بسمه تعالی

سهامی خاص- شماره ثبت: ۱۹۱۵۳۴

تهران، خیابان شهید بهشتی، خیابان سهند، شماره ۲۰، طبقه سوم، تلفن و فاکس: ۸۷۳۷۱۳۴ و ۸۷۳۷۱۲۳

گروه مشاوره امنیتی و امن‌سازی

شمارهٔ گزارش: SSW_TR_SC_83176	**تاریخ تهیه: ۸۳/۵/۱**

امنیت شبکه و فایروال

چکیده:

در این گزارش کاربرد و نقش فایروال‌ها در امنیت شبکه توضیح داده می‌شود.

فهرست مطالب

۱ امنیت شبکه و حافظ

با گسترش استفاده از شبکه‌های کامپیوتری و اتصال شبکه داخلی یک سازمان به شبکه جهانی و افزایش تبادل اطلاعات از طریق اینترنت، امنیت شبکه به یک مساله حیاتی برای سازمان‌های متصل به اینترنت تبدیل شده است. محور اصلی راه حل‌های موجود برای جلوگیری از نفوذ مهاجمان به شبکه محلی مبتنی بر استقرار یک دروازه امنیتی در جلوی جبهه ارتباط شبکه محلی سازمان با دنیای بیرون می‌باشد. دروازه امنیتی که می‌تواند در قالب نرم افزار یا سخت افزارهای خاص این نقش را برعهده بگیرد، تحت عنوان فایروال شناخته شده است.

معمولاً برای جلوگیری از انجام حملات از سوی میزبان خارجی به کارگزارهای داخل سازمان از فایروال استفاده می‌شود. این کارگزارها عمدتا به دلیل استفاده از خدمات ناامن TCP/IP در معرض حمله قرار می‌گیرند. در یک محیط بدون فایروال، امنیت سازمان وابسته به امنیت تک‌تک میزبان‌های موجود در داخل سازمان می‌باشد. با افزایش تعداد میزبان‌های سازمان، نگهداری میزبان‌ها در یک سطح مناسبی از امنیت بسیار مشکل می‌شود. علاوه بر این بسیاری از حملات به خاطر وجود خطاهای ساده در پیکربندی میزبان‌ها و خدمات و عدم آشنایی کافی کاربران میزبان‌های داخلی به مسائل امنیتی می‌تواند رخ بدهد. فایروال با قرار گرفتن در مسیر اتصال شبکه داخلی به اینترنت می‌تواند امنیت متمرکز، یکسان و قابل قبول برای کلیه میزبان‌های شبکه داخلی فراهم کند.

۱-۱ وظایف فایروال

با توجه به نقش فایروال در برآوردن امنیت شبکه محلی، می‌توان وظایف فایروال را در چهار مورد زیر خلاصه نمود.

کنترل دستیابی به شبکه داخلی سازمان

کنترل تبادل اطلاعات بین دو شبکه

بوجود آوردن امنیت برای شبکه داخلی

رفع ناامنی‌های غیردادهای

فایروال یک سیستم با مدل امنیتی کنترل دستیابی است. بنابراین موظف است که با کنترل دسترسی کاربران خارجی به کارگزارهای داخلی، از ارتباطات غیر مجاز جلوگیری کند. این که فایروال چه ارتباطی را مجاز و چه ارتباطی را غیرمجاز بداند، توسط شرایطی مشخص می‌شود که بوسیله مدیر فایروال تعریف شده است. به مجموعه این شرایط سیاست امنیتی فایروال گفته می‌شود. با توجه به این که فایروال در لایه‌های مختلف شبکه پیاده‌سازی می‌شود، مجموعه سیاست‌های امنیتی هر کدام از این لایه‌ها، سیاست امنیتی کل فایروال را تعریف می‌کند.

کنترل استفاده کاربران داخلی از امکانات شبکه جهانی و بطور کلی تبادل اطلاعات بین شبکه داخلی و خارجی از دیگر وظایف فایروال می‌باشد. این کنترل نیز مبتنی بر سیاست امنیتی می‌باشد. با توجه به نوع خدمات موجود در اینترنت و وجود کارگزارهای مختلف در شبکه جهانی تعریف سیاست امنیتی کارآمد و جامع برای این بخش بسیار پیچیده است.

