مقدمه ای بر امنیت شبکه

چکیده :

امنیت شبکه یک موضوع پیچیده است که از نظر تاریخی فقط توسط افراد با تجربه و آنهایی که آموزش کافی دیده اند مورد توجه قرار می گیرد. با اینحال ، همچنان که افراد بیشتری به شبکه متصل میشوند ، تعداد افرادی که بایستی اصول امنیت را در دنیای شبکه شده بدانند ، نیز افزایش می یابد. این مقاله بر اساس ماربری کامپیوتر و مدیریت سیستمهای اطلاعاتی که در خاطرم بوده است نوشته شده است و مفاهیم مورد نیاز برای آشنا شدن با بازار و خطرات و نحوه مواجه شدن با آنها را توضیح می دهد.

مدیریت ریسک: بازی امنیتی

این بسیار مهم است که دانسته شود که در بحث امنیت ، یک فرد به آسانی نمی تواند بگوید که " بهترین فایروال کدام است؟"

در این رابطه دو مطلب وجود دارد : امنیت مطلق و دسترسی مطلق.

بهترین راه برای بدست آوردن یک امنیت مطلق برای ماشین این است که آنرا از شبکه و برق جدا کرده آنرا درون یک جای امن قرار داده و آنرا به کف اقیانوس بفرستیم. متاسفانه ،در اینحالت از ماشین نمی توان استفاده کرد. یک ماشین با دسترسی مطلق برای استفاده بسیار راحت است : این ماشین به آسانی در جایی قرار می گیرد ، و بدون هیچ پرسشی ، تاییدی ، کدرمزی یا هر مکانیسم دیگری ، می توانید هر چه

را که می خواهید از او بخواهید. متاسفانه ،این حالت امکان پذیر نیست یا اینکه اینترنت یک همسایه بد است و در صورتی که یک آدم احمق و کله خراب به کامپیوتر فرمان کاری همانند خراب کردن خوش را بدهد ،مدت طولانی این سیستم پایدار نمی ماند.

این وضعیت با زندگی روزمره ما فرقی ندارد. ما مرتباً تصمیماتی را در مورد اینکه چه ریسکی را قبول کنیم ، اتخاذ میکنیم . وقتی که ما درون خودرو نشسته و به محل کار می رویم ، برخی مخاطرات وجود دارند که می توانند اتفاق بیفتند ،این احتمال وجود دارد برخی چیزها به طور کامل از کنترل خارج شده و باعث شود که ما در بخشی از تصادفی که در بزرگراه اتفاق افتاده قرار بگیریم. زمانیکه ما وارد یک هواپیما می شویم مقداری خطر را به قیمت آسایش و راحتی، پذیرفته ایم . با اینحال برخی از مردم یک تصویر خیالی از یک ریسک قابل قبول دارند و در بیشتر موارد آنرا نمی پذیرند. اگر من در طبقه بالا باشم و بخواهم سرکار بروم خودم را از پنجره پرت نمی کنم . بله ، اینکار بسیار راحت است اما خطر آسیب دیدگی بخاطر این راحتی وجود دارد.

هر سازمانی نیاز دارد تا برای خودش تصمیم بگیرد که بین امنیت کامل و دسترسی کامل برای خود موقعیتی را در نظر بگیرد. یک خط مشی برای بکارگیری مطالب لازم است و آنگاه مشخص شود که چگونه دستورات را اجرا کرد. هر چیزی که به نام امنیت انجام گیرد بایستی در چارچوب این قانون باشد.

انواع و منابع تهدیدهای شبکه:

در حال حاضر ما آنقدر اطلاعات در زمینه شبکه گذاری داریم که می توانیم وارد جنبه های امنیتی آن شویم. اول از همه ما وارد انواع تهدیدهایی که شبکه با آنها مواجه است می شویم و آنگاه برخی از کارهایی که می توان برای حفاظت از خود در مقابل آنها انجام دهیم ،توضیح می دهیم.

