف زیادی از حملات آسیب‌پذیر خواهد بود.

۲-۱۱- معرفی اجمالی نحوه فیلترینگ و فایروال در کشور چین

برنامه فیلترینگ در کشور چین که به Golden Shield یا با توجه به دیواره باستانی چین (Great Wall of China) به نام The Great Firewall of China معروف است به لحاظ تکنیکی شامل بخش‌های زیر است:

مسدود کردن آدرس‌های اینترنتی(IP) : دسترسی به برخی از آدرس‌های اینترنتی غیر مجاز است. برای مثال اگر این آدرس اینترنتی یک وب سرور اشتراکی باشد، دسترسی به تمام وب سایت‌های این وب سرور مسدود خواهد شد. این مساله تمام پروتکل‌های زیر مجموعه TCP مانند Web، Ftp، IMAP و POP را نیز شامل می‌شود. کاربران چینی، برای دور زدن این مساله مجبورند از پروکسی سرورها استفاده کنند، ولی بسیاری از سایت‌های معروف مانندWikiPedia، استفاده از پروکسی را ممکن نمی‌کنند. برخی شرکت‌ها مانند Google که مسدود شده بودند، برای حل این مشکل، آدرس‌های اینترنتی جدید به مجموعه خود اضافه کردند ولی خیلی سریع، آدرس‌های جدید نیز توسط این برنامه مسدود شد.

مسدود کردن و فیلتر کردن DNS: با استفاده از این سیستم، آدرس واقعی سایت‌های غیرمجاز، به غلط گزارش می‌شده است. این مساله مجددا، فیلتر کردن تمام پروتکل‌های زیر مجموعه TCP مانند Web، Ftp، IMAP و POP را نیز شامل می‌شود. کاربران چینی برای دور زدن این مساله می‌باید از DNS سرورهایی استفاده می‌کردند که آدرس صحیح سایت‌ها را گزارش کند و این DNS سرورها به تدریج توسط برنامه مسدود شدند.

مسدود کردن و فیلتر کردن URL: با استفاده از این سیستم بسته‌های اطلاعاتی به دنبال آدرس‌های URL خاص جستجو می‌شود و دامنه‌ها و آدرس‌های خاص مسدود می‌شوند. این

مساله فقط پروتکل HTTP را تحت تاثیر قرار می‌دهد. کاربران چینی برای دور زدن این مساله ناچار به استفاده از پروتکل HTTPS و یا استفاده از VPN و SSL هستند.

مسدود کردن و فیلتر کردن Packetها: در این سیستم، هنگامیکه در یک ارتباط دو طرفه بین کاربر و مقصد، تعداد مشخصی از واژه‌های سیاه در یک بسته اطلاعاتی وجود داشته باشد، بسته مربوطه فیلتر می‌شود. کاربران چینی برای دور زدن این مساله ناچار به استفاده از VPN و SSL هستند.

مسدود کردن ارتباطات سیاه قبلی: در این سیستم، هنگامیکه ارتباط کاربر و مقصد به دلایل مختلف قطع شده است، ادامه این ارتباط به مدت ۳۰ دقیقه به طور دو طرفه مسدود می‌شود.

در مورد فیلترینگ نیز یکی از موارد مسدود شده نتایج جستجوی عبارت‌های خاص و معینی در موتورهای جستجویی مانند Yahoo و Google بوده است. در واقع جستجوی این قبیل عبارت‌ها یا نتیجه ای در بر نداشته و یا نتایج غیر قابل استفاده برای کاربران ارائه می‌داده است. از همین رو و با توجه به نوع سانسور و فیلترینگ در کشور چین، بسیاری از شرکت‌ها و سایت‌های تجاری مانند Google و AltaVista خود اقدام به برپایی سانسور داخلی با توجه به قوانین کشور چین کردند تا بتوانند در این کشور سرویس دهند.

پس از مطالعات و تحقیقات بعمل آمده بر روی اصول و قوانین سانسور و مسدود کردن محتوای اینترنتی در چین ، می‌توان مضامین مسدود شده را بصورت زیر دسته بندی کرد:

- وب سایت‌های وابسته به گروه‌های مخالف.
- اخبار و منابعی که شامل عناوینی می‌باشند که از دیدگاه مذهبی نهی شده باشد.
- وب سایت‌های وابسته و مربوط به دولت تایوان و همچنین مربوط به رسانه‌ها و یا سازمان‌های تایوان.
- وب سایت‌هایی که شامل محتوای غیر اخلاقی از قبیل خشونت و Porno .

مدل فایروال در کشور چین می‌تواند به عنوان یک الگو برای فایروال در کشور ما محسوب شود.

۲-۱۲- نتایج

در این قسمت نرم‌افزارهای متن‌باز مختلفی برای تولید فایروال و بر پایی فیلترینگ عنوان شدند که هر کدام ویژگی و شرایط کاری و امکانات خاص خود را دارند.

در میان نرم‌افزارهای فایروال و Packet Filtering با توجه به اینکه نرم‌افزار iptables به عنوان یک برنامه در حال توسعه و سریع در میان سایر برنامه‌ها کاملا متمایز است، از این نرم‌افزار می‌توان در بسیاری از کاربردهای عمومی استفاده کرد و از مزایای خوب این برنامه بخصوص در محیط‌های NAT شده استفاده کرد.

در میان برنامه‌های فیلترینگ، در صورتیکه هدف کنترل کامل محتوا باشد، می‌توان از برنامه DansGuardian و امکانات ویژه و متمایز آن استفاده کرد. در صورتیکه هدف فقط فیلترینگ URL باشد، می‌توان همچنین از برنامه DansGuardian یا برنامه‌های مشابه مانند SquidGuard استفاده کرد.

لطفاً دقت شود که اگرچه برنامه DansGuardian یک برنامه متن‌باز است، ولی مولف آن استفاده تجاری از این برنامه را منوط به پرداخت هزینه جزئی برای ادامه حیاط این پروژه کرده است.

فصل سوم– سیستم‌های تشخیص نفوذ

نرم‌افزارهای IDS در واقع نفوذ و یا تلاش برای نفوذ کردن افراد بیگانه را شناسایی می‌کند. از آنجایی که انواع روش‌هایی که ممکن است یک نفوذگر به کار گیرد تا بتواند به یک سیستم نفوذ کند بسیار متنوع و گسترده است، نرم‌افزارهای IDS بسیار متنوع و متفاوت از یکدیگر به وجود آمده اند. تقریبا تمام نرم‌افزارهای IDS بخصوص نرم‌افزارهای NIDS از سه جزء منطقی زیر تشکیل شده‌اند:

- سنسورها: برای دریافت اطلاعات اولیه و کشف نفوذها.
- کنسول: برای نمایش اطلاعات و نفوذهای کشف شده و ارسال اخطارها.
- هسته مرکزی: برای ثبت کلیه اطلاعات ، دریافت آمار و انجام پردازش‌های مختلف.

نرم‌افزارهای IDS را می‌توان بسته به اختلاف این سه جزء مانند محل قرار گیری سنسورها، انواع نفوذهای قابل تشخیص، انواع کنسول‌ها و اخطارهای صادره و نوع هسته مرکزی به رده‌های زیر تقسیم بندی کرد:

نرم‌افزارهای NIDS[1]: این برنامه‌ها و نرم‌افزارها برای تشخیص نفوذها در محیط‌های شبکه استفاده می‌شوند. محل قرار گیری مناسب این نرم‌افزارها معمولا در ابتدای اتصال شبکه محلی به اینترنت و یا در فضای DMZ و نقاط کلیدی دیگر بسته به توپولوژی و طرح شبکه است.

نرم‌افزارهای PIDS[2]: این برنامه‌ها بین نرم‌افزارهای سرویس دهنده مانند HTTP Server و SMTP Server و برنامه‌های سرویس گیرنده مانند Internet Explorer و Out Look قرار می‌گیرند و تنها به یک پروتکل خاص نظارت می‌کنند. این برنامه‌ها باید قادر باشند هرگاه سرویس دهنده یا سرویس گیرنده از عملکرد طبیعی پروتکل خارج شدند و سعی در تخریب و نفوذ در سیستم دیگری را داشتند، هشدارهای لازم را صادر کنند. پیاده سازی نرم‌افزارهای PIDS بسیار مشکل و هزینه‌بر است، از این رو نسخه‌های متن‌باز از این سیستم‌های تشخیص نفوذ بسیار کمیاب هستند.

نرم‌افزارهای APIDS[3]: این برنامه‌ها شبیه به نرم‌افزارهای PIDS هستند با این تفاوت که روابط بین برنامه‌ها را نظارت می‌کنند. به عنوان یک نمونه، یک APIDS می‌تواند به ارتباط

---

[1] Network Intrusion Detection System
[2] Protocol-Based Intrusion Detection System
[3] Application Protocol-Based Intrusion Detection System

برنامه‌ها با بانک اطلاعاتی SQL نظارت داشته باشد و هر گاه متوجه بشود که یک برنامه خاص، رفتار صحیح خود را ندارد، هشدارهای لازم را ارسال می‌کند. از آنجا که نرم‌افزارهای APIDS بسیار وابسته به برنامه‌های میانی مانند بانک‌های اطلاعاتی هستند، نسخه‌های عمومی و متن‌باز از این نوع برنامه‌ها چندان وجود ندارد.

نرم‌افزارهای HIDS[1]: نرم‌افزارهای HIDS برنامه‌هایی هستند که در یک کامپیوتر مستقل عمل می‌کنند و تلاش برای نفوذ یا نفوذهای موفق را کشف می‌کنند. این نرم‌افزارها از تمام امکانات متداول و موجود در یک سیستم‌عامل مانند Logها و اخطارهای کلی در کنار ابزارهای خاص خود، مانند ابزارهای کنترل محتویات فایل‌های پایه‌ای سیستم و ابزارهای کنترل سلامت هسته سیستم‌عامل استفاده می‌کنند تا حملات و نفوذها را کشف کنند.

نرم‌افزارهای Hybrid IDS[2]: این نرم‌افزارها، ترکیبی از چند نوع روش تشخیص نفوذ هستند و با استفاده همزمان از این روش‌ها تلاش می‌کنند نفوذهای ترکیبی و پیشرفته را تشخیص دهند. برای نمونه ممکن است یک نرم‌افزار Hybrid IDS روش‌های تشخیص نفوذ ترکیبی مانند NIDS و HIDS را در کنار یکدیگر به کار گیرد تا بتواند یک سیستم IDS متمرکز و کارا فراهم آورد. نرم‌افزارهای Hybrid IDS نسل جدید نرم‌افزارهای IDS محسوب می‌شوند.

نرم‌افزارها و سیستم‌های تشخیص نفوذ (IDS) در واقع به عنوان سپر دوم مقابله با ویروس‌ها، خرابکاران و نفوذگران محسوب می‌شوند. سپر اول همواره نرم‌افزارهای فایروال (Firewall) است که جلوی بسیاری از حملات و نفوذها را می‌گیرند. به بیان دیگر، نرم‌افزار IDS به عنوان مکمل Firewall محسوب می‌شود و نقاط ضعف Firewall را مشخص می‌کند. نرم‌افزار IDS هوشمند در صورتیکه امکان مقابله با حمله یا نفوذگر را داشته باشد به Intrusion Detection and Prevention System یا IDP معروف است. برای مثال نرم‌افزارهای IDP در محیط شبکه با Firewall ارتباط برقرار می‌سازند و Firewall را در جهت مقابله با حملات کشف شده آگاه و تنظیم می‌کنند. نرم‌افزارهای IDP نسل تکمیل یافته نرم‌افزارهای IDS محسوب می‌شوند و عمدتا با Firewallهای تجاری مانند PIX ، Juniper و غیره سازگارند.

تقریبا تمام ارگان‌های ارئه دهنده سرویس، مانند IDCها و ارگان‌هایی نظیر بانک‌ها که برای نفوذگران جذابیت دارند، به ناچار می‌باید در کنار Firewall از نرم‌افزارهای IDP و

---

[1] Host-based Intrusion Detection System
[2] Hybrid Intrusion Detection System

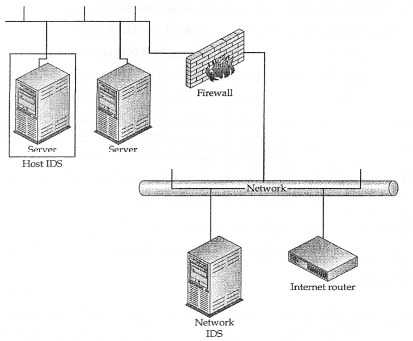
نرم‌افزارهای مشابه دیگر مانند Honey Pot (بررسی نرم‌افزارهای Honey Pot از موضوع این گزارش خارج است) برای کشف حملات و نفوذها استفاده کنند تا بتوانند امنیت اطلاعات و شبکه خود را محفوظ کنند.

۳-۱- انواع سیستم‌های IDS (تشخیص ورود غیرمجاز)

IDS دو نوع اصلی دارد:

- Host-based که به اختصار H-IDS گفته می‌شود.
- Network-based که به اختصار N-IDS گفته می‌شود.

H-IDS روی خود سیستم تحت نظر نصب می‌شود و به دنبال نشانه‌های حمله به سیستم می‌گردد. N-IDS روی سیستم جداگانه‌ای نصب می‌شود و باکنترل و مشاهده ترافیک شبکه، به دنبال نشانه حملاتی می‌گردد که روی آن بخش از شبکه در حال انجام است. شکل (۳-۱) نشان داده است این دو نوع IDS چگونه در شبکه قرار می‌گیرند.



شکل ۳-۱: مثالی از نحوه قرار گرفتن IDS در شبکه

۳-۱-۱- H-IDS

H-IDS بصورت فرآیندی نرم‌افزاری روی سیستم نصب می‌شود. سیستم سنتی H-IDS به بررسی لاگ فایل‌های ثبت شده، برای یافتن اطلاعات خاص می‌پرداخت. برای مثال در سیستم Unix در حالت عادی لاگ فایل‌های Wtmp, Lastlog, Messages, Syslog مورد بررسی قرار می‌گیرند. در سیستم ویندوز فایل‌های System، Application، Security Event logs بررسی می‌شود. فرآیند H-IDS بصورت دوره‌ای بدنبال لاگ فایل‌های جدید ثبت شده می‌گردد و آنها

را با قواعد از پیش تنظیم شده مقایسه می‌کند. اگر لاگ فایل با قاعده‌ای مطابقت کند، H-IDS کار خود را بدرستی انجام دهد لازم است اطلاعات لازم در لاگ فایل‌ها ثبت شده باشد. بنابراین در صورتی که اطلاعاتی که بیشتر جالب توجه است توسط برنامه‌ای کاربردی تولید شده باشد، لازم است آن اطلاعات توسط برنامه کاربردی مذکور داخل لاگ فایل‌های استاندارد قرار داده شود یا H-IDS قادر به بررسی لاگ فایل‌های برنامه کاربردی باشد.

اخیراً شکل جدیدی از H-IDS ایجاد شده است که درخواست‌های رسیده به هسته سیستم عامل[1] را بررسی می‌کند. این نوع H-IDS بر طبق نشانه‌های حملات شناخته شده برنامه‌ریزی شده است. بطوریکه اگر درخواست سیستمی با هر یک از این نشانه‌ها تطبیق داشته باشد هشدار داده خواهد شد.

هر دو نوع H-IDS قادرند فایل‌های روی سیستم را از نظر دستکاری کنترل کنند. این کار با پیاده‌سازی Checksum رمزنویسی روی فایل و با استفاده از یک تابع درهم‌سازی[2] همانند MD5 انجام می‌شود. Checksum ذخیره می‌شود و به عنوان مرجعی برای مقایسه با Checksumهای دوره‌ای مربوط به آن فایل استفاده می‌شود. اگر نتیجه مقایسه عدم تطبیق Checksum با مقدار اولیه آن باشد، این فایل تغییر داده شده است پس H-IDS این اطلاعات را گزارش می‌کند و هشدار می‌دهد.

سیستم H-IDS دارای سه مزیت اصلی زیر است:

- مادامیکه تهاجم انجام شده Log Message تولید می‌کند، H-IDS ترافیک حمله‌ای که به سیستم گسیل داده شده است را گم نخواهد کرد.
- H-IDS می‌تواند موفق بودن تهاجم را تشخیص دهد. H-IDS این کار را با بررسی Log message و دیگر نشانه‌های موجود روی سیستم (از قبیل دستکاری فایل‌های پیکره‌بندی و یا Key System Binaries) انجام می‌دهد.
- H-IDS می‌تواند با تعیین کاربران قانونی سیستمی، تلاش‌های غیرمجاز برای دسترسی را تشخیص دهد.

سیستم H-IDS دارای اشکالات زیر است:

- مهاجم می‌تواند فرآیند H-IDS را شناسایی و غیرفعال کند.

---

[1] Kernel
[2] Hashing

- سیستم H-IDS فقط در مواردی اعلام خطر می‌کند که درخواست‌های سیستم و محتویات لاگ فایل با قواعد و نوشته‌های از قبل تعیین شده تطبیق داشته باشد.
- برخی سیستم‌های H-IDS روی پشتیبانی و سیستم عامل تاثیر می‌گذارند. این مسئله با H-IDS که درخواست‌های سیستمی را بررسی می‌کند مربوط است.

N-IDS–۲–۱–۳

N-IDS بصورت فرآیندی نرم‌افزاری است که روی سیستم سخت‌افزاری بخصوص نصب می‌شود. N-IDS کارت واسط شبکه موجود روی سیستم را به حالت بی‌قید و شرط می‌برد، به این معنی که تمام ترافیک شبکه، توسط کارت به نرم‌افزار N-IDS عبور داده می‌شود (طرف‌نظر از اینکه ترافیک مذکور برای این سیستم فرستاده شده است یا نه). پس از آن بر طبق قواعد و قوانین مربوط به حمله، ترافیک تحلیل می‌شود تا بخشی از ترافیک که جالب توجه است تعیین شود و در صورت کشف حمله، یک رویداد یا Event تولید و ثبت می‌شود.

در حال حاضر سیستم N-IDS بگونه‌ای است که نشانه‌های حمله در سیستم کامپیوتری تعریف می‌شود و این نشانه‌ها با ترافیک سیستم مقایسه می‌گردد. حال اگر حمله‌ای انجام شود که در فایل نشانه‌ها[1] وجود نداشته باشد، N-IDS آن را بر نمی‌دارد.

سیستم N-IDS قادر است ترافیک جالب توجه را بر اساس آدرس مبدا، آدرس مقصد، پورت مبدا و پورت مقصد تعیین کند. بدین ترتیب سازمان قادر است ترافیک خارج از حوزه نشانه‌های حمل را تعریف کند.

شایع‌ترین راه پیکره‌بندی N-IDS استفاده از دو کارت واسط شبکه است. یکی از کارت‌ها جهت مشاهده و کنترل شبکه است. این کارت در حالت پنهان[2] نصب می‌شود بطوریکه آدرس IP ندارد، به همین دلیل به اتصالات ورودی پاسخ نمی‌دهد.

کارت مخفی دارای Protocol Stack Bound نمی‌باشد از این‌رو قادر به پاسخگویی به پروب‌هایی از قبیل Ping نیست. کارت دوم برای ارتباط با سیستم مدیریتی IDS و ارسال هشدار و اعلام خطر مورد استفاده قرار می‌گیرد. این کارت وابسته به شبکه داخلی است که از دید شبکه تحت کنترل مخفی است.

---

[1] Sing Nature File
[2] Stealthy

مزایای N-IDS به ترتیب زیر است:

- می‌توان N-IDS را کاملاً روی شبکه مخفی کرد بطوریکه مهاجم نمی‌داند تحت کنترل است.
- برای کنترل و مشاهده ترافیک می‌توان از یک N-IDS برای تعداد زیادی سیستم استفاده کرد.
- N-IDS می‌تواند محتوای تمام بسته‌هایی که به سوی هدف در حرکت است را بدست آورد.

اشکالات سیستم N-IDS شامل موارد زیر است:

- سیستم N-IDS فقط زمانی اعلام خطر می‌کند که ترافیک با قواعد و نشانه‌های از پیش تعیین شده تطبیق داشته باشد.
- به دلیل آنکه سیستم N-IDS پهنای باند بالا و مسیرهای جایگزین را به کار می‌گیرد امکان از دست دادن ترافیک توسط آن وجود دارد.
- N-IDS قادر به بررسی ترافیک رمزشده نمی‌باشد.
- N-IDS نمی‌تواند موفق بودن حمله را تعیین کند.
- در شبکه‌های سوئیچی (که با به اشتراک گذاشتن شبکه واسط مخالف هستند) باید تنظیمات خاصی انجام شود تا N-IDS بتواند تمام ترافیک را مشاهده کند.

۳-۱-۳- کدام نوع IDS بهتر است؟

نمی‌توان به صراحت گفت کدام نوع IDS بهتر است چون هر کدام مزایا و معایب خاص خود را دارند. در حالیکه N-IDS می‌تواند بیشتر مقرون به صرفه باشد (چون یک N-IDS می‌تواند ترافیک تعداد زیادی کامپیوتر را کنترل کند) اما در سازمان‌هایی که نگرانی در مورد کاربران قانونی بیشتر از هکرهای خارجی است H-IDS مناسب‌تر است. عامل دیگر در انتخاب نوع IDS تهدیدات اصلی متوجه سازمان است.

