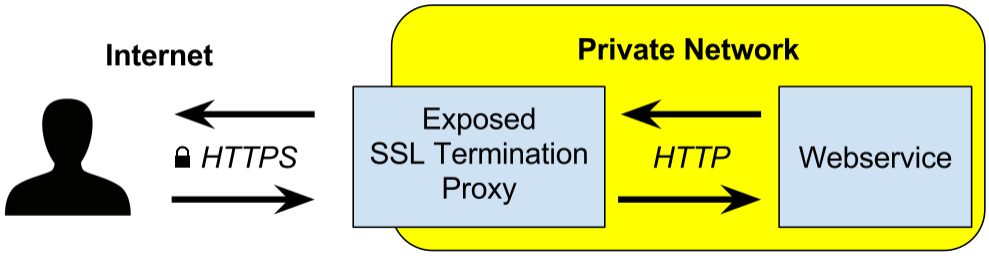
ویکی‌پدیا

پراکسی پایاندهی تی‌ال‌اس

پیشکار[۱] **پایاندهی تی‌ال‌اس**، یا **پروکسی پایاندهی TLS** (یا **پروکسی پایاندهی SSL**، [۲] یا **بارگیری SSL** [۳]) یک سرور پروکسی است که به عنوان یک نقطه واسطه بین کارخواه و سرور عمل می کند، و برای خاتمه و یا ایجاد تونل های TLS (یا DTLS) با رمزگشایی و / یا رمزگذاری ارتباطات استفاده می‌شود. این موضوع با **پروکسی های عبور TLS** که ترافیک رمزگذاری شده TLS(D) را بین کارخواه ها و سرورها بدون خاتمه دادن به تونل هدایت می کنند، متفاوت است.



ترافیک ورودی HTTPS رمزگشایی می شود و به یک سرویس وب در شبکه خصوصی هدایت می شود.

کاربردها

از پیشکار های پایاندهی TLS می توان برای موارد زیر استفاده کرد:

- امن کردن ارتباطات متن آشکار بر روی شبکه های غیرقابل اعتماد با تونل کردن آنها در TLS(D)

- اجازه بازرسی از ترافیک رمزگذاری شده توسط یک سامانه تشخیص نفوذ برای شناسایی و مسدود کردن فعالیت های مخرب
- اجازه نظارت بر شبکه و تجزیه و تحلیل ترافیک رمزگذاری شده.
- فعال سازی یکپارچگی پشتیبانی نشده با کاربردهای دیگر که توانایی های اضافی مانند کنترل محتوا یا ماژول امنیتی سخت‌افزاری را فراهم می کند.
- امکان استفاده از نسخه های پروتکل TLS(D)، برنامه های افزودنی یا قابلیت ها (به عنوان مثال ALPN، OCSP ، DANE ، اعتبار سنجی CT و غیره) که توسط کارخواه یا سرور برای تقویت سازگاری و / یا امنیت آنها پشتیبانی نمی شود.
- کار در زمینه اشکال نرم‌افزاری / ناامن در مورد پیاده سازی TLS در برنامه های کارخواه یا سرور برای بهبود سازگاری و / یا امنیت آنها
- احراز هویت مبتنی بر گواهی اضافی که توسط سرور و / یا کارخواه برنامه های کاربردی یا پروتکل ها پشتیبانی نمی شود.
- یک لایه دفاعی عمیق اضافی برای کنترل متمرکز و مدیریت مداوم پیکربندی TLS(D) و سیاست‌های امنیتی مرتبط با آن فراهم می کند.
- کاهش بار بر روی سرورهای اصلی با تخلیه پردازش رمزنگاری به یک ماشین دیگر.

انواع

پیشکار های پایاندهی TLS می توانند سه الگوی اتصال را فراهم کنند: [۴]

- **برداشتن بار TLS** اتصال رمزگذاری شده ورودی TLS(D) از کارخواه و انتقال ارتباطات از طریق یک اتصال متنی ساده به سرور.
- **رمزگذاری TLS** اتصال متن ساده خروجی از یک سرویس گیرنده و انتقال ارتباطات از طریق یک اتصال TLS رمزگذاری شده TLS(D) به سرور.
- **پل زدن TLS** دو اتصال رمزگذاری شده TLS(D) برای بازرسی و فیلتر کردن ترافیک رمزگذاری شده با رمزگشایی اتصال TLS(D) ورودی از کارخواه و رمزگذاری مجدد آن با اتصال TLS(D) دیگر به سرور.