Denial-of-Service

احتمالاً حملات *DoS* خطرناکترین تهدیدها است که برای توضیح دادن هم مشکل هستند. آنها بدین دلیل خطرناکترین هستند که به آسانی می توانند اجرا شوند ، به سختی رهگیری می شوند (برخی مواقع غیرممکن است) ، و سرپیچی از درخواست حمله کننده آسان نیست حتی اگر این درخواست غیر قانونی باشد.

منطق یک حمله *DoS* ساده است . درخواستهای زیادی به ماشین ارسال می شود که از اداره ماشین خارج است. ابزارهای در دسترسی در محافل زیر زمینی وجود دارد که که این کار را به صورت یک برنامه در می آورند و به آن می گویند در چه میزبانی درخواستها را منتشر کنند. برنامه حمله کننده به راحتی با برخی از پورتهای خدماتی ارتباط برقرار می کند ،شاید اطلاعات عنوان پاکت را که می گوید بسته از کجا آمده را جعل می کند و آنگاه ارتباط را قطع می کند. اگر میزبان قادر باشد که در هر ثانیه به ۲۰ درخواست پاسخ دهد ، و حمله کننده در هر ثانیه ۵۰ درخواست را ارسال کند ،مشخص است که میزبان قادر به پاسخگویی به تمامی در خواستهای حمله کننده ، که کم و بیش غیر قانونی هستند ، نیست .

چنین حملاتی در اواخر ۱۹۹۶ و اوایل ۱۹۹۷ به شدت فراگیر شده بود ولی حالا چندان عمومیت ندارد.

برخی کارهایی که می توان برای کاهش خطر مواجه شدن با یک حمله *DoS* (رد درخواست) انجام داد عبارتند از:

- عدم اجرای خدمات قابل مشاهده به صورت جهانی در نزدیکی ظرفیت اجرایی
- استفاده از فیلترینگ بسته برای جلوگیری از بسته های جعل شده در ورودی به فضای آدرس شبکه شما .

مشخصاً بسته های جعلی شامل آنهایی هستند که ادعا می کنند از طرف میطبان شما آمده اند ،بر اساس *RFC1918* برای شبکه های خصوصی و شبکه *loopback* آدرس دهی شده اند.

- موارد مربوط به امنیت سیستمهای عامل میزبان خود را به روز کنید.

دسترسی غیر مجاز:

دسترسی غیر مجاز یک واژه سطح بالا است که می تواند به انواع مختلف حملات مرتبط باشد. هدف از این نوع حملات دسترسی به برخی منابع است که ماشین شما نبایستی آنرا در اختیار حمله کنندگان قرار دهد. برای مثال ، یک هاست می تواند یک وب سرور باشد و بایستی صفحهت وب را برای هر کسی که در خواست میکند در اختیار قرار دهد. با اینحال این هاست نباید دسترسی به لایه فرمان را بدون اینکه مطمئن شود که فرد درخواست کننده مجاز به این کار است ،مثل یک مدیر محلی ،فراهم آورد.

اجرای فرامین غیر قانونی

مشخص است که یک فرد ناشناس و غیر مطمئن نبایستی بتواند فرامین را روی ماشینهای سرور شما اجـرا کند. دو طبقه بندی عمده امنیتی برای این مشکل وجود دارد:

دسترسی کاربر معمولی

و دسترسی مدیریت

یک کاربر معمولی می تواند تعدادی از موارد سیستم را اجرا نماید (همانند خواندن فایلها ، ارسال ایمیـل به سایر افراد و غیره) که افراد مهاجم قادر به اجرای آنها نیستند . این حالت ممکن اسـت تمـام آن چیـزی باشد که یک مهاجم به آن نیاز دارد. بعبارت دیگر ، یک مهاجم ممکن است بخواهد تغییرات پیکربنـدی را برای یک هاست اجرا نماید (شاید تغییر در آدرس *IP* ، قرار دادن یک فرمـان راه انـدازی در جاییکـه باعث می شود هر زمان که ماشین استارت شـد ، *shut down* شـود یـا مـوارد مشـابه). در چنـین حـالتی ، مهاجم نیاز دارد که امتیاز مدیریتی را بر روی هاست بدست آورد.

