ارسال پیام خصوصی ()

() () () مشاهده پروفایل (http://itpro.ir/profiles/%d9%81%d8%a7%d8%b7%d9%85%d9%87%20%d9%82%d8%b1%d8%a8%d8%a7%d9%88%db%8c)

امتیازات این مطلب

۱- فاطمه قرباوی ۳۸۵ امتیاز

مشاهده پروفایل (http://itpro.ir/profiles/%d9%81%d8%a7%d8%b7%d9%85%d9%87%20%d9%82%d8%b1%d8%a8%d8%a7%d9%88%db%8c)

مقاله: تکنولوژی های فایروال -- Firewall Technologies ()

زمان ارسال: ۴۸ ماه قبل جزیره امنیت اطلاعات و ارتباطات ()

پسندها (۱۱ نفر) ۱۵۸۳ بازدید

-آ آ +آ () () () ()

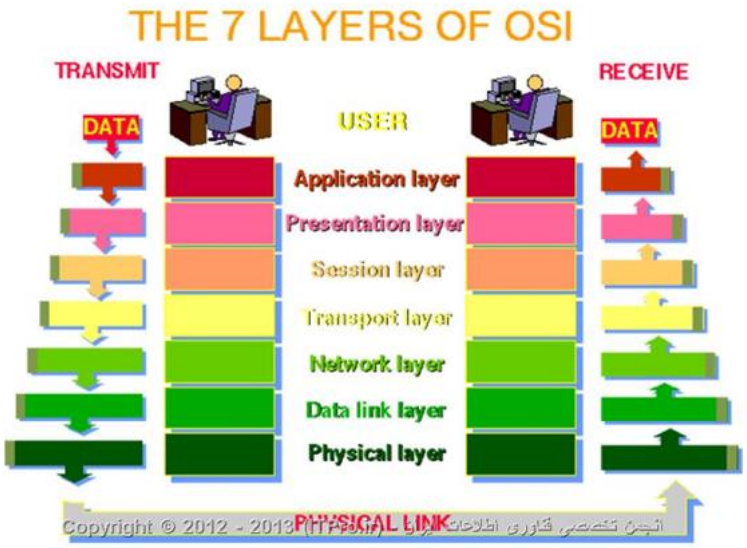
سلام...

در مقاله های قبلی در مورد اهمیت فایروال در میان دیگر تجهیزات امنیتی در سیستم ها و همینطور در سازمانها صحبت کردم و به معرفی جایگاه فایروالها در شبکه ها پرداختم.همچنین فاکتورهای مهمی که برای خرید یک فایروال باید در نظر بگیریم را معرفی کردم. اما در این مقاله قصد دارم از کلیات بیرون بیام و وارد جزئیات بشم .در واقع می خوام با یهه ذره بین به عمق فایروالها بروم .اینکه در بطن فایروالها چه اتفاقی می افتد و این packet های بیچاره در عبور از فایروالها چه بلایی بر سرشان می آید و از چه زوایایی مورد کالبد شکافی قرار میگیرند موضوع مورد بررسی در این مقاله است.به عبارتی در این مقاله به معرفی چهار تکنولوژی فایروال می پردازم و این چهار تکنولوژی رو از نظر پیکربندی،مزایا و عملکردشون مورد بررسی قرار میدهم.

حتما همه ی شما شنیدید که میگن خونه ای که پی اش محکم نباشه خونه نمیشه ! این در مورد فایروالها هم صدق میکنه.فایروالی که سیاست های محافظت در ریشه و عمق اون قوی باشه حتما یک فایروال خوب و محکم خواهد بود.اصطلاح و سیاست محافظت در عمق از سیاست های نظامی گرفته شده است که در این سیاست ها برای تضعیف هر چه بیشتر دشمن ،لایه های محافظتی متعددی ساخته میشده است.براساس IA یا Information Assurance ،محافت در عمق یعنی تولید سطوح مختلف حفاظ در شبکه برای محافظت از منابع، البته نه تنها برای یک محصول و تکنولوژی خاص ! به عنوان یک فردی که در زمینه ی IT مشغول فعالیت است،حتما هر وقت حرفی از لایه ها در شبکه باشد ذهن شما به سمت لایه های OSI کشیده می شود.بله درست حدس زدید :) ! فایروالها هم برای ساختن یک ریشه ی محکم و داشتن سیاست ها و استراتژیک های صحیح و اصولی در شبکه از لایه های OSI استفاده کرده اند.

