فیلتر کردن محتویات اینترنت

تکنولوژی فیلتر کردن محتویات اینترنت امکان کنترل دسترسی کاربران به محتویات اینترنت را فراهم می‌آورد. اگر چه تمرکز اولیه این تکنولوژی در سطح فردی بود (مثلا به والدین امکان میداد دسترسی کودکان را به مطالب نامناسب محدود سازند.) این تکنولوژی امروزه به طور گسترده‌ای در سطح سازمانها و کشورها به کار گرفته می‌شود. برای برخی از سازمانها مثل مدارس، کتابخانه‌ها و شرکتها کنترل دسترسی به اینترنت یک اولویت مهم تلقی می‌شود. در سطح ملی نیز به طور فزاینده‌ای از این تکنولوژی استفاده می‌شود. دسترسی به برخی از مطالب بدون توجیه قابل قبولی برای همه افراد یک ملت ناممکن می‌شود.
تکنولوژیهای فیلترینگ محتوا مبتنی بر شیوه انسداد فهرستی از وب‌سایت‌ها است. این شیوه عمدتا در ترکیب با روشهای انسداد مبتنی بر کلیدواژه‌ها قرار می‌گیرد تا به طور پویا و فعال محتوا را سانسور کنند. فهرستی از اسامی سایتها و آدرس آنها بررسی و طبقه‌بندی شده و در اختیار نرم‌افزار فیلترینگ که تنها می‌تواند گروه محدودی از سایتها را فیلتر کند قرار می‌گیرد. زمانی که کاربران تلاش می‌کنند به یک صفحه اینترنتی دسترسی بیابند، نرم‌افزار فیلترینگ بانک اطلاعاتی خود را بررسی کرده و دستیابی به صفحاتی را که در آن فهرست هستند محدود می‌سازد. اگر انسداد با توجه به کلیدواژه‌ها نیز فعال شده باشد، نرم‌افزار هر صفحه را بررسی کرده و اگر کلمات ممنوعه در آدرس، یا متن صفحه موجود باشد، آن صفحه را مسدود می‌سازد.

سیستمهای فیلترینگ مستعد دو گونه اشکال ذاتی هستند: "انسداد زیاد" و "انسداد کم". تکنولوژیهای فیلترینگ نه تنها گاهی برخی سایتها را به اشتباه فیلتر میکنند، بلکه گاهی بعضی از سایتها از دست شان در می‌رود. نکته کلیدی محرمانه بودن این فهرست ها است. اگرچه برخی از لیست های همگانی و منتشر شده در این زمینه وجود دارد (معمولا مربوط به سایتهای پورنوگرافیک)، ولی لیست های سیاه تجاری و لیست هايي که در سطح ملی مورد استفاده قرار مي گيرند، معمولا سری هستند. لیستهای تجاری طبقه بندی شده معمولا جزو داراییهای معنوی تولیدکنندگان آنها محسوب شده و منتشر نمی‌شوند. اگرچه برخی از تولیدکنندگان لیست ها امکان کنترل کردن آنلاین اسامی را فراهم آورده‌اند، اما در کل می‌توان گفت که لیست های مورد استفاده برای فیلترینگ محرمانه هستند و برای بررسی و تحلیل مستقل در دسترس نیستند.

دول برخی کشورها، به لیستهای تجاری تعدادی از سایتها را افزوده و مورد استفاده قرار می‌دهند. سایت‌های مسدود شده عمدتا مربوط به احزاب سیاسی مخالف یا مطبوعات، سازمانهای حقوق بشر، خبرگزاریهای بین‌المللی و به طور خلاصه هر محتوای حساسیت برانگیزی برای دولت مورد بحث است. بسیاری از کشورها برای فیلترینگ بر روی زبان محلی خود تمرکز می‌کنند و به طور فزاینده‌ای نیز وبلاگها و تالارهای گفتگوی اینترنتی را مورد هدف قرار مي دهند.

تکنولوژیهای گذر از فیلتر

در پاسخ به روش کنترل و فیلترینگ بکار گرفته شده از سوی دولتها ، روشهای بسیاری برای گذر کردن از فیلترینگ ایجاد شده است. طرح های متعددی برای توسعه تکنولوژیهایی که به شهروندان و نهادهای مدنی امکان مقابله و حفظ امنیت خود در برابر سانسور اینترنتی می‌دهد، انجام شده است. این ابزارها اصطلاحا "تکنولوژیهای گذر از فیلتر" نامیده میشوند. در حالت کلی این کار بدین صورت انجام می‌پذیرد که درخواست برای محتوای مورد نیاز فردی از کشوری که فیلترینگ را اجرا میکند، از طریق یک کامپیوتر واسطه که بوسیله فیلترینگ محدود نشده است به وب‌سایت هدف می‌رسد و محتوا از طریق کامپیوتر واسطه برای کاربر فرستاده می‌شود. گاهی ممکن است این تکنیک ها برای شرایط خاصی طراحی شده باشند یا کاربران در کشوری که دچار سانسور است به فراخور اقتضائات تغییراتی در آنها ایجاد کرده باشند. گاهی نیز ممکن است از این تکنیکها به شیوه‌هایی غیر از آنچه هدف اصلی طراح بوده است استفاده شود.

بعضی از این تکنولوژیها توسط شرکتهای خصوصی ایجاد شده‌اند و برخی نیز توسط گروههای فعالان اجتماعی یا هکرها. این تکنولوژیها از تکنیک های ساده و دم‌دستی و برنامه‌های ابتدایی تا تکنیکهای بسیار پیچیده رمزنگاری و پروتکل های اتصال شبکه پیشرفته را در بر می‌گیرد. با توجه به این گستردگی، برای کاربران ضروری است که ارزیابی از نقاط قوت و ضعف این تکنولوژیها داشته باشند تا بتوانند روشی را که مناسب شرایط آنان است انتخاب کنند.

باید میان "ارائه دهنده گان سیستمهای فیلتر شکن" و استفاده کنندگان آن تفاوت قائل شد. ارائه دهنده کسی است که نرم‌افزاری را در جایی که محدودیتی وجود ندارد روی کامپیوتر اجرا کرده و آنها را در اختیار کاربران در کشورهايي که اینترنت سانسور و مسدود مي شود، مي گذارد. از این رو برای موفقیت در گذر از فیلترینگ باید هر دو سوی آنها موفق باشند.

این مقاله در پی آن است که به کاربرانی که مایل به استفاده از تکنولوژیها گذر از فیلترهستند اطلاعات کافی در مورد گزینه‌های ممکن ارائه کرده و آنها را در ارزیابی اینکه کدام تکنولوژی برای آنها مناسب است کمک کند. این امر بوسیله تعیین نیازها و ظرفیت های کاربران درگیر با مساله قابل انجام است. در عین حال باید تعادلی بین سطح امنیت مورد نیاز و کارآمدی این تکینیک ها برقرار کرد.