شکافهای محرمانه:

لازم است که ما مدل تهدید را توضیح دهیم: شما سعی کنید که در برابر چه چیزی از خودتان محافظـت کنید؟ برخی اطلاعات خاص وجود دارند که اگر در دست رقیب ،یـک دشـمن یـا عمـوم ، بیفتـد باعـث آسیب جدی می شوند. در چنین حالتهایی ،این امکان وجود داردکه توافق مربوط به حساب یـک کـاربر معمولی روی ماشین برای آسیب رساندن کافی باشد (شاید به شکل *PR* ، یا بدست آوردن اطلاعاتی که می توانند بر علیه شرکت مورد استفاده قرار گیرند و غیره).

هرچند بسیاری از مرتکبان چنین نفوذهایی بندرت افـرادی هسـتند کـه از روی کنجکـاوی و فقـط بـرای مشاهده یک لایه اعلان در روی کامپیوتر شما وروی صفه نمایش خودشان این کـار را انجـام مـی دهنـد ،ولی افراد بد نیتی هم هستند که ما آنها در ادامه مورد بررسی قرار می دهیم. (بعلاوه ،بخاطر داشته باشـید که این احتمال وجود دارد که فردی فقط برای کنجکاوی نفوذ کرده است می تواند ترغیب شئد که کار بیشتری انجام دهد: شاید یک رقیب سرسخت مایل باشد که چنـین شخصـی را بـرای ضـربه زدن بـه شـما استخدام کند.)

رفتار مخرب:

در بین انواع مخرب نفوذ و حمله ، دو گروه عمده وجود دارد:

Data Diddling

data diddler احتمالاً بدترین نوع است ، زیرا واقعیت یک نفوذ امکان ندارد که بلافاصله مشـاهده شـود. شاید او با تعدادی از صفحات گسترده شما در حال بازی است یا اطلاعـات را در پـروژه هـا و طرحهـای شما دستکاری میکند . شاید او شماره حسابها را برای سپرده گذاری خودکـار برخـی پرداختهـای چکـی خاص را تغییر میدهد . در هر حالت ، بندرت پیش می آید که شما یک روز به سر کار بیایید و به آسـانی ببینید که برخی چیزها تغییر کرده است. برای پیدا کردن اختلاف در دفـاتر بوسـیله روشـهای حسـایداری سه تا چهار ماه زمان نیاز است. سعی کنید که مشکل را در جاهـایی کـه مشـکل هسـتند تعقیـب کنیـد ، و زمانی که مشکل پیدا شد ، چگونه می توان فهمید که کدامیک از شما در آن زمان همدست بوده اسـت؟ قبل از اینکه بفهمید اطلاعات شما ایمن هستند تا کجا باید پیش بروید؟

تخریب اطلاعات:

برخی از مهاجمان به آسانی با افرادی همکاری می کنند که دوست دارند همه چیز را از بین ببرند. در چنین حالتی ،تاثیر روی توان محاسباتی شما و در نتیجه شرکت شما ، میتواند چیزی کمتر از یک حریق یا بلایای دیگری باشد که باعث می شود تجهیزات محاسباتی شما بطور کامل تخریب شوند.

