دانشکده فنی شهید رجایی قوچان

مطالعه و بررسی عملکرد فایروال های نرم افزاری و سخت افزاری

استاد راهنما : اقای فرجام

گرداورنده: ابراهیم بنفشه

بهار ۱۳۹۲

باسپاس ازسه وجود مقدس:

آنان که ناتوان شدند تا ما به توانایی برسیم...

موهایشان سپید شد تا ما روسفید شویم...

وعاشقانه سوختند تا گرما بخش وجود ما و روشنگر راهمان باشند...

پدرانمان

مادرانمان

استادانمان

چکیده :

اکنون که ما در جهانی زندگی میکنیم که شبکه ها ما را به زندگی در یک دهکده جهانی وادار کرده اند ما باید بتوانیم در و پنجره های شبکه خود را محکم ببندیم. این روزها نگهداری اطلاعات بسیار مهم است و ما باید مراقب خطرات و تهدیدات احتمالی باشیم.

در محیط های علمی و نیمه علمی تا بحث امنیت شبکه پیش می اید فکرها متمرکز دیوار اتش (firewall) می شود. حال این firewall چیست؟ چه کارایی هایی دارد؟ در چه حملاتی از ما محافظت میکند؟ اشنایی با فایروال های نرم افزاری و سخت افزاری و مقایسه ان ها با یکدیگر و ... . این ها چیزهایی است که در این مقاله به اختصار به ان ها اشاره می شود.

فهرست مطالب

عنوان **صفحه**

فصل اول:

انواع فایروال

۱-۱ مقدمه

اتصال به اینترنت بدون استفاده از یک فایروال[۱] 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 downloadکنید، 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

[۱] firewall

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.

۱-۲ 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[۲] نامیده می‌شد در سال ۵۸۹۱ توسط شبکه‌ی عظیم سیسکو[۳] به وجود آمد. سه سال بعد،اولین صفحه‌ی فایروال با موفقیت ایجاد شد،که موسس آن جف موگل[۴] ۴ از شرکت تجهیزات دیجیتالی DEC[۵] بود.با این وجود در طول این سه سال دیو پرستو[۶] وهاوارد تری کی[۷] از شرکت AT&T Bell[۸] Laboratoriesدر حال توسعه ی نسل دوم فایروال‌ها یعنی فایروال‌های دوره ای[۹] بودند.

کار آن ها یک دهه طول کشید،در سال ۰۸۹۱ شروع و در سال ۰۹۹۱ به سرانجام رسید.

در سال‌های۰۹۹۱و۱۹۹۱،بیل چسویک[۱۰] و مارکوس رانوم[۱۱] و ژن اسپافورد[۱۲] صفحاتی را که نسل سوم فایروال‌ها یعنی فایروال‌های لایه‌ای[۱۳] را توصیف می‌کرد، منتشر کردند این نوع فایروال،

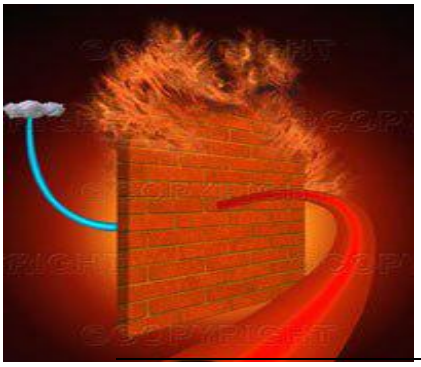
---

[۲] Packet filtering firewalls
[۳] cisco
[۴] Jeff mogul
[۵] Digital equipment corporation
[۶] Dave presetto
[۷] Howard trickey
[۸] این شرکت در سال 1876 توسط گراهام بل تاسیس شد
[۹] Circuit level firewalls
[۱۰] Bill cheswick

فایروال مبتنی بر پروکسی[۱۴] 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 DECاولین فایروال تجاری را منتشر کرد و نام این محصول را "SEAL" گذاشت . Sael . بر اساس کارهای مارکوس رانوم ساخته شده بود . در سال بعد از آن باب باردن[۱۵] و انت دشولان[۱۶] از دانشگاه کالیفرنیای جنوبی شروع به توسعه نسل چهارم فایروال ها کردند که ویزاس[۱۷] نامیده می شد. این سیستم دارای اولین یکپارچگی مجازی[۱۸] و دارای رنگ‌ها و آیکون‌هایی بود . ویزاس اولین نوع فایروال‌های تجاری بود که در سال ۱۹۴۴ توسط شرکت اسرائیلی چک پینت[۱۹] منتشر شد. در سال ۱۹۹۶ اسکات ویگل[۲۰] از شرکت نرم افزارهای جهانی اینترنت[۲۱] شروع به کار بر روی نسل پنجم فایروال ها کرد که معماری با کرنل پروکسی[۲۲] نامیده می شد. 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

۱-۳ فایروال چیست ؟



"اساساً یک فایروال سدی است برای دور نگهداشتن نیروهای

[۱۱] Marcuse ranum
[۱۲] Gene spafford
[۱۳] Application layer firewalls
[۱۴] Proxy – based firewalls
[۱۵] Bob braden
[۱۶] Annette deschlon
[۱۷] visas
[۱۸] Visual integration
[۱۹] Check point software
[۲۰] Scott wiegel
[۲۱] Global internet software group
[۲۲] Kernel proxy architecture

مخرب از دارائی شما.در حقیقت علت اینکه فایروال[۲۳] نامیده می‌شود همین است. کار آن مشابه فایروال فیزیکی است که از گسترش آتش از یک ناحیه به ناحیه دیگرممانعت به عمل می‌آورد."

تعریف فوق، تعریف ساده و عامیانه‌ای از فایروال است. در حقیقت، تا چندسال پیش فقط کسانی که در بانک‌ها، مشاغل تجاری بزرگ و دوایر دولتی کارمی‌کردند، از فایروال استفاده می‌نمودند. اما زمانه به کلی تغییر کرده است .امروزه‌داشتن یک فایروال خوب به اندازه داشتن ضدویروس قوی، مسئله امنیتی مهمی‌حساب 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:

[۲۳] firewall

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.

۱-۴ فایروال چه می کند؟

یک firewall ترافیکی را که بین دو شبکه عبور می کند را امتحان و بررسی می کند تا ببیند آیا ملاقات ها طبق معیارهای خاصی صورت می گیرد یا نه. در واقع بسته های TCP و IP قبل و بعد از ورود به شبکه وارد دیوار آتش می شوند و منتظر می مانند تا طبق معیارهای امنیتی خاصی پردازش شوند حاصل این پردازش احتمال وقوع سه حالت است:

- اجازه عبور بسته داده می شود (Accept Mode)
- بسته حذف می شود (Blocking Mode)
- بسته حذف می شود و پیغام مناسب به مبدا ارسال بسته فرستاده می شود. (Response Mode)

(به غیر از پیغام حذف بسته می توان عملیاتی نظیر اخطار , ردگیری و جلوگیری از ادامه استفاده از شبکه و توبیخ هم در نظر گرفت.)

در حقیقت دیوار اتش محلی است برای ایست و بازرسی بسته های اطلا عاتی به گونه ای که بسته ها بر اساس تابعی از قواعد امنیتی و حفاظتی ، پردازش شده و برای انها مجوز عبور یا عدم عبور صادر شود.اگر P مجموعه ای از بسته های ورودی به سیستم دیوار اتش در نظر گرفته شود و S مجموعه ای متناهی از قواعد امنیتی باشد داریم :

$$X=F(P,S)$$

F تابع عملکرد firewall و X نتیجه بسته (شامل سه حالت , Response,Accept Blocking) خواهد بود.همانطور که همه جا ایست و بازرسی وقت گیر و اعصاب خردکن است firewall نیز می تواند به عنوان یک گلوگاه باعث بالارفتن ترافیک, تأخیر وبن بست در شبکه شود.بن بست زمانی است که بسته ها انقدر در حافظه دیوار اتش معطل می شوندتا طول عمرشان تمام شده و فرستنده اقدام به ارسال مجدد انها کرده و این کار به طور متناوب تکرار شود.به همین دلیل firewall نیاز به طراحی صحیح و دقیق دارد تا از حالت گلوگاهی خارج شود.اابته تاخیر در firewall اجتناب ناپذیر است فقط باید بگونه ای باشد که بحران ایجاد نکند.بیایید داخل پرانتز کمی جزئی تر به این مساله نگاه کنیم،اگر از دیدگاه نظریه صف به یک دیوار آتش یا همان firewall نگاه کنیم میتوان تخمینی از تأخیر تحمیل شده به هر بسته را بدست آورد. معمولا تابع توزیع بسته ها را در شبکه های اطلاعاتی پو آسون در نظر میگیرند.فرض کنید

