ویکی‌پدیا
دانشنامهٔ آزاد

پروتکل تونل‌زنی

از ویکی‌پدیا، دانشنامهٔ آزاد

مجموعه پروتکل اینترنت

لایه کاربرد

BGP • DHCP • DHCPv6 • DNS • FTP • HTTP • IMAP • IRC • LDAP • MGCP • NNTP • NTP • POP • RPC • RTP • RTSP • RIP • SIP • SMTP • SNMP • SOCKS • SSH • Telnet • TLS/SSL • XMPP (بیشتر)

لایه حمل

TCP • UDP • DCCP • SCTP • RSVP (بیشتر)

لایه اینترنت

IP (IPv4 • IPv6) • ICMP • ICMPv6 • ECN • IGMP • IPsec (بیشتر)

لایه پیوند

ARP/InARP • NDP • OSPF • Tunneling (L2TP) • PPP • MAC (Ethernet • DSL • ISDN • FDDI) • (بیشتر)

قرارداد تونل‌زنی (به انگلیسی: Tunneling protocol) در شبکه‌های رایانه‌ای به کاربر اجازه می‌دهد تا به سرویس‌هایی که در شبکه‌اش ارائه نمی‌شوند، دسترسی پیدا کند. یکی از استفاده‌های مهم پروتکل‌های تونل‌زنی اجرای یک پروتکل خارجی بر روی شبکه‌ایست که آن پروتکل را پشتیبانی نمی‌کند؛ برای مثال استفاده از IPv6 بر روی شبکه مبتنی بر IPv4. استفادهٔ دیگر این نوع پروتکل‌ها فراهم کردن سرویس‌هایی است که ارائه کردن آن‌ها توسط شبکه غیرممکن یا ناامن است. برای مثال فراهم کردن دسترسی یک کاربر خارجی به شبکهٔ داخلی یک شرکت. از آنجایی که پروتکل‌های تونل‌زنی داده‌های ارسالی را مجدداً به‌شیوه‌ای جدید بسته‌بندی کرده و احتمالاً براساس استاندارد بر روی آن‌ها رمزگذاری اعمال می‌کنند، مخفی کردن محتویاتِ تونل نیز می‌تواند از استفاده‌های این نوع پروتکل‌ها باشد.

پورتکل‌های تونل‌زنی با استفاده از قرار دادن بستهٔ درخواستِ سرویس در درون قسمت دادهٔ یک پروتکل دیگر عمل می‌کنند. تونل‌زنی نیز مانند TCP/IP از مدل لایه‌ای استفاده می‌کند اما معمولاً لایه‌های با حمل بستهٔ سرویس در درون بدنهٔ یک بستهٔ دیگر، لایه‌بندی شبکهٔ حمل‌کننده را به‌هم می‌زند. عموماً پروتکل مقصد در لایه‌هایی بالاتر از پروتکل حمل‌کننده قرار می‌گیرند.

محتویات

مرورفنی

برای فهمیدن پشتهٔ پروتکل خاص که با پشتهٔ پروتکل اعمال شده، مهندسان شبکه باید هر دو قابلیت حمل و تحویل دستگاه پروتکل رادرک کنند. برای مثال شبکه‌ای لایه‌ای بر روی شبکهٔ لایه‌ای،(GRE) محفظهٔ مسیریابی کلی، یک پروتکل اجرایی بر روی IP (پروتکلIPشماره ی۴۷)، معمولاً خدمت‌ها را با بسته‌ای کوچک IPانتقال می‌دهد، با آدرس خصوصی RFC1918، پیش از استفاده از اینترنت بسته‌ها با آدرس‌های IPعمومیت تحویل داده می‌شدند؛ بنابراین قابلیت حمل و تحویل پروتکل‌ها یکسان هستند اما آدرس‌ها (قابلیت حمل با شبکهٔ دریافت آنها) ناسازگار هستند.
آن همچنین ممکن است که لایهٔ پیوندی بر روی شبکهٔ لایه‌ای استفاده شود.(L2TP)به بسته‌های لایهٔ پیوندی اجازه می‌دهد

که داده را درون UDPانتقال دهد؛ بنابراین L2TP پیش از انتقال لایه‌ها کار می‌کند.TP در انتقال پروتکل می‌تواند پیش از پروتکل پیوند داده ازIEEE802.2 بر روی IEEE802.3 (یعنی استاندارد مبتنی اترنت) به پروتکل نقطه به نقطه (PPP) بر روی پیوند مدرن شماره‌گیری کار می‌کند.

پروتکل‌های تونل سازی امکان دارد از داده‌های پنهان برای انتقال دادن قابلیت حمل ناامن بر روی شبکه عمومی (مانند اینترنت)استفاده کند، به این وسیله عاملیت VPN راعرضه می‌کند. IPsec به‌طور پیوسته روش‌ها را انتقال می‌دهد، اما همچنین می‌تواند روش‌های تونل زنی مدرن را در میان گذرگاه امنیتی امن اتصال دهد.

