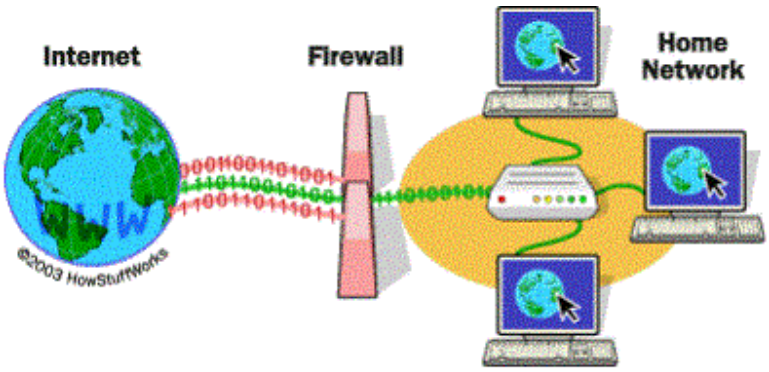
آشنایی با نحوه عملکرد فایروال ها، پروکسی سرورها و DMZ

اگر مدتی (هرچند کوتاه) است که از اینترنت استفاده می کنید و به خصوص اگر در یک شرکت بزرگ کار می کنید و معمولا در محل کار به رایانه و اینترنت دسترسی دارید، احتمالا بارها کلمه فایروال (firewall، دیواره آتش) به گوش تان خورده است.

در این کقاله که توسط وب سایت امنیتی نگهبان تهیه شده است، می خواهیم با مفهوم فایروال و نحوه عملکرد آن آشنا شویم. به عنوان مثال، اغلب هنگام گفتگو با همکاران تان در شرکت چیزهایی مشابه این جمله را شنیده اید:«من نمی توانم به این سایت وارد شوم چرا که از طریق فایروال اجازه دسترسی به آن را به کاربران شبکه نمی دهند» و از این بحثها.



۱- مقدمه ای بر فایروال

اگر شما از اینترنت پر سرعت در منزل خود استفاده می کنید (ADSL)، ممکن است در مورد فایروال برای شبکه خانگی خود نیز چیزهایی شنیده باشید. این طور به نظر می رسد که یک شبکه خانگی کوچک با مسایل امنیتی مشابهی با شبکه های شرکت های بزرگ درگیر است. شما می توانید برای محافظت از شبکه خانگی خود و خانواده در مقابل وب سایت های مخرب یا نفوذ بالقوه هکرها از فایروال استفاده کنید.

در واقع ، فایروال مانعی برای جلوگیری از نفوذ نیروهای مخرب به دارایی های مجازی شما است. به همین دلیل است که به آن فایروال (دیواره آتش) نام داده اند. کار آن شبیه به دیوار فیزیکی است که از گسترش آتش از یک منطقه به منطقه دیگر جلوگیری می کند. در ادامه درباره فایروال ها چیزهای بیشتر یاد می گیرید، اینکه آنها چگونه کار می کنند و از چه نوع تهدیداتی می توانند شما را محافظت کنند.

۲-ابزار فایروال چه می کند؟

به زبان ساده فایروال یک برنامه نرم افزاری یا وسیله سخت افزاری است برای نظارت بر اطلاعاتی کـه از طریـق اتصال به اینترنت بین شبکه خصوصی و یا سیستم کامپیوتر شما و جهان خارج رد و بدل می شـود. اگـر بسـته ورودی اطلاعات از طریق فیلترهای اعمالی مورد سوء ظن قرار بگیرد، به آن اجازه ورود داده نمی شود.

اجازه دهید فرض کنیم شما در شرکتی با ۵۰۰ کارمند کار می کنید. بنابراین شـرکت بـه طـور طبیعـی صـدها دستگاه کامپیوتر دارد که تمام آنها توسط کارت های شبکه به هم متصل شده اند. علاوه بر ایـن، شـرکت دارای یک یا چند اتصال به اینترنت از طریق چیزی شبیه خطوط ADSL یا ماهواره است. بدون اسـتفاده از فـایروال در چنین شبکه ای، تمام این صدها کامپیوتر به طور مستقیم در دسترس هر کسی که در اینترنت فعالیت می کند خواهند بود. کسی که این مسئله را بداند می تواند در کامپیوترها به سادگی کاوش و کند و کاو کند، سعی کند اتصال FTP به شبکه برقرار کند، یا سعی در ایجاد ارتباط راه دور به شبکه و غیره کند. اگر یک کارمنـد مرتکـب اشتباهی شود و حفره امنیتی در رایانه خود ایجاد کند، هکرها می توانند به دستگاه او نفوذ کرده و از حفـره بـه بهترین نحو بهره برداری کنند.

با استفاده از فایروال در شبکه فوق، چشم انداز بسیار متفاوت خواهد بود. شرکت کافی است در سر راه هر اتصال به اینترنت شرکت (برای مثال، در هر خط ADSL که از شرکت خدمات اینترنـت آیـد) فـایروال یـا دیـواره آتـش تنظیم کند. فایروال می تواند پیاده سازی قوانین امنیتی مدنظر مدیران شبکه را بسیار آسان نمایـد. بـه عنـوان مثال، یکی از قوانین امنیتی داخل شرکت ممکن است این باشد :

«از ۵۰۰ کامپیوتر موجود در این شرکت، تنها یکی از آنها مجاز به دریافت ترافیک های FTP عمومی است. پـس تنها اجازه اتصال به FTP به این کامپیوتر مشخص داده می شود و از اتصال بقیه به FTP عمومی باید جلوگیری به عمل آید»

شرکت می تواند قوانینی مانند مورد بالا را برای سرورهای FTP، سرویس دهنده شـبکه راه دور (Telnet) و غیـره راه اندازی کند. علاوه بر این، شرکت می تواند چگونگی اتصال کارکنان به سایت های اینترنتی، اعم از آنکه چـه فایلهایی مجاز به ارسال از رایانه شرکت بر شبکه باشند و غیره را کنترل نماید. پس ملاحظه می کنید که فایروال به شرکت ابزار کنترل فوق العاده ای برای نظارت بر چگونگی استفاده از شبکه خـارجی توسـط کـاربران شـبکه محلی می دهد.

فایروال ها از سه روش ممکن برای کنترل ترافیک اطلاعات در داخل و خارج از شبکه استفاده می کنند :

• فیلتر کردن بسته اطلاعات (Packet filtering) – بسته ها (تکه های کوچک اطلاعات) توسط مجموعه ای از فیلترهای فایروال آنالیز می شوند. بسته هایی که از فیلتر عبور کرده و فایروال آنها را مجاز تشخیص دهد، به سیستم درخواست کننده اطلاعات فرستاده شده و همه بسته های دیگر که نتوانند از فیلتر عبور کنند رد صلاحیت شده و فاقد مجوز عبور شناخته می شوند.

• سرویس پروکسی (Proxy service)- اطلاعات دریافتی از اینترنت ابتدا توسط فایروال بازیابی شده و در صورت مجاز بودن به سیستم درخواست کننده فرستاده می شود و بالعکس.

• بازرسی اختصاصی (Stateful inspection)- روش جدیدتری است که در آن فایروال محتویات تمام بسته های اطلاعاتی را بررسی نمی کند، بلکه در عوض برخی از اجزا کلیدی بسته را با بانک اطلاعاتی اطلاعات قابل اعتماد مقایسه می کند. اطلاعاتی که از شبکه محلی به بیرون منتقل می شوند از فیلتر فایروال برای نظارت بر حصول ویژگی های خاص از پیش تعریف شده گذشته، و سپس اطلاعات دریافتی از بیرون با این خصوصیات تعریف شده مقایسه می شوند. اگر نتیجه مقایسه مطابقت معقولی باشد، عبور اطلاعات به یا از شبکه محلی مجاز است. در غیر این صورت درخواست رد می شود.

