شبکه فن آوری اطلاعات ایران www.IRITN.com

آشنایی با دیواره آتش Firewalls

نوشته شده در تاریخ: دوشنبه,۷ فروردین ۱۳۸۵

از: دنیای رایانه

دیواره آتش Firewalls
مقدمه :
Firewall در فرهنگ کامپیوتر یعني محافظت از شبکه هاي داخلي در مقابل شبکه هاي خطاکار . معمولا يك شبکه کامپیوتري با تمام دسترسي ها در طرف و در طرف دیگر شما شبکه تولیدات شرکت را دارید که باید در مقابل رفتارهاي مخرب محافظت شود. چند سوال مطرح مي شود که آیا واقعا نیاز به محافظت از يك شبکه داخلي داریم و سوال دیگر اینکه چگونه از طریق يFirewall در فرهنگ کامپیوتر یعني محافظت از شبکه هاي داخلي در مقابل شبکه هاي خطاکار .

معمولا يك شبکه کامپیوتري با تمام دسترسي ها در طرف و در طرف دیگر شما شبکه تولیدات شرکت را دارید که باید در مقابل رفتارهاي مخرب محافظت شود. چند سوال مطرح مي شود که آیا واقعا نیاز به محافظت از يك شبکه داخلي داریم و سوال دیگر اینکه چگونه از طریق يك شبکه عمومي مانند اینترنت به آن دسترسي داشته باشیم .
دلیل بسیار ساده اي دارد ؟ که آن نیاز به بقاء و رقابت است . اعتبار کمپانیها در اینترنت به تبلیغات تولیداتشان مي باشد . اینترنت به صورت شگفت انگیزي در حال رشد است .
مانند يك فروشگاه بسیار بزرگ بیشتر مردم به طرف اینترنت مي آیند وهمانطوریکه در يك فروشگاه باید محصولات سالم باشند و بعد از فروش گارانتي بشوند اطلاعات و داده و انتقالات آنها نیز باید به صورت امن و گارانتي شده باشد .
حال باید مکانیزمهایي براي حفاظت از شبکه داخلي یا اینترنت شرکت در مقابل دسترسي هاي غیر مجاز ارائه دهیم

Firewall هاي مختلفي با ساختارهاي مختلف وجود دارد ولي عقیده اصلي که پشت آنها خوابیده یکسان است . شما به شبکه اي نیاز دارید که به کاربرانتان اجازه دسترسي به شبکه هاي عمومي مانند اینترنت را بدهد و برعکس .
مشکل زماني پیش مي آید که کمپاني شما بدون در نظر گرفتن معیارهاي امنیت بخواهد به اینترنت وصل شود و شما در معرض دسترسي از طرف Server هاي دیگر در اینترنت هستید. نه تنها شبکه داخلي کمپاني در مقابل دسترسي هاي غیر مجاز آسیب پذیر است بلکه تمام Server هاي موجود در شبکه کمپاني در معرض خطر هستند .
بنابراین به فکر محافظت از شبکه مي افتید و اینجاست که نیاز به يك Firewall احساس مي شود .
به هر حال قبل از فکر کردن درباره Firewall باید سرویسها واطلاعاتي که مي خواهید روي اینترنت در دسترس عموم قرار دهید مشخص کنید .
آشکارست که در ابتدا شما مي خواهید مطمئن شوید که سرور شما امن است شما مي توانید مجوزهاي دسترسي , انتقال فایل و اجراي راه دور و همچنین منع مجوزهاي ورود دوباره , Telnet , Ftp , SMTP ودیگر سرویسها . اگر شما بخواهید از این سرویسها استفاده کنید نیاز به Firewall دارید
به هر حال Firewall چیست ؟ اساسا يك فایروال جداکننده شبکه هاي امن از ناامن در اینترنت است . Firewall تمام اتصالاتي که از اینترنت به شبکه هاي محافظت وارد مي شوند را فیلتر مي کند .
قبل از تعریف اینکه چه نوع از Firewall ها بهترین مجموعه براي نیازهاي ماست , ما باید توپولوژي شبکه را براي تعیین اجزاي آن مانند Hub ها , Switch ها , Router ها و Cabling آنالیز کنیم تا بهترین Firewall که مخصوص این توپولوژي باشد را پیدا کنیم .
براي ایجاد امنیت در شبکه ما نیاز به بررسي شبکه داخلي از لحاظ مدل لایه بندي ISO آن داریم بطوریکه مي دانید Reapter ها و Hub ها در لایه اول , Switch ها و Bridge ها در لایه دوم و Router ها در لایه سوم , يك Firewall در تمام لایه هاي شبکه مي تواند عمل کند (از جمله در هر هفت لایه) لایه ها مسئول پاسخگویي به کنترل و ایجاد نشستها و بکارگیري آنها مي باشند . بنابراین با يك Firewall ما مي توانیم جریان اطلاعات را در طول ایجاد کنترل کنیم .
Firewall ها به ما امکان مدیریت دروازه هاي ورود به Web را مي دهد و امکان تمرکز روي پروژه اصلي را مي دهد .