فایروال مکان مناسبی برای برقراری امنیت شبکه محلی است. به عبارت دیگر می‌توان وظیفه برقراری ویژگی‌های تشخیص هویت، جامعیت و محرمانگی را برای ارتباطات بین شبکه‌ای برعهده فایروال نهاد. البته با توجه به هزینه زیاد برقراری تمام ویژگی‌های فوق، امکان وجود تمام این ویژگی‌ها برای تمام این ارتباطات تضمین پذیر نخواهد بود.

مختل کردن کارآیی کارگزارهای داخلی یکی از اهداف معمول مهاجمان می‌باشد. وجود این گونه حملات منجر به ناامنی غیر داده‌ای می‌شود، چرا که در این حملات اطلاعاتی به سرقت نمی‌رود و تنها وظایف کارگزارهای داخلی مختل می‌شود. نمونه‌ای از این نوع حملات نفی خدمت[1] می‌باشد. رفع این گونه ناامنی‌ها را می‌توان یکی از وظایف فایروال دانست.

۱-۲ انواع فایروال

فایروال‌ها به دو نوع اصلی تقسیم می‌شوند.

[1] Denial of Service

فایروال سطح شبکه

فایروال سطح کاربرد

فایروال‌های سطح شبکه معمولا تصمیم‌گیری در مورد رد یا قبول بسته‌ها را بر مبنای سرآیند قراردادهای لایه IP انجام می‌دهند. این فایروال علاوه بر اعمال سیاست امنیتی روی بسته‌ها، ترجمه آدرس را نیز می‌تواند انجام دهد. بنابراین می‌تواند خود را به عنوان نماینده تمام میزبان‌های داخلی شبکه محلی به اینترنت معرفی کند.

فایروال‌های سطح شبکه خود به دو نوع حالت‌مند و غیر حالت‌مند تقسیم می‌شوند. فایروال‌های غیر حالت‌مند تنها فیلترینگ بسته‌ها را مبتنی بر اطلاعات سرآیند لایه IP انجام می‌دهند. بنابراین این فایروال‌ها برای فیلترینگ بسته‌ها به اطلاعات لایه TCP مراجعه نمی‌کنند. نمونه این فایروال‌ها معمولاً در روترهای شبکه امکانات کنترل دسترسی دارند، پیاده‌سازی شده است.

فایروال‌های حالت‌مند می‌توانند فیلترینگ را در سطح لایه TCP و با تشخیص ماشین حالت این لایه انجام بدهند. به عبارت دیگر یک فایروال حالت‌مند باید بتواند ماشین حالت TCP را برای ترافیک عبوری پیاده‌سازی نماید. بنابراین می‌توانند عملیات فیلترینگ را مبتنی بر حالات مختلف یک بسته در لایه TCP انجام دهد.

حالت‌مند بودن یک فایروال منجر به امکان تشخیص برخی حملات مربوط به لایه TCP می‌شود و مچنین در برخی شرایط تعریف سیاست امنیتی را برای مدیران شبکه ساده‌تر می‌نماید. از طرف دیگر حالت‌مند بودن باعث افت کارایی فایروال خواهد شد. این بدین دلیل است که بسته باید در سطح لایه TCP فیلتر شده و ماشین حالت TCPنیز ایجاد شود.

فایروال‌های سطح کاربرد معمولا برای هر قرارداد سطح کاربرد یک کارگزار نماینده (Proxy Server) دارند، که تمام ترافیک مربوط به یک قرارداد به کارگزار نماینده آن قرارداد ارسال می‌شود. کارگزارهای نماینده مکان مناسبی برای انجام عملیات رویدادنگاری و کنترل دستیابی می‌باشند ولی وجود چنین کاربردهایی می‌تواند روی کارایی تأثیر منفی بگذارد و فایروال را نیز غیر مخفی کند.

