*Firewall*چيست ؟

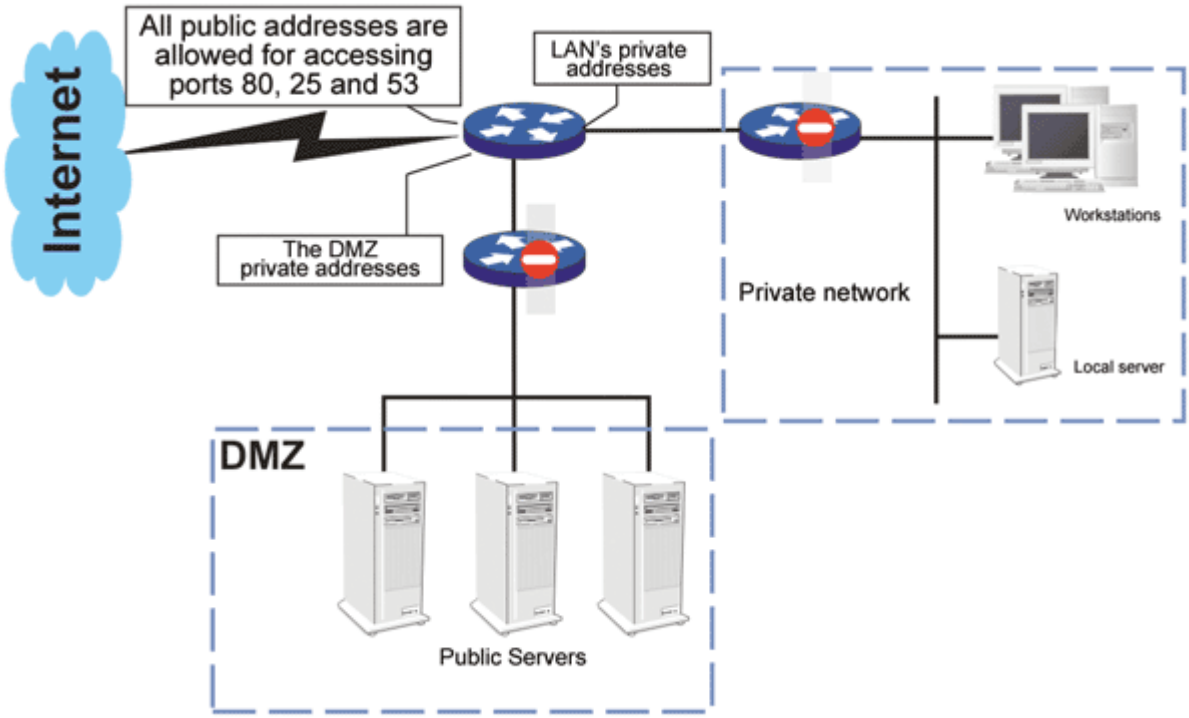
وقتي قرار باشد از يك ساختمان و وسايل داخل آن محافظت كنيم، اولين كاري كه انجام می دهيم، كنترل مبادي ورود و خروج ساختمان است. به بيان ديگر فقط به افراد منتخبي ، اجازه وارد شدن (و يا خارج شدن) از ساختمان را می دهيم. معيار انتخاب افراد براي كسي كه مامور كنترل ورود و خروج است بايستي در چارچوب يك خط مشي امنيتي، از قبل مشخص باشد.

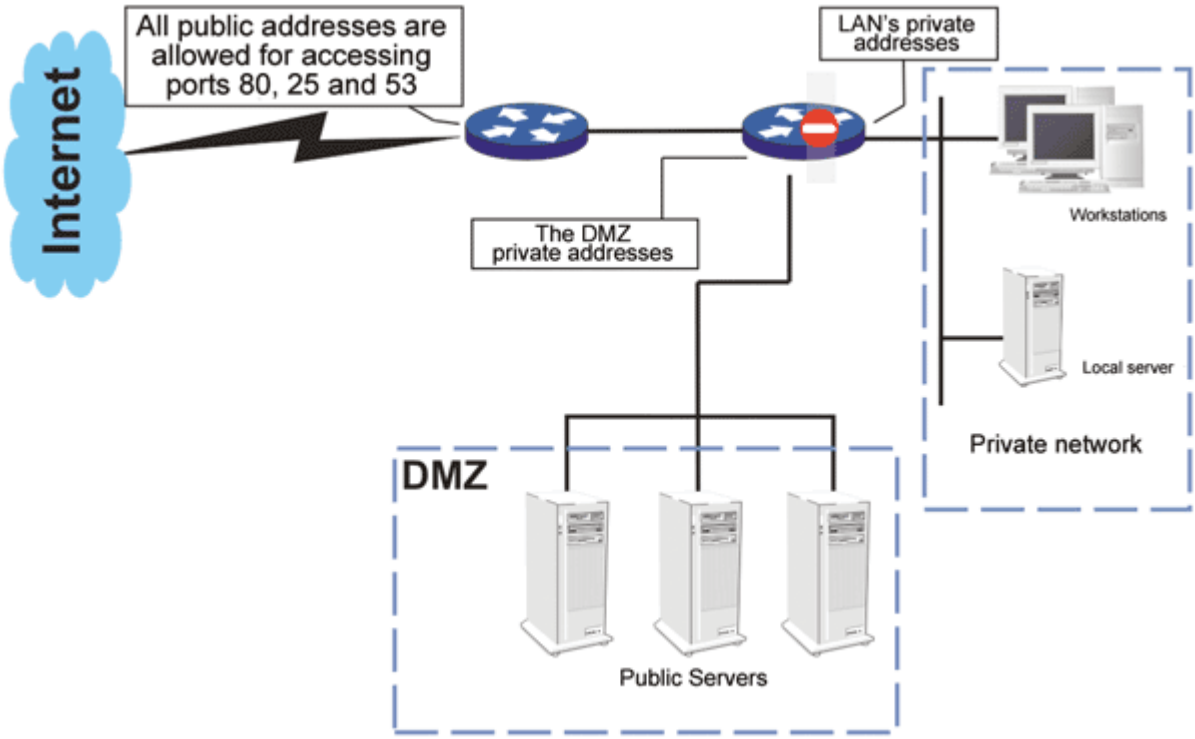
در مورد شبكه‌هاي كامپيوتري نيز بطور مشخص، همين روال را پيش می گيريم. يعني مرزهاي شبكه داخلي خود را كنترل مي‌كنيم. منظور از مرز شبكه، لبه تماس شبكه داخلي با شبكه(هاي) خارجي نظير اينترنت، شبكه يكي از شعب سازمان و يا شبكه يك سازمان ديگر است.

