دیواره آتشین (Fire wall) سیستمی است بین کاربران یک شبکه محلی و یک شبکه بیرونی) مثل اینترنت) که ضمن نظارت بر دسترسی ها، در تمام سطوح، ورود و خروج اطلاعات را تحت نظر دارد. بر خلاف تصور عموم کاربری این نرم افزارها صرفاً در جهت فیلترینگ سایت ها نیست. برای آشنایی بیشتر با نرم افزارهای دیواره های آتشین، آشنایی با طرز کار آنها شاید مفیدترین راه باشد. در وهله اول و به طور مختصر می توان گفت بسته های TCP/IP قبل و پس از ورود به شبکه وارد دیواره آتش می شوند و منتظر می مانند تا طبق معیارهای امنیتی خاصی پردازش شوند. حاصل این پردازش احتمال وقوع سه حالت است: ۱ -اجازه عبور بسته صادر می شود. ۲- بسته حذف می شود.۳- بسته حذف می شود و پیام مناسبی به مبدا ارسال بسته فرستاده می شود. •

ساختار و عملکرد با این توضیح، دیواره آتش محلی است برای ایست بازرسی بسته های اطلاعاتی به گونه ای که بسته ها براساس تابعی از قواعد امنیتی و حفاظتی پردازش شده و برای آنها مجوز عبور یا عدم عبور صادر شود .همانطور که همه جا ایست بازرسی اعصاب خردکن و وقت گیر است دیواره آتش نیز می تواند به عنوان یک گلوگاه باعث بالا رفتن ترافیک، تاخیر، ازدحام و بن بست شود. از آنجا که معماری TCP/IP به صورت لایه لایه است (شامل ۴ لایه: فیزیکی، شبکه، انتقال و کاربردی) و هر بسته برای

ارسال یا دریافت باید از هر ۴ لایه عبور کند بنابراین برای حفاظت باید فیلدهای مربوطه در هر لایه مورد بررسی قرار گیرند. بیشترین اهمیت در لایه های شبکه، انتقال و کاربرد است چون فیلد مربوط به لایه فیزیکی منحصر به فرد نیست و در طول مسیر عوض می شود. پس به یک دیواره آتش چند لایه نیاز داریم. سیاست امنیتی یک شبکه مجموعه ای از قواعد حفاظتی است که بنابر ماهیت شبکه در یکی از سه لایه دیواره آتش تعریف می شوند. کارهایی که در هر لایه از دیواره آتش انجام می شود عبارت است از: ۱- تعیین بسته های ممنوع (سیاه) و حذف آنها یا ارسال آنها به سیستم های مخصوص ردیابی (لایه اول دیواره آتش) ۲- بستن برخی از پورت ها متعلق به برخی سرویس ها مثلTelnet، FTPو... (لایه دوم دیواره آتش) ۳- تحلیل برآیند متن یک صفحه وب یا نامه الکترونیکی یا .... (لایه سوم دیواره آتش) ••• در لایه اول فیلدهای سرآیند بسته IP مورد تحلیل قرار می گیرد: آدرس مبدأ: برخی از ماشین های داخل یا خارج شبکه حق ارسال بسته را ندارند، بنابراین بسته های آنها به محض ورود به دیواره آتش حذف می شود. آدرس مقصد: برخی از ماشین های داخل یا خارج شبکه حق دریافت بسته را ندارند، بنابراین بسته های آنها به محض ورود به دیواره آتش حذف می شود IP .آدرس های غیرمجاز و مجاز برای ارسال و دریافت توسط مدیر مشخص