λn متوسط انتقال بسته IP در واحد زمان از شبکه N به دیوار آتش و m متوسط انتقال بسته در واحد زمان از شبکهM باشد. q را احتمال عبور بسته PM وr را احتمال عبور بسته PN فرض کنید،

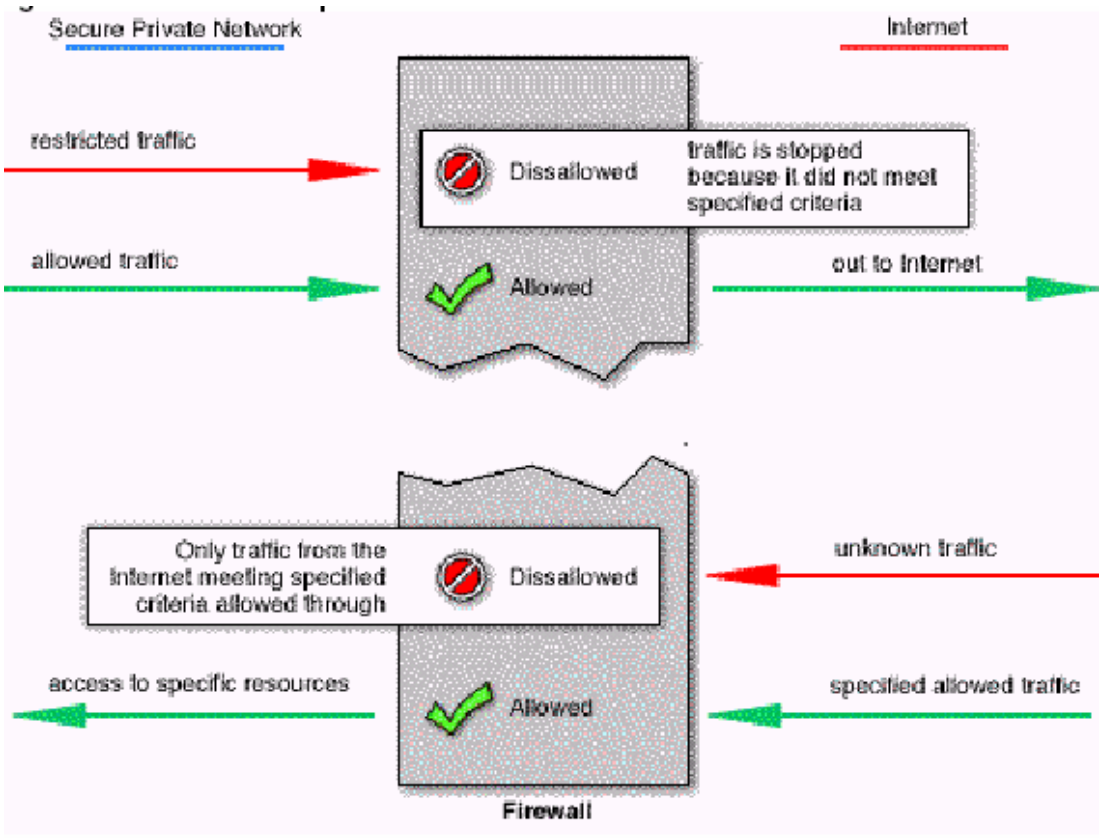
- متوسط بسته های حذف شده =(1-q). λm+(1-r). λn
- متوسط انتقال بسته از دیوار آتش بهM = r.λn
- متوسط انتقال بسته از دیوار آتش به N = q. λm

طبق نظریه صف اگر دیوار آتش بخواهد از نقش گلوگاهی خود بکاهد بایستی به گونهای طراحی شود که نسبت متوسط خروجی بسته ها از دیوار آتش (μ)به ورودی بسته ها (یعنی نسبت μ/λ) تا حد امکان زیاد باشد که این کار منوط به افزایش سرعت پردازش ، داشتن حافظه کافی برای ذخیره بسته های پردازش نشده و هر چه سریعتر کردن تابع تصمیم گیری میباشد.

مشکل زمانی حاد میشود که دیوار آتش مجبور باشد برای تصمیمگیری و اجازه عبور تعدادی از بسته ها را نگه دارد تا تصمیم گیری بر اساس مجموعهای از بسته ها انجام شود این نکته در ادامه آشکارتر خواهد شد.

۱-۵ firewall چگونه کار میکند؟

۲ متدولوژی در firewall استفاده میشود. firewall میتواند به تمام ترافیک اجازه عبور دهدتااینکه به معیار مشخصی برسد یااینکه به هیچ کس اجازه عبور ندهد مگر اینکه به معیار مشخصی برسد.



این معیار ها از یک firewall به firewall دیگر تفاوت می کند. firewall ها می توانند به محتوای داده حساس باشند یا آدرس مبدا و مقصد و شماره پورت و یا... . تصمیم نهایی

در مورد پذیرش یا رد بسته، بستگی به لایه شبکه ای دارد که روی آن کار می کند. firewall ها روی لایه های مختلفی از شبکه سوار می شوند تا معیارهای مختلفی را برای محدود کردن ترافیک بکار برند. همان طور که می دانیم،مدل شبکه OSI ۷ لایه دارد، (لایه ۱: لایه فیزیکی ، لایه ۲: لایه پیوند داده ها ، لایه ۳: لایه شبکه ، لایه ۴: لایه انتقال ، لایه ۵: لایه جلسه ، لایه ۶: لایه ارائه (نمایش) ، لایه ۷: لایه کاربرد)

و مدل شبکه اینترنت (لایه ۱: واسط شبکه ، لایه ۲: لایه شبکه ، لایه ۳: لایه انتقال ، لایه ۴: لایه کاربرد) ، حال مختصر بپردازیم به اینکه firewall چگونه کار می کند.

۱-۶ ضرورت استفاده از دیواره اتش:

به منظور جلوگیری از انجام حملات از میزبان های خارج از شبکه محلی به میزبان ها و کارگذار های داخل ان، استفاده از دیواره اتش ضروری است. این کارگذارها عمدتا به علت استفاده از خدمات ناامن قرارداد TCP/IP در معرض حمله قرار دارند. در یک محیط بدون دیواره اتش ، امنیت شبکه وابسته به امنیت تک تک میزبان های داخل شبکه است و تمام میزبان ها باید برای دستیابی به سطح بالاتری از امنیت در مقایسه با حالت منفرد ، با یکدیگر همکاری کنند. در نتیجه هر چه شبکه محلی بزرگتر و تعداد میزبان های ان بیشتر باشد ، نگهداری از میزبان ها در سطح یکسانی از امنیت مشکل تر می شود. دیواره اتش می تواند با قرار گرفتن در س راه اتصال شبکه داخلی به شبکه سراسری ، امنیت یکسانی را در یک سطح بالا و قابل قبول برای کلیه میزبان های مشترک داخلی تامین کنند.

۱-۷ فایروال ویندوز:

فایروال، ابزار امنیتی مفیدی است که وظیفه کنترل پورت های را بر عهده دارد. فایروال با بستن پورت های غیر ضروری، راه را برای نفوذ گران بسته و از اسکن شدن پورت ها جلوگیری می کند. معمولاً هکرها با اسکن کردن پورت ها پورت های باز را یافته و از طریق آنها اقدام به نفوذ می کنند.

مایکروسافت برای اولین بار، در ویندوز XP، فایروالی قرار داد که علیرغم استقبال کاربران، انتقادهای زیادی را برانگیخت. یکی از این انتقادها، درباره سختی تنظیم این فایروال بود که اغلب کاربران از انجام آن عاجز بودند. انتقاد دیگر، برگشت به غیر فعال بودن آن، به عبارت دیگر، به عبارت دیگر، این فایروال به طور پیش فرض فعال نمی شدو لازم بود کاربر شخصاً آن را فعال کند.

مایکروسافت در SP2، مشکلات قبلی فایروال ویندوز را اصلاح و ابزارهای جدیدی را برای به اشتراک گذاشتن فایل و چاپگر، ترتیب داده است. نسخه اصلاحی شده نسبت به فایروال قبلی، از انعطاف بیشتری برخوردار است. مثلاً در نسخه اصلاحی، امکانی وجود دارد که با فعال کردن آن، فایروال ویندوز راه ورود اطلاعات مشکوک از طریق شبکه های شخصی (مثل شبکه های بی سیم فعال در هتل ها، رستوران ها و غیره) را مسدود می کند.