یک فایروال ایده آل شامل هر دو فایروال سطح مدار و کاربرد می‌باشد. به عبارت دیگر وضعیت مطلوب برای هر یک از این دو فایروال، استفاده از خدمات نوع دیگر است؛ به نحوی که فایروال‌های سطح شبکه اطلاعات بیشتری از بسته‌های در حال عبور داشته باشند و فایروال‌های سطح کاربرد نیز بخشی از

کنترل‌های خود را در یک سطح پایین‌تر و بصورت شفاف اعمال کنند. نتیجه نهایی از ترکیب این دو فایروال می‌تواند یک سیستم سریع باشد که داده‌ها هنگام عبور از آن ثبت و وارسی می‌شوند.

۱-۳ مکانیسم‌های امنیتی در فایروال

فایروال‌ها می‌توانند در لایه‌های مختلف شبکه عمل کنند، بنابراین فایروال‌های مختلف توانایی اعمال رده‌های مختلفی از سیاست‌های امنیتی را دارند. یک فایروال کامل دارای بخش‌های مختلفی است که در کنار یکدیگر می‌توانند امنیت شبکه محلی را برآورده سازند. در این بخش به معرفی بخش‌های اصلی یک فایروال پرداخته می‌شود.

۱-۴ بسته صافی[1]

بسته صافی مولفه‌ای است که بررسی بسته‌ها را در لایه شبکه انجام می‌دهد. سیاست امنیتی در یک بسته صافی مبتنی بر اطلاعات قرارداد لایه شبکه است. البته در حالی که بسته صافی به عنوان بخشی از فایروال پیاده‌سازی می‌شود، می‌توان با استفاده از آن بررسی‌های دقیق‌تری روی بسته‌ها انجام داد.

۱-۵ بسته‌صافی حالت‌مند[2]

بسته صافی قرارداد TCP که مبتنی بر اتصال باشد را بسته صافی حالت‌مند می‌گویند. در حقیقت بسته صافی حالت‌مند وضعیت اتصالات موجود را نگهداری می‌کند. با دریافت هر بسته درخواست اتصال جدید، بسته صافی به پایگاه قواعد خود مراجعه می‌کند. در صورتی که عمل قاعده منطبق شونده با اتصال جدید، {\iranic قبول} باشد، اتصال جدید به مجموعه اتصالات موجود اضافه می‌شود. در مورد سایر بسته‌های دریافتی در صورتی که متعلق به اتصالات موجود در سیستم باشند، عمل انجام شده روی بسته‌های قبلی از آن اتصال، روی بسته دریافتی نیز اعمال می‌شود.

[1] Packet Filter
[2] Stateful Packet Filter

۱-۶ ترجمه آدرس و پورت[1]

وجود دو آدرس متفاوت داخلی و خارجی برای میزبان‌های داخلی شبکه می‌تواند مزایای زیادی داشته باشد. مخفی سازی ساختار داخلی شبکه محلی و امکان تخصیص آدرس‌های غیرمعتبر به میزبان‌های داخلی از مزایای این امکان می‌باشد. در چنین شرایطی در نقطه اتصال شبکه محلی با شبکه جهانی باید آدرس‌های داخلی به آدرس‌های خارجی ترجمه شوند. این وظیفه در فایروال برعهده مترجم آدرس می‌باشد. ترجمه در دو نوع زیر می‌تواند انجام شود.

ترجمه ایستا: در این شرایط یک رابطه یک به یک بین آدرس‌های داخلی و خارجی شبکه محلی وجود دارد.

ترجمه پویا: با ترجمه پویا امکان استفاده از یک آدرس خارجی برای چند آدرس داخلی و در نتیجه امکان گسترش بیشتر شبکه وجود دارد.

تعدادی از قراردادهای لایه کاربرد با ترجمه آدرس ناسازگارند. این قراردادها معمولا آدرس‌های کارفرما یا کارگزار را در بخش داده‌ای لایه کاربرد قرار می‌دهند. کارفرمای قرارداد FTP در حالت فعال و هنگام تولید اتصال برگشتی، اطلاعات این اتصال را بخش داده‌ای قرار می‌دهد. بنابراین بعد از ترجمه آدرس کارفرما، آدرس موجود در بخش داده‌ای نامعتبر می‌شود. معمولا پیمانه مترجم و یا پراکسی ها باید این مشکلات را حل نمایند.

