فایروال

گردآورنده و مترجم:

رضا قنبرزاده

زیر نظر استاد ارجمند:

جناب آقای مهندس عقیقی

بهار ۱۳۹۰

مرکز آموزش علمی –کاربردی قوچان

گروهIT

پروردگارا:

مرا به بزرگی چیز هایی که داده ای آگاه و راضی کن تا کوچکی چیز هایی که ندارم ، آرامشم را بر هم نزند.

فهرست

مقدمه ----------۴

تاریخچه فایروال----------۵

فایروال چیست ؟----------۶

مشخصه‌های مهم یک فایروال----------۶

انواع فایروال----------۸

- فایروال‌های سخت‌افزاری ----------۱۰
- فایروال‌های نرم‌افزاری ----------۱۰
  - o مزایای استفاده از فایروال سخت‌افزاری----------۱۲
  - o معایب استفاده از فایروال سخت‌افزاری ----------۱۲
  - o مزایای استفاده از فایروال نرم‌افزاری----------۱۲
  - o معایب استفاده از فایروال نرم‌افزاری----------۱۲
  - o برتری فایروال سخت‌افزاری به فایروال نرم‌افزاری----------۱۳
  - o برتری فایروال نرم‌افزاری به فایروال سخت‌افزاری----------۱۳
- فایروال‌های سطح مدار----------۱۳
- فایروال‌های پروکسی ----------۱۴
- فیلترهای Nosstateful ----------۱۴

- فیلترهای Stateful ---------- ۱۵
- فایروالهای شخصی ---------- ۱۵

موقعیت یابی برای فایروال ---------- ۱۶

متناسب ساختن فایروال ---------- ۱۷

نحوه انتخاب یک فایروال ---------- ۱۹

جگونگی کارکرد فایروال در یک نگاه کلی ---------- ۲۰

آنچه فایروال‌ها سیستم را از آن محافظت می‌نمایند ---------- ۲۳

سرورهای Proxy وDMZ ---------- ۲۵

مزایا و معایب استفاده از فایروال ---------- ۲۵

معرفی برخی از نرم‌افزارهای فایروال جدید و معروف دنیا ---------- ۲۷

آنتی فیلتر چیست؟ ---------- ۲۸

منابع ---------- ۲۹

مقدمه

اتصال به اینترنت بدون استفاده از یک فایروال[1] همانند گذاشتن سوئیچ در اتومبیل، قفل نکردن درب‌های آن و رفتن به یک فروشگاه برای تهیه لوازم مورد نیاز است. با این که ممکن است بتوانید در صورت سرقت اتومبیل، سریعاً واکنش مناسبی را انجام دهید، ولی فرصت ارزشمندی را برای سارقین ایجاد نموده‌اید تا آنان بتوانند در سریع ترین زمان ممکن به اهداف مخرب خود دست یابند. چنین وضعیتی در اینترنت نیز وجود دارد و مهاجمان در ابتدا با استفاده از کدهای مخربی نظیر ویروس‌ها، کرم‌ها و تروجان‌ها اقدام به شناسائی قربانیان خود می‌نمایند و در مرحله بعد، اهداف شناسائی شده را مورد تهاجم قرار می‌دهند. برنامه‌های فایروال یک سطح حفاظتی و امنیتی مناسب در مقابل این نوع حملات را ارائه می نمایند.

در حقیقت فایروال، دیواری بین کامپیوتر شما و اینترنت است فایروال به شما اجازه می‌دهد صفحات وب را ببینید و به آنها دسترسی داشته باشید، فایل download کنید، چت کنید و ... . در حالیکه مطمئن هستید افراد دیگری که در اینترنت مشغول هستند نمی‌توانند به کامپیوتر شما دست درازی کنند. بعضی از فایروال‌ها نرم افزارهایی هستند که روی کامپیوتر اجرا می شوند اما فایروالهای دیگر به صورت سخت افزاری ساخته شده‌اند و کل شبکه را از حمله مصون می‌کنند

در این مقاله سعی بر آن است تا توضیح جامع و مختصری در مورد فایروال، انواع آن و مشخصات یک فایروال و .... در اختیار خوانندگان قرار گیرد.

[1] Firewall

www.Prozhe.com

تاریخچه فایروال

هنگام بررسی تاریخچه فایروال با دیگر تکنولوژی‌ها ،پی می‌بریم که تکنولوژی نوجوان و تازه وارد است. اولین نسل معماری فایروال‌ها که فایروال فیلترشده بسته‌ای[2] نامیده می‌شد در سال ۱۹۸۵ توسط شبکه‌ی عظیم سیسکو[3] به وجود آمد. سه سال بعد،اولین صفحه‌ی فایروال با موفقیت ایجاد شد،که موسس آن جف موگل[4] از شرکت تجهیزات دیجیتالی DEC[5] بود.با این وجود در طول این سه سال دیو پرستو[6] وهاوارد تری کی[7]از شرکت AT&T Bell Laboratories[8] در حال توسعه ی نسل دوم فایروال‌ها یعنی فایروال‌های دوره‌ای[9] بودند.

کار آن ها یک دهه طول کشید،در سال ۱۹۸۰ شروع و در سال ۱۹۹۰ به سرانجام رسید.

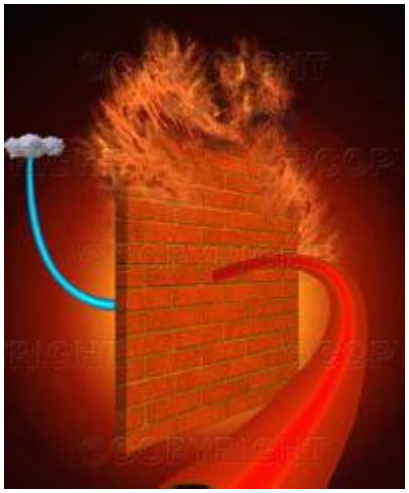
در سال‌های۱۹۹۰و۱۹۹۱،بیل چسویک[10] و مارکوس رانوم[11] و ژن اسپافورد[12] صفحاتی را که نسل سوم فایروال‌ها یعنی فایروال‌های لایه‌ای[13] را توصیف می‌کرد، منتشر کردند این نوع فایروال، فایروال مبتنی بر پروکسی[14] نیز نامیده می‌شد.این گروه سه نفری،هر یک به تنهایی نسل سوم را توسعه دادند ودر پایان رانوم موفقیت بیشتری بدست بیاورد.

در سال ۱۹۹۱،شرکت DEC اولین فایروال تجاری را منتشر کرد و نام این محصول را "SEAL" گذاشت SEAL .بر اساس کارهای مارکوس رانوم ساخته شده بود.در سال بعد از آن باب باردن[15] و آنت دشولان[16] از دانشگاه کالیفرنیای جنوبی شروع به توسعه نسل چهارم فایروال ها کردند که ویزاس[17] نامیده می‌شد.این سیستم دارای اولین یکپارچگی مجازی[18] و دارای رنگ‌ها و آیکون‌هایی بود.ویزاس اولین نوع فایروال‌های تجاری بود که در سال ۱۹۹٤ توسط شرکت اسرائیلی چک پینت[19] منتشر شد. در سال ۱۹۹٦ اسکات ویگل[20] از شرکت نرم افزارهای جهانی اینترنت[21] شروع به کار بر روی نسل پنجم فایروال‌ها کرد که معماری با کرنل پروکسی[22] نامیده می‌شد. شرکت Cisco اولین فایروال بر مبنای این تکنولوژی را ایجاد کرد وسپس منتشر کردر حال حاضر این صنعت در حال دیدن یک همگرایی در تکنولوژی فایروال ها و ضدنفوذگرها است

---

[2] Packet Filtering Firewalls
[3] Cisco
[4] Jeff Mogul
[5] Digital Equipment Corporation
[6] Dave Presetto
[7] Howard Trickey
[8] این شرکت در سال۱۸۷٦ توسط گراهام بل تأسیس شد
[9] circuit level firewalls
[10] Bill Cheswick
[11] Marcus Ranum
[12] Gene Spafford
[13] Application Layer Firewalls
[14] Proxy-Based Firewalls
[15] Bob Braden
[16] Annette DeSchlon
[17] Visas
[18] Visual Integration
[19] Check Point Software
[20] Scott Wiegel
[21] Global Internet Software Group
[22] Kernel Proxy architecture

فایروال چیست ؟



"اساساً یک فایروال سدی است برای دور نگهداشتن نیروهای مخرب از دارائی شما.در حقیقت علت اینکه فایروال[23] نامیده می‌شود همین است. کار آن مشابه فایروال فیزیکی است که از گسترش آتش از یک ناحیه به ناحیه دیگر ممانعت به عمل می‌آورد."