می شود. شماره شناسایی یک دیتا گرام تکه تکه شده: بسته هایی که تکه تکه شده اند یا متعلق به یک دیتا گرام خاص هستند حذف می شوند. زمان حیات بسته: بسته هایی که بیش از تعداد مشخصی مسیریاب را طی کرده اند حذف می شوند. بقیه فیلدها: براساس صلاحدید مدیر دیواره آتش قابل بررسی اند. بهترین خصوصیت لایه اول سادگی و سرعت آن است چرا که در این لایه بسته ها به صورت مستقل از هم بررسی می شوند و نیازی به بررسی لایه های قبلی و بعدی نیست. به همین دلیل امروزه مسیریاب هایی با قابلیت انجام وظایف لایه اول دیواره آتش عرضه شده اند که با دریافت بسته آنها را غربال کرده و به بسته های غیرمجاز اجازه عبور نمی دهند. با توجه به سرعت این لایه هر چه قوانین سختگیرانه تری برای عبور بسته ها از این لایه وضع شود بسته های مشکوک بیشتری حذف می شوند و حجم پردازش کمتری به لایه های بالاتر اعمال می شود. ••• در لایه دوم فیلدهای سرآیند لایه انتقال بررسی می شوند: شماره پورت پروسه مبدأ و مقصد: با توجه به این مسئله که شماره پورت های استاندارد شناخته شده اند ممکن است مدیر دیواره آتش بخواهد مثلاً سرویس FTP فقط برای کاربران داخل شبکه وجود داشته باشد بنابراین دیواره آتش بسته های TCP با شماره پورت ۲۰ و ۲۱ که قصد ورود یا خروج از شبکه را داشته باشند حذف می کند و یا

پورت ۲۳ که مخصوص Telnet است اغلب بسته است. یعنی بسته هایی که پورت مقصدشان ۲۳ است حذف می شوند. کدهای کنترلی: دیواره آتش با بررسی این کدها به ماهیت بسته پی می برد و سیاست های لازم برای حفاظت را اعمال می کند. مثلاً ممکن است دیواره آتش طوری تنظیم شده باشد که بسته های ورودی با SYN=1 را حذف کند. بنابراین هیچ ارتباط TCP از بیرون با شبکه برقرار نمی شود. فیلد شماره ترتیب و Acknowledgement: بنابر قواعد تعریف شده توسط مدیر شبکه قابل بررسی اند. در این لایه دیواره آتش با بررسی تقاضای ارتباط با لایهTCP ، تقاضاهای غیرمجاز را حذف می کند. در این مرحله دیواره آتش نیاز به جدولی از شماره پورت های غیرمجاز دارد. هر چه قوانین سخت گیرانه تری برای عبور بسته ها از این لایه وضع شود و پورت های بیشتری بسته شوند بسته های مشکوک بیشتری حذف می شوند و حجم پردازش کمتری به لایه سوم اعمال می شود. ••• در لایه سوم حفاظت براساس نوع سرویس و برنامه کاربردی صورت می گیرد: در این لایه برای هر برنامه کاربردی یک سری پردازش های مجزا صورت می گیرد. بنابراین در این مرحله حجم پردازش ها زیاد است .مثلاً فرض کنید برخی از اطلاعات پست الکترونیکی شما محرمانه است و شما نگران فاش شدن آنها هستید. در اینجا دیواره آتش به کمک شما

می آید و برخی آدرس های الکترونیکی مشکوک را بلوکه می کند، در متون نامه ها به دنبال برخی کلمات حساس می گردد و متون رمزگذاری شده ای که نتواند ترجمه کند را حذف می کند. یا می خواهید صفحاتی که در آنها کلمات کلیدی ناخوشایند شما هست را حذف کند و اجازه دریافت این صفحات به شما یا شبکه شما را ندهد. • انواع دیواره های آتش دیواره های آتش هوشمند: امروزه حملات هکرها تکنیکی و هوشمند شده است به نحوی که با دیواره های آتش و فیلترهای معمولی که مشخصاتشان برای همه روشن است نمی توان با آنها مقابله کرد. بنابراین باید با استفاده از دیواره های آتش و فیلترهای هوشمند با آنها مواجه شد. از آنجا که دیواره های آتش با استفاده از حذف بسته ها و بستن پورت های حساس از شبکه محافظت می کنند و چون دیواره های آتش بخشی از ترافیک بسته ها را به داخل شبکه هدایت می کنند، (چرا که در غیر این صورت ارتباط ما با دنیای خارج از شبکه قطع می شود)، بنابراین هکرها می توانند با استفاده از بسته های مصنوعی مجاز و شناسایی پورت های باز به شبکه حمله کنند. بر همین اساس هکرها ابتدا بسته هایی ظاهراً مجاز را به سمت شبکه ارسال می کنند. یک فیلتر معمولی اجازه عبور بسته را می دهد و کامپیوتر هدف نیز چون انتظار دریافت این بسته را نداشته به آن پاسخ لازم را می دهد. بنابراین هکر نیز بدین وسیله