آنها از کجا می آیند؟

چگونه یک مهاجم دسترسی به تجهیزات شما را بدست می آورد ؟ از طریق هر ارتباطی که شما با دنیای بیرون دارید. این شامل اتصالات اینترنتی ،مودمهای شماره گیر و حتی دسترسی فیزیکی می باشد. (چقدر اطلاع دارید که یکی از افراد موقتی که شما برای کمک به وارد کردن اطلاعات بکار گرفته اید یک نفوذگر سیستم که بدنبال کد رمزها ، شماره تلفنها ،موارد حساس و هر چیزی که از طریق آنها می توانند به تجهیزات شما دسترسی پیدا کنند ، نمی باشد؟)

به منظور حفظ توانایی در ایجاد امنیت مناسب ، تمامی احتمالات بایستی شناسایی و ارزیابی شوند. امنیت آن نقطه ورود بایستی بر اساس سیاست شما در مورد میزان ریسک قابل قبول بایستی تامین شود.

درسهای یاد گرفته شده:

با بررسی انواع حملاتی که متداول هستند ، می توانیم فهرستی کوتاه از روشهای سطح بالا را که می توانند در جلوگیری از بلاهای امنیتی و کنترل آسیب در مواقعی که معیارهای پیشگیرانه در جل.گیری از یک حمله ناموفق هستند، به ما کمک کنند را تهیه کنیم.

امیدواریم که شما بک آپ داشته باشید

از دیدگاه امنیتی این فقط یک ایده خوب نیست. مقررات عملیاتی ،سیاست بک آپ را توصیه می کنند و این بایستی همراه با برنامه کشف آسیب باشد،انگار که یک هواپیما نصف شب روی ساختمان شما سقوط کند ، شما بایستی بتوانید شرکتتان را به جای دیگری منتقل کنید. مشابهاً این موارد می تواند در بازیابی اطلاعات شما در صورت بروز مشکل الکترونیکی ، ایراد سخت افزاری یا یک نفوذ که اطلاعات شما را تغییر یا آسیب میرساند ،کمک می کند.

اطلاعات را در جاییکه لازم نیستند قرار ندهید

البته این نیازی به گفتن ندارد ،که این حالت برای هر قومی پیش می آید. بنابراین ،اطلاعاتی که نیازی به دسترسی از بیرون به آنها وجود ندارد،برخی اوقات در دسترس هستند و این امر می تواند وضعیت نفوذ را بنحو چشمگیری افزایش دهد.

دوری از سیستمهایی با نقاط ضعف مشترک

هر سیستم امنیتی که بتواند بوسیله هر قسمت آن شکسته شود ،در واقع خیلی قوی نیست. از نظر امنیتی ، مقداری تکثیر (*redundancy*) خوب است و می تواند به شما در محافظت شرکتتان از یک حمله امنیتی ضعیف قبل از اینکه به فاجعه تبدیل شود کمک کند.

سیستم عاملهای به روز و مرتبط را داشته باشید.

مطمئن باشید که فردی که می داند شما چه چیزی دارید بدنبال آن است که توصیه های امنیتی را به شما بفروشد. استفاده از میکروفونهای قدیمی متداولترین (و موثرترین!) راه برای نفوذ به سیستمها هستند.

بدنبال متخصصان امنیتی مرتبط باشید.

علاوه بر مراقب مطالبی که توصیه کنندگان می کنند هستید ، مراقب گروههایی همانند *CERT* و *CIAC* باشید. مطمئن شوید که حداقل یک نفر (ترجیحاً بیشتر) عضو این لیستهای پستی هستند.

تعدادی از کارمندان را با توصیه های امنیتی آشنا کنید.

داشتن حداقل یک نفر را که مسئول حفظ توسعه امنیت است ،ایده خوبی است. این فرد یک نابغه فنی نیست ،اما می تواند فردی باشد که به آسانی می تواند مقالات توصیه کنندگان را خوانده و مراقب انواع مشکلات ایجاد شده باشد. چنین شخصی باید بتواند بطور معقول با موارد مرتبط با امنیت برخورد داشته و مشکلات ناشناخته نرم افزار وب سرور و غیره را بشناسد.

این شخص همچنین باید و نبایدهای امنیتی را با خواندن هندبوک امنیتی سایت بداند.