البته فایروال ویندوز هنور با فایروال های قدرتمندی همچون Symantec, MacAfee فاصله های زیادی دارند و از نظر امکانات نرم افزاری به پای آن ها نمی رسد. اما به هر ترتیب تعبیه ی یک فایروال داخل در ویندوز قدم بزرگی در جهت امنیت این سیستم عامل به شمار می رود و در بسیاری از مواقع راه نفوذ هکرها را می بندد.

همچنین نفوذ یک فایروال از شبکه شما در برابر ترافیک ناخواسته اولیه یک فایروال به این توابع دیگران به کامپیوتر شما حفاظت می کند و ترافیک بد را صورت هستند که اجازه می دهند ترافیک خوب عبور کند دستیابی آن مسدود می کنند! مهمترین قسمت یک فایروال ویژگی

کنترل است که بین ترافیک خوب و بد تمایز قائل می شود آن را نصب می کنند فایروال بین کامپیوتر شما و اینترنت قرار می وقتی فایروال به شما اجازه عبور می دهد صفحات وب را ببینید و به آنها گیرد در .. کنید چت کنید و download باشید، فایل دسترسی داشته حالیکه مطمئن هستید افراد دیگری که در اینترنت مشغول هستند نمی توانند به کامپیوتر شما دست درازی کنند. بعضی از فایروالهای نرم هستند که روی کامپیوتر اجرا می شوند اما فایروالهای دیگر به افزارهایی افزاری ساخته شده اند و کل شبکه را از حمله مصون می صروت سخت کنند.

هر کسی که از اینترنت استفاده می کند باید از بعضی از انواع فایروالها download استفاده کند. برنامه هایی هستند که می توانند از ایتنرنت آسیب پذیر برای IP شوند این برنامه ها می توانند تعداد زیادی آدرسهای شده و اجرا می download نفوذ را پیدا می کنند این برنامه ها به راحتی شوند و برای سوء استفاده یا مشکل دار کردن کامپیوتر شما از طریق این شبکه نیست معمولاً همه انواع فایروالها از برنامه ها احتیاجی به دانش شما در برابر این حملات می کند.

۱-۸ فواید استفاده از دیواره اتش:

۱ ۸ ۱ حفاظت در مقابل خدمات ناامن : دیواره اتش می تواند به عنوان یک صافی برای خدمات اینترنت عمل کند و قراردادهایی را که امنیت شبکه داخلی را به خطر می اندازند ، از شبکه محلی دور نگاه دارد.

۱ ۸ ۲ دسترسی کنترل شده به میزبان های داخلی : با استفاده از دیواره اتش می توان دسترسی به میزبان های داخلی را کنترل و مدیریت کرد. در نتیجه بعضی از میزبان

ها می توانند از خارج از شبکه محلی مورد دسترسی قرار گیرند در حالی که سایر میزبان ها غیرقابل دسترس هستند.

۱ ۸ ۳ امنیت متمرکز : استفاده از دیواره اتش می تواند برای یک سازمان بسیار مقرون به صرفه باشد چون اکثر نرم افزار های امنیتی می توانند به جای این که روی کلیه میزبان های داخلی قرار گیرند ، تنها روی دیواره اتش قرار داده شوند.

۱ ۸ ۴ محرمانگی پیشرفته: منظور از محرمانگی ، دور نگه داشتن کلیه اطلاعات داخلی _ حتی اگر محرمانه به نظر نرسند – از دسترس افراد غیر مجاز می باشد. هر اطلاعاتی که در اهر بی خطر به نظر می رسد ، ممکن است حاوی داده هایی باشد که برای مهاجمان مفید است و می تواند در انجام حملات ان ها را یاری دهد.

۱ ۸ ۵ رویدادنگاری و امارگیری روی میزان استفاده و سوء استفاده از شبکه: با توجه به این که تمامی دسترسی ها از شبکه محلی به اینترنت و بالعکس از دیواره اتش عبور می کنند ، دیواره اتش می تواند ان ها را ثبت کند و امار با ارزشی را درباره ان ها در اختیار سرپرست شبکه قرار دهد.

۱ ۸ ۶ پیاده سازی سیاست های امنیتی سازمان: دیواره اتش روشی برای پیاده سازی اجباری کردن رعایت سیاست های دسترسی به شبکه است.

۱-۹ 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:

۱-۹-۱ 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.

۱-۹-۲ 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 URLو بررسی وقایع ثبت شده را به نرم افزارهای دیگر می‌سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

۱-۹-۳ 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.

۱-۹-۴ 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:

۱-۹-۴-۱ **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

۱-۹-۴-۲ **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

فصل دوم :

انواع فایروال

۲-۱ 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 نرم افزاری 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:

۲-۱-۱ فایروال های سخت افزاری

دیوار اتش سخت افزاری که به انگلیسی به ان Hardware Firewall گفته میشود, اساسا در مودمها یی با باند پهن دیده میشوند و با فیلتر کردن بسته ها اولین خط دفاعی محسوب میشوند.

قبل از اینکه یک بسته اینترنتی به کامپیوتر برسد, دیوار اتش سخت افزاری بسته را کنترل میکند تا بداند از کجا میاید. همچنین این دیوار اتش سخت افزاری ادرس ای پی و هدر انرا چک میکند تا بداند که قابل اطمینان است یا خیر. بعد از این کنترلها, این بسته به کامپیوتر میرسد.

دیوار اتش سخت افزاری تمامی لینکهائی که رفتاری مخربانه دارند را بر اساس تنظیمات خود مسدود میسازد.

این دیوار اتشها معمولا به تنظیمات زیادی نیاز ندارند و اکثر قوانین در انها بکار رفته و از پیش تعیین شده اند و با توجه به این قوانین و یا تنظیمات است که بسته ها فیلتر میشوند.

امروزه فناوری انقدر پیشرفت کرده که فقط این قوانین فیلتراژ بکار نمیروند. در این دیوار اتشها IPS/Intrusion Prevention Systems یا سیستم پیشگیری از رخنه و (IPDS/intrusion detection and prevention systems)یا سیستم یافتن و پیشگیری رخنه ادغام شده و دیگر همانند گذشته جداگانه از انها استفاده نمیشود و به همین دلیل بیشتر میتوانند محافظت کنند.

زمانیکه یکIPDS فعالیتی مخرب را میابد, سیگنالی ارسال کرده و کانکشن را ریست کرده و ادرس ای پی مربوطه را مسدود مینماید. اینکار بر اساس امضاها و امار های غیر طبیعی بودن و انالیز پروتکل انجام میشود. اما اشکال انها در این است که به تمام بسته هائی که خارج میشوند امکان دیدن ملویری را که احیانا وارد سیستم شده و مشغول ارسال داده ها میباشد را میدهد. مطمئنا اگر کاربر امکانش را داشته باشد حتما مانع این امر میشود اما در اکثر موارد کاربر این امکان را ندارد.

دیوار اتشهای سخت افزاری بیشتر به درد صاحبان شرکتهای کوچک و یا متوسط با حداکثر ۵ کامپیوتر میخورند. دلیل انهم بیشتر از نظر اقتصادی است چون اگر قرار باشد این شرکتها لیسانس برنامه های امنیتی اینترنت یعنی دیوار اتشهای نرم افزاری برای ۱۰ تا ۵۰ دستگاه کامپیوتر به اضافه حق اشتراک یکساله را خریداری کنند بسیار پر هزینه تر خواهد بود. علاوه بر این گاهی این امر میتواند مشکل ساز نیز بشود چون کاربران کنترل بیشتری از این نظر روی دستگاه های خود خواهند داشت و ممکن است به کانکشنی که رفتاری مخرب دارد اجازه عبور بدهند و این میتواند منجر به الودگی شبکه و به خطر انداختن شرکت و داده های ان شود. در نتیجه برای این شرکتها این دیوار اتش سخت افزاری میتواند لازم باشد.

قبل از خرید یک دیوار اتش سخت افزاری به چند چیز باید توجه کرد : تعداد کاربران شبکه, تعداد کاربران شبکه وی *ی ان چون دست کم گرفتن و یا اهمیت ندادن به این دو موضوع میتواند کارایی ان را کاهش داده و همچنین روی کانکشن اینترنت نیز تاثیر بگذارد. بعلاوه باید دقت شود که به اندازه کافی لیسانس برای کانکشنهای وی*ی ان و اس اس ال و پی پی تی پی و

غیره موجود باشد و حتی اگر برای ان باید حق اشتراکی پرداخت کرد بهتر است که این حق شتراک را پرداخته و در ازا از اخرین به روز رسانیها برخوردار شد.