براي كنترل اين مرزها از Firewall استفاده مي‌شود

با پياده‌سازي تكنيك‌هاي Packet Filtering، بخشي از وظايف يك Firewall را می توان به Router(هاي) لب مرز واگذار كرد. ولي Routerها به تنهايي قادر به انجام كل وظايف يك Firewall نيستند و استفاده از Firewallها امري اجتناب ناپذير است. دليل ناكافي بودن Packet Filtering در Router لب مرز دو چيز است: يكي اينكه اصولا" تمامي تكنيك‌هايي كه در Firewallها پياده سازي مي‌شوند، در Router قابل اجرا نيست و گذشته از آن، اصل دفاع لايه به لايه (يا دفاع در عمق) ميگويد كه محافظت بايستي در بيش از يك لايه انجام شود. (مانند دژهاي قديمي كه با لايه‌هاي مختلف (خندق، دروازه اصلي، دروازه‌هاي فرعي، برجها و ...) از آنها محافظت مي‌شد.

در شكل‌هاي زير يك نمونه از پياده سازي Firewallها را مشاهده می كنيد.





در شكل‌هاي فوق، Router لب مرز، ترافيك را در سطح IP كنترل می كند. اين Router اولين لايه دفاعي شبكه محسوب مي‌شود. همانطور كه مشاهده مي‌شود در اين Router فقط به كاربراني از اينترنت اجازه عبور داده مي شود كه متقاضي يكي از سرويس‌هاي وب، پست الكترونيك و يا DNS باشند.

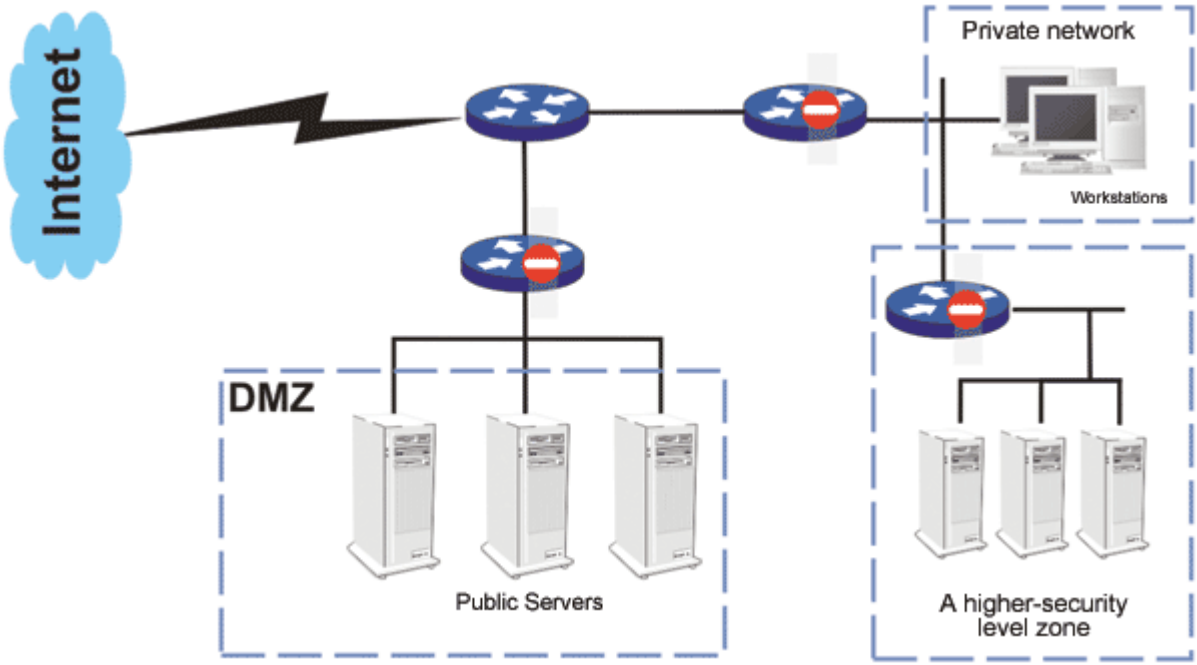
در هر شكل ناحيه وجود دارد موسوم به DMZ مخفف DeMilitarized Zone كه در اين ناحيه سرورهايي را قرار ميدهيم كه بايستي از اينترنت ديده شوند مانند Web Server، E-Mail Server و DNS Server. اگر بخواهيم DMZ را با يك مثال روشنتر توصيف كنيم، بايستي بگوييم كه DMZ مانند نمايشگاه و فروشگاه يك شركت است كه تقريبا" به همه اجازه داده مي‌شود به داخل آن بيايند و از محصولات ما ديدن كنند، اصولا" نمايشگاه به همين منظور ايجاد شده، فلسفه وجودي Web Server اين است كه از اينترنت ديده شود.

ناحيه ديگري كه در شبكه‌ها وجود دارد، ناحيه Private Network است. هيچ بسته‌اي از طريق اينترنت اجازه ورود به ناحيه اختصاصي شبكه ما را ندارد مگر آنكه يكي از طرف يكي از كاربران داخلي درخواست شده باشد.

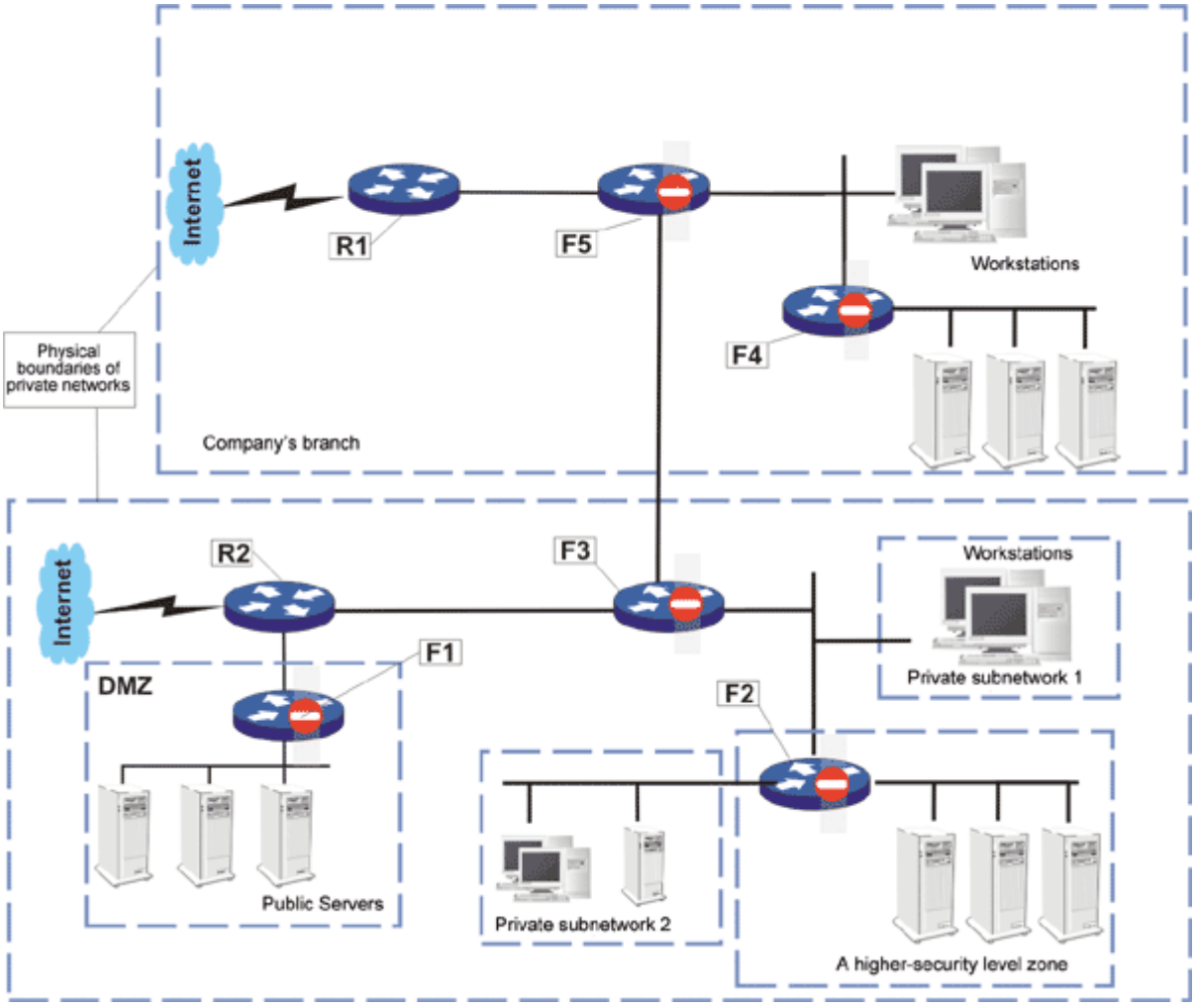
پس در ساده‌ترين شكل، شبكه ما از سه ناحيه Public Network، DMZ و Private Network تشكيل شده و در مرز هر كدام از اين نواحي بايستي تمهيدات كنترلي اتخاذ كرده و عبور و مرور بسته‌هاي اطلاعاتي را كنترل كنيم. در ادامه مقاله از اين سه بخش تحت عناوين Internat، DMZ و LAN نام خواهيم برد.

