راهنمای جامع مقابله با فیلترینگ

نگارش ۱,۰

مرداد ۱۳۸۵

نسخه غیر قابل چاپ

No-filter.com

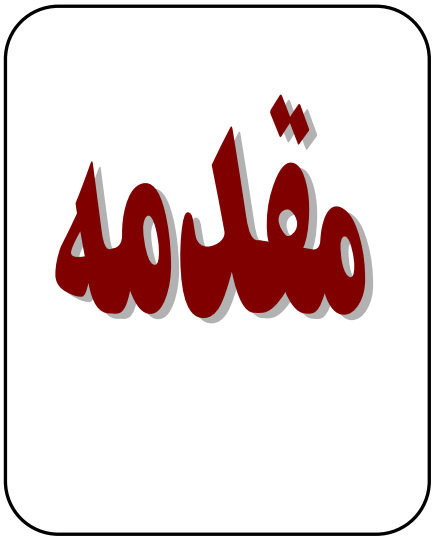
The Comprehensive Guide to
Bypassing Internet Censorship

First Edition (Ver1.00)

August 2006

No Printable Version

No-filter.com



مقدمه

ایران یکی از بزرگترین سانسور کنندگان اینترنت در جهان به شمار میرود و نتایج یک تحقیق معتبر نشان میدهد که یک سوم سایتهای اینترنتی در ایران فیلتر شده‌اند. با این وجود، متأسفانه، هیچ مرجع جامع و کاملی که به صورت علمی به مسئله فیلترینگ پرداخته باشد به زبان فارسی وجود نداشت و سایتهایی که در این زمینه مطلبی ارائه کرده بودند عمدتاً توسط افراد آماتور و به سبک بسیار مبتدی نوشته شده بودند. تنها چیزی که در این سایتها می‌شد پیدا کرد آدرس پروکسی، معرفی چند نرم‌افزار و تعدادی راهنمایی عامیانه در مورد فیلترینگ بود. هر چند منابع تخصصی معتبری در این زمینه به زبان انگلیسی وجود دارد ولی اکثر کاربران ایرانی به علت ندانستن زبان خارجی و سطح پایین دانش IT قادر به استفاده از این منابع نیستند.

بر همین اساس بود که تصمیم به نگارش "راهنمای جامع مقابله با فیلترینگ" گرفته شد. مطالبی که در اینجا میخوانید برگرفته از مجموعه مقالات وب سایت نوفیلتر است که در قالب یک جزوه الکترونیکی (PDF) گردآوری شده‌اند. در این مقالات سعی شده خواننده قدم به قدم و به طور اصولی با فیلترینگ و روشهای مقابله با آن آشنا شود. در اینجا شما مانند بسیاری از سایتها، لیستی از پروکسی‌ها و فیلترشکن‌ها را نخواهید یافت، بلکه ما به شما خواهیم آموخت که پروکسی چیست و چگونه خودتان میتوانید یک پروکسی درست کنید. مقالات ما هیچ کدام ترجمه خالص یک متن خارجی نیستند بلکه بر اساس متون معتبر تألیف شده‌اند. این مقالات تماماً اختصاصی وب سایت نوفیلتر هستند و تا به حال در هیچ کجا منتشر نشده‌اند، هر چند مطمئن هستیم به زودی تعداد زیادی از سایتها آن را به نام خودشان کپی خواهند کرد. مهمترین تفاوتی که این کپی‌ها با اصل خواهند داشت این است که ما مکرراً مطالب خود را به روز خواهیم کرد و قسمتهای جدیدی را به آن خواهیم افزود؛ کاری که آنها از انجام آن ناتوان خواهند بود.

تلاش شده مطالب در عین حفظ اصالت علمی، به زبان ساده و برای کاربرانی نوشته شود که از دانش کامپیوتر سررشته زیادی ندارند. با این حال، برای فهم بعضی قسمتها لازم است خواننده مقداری اطلاعات قبلی داشته باشد. مقالات این

جزوه، یک سیر منطقی را طی میکنند و میکوشند خواننده را قدم به قدم در مسیر به پیش برند. به همین جهت اکیداً توصیه میشود مطالب را به همان ترتیبی که آمده‌اند مطالعه کنید.

هدف از گردآوری مقالات آموزشی وب سایت نوفیلتر در قالب جزوه الکترونیکی (فایل PDF) این بود تا به راحتی در بین افراد و سایر وب سایتها منتشر شود و به این ترتیب امکان فیلتر کردن آن برای حکومت ایران از بین برود. با این حال این جزوه حاوی تمام مقالات نیست و سایت نوفیلتر علاوه بر مقالاتی که در این جزوه آمده دارای مطالب خواندنی دیگری نیز میباشد. همچنین مطالب جدید ابتدا در وب سایت منتشر میشوند و سپس طبق فواصل زمانی معینی به جزوه الکترونیکی افزوده میشوند. کلیه دوستانی که مایل هستند میتوانند این جزوه را در سایتهای شخصی خود قرار دهند. خواهش ما از این عزیزان این است که رسم امانت داری را حفظ کنند و از تغییر در نام و محتوای فایل خودداری کنند.

وب سایت نوفیلتر علاوه بر قسمت آموزش، دارای انجمن تبادل نظر (Forum) نیز هست. انجمن سایت نوفیلتر به خوانندگان این امکان را میدهد تا در آنجا سؤالات و نظرات خود را در ارتباط با مقالات این سایت مطرح کنند و پاسخ مناسب را از مؤلفین یا سایر کاربران دریافت نمایند. همچنین انجمن سایت نوفیلتر، محیطی را فراهم می‌آورد تا کاربران بتوانند تجربیات و دانسته‌های خود را در زمینه فیلترینگ با یکدیگر به اشتراک بگذارند و به بحث و تبادل نظر بنشینند.

مطمئناً به زودی دسترسی به سایت ما توسط فیلترینگ جمهوری اسلامی مسدود خواهد شد. با این وجود ما تصمیم به تغییر آدرس سایت نداریم و وب سایت ما برای همیشه در آدرس No-filter.com باقی خواهد ماند. امیدواریم هنگامی که شما با کمک آموزشهای این سایت توانستید خود را از چنگال سانسور خلاص کنید، اول از همه به سراغ ما بیایید و در قسمت انجمن سایت، نظرات و احساسات خود را با ما و دیگر خوانندگان در میان بگذارید.

تنها قسمتی از سایت که ممکن است تغییر آدرس دهد، پروکسی سایت است. چنانچه این قسمت توسط مخابرات شناسایی و مسدود شد، ما آدرس جدید را از طریق ایمیل به اطلاع اعضا خواهیم رساند. با وجودی که ما از یکی از معتبرترین شرکتها، خدمات میزبانی وب دریافت میکنیم و پهنای باند بسیار بالایی داریم ولی به علت احتمال فیلتر شدن نمیتوانیم آدرس پروکسی را در اختیار عموم قرار دهیم. چنانچه شما مایل به استفاده از پروکسی و سایر امکانات سایت نوفیلتر هستید میتوانید به عضویت سایت درآیید. برای اطلاعات بیشتر به قسمت دعوت به همکاری سایت نوفیلتر مراجعه فرمایید.

تاریخچه و اهداف سایت

هسته اولیه وب سایت نوفیلتر توسط تعدادی از دوستان نزدیک و با هدف مبارزه با سانسور شکل گرفت. این عده در اوقات فراقتشان بر روی مطالب این سایت کار کردند و بعد از یک ماه توانستند حدود ۲۰ مقاله در زمینه فیلترینگ و

روشهای مقابله با آن تهیه کنند. با وجودی که کارهای زیادی باقی مانده بود و هنوز مطالب زیاد دیگری باید تألیف می‌شد ولی به هر حال تصمیم گرفته شد با همین تعداد مطلب، کار شروع شود و باقی مقالات به تدریج به سایت اضافه شوند. به این ترتیب وب سایت نوفیلتر در مرداد ماه ۱۳۸۵ متولد شد و از طریق آدرس No-filter.com در شبکه جهانی اینترنت در دسترس علاقمندان قرار گرفت.

اگر چه هسته اولیه وب سایت نوفیلتر توسط تعدادی از دوستان نزدیک شکل گرفته ولی سیاست کاری ما بر اساس مشارکت جمعی است. بر همین اساس، ما از تمام کسانی که با اهداف و اعتقادات ما موافقند دعوت میکنیم تا به جمع ما بپیوندند و ما را در این راه یاری کنند.

اهداف و اعتقادات ما

- مهمترین هدف ما از احداث این وب سایت، کمک به هموطنانی است که مایلند از اینترنت به نحو شایسته‌ای استفاده کنند ولی به علت سد فیلترینگ، جلوی دسترسی آنها به بسیاری از منابع علمی، فرهنگی و سیاسی گرفته شده است. ما به این نکته یقین داریم که قربانیان اصلی فیلترینگ، این دسته از کاربران هستند وگرنه کسانی به دنبال سایتهای مبتذل می‌باشند به علت تعداد زیاد این گونه سایتها و یکسان بودن محتوای آنها کمتر با مشکل مواجه میشوند.
- ما به هیچ عنوان از هرزگی و ابتذال حمایت نمیکنیم و از کلیه دوستان، خصوصاً دوستان جوانمان استدعا داریم به ندای وجدان خود احترام بگذارند و هرگز سعی نکنند از سد فیلترینگ عقل سلیم و شعور انسانی خود فرار کنند؛ زیرا هرزگی و ابتذال برایشان هیچ چیز به جز تباهی عمر به ارمغان نخواهد آورد.
- ما معتقد به اصل آزادی بیان و تبادل آزاد افکار و اندیشه‌ها هستیم. زیرا ایمان داریم خداوند انسان را آزاد آفریده و نعمت عقل و شعور را در او به ودیعه نهاده تا خیر و شر خود را تشخیص دهد. هیچ شخص، در هیچ مقام و منصبی و با هیچ دین و مذهبی حق ندارد این عطیه الهی را از انسان بگیرد. باید به انسانها اجازه داده شود تا افکار و اندیشه‌های خود را آزادانه بیان کنند و تصمیم گیری در مورد درست یا نادرست بودن این اندیشه‌ها را باید به مخاطبان آن سپرد. تنها در سایه این تبادل اندیشه‌هاست که جامعه به رشد و بلوغ سیاسی و اجتماعی خواهد رسید.
- ما رفتارهای قیم مأبانه را توهینی به انسانها تلقی کرده و به شدت با آن مخالفیم. این که عده‌ای کوته فکر خود را عقل کل تصور کنند و به خویشتن اجازه دهند تا با عموم جامعه تحت سلطه‌شان همانند کودکی رفتار کنند که خیر و صلاح خود را نمیفهمد، برای ما با هیچ عقل و منطقی قابل توجیه نیست.
- ما به عنوان ایرانی به فرهنگ و زبان فارسی عشق می‌ورزیم و عقیده داریم همانطور که نیاکان ما در طول هزاران سال این زبان را به رشد و بالندگی رساندند، ما نیز موظف به حفظ و گسترش آن هستیم. در شرایط کنونی که

همه کشورها سعی در گسترش زبان و فرهنگ ملی خود در اینترنت دارند، فیلترینگ کورکورانه و بدون منطق سایتهای فارسی زبان بزرگترین خیانت به فرهنگ و زبان فارسی است.

- ما در اینجا هیچ خط و مشی سیاسی را طی نمیکنیم و به هیچ گروه سیاسی یا کشور خارجی وابستگی نداریم. هزینه راه‌اندازی وب سایت نوفیلتر از بودجه شخصی مؤسسین و هزینه نگهداری آن از محل تبلیغات تأمین میشود. هدف ما در اینجا صرفاً کار فرهنگی است؛ زیرا به این سخن از بزرگ مرد تاریخ بشریت، علی علیه‌السلام، ایمان داریم که "هر ملتی شایستگی حاکمانی را دارد که بر او حکومت میکنند" و یقین داریم هنگامی که ملت ما از لحاظ فرهنگی به رشد و کمال بالاتری دست پیدا کند خواه نا خواه حاکمان لایق‌تری نیز پیدا خواهد کرد. ولی تا آن زمان هرگونه توسل به زور در جهت براندازی حکومت، تنها منجر به پیدایش یک انقلاب نافرجام دیگر خواهد شد.

تماس با ما

دوستانی که مایلند با ما در ارتباط باشند میتوانند این کار را از طریق انجمن سایت نوفیلتر انجام دهند. انجمن سایت به ما این امکان را میدهد تا با کلیه خوانندگان خود یک ارتباط چند جانبه برقرار کنیم و بتوانیم به سؤالات و پرسشهای آنها پاسخ دهیم. همچنین در این قسمت شما میتوانید پیشنهادها و انتقادات خود را مطرح کنید. چنانچه دسترسی شما به قسمت انجمن سایت مسدود شده یا اینکه به دلایلی نمی‌خواهید مطالب خود را در یک انجمن عمومی مطرح کنید، میتوانید از طریق ایمیل با ما تماس بگیرید.

برای آگاهی از نظرات خوانندگان و استفاده از آن در جهت ارتقا سطح کیفی مطالب، یک فرم نظرسنجی به انتهای این جزوه ضمیمه شده است. از کلیه خوانندگان عزیز خواهشمندیم پس از این که مطالب جزوه را کاملاً مطالعه کردند، این فرم را تکمیل و برای ما ارسال کنند.

انجمن نوفیلتر

forum.No-filter.com

ایمیل

pdf@no-filter.com

نظرسنجی

Survey form

آشنایی با فیلترینگ

علل و زمینه‌های پیدایش فیلترینگ

گسترش اینترنت زمینه‌ای را پدید آورد که طیف وسیعی از اطلاعات بتوانند بدون هیچ گونه محدودیتی در سراسر جهان منتشر شود. از طرف دیگر طیف مخاطبان اینترنت هم به همان اندازه محتویات آن وسیع و مختلف بود. دسترسی بی حد و حصر به اطلاعات و این حقیقت که هر کسی به هر گونه اطلاعاتی دسترسی داشته باشد بسیاری را به هراس انداخت و انتقادات شدیدی را به همراه آورد. گروهی از منتقدان کسانی بودند که به محتویات غیر اخلاقی اینترنت اعتراض داشتند و آن را خصوصاً برای جوانان و نوجوانان مضر و منحرف کننده میدانستند. گروه دیگر حکومتهایی بودند که تاب سخن مخالفان را نمی‌آوردند. این حکومتها سالها بود که با بسته و محدود نگه داشتن جامعه تحت سلطه‌شان و اِعمال سانسور بر رسانه‌های سنتی نظیر مطبوعات و روزنامه‌ها سعی داشتند تفکر و ایدئولوژی خود را بر مردمانشان تحمیل کنند و به همین منظور با هرگونه تجدد و دگر اندیشی که مخالف با امیال آنها بود به شدت برخورد میکردند. تعجب ندارد که این قبیل حکومتها اینترنت و انتشار خارج از کنترل اطلاعات را تهدیدی جدی برای موجودیت خود تلقی کنند و با آن به مبارزه برخیزند. از آنجایی که اکثر این حکومتها سعی داشتند برخلاف ماهیت ذاتیشان از خود وجهه‌ای دمکرات و آزادی خواه به نمایش بگذارند، نمی‌توانستند دلیل اصلی مخالفت خود را با تبادل آزاد اطلاعات ابراز کنند. این بود که آنها نیز به گروه قبلی پیوستند و لوای مبارزه با فساد و مطالب غیر اخلاقی را سر دادند.

به هر حال برای هیچ یک از دو گروه از اینترنت گریزی نبود. در واقع دستاوردهای علمی و فرهنگی اینترنت آنقدر شگرف بود که چشم پوشی از آن به راحتی میسر نمی‌شد. از آنجایی که اینترنت شبکه‌ای جهانی بود و بر اساس ساختار آن، هیچ گروه یا دولتی نمی‌توانست بر مطالبی که در آن انتشار میابد نظارت کامل داشته باشد، کم‌کم این ایده شکل گرفت تا به جای کنترل انتشار مطالب، بر دسترسی و استفاده افراد از اینترنت نظارت شود.

از اینجا بود که واژه "فیلترینگ" وارد فرهنگ اینترنت شد. فیلترینگ در لغت به معنای پالایش و زدودن ناپاکیهاست و در فرهنگ اینترنت به معنی جلوگیری از دسترسی کاربران به سایتهایی است که حاوی مطالب ناشایست هستند که البته تعریف خود کلمه ناشایست مورد اختلاف نظر شدید میباشد.

برعکس آنچه ابتدا تصور می‌شد، فیلترینگ در زمینه مبارزه با فساد و مطالب غیر اخلاقی چندان موفق عمل نکرد و نه تنها نتوانست کاملاً جلوی انتشار این قبیل مطالب را در اینترنت بگیرد بلکه با خود مشکلات غیر منتظره‌ای را به همراه آورد که زمینه‌ساز انتقادات و حتی مخالفتهای شدیدی گشت.

مهمترین نقطه ضعف سیستمهای فیلترینگ این بود که از طریق نرم‌افزارهای کامپیوتری به اجرا گذاشته می‌شد. جای تعجبی ندارد که این سیستمها به علت ماهیت ماشینی‌شان هیچ درک و فهمی از نوشته‌ها و مطالب انسانی نداشته باشند و کورکورانه عمل کنند. مثلاً در بعضی وب سایتها، خصوصاً سایتهایی که خدمات وبلاگ نویسی ارائه میدهند، ممکن است صدها و شاید هزاران مطلب وجود داشته باشد که تنها درصد کمی از آنها دربردارنده نکات غیر اخلاقی باشد. از آنجایی که سیستمهای فیلترینگ قادر به افتراق این موارد نیستند، دسترسی به کل سایت را مسدود میکنند و به این ترتیب باعث غیر قابل استفاده شدن حجم عظیمی از اطلاعات و مطالب ارزشمند میشوند.

مشکل بعدی فیلترینگ به این موضوع برمی‌گشت که کاربران اینترنت را طیف وسیعی از افراد تشکیل میدادند. از کودک ۷ ساله گرفته تا پیرمرد ۷۰ ساله و از یک فرد کم سواد گرفته تا یک استاد مجرب دانشگاه و همچنین افرادی با جنسیت مختلف، مذاهب گوناگون و سطوح فکری متفاوت. واضح است که افراد مختلف، نیازهای متفاوت داشته باشند و چه بسا مطالبی که برای یک عده مضر و گمراه کننده محسوب میشود برای عده‌ای دیگر مفید و حتی ضروری باشد. ولی سیستمهای فیلترینگ این قابلیت را نداشتند که این تفاوتها را متوجه شوند و به همین سبب، همه را به یک شکل تحت سانسور قرار میدادند.

معمولاً، سایتهایی غیر اخلاقی در نظر گرفته میشوند که حول و حوش مسائل جنسی و ابتذال دور میزنند. از آنجایی که محتویات این سایتها کم و بیش مشابه است، امکان فیلتر کردن کامل آنها وجود ندارد. زیرا هر روزه صدها عدد از این سایتها تأسیس میشوند و عملاً این امکان برای فیلتر کنندگان وجود ندارد تا همه آنها را شناسایی و مسدود کنند. در سخت‌ترین سیستمهای فیلترینگ، حتی یک کاربر کم تجربه به کمک موتورهای جستجو میتواند در کمتر از ده دقیقه به یکی از این سایتها دسترسی پیدا کند. به همین جهت، متأسفانه اغلب قربانیان فیلترینگ، کاربرانی هستند که مایلند از اینترنت به نحو شایسته‌ای استفاده کنند.

با توجه به مطالب فوق به نظر میرسد فیلترینگ بیش از آن که توانسته باشد اینترنت را از ناپاکیها پاک کند، وسیله‌ای شده است برای اعمال سلیقه در دست حکومتهای خودکامه. این موضوع را با توجه به گسترش جغرافیایی فیلترینگ، بهتر میتوان متوجه شد. چنانکه واضح است فیلترینگ در کشورهای عقب افتاده‌ای به اجرا گذاشته شده که کارنامه‌ای سیاه در حقوق بشر دارند و تقریباً هیچ کشور پیشرفته و آزادی را نمیتوان پیدا کرد که عموم شهروندان خود را از دسترسی آزاد به اطلاعات محروم کرده باشد. البته لازم به توضیح است که در کشورهای غربی نیز فیلترینگ تا حدودی مورد توافق قرار دارد ولی حوزه آن به شدت محدود و مربوط به سایتهایی میشود که اقدام به پخش تصاویر مستهجن و مطالب غیر اخلاقی میکنند. در این کشورها دولت به هیچ وجه وارد وادی فیلترینگ نشده و این کار صرفاً توسط برخی

سرویس دهندگان اینترنت (ISP) انجام میگیرد. والدینی که نگران سلامت کودکان و نوجوانان خود هستند از این گونه ISPها اشتراک اینترنت تهیه میکنند.

در کشورهایی که فیلترینگ اجرا میشود دیر یا زود هر کاربر اینترنتی این مسئله را تجربه میکند که سایت مورد نیازش به غلط فیلتر شده است. از آنجایی که در اکثر این کشورها هیچ مقام و مرجعی برای اعتراض وجود ندارد، برای کاربر دو راه بیشتر باقی نمی‌ماند. یا تسلیم شود و اجازه دهد حاکمانش در مورد خیر و صلاح او تصمیم بگیرند یا این که بر خواسته خود پا فشاری کند و سعی کند خود را از چنگال دیکتاتوری و سانسور بیرون بکشد.

فطرت انسان به گونه‌ای است که از هر نوع محدودیت و سلطه‌ای میگریزد، حتی اگر آن محدودیت از روی خیرخواهی وضع شده باشد. از این رو بسیاری از کاربران در مواجهه با سانسور راه دوم را در پیش گرفتند و سعی کردند به هر نحو ممکن، آزادی از دست رفته خویش را باز پس‌گیرند. به این ترتیب بود که به موازات شکل گیری و گسترش فیلترینگ، فرهنگ مبارزه با فیلترینگ نیز شکل گرفت.

خوشبختانه طراحی اولیه اینترنت در کشورهایی انجام گرفته که در آنها تفکر ارتجاعی و قیم مأبانه جایی ندارد. در این کشورها انسان به عنوان موجودی صاحب عقل و خرد در نظر گرفته میشود که قادر است خیر و شر خود را تشخیص دهد. بر همین اساس، ساختار اینترنت بر پایه تبادل آزاد و بدون نظارت اطلاعات طراحی شده است و در واقع سیستمهای فیلترینگ اجزا تحمیل شده به اینترنت هستند که با دیگر ساختارهای آن تطابق کامل ندارند. این ناسازگاری، راههای فرار متعددی را بوجود آورده که کاربران میتوانند از آنها برای دور زدن و عبور از سد فیلترینگ بهره بگیرند.

