آشنایی با Firewall و طرز کار آنها

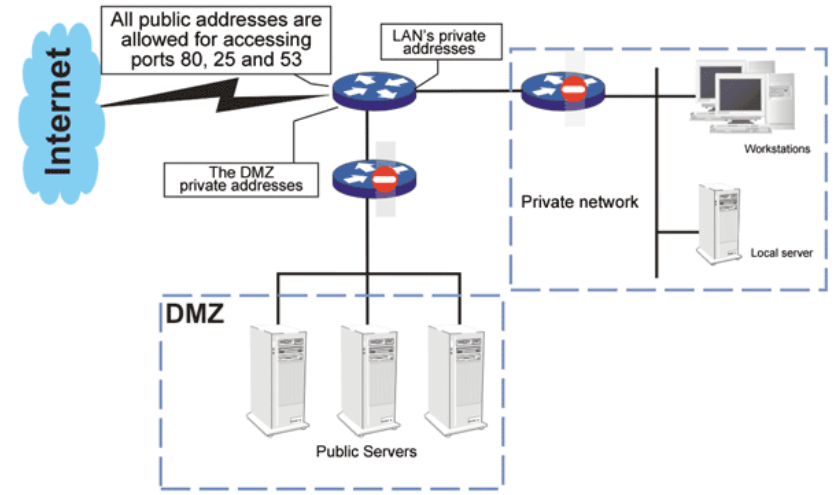
وقتی قرار باشد از یک ساختمان و وسایل داخل آن محافظت کنیم، اولین کاری که انجام می دهیم، کنترل مبادی ورود و خروج ساختمان است. به بیان دیگر فقط به افراد منتخبی ، اجازه وارد شدن (و یا خارج شدن) از ساختمان را می دهیم. معیار انتخاب افراد برای کسی که مامور کنترل ورود و خروج است بایستی در چارچوب یک خط مشی امنیتی، از قبل مشخص باشد.

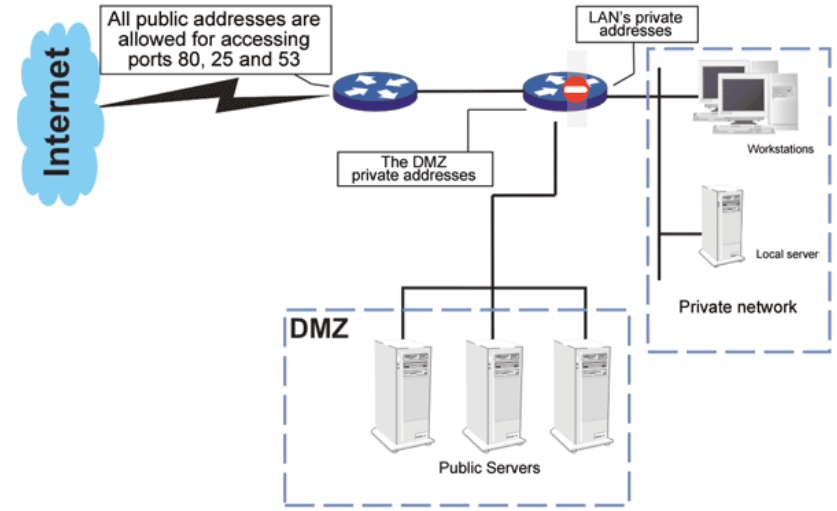
در مورد شبکه‌های کامپیوتری نیز بطور مشخص، همین روال را پیش می گیریم. یعنی مرزهای شبکه داخلی خود را کنترل می‌کنیم. منظور از مرز شبکه، لبه تماس شبکه داخلی با شبکه(های) خارجی نظیر اینترنت، شبکه یکی از شعب سازمان و یا شبکه یک سازمان دیگر است.

برای کنترل این مرزها از Firewall استفاده می‌شود

با پیاده‌سازی تکنیک‌های Packet Filtering ، بخشی از وظایف یک Firewall را می توان به Router های لب مرز واگذار کرد. ولی Router ها به تنهایی قادر به انجام کل وظایف یک Firewall نیستند و استفاده از Firewall ها امری اجتناب ناپذیر است. دلیل ناکافی بودن Packet Filtering در Router لب مرز دو چیز است: یکی اینکه اصولا" تمامی تکنیک‌هایی که در Firewall ها پیاده سازی می‌شوند، در Router قابل اجرا نیست و گذشته از آن، اصل دفاع لایه به لایه (یا دفاع در عمق) میگوید که محافظت بایستی در بیش از یک لایه انجام شود. (مانند دژهای قدیمی که با لایه‌های مختلف (خندق، دروازه اصلی، دروازه‌های فرعی، برجها و ...) از آنها محافظت می‌شد.