اکنون تولید کنندگان در انها انتی ویروس و اسکنر ملویر و فیلتر محتوا نیز بکار میبرند بطوریکه با انها میتوان گفت که امنیت حداکثر است.

به این نوع از فایروال‌ها ، فایروال‌های شبکه نیز گفته می‌شود که بین کامپیوتر ۱. کاربر (و یا شبکه) و کابل و یا خط DsLقرار 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 patchها ، 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 شخصی

۲-۱-۱-۱ مزایای روترهای فایروال:

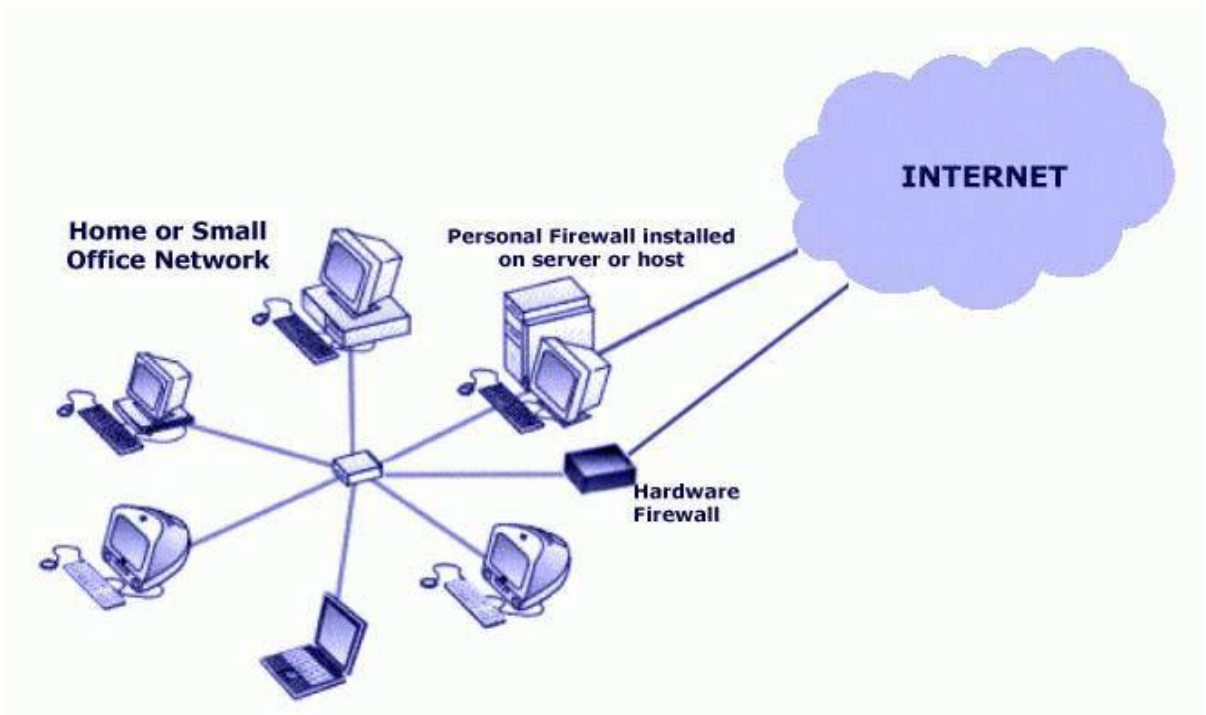
معمولاً دارای حداقل چهار پورت برای اتصال سایر کامپیوترها می‌باشند

امکان حفاظت چندین کامپیوتر را ارائه می‌نمایند

۲-۱-۱-۲ معایب روترهای فایروال:

کابل‌کشی اضافه که مسلماً هزینه‌ای اضافی را نیز در بردارد

فایروال های سخت افزاری ، از تکنیک فیلتر کردن بسته ها[۲۴] 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.



[۲۴] Packet filtering

شکل ۲) محل قرارگیری فایروال سخت‌افزاری در شبکه

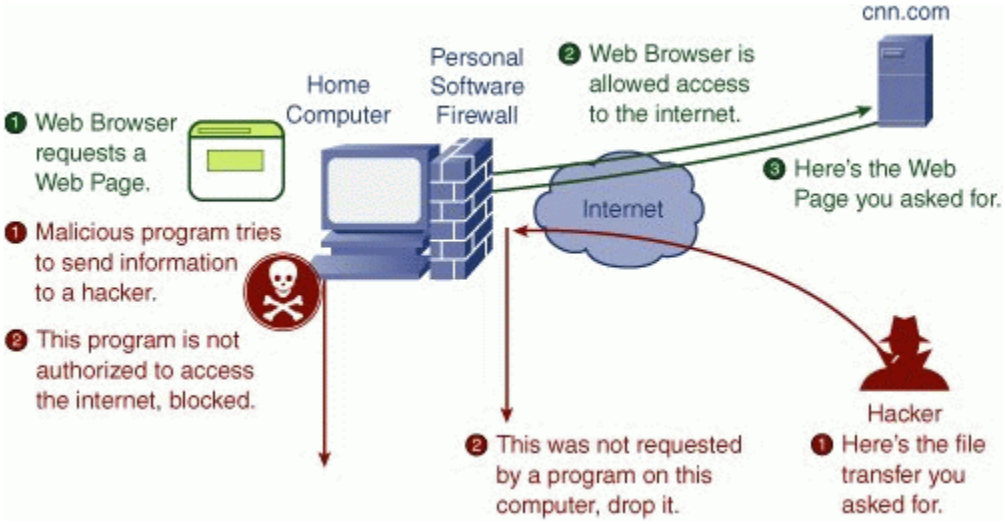
معمولاً این نوع فایروال‌ها به علت داشتن سیستم‌عامل جدایی که دارند، در معرض خطر کمتری از طرف شبکه قرار می‌گیرند و می‌توان مانند یک نود در شبکه یا یک mini Computerبه آن‌ها نگاه کرد.

۲-۱-۲ **فایروال های نرم افزاری** برخی از سیستم‌های عامل ها 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 CDو یا DVDمربوطه استفاده گردد .

اما این نرم افزارهاهر چند که برای امنیت و حفاظت داده ها و کامپیوتر نصب میگردند ولی گاهی بی احتیاطی های خود کاربر و گشودن کانکشنی مخرب میتواند باعث در هم ریختن این امنیت گردد. این امر به دلیل این است که کاربر میتواند تنظیمات انرا به دلخواه تغییر داده و یا کانکشنی را که توسط نرم افزار مسدود گشته و خطرناک تشخیص داده شده را بگشاید.

در غیر اینصورت این دیوار اتشهای نرم افزاری مدام به روز شده و تولید کنندگان سعی میکنند که همیشه انها را به روز نگاهداشته و بیشتر توسعه دهند تا هر چه بیشتر امنیت کامپیوتر و داده های کاربران را حفظ کنند.

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



شکل ۳) چگونگی کار یک فایروال نرم افزاری

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

فایروال‌های نرم افزاری،مانند هر نرم افزار 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 نرم افزار می‌توان جلوی حملات Trojanو کرم‌های E-mail[۲۵]را نیز گرفت و اجازه اجرای دوباره این برنامه‌ها را نمی‌دهد.

بعضی از بسته‌های فایروال‌های نرم افزاری،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 نرم افزاری است!

[۲۵] E – mail worms

در جواب این سوال، E-mail Wormsرا مثال می‌زنیم. برای ارسال ایمیل،همانطور که می‌دانیم از پورت ۲۵ یعنی SMTP[۲۶] استفاده می‌شود. زمانی‌که این ایمیل که حاوی Wormنیز 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.

۲-۱-۲-۱ مزایای استفاده از فایروال سخت‌افزاری

- حفاظت بیشتر و کلی‌تری نسبت به فایروال‌های نرم افزاری 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 نرم افزارهای سیستم عمل می‌کندو دارای سیستم‌عامل جدایی هستند.

۲-۱-۲-۲ معایب استفاده از فایروال سخت‌افزاری

[۲۶] Simple mail transfer protocol

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

۲-۱-۲-۳ مزایای استفاده از فایروال نرم افزاری

- 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 نرم افزاری آن، آنتی ویروس و آنتی اسپم هم هست.
- به راحتی upgradeمی‌شوند.

