فایروال ها : یک ضرورت اجتناب ناپذیر در دنیای امنیت اطلاعات

امنیت اطلاعات و ایمن سازی کامپیوترها به یک ضرورت غیرقابل انکار در عصر اطلاعات تبدیل شده است. پرداختن به مقوله امنیت اطلاعات با زبانی ساده بیش از هر زمان دیگر احساس می شود، چراکه هر یک از عوامل انسانی و غیرانسانی دارای جایگاه تعریف شده ای در نظام مهندسی امنیت اطلاعات می باشند. آشنائی اصولی و منطقی با این نظام مهندسی و آگاهی از عناصر موجود در این ساختار به همراه شناخت علمی نسبت به مسئولیت هر یک از عناصر فوق، امری لازم و حیاتی است.

فایروال ها ، یکی از عناصر اساسی در نظام مهندسی امنیت اطلاعات می باشند که استفاده از آنان به یک ضرورت اجتناب ناپذیر در دنیای امنیت اطلاعات و کامپیوتر تبدیل شده است . بسیاری از افرادی که جدیدا" قدم در عرصه گسترده امنیت اطلاعات می گذارند ، دارای نگرانی و یا سوالات مفهومی خاصی در ارتباط با فایروال ها و جایگاه استفاده از آنان در جهت ایمن سازی شبکه های کامپیوتری می باشند .

در این مطلب قصد داریم به برخی از مفاهیم و نکات مهم و اساسی در خصوص فایروال ها اشاره ای داشته باشیم تا از این رهگذر بتوانیم دانش لازم به منظور بکارگیری و مدیریت بهینه فایروال ها را بدست آوریم .

NAT (برگرفته از Network Address Translation)

اولین و در عین حال مهم ترین وظیفه یک فایروال ، جداسازی شبکه داخلی یک سازمان از اینترنت است . یکی از فنآوری های موجود که ما را در جهت نیل به خواسته فوق کمک می نماید ، جداول NAT می باشند (NAT ، همچنین کمک لازم در جهت حل معضل کمبود آدرس های IP را ارائه می نماید) . مهمترین ایده مطرح شده توسط NAT ، عدم دستیابی به اکثر کامپیوترهای موجود در یک شبکه خصوصی از طریق اینترنت است . یکی از روش های نیل به خواسته فوق ، استفاده از آدرس های IP غیرمعتبر (Invalid) می باشد .

در اکثر موارد بکارگیری NAT ، صرفا" آدرس IP معتبر (Valid) به فایروال نسبت داده می شود و تمامی کامپیوترهائی که مسئولیت حفاظت از آنان به فایروال واگذار شده است ، از آدرس های IP که صرفا" بر روی شبکه داخلی معتبر می باشد ، استفاده می نمایند . با تبعیت از چنین رویکردی ، زمانی که یک کامپیوتر موجود در شبکه داخلی نیازمند برقراری ارتباط با دنیای خارج است ، اقدام به ارسال درخواست خود برای فایروال می نماید . در ادامه فایروال به نمایندگی از کامپیوتر متقاضی ، درخواست مورد نظر را ارسال می

نماید . در زمان مراجعت درخواست ارسالی ، پاسخ مربوطه به فایروال رسیده و در نهایت ، فایروال آن را برای کامپیوتر موجود در شبکه داخلی ارسال می نماید .

فرض کنید ، کاربری قصد داشته باشد که یک وب سایت خاص را از طریق کامپیوتر موجود بر روی یک شبکه داخلی ملاقات نماید .پس از درج آدرس وب سایت مورد نظر در بخش آدرس برنامه مرورگر ، درخواست وی به یک درخواست HTTP ترجمه شده و برای فایروال ارسال می گردد . در ادامه ، فایروال از آدرس IP مختص به خود در ارتباط با درخواست HTTP و به نمایندگی از کاربر ارسال کننده درخواست ، استفاده می نماید . پس از پاسخ به درخواست ، پاسخ مربوطه برای فایروال ارسال شده و در نهایت فایروال آن را برای کاربر مربوطه ارسال می نماید .