ترکیب یک پروکسی رمزگذاری TLS در مقابل یک کارخواه با پروکسی برداشتن بار TLS در مقابل سرور، می تواند امکان رمزگذاری TLS(D) و احراز هویت برای پروتکل‌ها و برنامه‌هایی که از آن پشتیبانی نمی‌کنند را فراهم کند، با دو پروکسی که یک تونل ایمن TLS را بر روی شبکه های غیر قابل اعتماد حفظ می کنند بین کارخواه و سرور.

یک پروکسی که توسط کارخواه ها به عنوان یک دروازه واسط برای تمام اتصالات خروجی استفاده می شود، به طور معمول پروکسی Forward نامیده می شود، در حالی که یک پروکسی که توسط سرورها به عنوان دروازه واسط برای تمام اتصالات ورودی استفاده می شود، به طور معمول پراکسی معکوس نامیده می شود. پروکسی های پل TLS که به سیستم

تشخیص نفوذ اجازه می دهد تمام ترافیک کارخواه را تجزیه و تحلیل کند، معمولاً با عنوان "SSL Forward Proxy" در بازار عرضه می شوند. [۵] [۶] [۷]

پروکسی های برداشتن بار TLS و پل زدن TLS معمولاً نیاز دارند که خود را با گواهی دیجیتال با استفاده از PKIX یا DANE احراز هویت کنند. معمولا اپراتور سرور یک گواهی معتبر را برای استفاده در طول TLS(D) به مشتریان ارائه می کند. با این وجود یک اپراتور پروکسی باید CA خصوصی خود را ایجاد کند، آن را در فروشگاه اعتماد همه مشتریان نصب کند و از پروکسی ها برای هر سرور که کارخواه سعی در اتصال به آن دارد، یک گواهی جدید امضا کند که توسط CA خصوصی در زمان واقعی است.

هنگامی که ترافیک شبکه بین کارخواه و سرور از طریق پروکسی هدایت می شود، می‌تواند با استفاده از نشانی آی‌پی کارخواه به جای خودش در هنگام اتصال به سرور و استفاده از نشانی آی‌پی سرور در هنگام پاسخ به کارخواه، در حالت شفاف عمل کند. اگر یک **پروکسی پل شفاف TLS** دارای یک گواهی سرور معتبر باشد، نه نه کارخواه و نه سرور نمی توانند حضور پروکسی را تشخیص دهند. دشمنی که کلید خصوصی گواهی دیجیتال سرور را به خطر بیندازد یا بتواندPKIX CA را به خطر بیندازد / یا مجبور کند یک گواهینامه معتبر جدید برای سرور صادر کند، می تواند با مسیریابی ترافیک TLS بین کارخواه و سرور از طریق یک پراکسیِ پل شفاف TLS یک حمله مرد میانی را انجام دهد. و توانایی کپی کردن ارتباطات رمزگشایی شده، از جمله اطلاعات ورود به سیستم و تغییر محتوای ارتباطات را بدون شناسایی شدن دارد.

منابع

1. پیشکار از واژه‌های مصوب فرهنگستان زبان و ادب فارسی به جای proxy یا proxy server در انگلیسی و در حوزهٔ رایانه است. «فرهنگ واژه‌های مصوّب فرهنگستان: ۱۳۷۶ تا ۱۳۸۵، بخش لاتین» (https://web.archive.org/web/20120512142332/http://www.persianacademy.ir/UserFiles/File/Mosavvab/01_Latin_(A_Z).rar). فرهنگستان زبان و ادب فارسی. ص. ۱۶۳. بایگانی‌شده از اصلی (http://www.persianacademy.ir/UserFiles/File/Mosavvab/01_Latin_(A_Z).rar) در ۱۲ مه ۲۰۱۲. دریافت‌شده در ۳ خرداد ۱۳۹۱.
2. SSL Termination (https://f5.com/glossary/ssl-termination), F5 Networks .
3. Setup IIS with URL Rewrite as a reverse proxy" (https://docs.microsoft.com/fr-fr/archive/blog/friis/setup-iis-with-url-rewrite-as-a-reverse-proxy-for-real-world-apps). Microsoft .
4. Infrastructure Layouts Involving TLS" (https://www.haproxy.com/documentation/hapee/latest/deployment-guides/tls-infrastructure/). HAProxy Technologies .
5. SSL Forward Proxy Overview" (https://www.juniper.net/documentation/en_US/junos-space15.2/topics/concept/junos-space-ssl-forward-proxy-overview.html). Juniper Networks .
6. SSL Forward Proxy" (https://web.archive.org/web/20171201081116/https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/ssl-forward-proxy). Palo Alto Networks. Archived from the original (https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/ssl-forward-proxy) on 1 December 2017. Retrieved 4 April 2021 .

7. *Overview: SSL forward proxy client and server authentication" (https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ssl-administration-11-6-0/13.html). F5 Networks.*