۲-۱-۲-۴ معایب استفاده از فایروال نرم افزاری

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

- اشغال کردن فضای CPUو memory

۲-۱-۲-۵ برتری فایروال سخت‌افزاری به فایروال نرم افزاری

- ۲-۱-۲-۵-۱ 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.
- ۲-۱-۲-۵-۲ امنیت: فایروال‌های سخت‌افزاری به دلیل داشتن سیستم‌عامل جدا،کمتر از فایروال‌های نرم افزاری در معرض توجه نفوذگران قرار می‌گیرند.از طرفی دارای کنترل‌کننده‌های بسیار قوی است.
- ۲-۱-۲-۵-۳ 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 دوباره نصب شود بدون هیچ تداخلی در شبکه.

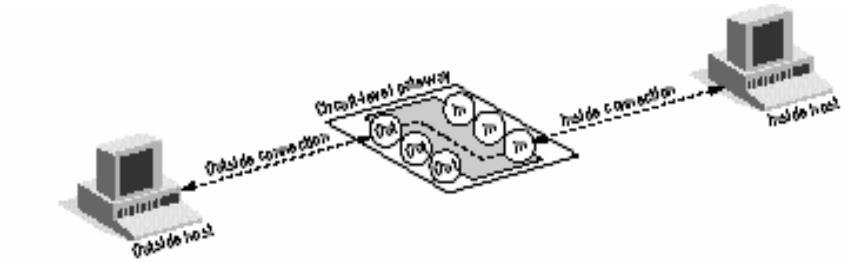
۲-۱-۲-۶ برتری فایروال نرم افزاری به فایروال سخت‌افزاری

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

[۲۷] No interface

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:

۲ ۲ **فایروال های سطح مدار**[۲۸] این فایروال‌ها به عنوان یک رله برای ارتباطات TCPعمل می‌کنند. آنها ارتباط TCPرا 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 (TCPرا نیز نمی‌دهند.



۳ 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

[۲۸] Circuit - level

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.

۴ ۲ **فیلتر های 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.

۵ ۲ **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 TCPو UDPمبدا و مقصد، شماره ترتیب TCP و پرچم‌های .TCPبسیاری از فیلترهای جدید Statefulمی‌توانند پروتکل‌های لایه کاربرد مانند FTPو HTTP را تشخیص دهند و لذا می‌توانندداعمال کنترل دسترسی را با توجه به نیازها و سرعت این پروتکلها انجام دهند.

۲ ۶ **فایروال های 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

۲-۷ 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 :

۲-۷-۱ 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.

۲-۷-۲ 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 DMZقرار 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 ، DMZسرورهای 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.

۲-۷-۳ 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 از شبکه خصوصی از طریق یک فایروال باشد.

۲-۸ 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.

- ### ۲-۸-۱ لایه اول فایروال

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

۲-۸-۱-۱ آدرس مبدا : برخی از ماشین‌های داخل و یا خارج شبکه با آدرس IPخاص حق ارسال بسته نداشته باشند و بسته‌های آنها به محض ورود به فایروال حذف شود.

۲-۸-۱-۲ آدرس مقصد : برخی از ماشین‌های داخل و یا خارج شبکه با آدرس IPخاص حق دریافت بسته نداشته باشند و بسته های آنها به محض ورود به فایروال حذف شود. (آدرس های IPغیر مجاز توسط مسئول فایروال تعریف می‌شود)

۲-۸-۱-۳ شماره شناسایی یک دیتاگرام قطعه قطعه شده[۲۹]: بسته‌هایی که قطعه قطعه شده اند یا متعلق به یک دیتاگرام خاص هستند باید حذف شوند.

۲-۸-۱-۴ 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؟

[۲۹] Identifier & fragment offset

۲-۸-۱-۵زمان حیات بسته : بسته‌هایی که بیش از تعداد مشخصی مسیریاب را طی کرده اند مشکوک هستند و باید حذف شوند.

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[۳۰] گفته می‌شود. بنابراین مسیریاب قبل از اقدام به مسیریابی بر اساس جدولی بسته های IPرا 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.

- **۲-۸-۲ 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:

[۳۰] Pocket filtering router

۲-۸-۲-۱ شماره پورت پروسه مبدا و مقصد : با توجه به آنکه پورت‌های استاندارد شناخته شده هستند ممکن است مسئول یک فایروال بخواهد سرویس ftpفقط در محیط شبکه محلی امکان پذیر باشد و برای تمام ماشین‌های خارجی این امکان وجود نداشته باشد. بنابراین فایروال می‌تواند بسته های TCPبا شماره پورت های ۲۰ و ۲۱ مربوط به ftpکه قصد ورود و خروج از شبکه را دارند ، حذف کند. یکی دیگر از سرویس‌های خطرناک که ممکن است مورد سو استفاده قرار گیرد Telnetاست که می‌توان به راحتی پورت ۲۳ را مسدود کرد. یعنی بسته‌هایی که مقصدشان شماره پورت ۲۳ است حذف شوند.

۲-۸-۲-۲ فیلد شماره ترتیب و فیلد[۳۱] : این دو فیلد نیز بنا بر قواعد تعریف شده توسط مسئول شبکه قابل استفاده هستند.

۲-۸-۲-۳ کدهای کنترلی[۳۲] : 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 ۱= SYNهستند را حذف کند. بدین ترتیب هیچ ارتباط TCPاز بیرون به درون شبکه برقرار نخواهد شد

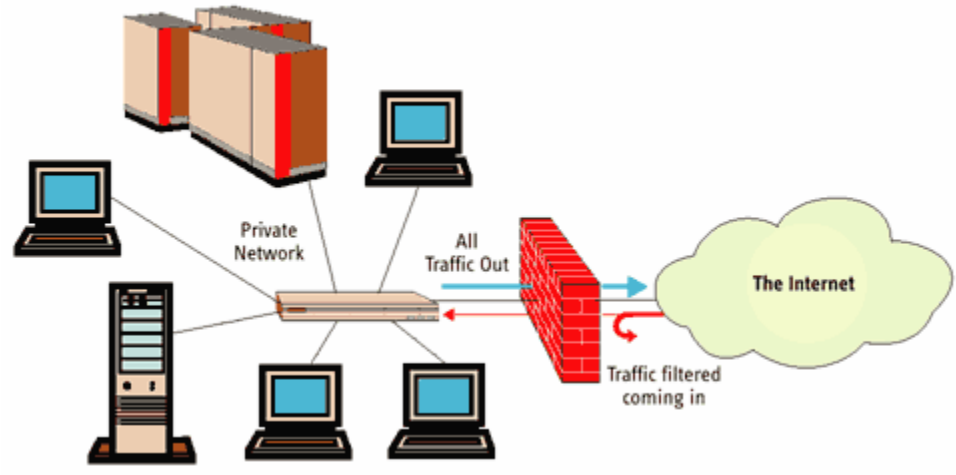
از مهمترین خصوصیات این لایه آنست که تمام تقاضا های برقراری ارتباط TCPبایستی از این لایه بگذرد و چون در ارتباط ، TCPتا مراحل " سه گانه اش "به اتمام نرسد انتقال داده امکان پذیر نیست لذا قبل از هر گونه مبادله داده فایروال می‌تواند مانع برقراری هر ارتباط غیر مجاز شود. یعنی فایروال می‌تواند تقاضاهای برقراری ارتباط TCPرا قبل از ارائه به ماشین مقصد

[۳۱] acknowledgment
[۳۲] Tcp code bits

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.

- **۲-۸-۳ 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 headerها 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.



۲-۹ 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:

۲-۹-۱ ادرس های IP به هر دستگاه در اینترنت یک آدرس منحصر به فرد به نام آدرس IPتخصیص داده می‌شود. آدرس‌های IPاعداد ۳۲بیتی هستند که معمولاً بصورت چهار بایت به شکل اعداد دهدهی نقطه دار بیان می‌گردد. یک آدرس IPنمونه شبیه به این می باشد ۶۴,۲۳۶,۱۶,۵۲ :به عنوان مثال اگر یک آدرس IPمعین خارج از شرکت در حال خواندن فایل‌های بسیار زیادی از یک سرور باشد، فایروال می‌تواند تمام ترافیک را از یا به آن آدرس IPمسدود نماید.

۲-۹-۲ نام‌های دامنه از آنجا که به یاد آوری رشته ای از اعداد که آدرس IPرا 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[۳۳] می‌باشند. به عنوان مثال برای اغلب ما یادآوری www.goole.comراحتتر از ۶۹,۲۵۴,۱۵,۲۵ می‌باشد. یک شرکت ممکن است تمام دسترسی‌ها به نام‌های دامنه خاصی را ببندد یا فقط دسترسی به نام‌های دامنه خاصی را اجازه دهد.