۱-۷ صافی سطح مسیر

صافی سطح مسیر قبل از لایه کاربرد و بالای لایه انتقال فعالیت می‌کند. در حقیقت این صافی یک نوع پراکسی می‌باشد که مستقل از قرارداد لایه کاربرد کار می‌کند. کارفرما برای استفاده از یک کارگزار مستقیماً به این صافی وصل می‌شود؛ یا این که اتصالات رسیده به فایروال توسط بسته صافی به صافی سطح مسیر تغییر جهت داده می‌شود. با توجه به این که بررسی در سطح بسته صافی منحصر به اطلاعات سرآیند لایه شبکه است، می‌توان برای اعمال محدودیت روی بخش داده‌ای بسته‌ها از صافی های سطح مسیر استفاده

[1] NAT/PAT

نمود. برای نمونه تشخیص هویت و بازرسی اطلاعات مبادله شده بین کاربر و کارگزار از نمونه این محدودیت‌ها می‌باشد.

برای پیاده‌سازی صافی‌های سطح مسیر نیاز است که بخش کارفرما و کارگزار نیز تغییر داده شوند. البته در برخی از موارد می‌توان بخش ارتباط با صافی سطح مسیر را بصورت یک کتابخانه سطح پایین در کارفرما و کارگزار قرار داد. در این شرایط کاربر می‌تواند بدون تغییر در کارفرما و کارگزار خود از خدمات صافی سطح مسیر استفاده نماید. نمونه‌ای از پیاده‌سازی صافی سطح مسیر نیز وجود دارد که می‌تواند بطور کاملا مخفیانه کار خود را انجام دهد. نمونه یک صافی سطح مسیر که کاربرد زیادی دارد، SOCKS می‌باشد.

۱-۸ پراکسی‌ها یا دروازه‌های کاربرد

بدلیل این که بسته صافی هیچ‌گونه کنترلی روی بخش داده‌ای بسته انجام نمی‌دهد و بررسی آن محدود به اطلاعات سرآیند بسته می‌باشد، یک فایروال کامل نیاز به داشتن برنامه‌های کاربردی برای بررسی اتصالات در سطح خدمات لایه کاربرد دارد. در حقیقت دروازه کاربرد و یا پراکسی، یک صافی سطح مسیر می‌باشد که خاص یک قرارداد لایه کاربرد پیاده‌سازی شده است. کارفرما برای اتصال با کارگزار به پراکسی مربوط به آن خدمت وصل می‌شود. پراکسی بعد از بررسی مجوز اتصال کارفرما به کارگزار، خدمت موردنظر را به کارفرما ارائه می‌دهد.

معمولا پراکسی‌ها در یکی از دو حالت شفاف[1] یا غیرشفاف کار می‌کنند. در حالت غیرشفاف وجود پراکسی از سوی کارفرما و کارگزار کاملا مشهود است. در این حالت پراکسی اتصال کارفرما به کارگزار را برقرار می‌کند. در حالت شفاف، پراکسی از دید کارفرما و کارگزار مخفی است. البته در این حالت باید بسته صافی در کنار پراکسی همکاری کند.

۱-۹ تشخیص هویت

یکی از روش‌های مهم ایجاد امنیت، تشخیص هویت افراد متقاضی برای ورود و دریافت خدمات از شبکه است. اساس کار فایروال بررسی جواز درخواست‌ها بر مبنای اطلاعات اتصال و کاربران است. بنابراین

[1] Transparent

وجود روشی برای تشخیص هویت کاربران ضروری است. بطور کلی روش‌های تشخیص هویت می‌توانند در دو رده تقسیم شوند.

تشخیص هویت مبتنی بر گذرواژه

تشخیص هویت مبتنی بر کلید

در تشخیص هویت مبتنی بر گذرواژه، کاربر علاوه بر شناسه دارای یک گذرواژه می‌باشد. سیستم، شناسه و گذرواژه را دریافت کرده و صحت آن را با توجه به اطلاعات کاربر بررسی می‌کند. گرچه این روش بسیار ساده است ولی امکان افشای گذرواژه در این روش وجود دارد.