۳- پیکربندی فایروال

فایروال ها قابل تنظیم و سفارشی سازی هستند. این به دان معنی است که شما می توانید فیلتر ها را براساس شرایط مختلف اضافه یا حذف کنید. برخی از این فیلترها عبارتند از:

• آدرس های آی پی (IP addresses) – به هر سیستمی در اینترنت یک آدرس منحصر به فرد به نام آدرس آی پی تخصیص داده شده. آدرس های آی پی اعداد ۳۲ بیتی هستند، به طور معمول به شکل چهار «octets» در سیستم «عدد ده دهی نقطه گذاری شده» بیان می شوند. یک آدرس آی پی مرسوم مثل این است : ۲۱۶.۲۷.۶۱.۱۳۷. برای مثال، اگر یک آدرس آی پی خاص در خارج از شرکت در تلاش برای خواندن فایل های بیش از حد زیاد از سرور باشد، دیوار آتش وارد عمل شده و می تواند تمام ترافیک شبکه یا آن آدرس آی پی را مسدود کند.

• نام های دامنه (Domain names) – به خاطر آن که به یاد داشتن رشته ای از اعداد که آدرس آی پی را تشکیل می دهند سخت است، و از آنجا که گاهی اوقات نیاز به تغییر آدرس آی پی می باشد، تمام سرورهای اینترنت دارای یک نام قابل فهم برای انسان هستند، که نام های دامنه نامیده می شوند. به عنوان مثال ، برای ما به یاد داشتن عبارت google.com آسان تر از به خاطر داشتن عبارت ۱۷۳.۱۹۴.۳۶.۱۰۴ است. شرکت بر طبق قوانین خود می تواند با استفاده از فایروال دسترسی به دامنه های خاصی را مسدود کرده یا فقط اجازه دسترسی به دامنه های خاص را بدهد.

• پروتکل ها (Protocols) – پروتکل راه از پیش تعریف شده ای است که با استفاده از آن هر کسی که بخواهد از سرویسی استفاده کند باید با آن سرویس ارتباط برقرار کند. "هر کسی" می تواند یک شخص باشد، اما اغلب یک برنامه کامپیوتری مانند مرورگر وب است. پروتکل ها معمولا به صورت متنی هستند و به زبان ساده، مکالمه و تعامل گیرنده و سرور را توصیف میکنند. در جهان وب، پروتکل http را داریم. برخی از پروتکل های رایج که شما می توانید فیلترهای فایروال را بر آن اساس تنظیم کنید عبارتند از :

الف: IP (پروتکل اینترنت) – سیستم اصلی انتقال اطلاعات بر روی اینترنت.

ب: TCP (پروتکل کنترل انتقال اطلاعات) – برای خرد کردن و بازسازی اطلاعاتی که بر روی اینترنت جا به جا می شود به کار می رود.

ج:HTTP (پروتکل انتقال ابر متن – Hyper Text Transfer) – برای صفحات وب استفاده می شود.

د: FTP (پروتکل انتقال فایل) – برای دانلود و آپلود فایل استفاده می شود.

ه: UDP (پروتکل دادهای کاربر) – برای اطلاعاتی استفاده می شود که نیاز به پاسخ ندارد ، مانند پخش فایل های صوتی و ویدئویی.

و: ICMP (پروتکل کنترل پیام اینترنت) – توسط یک روتر (router) به منظور مبادله اطلاعات با روترهای دیگر استفاده می شود.

ز: SMTP (پروتکل انتقال ساده ایمیل) – مورد استفاده برای ارسال اطلاعات متنی (ایمیل).

ح: SNMP (پروتکل مدیریت شبکه ساده) – برای جمع آوری اطلاعات سیستم از یک کامپیوتر از راه دور (remote computer).

ط: Telnet (شبکه راه دور) – برای انجام و اعمال دستورات بر روی یک کامپیوتر از راه دور.

شرکت بسته به شرایط خود می تواند قوانینی وضع کند که طبق آن تنها ۱ یا ۲ سیستم از سیستم های شبکه مسئولیت رسیدگی به یک پروتکل خاص را داشته باشند و استفاده از همین پروتکل در تمام رایانه های دیگر مسدود و ممنوع باشد.

• درگاه ها (Ports)- هر دستگاه سرور خدمات خود را با استفاده از تعدادی پورت در دسترس اینترنت قرار می دهد، یعنی برای هر سرویس یک پورت بر روی سرور در دسترس است. برای مثال، اگر دستگاه سرور در حال اجرای وب سرور (HTTP) و سرور FTP باشد، وب سرور به طور معمول روی پورت ۸۰ در دسترس خواهد بود و FTP سرور از طریق پورت ۲۱ در دسترس است. شرکت می تواند دسترسی به پورت ۲۱ را برای تمام دستگاه های شبکه جز یک یا چند رایانه تعریف شده داخل شبکه خود مسدود کند.

• فیلتر کلمات و عبارات خاص- این مورد می تواند هر چیزی باشد. دیواره آتش هر بسته اطلاعاتی را برای مطابقت دقیق متن ذکر شده در فیلتر جستجو می کند. به عنوان مثال ، شما می توانید فایروال را برای مسدود کردن هر بسته با کلمه "فیلم" در محتوای خود تنظیم کنید. نکته مهم این است که فایروال عین عبارت فوق را می تواند مسدود کند. فیلتر ایجاد شده "فیلم" نمی تواند محتوای "فی لم" را مسدود کند. اما در عوض می توانید بسیاری از کلمات، عبارات و تنوع آنها را تا حد نیاز برای فیلتر شدن تعریف کنید.

برخی از سیستم عامل ها دارای دیواره آتش پیش فرض اند. در غیر این صورت، باید نرم افزار فایروال را بر روی کامپیوتر منزل خود که به اینترنت متصل است نصب کنید. این کامپیوتر به عنوان دروازه در نظر گرفته می شود، زیرا تنها نقطه دسترسی بین شبکه خانگی شما و اینترنت است.

با فایروال سخت افزاری، به طور معمول خود فایروال به عنوان دروازه (gateway) در نظر گرفته می شود. مثال خوبی از فایروال سخت افزاری روتر Linksys Cable/DSL است. این دستگاه دارای کارت شبکه (Ethernet) و هاب است. کامپیوترهای موجود در شبکه خانگی شما که به روتر متصل می شوند، که روتر هم به یک مودم ADSL متصل است. تنظیمات روتر از طریق یک رابط کاربری تحت وب در اختیارتان قرار می گیرد که می توانید با مرورگر اینترنت تان آنها را ببینید و فیلترهای مورد نظرتان را تعریف کنید.

****

فایروال های سخت افزاری فوق العاده امن بوده و خیلی هم قیمت گرانی ندارند. نسخه خانگی که شامل روتـر و هاب اترنت برای اتصال به شبکه اینترنت را به سادگی می توان به بهای زیر ۱۰۰ دلار خریداری کرد.

۴- چرا از حفاظ امنیتی فایروال استفاده می کنیم؟

راه های بسیار زیادی وجود دارد که کاربران خرابکار و بی پروا برای دسترسی به کامپیوترهای محافظت نشده از آنها سوء استفاده می کنند که برخی از مهم ترین این راهها عبارتند از :

• ورود به سیستم از راه دور (Remote login)- هنگامی که کسی قادر به اتصال به کامپیوتر شما و کنتـرل آن از راه دور گردد، به طرق مختلفی ممکن است از سیستم تـان سوءاسـتفاده کنـد. ایـن توانـایی طیـف مختلفـی از مشاهده و یا دسترسی به فایل های موجود در رایانه قربانی گرفته تا اجرای برنامه های روی کامپیوتر او را در بر می گیرد.

• درهای پشتی برنامه ها (Application backdoors)- برخی از برنامه ها امکانات ویژه ای دارند که برای دسترسی از راه دور استفاده می شود. محصولاتی هم دارای اشکالات نرم افزاری یا باگ هستند که backdoor یا دسترسـی مخفی را برای کنترل برنامه توسط هکر فراهم می کند.