فیلترشکنی موثر، امن و پایدار بوسیله پیوند دادن تکنولوژی مناسب با کاربر مناسب محقق می‌شود.

تعیین نیازها و ظرفیتها استفاده از تکنولوژی

تکنولوژیهای فیلترشکنی برای کاربران مختلف با منابع متفاوت و میزان تخصص متنوع طراحی شده‌اند. روشی که در شرایط خاصی کار میکند ممکن است شیوه بهینه برای حالت دیگر نباشد. ضروری است که تهیه‌کننده و کاربر تکنولوژیهای گذر از فیلتر سوالهای زیر را از خود بپرسند:

- تعداد کاربران احتمالی و پهنای باند لازم چقدر است؟ (برای تهیه‌کننده و کاربر)
- نقطه اتصال مبدا برای کاربران احتمالی کجاست و آنها به چه منظوری از آن استفاده می‌کنند؟
- چه حدی از تخصص وجود دارد؟ (برای تهیه‌کننده و کاربر)
- آمادگي نقطه تماس مطمئن که تکنولوژی فیلترشکنی را ارائه مي کند تا چه حد است؟(برای کاربر)
- در صورت گیر افتادن، مجازات محتمل برای استفاده از تکنولوژیهای گذر از فیلتر چقدر است؟
- آیا کاربر نهایی از ریسکهای امنیتی محتمل هنگام استفاده از یک تکنولوژی خاص، مطلع است؟

تعداد کاربران و پهنای باند موجود

برای تهیه‌کننده فیلترشکن ضروری است که تخمینی از تعداد کاربرانی که از آن استفاده می‌کنند داشته باشد و آن را با پهنای باند موجود متوازن سازد. کاربر نهایی نیز باید به پهنای باند در دسترس خود توجه کند، چون استفاده از این تکنولوژیها سرعت استفاده از اینترنت را کند می‌کند.

کسانی که پروکسی های عمومی را ایجاد می‌کنند باید توجه داشته باشند که ممکن است برخی از افرادی که در منطقه‌ای بدون سانسور زندگی می‌کنند نیز از امکانات آنها استفاده کنند. مثلا فیلترشکنها ممکن است برای دانلود یک فیلم کامل به کار گرفته شوند و این کار پهنای باند زیادی اشغال می‌کند. لذا ممکن است بخواهند دسترسی به فیلتر شکن را محدود کرده و یا مجموع پهنای باند در دسترس را محدود سازید. تکنولوژیهای مختلفی وجود دارند که همه یا برخی از این خواسته‌ها را ارضا می‌کنند.

نقطه اصلي دسترسی و استفاده کننده

بسته به اینکه کاربران نهایی از کجا به اینترنت متصل میشوند و چه سرویسهایی دریافت میدارند، گزینه‌های مختلفی برای تکنولوژیهای فیلترشکن وجود دارد. مثلا کاربرانی که از کامپیوترهای عمومی یا کافی‌نت‌ها به شبکه متصل می‌شوند امکان نصب هیچ گونه نرم‌افزاری را ندارند و به شیوه‌های مبتنی بر وب محدود میشوند. کاربران دیگری ممکن است کاربردهایی غیر از مرورگر وب (HTTP)، مثل ایمیل (SMTP) و انتقال فایل (FTP) را مد نظر داشته از این روی ممکن است بخواهند نرم‌افزارهایی را روی کامپیوترهایشان نصب کنند و تنظیمات کامپیوتر را دست‌کاری کنند. البته این نیازمند میزانی از تخصص برای کاربران است.

میزان تخصص تکنیکی

هرچه تخصص کاربران بیشتر بوده (و تعدادشان محدود باشد) گزینه‌های پیش رو برای گذر از فیلتر بیشتر است. کاربران غیر متخصص محدودیتهایی از قبیل نصب و راه‌اندازی و نیز هرگونه تغییر تنظیمات و قدمهای اضافی برای آماده سازی تکنولوژی عبور از فیلترها را پیش روی خویش خواهند داشت. این هم برای فراهم‌آورنده این فناوریها و هم برای کاربران نهایی حائز اهمیت است. استفاده نادرست از این فناوریها کاربران را در معرض خطرهایي قرار دهد که قابل اجتناب هستند.

در دسترس بودن افراد مطمئن

در صورتی که کاربران نهایی افراد قابل اعتمادی را در خارج از کشور بشناسند می‌توانند گزینه‌های خود را بیشتر و بهتر سازند. اگر چنین کسانی در دسترس نباشند گزینه‌ها به سیستم‌های در دسترس عموم محدود می‌شود. اگر کاربری بتواند این گزینه را بیابد مجریان فیلترینگ نیز مي توانند آنها را یافته و مسدود کنند. با وجود یک فرد مطمئن، کاربر می‌تواند به راه‌حلی مطابق با نیازهای خویش دست یابد و درعین حال برای اجتناب از ردگیری، ناشناس بماند. گذر کردن از فیلترینگ پایدار، موفق و بلندمدت با داشتن فردی قابل اعتماد در نقطه‌ای که فیلترینگ وجود ندارد، سهولتي بیشتر می‌یابد.

مجازات محتمل

آگاهی از میزان مجازات محتمل برای کسانی که به دلیل استفاده از تکنولوژیهای فیلترشکن دستگیر می‌شوند، به شدت مهم و حیاتی است. شیوه‌های به کار گرفته شده بسته به شدت این مجازاتها، می‌تواند تغییر کند. اگر شرایط قانونی چندان سخت‌گیرانه نباشد، کاربران می‌توانند از شیوه‌هایی استفاده کنند که علیرغم کارایی برای گذر از فیلتر، از لحاظ امنیتی چندان مطمئن نیستند. اگر محیط قانونی خیلی خطرناک است، باید از روشهایی استفاده کرد که پنهان و نیز ایمن باشند. برخی نیز ممکن است با یک پوشش قانونی یا سایر شیوه‌های ردگم‌کنی به کار گرفته شوند.

مخاطرات امنیتی

کاربرانی که از فیلترشکنها برای گذر از محدودیتها و انسدادهای اعمال شده توسط دولت بهره می‌برند باید نسبت به مخاطرات امنیتی احتمالی از قبیل امکان ردگیری توسط مجریان فیلترینگ و اقدام متقابل مثل مسدود شدن و شناسایی و نظاره استفاده آنان، مطلع باشند. بسته به شیوه‌های به‌کاررفته در انسداد و شیوه‌های مقابله، کاربران باید از مخاطرات احتمالی و اقدامات متقابل آگاه بوده و با به‌کارگیری شیوه مناسب در موقعیت مناسب و با منش صحیح، این مخاطرات کمینه شوند.