مدل OSI و لایه های آن را حتما می شناسید،می توانید برای مطالعه ی بیشتر درمورد این مدل به‌مقاله ی جناب آقای نصیری (-۱۱/%D۹%۸۵%D۸%A۸%D۸%A۷%D۹%۸۶%DB%۸C%۲۰%D۸%B۴%D۸%A۸%DA%A۹%D۹%۸۷%۲۰%D۹%۸۲%D۸%B۳%D۹%۸۵%D۸%AA%۲۰%D۹%۸۷%D۹%۸۱%D۸%AF%D۹%۸۷%D۹%۸۵%۲۰-%۲۰%D۹%۸۷%D۹%۸۱%D۸%AA%۲۰%D۹%۸۴%D۸%A۷%DB%۸C%D۹%۸۷%۲۰OSI%۲۰%۲۰%DB%۸C%D۸%A۷%۲۰%D۹%۸۵%D۸%AF%D۹%۸۴%۲۰%D۹%۸۵%D۸%B۱%D۸%AC%D۸%B۹%۲۰OSI کنید.چرا که برای درک تکنولوژی فایروالها حتما باید لایه های Network ,Application,Session را به خوبی درک کرده باشید.

هر بسته یا packet دارای یک آدرس مبدا و یک آدرس مقصد می باشد و لایه ی network بر اساس این IP آدرس ها بسته ها را در شبکه منتقل می کند.زمانی که packet متوجه شد که در شبکه به کجا باید برود، لایه ی session دست بکار میشود و درواقع یک session تشکیل می شود.لایه ی session وظیفه ی شروع،مدیریت و اتمام session ها در شبکه را بر عهده دارد.درواقع شروع session ،سپس handshake یا همون دست دادن و در نهایت اتمام جلسه است.این لایه از پروتکل TCP استفاده می کند.لایه کاربردی یا Application Layer که به طور مستقیم با کاربر در ارتباط است برای انجام فعالیتهای شبکه به کار میرود.کلیه ی نرم افزارها در این لایه اجرا می شوند.این لایه از پروتکل http و ftp استفاده میکند.در شکل زیر مدل OSI را میتوانید مشاهده کنید.



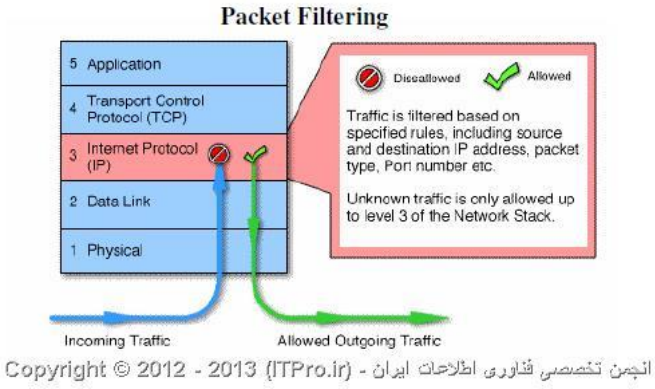
حال به سراغ انواع تکنولوژی در فایروال می رویم.این تکنولوژی ها به ۴ دسته تقسیم می شوند:

- Pcket Filtering Firewall
- Circuit Level Gateways
- Aplication Level Gateway
- Stateful Multilevel Inspection