ولی به هرحال باید توجه داشت که فیلترینگ و مبارزه با فیلترینگ یک جدال تمام نشدنی است. در یک سوی میدان حاکمان و صاحبان فیلترینگ قرار دارند که سعی میکنند با بهره‌گیری از تکنولوژیهای جدید، هرچه بیشتر راههای فرار را بر کاربران ببندند و حلقه سلطه را بر مردمان خود تنگ‌تر کنند و در سوی دیگر میدان، کاربرانی وجود دارند که تلاش میکنند با شناسایی و بهره‌گیری از نقاط ضعف سیستم، آزادی از دست رفته‌شان را باز پس‌گیرند.

چیزی که مسلم است این است که هیچ یک از طرفین به عنوان برنده مطلق از میدان بیرون نخواهد آمد و هر عملی با عکس‌العمل طرف مقابل پاسخ داده خواهد شد. لذا بهتر است بجای عبارت "مبارزه با فیلترینگ" از عبارت "مقابله با فیلترینگ" استفاده شود. زیرا این یک جنگ مجازی و در دنیایی مجازیست و کسانی که حقیقتاً میخواهند با فیلترینگ و سانسور مبارزه کنند باید با ریشه‌های آن که نشأت گرفته از کوته فکری و استبداد است در دنیای واقعی به مبارزه برخیزند.

فیلترینگ در ایران

هنوز بیش از یک دهه از ورود اینترنت به ایران نمی‌گذرد. اگر چه کاربران ایرانی در سالهای اولیه ورود این تکنولوژی به کشورشان خاطره‌ای خوب و به دور از سانسور را تجربه کردند ولی دیری نپایید که کشورشان به یکی از بزرگترین سانسور کنندگان اینترنت تبدیل شد. امروزه ایران به همراه چین از بزرگترین سانسور کنندگان اینترنت به شمار میرود و این در حالی است که رشد اینترنت در ایران بسیار چشمگیر است و از یک میلیون کاربر در سال ۲۰۰۱ به پنج میلیون در سال ۲۰۰۵ رسیده است و بنابر پیش‌بینی شرکت مخابرات تا سال ۲۰۰۹ این تعداد به بیست و پنج میلیون نفر خواهد رسید.

در حال حاضر در ایران ۶۵۰ سرویس دهنده اینترنت (ISP) و ۱۸ شرکت ICP وجود دارند. شرکت ارتباطات دیتا، وابسته به شرکت مخابرات ایران، بزرگترین سرویس دهنده اینترنت در کشور است و اغلب ISPها از او سرویس میگیرند.

مطابق آنچه در "مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای" آمده است، کلیه ایجاد کنندگان نقطه تماس بین‌الملل از جمله شرکت مخابرات موظفند سیستم فیلترینگ داشته باشند تا از دسترسی کاربران به سایتهای غیرمجاز ممانعت شود.

ضوابط و مصادیق موارد فیلتر توسط شورای عالی اطلاع رسانی تصویب و اعلام میشود. هم اکنون یک کمیته سه نفره متشکل از نمایندگان صداوسیما، وزارت ارشاد و وزارت اطلاعات از سوی شورای عالی انقلاب فرهنگی مأمور نظارت بر فعالیتهای اینترنتی است. این گروه با تهیه فهرست سایتهایی که باید مسدود شوند، تنها مرجع رسمی مسئول در این زمینه است. با این حال بارها دیده شده که قوه قضائیه راساً در امر فیلترینگ دخالت کرده و مستقیماً دستور مسدود سازی سایتهای اینترنتی را به مخابرات ابلاغ نموده است.

سانسور اینترنت در ایران به شیوه‌های مختلف و در سطوح مختلف انجام میگیرد. برای آن دسته از سایتهایی که سرویس‌دهنده (Server) و گردانندگان آن در ایران هستند برخورد به صورت قوه قهریه و سیستم قضائی است ولی برای آن دسته از سایتهایی که مرکز کنترل آنها در خارج از حیطه اقتدار جمهوری اسلامی قرار دارد، برخورد به صورت مسدود سازی دسترسی کاربران ایرانی به سایت مورد نظر می‌باشد.

بر اساس یکی از جدیدترین و معدود تحقیقات میدانی انجام شده توسط مؤسسه اپن‌نت (OpenNet) که سعی دارد وضعیت فیلترینگ را در کشورهای مختلف دنیا بررسی کند، حدود ۳۰ درصد از سایتهای مورد بررسی این مؤسسه در ایران مسدود بودند (۴۹۹ سایت از ۱۴۷۷). نتایج تحقیقات این مؤسسه که در یک گزارش ۲۹ صفحه‌ای منتشر شده است نشان میدهد که ایران یکی از سخت‌ترین و شدیدترین سیستمهای فیلترینگ را به اجرا گذاشته است. خلاصه‌ای از نتایج این تحقیق ذیلاً آمده است:

- **در حال حاضر فیلترینگ در ایران بر روی موضوعات مربوط به ایران، به ویژه سایتهای فارسی زبان تمرکز کرده است. سایتهای غیر مرتبط با مسائل داخلی ایران و نیز سایتهای غیر فارسی بسیار کمتر در معرض خطر فیلتر شدن قرار دارند.**
- **فیلترینگ خصوصاً وبلاگهای شخصی و سایتهای ارائه دهنده خدمات وبلاگ نویسی را مورد هدف قرار داده است. در طول دوره تحقیق (سالهای ۲۰۰۴ تا ۲۰۰۵) فیلتر کردن وبلاگها به طور فزاینده‌ای افزایش نشان میداد. با این که برای فیلتر کنندگان ساده تر است کل سایت ارائه دهنده خدمات وبلاگ نویسی را بلوک کنند ولی ایران در اکثر موارد به جای این کار، اقدام به مسدود کردن جداگانه وبلاگها نموده است. به نظر میرسد هدف ایران از این کار این باشد که میخواهد دسترسی به بعضی وبلاگها حفظ شود در حالیکه وبلاگهای مخالفان مسدود شده باشد.**
- **یکی دیگر از حوزه‌های تمرکز فیلترینگ سایتهای خبری است. آمار نشان میدهد در حالیکه تنها ۵ درصد سایتهای خبری انگلیسی فیلتر شده‌اند، این تعداد در مورد سایتهای خبری فارسی زبان به ۵۰ درصد میرسد.**
- **فیلترینگ در حوزه سایتهای سکس و فیلترشکن نیز به شدت فعال است. به طوری که ۱۰۰ درصد سایتهای سکس و ۹۵ درصد سایتهای فیلترشکن مورد مطالعه در این تحقیق مسدود بودند.**

General Category	Complete Blocks	Partial Blocks	Sites Tested	Total Block Percentage
Blogs	74	12	588	15%
International Organizations	0	0	17	0%
Lifestyles	2	2	15	27%
News	10	4	46	30%
Opposition & Dissent	15	10	62	40%
Political / Religious / Social	30	20	52	96%
Politics	28	22	51	98%
Proxy / Anonymizer Services	17	3	26	77%
Religion	3	1	24	17%
Sex	219	31	251	100%

جدول ۱- این جدول درصد مسدود سازی سایتهای مختلف اینترنتی را بر حسب محتوای آنها نشان میدهد. بیشترین میزان مسدود سازی مربوط به سایتهای سکس و کمترین مقدار مربوط به سایتهای سازمانهای بین‌المللی می‌باشد.

- **این تحقیق در آخر پیش‌بینی میکند علاوه بر این که فیلترینگ از لحاظ کمی در ایران گسترش پیدا میکند، از نظر کیفی نیز شیوه‌های فیلترینگ به تدریج دقیق‌تر و پیچیده‌تر خواهند شد.**

همانطور که پیشتر گفته شد اغلب ISPهای ایران از شرکت مخابرات سرویس میگیرند. این دسته از ISPها عمدتاً سیستم فیلترینگ مستقل ندارند و از این لحاظ به مخابرات وابسته‌اند. آن دسته از ISPهایی که پهنای باند خود را از سرویس دهندگان بین‌المللی تهیه میکنند (مانند پارس آنلاین و چند ICP بزرگ دیگر در تهران) موظف به نصب سیستم فیلترینگ مستقل شده‌اند.

از نظر نرم‌افزاری، ایران برای اعمال سانسور از برنامه اسمارت فیلتر (Smart Filter) ساخت شرکت آمریکایی سکیور کامپیوتینگ (Secure Computing) استفاده میکند. این مطلب را نخستین بار رضا پارسا، رئیس اتحادیه ISPها، عنوان کرد و در توجیه آن افزود که اکثر سانسور افزارهای تولید داخل فاقد کیفیت مشابه‌های خارجی هستند.

استفاده ایران از نرم‌افزار اسمارت فیلتر در حالی صورت میگیرد که برای اینکار از شرکت سازنده هیچ گونه مجوزی اخذ نکرده است. این کار از لحاظ حقوق بین‌الملل سرقت محسوب شده و اگر روزگاری ایران بخواهد به سازمانهای بین‌المللی نظیر سازمان تجارت جهانی (WTO) بپیوندد باید بابت آن تاوان سنگینی را بپردازد.

چندی پیش بخش فارسی بی‌بی‌سی BBC با آقای دیوید بارت، مدیر روابط عمومی شرکت سکیور کامپیوتینگ، مصاحبه‌ای انجام داده بود. وی در این مصاحبه ضمن تأکید بر این که شرکت متبوعش امتیاز نرم‌افزار خود را به هیچ شخص یا سازمانی در ایران واگذار نکرده، افزود بسیاری از شرکتهای ایرانی از نسخه آزمایشی (بتا) نرم‌افزار ما استفاده میکنند و شرکت سکیور کامپیوتینگ برای مقابله با این کار تمام IP آدرسهای ایران را بلوک کرده است به طوری که اکنون امکان دانلود و آپدیت این نرم‌افزار در ایران وجود ندارد.

از لحاظ تکنیکی، استفاده ایران از سانسورافزار اسمارت فیلتر محدود به صفحات وب است (پروتکل HTTP و پورت ۸۰). معمولاً سایر سرویسهای اینترنت نظیر ایمیل، اف تی پی و چت مورد سانسور قرار نمیگیرند. فیلترینگ در ایران بر اساس لیست سیاه انجام میشود که این لیست حاوی نام دامین و IP آدرس سایتهای مسدود شده می‌باشد. در حال حاضر از کلمات کلیدی برای سانسور استفاده نمی‌شود.

با وجودی که حکومت ایران به شدت اینترنت را مورد سانسور قرار داده و در این زمینه سرمایه گذاریهای کلانی کرده است ولی به نظر میرسد دولت جمهوری اسلامی موفقیتش در امر فیلترینگ را بیشتر از آن که مدیون سیستم پرهزینه فیلترینگ خود باشد، مدیون سطح پایین دانش IT در کاربران ایرانی است. چنانکه، کمتر کاربر با تجربه اینترنتی را در ایران میتوان پیدا کرد که مختصر اطلاعاتی راجع به ساختارهای شبکه و اینترنت داشته باشد ولی باز هم در پشت درهای فیلترینگ محصور مانده باشد. ضعف سیستم فیلترینگ ایران به دو علت برمیگردد:

۱. **اصول و طراحی اولیه اینترنت بر مبنای تبادل آزاد اطلاعات صورت گرفته است و سیستمهای فیلترینگ اجزایی هستند که بعداً به آن تحمیل شدند و به همین جهت با سایر ساختارهای اینترنت کاملاً همخوانی ندارند. این ناهمخوانی شکافها و سوراخهای زیادی را بوجود آورده که کاربران میتوانند از آنها برای فرار از فیلتر استفاده کنند. این مسئله نه تنها در مورد سیستم فیلترینگ ایران بلکه در مورد کلیه سیستمهای فیلترینگ صادق است.**

۲. **علت دوم به ضعف طراحی سیستم فیلترینگ ایران برمیگردد. همان طور که گفته شد هسته نرم‌افزاری سیستم فیلترینگ ایران را یک نرم‌افزار آمریکایی بنام اسمارت فیلتر تشکیل میدهد. این نرم‌افزار به پرخطا بودن (Erroneous) و بلوک بیش از حد (Overblocking) شهرت دارد. از طرف دیگر، از آنجایی که شرکت سازنده حاضر به فروش نرم‌افزارش به ایران نشده، ایران بطور غیر قانونی از نسخه آزمایشی این نرم‌افزار استفاده میکند و برای این که آن را با نیازهایش مطابق سازد ناچار شده تا در اصل برنامه تغییراتی بدهد و اصطلاحاً آن را بومی سازی کند. پروژه بومی سازی این نرم‌افزار زیر نظر وزارتخانه ارتباطات و فناوری اطلاعات انجام گرفته است. زیاد تعجب آور نیست که اگر این پروژه نیز مانند سایر پروژه‌های این وزارتخانه پر از ایراد و اشکال باشد.**

فیلترینگ معکوس

مشکلاتی که بر سر راه استفاده آزادانه مردم ایران از اینترنت وجود دارد شاید در نوع خود در تمامی جهان بی‌نظیر باشد. در حالی که حکومت ایران به همراه چین این افتخار را دارد که از بزرگترین سانسورگران اینترنت بشمار رود، ایالات متحده آمریکا نیز با وضع پاره‌ای قوانین، عرصه اینترنت را بر کاربران ایرانی تنگتر کرده است. بر اساس این قوانین، شرکتهای آمریکایی از ارائه خدمات به کشورهای ایران، کوبا، کره شمالی، سوریه و سودان فعالانه منع میشوند. اگرچه حوزه اصلی این تحریمها در ابتدا محدود به تراکنشهای مالی و پرداختهای اینترنتی بود ولی متأسفانه دیده میشود که این حوزه در حال گسترش است و امروزه حتی بعضی از شرکتها از دانلود نرم‌افزارهایشان توسط کاربران ایرانی جلوگیری میکنند.

این نوع از فیلترینگ نه در مبدأ بلکه در مقصد انجام میشود و سرور شرکت ارائه دهنده خدمات، قبل از ارائه هرگونه سرویسی، ابتدا IP آدرس مشتری را چک میکند و در صورتی که متعلق به یک کشور تحریم شده باشد از ارائه سرویس سرباز میزند. این نوع خاص از فیلترینگ را اصطلاحاً فیلترینگ معکوس (Reverse Filtering) میگویند.

در حال حاضر اغلب شرکتهای آمریکایی از قبول پرداختهای اینترنتی از داخل ایران امتناع میکنند و با این کار خرید اینترنتی را برای کاربران ایرانی بسیار سخت کرده‌اند. حتی اگر برای پرداخت، از کارتهای اعتباری بین‌المللی و یا آمریکایی هم استفاده شود، باز هم به دلیل اینکه تراکنش از داخل کشور ایران صورت گرفته مورد قبول قرار نمیگیرد. در مورد پرداختهای اینترنتی نحوه عملکرد این شرکتها به یکی از سه شکل زیر است:

1. **تعدادی از این شرکتها جلوی دسترسی کاربران ایرانی به وب سایتشان را به طور کامل گرفته‌اند. هنگامی که شخصی بخواهد از داخل ایران به وب سایت آنها دسترسی پیدا کند با خطاهایی مانند:** Forbidden، Time out **و غیره مواجه میشود. شرکتهای** Godaddy **و** Escrow **در این دسته جای دارند.**

2. **بعضی از شرکتها مثل پی‌پال** PayPal **به کاربر اجازه میدهند تا از وب سایتشان بازدید کند ولی هنگامی که کاربر بخواهد یک تراکنش مالی انجام دهد با یک پیام اخطار مبنی بر این که وی در یک کشور تحریم شده** (Sanctioned Country) **قرار دارد مواجه میشود. اخیراً جمهوری اسلامی سایت پی‌پال را فیلتر کرده است.**

3. **تعدادی از شرکتها مانند** 2CO **به کلیه کاربران اجازه دسترسی کامل به وب سایتشان را میدهند و در ابتدا خرید را از همه قبول میکنند ولی بعد از چند روز (معمولاً کمتر از ۳ روز) با عنوان این که پرداخت از داخل یک کشور تحریم شده صورت گرفته، معامله را لغو میکنند. لازم به توضیح است که در پرداختهای آنلاین، به طور معمول، یک فاصله زمانی حدوداً ۷۲ ساعته وجود دارد که طی آن شرکت فروشنده، صحت اطلاعات مشتری را مورد بررسی قرار میدهد و در خلال این مدت پولی از حساب مشتری کسر نمیشود.**

با توجه به اینکه هنوز خرید اینترنتی در ایران جا نیفتاده و اکثر مردم ایران از داشتن کارتهای اعتباری بین‌المللی محرومند، به نظر نمیرسد تحریمهای مالی آمریکا مشکل جدی را برای کاربران ایرانی بوجود آورده باشد. با این حال آنچه بیشتر باعث نگرانی است، این است که امروزه محدوده این تحریمها از حوزه مسائل مالی فراتر رفته و به دانلود نرم‌افزار و خدمات رایگان اینترنت کشیده شده است. شرکتهایی مانند سان ماکروسیستمز و مک‌آفی از دانلود و به روز رسانی نرم‌افزارهایشان توسط کاربران ایرانی جلوگیری میکنند. حتی شرکت گوگل نیز جلوی دانلود بسته نرم‌افزاری این شرکت موسوم به گوگل‌پک (Google Pack**) را از داخل ایران گرفته است.**

مبانی فیلترینگ در اینترنت

قبل از این که شما بخواهید سد سانسور را بشکنید و از فیلتر عبور کنید ابتدا لازم است اطلاعاتی راجع به سیستمهای فیلتر کننده محتوا (Content Filter) و شیوه کار آنها داشته باشید. همانطور که میدانید اینترنت شبکه‌ای است که از هزاران شبکه کوچکتر و میلیونها کامپیوتر که اطلاعاتشان را به اشتراک گذاشته‌اند شکل گرفته است. هنگامی که شما قصد دیدن یک صفحه وب را میکنید کامپیوتر شما درخواستی را به کامپیوتر میزبان میفرستد که این درخواست در طی مسیرش از دهها و شاید صدها کامپیوتر دیگر باید عبور کند. ISP و شبکه مخابراتی محلی شما در ابتدای این مسیر قرار گرفته‌اند. حال با فرض این که شبکه محلی شما مجهز به سیستم فیلترینگ باشد، ترتیب کار میتواند به صورت زیر پیش رود:

1. **کامپیوتر شما یک صفحه وب را درخواست میکند.**
2. **این درخواست در ابتدا به ISP و از آنجا به شبکه محلی شما فرستاده میشود.**
3. **قبل از اینکه درخواست از شبکه محلی به سروری که صفحه وب مورد نظرتان بر روی آن قرار گرفته ارسال شود، توسط سیستم فیلتر کننده بررسی میگردد.**
4. **در اینجا یکی از دو حالت زیر پیش می‌آید:**
   A. **سیستم فیلتر کننده درخواست شما را مجاز تشخیص داده و به آن اجازه عبور میدهد. در این حالت درخواست شما به سروری که صفحه مورد نظرتان بر روی آن قرار دارد میرسد و متعاقباً صفحه مربوطه برایتان ارسال میگردد.**
   B. **سیستم فیلتر کننده درخواست شما را غیرمجاز میداند و آن را بلوک میکند. در این حالت از ارسال آن به سرور مربوطه خودداری شده و در عوض یک پیام اخطار برایتان ارسال خواهد شد.**

از لحاظ فنی ممکن است سیستم فیلتر کننده بر روی ISP قرار گرفته باشد ولی این مسئله تأثیری در نتیجه کار ندارد. مراحل فوق عیناً به همان صورت تکرار میشود با این تفاوت که این بار درخواستها در یک سطح پایین‌تر، یعنی در ISP، مورد بررسی قرار میگیرند.

تا اینجا متوجه شدید که تمامی درخواستها ابتدا باید از یک سیستم فیلتر کننده عبور کنند. این سیستم درخواستها را با لیستی که دارد مقایسه کرده و بعد تصمیم میگیرد که به آنها اجازه عبور بدهد یا نه! اصطلاحاً به این لیست، لیست سیاه (Black List) گفته میشود. لیست سیاه از ۳ جزء تشکیل شده است:

1. **آدرس دامین (Domain Address): این در واقع نام همان وب سایتی است که قصد دسترسی به آن را دارید. مثلاً:** www.google.com .
2. **IP آدرس: این آدرس تماماً به صورت عددی است. IP آدرس شبیه شماره تلفن است و هر کامپیوتری که به اینترنت متصل است یک IP آدرس مخصوص به خود دارد. در واقع، تمام دامین آدرسها همیشه و به دور از**

چشم کاربر به IP آدرس متناظر خود تبدیل میشوند. مثلاً در مثال بالا google.com به IP آدرس متناظرش یعنی 66.249.93.104 تبدیل میشود.

۳. کلمات کلیدی (Keywords): اینها کلمات و عباراتی هستند که اگر در درخواست وجود داشته باشند باعث عکس‌العمل کامپیوتر فیلتر کننده و بلوک شدن درخواست میشوند.

هنگامی که درخواست شما به سیستم فیلتر کننده رسید، سیستم آن را با دامین آدرسها و IP آدرسهای موجود در لیست سیاهش مقایسه میکند. بعضی سیستمهای فیلترینگ پا را از این فرا گذاشته و درخواست را از نظر کلمات کلیدی نیز مورد بررسی قرار میدهند. حال اگر هیچ یک از کلمات و آدرسهای موجود در لیست سیاه در درخواست شما وجود نداشته باشد، درخواست اصطلاحاً تمیز (Clean) در نظر گرفته شده و به آن اجازه عبور داده میشود. در این حالت درخواست شما به سرور مربوطه رسیده و فایل یا صفحه مورد نظرتان برای شما ارسال میشود. ولی چنانچه یکی از موارد موجود در لیست سیاه در درخواست شما پیدا شود، درخواست آلوده (Dirty) تشخیص داده شده و بلوک میشود و در عوض برایتان یک پیام اخطار مانند "دسترسی به سایت مورد نظر امکان پذیر نمی‌باشد" فرستاده میشود.

بیایید مطلب را با ذکر ۲ مثال بیشتر توضیح دهیم. یکی برای یک درخواست تمیز و دیگری برای یک درخواست آلوده: فرض کنید در کادر آدرس مرورگر خود www.google.com را وارد کرده‌اید . این درخواست شما قبل از اینکه وارد دنیای اینترنت شود و به سایت گوگل برسد، باید از شبکه محلیتان و بالنتیجه از سیستم فیلترینگ آن عبور کند. در سیستم فیلتر کننده درخواست شما مورد بازبینی قرار میگیرد. ابتدا دامین آدرس google.com و IP آدرس متناظرش یعنی 66.249.93.104 با لیست سیاه مقایسه میشوند. سپس درخواست از لحاظ کلمات غیرمجاز چک میشود. در این مورد چون کامپیوتر فیلتر کننده هیچ مورد تشابهی بین درخواست شما با لیست سیاهش پیدا نمیکند، درخواست را تمیز در نظر گرفته و به آن اجازه عبور میدهد. درخواست شما به سایت گوگل میرسد و متعاقباً صفحه خانگی گوگل برایتان ارسال میگردد.