۳-۱-۳-۱- نصب و تنظیم IDS

به منظور گرفتن حداکثر بهره از IDS طرح‌ریزی‌های زیادی باید انجام شود. حتی قبل از آنکه سیاست مناسبی اتخاذ شود لازم است اطلاعات جمع‌آوری گردد، شبکه تحلیل شود و

مدیریت اجرا در آن لحاظ شود. همانند اکثر سیستم‌های پیچیده لازم است سیاست اتخاذ و ارزیابی شود و قبل از پیاده‌سازی مورد آزمایش قرار گیرد. مراحل اتخاذ سیاست IDS عبارتند از:

- تعریف اهداف IDS
- انتخاب آنچه باید کنترل و مشاهده گردد
- انتخاب واکنش مناسب
- تنظیم حدود آستانه
- پیاده‌سای سیاست

۳-۱-۳-۲- تعریف اهداف IDS

اهداف IDS نیازهای سیاست را برآورده می‌کند. این اهداف عبارتند از:

- کشف حملات
- پیش‌گیری از حملات
- کشف موارد تخلف از سیاست
- ضمانت اجرایی در سیاست استفاده
- ضمانت اجرایی در سیاست‌های ارتباطی
- جمع‌آوری مدارک

به خاطر داشته باشید این اهداف را می‌توان با هم ترکیب کرد، اهداف واقعی بستگی به سازمانی دارد که IDS در آن اعمال می‌شود بطوریکه نمی‌توان لیستی فراگیر تهیه کرد. امکان دارد IDS امکان کشف حمله را به هنگام آغاز آن به سازمان بدهد یا با خاتمه دادن به حادثه، امکان جمع‌آوری مدارک و جلوگیری از صدمات بیشتر را فراهم کند. البته اهدافی که توسط IDS دنبال می‌شود به همین موارد محدود نمی‌شود. از آنجائیکه اطلاعات جزئی اکثر وقایعی که روی شبکه و سیستم‌های کامپیوتری سازمان رخ می‌دهد توسط IDS گردآوری می‌شود، لذا می‌توان موارد نقض سیاست و موارد استفاده واقعی از منابع شبکه را تعیین کند.

عمومی‌ترین کاربرد IDS شناسایی[1] حمله است. IDS بگونه‌ای برنامه‌ریزی می‌شود که به دنبال وقایع معینی بگردد. این وقایع بگونه‌ای هستند که حمله در حال وقوع را آشکار می‌سازد.

[1] Attack Recognition

به عنوان مثالی ساده ارتباطی را به پورت TCP25 در نظر بگیرید که به دنبال آن دستور WIZ می‌آید. این واقعه می‌تواند نشانه‌ای از تلاش مهاجم برای اجرای حفره Wizard در نسخه قدیمی‌تر برنامه کلمه Sendmail باشد. شناسایی اکثر نشانه‌های حمله به سادگی میسر نیست. به عنوان مثال حدس زدن کلمه عبور یکی از شایع‌تری حملات در اینترنت است. به منظور مقابله با این نوع حمله می‌توان قاعده‌ای را در H-IDS قرارداد که به دنبال سه بار تلاش نادرست برای ورود به یک اکانت در یک دوره زمانی کوتاه بگردد. به منظور انجام این کار، H-IDS باید تعداد و زمان تلاش‌های نادرست برای ورود به هر اکانت را بطور جداگانه از روی لاگ فایل‌ها پیگیری کند و در صورتی که یکی از این تلاش‌ها به موفقیت انجامید یا زمان آن به اتمام رسید، اکانت را از نو تعریف کند. به عنوان مثالی پیچیده‌تر در شناسایی مهاجم، مزاحمی را در نظر بگیرید که همزمان سعی در حدس زدن کلمه عبور چندین اکانت و سیستم دارد. در این حالت مهاجم یک اکانت را دوبار امتحان نمی‌کند. در عوض یک کلمه عبور را روی چند اکانت و چند سیستم امتحان می‌کند. حال اگر زمان هر تلاش به اندازه کافی طولانی باشد، زمان‌سنجی که برای هر اکانت فاصله بین تلاشهای نادرست را اندازه می‌گیرد نمی‌تواند سه بار تلاش نادرست روی یک اکانت را تشخیص دهد. تنها رای برای تشخیص این نوع حمله جمع‌آوری اطلاعات لاگ فایل‌های سیستم‌های مختلف می‌باشد. اگر H-IDS قادر به جمع‌آوری اطلاعات در میان سیستم‌ها باشد، می‌تواند این نوع تحلیل را انجام دهد.

۳-۱-۴- نظارت بر سیاست

از جمله مواردی که در کشف حملات حتماً باید انجام شود نظارت بر سیاست است. IDS بگونه‌ای پیکره‌بندی می‌شود که با پیگیری برآورده شدن یا عدم برآورده شدن سیاست شرکت، بر آن سیاست نظارت کند. در ساده‌ترین حالت می‌توان N-IDS را بگونه‌ای پیکره‌بندی کرد که تمام ترافیک خروجی وب از شبکه را دنبال کند. این پیکره‌بندی به H-IDS امکان می‌دهد موارد برآورده نشدن سیاست استفاده از اینترنت را دنبال کند. در این حالت لیستی از وب‌سایت‌ها وجود دارد که بر طبق استاندارد شرکت، برقراری ارتباط با آنها تخلف محسوب می‌شود. در صورت برقراری ارتباط با این سایت‌ها، N-IDS را ثبت می‌کند.

از N-IDS می‌توان برای کنترل پیکره‌بندی روتر و فایروال هم استفاده کرد. در این حالت N-IDS به دنبال ترافیکی می‌گردد که روتر یا فایروال نباید آن را عبور دهد. پیدا شدن چنین ترافیکی دلالت بر تخلف از سیاست فایروال شرکت دارد.

۳-۱-۵- اعمال سیاست[1]

استفاده از IDS به عنوان ابزار اعمال سیاست باعث می‌شود پیکره‌بندی نظارت بر سیاست، یک قدم به جلو پیش برود. به منظور اعمال سیاست، IDS بگونه‌ای پیکره‌بندی می‌شود که به محض تخلف از سیاست واکنش نشان دهد. در مثال قبل که در مورد نظارت بر سیاست آورده شد، اعمال سیاست باعث می‌شود علاوه بر شناسایی ارتباطی که به یک وب‌سایت غیرمجاز انجام شده است، از برقراری ارتباط نیز جلوگیری شود.

IDS ابزاری با ارزش پس از شناسایی حمله می‌باشد. IDS قابل استفاده در شناسایی ابتدایی حادثه است و در عین حال پس از وقوع حادثه به عنوان ابزاری برای جمع‌آوری مدارک و ثبت لاگ فایل‌ها استفاده می‌شود. N-IDS را می‌توان در این نقش بگونه‌ای پیکره‌بندی نمود که به دنبال ارتباطات خاص بگردد و از کل ترافیک لاگ فایل تهیه کند. همزمان می‌توان H-IDS را بصورتی پیکره‌بندی کرد که تمام ورودی‌هایی را که به اکانت‌های بخصوص انجام می‌شود ثبت کند.

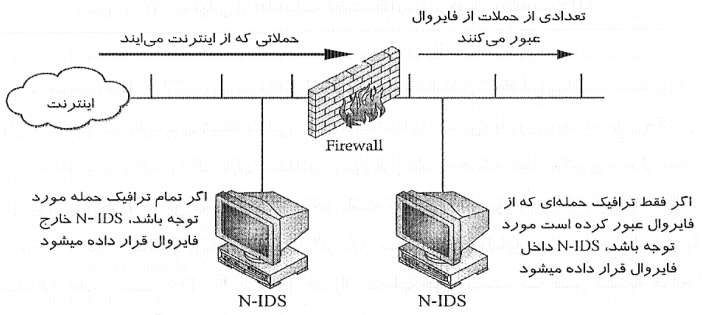
انتخاب آنچه باید تحت نظارت قرار گیرد تابع اهداف IDS و محیطی است که IDS در آن کار خواهد کرد. برای مثال اگر هدف IDS کشف حملات باشد و IDS روی اینترنت و خارج از فایروال شرکت قرار گرفته باشد، IDS برای شناسایی حملات ورودی باید تمام ترافیکی که به سوی فایروال می‌آید را نظارت کند. به طریق دیگر می‌توان IDS را داخل فایروال قرارداد تا فقط حملاتی که موفق به گذشتن از فایروال شده‌اند را شناسایی نماید. در این حالت می‌توان از ترافیک خروجی طرف‌نظر کرد (شکل۳-۲). در جدول ۱ به ازاء هر سیاست، مثال‌هایی ازآنچه باید نظارت شود دیده می‌شود.

در مرحله بعد محل قرارگیری سنسورها، تابع آنچه باید تحت نظارت باشد می‌باشد. سنسورها را می‌توان در خارج فایروال، روی شبکه داخلی، روی سیستم‌های حساس، یا روی

---

[1] Policy Enforcement

سیستم‌هایی که به منظور جمع‌آوری و پردازش لاگ فایل‌ها استفاده می‌شود قرار داد. به هنگام تصمیم‌گیری درباره محل قرارگیری سنسور IDS به این موضوع خیلی توجه داشته باشید که سنسور باید قادر به مشاهده وقایع جالب توجه، ترافیک شبکه و ورود به آن باشد. اگر مایل به گذشتن وقایع جالب توجه از فایروال نیستید، قراردادن سنسور N-IDS در داخل فایروال انتخاب خوبی نیست. به طور مشابه چنانچه وقایع جالب توجه فقط روی کنترل کننده اصلی حوزه[1] در شبکه ویندوز NT ثبت می‌شود لازم است نرم‌افزار H-IDS روی کنترل کننده اصلی حوزه قرار داده شود، حتی اگر مهاجم از لحاظ فیزیکی روی یک کامپیوتر، جایی در شبکه قرار داشته باشد.



شکل۳-۲: مثال برای انتخاب آنچه باید نظارت شود

به هنگام قرار دادن سنسور N-IDS باید به یک نکته کلیدی دیگر توجه داشته باشید. اگر در شبکه به جای هاب از سوئیچ استفاده شده است و سنسور N-IDS فقط به پورت سوئیچ اتصال دارد، سنسور N-IDS بدرستی کار نخواهد کرد، چون فقط ترافیکی که مخصوص خود N-IDS است، به پورتی که سنسور به آن خورده است فرستاده می‌شود. در این گونه شبکه‌های سوئیچی می‌توان از دو جایگزین برای سنسورهای N-IDS استفاده کرد. (در شکل ۳-۳ هر دو پیکره‌بندی دیده می‌شود)

استفاده از پورت ناظر سوئیچ[2] سه راهی شبکه ممکن است استفاده از پورت ناظر سوئیچ با وظائف مدیریت شبکه تداخل پیدا کند چون مدیریت شبکه از این پورت به منظور اشکال‌زدایی شبکه استفاده می‌کند. علاوه بر این در بسیاری از سوئیچ‌ها در هر لحظه فقط امکان نظارت بر

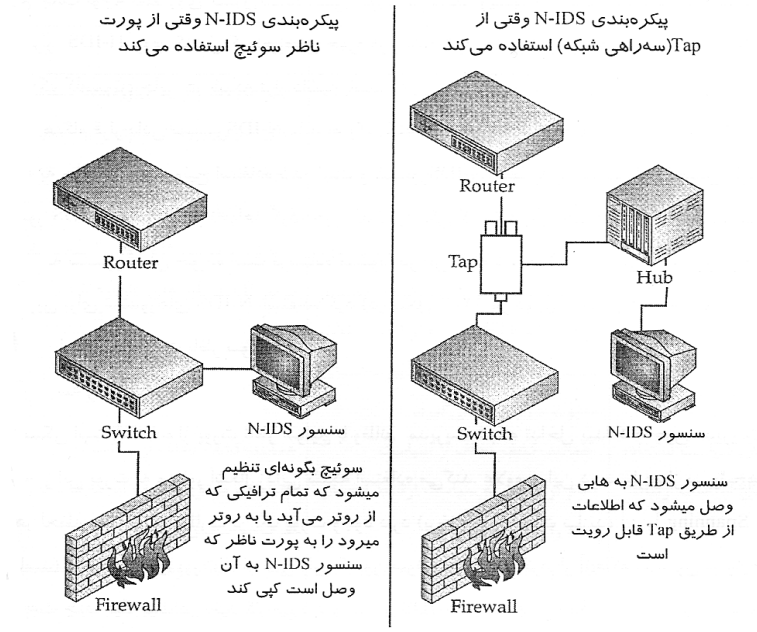
[1] Primary Domain Controller
[2] Switch Monitoring Port

یک پورت وجود دارد (برخی کارخانجات سازنده آن را Spanning می‌نامند) عموماً از روی پورت ناظر نمی‌توان Backbone سوئیچ را نظارت کرد. از آنجا که Backbone سوئیچ با سرعت چند گیگا بیت در ثانیه کار می‌کند و سنسور N-IDS از اتصال 100 BaseT (با سرعت صد مگابیت در ثانیه) استفاده می‌کند، پس در هیچ صورتی نمی‌تواند کار کند. این نوع اتصال دادن ارتباطات در این پیکره‌بندی میسر نیست.

جدول ۳-۱: مثال‌هایی از اطلاعات تحت نظارت بر طبق سیاست IDS

سیاست	N-IDS	H-IDS
کشف حملات	تمام ترافیکی که بداخل سیستم هدفهای احتمالی وارد می‌شود (فایروال،سروروب، سرور کاربردی و ...)	تلاش‌های ناموفق برای ورود. تلاشهای موفق برای ورود از طرف سیستم‌های دوردست.
پیشگیری از حملات	همانند کشف حملات	همانند کشف حملات
کشف تخلف از سیاست	تمام ترافیک HTTP که از سیستم‌های کلانیت سرچشمه می‌گیرد. تمام ترافیک FTP که از اتصالات سیستم‌های کلاینت روی پورت‌های معیوب سرچشمه می‌گیرد.	ارتباطات موفق HTTP، ارتباطات موق FTP، فایل‌های دان‌لود شده.
اعمال سیاست استفاده	همانند کشف تخلف از سیاست	همانند کشف تخلف از سیاست
اعمال سیاست ارتباط	تمام ترافیکی که سیاست ارتباط اعمال شده را نقض می‌کند.	ارتباطات موفق از طرف آدرس‌ها و یا به طرف پورت‌ها ممنوعه
جمع‌آوری مدارک	محتوای تمام ترافیکی که از سیستم هدف و مهاجم گرفته است.	تمام ارتباطات موفق از طرف سیستم مهاجم. تمام ارتباطات ناموفق از طرف سیستم مهاجم.

سه راهی یا Tap یک اتصال غیرفعال روی سیمی است که دو وسیله را (مانند روتر و سوئیچ) به هم وصل کرده است. عموماً Tap به همان هابی وصل می‌شود که سنسور N-IDS هم به همین هاب وصل شده است. بدین ترتیب امکان مشاهده ترافیک سنسور N-IDS فراهم می‌شود. از آنجا که در این پیکره‌بندی سنسور N-IDS مستقیماً بین فایروال و روتر قرار نگرفته است، لذا نمی‌تواند نقشی درارتباط دهی داشته باشد.



شکل ۳-۳: پیکره‌بندی سنسور N-IDS در شبکه سوئیچی

۳-۱-۶- انتخاب نحوه واکنش

همانند انتخاب آنچه باید نظارت شود، انتخاب واکنش مناسب هم تابع اهداف IDS می‌باشد. به هنگام بروز واقعه می‌توان واکنش پسیو (واکنشی که به طور مستقیم مانع فعالیت مهاجم نمی‌شود) یا واکنش اکتیو (واکنشی که مستقیماً سعی می‌کند مانع فعالیت مهاجم گردد) اتخاذ کرد.

منظور از واکنش پسیو این نیست که اجازه دهید واقعه رخ دهد و به کار خود ادامه دهد بلکه در این حالت فعالیت متقابل مستقیماً توسط IDS انجام نمی‌گیرد، این تفاوت مهم را به خاطر بسپارید.

علاوه بر این استفاده از واکنش خودکار یا واکنشی که توسط انسان کنترل می‌شود باید با ارزیابی انتخاب شود. در ادامه هر یک از واکنش‌های پسیو و اکتیو را بررسی می‌کنیم.

۳-۱-۶-۱- واکنش پسیو

شایع‌ترین کاری که به هنگام کشف ورود غیرمجاز انجام می‌گیرد واکنش پسیو است. دلیل این امر ساده است: احتمال اینکه واکنش پسیو باعث تجزیه و فروپاشی ترافیک مجاز شود کم است و در عین حال دارای ساده‌ترین پیاده‌سازی در روش‌های کاملاً خودکار می‌باشد. بطور کلی واکنش پسیو بیشتر جنبه جمع‌آوری اطلاعات دارد و با توجه دادن به افراد مجاز از آنها می‌خواهد در موقع لزوم فعالیت قوی‌تری از خود نشان دهند. در مورد واکنش پسیو می‌توان به موارد زیر اشاره کرد:

پرهیزکردن[1]. امروزه عمومی‌ترین و بیشترین واکنشی که در برابر تهاجم انجام می‌شود پرهیز کردن و یا نادیده پنداشتن آن است. در اکثر موارد پس از آنکه سازمان ارتباط اینترنت را برقرار و فایروال را نصب می‌کند این واکنش را بصورت پیش‌فرض اتخاذ می‌کند. در اینجا سازمان مذکور نسبت به توقف حملات از جانب اینترنت، به فایروال خود اعتماد می‌کند. از این نوع واکنش بصورت تصنعی‌تری هم استفاده می‌شود که به آن IDS مصنوعی گفته می‌شود. در این حالت اگر حمله‌ای نسبت به سرویس غیر موجود انجام شود یا حمله بصورتی باشد که فایروال در برابر آن آسیب‌ناپذیر باشد، IDS آن را نادیده می‌گیرد. یک دلیل خوب برای نادیده گرفتن حمله از جانب سیستم این است که سیستم حساسیتی نسبت به این نوع حمله ندارد. برای مثال می‌توان به تهاجم Microsoft IIS علیه سرور وب unix اشاره کرد و به عنوان مثالی دیگر می‌توان حمله Sensmail علیه سرور Microsoft Exchange را نام برد. هیچکدام از حملات نامبرده به موفقیت نخواهند رسید چون سیستم نسبت به آن آسیب‌ناپذیر می‌باشد.

واقعه نگاری[2]. اگر به محض بروز هر نوع واقعه‌ای تا آنجا که امکان دارد درباره آن اطلاعات جمع‌آوری گردد می‌توان تحلیل جزئی‌تری درباره آن انجام داد، بطوریکه در تصمیم‌گیری برای اقدامات بیشتر کمک می‌کند. واقعه‌نگاری از یک واقعه، واکنشی از نوع پسیو است. IDS می‌تواند از اطلاعات پایه جمع‌آوری شده (همانند آدرسIDS، زمان و تاریخ، نوع واقعه، ID فرآیند، ID کاربر و ...) واقعه را شناسایی کند.

واقعه نگاری تکمیلی. با جمع‌آوری اطلاعات بیشتر درباره واقعه می‌توان واکنش پسیو قوی‌تری انجام داد. برای مثال اگر در واقعه‌نگاری عادی برای تمام اتصالات فقط آدرس IP و

---

[1] Shunning
[2] Logging

شماره پورت ثبت گردد، واقعه نگاری تکمیلی باعث می‌شود IDکاربر، ID فرآیند و کل ترافیک موجود روی ارتباط واقعه نگاری گردد.

نوع دیگری از این نوع واکنش، استفاده از سرور مخصوص واقعه‌نگاری است. در این حالت سازمان از چند سیستم واقعه‌نگاری استفاده می‌کند که روی شبکه توزیع شده‌اند و به محض شناسایی یک واقعه روشن می‌شوند. این سرورهای مخصوص واقعه‌نگاری، اطلاعات را بصورت جزء به جزء جمع‌آوری و ثبت می‌کنند. از این اطلاعات جهت تشخیص مبدا ترافیک استفاده می‌شود و چنانچه اقدامات قانونی در آینده انجام شود می‌توان از آنها به عنوان مدرک استفاده کرد.

اخطار دادن. به جای اینکه به هنگام بروز واقعه فقط آگاهی داده شود، IDS می‌تواند با اخطار دادن چند نفر را درباره آن واقعه مطلع کند. اخطار می‌تواند شکل‌های متفاوتی داشته باشد که از آن جمله می‌توان به صفحه چشمک‌زن، آژیرخطر، ارسال Mail و پیام پیجر اشاره کرد. انتخاب چگونگی اخطار به وضعیت و چگونگی واقعه و پیکره‌بندی IDS بستگی دارد. برای مثال اگر IDS تا ۲۴ ساعت بعد کنترل نمی‌شود استفاده از صفحه چشمک‌زن مناسب نیست. با استفاده از پیام‌پست الکترونیک می‌توان اخطار را به مکان دوردست ارسال کرد اما امکان اینکه به موقع نرسد وجود دارد. علاوه بر این به دلیل ایجاد ترافیک روی شبکه، ممکن است مهاجم از وجود IDS اطلاع پیدا کند. مزیت استفاده از پیجر[1] اعلام به موقع اخطار است، اما معمولاً نمی‌تواند اطلاعات زیاد و کافی ارائه کند بطوریکه برای انجام اقدام مناسب ابتدا باید لاگ فایل‌ها بررسی شود.

۳-۱-۶-۲- واکنش اکتیو

بوسیله واکنش اکتیو می‌توان به منظور کاهش اثرات واقعه، سریع‌ترین اقدام ممکن را انجام داد. البته باید حواشی اقدامات مذکور به دقت بررسی و مجموعه قواعد آن مورد آزمایش قرار گیرد، در غیر این صورت واکنش اکتیو می‌تواند باعث اخلال گردد و حتی از سرویس‌دهی به کاربران قانونی جلوگیری کند. در مورد واکنش اکتیو می‌توان به اقدامات زیر اشاره کرد:

خاتمه دادن به اتصال، Sessions و پروسس شاید آسانترین اقدام قابل فهم، خاتمه دادن به واقعه باشد. این کار با خاتمه دادن اتصالی که مهاجم در حال استفاده از آن است (این کار فقط

[1] Pager

وقتی میسر است که واقعه از TCP استفاده می‌کند). خاتمه دادن به Sessions کاربر با خاتمه دادن فرآیندی که مشکل‌زا شده است اجرا می‌شود.