تونل‌زنی به‌وسیله پوستهٔ ایمن

یک کانال برنامهٔ امن شامل کانال متن رمزشده میان اتصال پروتکل SSH ساخته شده‌است. کاربران ممکن است کانال SSHرا برای انتقال متن رمز نشده بر روی شبکه در میان کانال رمز شده تنظیم کند. برای مثال ماشین‌های مایکروسافت ویندوز می‌توانند فایل‌ها را استفاده از پروتکل (SMB)، یک پروتکل رمز نشده، به اشتراک بگذارند. اگر شخصی بخواهد سیستم پروندهٔ از راه دور مایکروسافت رابر روی اینترنت وصل کند، شخص جاسوس در یک ارتباط می‌تواند فایل‌ها ی انتقال داده شده را ببیند. برای نصب سیستم پرونده‌های امن ویندوز، یک شخص می‌تواند یک تونل SSH که مسیر تمام ترافیک‌های SMB را برای ارتباط از راه دور فایل سرورها میان یک کانال متن رمزشده یا مجزا برقرار کند؛ بنابراین پروتکل SMB برای خودش شامل پنهان کردن نیست، متن رمزشدهٔ میان کانال SSH که آن راه‌ها امنیت را پیشنهاد می‌کند.

برای تنظیم کردن یک کانال SSH، یک ایجاد پیکربندی یک مشتری SSH برای فرستادن یک دریچهٔ محلی برای حمل کردن ماشین‌های از راه دور تعیین شده‌است. کانال SSH فقط یکبار ساخته می‌شود، کاربر می‌تواند بایک دریچهٔ محلی خاص برای دستیابی به خدمت‌ها شبکه وصل شود. یک دریچهٔ محلی شبیه یک دریچهٔ کنترل از راه دور نیست.
کانال‌های SSH یک مفهوم برای مسیرجانبی دیوار آتش فراهم می‌کند که از خدمت‌ها خاص اینترنت جلوگیری می‌کند-به شرطی که یک موقعیت به ارتباطات خارجی اجاز دهد. برای مثال یک سازمان ممکن است از کاربر برای دستیابی به صفحهٔ وب اینترنت به‌طور مستقیم بدون انتقال دادن میان یک سازمان proxy filterجلوگیری کند (که سازمان به وسیلهٔ بازبینی وکنترل کاربرانی که درمیان وب می‌بیند را فراهم می‌کند). اما ممکن است کاربران نخواهند که صفحه نمایش یا بلوک انتقال وب آن‌ها سازمان proxy filter داشته باشد. اگر کاربران بتوانند به یک خدمتگذار SSH خارجی وصل شوند، آنهامی توانند یک تونل SS برای ارسال کردن یک دریچهٔ دریافتی برای ماشین دریافتی آن‌ها بادریچهٔ ۸۰ با خدمت‌ها وب از راه دور بسازند. برای دستیابی به خدمت‌ها وب از راه دور کاربران می‌توانند مرورگرشان را با دریچهٔ محلی در http://localhost/ هدف گذاری کنند.
بعضی از مشتریانSSHاز ارسال دریچهٔ پویا که به کاربران اجازهٔ ساخت یکproxy SOCKS 4.5را می‌دهد حمایت می‌کنند؛ بنابراین کاربران می‌توانند برنامه هایشان را برای استفادهٔ خدمت‌ها socksمحلیشان پیکربندی کنند. برای دادن قابلیت انعطاف بیشتر از ساخت یک دریچهٔ SSH برای یک دریچهٔ تکی قبلاً توضیح دادیم. socks می‌تواند کاربران را از محدودیت اتصال فقط برای درچهٔ ارتباط از راه دوراز پیش تعریف شده و شبکه آزادمی‌کنند. اگر یک برنامه socks را پشتیبانی نکند یک proxifilter می‌تواند از تعیین جهت برنامه برای خدمت‌ها proxy socks محلی استفاده کند. بعضی از proxifilterها مثل SSH، proxycap را به‌طور مستقیم پشتیبانی می‌کنند، بنابراین نیاز به مشتری SSH را متوقف می‌کند.

دور زدن سیاست دیوارآتش

کاربران همچنین می‌توانند از تونل برای برای یک "snake through" یک دیوارآتش استفاده کنند و استفاده کنند واستفاده کردن از پروتکل که دیوارآتش می‌تواند به‌طور معمولی مانع شود، امادرون پروتکلی که دیواراتش مانع، مانند HTTP پیچیده شده. اگر یک دیوارآتش policy به صورت خاص نتواند مانع نوعی "wrapped" شد، این خطوط می‌توانند کار پیرامون دیوار آتش تعیین شده به دست آورند.
یکی دیگر از روش‌های کانال مبتنی HTTP از فرمان اتصال HTTP استفاده می‌کنند. یک مشتری فرمان اتصال TCP رابه HTTP می‌فرستد. proxy سپس اتصال TCP را برای یک شبکهٔ خاص می‌سازد. دریچه و ذخیره‌سازی داده بین شبکه، دریچه و ارتباط مشتری. زیرا آن امنیت میزبان، قابلیت اتصال HTTP Proxies وبه‌طور عادی دستیابی محدود برای روش اتصال را می‌سازد.

منابع

- مشارکت‌کنندگان ویکی‌پدیا. «Tunneling protocol (https://en.wikipedia.org/w/index.php?title=Tunneling_protocol&oldid=641825032)». در *دانشنامهٔ ویکی‌پدیای انگلیسی*، بازبینی‌شده در ۲۸ دی ۱۳۹۳.