تعریف فوق، تعریف ساده و عامیانه‌ای از فایروال است. در حقیقت، تا چند سال پیش فقط کسانی که در بانک‌ها، مشاغل تجاری بزرگ و دوایر دولتی کار می‌کردند، از فایروال استفاده می‌نمودند. اما زمانه به کلی تغییر کرده است .امروزه داشتن یک فایروال خوب به اندازه داشتن ضدویروس قوی، مسئله امنیتی مهمی حساب می‌شود

فایروال یک معیار امنیتی است که یک کامپیوتر تنها و یا کامپیوترهای موجود در یک شبکه را از دسترسی غیر مجاز حفظ می‌کند. متاسفانه در دنیای امروز کامپیوتری، تعداد زیادی هکر وجود دارد که با نفوذ به داخل کامپیوترها، سعی در ربودن اطلاعات مهم می‌کنند. هرچند که تا دیروز هدف هکرها حمله به شرکت‌های بزرگ بود اما هکرهای امروزی علاقمند به دزدیدن اطلاعات از کامپیوترهای کوچک هم هستند.

فایروال می‌تواند یک دستگاه سخت افزاری و یا یک برنامه نرم افزاری و یا ترکیبی از هردو باشد که در ادامه هر یک از آن‌ها توضیح داده می‌شود. در حقیقت یک فایروال خوب می‌تواند جلوی دسترسی هکرها بداخل کامپیوتر را بگیرد، در ضمن نمی‌گذارد هیچگونه اطلاعاتی بدون اجازه کاربر از کامپیوترتان خارج شود. فایروال نمی‌تواند مستقیماً جلوی حمله ویروسها را بگیرد اما گاهی جلوی ویروسها را برای ارسال ایمیل از یک کامپیوتر آلوده می‌گیرد.

در نتیجه در یک تعریف کلی، می‌توان فایروال را این‌چنین تعریف کرد:

فایروال وسیله‌ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف می‌کند.علاوه بر آن از آنجایی که معمولا یک فایروال بر سر راه ورودی یک شبکه می‌نشیند لذا برای ترجمه آدرس شبکه نیز بکار گرفته می‌شود

مشخصه‌های مهم یک فایروال

همانطور که گفته شد، فایروال سیستمی است که در بین کاربران یک شبکه محلی و شبکه جهانی قرار می‌گیرد و ضمن نظارت بر دسترسی‌ها در تمام سطوح ورود و خروج اطلاعات راتحت نظر دارد. در این ساختار هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات را کنترل‌کند موظف است تمام ارتباطات مستقیم شبکه داخلی خود را با دنیای خارج قطع کرده و هرگونه ارتباط خارجی از طریق یک دروازه که دیوارآتش یا فیلتر نام دارد انجام‌شود.بدیهی است هر چه این فیلتر قوی‌تر باشد، حفاظت کامپیوتر کاربر بهتر خواهد بود.

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

[23] fireWall

۱. توانایی ثبت و اخطار

ثبت وقایع یکی از مشخصه‌های بسیار مهم یک فایروال به شمار می‌رود 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.

۲. بازدید حجم بالایی از بسته‌های اطلاعات

یکی از تست‌های فایروال، توانایی آن در بازدید حجم بالایی از بسته های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده‌ای که یک فایروال می‌تواند کنترل کند، برای شبکه‌های مختلف متفاوت است اما یک فایروال قطعاً نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود.عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیت‌ها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی فایروال تحمیل می‌شوند.عامل محدودکننده دیگر می‌تواند کارت‌های واسطی 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 نرم افزارهای دیگر می‌سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است

۳. 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 شبکه ها 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.

۴. امنیت و افزونگی فایروال

امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است.فایروالی که نتواند امنیت خود را تامین کند ، قطعاً 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:

۴,۱. امنیت سیستم عامل فایروال :

اگر نرم افزار 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 بروزرسانی آن از نکات مهم در امنیت فایروال است

۴,۲. دسترسی امن به فایروال جهت مقاصد مدیریتی :

یک فایروال باید مکانیزمهای امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روشها می تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد

انواع فایروال

فایروال بطور واحد کار حفاظت از کامپیوتر و اطلاعات شخصی از نفوذگران را دارد، اما روش انجام کار توسط انواع مختلف، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می‌شود.براین اساس ۲ نوع دسته-بندی را برای فایروال‌ها در نظر می‌گیریم.

در دسته‌بندی نخست،فایروال را به ۲ دسته نرم‌افزاری و سخت‌افزاری تقسیم می‌نماییم که در ذیل توضیح داده شده است. و در تقسیم‌بندی دیگر فایروال‌ها را به ۵ گروه تقسیم می‌کنیم.

در ابتدا در مورد انواع نرم/سخت‌افزاری این فیلتر صحبت می‌کنیم:

۱. **فایروال‌های سخت‌افزاری** این نوع از فایروال‌ها که به آنان فایروال‌های شبکه نیز گفته می‌شود ، بین کامپیوتر کاربر (و یا شبکه) و کابل و یا خط DsL قرار خواهند گرفت. فایروال‌های سخت‌افزاری در مواردی نظیر حفاظت چندین کامپیوتر مفید بوده و یک سطح مناسب حفاظتی را ارائه می‌نمایند در صورتی که شما صرفاً دارای یک کامپیوتر پشت فایروال می‌باشید و یا این اطمینان را دارید که سایر کامپیوترهای موجود بر روی شبکه نسبت به نصب تمامی patch ها ، بهنگام بوده و عاری از ویروس‌ها و یا کرم‌ها می‌باشند ، ضرورتی به استفاده از یک سطح اضافه حفاظتی نخواهید داشت.

فایروال‌های سخت افزاری عموماً ترافیک بین شبکه و اینترنت را کنترل کرده و نظارت خاصی بر روی ترافیک بین کامپیوترهای موجود در شبکه را انجام نخواهند داد.

این نوع فایروال‌ها را می‌توان به صورت محصول جداگانه خریداری کرد اما معمولاً، به صورت تعبیه شده برروی روترهای شبکه هستند

شکل ۱) نمونه‌ای از یک فایروال سخت‌افزاری شخص

مزایای روترهای فایروال:

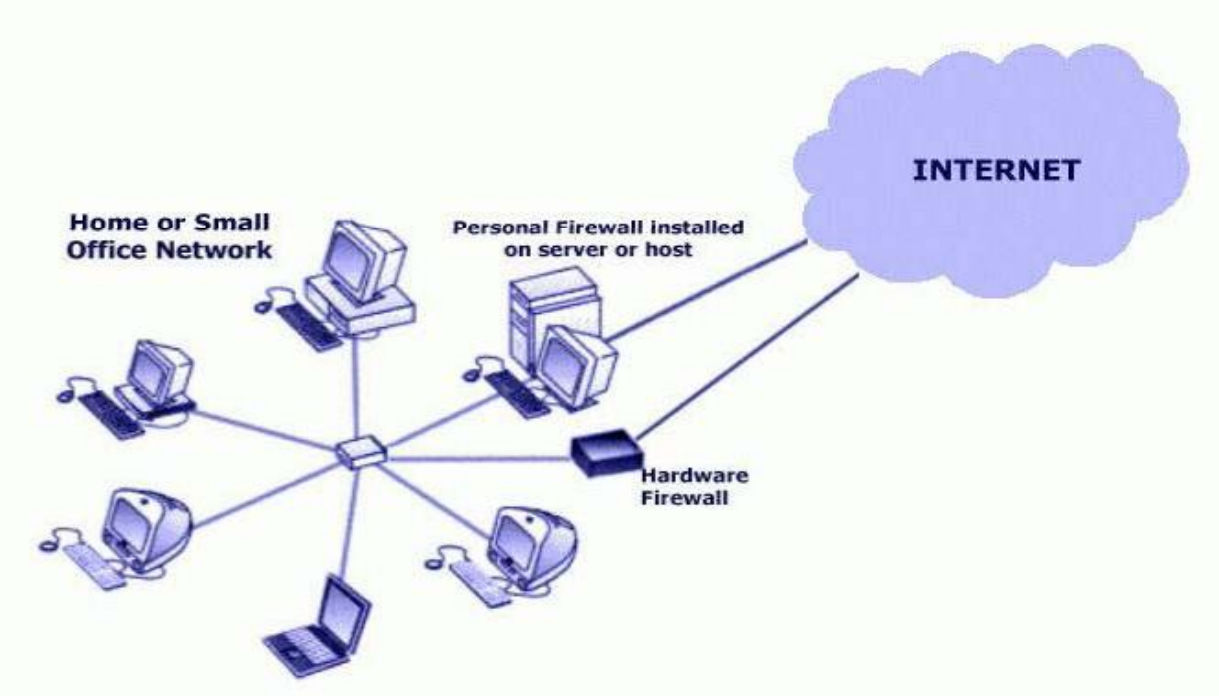
- معمولاً دارای حداقل چهار پورت برای اتصال سایر کامپیوترها می‌باشند
- امکان حفاظت چندین کامپیوتر را ارائه می‌نمایند

معایب روترهای فایروال:

- کابل‌کشی اضافه که مسلماً هزینه‌ای اضافی را نیز در بردارد

فایروال‌های سخت‌افزاری، از تکنیک فیلتر کردن بسته‌ها[24] برای تست هدر بسته،جهت تعیین مقصد و مبدا استفاده می‌کنند.اطلاعات به دست آمده از این تست، با تنظیمات پیش فرض یا تنظیماتی که کاربر انجام داده است مقایسه و تصمیم‌گیری می‌شود که آیا بسته ارسال یا متوقف شود.

