فیلترینگ و کاربران ایرانی

محمدمهدی واعظی‌نژاد

رهبـر معظم انقلاب سـال ۱۳۸۰ در دیدار اعضای شـورای انقلاب فرهنگـی وضع اینترنت را در کشـور «نابسامان» عنوان کردند و ضمن هشدار، بحث کنترل و پالایـش پایگاه‌های مخرب و لزوم برخورد با تخلفات اینترنتـی را در راس اولویت‌های فرهنگی دانسـتند و حتی برای انجام این کار، مهلت یکماهه تعیین کردند.

همچنین، ایشان در جلسه پرسش و پاسخ دانشجویان دانشـگاه شهید بهشتی در بیسـت‌ودوم اردیبهشت ۸۲ فرمودند: در همه جای دنیا، وقتی جهاز عظیم و فراگیر اینترنت وارد می‌شود، معمولا فیلترهایی هم وجود دارد که هر کشور به فراخور تمایلات و تفکرات و مصالحی که دارد، آنها را کار می‌گذارد. این یک امر طبیعی است. در ایـن جا هـم، در آغاز کار، مقداری بی‌توجهی شـد، لیکن بعد اقداماتی کردند و باید بکنند، این درست است. البته که باید فیلترهای مناسب و لازم را بگذارند.

با توجه به اهمیت بحث فیلترینگ از دیدگاه رهبر معظم انقلاب، مسئولان کشـور تلاش کرده‌اند با بهره‌گیری از روش‌هـای گوناگون و اتخاذ تمهیـدات و نظارت دقیق، به این خواسـته مهم تحقق بخشـند. بر این اساس، در مـاده ۲۱و ۲۲ قانون جرایم رایانه‌ای، قوانینی برای بحث فیلترینگ مطرح شـد که ارائه‌کنندگان خدمات دسترسی اینترنت، موظف هستند این قوانین را رعایت کنند.

اما، بـا وجود همه این تلاش‌هـا، در روزهای اخیر، بسـیاری از کاربران اینترنت داخل کشور برای گذشتن از سـد فیلترینـگ مخابرات، بـه سـراغ نرم‌افزارهای فیلترشـکن، سایت‌های پروکسـی و همچنین VPN (Virtual Private Network) رفته و این رجوع کاربران به استفاده از این روش‌های عبور از فیلترینگ، باعث رشـد فزاینده فـروش اکانت‌هـای نرم‌افزارهای فیلترشکن و VPN شده است.

در ایـن میان، مخابرات هم گاهی اوقات با بسـتن همـه پورت‌هـای VPN همراه با برخـی پورت‌های دیگر مانند SSL، به ایجاد فیلترینگ برای این دسـته از کاربران اقدام می‌کند. اگر چه اطلاعات تبادل شـده توسـط VPN، از طریـق ارتباط امـن SSL صورت می‌گیـرد و بجز خود کاربـر و رایانه سـرور، هیچ فرد دیگری به آن اطلاعات دسترسـی ندارد، ولی به علت رمزنگاری، رمزگشـایی و بازرسـی محتویات هر بسته، این سرویس عملکرد کندی دارد.

بنابراین، با توجه به بسـته شدن پورت‌های VPN در بعضی روزها، اکانت‌های HTTPS (Hypertext Transfer Protocol Secure) و SOCKS از محبوبیت قابل‌توجهی در بین کاربران برخوردار شده‌اند. ایـن دو اکانت، نوعی سـرویس Secure Tunnel اسـت که تقریبا کار VPN را انجام می‌دهند، البته با ضریب امنیتی بالا و سرعت بهتر.

SOCKS یـک پروتـکل اینترنتی امنیتی اسـت که در لایه نشسـت شـبکه ارتباطی عمـل می‌کند و دو نسـخه دارد که هرکدام ویژگی‌هـای خود را دارند: SOCKS v4 و SOCKS v5. البته نسـخه ۵ آن پیشرفته و کامل‌تر اسـت و مرورگر اُپرا مینی هم که در بعضی از رایانه‌ها و تلفن‌های همراه نصب شده، با استفاده از همین پروتکل، می‌تواند از فیلترینگ عبور کند.

و HTTPS از مهم‌تریـن مزایـای اکانت‌هـای علاوه بر تغییر هویت کاربران به آن کشوری SOCKS می‌توان به امنیت ،(Ip Dynamic) که می‌خواهنـد بالا که معمولا با نصب فایروال‌های سـخت‌افزاری در سـمت سـرور و رمزگـذاری داده‌ها تأمین می‌شـود، Windows) سازگاری کامل با انواع سیسـتم عامل‌ها 32 & 64 Bit – Mac – Ipad – Android – Linux - Iphone)، بـدون محدودیت در سـرعت، زمـان و پهنای باند، کیفیت و پایداری بالا، پشـتیبانی ADSL ،از تمام سـرویس‌های اینترنتـی (همراه اول و...) امـکان Wireless، Wimax، GPRS تبادلات مالی با تمام وب‌سایت‌های تجارت الکترونیک و...)، سازگار با وب سایت‌های Paypal، E-Gold) جلوگیری از (Gazzag،Orkut)، ارتبـاط جمعـی شـنود و پیگیری اطلاعات محرمانه کاربران، دور زدن تحریم‌هایی که برای کاربران ایرانی در اینترنت اعمال شـده، امکان به‌روزرسـانی ویندوز و آنتی‌ویروس‌ها، دسترسی به وب‌سایت‌های اینترنتی فیلتر شده و قابلیت اجـرا روی تلفن همراه را علاوه بـر ایمنی ارتباطات و .معاملات تجاری آنلاین آن، برشمرد