• ربودن جلسه SMTP (SMTP session hijacking) – SMTP رایج ترین روش ارسال ایمیل در اینترنت اسـت. یـک هکر می تواند با دسترسی به لیست نشانی های درون ایمیل شخص قربانی، هزاران هرزنامه (اسپم) را به کاربرانی که قربانی با آنها در تماس است ارسال کند. این اتفاق اغلب با تغییر مسیر ایمیلها از طریق سرور SMTP میزبـان غیر مشکوک انجام می گیرد ، که ردیابی فرستنده واقعی هرزنامه ها را مشکل می کند.

• باگ های سیستم عامل- درست مانند برنامه های کاربردی، برخی از سیستم عامل هـا هـم backdoor دارنـد. برخی سیستم های عامل هم امکان دسترسی از راه دور را البته با امنیتی ناکافی یا اشکالات نـرم افـزاری بـرای کاربرانشان فراهم می کنند که یک هکر با تجربه می توانند از این ضعف ها سوء استفاده کند.

• محرومیت از خدمات (Denial of service)- شما احتمالا این عبارت را در گزارش های خبری در مورد حمله به وب سایت های بزرگ شنیده یا دیده اید. مقابله با این نوع حمله ها تقریبا غیر ممکن است. اتفاقی که می افتـد این است که هکر درخواستی به سرور برای اتصال به آن می فرستد. هنگامی که سرور پاسـخ درخواسـت را مـی فرستد و سعی در برقراری جلسه (session) دارد، قادر نیست سیستم درخواست کننـده را پیـدا کنـد. بـا تعـداد

کافی درخواست و اشباع سرور با این جلسات مربوط به درخواست های بدون پاسخ، هکر می تواند باعث کاهش و افت سرعت سرور به حد زیاد یا در نهایت مسدود شدن و صدمه به آن شود.

• بمباران پست الکترونیکی (E-mail bombs)- بمباران ایمیلی معمولا یک حمله شخصی به شمار می رود. کسی به قصد آزار و اذیت به آدرس ایمیل شما یک ایمیل را به تعداد صدها یا هزاران نسخه ارسال می کند تا سیستم ایمیل شما نتواند هیچ پیام دیگری را قبول کند و صندوق پست الکترونیک شما از کار بیافتد.

• ماکرو(Macros)- برای ساده کردن مراحل پیچیده، بسیاری برنامه های کاربردی به ما اجازه ایجاد یک اسکریپت از دستورات برای اجرای برنامه را می دهند. این اسکریپت به عنوان ماکرو شناخته شده است. هکرها از این نکته استفاده می کنند تا ماکروهای خود را ایجاد و وارد سیستم کنند که بسته به برنامه، می تواند اطلاعات شما را نابود کرده یا باعث صدمه به کامپیوتر شما گردد.

• ویروس ها (Viruses)- احتمالا شناخته شده ترین خطرها، ویروس های رایانه ای هستند. ویروس یک برنامه کوچک است که می تواند خودش را در دیگر کامپیوترها کپی کند. با این روش به سرعت می تواند از یک سیستم به سیستم دیگر گسترش یابد. ویروس ها از پیام های بی ضرر شروع شده و در موارد خطرناک می توانند تمام اطلاعات حیاتی قربانیان را پاک کرده و از بین بردند.

• هرزنامه ها (Spam)- معمولا بی ضرر اما همیشه مزاحم اند! هرزنامه ها معادل الکترونیکی نامه های ناخواسته و مزخرف هستند. هرزنامه اما گاهی می تواند خطرناک باشد. اغلب هرزنامه ها شامل لینکی به وب سایت های هدف هستند. مراقب کلیک کردن بر روی این لینک ها باشید چرا که ممکن است به طور تصادفی با پذیرفتن کوکی باعث فراهم کردن backdoor روی کامپیوتر خود شوید.

• بمباران تغییر مسیر (Redirect bombs)- هکرها می توانند از ICMP برای تغییر (تغییر مسیر) اطلاعات با ارسال آن به روتر متفاوتی استفاده کنند. این یکی از راه هایی است که حمله محرومیت سرویس (D.O.S.) بر آن اساس پایه ریزی می شود.

• مسیریابی منبع (Source routing)- در اغلب موارد ، مسیری که بسته (packet) از آن طریق در اینترنت (یا هر شبکه دیگر) جا به جا می شود توسط روترهای مسیر مشخص می شود. اما منبع ارائه بسته به طور دلبخواه می تواند مسیر سفر بسته را مشخص کند. هکرها گاهی اوقات از این نکته استفاده می کنند تا اطلاعات ارسالی خود

به قربانی را به صورتی که گویی از منبع قابل اعتماد ارسال شده و یا حتی از داخل شبکه می آیند درآورند! به همین دلیل است که اکثر فایروال ها مسیریابی منبع را به صورت پیش فرض غیر فعال می کنند.

فیلتر کردن برخی از موارد لیست بالا با استفاده از فایروال، اگر غیر ممکن نباشد، سخت و دشوار است. در حالی که برخی از فایروال ها قابلیت حفاظت از ویروس ها را به طور پیش فرض دارند، ارزش آن را دارد که هزینه و وقت صرف کرده و نرم افزار آنتی ویروس بر روی هر کامپیوتری نصب کنیم. و حتی اگر آن را آزار دهنده بدانید، برخی از هرزنامه ها از دیوار آتش عبور می کنند و تا زمانی که شما ایمیل انها را قبول می کنید شما را گرفتار خود می کنند.

سطح امنیتی که شما برقرار می کنید تعیین می کند که کدام یک از تهدیدات بالا را فایروال می تواند متوقف کند. بالاترین سطح امنیتی این خواهد بود که به سادگی همه چیز توسط فایروال مسدود شود. بدیهی است که این مسئله ما را از هدف خود که داشتن اتصال به اینترنت کارآمد و مناسب است دور می کند. اما یک قاعده شایع است که توصیه می کند ابتدا از ورود همه نوع اطلاعاتی به شبکه جلوگیری کنیم، و سپس شروع به انتخاب موارد مجاز برای تبادل اطلاعات کنیم.

همچنین می توانید ترافیک اطلاعات را که از فایروال می گذرند طوری محدود کنید که فقط انواع خاصی از اطلاعات از قبیل پست الکترونیک و صفحات وب بتوانند از حصار امنیتی عبور کنند. این قانون خوبی برای شرکت های تجاری است که یک مدیر شبکه با تجربه دارند که نیازهای شرکت مطبوعش را به خوبی درک می کند و می داند که دقیقا به چه اطلاعاتی باید اجازه تبادل دهد. برای بسیاری از ما، احتمالا بهتر آن است که با گزینه های پیش فرض ارائه شده توسط توسعه دهنده فایروال کار کنیم، مگر آنکه دلیل موجهی برای تغییر آن داشته باشیم.

یکی از بهترین کارهایی که دیواره آتش از نقطه نظر امنیتی می تواند انجام دهد متوقف و مسدود کردن هر کسی است که در خارج از شبکه تحت نظر فایروال قصد ورود به یک کامپیوتر در شبکه را دارد. در حالی که این ویژگی خوبی برای شرکت های تجاری است، احتمالا بیشتر شبکه های خانگی، با این شیوه مورد تهدید واقع نمی شوند. با این حال، قرار دادن یک فایروال در شبکه به آسایش خیال مدیر شبکه کمک شایانی می کند.

۵- پروکسی سرورها و DMZ

پروکسی سرور دستور العملی است که اغلب همراه با فایروال است. پروکسی سرور برای کنترل دسترسی به صفحات وب توسط دیگر کامپیوترها به کار می رود. هنگامی که کامپیوتری درخواست ورود به یک صفحه وب را می دهد، آن صفحه توسط پروکسی سرور بازیابی شده و سپس به کامپیوتر درخواست کننده فرستاده می شود. تاثیر چنین کاری این است که کامپیوتر راه دوری که میزبانی صفحات وب را بر عهده دارد هیچ وقت در تماس مستقیم با هیچ چیز، به غیر از پروکسی سرور روی شبکه تان نیست.