حال فرض کنید شما یک سایت غیر مجاز را درخواست کرده‌اید، مثلاً www.sex.com . این سایتی است که به خاطر مطالب غیر اخلاقیش تقریباً در تمامی سیستمهای فیلترینگ مسدود شده است. هنگامی که درخواست شما به کامپیوتر فیلتر کننده برسد، از لحاظ دامین آدرس sex.com و IP آدرس 216.130.216.214 با لیست سیاه مقایسه میشود و چون این آدرسها در لیست سیاه وجود دارند درخواست بلوک شده و اجازه عبور نمی‌یابد و بجای صفحه مورد تقاضا، یک پیام اخطار از طرف سیستم فیلتر کننده برای شما فرستاده میشود.

تا اینجا شما با اساس کار سیستمهای فیلتر کننده محتوا در اینترنت آشنا شدید ولی لازم است قبل از پایان دادن به این مبحث یک نکته دیگر را نیز فرا بگیرید. اصولاً انجام عمل فیلترینگ در یک شبکه، کاری بسیار پرهزینه است، علی‌الخصوص در شبکه‌های بزرگ و کشوری، و نیاز به تجهیزات گرانقیمت و نیروی انسانی زبده دارد چرا که هر روزه هزاران سایت تأسیس و صدها سایت تعطیل میشوند و میلیاردها مگابایت اطلاعات رد و بدل میگردد. نظارت بر همه اینها

بسیار پرهزینه است و ضمناً میتواند بازده شبکه را نیز به طرز محسوسی کاهش دهد. از این رو مدیران شبکه همواره سعی میکنند تا فیلترینگ تنها بر قسمتهای ضروری و حساس اعمال شود. بر همین اساس غالباً ترافیک خروجی شبکه مورد کنترل قرار میگیرد و به جز در موارد خاص بر ترافیک ورودی نظارت نمیشود. این مطلب کاملاً قابل درک است چرا که یک درخواست چند بایتی میتواند یک صفحه یا فایل چند مگابایتی را به همراه داشته باشد و چنانچه بخواهد بر روی ترافیک ورودی هم نظارت صورت گیرد بار بسیار سنگینی بر کامپیوتر فیلتر کننده وارد میشود و اصطلاحاً در شبکه یک گلوگاه بوجود می‌آید.

از طرف دیگر، همان طور که میدانید سرویسهای مختلفی از طریق اینترنت عرضه میشود، مثل سرویس وب، ایمیل، اف‌تی‌پی (FTP)، چت و غیره. به دلیل حساسیت، این سرویس وب (پروتکل HTTP) است که در اکثر موارد مورد سانسور قرار میگیرد و تقریباً سایر سرویسها (مانند ایمیل و FTP) کم و بیش از سانسور در امان هستند.

انواع فیلترینگ

از لحاظ تکنیکی روشهای مختلفی برای انجام فیلترینگ وجود دارد که بر حسب شرایط و نیازها از یکی از آنها استفاده میشود. شناخت این روشها از آن جهت ضروری است که برای مقابله با هر کدام باید از راهکارهای متفاوتی استفاده شود. در اینجا به مهمترین شیوه‌های رایج برای فیلترینگ اشاره میشود:

فیلترینگ از طریق DNS:

این یک روش ساده و کم خرج فیلترینگ است ولی به همان اندازه عبور از آن نیز ساده و آسان است. قبل از بحث درباره این روش لازم است توضیح مختصری در مورد DNS بدهیم. DNS مخفف کلمات سرویس نام دامنه (Domain Name Service) می‌باشد. همان طور که میدانید سیستم آدرس‌دهی در اینترنت بر اساس IP آدرس است و هر کامپیوتری که به اینترنت متصل است یک IP آدرس مختص به خود دارد. IP آدرس به شماره تلفن شباهت دارد و از چهار عدد مختلف که توسط نقطه از هم جدا شده‌اند تشکیل شده است، به طوری که هر یک از این اعداد میتوانند مقداری بین ۰ تا ۲۵۵ داشته باشند. مثلاً IP آدرس سایت گوگل 66.249.93.104 است.

از آنجایی که به خاطر سپردن چنین اعدادی برای انسان مشکل است، دامین آدرسها بوجود آمدند. دامین آدرسها به جای اعداد و ارقام از حروف و کلمات تشکیل شده‌اند و به همین جهت به خاطر سپاری و کار کردن با آنها برای انسان راحت‌تر است. با این وجود دنیای ماشینها بر اساس اعداد و ارقام شکل گرفته و عملاً چیزی که کامپیوترها با آن کار

میکنند IP آدرسها هستند. برای تطابق این دو قسمت بود که سرویس DNS ابداع شد. این سرویس نام هر دامنه را به IP آدرس متناظرش ترجمه میکند. به عنوان مثال هنگامی که شما در مرورگر خود google.com را تایپ میکنید کامپیوتر شما درخواستی را به سرور DNS میفرستد و در جواب IP آدرس سایت گوگل یعنی 66.249.93.104 را دریافت میکند. این کار در پس‌زمینه و به دور از چشم شما انجام میگیرد.

آدرس سروری که سرویس DNS را ارائه میدهد، به طور اتوماتیک و در هنگام برقراری اتصال به اینترنت از طریق ISP در اختیار کامپیوتر شما گذاشته میشود. حال اگر این سرور DNS، سانسور کننده باشد کلیه درخواستها برای سایتهای غیرمجاز را بی پاسخ میگذارد یا این که آنها را به سوی یک صفحه حاوی پیام اخطار منحرف میکند.

فیلترینگ بوسیله پروکسی:

در این حالت، ISP دسترسی مستقیم به اینترنت را محدود کرده و شما را ملزم به استفاده از پروکسی میکند. شما مجبورید برای دسترسی به اینترنت در تنظیمات مرورگر خود آدرس پروکسی سروری را که ISPتان به شما داده وارد کنید. به این ترتیب کلیه درخواستهای شما به پروکسی فرستاده میشود و در صورتی که مجاز باشد پروکسی فایل مورد نظرتان را از اینترنت گرفته و برایتان ارسال میکند. لازم به ذکر است که پروکسی‌ها کاربردهای بسیار متعددی دارند. از آنها هم برای فیلترینگ و هم برای مقابله با فیلترینگ میتوان استفاده کرد. برای اطلاعات بیشتر به مبحث پروکسی مراجعه کنید.

فیلتر کردن به کمک روتر (مسیریاب):

روترها (Router) یکی از اجزای اصلی شبکه‌ها هستند. این دستگاهها وظیفه مسیریابی و هدایت ترافیک را در شبکه بر عهده دارند. هنگامی که در یک شبکه بخواهد سانسور به کمک روتر انجام شود، معمولاً ترتیب کار به این صورت است که در قسمت انتهایی شبکه (دروازه یا Gateway)، یعنی جایی که شبکه محلی به اینترنت متصل میشود، روتر طوری تنظیم میشود که ترافیک خروجی شبکه را به سمت یک سیستم فیلتر کننده منحرف کند. در این حالت کلیه درخواستها و گاه ندرتاً کل ترافیک شبکه از این سیستم فیلتر کننده عبور داده میشود. این سیستم، اطلاعات رد و بدل شده را از جهت وجود کلمات ناشایست و سایتهای غیرمجاز بررسی میکند و در صورت وجود چنین مواردی جریان اطلاعات را بلوک میکند.

سانسورافزارها:

اگرچه معمولاً سانسور از طریق کامپیوتر سرویس دهنده (Server) اعمال میشود ولی گاهی علت سانسور، نرم‌افزارهایی هستند که بر روی کامپیوتر سرویس گیرنده نصب میشوند. به این نرم‌افزارها اصطلاحاً سانسور افزار (Censorware)

میگویند. این نرم‌افزارها بیشتر درخانه (کنترل والدین بر فرزندان)، مدارس و دانشگاهها استفاده میشوند. این نرم‌افزارها روی هر کامپیوتر به طور جداگانه نصب میشوند تا از دسترسی کاربر آن کامپیوتر به سایتهای غیرمجاز جلوگیری شود. نام تعدادی از این نرم‌افزارها در زیر آمده است:

- Net Nanny
- Cyber Sitter
- Cyber Patrol
- Surf Control

مسدود کردن پورتها:

پورتها مانند درهایی هستند که یک سرور از طریق آنها سرویسهایش را ارائه میدهد. هر پورت با یک شماره بین ۰ تا ۶۵۵۳۵ مشخص میشود. اگر یک پورت بلوک شود تمام سرویسهایی که از طریق آن پورت ارائه میگردد غیر قابل دستیابی میشوند. بیشتر سانسور کنندگان اینترنت پورتهای ۸۰، ۱۰۸۰، ۳۱۲۸ و ۸۰۸۰ را مسدود میکنند. زیرا اینها، پورتهای متداول (متعارف) برای پروکسی‌ها هستند و بیشتر پروکسی‌ها سرویس خود را از طریق این پورتها عرضه میکنند. به همین ترتیب اگر پورتهای دیگری نیز مسدود شوند سرویسهای ارائه شده از طریق آنها نیز غیر قابل دستیابی میگردد. مثلاً اگر پورت ۱۱۰ بلوک شود، دریافت ایمیل غیر ممکن خواهد شد. در جدول زیر لیست تعدادی از پورتهای مهم و سرویس ارائه شده از طریق آنها آمده است:

شماره پورت	نام سرویس	توضیح سرویس
20,21	FTP	سرویس تبادل فایل (اف تی پی)
23	Telnet	سرویس دسترسی از راه د ور (تل نت)
25	SMTP	سرویس ارسال ایمیل
53	DNS	سرویس ترجمه نام دامنه به IP آدرس
80	HTTP	سرویس وب
80	Proxy	پروکسی
110	POP3	سرویس دریافت ایمیل
443	SSL (HTTPS)	سرویس اتصال ایمن (رمزنگاری شده)
1080	Socks Proxy	پروکسی ساکس
3128	Proxy	پروکسی
8000	Proxy	پروکسی
8080	Proxy	پروکسی

جدول ۲- در این جدول لیستی از مهمترین سرویسهای اینترنتی به همراه پورت مختص آنها آمده است.

لیست سیاه/ لیست سفید:

این مورد بیش از آن که یک روش مستقل فیلترینگ باشد، تکنیکی است که در سایر روشها از آن استفاده میشود. بیشتر سیستمهای فیلترینگ از طریق لیست سیاه عمل میکنند. لیست سیاه شامل آدرس مجموعه سایتهایی است که دسترسی به آنها مجاز نمی‌باشد و سایر سایتهایی که نامشان در این لیست نیامده مجاز محسوب میشوند. گاهی در لیست سیاه علاوه بر آدرس سایتهای فیلتر شده از کلمات کلیدی نیز استفاده میشود. کلمات کلیدی عباراتی هستند که اگر در سایت مورد درخواست وجود داشته باشند باعث واکنش سیستم فیلتر کننده و بلوک شدن درخواست میشوند. استفاده از کلمات کلیدی یک روش سخت گیرانه در سیستمهای فیلترینگ است و به این سیستمها امکان میدهد تا سایتهای غیرمجازی را که قبلاً از لحاظ محتوا مورد بررسی قرار نگرفته‌اند و آدرس آنها در لیست سیاه وجود ندارد، بر اساس کلمات بکار رفته در آنها مورد شناسایی قرار دهند. از آنجایی که استفاده از کلمات کلیدی، سیستمهای فیلترینگ را مستعد خطا و بلوک بیش از حد میکند، به جز در موارد خاص از این روش استفاده نمیشود. عبارات sex, porn, proxy **نمونه‌هایی از کلمات کلیدی هستند.**

لیست سفید برعکس لیست سیاه عمل میکند، یعنی مجموعه سایتهایی را دربر میگیرد که دسترسی به آنها مجاز است و باقی سایتها همگی غیرمجاز به حساب می‌آیند. لیست سفید شدیدترین حالت فیلترینگ است و بالنتیجه عبور از آن نیز بسیار مشکل می‌باشد. خوشبختانه این روش در مورد اینترنت کاربرد چندانی ندارد. زیرا با وجود لیست سفید، اینترنت معنی خود را از دست میدهد. از این روش معمولاً در ادارات و سازمانهایی استفاده میشود که میخواهند کارمندانشان فقط به تعداد معدودی سایتهای مرتبط با زمینه کاریشان دسترسی داشته باشند.

اصول مقابله با فیلترینگ

ترفندهای عبور از فیلتر

برای مقابله با فیلترینگ یک روش جامع و واحد وجود ندارد، بلکه انتخاب روش مناسب باید با توجه به عوامل متعددی انجام شود. از جمله نوع فیلترینگ، مسائل مالی، مسائل قانونی و غیره:

- همان طور که در مبحث انواع فیلترینگ گفته شد، شیوه‌های مختلفی برای انجام فیلترینگ وجود دارد که سانسورگران بر حسب شرایط و نیازها، یکی از آنها را انتخاب میکنند. متأسفانه ما نمی‌توانیم در شناسایی نوع فیلترینگ به شما کمک کنیم. بنابراین، این خودتان هستید که باید نوع فیلترینگی را که در منطقه شما استفاده میشود شناسایی کرده و بر اساس آن، راهکار مناسب مقابله را انتخاب کنید.
- نکته دیگری که در انتخاب روش مقابله اهمیت دارد این است که آیا شما برای این کار بودجه‌ای در نظر گرفته‌اید یا نه ! اگرچه در حالت عادی روشهای زیادی وجود دارند که شما میتوانید به رایگان از آنها برای عبور از فیلتر بهره بگیرید ولی این روشها در مقایسه با روشهای پولی از اعتبار و کارایی بسیار کمتری برخوردارند. اکثر این روشها خیلی زود توسط اداره فیلترینگ شناسایی و خنثی میشوند و شما ناچار خواهید شد تا به دنبال روشهای جدید باشید. تجربه نشان داده وقت و هزینه‌ای را که شما در مدت یک سال برای پیدا کردن پروکسی‌ها و فیلترشکنهای عمومی و سایر روشهای رایگان خرج میکنید بیشتر از روشهای پولی است.
- در بعضی کشورها سیستم فیلترینگ با پشتوانه قانونی حمایت میشود و برای کسانی که سعی کنند از فیلتر فرار کنند جریمه‌های نقدی و حتی گاهی حبس در نظر گرفته شده است. واضح است که در چنین مواردی شما باید بسیار محتاط باشید و تنها از روشهایی استفاده کنید که قابل شناسایی نباشند. ما از شما اکیداً میخواهیم قبل از مطالعه ادامه بحث، از قوانین حاکم بر کشور خود اطلاع کسب کنید، زیرا مسئولیت و عواقب استفاده از روشهایی که در اینجا آموزش داده شده صرفاً بر عهده خود شما خواهد بود.

در ادامه، روشهای مختلف عبور از فیلتر توضیح داده شده است و سعی شده به روشهایی که در ایران قابل استفاده است بیشتر پرداخته شود. از آنجایی که ۸۰ درصد سرویس دهندگان اینترنت (ISP) در ایران برای اعمال فیلترینگ به مخابرات وابسته هستند، تمرکز ما نیز بر روشهایی است که بر این نوع از فیلترینگ مؤثر می‌باشد. ولی به هرحال به این نکته توجه داشته باشید که ممکن است ISP شما از یک سیستم فیلترینگ مجزا استفاده کند یا این که علاوه بر فیلترینگ مخابرات، سیستم فیلترینگ مخصوص به خود را نیز داشته باشد.

تغییر ISP:

اگر شما بتوانید از شرکتهای خارجی یا از طریق ماهواره اشتراک اینترنت تهیه کنید، مشکل فیلترینگ شما به کلی رفع خواهد شد، ولی اینترنتهای ماهواره‌ای نیاز به تجهیزات خاص دارد و ممکن است قیمت آن برای کاربران خانگی خیلی مناسب نباشد.

سرویس‌دهندگان اینترنت ایرانی از لحاظ فیلترینگ وضعیت گوناگون دارند. از آنجایی که در ایران یک نظام هماهنگ برای فیلترینگ وجود ندارد، گاهی دیده میشود که یک سایت مشخص توسط بعضی ISPها فیلتر شده در حالیکه همان سایت از طریق ISPهای دیگر قابل دسترسی است. در این میان ISPهای بزرگ و شناخته شده، وضعیت نامطلوب‌تری دارند. به کرات دیده شده که این ISPها کاسه داغتر از آش شده و علاوه بر سایتهایی که مخابرات مسدود کرده تعدادی سایت را نیز خودشان بلوک میکنند. بهترین کار این است که از این ISPها اشتراک اینترنت نگیرید.

سایر روشهای مقابله با فیلتر که ذیلاً توضیح داده شده‌اند ممکن است در مورد بعضی ISPها بسیار موثر باشد در حالیکه در مورد بعضی دیگر از کارایی لازم برخوردار نباشند. این که بفهمید کدام روش مقابله در مورد ISP شما موثر است تنها با شناخت دقیق سیستم فیلترینگ آن ISP و یا به روش آزمون و خطا امکان پذیر است.

تغییر سرور DNS:

همانطور که در مبحث انواع فیلترینگ گفته شد، این ساده‌ترین و کم خرج‌ترین شیوه سانسور است ولی در عین حال عبور از آن نیز به همان اندازه راحت است. اگر DNS از نوع سانسور کننده باشد هرگونه درخواست برای سایتهای غیر مجاز را بی پاسخ گذاشته یا آنها را به سمت یک صفحه حاوی پیام اخطار منحرف میکند. راه حل بسیار آسان است: جایگزین کردن DNS سانسور کننده با یک DNS آزاد. اگر سرور DNS شما سانسور کننده است، میتوانید آن را با یکی از دو سرور زیر تعویض کنید.

- 171.64.7.55 (caribou.Stanford.EDU)
- 171.64.7.77 (cassandra.Stanford.EDU)

شرکت مخابرات از این شیوه استفاده نمیکند ولی ممکن است تعدادی از ISPها، به خاطر کم‌خرج بودن از آن استفاده کنند. برای اطلاع از نحوه تغییر سرور DNS به ضمیمه یک مراجعه کنید.

دستکاری URL:

URL مخفف کلمات Uniform Resource Locator و به معنی نشانگر یک شکل منبع می‌باشد. نگران نشوید، URL چیز پیچیده‌ای نیست. URL در واقع آدرس هر صفحه وب در اینترنت است. یعنی همان چیزی که در کادر آدرس مرورگرتان مشاهده میکنید. اگر بخواهیم خیلی ساده بگوییم URL از سه جزء تشکیل شده است:

۱. پروتکل مورد استفاده برای برقراری ارتباط: در مورد صفحات وب این پروتکل HTTP است.
۲. نام دامین (Domain): این در واقع نام سروری است که فایل مورد نظرتان بر روی آن قرار گرفته است.
۳. مسیر (Path): این قسمت محل قرار گرفتن فایل مورد نظر بر روی سرور را مشخص میکند.

به عنوان مثال مقاله "ترفندهای مقابله با فیلتر" در وب سایت نوفیلتر در URL زیر قرار گرفته است. این URL نشان میدهد که از پروتکل HTTP برای برقراری ارتباط با سرور سایت نوفیلتر استفاده میشود. باقی URL، محل قرار گرفتن فایل f1_howto_bypass.htm را بر روی سرور سایت نوفیلتر مشخص میکند.

http://www.no-filter.com/censor/f1_howto_bypass.htm

اغلب سیستمهای فیلترینگ بر اساس لیست سیاه کار میکنند. لیست سیاه شامل URL مجموعه سایتهایی است که دسترسی به آنها توسط دست اندرکاران فیلترینگ ممنوع شده است. همچنین گاهی صاحبان فیلترینگ از این فراتر رفته و کلمات کلیدی را نیز به لیست سیاه خود می‌افزایند. هنگامی که شما درخواست دیدن یک صفحه وب را میکنید، سیستم فیلتر کننده URL آن صفحه را با لیست سیاهش مقایسه میکند و اگر تشابهی پیدا کند، آن درخواست را بلوک می‌کند.

یک راه مقابله با این مشکل این است که ما URL را به نحوی تغییر دهیم که دیگر با لیست سیاه مطابقت نداشته باشد ولی همچنان به صفحه مورد نظر ما اشاره کند. در زیر چند ترفند برای انجام این کار آمده است:

۱. سعی کنید بجای نام دامین از IP آدرس سایت مورد نظرتان استفاده کنید. مثلاً به جای www.google.com بنویسید 66.249.93.104. هر دو اینها شما را به سایت گوگل می‌برد. اگر IP آدرس سایت مورد نظرتان را ندارید کافیست در ویندوز اکس پی پنجره Command Prompt را باز کرده و دستور زیر را تایپ کنید (به جای آدرس گوگل آدرس سایت مورد نظرتان را قرار دهید):

```
C:\> ping www.google.com
```

اگر به هر دلیلی به پنجره Command Prompt دسترسی ندارید، ناراحت نباشید. وب سایتهایی وجود دارند که با گرفتن نام سایت، IP آدرس آن را در اختیارتان قرار میدهند. selfseo.com و www.hcidata.co.uk دو تا از این سایتها هستند.

این روش تا حدودی در ایران مؤثر است. تأثیر این روش به این بستگی دارد که آیا IP آدرس سایت مورد نظر شما در لیست سیاه مخابرات قرار داشته باشد یا نه. با پیشرفت فیلترینگ روز به روز از تأثیر این روش کاسته میشود.

۲. شماره پورت را به انتهای نام دامین اضافه کنید. مثلاً به جای google.com بنویسید google.com:80 . پورت ۸۰، پورت پیش‌فرض برای پروتکل HTTP است. این روش در مورد فیلترینگ مخابرات مؤثر نیست.

۳. یک نقطه به انتهای نام دامین اضافه کنید. یعنی به جای google.com بنویسید google.com. . این روش در بعضی موارد بسیار مؤثر است. فقط توجه داشته باشید که گاهی در حین مرور صفحات وب، نقطه از انتهای نام دامنه پاک میشود. تنها کاری که شما باید انجام دهید این است که مجدداً نقطه را به انتهای نام دامنه اضافه کنید. در مورد بعضی ISPها این روش بسیار خوب عمل میکند. برای اینکه بفهمید در مورد ISP شما هم موثر است یا نه، با کلیک روی دو لینک زیر آن را امتحان کنید:

- http://www.radiofarda.com/
- http://www.radiofarda.com./

ترفندهای دستکاری URL، مبتنی بر نقص در طراحی و پیکربندی سیستمهای فیلترینگ هستند. به همین علت چندان قابل اطمینان نمی‌باشند. به محض اینکه مدیران فیلترینگ از وجود نقص در سیستم خود آگاه شوند، آن را برطرف کرده و این ترفندها خنثی میشوند.

استفاده از کش (Cache) موتورهای جستجو:

هنگامی که در کادر یک موتور جستجو مانند گوگل Google و یاهو YAHOO! عبارتی را تایپ کرده و اینتر را فشار میدهید، نتایج جستجو در یک صفحه نمایش داده میشود. حال فرض کنید روی یکی از این نتایج کلیک میکنید و به جای این که صفحه مورد انتظارتان نمایش داده شود، به صفحه "دسترسی مقدور نیست" برمیخورید. یک راه حل ساده این است که دکمه پس‌گرد (Back) را فشار داده به صفحه نتایج جستجو برگردید. این بار به جای این که روی نتیجه جستجو کلیک کنید، کمی پایین‌تر بر روی عبارت Cache کلیک کنید. در این حالت به جای این که صفحه مورد نظر از وب سایت اصلی برایتان بیاید، یک کپی از آن صفحه که در سرور موتور جستجو بایگانی شده برایتان ارسال میگردد. این کپی متعلق به چند روز قبل است و معمولاً فاقد عکس و مولتی‌مدیا می‌باشد ولی به هرحال ممکن است کار شما را راه بیاندازد.