فایر والها:

با توضیحاتی که ما در مورد اینترنت و شبکه های مشابه داده ایم ، اتصال شرکتی به اینترنت باعث ایجاد یک ترافیک دو طرفه می شود. برای بسیاری از شرکتها این مطلب قابل قبول نیست که اطلاعات خصوصی آنها درون یک انترانت شرکتی آزادانه به نمایش درآیند. (انترانت یک شبکه *TCP/IP* است که بعد از اینترنت شکل گرفت و فقط درون سازمانها کار می کند.)

بمنظور ایجاد سطوحی از جدایی بین انترانت سازمانی و اینترنت ،فایروالها بکار گرفته شده اند. یک فایروال گروهی از قطعات هستند که مجموعاً یک مانع را بین دو شبکه ایجاد می کنند.

تعدادی از واژه خاص مرتبط با فایروالها و شبکه بندی در این بخش مورد استفاده قرار می گیرند که اجازه بدهید آنها را معرفی کنیم.

باستیون هاست (*Bastion host*):

یک کامپیوتر با هدف عمومی که برای کنترل دسترسی بین شبکه(خصوصی) داخلی (انترانت)و اینترنت (یا هر شبکه ناشناخته دیگر)مورد استفاده قرار می گیرد. عموماً اینها هاستهایی هستند که دارای سیستم عامل یونیکس بوده و برای کاهش عملیات آن به عملیاتی که فقط برای پشتیبانی از وظایف آن اصلاح شده است .بسیاری ار اهداف عمومی آن خاموش شده است و در بسیاری از موارد به طور کامل حذف شده اند تا امنیت ماشین ارتقا یابد.

روتور:

یک کامیوتر با هدف خاص برای اتصال شبکه ها به یکدیگر. روتورها همچنین برخی عملیات خاص همانند مسیریابی،یا مدیریت ترافیک شبکه هایی که به آنها متصل هستند را به عهده دارند.

لیست کنترل دسترسی (*ACL*) :

بسیاری از روتورها در حال حاضر این توانایی را دارند به طور انتخابی برخی از وظایفشان را بر اساس اطلاعاتی در مورد اینکه یک بسته به کجا می رود ، انجام دهند.این اطلاعات شامل مواردی همانند : آدرس مبدا ، آدرس مقصد ، پورت سرویس مقصد ، و غیره است. این موارد می توانند به نوع خاصی از بسته ها که از یک شبکه خازج یا به آن وارد می شوند ، محدود گردد.

منطقه بیطرف (*DMZ*):

DMZ بخش مهمی از یک فایروال است: این منطقه شبکه ایی است که نه بخشی از شبکه مشترک شده می باشد و نه بخشی از شبکه مشترک نشده است. ولی شبکه ایی است که بخش مشترک نشده را به بخش مشترک شده ارتباط می دهد.اهمیت *DMZ* فوق العاده بزرگ است: هرکسی که از طریق اینترنت

بخواهد به شبکه شما نفوذ کند ، بایستی برای موفقیت در این کار از چند لایه بگذرد.این لایه ها توسط *DMZ* و در بخشهای مختلف ایجاد شده اند.

پراکسی *(Proxy)*:

این پروسه ایی است که یک هاست در طرف مقابل انجام می دهد. هاستی که دارای این قابلیت است که اسناد را از اینترنت واکشی کند می تواند بعنوان یک پراکسی سرور و هاست روی اینترانت باید به صورت پراکس کلاینت پیکربندی گردد. در چنین حالتی،بعنوان مثال ، وقتی که یک هاست روی اینترانت می خواهد صفحه وب <*http://www.interhack.net/*> را واکشی کند ،جستجوگر ارتباطی را با پراکسی سرور برقرار کرده و درخواست یک *URL* خاص را میدهد. پراکسی سرور اسناد را واکشی کرده و نتایج را به کلاینت بر میگرداند. با این روش ، تمامی هاستهای روی اینترانت قادر هستند که به منابع اینترنت بدون داشتن قابلیت صحبت با اینترنت ، دسترسی پیدا کنند.