گذر کردن از فیلترینگ به شیوه ی آنلاین

گذر کردن از فیلترینگ آنلاین صفحات خاصی از وب هستند که به کاربران اجازه می‌دهند در فرمهای مخصوصی آدرس اینترنتی مورد نظر خود را وارد کرده و محتویات آن صفحه را که از طریق این فیلترشکنها گرفته می‌شود، مشاهده کنند. هیچ اتصالی بین کاربر و صفحه مورد نظر برقرار نیست و فیلترشکن صفحه مطلوب را بدون تغییرات به کاربر نمایش می‌دهد و به او اجازه می‌دهد صفحه مسدود شده را ببیند. فیلترشکنهای مبتنی بر وب هم چنین پیوندهای اینترنتی را به گونه‌ای بازنویسی می‌کنند که مشتمل بر آدرس فیلترشکن نیز باشند و بدین ترتیب امکان ادامه کار بدون مشکل با وب را فراهم می‌آورند. (در غیر این صورت لینکها به آدرسهایی که فیلتر شده‌اند اشاره می‌کردند و کلیک کردن روی آنها منجر به مواجهه مجدد با سد فیلترینگ می‌شد.) به هنگام استفاده از چنین فیلترشکنهایی کاربر نیازی به نصب نرم‌افزارهای خاص یا تغییر تنظیمات مرورگر خود ندارد. همه کاری که کاربر باید انجام دهد آن است که وارد صفحه اینترنتی مربوط به فیلترشکن شده و آدرس مورد نظر خود را (که مسدود شده است) در مستطیلی که مخصوص وارد کردن آدرس مهیا شده است تایپ کند و دکمه تاییدرا بزند.

(ظاهر آنها ممکن است اندکی تفاوت کند اما اصول کار به شیوه فوق‌الذکر است.) از این رو هیچ تخصصی لازم نبوده و از هر نقطه‌ای قابل دسترسی است.

مزایا:

- کار با فیلترشکنهای مبتنی بر وب ساده است و به نصب نرم‌افزار روی کامپیوتر کاربر نهایی نیازی نیست.
- فیلترشکنهای مبتنی بر وب عمومی در دسترس کسانی است که فرد مطمئنی در نقطه‌ای سانسور نشده سراغ ندارند.
- فیلترشکنهای مبتنی بر وب خصوصی می‌توانند برای ارضای نیازهای کاربران تغییر داده شده و کمتر در معرض کشف شدن از سوی مراجع فیلترینگ هستند.

معایب:

- فیلترشکنهای مبتنی بر وب عمدتا برای استفاده از وب (HTTP) بوده و ممکن است از طریق "دسترسی رمزنگاشته" (SSL) قابل استفاده نباشد. به علاوه برخی از سرویسهای وب مثل ایمیل ممکن است با این فیلترشکن‌ها خوب کار نکنند.
- فیلترشکنهای مبتنی بر وب عمومی معمولا شناخته شده هستند و ممکن است خودشان نیز فیلتر شده باشند!
- لازمه فیلترشکنهای مبتنی بر وب خصوصی آن است که کاربر نقطه امنیی در خارج از مرزها داشته باشد. در شرایط ایده‌ال دو سوی این اتصال باید بتوانند به سویه‌ای که قابل ردگیری نباشد با یکدیگر ارتباط داشته باشند.

سرویسهای عمومی گذر کردن از فیلترینگ به شیوه ی آنلاین

هم سرویسهای مبتنی بر وب و هم نرم‌افزارهای مربوط به گذر از فیلتر در دسترس عموم هستند. سرویسهای گذر از فیلتر به افراد، سازمان ها و شرکتهایی اطلاق می‌گردد که نرم‌افزار گذر از فیلتر را نصب و راه-اندازی کرده‌اند و آن را در معرض استفاده عمومی قرار داده‌اند. تنوع بسیاري دراین زمینه وجود دارد. برخي رایگان بوده و برخي دیگر با پرداخت حق عضویت، امکانات بیشتري از قبیل دسترسي رمزنگاري شده (که امکان ردگیري را کمتر مي‌سازد) پیش رو مي‌نهند. برخي توسط شرکتهاي تجاري به راه افتاده‌اند و برخي دیگر توسط افراد داوطلب. فهرستي از آنها را در زیر میبینید:

- http://www.anonymizer.com/
- http://www.unipeak.com/
- http://www.anonymouse.ws/
- http://www.proxyweb.net/
- http://www.guardster.com/
- http://www.webwarper.net/
- http://www.proxify.com/
- http://www.the-cloak.com/

با توجه به اين واقعيت كه آدرس بسياري از موارد فوق كاملا شناخته شده مي‌باشند، بسياري از برنامه‌هاي فيلترينگ نام آنها را در ليست خود دارند و نيز كشورهايي كه روي دسترسي به اينترنت محدوديت مي‌گذارند آنها را مسدود كرده‌اند. در اين صورت آنها غيرقابل ستفاده خواهند شد. همچنين بيشتر فيلترشكنهاي عمومي مبتني بر وب محتواي انتقال يافته به كاربر را رمزنگاري نمي‌كنند. در اين صورت، هر اطلاعاتي توسط اپراتور فيلترشكن قابل ديدن است.

فيلترشكنهاي عمومي مبتني بر وب بيشتر براي كاربراني مناسب است كه در محيط هاي كم‌مخاطره از اينترنت استفاده كرده و فرد مطمئني در نقاط بدون سانسور ندارند. اين فيلترها به درد كساني مي‌خورد كه به طور مقطعي و موقت نياز به دسترسي به اينترنت دارند و نياز به انتقال اطلاعات حساس و مهم ندارند.

نرم‌افزارهاي گذر از فيلتر به شيوه ى آنلاين (مبتني بر وب)

نصب نرم‌افزارهاي گذر از فيلتر معمولا نيازمند قدري تخصص فني و نيز منابع مناسب از قبيل ميزبان وب و نيز پهناي باند مناسب است. با يك فيلترشكن خصوصي موقعيت كاربر فقط براي كاربران مورد نظر قابل شناسايي است در حاليكه فيلترشكنهاي عمومي و سرويسهاي ناشناس هم براي كاربران نهايي و هم كساني كه فيلترينگ را اعمال كرده‌اند قابل شناسايي است.(كه عمدتا هم فيلتر شده‌اند) احتمال شناسايي و انسداد فيلترشكنهاي خصوصي نسبت به عمومي‌ها كمتر است.