Packet Filtering Firewall

این نوع فایروالها یکی از ساده ترین و معمولی ترین انواع فایروالها است که در سال ۱۹۸۵ عرضه شد . درواقع عنوان packet filtering بیان کننده همه چیز در رابطه با این دسته از فایرواهاست.داده های خام به عنوان frame یا packet وارد شبکه می شوند.در این مدل ،بسته ها براساس پروتکل،پورت یا آدرس مبدا و مقصد از کارت شبکه عبور می کنند یا در آن block می شوند.به عبارتی در این مدل،فایروال آدرس مبدا و مقصد هر بسته را چک میکند،در صورتی که آن آدرس با پروتکل،پورت و آدرس هایی که برایش غیر مجاز تعریف شده است منافاتی نداشته باشد بسته اجازه خروج یا ورود را دارد،اما اگر منافات داشت یا آنها را بی سروصدا دور می اندازد و یا به مبدایی که از آنجا می آیند پیغام خطایی جهت عدم ارسال بسته میفرستد.همانطور که پیداست این نسل از فایروالها تنها با لایه های اول OSI ،برای به دست آوردن IP ها سروکار دارند .به عنوان مثال اگر در شبکه ای استفاده از Remote desktop غیرمجاز محسوب شود،پورت ۳۳۸۹ که پورت مربوط به remote است بسته می شود از اینرو هر بسته ای که در IP خود این پورت را داشته باشد نیز بسته ی غیرمجاز محسوب می شود و توسط فایروال به دور انداخته می شود.

Stateful Packet Inspection تکامل یافته ی packet filtering است که در سال ۱۹۹۳ ارائه شد.SPI عملکردی مشابه با packet filtering دارد با این تفاوت که دارای حافظه ای است که کلیه ی ارتباطات داخلی و خارجی را ذخیره و نگهداری میکند.

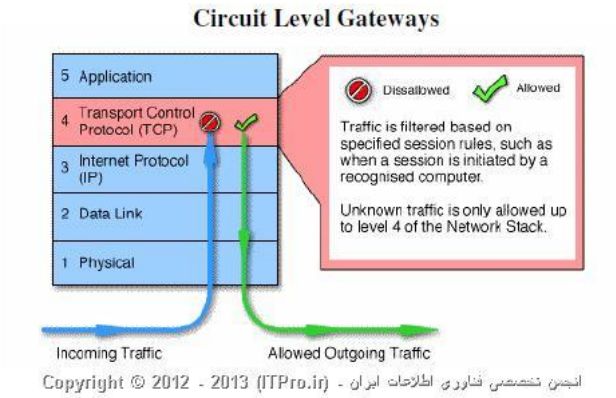


^ ()

Circuit Level Gateway

این دسته از فایروالها از دسته ی قبلی حرفه ای تر هستند.این نسل از فایروالها در سال ۱۹۸۹-۱۹۹۰ به میان آمدند.این دسته در لایه ی session مدل OSI کار می کنند و به عنوان واسط بین لایه کاربردی و لایه ی انتقال TCP/IP عمل می کنند و ترافیک شبکه را براساس آدرس و پورتها در لایه ی session فیلتر میکنند.زمانی که یک کامپیوتر تصمیم به برقراری ارتباط (ایجاد session) با کامپیوتری دیگر در خارج از شبکه میگیرد،gateway اطلاعات مربوط به این ارتباط را بررسی و چک میکند که این ارتباط بر اساس آدرس و شماره پورتش در شبکه مجاز است یا نه،سپس آن را به کامپیوتر مقصد میفرستد.تازمانی که gateway ارتباط را مجاز نشمارد،هیچ گونه دیتایی منتقل نمی شود.زمانی که دیتایی از gateway عبور میکند،کامپیوتر مقصد آدرس gateway را می بیند نه کامپیوتری که از آن دیتا ارسال شده است.این دسته از فایروالها از دسته ی قبلی دارای امنیت بیشتری هستند چرا که به عنوان مثال پس از ارسال اطلاعات به خارج از شبکه ، زمانی که همچنان یک session باز داریم،اگر به داخل شبکه نیز ارتباطی داشته باشیم،باز هم تنها پورتها و اطلاعات مجاز به ورود به داخل شبکه باز می شوند.همچنین از ورود ترافیک بیجا به داخل شبکه نیز جلوگیری می کنند. از معایبش این است که مادامی که circuit level gateway شبکه را در برابر ایجاد session های غیرمجاز محافظت میکند،قادر نیست آن را در برابر برخی حملات احتمالی محافظت کند که در مورد این موضوع بعدا صحبت خواهیم کرد.NAT مثالی از circuit level gateway است.NAT هم IP آدرس شبکه داخلی را از host مقصد مخفی نگه میدارد.سپس از packet filtering برای انتقال packet ها به مقصدصحیح خودشان استفاده میکند.