با بررسی واقعه می‌توان تعیین کرد چه چیزی باید خاتمه داده شود. برای مثال اگر فرآیند از منابع سیستمی استفاده می‌کند، اقدام واضح برای مقابله با آن متوقف کردن آن است. اگر کاربری سعی می‌کند به راه نفوذ خاصی دست پیدا کند یا به فایل‌هایی دسترسی داشته باشد که مجاز به دیدن آنها نیست، لازم است به Sessions آن کاربر خاتمه داده شود و بالاخره اگر مهاجمی سعی دارد با استفاده از اتصال شبکه‌ای به راه‌های نفوذ موجود سیستم دست پیدا کند، اقدام مناسب خاتمه دادن این اتصال است.

اگر مشاهده شود از یک آدرس IP خاص تلاش‌های زیادی برای دستیابی به سیستم‌های شرکت صورت می‌گیرد می‌توان نتیجه گرفت از آن آدرس تهاجمی در حال انجام است. در این صورت است که پیکره‌بندی مجدد فایروال یا روتر انجام می‌شود. عمل پیکره‌بندی مجدد بصورت‌های موقت و دائمی انجام می‌گیرد که این امر به آدرس IP و تبعات آن روی عملکرد شرکت (متوقف کردن کل ترافیک یک شریک تجاری تاثیرات منفی روی بازده شرکت خواهد داشت) بستگی دارد. می‌توان با استفاده از قواعد فیلترهای جدید، از برقراری هرگونه اتصالی از سایت متخلف جلوگیری کرد و یا روی پورت‌های خاص این محدودیت را اعمال کرد.

سخت‌ترین نوع واکنش اکتیو، فریب دادن می‌باشد. در واکنش فریبی سعی می‌شود مهاجم به این باور برسد که موفق شده است و هنوز کسی او را شناسایی نکرده است. همزمان سیستمی که هدف تهاجم قرار گرفته است در برابر مهاجم محافظت می‌شود بدین ترتیب که مهاجم به سیستم دیگری جهت داده می‌شود یا بخش‌های حیاتی سیستم هدف به مکان امنی انتقال داده می‌شود.

یکی از انواع واکنش فریبی Honey Pot می‌باشد. Honey Pot سیستمی است که به جای سیستم اصلی قرار می‌گیرد و مهاجم را گول می‌زند. همزمان روی عملکرد مهاجم نظارت می‌شود و تمام اعمالش ثبت می‌گردد. البته اطلاعات Honey Pot واقعی نیستند اما به‌گونه‌ای است که مشابه اکثر موضوعات موجود روی سایت به نظر می‌رسد.

۳–۱–۶–۳– واکنش نیمه خودکار و تمام خودکار

واکنش نیمه خودکار عبارت است از مجموعه اقدامات از پیش تعیین شده که به هنگام رخ دادن واقعه‌ای خاص اجرا می‌شوند. این واکنش تابع پروسه‌ای مستند شده است که با تعیین کارهای خاص، باعث به راه‌افتادن مجموعه‌ای از اقدامات می‌گردد این اقدامات می‌توانند پسیو یا اکتیو باشند. واکنش خودکار را می‌توان توسط انسان یا کامپیوتر کنترل کرد.

اگر واکنش در برابر وقوع حادثه به طور کامل توسط کامپیوتر و بدون نیاز به مداخله انسان انجام گیرد واکنش تمام خودکار خواهیم داشت. این قبیل واکنش‌ها باید تابع مجموعه قواعدی باشد که کاملاً شفاف و غیرمبهم باشد و بدرستی آزمایش شده باشد. از آنجا که این نوع واکنش بدون دخالت انسان انجام می‌شود، به محض اینکه شروط قاعده‌ها برآورده شد واکنش انجام می‌شود. ایجاد واکنشی تمام اتوماتیک که جلوی کل ترافیک شبکه را بگیرد کار آسانی خواهد بود. در جدول ۲ مثال‌هایی از واکنش اکتیو پسیو مناسب برای مجموعه سیاست‌هایی که در بالا توضیح داده شد، آورده شده است.

۳-۱-۶-۴- تنظیم حدود آستانه[1]

حدود آستانه از بروز اشتباه در معیارهای تشخیص جلوگیری می‌کند از اینرو تاثیرپذیری کلی سیاست IDS را افزایش می‌دهد. بوسیله حدود آستانه می‌توان وقایع تصادفی و غیرعمدی را از وقایع عمدی تفکیک کرد. برای مثال امکان دارد یکی از پرسنل با دنبال کردن پیوندهایی که یک موتور جستجو[2] به او ارائه کرده است و وب‌سایتی غیر تجاری وصل شود. در حالی که کارمند مذکور مجاز به استفاده از موتور جستجو بوده است اما به دلیل عدم استفاده از پارامترهای صحیح در جستجو به وب‌سایتی نامناسب رسیده است. از این دست نباید منجر به گزارش از جانب IDS شود چون اینگونه گزارشات باعث صرف منابع برای رسیدگی به عملی بی‌ضرر می‌شود.

به طریق مشابه حدود آستانه‌ای که تهاجمات را کشف می‌کند باید بصورتی تنظیم شود که از جمع‌آوری اطلاعات وقایع تکی و بازرسی‌های سطح پایین صرف‌نظر کند. این امکان وجود دارد این قبیل وقایع تلاشی برای Finger نمودن یک کارمند باشد. Finger برنامه‌ای عمومی در سیستم‌های یونیکس است که عموماً به منظور کنترل آدرس‌های پست الکترونیک صحیح یا به

[1] Setting Thresholds
[2] Search Engine

دست آورد کلید عمومی استفاده می‌شود. البته اگر در مدت زمان کوتاهی تلاش می‌شود تعداد زیادی از پرسنل Finger شوند نشانه‌ای از یک مهاجم است که سعی در جمع‌آوری اطلاعات با ارزش سیستم را دارد.

انتخاب حدود آستانه مناسب برای IDS، مستقیماً به نوع وقایع و تخلف‌های صورت گرفته از سیاست بستگی دارد. تعریف حدود آستانه بصورتی که بصورت فراگیر قابل اعمال باشد غیرممکن است، با این حال می‌توان پارامترهایی را تعریف کرد و بر اساس آن حدود آستانه را تنظیم کرد. این پارامترها عبارتند از:

جدول۳-۲ : مثال واکنش‌ها بر اساس سیاست IDS

سیاست	***واکنش پسیو مناسب***	***واکنش اکتیو مناسب***
کشف حمله	واقعه نگاری واقعه نگاری تکمیلی اخطار دادن	واکنش اکتیو مناسب وجود ندارد
جلوگیری از حمله	واقعه نگاری اخطار دادن	خاتمه دادن به اتصال خاتمه دادن به فرآیند پیکره‌بندی مجدد روتر یا فایروال
کشف تخلف از سیاست	واقعه نگاری اخطار دادن	واکنش اکتیو مناسب وجود ندارد
اعمال سیاست‌های استفاده	واقعه نگری اخطار دادن	خاتمه دادن به اتصال پیکره‌بندی مجدد پروکسی
اعمال سیاست‌های ارتباطی	واقعه نگاری اخطار دادن	خاتمه دادن به اتصال پیکره‌بندی مجدد روتر یا فایروال
جمع آوری مدارک	واقعه نگاری واقعه نگاری تکمیلی اخطار دادن	فریب دادن خاتمه دادن به اتصال

مهارت کاربر. تعداد خطای کافی از جانب کاربر منجر به اخطار خطای زیاد می‌شود.

سرعت شبکه. اگر شبکه کند باشد، برای وقایعی که در آنها لازم است بسته‌های خاص طی مدت زمان خاص پدیدار شوند اخطار داده می‌شود.

اتصال شبکه‌ای منتظره. اگر IDS بگونه‌ای پیکره‌بندی شده باشد که به ازاء اتصالات شبکه‌ای خاص اخطار دهد و آن اتصال شبکه‌ای به طور عادی ایجاد شود، اخطار بروز خطا تولید خواهد شد.

بارکاری مسئول امنیتی / مدیریتی. در مواردیکه بارکاری متصدی امنیتی بالا می‌رود، حدود آستانه افزایش داده می‌شود تا تعداد اخطارهای بروز خطا تحت کنترل درآید.

حساسیت سنسور. در مواردیکه از سنسور خیلی حساس استفاده شده است باید حدود آستانه را افزایش داد تا از صدور اخطار بروز خطا به میزان زیاد پرهیز شود.

برنامه موثر امنیتی. در صورتی که برنامه امنیتی سازمان بسیار موثر و کارا باشد می‌توان برخی حملات را نادیده گرفت، چون تدابیر دفاعی دیگری روی شبکه موجود است.

آسیب پذیری‌های موجود. دلیلی ندارد برای حمله به آسیب‌پذیری‌هایی که روی شبکه وجود ندارد اخطار داده شود.

حساسیت سیستم و اطلاعات. هر چه حساسیت اطلاعات مورد استفاده در سازمان بیشتر باشد باید حدود آستانه را در سطح پایین‌تر تنظیم کرد.

اهمیت خطا. خطا دو نوع است در نوع اول خطا، واقعه‌ای رخ می‌دهد و نوع دوم در اثر عدم وقوع یک اتفاق به وجود می‌آید. در مورد خطای اول هر چه اهمیت خطا بیشتر باشد حدود آستانه بالاتر در نظر گرفته می‌شود و در نوع دوم هرچه اهمیت خطا (عدم وقوع یک واقعه) بیشتر باشد حدود آستانه پایین‌تر تنظیم می‌شود.

تعیین حدود آستانه بسیار وابسته به سازمان است. اگرچه می‌توان بصورت کلی خطوط راهنمایی را تعیین کرد اما هر سازمانی بر اساس پارامترهای فوق، درباره تعیین حدود آستانه تصمیم می‌گیرد.

۳-۱-۷- پیاده‌سازی سیستم

پیاده‌سازی عملی سیاست IDS باید با همان دقتی که در خود سیاست وجود دارد طرح‌ریزی گردد. به خاطر داشته باشید سیاست IDS روی کاغذ و به امید اینکه آزمایش‌ها و تجارب دنیای واقعی را بگذراند ایجاد می‌شود. بنابراین پس از آنکه سیاست IDS تبیین شد و حدود آستانه ابتدایی محاسبه گردید. لازم است بر طبق سیاست نهایی در محل قرار داده شود. لازم است تا زمانی که حدود آستانه در حال ارزیابی است IDS از نزدیک و بصورت دوره‌ای نظارت شود. بدین ترتیب می‌توان تجارب لازم را درباره سیاست به دست آورد بدون اینکه ترافیک مجاز شبکه یا کاربران مجاز کامپیوتری دچار مشکلی شوند.

به عنوان یک مسئله مهم در طول دوره آزمایشی، هرگونه بررسی و ارزیابی که از IDS نشات گرفته است باید به دقت پیاده‌سای شود، البته باید به صحت اطلاعاتی که توسط IDS ارائه شده است هم توجه داشت. تهمت نابجا زدن به یک کارمند یا به یک فرد خارجی که از مدارک نادرست نشات گرفته است باعث می‌شود برنامه IDS چندین قدم به عقب بازگردد و کارآیی کل برنامه از جانب شرکت زیر سوال رود.

۳–۱–۸– مدیریت IDS

هم اکنون مفهوم IDS در امنیت مورد بحث است. در حال حاضر سیستم‌های IDS در بازارهای تجاری حضور چندانی ندارند و چند سیستم N-IDS و H-IDS از فروشنده‌های مختلف وجود دارد. البته چند سیستم هم موجود است که قیمت‌گذاری نشده است.

قبل از آنکه سازمانی درباره پیاده‌سازی IDS تصمیم بگیرد لازم است اهداف این برنامه را بفهمد. شاید تا حالا متوجه شده باشید در فصول قبل اشاره‌ای به IDS نکردیم. دلیل این مطلب عدم کارکرد سیستم IDS نیست بلکه دلیلش این است که ارزش آن اثبات نشده است. برای پیکره‌بندی و مدیریت درست IDS تلاش زیادی لازم است، در صورتیکه می‌توان این میزان انرژی را در پیشگیری از ورود غیرمجاز (با تولید یک برنامه خوب امنیتی) بکار برد و نتیجه خوبی هم گرفت. چنانچه گفته شد در پیاده‌سازی IDS منابع زیادی برای موفقیت برنامه لازم است.

۳–۱–۸–۱– درک آنچه IDS قادر به بیان است

سیستم IDS فقط مسائلی را گزارش می‌دهد که از قبل برایش تعریف و پیکره‌بندی شده باشد. برای پیکره‌بندی IDS دو جزء وجود دارد. اول علائم حمله است که در سیستم برنامه‌ریزی شده است. جزء دوم وقایع دیگری است که به تشخیص مدیریت جالب توجه هستند. این وقایع شامل انواع خاص ترافیک یا پیام‌های واقعه نگاری است.

درباره علائمی که فروشندگان یا ایجاد کننده‌های سیستم IDS آنها را از پیش برنامه‌ریزی می‌کنند باید گفت آنها تعبیر خود از اهمیت این وقایع را روی سیستم اعمال می‌کنند و امکان دارد میزان اهمیتی که یک سازمان به آن واقعه می‌دهد با میزان اهمیتی که سازنده برای آن قائل شده است تفاوت بسیاری داشته باشد. از اینرو مناسب است اولویت‌بندی اولیه بعضی علائم تغییر داده شود و علائمی که برای آن سازمان به کار نمی‌رود غیرفعال شود. به خاطر داشته

باشید IDS فقط در مورد وقایعی که مشاهده می‌کند هشدار می‌دهد. اگر یک سیستم توسط سنسور H-IDS نظارت شود بطوریکه وقایع خاص را ثبت نکند، نمی‌توان انتظار داشت سنسور H-IDS آن وقایع را مشاهده کند. به طور مشابه اگر سنسور نتواند وقایع خاصی را مشاهده کند حتی در صورت وقوع آن حوادث، هشدار نمی‌دهد.

با فرض اینکه IDS به طور مناسب و صحیح پیکره‌بندی شده باشد می‌تواند سه نوع واقعه را نمایش دهد:

- وقایع شناسایی مقدماتی (از طرف مهاجم)
- حملات
- وقایع مشکوک و غیرموجه

وقایع شناسایی مقدماتی

منظور از وقایع شناسی مقدماتی تلاش‌هایی است که مهاجم قبل از اقدام به حمله واقعی انجام می‌دهد و منظور از آن جمع‌آوری اطلاعات درباره سیستم یا سیستم‌ها می‌باشد. این وقایع به پنج طبقه تقسیم می‌شوند:

- اسکن مخفی
- اسکن پورت[1]
- اسکن Trojan
- اسکن آسیب‌پذیری‌ها
- فضولی در محتوای فایل

اکثر این وقایع روی شبکه اتفاق می‌افتد و اکثر آنها از طرف اینترنت و علیه سیستم‌های با آدرس خارجی رخ می‌دهد. وقایع شناسایی مقدماتی تلاشی جهت بدست آوردن اطلاعات درباره سیستم‌ها می‌باشد. این وقایع به خودی خود به سیستم نفوذ نمی‌کنند. برخی سیستم‌های تجاری IDS بگونه‌ای پیکره‌بندی می‌شود که برای وقایع شناسایی مقدماتی، اولویت بالایی قائل شود. با توجه به اینکه این وقایع مکانیزمی جهت نفوذ به سیستم‌ها ندارد لذا اولویت بالا دادن به آن مناسب به نظر نمی‌رسد. البته باید به این نکته توجه داشت احتمال دارد ترافیک این گونه

[1] Port Scans

وقایع از یک سیستم نفوذ یافته آمده باشد و هرگونه اطلاعات در این مورد باید با مدیریت سیستم در میان گذاشته شود.

اسکن مخفی. در اسکن مخفی تلاش می‌شود سیستم‌های موجود روی شبکه شناسایی شوند بطوریکه سیستم مبدا شناسایی نشود. این نوع اسکن روی سنسورهای N-IDS بصورت IP Half Scan یا IP Stealth Scan پدیدار می‌شود. واکنش در برابر این نوع اسکن، شناسایی مبدا انجام دهنده و مطلع کردن مالک سیستم مبدا است که احتمالاً مورد نفوذ قرار گرفته است.

اسکن پورت. اسکن پورت سرویس‌هایی که توسط سیستم روی شبکه ارائه شده است را شناسایی می‌کند. اگر در طی دوره‌ای کوتاه، تعداد خاصی از پورت‌ها (حد آستانه) روی یک سیستم باز شوند سیستم IDS عمل اسکن پورت را شناسایی می‌کند. سنسورهای N-IDS و بعضی از سنسورهای H-IDS نیز به همین ترتیب اسکن پورت را شناسایی و آن را گزارش می‌کنند. واکنش مناسب در برابر این نوع اسکن همان واکنشی است که در برابر اسکن مخفی انجام می‌شود.

اسکن Trojan. برنامه‌های Trojan زیادی وجود دارد و سنسور N-IDS با نشانه‌هایی که دارد، آنها را شناسایی می‌کند. متاسفانه ترافیک روان به سوی برنامه Trojan با آدرس مقصد بسته شناسایی می‌شود و این مطلب باعث بروز خطاهای زیادی می‌شود. در مورد واقعه، پورت مبدا ترافیک را بررسی نمایید. به عنوان مثال ترافیکی که مبدا آن پورت ۸۰ است احتمالا ترافیک برگشت از این وب سایت است.

عمومی‌ترین نوع اسکن Trojan برای Back Orifice رخ می‌دهد. Back Orifice از پورت ۳۱۳۳۷ استفاده می‌کند و یک مهاجم اغلب محدوده‌ای از آدرس‌ها را برای این پورت اسکن می‌کند. کنسول Back Orifice هم دارای تابع Ping Host است که این کار را بصورت خودکار انجام می‌دهد. برای این مطلب نگرانی وجود ندارد مگر اینکه از طرف یک سیستم داخلی ترافیکی دیده شود. در اینجا هم واکنش مناسب آن است که با مالک سیستم مبدا که احتمالاً مورد نفوذ قرار گرفته است تماس گرفته شود.

اسکن آسیب‌پذیری‌ها. اسکن آسیب‌پذیری بصورت نشانه‌های زیاد و متفاوت حمله روی N-IDS ظاهر خواهد شد. عموماً این نوع اسکن روی چند سیستمی که موجود هستند به عنوان هدف انجام می‌شود. اسکن آسیب‌پذیری فقط سیستم‌های موجود و فعال را هدف می‌گیرد.

اسکن آسیب‌پذیری که توسط هکر انجام می‌شود را نمی‌توان از اسکن آسیب‌پذیری که توسط شرکت امنیتی اجرا می‌شود تفکیک کرد. در هر حال اسکن به خودی خود نمی‌تواند به سیستم نفوذ کند اما پس از آنکه هکر این نوع اسکن را اجرا کرد و سیستم‌های آسیب‌پذیر را شناسایی کرد، اقدام به حمله می‌کند. در واکنش به اسکن آسیب‌پذیری باید با سیستم مبدا تماس گرفته شود و سیستم‌های داخلی از نظر به روز بودن Patchها کنترل شوند.

فضولی در محتوای فایل. فضولی در فایل یا آزمایش دسترسی به فایل، اغلب توسط کاربر داخلی انجام می‌شود. کاربر مذکور سعی می‌کند بفهمد به کدام فایل‌ها می‌تواند دست پیدا کند و محتوای آنها چیست؟ این نوع شناسایی فقط توسط سنسور H-IDS آشکار می‌شود. البته اگر تلاش‌های غیرمجاز برای دسترسی ثبت شده باشد، شناسایی آن امکان‌پذیر می‌شود. وقایعی که فقط یکبار اتفاق می‌افتند ناشی از اشتباهات سهوی است اما اگر نقشه‌ای از جانب یک کاربر دیده شد باید با او تماس گرفته شود تا معلوم شود چه کار می‌کند.

حملات

وقایع تهاجمی وقایعی هستند که باید به سرعت در برابر آنها عکس‌العمل نشان داده شود. اگر از یک آسیب‌پذیری شناخته شده داخلی سوء استفاده شود IDS برای شناسایی وقایع با اولویت بالا پیکره‌بندی می‌شود. در این حالت لازم است پروسه واکنش در برابر حادثه بلافاصله به اجرا درآید.

به خاطر داشته باشید IDS تفاوتی بین حمله واقعی و اسکن آسیب‌پذیری که شبیه حمله به نظر می‌رسد قائل نمی‌شود. مدیر باید برای تشخیص واقعی بودن حمله، اطلاعاتی را که توسط IDS ارائه می‌شود مورد بررسی قرار دهد. اولین چیزی که به نظر می‌رسد تعداد وقایع است. مشاهده تعدادی از نشانه‌های حمله روی یک سیستم و در طی دوره زمانی کوتاه دلالت بر انجام اسکن آسیب‌پذیری (و نه حمله واقعی) دارد. کشف نشانه یک حمله روی یک یا چند سیستم دلالت بر حمله واقعی دارد.