فيلترشكنهاي شخصي را مي‌توان با اندكي تغييرات و تطابق با نيازهاي كاربر به راه انداخت. برخي از تغييرات رايج تغيير دادن نام پورت مورد استفاده توسط سِرور و نيز اعمال رمزنگاري است. SSL پروتكلي براي انتقال امن اطلاعات در اينترنت است. اين پروتكل عمدتا توسط وب‌سايتها براي انتقال امن اطلاعاتي سري از قبيل اطلاعات كارت اعتباري و ... به كار برده مي‌شود. وب سايت هايي كه با اين پروتكل كار ميكنند به جاي HTTP معمولي از طريق HTTPS قابل دسترسي‌اند. گزينه ديگري كه هنگام استفاده از SSL پيشنهاد مي‌شود ايجاد يك صفحه خالي و بي-ضرر در روت مربوط به سِرور وب و پنهان ساختن فيلتر شكن در يك آدرس و نام تصادفي است. اگرچه يك واسطه ممكن است وب سايتي كه كاربر قصد اتصال به آن را

دارد كشف كند اما نخواهد توانست آدرس صفحه درخواست شده را دريابند چرا كه رمزنگاري شده است. مثلا اگر كاربري مايل به مشاهده صفحه زير باشد

https://example.com/secretcircumventor

يك واسطه مي‌تواند كشف كند كه كاربر بهhttps://example.com متصل شده است اما نميتواند صفحه مورد نظر را بيابد. اگر اپراتور فيلترشكن يك صفحه خالي در https://example.com قرار دهد آنگاه فيلترشكن كشف نخواهد شد.

- CGIProxy : يك متن CGI مانند پروكسيهاي HTTPS و يا FTP كار مي‌كند:
  - http://www.jmarshall.com/tools/cgiproxy/
- فيلتر شكن صلح جنگ : برنامه‌اي است كه به صورت خودكار نصب ميشود و براي كاربراني كه تخصص فني ندارند فرايند نصب و استفاده از CGIProxy را بسيار تسهيل مي‌كند.
  - http://www.peacefire.org/circumventor/simple-circumventor-instructions.html
- pHproxy: يك فيلترشكن مبتني بر وب تجربي و بسيار قابل تغيير به فراخور نياز كاربر
  - http://ice.citizenlab.org/projects/phproxy/
- Psiphon: يك وب‌سرور كه قابليت SSL را داشته و يك فيلترشكن مبتني بر وب در خود دارد.
  - http://Soon to be released

فيلترشكنهاي خصوصي مبتني بر وب كه قابليت رمزنگاري داشته باشند به كار كساني مي‌آيد كه يك اتصال به اينترنت پايدار و نيز قابل اعتماد نياز داشته و فرد مطمئني در نقاط فيلترنشده سراغ دارند. علاوه بر اين تخصص فني كافي و پهناي باند مناسب براي راه‌اندازي و نگهداري يك فيلترشكن را در اختيار دارند. اين منعطف‌ترين نوع ارتباط اينترنتي براي استفاده عمومي بوده و احتمال ردگيري و انسداد آن اندك است.

فيلترشكنهاي به شيوه ى آنلاين : ملاحظات امنيتي

بايد توجه داشت كه سيستمهاي فيلترشكن لزوما ناشناس بودن را به ارمغان نمي‌آورند. اگر چه هويت كاربر نهايي از اپراتور سايتهايي كه از طريق فيلترشكن ديده مي‌شوند،مخفي ميگردد اما اگر ارتباط متني باشد (از طريق http) باشد، همان‌گونه كه عمدتا در سرويسهاي رايگان ميباشد، ردگيري و مشاهده آن براي يك حضور واسطه مثل ISP امري سهل است. از اين رو، اگر فرايند فيلترشكني با موفقيت انجام شود، نهادي كه فيلترينگ را انجام داده است ميداند كه كاربر از يك فيلترشكن مبتني بر وب استفاده كرده است.

بعضي از فيلترشكنهايي كه براي متن ساده به كار مي‌روند (رمزنگاري نشده) اقدام به ايجاد ابهام در URL كرده تا فيلترهايي كه در URLها دنبال كلمات كليدي مي‌گردند گمراه شوند. به عنوان مثال استفاده از تكنيك ساده‌اي مثل ROT-۱۳ كه در ان هر حرفي با حرفي كه ۱۳ تا از آن جلوتر است جايگزين ميشود، آدرس

http://ice.citizenlab.org به آدرس uggc://vpr.pvgvmrayno.bet تبديل ميشود. در واقع متن URL به رمز تبديل ميشود تا كلمات كليدي كه تكنولوژيهاي فيلترينگ به دنبالشان مي‌گردند در URL موجود نباشد. با اين همه اگرچه فيلترشكن موفق عمل كرده است، اما ممكن است محتواي صفحه ديده شده مورد رديابي واقع شود.

مخاطراتي در مورد استفاده از كوكي‌ها و اسكريپت‌ها وجود دارد. بسياري از فيلترشكنها امكان زدودن كوكي-ها و اسكريپت‌ها را در اختيار مي گذارند، اما برخي از سايتها (مثل سرويسهاي ايميل) نيازی كاركردی به آنها دارند. هنگام فعال كردن اين گزينه‌ها بايد محتاط بود.

خطر محتمل ديگر به خصوص هنگامي كه با سايت هايي سرو كار داريد كه نيازمند رمز ورود است، اتصال به فيلترشكن از طريق ارتباط متني و پس از آن درخواست اطلاعات رمزنگاري شده است. دراين حالت فيلترشكن اطلاعات را از يك سرور مبتني بر SSL و از طريق يك ارتباط رمزنگاري شده دريافت ميكند اما اين اطلاعات را به صورت متن ساده براي كاربر ميفرستد و اين كار اطلاعات حساس را در معرض آشكار شدن قرار مي‌دهد.

برخي از اين مسائل امنيتي با استفاده از پروكسي هاي مبتني بر وب از طريق ارتباط رمزنگاري شده، قابل حل است. برخي پروكسي ها براي اتصال از طريق SSL (HTTPS) كه اتصال بين فيلترشكن و كاربر را رمزنگاري مي‌كند، تنظيم شده‌اند. دراين حالت، واسطه‌ها تنها مي‌توانند كشف كنند كه كاربر به فيلترشكن مبتني بر وب متصل شده است (آنها نميتوانند محتوا را مشاهده كنند).