[24] Packet Filtering

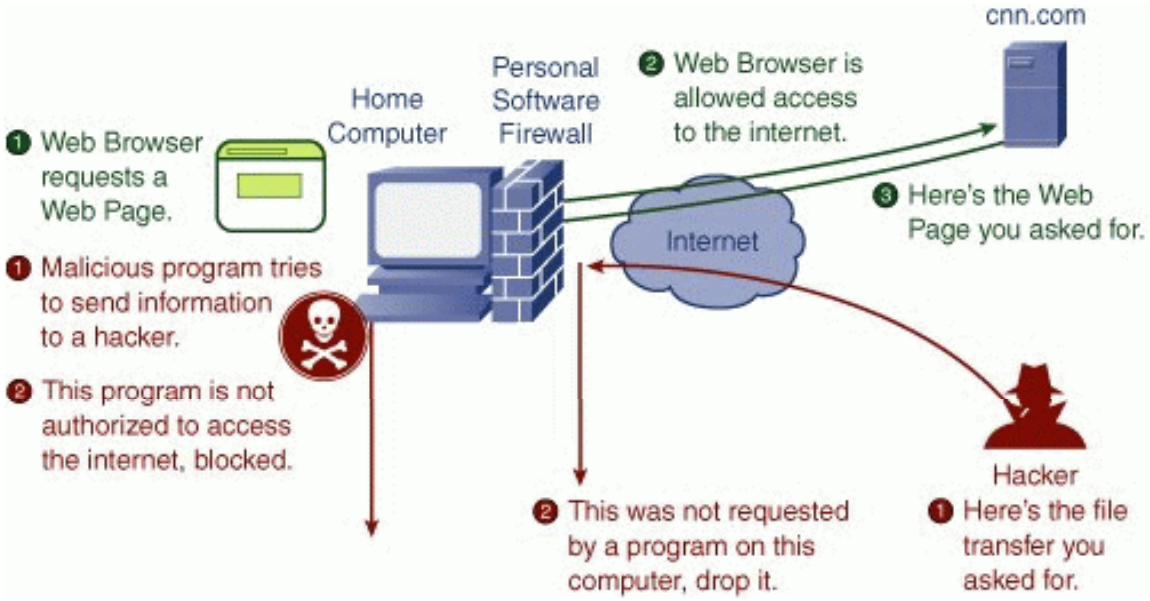


شکل ۲) محل قرارگیری فایروال سخت‌افزاری در شبکه

معمولاً این نوع فایروال‌ها به علت داشتن سیستم‌عامل جدایی که دارند، در معرض خطر کمتری از طرف شبکه قرار می‌گیرند و می‌توان مانند یک نود در شبکه یا یک mini Computer به آن‌ها نگاه کرد

۲. **فایروال‌های نرم‌افزاری** برخی از سیستم‌های عامل دارای یک فایروال تعبیه شده درون خود می‌باشند . در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای ویژگی فوق می‌باشد، پیشنهاد می‌گردد که آن را فعال نموده تا یک سطح حفاظتی اضافی در خصوص ایمن سازی کامپیوتر و اطلاعات ، ایجاد گردد .(حتی اگر از یک فایروال خارجی یا سخت افزاری استفاده می‌نمائید). در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال تعبیه شده نمی‌باشد ، می‌توان اقدام به تهیه یک فایروال نرم افزاری کرد . با توجه به عدم اطمینان لازم در خصوص دریافت نرم افزار از اینترنت با استفاده از یک کامپیوتر محافظت نشده ، پیشنهاد می‌گردد برای نصب فایروال از CD و یا DVD مربوطه استفاده گردد .

در شکل زیر، چگونگی کارکرد یک فایروال نرم‌افزاری به صورت ساده بیان شده است.



شکل ۳) چگونگی کار یک فایروال نرم‌افزاری

این نوع فایروال‌ها،اغلب توسط کاربران خانگی که به صورت جدا از شبکه خاصی،به شبکه جهانی اینترنت متصل می‌شوند استفاده می‌شود.

فایروال‌های نرم‌افزاری،مانند هر نرم‌افزار دیگری بر روی سیستم نصب و تنظیمات و تعاریفی برای آن انجام می‌شود.این نوع فایروال‌ها،از هر گونه حمله به کامپیوتر شخصی جلوگیری می‌کنند و حتی با تنظیمات خاص این نرم‌افزار می‌توان جلوی حملات Trojan و کرم‌های E-mail [۲۵] را نیز گرفت و اجازه اجرای دوباره این برنامه‌ها را نمی‌دهد.

بعضی از بسته‌های فایروال‌های نرم‌افزاری،حاوی آنتی ویروس و آنتی اسپم نیز هستند.

سوالی که در این‌جا مطرح است این است که چرا با وجود یک فایروال سخت‌افزاری باز هم نیاز به فایروال‌های نرم‌افزاری است!

در جواب این سوال،E-mail Worms را مثال می‌زنیم. برای ارسال ایمیل،همانطور که می‌دانیم از پورت ۲۵ یعنی SMTP[26] استفاده می‌شود. زمانی‌که این ایمیل که حاوی Worm نیز می‌باشد به فایروال سخت‌افزاری که معمولاً در روتر شبکه تعبیه شده است می‌رسد به عنوان یک پورت صحیح عبور می‌کند. در ثانی، فایروال‌های سخت‌افزاری تنها ترافیک کلی شبکه را در نظر دارند و به کاربر هشدار یا پیغامی مبتنی بر نفوذ و حمله به کامپیوتر شخصی وی را نمی‌دهند.

در نتیجه،پیشنهاد می‌شود از هر دو نوع فایروال استفاده شود.

در ادامه، مزایا و معایب استفاده از هر نوع فایروال مطرح می‌شود و سپس به مقایسه این دو می‌پردازیم.

[25] E-mail Worms
[26] Simple Mail Transfer Protocol

مزایای استفاده از فایروال سخت‌افزاری

- حفاظت بیشتر و کلی‌تری نسبت به فایروال‌های نرم‌افزاری دارند
- کل شبکه را محافظت می‌کنند
- تا زمانی که در سیستم اجرا نشده‌اند، هیچ تاثیری بر روی عملکرد سیستم ندارند.
- این نوع فایروال‌ها،به صورت مستقل از سیستم‌عامل و نرم‌افزارهای سیستم عمل می‌کندو دارای سیستم‌عامل جدایی هستند.

معایب استفاده از فایروال سخت‌افزاری

- هزینه بیشتری نسبت به فایروال‌های نرم‌افزاری دارند،حتی با وجود اینکه به نظر خرید یک فایروال سخت‌افزاری کم هزینه‌تر از خرید چند فایروال نرم‌افزاری در یک شبکه بزرگ است.
- جاگیر و کابل‌کشی پیچیده دارد.
- فایروال‌های سخت‌افزاری،با مودم‌های Dial up کار نمی‌کنند
- نصب و upgrade کردن آن دشوار است.

مزایای استفاده از فایروال نرم‌افزاری

- این نوع فایروال‌ها،برای کامپیوترهای شخصی استفاده می‌شوند و در نتیجه بر روی هر سیستم‌عاملی کار می‌کنند.
- به صورت مستقل و جداگانه و کامل قابل نصب هستند و نیاز به بسته یا دستور خاصی ندارند.
- معمولاً همراه بسته نرم‌افزاری آن، آنتی ویروس و آنتی اسپم هم هست.
- به راحتی upgrade می‌شوند.

معایب استفاده از فایروال نرم‌افزاری

- برای هر کامپیوتر موجود در شبکه، نیاز به نصب جداگانه‌ای دارد در نتیجه زمان‌بر است
- گاهی un-install کردن کامل آن دشوار است.
- در زمانی که زمان پاسخ‌گویی سیستم بحرانی و مهم است، مناسب نیستند.
- اشغال کردن فضای CPU و memory

برتری فایروال سخت‌افزاری به فایروال نرم‌افزاری

- سرعت: فایروال‌های سخت‌افزاری برای پاسخ‌گویی سریعتر طراحی شده‌اند و از اینرو در کنترل بار ترافیکی شبکه و جایی که زمان پاسخ‌گویی اهمیت دارد استفاده می‌شوند.
- امنیت: فایروال‌های سخت‌افزاری به دلیل داشتن سیستم‌عامل جدا،کمتر از فایروال‌های نرم‌افزاری در معرض توجه نفوذگران قرار می‌گیرند.از طرفی دارای کنترل‌کننده‌های بسیار قوی است.
- بدون مداخله:[۲۷] این فایروال،به دلیل جدا بودن از نودهای شبکه مدیریت بهتر و آسان‌تری دارد و تاثیری بر کند یا تند کردن بقیه قسمت‌ها ندارد. به راحتی و جدا از سیستم می‌تواند خاموش،یا ذوباره نصب شود بدون هیچ تداخلی در شبکه.