فیلترینگ پورت ها

فیلترینگ پورت ها از جمله مهمترین عملیاتی است که توسط فایروال ها انجام می شود و شاید به همین دلیل باشد که اکثر مردم بر این اعتقاد هستند که فایروال ها صرفا" به همین دلیل خاص طراحی و پیاده سازی شده اند و اغلب ، آنان را به عنوان ابزاری در جهت فیلترینگ پورت ها تصور می نمایند . همانگونه که می دانید ، مبادلات اطلاعات مبتنی بر پروتکل TCP/IP با استفاده و محوریت پورت ها انجام می گردد . در این رابطه ٦٥،٥٣٥ پورت TCP و به همین اندازه پورت UDP جداگانه وجود دارد که می توان از آنان به منظور مبادله اطلاعات استفاده نمود .

به منظور آشنائی با جایگاه پورت ها و نقش آنان در مبادله اطلاعات در پروتکل TCP/IP ، می توان آنان را نظیر ایستگاه های رادیوئی تصور نمود . فرض کنید TCP به عنوان موج FM و UDP به عنوان موج AM باشد . در چنین وضعیتی ، می توان یک پورت در پروتکل TCP/IP را همانند یک ایستگاه رادیوئی تصور نمود .

همانگونه که یک ایستگاه رادیوئی با اهداف خاصی طراحی شده است ، پورت های TCP و UDP نیز چنین وضعیتی را داشته و با اهداف خاصی طراحی شده اند . یکی از مهمترین دلایل ضرورت استفاده از فایروال ها و فیلترینگ پورت ها ، استفاده غیرمتعارف از پورت ها به منظور نیل به اهدافی دیگر است . مثلا" پورت ٢١ مربوط به پروتکل TCP بطور سنتی به منظور FTP استفاده می گردد و مهاجمان می توانند از پورت فوق و با استفاده از برنامه هائی نظیر Telnet سوء استفاده نمایند (با این که پورت فوق به منظور استفاده توسط برنامه Telnet طراحی نشده است) .

پویش پورت ها و آگاهی از پورت های باز ، از جمله روش های متداولی است که توسط مهاجمان و به

منظور یافتن یک نقطه ورود مناسب به یک سیستم و یا شبکه کامپیوتری ، مورد استفاده قرار می گیرد . مهاجمان پس از آگاهی از پورت های باز ، با بکارگیری برنامه هائی نظیر Telnet زمینه ورود غیر مجاز به یک سیستم را برای خود فراهم می نمایند .

وضعیت فوق و تهدیدات امنیتی مرتبط با آن ، ضرورت فیلترینگ پورت ها را به خوبی نشان می دهد . با فیلترینگ پورت ها ، این اطمینان ایجاد خواهد شد که هیچ چیزی نمی تواند از طریق یک پورت باز ارسال گردد مگر پروتکل هائی که توسط مدیریت شبکه به آنان اجازه داده شده است . مثلا" در صورتی که فیلترینگ پورت بر روی پورت ۲۱ مربوط به پروتکل TCP اعمال گردد ، صرفا" به مبادلات اطلاعات مبتنی بر FTP اجازه داده خواهد شد که از این پورت استفاده نمایند و مبادله اطلاعات به کمک سایر پروتکل ها و بکارگیری پورت فوق ، امکان پذیر نخواهد بود .

محدوده عملیاتی فیلترینگ پورت ها می تواند از موارد اشاره شده نیز تجاوز نموده و در سطح هدر یک بسته اطلاعاتی و حتی محتویات آن نیز تعمیم یابد . در چنین مواردی ، هدر بسته اطلاعاتی بررسی و با مشاهده اطلاعاتی نظیر آدرس مبداء ، مقصد ، شماره پورت و سایر موارد دیگر در رابطه با آن اتخاذ تصمیم می گردد . مشکل موجود در این رابطه به وجود اطلاعات جعلی و یا نادرست در هدر بسته های اطلاعاتی برمی گردد . مثلا" فرستنده می تواند آدرس های IP و سایر اطلاعات ذخیره شده در هدر بسته های اطلاعاتی را جعل نماید . به منظور غلبه بر مشکل فوق ، نوع دیگری از فیلترینگ که برخی فایروال ها به آن stateful packet inspections و یا فیلترینگ پویای بسته های اطلاعاتی می گویند ، ایجاد شده است . در مدل فوق ، در مقابل بررسی هدر بسته های اطلاعاتی ، محتویات آنان مورد بازبینی قرار می گیرد . بدیهی است با آگاهی از این موضوع که چه چیزی در بسته اطلاعاتی موجود است ، فایروال ها بهتر می توانند در رابطه با ارسال و یا عدم ارسال آن برای یک شبکه داخلی تصمیم گیری نمایند .