در صورتي كه مخاطرات امنيتي زياد باشد استفاده از فيلترشكنهاي مبتني بر وب كه SSL در آنها فعال باشد به شدت توصيه مي‌شود. با اين همه عليرغم آنكه اتصال كاربر نهايي به فيلترشكن ممكن است امن باشد اما صاحب آن فيلترشكن مي‌تواند اطلاعاتي كه به كاربر فرستاده مي‌شود مرور كند. يك مساله امنيتي ديگر پرونده‌هاي ارتباط كاربران با فيلتر شكن است. بسته به موقعيت فيلترشكن يا محل سِرور آنها، ممكن است مسئولاني وجود داشته باشند كه امكان دسترسي به اين اطلاعات را داشته باشند.
حتي در صورت استفاده از فيلترشكنهاي مبتني بر وب كه در آنها SSL فعال است باز هم نگرانيهايي وجود دارد. اولين مورد آن است كه استفاده از رمزنگاري موجب جلب توجه به فعاليتهاي گذر از فيلتر توسط كاربر مي‌شود. همچنين ممكن است استفاده از رمزنگاري در همه كشورها قانوني نباشد. ثانيا براي مراجع فيلترينگ كشف اينكه كاربر چه وب-سايتهايي را مشاهده كرده است ميسر است و اين امر با استفاده از تكنيكهايي به نام اثرانگشت HTTPS و حمله به اصطلاح "مرد ميانه" MITM امكان پذير است. اگر چه، صفحاتي با محتواي ديناميك يا فيلترشكنهايي كه مقداري متن تصادفي را براي ردگم‌كردن به محتواي درخواست شده مي-افزايند و/يا چند تصوير به محتوا اضافه مي‌كنند باعث مي‌شود كه اين تكنيك تا حد بسيار زيادي كم مخاطره و مطمئن شود. اگر ”اثر انگشت SSL “ يا امضاي امنيتي براي كاربران مهيا باشد، آنها مي‌توانند شخصا نسبت به سنجش اينكه گواهينامه و اينكه قابل اعتماد هست يا نه اقدام كنند. اگر معتبر باشد، جلوي حمله MITM را خواهد گرفت. (براي اطلاعات بيشتر در مورد حملات احتمالي به سيستم‌هاي فيلترشكن مقاله زير را ببينيد:

"فهرست نقاط ضعف احتمالي در سيستم‌هاي عبور از سانسور اينترنت نوشته بنت هاسلتون كه در آدرس زير موجود است:

http://peacefire.org/circumventor/list-of-possible-weaknesses.html

و نيز جوابيه پل بارانوفسكی در:

http://www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

سِرورهاي پروكسي

يك سِرور پروكسي، نوعي از سِرور است كه بين يك كاربر مثل مرورگر وب، و يك سرور، مثل سرور وب، واقع شده است. پروكسي در نقش يك حايل و يا واسط ميان كاربر و سرور ظاهر مي‌شود و انواعي از درخواست‌هاي اطلاعات را پشتيباني مي‌كند. داده هايي از چون تبادل اطلاعات مرور وب (HTTP) ، تبادل فايل (FTP)، و تبادل اطلاعات رمزنگاري شده (SSL). سرورهاي پروكسي توسط افراد، نهادها و حتي دولت‌ها براي اهداف مختلفي مانند مسائل امنيتي، ناشناس بودن، ذخيره اطلاعات و فيلترينگ مورد استفاده واقع مي‌شوند. كاربر نهايي براي بهره‌گيري از سرورهاي پروكسي بايد تنظيماتي را در مرورگر وب خويش تغيير داده و آدرس IP يا آدرس اينترنتي ميزبان پروكسي را به همراه شماره پورت مورد استفاده پروكسي را وارد كنند. اگر چه اين كار ساده است ولي ممكن است انجام آن در مكانهاي عمومي مثل كافي‌نت يا كتابخانه و محل كار ... ميسر نباشد.

مزايا:

- مي توان از ميان نرم‌افزاري بسيارى كه موجود هستند و قادرند به خوبي گردش مرور وب http را به صورت شفاف به كاربر منتقل كنند و قابليت تنظيم براي كاركردن با پورتهاي غيراستاندارد را دارند، انتخاب كرد.
- تعداد كثيري از پروكسيهاي عمومي در دسترس همگان قرار دارد.

معايب:

- بيشتر سرورهاي پروكسي به طور پيش‌فرض براي رمزنگاري تنظيم نشده‌اند و از اين رو صرفا در نقش يك واسطه ساده اطلاعات را به كاربران مي‌رسانند و به همين دليل چندان ايمن نيستند.
- كاربر بايد اجازه لازم براي تغيير در تنظيمات مرورگر وب را داشته باشد (چيزي كه در بيشتر مكانهاي عمومي وجود ندارد). به علاوه اگر ISP بخواهد كه همه اطلاعات از يك پروكسي خاص عبور كند، آنگاه نميتوان از يك پروكسي آزاد استفاده نمود.
- جستجو و استفاده از پروكسيهاي عمومي ممكن است غيرقانوني بوده و در هر زماني از سوي مراجع مربوطه مسدود شده و از اين رو غيرقابل دسترسي گردد.

نرم افزار سرور پروكسي

نرم افزار سرور پروكسي ميتواند توسط يك فرد مورد اعتماد كه اندكي تخصص دارد و در محلي بدون سانسور زندگي ميكند نصب شده و يك سرور پروكسي را ايجاد كند. پروكسي ها بايد جايي راه‌اندازي شوند كه پهناي باند كافي وجود داشته و لازم است كه تكنولوژيهاي رمزنگاري نيز به كار گرفته شود. به طور خاص زماني كه يك سازمان يا اداره نياز به يك فيلترشكن پايدار دارد اين راه حل مناسب است. پس از آنكه كاربراني كه در منطقه فيلترشده قرار دارند، مرورگر وب خود را طوري تنظيم كردند كه به آدرس پروكسي اشاره كند، مي‌توانند بدون مشكل خاصي به گردش در اينترنت بپردازند. اگر چه سرورهاي پروكسي بهترين راه حل نيستند اما نسبت به پروكسيهاي مبتني بر وب شيوه مناسب‌تري به حساب مي‌آيند. يكي از دلايل اين برتري در زمان كاركردن با سايتهايي كه نياز به كوكي يا شناسايي كاربر دارند (مثل وب‌سايتهاي مربوط به ايميل) به چشم مي‌آيد چون سرورهاي پروكسي به طور يكنواخت‌تري كار مي‌كنند. سرورهاي پروكسي ميتوانند براي ارضاي نيازهاي مشتري تغيير داده شوند و با توجه به شرايط محيطي فيلترينگ تنظيم شوند.

- Squid يك نرم‌افزار پروكسي رايگان است و مي‌توان ايمني آن را توسط سِرور Stunnel بالا برد:
  - http://www.squid-cache.org/
  - http://www.stunnel.org/
  - http://ice.citizenlab.org/projects/aardvark/
- Privoxy يك پروكسي با امكانات بالايي جهت فيلترينگ مي-باشد كه امكان حفظ حوزه شخصي را فراهم ميكند.
  - http://www.privoxy.org/
- Secure Shell (SSH) يك پروكسي socks دروني دارد.
  ($ ssh -D port secure.host.com)
  - http://www.openssh.com/

HTTPport/HTTPhost امكان گذر از پروكسي HTTP را كه شما را از دسترسي به اينترنت باز ميدارد فراهم ميكند.