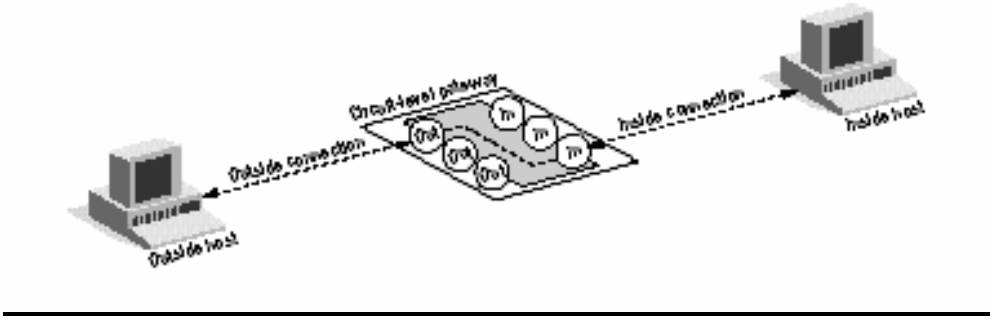
برتری فایروال نرم‌افزاری به فایروال سخت‌افزاری

- هزینه: هزینه کمتری نسبت به فایروال‌های سخت‌افزاری دارد.
- جاگیر نیست و هیچ‌گونه کابل‌کشی ندارد
- با مودم‌های dialup نیز کار می‌کند.
- نصب و راه‌اندازی آن نیاز به دانش خاصی ندارد.

همانطور که اشاره کردیم نوع دیگری تقسیم‌بندی فایروال‌ها را نیر داریم که در این تقسیم‌بندی، فایروال‌های سخت‌افزرای به ۵ دسته تقسیم می‌شوند.این تقسیم‌بندی بر اساس کارکرد و سطح امنیتی فایروال در نظر گرفته شده است:

۱. **فایروال‌های سطح مدار**[۲۸] این فایروال‌ها به عنوان یک رله 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 بسته های 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.

[27] No Interface
[28] Circuit-LeveL



۲. **فایروال‌های پروکسی سرور** فایروال‌های پروکسی سرور به بررسی بسته‌های اطلاعات در لایه کاربرد می‌پردازد. 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 برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین 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 کند، 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.

۳. **فیلترهای Nosstateful packet** این فیلترها روش کار ساده ای دارند. آنها بر مسیر یک شبکه می‌نشینند و با استفاده از مجموعه‌ای از قواعد ، به بعضی بسته‌ها اجازه عبور می‌دهند و بعضی دیگر را بلاک می‌کنند. این تصمیم‌ها با توجه به اطلاعات آدرس‌دهی موجود در پروتکل‌های لایه شبکه مانند IP.. 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 پروکسی ها عمل نمی‌کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند.

۴. **فیلترهای Stateful Packet** این فیلترها بسیار باهوشتر از فیلترهای ساده هستند. آنها تقریباً تمامی ترافیک ورودی را بلاک می کنند 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 شبکه های مدرن هستند.این فیلترها می‌توانند رد پای اطلاعات مختلف را از طریق بسته‌هایی که در حال عبورند ثبت کنند. برای مثال شماره پورت های 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 می‌توانندداعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

۵. **فایروالهای شخصی** فایروال‌های شخصی ، فایروال‌هایی هستند که بر روی رایانه های شخصی نصب می‌شوند.آنها برای مقابله با حملات شبکه ای طراحی شده اند. 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. معمولاً نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست

موقعیت یابی برای فایروال

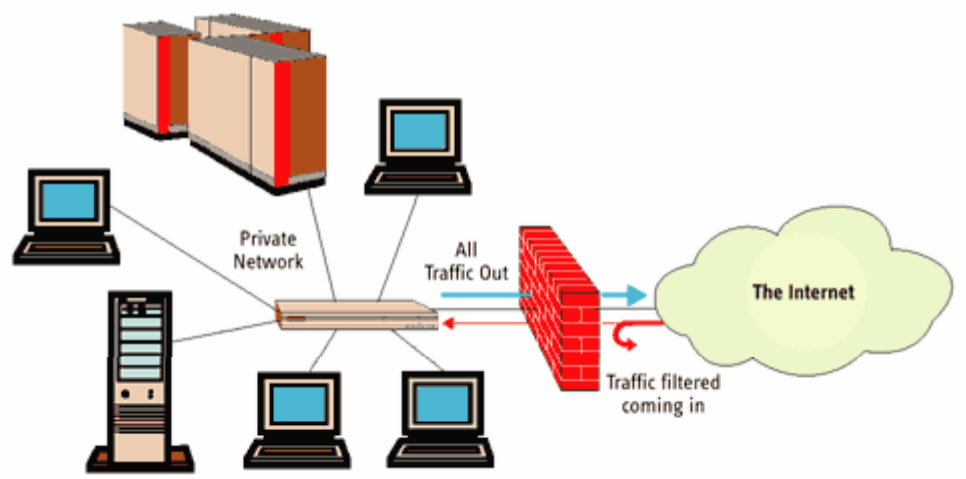
محل و موقعیت نصب فایروال همانند انتخاب نوع صحیح فایروال و پیکربندی کامل آن ، از اهمیت ویژه ای برخوردار است. نکاتی که باید برای یافتن جای مناسب نصب فایروال در نظر گرفت عبارتند از :

۱. **موقعیت و محل نصب از لحاظ توپولوژیکی** معمولاً 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.

۲. **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 وتنظیم 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.

۳. **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.

۴. **فایروالهای لایه‌ای** در شبکه های با درجه امنیتی بالا بهتر است از دو یا چند فایروال در مسیر قرار گیرند. اگر اولی با مشکلی روبرو شود، دومی به کار ادامه می‌دهد.معمولاً بهتر است دو یا چند فایروال مورد استفاده از شرکتهای مختلفی باشند تا در صورت وجود یک اشکال نرم افزاری یا حفره امنیتی در یکی از آنها ، سایرین بتوانند امنیت شبکه را تامین کنند. در شکل زیر این روند مشاهده می‌شود.



متناسب ساختن فایروال

فایروال‌ها قابل تنظیم متناسب با نیازهای کاربران می‌باشند. این بدان معنی است که کاربر می‌توانید فیلترهایی را بر اساس شرایط مختلف اضافه یا حذف نمائید. برخی از این‌ها عبارتند از:

۱. **آدرس‌های IP** به هر دستگاه در اینترنت یک آدرس منحصر به فرد به نام آدرس IP تخصیص داده می‌شود. آدرس‌های IP اعداد ۳۲بیتی هستند که معمولاً بصورت چهار بایت به شکل اعداد دهدهی نقطه دار بیان می‌گردد. یک آدرس IP نمونه شبیه به این می باشد .64,236,16,52 :به عنوان مثال اگر یک آدرس IP معین خارج از شرکت در حال خواندن فایل‌های بسیار زیادی از یک سرور باشد، فایروال می‌تواند تمام ترافیک را از یا به آن آدرس IP مسدود نماید.

۲. **نام‌های دامنه** از آنجا که به یاد آوری رشته ای از اعداد که آدرس IP را درست می‌کنند ، سخت می‌باشد و آدرس‌های IPگاهی نیاز به تغییر دارند ، تمام سرورها در اینترنت همچنین دارای نام‌های قابل خواندن توسط بشر به نام‌های دامنه[۲۹] می‌باشند. به عنوان مثال برای اغلب ما یادآوری www.goole.com راحتتر از 69,254,15,25 می‌باشد. یک شرکت ممکن است تمام دسترسی‌ها به نام‌های دامنه خاصی را ببندد یا فقط دسترسی به نام‌های دامنه خاصی را اجازه دهد.