وقایع مشکوک و غیرموجه[1]

وقایعی که جزء دسته‌بندی‌های قبلی قرار نگیرند به عنوان وقایع مشکوک تلقی می‌شود. تعریف ساده واقعه مشکوک، واقعه‌ای است که فهمیده نشود. به عنوان مثال فرض کنید در سرور ویندوز NT کلید Registry بدون دلیل واضحی عوض شود. در این حال علائمی از تهاجم ظاهر نشده است و نشانه‌ای هم درباره علت تغییر وجود ندارد. مثال دیگری از این دست بسته‌ای است که پرچم‌های هکر آن با پروتکل‌های استاندارد مغایرت دارد. آیا این مسئله یک واقعه شناسایی مقدماتی است؟ یا به خاطر استفاده از کارت شبکه بد یا بروز خطا در محتوای بسته به هنگام انتقال به وجود آمده است؟ IDS نمی‌تواد برای پاسخگویی به این سوالات اطلاعات کافی ارائه نماید و تهاجمی بودن این واقعه را تشخیص دهد. ترافیک غیرمنتظره‌ای که روی شبکه داخلی ظاهر می‌شود هم از نوع وقایع مشکوک است. به عنوان مثال اگر کامپیوتر رومیزی شروع به درخواست اطلاعات SNMP از سیستم‌های دیگر نماید. این کار یک تهاجم است یا از پیکره‌بندی بد سیستم ناشی شده است؟ وقایع مشکوک را تا آنجایی که منابع اجازه می‌دهد باید مورد بررسی قرار داد.

۳-۱-۸-۲- بررسی وقایع مشکوک

وقتی فعالیت مشکوکی اتفاق می‌افتد باید چهار مرحله انجام شود تا معلوم شود آن فعالیت تلاشی واقعی برای ورود غیرمجاز بوده است یا اقدامی بی‌خطر. این مراحل عبارتند از:

- شناسایی سیستم
- ثبت ترافیک بیشتر بین مبدا و مقصد
- ثبت کل ترافیکی که از مبدا می‌آید
- ثبت محتوای بسته‌هایی که از مبدا می‌آید

پس از انجام هر مرحله تعیین می‌شود آیا مدارک کافی برای شناسایی آن فعالیت به عنوان یک تهاجم پیدا شده است یا نه. به هنگام بررسی واقعه این نکته را به خاطر بسپارید که اگر واقعه‌ای یکبار رخ دهد وتکرار نشود، یادگیری اطلاعات بیشتر درباره آن بسیار مشکل است. بررسی کامل خلافهایی که فقط یکبار می‌افتد اغلب غیرممکن است.

---

1 Suspicious Events

شناسایی سیستم

اولین اقدام در بررسی فعالیت مشکوک، شناسایی سیستم‌هایی است که در آن فعالیت نقش دارند. یکی از راه‌های شناسایی، تبدیل آدرس IP به Host Name است اما در برخی موارد نمی‌توان Host Name را پیدا کرد. (ممکن است سیستم کلاینت DHCP باشد یا سرور دوردست DNS در حال حاضر فعال نباشد و ...) اگر در پیدا کردن DNS با مشکل موجه شدید جستجو را از راه‌های دیگری دنبال کنید از جمله می‌توانید از سایت American Registry of Internet Number با آدرس http://www.arin.net و یا از سایت http://www.networksolution.com و یا از دایرکتوری‌های دیگر اینترنت کمک بگیرید. ناتوانی در شناسایی مبدا یا مقصد فعالیت مشکوک را نمی‌توان مدرکی دال بر واقعی بودن حمله تلقی کرد. به طور مشابه موفقیت در شناسایی را نیز نمی‌توان به عنوان مدرکی دال بر بی‌خطر بودن فعالیت مشکوک تلقی کرد.

لازم به ذکر است مبدا ترافیک مشکوک لزوما مبدا اصلی تهاجم نیست. معمولاً در تلاش‌هایی که برای جلوگیری از سرویس‌دهی (Dos) صورت می‌گیرد آدرس مبدا جعلی است. علاوه بر این امکان دارد تلاش‌هایی که برای دسترسی غیرمجاز صورت می‌گیرد از سیستم‌های دیگری بیاید که از قبل از آن توسط مهاجم مورد سوء استفاده قرار گرفته است.

ثبت ترافیک بیشتر بین مبدا و مقصد

با نگاه کردن به یک واقعه (از قبیل تخلف از پروتکل IP) نمی‌توان همه چیز را درباره ترافیکی که بین دو سیستم مبادله شده است فهمید. به عبارت دیگر فهمیدن زمینه فعالیت مشکوک، مهم است. علامت تهاجم Sendmail WIZ مثال خوبی از این دست است. از این علامت در شناسایی تلاشهایی که سعی در سوء استفاده از دستور WIZ در برنامه Send mail دارند استفاده می‌شود. این واقعه امنیتی هر موردی از عبارت "WIZ" را در پیام پست الکترونیک شناسایی می‌کند. اگر WIZ در بدنه پیام موجود باشد نمی‌توان به وضوح گفت تلاشی برای ورود غیرمجاز صورت گرفته است. فهمیدن محتوای واقعه در شناسایی خطا کمک می‌کند.

IDS را بگونه‌ای پیکره‌بندی کنید که به دنبال ترافیک بین مبدا فعالیت مشکوک و مقصد بگردد. مثالی از این نمونه در جدول (۳-۳) دیده می‌شود.

جدول ۳-۳: مثالی از پیکره‌بندی IDS برای ثبت کل ترافیک بین دو سیستم

نام واقعه	اقدام	IP مبدا	IP مقصد	پروتکل	پورت مبدا	پورت مقصد
SUS-ACT (فعالیت مشکوک)	اخطار واقعه نگاری	مبدا فعالیت مشکوک	مقصد فعالیت مشکوک	TCP، UDP و ICMP که بستگی به نوع فعالیت دیده شده دارد	هر چیز	هر چیز

اما این پیکره‌بندی به ما چه می‌گوید؟ اول آنکه ایده‌ای از اینکه چه ترافیک دیگری بین مبدا و مقصد وجود دارد به ما می‌دهد. اگر تنها ترافیک موجود بین دو سیستم، بسته WIZ باشد می‌تواند بیانگر تلاشی برای تخلف روی سیستم باشد. از طرف دیگر اگر مقدار زیادی ترافیک SNMP (پست الکترونیک) بین دو سیستم پیدا کنیم به احتمال زیاد باید به ترافیک قانونی پست الکترونیک نگاه کنیم.

ثبت کل ترافیکی که از مبدا می‌آید

فرض کنید اطلاعاتی که از ثبت کل ترافیک بین دو سیستم جمع‌آوی شده است برای تعیین مجاز یا غیرمجاز بودن فعالیت کافی نباشد. در این حال می‌توان ترافیک‌های دیگری که از مبدا گسیل می‌شود را جمع‌آوری نمود. به خاطر داشته باشید در بعضی موارد این کار محدودیت دارد. اگر مبدا فعالیت مشکوک روی شبکه‌ای دور دست واقع شده باشد تنها ترافیکی را که به سمت سایت خودمان می‌آید می‌توانیم مشاهده کنیم. اما اگر مبدا فعالیت مشکوک محلی باشد می‌توانیم تمام ترافیکی که از ماشین می‌آید را جمع‌آوری کرده و ایده بهتری از مقصود واقعی آن به دست آوریم.

برای اینکه جمع‌آوری کل ترافیکی که از مبدا می‌آید شروع شود آشکارساز را برای جمع‌آوری‌کل اطلاعات از مبدا مشکوک پیکره‌بندی کنید. مثالی از این پیکره‌بندی در جدول(۳-۴) دیده می‌شود.

جدول ۳-۴: مثالی از پیکره‌بندی IDS برای جمع‌آوری کلی ترافیکی که از آدرس مبدا گسیل می‌شود

نام واقعه	اقدام	IPمبدا	IP مقصد	پروتکل	پورت مبدا	پورت مقصد
SUS-ACT (فعالیت‌مشکوک)	اخطار واقعه نگاری	مبدا فعالیت مشکوک	مقصد فعالیت مشکوک	TCP، UDP و ICMP که بستگی به نوع فعالیت دیده شده دارد	هر چیز	هر چیز

احتمالاً این پیکره‌بندی باعث تولید اطلاعات می‌شود که در بررسی شما ارزشی ندارد. مادامیکه می‌توان اطلاعات را بصورت شی‌گرا[1] آزمایش و بررسی کرد. می‌توان این واقعه نگاری را استفاده کرد تا تصویر خوبی از تعامل بین مبدا و سایت شما ارائه کند. سعی کنید در مورد فعالیتی که مشاهده می‌کنید بفهمید آیا ترافیک وب است؟ آیا ترافیک پست الکترونیک است؟ آیا ترافیک از مبدا مشکوک سرچشمه می‌گیرد یا از سایت شما؟

در این نقطه از بررسی باید موارد زیر را بدانید:

- نام سیستم مبدا
- نوع و فراوانی ترافیک مبادله شده بین مبدا و مقصد
- نوع و فراوانی ترافیک مبادله شده بین مبدا و مقصد و هر سیستم موجود در سایت

این اطلاعات ایده خوبی درباره طبیعت ترافیک مشکوک به شما می‌دهد. اما امکان دارد نتوانید با استفاده از این مدارک تهاجمی بودن فعالیت را ثابت کنید.

ثبت محتوای بسته‌هایی که از مبدا می‌آید

آخرین مرحله رسیدگی و بررسی، ثبت محتوای بسته‌هایی است که از مبدا گسیل می‌شود. لازم به ذکر است این تکنیک فقط روی پروتکل‌هایی که بر پایه متن بنا شده‌اند مفید است. به عنوان مثال می‌توان پروتکل‌های Telnet، FTP، SMTP و HTTP را نام برد. اگر پروتکل مورد استفاده از نوع باینری و رمز شده باشد این تکنیک به هیچ‌وجه مفید نمی‌باشد. برای انجام اینکار IDS را مطابق جدول(۳-۵)پیکره‌بندی کنید.

با ثبت محتوای بسته‌ها می‌توانید سابقه کل session و دستوراتی که برای مقصد فرستاده شده است را جمع‌آوری نمایید. یکبار که مقداری دیتا جمع‌آوری کردید آنرا بررسی نمایید. آیا احتمال تهاجم در آن session وجود دارد یا به نظر قانونی می‌رسد؟ ترکیب این اطلاعات با آنچه از قبل جمع‌آوری کرده‌اید باید جوابتان را بدهد.اگر موفق نشدید از فردی ماهر در زمینه پروتکل تحت بررسی کمک بخواهید.

---

[1] Objectively

جدول ۳-۵: مثالی از پیکره‌بندی IDS برای جمع‌آوری محتوای بسته

نام واقعه	اقدام	IPمبدا	IP مقصد	پروتکل	پورت مبدا	پورت مقصد
SUS-ACT	اخطار،ثبت محتوای بسته	مبدا فعالیت مشکوک	مقصد فعالیت مشکوک	TCPیا UDP	هر چیز	پورتی که ترافیک مشکوک به آن می‌رود
SUS-ACT	اخطار،ثبت محتوای بسته	مقصد فعالیت مشکوک	مبدا فعالیت مشکوک	TCPیا UDP	پورتی که ترافیک مشکوک به آن می‌رود	هر چیز

۳-۲- بررسی نرم‌افزارهای متن باز

۳-۲-۱- بررسی نرم‌افزار Snort

برنامه Snort در سال ۱۹۹۸ توسط Martin Roesch نگارش شد. آقای Roesch در ابتدا قصد نگارش یک برنامه Sniffer با استفاده از امکانات کتابخانه pcap داشت. استفاده از امکانات کتابخانه pcap به منظور دریافت بسته‌های شبکه به جای دسترسی مستقیم به هسته سیستم‌عامل، امکان انتقال برنامه Snort را به سیستم‌عامل‌های متعدد دیگر می‌داد. در حال حاضر نرم‌افزار Snort معروفترین نرم‌افزار متن‌باز در زمینه IDS محسوب می‌شود و یک برنامه NIDS با لیسانس GPL است.

شکل ۳-۴: آرم نرم‌افزار Snort

با اوج گرفتن محبوبیت برنامه Snort، شرکت Sourcefire توسط آقای Martin Roesch در سال ۲۰۰۱ تاسیس شد و این شرکت در حال حاضر سرویس‌های تجاری برنامه Snort را به مشتریان خود ارائه می‌کند.

برنامه Snort برپایه الگوهای نفوذ عمل می‌کند و با تطبیق این الگوها با بسته‌های شبکه، سعی در تشخیص انواع نفوذ دارد که به تفصیل در ادامه توضیح داده شده است.

۳-۲-۱-۱- مدهای کاری برنامه Snort

برنامه Snort چهار مد کاری دارد که به‌طور تقریبی مستقل از یکدیگر عمل می‌کنند و می‌توان از این برنامه به منظورهای زیر استفاده کرد:

مد Sniffer. در این مد برنامه Snort، تمام بسته‌های شبکه را خوانده و به طرق مختلف در کنسول نمایش می‌دهد. از این مد هنگامی استفاده می‌شود که یک اپراتور یا برنامه دیگر به‌صورت Real Time بر خروجی‌ها نظارت داشته باشد.

مد Packet Logger. در این مد برنامه Snort، تمام بسته‌های شبکه را خوانده و در دیسک ذخیره می‌کند. این مد برای آنالیز Off Line بسته‌ها کاربرد دارد.

مد NIDS. در این مد که مهمترین و پیچیده‌ترین مد آن محسوب می‌شود، به‌عنوان یک برنامه IDS ترافیک شبکه را آنالیز کرده و بسته به تنظیمات برنامه، اخطارهای لازم را صادر می‌کند. هدف ما از بررسی برنامه Snort، بررسی عملکرد و امکانات برنامه در این مد کاری است.

مد Inline. در این مد برنامه Snort به جای استفاده از کتابخانه pcap از طریق برنامه IPTables (موجود در لینوکس) بسته‌ها را دریافت کرده و سبب می‌شود تا برنامه IPTables بسته‌های شبکه را پس از بررسی برنامه Snort، قبول یا رد کند. در این مد برنامه Snort به عنوان یک IDP برای یک کامپیوتر با سیستم‌عامل لینوکس عمل می‌کند.

۳-۲-۱-۲- الگوهای نفوذ

همانطور که گفته شد، برنامه Snort بر پایه مجموعه‌ای از قواعد و الگوهای تشخیص نفوذ که با فرمت خاصی نگارش می‌شود (Rule-Based Language) عمل می‌کند. این الگوها شامل الگوهایی از رفتار برنامه‌های نفوذگر، رفتار پروتکل‌ها و رفتار ترافیک نرمال و غیر نرمال یک شبکه است. قدرت برنامه Snort در تنوع الگوهای موجود در این برنامه است که استفاده کنندگان این برنامه و خود شرکت Sourcefire آنها را تولید می‌کنند. این الگوها قابل تعمیم، اصلاح و گسترش نیز هستند؛ به این معنی که سایرین نیز می‌توانند با آنالیز ترافیک و یا رفتار برنامه‌ها و پروتکل‌ها، قواعد جدید برای کشف نفوذ تولید کنند.

در حال حاضر شرکت Sourcefire الگوهای جدید و نوین را به محض تولید، فقط به مشتریان ثبت شده و تجاری خود می‌دهد و پس از گذشت مدتی زمان (ظاهرا در حال حاضر این زمان ۵ روز است.)، این الگوها را در اختیار سایر افراد نیز قرار می‌دهد. اهمیت الگوهای جدید برای مقابله با نفوذهای جدید است و مدت زمانی که شرکت Sourcefire برای در اختیار

قراردادن الگوهای جدید به عموم به تاخیر می‌اندازد بزرگترین اشکال برنامه Snort می‌باشد و اهرم شرکت Sourcefire برای کسب درآمد محسوب می‌شود.

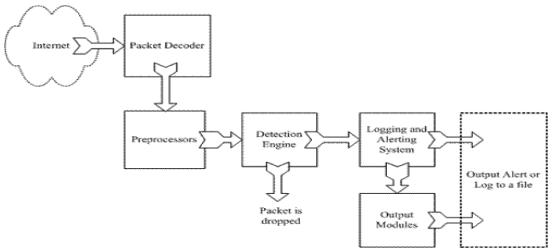
زبان یا طریقی که این الگوها نگارش می‌شوند مخصوص خود برنامه Snort است و یادگیری آن بسیار ساده است. سادگی نگارش این الگوها سبب می‌شود تا مدیران شبکه بتوانند به سادگی الگوهای بسیار کاربردی برای شبکه خود نگارش کنند. ساختار الگوهای Snort به گونه‌ای است که در لایه‌های Network و Protocol در مدل TCP/IP عمل می‌کنند، ولی روش‌هایی برای تعمیم این الگوها در لایه Data Link و Application نیز وجود دارد.

۳-۲-۱-۳- اجزا و طرز کار برنامه Snort

برنامه Snort از پنج جزء منطقی زیر تشکیل شده است:

- دریافت کننده بسته‌ها[1]
- پیش پردازش کننده[2]
- موتور آشکارساز[3]
- اخطار دهندگان و ثبت کنندگان[4]
- خروجی دهندگان[5]

در شکل (۳-۵) این اجزا به تفکیک آورده شده است:



شکل ۳-۵: اجزای برنامه Snort

[1] Packet Decoder
[2] Preprocessor
[3] Detector Engine
[4] Logging & Alerting
[5] Output Models

دریافت کننده بسته‌ها

دریافت کننده بسته‌ها، بسته‌های شبکه را از منابع مختلف مانند کارت شبکه، اتصال SLIP، اتصال PPP و غیره دریافت کرده و به لایه بالاتر خود ارسال می‌کند.

پیش پردازنده

پیش پردازنده بسته‌ها را از لایه ماقبل خود (دریافت کننده) دریافت کرده و عملیات پردازش اولیه لازم را قبل از تحویل به موتور آشکارساز اعمال می‌کند. بعضی از پیش پردازنده‌ها در همان پردازش اولیه قدرت تشخیص بسته‌های غیر طبیعی را دارند و می‌توانند اخطارهای لازم را تولید کنند. مهمترین وظیفه پیش پردازنده، آماده کردن و استاندارد کردن فرمت بسته و محتویات آن برای موتور آشکار ساز است.

موتور آشکارساز

موتور یا هسته آشکار ساز مهمترین جزء برنامه Snort است و با مقایسه بسته و اطلاعات آن با الگوهای موجود سعی در تشخیص بسته‌هایی می‌دهد که حاکی از علائم تلاش برای نفوذ در شبکه هستند. تطبیق دادن بسته‌ها با الگوهای موجود یکی از گلوگاه‌های زمانی برنامه Snort می‌باشد. در صورتیکه تعداد الگوهای تعریف شده یا تعداد بسته‌ها شبکه زیاد باشند، این عملیات ممکن است زمان‌گیر باشد و بار زیادی را بر دوش پردازنده وارد سازد به طوریکه برنامه Snort نتواند به‌صورت بلادرنگ[1] تمام بسته‌ها را کنترل کند و مجبور شود از کنترل بعضی از بسته‌ها صرفنظر کند که موجب گریز نفوذگر از الگوهای این برنامه خواهد شد.

میزان زمان صرف شده برای پردازش هر بسته به موارد زیر بستگی دارد:

- تعداد الگوهای قابل تطبیق.
- قدرت پردازنده ماشین (کامپیوتر) که برنامه Snort در آن اجرا می‌شود.
- سرعت درگاه ارتباطی داخلی[2].
- تعداد بسته‌های موجود در شبکه.

[1] Real Time
[2] Internal Bus

روش‌ها و ترفندهای فراوانی وجود دارد که با تنظیم صحیح برنامه Snort و با در نظر گرفتن طرح کلی شبکه و سرویس موجود در آن، می‌توان بار کاری را از دوش این قسمت از برنامه برداشت. برای مثال می‌توان فقط به محدوده آدرس IPهای کامپیوترهای Server نظارت کرد.

اخطار دهندگان و ثبت کنندگان

این بخش از برنامه Snort معطوف به ثبت وقایع و ارسال اخطارهای لازم است. بسته به تنظیمات برنامه Snort به‌صورت پیش فرض این اخطارها به‌صورت متنی در محل خاصی (/var/log/snort/ در سیستم‌های یونیکس) نگارش می‌شوند.

خروجی دهندگان

یکی از محاسن برنامه Snort تنوع روش‌ها و ماژول‌های خروجی این برنامه است. ماژول‌های خروجی دهنده، اطلاعات و اخطارهای تولید شده را بسته به تنظیمات برنامه و تنظیمات این ماژول‌ها، می‌توانند به فرمت‌های گوناگون تبدیل سازند و در قالب‌های متنوع ذخیره کنند. در زیر نمونه‌ای از کارایی این ماژول‌ها آورده شده است:

- ثبت به‌صورت بسیار ساده در پوشه ای خاص
- ارسال به‌صورت پیام SNMP
- ارسال به Syslog استاندارد سیستم
- ثبت در بانک‌های اطلاعاتی مانند MySQL و PostgreSQL
- تولید فایل‌های XML
- تغییر تنظیمات Router و Firewall
- ارسال پیامهای SMP به ماشین‌های سیستم‌عامل ویندوز و ...

لیست خروجی‌های برنامه Snort محدود به موارد فوق نیست و در کنار ماژول‌های استاندارد برنامه Snort ابزارهایی برای ارسال email و مشاهده در مرورگر وب و غیره نیز وجود دارد که در ادامه به‌طور خلاصه گفته شده است.

۳-۲-۱-۴- ابزارها و برنامه‌های جانبی

از آنجا که برنامه Snort واسط کاربری خاصی ندارد و یک برنامه کاملا متن‌باز است، ابزارها و برنامه‌های جانبی متفاوتی به وجود آمده است که در کنار این برنامه استفاده می‌شوند.