۲-۹-۳ پروتکل ها 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[۳۴] و سرویس دهنده[۳۵] مکالماتشان را چگونه خواهند داشـــت ، httpپروتکل وب می‌باشد . برخی از

[۳۳] Domain names
[۳۴] client
[۳۵] server

پروتکل‌های متداول را که می‌توانید فیلترهای فایروال را جهت آنها تنظیم نمائید در زیر نام برده شده است:

IP[۳۶] پروتکل اینترنت - سیستم اصلی تحویل اطلاعات روی اینترنت

TCP[۳۷] پروتکل کنترل ارسال-جهت شکستن و بازسازی اطلاعاتی که روی اینترنت در حال گردش هستند ، استفاده می‌گردد.

HTTP[۳۸] پروتکل انتقال ابر متن- جهات صفحات وب استفاده می‌شود

UDP[۳۹] پروتکل ثبت داده‌های کاربر

FTP[۴۰] پروتکل انتقال فایل

ICMP[۴۱] پروتکل کنترل پیام اینترنت- بوسیله یک روترجهت تبادل اطلاعات با روتر های دیگر استفاده می‌گردد.

SMTP[۴۲] پروتکل حمل پست ساده- برای ارسال اطلاعات متنی

SNMP[۴۳] پروتکل مدیریت شبکه ساده

---

[۳۶] Internet protocol
[۳۷] Transmission control protocol
[۳۸] Hyper text transfer protocol
[۳۹] User datagram protocol
[۴۰] File transfer protocol
[۴۱] Internet control message protocol
[۴۲] Simple mail transport protocol
[۴۳] Simple network management protocol

۲-۹-۴ **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 پورت۸۰ وسرور FTPدر پورت ۲۱ در دسترس خواهد بود. ببندد. یک شرکت ممکن است دسترسی به پورت۲۱ را درتمام دستگاهای داخل شرکت بجز یکی ببندد.

۲-۹-۵ **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.اما شما می‌توانید کلمات ، عبارات وگونه های مختلف آنها را تا حد ی که نیاز دارید ، بگنجانید

۲-۱۰ 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.

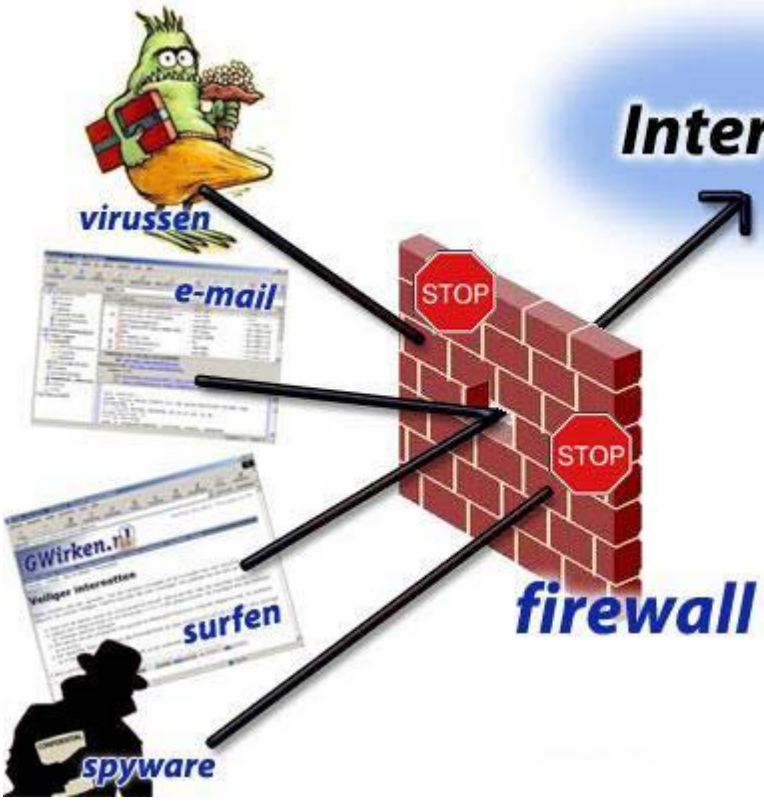
فایروال‌های موجود را می توان به سه گروه اساسی تقسیم نمود که هر یک دارای مزایا و معایب مختص به خود می‌باشند. اولین مرحله برای انتخاب یک فایروال، بررسی و تشخیص فایروالی است که با اهداف و خواسته شما به درستی مطابقت می‌نماید. در این رابطه از سه گزینه متفاوت می توان استفاده نمود:

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...)

۲-۱۱ 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.

۲-۱۲ روش های حمله

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 ذیل اشاره شده است :

۲-۱۲-۱ ورود به سیستم از راه دور[۴۴] 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.

۲-۱۲-۲ در های مخفی برنامه کاربردی[۴۵] برخی از برنامه‌ها خصوصیات خاصی دارند که اجازه دسترسی از راه دور را می‌دهد . بقیه آنها اشکالاتی دارند که یک در مخفی) (backdoorیا دسترسی نهانی را فراهم می‌سازند، که بعضی از سطوح کنترل برنامه را فراهم می‌سازد.

۲-۱۲-۳ دزدیدن ارتباط[۴۶] متداولترین شیوه ارسال e-mailدر اینترنت می‌باشد با استفاده از دسترسی به لیستی از آدرس‌های ، e-mailیک فرد می‌تواندe-mail های آشغال ناخواسته[۴۷] را برای هزاران کاربر ارسال نماید. این کار اغلب

[۴۴] Remote login
[۴۵] Application backdoor
[۴۶] Smtp session hijacking
[۴۷] spam

اوقات با تغییر دادن مسیر e-mailها از طریق سرور SMTPبرروی یک میزبان که مورد ظن نمی‌باشد، صورت گرفته، ردیابی فرستنده اصلی هرزنامه را مشکل می‌سازد.

۲-۱۲-۴ **اشکلات سیستم عامل**[۴۸] برخی از سیستم عامل‌ها نیز مشابه با برنامه‌های کاربردی دارای backdoorهستند. 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.

۲-۱۲-۵ **رد سرویس**[۴۹] 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.

۲-۱۲-۶ **بمب‌های E-mail** یک بمب e-mailمعمولاً یک حمله شخصی می‌باشد . در این حمله ، فرد e-mailهای یکسان را صدها و هزاران بار برایتان می‌فرستد تا آنکه سیستمe-mail تان دیگر نتواند e-mailبیشتری را بپذیرد.

[۴۸] Operation system bugs
[۴۹] Denial of service

۲-۱۲-۷ **ماکروها**[۵۰] 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

۲-۱۲-۸ **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.

۲-۱۲-۹ **هرزنامه**[۵۱] نوعاً بی ضرر اما همواره رنجش آور است؛هرزنامه معادل االکترونیکی 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 cookieکه یک backdoorرا به کامپیوترتان فراهم می‌سازد ، باشد.

۲-۱۲-۱۰ **تغییر دادن مسیر بمب‌ها**[۵۲] هکرها می‌توانند از ICMPبرای 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

۵۰ macros
۵۱ spam
۵۲ Redirect bombs

۲-۱۲-۱۱ **مسیر یابی مبدأ**[۵۳] 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-mailهستید 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-mailبتوانند از این طریق برسند.

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. احتمالاّ برای اغلب کاربران

[۵۳] Source routing

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.

۲-۱۳ سرورهای ProxyوDMZ

وظیفه‌ای که غالباً با یک فایروال ترکیب می‌گردد، سرور proxyمی‌باشد. 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 [۵۴] 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 DMZرا 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 DMZبسیار 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 gatewayرا به عنوان DMZتخصیص دهید

۲-۱۴ مزایا و معایب استفاده از فایروال

- **۲-۱۴ -۱ 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.

[۵۴] Demilitarized zone

۳. فضای منطقی برای گسترش آدرس‌های شبکه -NAT - ایجاد می‌کند. این آدرس‌ها به کم کردن فضای آدرس کمک می‌کنند.

۴. به مدیر شبکه اجازه می‌دهد که از پهنای باند هر یک از کاربران آگاهی داشته باشد و در صورت لزوم به آن‌ها اخطار دهد.