۳. **پروتکل‌ها** پروتکل روش از پیش تایین شده است که کسی که می‌خواهد از سرویسی استفاده نماید، بوسیله آن با آن صحبت می‌نماید. این کس می‌تواند یک شخص باشد اما در اغلب اوقات یک برنامه کامپیوتری شبیه یک browser وب است. پروتکل‌ها غالباً متن هستند و بسادگی توصیف می‌کنند که سرویس گیرنده[۳۰] و سرویس دهنده[۳۱] مکالماتشان را چگونه خواهند داشـــت ، http پروتکل وب می‌باشد . برخی از پروتکل‌های متداول را که می‌توانید فیلترهای فایروال را جهت آنها تنظیم نمائید در زیر نام برده شده است:

[29] domain names
[30] client
[31] server

www.Prozhe.com

- **IP**[32] پروتکل اینترنت – سیستم اصلی تحویل اطلاعات روی اینترنت
- **TCP** [۳۳] پروتکل کنترل ارسال–جهت شکستن و بازسازی اطلاعاتی که روی اینترنت در حال گردش هستند ، استفاده می‌گردد.
- **HTTP**[34] پروتکل انتقال ابر متن– جهات صفحات وب استفاده می‌شود
- UDP [۳۵] پروتکل ثبت داده‌های کاربر
- FTP [۳۶] پروتکل انتقال فایل
- ICMP [۳۷] پروتکل کنترل پیام اینترنت– بوسیله یک روترجهت تبادل اطلاعات با روتر های دیگر استفاده می‌گردد.
- **SMTP** [۳۸] پروتکل حمل پست ساده– برای ارسال اطلاعات متنی
- **SNMP**[۳۹] پروتکل مدیریت شبکه ساده

۴. **پورت‌ها** هر دستگاه سرور ، سرویسهایش را در اینترنت با استفاده از پورت‌های شماره گذاری شده ، یک پورت برای هر سرویس که در سرور موجود است ، فراهم می‌سازد. به عنوان مثال ، اگر یک سرور در حال اجرای یک سرور وب (HTTP)ویک سرور (FTP)باشد، سرور وب نوعاً در پورت ۸۰ وسرور FTP در پورت ۲۱ در دسترس خواهد بود. یک شرکت ممکن است دسترسی به پورت۲۱ را درتمام دستگاهای داخل شرکت بجز یکی ببندد.

۵. **کلمات و عبارات خاص** این می‌تواند هر چیزی باشد. فایروال هر بسته از اطلاعات را برای مطابقت دقیق متنی که در فیلتر لیست شده، جستجو می‌کند مثلاً می‌توانید به فایروال بگوئید هر بسته‌ای که در آن کلمه "x-rated" باشد را منع نماید. نکته کلیدی اینجاست که این مطابقت باید دقیق باشد، فیلتر "x rated" ، "x-rated" را نخواهد فهمید.اماشما می‌توانید کلمات ، عبارات وگونه های مختلف آنها را تا حد ی که نیاز دارید ، بگنجانید

[32] Internet Protocol
[33] Transmission Control Protocol
[34] Hyper Text Transfer Protocol
[35] User Datagram Protocol
[36] File Transfer Protocol
[37] Internet Control Message Protocol
[38] Simple mail transport protocol
[39] Simple Network Management protocol

نحوه انتخاب یک فایروال

فایروال‌ها اطلاعات دریافتی از اینترنت و یا ارسالی بر روی اینترنت را بررسی نموده و در صورتی که اطلاعات دریافتی از منابع غیرایمن و خطرناک باشد، آنان را شناسائی و حذف می نمایند. در صورتی که یک فایروال به درستی پیکربندی گردد، مهاجمانی که تلاشی مستمر به منظور شناسائی کامپیوترهای حفاظت نشده و آسیب پذیر را انجام می‌دهند در ماموریت خود با شکست مواجه خواهند شد.

فایروال‌های موجود را می توان به سه گروه اساسی تقسیم نمود که هر یک دارای مزایا و معایب مختص به خود می‌باشند. اولین مرحله برای انتخاب یک فایروال، بررسی و تشخیص فایروالی است که با اهداف و خواسته شما به درستی مطابقت می‌نماید. در این رابطه از سه گزینه متفاوت می توان استفاده نمود:

۱. فایروال های نرم افزاری
۲. روترهای سخت افزاری
۳. روترهای بدون کابل

در زمان انتخاب یک فایروال سوالات متعددی مطرح می‌گردد که پاسخ به برخی از آنان دارای اولویت بیشتری است :
- چه تعداد کامپیوتر می‌بایست از فایروال استفاده نمایند ؟
- از چه نوع سیستم عاملی استفاده می‌گردد؟ (ویندوز، یونیکس، لینوکس...)

چگونگی کارکرد فایروال در یک نگاه کلی

فایروال سیستمی سخت افزاری یا نرم افزاری است که بین کامپیوتر شما یا یک شبکه LAN و شبکه بیرونی (مثلا اینترنت) قرار گرفته و ضمن نظارت بر دسترسی به منابع resource سیستم ، در تمام سطوح ورود و خروج اطلاعات را تحت نظر دارد. هر سازمان یا نهادی که بخواهد ورود و خروج اطلاعات شبکه خود را کنترل کند موظف است تمام ارتباطات مستقیم شبکه خود را با دنیای خارج قطع نموده و هر گونه ارتباط خارجی از طریق یک دروازه که فایروالیا فیلتر نام دارد ، انجام شود.

قبل از تحلیل اجزای فایروال عملکرد کلی و مشکلات استفاده از فایروال را بررسی می‌کنیم.

بسته های TCP و IP قبل از ورود یا خروج به شبکه ابتدا وارد فایروال می‌شوند و منتظر می‌مانند تا طبق معیارهای حفاظتی و امنیتی پردازش شوند. پس از پردازش و تحلیل بسته سه حالت ممکن است اتفاق بیفتد:

۱. اجازه عبور بسته صادر می‌شود[40]
۲. بسته حذف می‌شود[41]

[40] Accept Mode
[41] Blocking Mode

۳. بسته حذف شده و پاسخ مناسب به مبدا آن بسته داده شود[42]

غیر از حذف بسته می‌توان عملیاتی نظیر ثبت ، اخطار، ردگیری، جلوگیری از ادامه استفاده از شبکه و توبیخ هم در نظر گرفت.

به مجموعه قواعد فایروال سیاست‌های امنیتی نیز گفته می‌شود. همانطور که همه جا عملیات ایست و بازرسی وقتگیر و اعصاب خرد کن است فایروال هم بعنوان یک گلوگاه می‌تواند منجر به بالا رفتن ترافیک ، تاخیر، ازدحام و نهایتاً بن بست در شبکه شود. یعنی بسته ها آنقدر در پشت فایروال معطل می‌مانند تا زمان طول عمرشان به اتمام رسیده و فرستنده مجبور می‌شود مجددا اقدام به ارسال آنها کند و این کار متناوباً تکرار می‌گردد. به همین دلیل فایروال نیاز به طراحی صحیح و دقیق دارد تا کمترین تاخیر را در اطلاعات امن و صحیح ایجاد نماید. تاخیر در فایروالاجتناب ناپذیر است و فقط باید به گونه‌ای باشد که بحران ایجاد نکند.

از آنجایی که معماری شبکه به صورت لایه لایه است ، در مدل TCP/IP برای انتقال یک واحد اطلاعات از لایه چهارم بر روی شبکه باید تمام لایه‌ها را بگذراند، هر لایه برای انجام وظیفه خود تعدادی فیلد مشخص به ابتدای بسته اطلاعاتی اضافه کرده و آنرا تحویل لایه پایین‌تر می‌دهد. قسمت اعظم کار یک فایروال تحلیل فیلدهای اضافه شده در هر لایه و header هر بسته می‌باشد

سیاست امنیتی یک شبکه مجموعه‌ای متناهی از قواعد امنیتی است که بنابر ماهیتشان در یکی از لایه های فایروال تعریف می‌شوند:

۱. قواعد تعیین بسته های ممنوع (بسته های سیاه) در اولین لایه از دیوار آتش
۲. قواعد بستن برخی از پورتها متعلق به سرویسهایی مثل Telnet یا FTP در لایه دوم
۳. قواعد تحلیل header متن یک نامه الکترونیکی یا صفحه وب در لایه سوم

- **لایه اول فایروال**

لایه اول فایروال بر اساس تحلیل بسته IP و فیلدهای header این بسته کار می‌کند و در این بسته فیلدهای زیر قابل نظارت و بررسی هستند:

۱. آدرس مبدا : برخی از ماشین‌های داخل و یا خارج شبکه با آدرس IP خاص حق ارسال بسته نداشته باشند و بسته‌های آنها به محض ورود به فایروال حذف شود.
۲. آدرس مقصد : برخی از ماشین‌های داخل و یا خارج شبکه با آدرس IP خاص حق دریافت بسته نداشته باشند و بسته های آنها به محض ورود به فایروال حذف شود. (آدرس های IP غیر مجاز توسط مسئول فایروال تعریف می‌شود)
۳. شماره شناسایی یک دیتاگرام قطعه قطعه شده[43] : بسته‌هایی که قطعه قطعه شده اند یا متعلق به یک دیتاگرام خاص هستند باید حذف شوند.

[42] Response Mode
[43] Identifier & Fragment Offset

www.Prozhe.com

٤. شماره پروتکل : بسته‌هایی که متعلق به پروتکل خاصی در لایه بالاتر هستند می‌توانند حذف شوند. یعنی بررسی اینکه بسته متعلق به چه پروتکلی است و آیا تحویل به آن پروتکل مجاز است یا خیر؟
٥. زمان حیات بسته : بسته‌هایی که بیش از تعداد مشخصی مسیریاب را طی کرده اند مشکوک هستند و باید حذف شوند.
٦. بقیه فیلدها بنابر صلاحدید و قواعد امنیتی مسئول فایروال قابل بررسی هستند.