ناحیه غیرنظامی (Demilitarized Zone)

نواحی غیرنظامی (DMZ) ، یکی دیگر از ویژگی های ارائه شده توسط اکثر فایروال ها می باشد . DMZ ، ناحیه ای است که تحت قلمرو حفاظتی فایروال قرار نمی گیرد . فایروال های مختلف ، نواحی DMZ را با روش های متفاوتی پیاده سازی می نمایند . مثلا" برخی از فایروال ها ، صرفا" شما را ملزم به معرفی آدرس IP ماشینی می نمایند که قصد استقرار آن در ناحیه DMZ وجود دارد .برخی از فایروال ها دارای یک پورت شبکه ای اختصاصی می باشند که می توان از آن برای هر نوع دستگاه شبکه ای که قصد استقرار آن

در ناحیه DMZ وجود دارد ، استفاده گردد .

پیشنهاد می گردد ، حتی المقدور از نواحی DMZ استفاده نگردد ، چراکه ماشین های موجود در این نواحی از امکانات حفاظتی و امنیتی فایروال استفاده نخواهند کرد و تنها گزینه موجود در این رابطه امکانات ارائه شده توسط سیستم عامل نصب شده بر روی ماشین و سایر توصیه هائی است که با رعایت و بکارگیری آنان ، وضعیت امنیتی سیستم بهتر می گردد .

در صورتی که برای ایجاد یک ناحیه DMZ دلایل موجه و قانع کننده ای وجود دارد ، می بایست با دقت و برنامه ریزی صحیح توام با رعایت مسائل امنیتی اقدام به انجام چنین کاری گردد. در صورتی که ماشین مستقر در ناحیه DMZ دارای یک اتصال به شبکه داخلی نیز باشد ، مهاجمان با تمرکز بر روی ماشین فوق می توانند نقطه مناسبی برای ورود به شبکه را پیدا نمایند . پیشنهاد می گردد به عنوان یک قانون و اصل مهم ، ماشین های موجود در ناحیه DMZ دارای اتصالاتی به غیر از پورت DMZ فایروال نباشند .

فورواردینگ پورت ها

در بخش قبل به نحوه عملکرد فیلترینگ پورت ها به منظور بلاک نمودن استفاده از یک پروتکل بجزء یک آدرس IP خاص، اشاره گردید . فورواردینگ پورت نیز بر اساس همین مفاهیم مطرح و در سازمان هائی که در ارتباط با NAT می باشند ، کارساز خواهد بود .

برای آشنائی با مفهوم فورواردینگ پورت ها ، یک مثال نمونه را بررسی می نمائیم .

فرض کنید ، سازمانی دارای یک سرویس دهنده وب است که از آدرس IP: 192.168.0.12 (یک آدرس معتبر نمی باشد ولی فرض کنید که چنین واقعیتی وجود ندارد) استفاده می نماید و می بایست امکان دستیابی عمومی به آن فراهم گردد . در صورتی که سرویس دهنده وب فوق تنها سرویس دهنده موجود در سازمان است که می بایست امکان دستیابی عمومی به آن فراهم گردد ، می بایست یک قانون فیلترینگ بسته های اطلاعاتی در سطح فایروال تعریف گردد که تمامی درخواست های HTTP بر روی پورت ۸۰ و به مقصد هر آدرس موجود در شبکه بجزء آدرس IP:192.168.0.12 ، بلاک گردد . پس از تعریف قانون فوق ، در صورتی که کاربری یک درخواست HTTP را برای آدرس های دیگری ارسال نماید ، با پیامی مبنی بر این که وب سایت درخواستی وجود ندارد ، مواجه خواهد شد .