ممكن است علاوه بر سه ناحيه فوق، در ناحيه LAN، بخشي داشته باشيم كه از نظر حساسيت در سطح بالاتري نسبت به ساير LAN باشد. اين ناحيه، ناحيه‌ايست كه سرورهاي حساس شبكه مانند سرور مالي و يا فايل سرور بخش تحقيق و توسعه قرارداد. براي اين ناحيه لازم است Firewall مجزايي پياده سازي شود. اين Firewall لايه‌اي است كه به لايه‌هاي امنيتي اضافه شده و دسترسي غير مجاز به اين ناحيه را مشكل‌تر مي‌كند:

د:



به شکل زیر توجه کنید: (Routerها با R و Firewallها با F مشخص شده‌اند)



همانطور كه ملاحظه مي‌كنيد، R1 و R2 بعنوان Routerهاي لب مرز شبكه‌ها را از اينترنت جدا كرده‌اند. در كل مجموعه، يك DMZ داريم كه با F1 از بقيه مجموعه جدا شده است. F3 و F5 دو وظيفه بعهده دارند، يكي مرز بين اينترنت و LANهاي مربوط به خود را كنترل ميكنند، و ديگر اينكه ارتباط بين دو LAN را كنترل مي‌كنند اين ارتباط ممكن است Lease Line، Wireless و يا يك زوج سيم مسي باشد. اين Firewallها با پشتيباني از سرويس VPN، ارتباط داخلي امني را بين دفترمركزي و شعبه برقرار ميكنند.

اما F2 و F4 نيز در شرايط مشابهي هستند، اين دو وظيفه جدا سازي منطقه حساس را از بقيه LAN بر عهده دارند و علاوه برآن F2 دو Subnet موجود در شبكه دفتر مركزي را نيز از هم جدا ميكند. جداسازي Subnetها از هم در راستاي محدود كردن حملات احتمالي است. اگر به نحوي يكي از Subnetها مورد حمله واقع شد، (مثلا" با Wormي كه از طريق e-mail و يا حتي از طريق ديسكت و CD وارد آن شده) اين آلودگي به همان Subnet محدود شده و ساير بخشهاي شبكه ايمن باقي بمانند.

نتيجه گيري:

ديديم كه برای تامين امنيت يك شبكه، Firewall اولين چيزی است كه بايستی پياده سازی شود. نكته حائز اهميت آنكه، نصب يك Firewall در شبكه به تنهايی امنيت آن شبكه را تامين نخواهد كرد، آنچه مهمتر است، تعريف قواعد كنترل (Rules) و اعمال تنظيمات اوليه و همچنين مهمتر از آن به روزرسانی قواعد برمبنای تكنيكهای نفوذ و حملات جديد است.

فايروال وسيله ای است كه كنترل دسترسی به يک شبكه را بنابر سياست امنيتی شبكه تعريف می كند.علاوه بر آن از آنجايی كه معمولا يک فايروال بر سر راه ورودی يک شبكه می نشيند لذا برای ترجمه آدرس شبكه نيز بكار گرفته می شود.

مشخصه های مهم يک فايروال قوی و مناسب جهت ايجاد يک شبكه امن عبارتند از:

۱- توانايی ثبت و اخطار :ثبت وقايع يكی از مشخصه های بسيار مهم يک فايروال به شمار می شود و به مديران شبكه اين امكان را می دهد كه انجام حملات را كنترل كنند. همچنين مدير شبكه می تواند با كمک اطلاعات ثبت شده به كنترل ترافيک ايجاد شده توسط كاربران مجاز بپردازد. در يک روال ثبت مناسب ، مدير می تواند براحتی به بخشهای مهم از اطلاعات ثبت شده دسترسی پيدا كند. همچنين يک فايروال خوب بايد بتواند علاوه بر ثبت وقايع، در شرايط بحرانی، مدير شبكه را از وقايع مطلع كند و برای وی اخطار بفرستد.

۲- بازديد حجم بالايی از بسته های اطلاعات: يكی از تستهای يک فايروال ، توانايی آن در بازديد حجم بالايی از بسته های اطلاعاتی بدون كاهش چشمگير كارايی شبكه است. حجم داده ای كه يک فايروال می تواند كنترل كند برای شبكه های مختلف متفاوت است اما يک فايروال قطعا نبايد به گلوگاه شبكه تحت حفاظتش تبديل شود.عوامل مختلفی در سرعت پردازش اطلاعات توسط فايروال نقش دارند. بيشترين محدوديتها از طرف سرعت پردازنده و بهينه سازی كد نرم افزار بر كارايی فايروال تحميل می شوند. عامل محدودكننده ديگر می تواند كارتهای واسطی باشد كه بر روی فايروال نصب می شوند. فايروالی كه بعضی كارها مانند صدور اخطار ، كنترل دسترسی مبنی بر URL و بررسی وقايع ثبت شده را به نرم افزارهای ديگر می سپارد از سرعت و كارايی بيشتر و بهتری برخوردار است.