پروکسی سرورها همچنین می توانند دسترسی به اینترنت شما را کارآمدتر کند. اگر به صفحه ای از وب سایت دسترسی پیدا کنید، این صفحه بر روی پراکسی سرور (کش) ذخیره سازی می شود. بدان معنی که دفعه بعد که دوباره از آن صفحه بازدید می کنید، به طور معمول لازم نیست دوباره آن را از وب سایت بارگذاری کند. در عوض ، این بار بلافاصله از پروکسی سرور صفحه بارگذاری می شود.

ممکن است گاهی مواقع بخواهید کاربران از راه دور امکان دسترسی به موارد موجود بر روی شبکه شما را داشته باشند. برخی از نمونه ها عبارتند از :

- وب سایت ها
- کسب و کار آنلاین
- استفاده از محیط دانلود و آپلود FTP

در مواردی مانند بالا، ممکن است بخواهید منطقه غیرنظامی یا DMZ – Demilitarized Zone ایجاد کنید. البته باید توجه جدی به این نکته داشته باشید که این منطقه تنها نقطه از شبکه تان در خارج از فایروال است. به DMZ به عنوان حیاط جلویی خانه خود نگاه کنید. درست است که حیاط بخشی از ملک شما است و ممکن است بعضی چیزها را انجا قرار دهید، اما بی شک هر چیز با ارزش را در داخل خانه قرار می دهید تا به طور مناسبی از لحاظ امنیتی ان را محافظت کنید.

راه اندازی یک DMZ بسیار آسان است. اگر شبکه ای با چندین کامپیوتر دارید، می توانید به سادگی یکی از کامپیوترها را بین اتصال اینترنت و فایروال قرار دهید. بسیاری از نرم افزارهای فایروال موجود اجازه خواهند داد که شما یک پوشه را در کامپیوتر دروازه (gateway) به عنوان DMZ تعیین کنید.

هنگامی که شما یک فایروال در محلی راه اندازی کردید، باید آن را تست کنید. یکی از بهترین راه ها برای انجام این کار رفتن به سایت www.grc.com و سعی برای عبور از حفاظ فایروالی است که ایجاد کرده اید! با این کار بازخورد فوری از اینکه سطح امنیتی سیستم شما در چه حدی است دریافت خواهید نمود

****

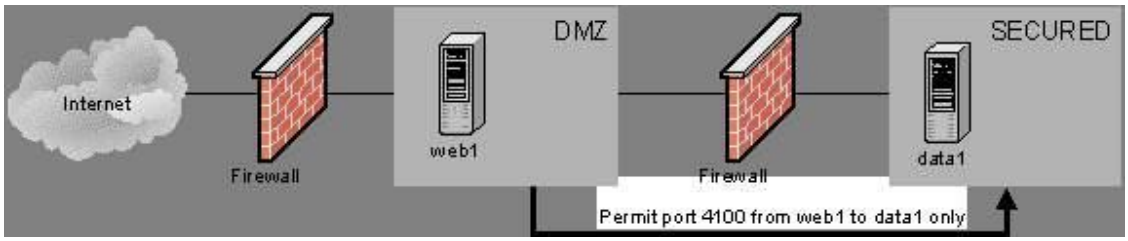
ب. قرار ندادن پایگاه داده در DMZ:

در صورتی که از یک معماری امن برای پیاده سازی شبکه خود استفاده کرده باشید به احتمال زیاد شبکه شما دارای یک بخش DMZ(Don't Militarized Zone) خواهد بود. معمولا ارائه دهندگان خدمات عمومی را درین بخش از شبکه قرار میدهند. بعنوان مثال سرورهای وب، سرورهای میل ... که همگی جهت خدمات عمومی بکار میروند درین بخش از شبکه قرار دارند.

ایده عمومی داشتن یک بخش DMZ ساده ست: سرورهایی که خدمات عمومی بیرون سازمانی ارایه میدهند نیازمند سطح کمتری از امنیت هستند. در واقع همه میتوانند به آنها دسترسی داشته باشند. این دسترسی همگانی به هیچ وجه لازم نیست در مورد تمامی منابع شبکه اعمال شود. بنابرین منابع عمومی شبکه را در بخشی از شبکه قرار میدهند که حساسیت امنیتی کمتری نسبت به آن وجود دارد. این همان بخش DMZ است. با توجه به مطالب بالا بسیار بدیهی به نظر میرسد سرور پایگاه داده را باید در همان بخش DMZ قرار دهیم زیرا که عموما این سرور نیز مسئولیت ارائه خدمات همگانی را بعهده دارد. اما قضیه در باره سرور پایگاه داده تا حدی متفاوت است. این سرور گرچه خدمات همگانی نیز عرضه میکند اما تنها بخشی از داده های آن ممکن است جنبه همگانی داشته باشد در حالی که عمده آن در اغلب اوقات سری ست. بعنوان مثال سروری که اطلاعات مربوط به کارت اعتباری افراد را نگهداری میکند از اهمیت فوق العاده ای برخوردار است و هرگونه دسترسی به کل داده های آن میتواند فاجعه بار باشد.

بنابراین بر خلاف دید اولیه به این نتیجه میرسیم که پایگاه داده نمیتواند و نباید که در بخش DMZ قرار گیرد. اما راهکار جداسازی آن ازین بخش چیست؟

شکل ۱: پایگاه داده و DMZ



راه حل ایده آل برای این جداسازی به شرح زیر است: به صورت عام از یک فایروال اصلی برای ایمنی کل شبکه و جداسازی آن از دنیای بیرون استفاده میشود. این فایروال در قسمت بیرونی DMZ قرار دارد و دارای قواعد خاص خود است. بدلایلی که در بخش پیش ذکر شد که کلا عبارت بود از نیاز به ارائه خدمات عمومی ،این فایروال نمیتواند کل ترافیک ورودی را محدود کند و ناچار است یک سیاست (Policy) حداکثری را اعمال کند.

اما در داخل خود شبکه ، مابیت LAN داخلی و DMZ از فایروال دومی استفاده میشود. این فایروال دوم در حالت ایده آل تمامی ترافیک ورودی را سد میکند بجز ترافیک ورودی از وب سرور به پایگاه داده. با این تمهید خاص هم پچایگاه داده خدمات عمومی خود را ارائه میدهد و هم دستیابی عموم را به آن سد کرده ایم. درین صورت یک نفوذ گر حتی پس ازینکه کنترل کامل سرور وب را در اختیار گرفت ناچار است از قواعد سختگیرانه فایروال دوم نیز عبور کند و تازه پس ازان باید بتواند به سرور پایگاه داده نیز نفوذ کند که انجام این هر دو کار بسیار دشوار میباشد و ریسک چنین شبکه ای عملا پایین می باشد.

اما شاید در مقابل روش ما استدلالی اینچنین ارائه شود: میتوان تنها با استفاده از یک فایروال امنیت را تامین کرد. روش آنهم اینست که برای سرورهای پایگاه داده از IP مجازی استفاده کنیم. در واقع این سرورها پشت یک NAT قرار داشته باشند. درین صورت نفوذگر اساسا از وجود پایگاه داده خبر ندارد تا بخواهد به آن نفوذ کند. این استدلال یک ابراد عمده دارد و آنهم اینست که اگر نفوذ گر بتواند کنترل سرور وب را در اختیار بگیرد عملا در همان شبکه ای قرار گرفته است که سرور پایگاه داده دران قرار دارد و دارای همان رنج IP میشود. بنابراین پس ازینکار در واقع تمهید قبلی ما بلااثر میشود و نفوذ گر میتواند بسادگی مانند یک کاربر داخلی شبکه ما عمل کند.