برای تفهیم بهتر این روش مثالی میزنم:فرض کنید کامپیوتر A در شبکه ای که توسط circuit level gateway محافظت می شود قرار دارد، و می خواهد یک صفحه وب را که در کامپیوتر B که واقع در خارج از شبکه است مشاهده کند.کامپیوتر A درخواست خود را برای تماشای صفحه وب به کامپیوتر B ارسال می کند که این درخواست توسط فایروال ضبط و مورد بررسی قرار میگیرد.کامپیوتر B درخواست را میگیرد و در پاسخ شروع به فرستادن صفحات میکند.زمانی که صفحات به فایروال میرسند،فایروال آنها را با درخواست کامپیوتر A مقایسه می کند تا ببیند که آدرس و پورتها یکی هستند و بسته مجاز به وارد شدن به شبکه است یا خیر ، در نهایت براساس سیاست ها packet ها یا وارد می شوند یا به دور انداخته می شوند.

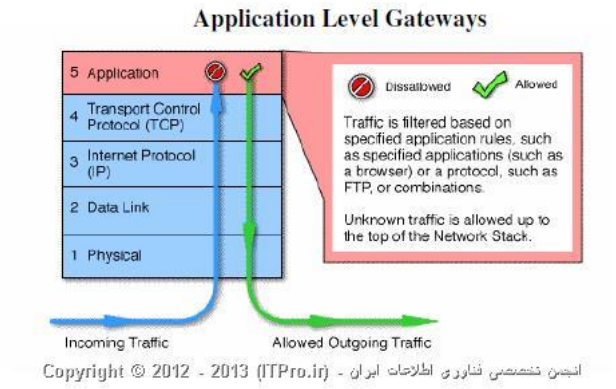


Aplication Level Gateway

دودسته ی قبلی فایروالها تنها هدرهای لایه های network و session را مورد بررسی قرار می دادند.در آنها امکان دیدن payload بسته ها وجود نداشت. هیچ کدام از فایروالها آنقدر قدرتمند نبودند که بتوانند محتویات بسته ها را مشاهده کنند.تا قبل ازاین نسل از فایروالها،ارتباطی مجاز بود که IP و پورت مجازی داشته باشد و session مجازی را نیز تشکیل دهد که این می توانست موجب بروز حملاتی به داخل شبکه شود.مثلا اگر در شبکه ای استفاده از telnet مجاز نبوده اما استفاده از HTTP مجاز بوده باشد،از نظر این فایروال ارتباط مجاز است اگر از پورت ۸۰ استفاده شده باشد و غیرمجاز است اگر از پورت ۲۳ استفاده شود.خوب اگراز telnet پورت ۸۰ استفاده کنیم فایروال متوجه نخواهد شد چون محتویات داخل بسته ها را چک نمیکند و فقط شماره پورت ها رو بررسی می کند.application level gateway یا فایروالهای proxy ،نرم افزارهای کاربردی هستند که دو mode یا حالت دارند:proxy server و proxy client .زمانی که یک user در یک trusted network یا شبکه مطمئن می خواهد با یک user دیگر در یک untrusted network یا شبکه غیرمطمئن مانند اینترنت متصل شود،درخواست به صورت مستقیم به proxy server ارسال می شود.proxy server یه جورایی حکم سرور واقعی در اینترنت را دارد.او درخواست هایی که به آن می شود را بررسی می کند و براساس قوانینی که برایش تعریف شده ، تصمیم می گیرد که درخواست ها را تائید یا رد کند.درواقع او اینکار را با یررسی محتویات بسته ها ،پورتها و IP ها انجام میدهد.اگر درخواستی تائید شد،proxy server آن را به proxy client که با سرور واقعی در اینترنت مرتبط است ،ارسال می کند. همانطور که کلیه ی درخواست هایی که از داخل شبکه می خواهند به بیرون بروند،به proxy server ارسال می شود، درخواست هایی که از بیرون می خواهند به داخل شبکه وارد شوند،به client server ارسال می شود،که client proxy آنها را برای تحویل دادن به client ها ،به proxy server ارسال می کند.در این روش شما اطمینان دارید که کلیه ارتباطات داخلی همیشه به proxy server و کلیه ی ارتباطات خارجی توسط client server برقرار می شوند.بنابراین هیچ ارتباط مستقیمی میان شبکه های مطمئن (trusted ها) با غیرمطمئن (untrusted ها) وجود ندارد.از مزایای این روش این است که:

- میتواند قوانین را براساس پروتکل های سطح بالا وضع کند.
- وضعیت اطلاعات در مورد ارتباطاتی که از سرور فایروال گذشته اند را نگه میدارد.
- جزئیات را در مورد فعالیت ها ضبط میکند.

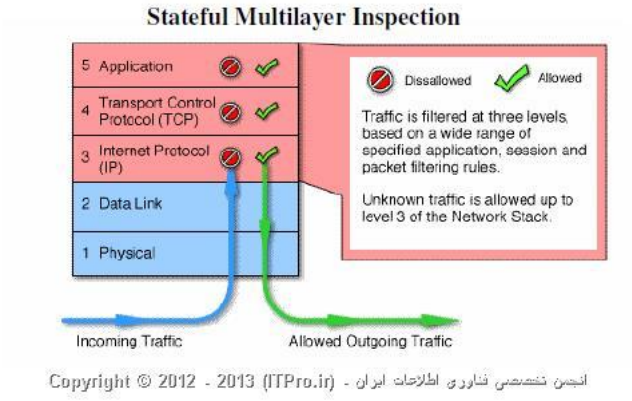
اما عیب اصلی این روش این است که فیلترینگ پیچیده و تصمیمات در کنترل دسترسی ها نیازمند منابع محاسباتی مهم است که این باعث پایین آمدن کارایی و آسیب پذیری سیستم عامل می شود.Microsoft Internet Security و Acceleration مثالی خوب از application level gateway هستند.



Staeful Multi Level Inspection (SMLI)

فایروالهای SMLI نسل چهارم از فایروالها هستند که در سال ۱۹۹۴ ارائه شدند.در این فایروالها از تکنولوژی بکار برده شده در سه نسل قبلی استفاده شده است.درواقع SMLI ها می توانند عمل filter packet یا فیلترکردن بسته ها را در لایه شبکه ،session و همچنین لایه کاربردی نیز انجام دهند.درواقع این فایروال با مانیتورینگ داده هایی که در حال رد و بدل در لایه کاربردی و یا پورتها هستندسطح امنیتی بالایی را برقرار می کند. ارتباطاتی که از طریق SMLI انجام می شود برای طرفین کاملا مشخص و شفاف بوده و compatibility به هیچ عنوان مشکل ساز نمی باشد.به جای استفاده از application level filtering یا نسل سوم تکنولوژی فایروالها، در فایروالهای دیگر،SMLI device از الگوریتم هایی استفاده میکنند که منابع کمتری را برای بررسی بسته ها در لایه کاربردی لازم

داشته باشند (استفاده از منابع زیاد در نسل سوم از فایروالها از معایب آن دسته بود).این دسته از فایروالها سطح بالایی از امنیت را برقرار میکنند و دارایی کارایی خوبی نیز هستند اما قیمت آنها نیز بالاست .تنظیم قوانین در این فایروالها کمی پیچیده است و اگر اینکار خوب صورت نپذیرد،فایروال قادر به برقراری امنیت نخواهد بود. یکی از مزایای آنها این است که زمانی که یک session کامل شد،هر پورتی که در آن session استفاده می شده است ،بسته می شود.SMLI ها می توانند به صورت داینامیکی پورتها را برای هر session بسته یا باز کنند،که در نسل اول یا packet filtering بعد از هر session آن پورت درهمان وضعیت قبلی باقی می ماند . آخرین ورژن Checkpoint Firewall-۱ نمونه ای ازتکنولوژی SMLI فایروالهاست.