۳- سادگی پيكربندی: سادگی پيكربندی شامل امكان راه اندازی سريع فايروال و مشاهده سريع خطاها و مشكلات است.در واقع بسياری از مشكلات امنيتی كه دامنگير شبكه های می شود به پيكربندی غلط فايروال بر می گردد. لذا پيكربندی سريع و ساده يک فايروال ، امكان بروز خطا را كم می كند. برای مثال امكان نمايش گرافيكی معماری شبكه و يا ابزرای كه بتواند سياستهای امنيتی را به پيكربندی ترجمه كند ، برای يک فايروال بسيار مهم است.

۴- امنیت و افزونگی فایروال: امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است.فایروالی که نتواند امنیت خود را تامین کند ، قطعا اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال ، تامین کننده امنیت فایروال و شبکه است:

الف- امنیت سیستم عامل فایروال : اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می کند، نقاط ضعف امنیتی سیستم عامل ، می تواند نقاط ضعف فایروال نیز به حساب بیاید. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی : یک فایروال باید مکانیزمهای امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روشها می تواند رمزنگاری را همراه با روشهای مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

انواع فایروال

انواع مختلف فایروال کم و بیش کارهایی را که اشاره کردیم ، انجام می دهند، اما روش انجام کار توسط انواع مختلف ، متفاوت است که این امر منجر به تفاوت در کارایی و سطح امنیت پیشنهادی فایروال می شود.بر این اساس فایروالها را به ۵ گروه تقسیم می کنند.

۱- فایروالهای سطح مدار (Circuit-Level): این فایروالها به عنوان یک رله برای ارتباطات TCP عمل می کنند. آنها ارتباط TCP را با رایانه پشتشان قطع می کنند و خود به جای آن رایانه به پاسخگویی اولیه می پردازند.تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت رایانه مقصد جریان پیدا کند و تنها به بسته های داده ای مرتبط اجازه عبور می دهند. این نوع از فایروالها هیچ داده درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند. ضمنا امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند.

۲- فایروالهای پروکسی سرور : فایروالهای پروکسی سرور به بررسی بسته های اطلاعات در لایه کاربرد می پردازد. یک پروکسی سرور درخواست ارائه شده توسط برنامه های کاربردی پشتش را قطع می کند و خود به جای آنها درخواست را ارسال می کند.نتیجه درخواست را نیز ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند. این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی امنیت بالایی را تامین می کند. از آنجایی که این فایروالها پروتکلهای سطح کاربرد را می شناسند ، لذا می توانند بر مبنای این پروتکلها محدودیتهایی را ایجاد کنند. همچنین آنها می توانند با بررسی محتوای بسته های داده ای به ایجاد محدودیتهای لازم بپردازند. البته این سطح بررسی می تواند به کندی این فایروالها بیانجامد. همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کند، کارایی آنها بیشتر کاهش می یابد. اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتوان داین فایروالها را به کار بگیرد.هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد

فایروال چگونه کار مي‌کنند؟ (بخش نخست)

دنياي امروز که به دنياي اطلاعات يا عصر ارتباطات لقب گرفته است و انسان‌ها در اين عصر در پي به دست آوردن اطلاعات از سراسر دنيا و در موضوعات گوناگون هستند و در اين ميان شبکه جهاني اينترنت نقش مهمي را ايفا مي‌کند.

اينترنت اطلاعات زيادي را براي كاربران كامپيوتر در خانه‌ها و ادارات و موسسات گوناگون در مورد مسائل تجاري و آموزشي و غيره فراهم كرده است كه براي بيشتر مردم دسترسي به چنين اطلاعاتي نه تنها يك حسن محسوب مي شود بلكه ضروري به نظر مي‌رسد.

به هر حال اتصال شبكه خصوصي به اينترنت مي‌تواند سبب در معرض قرار گرفتن اطلاعات مهم و محرمانه و در نتيجه تخريب اطلاعات شما توسط افراد مخرب سودجو در ديگر نقاط جهان شود.

افرادي كه كامپيوترشان را به اينترنت وصل مي‌كنند و از آن استفاده مي‌كنند و بايد از اين خطرات آگاه باشند و بدانند چگونه اطلاعات و سيستم‌هاي مهم خود را محافظت كنند.ما براي حفاظت از اطلاعات خودمان در مقابل تهاجم افراد مخرب سودجو از Firewall استفاده مي‌كنيم.

Firewall از كامپيوترهاي شخصي و همچنين از شبكه در برابر هجوم افراد مخرب در اينترنت مراقبت مي‌كند.چيزي كه بسيار اهميت دارد استفاده درست و بهينه از اين سيستم‌ها است.

Firewal چيست؟

Firewall كامپيوترهايي كه به صورت شبكه به هم وصل شده‌اند را از حملات نفوذگران سودجو و متخاصم بين‌المللي كه مي‌توانند اطلاعات داخل شبكه را كشف كنند يا اينكه آنها را از بين ببرند و يا اينكه سرويس‌ها را از كار بياندازند، محافظت مي‌كند.

Firewall ممكن است يك دستگاه سخت‌افزاري يا يك نرم‌افزار نصب شده بر روي كامپيوتر باشد كه باعث مي‌شود اطلاعاتي كه از طريق اينترنت در داخل شبكه شما يا كامپيوتر شما وارد مي‌گردد را فيلتر مي‌نمايد و به نفوذگران اجازه ورود به سيستم‌هاي شما و يا دسترسي به آنها را نمي‌دهد.

در هر حالت نرم‌افزاري يا سخت‌افزاري آنها بايد در يكي از دو حالت شبكه قرار گيرند. اول اينكه زماني كه شبكه براي حفاظت انتخاب شده و ديگري براي زماني كه شبكه در معرض ديد قرار گرفته.

Firewall در محل تقاطع يا اتصال دو شبكه قرار مي‌گيرد مثل شبكه خصوصي ما و شبكه عمومي مانند اينترنت.

Firewall هاي اوليه دقيقا شبيه يك مسير ياب عمل مي كردند و زماني Firewallها فقط يك قسمت از شبكه بودند كه شبكه را به يك شبكه با subnet ديگر متصل مي‌كرد.

در گذشته براي اينكه جلوي آتش را در مزارع و جاهاي مختلف بگيرند از ديوار استفاده مي‌كردند و يك ديوار در دور تا دور جايي كه آتش مي‌گرفته، مي‌كشيدند تا آتش به جاهاي ديگر سرايت نكند و واژه Firewall از همان گرفته شده است و در كامپيوتر از تقسيم كردن شبكه به شبكه هاي كوچكتر سرچشمه مي‌گيرد و اين كار خطرات مربوط به پخش اطلاعات را كاهش مي‌دهد.