برای اینکه یک صفحه را مستقیماً از طریق کش گوگل دریافت کنید، ابتدا در کادر جستجوی گوگل کلمه "cache:" را نوشته و سپس در کنار آن آدرس صفحه مورد نظرتان را تایپ کنید. به عنوان مثال برای اینکه دیدن صفحه خانگی بخش فارسی بی‌بی‌سی BBC عبارت زیر را در کادر جستجوی گوگل تایپ کنید:

- cache:http://bbc.co.uk/persian

این روش تا چند وقت پیش به خوبی در ایران جواب میداد ولی اخیراً به علت ارتقا سیستم فیلترینگ از تأثیر آن کاسته شده است. با این حال هنوز هم قابل استفاده است و در مورد بعضی سایتها جواب میدهد. اگر سیستم فیلترینگ نمیگذارد از طریق کش گوگل به مطالب یک وب سایت دسترسی پیدا کنید، سعی کنید آدرس آن سایت را کمی دستکاری کنید. مثلاً www را جلوی آن بردارید و یا اینکه از IP آدرس سایت گوگل استفاده کنید.

شبکه‌های نظیر به نظیر (Peer to Peer):

شبکه‌های نظیر به نظیر شبکه‌های مجازیی هستند که در درون اینترنت و بر مبنای ارتباط یک به یک کامپیوترها شکل گرفته‌اند. در شبکه‌های نظیر به نظیر (P2P)، یک سرور مرکزی که کلیه اطلاعات بر روی آن قرار گرفته باشد وجود ندارد، بلکه اطلاعات بر روی کلیه کامپیوترهای عضو شبکه پخش شده است و هر کامپیوتر هم به عنوان سرویس‌دهنده و هم به عنوان سرویس گیرنده عمل میکند. به علت گستردگی و غیر متمرکز بودن این گونه شبکه‌ها امکان کنترل و سانسور آنها وجود ندارد. برای اینکه به عضویت یکی از این شبکه‌ها در آیید لازم است نرم‌افزار مربوط به آن را بر روی کامپیوتر خود نصب کنید. به این ترتیب میتوانید فایلهای مورد علاقه‌تان را با دیگر کاربران آن شبکه به اشتراک بگذارید و از فایلهای آنها نیز استفاده کنید. این شبکه‌ها در ابتدا برای به اشتراک گذاری فایلهای موسیقی و نرم‌افزار پدید آمدند ولی امروزه تقریباً هر چیزی را میتوان بر روی آنها یافت. به این نکته توجه داشته باشید که بسیاری از موسیقیها و نرم‌افزارهایی که در این شبکه‌ها به اشتراک گذاشته شده‌اند، مشمول قانون کپی رایت هستند. اگر در کشور شما قانون کپی رایت رعایت میشود قبل از دانلود و استفاده از این گونه فایلها به جنبه‌های قانونی مسئله توجه داشته باشید. ذیلاً اسامی تعدادی از شبکه‌های P2P آمده است:

- eDonkey
- BitTorrent
- FreeNetwork
- eMule
- Entropy

دریافت صفحات وب از طریق ایمیل:

در سالهای آغازین اینترنت در دهه ۱۹۹۰ سرویس وب، تازه ابداع شده بود و هنوز دسترسی اکثر کاربران به اینترنت، محدود به ایمیل بود. در آن زمان بود که روباتهای ایمیل (Email Robots) پدید آمدند. کار این روباتها این بود که صفحات وب را گرفته و برای کاربران ایمیل میکردند. هنوز هم تعدادی از این روباتها وجود دارند که می‌توان از آنها برای گذشتن از سد سانسور استفاده کرد. اگرچه این روباتها برای صفحات فقط متن (Text) بسیار مناسب هستند ولی مطمئناً با صفحاتی که مولتی‌مدیا دارند مشکل خواهند داشت. آدرس تعدادی از این روباتها در زیر آمده است:

۱. agora@dna.affrc.go.jp
اطلاعات: یک ایمیل با متن www به آدرس فوق بفرستید.

۲. web@pagegetter.com
اطلاعات: http://www.pagegetter.com/

۳. webgate@vancouver-webpages.com
اطلاعات: http://vancouver-webpages.com/webgate/

۴. www4mail@wm.ictp.trieste.it
اطلاعات: http://www4mail.org/

۵. www4mail@kabissa.org
اطلاعات: http://www.kabissa.org/members/www4mail/

۶. iliad@prime.jsc.nasa.gov
اطلاعات: http://prime.jsc.nasa.gov/iliad/

شما میتوانید توضیحات جامعی را درباره چگونگی دریافت صفحات وب از طریق ایمیل در اینجا پیدا کنید.

فیدهای RSS:

آر اس اس تکنیکی است که به وب سایتها خصوصاً سایتهای خبری و وبلاگها اجازه میدهد تا عناوین و خلاصه اخبار و مطالب خود را به صورت فیدهای خبری منتشر کنند. همچنین RSS کاربران را از مراجعه به وب سایتها و وبلاگهای مختلف برای خواندن مطالب مورد نظرشان بی‌نیاز میکند و به آنها امکان میدهد تا همه مطالب مورد علاقه‌شان را به صورت یکجا و در کنار هم مشاهده کنند. برای این که شما بتوانید فیدهای RSS را دریافت کنید و آنها را بخوانید لازم است از خبرخوانهای آر اس اس (RSS Reader) استفاده کنید. این خبرخوانها به سه شکل وجود دارند:

۱. **خبرخوانهای رومیزی: اینها به صورت برنامه‌های نرم‌افزاری هستند که لازم است ابتدا بر روی کامپیوتر شما نصب شوند، سپس به شما امکان میدهند تا فیدهای خبری را دریافت کرده و آنها را بخوانید.**

۲. خبرخوانهای تحت وب: وب سایتهایی وجود دارند که این امکان را فراهم می‌آورند تا شما از طریق آنها فیدهای RSS را دریافت و مطالعه کنید. در اینجا شما نیاز به نصب نرم‌افزار بر روی کامپیوترتان ندارید. خبرخوانهای یاهو و گوگل در این زمینه از بهترینها هستند.

۳. خبرخوانهای ایمیل کننده: وب سایتهایی وجود دارند که فیدهای RSS را دریافت و آنها را در قالب ایمیل برایتان ارسال میکنند. شما میتوانید لیست کاملی از خبرخوانهای رومیزی، تحت وب و ایمیل کننده را در اینجا بیابید.

امروزه اکثر وبلاگها و تعداد زیادی از سایتهای خبری از RSS پشتیبانی میکنند. در این سایتها معمولاً دکمه‌هایی به صورت RSS یا XML وجود دارد. برای اینکه مطالب این سایتها را از طریق RSS دریافت کنید لازم است بر روی این دکمه‌ها کلیک راست کرده و سپس گزینه Copy Shortcut را انتخاب کنید. به این ترتیب آدرس RSS آن سایت در کلیپ بورد شما کپی میشود. حال این آدرس را به خبرخوان خود بدهید. با این کار شما میتوانید عناوین و مطالب آن سایت را در خبرخوان خود مشاهده کنید.

توجه داشته باشید که اگر وب سایتی فیلتر شده باشد ممکن است شما نتوانید از طریق خبرخوانهای رومیزی به فیدهای آن دسترسی پیدا کنید ولی این کار به خوبی از طریق خبرخوانهای تحت وب و ایمیل‌کننده قابل دستیابی است. در زیر آدرس فیدهای خبری خبرگزاریهای بی‌بی‌سی و صدای آمریکا آمده است. اگرچه وب سایت این خبرگزاریها مسدود شده است ولی شما با دادن این آدرسها به خبرخوانتان میتوانید از آخرین اخبار و گزارشهای این وب سایتها آگاه شوید.

- http://feeds.bbc.co.uk/persian/iran/index.xml
- http://voanews.com/persian/customCF/RecentStoriesRSS.cfm?keyword=Iran

پروکسی:

پروکسی به کامپیوتری گفته می‌شود که به سایر کامپیوترها اجازه میدهد از طریق آن با مقصدشان یک ارتباط غیر مستقیم برقرار کنند. کاربرد پروکسی‌ها بسیار متنوع است. هم برای فیلترینگ و هم برای فرار از فیلتر میشود از آنها استفاده کرد. برای اطلاعات بیشتر به مبحث پروکسی مراجعه کنید.

استفاده از سایر پروتکلها:

همانطور که قبلاً گفته شد فیلترینگ یک امر هزینه‌بر است و هزینه سنگینی را بر صاحبان آن تحمیل میکند. از اینرو دست اندرکاران فیلترینگ همواره سعی میکنند در عین مؤثر بودن، سانسور فقط بر بخشهای ضروری و حساس اعمال گردد. مثلاً در ایران فیلترینگ فقط بر پروتکل HTTP (صفحات وب) اعمال میشود و سایر پروتکلها تقریباً از سانسور

در امان هستند. معنی این حرف این است که اگرچه دسترسی شما به صفحاتِ وبِ یک سایت، مسدود شده ولی شما میتوانید:

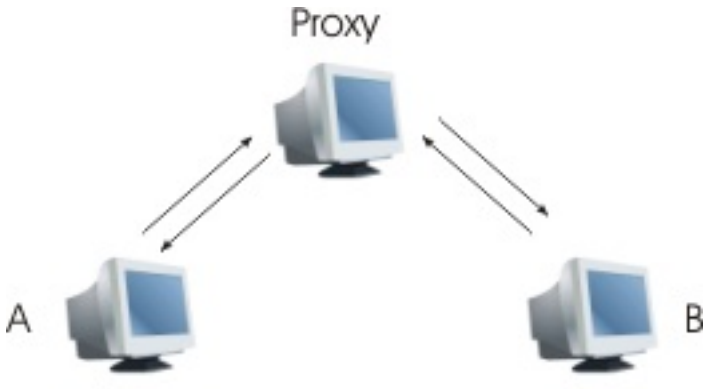
1. **به این سایت ایمیل بزنید و یا از آن ایمیل دریافت کنید.**
2. **از طریق اتصال ایمن (HTTPS یا SSL) به صفحات وب موجود بر روی این سایت دسترسی پیدا کنید.**
3. **از طریق FTP به فایلهای موجود بر روی این سایت دسترسی پیدا کنید.**
4. **از طریق برنامه‌های مسنجر(چت) با این سایت ارتباط برقرار کنید.**

البته اینها مشروط بر این است که این سرویسها توسط سایت مذکور ارائه گردد.

پروکسی (Proxy)

پروکسی در لغت به معنای "وکیل" و "به نیابت کسی کاری را انجام دادن" است. در دنیای اینترنت پروکسی به کامپیوتری گفته میشود که به سایر کامپیوترها اجازه میدهد تا از طریق آن با مقصدشان یک ارتباط غیر مستقیم برقرار کنند. بیایید این مطلب را با یک مثال ساده بیشتر توضیح دهیم. فرض کنید شما در یک اداره کار میکنید. هر اتاق این اداره یک خط تلفن دارد که به تلفنخانه مرکزی اداره وصل است. حال اگر شما بخواهید از اداره به منزلتان زنگ بزنید لازم است یک شماره (مثلاً ۹) را بگیرید و بعد از تلفنچی اداره بخواهید که شماره تلفن منزلتان را گرفته و به شما وصل کند. نقش تلفنخانه و تلفنچی در این مثال دقیقاً مانند نقش پروکسی در اینترنت است. وقتی کامپیوتری از طریق پروکسی به اینترنت وصل است و میخواهد به یک فایل دسترسی پیدا کند، ابتدا درخواستش را به پروکسی میفرستد. سپس پروکسی به کامپیوتر مقصد متصل شده و فایل درخواستی را دریافت میکند و بعد آن را برای کامپیوتر درخواست کننده میفرستد.

شکل ۱ : این شکل ارتباط مستقیم بین کامپیوترهای سرویس دهنده و سرویس گیرنده را نمایش میدهد.



شکل ۲ : این شکل ارتباط از طریق پروکسی را نشان میدهد. همانطور که می‌بینید عملاً هیچ ارتباط مستقیمی بین کامپیوتر سرویس دهنده و کامپیوتر سرویس گیرنده وجود ندارد.

همانطور که می‌بینید پروکسی در اینجا به عنوان یک واسطه عمل میکند و عملاً هیچ ارتباط مستقیمی بین کامپیوترهای سرویس‌دهنده و سرویس‌گیرنده وجود ندارد. حال ممکن است برایتان این سوال پیش آید که کاربرد پروکسی چیست و چرا گاهی از آن استفاده میشود. پاسخ این است که برای استفاده از پروکسی دلایل زیادی وجود دارد که ذیلاً به مهمترین آنها اشاره میشود:

بالا بردن امنیت شبکه:

گاهی مدیران شبکه برای بالا بردن امنیت شبکه‌شان و حفاظت کاربران در برابر هکرها از پروکسی استفاده میکنند. در این حالت به جای این که تک‌تک کاربران مستقیماً به اینترنت متصل شوند، همگی از طریق یک پروکسی به اینترنت وصل میشوند. به این ترتیب مدیر شبکه می تواند با نصب فایروال و سایر نرم‌افزارهای امنیتی و با نظارت بر پروکسی از کل شبکه تحت مدیریتش محافظت کند.

اعمال محدودیت بر کاربران:

گاهی علت استفاده مدیران شبکه از پروکسی، اعمال محدودیت بر کاربران است. البته توجه کنید که اعمال محدودیت، صرفاً به معنی فیلترینگ یا سانسور نیست بلکه ممکن است مدیر شبکه فقط استفاده از برخی نرم‌افزارها (مانند چت) را برای کاربرانش ممنوع کند.

کش کردن (Caching):

یکی از کاربردها مهم پروکسی انجام کش است. کش به یک نسخه بایگانی شده از محتویات اینترنت بر روی پروکسی گویند. فرض کنید در شبکه‌ای که از پروکسی استفاده میکند چند صد کاربر وجود دارد. حال یکی از این کاربران میخواهد اخبار سایت بی‌بی‌سی BBC را بخواند، لذا درخواستی را به پروکسی فرستاده و پروکسی نیز صفحه مورد نظر را از سایت بی‌بی‌سی گرفته و برایش ارسال میکند. در اینجا پروکسی میتواند یک نسخه از این صفحه را بر روی هارد دیسکش ذخیره کند. حال اگر کاربر دیگری تقاضای همین صفحه را بکند دیگر لازم نیست پروکسی مجدداً به سایت بی‌بی‌سی مراجعه کند، بلکه خیلی راحت نسخه‌ای که روی هارد دیسکش ذخیره شده را برای وی میفرستد. با انجام این کار هم به سرعت و کارایی شبکه اضافه میشود و هم از ترافیک و بار شبکه کاسته میگردد. البته انجام عمل کش، الگوریتم پیچیده‌ای دارد و پروکسی باید به نحوی این کار را انجام دهد تا از ارسال اطلاعات تاریخ گذشته اجتناب شود.

حفظ هویت:

علت استفاده بعضی کاربران از پروکسی، مخفی ماندن و شناسایی نشدن است، زیرا از دید کامپیوتر میزبان، آن کسی که تقاضای اطلاعات کرده پروکسی است نه کاربر. البته هر کس برای مخفی کاری دلایل خاص خود را دارد. ممکن است شما یک شخص معروف باشید و نخواهید کسی بفهمد که شما از چه سایتهایی بازدید کرده‌اید. حالت دیگر این است که یک هکر بخواهد به یک سیستم نفوذ کند و هیچ ردپایی از خود بجا نگذارد.

توجه داشته باشید که همه پروکسی‌ها برای مخفی کاری مناسب نیستند و از این نظر به دو دسته ناشناس (Anonymous) و غیر ناشناس (Non-Anonymous) تقسیم میشوند. پروکسیهای ناشناس، هویت فردی که ازشان استفاده میکند را حفظ میکنند در حالی که پروکسیهای غیر ناشناس هویت (IP آدرس) کاربرشان را به کامپیوتر هدف اطلاع میدهند.

تحت نظر گرفتن و سرقت اطلاعات:

به مثالی که در اول این بحث آورده شد برگردید. همواره برای تلفنچی اداره این امکان وجود دارد که به مکالمات شما دزدکی گوش دهد و از کارتان سر درآورد. عین همین مسئله برای پروکسی صادق است. گاهی یک سازمان امنیتی یا یک نهاد دولتی مثل FBI اقدام به ایجاد پروکسی عمومی میکند و سعی میکند با تحت نظر قرار دادن کسانی که از پروکسی آنها استفاده میکنند، اقدام به شناسایی هکرها و خرابکاران کند. گاهی نیز این هکرها و دزدان اینترنتی هستند که اقدام به ایجاد پروکسی میکنند و قصدشان این است تا با زیر نظر گرفتن کاربران، اطلاعات مهم آنها مثل شماره کارت اعتباری و پسوردها را سرقت کنند.

گذشتن از سد سانسور (فیلترینگ):

این خصوصیت پروکسی که یک ارتباط غیر مستقیم بین مبدا و مقصد بوجود می‌آورد، آن را برای دور زدن سیستمهای فیلترینگ بسیار مناسب ساخته است. زمانی که ارتباط مستقیم شما با یک سایت به دلیل فیلترینگ قطع شده، شما میتوانید به طور غیر مستقیم و به کمک پروکسی به آن دسترسی پیدا کنید، البته به شرط این که خود پروکسی فیلتر نشده باشد. در ادامه این کاربرد پروکسی را بیشتر توضیح میدهیم.

اگر شما قصد دارید از پروکسی برای عبور از فیلتر استفاده کنید، لازم است ۳ مرحله را طی کنید. اول این که یک پروکسی آزاد در خارج از محدوده فیلترینگ پیدا کنید. سایتهای زیادی وجود دارند که لیستی از پروکسی‌ها را در اختیارتان میگذارند. آدرس تعدادی از این سایتها در اینجا آمده است:

- Stayinvisible
- Proxy 4 Free
- Public Proxy Servers
- Proxz
- NNTime
- AliveProxy

به احتمال زیاد دسترسی شما به اکثر سایتهای فوق الذکر مسدود شده است. اگر چنین است با تایپ عبارت " proxy list" **در گوگل سعی کنید سایتی را پیدا کنید که فیلتر نشده باشد. برای این کار میتوانید از کش** (Cache) **گوگل نیز کمک بگیرید. مطمئناً با کمی حوصله میتوانید به لیستی از پروکسی‌ها دسترسی پیدا کنید. ولی توجه داشته باشید که ممکن است تنها تعداد کمی از آن پروکسی‌ها برای شما کار کنند. راهنمائیهای زیر شما را در انتخاب پروکسی مناسب کمک میکند:**

پورت پروکسی:

پروکسی‌ها نیز مانند سایر سرویسهای اینترنت خدمات خود را بر روی پورتهای خاصی ارائه میدهند. پورتهای متعارف (Common Ports) **برای پروکسی‌ها عبارتند از ۸۰، ۱۰۸۰، ۳۱۲۸ و ۸۰۸۰ . به طور معمول شماره پورت پروکسی به همراه دو نقطه : در انتهای آدرس پروکسی نوشته میشود، مثلاً:**

- 195.175.37.6:8080
- proxy.net:3128

بسیاری از سانسور کنندگان اینترنت برای این که جلوی استفاده کاربرانشان از پروکسی را بگیرند، پورتهای متعارف را مسدود میکنند. لذا شما باید به دنبال پروکسی بگردید که خدماتش را بر روی پورتی ارائه کند که مسدود نباشد.

در ایران پروکسیهایی که روی پورت ۸۰ قرار دارند برایتان کار نخواهند کرد. پس وقتتان را بیهوده تلف نکرده و به راحتی از آنها صرف‌نظر کنید. پروکسیهایی که روی پورتهای ۳۱۲۸ و ۸۰۸۰ هستند چندان قابل اعتماد نیستند، زیرا دیده میشود که ISPها و مخابرات مکرراً این پورتها را بلوک میکند. سایر پورتها باز هستند ولی متأسفانه پیدا کردن پروکسی که روی پورتهای نامتعارف کار کند چندان آسان نیست.

آدرس پروکسی:

آدرس پروکسی که قصد استفاده از آن را دارید نباید در لیست سیاه مخابرات باشد وگرنه کار نخواهد کرد. عملاً این امکان برای سانسور کنندگان وجود ندارد که آدرس تمام پروکسی‌ها را در لیست سیاهشان قرار دهند. چون هر روزه هزاران پروکسی شروع به کار میکنند و صدها عدد نیز از ارائه سرویس باز می‌مانند. کنترل و شناسایی همه پروکسی‌ها برای سانسور کنندگان کاری غیر ممکن است.

پروکسی عمومی:

بسیاری از پروکسی‌ها توسط سازمانها و مؤسسات و برای ارائه خدمت به کاربران خودشان ایجاد شده‌اند. این دسته از پروکسی‌ها از ارائه سرویس به شما امتناع خواهند کرد. برای استفاده از گروهی دیگر از پروکسی‌ها ممکن است نیاز به پسورد داشته باشید. برای این که بتوانید از آنها استفاده کنید باید مشترکشان شوید و آبونمان بپردازید. خوب، اگر قصد پول خرج کردن ندارید تنها گزینه باقیمانده برایتان پروکسیهای عمومی و پروکسیهای حفاظت نشده هستند. پروکسیهای حفاظت نشده در اصل متعلق به مؤسسات و سازمانها هستند و برای استفاده داخلی خودشان طراحی شده‌اند ولی به علت ضعف در مدیریت و پیکربندی، به افراد خارج از آن سازمان نیز سرویس میدهند. بدیهی است که عمر این پروکسی‌ها بسیار کوتاه می‌باشد و به محض اینکه صاحبان پروکسی به سوء استفاده از پروکسیشان پی ببرند آن را خواهند بست. پروکسی عمومی (Public Proxy) به پروکسی میگویند که برای استفاده رایگان عموم کاربران اینترنت طراحی شده است. عملاً چنین پروکسی وجود ندارد، چرا که ایجاد و نگهداری یک پروکسی هزینه زیادی برای صاحب آن دارد و در مقابل هیچ منفعتی هم برای او به همراه ندارد (البته بجز وب پروکسیها). بنابراین نسبت به پروکسیهای عمومی به دیده احتیاط نگاه کنید، زیرا ممکن است متعلق به سازمانهای جاسوسی یا دزدان اینترنتی باشد. البته گاهی چنین پروکسیهایی از طرف سازمانهای مبارزه با سانسور هم راه اندازی میشوند.