برای جلوگیری از احتمال افشای گذرواژه، از روش گذرواژه یک بار مصرف استفاده می‌شود. در این روش بعد از هر ورود، گذرواژه تغییر می‌کند و برای ورود بعدی گذرواژه قبلی قابل استفاده نیست. در نتیجه در صورت افشای یک گذرواژه، مشکل زیادی پیش نخواهد آمد. استفاده از این روش برای کاربران مشکل است و احتمال فراموشی گذرواژه ها زیاد است.

روشی دیگری که مبتنی بر گذرواژه یک بار مصرف می‌باشد، روش S/Key می‌باشد. در این روش کاربر تنها یک گذرواژه را وارد می‌کند و برنامه کارفرما هر بار براساس یک تابع درهم این گذرواژه را تغییر داده و به کارگزار ارسال می‌کند. بدین ترتیب هر بار یک گذرواژه جدید بین کارفرما و کارگزار منتقل می‌شود و هر کاربر نیز در هر زمان تنها یک گذرواژه را بخاطر می‌سپارد.

یک روش دیگر برای جلوگیری از افشای رمز استفاده از کلید به جای گذرواژه است. در روش‌های مبتنی بر کلید به جای انتقال گذرواژه، از تبادل داده رمز شده استفاده می‌شود. تشخیص هویت کننده داده‌ای را برای تشخیص هویت شونده ارسال می‌کند. تشخیص هویت شونده داده را با یک کلید مشترک رمز کرده و ارسال می‌کند. در صورتی که داده درست رمز شده باشد، هویت طرف مقابل تأیید می‌شود. البته برعکس این روش نیز ممکن است، به ترتیبی که تشخیص هویت کننده داده‌ای را رمز کرده و برای تشخیص هویت شونده ارسال می‌کند. تشخیص هویت شونده داده را با کلید مشترک رمزگشایی کرده و ارسال می‌کند. در صورتی که داده درست رمزگشایی شده باشد، هویت طرف مقابل تأیید می‌شود. در این روش داده بصورت تصادفی انتخاب می‌شود، بنابراین عملی شبیه گذرواژه یک بار مصرف انجام می‌شود. نمونه‌ای از پیاده‌سازی این روش برای قرارداد HTTP، روش Digest می‌باشد.

تمام روش‌های فوق برای تشخیص هویت یک طرف به کار می‌روند. در بعضی از کاربردها نیاز است که هر دو طرف کارفرما و کارگزار یکدیگر را تشخیص هویت کنند. به این نوع تشخیص هویت، تشخیص

هویت دوجانبه گفته می‌شود. برای بدست آوردن نتیجه مطلوب برای این نوع تشخیص هویت از دو کلید برای دو طرف استفاده می‌شود. هر طرف از دیگری درخواست رمزگشایی یا رمز کردن داده تصادفی را می‌کند.

۱-۱۰ محرمانگی اطلاعات

در برخی از موارد لازم است اطلاعاتی که به فایروال می‌رسند قبل از ارسال به مقصد رمزنگاری و یا رمزگشایی شوند، در این زمان از کارگزار محرمانگی اطلاعات استفاده می‌شود. یکی از موارد کاربرد این کارگزار زمانی است که لازم به ایجاد یک شبکه خصوصی مجازی[1] باشد.

رمزنگاری فایروال باید در یک سطح پایین تر صورت بگیرد، زیرا تبادل بین دو میزبان بدون خدشه دار شدن قراردادهای ارتباطی باید رمز شود. بنابراین در فایروال از قراردادهایی نظیر IPSec یا سایر امکانات ایجاد شبکه خصوصی مجازی باید استفاده نمود. گرچه در سایر مکانیسم‌ها فایروال می‌توانست بصورت مستقل و شفاف عمل کند، ولی در مورد محرمانگی اطلاعات باید فایروال یا میزبان مقابل قراردادهای لازم را پشتیبانی کند.