The purpose of a Firewall

Firewall ها به تنهايي نمي توانند امنيت شبكه را برقرار كنند آنها فقط يك قسمت از سايت شما را امن مي كنند و به منظور امنيت شبكه بايد محدوده اي از شبكه را مشخص كنيد و نياز به اين داريد كه چيزهايي در شبكه كه بايد محدود شوند را تعيين كنيد ويك سياست امن را گسترش دهيد و مكانيسمهايي براي اعمال سياستهاي مورد نظر روي شبكه را ايجاد كنيد البته مكانيسمهايي پشت Firewall ها هستند كه مي توانيد به صورت عجيبي سطح امنيت را بالا ببريد .
اين مكانيسمها بعد از اعمال سياست امنيت مشخص مي شوند و نه قبل از آن . براي ايجاد يك مكانيسم امن براي محافظت از Web Site شما بايد يك Firewall براي نيازهاي خود مشخص كنيد وآن را پياده سازي كنيد.
ايجاد امنيت از سازماني به سازماني ديگر متفاوت است البته اين بستگي به چيزي كه آنها مخواهند توسعه دهند دارد . مثلا Firewall من اختصاصا روي UNIX , NT , Dos كار مي كند . شما دقيقا به بستر اجرايي مورد نظر خود دقت كنيد همانطور كه اجراي پروژه را مشخص مي كنيم بايد سطوح امنيت را نيز مشخص كنيم تا بتوانيم آن را پياده سازي كنيم . اين يك روش براي موفقيت در پياده سازي مكانيسمهاي امنيت است .
Firewall ها علاوه براين كه امنيت واقعي را برقرار مي كنند يك نقش اساسي در مديريت امنيت را پوشش مي دهند .

Firewall Role of Protection The

Firewall ها امنيت در شبكه را برقرار مي كنند و ريسك Server هاي روي شبكه را با فيلتر كردن كاهش مي دهند به عنوان مثال : شببكه داراي ريسك كمتري مي باشد به علت اينكه پروتكلهاي مشخص شده روي Firewall مي توانند روي شبكه اعمال وظيفه كنند .
مشكل فايروالها محدوديت آنها در دسترسي به و از اينترنت است و شما مجبور مي شويد كه از Proxy Server استفاده كنيد .
Firewalls Providing Access Control
سرورها مي توانند از بيرون قابل دسترس باشند مثلا كسي ويروسي را با Mail مي فرستند و بعد از اجرا , فايروال را از كار مي اندازد . بنابراين تا جايي كه امكان دارد از دسترسي مستقيم به سرورها جلوگيري كرد .

The Security Role of a Firewall
ما مي توانيم به جاي آنكه Server را محدود كنيم يك سرور را با تمام دسترسيهاي ممكن به اينترنت وصل كنيم و Server ديگر را پشت Firewall به عنوان Backup از سرور قبلي داشته باشيم . با هك شدن يا خرابي سرور اولي ما مي توانيم آن را بازيابي كنيم .
روشهاي ديگر براي اعمال امنيت روي شبكه ممكن است موجب تغييراتي روي هر Server شبكه شود ممكن است تكنيكهاي بهتري نسبت به Firewall ها باشد ولي Firewall ها براي پياده سازي بسيار آسان هستند براي اينكه Firewall ها فقط يك نرم افزار مخصوص هستند .
يكي از مزاياي Firewall ها استفاده آنها براي اينكه بتوانيم با Log كردن دسترسي به سايت آمار دسترسيهاي به سايت خود را مشخص كنيم

Advantages and Disadvantages of Firewalls

Firewall ها داراي مزاياي بسياري مي باشند با اين وجود داراي معايب نيز هستند . بعضي از Firewall در مقابل محدود كردن كاربران و درهاي پشتي (Back door) كه محل حمله هكرها ست كه امنيت ندارند .
Access Restrictions