پروکسی فیلتر کننده:

گاهی ممکن است به پروکسیهای حفاظت نشده‌ای بر بخورید که خودشان برای اعمال سانسور طراحی شده‌اند. از آنجایی که این پروکسی‌ها متعلق به سایر کشورها هستند ممکن است بتوانید از آنها برای دسترسی به سایتهای سیاسی فیلتر شده استفاده کنید.

همان طور که از مطالب بالا متوجه شدید تنها تعداد کمی از پروکسی‌ها برای شما کار خواهند کرد. پس قدم دوم بعد از این که لیستی از پروکسی‌ها را بدست آوردید این است که آنها را امتحان کنید تا ببینید کدامیک برای شما کار میکنند. برای چک کردن پروکسی‌ها، برنامه‌هایی وجود دارد که لیست پروکسی‌ها را از شما گرفته و یک به یک آنها را تست میکند. به این نرم‌افزارها اصطلاحاً پروکسی چکر (Proxy Checker) میگویند. شما میتوانید لیستی از نرم‌افزارهای مرتبط با پروکسی را در اینجا پیدا کنید:

- MultiProxy
- ProxyAnalyzer
- ProxyScanner
- ProxyPing
- ProxyRama

بعد از این که یک پروکسی خوب پیدا کردید، قدم سوم این است که مرورگر خود را طوری تنظیم کنید تا به جای ارتباط مستقیم با اینترنت از پروکسی استفاده کند. برای این منظور، روش تنظیم پروکسی در اینترنت اکسپلورر و فایر فاکس را در ضمیمه یک بخوانید.

اگر مراحل فوق را با موفقیت انجام داده باشید، اکنون می‌توانید آزادانه در اینترنت گردش کنید. توجه داشته باشید که از پروکسی فقط برای سایتهای فیلتر شده استفاده کنید و برای سایر سایتها پروکسی را غیر فعال کنید، زیرا ممکن است سرعت اینترنت شما را کاهش دهد.

حال که با اصول و روش کار پروکسی‌ها آشنا شدید، لازم است کمی هم راجع به انواع پروکسی‌ها بدانید. از نظر فنی پروکسی‌ها به چند گروه تقسیم میشوند که مهمترین آنها عبارتند از:

1. **پروکسی HTTP: اکثر پروکسیهایی که به آنها برخورد میکنید از این گروه هستند. این پروکسی‌ها برای دیدن صفحات وب طراحی شده‌اند و فقط از پروتکل HTTP پشتیبانی میکنند. البته گاهی پروتکل FTP نیز توسط بعضی از آنها پشتیبانی میگردد. از این پروکسی‌ها نمیتوان برای دیدن صفحات رمزنگاری شده (Secure) استفاده کرد، زیرا پروتکل مورد استفاده برای این صفحات HTTPS است.**

۲. پروکسی HTTPS: معمولاً این پروکسی‌ها از هر دو پروتکل HTTP و HTTPS پشتیبانی میکنند و میتوان از آنها برای مرور صفحات وب رمزنگاری شده نیز بهره برد.

۳. پروکسی ساکس (Socks): این پروکسی‌ها که خود به دو دسته Socks 4 و Socks 5 تقسیم میشوند، طوری طراحی شده‌اند تا از کل پروتکلهای اینترنت پشتیبانی کنند. این پروکسی‌ها، غالباً روی پورت ۱۰۸۰ قرار دارند.

۴. وب پروکسی (CGI-Proxy): این پروکسی‌ها که در اصطلاح عوام به آنها فیلتر شکن میگویند با سایر پروکسیهای فوق‌الذکر اختلاف ریشه‌ای دارند. اینها در واقع وب سایتهایی هستند که به کاربر اجازه میدهند از طریق آنها به سایر وب سایتها دسترسی یابد و برای این منظور از برنامه‌هایی (اسکریپت) استفاده میکنند که به زبانهای برنامه نویسی تحت وب (مثل PHP و Perl) نوشته شده‌اند. از آنجایی که کار کردن با این پروکسی‌ها بسیار ساده است، محبوبیت زیادی پیدا کرده‌اند. به علت گستردگی مطلب، وب پروکسی‌ها در مبحث بعدی مفصلاً توضیح داده شده‌اند.

وب پروکسی (CGI-Proxy)

این پروکسی‌ها که امروزه در ایران به نام فیلترشکن معروف شده‌اند در واقع وب سایتهایی هستند که به زبانهای برنامه نویسی تحت وب مثل PHP و Perl برنامه نویسی شده‌اند و برای کاربر این امکان را پدید می‌آورند تا از طریق آنها به سایر وب سایتها دسترسی پیدا کند. مزیت عمده این پروکسی‌ها سهولت استفاده از آنهاست. تنها کاری که شما لازم است انجام دهید این است که به یکی از این وب پروکسی‌ها بروید و آدرس سایت مورد نظرتان را در فرم مربوطه تایپ کنید. ظرف چند ثانیه پروکسی صفحه مورد نظرتان را در برابر چشمانتان به نمایش میگذارد.

همان طور که قبلاً گفته شد این دسته از پروکسی‌ها با سایر پروکسی‌ها (HTTP و Socks) تفاوت اساسی دارند. مهمترین تفاوت آنها این است که این پروکسی‌ها محتویات صفحه وب را تغییر میدهند و اگر علمی‌تر بخواهیم بگوییم آن را بازنویسی میکنند. بازنویسی صفحه وب شامل موارد زیر است:

۱. افزودن آگهی‌های تبلیغاتی (Banner):

این حقیقت که وب پروکسی‌ها میتوانند با بازنویسی صفحات وب، آگهی‌های تبلیغاتی را به آنها اضافه کنند زمینه‌ای را فراهم آورده است تا بسیاری از شرکتها اقدام به عرضه رایگان این گونه پروکسی‌ها کنند.

۲. تغییر لینکها:

یک وب پروکسی، لینکهای صفحه را طوری تغییر میدهد که باز از میان همان پروکسی عبور کنند. یعنی وقتی شما روی یکی از لینکهای صفحه‌ای که با وب پروکسی باز شده کلیک میکنید بجای این که آن لینک از سایت اصلی باز شود از طریق وب پروکسی باز میشود. بیایید مطلب را با یک مثال بیشتر توضیح دهیم. فرض کنید شما از طریق وب پروکسی سایت نوفیلتر به صفحه خانگی یاهو مراجعه کرده‌اید. در بالای این صفحه لینکی وجود دارد که شما را به بخش ایمیل یاهو می‌برد. اگر آدرس لینک اصلی به صورت http://mail.yahoo.com/ **باشد، وب پروکسی آن را بازنویسی کرده و به شکل زیر درمی‌آورد:**

http://no-filter.com/proxy/nph-proxy.cgi/010110A/**http/mail.yahoo.com/**

حال اگر شما روی این لینک کلیک کنید، بجای این که مستقیماً وارد یاهو میل شوید باز هم از طریق پروکسی سایت نوفیلتر به آن دسترسی پیدا میکنید. حتی بعضی وب پروکسی‌ها از این هم فراتر رفته و لینکها را به گونه‌ای بازنویسی میکنند که قابل شناسایی نباشند. مثلاً لینک فوق را به صورت زیر در می‌آورند:

http://no-filter.com/proxy/nph-proxy.cgi/010010A/**uggc/znvy.lnubb.pbz/**

به این ترتیب هیچکس متوجه نمیشود شما از چه سایتهایی بازدید کرده‌اید و سیستمهای فیلترینگ نیز از کار باز می‌مانند. زیرا از نظر آنها شما در حال مشاهده سایت نوفیلتر هستید.

وب پروکسی‌ها در کنار مزایایشان نقاط ضعفی نیز دارند که عبارتند از:

۱. **این پروکسی‌ها به علت محبوبیت و سهولت در استفاده‌شان شدیداً مورد سانسور قرار گرفته‌اند. همانطور که در مبحث فیلترینگ در ایران گفته شد، مخابرات ۹۵ درصد از این سایتها را فیلتر کرده است. به همین علت پیدا کردن یک وب پروکسی فعال کار آسانی نیست و اگر هم چنین پروکسی پیدا کنید مطمئناً مدت زیادی برای شما کار نخواهد کرد.**

صدای آمریکا با همکاری شرکت انونیمایزر (Anonymizer) **اقدام به ایجاد یک وب پروکسی برای کاربران ایرانی کرده است و برای این که از دست فیلترینگ مخابرات در امان باشد مرتباً آدرس آن را عوض میکند. شما میتوانید با اشتراک خبرنامه صدای آمریکا، هر روزه تازه‌ترین اخبار و جدیدترین آدرس پروکسی را بوسیله ایمیل دریافت کنید. وب پروکسی صدای آمریکا مختص به کاربران ایرانیست و از خارج ایران قابل دسترسی نمی‌باشد. ضمناً این پروکسی از نوع سانسور کننده است و سایتهای غیر اخلاقی را فیلتر کرده، با این حال شما میتوانید از آن برای دسترسی به سایتهای سیاسی استفاده کنید. برای اشتراک خبرنامه به وب سایت صدای آمریکا مراجعه کنید.**

۲. وب پروکسی‌ها با بعضی صفحات پیچیده اینترنت، خصوصاً صفحاتی که در آنها از جاوا (Java) استفاده شده مشکل دارند و گاهی آنها را درست نشان نمیدهند.

۳. بعضی مواقع وب پروکسیهای عمومی با حجم عظیمی از درخواستهای کاربران مواجه میشوند که نمی‌توانند به همه آنها پاسخ دهند. در این وضعیت پروکسی از ارائه سرویس باز می‌ماند و یا از سرعتش به نحو محسوسی کاسته میشود. این مسئله بیشتر در مورد پروکسیهای عمومی صادق است ولی اگر شما به یکی از شرکتهای فعال در این زمینه آبونمان بپردازید و اصطلاحاً مشترکشان شوید، ندرتاً با چنین مشکلی برخورد خواهید کرد.

۴. اصولاً وب پروکسی‌ها برای دیدن صفحات وب از طریق مرورگرها طراحی شده‌اند و با سایر نرم‌افزارها سازگاری ندارند. مثلاً شما نمیتوانید یاهو مسنجر (یا هر نرم‌افزار دیگری) را طوری تنظیم کنید تا از طریق وب پروکسی به اینترنت متصل شود.

مقابله با فیلترینگ معکوس

فیلترینگ معکوس محصول تحریمهای ایالات متحده آمریکا بر علیه نظام جمهوری اسلامی است. این تحریمها در ابتدا برای اعمال محدودیتهای مالی و تجاری علیه ایران و چند کشور دیگر وضع شدند، ولی دامنه آنها امروزه به دانلود نرم‌افزار و سایر خدمات رایگان اینترنت در حال گسترش است.

این نوع از فیلترینگ به طور اساسی با فیلترینگی که تا کنون در مورد آن صحبت کردیم متفاوت است. این گونه از فیلترینگ نه توسط دولت ایران، بلکه بوسیله شرکتهای آمریکایی اعمال میشود و اساس آن بر کنترل IP آدرس مشتری توسط وب سایت شرکتهای مذکور استوار است، به طوری که اگر IP آدرس مشتری متعلق به یکی از کشورهای مورد تحریم باشد از ارائه خدمت به او امتناع میشود.

شیوه مقابله با این نوع از فیلترینگ، بر دو رویکرد کلی متکی است: اول، استفاده از خدمات شرکتهای مشابه (غیر آمریکایی) و دیگری تغییر IP آدرس. ذیلاً روشهای مقابله با فیلترینگ معکوس توضیح داده شده‌اند:

تغییر ISP:

همانطور که گفته شد اساس فیلترینگ معکوس بر بلوک کردن IP آدرسهای ایرانی توسط شرکتهای آمریکایی است. به همین جهت، بهترین راه حل، پیدا کردن سرویس‌دهنده اینترنتی هست که IP آدرسهای آن به نام ایران ثبت نشده

باشند. سرویس‌دهندگان تازه تأسیس و سرویس‌دهندگان اینترنتی که پهنای باند خود را از طریق ماهواره یا شرکتهای خارجی تأمین میکنند ممکن است مفید واقع شوند. برای اینکه بفهمید یک IP آدرس به نام چه کشوری ثبت شده است میتوانید از سایتهای زیر کمک بگیرید:

- 2privacy.com
- www.hcidata.co.uk

اگر نتوانستید در داخل کشور ISP مناسبی پیدا کنید ممکن است مجبور شوید از ISPهای خارج از کشور استفاده کنید. به کمک ویندوز XP میتوانید به لیستی از ISPهای کشورهای مختلف دسترسی پیدا کنید. این ISPها عمدتاً رایگان هستند ولی توجه داشته باشید که شما برای اتصال به آنها متحمل هزینه تماس بین‌الملل خواهید شد. در موارد اضطرار و برای کارهای حساسی مانند پرداختهای آنلاین شاید معقولانه‌ترین کار این باشد که به جای قبول مشکلات و ریسک استفاده از پروکسیهای عمومی، هزینه چند دقیقه تماس بین‌الملل را متقبل شوید.

میرورها (Mirrors):

اگر مشکل شما با فیلترینگ معکوس تنها در دانلود فایل یا نرم‌افزار است، برایتان ساده‌تر است تا به جای تغییر IP آدرس، از میرورها استفاده کنید. میرورها، کپی مطالب و فایلهای یک وب سایت در سایتهای دیگر هستند. اگر وب سایت اصلی به شما اجازه دانلود فایل مورد نظرتان را نمیدهد سعی کنید آن فایل را از وب سایتهای دیگر دریافت کنید. برای پیدا کردن میرور مناسب میتوانید از سایت filemirrors.com کمک بگیرید.

شرکتهای مشابه:

اگر شرکتی از فروش محصول یا خدماتش به شما خودداری میکند، منطقی‌ترین کار این است که شما هم سعی نکنید به زور پولتان را به جیب آن شرکت واریز کنید. در عوض سعی کنید محصول یا خدمات مورد نیازتان را از شرکتهای مشابه خریداری کنید. در این میان شرکتهای کانادایی و با یک رتبه پایین‌تر، شرکتهای اروپایی بهترین جایگزینها هستند. ولی به هر حال، گاهی بعضی محصولات (خصوصاً محصولات نرم‌افزاری) فقط توسط شرکتهای آمریکایی عرضه میشود، همچنین محصولات و خدمات این شرکتها در مقایسه با رقبای اروپایی‌شان از کیفیت و قیمت مناسب‌تری برخوردار است.

پروکسی:

پروکسی یک ارتباط غیر مستقیم بین کامپیوتر مشتری با سرور شرکت میزبان ایجاد میکند. این ویژگی باعث میشود تا بتوان از پروکسی برای فائق آمدن بر مشکل فیلترینگ معکوس استفاده کرد. زیرا در این حالت IP آدرس مشتری از دید شرکت میزبان مخفی میماند و در واقع کامپیوتر میزبان به جای IP آدرس حقیقی مشتری، IP آدرس پروکسی را

می‌بیند و چنین تصور میکند که مشتری در کشوری که پروکسی در آن قرار دارد ساکن است. نکات زیر شما را در استفاده از پروکسی راهنمایی میکند:

1. **اگر قصد دارید از پروکسیهای عمومی برای کارهای حساس استفاده کنید، حتماً به خطرات امنیتی استفاده از این گونه پروکسی‌ها توجه داشته باشید. زیرا ممکن است ناخواسته اطلاعات مهم خود را در اختیار هکرها یا دزدان اینترنتی قرار دهید. در واقع پروکسیهای عمومی به هیچ وجه برای کارهای مهمی مانند پرداختهای اینترنتی توصیه نمیشوند. با این حال اگر شما همچنان به استفاده از این پروکسی‌ها مصر هستید از شما میخواهیم یک بار دیگر مطالب مبحث پروکسیها را به دقت مطالعه کنید.**

2. **از آنجایی که برای کارهای حساس نظیر وارد کردن اطلاعات کارت اعتباری از پروتکل اتصال ایمن (SSL) یا رمزنگاری شده استفاده میشود، شما حتماً باید از پروکسیهای HTTPS یا Socks استفاده کنید. پروکسیهای معمولی (HTTP) در این مورد کارایی ندارند. اکثر وب پروکسی‌ها نیز از اتصال ایمن پشتیبانی نمیکنند و برای این منظور مناسب نیستند.**

3. **پروکسی مورد استفاده شما باید از نوع ناشناس (Anonymous) باشد تا IP آدرس حقیقی شما را به سایت میزبان اطلاع ندهد.**

4. **استفاده از پروکسی، دقیقاً همان روشی است که هکرها و سارقان اینترنتی برای شناسایی نشدن از آن استفاده میکنند. به همین جهت بانکها و مؤسسات مالی آنلاین نظیر پی‌پال PayPal به شدت نسبت به استفاده از پروکسی‌ها حساس هستند و چنانچه متوجه شوند برای دسترسی به حساب شما از پروکسی استفاده شده یا اینکه به طور مکرر از IP آدرسهای مختلف به حساب شما دستیابی شده، ممکن است حساب شما را به حال تعلیق درآورند و از شما بخواهند برای فعال کردن مجدد آن با آنها تماس بگرید.**

روشهای پیشرفته مقابله با فیلتر

اگر مطالب ما را تا اینجا دنبال کرده باشید حتماً متوجه شده‌اید که استفاده از پروکسیهای عمومی و سایر روشهای رایگان برای عبور از فیلتر چندان قابل اعتماد نیست. زیرا:

- پروکسیهای عمومی عمر نسبتاً کوتاهی دارند و خیلی زود توسط مخابرات شناسایی و فیلتر میشوند. به علاوه، خیلی از پروکسیهایی که به عنوان پروکسی عمومی در نظر گرفته میشوند در واقع پروکسیهای حفاظت نشده متعلق به شرکتها هستند. به محض این که صاحبان این شرکتها از سوء استفاده از پروکسی خود آگاه شوند آن را خواهند بست.
- اگرچه پروکسیهای عمومی برای گشت و گذار در میان وب سایتها مناسب هستند ولی چنانچه میخواهید از آنها برای کارهای حساسی مثل خرید اینترنتی، وارد کردن اطلاعات کارت اعتباری و پسوردها استفاده کنید باید محتاط باشید زیرا ممکن است صاحبان پروکسی اطلاعات محرمانه شما را سرقت کنند.
- اکثر پروکسیهای عمومی توسط تعداد زیادی از کاربران مورد استفاده قرار میگیرند و به همین علت سرعت مناسبی ندارند و استفاده از آنها موجب کند شدن سرعت اینترنت شما میشود.
- ترفندهایی که مبتنی بر نقاط ضعف سیستم فیلترینگ هستند، مثل روشهای دستکاری URL زیاد معتبر نیستند. زیرا به محض این که مدیران فیلترینگ از این نقاط ضعف آگاهی پیدا کنند آنها را بر طرف کرده و شما مجبور میشوید به دنبال ترفندهای جدید بگردید.

در این وضعیت، شما دو راه بیشتر پیش رو ندارید. یا به همین منوال ادامه دهید و با وضعیت موجود سر کنید و یا این که دست به جیب شده و یکی از روشهای زیر را انتخاب کنید. تجربه نشان داده، وقت و هزینه‌ای را که شما در طول یک سال برای پیدا کردن پروکسیهای عمومی صرف میکنید بیشتر از مبلغی است که برای یکی از روشهای زیر می‌پردازید. البته انتخاب روش مناسب بستگی مستقیم به شرایط و تواناییهای شما دارد. اگر شما یک کاربر باتجربه اینترنت هستید و با مدیریت وب سایت آشنایی دارید، پیشنهاد ما به شما این است که خودتان اقدام به ایجاد یک وب سایت و نصب

پروکسی بر روی آن کنید. این روش علاوه بر اینکه مقرون به صرفه‌تر است، امکانات بیشتری نیز در اختیار شما قرار میدهد. ذیلاً چند روش مطمئن برای عبور از فیلتر توضیح داده شده‌اند:

اگر دوست یا آشنایی در خارج کشور (جایی که سانسور اعمال نمیشود) دارید که یک اتصال دائمی به اینترنت دارد، از او بخواهید بر روی کامپیوترش یک برنامه پروکسی نصب کند. به این ترتیب شما می‌توانید با داشتن IP آدرس کامپیوتر دوستتان و شماره پورت پروکسی از آن استفاده کنید. از آنجایی که این امکان برای اکثر کاربران وجود ندارد، ما نیز به همین حد بسنده کرده و توضیح بیشتری در این مورد نمیدهیم.

راه دیگر این است که به یکی از شرکتهایی که خدمات پروکسی ارائه میدهند آبونمان بپردازید و مشترکشان شوید. از آنجایی که آدرس پروکسیهای اختصاصی این شرکتها تنها در اختیار معدودی از کاربران قرار میگیرد، به ندرت پیش می‌آید که فیلتر شوند و اگر هم چنین اتفاقی بیافتد، شرکت آدرس یک پروکسی جدید را به شما میدهد. مبلغ آبونمان برای شرکتهایی که خدمات پروکسی ارائه میدهند چیزی حدود ۳ تا ۳۰ دلار در ماه است. شرکتهای زیادی در این زمینه فعالیت دارند که اکثراً غربی هستند. از آنجایی که در کشورهای غربی مشکل سانسور وجود ندارد، بیشتر این شرکتها خدمات خود را تحت عنوان حفظ هویت و امنیت در اینترنت (Anonymous or Safe surfing) عرضه میکنند.
سرویس این شرکتها اساساً برای گشت و گذار ناشناس در اینترنت طراحی شده ولی برای فرار از فیلتر نیز کاملاً مناسب است. به طور کلی این شرکتها سرویس خود را به یکی از سه شکل زیر عرضه میکنند:

1. **وب پروکسی: در این حالت به شما یک آدرس اینترنتی داده میشود که با وارد کردن آن در کادر آدرس مرورگرتان به وب پروکسی شرکت مربوطه دسترسی پیدا میکنید. همان طور که در مبحث وب پروکسیها گفته شد، مهمترین مزیت این پروکسی‌ها سهولت استفاده از آنهاست و بزرگترین اشکال آنها نیز این است که فقط برای دیدن صفحات وب از طریق مرورگرها مناسبند و با سایر نرم‌افزارها سازگاری ندارند.**
2. **پروکسیهای HTTP و Socks: استفاده از این پروکسی‌ها نیازمند اندکی تنظیمات است و شما باید مرورگر و سایر برنامه‌هایتان را طوری تنظیم کنید تا به جای ارتباط مستقیم با اینترنت، از طریق پروکسی متصل شوند. پروکسیهای HTTP فقط برای دیدن صفحات وب مناسب هستند در حالی که پروکسیهای ساکس از کلیه پروتکلهای اینترنت پشتیبانی میکنند و با نرم‌افزارهای بیشتری سازگاری دارند.**
3. **VPN: این عبارت مخفف کلمات شبکه خصوصی مجازی (Virtual Private Network) میباشد. در این حالت بین کامپیوتر شما و سرور شرکت مربوطه یک تونل امن بوجود می‌آید و کلیه تبادلات اینترنتی شما به صورت رمزنگاری شده از طریق این تونل رد و بدل میشود. این روش از اعتبار بسیار بالایی برخوردار است و با کمک آن فعالیتهای اینترنتی شما به هیچ عنوان قابل ردیابی نیست. اشکال این روش این است که شما برای استفاده از آن نیاز به نصب نرم‌افزار و انجام مقداری تنظیمات دارید.**

ذیلاً اسامی تعدادی از شرکتهایی که خدمات پروکسی ارائه میدهند آمده است. قبل از خرید، در مورد سرویس این شرکتها کاملاً تحقیق کنید و مطمئن شوید که در منطقه شما قابل دسترسی است.