خلاصه

چیزی که همیشه باید در مورد فایروالها به خاطر داشته باشید این است که آنها باید بتوانند محافظت را در عمق شبکه شما انجام دهند و از جزئیات نیز نگذرند.هر تکنولوژی فایروالی راهکارهایی برای کاربردهای مختلفی دارد.packet filtering firewall از ساده ترین تکنولوژی هاست که به آسانی پیاده سازی می شود و ارزان هم هست اما ایمنی کمتری دارد.circiut level gateway هم ،ارازن است و راحت پیاده سازی می شود اما از آنها می توان برای حفظ امنیت چندکامپیوتر استفاده کرد.از circuit level gateway میتوان در NAT که از یک شبکه خانگی محافظت می کند استفاده کرد و تک تک کامپیوتر های آن شبکه می توانند از packet filtering استفاده کنند.aplication level firewall ها پیچیده ترند و پیاده سازی آنها گرانتر است اما میتوان برای محافظت از سرورهای زیادی از آنها استفاده کرد.و در نهایتدر شبکه های بسی یزرگتر،که نیازمند محافظت بیشتری هستند و امنیت نیز اهمیت مضاعفی دارد،می توان از SMLI ها استفاده کرد.

نویسنده : فاطمه قرباوی

منبع : انجمن حرفه ای های فناوری اطلاعات ایران (http://www.itpro.ir)

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

برچسب ها

تکنولوژی فایروالها
(http://itpro.ir/tags/%d8%aa%da%a9%d9%86%d9%88%d9%84%d9%88%da%98%db%8c%20%d9%81%d8%a7%db%8c%d8%b1%d9%88%d8%a7%d9%84%d9%87%d8%a7)

تفاوت utm و firewall (http://itpro.ir/tags/%d8%aa%d9%81%d8%a7%d9%88%d8%aa%20utm%20%d9%88%20firewall)

معرفی انواع فایروال در شبکه
(%d9%81%db%8c%20%d8%a7%d9%86%d9%88%d8%a7%d8%b9%20%d9%81%d8%a7%db%8c%d8%b1%d9%88%d8%a7%d9%84%20%d8%af%d8%b1%20%d8%b4%d8%a8%da%a9%d9%87)

قابلیت stateful چیست (http://itpro.ir/tags/%d9%82%d8%a7%d8%a8%d9%84%db%8c%d8%aa%20stateful%20%da%86%db%8c%d8%b3%d8%aa)

فایروال های چگونه کار می کنند
(%d8%a7%d9%84%20%d9%87%d8%a7%db%8c%20%da%86%da%af%d9%88%d9%86%d9%87%20%da%a9%d8%a7%d8%b1%20%d9%85%db%8c%20%da%a9%d9%86%d9%86%d8%af)

نحوه کار کردن فایروال ها
(%d9%86%d8%ad%d9%88%d9%87%20%da%a9%d8%a7%d8%b1%20%da%a9%d8%b1%d8%af%d9%86%20%d9%81%d8%a7%db%8c%d8%b1%d9%88%d8%a7%d9%84%20%d9%87%d8%a7)

مکانیزم کاری فایروال در شبکه
(db%8c%d8%b2%d9%85%20%da%a9%d8%a7%d8%b1%db%8c%20%d9%81%d8%a7%db%8c%d8%b1%d9%88%d8%a7%d9%84%20%d8%af%d8%b1%20%d8%b4%d8%a8%da%a9%d9%87)

معرفی packet filtering فایروال (http://itpro.ir/tags/%d9%85%d8%b9%d8%b1%d9%81%db%8c%20packet%20filtering%20%d9%81%d8%a7%db%8c%d8%b1%d9%88%d8%a7%d9%84)

معرفی فایروال circuit level (http://itpro.ir/tags/%d9%85%d8%b9%d8%b1%d9%81%db%8c%20%d9%81%d8%a7%db%8c%d8%b1%d9%88%d8%a7%d9%84%20circuit%20level)

web application firewall چیست (http://itpro.ir/tags/web%20application%20firewall%20%da%86%db%8c%d8%b3%d8%aa)

ویدئوهای مرتبط