به دلیل بیماری و همچنین سورپرایز چند روزی نمیتونم ویدیو تولید کنم از همگی عذرخواهی میکنم

ارسال پیام خصوصی ()

() () ()

مشاهده پروفایل (http://itpro.ir/profiles/unity)

امتیازات این مطلب

۱- UNITY

۹۴۵ امتیاز

مشاهده پروفایل (http://itpro.ir/profiles/unity)

۲- taher

۵ امتیاز

مشاهده پروفایل (http://itpro.ir/profiles/taher)

مقاله: معرفی ساختار DMZ یا Demilitarized Zone ()

زمان ارسال: ۳۹ ماه قبل جزیره امنیت اطلاعات و ارتباطات ()

پسندها (۲۷ نفر) ۳۹۲۴ بازدید

-آ آ +آ () () () ()

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.

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 (http://itpro.ir/gotorel/technichaltext/۳۱۰۱۰) 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 :

۱. سرویس دهنده های وب یا Web Server ها
۲. سرویس دهنده های ایمیل یا Mail Server ها
۳. سرویس دهنده های Voip
۴. 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.

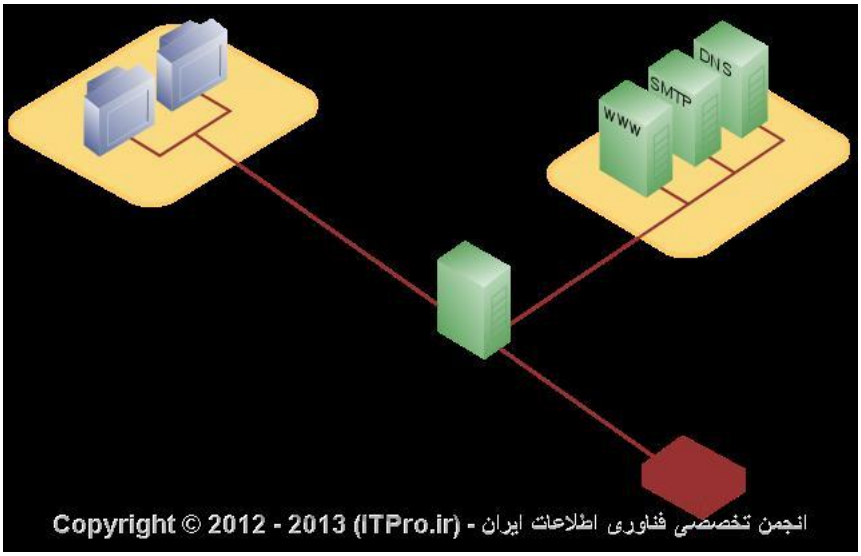
معماری ها مختلف در ساختار DMZ

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

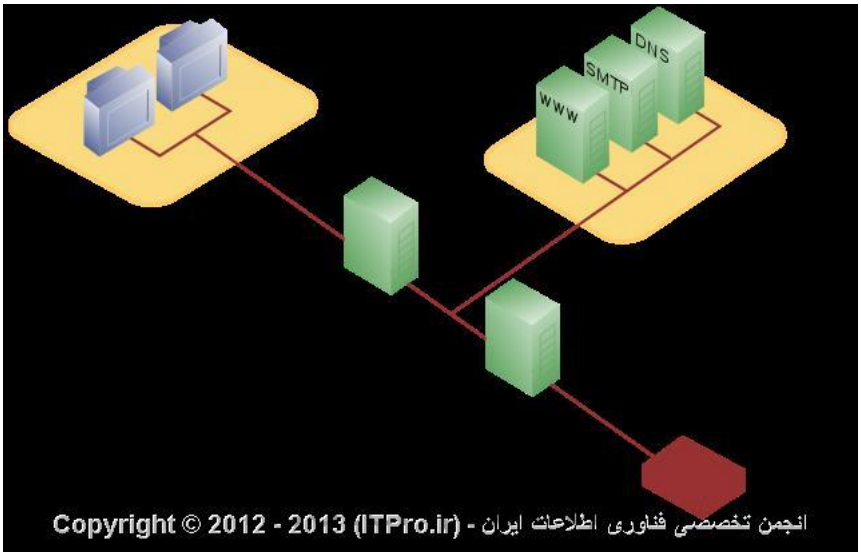
در این حالت شما یک فایروال سخت افزاری یا نرم افزاری دارید که دارای حداقل سه کارت شبکه می باشد که طراحی DMZ شما در این سه کارت شبکه جای می گیرد. ارتباط خارجی شما که به اینترنت و شبکه ISP متصل می شود به درون کارت شبکه اول متصل می شود. شبکه داخلی شما به کارت شبکه دوم موجود و در نهایت شبکه DMZ شما نیز به 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.



DMZ با استفاده از دو فایروال

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.



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 قرار داده اید ، حال اگر نقطه 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.**

نویسنده : محمد نصیری

منبع : انجمن حرفه ای های فناوری اطلاعات ایران

هرگونه نشر و کپی برداری بدون ذکر منبع و نام نویسنده دارای اشکال اخلاقی می باشد

برچسب ها

تفاوت فایروال و پروکسی
(http://itpro.ir/tags/%d۸%aa%d۹%۸۱%d۸%a۷%d۹%۸۸%d۸%aa%۲۰%d۹%۸۱%d۸%a۷%db%۸c%d۸%b۱%d۹%۸۸%d۸%a۷%d۹%۸۴%۲۰%d۹%۸۸%۲۰%d۹%be%d۸%b۱%d۹%۸۸%da%a۹%d۸%b۳%db%۸c)

فایروال چیست (http://itpro.ir/tags/%d۹%۸۱%d۸%a۷%db%۸c%d۸%b۱%d۹%۸۸%d۸%a۷%d۹%۸۴%۲۰%da%۸۶%db%۸c%d۸%b۳%d۸%aa)