

# امنیت در شبکه های خانگی

تهیه کننده : میثم رجبی

ش.د. ۸۸۰۲۵۳۹۳۴

## چکیده :

امنیت شبکه یک موضوع پیچیده است که از نظر تاریخی فقط توسط افراد با تجربه و آنها یی 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 اصول کامپیوتر و مدیریت سیستمهای اطلاعاتی که در حال حاضر وجود دارد ، 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 خودش را بدهد ، مدت طولانی این سیستم پایدار نمی ماند.

این وضعیت با زندگی روزمره ما فرقی ندارد. ما مرتبأً 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 موقع 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 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 درخواستهای حمله کننده ، که کم و بیش غیر قانونی هستند ، نیست .

چنین حملاتی در اوخر ۱۹۹۶ و اوایل ۱۹۹۷ به شدت فraigیر 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 میزبان شما آمده اند، بر اساس

*RFC1918* برای شبکه های خصوصی و شبکه *loopback* آدرس دهی شده اند.

- موارد مربوط به امنیت سیستمها 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 صفحه هات 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 اجرا کند. دو طبقه بندی عمدۀ 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 ایمیل به سایر افراد و غیره ) که افراد مهاجم قادر به اجرای آنها نیستند . این حالت ممکن است تمام آن چیزی باشد که یک مهاجم به آن نیاز دارد. بعبارت دیگر ، یک مهاجم ممکن است بخواهد تغییرات پیکربندی را برای یک هاست اجرا نماید ( شاید تغییر در آدرس IP ، قرار دادن یک فرمان راه اندازی در جاییکه باعث می شود هر زمان که ماشین استارت شد ، shut down شود یا موارد مشابه ). در چنین حالتی ، مهاجم نیاز دارد که امتیاز مدیریتی را بر روی هاست بدست آورد.

## شکافهای محرومانه:

لازم است که ما مدل تهدید را توضیح دهیم: شما سعی کنید که در برابر چه چیزی از خودتان محافظت کنید؟ برخی اطلاعات خاص وجود دارند که اگر در دست رقیب ، یک دشمن یا عموم ، بیفتند باعث آسیب جدی می شوند. در چنین حالتها بایی ، این امکان وجود دارد که توافق مربوط به حساب یک کاربر 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 مرتكبان چنین نفوذ‌هایی بندرت افرادی هستند که از روی کنجکاوی و فقط برای مشاهده یک لایه اعلان در روی کامپیوتر شما و روی صفحه نمایش خودشان این کار را انجام می دهند ، ولی افراد بد نیتی هم هستند که ما آنها در ادامه مورد بررسی قرار می دهیم. (علاوه ، با خاطر داشته باشید که این احتمال وجود دارد که فردی فقط برای کنجکاوی نفوذ کرده است می تواند ترغیب شود که کار بیشتری انجام دهد: شاید یک رقیب سرسخت مایل باشد که چنین شخصی را برای ضربه زدن به شما استخدام کند.)

### رفتار مخرب:

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

#### *Data Diddling*

احتمالاً بدترین نوع است ، زیرا واقعیت یک نفوذ امکان ندارد که بلا فاصله مشاهده شود. شاید او با تعدادی از صفحات گسترش شما در حال بازی است یا اطلاعات را در پروژه ها و طرحهای شما دستکاری میکند . شاید او شماره حسابها را برای سپرده گذاری خود کار برخی پرداختهای چکی خاص را تغییر میدهد . در هر حالت ، بندرت پیش می آید که شما یک روز به سر کار بیایید و به آسانی ببینید که برخی چیزها تغییر کرده است. برای پیدا کردن اختلاف در دفاتر بوسیله روش‌های حسابداری سه تا چهار ماه زمان نیاز است. سعی کنید که مشکل را در جاهایی که مشکل هستند تعقیب کنید ، و زمانی که مشکل پیدا شد ، چگونه می توان فهمید که کدامیک از شما در آن زمان همدست بوده است؟ قبل از اینکه بفهمید اطلاعات شما ایمن هستند تا کجا باید پیش بروید؟

### تخريب 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 تخريب 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 موقعی که معیارهای پیشگیرانه در جلوگیری 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 هوایپیما نصف شب روی ساختمان شما سقوط کند، شما بایستی بتوانید شرکتتان را به جای دیگری منتقل کنید. مشابهًاً این موارد می توانند 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 جایی که 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 به نحوه چشمگیری افزایش دهد.

#### دوری از سیستمها یی 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 می‌تواند 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 می‌داند شما چه چیزی دارید بدنبال آن است که توصیه‌های 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 می‌کنند هستند، مراقب گروههای همانند *CERT* و *CIAC* باشید. مطمئن شوید که حداقل یک نفر (ترجیحاً بیشتر) عضو این لیستهای پستی هستند.

تعدادی از کارمندان و همچنین خانواده را با توصیه‌های امنیتی آشنا کنید.