سرورهاي پروكسي خصوصي كه امكان رمزنگاري نيز داشته باشند بيش از همه براي گروهها و يا افرادي كه در يك اداره مشغول به فعاليت هستند مناسب است. اين پروكسيها براي كساني مناسبند كه يك فيلترشكن هميشگي و پايدار نياز داشته و فرد قابل اعتمادي با مهارتهاي تخصصي كافي و نيز دسترسي به پهناي باند زياد در نقطه-اي بدون سانسور سراغ دارند كه امكان نصب و راه‌اندازي يك سرور پروكسي را براي ايشان فراهم كند.

سرورهاي پروكسي عمومي

پروكسي هاي باز، سرورهايي هستند كه عمدا ويا سهوا براي اتصال كامپيوترهاي ديگر باز گذاشته شده‌اند. پورتهاي كامپيوتري كه به عنوان پروكسي باز گذاشته شده‌اند تا به كاربران پراكنده در مناطق مختلف دور و نزديك امكان اتصال بدهند يكي از ويژگيها و حتي ضروريات ساختار در هم تنيده شبكه اينترنت است.به هرحال مشخصا معلوم نيست كه پروكسيهاي باز به عنوان يك سرويس عمومي در اختيار همگان هستند يا اينكه صرفا به علت تنظيم نامناسب به صورت سهوي به كاربران عمومي امكان اتصال مي‌دهند.

اخطار: بسته به تفسيري كه از قانون هر كشور، استفاده از پروكسيهاي باز ممكن است به دسترسي غيرمجاز تفسير شده و استفاده كنندگان از آن ممكن است در معرض مجازات احتمالي واقع شوند. استفاده از اين پروكسيها چندان توصيه نميشود.

يافتن پروكسي هاي باز

وب‌سايتهاي متعددي ميتوان يافت كه فهرست هاي مفصلي از پروكسيهاي باز ارائه كرده‌اند با اين وجود تضميني نيست كه آنها هنوز هم كار كنند . بسياري از اين پروكسيها ممكن است ديگر براي عموم قابل استفاده نباشند. به علاوه تضميني وجود ندارد كه اطلاعات موجود در اين ليستها به خصوص اطلاعات مربوط به ميزان ناشناس بودن و نيز مكان جغرافيايي آنها دقيق باشد. دقت كنيد كه شما با مسئوليت خودتان از آنها استفاده مي‌كنيد!
وب‌سايتهايي كه ليست پروكسيهاي باز در آنها موجود است:

- http://www.samair.ru/proxy/
- http://www.antiproxy.com/
- http://tools.rosinstrument.com/proxy/
- http://www.multiproxy.org/
- http://www.publicproxyservers.com/

نرم‌افزار: ProxyTools/LocalProxy

- http://proxytools.sourceforge.net/

پروكسي هاي باز: پورتهاي نامعمول

برخي كشورها كه اقدام به انسداد اينترنت در سطح ملي مي‌كنند دستيابي به پورتهاي پروكسي استاندارد را مسدود مي‌سازند."پورت" يك مكان اتصال منطقي است كه توسط پروتكلهاي خاصي مورد استفاده قرار مي‌گيرد. سرويسهاي اينترنتي مختلف اطلاعات را از طريق شماره پورتهاي خاصي عبور مي‌دهند. شماره پورتهاي خاصي به پروتكلها و سرويسهاي مشخصي تخصيص داده شده است. اين كار توسط"مرجع تخصيص شماره‌هاي اينترنت "انجام مي‌شود. مثلا پورت ۸۰ براي تبادل ديتاي معمولي (HTTP) تخصيص يافته است. وقتي شما در مرورگر وب خود به يك سايت متصل مي‌شويد، در واقع به يك سرور وب كه روي پورت ۸۰ كار مي‌كند متصل شده‌ايد. سرورهاي پروكسي نيز پورتهايي دارند كه به صورت پيش‌فرض به آنها تخصيص يافته است. در نتيجه بسياري از تكنولوژيهاي فيلترينگ اجازه دسترسي به اين پورتها را نميدهند. از اين رو ممكن است براي موفقيت در گذر از فيلتر نياز باشد كه استفاده از پروكسي كه با پورتهاي استاندارد كار نمي‌كند ضروري باشد

- http://www.web.freerk.com/proxylist.htm

سرورهاي پروكسي : نگرانيهاي امنيتي

تنظيمات و راه‌اندازي سرورهاي پروكسي بسيار مهم است. بسته به تنظيمات صورت گرفته، پروكسيها ممكن است به خوبي هويت كاربر را مخفي نكرده و يا مشكلات امنيتي به بار بياورند. علاوه بر كاستي در مورد رمزنگاري محتوا، پروكسيها ممكن است اطلاعاتي را از كاربر نهايي به سروري كه اطلاعات از آن دريافت ميشوند بدهند كه شايد بتوان از آن اطلاعات، آدرس IP كاربر را كشف كرد. ضمنا همه محتواي تبادل شده ممكن است به صورت متني ساده باشد و از اين رو ممكن است توسط مراجع فيلترينگ، پيش از رسيدن به شما فيلتر شود. همچنين صاحب سرور پروكسي مي‌تواند هرآنچه از آن مي‌گذرد فيلتر نمايد.
استفاده از سرورهاي پروكسي كه در دسترس عموم هستند توصيه نمي‌شود. سرورهاي پروكسي باز به خاطر در دسترس بودنشان مورد استفاده واقع مي‌شوند اما حتي اگر بتوانند از فيلترينگ عبور كنند، در مورد مسائل امنيتي هيچ تضميني در مورد آنها وجود ندارد. يعني ممكن است شما بتوانيد يك صفحه مسدود شده را ببينيد ولي در عين حال احتمال شناسايي شما توسط مراجع قضايي وجود دارد. مشابه پروكسي‌هاي مبتني بر وب، سرورهاي پروكسي نيز در معرض مخاطرات يكساني هستند. كوكيها و اسكريپت‌هاي خطرناك هنوز هم ممكن است كه به كاربر نهايي منتقل شود. حتي اگر سرور پروكسي از تكنولوژي رمزنگاري استفاده نمايد باز هم ممكن است در معرض حمله MITM و يا اثر انگشت HTTPS قرار بگيرد. همچنين بايد توجه داشت كه برخي مرورگرهاي وب هنگام كاركردن با پروكسيهاي socks اطلاعات را درز مي‌دهند. اين نوع پروكسيها علاوه بر تبادل اطلاعات عادي (HTTP) ساير عمليات را نيز ممكن مي‌سازند. وقتي درخواست مربوط به يك وب‌سايت مي‌رسد، آدرس آن به يك آدرس IP ترجمه مي‌شود. برخي از مرورگرهاي وب اين كار را به صورت محلي انجام مي‌دهند و از اين رو پروكسي نقشي در آن ندارد. در اين حالات، درخواست براي وب سايت مسدود شده از طريق سرورهاي "سيستم اسامي دامنه كه درون كشور مجري فيلترينگ واقع است اجرا مي‌شود.استفاده از پروكسيهاي باز كه در دسترس عموم هستند يك روش مرجع نبوده و فقط براي كساني كه در مخاطرات امنيتي پاييني هستند توصيه مي‌شود. كساني كه استفاده تفننی و جاري داشته و نيازي به تبادل اطلاعات سري و حساسيت‌برانگيز ندارند.

