ویکی‌پدیا

Stunnel

این مقاله دقیق، کامل و صحیح ترجمه نشده و نیازمند ترجمه به فارسی است.

کل یا بخشی از این مقاله به زبانی به‌جز زبان فارسی نوشته شده‌است. اگر مقصود ارائهٔ مقاله برای مخاطبان آن زبان ا

بیشتر بدانید

این مقاله نیازمند تمیزکاری است. لطفاً تا جای امکان آن‌را از نظر املا، انشا، چیدمان و درستی بهتر کنید، سپس این برچسب را بردارید.

محتویات این مقاله ممکن است غیر قابل اعتماد و نادرست یا جانبدارانه باشد یا قوانین حقوق پدیدآورندگان را نقض ک

بیشتر بدانید

این نوشتار نیازمند عنوان مترادف فارسی است. خواهشمند است این کار را با توجه به متن اصلی و رعایت دستور خط فارسی و برابر سازی به زبان فارسی انجام دهید.

بیشتر بدانید

stunnel یک برنامه منبع باز چند سطحی است که برای ارائه یک سرویس تونل زنی TLS/SSL جهانی استفاده می‌شود.

stunnel	
توسعه‌دهنده(ها)	Michał Trojnara
انتشار پایدار	5.49[۱] (https://www.stunnel.org/downloads.htm) (l ۳ سپتامبر ۲۰۱۸
مخزن	https://www.stunnel.org/downloads.html
سیستم‌عامل	Multi-platform
گونه	Proxy, Encryption
پروانه	GNU General Public License
وبگاه	www.stunnel.org (https://www.stunnel.org/)

می‌توان از stunnel جهت ارائه اتصالات رمزگذاری شده ایمن برای کاربران یا سرورهایی که به صورت بومی از TLS یا SSL بهره نمی‌برند، استفاده کرد.[۱] این برنامه در سیستم عامل‌های مختلفی[۲] شامل سیستم عامل‌های شبه یونیکس و ویندوز، اجرا می‌شود. stunnel به منظور پیاده‌سازی پروتکل TLS یا SSL از کتابخانه OpenSSL استفاده می‌کند.

stunnel از رمزنگاری کلید عمومی با استفاده از گواهی های دیجیتال X.509 برای اتصال SSL استفاده می‌کند و کاربران می‌توانند از طریق یک گواهی معتبر احراز هویت شوند.[۳]

در صورت ارتباط با libwrap، می‌توان آن را به گونه ای پیکربندی کرد که به عنوان یک سرویس پروکسی - فایروال نیز عمل کند.

stunnel توسط Michał Trojnara ساخته شده و تحت شرایط مجوز عمومی عمومی GNU (GPL) به استثناء OpenSSL منتشر می‌شود.

سناریوی مثال

به عنوان مثال، می‌توان از stunnel برای ایجاد یک اتصال SSL امن به یک سرور ایمیل SMTP غیر SSL استفاده کرد. فرض کنید که سرور SMTP منتظر اتصال TCP در پورت ۲۵ است. می‌توان stunnel را به گونه ای تنظیم کرد که پورت SSL شماره ۴۶۵ را به پورت ۲۵ غیر SSL هدایت کند. یک کاربر ایمیل از طریق SSL به پورت ۴۶۵ متصل می‌شود. ترافیک شبکه سمت کاربر در ابتدا از طریق SSL به برنامه stunnel انتقال می‌یابد که به‌طور شفاف ترافیک را رمزگذاری و بازگشایی می‌کند و ترافیک غیر امن را به پورت ۲۵ منتقل می‌کند. سرور ایمیل یک کاربر ایمیل غیر SSL را می‌بیند.

منابع

1. *او دونوان، بری (اکتبر 2004). "ارتباط امن با Stunnel" (http://linuxgazette.net/107/odonovan.html). روزنامه لینوکس، شماره 107.*

2. *"stunnel: ports" » (https://web.archive.org/web/20190401195456/http://www.stunnel.org/ports.html). بایگانی‌شده از اصلی (https://www.stunnel.org/ports.html) در ۱ آوریل ۲۰۱۹. دریافت‌شده در ۱۳ آوریل ۲۰۱۹.*

3. *"stunnel (8) manual" (https://www.stunnel.org/static/stunnel.html)*

پیوند به بیرون

- استفاده از stunnel به عنوان وی پی ان (https://www.wvpns.site/%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D8%A7%D8%B2-stunnel-%D8%A8%D9%87-%D8%B9%D9%86%D9%88%D8%A7%D9%86-%D9%88%DB%8C-%D9%BE%DB%8C-%D8%A7%D9%86/)