- Anonymizer.com
- FindNot.com
- Anonybrowser
- Secure-Tunnel
- Guardster
- Cotse.Net
- IDzap
- NoMoreLimits

راه حل سوم این است که خودتان یک وب سایت بزنید و روی آن وب پروکسی نصب کنید. برای این کار لازم است شما یک دامنه (Domain) بنام خودتان ثبت کنید و از یک شرکت که خدمات میزبانی وب ارائه میدهد یک اشتراک بخرید. ممکن است در نگاه اول این کار به نظرتان پرخرج بیاید ولی ابداً چنین نیست . در واقع شما با کمتر از ۱۰ دلار (حدود ۱۰ هزار تومان) در سال می‌توانید صاحب یک وب سایت شوید. برای کمتر شدن هزینه‌ها می‌توانید این کار را مشترکاً با دو یا چند نفر از دوستانتان انجام دهید. همچنین ممکن است خیلی از شما یک وب سایت داشته باشید ولی نمیدانید سایت شما چه از چه قدرت نهفته‌ای برخوردار است. برای ایجاد یک وب سایت و داشتن یک پروکسی اختصاصی لازم است سه مرحله را طی کنید:

۱. **قدم اول برای ایجاد یک وب سایت، ثبت یک دامین هست. برای اطلاعات بیشتر در این زمینه به قسمت "راهنمای ثبت دامنه و انتخاب میزبان وب" مراجعه کنید.**
۲. **بعد از این که یک دامنه را بنام خود به ثبت رساندید، در قدم دوم لازم است برای وب سایتتان یک میزبان (وب هاست) بیابید. برای اطلاعات بیشتر در این زمینه به قسمت "راهنمای ثبت دامنه و انتخاب میزبان وب" مراجعه کنید.**
۳. **هنگامی که وب سایت شما آماده شد، در سومین قدم، شما باید بر روی آن یک برنامه وب پروکسی نصب کنید. برنامه‌های وب پروکسی در واقع اسکریپت‌هایی (Script) هستند که به زبانهای برنامه نویسی تحت وب مثل Perl و PHP نوشته شده‌اند. در ادامه دو تا از بهترین اسکریپت‌های موجود معرفی شده‌اند:**

۱. **پروکسی جیمز مارشال (James Marshall CGI-Proxy):**

این اسکریپت، بهترین اسکریپتی هست که در دسترس عموم قرار دارد و در واقع اکثر اسکریپت‌های دیگر بر مبنای آن نوشته شده‌اند. نویسنده آن، آقای جیمز مارشال، متن این اسکریپت را به زبان Perl نوشته است. این اسکریپت قابلیتهای

فراوانی دارد و از پروتکلهای HTTP و FTP پشتیبانی میکند. در نسخه جدید آن قابلیت پشتیبانی از جاوا هم به آن اضافه شده است. برای اطلاعات بیشتر به قسمت "راهنمای نصب پروکسی جیمز مارشال" مراجعه کنید.

۲. پی اچ پروکسی (PHProxy):

این اسکریپت که به زبان PHP است، در اصل بر مبنای پروکسی جیمز مارشال نوشته شده ولی نسبت به آن ساده‌تر است و تنظیمات کمتری دارد. برای اطلاعات بیشتر به قسمت "راهنمای نصب و تنظیمات پروکسی PHProxy" مراجعه کنید.

در آخر، تذکر این نکته ضروری است که این اسکریپت‌ها باید بر روی سرور نصب و اجرا شوند و شما نمی‌توانید آنها را مستقیماً از روی کامپیوتر شخصی خودتان اجرا کنید.

راهنمای ثبت دامین و میزبانی وب

امروزه با پیشرفت تکنولوژی و پایین آمدن قیمت تجهیزات، هزینه ایجاد یک وب سایت شخصی به طرز باور نکردنی کاهش یافته است به طوری اکنون شما میتوانید با کمتر از ۱۰ دلار در سال صاحب یک وب سایت شوید. داشتن یک وب سایت امکانات زیادی در اختیار شما میگذارد از جمله:

۱. دارای یک دامین میشوید که به نام خود شما ثبت شده و در تمام دنیا قابل دسترسی است.

۲. بسته به وب هاستی که انتخاب میکنید، تعدادی آدرس اختصاصی ایمیل در اختیارتان قرار میگیرد که می‌توانید آنها را به دوستان و آشنایانتان بدهید. غالباً این ایمیل‌ها POP3 و SMTP هستند، چیزی که اکثر فراهم کنندگان ایمیل رایگان (مثل یاهو) بابت آن از شما طلب پول میکنند.

۳. مقداری فضای ذخیره سازی به شما تعلق میگیرد که می‌توانید از آن برای انتشار مطالب، خاطرات و عکسهایتان استفاده کنید.

۴. مهمتر از همه، شما می‌توانید بر روی وب سایت خود یک وب پروکسی نصب کنید و از شر فیلترینگ خلاص شوید.

برای ایجاد یک وب سایت لازم است شما دو کار را انجام دهید. اول یک دامین را به ثبت برسانید و دوم یک میزبان وب (وب هاست) برای وب سایتتان انتخاب کنید. در ادامه روش انجام این کارها آمده است.

ثبت دامین (Domain Registration):

قدم اول در ایجاد یک وب سایت ثبت یک دامین هست. دامین در واقع همان نام سایت شماست، چیزی شبیه "www.YourSite.com" . شرکتهای زیادی وجود دارند که دامین ثبت میکنند و قیمتی در حدود ۳ تا ۱۵ دلار در سال دارند. نام تعدادی از این شرکتها در زیر آمده است:

- Yahoo Smalbusiness
- NetFirms
- 1 and 1
- VERIO
- Register.Com
- IPOWER.Com
- ValueWeb.com
- MyDomains.com
- Fxdomains.com

نکات زیر شما را در خرید دامین کمک میکند:

۱. **دامینهای رایگان مثل tk. مناسب نیستند، چون امکان مدیریت دامین را به شما نمیدهند.**

۲. **از دامین‌های ir. استفاده نکنید زیرا تحت نظارت جمهوری اسلامی است و می‌توانند در صورت صلاحدید، وب سایت شما را تعطیل و خودتان را تحت تعقیب قرار دهند.**

۳. **اگر خدمات ثبت دامین و میزبانی وب را از دو شرکت جداگانه تهیه میکنید، مطمئن شوید که شرکت ثبت دامین امکان مدیریت دامین (Domain Management) را به شما میدهد. اغلب شرکتها این امکان را واگذار میکنند.**

۴. **بعضی وب هاستها به همراه خدمات میزبانی وب خود یک یا چند دامین را به رایگان در اختیار شما قرار میدهند و شما نیاز به پرداخت وجه جداگانه‌ای بابت دامین ندارید. لذا قبل از خرید دامین ابتدا وب هاست خود را مشخص کنید و تنها در صورت نیاز اقدام به خرید جداگانه دامین کنید.**

میزبانی وب:

بعد از این که دامین خود را ثبت کردید نوبت به پیدا کردن یک میزبان وب میرسد. بهتر است خدمات میزبانی وب را از همان شرکتی بگیرید که دامین خود را ثبت کرده‌اید. این شرکتها قیمت نسبتاً بالایی دارند که ممکن است برای کاربران خانگی خیلی مناسب نباشد ولی به هر حال خدمات آنها از کیفیت و اعتبار بالایی برخوردار است. نکات زیر به شما در انتخاب میزبان وب مناسب کمک میکند:

۱. شرکتهایی که خدمات میزبانی وب رایگان ارائه میکنند مناسب نیستند. چون این شرکتها از اسکریپت‌های CGI پشتیبانی نمیکنند و اگر هم بکنند اسکریپت‌های پروکسی روی آنها کار نمیکند (چون سوکت خروجی بسته است).

۲. مطمئن شوید وب هاست شما از اسکریپت‌های CGI و PHP پشتیبانی میکند.

۳. مطمئن شوید سوکت خروجی (Outgoing Socket) برای اسکریپت‌های CGI باز است. بعضی وب هاستها برای جلوگیری از نصب برنامه‌های پروکسی سوکت خروجی را میبندند ولی در غالب موارد این سوکت باز است.

۴. اگرچه اسکریپتهای پروکسی بسیار کوچک هستند (کمتر از ۳۰۰ کیلو بایت) و نیاز به فضای ذخیره سازی زیادی ندارند ولی توصیه میشود حداقل فضای وب سایتتان ۱۰ تا ۵۰ مگابایت باشد. برای استفاده شخصی معمولاً پهنای باند ۱۰۰ تا ۲۰۰ مگابایت در ماه کافی است ولی اگر میخواهید از پروکسی با دوستانتان مشترکاً استفاده کنید، به نسبت به پهنای باند بیشتری نیاز خواهید داشت.

۵. وب هاست شما باید خارج از منطقه فیلترینگ باشد. لذا کسانی که در داخل کشور اقدام به ارائه خدمات میزبانی وب میکنند مناسب نیستند. البته خیلی از شرکتهایی که در ایران اقدام به ارائه خدمات میزبانی وب میکنند در واقع نمایندگان فروش شرکتهای خارجی هستند. سرویس ارائه شده توسط این شرکتها ممکن است مناسب باشد ولی این نکته را مد نظر داشته باشید که این شرکتها تحت نظارت جمهوری اسلامی هستند و ممکن است به دستور مقامات حکومتی وب سایت شما را تعطیل کنند.

۶. بسیاری از وب هاستها از این که بر روی سرورشان پروکسی نصب شود خوششان نمی‌آید. زیرا برنامه‌های پروکسی فشار زیادی را (چه از لحاظ پردازش و چه از نظر ترافیک) بر سرور وارد می‌کنند. بنابراین سعی کنید از عمومی کردن پروکسیتان اجتناب کنید و از دسترسی افراد متفرقه به آن بوسیله پسورد جلوگیری نمایید. از طرف دیگر عمومی کردن پروکسی، آن را در معرض خطر فیلتر شدن قرار میدهد.

برای پیدا کردن وب هاست مناسب به یکی از سایتهای زیر بروید. در آنجا میتوانید وب هاستهای مختلف را بر اساس قیمت و سایر ویژگیها مورد جستجو قرار دهید. در خرید، تنها قیمت را ملاک قرار ندهید بلکه به کیفیت خدمات و اعتبار شرکت فروشنده نیز توجه داشته باشید. مشکل دیگری که ممکن است به آن برخورد کنید پرداخت وجه است که برای حل آن از راهنمائیهای مبحث فیلترینگ معکوس بهره بگیرید.

- FindmyHosting.com
- WebhostingStuff.com

راهنمای نصب و تنظیمات پی اچ پروکسی

پی اچ پروکسی (PHProxy) یک اسکریپت نوشته شده به زبان PHP است و در طراحی آن از پروکسی جیمز مارشال الهام گرفته شده است. ساختاری ساده‌تر دارد و نسبت به پروکسی جیمز مارشال از تنظیمات کمتری برخوردار است. این اسکریپت فقط از پروتکل HTTP پشتیبانی میکند ولی به گفته طراحش به زودی قابلیت پشتیبانی از FTP نیز به آن افزوده میشود. این اسکریپت باید بر روی سروری که از PHP نسخه ۴,۲ و بالاتر پشتیبانی میکند نصب و اجرا گردد. همچنین وضعیت Safe Mode برای اسکریپتهای PHP باید غیر فعال باشد. برای نصب آن مراحل زیر را طی کنید:

1. **فایل فشرده اسکریپت را به کامپیوتر خود دانلود کنید. (دریافت فایل از سایت اصلی یا سایت نوفیلتر)**
2. **فایل را از حالت فشرده خارج کنید.**
3. **فولدر phproxy را به دایرکتوری اصلی (معمولاً public_html) سایت خود کپی کنید.**
4. **به شاخه phproxy بروید و فایل index.php را پیدا کنید.**
5. **مجوز (Permissions) این فایل را به ۶۴۴ تغییر دهید.**
6. **از درون مرورگر خود فایل index.php را صدا کنید. برای این کار در کادر آدرس مرورگرتان تایپ کنید:**

http://www.YourSite.com/phproxy/index.php

اگر مراحل فوق را با موفقیت انجام داده باشید، صفحه اصلی PHProxy نمایش داده میشود و شما میتوانید گشت و گذار در اینترنت را با کمک آن شروع کنید. همه تنظیمات PHProxy از صفحه اصلی در دسترس هستند. این تنظیمات به همراه شرح مختصری از هر کدام ذیلاً آمده‌اند:

- **Include Form: این قسمت مشخص میکند که آیا باید کادر آدرس PHProxy در بالای تمام صفحات نمایش داده شود یا نه.**
- **Remove Scripts: اسکریپتهای جاوا را از صفحه حذف میکند. اگر این قسمت را تیک بزنید ممکن است بعضی صفحات درست نمایش داده نشوند.**
- **Accept Cookies: پذیرش کوکی. اگر تیک را از جلوی آن بردارید با وب سایتهایی که نیاز به Log-in دارند به مشکل برمیخورید.**
- **Show Images: نشان دادن تصاویر. اگر تیک این قسمت را بردارید، عکسها و گرافیکها از صفحه حذف میشوند و فقط متن نمایش داده میشود. این گزینه برای زمانی که میخواهید در پهنای باند خود صرف جویی کنید مفید است.**
- **Show Refer: اگر این قسمت تیک نخورده باشد، پروکسی بخش refer را از HTML Header حذف میکند. به این ترتیب، وب سایتی که در حال مشاهده آن هستید متوجه نمیشود شما قبلاً از کدام سایت بازدید میکردید.**

- Rotate13: از روش rot-13 برای درهم ریختن URL استفاده میکند. برای عبور از فیلتر لازم است شما حداقل یکی از دو گزینه rot-13 یا base64 را انتخاب کنید.
- Base64: از روش base64 برای درهم ریختن URL استفاده میکند. برای عبور از فیلتر لازم است شما حداقل یکی از دو گزینه rot-13 یا base64 را انتخاب کنید.
- Strip Meta: متا تگ‌های HTML را حذف میکند.
- Strip Title: عنوان صفحه را از نوار عنوان (Title bar) حذف میکند.
- Session Cookies: تنها کوکی‌های دوره‌ای را ذخیره میکند.
- New Window: آدرس مورد نظر را در یک صفحه جدید مرورگر باز میکند.

راهنمای نصب پروکسی جیمز مارشال (CGI-Proxy)

پروکسی جیمز مارشال (James Marshall CGI-Proxy) یکی از بهترین اسکریپتهایی هست که در دسترس عموم قرار دارد. این اسکریپت توسط آقای جیمز مارشال به زبان پرل (Perl) نوشته شده است. خوشبختانه نویسنده مرتباً آن را آپدیت کرده و قابلیتهای جدیدی به آن می‌افزاید. در حال حاضر این پروکسی از پروتکلهای HTTP، HTTPS و FTP پشتیبانی میکند و در نسخه جدید قابلیت پشتیبانی از جاوا به صورت بتا به آن افزوده شده است. مزیت دیگر این اسکریپت این است که نویسنده آن را در درون سورس برنامه کاملاً توضیح داده است. این مسئله می‌تواند برای دانشجویان و علاقمندان به یادگیری پرل بسیار آموزنده باشد. سروری که میخواهید این اسکریپت را بر روی آن اجرا کنید باید از قابلیتهای زیر برخوردار باشد:

- پشتیبانی از پرل نسخه ۵,۸ یا بالاتر (Perl 5.8).
- پشتیبانی از اسکریپتهای NPH-CGI.
- سوکت خروجی برای اسکریپتهای CGI باز باشد (Outgoing Socket Enabled).

نصب این اسکریپت نسبتاً آسان است. شما می‌توانید به دو روش دستی (Manual) و یا از طریق نصاب (Installer) آن را نصب کنید. برای نصب دستی مراحل زیر را طی کنید :

۱. فایل فشرده اسکریپت را به کامپیوتر خود دانلود کنید. (دریافت فایل از سایت اصلی یا سایت نوفیلتر)
۲. فایل را از حالت فشرده خارج سازید.

۳. **فایل nph-proxy.cgi را به درون شاخه cgi-bin بر روی سرور خود آپلود کنید.**

۴. **مجوز (Permission) فایل را به ۷۵۵ تغییر دهید.**

۵. **فایل مذکور را از درون مرورگر خود صدا کنید. برای این کار در کادر آدرس مرورگرتان تایپ کنید:**

http://www.YourSite.com/cgi-bin/nph-proxy.cgi

اگر مراحل فوق را درست انجام داده باشید، صفحه پروکسی جیمز مارشال به نمایش درمی‌آید و شما میتوانید به کمک آن، گشت و گذار در اینترنت را شروع کنید. اگرچه نصب پروکسی جیمز مارشال آسان است ولی ممکن است بعضی کاربران مبتدی به مشکل بر بخورند. اگر چنین است نگران نباشید؛ وب سایتی وجود دارد که به صورت اتوماتیک پروکسی را برای شما نصب میکند. برای این کار مراحل زیر را طی کنید:

۱. **به این آدرس مراجعه کنید.**

۲. **از لیست موجود آخرین نگارش پروکسی را انتخاب کنید و کلید Next را بزنید.**

۳. **در صفحه بعد، روی دکمه Accept کلیک کنید.**

۴. **حال به یک فرم بر میخورید. شما فقط نام سایت به همراه نام کاربری و رمزتان را وارد کنید و بقیه قسمتها را خالی بگذارید (جدول ۳). نصاب سعی میکند آنها را بر اساس تنظیمات پیش‌فرض تکمیل کند. اگر سرور شما از تنظیمات استاندارد پیروی نمیکند و تنظیمات خاص خود را دارد، لازم است این قسمتها را خودتان به صورت دستی پر کنید. برای کسب اطلاعات با وب هاست خود تماس بگیرید.**

Your Website	در این قسمت آدرس وب سایت خودتان را بنویسید. مثلا http://www.YourSite.com/
FTP User-Name	در این قسمت نام کاربری وب سایت خود را بنویسید.
FTP Password	در این قسمت پسوردی که با آن به سایت‌تان دسترسی پیدا میکنید را بنویسید.
FTP Server	خالی بگذارید.
FTP Path	خالی بگذارید.
Perl Path	خالی بگذارید.
Perl cgi Extension	خالی بگذارید.

جدول ۳ – نحوه پر کردن فرم نصاب پروکسی جیمز مارشال.

۵. در این مرحله نصاب (Installer) وب سایت شما را بررسی کرده و توضیحات مختصری را در مورد آن نشان میدهد. روی دکمه Finish کلیک کنید.

۶. اگر نصب با موفقیت انجام شود در صفحه بعدی به یک پیام تبریک (Congratulations) برخورد میکنید. حال روی لینکی که در این صفحه وجود دارد کلیک کنید تا به صفحه پروکسی بروید. به طور پیش‌فرض، پروکسی در آدرس زیر قرار میگیرد:

http://www.YourSite.com/cgiproxy/nph-proxy.pl

بعد از این که پروکسی با موفقیت نصب شد بهتر است پسورد وب سایتتان را عوض کنید. ضمناً توجه داشته باشید که پروکسی جیمز مارشال، در شکل اولیه، برای عبور از فیلتر مناسب نیست. برای این که شما بتوانید از پروکسی جیمز مارشال برای فرار از فیلتر استفاده کنید لازم است یکی از کارهای زیر را انجام دهید:

۱. آن را از روی یک سرور امن اجرا کنید. سرور امن، سروری است که از ارتباطات رمزنگاری شده (SSL) پشتیبانی میکند. در این حالت آدرس وب سایت شما به جای http با https شروع میشود. این امکان، به طور معمول، همراه با خدمات وب هاستینگ ارائه نمیشود و شما برای بهره‌مندی از آن باید مبلغی را جداگانه پرداخته و یک گواهینامه SSL خریداری کنید. با این حال بعضی وب هاستها به شما این امکان را میدهند که از گواهینامه آنها به صورت اشتراکی استفاده کنید. برای اطلاعات بیشتر با شرکت وب هاست خود تماس بگیرید. اگر برایتان مقدور بود، از این روش استفاده کنید، زیرا در این حالت کلیه تبادلات اینترنتی شما به صورت رمزنگاری شده در می‌آید و غیر قابل ردیابی میشود.

۲. پروکسی را بر روی پورتی به غیر از پورت ۸۰ قرار دهید. مثلاً با فرض این که پروکسی بر روی پورت ۸۰۰۰ تنظیم شده باشد، URL دسترسی به پروکسی به صورت زیر در می‌آید. اکثر وب هاستها این امکان را واگذار نمیکنند.

http://www.YourSite.com:8000/cgi-bin/nph-proxy.cgi

۳. متن اسکریپت را کمی تغییر دهید و کاری کنید که پروکسی URLها را به صورت درهم ریخته درآورد. برای اطلاعات بیشتر به قسمت "راهنمای تنظیمات پروکسی جیمز مارشال" مراجعه کنید. اگر انجام این کار برایتان سخت است یا حوصله آن را ندارید، میتوانید به جای نسخه اصلی از نسخه تغییر یافته پروکسی استفاده کنید. ما این تغییرات را در آن انجام داده‌ایم. برای دریافت نسخه تغییر یافته به سایت نوفیلتر مراجعه کنید.

تنظیمات پروکسی جیمز مارشال

تنظیمات این پروکسی به دو دسته تقسیم میشود. یکی تنظیمات ساده که از طریق صفحه اصلی پروکسی قابل دسترسی هستند و دیگری تنظیمات پیشرفته که برای تغییر آنها باید متن اسکریپت را ویرایش کنید.

تنظیمات ساده پروکسی:

این تنظیمات از طریق صفحه اصلی پروکسی و فرم بالای صفحه در دسترس هستند. برای تغییر آنها کافیست آنها را تیک بزنید یا علامت تیک را از کنار آنها بردارید.