نقب‌زدن

نقب‌زدن كه همچنين با نام "دور زدن پورت نيز شناخته مي‌شود به هركس اجازه مي‌دهد محتواي غير ايمن و رمزنگاري نشده را توسط يك پروتكل رمزنگاري شده منتقل سازد. كاربري كه در مكان داراي انسداد اينترنت به سر مي‌برد بايد نرم‌افزاري را كه نقب را ايجاد مي‌كند دانلود كند. اين نرم‌افزار به يك كامپيوتر در نقطه‌اي بدون فيلترينگ، يك تونل مي‌زند. سرويسهاي معمولي روي كامپيوتر كاربر قابل دستيابي هستند ولي از طريق تونلي رمزنگاري شده به كامپيوتري فيلترنشده. اين كار با ارسال درخواستهاي كاربر و نيز پاسخهاي رسيده به او انجام مي‌شود. محصولات موجود در اين زمينه متنوع هستند. كساني كه افراد مطمئني در كشورهاي فيلتر نشده دارند مي‌توانند ميتوانند سرويسهاي نقب زدن شخصي را راه بيندازند. كساني هم كه چنين امكاني ندارند ميتوانند سرويسهاي تجاري را كه عمدتا حق اشتراك ماهيانه دريافت ميكنند بخرند. كاربران بايد توجه داشته باشند كه سرويسهاي رايگان نقب زدن عمدتا همراه با آگهي‌هاي تبليغاتي هستند. تبليغات از طريق درخواستهاي مربوط به متنهاي ساده (HTTP) ارسال مي‌شود و ممكن است توسط يك حايل كه مي‌تواند تشخيص دهد كه كاربر در حال استفاده از شيوه نقب زدن است، مسدود شود. به علاوه هر روشي در نقب زدن متكي به استفاده از پروكسيهاي SOCKS است كه ممكن است اسامي دامنه را درز بدهد.

- http://www.http-tunnel.com/
- http://www.hopster.com/
- http://www.htthost.com/

مزايا:

- برنامه‌هاي نقب زدن اطلاعات را به صورت رمزنگاري شده منتقل مي‌كنند.
- اين برنامه‌ها عموما امكان كار كردن با پروتكلهاي بسياري را دارند (نه فقط ترافيك وب يعني پروتكل HTTP)
- در اين زمينه براي كساني كه افراد مطمئني در نقاط فيلتر نشده در دسترس ندارند سرويسهاي تجاري وجود دارد كه قابل ابتياع هستند.

معايب:

- سرويسهاي تجاري شناخته شده هستند و ممكن است فيلتر شوند.
- برنامه‌هاي نقب زدن در مكانهاي عمومي مثل كافي‌نت و كتابخانه كه امكان نصب نرم‌افزار وجود ندارد قابل استفاده نيستند.
- استفاده از شيوه‌هاي نقب زدن ممكن است نسبت به ساير روشها تبحر بيشتري نياز داشته باشد.

سرويسهاي نقب زدن بيشتر براي كساني مناسب است كه از لحاظ تكنيكي نسبتا ماهر بوده و نياز به يك اتصال ايمن (ولي نه لزوما ناشناس) داشته و از مكانهاي عمومي به اينترنت متصل نميشوند. سرويسهاي تجاري نقب زدن يك راه حل عالي براي كساني است كه در كشورهاي دچار سانسور قرار داشته و افراد مطمئني در خارج از كشور ندارند.

سيستم‌هاي ارتباطاتي ناشناس

تكنولوژيهاي فيلتر شكن و سيستمهاي ارتباطاتي ناشناس هر دو به يك شيوه كار مي‌كنند و گاهي به هم مرتبط اند اما در حوزه‌هاي كاملا متفاوتي به كار مي‌روند. سيستمهاي ارتباطاتي ناشناس بر تضمين اختفاي كاربر بوسيله پنهان كردن هويت او از ارائه دهنده محتوا متمركز مي‌شوند. به علاوه، مجموعه‌اي از سيستم‌هاي پيشرفته روتينگ به كار گرفته مي‌شود تا تصميني براي اختفاي هويت كاربر از خود سيستم ارتباطاتي ناشناس فراهم نمايد. در كنار امكان دريافت اطلاعات به صورت ناشناس، اين سيستم‌ها به كاربر امكان انتشار مطالب به صورت ناشناس را بر روي اينترنت ميدهد. سيستمهاي گذر از فيلتر لزوما بر ناشناس بودن تمركز ندارند. به جاي آن تمركز بر ايجاد

ارتباط ايمن براي گذر از محدوديت‌هاي اعمال شده بر كاربران براي دريافت محتوا يا انتشار مطالب است. دورزدن موانع اعمال شده نيازمند ارتباطات ايمن و مطمئن و نيز اندكي چاشني پنهان‌كاري است و در اين فرايند لزوما نيازي به ناشناس بودن نيست.

در موارد بسياري سيستمهاي ارتباطاتي ناشناس براي گذر از فيلترها به كار گرفته مي‌شود. مزيت اين سيستمها در آن است كه تعداد زيادي از شبكه‌هاي موجود در دسترس هستند كه ميتوان بلادرنگ به آنها وارد شد و ميتوانند براي گذر از فيلتر مورد استفاده واقع شوند و نيز ميتوان از اين مزيت استفاده كرد كه ناشناس ماند.

نرم‌افزار مربوطه كه برخي از انواع آن نياز به تخصص فني دارند، بايد روي كامپيوتر كاربر نصب شود. تعداد زيادي از اين پروژه‌ها وجود دارد و محبوب‌ترين هاشان به سرعت در حال افزايش سهولت و سادگي براي كاربران هستند و انجمنهاي توسعه‌ی اين نرم‌افزارها به شدت فعال هستند. استفاده از سيستم‌هاي ارتباطاتي ناشناس به كاربراني محدود مي‌شود كه مجوز نصب نرم‌افزار مربوطه را روي كامپيوتر داشته باشند. كاربراني كه از مكانهاي عمومي به اينترنت دسترسي دارند، عمدتا نميتوانند از اين شيوه استفاده كنند. به علاوه مساله كندي ارتباط نيز مطرح است. مهمترين نگراني مربوط به قابليت تكنولوژيهاي فيلترينگ براي مسدود كردن ارتباط با اين شيوه است.