در صورت بسـتن پورت SSL، سـایت‌هایی که با این پروتکل امن، رمزگـذاری داده‌ها را انجام می‌دهند همچون بانک‌ها و مؤسسـات مالی و اعتباری، خدمات الکترونیـک آنهـا قابل دسـترس نیسـت. همچنین، سـرویس‌های ایمیـل Gmail و Yahoo نیـز به دلیل اسـتفاده از پروتـکل SSL، در صورت مسـدود شـدن این پورت، غیرقابل استفاده می‌شوند. در صورت بسـتن پورت SSL، عملا بخشی از اینترنت، با مشکل دسترسـی مواجه می‌شود. البته بعضی از سایت‌ها مانند Facebook دو نسخه HTTP و HTTPS دارند که در این هنگام، نسـخه HTTP آنها قابل مشاهده است. در این مواقع، استفاده از پراکسی HTTPS هم برای مشاهده این وب‌سایت‌ها، کاربردی ندارد.

معمولا از HTTPS بـرای تراکنش‌های پرداخت آنلاین و همچنین تراکنش‌های حسـاس سـامانه‌های اطلاعات سـازمانی اسـتفاده می‌شـود. گفتنی اسـت HTTPS را نبایـد بـا پروتکل انتقال ابـر متن امن (S-HTTP) که در RFC ۲۶۶۰ مشـخص شده و غیرقابل فیلتر شدن است، اشتباه گرفت. گاهی وقت‌ها، محدودیت‌های فیلترینگ شامل پورت‌های SOCKS و SSH در داخل کشور نیز می‌شود.

در بعضـی روزهـا نیز، محدودیت پـورت PPTP بعد از سـاعت اداری اعمال می‌شـد که کاربران، قبل از سـاعت اداری، با اسـتفاده از این پورت و بعد از آن، با اسـتفاده از پورت L2TP اقدام به عبور از فلیترینگ می‌کردند.

پورت PPTP (Point-to-Point Tunneling Protocol) برای ساخت شبکه‌های خصوصی مجازی (VPN) مورد استفاده قرار می‌گیرد و نیاز به هیچ‌گونه تنظیمی نداشته و در تمام ویندوزها قابل استفاده است. مسدود کردن این پورت امکان استفاده از VPNها را غیرممکن می‌کند که با بروز خطای ۸۰۰، ۸۰۶ و ۶۸۷ هنگام اتصال به وب، می‌توان از این موضوع آگاه شـد.

L2TP (Layer 2 Tunneling Protocol) و SSTP (Secure Socket Tunneling Protocol) نیز کاربرد مشابهی دارد.

پورت SSTP هم که ترکیبی از پروتکل HTTP و SSL/TLS است، بعضی وقت‌ها شامل این محدودیت می‌شـود و مخابرات برای کم کردن سـرعت SSTP، کل پـورت ۴۴۳ را که مربوط به آدرس‌های HTTPS اسـت، محدود می‌کند که به این مسـاله، با چک کردن ایمیل‌ها در Gmail (بدون استفاده از VPN) می‌توان پی برد. البته باید توجه داشـت SSTP از پروتکل‌های جدید و امن مایکروسـافت بوده و فقط در ویندوزهای ۷ و Vista قابل استفاده است. هدف این پروتکل، فراهم آوردن ارتباطات رمز شـده و شناسایی امن یک کارگزار وب است. برای اتصال به این پورت، نیاز به تنظیم خاصی نبوده و فقط باید تاریخ رایانه به روز باشد.

گاهـی اوقات نیز، ناآشـنایی با تنظیمـات پورت‌ها در فایـروال ویندوز و آنتی ویروس‌های نصب شـده در سیستم، مشکلی جدی برای کاربران مبتدی در عبور از فیلترینگ است.

بتازگی نیز، شـرکت زیرساخت الگوریتم، روش‌های جدید اتصال VPN را با استفاده از مهندسی معکوس شناسایی کرده و ارتباط آنها را قطع می‌کند، مانند آنچه برای اتصال‌های IP–IP اتفاق افتاده است. از آنجا که کاربران تمایل دارند به هر نحوی اتصال بدون فیلتر را برای مشاهده سایت‌های شـبکه‌های اجتماعی و فیلم چون youtube داشـته باشند و قوانین کشور نیز این امر را نفی می‌کند، باید دید که این دور تسلسل در ادامه چگونه خواهد بود، آن هم با حضور شورای عالی فضای مجازی و اراده سخت آن برای قطع تمامی VPNها.