نكاتي كه براي پياده‌سازي Firewall به دانستن آنها نيازمنديم:

فيلترها مي‌توانند در جاهاي مختلف استفاده شوند كه به تعدادي از آنها ما اشاره خواهيم كرد و عبارتند از:

۱- آدرس IP :هر ماشين در اينترنت به وسيله يك آدرس واحد كه به آن آدرس IP گفته مي‌شود مشخص مي‌شود. آدرس IP داراي ۳۲ بيت شماره است كه از چهار octets داخل يك dotted docimal Number يك آدرس IP متداول بدين ترتيب است:

216.27.61.137. براي مثال اگر يك آدرس IP در خارج از شركت همواره فايل‌هاي زيادي را از روي سرور بخواند Firewallمي‌تواند تمام ترافيك را از روي آن آدرس IP ببندد.

۲- اسامي Domain : براي اينكه به خاطر سپردن آدرس IP كه از تعدادي زيادي عدد تشكيل شده بسيار مشكل است و بعضي اوقات آدرس‌هاي IP الزاما بايد تغيير كنند. تمام سرورها در روي اينترنت داراي اسامي قابل درك انسان‌ها هستند كه به آنها اسامي Domain گفته مي‌شود.

براي مثال براي بيشتر افراد آسان‌تر است كه به خاطر بسپارند www.howstuffworks.com تا اينكه به خاطر بسپارند. ۲۱۶,۲۷,۶۱,۱۳۷.

يك شركت ممكن است تمام دسترسي‌ها را به يك Domain مسدود كند و يا اينكه اجازه بدهد دسترسي به يك Domainمشخص صورت گيرد.

۳- پروتكل‌ها: قراردادي كه بين دو كاربر يا سيستم به طور يكسان تعريف مي‌شود كه آن دو بتوانند با يكديگر ارتباط برقرار كنند.

پروتكل‌ها به صورت text هستند و به طور ساده تشريح مي‌كنند كه چگونه مشتري client و سرور server مي‌توانند با يكديگر ارتباط برقرار كنند.

مانندhttpدر داخل پروتكل .web در زير چند نمونه از پروتكل‌ها كه فيلترهاي Firewall بر روي آن‌ست set مي‌شود آمده است:

IP (interenet protocol) - سيستم فرستنده اصلي براي كسب اطلاعات روي اينترنت.

TCP (transport control protocol) - استفاده مي‌شود براي اينكه جدا كند و يا اينكه بازسازي كند اطلاعاتي كه در اينترنت وجود دارند.

HTTP (Hyper text trsnsfer protocol)- استفاده مي‌شود براي صفحات web

FTP (File transter protocol) براي‌uploadپ down load فايل‌ها استفاده مي‌شود.

UDP (user datagram protocol) -استفاده مي‌شود براي اطلاعاتي كه هيچ گونه جوابي لازم ندارند مانند صوتي audioو تصويري.video

ICMP (INTERNET CONTROL MESSAGE) -استفاده مي‌شود به وسيله router تا به routerهاي ديگر تبادل اطلاعات نمايد.

SMTP (Sample mail transport) -استفاده مي‌شود براي فرستادن اطلاعات يا e-mail.

SNMP (Simple network transport protocol) -استفاده مي‌شود براي اينكه جمع‌آوري كند اطلاعات سيستم را از يك رموت كامپيوتر.

Telnet -استفاده مي‌شود براي انجام دستور در يك رموت كامپيوتر.

يك شركت مي‌تواند فقط يك يا دو ماشين را براي انجام يك پروتكل خاص به كار گيرد يا مي‌تواند پروتكل را در تمامي ماشين‌هاي ديگر متوقف نمايد.

٤- Port : اعدادي هستند كه ماشين سرور server سرويس‌هايش را از طريق آنها ارايه مي‌دهد.

براي مثال اگر سرور server يك وب HTTP را اجرا مي‌كند و يك سرور FTP را اجرا مي‌كند به طور معمول سرور وب در٨٠ -port در دسترس است و سرور FTP بايستي در١٢ - port در دسترس باشد يك شركت مي‌تواند ببندد١٢ -portرا براي دسترسي به تمام ماشين‌ها در داخل شركت كه به آن دسترسي نداشته باشند.

٥- كلمات و جملات مشخص:

كه اين كلمات مي‌تواند همه چيز باشد و Firewall مي‌تواند جست‌وجو كند هر پكيج اطلاعاتي براي مطابقت كامل با محتويات ليست شده داخل فيلتر. براي مثال شما مي‌توانيد درخواست كنيد از Firewall كه هر پكيج كه كلمه-x ratedروي آن است را ببندد و آن را باز نكند. نكته مهم در اينجا اين است كه مطابقت كامل داشته باشد مثلا فيلتر x-raterنمي‌تواند پيدا كند x-rated وليكن شما مي‌توانيد هر تعداد كلمه يا جمله يا تركيبي از آنها را كه احتياج است، استفاده كنيد.

يك firewall software مي‌تواند نصب شود روي كامپيوتر داخل منزل شما كه به اينترنت وصل است. اين كامپيوتر خوانده مي‌شود gateway براي اينكه به وجود مي‌آورد يك نقطه دسترسي از شبكه منزل شما به اينترنت.

FIREWALL چه كاري انجام مي‌دهد:

Firewall كل ترافيك بين دو شبكه را بازرسي كرده تا واقعا با ضوابط و معيارها مطابقت كنند اگر اين طور بود كه ترافيك عبور مي‌كند در غير اين صورت آن را متوقف مي نمايد.

يك Firewall ترافيك ورودي و خروجي را فيلتر مي‌نمايد همچنين مي‌تواند كه دسترسي عمومي به شبكه خصوصي و منابع آن از قبيل برنامه‌هاي ميزبان را مديريت كند.

Firewall مي‌تواند مورد استفاده قرار بگيرد و جهت گزارش كردن كليه تلاش‌هايي كه جهت اتصال به شبكه خصوصي صورت مي‌گيرد و فعال كردن اعلان خطر وقتي كه نفوذگر يا ورود كاربري كه بدون مجوز وارد شبكه مي‌شود يا سعي مي‌كند وارد شود.

Firewall مي‌تواند كه بسته‌هاي ارسالي را برپايه آدرس مبدا و مقصد و شماره پورت جدا نمايد اين راه به فيلتر آدرس‌ها معروف است همچنين مي‌توانند انواع خاصي از ترافيك شبكه را كنترل نمايند. اين راه را كنترل پورت مي نامند. زيرا سيستم معين كننده جهت عبور يا برگرداندن ترافيك وابسته به استفاده از پروتكل‌ها است براي مثال TELNET,HTTP, FTPهمچنين مي‌توانند بسته را برحسب مشخصه و وضعيت آنها كنترل نمايند.

در اينجا، يك مثال براي شما مي‌آوريم. فرض كنيد كه يك شركت با ٥٠٠ كارمند كار مي كند و شركت هم براي آنها صدها كامپيوتر دارد كه همه داراي كارت شبكه مي‌باشند و به همه مرتبط هستند و همچنين اين شركت داراي يك يا چند راه ارتباطي از طريق خطوط١ T3, T به اينترنت خواهد بود بدون Firewall در تمام آن صدها كامپيوتر مستقيما

به خطوط اينترنت متصل مي‌شوند و كسي كه مي‌خواهد با ما ارتباط برقرار كند به وسيله‌هاي گوناگون مانند FTP.telnetو ... با ما مرتبط مي‌شود.