۱-۱۱ رویدادنگاری[2]

علاوه بر تصفیه، رویدادنگاری وقایع و اطلاعات مبادله شده از وظایف اصلی فایروال به شمار می‌آید. رویدادنگاری این امکان را به مدیر شبکه می‌دهد که سابقه‌ای از تبادلات مشکوک را دراختیار داشته باشد. بنابراین با استفاده از اطلاعات رویدادنامه می‌توان برخی از حملات انجام شده را تشخیص داد. در صورت وجود ابزاری مناسب برای تهیه گزارشات مختلف از اطلاعات رویدادنامه، رویدادنگاری می‌تواند به ابزاری قدرتمند برای مدیریت شبکه تبدیل شود. همچنین یک تحلیل‌گر رویدادنامه می‌تواند برای تشخیص حملات احتمالی استفاده شود. در این زمینه تحقیقات زیادی نیز صورت گرفته است؛ برای نمونه می‌توان روش‌های تشخیص نفوذی[3] مبتنی بر تحلیل رویدادنامه را نام برد.

---

[1] Virtual Private Network
[2] Logging
[3] Inrusion Detection

۲ مشکلات موجود در فایروال

با وجود این که امروزه فایروال به عنوان یکی از بهترین ابزار برآورده کردن سیاست امنیتی در یک سازمان استفاده می‌شود، واقعیت این است که فایروال در هر دو بخش امنیت و مدیریت با مشکلاتی مواجه است. در بخش امنیت یکی از مشکلات فایروال، عدم حفاظت سازمان در مقابل نفوذهای داخلی است. به طور کلی فایروال قابلیت حفاظت از اتصالاتی که از آن نمی‌گذرد را ندارد. علاوه بر این حملاتی وجود دارند که بطور کامل قابل حفاظت توسط فایروال نمی‌باشند. این که فایروال شبکه محلی را در برابر چه حملاتی می‌تواند حفاظت کند، وابسته به طراحی آن فایروال می‌باشد. همچنین تکنولوژی فایروال منحصراً برای شبکه‌های TCP/IP طراحی شده است. راه حل‌هایی برای توسعه معماری فایروال برای شبکه‌های دیگر نیز ارائه شده است، که هنوز هیچ پیاده‌سازیی از این راه حل‌ها ارائه نشده است.

علاوه بر مشکلات امنیتی، مشکلات مدیریتی نیز برای فایروال وجود دارد. وجود این قبیل مشکلات می‌تواند منجر به ایجاد مسائل امنیتی و کارایی در شبکه محلی شود. این بدان علت است که پیکربندی نادرست فایروال نه تنها به اعمال سیاست امنیتی سازمان کمک نمی‌کند بلکه مشکلات امنیتی و کارایی را نیز اضافه می‌کند.

همان‌طور که گفته شد، فایروال مدیریت امنیتی سازمان را در نقطه اتصال آن با شبکه جهانی انجام می‌دهد. گرچه وجود یک مدیریت متمرکز یک راه حل ساده است که می‌تواند به یک شبکه محلی با امنیت یکنواخت در میزبان‌های داخلی منجر شود، ولی در عمل نشان داده شده است که این مدیریت متمرکز تنها برای شبکه‌های با میزبان‌های کم کارا است. در شبکه‌هایی که تعداد میزبان‌های زیادی دارند، به علت تنوع در سیاست امنیتی میزبان‌های متفاوت، بالا بودن پهنای باند شبکه، و تنوع در خدمات استفاده شده توسط میزبان‌های داخلی، مدیریت متمرکز توسط فایروال بسیار مشکل می‌شود. ایده فایروال‌های توزیع شده می‌تواند بخشی از این مشکلات را مرتفع سازد.

با توجه به این که بیشتر فایروال‌ها براساس پایگاه قواعد طراحی می‌شوند، لازم است مدیر سازمان سیاست امنیتی سازمان را از طریق پیکربندی سطح پایین فایروال بیان کند. این در حالی است که سیاست امنیتی بصورت سطح بالا و ورای تمام فایروال‌های موجود تعریف می‌شود. به طور کلی مدیر مایل به حفظ اطلاعات است، اما فایروال محافظ منابع شبکه می‌باشد. بنابراین مدیر با دسته بندی منابع و نگاشت آن‌ها به اطلاعات، سعی می‌کند سیاست امنیتی موردنظر خود را بیان کند. به طور مسلم این سیاست‌ها بطور کامل برهم منطبق نمی‌شوند و امکان نقض سیاست امنیتی مدیر، بدون این که سیاست امنیتی ارائه شده به فایروال نقض شود، وجود دارد.