مهمترین خصوصیت لایه اول از فایروال آنست که در این لایه بسته ها بطور مجزا و مستقل از هم بررسی می‌شوند و هیچ نیازی به نگه داشتن بسته های قبلی یا بعدی یک بسته نیست. بهمین دلیل ساده‌ترین و سریع‌ترین تصمیم گیری در این لایه انجام می‌شود. امروزه برخی مسیریابها با امکان لایه اول فایروال به بازار عرضه میشوند یعنی به غیر از مسیریابی وظیفه لایه اول یک فایروال را هم انجام می‌دهند که به آنها مسیریابهای فیلترکننده بسته [44] گفته می‌شود. بنابراین مسیریاب قبل از اقدام به مسیریابی بر اساس جدولی بسته های IP را غربال می‌کند و تنظیم این جدول بر اساس نظر مسئول شبکه و برخی قواعد امنیتی انجام می‌گیرد.

با توجه به سریع بودن این لایه هرچه درصد قواعد امنیتی در این لایه دقیقتر و سخت‌گیرانه‌تر باشند حجم پردازش در لایه های بالاتر کمتر و در عین حال احتمال نفوذ پایین تر خواهد بود ولی در مجموع بخاطر تنوع میلیاردی آدرسهای IP نفوذ از این لایه با آدرسهای جعلی یا قرضی امکان پذیر خواهد بود و این ضعف در لایه های بالاتر باید جبران شود.

- **لایه دوم فایروال:**

در این لایه از فیلدهای header لایه انتقال برای تحلیل بسته استفاده می‌شودعمومی‌ترین فیلدهای بسته های لایه انتقال جهت بازرسی در فایروال عبارتند از:

١. شماره پورت پروسه مبدا و مقصد : با توجه به آنکه پورت‌های استاندارد شناخته شده هستند ممکن است مسئول یک فایروال بخواهد سرویس ftp فقط در محیط شبکه محلی امکان پذیر باشد و برای تمام ماشین‌های خارجی این امکان وجود نداشته باشد. بنابراین فایروال می‌تواند بسته های TCP با شماره پورت های ٢٠ و ٢١ مربوط به ftp که قصد ورود و خروج از شبکه را دارند ، حذف کند. یکی دیگر از سرویس‌های خطرناک که ممکن است مورد سو استفاده قرار گیرد Telnet است که می‌توان به راحتی پورت ٢٣ را مسدود کرد. یعنی بسته‌هایی که مقصدشان شماره پورت ٢٣ است حذف شوند.
٢. فیلد شماره ترتیب و فیلد[45] : این دو فیلد نیز بنا بر قواعد تعریف شده توسط مسئول شبکه قابل استفاده هستند.
٣. کدهای کنترلی [46]: فایروال با بررسی این کدها ، به ماهیت آن بسته پی برده و سیاست‌های لازم را بر روی آن اعمال می‌کند. بعنوان مثال یک دیوار آتش ممکن است بگونه ای تنظیم شود که تمام بسته هایی که از بیرون به شبکه وارد می‌شوند و دارای بیت SYN=1 هستند را حذف کند. بدین ترتیب هیچ ارتباط TCP از بیرون به درون شبکه برقرار نخواهد شد

[44] Pocket Filtering Router
[45] Acknowledgment
[46] TCP code Bits

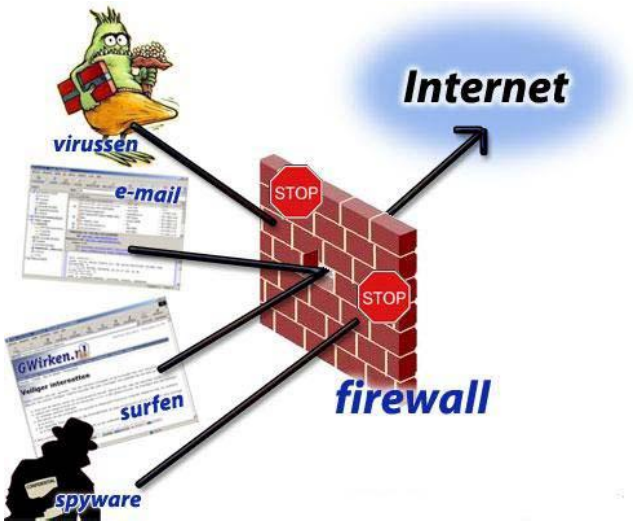
www.Prozhe.com

از مهمترین خصوصیات این لایه آنست که تمام تقاضا های برقراری ارتباط TCP بایستی از این لایه بگذرد و چون در ارتباط TCP ، تا مراحل " سه گانه اش "به اتمام نرسد انتقال داده امکان پذیر نیست لذا قبل از هر گونه مبادله داده فایروال می‌تواند مانع برقراری هر ارتباط غیر مجاز شود. یعنی فایروال می‌تواند تقاضاهای برقراری ارتباط TCP را قبل از ارائه به ماشین مقصد بررسی نموده و در صورت قابل اطمینان نبودن مانع از برقراری ارتباط گردد .فایروال این لایه نیاز به جدولی از شماره پورت‌های غیر مجاز دارد.

- **لایه سوم فایروال:**

در این لایه حفاظت بر اساس نوع سرویس و برنامه کاربردی انجام می‌شود. یعنی با در نظر گرفتن پروتکل در لایه چهارم به تحلیل داده ها میپردازد. تعداد header ها در این لایه بسته به نوع سرویس بسیار متنوع و فراوان است .بنابراین در لایه سوم فایروال برای هر سرویس مجزا (مانند وب، پست الکترونیک و...) باید یک سلسله پردازش و قواعد امنیتی مجزا تعریف شود و به همین دلیل حجم و پیچیدگی پردازش ها در لایه سوم زیاد است. توصیه موکد آنست که تمام سرویسهای غیر ضروری و شماره پورتهایی که مورد استفاده نیستند در لایه دوم مسدود شوند تا کار در لایه سوم کمتر باشد.

آنچه فایروال‌ها سیستم را از آن محافظت می‌نمایند



شاید این سوال مطرح باشد که یک مهاجم قادر به انجام چه کاری خواهد بود و یا اصطلاحاً شعاع میدان تخریب وی به چه میزان است و چه اطلاعاتی در معرض تهدید و یا آسیب قرار خواهند گرفت؟ پاسخ به سوال فوق به نوع و ماهیت تهاجم بستگی دارد. با این که برخی از حملات صرفاً در حد و اندازه یک مزاحمت و یا شوخی ساده می‌باشد ولی برخی دیگر با اهداف کاملاً مخرب طراحی و پیاده سازی می‌گردند. در چنین مواردی، مهاجمان سعی می‌نمایند که به اطلاعات، آسیب رسانده و آنان را حذف نموده و حتی اقدام به سرقت اطلاعات شخصی و حساس نظیر رمزهای عبور و یا شماره کارت های اعتباری نمایند.

برای برخی از مهاجمان، نفوذ به یک کامپیوتر شیرین‌ترین و فراموش نشدنی‌ترین لحظات زندگی شان است! چرا که آنان ماحصل تلاش خود را عملاً مشاهده نموده و از این بابت لذت می‌برند. با استفاده از یک فایروال می‌توان میزان مقاومت سیستم خود را در مقابل این نوع حملات افزایش دهید.

روش‌های زیادی وجود دارد که افراد جهت دسترسی یا سوءاستفاده از کامپیوترهای محافظت نشده بکار می‌برند که در ذیا اشاره شده است :

۱. **ورود به سیستم از راه دور**[۴۷] هنگامیکه افراد قادر به اتصال به کامپیوتر و کنترل آن در برخی از اشکال باشند . این مورد می‌تواند از قادر بودن به مشاهده یا دسترسی فایل‌هایتان تا عملاً اجرای برنامه‌ها روی کامپیوترتان متغیر باشد.

۲. **درهای مخفی برنامه کاربردی**[۴۸] برخی از برنامه‌ها خصوصیات خاصی دارند که اجازه دسترسی از راه دور را می‌دهد . بقیه آنها اشکالاتی دارند که یک در مخفی (backdoor) یا دسترسی نهانی را فراهم می‌سازند، که بعضی از سطوح کنترل برنامه را فراهم می‌سازد.

۳. **دزدیدن ارتباط**[۴۹] متداولترین شیوه ارسال e-mail در اینترنت می‌باشد با استفاده از دسترسی به لیستی از آدرس‌های e-mail ، یک فرد می‌تواندe-mail های آشغال ناخواسته[۵۰] را برای هزاران کاربر ارسال نماید. این کار اغلب اوقات با تغییر دادن مسیر e-mail ها از طریق سرور SMTP برروی یک میزبان که مورد ظن نمی‌باشد، صورت گرفته، ردیابی فرستنده اصلی هرزنامه را مشکل می‌سازد.

٤. **اشکلات سیستم عامل**[۵۱] برخی از سیستم عامل‌ها نیز مشابه با برنامه‌های کاربردی دارای backdoor هستند. انواع دیگر دسترسی از راه دور با کنترل‌های امنیتی نا کافی را فراهم می‌سازد . یا اشکالاتی دارد که یک هکر با تجربه می‌تواند از آنها بهره برداری نماید.