انواع فایروالها:

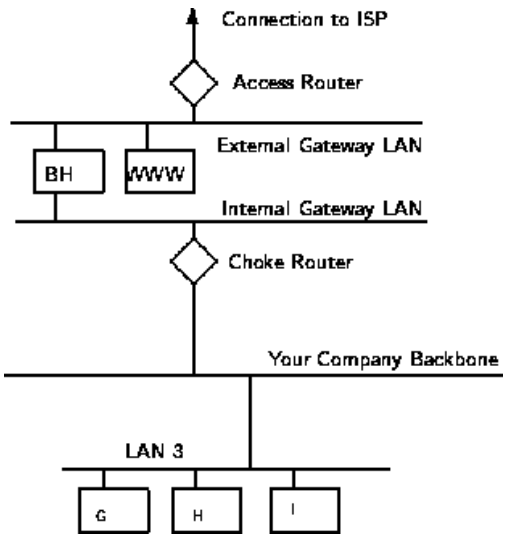
سه نوع عمده فایروال وجود دارد که ما آنها را مورد بررسی قرار میدهیم:

مسیر کاربردی:

اولین فایروال ، مسیر کاربردی هستند که بعنوان پراکسی مسیری شناخته می شوند.آنها از باستین هاستهایی ساخته شده اند که برای عمل کردن به صورت پراکسی سرور یک نرم افزار خاص را اجرا می کند. این نرم افزار در لایه کاربردی دوست قدیمی ما مدل مرجع *ISO/OSI* اجرا می شود. کلاینتهای پشت سر فایروال بایستی *proxitized* (به این معنا که بایستی دانست که چگونه از پراکسی استفاده کرد و

آنها را پیکربندی نمود)شوند تا از خدمات اینترنتی استفاده کرد.معمولاً اینها دارای ویژگی امنیتی هستند ، زیرا آنها به همه چیز اجازه عبور بدون اشکال را نمی دهند و نیاز به برنامه هایی دارند که برای عبور از ترافیک نوشته و اجرا شده اند.

شکل ۱ : یک نمونه از مدخل کاربردی



آنها عموماً کندترین هستند زیرا برای داشتن یک درخواست سرویس نیاز به اجرای پروسه های زیادی دارند. شکل ۵ یک نوع مدخل کاربردی را نشان می دهد.

فیلتر کردن بسته

فیلتر کردن بسته تکنیکی است که بواسطه آن روتورها دارای *ACL* های (لیستهای کنترل دسترسی) فعال می شوند. به طور پیش فرض ،یک روتور تمامی ترافیک به سمت خود را عبور می دهد و همه نوع کار را بدون هیچ محدودیتی انجام می دهد .استفاده از *ACL*ها روشی برای اعمال سیاست امنیتی شما با توجه به نوع دسترسی که می خواهید جهان خارج به شبکه داخلی شما داشته باشد و غیره ، می باشد.

استفاده از فیلتر کردن بسته بجای مدخل کاربردی دارای هزینه اضافی است زیرا ویژگی کنترل دسترسی در لایه پایینتر *ISO/OSI* اجرا می شود. (عموماً لایه انتقال یا لایه *session*). با توجه به سربار کمتر و این

واقعیت که فیلترینگ بوسیله روتورهایی انجام میشوند که به صورت کامپیوترهای خاص برای اجرای موارد مرتبط با شبکه بندی ،بهینه شده اند ،یک مسیر فیلترینگ بسته اغلب بسیار سریعتر از لایه کاربردی آن است.

با توجه به آنکهما بر روی یک لایه پایینترکار میکنیم ،پشتیبانی از کاربردهای جدید یا به صورت خودکار انجام می شود یا یک موضوع ساده است که در آن بسته های خاص از مسیر عبور میکنند.