داشتن حداقل یک نفر را که مسئول حفظ توسعه امنیت است، ایده خوبی است. این فرد یک نابغه فنی نیست، اما می‌تواند فردی باشد که به آسانی می‌تواند 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 و سرور و غیره را بشناسد. این شخص همچنین باید و نبایدهای امنیتی سایت را بداند.

## فایر والها:

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

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

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

### **:bastion host**

یک کامپیوتر با هدف عمومی که برای کنترل دسترسی بین شبکه (خصوصی) داخلی (اینترنت) و اینترنت (یا هر شبکه ناشناخته دیگر) مورد استفاده قرار می‌گیرد. 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 از اهداف عمومی آن خاموش شده است و در بسیاری از موارد به طور کامل حذف شده اند تا امنیت ماشین ارتقا یابد.

### **روتور:**

یک کامپیوتر با هدف خاص برای اتصال شبکه‌ها به یکدیگر. روتورهای همچنین برخی عملیات خاص همانند مسیریابی، یا مدیریت ترافیک شبکه‌هایی که به آنها متصل هستند را به عهده دارند.

### **:list control (ACL)**

بسیاری از روتورهای حال حاضر این توانایی را دارند به طور انتخابی برخی از وظایف‌شان را بر اساس اطلاعاتی در مورد اینکه یک بسته به کجا می‌رود، انجام دهند. این اطلاعات شامل مواردی همانند: آدرس مبدا، آدرس مقصد، پورت سرویس مقصد، و غیره است. این موارد می‌توانند به نوع خاصی از بسته‌ها که از یک شبکه خارج یا به آن وارد می‌شوند، محدود گردد.

### **:DMZ**

بخش مهمی از یک فایروال است: این منطقه شبکه ایی است که نه بخشی از شبکه مشترک شده می‌باشد و نه بخشی از شبکه مشترک نشده است. ولی شبکه ایی است که بخش مشترک نشده را به بخش مشترک شده ارتباط می‌دهد. اهمیت **DMZ** فوق العاده بزرگ است: هر کسی که از طریق اینترنت بخواهد به شبکه شما نفوذ کند، بایستی برای موفقیت در این کار از چند لایه بگذرد. این لایه‌ها توسط **DMZ** و در بخش‌های مختلف ایجاد شده اند.

## پراکسی (Proxy):

این پروسه ایبی 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 [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.](http://www.interhack.net/)

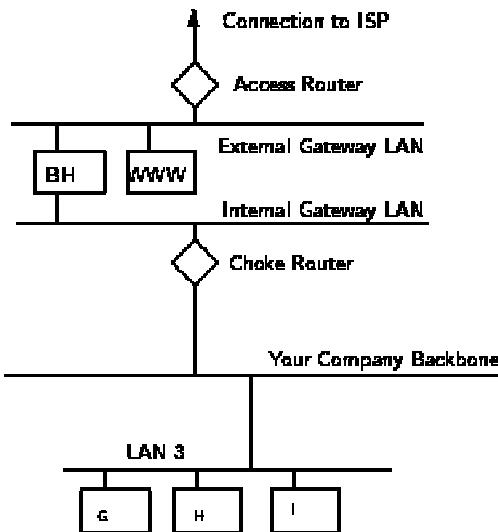
## أنواع فايروالها:

سه نوع عمدۀ 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 کنند. این نرم افزار در لایه کاربردی دوست قدیمی ما مدل مرجع ISO/OSI اجرا می شود. کلاینتهای پشت سر فایروال بایستی (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.

شكل ۱: یک نمونه از مدخل کاربردی



آنها عموماً کنترل زیرا برای داشتن یک درخواست سرویس نیاز به اجرای پروسه های زیادی دارند.  
شکل ۱ 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 روشهای 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 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 آنکه ما بر روی یک لایه پایینتر کار 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).

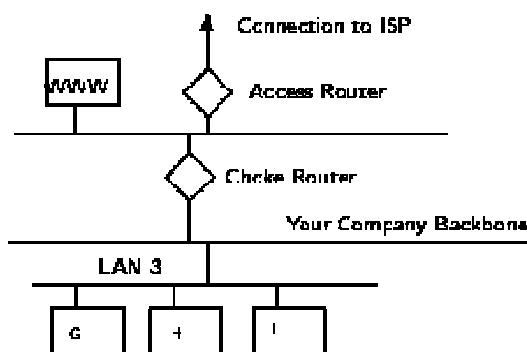
در این روش مشکلاتی وجود دارد، بنابراین بخاربرای TCP/IP به صورت مطلق است یعنی اینکه هیچ تعهدی برای آدرسها یی که ادعایی کنند به آن مرتبط هستند وجود ندارد. بنابراین، به منظور محلی کردن ترافیک

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 فروشنده‌گان 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 و به 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.

علاوه، 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.

## منابع

: سایتهاي

[www.Google.com](http://www.Google.com)

[www.civilca.com](http://www.civilca.com)

[www.Irandoc.ir](http://www.Irandoc.ir)

كتاب : شبکه سازی خانگی با ویندوز XP مترجم : بهناز منجی آزاد