✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

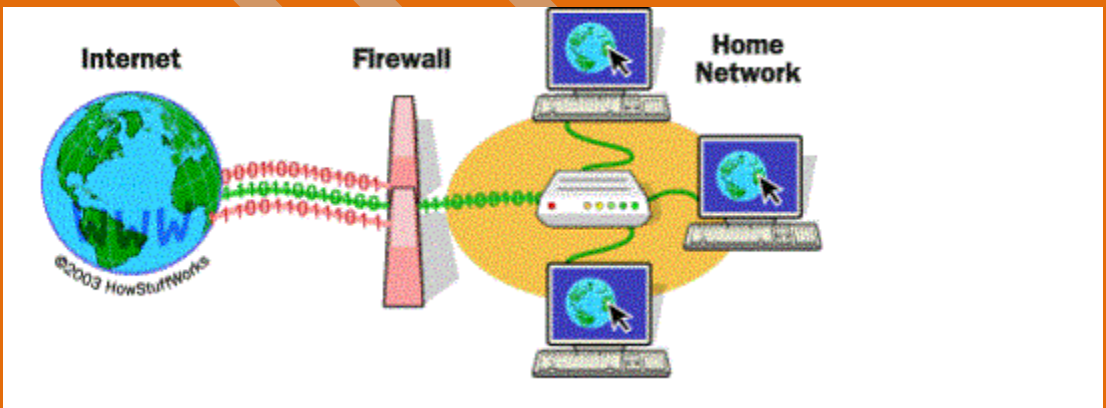
https://telegram.me/karnil

# نحوه ی عملکرد فایروال ها

پسران افتاب

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 مقاله 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 که از طریق اتصال به اینترنت بین شبکه خصوصی و یا سیستم کامپیوتر شما و جهان خارج رد و بدل می شود. اگر بسته 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 شرکت به طور طبیعی صدها دستگاه کامپیوتر دارد که تمام آنها توسط کارت های شبکه به هم متصل شده اند. علاوه بر این، شرکت دارای یک یا چند اتصال به اینترنت از طریق چیزی شبیه خطوط ADSL یا ماهواره است. بدون استفاده از فایروال 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 کارمند مرتکب اشتباهی شود و حفره امنیتی در رایانه خود ایجاد کند، هکرها می توانند به دستگاه او نفوذ کرده و از حفره به 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 اینترنت آید) فایروال یا دیواره آتش تنظیم کند. فایروال می تواند پیاده سازی قوانین امنیتی مدنظر مدیران شبکه را بسیار آسان نماید. به عنوان 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. پس 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 شبکه راه دور (Telnet) و غیره راه اندازی کند. علاوه بر این، شرکت می تواند چگونگی اتصال کارکنان به سایت های اینترنتی، اعم از آنکه چه 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 خارجی توسط کاربران شبکه 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 روتر 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 کنترل آن از راه دور گردد، به طرق مختلفی ممکن است از سیستم تان سوءاستفاده کند. این توانایی طیف مختلفی 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 دسترسی مخفی را برای کنترل برنامه توسط هکر فراهم می کند.

• ربودن جلسه SMTP (SMTP session hijacking) - SMTP رایج ترین روش ارسال ایمیل در اینترنت است. یک 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 میزبان 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 ها هم backdoor دارند. برخی سیستم های عامل هم امکان دسترسی از راه دور را البته با امنیتی ناکافی یا اشکالات نرم افزاری برای 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 افتد این است که هکر درخواستی به سرور برای اتصال به آن می فرستد. هنگامی که سرور پاسخ درخواست را می فرستد و سعی در برقراری جلسه (session) دارد، قادر نیست سیستم درخواست کننده را پیدا کند. با تعداد 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.

پسر ان افتاب مرجع نشرونویسندگی کتابهای الکترونیکی

www.sunboys.ir

www.parlaq.ir