از باز بودن پورت مورد نظر و فعال بودن کامپیوتر هدف اطمینان حاصل می کند. برای جلوگیری از آن نوع نفوذها دیواره آتش باید به آن بسته هایی اجازه عبور دهد که با درخواست قبلی ارسال شده اند. حال با داشتن دیواره آتشی که بتواند ترافیک خروجی شبکه را برای چند ثانیه در حافظه خود حفظ کرده و آن را موقع ورود و خروج بسته مورد پردازش قرار دهد می توانیم از دریافت بسته های بدون درخواست جلوگیری کنیم. مشکل این فیلترها زمان پردازش و حافظه بالایی است که نیاز دارند. اما در عوض ضریب اطمینان امنیت شبکه را افزایش می دهند. دیواره های آتش مبتنی بر پروکسی: دیواره های آتش هوشمند فقط نقش ایست بازرسی را ایفا می کنند و با ایجاد ارتباط بین کامپیوترهای داخل و خارج شبکه کاری از پیش نمی برد. اما دیواره های آتش مبتنی بر پروکسی پس از ایجاد ارتباط فعالیت خود را آغاز می کند. در این هنگام دیواره های آتش مبتنی بر پروکسی مانند یک واسطه عمل می کند، به نحوی که ارتباط بین طرفین به صورت غیرمستقیم صورت می گیرد. این دیواره های آتش در لایه سوم دیواره آتش عمل می کنند، بنابراین می توانند بر داده های ارسالی در لایه کاربرد نیز نظارت داشته باشند. دیواره های آتش مبتنی بر پروکسی باعث ایجاد دو ارتباط می شود: ۱ - ارتباط بین مبدا و پروکسی ۲ - ارتباط بین پروکسی و مقصد حال

اگر هکر بخواهد ماشین هدف در داخل شبکه را مورد ارزیابی قرار دهد در حقیقت پروکسی را مورد ارزیابی قرار داده است و نمی تواند از داخل شبکه اطلاعات مهمی به دست آورد. دیواره های آتش مبتنی بر پروکسی به حافظه بالا و CPU بسیار سریع نیاز دارند و از آنجایی که دیواره های آتش مبتنی بر پروکسی باید تمام نشست ها را مدیریت کنند گلوگاه شبکه محسوب می شوند. پس هرگونه اشکال در آنها باعث ایجاد اختلال در شبکه می شود. اما بهترین پیشنهاد برای شبکه های کامپیوتری استفاده همزمان از هر دو نوع دیواره آتش است. با استفاده از پروکسی به تنهایی بارترافیکی زیادی بر پروکسی وارد می شود. با استفاده از دیواره های هوشمند نیز همانگونه که قبلاً تشریح شد به تنهایی باعث ایجاد دیواره نامطمئن خواهد شد. اما با استفاده از هر دو نوع دیواره آتش به صورت همزمان هم بار ترافیکی پروکسی با حذف بسته های مشکوک توسط دیواره آتش هوشمند کاهش پیدا می کند و هم با ایجاد ارتباط واسط توسط پروکسی از خطرات احتمالی پس از ایجاد ارتباط جلوگیری می شود.