سيستم‌هاي ارتباطاتي ناشناس لزوما براي كاربراني كه با مساله انسداد اينترنت مواجهند طراحي نشده است. كاربراني كه در سطح كشور يا ISP قصد دور زدن محدوديت‌ها را دارند ممكن است ببينند كه مراجع فيلترينگ با شيوه‌هاي خاصي اقدام به محدودسازي دستيابي به اين سرويسها نموده‌اند. اگر سيستم‌هاي ارتباطاتي ناشناس براي گذر از فيلتر از يك پورت ثابت استفاده كند، نرم‌افزار فيلترينگ به سادگي ميتواند آن را مسدود سازد. هر چه سيستم ارتباطاتي ناشناس معروف‌تر باشد، احتمال آنكه مراجع فيلترينگ و تكنولوژيهاي مربوطه آن را كشف و مسدود كرده باشند، بيشتر است. به علاوه براي مبارزه با سيستمهايي كه بر PEERS يا نقاط معرف اتصال همگاني متكي هستند، مراجع فيلترينگ مي‌توانند به سادگي دسترسي به اين ميزبانهارا مسدود سازند. آنها مي‌توانند پورت خودشان را جايگزين كنند و كاربري را كه تلاش مي‌كند به آن وصل شود شناسايي كنند. نهايتا، در بعضي محيط هاي محدود شده كه سيستمهاي معروف مورد ردگيري و كنترل قرار دارند، استفاده از آنها موجب جلب توجه به سمت كاربر ميشود

مزايا:

- سيستم‌هاي ارتباطاتي ناشناس هم امنيت و هم ناشناس بودن را به ارمغان مي‌آورند.
- اين سيستمها عموما امكان كار كردن با پروتكلهاي بسياري را دارند (نه فقط ترافيك وب يعني پروتكل HTTP)

- سيستم‌هاي ارتباطاتي ناشناس اغلب داراي رشد مداوم و انجمن كاربران و توسعه‌دهندگان هستند كه ميتوانند از لحاظ فني به كاربران كمك كنند.

معايب:

- سيستم‌هاي ارتباطاتي ناشناس مشخصا براي گذر از فيلتر طراحي و ساخته نشده‌اند. آنها معروف هستند و ممكن است به سادگي فيلتر شوند.
- سيستم‌هاي ارتباطاتي ناشناس در مكانهاي عمومي مثل كافي‌نت و كتابخانه كه امكان نصب نرم‌افزار وجود ندارد قابل استفاده نيستند.
- استفاده از سيستم‌هاي ارتباطاتي ناشناس ممكن است نسبت به ساير روشها تبحر بيشتري نياز داشته باشد.

- Tor يك شبكه از نقبهاي مجازي است كه به مردم و گروهها امكان ارتقاي سطح اختفا و نيز امنيت در اينترنت را مي‌دهد. همچنين به نرم‌افزارنويسان امكان خلق ابزارهاي ارتباطاتي جديد با صورتبندي اختفاي دروني را ميدهد. Tor مبناي طيف وسيعي از برنامه‌ها است كه به سازمانها و افراد اجازه مي‌دهد اطلاعات را بدون در معرض تهديد نهادن هويت خويش در شبكه‌هاي عمومي به اشتراك بگذارند.
  - **http://tor.eff.org/**
- JAP اين امكان را فراهم مي‌آورد كه در اينترنت به صورت ناشناس گشت و گذار كنيد! به جاي اتصال مستقيم به سرور، كاربران از يك مسير انحرافي استفاده مي‌كنند و با استفاده از رمزنگاري و از طريق واسطه‌هاي متعدد متصل مي‌شوند.
  - **http://anon.inf.tu-dresden.de/index_en.html**
- Freenet يك نرم‌افزار رايگان است كه به شما اجازه مي‌دهد اطلاعات را بدون واهمه از سانسور دريافت كرده يا در اينترنت منتشر سازيد. براي نيل به اين آزادي، شبكه كاملا غيرمتمركز شده است و نشردهندگان و مصرف-كنندگان اطلاعات كاملا ناشناس هستند.
  - **http://freenet.sourceforge.net/**

سيستم‌ها ارتباطاتی ناشناس بيشتر براي كساني مناسب است كه از لحاظ تكنيكي نسبتا ماهر بوده و هم نياز به اختفاي هويت و هم نياز به گذر از فيلتر دارند و از مكانهاي عمومي به اينترنت متصل نميشوند.

نتيجه‌گيري

تصميم در مورد استفاده از تكنولوژي گذر از فيلتر بايد جدي انگاشته شود: با تحليل دقيق نيازهاي خاص، منابع موجود و نگرانيهاي امنيتي كاربر نهايي. طيف گسترده‌اي از تكنولوژيها براي كساني كه مايلند از فيلتر عبور كنند، وجود دارد اما استفاده موفق و پايدار از اين تكنولوژيها در دسترسي به اينترنت به عوامل متعددي از قبيل سطح دانش فني كاربر، مخاطرات امنيتي احتمالي و نيز افراد مورد اعتماد در خارج از منطقه

سانسور شده بستگي دارد. به علاوه دولتها ممكن است به اقدامات متقابل براي مسدود كردن اين تكنولوژيها دست يازند.

كليد قابليت فيلترشكني موفق و پايدار، اعتماد و كارايي است. سيستمهاي فيلترشكن بايد براي كاربر در شرايط خاص هدف گرفته شوند و يا براي نيازهاي خاص او آماده استفاده باشند. لازم است آنها ايمن بوده و قابليت تنظيم و امكان اختفا داشته باشند. بين فراهمآورنده فيلترشكن و كاربر نهايي بايد اعتماد وجود داشته باشد و اين ميسر نيست مگر از خلال درك شرايط قانوني و سياسي كه كاربر نهايي در آن به سر مي‌برد. به علاوه كاربر بايد از محدوديتها و مخاطرات احتمالي مطلع باشد. كاربران و فراهمآورندگان فيلترشكنها بايد همانگونه كه از تكنولوژيهاي فيلتر شكن مطلع هستند از تكنولوژيهاي فيلترينگ نيز با خبر باشند. بدين ترتيب تصميمي مبتني بر اطلاعات جامع در مورد انتخاب و استفاده از يك تكنولوژي فيلترشكن اتخاذ خواهد شد.

شما در صورت هر گونه سوالی درمورد مقالات میتوانید با این آدرس با من تماس بگیرید:

taghavishahri@yahoo.com