در شکل‌های زیر یک نمونه از پیاده سازی Firewall ها را مشاهده می کنید.





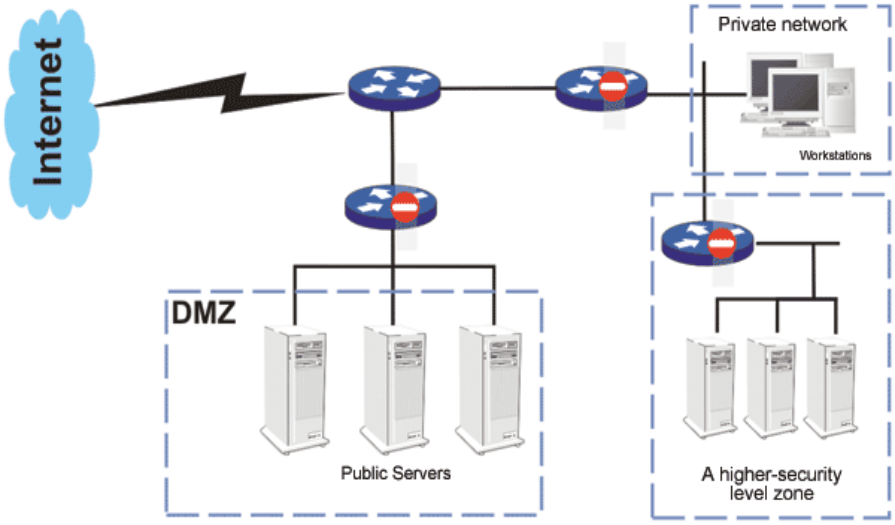
در شکل‌های فوق، Router لب مرز، ترافیک را در سطح IP کنترل می کند. این Router اولین لایه دفاعی شبکه محسوب می‌شود. همانطور که مشاهده می‌شود در این Router فقط به کاربرانی از اینترنت اجازه عبور داده می شود که متقاضی یکی از سرویس‌های وب، پست الکترونیک و یا DNS باشند.

در هر شکل ناحیه وجود دارد موسوم به DMZ مخفف DeMilitarized Zone که در این ناحیه سرورهایی را قرار میدهیم که بایستی از اینترنت دیده شوند مانندWeb Server ، E-Mail Serverو .DNS Server اگر بخواهیم DMZ را با یک مثال روشنتر توصیف کنیم، بایستی بگوییم که DMZ مانند نمایشگاه و فروشگاه یک شرکت است که تقریبا" به همه اجازه داده میشود به داخل آن بیایند و از محصولات ما دیدن کنند، اصولا" نمایشگاه به همین منظور ایجاد شده، فلسفه وجودی Web Server این است که از اینترنت دیده شود.

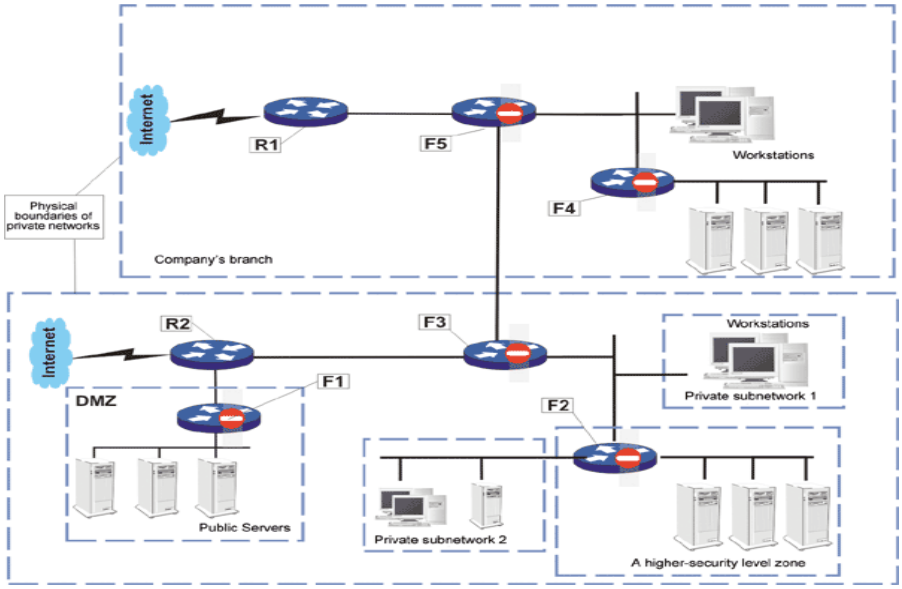
ناحیه دیگری که در شبکه‌ها وجود دارد، ناحیه Private Network است. هیچ بسته‌ای از طریق اینترنت اجازه ورود به ناحیه اختصاصی شبکه ما را ندارد مگر آنکه یکی از طرف یکی از کاربران داخلی درخواست شده باشد .