نمونه‌ای از این ابزارها و برنامه‌ها، برنامه‌هایی هستند که از خروجی‌های برنامه Snort استفاده کرده و آنها را به روش‌های مختلف به کاربران عرضه می‌کنند. لیست زیر مجموعه‌ی کوچکی از ابزارهایی است که در کنار برنامه Snort می‌توان از آنها استفاده کرد.

برنامه Barnyard

برنامه Barnyard یکی از برنامه‌های معروف برای Snort است که در سایت اصلی برنامه Snort نیز قابل دریافت است. این برنامه به Snort این امکان را می‌دهد تا خروجی‌های خود را به‌صورت فایل‌های باینری به دیسک ذخیره کند و زمان را برای پارس کردن خروجی‌ها و تبدیل و آنها به فرمت‌های دیگر و یا ارسال آنها به سایر برنامه‌ها تلف نکند.

استفاده از برنامه Barnyard در کنار برنامه Snort سبب می‌شود تا بار پردازش خروجی‌ها از دوش برنامه Snort برداشته شود و برنامه Snort هیچ بسته شبکه‌ای را از دست ندهد. برنامه Barnyard مشابه برنامه Snort می‌تواند خروجی‌ها را قالب‌های گوناگون مانند فایل و ذخیره کردن در بانک اطلاعاتی تولید کند.

برنامه ACID

برنامه ACID[1] یکی از قدیمی‌ترین و محبوب ترین برنامه‌هایی است که در کنار برنامه Snort استفاده می‌شود. از آنجا که می‌توان برنامه Snort را تنظیم کرد تا خروجی‌های خود را در بانک‌های اطلاعاتی مانند MySQL و PostgreSQL ثبت کند، برنامه‌هایی مانند ACID وجود دارند که نقش کنسول و رابط کاربری را برای برنامه Snort بازی می‌کنند و اطلاعات ثبت شده در بانک‌های اطلاعاتی را در قالب وب به کمک زبان برنامه‌سازی PHP و ابزارهای ترسیم نمودار مانند PHPlot و JPGraph به کاربران نمایش قرار می‌دهند.

برنامه ACID طی سال‌های ۲۰۰۱ الی ۲۰۰۳ توسط Roman Danyliw نگارش شده و محصول یک پروژه به نام AIRCERT Project در مجموعه Cert.org (متعلق به Carnegie Mellon University) است.

---

1 Analysis Console for Intrusion Databases

برنامه BASE

برنامه BASE[1] همانند برنامه ACID یک کنسول برای برنامه Snort محسوب می‌شود و از کد برنامه ACID نیز در این برنامه استفاده شده است. این برنامه روش نصب بسیار ساده‌تری نسبت به ACID دارد و راهنماهای نصب به روز تری نسبت به برنامه ACID و سایر برنامه‌ها دارد.

در برنامه BASE مسائل امنیتی نیز لحاظ شده است و این برنامه امکانات تعریف کاربر و تعریف سطح دسترسی نمایش اخطارها و خروجی‌های Snort را نیز دارد. در حال حاضر طرفداران برنامه BASE در حال گسترش هستند و در خود سایت برنامه Snort نیز اشاره به برنامه BASE شده است.

۳-۲-۱-۵- جمع بندی برنامه Snort

اگرچه برنامه Snort یک NIDS قوی با تیم پشتیبانی بسیار اکتیو است، ولی همواره باید در نظر داشت که ایده‌های تجاری در پشت این برنامه وجود دارد و امکان استفاده کردن از آخرین الگوهای این برنامه فقط برای مشتریان خاص شرکت Sourcefire وجود دارد. این برنامه یک راه حل سریع برای راه‌اندازی NIDS با امکانات محدود و خاص خود در سازمان‌های مختلف محسوب می‌شود.

۳-۲-۲- بررسی برنامه Bro

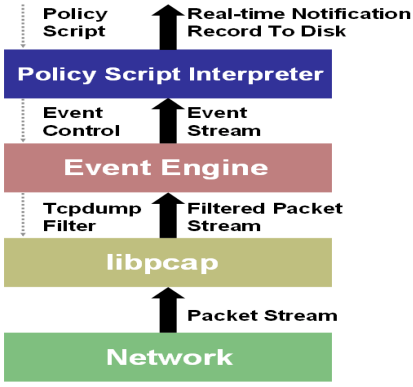
برنامه Bro یک NIDS بسیار قدیمی است که ظاهرا پروژه آن از حدود سال ۱۹۹۵ شروع شده و حتی امروزه نیز به خوبی از آن استفاده می‌شود. اگرچه امروزه حرکت و به‌روز رسانی چندانی در این پروژه به چشم نمی‌خورد ولی امکانات خاص این برنامه و بهینه بودن آن هنوز چشمگیر است. این برنامه توسط آقای Vern Paxson در Lawrence Berkeley National Lab و International Computer Science Institute نگارش شده است. این برنامه از سال ۱۹۹۶ در

1 Basic Analysis and Security Engine

LBNL همه روزه در حال کار بوده است و طبعا در طول این ۱۰ سال بهینه سازی‌های مختلفی داشته است. منطق برنامه Bro که به‌طور مفصل در ادامه توضیح داده شده است، بسیار پیچیده‌تر از برنامه‌های جدیدتر مانند Snort است، این برنامه بر اساس Policy Scripts که زبان ویژه‌ای نگارش می‌شود و الگوهای نفوذ (مانند Snort) عمل می‌کند و ترافیک شبکه را آنالیز کرده، اخطارهای لازم را تولید می‌کند. با تنظیمات مناسب، برنامه Bro توانایی اجرای برنامه‌های ثانویه را در صورت کشف نفوذ دارد. این برنامه‌های ثانویه می‌توانند وارد عمل شده و برای مثال جلوی نفوذ را بگیرند یا هشدارهای لازم را تولید کنند. همانطور که گفته شد، برنامه Bro بسیار بهینه طراحی شده و قدرت آنالیز ترافیک گیگا بیتی دارد. در زیر خصیصه‌های مهم و کلی نرم‌افزار Bro آورده شده است.

شکل ۳-۶: آرم برنامه Bro

- یک نرم‌افزار NIDS بسیار قدرتمند است.
- دارای زبان خاص خود برای نگارش برنامه‌های Policy Script برای آنالیز و تشخیص نفوذ است.
- از قبل دارای برنامه‌های Policy Script به منظورهای گوناگون و قابل استفاده دارد.
- دارای امکانات تشخیص الگوی نفوذ است.
- قدرت آنالیز ترافیک شبکه و پروتکل‌های آن را دارد و می‌تواند این اطلاعات را ذخیره سازد.
- قدرت اجرای برنامه‌های خارجی را در صورت کشف نفوذ دارد و همچنین می‌تواند نفوذهای کشف شده را ثبت کند.
- ابزار تبدیل الگوهای تشخیص نفوذ در برنامه Snort را به الگوهای خود دارد.



شکل۳-۷: طرز کار برنامه Bro

۳-۲-۲-۱- اجزا و طرز کار برنامه Bro

برنامه Bro در ابتدا بر اساس یک موتور رویداد (Event Engine) کار می‌کند که هر بسته شبکه را به محض دریافت به یک رویداد (Event) تبدیل می‌کند. این رویدادها به لحاظ تکنیکی و منطقی در سطوح مختلفی هستند، برای مثال بعضی رویدادها، از نظر تکنیکی بسیار ساده و سطح پایین هستند، مانند دیده شدن یک نمونه تلاش برای برقراری ارتباط در شبکه؛ بعضی رویدادهای دیگر مربوط به پروتکل‌ها هستند، مانند درخواست برای برقراری ارتباط در پروتکل FTP و پاسخ‌های مربوط به آن؛ بعضی رویدادهای دیگر به لحاظ تکنیکی و منطقی بسیار سطح بالا هستند، مانند رویداد ورود موفق یک کاربر به یک سیستم.

پس از وقوع یک رویداد، این رویداد به یک مفسر داخلی مرسوم به Policy Script Interpreter وارد می‌شود. بخش مفسر به توجه به نوع رویداد، قسمت یا قسمت‌های مناسب از برنامه داخلی خود به نام Policy Script را اجرا می‌کند. برنامه Policy Script همان هسته اصلی برنامه Bro برای کشف نفوذها است که به زبان مخصوصی مشابه زبان‌های برنامه سازی نگارش می‌شود و قسمت‌های مختلف آن بر اساس رویدادهای خاص اجرا می‌شوند.

۳-۲-۲-۲- رابط کاربری برنامه Bro

برنامه Bro هیچ رابط کاربری به خودی خود ندارد و ابزارهای ثالث چندانی هم از آن حمایت نمی‌کنند. تنها رابط کاربری که می‌توان از آن برای برنامه Bro یاد کرد برنامه Brooery

است. این برنامه مدت‌هاست که به روز نشده و علت اصلی آن نبودن تیم پشتیبان برای این برنامه است. برنامه Brooery به زبان Perl نگارش شده و تحت وب اجرا می‌شود. این برنامه لیسانس BSD دارد و مشابه برنامه Bro دارای منطق پیچیده‌ای است. اگرچه استفاده از این برنامه توصیه نمی‌شود ولی آخرین نسخه این برنامه از سایت http://www.cl.cam.ac.uk/~cpk25/brooery قابل دریافت است و متاسفانه هیچ راهنمایی حتی در بسته اصلی آن برای طریقه نصب وجود ندارد

شکل ۳-۸: رابط کاری برنامه Bro

۳-۲-۲-۳- جمع بندی برنامه Bro

امروزه متاسفانه نرم‌افزار Bro هرچند که به لحاظ عملیاتی هم رده یا حتی بالاتر از برنامه Snort و سایر برنامه‌های نوین دیگر به نظر می‌رسد ولی به علت ضعف در مستند سازی، عدم وجود پشتیبانی فنی/تجاری مناسب، وجود نکات و ابهامات فنی در بدنه برنامه و به‌روز نشدن سیستم و وب سایت، این برنامه آنچنان مورد استقبال عمومی قرار نگرفته است و تنها در محیط‌های ویژه عملیاتی مانند خود سازمان LBNL و معدودی سازمان‌های بزرگ دیگر کاربرد دارد.

این برنامه در محیط‌های تحقیقاتی یا سازمان‌های دولتی ویژه که مجهز به نیروهای فنی هستند و امنیت یک پارامتر بسیار مهم است، ارزشمند است. با توجه به اینکه این برنامه تمام آمار اطلاعاتی ترافیک شبکه را ذخیره می‌کند، می‌توان به سادگی ترافیک نرمال و غیر نرمال را در یک سیستم تشخیص داد و حتی رخ دادن اتفاقات و حادثه‌های نوین مانند به‌وجود آمدن نفوذها و ویروس‌های جدید را کشف کرد.

از محاسن دیگر این برنامه لیسانس مشابه BSD این برنامه است که می‌تواند پایه پروژه‌های تجاری متن‌بسته دیگر قرار گیرد.

۳-۲-۳- بررسی برنامه Prelude

پروژه Prelude از حدود سال ۱۹۹۸ شروع شده و یک Hybrid IDS است. منظور از Hybrid IDS یک IDS مرکزی و متمرکز است که اطلاعات آن از چندین سنسور یا IDS متفاوت (چندین NIDS و یا HIDS) به‌دست می‌آید. سنسورها و برنامه‌های IDS متفاوتی که در نقاط مختلف یک سیستم توزیع شده قرار دارند، اطلاعات و نفوذهای کشف شده را برای هسته مرکزی ارسال می‌کنند و هسته مرکزی قابلیت تصمیم گیری و گزارش گیری‌های متنوع را دارد. برای نمونه برنامه Prelude می‌تواند در کنار استفاده از سنسورهای داخلی خود، از برنامه Snort در قالب یک سنسور NIDS، اطلاعات و هشدارهای لازم را دریافت کند. در حالت فوق می‌توان از برنامه Snort در نقش یک سنسور قدرتمند برای Prelude استفاده کرد.

شکل ۳-۹: آرم برنامه Prelude

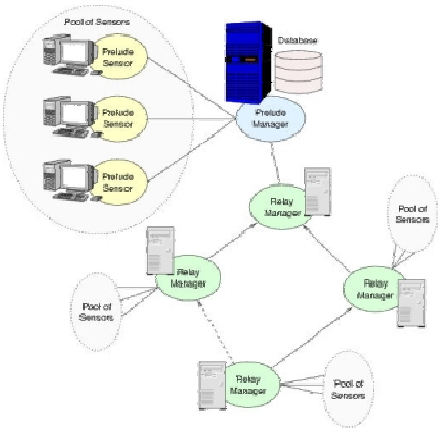
برنامه Prelude از متد IDMEF[1] که از استانداردهای نوین IETF است برای جمع آوری و تجمیع اطلاعات استفاده می‌کند. اگرچه در حال حاضر نسخه نهایی این استاندارد هنوز نگارش نشده، ولی نسخه پیش نویس این استاندارد قابل استناد است و ملاک کار بسیاری از برنامه‌های متن‌باز و تجاری محسوب می‌شود. در استاندارد IDMEF اطلاعات مربوط به کشف نفوذ در قالب گزارشات با فرمت XML در برنامه‌ها و سنسورهای IDS تولید می‌شوند و به یک هسته مرکزی یا سایر برنامه‌های IDS دیگر ارسال می‌شوند. نوع فرمت این گزارشات، قالب کلی فایل XML و اطلاعات درون آن و نحوه تبادل اطلاعات به طور کلی در این استاندارد IETF عنوان شده است.

1 Intrusion Detection Message Exchange Format

۳-۲-۳-۱- اجزا و طرز کار برنامه Prelude

برنامه Prelude از پنج بخش منطقی تشکیل شده است که به تفکیک در زیر آورده شده اند.

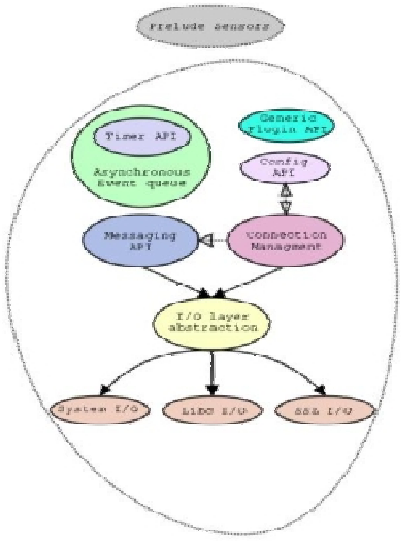
- کتابخانه LibPrelude . این کتابخانه قدرت ارتباط اجزای Prelude را با فرمت استاندارد IDMEF فراهم می‌کند. از این کتابخانه می‌توان استفاده کرد و سنسورهای جدید برای Prelude تولید کرد.
- سنسورها (Sensors). سنسورها در نقاط استراتژیک نصب می‌شوند و قدرت تشخیص نفوذ را دارند. این سنسورها، نفوذهای کشف شده را برای هسته مرکزی ارسال می‌کنند.
- مدیران (Managers). مدیران اطلاعات سنسورها را ارسال و پردازش می‌کنند. مدیران می‌توانند این اطلاعات را برای مدیران دیگر یا سیستم مدیریت مرکزی منتقل کنند.
- پاسخ دهندگان (Counter Measure Agents). پاسخ دهندگان اطلاعات را از مدیران دریافت و پاسخ مناسب می‌دهند. این پاسخ ممکن است برای متوقف کردن نفوذ و غیره باشد.
- رابط کاربری مرکزی (Frontend). رابط مرکزی برای نمایش اطلاعات و دریافت گزارشات می‌باشد. این رابط اطلاعات را در قالب فرمت‌های منطقی و قابل درک ذخیره می‌کند.



شکل۳-۱۰: طرز کار برنامه Prelude

کتابخانه Prelude library

این کتابخانه برای سهولت نگارش سنسورها با امکانات متنوع و با یک واسط کتابخانه‌ای استاندارد (API) طراحی شده است. این کتابخانه در سنسورهای Prelude استفاده می‌شود و امکان ارتباطات استاندارد با فرمت IDMEF برای این اجزا به‌وجود می‌آورد. کارایی و نقش کلی این کتابخانه به شرح زیر است:



شکل ۳-۱۱: کتابخانه Prelude

ارتباط منطقی سنسور با مدیر[1] مربوطه: توسط این کتابخانه سنسورها می‌توانند با مدیر مربوط به خود ارتباط بر قرار سازند. اگر برای یک سنسور ارتباط با مدیر مربوطه ممکن نباشد، سنسور می‌تواند بنا به تنظیمات با مدیران دیگری ارتباط برقرار کند و اگر هیچ مدیری در دسترس نباشد، هشدارها در قالب فایل‌ها به‌صورت محلی ذخیره می‌شوند تا از بین نروند و بعدا به مدیران ارسال شوند.

[1] Manager

ارتباط نا محسوس[1]: در صورتیکه یک ارتباط بین مدیر و کتابخانه بر قرار باشد، این کتابخانه می‌تواند بنا به انتخاب خود اطلاعات را به‌صورت رمز با استاندارد SSL و یا فرمت متنی ساده ، برای مدیر ارسال کند.

صف رویدادهای عمومی غیر همزمان[2]: این کتابخانه قدرت ارسال غیر همزمان رویدادها (نفوذهای کشف شده) را به سنسورها می‌دهد. به این ترتیب یک سنسور می‌تواند درصورت بروز رویدادهای متوالی، رویدادهای اولویت دار را سریع تر از رویدادهای معمول ارسال کند.

تولید تایمرهای همزمان و غیر همزمان: این کتابخانه امکان تولید تایمرهای نرم‌افزاری همزمان و غیر همزمان را برای سهولت کار سنسورها قرار می‌دهد.

دریافت تنظیمات عمومی: این کتابخانه قابلیت عمومی دریافت و آنالیز پارامترهای خط فرمان را برای سهولت کار سنسورها فراهم می‌سازد.

رابط تولید Plug-in های ثالث: این کتابخانه امکانات استفاده از Plug-in های ثالث را با استفاده از کتابخانه libltd برای سنسورها فراهم می‌آورد.

سنسورهای Prelude

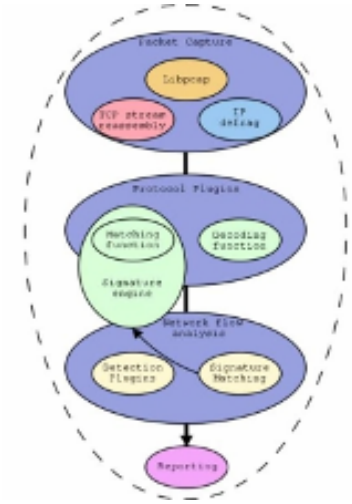
در حال حاظر برنامه Prelude دارای سه سنسور Prelude NIDS برای آنالیز ترافیک شبکه، Prelude LML برای آنالیز Log استاندارد سیستم و libsafe که ویژه سیستم‌عامل لینوکس است و برای جلوگیری از Buffer Overflow طراحی شده است. این سه سنسور به تفصیل در زیر توضیح داده شده‌اند.

سنسور Prelude NIDS . این سنسور مهمترین سنسور برنامه Prelude محسوب می‌شود و ترافیک شبکه را به‌صورت بلادرنگ آنالیز می‌کند. این سنسور با استفاده از یک نسخه تغییر یافته کتابخانه pcap عمل می‌کند. این سنسور به محض دریافت یک بسته شبکه، ابتدا سر آیند IP بسته و سر آیند پروتکل آن را آنالیز می‌کند تا صحیح بودن اطلاعات آن بررسی شود و اجازه ندهد یک نفوذگر با ارسال بسته‌های خراب از روتین کنترل این برنامه در امان بماند. پس از کنترل صحت اطلاعات، توسط plug-inهای مختلف این برنامه، اطلاعات داخلی بسته بررسی، تغییر و کنترل می‌شود که لیست این plug-inها در ادامه آورده شده است.

---

[1] Transparent Communication Layer
[2] Asynchronous Generic Event Queue

- نرمال کردن اطلاعات بسته: در این پردازش، اطلاعات داخلی بسته در صورت لـزوم نرمال می‌شود تا plug-inهای بعدی بتوانند به درسـتی عمـل کننـد و اگـر بسـته معیوب شناخته شود، اخطارهای لازم صادر می‌شود. نرمال سـازی بـه صـورت زیـر انجام می‌گیرد:
- درخواست‌های HTTP بـرای نرمـال شـدن براسـاس اسـتاندارد پروتکـل Decode می‌شوند و کارکترهای یونیکد تبدیل و بررسی می‌شوند.
- در درخواست‌های FTP و Telnet کارکترهای ویژه Decode می‌شوند.
- رمز شکافی سرآیند درخواست‌های RPC انجام شده و کنترل می‌شود.
- با مشخص شدن پروتکل بسته، plug-in های مربوط به پروتکل شروع بـه فعالیـت کرده و در صورت لزوم اخطار می‌دهند.
- بخش Plug-in ویژه برنامه Snort بـا اسـتفاده از الگوهـای Snort بسـته را کنتـرل می‌کند.



شکل ۳-۱۲: سنسور NIDSدر Prelude

- بخش Plug-in ویژه آشکار سازی Scan، بسته را بـا توجـه بـه بسـته‌هـای ماقبـل کنترل می‌کند.