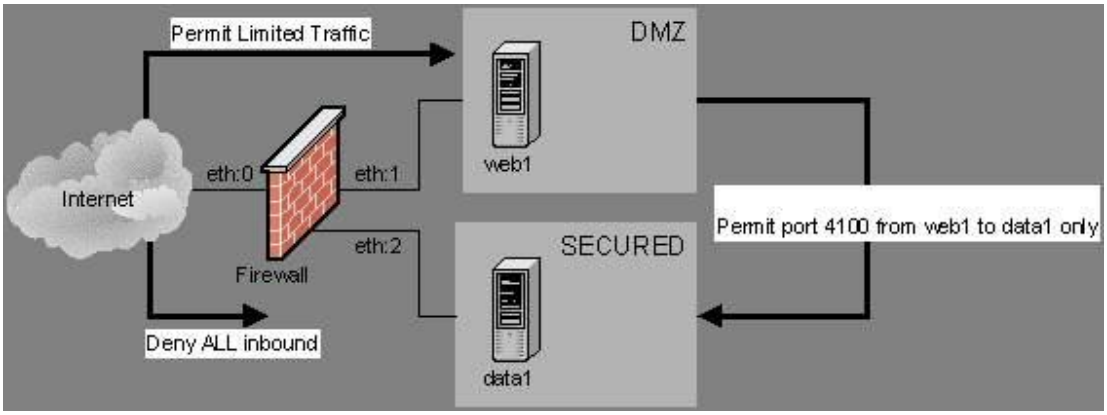
حال که استدلالات فوق را پذیرفته ایم میتوانیم کمی ایده آل تر باشیم و شبکه را ایمن تر کنیم. فرض کنید که یک نفوذگر بتواند از لایه اول امنیتی شما عبور کرده وارد DMZ شود. اگر این نفوذ به دلیل نقص قواعد امنیتی فایروال شماره یک باشد احتمال نفوذ همین شخص به لایه دوم بسیار پایین است. اما اگر این نفوذ به دلیل وجود شکاف امنیتی خاصی بر روی فایروال باشد چطور؟ فرض کنید به عنوان مثال هردو فایروال شما Check

Point است. آنوقت نفوذگر بهمان سادگی که از لایه اول عبور کرده از لایه دوم امنیتی شما نیز خواهد گذشت چون هر دو فایروال ما از یک نوع است و طبیعتا شکاف امنیتی هردو یکسان است. بنابراین میتوان پیشنهاد داد که فرضا اگر فایروال لاه اول شما Check Point است در لایه دوم بهتر است از PIX استفاده کنید. این مطلب باعث امنیت بالاتر شبکه شما خواهد شد.

این روش گرچه موثر است اما از عهده هرسازمانی بر نمی آید. نگهداری، بروزسازی و پیکربندی فایروال عموما خودش یک تخصص خاص و بالنسبه گرانقیمت است. بنابراین وقتی از دو نوع فایروال استفاده میکنید دو تخصص جداگانه را در سازمان خود نیاز خواهید داشت که این مطلب باعث دو برابر شدن هزینه نیروی انسانی شما خواهد شد. علاوه برینکه اصولا خود سخت افزار فایروال هم گرانقیمت است و اصولا مشخص نیست که سازمان شما حاضر باشد چنین هزینه ای را متقبل شود (حتی با فرض دانستن ریسک امنیتی بالای آن)

راه حل دیگری که میتوان برای جداسازی بخش امن شبکه ارائه داد استفاده از بیش از یک کارت شبکه در فایروال است (شکل ۲)

شکل ۲: استفاده از دو کارت شبکه برای جداسازی DMZ



همانطور که مشخص است درین روش توسط یک فایروال، DMZ از بخش امن شبکه جداسازی میشود. تنها ترافیکی که حق عبور از اینترفیس اول (eth1) به اینترفیس امن (eth2) را دارد ترافیک ورودی از وب سرور به سرور پایگاه داده میباشد. این روش بسیار ارزان تر از روش قبلی ست اما مشخصا امنیت آن در حد امنیت روش قبل نیست و علاوه برآن ممکن است فایروال موجود ما عملا از چندین کارت شبکه پشتیبانی نکند.

علاوه بر دو راهی که در فوق برای جداسازی پایگاه داده از مابقی شبکه ارائه دادیم راه حل سومی هم وجود دارد: اینکه اساسا پایگاه داده را از مابقی شبکه جدانکنیم! دقت کنید که با توجه به هزینه و نیز اندازه سازمان ممکن است جداسازی امکان پذیر نباشد و حتی مجبور شویم که این دو سرور را برروی یک ماشین اجرا کنیم. حتی درین صورت نیز بهتر است حداقل کارهایی که جهت ایمنی مضاعف پایگاه داده از دستمان بر می آید انجام دهیم. بعنوان مثال میتوانیم از یک فایروال نرم افزاری ارزان قیمت جهت ایمنی بیشتر استفاده کنیم. بهر حال این راه حل توصیه نمیشود مگر در شرایط اجبار.

ج. رمز نگاری اطلاعات مابین سرور وب و سرور پایگاه داده

برای جلوگیری از سرقت اطلاعات در بین راه(Sniffing) عموما از روشهای رمز نگاری استفاده میشود. متداول ترین روش تحت وب برای انجام این منظور استفاده از پروتکل SSL است. عموم اطلاعات امن که بر روی اینترنت منتقل میشوند از همین پروتکل استفاده میکنند . بعنوان مثال انتقال اطلاعات شناسایی با سرورهای معروف ایمیل، انتقال اطلاعات مربوط به کارت اعتباری و غیره.

تا بدینجا این پروتکل که اغلب سرورهای وب و نیز مرورگرها ازان پشتیبانی میکنند سطحی از امنیت را تامین میکند. اما آیا همین کافی ست؟

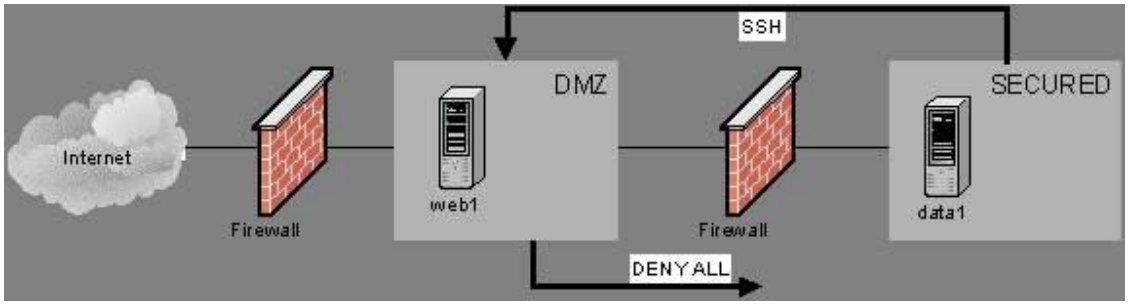
اغلب این اشتباه پیش می آید که همین سطح از رمز نگاری را در مقابل حمله Sniffing کافی میدانند. باید دقت کرد که SSL به صورت عام تنها برای رمزنگاری اطلاعات مابین Client و سرور وب به کار میرود و به صورت عادی اطلاعات مابین وب سرور و سرور پایگاه داده به صورت عادی و بدون رمزنگاری (Plain Text) منتقل میشوند. بنابراین حتی اگر همه جوانب را در شبکه بیرونی رعایت کرده باشیم، یک نفوذگر داخلی به سادگی میتواند اطلاعات در حال انتقال مابین این دو سرور را شنود کند. این مطلب زمانی بسیار جدی میشود که بدانیم بر اساس داده های موجود، بالاتر از ۶۰٪ حملات موجود حملات درون سازمانی می باشد.

چاره کار استفاده از یک روش رمز نگاری مابین سرور وب و سرور پایگاه داده است. اغلب سرور های پایگاه داده امروزه از SSL حمایت میکنند. MS SQL Server2000، Oracle،Sybase ازین جمله اند. البته استفاده از SSL برای ارتباط مابین این دو سرور لازمه اش اینست که برنامه اصلی شما (Web Application) با همین ملاحظه طراحی و پیاده سازی شده باشد.

اما در صورتی که برنامه شما از قبل موجود باشد یا از SSL پشتیبانی نکند یا به هر صورت شما مایل به ایجاد هزینه اضافی نباشید چه؟ آیا راه حل دیگری برای رمزنگاری مابین دو سرور وجود دارد؟ خوشبختانه چنین راه حلی وجود دارد: استفاده از SSH یا یک برنامه مشابه.