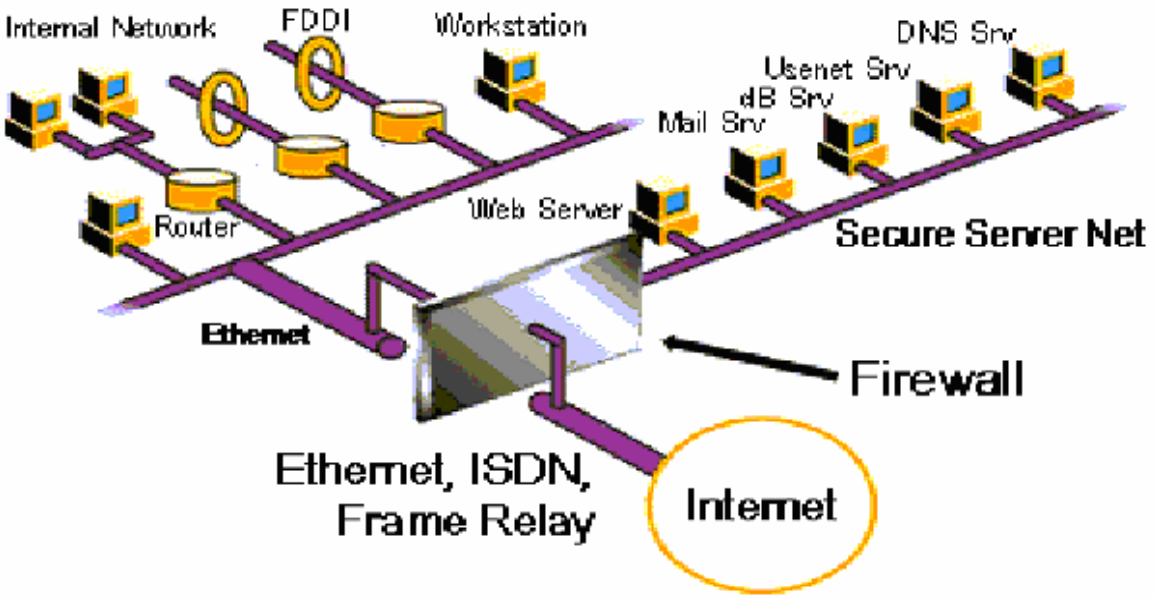
- ۲-۱۴-۲ **معایب**

۱. بسته‌ها و نرم افزارهای ویروسی توسط فایروال سخت‌افزاری تشخیص داده نمی‌شوند.

۲. برای فایروال‌های سخت‌افزاری مسئله هزینه و کابل‌کشی و برای فایروال نرم افزاری 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.

۴. فایروال‌های نرمافزرای سرعت را پایین می‌آورند.



فصل ۳

کاربرد ها و ویژگی های فایروال

۳-۱ کارایی بالا و سرعت:

یکی از مهمتری ویژگی هایی که می توان برای یک فایروال در نظر گرفت، کارایی بالای آن است. فایروال معمولا در محل اتصال شبکه داخلی به شبکه سراسری قرار می گیرد و تنها راه ارتباط شبکه داخلی با شبکه جهانی است. بنابراین تمامی بسته هایی که بین طرفین صافی رد و بدل می شوند، باید از آن عبور کرده و مورد بررسی قرار گیرند. در نتیجه ممکن است فایروال باعث کند شدن سرعت انتقال اطلاعات شود و یک گلوگاه در محل آن ایجاد گردد.

آمارها نشان میدهند که بسیاری از فایروال های موجود، با مشکل پایین بودن کارایی مواجهند. بنابراین یکی از مهمترین پارامترهایی که در طراحی و پیاده سازی سپر در نظر گرفته شده، کارایی بالای آن است، طوریکه بتواند با سرعتی بالا و مورد قبول به تصفیه اتصالات وب بپردازد. برای این منظور تلاش شده است تا عملیات تصفیه URL تا حد امکان در هسته سیستم عامل انجام شود و از سربار اضافی عملیات Context Switching در سیستم عامل جلوگیری شود.

ارزیابی کارایی سپر با استفاده از ابزار استاندارد Specweb و Netperf انجام شده است و سپر در محیط تست Mbps۱۰۰ برای پهنای باند بیش از Mbps۵۰ گلوگاه نشده است. این نتایج نشان از استحکام سپر برای محیط های با پهنای باند بالا (تاحدود Mbps۵۰) را می دهد. همچنین نتایج دقیق ارزیابی کارایی سپر با استفاده از ابزارهای استاندارد برای ارزیابی فایروال ها موجود است.

۳-۲ پیکربندی پیشرفته، انعطاف پذیر، امن و ساده:

سپر با در اختیار گذاشتن واسط کاربری پیشرفته ای امکان مدیریت و تعریف سیاست های امنیتی سازمان را ممکن نموده است. با استفاده از این واسط کاربری که مرکز کنترل و مدیریت سپر نامیده می شود، امکان ایجاد، تغییر و حذف سیاسته های امنیتی توسط یک کانال امن در اختیار مدیر قرار داده شده است. مزیت این روش، سهولت استفاده از انعطاف پذیری بالا، واسط گرافیکی قدرتمند و راهنمای جامع آن می باشد.

این واسط گرافیکی با استفاده از یک کانال امن به سپر وصل شده و تغییرات پیکربندی و سیاست امنیتی را به سپر منتقل می کند. همچنین از این طریق مدیر می تواند وضعیت اتصالات مورد تصفیه را به صورت Online مشاهده نماید. علاوه برای واسط گرافیکی، مدیر میتواند با استفاده یک کانال امن SSH به ماشین سپر وصل شده و عملیات پیکربندی سیستم را از این طریق انجام دهد. با اتصال مدیر به سپر، یک CLI (Command Line Interface) مدیریتی به وی نشان داده می شود که به سادگی می تواند آخرین پیکربندی را مشاهده نموده و تغییرات خود را اعمال نماید.

۳-۳ صفحه نمایش LCD:

یکی از قابلیت های حفاظ سپر، نمایش اطلاعات ترافیک شبکه و وضعیت عمومی سیستم بر روی نمایشگر LCD می باشد. با استفاده از این نمایشگر می توان اطلاعات زیر را مشاهده نمود:

- اطلاعات عمومی راجع به پیکربندی شبکه
- وضعیت حافظه

- وضعیت CPU
- میزان تقاضاهای وب دریافتی
- میزان تقاضاهای وب پذیرفته شده
- میزان تقاضاهای وب رد شده
- میزان اتصالات وب جاری
- زمان بالا بودن سیستم

۳-۴ مشخصات سخت افزاری سپر:

سپر یک حفاظ شبکه ای است که بصورت یک Appliance و قابل نصب در Rack ارائه می شود. جعبه سپر دارای چهار کارت شبکه ۱۰۰۰/۱۰۰/۱۰ Mbps یک نمایشگر LED,LCD های نمایش وضعیت و یک درگاه سریال RS232 می باشد.

۳-۵ نصب در شبکه:

سپر در قالب یک بسته سخت افزاری – نرم افزاری ارائه می گردد و براساس کاربردهای مورد نیاز سازمان ها و با توجه به شرایط محیطی، می توان امکانات و بسترهای نرم افزاری و سخت افزاری آن را تنظیم کرد. با توجه به توپولوژی های مختلف سه حالت برای نصب سپر در نظر گرفته شده است. به عبارت دیگر سپر در یکی از سه حالت زیر در شبکه سازمان قرار می گیرد.

- مسیریاب (Router)
- پل (Bridge)

- Sniffer

زمانی که سپر در حالت Sniffer باشد، ابتدا یک آدرس IP به سپر داده می شود و سپس به Switch وصل خواهد شد و خود اقدام به Sniff کردن و تصفیه بسته ها می‌کند.

در حالتی که سپر به عنوان روتر قرار می گیرد، باید بسته ها به نحوی به سپر هدایت شوند. بنابراین در این شرایط سپر باید مستقیما به روتر سازمان وصل باشد. باید دقت نمود در این حالت اصلا نیازی نیست تا پیکربندی ماشین های داخلی تغییر کند و خود سپر به نحوی عمل می کند که به عنوان روتر برای سازمان نقش داشته باشد.