در اين هنگام اگر يكي از كارمندان ما يك اشتباه مرتكب شود و يك راه نفوذ برجا گذارد سود جريان از همين راه استفاده مي‌كنند و از اطلاعات ما بهره‌برداري مي‌كنند و يا آنها را از بين مي‌برند.

اگر Firewall در محل خودش قرار گيرد چشم‌انداز خيلي متفاوت مي‌شود و در اين موقع شركت Firewall را در هر نقطه ارتباطي به اينترنت قرار مي‌دهد.

Firewall مي‌تواند قوانين امنيتي را نيز به اجرا در بياورد يكي از قوانين امنيتي يك شركت مي‌تواند اين باشد كه از ميان۵۰۰ كامپيوتر متعلق به اين شركت فقط يكي از آنها اجازه دارد كه ترافيك عمومي FTP را دريافت كند.و آن قوانين ارتباطي FTP را فقط منحصر به آن كامپيوتر كنند و مانع استفاده ديگر كامپيوترها از آن شوند.

يك شركت مي‌تواند قوانين مانند اين را براي سرورهاي FTP يا سرورهاي WEB با سرورهاي Telnet و غيره وضع كند.به اضافه آن شركت مورد نظر مي‌تواند نحوه اتصال كاركنان خود را به وب سايت كنترل كند حتي فايل‌هايي كه اجازه خروج از شركت را از طريق شبكه دارند و غيره Firewall. به شركت توانايي كنترل نحوه استفاده كاركنان از شبكه را مي‌ده

Firewall چه كاري نمي‌تواند انجام دهد:

Firewall نمي‌تواند كه يك كاربر شخصي كه با مودم به داخل يا خارج از شبكه متصل مي شود را كنترل نمايد در حقيقت اين عمل را كنار زدن Firewall گويند كارمندان خلافكار و يا بي‌دقت را نمي‌توان توسط Firewall كنترل كرد براي همين بايد از سياست پيشگيري يا استفاده توسط رمزهاي عبور و مجوز به كاربران با نهايت قدرت استفاده كرد اينها تماما پي‌آمد مديريت هستند كه بايد به طور كامل برنامه‌ريزي شود و قوانين امنيتي به كار گرفته شوند اما اين مشكل توسط Firewall حل نمي‌شود. اطلاعات گردآوري‌شده نشان مي‌دهد كه از اين طريق اطلاعات شركت‌هاي BritshATو communication T و خيلي از شركت‌هاي بزرگ به خاطر بي‌دقتي در اعمال قوانين داخلي به سرقت رفته‌اند بيشتر اين اعمال توسط كارشناسان خود شركت‌ها و يا كارمندان شياد و اخراجي آنها روي داده است و در هر صورت Firewall در اين زمينه كمكي نمي‌نمايد.

چه كسي به Firewall نياز دارد

هر شخصي كه مسوول ارتباط يك شبكه خصوصي به عمومي است نياز به حفاظت Firewall دارد از اين گذشته هر كسي كه از طريق مودم با كامپيوتر شخصي خود به اينترنت وصل مي شود نياز به Firewall شخصي دارد.

اغلب كاربران مودمي در اينترنت بر اين عقيده‌اند كه گمنامي مي‌تواند آنها را محافظت كند آنها احساس مي‌كنند كه نفوذگران با وجود Firewall تحريك مي شوند كه كامپيوتر آنها را از كار بياندازند. كاربران تلفني كه قرباني نفوذ گران بدخواه مي‌گردند نتايج كار يك روز خود را از دست مي‌دهند و گاهي اوقات مجبور به نصب مجدد سيستم عامل خود مي شوند برنامه‌هايي وجود دارد كه افراد متهاجم سودجو از آن استفاده مي‌كنند و تعداد زيادي شناسه را به صورت تصادفي جست‌وجو كرده و قرباني را انتخاب مي‌نمايند.

Firewall چگونه عمل مي‌نمايد:

دو راه براي عدم دسترسي توسطFirewall ها وجود دارد يك Firewall مي‌تواند به كل ترافيك اجازه دسترسي دهد مگر اينكه با قوانين و ضوابط خودش مغايرت داشته باشد و يا اينكه كل ترافيك را مسدود كند مگر اينكه با ضوابط و شرايط Firewall صدق نمايد. ضوابط استفاده مي‌شوند جهت تعيين اينكه ترافيك مي‌تواند از يك Firewall عبور نمايد يا خير.

يك Firewall ممكن است از انواع مختلف قوانين استفاده كند استفاده از آدرس مبدا و مقصد و شماره و پورت و نوع پروتكل تا استفاده از قوانين پيچيده‌تري نظير كنترل برنامه‌ها و دادن مجوز به آنها جهت انتقال ترافيك به ساير شبكه‌ها.

Firewall سيستم را در برابر چه چيزهايي محافظت مي‌كند:

Remote login

هنگاميكه شخصي بتواند با كامپيوترهاي ما ارتباط برقرار كند مي‌تواند به اطلاعات و فايل‌هاي ما دسترسي داشته باشد يكي از وظايفFirewallها اين است كه اجازه ورود اشخاص را به شبكه‌ها نمي‌دهد.

Application backdoors

برنامه‌هايي نظير Trojanها كه مي‌توانند كنترل يك سيستم را در اختيار شخصي قرار دهند.

Denial of service

انواع روش‌هاي حمله به شبكه كه باعث از كار انداختن سرويس‌هاي مختلف آن شبكه مي‌شوند.

Emali bombs

به معني ارسال پيام‌هاي اينترنتي در حجم‌هاي بسيار بالا مي باشد كه باعث مي‌شود سرويس e-mail مختل شود.

ويروس‌ها Virus

انواع ويروس هاي كامپيوتري كه باعث ايجاد مشكلات براي كاربران شبكه مي‌شود.

اسپم‌ها Spam

به معني پيام‌هاي اينترنتي ناخواسته كه باعث ايجاد مشكلات براي كاربران شبكه مي‌شود.

نحوه برخورد Firewall ها با موارد فوق بستگي به انتخاب نوع Firewall و ميزان امنيت آن دارد و يكي از بهترين روش‌ها اين است كه از ارتباط كليه اشخاص به شبكه جلوگيري شود.

دانستن اين كه يك Firewall چگونه كار مي كند به شما كمك مي‌كند كه روابط لايه‌هاي شبكه را بهتر متوجه شويد طراحان شبكه يك ساختار هفت لايه‌اي براي شبكه تعيين كرده‌اند كه هر لايه مسووليت خاص خود را دارا مي‌باشد. اين لايه‌ها شبكه را قادر مي‌سازند كه پروتكل‌هاي شبكه را با لايه‌هاي سخت‌افزاري همگام كنند. در يك شبكه معين يك پروتكل تا لايه بالايي سخت‌افزار بيشتر نمي‌تواند وارد شود زيرا لايه سخت‌افزار جداي از لايه پروتكل مي‌باشد. به همين صورت كه يك كابل فيزيكي نمي‌تواند بيشتر از لايه يك حركت كند.