- بخش Polymorphic Shell Code Detection در محتویات بسته به دنبال حد خاصی از دستورات خاص میکرو کنترلی CPU مانند NOP می‌گردد تا امکان به وجود آوردن Buffer Overflow را توسط نفوذگر در برنامه‌ها بررسی کند.
- بخش Plug-in مربوط به ARPSpoof به دنبال سر آیندهای معیوب در بسته گشته و در صورت معیوب بودن بسته اخطار می‌دهد.
- بخش IP Defragmentation Stack بسته‌ها را با توجه به MTU بسته و شکسته شدن بسته‌ها در چندین بسته کنترل می‌کند تا نفوذگر نتواند با استفاده از الگوریتم‌های مختلف، بسته‌های آلوده ارسال کند.
- بخش TCP stream Reassembly برای مقابله با Stateless Attacks طراحی شده و قدرت دوباره سوار کردن دنباله‌های بسته‌ها (TCP Stream) را دارد.
- بخش Evasion Trials, with Fragroute برای کنترل صحیح بودن دنباله بسته‌ها می‌باشد و امکان ارسال دنباله بسته‌ها به‌صورت غیره مجاز را کنترل می‌کند.

سنسور Prelude LML. سنسور LML[1] برای فراهم کردن بخشی از ویژگی‌های HIDS طراحی شده است و دو مد کاری مختلف دارد. در مد کاری اول، این سنسور مشابه Syslogd به عنوان یک سرور عمل می‌کند و پیام‌های Sys Log را از کامپیوترها و سایر دستگاه‌هایی که امکان تولید Sys Log دارند را دریافت کرده و آنالیز می‌کند.

نمونه‌ای از دستگاه‌هایی که امکان تولید Sys Log دارند در لیست زیر آورده شده است:

- تمام سیستم‌عامل‌های یونیکس و متشابهات آن مانند Linux و FreeBSD
- اغلب Switchها و Routerها
- اغلب Firewallها
- اغلب Printerها
- سیستم‌عامل‌های Windows با ابزارهای جانبی مانند NTSysLog و غیره.

برای استفاده از این مد سایر ماشین‌ها می‌باید تنظیم شوند تا پیام‌ها را به سرور LML ارسال کرده و این سرور پیام‌های Syslog را دریافت کرده و آنالیز کنند.

---

1 Log Monitoring Lackey

شکل ۳-۱۳: سنسور LML در Prelude

در مد کاری دوم LML توانایی آنالیز فایل Syslog را دارد و به عنوان یک سرور برای دریافت این Syslogها عمل نمی‌کند می‌توان از خود Syslogd و ابزارهای مشابه برای دریافت پیام‌های Syslog در ماشین‌های مختلف استفاده کرد.

سنسور LML پس از دریافت Syslog چه به‌صورت سرور و چه به‌صورت آنالیز فایل‌ها، plug-inهای خاصی دارد که می‌تواند انواع Logها را تشخیص دهد. برای مثال یک Plug-in به نام Simple وجود دارد که با استفاده از امکانات PCRE و Regular Expressions پیام‌های SysLog را آنالیز کرده و اخطارهای لازم را تولید می‌کند. در حال حاضر این Plug-in الگوهای زیر را تشخیص می‌دهد:

IpFW
NetFilter
IpChains
CheckPoint
Nokia Appliance
NtSysLogd
GRSecurity
Exim
PortSentry
Proftpd
Qpopper
Squid
Secure Shell Daemon (sshd)

Vigor
vpopmail
Unix Log

سنسور LibSafe این سنسور متفاوت از سنسورهای قبلی است. این کتابخانه توسط تیم Prelude نگارش نشده و تنها در سیستم‌عامل Linux قابل استفاده است. سنسور LibSafe در اصل یک کتابخانه خارجی است و می‌باید از طریق تنظیمات LD در لینوکس، قبل از اجرای برنامه‌ها Load شود. این کتابخانه قدرت تشخیص فراخوانی‌های برنامه‌ها به توابع نا امن مانند sprintf و strcpy را دارد و Buffer Over Flow را در صورت بروز در برنامه‌ها تشخیص می‌دهد. کتابخانه LibSafe می‌تواند برنامه اشکال دار یا پروسه Child یک برنامه را متوقف کند و در صورتیکه LibPrelude نیز در سیستم وجود داشته باشد، این کتابخانه مانند یک سنسور برای Prelude عمل کرده و اخطارهای لازم را تولید و ارسال می‌کند.

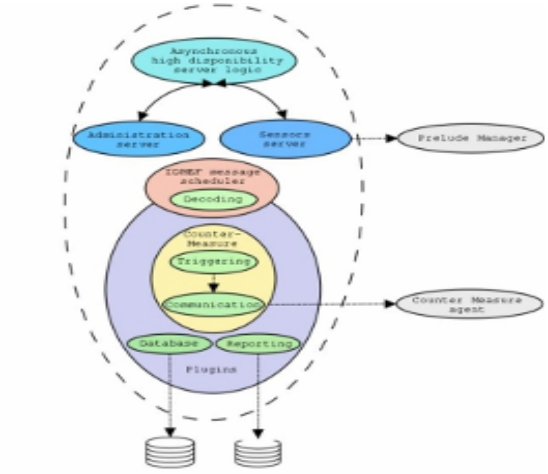
مدیرهای Prelude

مدیرهای Prelude برنامه‌هایی هستند که اطلاعات را از سنسورها دریافت می‌کنند و پس از آنالیزهای متفاوت و ثبت اطلاعات می‌توانند به پاسخ دهندگان اطلاع دهند تا پاسخ مناسب به نفوذ داده شود.

مدیرهای Prelude می‌توانند اطلاعات و نفوذهای کشف شده را به اشکال مختلف ذخیره کنند. اشکال متداول عبارتند از:

- ثبت در بانک اطلاعاتی MySQL
- ثبت در بانک اطلاعاتی PostgreSQL
- ثبت در بانک Oracle
- ثبت در قالب فایل‌های XML
- ثبت در قالب فایل‌های متنی

مدیرهای Prelude می‌توانند اطلاعات نفوذها و اخطارها را برای یکدیگر نیز ارسال کنند و با استفاده از مدیرهای Prelude می‌توان یک سیستم مدیریت مرکزی و متمرکز را به‌وجود آورد.



شکل ۳-۱۴: طرز کار مدیریت Prelude

رابط کاربری Prelude

برنامه Prelude دارای رابط کاربری تحت وب به نام PIWI می‌باشد. این رابط کاربری به زبان Perl نگارش شده و در بسیاری از وب سرورها قابل استفاده است. قابلیت‌های این رابط به شرح ذیل است:

- لیست اخطارهای امنیتی
- مرتب کردن اخطارها و نمایش آنها
- کنترل کیفیت اخطارهای ثبت شده
- دو گزارشات مبنی بر ۲۰ نفوذ مهم کشف شده و ۲۰ نفوذگر کشف شده
- امکان کنترل و استفاده از چندین بانک اطلاعاتی
- امکان کنترل دسترسی اپراتورها به رابط کاربری
- امکان ارائه آمارهای مختلف

۳-۲-۳-۲- جمع بندی برنامه Prelude

همانطور که گفته شد، برنامه Prelude در کنار ابزارهای لازم برای توزیع پذیری، دارای مجموعه‌ی کاملی از امکانات و ابزارهای NIDS و HIDS می‌باشد و همچنین می‌تواند از ابزارهای دیگر مانند Snort و برنامه‌های تجاری دیگر که اطلاعات را از طریق پروتکل IDMEF ارسال می‌کنند، استفاده کند. از ویژگی‌های خوب دیگر این برنامه قابلیت بسط ساده این برنامه

و نگارش سنسورهای جدید و مدیران جدید برای این برنامه است که همگی با پروتکل IDMEF با یکدیگر تبادل ارتباط می‌کنند.

توزیع پذیری Prelude و مدیریت جامع این برنامه بسیار قابل توجه است و می‌توان به خوبی از این برنامه در سازمان‌های بزرگ که امنیت نقش پررنگی دارد و کامپیوترهای سازمان توزیع شده و نا همگون است (مانند بانکها)، استفاده کرد.

۳-۲-۴- بررسی برنامه OSSEC

پروژه OSSEC از سال ۲۰۰۳ توسط Daniel Cid در کشور برزیل آغاز شده است و یک HIDS[1] قدرتمند با قابلیت‌ها و امکانات توزیع به کامپیوترهای مختلف و مدیریت مرکزی می‌باشد. این نرم‌افزار از سپتامبر ۲۰۰۶ توسط شرکت BRConnection[2] نیز حمایت می‌شود.

نرم‌افزار OSSEC در زمینه HIDS امکانات بسیار متنوعی دارد که لیست آن در زیر آورده شده است:

- آنالیز فایل‌های Log سیستم، Logهای مختلف دیگر مانند Web Server و غیره (log analysis).
- کنترل محتویات فایل‌های سیستمی و آگاه شدن از تغییر آنها (File Integrity Checking).
- کنترل هسته سیستم‌عامل و تشخیص نرم‌افزارهای Root Kit (Rootkit Detection).
- تولید اخطارها و پاسخ‌های لازم بر حسب بازه‌های زمانی .

این نرم‌افزار برای کنترل سلامت و کشف تلاشهای نفوذ در یک کامپیوتر و یا مجموعه‌ای از کامپیوترها طراحی شده است. این نرم‌افزار علی الخصوص هنگامی که تعداد کامپیوترهای زیاد شود و تنوع سیستم‌عامل‌ها به‌وجود آید، با پشتیبانی از تعداد قابل توجهی از انواع سیستم‌عامل‌ها بسیار مناسب است.

این نرم‌افزار متن‌باز حتی از سیستم‌عامل‌های تجاری مانند ویندوز نیز به خوبی پشتیبانی و حمایت می‌کند.

---

1 Host-based Intrusion Detection
2 www.brc.com.br

۳-۲-۴-۱- اجزاء و طرز کار OSSEC

نرم‌افزار OSSEC به‌طور منطقی از دو بخش Server و Agent تشکیل می‌شود. بخش Agent برای نظارت و تشخیص نفوذ است و در واقع سنسورهای برنامه OSSEC محسوب می‌شود. بخش Server برای دریافت پیام‌ها از Agentها و عملکرد و مدیریت مرکزی این نرم‌افزار است. نرم‌افزارهای Agent بر روی اکثر کامپیوترها و سیستم‌عامل‌ها منجمله سیستم‌عامل ویندوز، قابل نصب است و نرم‌افزار Server در عمده سیستم‌عامل‌های مبتنی بر یونیکس منجمله لینوکس و FreeBSD قابل نصب است. در زمانیکه هم Server و هم Agent در یک کامپیوتر باشد و هدف استفاده از این نرم‌افزار، فقط حفاظت یک کامپیوتر باشد، همچنان این نرم‌افزار قابل استفاده است و این مد برنامه به Local معروف است.

این نرم‌افزار همچنین قدرت آنالیز فایل‌های Snort را نیز دارد و چون قدرت پاسخ دهی به نفوذ کشف شده را دارد، می‌توان از Snort نیز در کنار این برنامه هم استفاده کرد.

با استفاده از برنامه متن‌باز nmap ، برنامه OSSEC قدرت اسکن یک شبکه یا مجموعه‌ای از کامپیوترها را برای تشخیص پورت‌های جدید باز شده را دارد. به این ترتیب اگر یک برنامه مخرب مانند ویروس یا یک نفوذگر بتواند در یک کامپیوتر نفوذ کرده و پورت‌های جدید به‌منظور نفوذهای جدید خارجی باز کند، برنامه OSSEC آن را تشخیص خواهد داد.

۳-۲-۵- معرفی سایر برنامه‌های HIDS

در حال حاضر برنامه‌های HIDS متن‌باز بسیار متنوعی وجود دارند که عمدتا با منطق کشف تغیرات در فایل‌ها عمل می‌کنند. در این بخش به مهمترین عناوین آنها اشاره شده است.

۳-۲-۵-۱- معرفی Tripwire

پروژه Tripwire یکی از قدیمی‌ترین برنامه HIDS است که با ساختن یک بانک اطلاعاتی از مشخصات فایل‌ها و با استفاده از الگوریتم‌هایMD5 و مشابه آن، توانایی کشف فایل‌های تغییر یافته را دارد. در حال حاضر نسخه‌های تجاری این برنامه توسط شرکت .Tripwire Inc به فروش می‌رسد و نسخه متن‌باز آن از اهمیت چندانی برخوردار نیست. متن برنامه رایگان Tripwire در سال ۲۰۰۰ توسط شرکت Tripwire ارائه شده و تحت لیسانس GPL است. نسخه رایگان این برنامه از سایت SourceForge.net قابل دریافت است.

۳-۲-۵-۲- معرفی AIDE[1]

پروژه AIDE یک HIDS قدیمی و ساده است که به عنوان یک جایگزین برای برنامه Tripwire طراحی شده است. این برنامه که به زبان برنامه‌سازی C نگارش شده است، قادر است مشابه برنامه Tripwire با ساختن یک بانک اطلاعاتی از مشخصات فایل‌ها، تغییرات به‌وجود آمده در فایل‌ها را کشف و گزارش کند. برنامه AIDE در سیستم‌عامل‌های متشابه با یونیکس و در ویندوز در محیط محدود Cygwin قابل‌استفاده است. این برنامه از الگوریتم‌های بسیار متنوعی برای کنترل تغییرات در فایل‌ها منجمله MD5، SHA1، RMD160 و غیره استفاده می‌کند و اضافه کردن الگوریتم‌های جدید به آن بسیار ساده است. این برنامه با لیسانس GPL توزیع می‌شود.

۳-۲-۵-۳- معرفی AFICK[2]

پروژه AFICK یک HIDS ساده برای کنترل تغییرات در فایل‌ها است که به زبان برنامه‌سازی Perl نگارش شده و تقریبا در تمام سیستم‌عامل‌ها منجمله لینوکس و ویندوز قابل استفاده است. این HIDS در سه بسته نرم‌افزاری شامل ۱- هسته برنامه ۲- محیط کاربری با Perl/TK ۳- رابط کاربری در برنامه Webmin توزیع می‌شود. سهولت استفاده و نصب این برنامه و امکان استفاده از این برنامه در Webmin سبب محبوبیت این برنامه شده است. خالق برنامه AFICK مدتها از AIDE استفاده می‌کرده است و برنامه AFICK را با هدف امکان انتقال آن به سایر سیستم‌عامل‌ها منجمله ویندوز نگارش کرده است.

۳-۳- نتایج

نرم‌افزارهای IDS بسیار متنوعی در حال حاضر به صورت متن‌باز وجود دارند که مهمترین‌ها و معروفترین‌های آنها در این گزارش بیان شده‌اند.

در زمینه NIDS، نرم‌افزارSnort از سایر برنامه‌ها معروفتر است و می‌توان در بسیاری از پروژه‌ها که هدف فقط راه‌اندازی یک NIDS است، از آن استفاده کرد. نرم‌افزار Snort پشتیبانی تجاری نیز دارد که از مزایای این نرم‌افزار است. نرم‌افزار Bro در محیط‌های تحقیقاتی و

1 Advanced Intrusion Detection Environment
2 Another File Integrity Checker

دانشگاه‌ها در صورتیکه که هدف تحقیقات، آنالیز، شناخت ترافیک و غیره باشد، با اهمیت است. این برنامه دارای لیسانس BSD است و می‌تواند مبنای پروژه‌های متن بسته نیز قرار گیرد.

در زمینه HIDS، نرم‌افزار OSSEC ،Tripwire و AIDE از سایر برنامه‌ها محبوب‌تر هستند، ولی برنامه OSSEC امکانات بسیار جامع‌تر و متنوع‌تری را نسبت به سایر برنامه‌ها در این زمینه ارائه می‌کند و پشتیبانی تجاری نیز دارد.

برنامه Prelude همانطور که گفته شد یک Hybrid IDS است و امکانات NIDS وHIDS را در یک محیط توزیع شده دارد. این برنامه در راهکارهای توزیع شده (Distributed) و علی‌الخصوص در زمانیکه سیستم‌عامل‌ها هم جنس نباشند و کامپیوترها در یک شبکه گسترده باشند بسیار کارا است. از برنامه Prelude می‌توان به عنوان یک NIDS یا HIDS منفرد نیز استفاده کرد که برای سازمان‌ها و شبکه‌های کوچک مفید است.

فصل چهارم– نرم‌افزار آنتی ویروس

آنتی‌ویروس‌ها[1] یکی از عناصر مهم در تامین امنیت و سلامت کامپیوترها و اطلاعات هستند که امروزه در تمام کاربردهای کامپیوترها به چشم می‌خورند. تمام کامپیوترهایی که به‌صورت فردی و یا در قالب یک شبکه، متصل به شبکه جهانی اینترنت می‌شوند، در معرض ابتلا به ویروس هستند. چون تعداد کامپیوترهای متصل به اینترنت هر روز افزایش می یابد، به اهمیت و کاربردهای نرم‌افزارهای آنتی‌ویروس نیز افزوده می‌شود. آنتی‌ویروس‌ها در تعریف، عبارتند از برنامه‌هایی که قدرت تشخیص و مقابله با برنامه‌های مخرب (ویروسها) را دارند. برنامه‌های مخربی که در عموم به ویروس معروفند، به لحاظ ساختاری و عملکرد به ویروسها، کرمها، Trojanها، میکروکدها و غیره تقسیم می‌شوند و یک آنتی‌ویروس می‌باید توان شناسایی و مقابله با تمام انواع این برنامه‌ها را داشته باشد. امروزه به وفور از آنتی ویروسی‌های تجاری در کاربردهای مختلف استفاده می‌شود و این برنامه‌ها در کامپیوترهای شخصی، ایستگاه‌های کاری، سرورها، سرویس دهندگان مختلف مانند پست الکترونیک و تقریبا همه جا یافت می‌شوند.

از آنجا که لیست ویروسها و برنامه‌های مخرب همه روزه افزایش می‌یابد، به‌روز بودن برنامه و بانک اطلاعاتی برنامه آنتی‌ویروس بسیار با اهمیت است و از آنجا که معمولا برنامه‌های متن‌باز دارای تیم‌های پشتیبانی تمام وقت نیستند، برنامه‌های آنتی‌ویروس متن‌باز چندانی وجود ندارند و یا بانکهای این برنامه‌ها آنچنان به روز نیستند و لذا اکثر آنتی ویروسهای متن‌باز قادر نیستند ویروسهای جدید را شناسایی کنند. در میان برنامه‌های متن‌باز آنتی‌ویروس، برنامه ClamAV دارای تیم پشتیبانی و به‌روز رسانی است. این برنامه به عنوان تنها برنامه آنتی‌ویروس قابل قبول متن‌باز بررسی شده و سپس برنامه‌های ثالثی که از آنتی ویروس ClamAV در کاربردهای مختلف استفاده می‌کنند، معرفی خواهندشد.

۴–۱– معرفی برنامه ClamAV

برنامه ClamAV یک ابزار برای شناسایی ویروس در یونیکس است که در اصل برای شناسایی ویروس در محتویات نامه‌های الکترونیکی و ضمائم آنها در سرورهای پست الکترونیک طراحی شده است. این برنامه دارای یک Daemon چند ریسمانی[2] و قابل تنظیم، ابزارهای

---

[1] Antivirus
[2] Multi Thread

پویش[1] مبنی بر خط فرمان[2] و ابزارهای پیچیده برای عملیات به‌روز رسانی است. این برنامه همچنین دارای یک کتابخانه اشتراکی[3] برای پویش فایل‌ها و شناسایی ویروس‌ها است.

۴-۱-۱- امکانات ClamAV

امکانات این برنامه به طور مختصر به شرح زیر است:

- دارای لیسانس GPL نسخه ۲.
- کد منبع مبنی بر استاندارد POSIX.
- سرعت بالا در پویش فایل‌ها.
- پشتیبانی از پویش فایل‌ها به محض دستیابی به فایل در سیستم‌های یونیکس و لینوکس.
- شناسایی بیش از ۷۰،۰۰۰ ویروس، Trojan، کرم‌ها و میکرو ویروس‌های Microsoft Office و MacOffice (نسخه 0.88.5).
- پشتیبانی از انواع متدهای فشرده سازی منجمله: Zip ، RAR ، TAR ، Gzip ، Bzip2 ، MS OLE2 ، MS Cabinet ، MS CHM ، MS SZDD..
- پشتیبانی از فایل‌های اجرایی فشرده شده با فرمت‌های UPX ، FSG ، Petite.
- امکانات قدرتمند شناسایی ویروس‌ها در نامه‌های الکترونیکی.
- امکان به‌روز رسانی بانک اطلاعاتی ویروس‌ها.

۴-۱-۲- سیستم عامل های پشتیبانی شده در ClamAV

همانطور که گفته شد، برنامه ClamAV با استاندارد POSIX نگارش شده و از این رو در تمام سیستم‌عامل‌هایی که از این استاندارد حمایت می‌کنند منجمله لینوکس و سیستم‌های متشابه با یونیکس قابل استفاده است. لیست سیستم‌عامل‌هایی که این برنامه از آنها پشتیبانی می‌کند به شرح ذیل است:

Gnu/Linux
Solaris
FreeBSD

---

[1] Scan
[2] Command Line
[3] Shared Library

OpenBSD
AIX 4.1/4.2/4.3/5.1
HPUX 11.0
SCO UNIX
IRIX 6.5
Mac OS X
BeOS
Cobalt MIPS
MS Windows + Cygwin
MS Windows + Windows Services for Unix 3.5 (Interix)

برنامه ClamAV دارای بسته‌های نصب خاص برای بعضی توزیع‌ها و سیستم‌عامل‌ها می‌باشد که به شرح ذیل است:

- توزیع Debian: در این توزیع، برنامه ClamAV به‌طور رسمی از نسخه Sarge حضور داشته است و توسط دستورات apt به سادگی قابل نصب است.
- توزیع RedHat – Fedora : در توزیع Fedora، این برنامه به طور رسمی در یک بسته RPM وجود دارد و به سادگی توسط دستور yum نصب می‌شود.
- توزیع Mandrake: در این توزیع، این برنامه به‌صورت رسمی و در قالب یک فایل RPM در سایت Mirror این توزیع، قابل نصب است.
- توزیع Slackware: بسته قابل نصب مربوط به این توزیع کننده از آدرس www.linuxpackages.net قابل دریافت است.
- توزیع SuSE: در این توزیع، برنامه ClamAV به طور رسمی وجود دارد و قابل نصب است.
- سیستم‌عامل FreeBSD: در این سیستم‌عامل در بخش برنامه‌های منتقل شده (Ports) برنامه ClamAV قابل نصب است.
- سیستم‌عامل OpenBSD: در نسخه ۳.۷ این سیستم‌عامل در بخش Ports وجود خواهد داشت.
- سیستم‌عامل NetBSD: در این سیستم‌عامل، نسخه رسمی این برنامه وجود دارد.
- سیستم‌عامل Solaris: بسته‌های قابل نصب این برنامه برای این سیستم‌عامل در آدرس http://www.citrus-it.co.uk/clamav وجود دارند.
- سیستم‌عامل AIX: بسته‌های قابل نصب در آدرس http://aixpdslib.seas.ucla.edu/packages/clamav.html وجود دارند.