اصولا SSH برنامه ای شبیه Telnet است اما نسخه امن آن. یکی از قابلیتهای SSH ایجاد یک تونل امن است. به این صورت که میتوان برنامه SSH را به گونه ای اجرا کرد که بر روی یک پورت شنود کند کل اطلاعات آن را رمز کرده به کامپیوتر مقصد ارسال کند و آنجا پس از تبدیل به حالت عادی به پورت مقصد تحویل دهد. با استفاده از این روش (SSH Port Forwarding) یک تونل امن به صورت شفاف مابین دو سرور ایجاد شده است(شکل ۳).

شکل ۳: استفاده از SSH برای برقراری تونل امن



مزیت استفاده ازین روش اینست که نیاز به هیچگونه تغییری در سرورها و یا برنامه ها ندارد و تنها توسط چند خط دستور قابل اجراست.

د. عدم استفاده از Hub و بهره گیری از Switch

به صورت عادی زمانی که از Hub استفاده میکنیم تمامی اطلاعات عبوری در هریک از سیستمهای موجود در شبکه داخلی قابل شنود است. یک نفوذ گر معمولی با استفاده از یکی از ابزارهای Sniffing میتواند اینترفیس شبکه با به حالت Promiscuous برده ، تمامی اطلاعات در حال جابجایی بر روی LAN را دریافت کند. البته استفاده از رمز نگاری خطر بالقوه بهره گیری ازین روش را کم میکند اما هیچگاه نمیتوان مطمئن بود که کل اطلاعات رمز نگاری شده است. بنابراین بهتر است حتی المقدور امکان بهره گیری از Sniffing را بر روی شبکه کاهش دهیم. استفاده از سوپیچها به جای هاب یکی از روشهای حل این مساله است. با استفاده از سوئیچ در واقع یک مدار مجازی (Virtual Circuit) مابین دو نود در حال مکالمه ایجاد میشود و دیگران به اطلاعات در حال انتقال مابین آن دو دسترسی ندارند.

****

معرفی ساختار DMZ یا Demilitarized Zone

سالها پیش و در جریان جنگی که بین کره شمالی و جنوبی پیش آمده بود (سال ۱۹۵۰ میلادی) ، در پیشنهادی که از طرف سازمان ملل به دو کشور شد ، قرار بر این شد که در میان مرز این کشور قسمتی را به عنوان منطقه غیرنظامی یا Demilitarized Zone انتخاب کنند تا مردم بتوانند از آن برای زندگی و امرار معاش بدون وارد شدن ساختار نظامی و جنگ استفاده کنند و همین مورد بین دو کشور توافق شد . مردم از این منطقه به عنوان منطقه ارتباطی بین دو کشوری که در حال جنگ بودند و به یکدیگر اعتماد نداشتند استفاده می کردند اما در محیطی که به هیچیک از دو کشور صدمه ای وارد نشود.

طراحی ساختار DMZ در شبکه

همین مفهوم در شبکه های کامپیوتری نیز به وجود آمد ، DMZ یک نوع طراحی شبکه است ، در واقع DMZ یک شبکه است که در میان شبکه خصوصی یا داخلی شما و شبکه خارجی یا اینترنت قرار می گیرد . این شبکه به کاربران خارج از سازمان اجازه برقراری ارتباط با سرورهای داخلی سازمان بصورت مستقیم را نمی دهند و به همین وسیله از اطلاعات سازمان حفاظت می کند. DMZ یک مرز ارتباطی بین دو شبکه است که به هم اعتماد ندارند و شما نیز قطعا به شبکه اینترنت اعتماد ندارید. ساختار DMZ معمولا توسط فایروال ها و یا پروکسی سرور هایی طراحی می شوند که در لایه های مختلف شبکه قرار می گیرند.

در یک ساختار DMZ ساده در یک شبکه معمولی ، یک سرور یا کامپیوتر که در اینجا به عنوان Host معرفی می شود در محیط DMZ قرار می گیرد و تمامی درخواست هایی که کاربران داخلی برای برقراری ارتباط با خارج از شبکه دارند را دریافت می کند ، این سرور بعد از دریافت این بسته های درخواست (مثلا درخواست وب سایت) آنها را به سمت شبکه عمومی یا اینترنت هدایت می کند و سپس پاسخ این درخواست ها را در همان Session ای که توسط کاربر داخلی ایجاد شده بود برای وی ارسال می کند ، توجه کنید که در این طراحی ساده ، هیچگونه ترافیکی نمی تواند از شبکه بیرونی به شبکه داخلی وارد شود.

کاربرانی که در شبکه اینترنت یا خارجی قرار دارند صرفا می توانند به Host ای که برای DMZ استفاده می شود دسترسی پیدا کنند و به هیچ عنوان به شبکه داخلی دسترسی نخواهند داشت. یکی دیگر از کارهایی که در این Host می تواند انجام شود این است که صفحات وب ای که قرار است از طرف سازمان بر روی اینترنت در معرض

دسترسی قرار بگیرند می توانند بر روی این Host قرار بگیرند. اما توجه کنید که DMZ به شبکه داخلی نیز در این حالت دسترسی نخواهد داشت. شما فرض کنید که در این حالت یک هکر قصد حمله به وب سایت سازمان را دارد ، حتی اگر موفق به هک این صفحات شود ، به اطلاعات خاصی در خصوص شبکه داخلی و اطلاعات خصوصی سازمان دست پیدا نخواهد کرد. بدون شک یکی از بهترین تجهیزات شبکه ای که برای استفاده ویژه در ساختار DMZ مورد استفاده قرار می گیرد تجهیزات فایروال شرکت سیسکو می باشد.

اگر بخواهیم از نظر امنیتی DMZ را تعریف کنیم ، می توانی آنرا به نوعی تنظیمات پیشرفته در فایروال های شبکه نیز معرفی کنید. در تنظیمات DMZ اکثر کامپیوترهایی که در شبکه LAN قرار گرفته اند در پشت فایروال قرار می گیرند که این فایروال به شبکه اینترنت یا شبکه عمومی متصل شده است . از طرفی یک یا چندین سرور نیز در محلی بعد از فایروال قرار می گیرند ، یعنی در شبکه داخلی نیستند ، این سرورهایی که در بعد از فایروال قرار می گیرند ، درخواست های کاربران داخلی را همانطور که اعلام شد از شبکه داخلی دریافت کرده و سپس آنها را به شبکه اینترنتی که به آن متصل هستند ارسال می کنند ، این دقیقا همان مفهوم امنیتی است که مد نظر است ، خاطرتان هست که در جنگ بین کره شمالی و جنوبی یک شهر به عنوان محل رابط بین دو کشور انتخاب شد که در آن جنگی در کار نبود ، این را دقیقا در شبکه نیز می توانید تصورکنید.

توجه کنید که شما واژه DMZ را در بسیاری از تجهیزات شبکه اعم از روترهای اینترنتی خانگی نیز مشاهده می کنید اما آنها واقعا DMZ نیستند بلکه صرفا قابلیت پشتیبانی از این نوع تنظیمات هستند که در تجهیزات شبکه دیده شده است . این نوع تجهیزات با طراحی واقعی DMZ در ساختار های سازمانی به کلی تفاوت دارند ، آنها صرفا چند Rule ساده در تنظیمات روتر خانگی هستند ، اما در DMZ های سازمانی ، سرورها و تجهیزات حرفه ای در طراحی DMZ استفاده می شود.

در حوزه امنیت اطلاعات ممکن است DMZ به عنوان Perimeter Network نیز مطرح شود که نام دیگر همین نوع طراحی شبکه است. در اکثر سازمان های دولتی و حتی شرکت ها ، سرویس هایی وجود دارد که سازمان ها قصد دارند به بیرون از شبکه ارائه دهند ، مثلا وب سایت یا پورتال سازمانی ، سرویس ایمیل ، سرویس میزبانی وب یا حتی سرویس DNS . فرض کنید که این سرویس ها را در درون شبکه داخلی قرار بدهید و به کاربرانی که از اینترنت قصد استفاده از این سرویس ها را دارند اجازه ورود به شبکه داخلی را بدهید ، این خود یک نقطه ضعف امنیتی می باشد ، بنابراین همیشه برای اینگونه سرویس های عمومی استفاده از طراحی DMZ توصیه می شود.