TCP/IP قديمي‌تر از مدل OSI است اما استاندارد اين دو شبيه به هم نيست. در TCP/IP لايه‌هاي اول دقيقا مطابق مدل OSI هستند فايروال‌ها در لايه‌ها مختلف فعاليت مي‌كنند. پايين‌ترين لايه‌اي كه فايروال‌ها در آن كار مي‌كنند لايه سوم است كه در مدل OSI لايه شبكه و در TCP/IP لايه IP مي‌باشد.

كار اين لايه مسيريابي و ارسال بسته‌ها به مقصد مي‌باشد. در اين لايه Firewall مي‌تواند تشخيص دهد كه بسته از چه مبدايي آمده است اما نمي‌تواند محتويات بسته و يا اينكه بسته به چه بسته‌هاي ديگري وابسته است را مشخص كند Firewall در لايه ترانسپورت راجع به بسته كمي بيشتر اطلاعات دارد و قادر است كه اجازه يا عدم اجازه دسترسي با قوانين و ضوابط در سطوح بالاتري را صادر كند. در لايه، نرم‌افزار Firewall قدرت بسيار زيادي در صدور مجوزها براي بسته‌ها دارد و مشكل وقتي پديدار مي شود كه تابع Firewall را در داخل شبكه در سطح بالاتري نسبت به لايه برنامه‌ها قرار گيرد كه اين هيچ الزامي ندارد و كار كردن Firewall در سطوح پاييني شبكه باعث امنيت بيشتر آن مي‌شود.

اگر يك نفوذگر نتواند سه مرحله قبل را متعلق به خود كند مسلما نمي‌تواند كنترل سيستم عامل را در دست بگيرد. Firewallهاي جديد و پيشرفته كل ترافيك شبكه را در خود ذخيره كرده و اجازه نمي‌دهند كه آنها مستقيما به شبكه TCP/IP دسترسي پيدا كنند و اين كار را براي يك نفوذگر جهت نفوذ به سيستم و بازكردن درب پشتي براي نفوذ بعدي مشكل مي‌نمايد.

ديوارهاي آتش چگونه كار مي‌كنند؟

انواع مختلف Firewall كدامند؟

Firewall به چهار مقوله تقسيم مي‌شود:

1- packet filter

2- circuit level gateway

3- Firewall هاي سطح كاربردي

4 - Firewall هاي چند لايه‌اي

PACKETFILTERINGFIREWALL

اين Firewall ها در سطح شبكه (Network layer) مدل OSI يا لايه IP در مدل TCP/IP عمل مي‌كنند آنها بخشي از روتر (Router) هستند (روتر وسيله‌اي است كه بسته‌ها را از اينترنت دريافت مي‌كند و آنها را به سوي جهت ديگري مي‌فرستد.

در PACKETFILTERFIREWALL هر بسته طبق يك معيار بازرسي مي‌شود. سپس فرستاده مي‌شود و اين امر به نوع بسته و معيار آن بستگي دارد.

Firewall مي‌تواند بسته را به لايه بعدي بفرستد و يا پيغامي را به مبدا اصلي خود در مورد چگونگي عملكرد ارسال نمايد.

بهترين مزيت PACKETFILTERFIREWALL

ارزاني اجراي آن در اعمال مربوط به اينترنت مي‌باشد در بيشتر روترها (Router) مي‌توانيم از اين نوع firewall استفاده كنيم. پياده‌سازي اين گونه firewall در روتر باعث ايجاد امنيت در سطح لايه شبكه مي‌شود

CIRCUIT LEVEL GATEWAY

گونه ديگر FIREWALL كه با نام CIRCUIT LEVEL GATEWAY معرفي مي‌شود، در لايه حمل (Trasport) مدل OSI يا در سطح TCP از مدل TCP/IP عمل مي‌كند و بسته و بخش مورد استفاده را كنترل مي‌كند. اين روش براي پنهان كردن اطلاعات مهم روشي است بسيار مناسب و همچنين براي شبكه‌هاي خصوصي هم مي‌تواند به كار رود به عبارت ديگر آنها بسته‌هاي افراد را كنترل و يا فيلتر نمي‌نمايند.

براي فهميدن چگونگي عملكرد CIRCUIT LEVEL GATEWAY مثالي مي‌زنيم، كامپيوتر A درون شبكه‌اي قرار دارد كه به وسيله CIRCUIT LEVEL GATEWAY firewall محافظت مي‌شود .

اين كامپيوتر A مي‌خواهد صفحه وبي (Web page) را كه روي كامپيوتر B كه خارج از محدوده firewall قرار دارد را ببيند.

كامپيوتر A تقاضا براي صفحه وب را به كامپيوتر B مي‌فرستد، كه اين تقاضا قبل از فرستاده شدن كامپيوتر B در firewallبازرسي مي‌شود سپس كامپيوتر B شروع به فرستادن صفحات تقاضا شدن مي‌كند و اگر اين تقاضاها با تقاضاهاي دريافت شده كامپيوتر A مطابقت كند (كه اگر از نظر آدرس ip و port تطابق داشته باشند) به اطلاعات اجازه ارسال داده مي‌شود و در غير اين صورت ارسال آن متوقف مي‌گردد.

مزيت استفاده از اين گونه firewall اين است كه هيچ‌گونه مطالب درخواست نشده از خارج firewall اجازه ورود به كامپيوتر و شبكه را ندارند.

APPLICATION LEVEL GATEWAY FIREWALL

(APPLICATION LEVEL GATEWAY firewallهاي‌سطح كاربردي) كه با نام proxy نيز معرفي مي‌شوند، بسيار شبيه APPLICATION LEVEL GATEWAY عمل مي‌كنند به اين معني كه هر دو از ورود اطلاعات درخواست نشده به شبكه جلوگيري مي‌كنند.

تفاوت اين دو گونه firewall در روش‌هاي مختلف آنها در مديريت و رسيدگي به اطلاعات است.

فايروال‌هاي CIRCUIT LEVEL GATEWAY تنها آدرس و پورت مربوط به اطلاعات دريافت شده را بازرسي مي‌كنند.

اين گونه firewall ها هيچگونه دسترسي به خود اطلاعات ندارند در حالي‌كه APPLICATION LEVEL GATEWAY عمق بيشتري را بررسي مي‌كند.

برنامه‌هاي proxy قابليت‌هايي را براي ديدن اطلاعات دارا هستند مثل HTTP براي صفحات وب، FTP، SMTPو يا۳ POPبراي e-mail.

اين گونه firewall ها دو مزيت اساسي دارند.

اول اينكه هيچ ارتباطي مستقيمي بين كامپيوترهاي بيرون از شبكه و كامپيوترهايي كه توسط firewall محافظت مي‌شوند، وجود ندارد.

دومين مزيت اساسي اين كه تصفيه اطلاعات در اين نوع به معني بازرسي كل محتويات مي‌باشد.