پس در ساده‌ترین شکل، شبکه ما از سه ناحیهPublic Network ، DMZ و Private Network تشکیل شده و در مرز هر کدام از این نواحی بایستی تمهیدات کنترلی اتخاذ کرده و عبور و مرور بسته‌های اطلاعاتی را کنترل کنیم. در ادامه مقاله از این سه بخش تحت عناوین Internat، DMZ و LAN نام خواهیم برد.

ممکن است علاوه بر سه ناحیه فوق، در ناحیهLAN ، بخشی داشته باشیم که از نظر حساسیت در سطح بالاتری نسبت به سایر LAN باشد. این ناحیه، ناحیه‌ایست که سرورهای حساس شبکه مانند سرور مالی و یا فایل سرور بخش تحقیق و توسعه قرارداد. برای این ناحیه لازم است Firewall مجزایی پیاده سازی شود. این Firewall لایه‌ای است که به لایه‌های امنیتی اضافه شده و دسترسی غیر مجاز به این ناحیه را مشکل‌تر می‌کند:



به شکل زیر توجه کنید : (Router ها با R و Firewall ها با F مشخص شده‌اند)



همانطور که ملاحظه می‌کنید، R1و R2 بعنوانRouter های لب مرز شبکه‌ها را از اینترنت جدا کرده‌اند. در کل مجموعه، یک DMZ داریم که با F1 از بقیه مجموعه جدا شده است F3 .و F5 دو وظیفه بعهده دارند، یکی مرز بین اینترنت وLAN های مربوط به خود را کنترل میکنند، و دیگر اینکه ارتباط بین دو LAN را کنترل می‌کنند این ارتباط ممکن است Lease Line ، Wireless و یا یک زوج سیم مسی باشد. این Firewalها با پشتیبانی از سرویس VPN ، ارتباط داخلی امنی را بین دفترمرکزی و شعبه برقرار میکنند .

اما F2 و F4 نیز در شرایط مشابهی هستند، این دو وظیفه جدا سازی منطقه حساس را از بقیه LAN بر عهده دارند و علاوه برآن F2 دو Subnetموجود در شبکه دفتر مرکزی را نیز از هم جدا میکند. جداسازیSubnet ها از هم در راستای محدود کردن حملات احتمالی است. اگر به نحوی یکی ازSubnet ها مورد حمله واقع شد، (مثلا "باWorm ی که از طریق e-mail و یا حتی از طریق دیسکت و CD وارد آن شده) این آلودگی به همان Subnet محدود شده و سایر بخشهای شبکه ایمن باقی بمانند.

نتیجه گیری:

دیدیم که برای تامین امنیت یک شبکه، Firewall اولین چیزی است که بایستی پیاده سازی شود. نکته حائز اهمیت آنکه، نصب یک Firewall در شبکه به تنهایی امنیت آن شبکه را تامین نخواهد کرد، آنچه مهمتر است، تعریف قواعد کنترل (Rules) و اعمال تنظیمات اولیه و همچنین مهمتر از آن به روزرسانی قواعد برمبنای تکنیکهای نفوذ و حملات جدید است.

پایان

امید شمس دیوبند

پائیز ۱۳۸۴

www.clicker.blogfa.com