۵. **رد سرویس**[۵۲] شما احتمالاً این اصطلاح را در گزارشات خبری در حملات به وب سایت‌های بزرگ شنیده‌اید مقابله با این نوع حمله تقریباً غیر ممکن است. آنچه اتفاق می‌افتد این است که هکر یک تقاضا به سرور جهت اتصال به آن می‌فرستد . وقتی سرور بایک تاییدیه پاسخ می‌دهد و سعی می‌کند ارتباط را برقرار سازد ، نمی‌تواند سیستمی که این تقاضا را داده است پیدا کند. با مواجه کردن سرور با سیلی از تقاضاهای غیر قابل پاسخ برای ارتباط ، هکر باعث می‌شود سرور تا حد خزیدن کند شده یا سر انجام از کار بیافتد.

٦. **بمب‌های E-mail** یک بمب e-mail معمولاً یک حمله شخصی می‌باشد . در این حمله ، فرد e-mail های یکسان را صدها و هزاران بار برایتان می‌فرستد تا آنکه سیستمe-mail تان دیگر نتواند e-mail بیشتری را بپذیرد.

---

[47] Remote Login
[48] Application Backdoor
[49] SMTP session hijacking
[50] spam
[51] Operating system bugs
[52] Denial of service

۷. **ماکروها**[۵۳] برای آسانتر نمودن رویه‌های پیچیده ، بسیاری از برنامه‌های کاربردی به شما اجازه ایجاد اسکرپتی از فرامین که آن برنامه می‌تواند اجرا کند را می‌دهند .این اسکریپت تحت عنوان ماکرو معروف می‌باشد .هکرها از این ویژگی برای ایجاد ماکروهای خودشان سود می‌جویند که بسته به آن برنامه کاربردی، می‌تواند داده های شما را از بین برده یا کامپیوتر شما را از کار بیاندازد

۸. **ویروس‌ها** احتمالاً شناخته‌ترین تهدید ، ویروس‌های کامپیوتری می‌باشند . یک ویروس برنامه‌ای است که می‌تواند خودش را به کامپیوترهای دیگر کپی کند. با این روش ویروس می‌تواند به سرعت از یک سیستم به سیستم دیگر گسترش یابد. خطر ویروس‌ها از پیغامهای بی ضرر تا پاک کردن تمام فایل‌هایتان ، متغیر می‌باشند.

۹. **هرزنامه**[۵۴] نوعاً بی ضرر اما همواره رنجش آور است؛هرزنامه معادل ااکترونیکی نامه آشغال می‌باشد. اغلب اوقات هرزنامه شامل لینک‌هایی به سایت‌های وب است. باید مراقب بود که بر روی این هرزنامه‌ها کلیک نکرد چون ممکن است تصادفاً یک cookie که یک backdoor را به کامپیوترتان فراهم می‌سازد ، باشد.

۱۰. **تغییر دادن مسیر بمب‌ها**[۵۵] هکرها می‌توانند از ICMP برای تغییر دادن مسیر اطلاعات با ارسال به یک روتر متفاوت استفاده کنند. این یکی از شیوه‌هایی است که با آن حمله رد سرویس صورت می‌گیرد

۱۱. **مسیر یابی مبدأ** [۵۶] در بیشتر موارد مسیری که یک بسته در اینترنت (یا هر شبکه دیگر)گردش می‌کند، بوسیله روترها طول آن مسیر مشخص می‌شود. اما مبدأ فراهم کننده بسته می‌تواند به دلخواه مسیری که بسته باید گردش کند رامشخص نماید. گاهی اوقات هکرها از ابن امر جهت نشان دادن اینکه اطلاعات در ظاهر از یک منبع مطمئن یا حتی از داخل شبکه می‌آیند ، سود می‌جویند!اغلب محصولات فایروال بصورت پیش فرض ، مسیر یابی مبدأ را غیر فعال می‌سازد.

برخی از موارد در لیست فوق برای فیلتر کردن بوسیله فایروال ،اگر نگوئیم غیر ممکن ، مشکل می‌باشند. با وجود آنکه بعضی از فایروال‌ها محافظت در مقابل ویروس را ارائه می‌دهند، نصب نرم افزار ضد ویروس روی کامپیوتر ارزش سرمایه گذاری را دارد. باید توجه داشت، برخی از هرزنامه ها ، مادامیکه پذیرای e-mail هستید قصد رسیدن از طریق فایروال را دارند

سطح امنیتی که برقرار می‌سازید ، تعیین خواهد نمود چه تعداد از این تهدیدات می‌تواند با استفاده از فایروال متوقف گردد. بالاترین سطح امنیت ، بطور ساده مسدود نمودن همه چیز خواهد بود. واضح است این کار هدف از داشتن یک اتصال اینتر نت را خنثی می‌نماید. اما یک قائده سرانگشتی مرسوم ، مسدود نمودن هرچیز، سپس انتخاب انواع ترافیک‌هایی که می خواهید اجازه دهید، می‌باشد .همچنین می‌توان ترافیکی که از طریق فایروال گردش می‌کند را محدود نمائید بطوریکه فقط انواع معینی از اطلاعات از قبیل e-mail بتوانند از این طریق برسند.

[53] Macros
[54] Spam
[55] Redirect bombs
[56] Source routing

www.Prozhe.com

این قاعده خوبی برای بنگاه‌های تجاری می‌باشد که مدیر شبکه با تجربه‌ای که دارد بفهمد چه نیازهایی وجود دارد ودقیقاً بداند چه ترافیکی را اجازه عبور بدهد. احتمالاً برای اغلب کاربران عادی بهتر است با پیش فرض‌های فراهم شده توسط توسعه دهنده فایروال کار کنیم. مگر آنکه دلیل خاصی برای تغییر آنها وجود داشته باشد.

یکی از بهترین راه‌ها برای فایروال‌ها از نقطه نظر امنیتی این است که هر کسی را در بیرون ، از متصل شدن به کامپیوتر در شبکه خصوصی متوقف می‌سازد . در حالی که این موضوع برای بنگاه‌های تجاری مهم می‌باشد ، احتمالاً اغلب شبک های خانگی از این طریق مورد تهدید نخواهند بود. بااین وجود قرار دادن یک فایروال در محل، قدری آرامش فکر را فراهم می‌آورد.

سرورهای Proxy وDMZ

وظیفه‌ای که غالباً با یک فایروال ترکیب می‌گردد، سرور proxy می‌باشد. سرور پراکسی برای دسترسی به صفحات وب بوسیله کامپیوترهای دیگر استفاده می‌گردد. وقتی کامپیوتری تقاضای یک صفحه وب را می‌کند آن صفحه توسط سرور پراکسی دریافت شده وسپس به کامپیوتر متقاضی ارسال می‌گردد. نتیجه اصلی این کار این است که کامپیوتر راه دور که میزبان صفحه وب است، هرگز در تماس مستقیم باچیزی در شبکه خانگی شما بجز سرور پراکسی قرار نمی گیرد

سرورهای پراکسی همچنین می‌توانند باعث عملکرد موثرتر دسترسی اینترنت شما می‌گردند .چنانچه شما به یک صفحه وب در یک سایت وب دسترسی پیدا کنید، آن صفحه معمولاً نباید دوباره از سرور وب بارگیری گردد. در عوض، آن صفحه از سرور پراکسی بارگیری می‌شود.

مواقعی وجود دارد که ممکن است شما بخواهید کاربران راه دور به بخش‌هایی از شبکه شما دسترسی داشته باشند. برخی مثالها در این زمینه عبارتند از:

- سایت وب
- تجارت online
- فضای دریافت و ارسال FTP

در مواردی شبیه به این، ممکن است بخواهید یک DMZ[57] یا - منطقه غیر نظامی ایجاد نمائید. گرچه این کار تا حدی سخت به نظر می‌رسد ، اما در واقع ناحیه‌ای است که بیرون از فایروال قرار دارد DMZ را همچون حیاط جلوی خانه‌تان در نظر بگیرید ، حیاط متعلق به شماست و ممکن است بعضی چیزها را آنجا بگذارید ، اما هر چیز با ارزش را داخل خانه جائیکه به نحو شایسته امن باشد خواهید گذاشت.