۳-۶ پایگاه آدرس ها و تصفیه URL:

سپر براساس سیاست های تصفیه وب و پایگاه داده خود از برقراری برخی از اتصالات HTTP جلوگیری می کند. آدرس های موجود در پایگاه آدرس، به صورت موضوعی سامان یافته اند و مدیر سیستم قادر است تا از طریق واسط کاربری مبتنی بر وب، هر یک از موضوعات را برای انجام عمل تصفیه انتخاب کند. در حال حاضر بیش از ۱۵ موضوع مختلف در پایگاه داده موجودند و این در حالی است که مدیر سیستم می تواند آدرس های مورد نیاز را به صورت دستی نیز وارد کند. علاوه بر آن وی قادر است تا الگوهای خاصی را به عنوان کلمات غیرمجاز اعلام کند تا سپر از اتصال کاربران به آدرس هایی که حاوی این نوع کلمات هستند، جلوگیری نماید. قابل توجه این که بعد از تعریف نمودن کلمات (Black List)، سپر از جستجوی این کلمات درموتورهای جستجو نیز جلوگیری می کند. همچنین مدیر می تواند کلمات فارسی را در قالب Unicode به عنوان

Black List وارد نماید و بدین وسیله از جستجوی فارسی در موتورهای جستجو برای کلمات مورد نظر جلوگیری نماید.

همانطور که گفته شد سپر از یک پایگاه داده مرکزی آدرس ها استفاده می کند که دائما در حال بروز شدن است. این پایگاه آدرس ها براساس نوع نیاز کاربر، می تواند روزانه، هفتگی و یا ماهانه به روز درآید. برای به روزرسانی نرم افزارهای صافی شرکت امن افزار(از جمله سپر) سیستم مدیریت مشتریان برای به روز رسانی وجود دارد که به درخواست به روزرسانی صافی ها پاسخ می دهد. همچنین تعدادی روبات نرم افزاری با معماری توزیع شده به صورت تمام وقت در حال جستجو در اینترنت و دسته بندی آدرس های اینترنتی هستند. خروجی این روبات ها به سیستم بروزرسانی داده می شود و این سیستم نیز آخرین نتایج را به صافی ها (از جمله سپر) می رساند.

سیستم دسته بندی اینترنت (کاوا) به طور متوسط پهنای باندی حدود ۲Mbps را در اختیار روبات ها قرار داده است و تا کنون بیش از ۳۵۰میلیون سایت را بررسی نموده است که خروجی این بررسی، دسته بندی بیش از ۴میلیون آدرس اینترنتی در ۱۵ دسته (Category) می باشد. همانطور که گفته شد این سیستم به صورت تمام وقت در حال کار است و به طور میانگین روزانه بیش از ۱۰۰۰۰آدرس اینترنتی را به پایگاه آدرس های دسته بندی شده اضافه می کند.

۳-۷ رویدادنگاری:

یکی از مهمترین نیازهای امنیتی، داشتن سابقه عملیات است. سپر امکان ثبت رویدادها را با جزئی ترین مشخصات بوجود می آورد. سه نوع رویدادنگاری زیر در سپر پشتیبانی می شود.

- رویدادنگاری تصفیه HTTP در سطح اطلاعات لایه کاربرد
- رویدادنگاری بسته صافی حالت مند و ترجمه آدرس در سطح اطلاعات لایه شبکه

- رویدادنگاری بروزرسانی پایگاه آدرس های دسته بندی شده

مدیر سیستم می تواند در هر زمانی بخش مشخصی از رویدادنامه را پاک نماید و یا این که روی کامپیوتر شخصی خود Download کند. همچنین قالب فایل رویدادنامه سپر به نحوی است که توسط نرم افزار Sawmill قابل قبول می باشد. این نرم افزار یک تحلیل گر رویدادنامه (Log Analyzer) است که می تواند رویدادنامه سپر را به عنوان ورودی گرفته و نمودارهای تحلیلی از این رویدادنامه تولید نماید. این نمودارها با سلیقه مدیر قابل بومی شدن هستند.

با توجه به این که رویدادنگاری در سپر مبتنی بر مکانیسم استاندارد syslog انجام می شود، می توان رویدادنامه سپر را بصورت متمرکز و منطبق با دیگر تجهیزات شبکه پیکربندی نمود. در این شرایط می توانید از نرم افزار تحلیل گر رویدادنامه سپر نیز استفاده نمایید. این نرم افزار مبتنی بر وب بوده و نمودارهای تحلیلی از رویدادنامه را تولید می نماید.

۳-۸ نظارت Online:

مدیر با استفاده از رویدادنامه می تواند به صورت Offline سیستم را بازرسی نماید ولی برای نظارت Online مدیر باید بتواند در هر لحظه ای از زمان از راه دور به سیستم وصل شده و اطلاعات نظارتی را مشاهده نماید. برای این منظور در سپر دو نوع نظارت Online وجود دارد. این اطلاعات با استفاده از برنامه واسط گرافیکی (GUI) قابل رویت هستند.

- نظارت بر وضعیت کلان سیستم سپر
- نظارت بر اتصالات در حال تصفیه

در نوع اول اطلاعات سیستمی برای نظارت بر سیستم نمایش داده می شود و این اطلاعات در هر ۵ ثانیه بروز رسانیده می شود. این اطلاعات شامل نمودارهای درصد استفاده از CPU،

حافظه، پهنای باند ورودی و خروجی و آمار اتصالات تصفیه شده و نتایج آنها است. به طور کلی این بخش تنها شامل برخی از اطلاعات آماری است.

نوع دیگر از نظارت، امکان نمایش جزئیات اتصالات در حال تصفیه را می دهد. در این بخش اطلاعات تمامی اتصالات در حال تصفیه هر ۵ثانیه بروز شده و نمایش داده می شود. به ازای هر اتصال آدرس IP مبدا، زمان شروع، نام کاربری، کنش، و URL نشان داده می شود.

۳-۹ امنیت:

سپر به گونه ای ساخته شده که تمامی ارتباطات با آن تنها از طریق کانال های امن ممکن است و امکان حملات کلاسیک در آن از بین رفته است. استفاده از تشخیص هویت و رمز نگاری در مرکز کنترل و مدیریت سپر نمونه ای از این امر می باشد. در صورت لزوم، سپر می تواند بدون داشتن شماره IP بخش های عمده ای از کار خود (ازجمله فیلترینگ وب) را انجام دهد. اهمیت این مساله در آن است که عدم وجود IP، امکان حملات نفوذی را به کلی از بین می برد. همچنین سیستم عامل سپر که بنای آن یک سیستم عامل یونیکسی است، تا حد امکان بومی شده است. این بومی سازی در راستای امن سازی و افزایش کارایی سیستم عامل انجام شده است و تلاش شده تا حد امکان سرویس های اضافی از سیستم عامل حذف شده و به سطح مناسبی از لحاظ امنیتی و کارایی برسد.

۳-۱۰ مقاوم در برابر حملات:

یکی از امکانات اصلی در فایروال ها مقاومت در برابر حملات است. سپر از حملات کلاسیک که در اثر مشکلات قرارداد TCP/IP پیش می آیند. جلوگیری می کند. این حملات

دامنه وسیعی از حملات DOS حملات ناشی از Data Fragmentation و سرریز بافر (Buffer Overflow) را شامل می شود که برخی از آنها عبارتند از:

- LAND
- BONK و TEARDROP
- NESEA
- NEWTEAR
- SYNDROP
- WinNuke
- Ping OF Death)JOLT(
- IGMP

استحکام و Watch Dog:

سپر جزئی از شبکه سازمان است که به تصفیه اتصالات و درخواست های شبکه محلی می پردازد. بنابراین باید همیشه سرپا و فعال نبودن آن می تواند منشا ناامنی باشد. به همین دلیل، سپر طوری طراحی شده است که در صورت بروز تخریب سخت افزاری و نرم افزاری، مجددا و به سرعت راه اندازی گردد. بدین صورت که اگر در اثر قطع برق و یا دیگر عوامل، سپر خاموش شود، باز آغازی و راه اندازی مجدد آن، به سرعت انجام می شود. زمان کوتاه باز آغازی باعث می شود تا اتصال به اینترنت تنها برای زمان کوتاهی قطع شود.

همچنین برای افزایش درجه استحکام سیستم، ابزاری به نام Watch Dog در داخل سیستم وجود دارد که وظیفه مراقبت از سرویس ها و کارکرد سپر را بر عهده دارد. این ابزار به طور مداوم تمامی بخش های سپر را بررسی می کند و در صورت مشاهده هر گونه خرابی و عیب، ابتدا تلاش در رفع خرابی می کند و در صورت عدم موفقیت، سیستم را دوباره راه اندازی نموده و گزارش مناسبی را برای مدیر Mail می زند.

منابع:

http://www.prozhe.com

http://www.irstu.com/?p=3397

http://www.irstu.com/?p=3433

http://www.tarfandestan.com/forum/thread130732.html

www.takbook.com/content/282

http://saeidsaadatit.blogfa.com/post/45