Was ist ein SSL-Proxy?

Was ist ein SSL-Proxy?

Ein SSL-Proxy ist ein Gerät, normalerweise ein Router oder Computer, der den Datenverkehr von einem Client zu anderen Servern mithilfe des SSL-Protokolls (Secure Sockets Layer) weiterleitet. SSL ist ein verschlüsseltes Protokoll, das eine sichere Verbindung von einem Client zu einem anderen Client oder Server herstellt. SSL wird häufig in Verbindung mit dem Hypertext Transfer Protocol verwendet, um beim Surfen im Internet eine sicherere Verbindung herzustellen. Das resultierende Protokoll oder die Sprache in einfacheren Ausdrücken wird als HTTPS bezeichnet.

Die Funktion eines Proxyservers besteht darin, den Datenverkehr für ein Netzwerk oder einen Client weiterzuleiten und zu filtern. In einem typischen Szenario gibt der Client, normalerweise ein Computer, eine Anforderung aus, in der Regel das World Wide Web zu besuchen, und der Proxy-Server empfängt diese Anforderung, filtert sie und leitet sie entsprechend weiter. Der Vorteil eines Proxyservers besteht darin, dass er den Netzwerkverkehr zentralisieren und gleichzeitig Sicherheit bieten kann.

Der Proxy kann Anfragen nach fast allen gewünschten Kriterien filtern. Wenn ein Unternehmen beispielsweise nur zu einer bestimmten Tageszeit zulassen möchte, dass der Datenverkehr aus dem Hauptnetz in ein anderes Netzwerk oder das World Wide Web geleitet wird, kann es den Proxyserver so einstellen, dass der gesamte Datenverkehr außerhalb des Netzwerks für den Rest des Netzwerks blockiert wird die Zeit. Da der Datenverkehr einen Server durchlief, konnte er auch für Nutzungsstatistiken überwacht werden. Eine hilfreiche Sache für viele Unternehmen.

Secure Sockets Layer (SSL) ist ein Protokoll, das Daten aus Sicherheitsgründen verschlüsselt. Zusätzlich zur Verschlüsselung wird auch ein System von Zertifikaten verwendet, mit denen andere Computer oder Server ihre Authentizität überprüfen. Das HTTPS-Protokoll, die Kombination aus HTTP und SSL, wird häufig zum Herstellen sicherer Verbindungen im Internet verwendet. Viele Unternehmen, die Kreditkarten online akzeptieren, verwenden beispielsweise das HTTPS-Protokoll, sodass niemand auf den Datenstrom zugreifen und vertrauliche Informationen abrufen kann.

Der Hauptzweck eines SSL-Proxys besteht darin, vertrauliche Daten in großem Umfang zu schützen. Es gibt viele Fälle, in denen dies wünschenswert wäre. Ein typisches Beispiel wäre ein großes Unternehmen, das sensible Daten wie finanzielle oder rechtliche Informationen verarbeitet. Das Netzwerk könnte so eingerichtet werden, dass der gesamte ausgehende Datenverkehr des gesamten Unternehmens oder einer bestimmten Abteilung über einen SSL-Proxy geleitet wird. Dies kann zu einem zusätzlichen Schutz beim Senden von Informationen führen, insbesondere von Daten, die über das Internet übertragen werden müssen.

Eine andere typische Verwendung für einen SSL-Proxyserver wäre für Unternehmen, die Zahlungen in irgendeiner Form entgegennehmen. Oft haben sie einen Reverse-SSL-Proxy. Der Reverse-Proxy nimmt den eingehenden und nicht den ausgehenden Datenverkehr auf und kann das SSL-Protokoll intakt halten sowie das Innere des Netzwerks vor möglichen Eindringlingen schützen.

Was ist ein SSL-Proxy?

Was ist ein SSL-Proxy?