*Stateful*فايروال چيست و چگونه كار مي كند؟

Stateful فايروال نوعي از فايروال است كه بررسي و رديابي وضعيت (State) ارتباطات شبكه را در موقع فيلتر كردن بسته هاي اطلاعاتي انجام مي دهد.

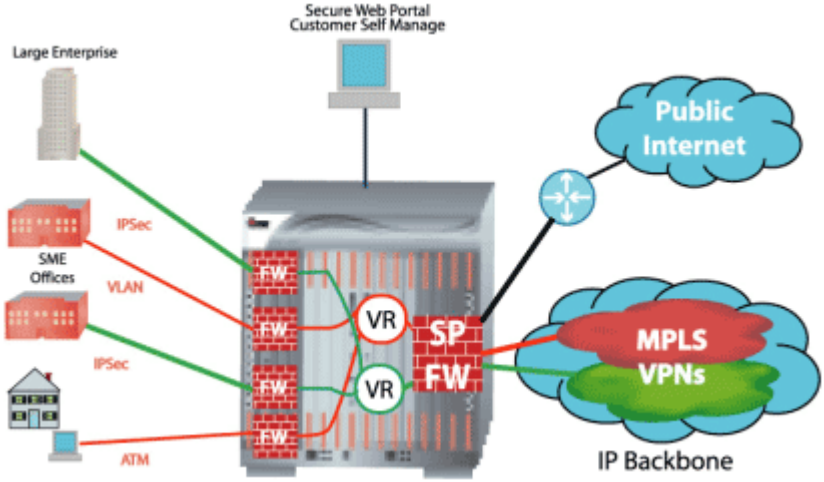
Stateful فايروال بيشتر كنترل و تست بسته هاي اطلاعاتي از لايه ۴ به پايين را انجام مي دهد. همچنين سيستم پيشرفته بازرسي را نيز جهت كنترل بسته هاي مورد نياز لايه ۷ ارائه مي دهد.

اگر بسته اطلاعاتي مجوز عبور از فايروال را دريافت نمايد، اجازه عبور به اين بسته داده شده و يك ركورد به جدول وضعيت(State Table) اضافه مي شود.

از اين به بعد ارتباط هايي كه از اين ركورد انتقال پيدا مي كنند بدون چك كردن لايه ۷ گذر داده مي شوند و فقط بسته هايي كه لازم است تا اطلاعات آنها كه شامل آدرس مبداء و مقصد و پورت Tcp/Udp مي باشند چك شود با اين جدول كنترل خواهند شد تا صحت آنها تاييد شود. اين روش كارآيي فايروال را افزايش خواهد داد چرا كه فقط بسته هاي اطلاعاتي كه مقدار دهي شده باشند ميبايست پردازش شوند.

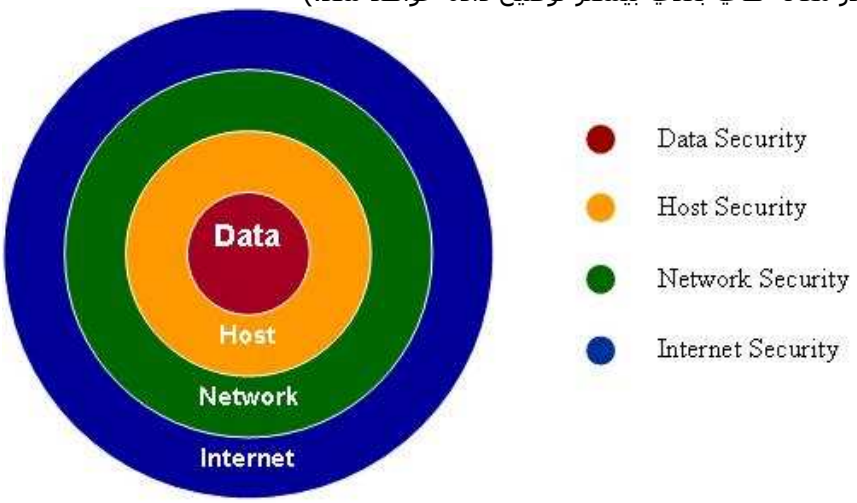
چون اين فايروالها براي فيلتر كردن از اصول مشابه استفاده مي كنند، دستورات لايه ۷ را در يك ارتباط در نظر نمي گيرند درصورتي كه پروكسي فايروال ها اين كار را انجام مي دهند. ناتواني فايروال ها، در كنترل كردن ارتباطات لايه ۷ نقطه ضعفي است كه در برابر پروكسي ها دارند در صورتيكه مزيت آنها كنترل دامنه وسيعي از پروتكل ها(در مقايسه با پروكسي ها كه محدوده كمتري از پروتكل هاي لايه ۷ را پشتيباني مي كنند) و سرعت بالاي آنها مي باشد و مي توانند بهترين انتخاب براي محافظت از شبكه باشند.

فايروال به منزله نقطه كنترلي شبكه مي باشد. از خصوصيات نقطه كنترلي يكي بودن و قابل كنترل بودن آن است. در اين نقطه كاهش ترافيك ورودي و خروجي را خواهيم داشت، درست مانند دستگاه فلز ياب فرودگاه كه افراد مي بايست نفر به نفر از آن عبور كنند و همين امر باعث كندي در مراحل انتقال مسافران خواهد بود. فايروال نقش دستگاه فلزياب را روي شبكه ايفا مي كند، به اين ترتيب كه تمامي ترافيك خروجي و ورودي به شبكه مي بايست توسط آن بازرسي شود و مزيت ديگر علاوه برکنترل، ثبت ورود و خروجها و دريافت گزارش مي باشد.



در اين قسمت مفهوم Defense-in-Depth يا دفاع در عمق را به خوبي مي توان دريافت. در مثال فوق اگر شخص خرابكار از بازرسي اول فرودگاه با موفقيت عبور كند در بازرسي هاي بعدي كه به منزله فايروال مي باشد و تا رسيدن به هواپيما قرار دارد، متوقف خواهد شد.

دفاع در عمق يعني دفاع لايه به لايه و قرار دادن عنصر مهم اطلاعاتي در مركز لايه.(بحث دفاع در عمق در مقاله هاي بعدي بيشتر توضيح داده خواهد شد.)



Stateful فايروال داراي يك جدول وضعيت است بطوري كه با اولين ارتباط كه از داخل فايروال مي گذرد اين جدول ايجاد شده و ركوردي در اين جدول ثبت مي شود كه حاوي اطلاعات زيادي از جمله آدرس مبدا و مقصد، پورت استفاده شده، Flag ها،Sequenceهاو... مي باشد. اين اطلاعات مي بايست تا حدي دقيق و مشخص آورده شود كه از ايجاد ترافيك توسط هكرها كه مجوز ورود آنها را به شبكه ميسر مي سازد، جلوگيري نمايد. نمونه اي از Stateful فايروال ها، فايروال هاي مبتني بر Netfilter/IPtabels مي باشند.