- سیستم‌عامل Mac OS X: بسته‌های قابل نصب این برنامه برای این سیستم‌عامل در آدرس: http://www.markallan.co.uk/clamXav وجود دارد.
- سیستم‌عامل BeOS: نسخه قابل نصب این برنامه برای این سیستم‌عامل در آدرس http://www.bebits.com/app/3930 وجود دارد.
- سیستم‌عامل MS Windows – Cygwin : نسخه رسمی و قابل نصب وجود دارد.
- سیستم‌عامل MS Windows – Cygwin.dll : تمام نسخه‌های این برنامه در سیستم‌عامل Windows بر اساس امکانات Cygwin است.
- سیستم‌عامل MS Windows – Interix: نسخه قابل نصب در آدرس زیر وجود دارد. http://www.interopsystems.com/tools/warehouse.htm
- سیستم‌عامل MS Windows- Graphical Version: یک نسخه گرافیکی منفرد برای سیستم‌عامل ویندوز در آدرس ClamWin.com نیز موجود است.

۴-۲- اجزای برنامه ClamAV

همانطور که گفته شد، برنامه ClamAV دارای یک سرور Daemonچند ریسمانی و قابل تنظیم، ابزارهای پویش مبنی بر خط فرمان و ابزارهای پیچیده برای عملیات به‌روز رسانی است. این برنامه همچنین دارای یک کتابخانه برای پویش فایل‌ها و شناسایی ویروس است که این ابزارها در زیر به تفکیک تشریح شده‌اند.

۴-۲-۱- سرور ClamAV یا Clamd

سرور ClamAV با نام Clamd از کتابخانه LibClamAV برای شناسایی ویروس‌ها در فایل‌ها و دایرکتوری‌ها استفاده می‌کند و یک Daemon با متد برنامه‌سازی چند ریسمانی است. این Daemon امکان پاسخ دادن به درخواست‌های مبنی بر Unix Socket و TCP Socket را دارد و توسط فایل clamd.conf به صورت کلی قابل تنظیم است. برنامه Daemon دستورهای زیر را می‌پذیرد:

- دستور PING: این دستور برای کنترل وضعیت سرور استفاده می‌شود و Demon با PONG جوابگو خواهد بود.

- دستور VERSION: این دستور برای دریافت Version برنامه و بانک اطلاعات ویروس‌ها است.
- دستور RELOAD: برای بارگزاری مجدد بانک ویروس‌ها می‌باشد.
- دستور SHUTDOWN: برای متوقف کردن برنامه Daemon.
- دستور SCAN File/Directory: برای پویش فایل‌ها و دایرکتوری‌ها به‌صورت بازگشتی و با پشتیبانی از فشرده‌سازی فایل‌ها.
- دستور RAWSCAN File/Directory: برای پویش فایل‌ها و دایرکتوری‌ها به‌صورت بازگشتی و بدون پشتیبانی از فشرده‌سازی فایل‌ها.
- دستور CONTSCAN File/Directory: مشابه دستور SCAN ولی با کشف یک ویروس عملیات پویش متوقف نمی‌شود.
- دستور STREAM: با این دستور، سرور ClamAV یک پورت معرفی می‌کند که می‌باید اطلاعات به این پورت جهت پویش ارسال شوند.
- دستور SESSION,END: شروع/پایان یک ارتباط با Daemon.

۴-۲-۲- پویش فایل‌ها حین دستیابی با استفاده از Clamuko

در سیستم‌عامل‌های لینوکس و FreeBSD برنامه Clamd با استفاده از ماژول Dazuko (قابل دریافت از Dazuko.org) که برای هسته این سیستم‌عامل‌ها نگارش شده، قدرت پویش فایل‌ها را به محض دستیابی دارد. در این حالت یک ریسمان[1] خاص به نام Clamuko در Clamd به درخواست‌های این ماژول پاسخ می‌دهد. نام Clamuko با توجه به نام ماژول Dazuko انتخاب شده است. استفاده از این ماژول در سرورهای عملیاتی که زیر بار سنگین هستند، پیشنهاد نمی‌شود.

۴-۲-۳- پویش نامه‌ها در سرور پست الکترونیک با استفاده از Clamav-milter

برنامه ClamAV دارای یک بخش به نام Clamav-milter است که به زبان برنامه سازی C نگارش شده است و از کتابخانه LibClamAV یا سرور Clamd برای پویش نامه‌های الکترونیکی

[1] Thread

استفاده می‌کند. برنامه Clamav-milter برای برنامه Sendmail طراحی شده است و بسیار سریع و بهینه است. نصب این برنامه و تنظیم آن نیز با Sendmail بسیار ساده است.

۴-۲-۴- پویش فایل‌ها با استفاده از Clamscan

برنامه Clamscan برای پویش فایل‌ها و دایرکتوری‌ها به کار می‌رود. از این برنامه می‌توان برای شناسایی ویروس‌ها در فایل‌ها و دایرکتوری‌ها به صورت دستوری و غیر اتوماتیک استفاده کرد.

۴-۲-۵- پویش فایل‌ها با استفاده از Clamdscan

برنامه Clamdscan مشابه برنامه Clamscan برای پویش فایل‌ها و دایرکتوری‌ها به کار می‌رود با این تفاوت که این برنامه فقط از سرور Clamd برای شناسایی ویروس‌ها در فایل‌ها و دایرکتوری‌ها استفاده می‌کند و به ناچار از تنظیمات سرور پیروی می‌کند.

۴-۲-۶- به روز رسانی با استفاده از Freshclam

برنامه Freshclam یک برنامه مفصل و پیچیده برای به‌روز رسانی بانک اطلاعاتی ویروس‌ها است. این برنامه می‌تواند به صورت محاوره‌ای با کاربر یا به صورت یک Daemon در کامپیوتر عمل کند. این برنامه امکانات متنوع برای کنترل سلامت و صحت بانک اطلاعاتی ویروس‌ها دارد. این برنامه با استفاده از فایل freshclam.conf قابل تنظیم است.

برنامه Freshclam امکان تنظیم طریقه اتصال به اینترنت مانند تنظیم پروکسی سرورهای شبکه را دارد و به‌صورت اتوماتیک به نزدیک‌ترین سایت برنامه ClamAV متصل می‌شود.

۴-۲-۷- کتابخانه LibClamAV

کتابخانه LibClamAV کتابخانه‌ای با لیسانس GPL است که امکان پویش و شناسایی ویروس‌ها را به برنامه‌ها می‌دهد. این کتابخانه تمام ویژگی‌های برنامه ClamAV منجمله باز کردن فایل‌های فشرده و پویش نامه‌های الکترونیکی را در اختیار برنامه‌های ثالث قرار می‌دهد، البته به علت نوع لیسانس این کتابخانه، فقط برنامه‌های متن‌باز دیگر با لیسانس GPL می‌توانند از این کتابخانه استفاده کنند.

۴-۳- برنامه های ثالث مبتنی بر ClamAV

با توجه به ماهیت متن‌باز برنامه ClamAV و امکانات متنوع این برنامه، تعداد قابل توجهی از برنامه‌های متن‌باز دیگر از این برنامه به عنوان یک آنتی ویروس استفاده می‌کنند. این ابزارها و برنامه‌های ثالث، گستره کاربرد برنامه ClamAV را نسبت به یک آنتی‌ویروس ساده، بسیار افزایش می‌دهند و راهکارهای امنیتی جدیدی را به وجود می‌آورند. اگرچه شناخت کامل همه برنامه‌هایی که قدرت استفاده از برنامه ClamAV را دارند ضروری و عملی نیست، ولی آگاهی و شناخت نسبی از وجود این برنامه‌ها برای مدیران ارشد، طراحان سیستم و مشاوران امنیتی لازم است.

۴-۳-۱- برنامه های انتقال نامه های الکترونیکی (MTA)

پست الکترونیک در حال حاضر یکی از متداول‌ترین پروتکل‌های ارتباط است که توسط آن ویروس‌ها نیز می‌توانند خود را توزیع کنند. تعداد بسیار قابل توجهی از برنامه‌های متن‌باز که برای ارسال و دریافت نامه‌های الکترونیکی (MTA)[1] (برنامه‌های که مبتنی بر پروتکل SMTP هستند) استفاده می‌شوند ، قادرند به‌طور مستقیم یا به کمک ابزارهای ثالث از برنامه ClamAV به عنوان یک برنامه آنتی ویروس استفاده کنند و نامه‌ها را به محض دریافت پویش کرده و در صورت مبتلا بودن به ویروس آن را شناسایی و در صورت امکان ترمیم کنند. ابزارهای ثالث کمک کننده، معمولا بین برنامه دریافت کننده نامه (MTA) و برنامه آنتی ویروس قرار می‌گیرند و نامه‌های دریافت شده از طریق MTA را به برنامه آنتی ویروس می‌دهند تا پویش شوند. لیست مهمترین عناوین این ابزارها (شامل ۴۲ برنامه) به ترتیب الفبای لاتین در ادامه آورده شده است.

برنامه amavisd-new

برنامه amavisd-new[2] یک نسخه نوین از برنامه AMaViS است که برای پویش نامه‌ها و شناسایی ویروسها استفاده می‌شود.

---

1 Mail Transport Agents
2 http://www.ijs.si/software/amavisd

برنامه "AMaViS – "Next Generation

برنامه AMaViS[1] ، یکی از برنامه‌های بسیار معروف و قدیمی برای پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها است. برنامه AMaViS از آنتی ویروس‌های متنوع و MTAهای گسترده پشتیبانی می‌کند.

برنامه ClamdMail

برنامه Clamdmail یک برنامه جایگزین برای qmail-queue است که برای پویش نامه‌های الکترونیکی و شناسایی ویروسها ، حذف نامه‌های ناخواسته (spam) ، حذف نامه‌های موجود در لیست‌های سیاه و غیره است. این برنامه بسیار سریع عمل می‌کند و نصب آن ساده است.

برنامه Celement

برنامه Celement[2] یک برنامه دیواره آتش و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها برای MTAها است.

برنامه cgpav

برنامه cgpav[3] یک plug-in برای برنامه CommuniGate Pro است که به زبان برنامه‌سازی C نگارش شده است و برای پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها است.

برنامه ClamCour

برنامه ClamCour[4] یک برنامه فیلتر کردن و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها برای برنامه Courier است

برنامه clamfilter

برنامه clamfilter[1] یک برنامه کوچک، امن و کارا برای فیلتر کردن و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها در برنامه Postfix است.

---

1 http://amavis.sourceforge.net
2 http://www.clement.safe.ca/
3 http://program.farit.ru/
4 http://sourceforge.net/projects/clamcour/

برنامه ClamSMTP

برنامه ClamSMTP[2] یک برنامه فیلتر کردن و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها برای برنامه Postfix و سایر برنامه‌های MTA است.

برنامه clapf

برنامه clapf[3] برای حذف نامه‌های ناخواسته و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها برای برنامه Postfix است.

برنامه DSpamPD

برنامه DSpamPD[4] یک SMTP Proxy است که نامه‌ها را به برنامه DSPAM ارائه می‌کند تا نامه‌های ناخواسته حذف شوند. این برنامه امکان ارسال نامه‌ها را به برنامه ClamAV نیز دارد و برای پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها نیز استفاده می‌شود.

برنامه exiscan

برنامه exiscan[5] یک Patch برای برنامه Exim است که امکانات پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها ، حذف نامه‌های ناخواسته، حذف ضمائم ناخواسته بر حسب پسوند فایل و حذف نامه‌ها بر اساس دستورات regular expressions را به برنامه Exim اضافه می‌کند.

برنامه Gadoyanvirus

برنامه Gadoyanvirus[6] یک آنتی ویروس دیگر برای برنامه qmail است که برای پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها استفاده می‌شود.

---

1 http://www.ensita.net/products/clamfilter/
2 http://memberwebs.com/nielsen/software/clamsmtp/
3 http://dev.acts.hu/clapf/
4 http://caspian.dotconf.net/menu/Software/DspamPD/
5 http://duncanthrax.net/exiscan-acl/
6 http://oss.mdamt.net/gadoyanvirus/

برنامه hMailServer

برنامه hMailServer[1] معروفترین برنامه متن‌باز و گسترده پست الکترونیک در سیستم‌عامل ویندوز است. این برنامه قدرت پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها را به‌وسیله ClamAV دارد.

برنامه IVS Milter

برنامه IVS Milter [2] یک برنامه برای حذف نامه‌های ناخواسته و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها است.

برنامه j-chkmail

برنامه j-chkmail[3] یک برنامه برای حذف نامه‌های ناخواسته و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها است که به زبان C نگارش شده و برای کار در سرورهای زیر بار سنگین طراحی شده است. این برنامه برای کاربران ثبت شده در وب سایت خود و برای استفاده غیر تجاری رایگان است.

برنامه Mail Avenger

برنامه Mail Avenger[4] یک SMTP Server بسیار قابل تنظیم است که قدرت پویش نامه‌های الکترونیکی ، شناسایی ویروس‌ها و حذف نامه‌های ناخواسته را دارد.

برنامه Mailnees

برنامه Mailnees[5] یک برنامه فیلتر کردن محتوا برای sendmail و postfix که امکان پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها را دارد.

---

1 http://www.hmailserver.com/
2 http://ivs-milter.lbsd.net/
3 http://j-chkmail.ensmp.fr/
4 http://www.mailavenger.org/
5 http://mailnees.kicks-ass.org/

برنامه MailScanner

برنامه MailScanner[1] یک برنامه برای پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها ، حذف نامه‌های ناخواسته و کنترل مسائل امنیتی است که با تعداد قابل توجهی از آنتی ویروسها منجمله ClamAV سازگار است.

برنامه Maverix

برنامه Maverix[2] ماژول سرور AOL است که پروتکل SMTP را پیاده سازی می‌کند و نقش یک پروکسی SMTP را ایفا می‌کند. این برنامه توانایی پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها و حذف نامه‌های ناخواسته را دارد.

برنامه MIMEDefang

برنامه MIMEDefang[3] یک برنامه پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها برای برنامه sendmail است.

برنامه mxGuard for IMail

برنامه mxGuard[4] ماژول فیلتر کردن برای IMail است که توانایی استفاده از ClamAV را برای پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها، دارد.

برنامه OdeiaVir

برنامه OdeiaVir[5] یک فیلتر کننده پست الکترونیک و برنامه پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها برای qmail و Exim است.

1 http://www.mailscanner.info/
2 http://www.crystalballinc.com/vlad/software/maverix/
3 http://www.roaringpenguin.com/mimedefang
4 http://www.mxguard.com/postmaster/
5 http://odeiavir.sourceforge.net/

برنامه OpenProtect

برنامه OpenProtect[1] یک راهکار حفاظت پست الکترونیک است که خود از برنامه‌های MailScanner ، Spamassassin و ClamAV استفاده می‌کند و از برنامه‌های Sendmail ، Postfix و Exim پشتیبانی می‌کند. این بسته دارای برنامه‌های نصاب و حذف اتوماتیک است و ماژول‌های مورد نیاز خود را به‌صورت اتوماتیک نصب می‌کند.

برنامه Protea AntiVirus Tools

برنامه Protea AntiVirus Tools[2] برای Lotus Domino است و برای پویش نامه‌های الکترونیکی و شناسایی ویروسها استفاده میشود.

برنامه PSCM

برنامه PSCM[3] یک بسته RPM است که یک SMTP سرور امن با امکانات حذف نامه‌های ناخواسته و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها را نصب می‌کند.

برنامه PTSMail Utilities

برنامه PTSMail Utilities[4] از ClamAV در فیلتر کردن نامه‌ها برای sendmail و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها، استفاده می‌کند..

برنامه pymavis

برنامه pymavis[5] یک برنامه مشابه AMaViS است که برای فیلتر کردن نامه‌ها و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها طراحی شده است. این برنامه فایل‌های ضمیمه نامه که آسیب دیده باشند را نیز شناسایی و پویش می‌کند.

---

1 http://opencompt.com/
2 http://www.proteatools.com/
3 http://www.metawire.org/~pscm/
4 http://www.scanmail-software.com/
5 http://mplayerhq.hu/~arpi/pymavis/

برنامه Qmail-Scanner

برنامه Qmail-Scanner[1] یک برنامه پویش محتوا برای برنامه qmail است. این برنامه برای آنتی ویروس و حذف نامه‌های ناخواسته استفاده می‌شود.

برنامه qpsmtp

برنامه qpsmtp[2] ابزاری کامل برای پروتکلSMTP است که به زبان Perl نگارش شده است. این برنامه امکانات خود را در plug-inهای کوچک پیاده سازی کرده است و امکان حذف نامه‌های ناخواسته و پویش محتویات نامه‌ها را برای یافتن ویروس‌ها دارد.

برنامه qscanq

برنامه qscanq[3] به عنوان یک جایگزین برای qmail-queue طراحی شده است و امکان پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها را دارد.

برنامه qSheff

برنامه qSheff[4] برای حذف نامه‌های ناخواسته بر اساس ضمیمه، عنوان و محتویات نامه است که امکان پویش نامه‌ها را برای شناسایی ویروس‌ها نیز دارد.

مجموعه RevolSys SMTP kit

مجموعهRevolSys SMTP kit[5]، مجموعه‌ای از ابزارها برای افزایش امنیت و کارایی برنامه Postfix است. این مجموعه شامل ابزارهایی برای حذف نامه‌های ناخواسته و پویش محتویات نامه‌ها برای شناسایی ویروس‌ها است. این مجموعه از برنامه‌های spamassassin، ClamAV و Razor استفاده می‌کند.

1 http://qmail-scanner.sf.net/
2 http://smtpd.develooper.com/
3 http://budney.homeunix.net:8080/users/budney/software/qscanq/index.html
4 http://www.enderunix.org/qsheff
5 http://smtp.revolsys.org/

برنامه Sagator

برنامه Sagator[1] یک رابط برای برنامه‌های SMTP مانند Postfix است که امکان حذف نامه‌های ناخواسته و پویش نامه‌ها برای شناسایی ویروس‌ها را دارد.

برنامه Scrubber

برنامه Scrubber[2] یک daemon برای فیلتر کردن محتوای نامه با امکانات plug-inهای مختلف است که با هدف ارتقا سرعت و کارایی طراحی شده است. این برنامه امکان پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها را دارد.

برنامه Secure Mail Intelligence

برنامه Secure Mail Intelligence![3] که به‌طور مختصر !SMI نامیده می‌شود، یک راهکار برای حفاظت سیستم‌های پست الکترونیک است. این برنامه ترکیبی از سیستم‌های دیواره‌آتش، آنتی ویروس‌ها، سیستم‌های تشخیص نفوذ (IDS) و برنامه‌های حذف نامه‌های ناخواسته است. این برنامه امکان استفاده از ۷ برنامه آنتی ویروس و ۳ برنامه حذف نامه‌های ناخواسته در آن واحد دارد. ذکر امکانات متنوع این برنامه از حوصله این گزارش خارج است و فقط بخش daemon این برنامه با لیسانس GPL ارائه می‌شود.

برنامه simscan

برنامه simscan[4] برای حذف ضمیمه‌های نامه‌ها در برنامه qmail استفاده می‌شود و به زبان C نگارش شده است. این برنامه امکان پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها را دارد.

برنامه SmarterMail Filter

برنامه SmarterMail Filter[5] یک plug-in رایگان برای برنامه SmarterMail Server است که برای فیلترکردن نامه‌ها و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها، استفاده می‌شود.

---

1 http://www.salstar.sk/sagator/
2 http://projects.gasperino.org/scrubber/
3 http://www.m2smi.com/
4 http://www.inter7.com/?page=simscan
5 http://www.efextra.com/smfilter.htm

برنامه smf-clamd

برنامه smf clamd[1] که مخفف Smart Sendmail Filter است، یک برنامه سبک به زبان C با کمتر از ۵۵۰ خط کد منبع است. این برنامه برای فیلترکردن نامه‌ها، پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها در برنامه sendmail می‌باشد .

برنامه smtpfilter

برنامه smtpfilter[2] یک برنامه نا محسوس و بلادرنگ است که بین فرستنده و گیرنده نامه قرار می‌گیرد و متن نامه‌ها را برای شناسایی نامه‌های ناخواسته و ویروس‌ها پویش می‌کند.

