به نام خدا

برنامه نویسی وب - تمرین عملی سری اول

مریم کرمانشاهانی-۹۷۲۳۰۷۳

روی اینترفیس های مختلفی از دستگاه میتوانیم پورت هامون رو باز کنیم اگر روی wifi باز کنیم برای همه باز میشه و اگر روی اینترفیس loop back داخلی فقط روی لوکال هاست خودمون میشه.

-۲

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 (DTLSبا رمزگشایی و / یا رمزگذاری ارتباطات استفاده می‌شود.

TLS termination پراکسی ها میتوانند ۳ الگوی اتصال مختلف را فراهم کنند:

TLS offloading

TLS encrypting

TLS bridging

TLS termination پراکسی ها استفاده می شوند برای secure کردن plaintext در یک شبکه غیر مطمئن، اجازه نظارت بر شبکه، اجازی بازرسی از ترافیک رمزگذاری شده توسط یک سامانه تشخیص نفوذ برای شناسایی و مسدود کردن فعالیت های مخرب، احراز هویت مبتنی بر گواهی اضافی که توسط سرور و /یا کارخواه برنامه های کاربردی و یا پروتکل ها پشتیبانی نمی شود، کاهش بار سرور و ...

کاری که TLS termination proxy انجام میدهد به عبارتی این است که با کلاینت روبرو می شود و کلاینت و پراکسی توافق می کنند بر روی کلید بین آن ها؛

مزایای یک پراکسی واسط در اینجا هم مثل قبل مثلا load balancer و امکان کش کردن داده و ... است

اما مزایای decrypt کردن ترافیک این است که اگر نداند داخل آن چه چیزی است نمیتواند به ما کمکی کند یا دیتایی را کش کند(که باعث تسریع بار گذاری صفحات وب میشود.)

پس به صورت جمع بندی بخواهیم بگوییم

SSL(لایه سوکت ایمن) یا) TLSلایه امنیتی حمل و نقل) یک پروتکل امنیتی است که برای رمزگذاری ترافیک بین دو نقطه پایانی، معمولاً یک سرویس وب و یک مرورگر، یا یک سرور ایمیل و یک سرویس گیرنده ایمیل، استفاده می شود تا اطمینان حاصل شود که همه داده های مبادله شده ایمن هستند و محرمانه

SSL/TLS بیشتر ترافیک اینترنت امروزی را ایمن می کند. به عنوان مثال: در حین معاملات آنلاین یا هنگام تبادل اطلاعات حساس.
بسیاری از پروتکل‌های اینترنت و اشتراک‌گذاری فایل، مانند HTTPS، FTPS، SMTPS، POP3S و غیره برای رمزگذاری به SSL/TLS متکی هستند.

ترافیک SSL توسط یک گواهی امنیتی ((SSL Certificateمحافظت می شود که برای تأیید هویت میزبان/سرویس هدف و رمزگذاری ترافیک استفاده می شود.

خاتمه SSL، همچنین به عنوان " "SSL Offloadingشناخته می شود، فرآیند رمزگشایی ترافیک رمزگذاری شده با SSL است. فرآیند رمزگشایی ترافیک رمزگذاری شده با SSL فشرده CPU است و به دلیل پردازش اضافی مورد نیاز می تواند بر عملکرد برنامه شما تأثیر بگذارد.

خوشبختانه، متعادل‌کننده‌های بار مدرن می‌توانند ترافیک SSL را خاتمه دهند و بار سرویس‌های برنامه پشتیبان شما را کاهش دهند، بنابراین منابع آن‌ها برای اجرای منطق تجاری برنامه (مثلاً ارائه صفحه وب به کاربر) استفاده می‌شود. که مزایای گفته شده در بالا را هم دارد