Firewall ها براي ايجاد امنيت بعضي از سرويسها مانند Telnet , Ftp , Xwindow را از كار مي اندازند و اين تنها محدود به فايروالها نمي شود . بلكه در سطح سايت نيز مي شود اين كار را انجام داد .
Back-Door Challenges: The Modem Threat
تا حالا مشخص شد كه امنيت درهاي پشتي كمپاني به وسيله Firewall تامين نمي شود بنابراين اگر شما هيچ محدوديتي در دسترسي به مودم نداشته باشد اين در بازي براي هكرها ست
SLIP , PPP از راههاي ورودي مي باشند و سئوال پيش مي آيد كه اگر اين سرويسها وجود داشته باشند چرا از Firewall استفاده مي كنيم .

Risk of Insider Attacks

ريسك دسترسي اعضاي داخلي .

Firewall Components

Policy
Advanced Authentication
Packet Filtering
Application gateways

Network Security Policy

تصميم براي برپايي يك Firewall در شبكه دو سطحي مي باشد .
Installation , Use of the System

سياستهاي دسترسي به شبكه محدوديتهايي بر روي شبكه در سطح بالا به ما مي دهد . همچنين چگونگي به كارگيري اين سرويسها را نيز مشخص مي كند .
Flexibility Policy

اگر شما به عنوان گسترش دهنده يك سياست دسترسي به اينترنت يا مدير Web و سرويسهاي الكترونيكي معمولي هستيد اين سياستها به دلايل زير بايد انعطاف پذير باشند
اينترنت هر روز با سرعت غير قابل پيش بيني رشد مي كند . وقتي اينترنت تغيير تغيير مي كند سرويسهاي آن نيز تغيير مي كند . بنابراين سياستهاي كمپاني بايد تغيير كند و شما بايد آماده ويرايش و سازگار كردن اين سياستها بدون تغيير در امنيت اوليه باشد .
كمپاني شما داراي ريسكهاي متغير با زمان است و شما بايد در مقابل اين ريسكها امنيت پردازشها را تامين كنيد .

Service-Access Policy
سياستهاي دسترسي بايد روي ورودي كابران متمركز شود .

Advanced Authentication

با وجود استفاده از Firewall بسياري از نتايج بد در مورد امنيت از پسوردهاي ضعيف و غير قابل تغيير ناشي مي شوند .
پسوردها در اينترنت از راههاي زيادي شكسته مي شوند بنابراين بهترين پسوردها نيز بي ارزشند .
مسئله اين است كه پسوردهايي كه بايد با يك الگوريتم خاصي ساخته شوند مي توان با آناليز سيستم به پسوردها والگوريتم استفاده شده پي برد مگر اينكه پسوردها بسيار پيچيده باشند.يك كركر مي تواند با برنامه خود پسورد تعدادي از كاربران را امتحان كرده و با تركيب نتايج ساختار كلي الگوريتم استفاده شده را بدست آورد و پسورد كاربران مختلف را مشخص كند.
همچنين بايد فراموش نكرد كه بعضي از سرويسهاي TCP , UDP در سطح آدرس سرور هستند و نيازي به كاربران خاص خود ندارند .
به عنوان مثال يك هكر مي تواند آدرس IP خود را با سرور يك كاربر معتبر يكسان كند واز طريق اين كاربر يك مسير آزاد به سرور مورد نظر باز كند و اين كابر به عنوان يك واسط بين دو سرور عمل مي كند .
هكر مي تواند يك درخواست به كابر داده واين كاربر از سرور خود اطلاعات را به سرور هكر انتقال مي دهد.اين پروسه به عنوان IP Spoofing مي باشد.
بيشتر روترها بسته هاي مسير يابي شده منبع را بلاكه مي كنند و حتي مي توانند آنها از فيلتر Firewall بگذرانند.

Packet Filtering

معمولا IP Packet Filtering در يك روتر را بريا فيلتر كردن بسته هايي كه بين روترها مياني جابجا مي شوند به كار مي برند اين روترها بسته هاي IP را براساس فيلدهاي زير فيلتر مي كنند .

Source ip address
Destination ip address
Tcp/Udp source port
Tcp/Udp destination port

این خبر از سایت www.IRITN.com چاپ شده است.
/http://www.iritn.com

آدرس لینك این خبر:
http://www.iritn.com/index.php?action=show&type=news&id=10976