برنامه smtp-gated

برنامه smtp-gated[3] یک SMTP Proxy با امکانات Transparency در لینوکس و FreeBSD است. این برنامه امکان ارسال نامه‌ها به یک سرور SMTP خارجی نیز دارد. متن نامه‌ها در این برنامه به دنبال ویروس‌ها پویش می‌شود.

برنامه smtp-vilter

برنامه smtp-vilter[4] برنامه‌ای بسیار سریع و کار آمد برای برنامه sendmail است که با استفاده از واسط milter (API) نگارش شده است. برنامه ClamAV آنتی ویروس پیش فرض برنامه smtp-vilter است و امکان پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها را دارد.

برنامه Zabit

برنامه Zabit[5]، برنامه فیلتر کردن محتوا و ضمیمه‌های نامه و پویش نامه‌های الکترونیکی و شناسایی ویروس‌ها قابل استفاده در برنامه qmail است.

---

1 http://smfs.sourceforge.net/smf-clamd.html
2 http://www.gtoal.com/spam/smtpfilter.c.html
3 http://smtp-proxy.klolik.org/
4 http://www.etc.msys.ch/software/smtp-vilter/
5 http://www.enderunix.org/zabit

برنامه zmscanner

برنامه zmscanner [1] یک ماژول قابل بسط برای برنامه‌ای sendmail و zmailer است که برای ترافیک زیاد نگارش شده و قدرت پویش نامه‌های الکترونیکی و شناسایی ویروسها را دارد.

۴-۳-۲- برنامه های دریافت نامه های الکترونیکی (POP3)

پروتکل POP3 یکی از پروتکل‌های معروف و پر کاربرد در زمینه دریافت نامه از سرور پست الکترونیک به برنامه خواننده نامه در کامپیوتر کاربر است. برنامه‌های متن‌باز فراوانی برای این پروتکل وجود دارند که بعضی از آنها می‌توانند به کمک برنامه ClamAV محتویات نامه‌ها را قبل از ارسال به کاربر، پویش کنند. لیست این برنامه‌ها به ترتیب حروف الفبای لاتین در زیر آورده شده است.

پویش کردن نامه به محض دریافت در MTAها، امکانات حذف بلادرنگ نامه‌های ناخواسته و ویروس‌ها و همچنین صرفه جویی در فضای ذخیره سازی کامپیوتر سرور را نیز به‌وجود می‌آورد. از این رو استفاده از برنامه ClamAV و برنامه‌های حذف کننده نامه‌های ناخواسته در MTAها بیشتر متداول است.

برنامه ClamMail

برنامه ClamMail [2] یک برنامه آنتی ویروس و پروکسی برای پروتکل POP3 است. این برنامه قابل استفاده در سیستم‌عامل ویندوز است.

برنامه p3scan

برنامه p3scan [3] ، یکی برنامه POP3 پروکسی نا محسوس [4] در سیستم‌عامل لینوکس است که علی الخصوص برای حفاظت POP3 سرورهای داخلی یک شبکه از دنیای اینترنت طراحی شده است.

---

1 http://www.average.org/zmscanner/
2 http://www.bransoft.com/
3 http://p3scan.sourceforge.net/
4 Transparent

برنامه pop3.proxy

برنامه pop3.proxy[1] ، یک برنامه POP3 پروکسی است که معمولا در سیستم‌های دیواره آتش استفاده می‌شود و کنترل می‌کند تا هم برنامه کاربر و هم برنامه سرور از استاندارد پروتکل POP3 که در RFC شماره ۱۹۳۹ تشریح شده، خارج نشوند و خطری برای یکدیگر به‌وجود نیاورند. این برنامه همچنین امکان ارسال فایل‌های دریافت شده از سرور را به یک برنامه آنتی‌ویروس مانند ClamAV برای پویش محتویات فایل‌ها و کشف ویروس‌ها دارد.

۴-۳-۳- برنامه های پروکسی Web و FTP

برنامه‌های پروکسی وب و FTP کاربرد فراوانی در شبکه‌های محلی و شبکه‌های بزرگ دارند. یکی از کاربردهای این برنامه‌ها افزایش امنیت برای کاربران و کامپیوترهای یک شبکه است. در زیر لیست برنامه‌هایی که امکان استفاده از برنامه ClamAV را دارند آورده شده است.

برنامه DansGuardian

برنامه DansGuardian[2] یک برنامه پروکسی وب با امکان فیلتر کردن محتوا و آدرس‌ها است. این برنامه قدرتمند که نسخه غیر تجاری آن با لیسانس GPL توزیع می‌شود با استفاده از یک patch به نام DG Antivirus Patch، امکان استفاده از ClamAV برای کنترل کردن فایل‌ها دارد.

برنامه Frox

برنامه Frox[3] ، یکی برنامه پروکسی FTP است که توانایی Cache فایل‌های دریافتی را به صورت محلی یا با استفاده از یک Proxy دیگر مانند squid دارد. این برنامه همچنین قدرت پویش فایل‌های دریافتی توسط ClamAV را دارد و در سیستم‌عامل‌های FreeBSD و سایر سیستم‌عامل‌هایی که بسته IPFilter را دارند می‌تواند به‌صورت نا محسوس (Transparent) عمل کند.

---

1 http://quietsche-entchen.de/cgi-bin/wiki.cgi/proxies/Pop3Proxy
2 http://www.harvest.com.br/asp/afn/dg.nsf
3 http://www.hollo.org/frox/

برنامه HTTP Anti Virus Proxy

برنامه HTTP Anti Virus Proxy[1] یا اصطلاحا HAVP، یک برنامه پروکسی وب با امکان پویش فایلهای دریافتی برای شناسایی ویروسها می‌باشد. این برنامه به خودی خود امکان Cache کردن فایل‌ها را ندارد و تنها برای پویش تمام محتویات وب، حتی فایل‌های JPEG و HTML طراحی شده است.

برنامه mod clamav

برنامه mod clamav[2] یک ماژول برای برنامه Apache است که قدرت پویش فایل‌ها را برنامه Apache اضافه می‌کند. این برنامه امکان پویش فایل‌های محلی موجود در همان کامپیوتر و فایل‌های دریافتی توسط mod_proxy را فراهم می‌کند.

برنامه ClamAV module for ProFTPD

برنامه ClamAV module for ProFTPD[3] ، یک ماژول قابل اضافه‌کردن به برنامه ProFTPD است که قدرت پویش فایل‌های جدید را به برنامه ProFTPD اضافه می‌کند.

برنامه SafeSquid

برنامه SafeSquid[4] یک برنامه قدرتمند برای فیلتر کردن محتوا و کاربردهای دیگر است که توانایی استفاده از پروکسی‌های دیگر مانند squid را نیز دارد. این برنامه امکان استفاده از برنامه ClamAV را برای پویش فایلها برای شناسایی ویروسها دارد. نسخه رایگان این برنامه محدودیت زمانی یا محدودیت در تعداد کاربران ندارد.

برنامه SquidClamAV Redirector

برنامه SquidClamAV Redirector[5] یک برنامه کمک کننده به squid برای پویش فایل‌ها به دنبال ویروس‌ها است. این برنامه امکان استفاده از برنامه ClamAV را دارد.

---

1 http://www.server-side.de/
2 http://software.othello.ch/mod_clamav/
3 http://www.uglyboxindustries.com/open-source.php
4 http://www.safesquid.com/
5 http://www.jackal-net.at/tiki- read_article.php?articleId=1

برنامه Squidclam

برنامه Squidclam[1] ، یک برنامه جایگزین برای SquidClamAV-Redirector.py است که به زبان C نگارش شده است.

برنامه Viralator

برنامه Viralator[2] یک برنامه به زبان Perl است که قدرت پویش فایل‌ها را به کمک آنتی‌ویروس ClamAV و برنامه squid دارد.

۴-۳-۴- فایل سیستم‌ها و برنامه های ثالث

فایل‌سیستم‌ها، برای ذخیره‌سازی فایل‌ها و دایرکتوری‌ها می‌باشند، برنامه‌هایی وجود دارند که امکان کنترل یا پویش فایل‌ها را به محض دستیابی به آنتی ویروس‌ها می‌دهند که لیست مهمترین عناوین آنها در زیر آمده است.

برنامه Dazuko

برنامه Dazuko[3] یک ماژول برای Kernel لینوکس، FreeBSD و Linux/RSBAC است که روال‌های امکان سنجی دستیابی به فایل‌ها را برای هسته سیستم‌عامل فراهم می‌کند. این ماژول غیر از افزایش امنیت و به‌وجود آوردن روال‌های ویژه کنترل دستیابی، امکان پویش فایل‌های سیستم به منظور شناسایی ویروس‌ها را توسط برنامه ClamAV فراهم می‌کند.

برنامه Famuko

برنامه Famuko[4] مشابه برنامه Dazuko است و خالق آن با توجه به برنامه Dazuko و جهت تسهیل استفاده و رفع مشکلات برنامه Dazuko، آن را نگارش کرده است. این برنامه در فضای سیستمی کاربران (User Space) اجرا می‌شود.

---

1 http://squidclam.sourceforge.net/
2 http://viralator.sourceforge.net/
3 http://dazuko.org
4 http://www.campana.vi.it/ottavio/Progetti/Famuko/

برنامه OpenAntiVirus samba-vscan

برنامه OpenAntiVirus samba-vscan[1] برای کنترل فایلهای اشتراکی در برنامه Samba نگارش شده است و توسط پروژه OpenAntiVirus پشتیبانی می‌شود.

۴-۳-۵- برنامه های نامه نگاری

برنامه‌های متعددی برای نامه‌نگاری متنی وجود دارند که تعداد متعددی از این برنامه‌ها از آنتی ویروس ClamAV پشتیبانی می‌کنند. از آنجا که این برنامه‌ها اهمیت چندانی در مسائل Enterprise ندارند، فقط نام آنها در این قسمت آورده شده است.

Clamailfilter: http://quiston.tpsa.com/hacks/clamailfilter.xhtml
ClamAssassin: http://drivel.com/clamassassin/
clamscan-procfilter: http://www.virtualblueness.net/~blueness/clamscan-procfilter/
KMail: http://kmail.kde.org/
MyClamMailFilter: http://muncul0.w.interia.pl/projects.html#myclammailfilter
OpenWebMail: http://openwebmail.com/openwebmail/
QClam: http://sageshome.net/oss/qclam.php
QMVC - QmailMail and Virus Control: http://www.fehcom.de/qmail/qmvc.html
Sylpheed-Claws: http://claws.sylpheed.org/
SoftlabsAV: http://antivirus.softlabs.info/

۴-۳-۶- رابط های کاربری گرافیکی مبتنی بر ClamAV

از آنجا که برنامه ClamAV به‌خودی خود رابط گرافیکی ندارد، برنامه‌های متن‌باز ثالثی برای این منظور طراحی شده‌اند. در زیر رابط‌های کاربری گرافیکی ثالث برای برنامه ClamAV به ترتیب حروف لاتین ذکر شده‌اند.

برنامه AVScan

برنامه AVScan[2] یک برنامه گرافیکی آنتی ویروس در برنامه Endeavour Mark II[3] است. برنامه Endeavour Mark II خود یک راهکار گرافیکی برای مدیریت فایل‌ها با امکانات نمایش تصاویر، مدیریت دیسک‌ها و غیره در سیستم‌عامل یونیکس است که با استفاده از کتابخانه GTK نگارش شده است.

---

1 http://www.openantivirus.org/projects.php#samba-vscan
2 http://wolfpack.twu.net/Endeavour2/contrib/index.html#avscan
3 http://wolfpack.twu.net/Endeavour2/

برنامه BeClam

برنامه BeClam[1] رابط گرافیکی برنامه ClamAV در سیستم‌عامل BeOS است.

برنامه Clamaktion

برنامه Clamaktion[2] یک برنامه سبک و کوچک برای کاربران محیط رومیزی KDE است که به کاربران قدرت پویش فایل‌ها و دایرکتوری‌ها را می‌دهد.

برنامه ClamShell

برنامه ClamShell[3] یک رابط گرافیکی نگارش شده به زبان برنامه سازی Java است که برای کاربران ClamAV در لینوکس نگارش شده است.

برنامه ClamTk

برنامه ClamTk[4] یک رابط گرافیکی نگارش شده به زبان برنامه سازی Perl و TK است.

برنامه clamXav

برنامه clamXav[5] یک رابط گرافیکی برای سیستم‌عامل Mac OS X است.

برنامه ClamWin

برنامه ClamWin[6] یک رابط گرافیکی در سیستم‌عامل ویندوز است که امکانات پویش فایل و دایرکتوری را در این سیستم‌عامل به صورت گرافیکی فراهم می‌کند. این برنامه یک Taskbar Tray Icon و امکانات پویش فایلها به وسیله کلیک راست موس را اضافه می‌کند. در این برنامه فایلهای کتابخانه Cygwin به‌صورت خودکار نصب می‌شود.

---

1 http://www.bebits.com/app/3930/
2 http://web.tiscali.it/rospolosco/clamaktion/
3 http://home.comcast.net/~schwalbrichard/
4 http://www.rootshell.be/~phen0m/clamtk/
5 http://www.markallan.co.uk/clamXav
6 http://clamwin.sourceforge.net/

برنامه FETCAV

برنامه FETCAV[1] یک رابط گرافیکی نگارش شده به کمک Xdialog است.

برنامه KlamAV

برنامه KlamAV[2] یک رابط گرافیکی نگارش شده برای محیط رومیزی KDE است که امکان پویش فایل‌ها و دایرکتوری‌ها را فراهم می‌آورد. این برنامه به کمک ماژول Dazuko امکان پویش فایل‌ها را حین دستیابی اضافه می‌کند.

برنامه QtClamAVclient

برنامه QtClamAVclient[3] یک رابط گرافیکی نگارش شده به کمک کتابخانه QT است که امکان پویش فایل‌ها را به کمک سرور ClamAV و قابلیتهای Stream این daemon فراهم می‌کند.

برنامه wbmclamav

برنامه wbmclamav[4] یک ماژول تنظیم و کنترل برنامه ClamAV است که برای Webmin نگارش شده است.

۴-۳-۷- کتابخانه های مبنی بر ClamAV

کتابخانه‌های زیر همگی مبتنی بر ClamAV هستند که امکان استفاده از ClamAV را در زبان‌های برنامه‌سازی مختلف فراهم می‌کنند.

کتابخانه ClamAV-Sharp

کتابخانه ClamAV-Sharp[5] برای استفاده برنامه ClamAV در محیط مانو استفاده می‌شود.

---

1 http://www.thymox.uklinux.net/
2 http://sourceforge.net/projects/klamav/
3 http://www.xystumnet.com/qtclamavclient.html
4 http://wbmclamav.labs.libre-entreprise.org/
5 http://clamav-sharp.pcode.nl/

کتابخانه ClamAVPlugin

کتابخانه ClamAVPlugin[1] برای استفاده از آنتی ویروس ClamAV در SpamAssassin استفاده می‌شود.

کتابخانه clamavr

کتابخانه clamavr[2] برای استفاده از برنامه ClamAV در زبان برنامه سازی Ruby است.

کتابخانه D bindings for ClamAV

کتابخانه D bindings for ClamAV[3] برای استفاده ClamAV در زبان برنامه‌سازی D است.

کتابخانه File::Scan::ClamAV

کتابخانه File::Scan::ClamAV[4] برای استفاده از برنامه ClamAV در زبان برنامه سازی Perl است.

کتابخانه Mail::ClamAV

کتابخانه Mail::ClamAV[5] برای استفاده از برنامه ClamAV در زبان برنامه سازی Perl است.

کتابخانه PHP ClamAV Lib

کتابخانه PHP ClamAV Lib۶ برای استفاده از برنامه ClamAV در زبان برنامه سازی PHP است.

1 http://wiki.apache.org/spamassassin/ClamAVPlugin
2 http://raa.ruby-lang.org/list.rhtml?name=clamavr
3 http://dmd.kuehne.cn/diverse.html#clamav_d
4 http://search.cpan.org/~cfaber/File-Scan-ClamAV-1.06/lib/File/Scan/ClamAV.pm
5 http://cpan.gossamer-threads.com/modules/by-authors/id/S/SA/SABECK/
6 http://phpclamavlib.org/

کتابخانه pyclamav

کتابخانه pyclamav[1] برای استفاده از برنامه ClamAV در زبان برنامه سازی Python است.

کتابخانه WRAVLib

کتابخانه WRAVLib[2] برای استفاده از برنامه ClamAV در محیط مانو است که به زبان برنامه‌سازی C# نگارش شده است.

۴-۴- نتایج

برنامه آنتی ویروس ClamAV به روز ترین و قدرتمندترین برنامه در آنتی ویروس‌های متن‌باز است که به همراه تعداد قابل توجهی از ابزارهای ثالث ارائه می‌شود. وجود ابزارها، برنامه‌های ثالث و کتابخانه‌ها برای این آنتی‌ویروس، کاربردهای این برنامه را در سطح آنتی‌ویروس‌های تجاری و یا بالاتر از آنها قرار می‌دهد.

اشکال آنتی ویروس‌های متن‌باز منجمله برنامه ClamAV، کم بودن ویروس‌های شناخته شده و به روز نشدن سریع این بانک اطلاعاتی است که یک معضل بسیار بزرگ محسوب می‌شود و سبب می‌شود شرکت‌ها و سازمان‌های تجاری بزرگ از این آنتی‌ویروس و مشابهات آن استفاده نکنند.

استفاده از آنتی‌ویروس‌های متن‌باز، فقط در پروژه‌ها و راهکارهایی که حساسیت بسیار زیادی ندارند و وجود آنتی‌ویروس‌ها در آنها الزامی می‌باشد، قابل قبول است. نمونه این راهکارها مراکز آموزشی، دانشگاه‌ها و غیره است.

1 http://xael.org/norman/python/pyclamav/index.html
2 http://www.wolfereiter.com/wravlib/

مراجع

[۱] نفوذگری در شبکه و روش‌های مقابله نوشته مهندس احسان ملکیان – انتشارات نص – سال ۸۳

[2] IP filter based firewalls HOWTO - Brendan Conoboy – Erik Fichtner- 2002

[3] Firewalling with OpenBSD Packet Filter - Peter N.M.Hansteen - 2005-2006

[4] Iptables Tutorial 1.2.0 - Oskar Andreasson - 2005

[5] http://www.netfilter.org/ (netfilter/iptables Project)

[6] http://www.squid-cache.org/ (Squid Cache Project)

[7] http://coombs.anu.edu.au/ipfilter/ (IPFilter Project)

[8] http://www.privoxy.org/ (Privoxy Project)

[9] http://dansguardian.org/ (DansGuardian Project)

[10] http://internet.junkbuster.com/ (Internet Junk Buster Project)

[11] http://web.archive.org/web/20060824110625/http://www.squidguard.org/ (squidGuard Project)

[12] http://www.ircert.com/articles/Firewall.htm (Introduction to Firewall)

[13] http://en.wikipedia.org/wiki/Great_Firewall_of_China (China Firewall)

[14] http://www.bsdcan.org/2004//papers/introduction_to_pf-mcbride-bsdcan2004.pdf (Introduction to PF)

[15] http://www.pc-help.org/www.nwinternet.com/pchelp/security/firewalls.htm (Introduction to Firewalls)

[16] http://www.vicomsoft.com/knowledge/reference/firewalls1.html (Introduction to Firewalls)

[17] http://www.hipac.org/ (nf-hipac Project)

[18] http://www.cs.aau.dk/~mixxel/cf (Compact Filter Project)

[19] http://www.geocities.com/hamidreza_jm (iptables with classifiers)

[20] http://ipset.netfilter.org/ (ipset Project)

[21] http://netsecurity.about.com/od/hackertools/a/aa072004.htm

[22] http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm (History of Firewalls)

[23] http://www.more.net/technical/netserv/tcpip/firewalls/ (Introduction to Firewalls and type of firewalls)

[24] http://www.informit.com/articles/article.asp?p=170452&seqNum=2&rl=1 (What a firewall cannot do)

[25] http://www.webopedia.com/TERM/f/firewall.html

[26] World-Wide-Web Consortium PICS Home Page: http://www.w3.org/PICS

[27] Internt Content Rating Association:http://www.icra.org

[28] SafeSurf: http://www.safesurf.com

[29] CyberPatrol: http://www.cyberpatrol.com

[30] NetNanny: http://www.netnanny.com

[31] Fahrenheit 451.2: Is Cyberspace Burning - The ACLU's Report on Filtering Software: http://www.aclu.org/issues/cyber/burning.html

[32] Peacefire: http://www.peacefire.org
[33] The Censorware Project http://www.censorware.net
[34] The Global Internet Liberty Campaign: http://www.gilc.org/speech/ratings
[35] The Internet Free Expression Alliance: http://www.ifea.net
[36] Computer Professionals for Social Responsibility (CPSR): http://www.cpsr.org
[37] http://www.sans.org/ : The SANS Institute
[38] http://www.snort.org/ : Open source network intrusion prevention and detection system (Snort).
[39] http://sourceforge.net/projects/barnyard : Output spool reader for Snort (Barnyard).
[40] http://acidlab.sourceforge.net/ : Analysis Console for Intrusion Databases (ACID).
[41] http://secureideas.sourceforge.net/ : Basic Analysis and Security Engine (BASE).
[42] http://www.bro-ids.org/ : Bro Intrusion Detection System.
[43] http://www.cl.cam.ac.uk/~cpk25/brooery/ : Brooery, Bro GUI.
[44] http://www.prelude-ids.org/ : Prelude-IDS - The Hybrid IDS framework
[45] http://www.ossec.net/ : Open Source Host-based Intrusion Detection System
[46] http://sourceforge.net/projects/tripwire : Open Source Tripwire.