در مثال فوق ، این فرض نادرست را کردیم که امکان دستیابی عمومی به آدرس IP:192.168.0.12 وجود دارد . آدرس فوق صرفا" بر روی یک شبکه خصوصی معتبر بوده و امکان دستیابی آن از طریق اینترنت وجود

نخواهد داشت . بدیهی است در چنین وضعیتی می بایست آدرس سرویس دهنده وب خصوصی خود را با یک آدرس عمومی جایگزین نمائید . (با این که یک گزینه مطلوب در این رابطه نمی باشد) . برخی از مراکز ارائه دهنده خدمات اینترنت (ISP) ، صرفا" امکان استفاده از یک آدرس IP عمومی را در اختیار شما قرار داده و بدیهی است که در چنین مواردی ما دارای گزینه های متعددی برای اختصاص این آدرس نخواهیم بود و می بایست آن را به فایروال اختصاص داد .

یکی از موارد استفاده سنتی از NAT به مواردی نظیر آنچه اشاره گردید ، بر می گردد . سازمان فرضی دارای صرفا" یک آدرس IP معتبر است و آن را به فایروال نسبت داده و از NAT به منظور تسهیل در مبادله اطلاعات بین ماشین های موجود در شبکه داخلی و اینترنت استفاده می نماید . در چنین مواردی یک مشکل همچنان باقی می ماند . NAT به منظور بلاک نمودن ترافیک تمامی ارتباطات ورودی بجزء آنانی که درخواست آنان از طرف یکی از ماشین های موجود در شبکه داخلی ارسال شده است ، طراحی شده است و ما همچنان دارای یک سرویس دهنده وب می باشیم که می خواهیم امکان دستیابی عمومی به آن را نیز فراهم نمائیم .

به منظور حل مشکل فوق می توان از فورواردینگ پورت استفاده نمود . در واقع فورواردینگ پورت ، قانونی است که به فایروال می گوید در صورتی که درخواست های خاصی بر روی یک پورت خاص برای وی ارسال شده باشد ، می بایست درخواست مربوطه را برای یک ماشین طراحی شده بدین منظور بر روی شبکه داخلی، ارجاع نماید . در مثال اشاره شده ، ما قصد داریم امکان دستیابی عمومی به سرویس دهنده وب را فراهم نمائیم . بدین منظور می بایست یک قانون فورواردینگ پورت بدین منظور تعریف که به فایروال اعلام نماید هر درخواست HTTP بر روی پروتکل TCP و پورت ۸۰ را به آدرس IP:192.168.0.12 تغییر مسیر داده و برای آن ارسال نماید. پس از تعریف قانون فوق ، شخصی که قصد دستیابی به وب سایت سازمان شما را داشته باشد ، پس از فعال نمودن برنامه مرورگر ، اقدام به درج آدرس سایت سازمان شما دربخش مربوطه می نماید. مرورگر کاربر مورد نظر به منظور آگاهی از آدرس domain سایت سازمان شما ، اقدام به ارسال یک درخواست DNS می نماید تا از این طریق نسبت به آدرس IP نسبت داده شده به domain آگاهی لازم را پیدا نماید . بدیهی است آدرسی که پیدا خواهد شد و به عنوان مرجع در اختیار مرورگر قرار خواهد گرفت، همان آدرس IPعمومی است که شما آن را به فایروال نسبت داده اید . مرورگر در ادامه ، درخواست HTTP را برای آدرس IP عمومی شما ارسال می نماید که در حقیقت این درخواست برای فایروال ارسال می گردد

. فایروال درخواست را دریافت و آن را برای سرویس دهنده وب ارسال می نماید (فورواردینگ) .

خلاصه

در این مطلب به جایگاه بسیار مهم فایروال ها در نظام مهندسی امنیت اطلاعات اشاره و پس از بررسی نحوه عملکرد آنان با چندین ویژگی مهم ارائه شده توسط فایروال ها آشنا شدیم .