در چنین شرایطی شما سرویس ها و سرورهای مورد نظر خود را در محیط DMZ قرار می دهید و ارتباط محدودی با شبکه داخلی برای آنها ایجاد می کنید ، ارتباطی که در سطح بسیار کم و با درصد خطر کمتری نسبت به ارتباطات معمول شبکه باشد. طراحی DMZ برای محافظت از حملاتی است که از بیرون سازمان به سرویس ها انجام می شود و معمولا در این نوع طراحی خطرات شبکه داخلی سازمان از جمله Spoofing و Sniffing و ... آنها دیده نمی شود.

اما چه سرویس هایی را ما در قسمت DMZ یا Perimeter شبکه قرار می دهیم ؟ همانطور که گفتیم سرویس هایی که نیازمند دسترسی عمومی می باشند را در این منطقه از شبکه قرار می دهیم ، مهمترین و معروف ترین سرویس هایی که در قسمت DMZ شبکه قرار می گیرند به شکل زیر می باشند :

سرویس دهنده های وب یا Web Server ها

سرویس دهنده های ایمیل یا Mail Server ها

سرویس دهنده های Voip

سرویس دهنده های FTP

نکته ای که در اینجا بسیار مهم است ، این است که وب سرورهای سازمانی معمولا صفحات ایستا نیستند که صرفا چند صفحه باشند ، بلکه صفحات دینامیکی هستند که در پس زمینه خود دارای یک پایگاه داده اطلاعاتی می باشند ، این وب سرور ها بایستی بتوانند از این پایگاه داده استفاده کنند ، قاعدتا اگر این پایگاه داده را در خود محیط DMZ قرار بدهید ، کار اشتباهی خواهد بود ، در این حالت پایگاه داده مورد نظر را یا در شبکه داخلی و پشت فایروال قرار می دهند و یا در پشت یک فایروال و در شبکه ای در همان طراحی DMZ قرار می دهند. در این حالت اگر هکری موفق به نفوذ به وب سایت شود ، صرفا به صفحات وب سایت دسترسی پیدا می کند و نمی تواند داده ها و اطلاعات موجود در پایگاه داده را که در پشت فایروال دیگری قرار دارد را مورد هجوم قرار دهد.

سرویس های ایمیل یا همان Email Server ها نیز دارای اطلاعات کاربری و پایگاه داده خاص خود می باشند که آنها نیز بایستی محافظت شوند. همانطور که در طراحی قبلی اشاره کردیم آنها را نیز در پشت یک فایروال جداگانه قرار می دهیم ، توجه کنید که معمولا سرویس دهنده های ایمیل از سرویسی به نام Webmail

پشتیبانی می کنند که می توان از طریق وب به آنها دسترسی داشت ، شما می توانید ایمیل سرور خود را در پشت فایروال DMZ قرار داده و از طریق امکانی به نام Pblishing صفحه وب ایمیل را برای دسترسی عمومی Publish کنید. توجه کنید که ایمیل سرور هایی که به این شکل هستند هم ترافیک ورودی و هم ترافیک خروجی ایمیل ها را بایستی به درستی مدیریت کنند ، طراحی DMZ ها با توجه به سرویس های موجود در شبکه متعیر هستند و DMZ یک ساختار ایستا و ثابت نمی باشد. به دلیل مسائل امنیتی و همچنین مسائل مانیتورینگ در یک محیط تجاری ، بیشتر سازمان ها و شرکت ها در محدوده DMZ خود یک Proxy Server راه اندازی می کنند ، راه اندازی این سرور در این محیط درای یک سری مزایا به شرح زیر می باشد :

اجبار کردن کاربران داخلی برای استفاده از Proxy Server برای استفاده از اینترنت

کاهش نیاز به پهنای باند اضافی بر روی شبکه اینترنت به علت استفاده از قابلیت cache در پروکسی سرور

ساده سازی فرآیند ضبط و مانیتورکردن استفاده کاربران از اینترنت

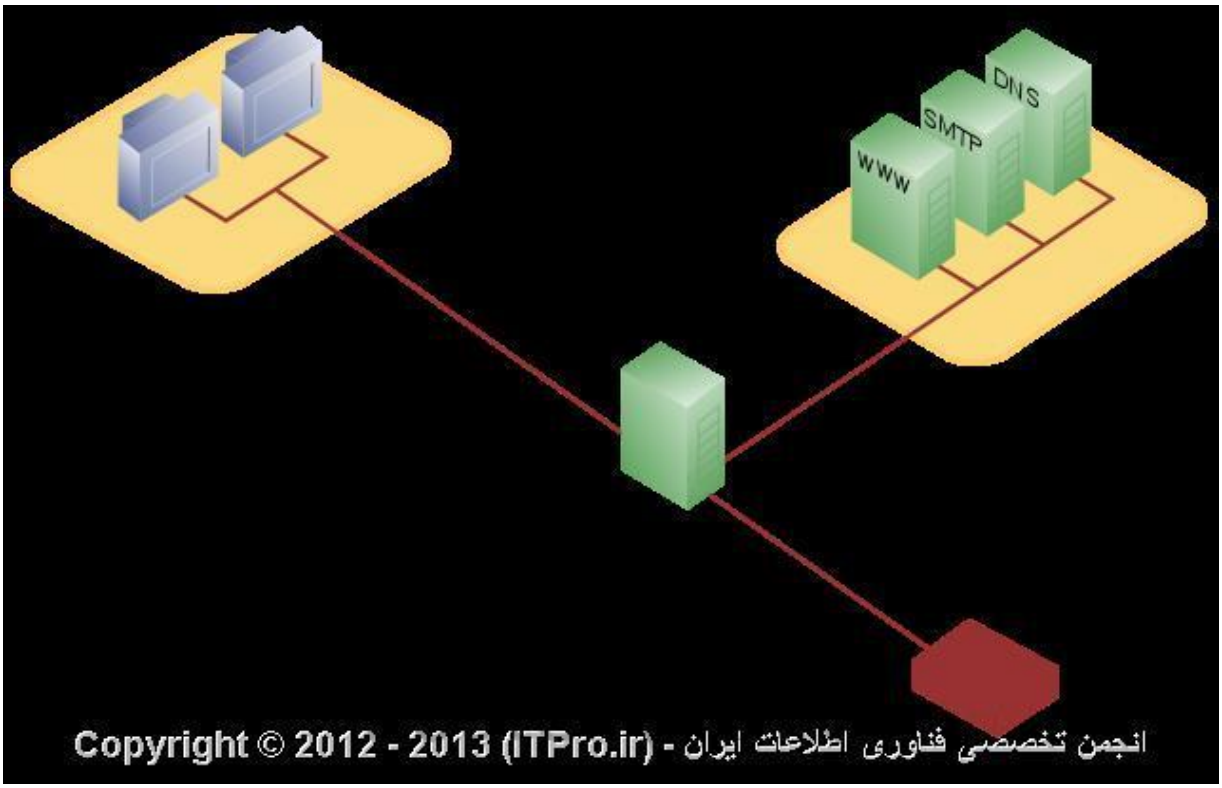
متمرکز سازی فرآیند فیلترکردن وب سایت ها و محتویات وب

ممکن است در اینجا این سئوال پیش بیاید که حال اگر نیاز به این باشد که کاربری بتواند از بیرون به شبکه داخلی دسترسی پیدا کند ، آیا ساختار DMZ این امکان را به وی می دهد یا خیر ؟ در پاسخ به این سئوال بایستی بگوییم که سرویسی به نام Reverse Proxy وجود دارد که امکان دسترسی پیدا کردن کاربران خارجی به منابع داخلی شبکه را فراهم می کند ، همانطور که Proxy Server به کاربران داخلی سرویس می دهد ، Reverse Proxy عکس این عمل را انجام می دهد ، یعنی به کاربران خارجی دسترسی داخلی را می دهد. برای مثال فرض کنید که شما در ساختار DMZ خود یک سرویس ایمیل دارید ، و کاربران اینترنتی از آن استفاده می کنند ، اما مدیر همین سرور تصمیم می گیرد به این سرور که در شبکه داخلی قرار داشته و توسط فایروال Publish شده است دسترسی پیدا کند ، چه مشکلی پیش می آید ؟ با استفاده از Reverse Proxy شما می توانید به وی اجازه برقرار ارتباط Remote به سرور مورد نظر را بدهید . توجه کنید که در چنین حالت هایی برای کاهش خطرات موجود شما از فایروال های لایه هفتم یا Application Layer Firewall ها استفاده می کنید تا درصد بروز حملات به سرورها از طریق Reverse Proxy را کاهش دهید. این روش امن ترین روش برقراری ارتباط از خارج شبکه به داخل آن می باشد.