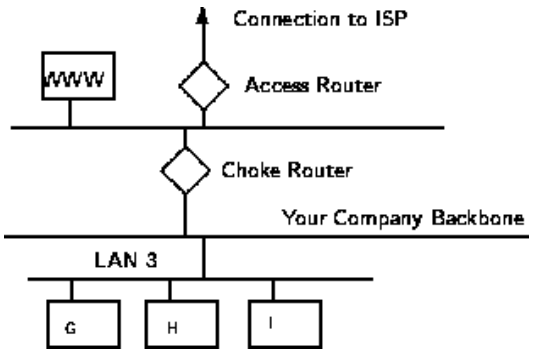
(البته احتمال اینکه برخی از چیزها به صورت خودکار آنرا ایجاد میکنند،یک نظر خوب است ، ولی مواردی که این مسیر را افشا میکنند می تواند پایینتر از سطح مورد نظر شما در رابطه با سیاست امنیتی باشد).

در این روش مشکلاتی وجود دارد،بنابراین بخاطر بسپارید که *TCP/IP* به صورت مطلق است یعنی اینکه هیچ تعهدی برای آدرسهایی که ادعا می کنند به آن مرتبط هستند وجود ندارد.بنابراین ،به منظور محلی کردن ترافیک ما از لایه های فیلترهای بسته استفاده می کنیم. ما نمی توانیم تمام مسیرهای منتهی به هاست واقعی را داشته باشیم اما از طریق دو لایه از فیلترهای بسته می توانیم بین بسته ایی که از اینترنت می آید با بسته ایی که از شبکه داخلی ما می آید ،تفاوت قائل شد.ما می توانیم مشخص کنیم که بسته از کدام شبکه می آید اما نمی توانیم مشخصات بیشتری در مورد آن داشته باشیم.

سیستمهای ترکیبی *(Hybrid systems)*:

در یک تلاش برای هماهنگ کردن مسیرهای لایه کاربردی با انعطاف پذیری و سرعت فیلترینگ بسته ، برخی از فروشندگان سیستمهایی را ایجاد کردند که از هر دو اصل استفاده می کنند.

شکل ۲ : یک مسیر فیلترینگ نمونه بسته



در چنین سیستمهایی ،اتصالات جدید باید در لایه کاربردی تایید وبه تصویب برسند. زمانی که این اتفاق افتاد ،بقیه اتصال به لایه *session* فرستاده می شود، که در آن برای فیلترهای بسته اتصال را کنترل می کنند تا مطمئن شوند که تنها بسته هایی که بخشی از یک محاوره در حال پیشرفت (که همچنین مجاز و مورد تایید هستند) عبور میکنند.

سایر احتمالات شامل استفاده از هر دو پراکسی فیلترینگ بسته و لایه کاربردی است. مزیتهای این حالت شامل ،ارائه معیاری برای محافظت از ماشینهای شما در مقابل خدماتی که به اینترنت ارائه میکند (همانند یک سرور عمومی وب) و همچنین ارائه امنیت یک مسیر لایه کاربردی به شبکه داخلی است.

بعلاوه ،با استفاده از این مدل ، یک مهاجم که قصد بدست آوردن خدمات روی شبکه داخلی را دارد ،از طریق روتور دسترسی ، هاست بوستین و روتور مسدود کننده با شکست مواجه می شود.

بنابراین برای من چه چیزی بهترین است؟

گزینه های مختلفی در دسترس است ، و انتخاب انها بستگی به صرف زمان و تجربه نیاز دارد، چه به صورت داخلی و چه به صورت یک مشاور با تجربه که می تواند زمانی را برای شناخت سیاست امنیتی موسسه شما صرف کند و می تواند فایروالی را طراحی و ساخته که بهترین استفاده را از سیاست شما کرده باشد. سایر موارد همانند ، خدمات مورد نیاز ، تسهیلات و مقیاس پذیری بایستی در طرح نهایی مورد توجه قرار گیرند.

/http://www.interhack.net/pubs/network-security

http://www.dlbartar.com/