- Remove all cookies: **اگر این قسمت تیک بخورد پروکسی از پذیرش کوکی امتناع خواهد کرد.**
- Remove all scripts: **اسکریپتهای جاوا را از صفحه حذف میکند. اگر این قسمت را تیک بزنید ممکن است بعضی صفحات درست نمایش داده نشوند.**
- Remove ads: **آگهی‌های تبلیغاتی را از صفحه حذف میکند.**
- Hide referrer information: **بخش** refer **را از** HTML Header **حذف میکند. به این ترتیب، وب سایتی که در حال مشاهده آن هستید متوجه نمیشود شما قبلاً از کدام سایت بازدید میکردید.**
- Show URL entry form: **این قسمت مشخص میکند که آیا باید کادر آدرس پروکسی به بالای تمام صفحات اضافه شود یا نه.**
- Manage cookies: **با کلیک روی این قسمت وارد صفحه مدیریت کوکی‌ها میشوید. در آنجا می‌توانید کوکی‌ها را مشاهده و در صورت نیاز، آنها را حذف کنید.**

تنظیمات پیشرفته:

این تنظیمات برعکس تنظیمات قبلی از طریق صفحه اصلی پروکسی در دسترس نیستند و برای تغییر آنها باید متن اسکریپت را ویرایش کنید. برای این کار، لازم است شما متن اسکریپت (فایل nph-proxy.cgi**) را در یک ویرایشگر متن مثل نوت‌پد** (Notepad) **باز کنید و قسمتهایی را که ذیلاً گفته میشود در آن پیدا کرده و تغییر دهید. مهمترین تغییری که در متن اسکریپت باید داده شود مربوط به کد کردن (درهم ریختن)** URL **است؛ زیرا برای عبور از فیلتر ضروری میباشد ولی باقی تنظیمات، اختیاری هستند. اگر به هر دلیلی، این قسمت به نظرتان مشکل می‌آید و یا فرصت انجام آن را ندارید، می‌توانید از خواندن قسمت زیر صرف نظر کرده و در عوض بجای فایل اصلی از فایل تغییر یافته پروکسی استفاده کنید.**

پروکسی جیمز مارشال تنظیمات متعددی دارد و خوشبختانه طراح آن، آنها را در درون متن اسکریپت کاملاً توضیح داده است. ما در اینجا تنها تنظیمات مهم و ضروری را توضیح میدهیم ولی چنانچه شما به اطلاعات بیشتری نیاز داشتید می‌توانید به توضیحات نویسنده در درون متن اسکریپت مراجعه کنید. پارامترهایی را که شما میتوانید تغییر دهید در جدول زیر آمده‌اند. عدد 0 نشانگر غیرفعال بودن و عدد 1 نشانگر فعال بودن آن پارامتر است و اعداد داخل کروشه، مقادیر پیش‌فرض را نشان میدهند.

$TEXT_ONLY [0]	فقط متن: اگر فعال باشد تصاویر و مولتی‌مدیا از صفحه حذف میشوند.
$REMOVE_COOKIES [0]	حذف کوکی‌ها: اگر فعال باشد پروکسی از قبول کوکی خودداری میکند.
$REMOVE_SCRIPTS [1]	حذف کلیه اسکریپت‌ها: کلیه اسکریپت‌ها را از صفحه حذف میکند.
$FILTER_ADS [0]	حذف تبلیغات: آگهی‌های تبلیغاتی را از صفحه حذف میکند.
$HIDE_REFERER [1]	حذف ارجاع: بخش refer را از HTML Header حذف میکند.
$REMOVE_TITLES [0]	حذف عنوان: عنوان صفحه را از نوار عنوان (Title bar) حذف میکند.
$INSERT_ENTRY_FORM [1]	نمایش کادر آدرس: کادر آدرس را در بالای همه صفحات نمایش میدهد.
$ALLOW_USER_CONFIG [1]	اجازه به کاربر برای تغییرات: اگر غیر فعال شود کاربر نمی‌تواند تنظیمات اولیه را تغییر دهد.
$MINIMIZE_CACHING [0]	جلوگیری از کش کردن مرورگر: از این که مرورگر صفحات را بایگانی کند جلوگیری میکند.
$OVERRIDE_SECURITY [0]	نادیده گرفتن امنیت: اگر فعال باشد، شما می‌توانید صفحات رمزنگاری شده (https) را از طریق یک اتصال غیر امن (http) دریافت کنید. اخطار! در تغییر این پارامتر محتاط باشید.
$NOT_RUNNING_AS_NPH [0]	اجرا در حالت غیر NPH: اگر سرور شما از اسکریپتهای NPH پشتیبانی نمیکند این پارامتر ر افعال کنید.
sub proxy_encode {}, proxy_decode {}	درهم ریختن URL: این قسمت URL را به صورت کد شده درمی‌آورد. به ادامه مبحث رجوع شود.
$USER_AGENT [none]	نوع مرورگر: نوع مرورگری را که به اطلاع سایت هدف میرسد را مشخص میکند.
$MAX_REQUEST_SIZE [4194304 = 4 Meg]	حداکثر اندازه فایل درخواستی را مشخص میکند.

جدول ۴- در این جدول پر کاربردترین تنظیمات پروکسی جیمز مارشال لیست شده‌اند. اگر به اطلاعات بیشتری در مورد این تنظیمات نیاز دارید به توضیحات نویسنده در درون متن اسکریپت مراجعه کنید.

درهم ریختن URL:

در درون متن اسکریپت دو روتین (Routine) برای درهم ریختن URL وجود دارد که هر دو به طور پیش‌فرض غیر فعال هستند. این روتین‌ها ذیلاً با رنگهای قرمز و آبی نشان داده شده‌اند. برای فعال کردن آنها، قسمتهای گفته شده را در درون متن اسکریپت پیدا کنید و علامت کامنت (# یا //) را از مقابل یکی از روتین‌ها بردارید. شما می‌توانید هر دو روتین را با هم فعال کنید ولی این کار توصیه نمیشود. در زیر نمونه‌ای از روش درهم ریختن URL توسط این دو روتین آمده است:

http://proxy.no-filter.com/nph-proxy.cgi/010110A/http/www.google.com/

http://proxy.no-filter.com/nph-proxy.cgi/010010A/uggc/jjj.tbbtyr.pbz/

http://proxy.no-filter.com/bypass/nph-proxy.cgi/010010A/687474702f7777772e676f6f676c652e636f6d2f

ابتدا در داخل متن اسکریپت، قسمت زیر را پیدا کرده و علامت # از مقابل یکی از روتین‌ها بردارید.

```
sub proxy_encode {
   my($URL)= @_ ;
   $URL=~ s#^([\w+.-]+)://#$1/# ;            # http://xxx -> http/xxx
#    $URL=~ s/(.)/ sprintf('%02x',ord($1)) /ge ;   # each char -> 2-hex
#    $URL=~ tr/a-zA-Z/n-za-mN-ZA-M/ ;          # rot-13

   return $URL ;
}

sub proxy_decode {
   my($enc_URL)= @_ ;

#    $enc_URL=~ tr/a-zA-Z/n-za-mN-ZA-M/ ;      # rot-13
#    $enc_URL=~ s/([\da-fA-F]{2})/ sprintf("%c",hex($1)) /ge ;
   $enc_URL=~ s#^([\w+.-]+)/#$1://# ;        # http/xxx -> http://xxx
   return $enc_URL ;
```

سپس در درون متن اسکریپت، کمی پایین‌تر بروید و قسمت زیر را پیدا کنید. علامت // از جلوی روتین همرنگ آن در قسمت قبل بردارید.

```
function _proxy_jslib_proxy_encode(URL) {
   URL= URL.replace(/^([\w\+\.\-]+)\:\/\//, '$1/') ;
//    URL= URL.replace(/(.)/g, function (s,p1);
//    URL= URL.replace(/([a-mA-M])|[n-zN-Z]/g, function (s,p1);

   return URL ;
}

function _proxy_jslib_proxy_decode(enc_URL) {
//    enc_URL= enc_URL.replace(/([a-mA-M])|[n-zN-Z]/g, function (s,p1);
//    enc_URL= enc_URL.replace(/([\da-fA-F]{2})/g, function (s,p1);
   enc_URL= enc_URL.replace(/^([\w\+\.\-]+)\//, '$1://') ;
```

```
   return enc_URL ;
```

با فرض این که شما روتین قرمز را فعال کرده باشید، اسکریپت به صورت زیر درمی‌آید:

```
sub proxy_encode {
   my($URL)= @_ ;
   $URL=~ s#^([\w+.-]+)://#$1/# ;              # http://xxx -> http/xxx
   $URL=~ s/(.)/ sprintf('%02x',ord($1)) /ge ;    # each char -> 2-hex
 #   $URL=~ tr/a-zA-Z/n-za-mN-ZA-M/ ;           # rot-13

   return $URL ;
}

sub proxy_decode {
   my($enc_URL)= @_ ;

#    $enc_URL=~ tr/a-zA-Z/n-za-mN-ZA-M/ ;       # rot-13
   $enc_URL=~ s/([\da-fA-F]{2})/ sprintf("%c",hex($1)) /ge ;
   $enc_URL=~ s#^([\w+.-]+)/#$1://# ;          # http/xxx -> http://xxx
   return $enc_URL ;
```

```
function _proxy_jslib_proxy_encode(URL) {
   URL= URL.replace(/^([\w\+\.\-]+)\:\/\//, '$1/') ;
   URL= URL.replace(/(.)/g, function (s,p1)
//   URL= URL.replace(/([a-mA-M])|[n-zN-Z]/g, function (s,p1)

   return URL ;
}

function _proxy_jslib_proxy_decode(enc_URL) {
//  enc_URL= enc_URL.replace(/([a-mA-M])|[n-zN-Z]/g, function (s,p1);
   enc_URL= enc_URL.replace(/([\da-fA-F]{2})/g, function (s,p1) ;
   enc_URL= enc_URL.replace(/^([\w\+\.\-]+)\//, '$1://') ;
   return enc_URL ;
```

پیشگیری از فیلترینگ

ترفندهای انتشار مطالب

در حالیکه عده‌ای در تلاشند تا خود از چنگال سانسور نجات دهند، عده‌ای دیگر در این فکرند تا چگونه مطالب خود را به مخاطبانشان در کشورهای سانسور زده برسانند. راهنمائیهای زیر به شما کمک میکند تا مطالب خود را به نحوی منتشر کنید تا کمتر دچار فیلترینگ شوید و اگر هم گرفتار فیلترینگ شدید به شما می‌آموزد تا چگونه مجدداً وب سایت خود را زنده کنید:

سرور و مرکز مدیریت سایت خود را در یک کشور آزاد قرار دهید:

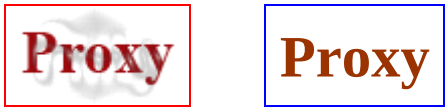
اگر شما دارای یک سرور اختصاصی هستید، تجهیزات و مرکز مدیریت سایت خود را در خارج از حیطه قدرت سانسورگران قرار دهید و چنانچه سایت شما توسط یک شرکت ثالث میزبانی میشود، سعی کنید میزبان وب خود را از یک کشور آزاد انتخاب کنید. در این میان، کشورهای آزادی که روابط حسنه‌ای با کشور متبوعتان ندارند مناسب‌تر هستند. به این ترتیب تنها کاری که از دست سانسورگران ساخته است این است که جلوی دسترسی به وب سایت شما را از داخل کشور بگیرند ولی نمیتوانند تجهیزات شما را مصادره کرده یا به خودتان آسیبی برسانند.

برای سایت خود میرور ایجاد کنید:

میرور (Mirror) به یک کپی از محتویات یک وب سایت گویند که در یک محل دیگر قرار داده شده است. هرچه یک مطلب، میرورهای بیشتری داشته باشد و به صورت گسترده تری پخش شده باشد امکان فیلتر کردن آن کمتر میشود. اگر شما مطلب جالبی را به زبان فارسی نوشته‌اید، لازم نیست زیاد نگران ایجاد میرور برای آن باشید زیرا خیلی زود بسیاری از اشخاص آن را در وب سایتها و وبلاگهای خود کپی خواهند کرد. تنها اشکال کار در این است که آنها نام شما را با نام خودشان عوض میکنند.

مطالب حساس را مخفی کنید:

بسیاری از سانسورگران برای شناسایی سایتهای غیرمجاز از یک سری برنامه کامپیوتری بنام خزنده (Crawler) استفاده میکنند. کار این خزنده‌ها این است که در درون وب سایتها بخزند و محتویات آنها را از لحاظ کلمات و عبارات غیرمجاز مورد بررسی قرار دهند و چنانچه چنین کلماتی پیدا کردند آدرس آن سایت را به لیست سیاه بیافزایند. این خزنده‌ها تنها برای تجزیه و تحلیل متون طراحی شده‌اند و از درک نوشته‌هایی که به صورت تصویر هستند عاجز می‌مانند. اگر در وب سایت شما عباراتی وجود دارد که فکر میکنید واکنش این خزنده ها را برمی‌انگیزد، سعی کنید آن عبارات را در قالب تصاویر مخفی کنید.



شکل۳- در قسمت سمت راست کلمه "پروکسی" به صورت متن (Text) نوشته شده و در چپ، همان کلمه در قالب تصویر (Image) آمده است. اگرچه انسانها هر دو کلمه را بدون هیچ مشکلی میخوانند ولی خزنده‌ها از شناسایی کلماتی که به صورت تصویر هستند ناتوانند.

یک نسخه از مطالب مهم سایت خود را به صورت یک فایل مجتمع درآورید:

در حالت عادی، برای این که خوانندگان بتوانند کلیه مطالب وب سایت شما را بخوانند لازم است مرتباً بر روی لینکهای سایت شما کلیک کنند یا اصطلاحاً در وب سایت شما به گشت و گذار (Browse) بپردازند. این کار برای کاربرانی که از داخل کشورهای سانسورزده و به کمک پروکسی به سایت شما دسترسی پیدا کرده‌اند کمی مشکل است. سعی کنید یک نسخه از مطالب مهم سایت خود را به صورت مجتمع درآورید و آن را در قالب یک فایل (مثل PDF یا Word) منتشر کنید. به این ترتیب کاربران میتوانند فایل مذکور را بر روی کامپیوتر خود دانلود کنند و سپس به مطالعه آن بپردازند. همچنین این کار اجازه میدهد تا مطالب شما خیلی راحت بین کاربران و نیز سایر سایتهای اینترنتی گسترش پیدا کند.

مطالب خود را از طریق شبکه‌های P2P به اشتراک بگذارید:

همانطور که در مبحث ترفندهای عبور از فیلتر گفته شد شبکه‌های نظیر به نظیر (P2P) برای به اشتراک گذاری فایلها بوجود آمده‌اند. از آنجایی که این شبکه‌ها دارای یک سرور مرکزی و محوریت متمرکز نیستند امکان سانسور آنها وجود ندارد. سعی کنید یک نسخه از مطالب مهم خود را در یکی از این شبکه‌ها به اشتراک بگذارید.

ارسال مطالب از طریق ایمیل:

این امکان را برای خوانندگان خود فراهم کنید تا با عضویت در سایت شما بتوانند اخبار و مطالب مهم سایت را به صورت خبرنامه از طریق ایمیل دریافت کنند.

مطالب مهم را به صورت فیدهای RSS منتشر کنید:

همانطور که در مبحث ترفندهای عبور از فیلتر گفته شد، فیدهای RSS به خوانندگان امکان میدهد تا بدون نیاز به مراجعه به سایت مورد نظرشان از عناوین و مطالب مهم آن سایت آگاه شوند. سعی کنید مطالب مهم سایت خود را از طریق فیدهای RSS در دسترس خوانندگان خود قرار دهید.

سایت خود را بر روی یک سرور امن قرار دهید:

اگر امکانش برایتان وجود دارد وب سایت خود را بر روی یک سرور امن (SSL) قرار دهید. در این حالت ارتباط بین سایت شما با کاربران به صورت رمزنگاری شده درمی‌آید و قابل ردگیری نیست.

وب سایت خود را بر روی پورتی غیر از پورت ۸۰ قرار دهید:

پورت ۸۰، پورت پیش‌فرض برای پروتکل HTTP است و اکثر قریب به اتفاق وب سایتها بر روی این پورت قرار گرفته‌اند. به همین علت سیستمهای فیلترینگ طوری تنظیم شده‌اند تا بر تبادلاتی که از طریق این پورت انجام میگیرد نظارت کنند. یکی از راههای جلوگیری از سانسور این است که شما وب سایت خود را بر روی پورتی غیر از پورت ۸۰ قرار دهید. توجه داشته باشید که در این حالت شما حتما باید شماره پورت را همراه با آدرس وب سایتتان ذکر کنید. با فرض این که وب سایت شما بر روی پورت ۸۸۸۸ قرارگرفته باشد، آدرس دسترسی به سایت شما به صورت زیر خواهد بود:

http://www.YourSite.com:8888/

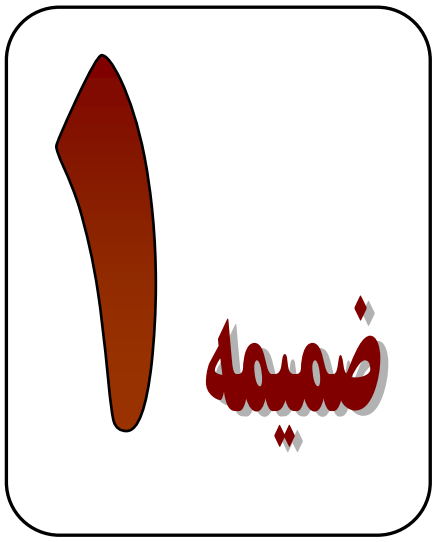
ثبت یک دامین جدید:

اگر نام وب سایت شما در لیست سیاه فیلترینگ قرار گرفت، راه حل آن این است که برای سایت خود یک نام جدید انتخاب کنید. برای این کار لازم است یک دامین جدید به ثبت برسانید و آن را در کنار دامین قبلی‌تان پارک کنید (Parked Domain). به این ترتیب وب سایت شما دارای دو یا چند آدرس متفاوت خواهد شد.

تغییر میزبان وب:

اگر IP آدرس سایت شما در لیست سیاه قرار گرفته، چاره آن این است که از وب هاست خود بخواهید سایت شما را بر روی یکی دیگر از سرورهایش میزبانی کند. اگر وب هاست شما این امکان را فراهم نمیکند، تنها راه حل ممکن این است که وب هاست خود را عوض کنید. در حالت عادی بلوک شدن IP آدرس اهمیت چندانی ندارد مگر اینکه شما بخواهید از طریق IP آدرس به وب سایتتان دسترسی پیدا کنید.

در آخر تذکر این نکته ضروری است که در پیشگیری از سانسور همواره قدم به قدم و همگام با سانسورچیان پیش روید و هیچگاه تمامی برگهای برنده خود را از اول رو نکنید. مثلاً اگر برای دسترسی به وب سایتتان دامین‌های متعددی را به ثبت رسانده‌اید، هرگز نام تمام آنها را به یکباره منتشر نکنید، بلکه به موازات این که فیلترینگ یکی از دامینهای شما را بلوک کرد، شما اقدام به اعلام دامین بعدی کنید.



راهنمای قدم به قدم

راهنمای تنظیم پروکسی در اینترنت اکسپلورر

آموزش مرحله به مرحله و مصور نحوه تنظیم پروکسی در مرورگر اینترنت اکسپلورر.

راهنمای تنظیم پروکسی در فایر فاکس

آموزش مرحله به مرحله و مصور نحوه تنظیم پروکسی در مرورگر فایر فاکس.

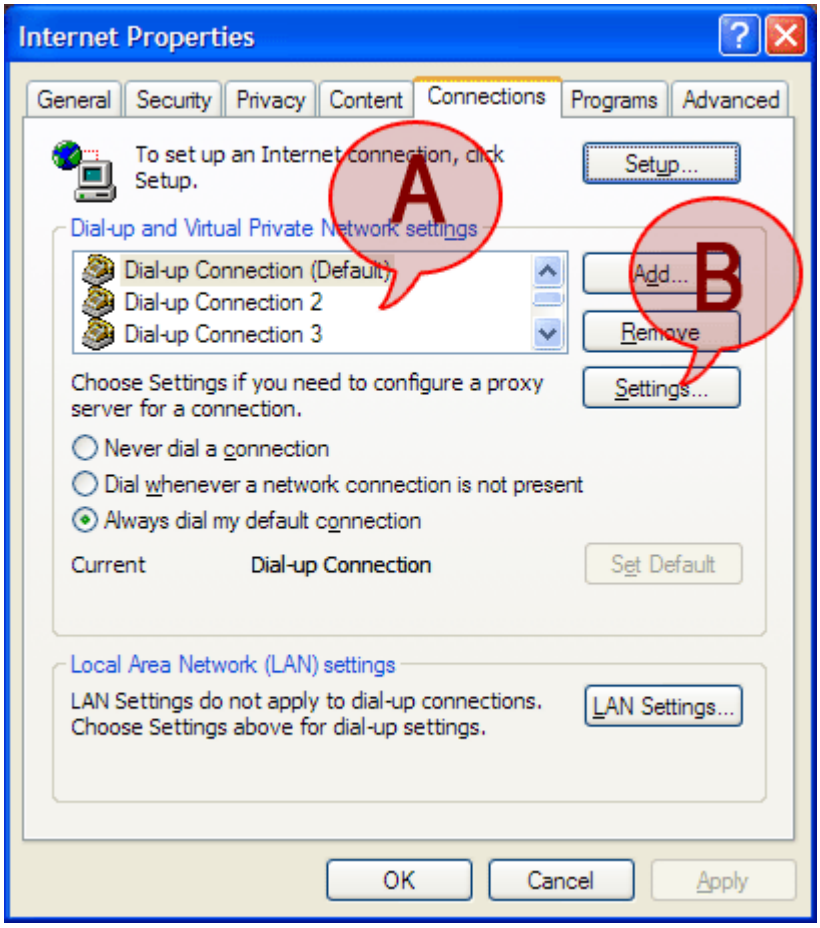
راهنمای تغییر سرور DNS

آموزش مرحله به مرحله و مصور نحوه تغییر سرور DNS در ویندوز ایکس پی.