نصب یک DMZ بسیار آسان است. اگر چندین کامپیوتر دارید می‌توانید بسادگی یکی از کامپیوترها را برای قرار گرفتن بین اتصال اینترنت وفایروال انتخاب نمائید. اکثر فایروال‌های نرم افزاری موجود به شما اجازه خواهند داد فهرستی در کامپیوتر gateway را به عنوان DMZ تخصیص دهید

[57] Demilitarized Zone

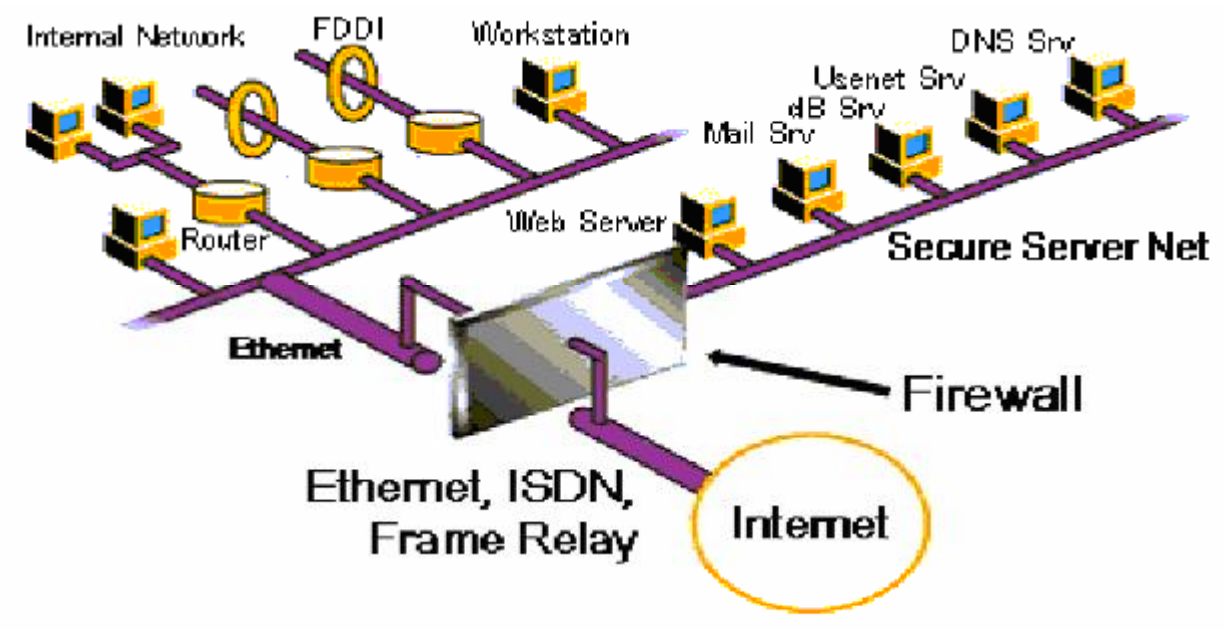
مزایا و معایب استفاده از فایروال

- **مزایا**

۱. ایجاد یک دریچه متمرکز بر روی شبکه که از ورود کاربران عیر مجاز جلوگیری می‌کند.
۲. فایروال برای کامپیوترها، حفاظتی را جهت جلوگیری از ایجاد ترافیک واخطار به کاربران ایجاد می‌کند اما در صورتی که کاربر به این پیغام‌ها توجهی نکند، این کار فایده‌ای ندارد.
۳. فضای منطقی برای گسترش آدرس‌های شبکه-NAT – ایجاد می‌کند. این آدرس‌ها به کم کردن فضای آدرس کمک می‌کنند.
٤. به مدیر شبکه اجازه می‌دهد که از پهنای باند هر یک از کاربران آگاهی داشته باشد و در صورت لزوم به آن‌ها اخطار دهد.

معایب

۱. بسته‌ها و نرم‌افزارهای ویروسی توسط فایروال سخت‌افزاری تشخیص داده نمی‌شوند.
۲. برای فایروال‌های سخت‌افزاری مسئله هزینه و کابل‌کشی و برای فایروال نرم‌افزاری مسدله زمان‌بر بودن و کمبود حافظه مطرح است.
۳. فایروال نمی‌تواند ویروس‌هایی که در میزبان کپی شده را تشخیص و در نتیجه در کل شبکه پخش می‌شود.
٤. فایروال‌های نرم‌افزرای سرعت را پایین می‌آورند.



معرفی برخی از نرم‌افزارهای فایروال جدید و معروف دنیا

۱. ZonAlram pro 2008

در این سری جدید از ZoneAlarm ، لایه‌های مختلف امنیتی به آنتی ویروس اضافه شده که امنیت بیشتری را ایجاد می‌کند.

همچنین شامل سیستم‌عامل جداکانه‌ای ،برنامه شبکه‌ای مجزا برای فایروال است.

این امکانات جدید، باعث مخفی ماندن کاربر از دید کاربران شبکه اینترنت می‌گردد.

۲. Shield Pro FireWall 2008

در این نرم‌افزار، از تکنیک Hauri برای آنتی ویروس استفاده می‌شود. در این تکنیک ویروس‌ها شناسایی و repair می‌شوند و آنتی ویروس را به ۳ قسمت برای ماکرو، اسکریپت و ویندوز تقسیم می‌کند. همچنین inbox را نیز جستجو و هرزنامه‌ها را از بین می‌برد.

۳. Prisma FireWall

اطلاعاتی در مورد ارتباط کاربر با شبکه اینترنت را می‌دهد و لیستی از فعالیت‌های وی و ترافیک شبکه را تهیه می‌کند.

همچنین به کاربر اجازه بستن ارتباط TCP ، و از بین بردن پروسس را می‌دهد.

۴. Panda

محصول آنتی‌ویروس و فایروال ۲۰۰۷ شرکت نرم‌افزاری پاندا که باویستا و همچنین ویندوز اکس پی ٦٤ بیتی سازگار است عرضه شد

آنتی ویروس و فایروال ۲۰۰۷ پاندا دارای قابلیت‌جلوگیری از نفوذ در شبکه‌های وای فای، تشخیص نرم افزارهای مخرب و اسکن ترافیک داخلو خارج از رایانه بوده و سیستم تشخیص نفوذ را کامل می‌کند .

این محصول جدید شرکت پاندا همچنین ازفن‌آوری طراحی شده‌ی ویژه برای محافظت از نرم‌افزارهای مخربی برخوردار است که ازروت کیت استفاده می‌کنند . .

نرم‌افزار پاندا همچنین دارای سیستم مسدود کردنURL های مخرب است که مانع دسترسی کاربران به صفحات وبی می‌شود که برای اجرای حملات فیشینگ طراحی شده‌اند یا حاوی جاسوس‌افزارهایی هستند که عملکرد تهدیدات ترکیبی راراحت‌تر می‌کند .

نرم‌افزار مذکور حفاظت حداکثر، اتوماتیک و دائم دربرابر تمامی انواع نرم افزارهای مخرب و هکرها و همچنین حفاظت اضافی رادر برابر انواع فراوان تهدیدات فراهم می‌کند

حال پس از بحثی کامل در مورد فایروال، مزایا و معایب این سخت/ نرم‌افزار را مطرح و سپس بحثی کوتاه در مورد آنتی فیلتر می‌کنیم.

آنتی فیلتر چیست؟

آنتی فیلترهایی که به صورت معمول برای رد شدن از فایروال‌ها استفاده می شوند مبتنی بر سرورهای proxy می باشند در این حالت که بیشتر برای دریافت http استفاده می‌شود درخواست کننده ، آدرس خود را به سرور proxyمی فرستد سرور صفحه را لود کرده سپس به صورت رمز نگاری شده به درخواست کننده می فرستد . یک فایروال که به طور مثال برای بستن واژه (ترور)پیکربندی شده است دیگر قادر به یافتن چنین واژه ای در صفحه وبی که درخواست شده نمی باشد سایت‌های مختلفی اقدام به ارائه نمودن چنین سرویسی به افراد می‌نمایند که هر کدام بنا به علل مختلفی چون تبلیغات اقدام به اختصاص free proxy برای افراد می‌کنند.

منابع:

۱. www.homenethelp.com/web/howto/free-firewall.asp
۲. http://www.all-internet-security.com/top_10_firewall_software.html
۳. http://networking.anandsoft.com/advantages-of-hardware-firewalls.html
۴. http://www.faqs.org/qa/qa-4838.html
۵. http://www.smallbusinesscomputing.com/webmaster/article.php/3103431
۶. http://personal-firewall-software-review.toptenreviews.com/hardware-firewalls-vs-software-firewalls.html
۷. http://www.webopedia.com/didyouknow/hardwaresoftware/2004/firewall_types.asp
۸. http://www.evaluateit.co.uk/small_business/firewalls.html
۹. http://cms-london.com/articletext.php?id=105
۱۰. http://www.srco.ir/Articles/TipsView.asp?ID=254
۱۱. http://www.alliancedatacom.com/firewall-tutorial.htm
۱۲. http://www.npc-rt.ir/newsdetail-fa-20.html
۱۳. http://fa.wikipedia.org/wiki
۱۴. http://atalebi.com/articles/show.asp?ID=427
۱۵. http://www.iran20.ir/view.asp?id=50005879719100001
۱۶. http://forum.sohail2d.com/viewtopic.php?t=9183
۱۷. http://www.iritn.com/?action=show&type=news&id=7216
۱۸. http://www.microrayaneh.com/Articles/Internet/Firewall2.htm
۱۹. http://www.indstate.edu/ect/ECT680/fall03_papers/Pramod.pdf