معماری ها مختلف در ساختار DMZ

همانطور که اشاره کردیم روش های زیادی برای طراحی DMZ وجود دارد و هر کس می تواند با توجه به شرایط موجود طراحی ویژه سازمان خود از این روش را داشته باشد. شما می توانید در طراحی های DMZ از یک فایروال با ۳ کارت شبکه ، یا از چندین فایروال جداگانه استفاده کنید. البته اینها طراحی های ساده ای از DMZ هستند ، DMZ می تواند در ابعاد بسیار گسترده آنقدر بزرگ و پیچیده شود که واقعا در حد این مقاله نمی باشد. این که چگونه DMZ را طراحی می کنید کاملا به نیازمندی های سازمانی شما بستگی دارد و طبیعی است که هر چقدر پول بدهید آش می خورید. در ادامه دو نوع از روش های معمولی که DMZ طراحی می شود را برای شما شرح می دهیم :

DMZ با استفاده از یک فایروال

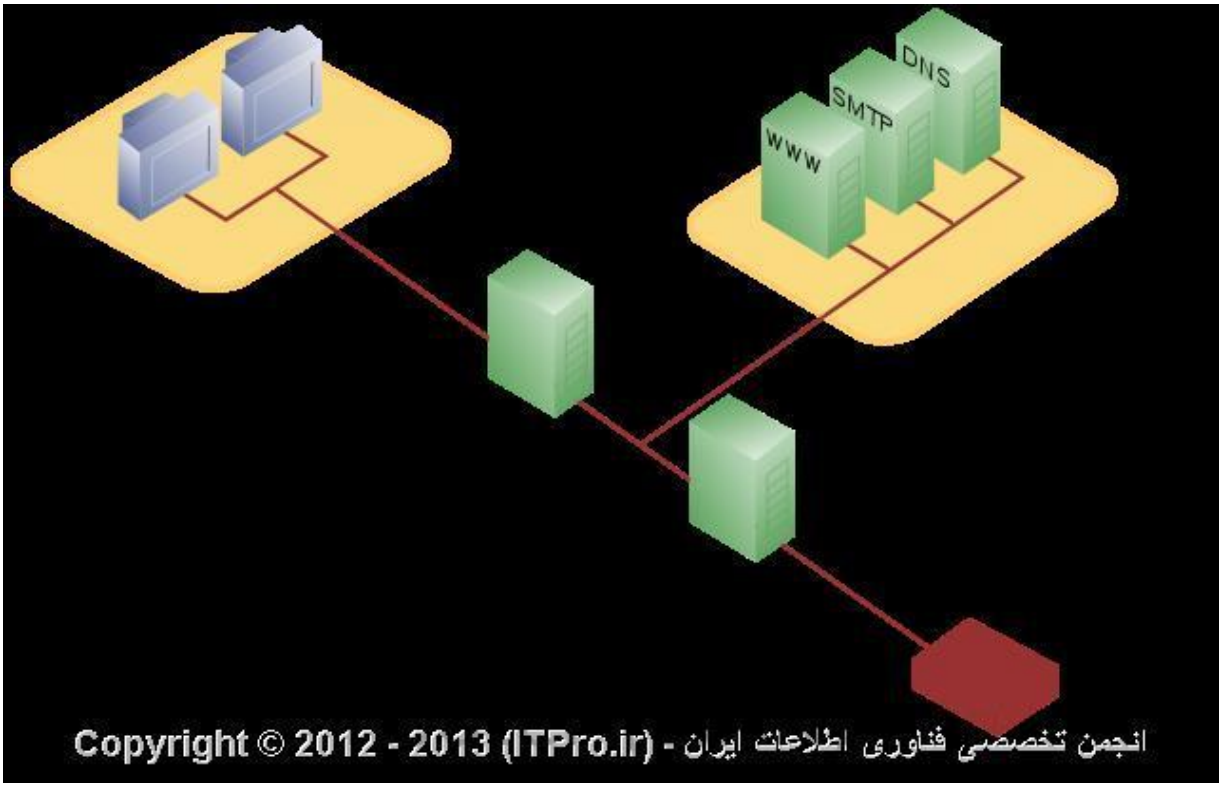


در این حالت شما یک فایروال سخت افزاری یا نرم افزاری دارید که دارای حداقل سه کارت شبکه می باشد که طراحی DMZ شما در این سه کارت شبکه جای می گیرد. ارتباط خارجی شما که به اینترنت و شبکه ISP متصل می شود به درون کارت شبکه اول متصل می شود. شبکه داخلی شما به کارت شبکه دوم موجود و در نهایت شبکه DMZ شما نیز به کارت شبکه سومی که بر روی فایروال قرار دارد متصل می شود. در اینجا فایروال ما یک Single Point Of Failure ایجاد کرده است ، به این معنی که با از بین رفتن این فایروال یا بروز اختلال در آن کلیه شبکه هایی که به آن متصل شده اند دچار مشکل خواهند شد. همچنین اگر ترافیک بین شبکه ها زیاد باشد این فایروال به تنهایی ممکن است نتواند سرویس دهی را انجام دهد و شبکه شما کند شود. به هر یک از این کارت شبکه ها در اصطلاح یک Zone یا محدوده گفته می شود. معمولا برای نمایش این ساختار برای مستند سازی از رنگ بنفش برای شبکه داخلی ، سبز برای شبکه DMZ و قرمز برای شبکه اینترنت استفاده می شود.

طراحی ساختار DMZ در شبکه

****

با استفاده از دو فایروالDMZ



استفاده از دو عدد فایروال در طراحی DMZ یکی از امن ترین طراحی های موجود در DMZ را به شما ارائه می دهد. اولین فایروال که به آن front-end firewall هم گفته می شود به گونه ای تنظیم می شود که ترافیک را از شبکه اینترنت دریافت و به آن ارسال می کند ، این ترافیک قاعدتا ابتدا به Zone ای که به DMZ معروف است متصل می شود. فایروال دوم به گونه ای تنظیم می شود که ترافیک ورودی و خروجی به شبکه داخلی را مدیریت می کند و در اصطلاح به آن back-end firewall گفته می شود.

طراحی ساختار DMZ در شبکه

این طراحی از امنیت بیشتری برخوردار است ، دلایل مختلفی برای اثبات این موضوع وجود دارد. ایجاد مشکل و خرابکاری در دو فایروال طبیعی است که از یک فایروال سخت تر است و یک هکر به ناچار بایستی انرژی بیشتری برای هک این سرورها بگذارد. اگر فایروالهای مورد استفاده در این طراحی از دو نوع مختلف باشند ، درجه امنیتی را بالاتر خواهند برد ، وجود نقطه ضعف امنیتی در یکی از سرورها باعث بروز مشکل در سرور دیگری یا فایروال دیگری نخواهد شد. برای مثال فرض کنید که در چنین طراحی ، به عنوان front-end فایروال

نرم افزاری TMG و به عنوان فایروال داخلی یا back-end فایروال سیسکو ASA قـرار داده ایـد ، حـال اگـر نقطـه ضعف امنیتی بر روی TMG وجود داشته باشد و هکر بتواند به منطقه DMZ نفوذ کند ، به دلیل عدم وجود همین نقطه ضعف در فایروال ASA حمله در همین نقطه باقی خواهد ماند.ITPro باشید.

****