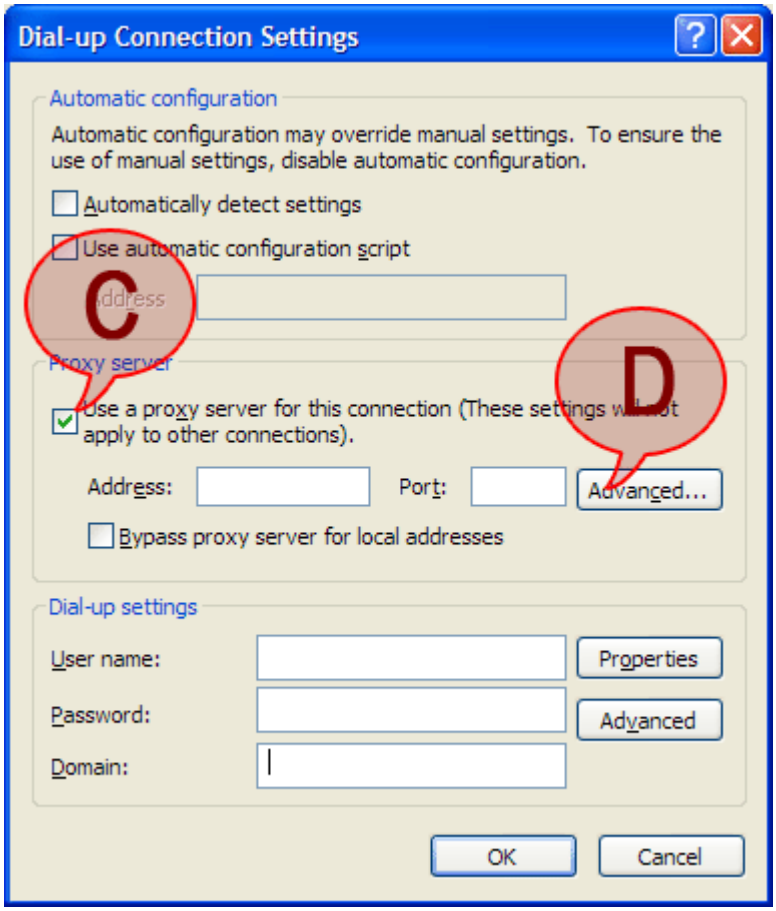
راهنمای تنظیم پروکسی در اینترنت اکسپلورر

برای این که اینترنت اکسپلورر را مجبور کنید از طریق پروکسی به اینترنت متصل شود، مراحل زیر انجام دهید:

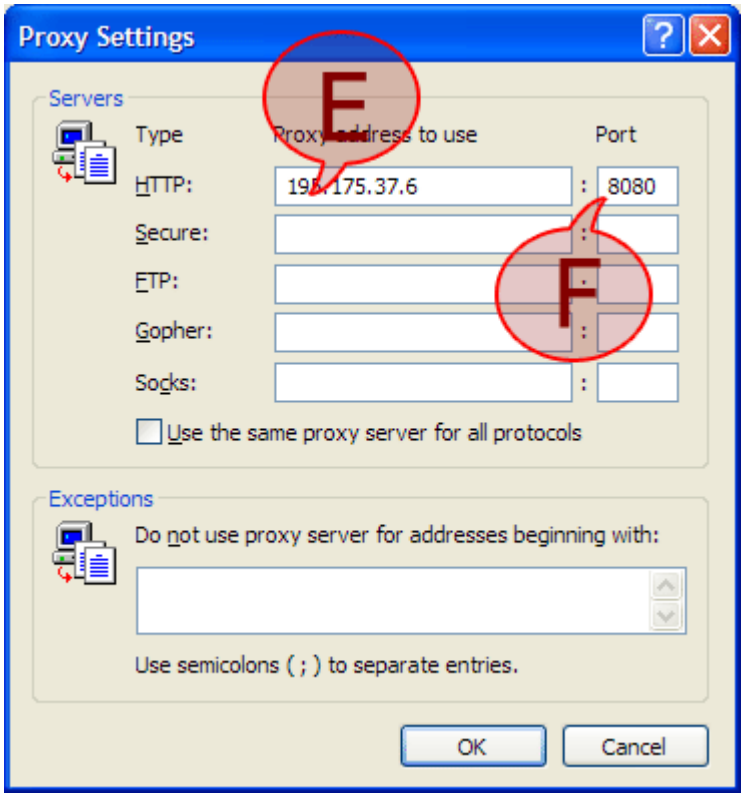
۱. **اینترنت اکسپلورر را اجرا کنید.**
۲. **به منوی** Tools **رفته و** Internet Options **را انتخاب کنید.**
۳. **قسمت** Connections **را انتخاب کنید.**
۴. **کانکشن مورد نظرتان را از لیست موجود انتخاب کنید** (A) **و سپس دکمه** Settings **را فشار دهید** (B).



۵. **در این صفحه، ابتدا** Use a proxy … **را علامت زده (C) و سپس دکمه** Advanced **را فشار دهید (D).**



۶. بر حسب این که از چه نوع پروکسی استفاده میکنید، آدرس (E) و پورت (F) پروکسی را در کادر مربوطه تایپ کنید.

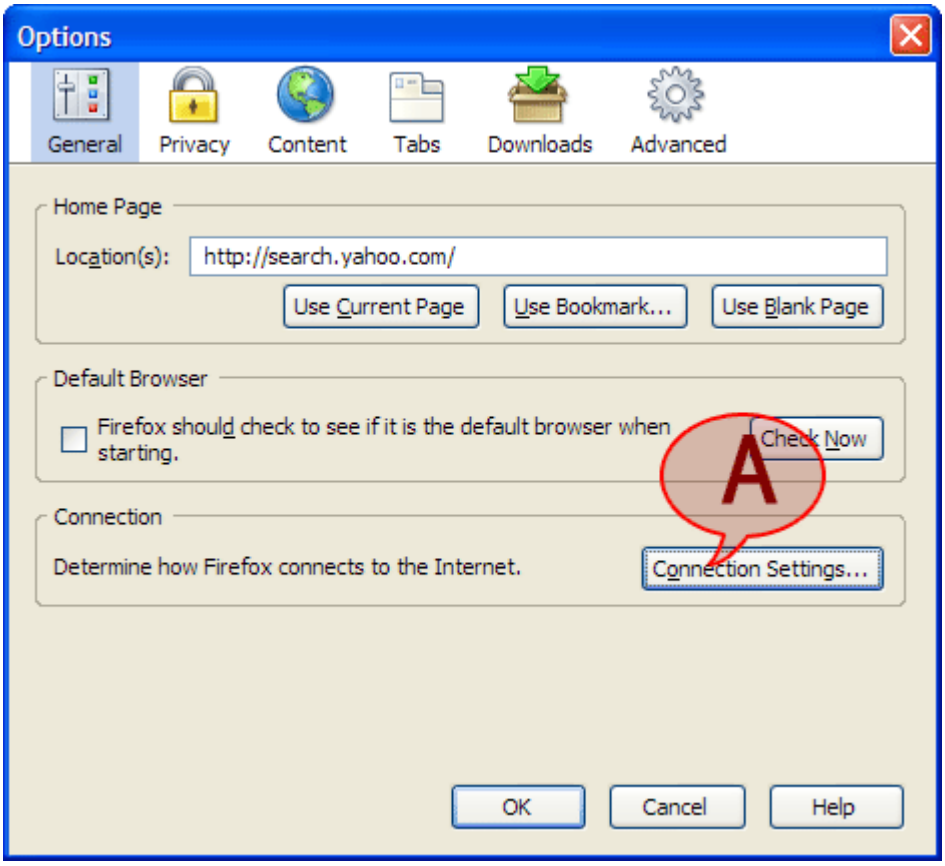


۷. روی دکمه OK کلیک کنید و از قسمت تنظیمات خارج شوید. بعدها اگر خواستید پروکسی را غیر فعال کنید کافیست به مرحله ۵ بگردید و علامت تیک را از کنار Use a proxy… بردارید (C).

راهنمای تنظیم پروکسی در فایر فاکس (Firefox)

برای این که فایر فاکس را مجبور کنید تا از طریق پروکسی به اینترنت متصل شود، به روش زیر عمل کنید:

۱. **فایر فاکس را اجرا کنید.**
۲. **به منوی** Tools **رفته و گزینه** Options **را انتخاب کنید.**
۳. **در قسمت** General **بر روی** Connections Settings **کلیک کنید** (A).

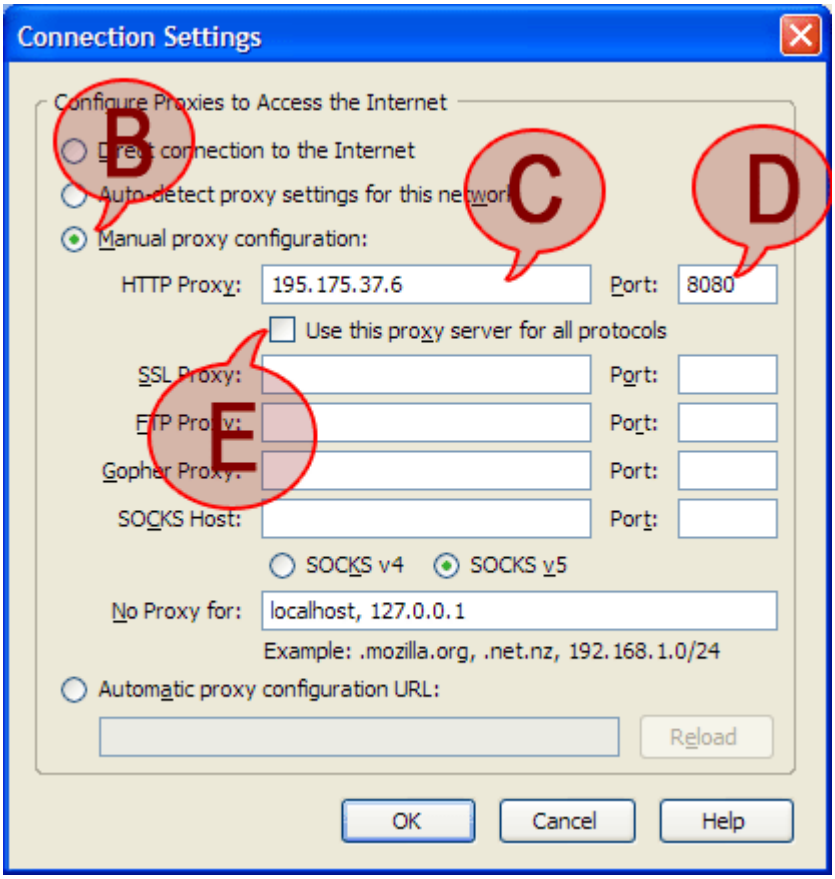


۴. گزینه Manual Proxy configuration را انتخاب کنید (B).

۵. آدرس (C) و پورت (D) پروکسی را در کادر مربوطه وارد کنید.

۶. علامت تیک را از کنار ... Use this proxy بردارید (E).

۷. اگر برای سایر پروتکلها نیز از پروکسی استفاده میکنید، آدرس و پورت پروکسی را در کادر مربوط به آن وارد کنید وگرنه باقی کادرها را خالی بگذارید.



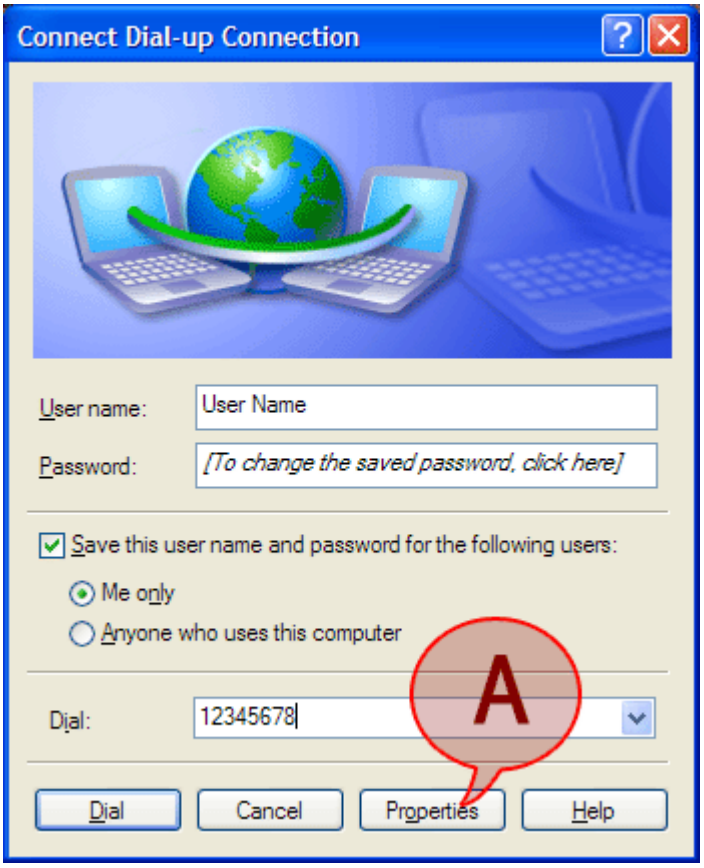
۸. دکمه OK را فشار دهید و از قسمت تنظیمات خارج شوید. بعدها اگر خواستید پروکسی را غیرفعال کنید کافیست به مرحله ۴ بروید و این بار Direct connection to... را انتخاب کنید (B).

روش تغییر سرور DNS

برای تغییر سرور DNS در ویندوز ایکس پی به ترتیب زیر عمل کنید:

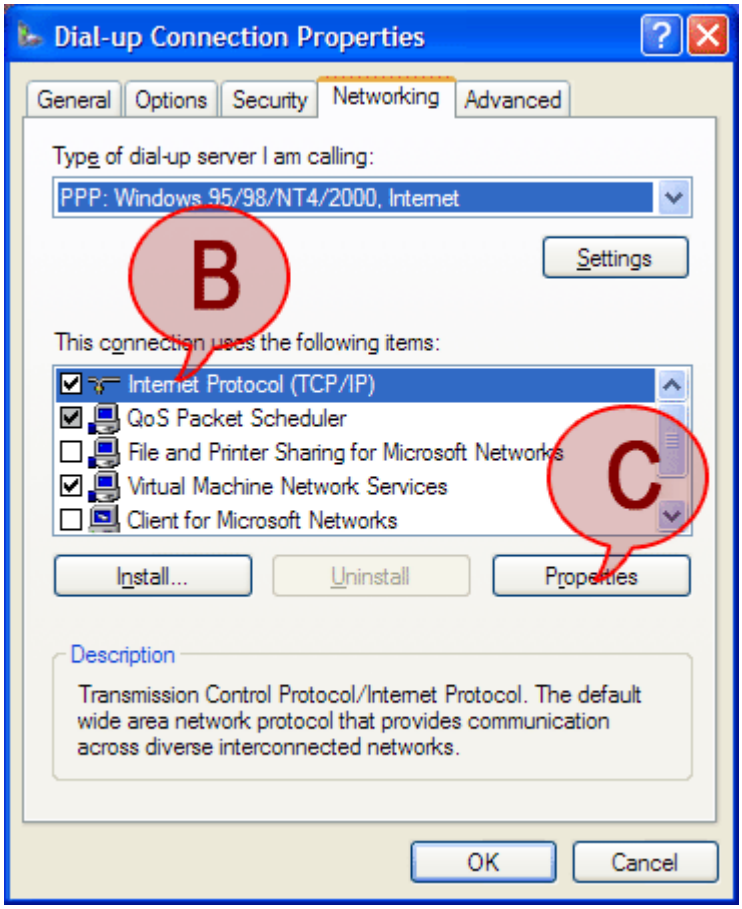
۱. **کانکشن مورد نظرتان را انتخاب کنید.**

۲. **بر روی دکمه** Properties **کلیک کنید** (A).



۳. **گزینه** Networking **را انتخاب کنید.**

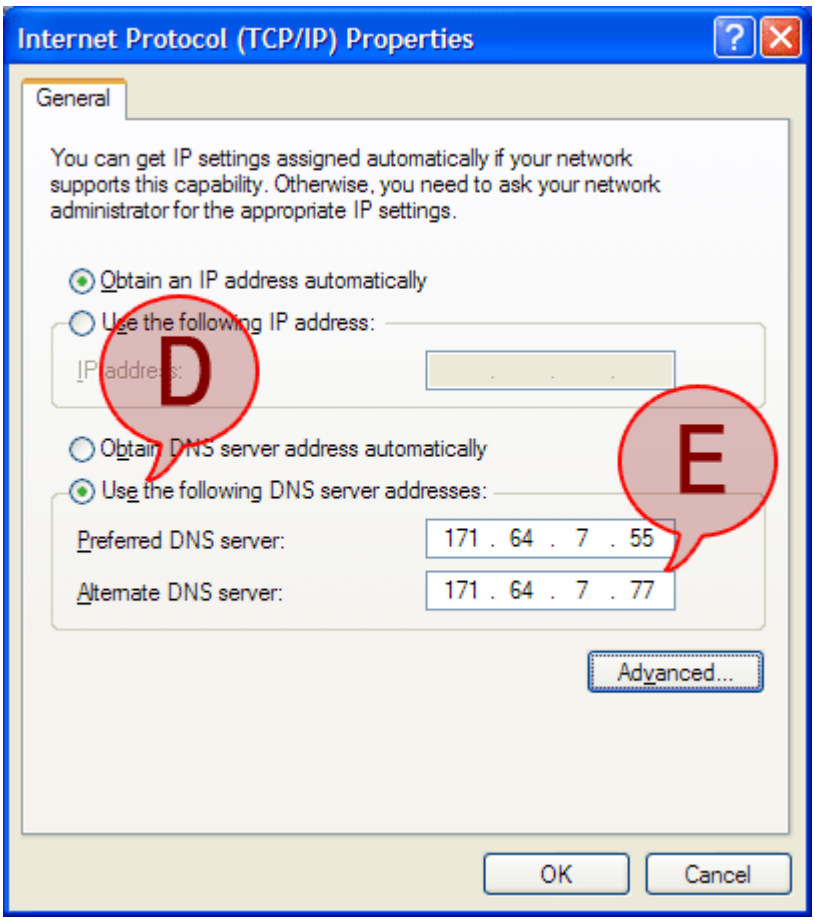
۴. **از لیست موجود** Internet Protocol (TCP/IP) **را انتخاب کرده** (B) **و دکمه** Properties **را فشار دهید** (C).



۵. در قسمت پایین صفحه ... Use the following را فعال کنید (D).

۶. در کادرهای موجود، آدرس DNS اولیه و جایگزین را به ترتیب وارد کنید (E). اگر دارید برای عبور از فیلتر دست به این تغییرات میزنید، میتوانید از سرورهای DNS زیر استفاده نمایید. (تذکر: این DNSها متعلق به دانشگاه استانفورد آمریکاست و ممکن است شما برای استفاده از آن نیاز به اخذ مجوز داشته باشید.)

- 171.64.7.55 (caribou.Stanford.EDU)
- 171.64.7.77 (cassandra.Stanford.EDU)



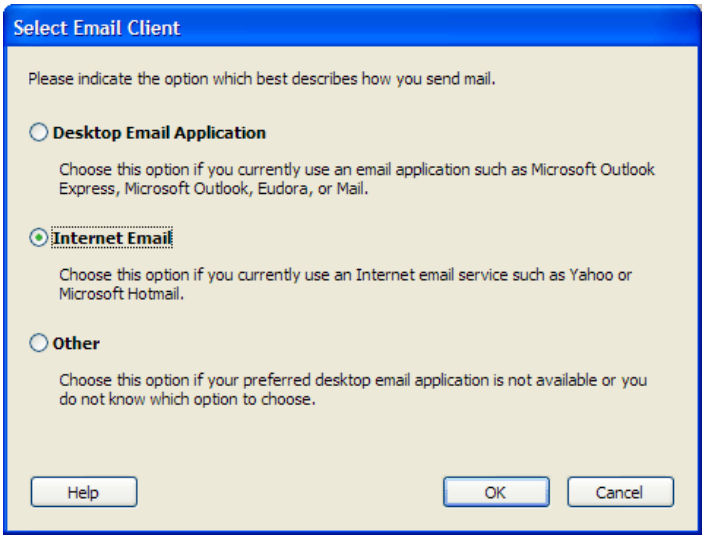
۷. دکمه OK را فشار دهید و از قسمت تنظیمات خارج شوید. برای این که بعداً این تغییرات را به حالت اولیه بر گردانید، به مرحله ۶ برگشته و این بار Obtain DNS server automatically انتخاب کنید (D).

نظرسنجی

بخش نظرسنجی به منظور آگاهی از نظرات و دیدگاههای خوانندگان در رابطه با مطالب مندرج در این جزوه تهیه شده است. بی شک این نظرات و دیدگاهها مهمترین عامل در ارتقای سطح کیفی مطالب در نگارشهای بعدی "راهنمای جامع مقابله با فیلترینگ" خواهد بود.

سوالاتی که در پرسشنامه مطرح شده‌اند تنها جنبه آماری دارند و در هیچ مورد دیگری مورد استفاده قرار نخواهند گرفت. پاسخ به قسمتهایی که با علامت ستاره * مشخص شده‌اند اختیاری است ولی سایر قسمتها حتماً باید تکمیل شوند. بعد از ارسال، ابتدا فرمها توسط کامپیوتر مورد تجزیه و تحلیل قرار خواهند گرفت و فرمهایی که به صورت ناقص یا نامربوط پر شده باشند به طور اتوماتیک حذف خواهند شد. لذا خواهشمند است در تکمیل فرم پرسشنامه نهایت دقت را مبذول دارید.

پس از این که فرم پرسشنامه را تکمیل کردید آن را بوسیله ایمیل برای ما ارسال کنید. برای این منظور بر روی دکمه Submit by Email **در انتهای فرم کلیک کنید. با این کار، کادر محاوره‌ای زیر باز میشود.**



در صورتی که از برنامه‌های رومیزی مانند اوت لوک (Outlook) برای ارسال ایمیل استفاده میکنید، گزینه اول یعنی Desktop Email Application را انتخاب کنید و در صفحه بعد بر روی Send Data File کلیک کنید. در این حالت برنامه ایمیل شما اجرا و فرم پرسشنامه به طور اتوماتیک ضمیمه ایمیل‌تان میشود.

اگر برای ارسال ایمیل از ایمیلهای تحت وب مثل یاهو استفاده میکنید، در کادر محاوره‌ای گزینه دوم (Internet Email) را انتخاب کنید و در صفحه بعد روی Save Data File کلیک کنید. در این حالت پرسشنامه به صورت فایل بر روی کامپیوتر شما ذخیره میشود. شما لازم است این فایل را به صورت دستی ضمیمه (Attachment) ایمیل خود کرده و آن را به آدرس Survey@no-filter.com ارسال کنید.

برای دریافت فرم پرسشنامه اینجا کلیک کنید.

مراجع

1. http://neworder.box.sk/newsread.php?newsid=8650
2. http://www.zensur.freerk.com/
3. http://www.jmarshall.com/
4. http://www.whitefyre.com/poxy/
5. http://www.opennetinitiative.net./studies/iran/
6. http://en.wikipedia.org/wiki/Proxy_server
7. http://en.wikipedia.org/wiki/Censorware
8. http://en.wikipedia.org/wiki/Censorship_in_cyberspace
9. http://en.wikipedia.org/wiki/RSS_%28file_format%29
10. http://www.xml.com/pub/a/2002/12/18/dive-into-xml.html
11. http://www.bbc.co.uk./persian/science/story/2006/01/060120_fb_filtering.shtml
12. http://www.bbc.co.uk/persian/iran/story/2005/06/050623_mj-ms-ir-internet.shtml
13. http://voanews.com./persian/email-subscription.cfm
14. http://computer.howstuffworks.com/internet-infrastructure.htm
15. http://www.2privacy.com/
16. http://www.freeproxy.ru/en/free_proxy/faq/index.htm
17. http://www.proxyblind.org/
18. http://www.spszone.com/articles/proxy_faq_en.htm
19. http://www.digitalcybersoft.com/ProxyList/docs.shtml
20. http://www.bedoonemarz.com/blog/39
21. http://www.securecomputing.com/
22. http://www.peacefire.org/censorware/SmartFilter/
23. http://stop.censoring.us/
24. http://www.stayinvisible.com/
25. http://www.proxyblind.org/
26. ftp://rtfm.mit.edu/pub/usenet/news.answers/internet-services/access-via-email