



sayTRUST[®] Access

IPsec und SSL VPN vs. sayTRUST Access

Whitepaper

Oktober 2010



IPsec und SLL VPN vs. sayTRUST® Access

Wenn es um die Anbindung mobiler Anwender an ein Firmennetzwerk geht, ist das "Virtual Private Network" - kurz VPN - der gängige Begriff. Doch unweigerlich denkt man dabei in der Regel automatisch an den verbundenen Aufwand und die Vielzahl von Problemen, die bei Installation und Betrieb eines VPN auftreten können.

Im Folgenden wollen wir einen kleinen Überblick über die- unserer Meinung nach - wesentlichen Nachteile der VPNs auf Basis von "IPsec", bzw. "SSL" aufzeigen und die Vorteile von sayTRUST Access gegenüberstellen.

IPsec

IPsec stellt eine der ersten Methoden dar, um ein VPN aufzubauen und wurde ursprünglich für Site-to-Site-Verbindungen entwickelt. Die Installation und Konfiguration einer IPsec-basierenden VPN-Lösung ist in der Praxis meist aufwändig und dabei auch fehleranfällig. So ist es z.B. erforderlich, sowohl client-, als auch serverseitig umfangreiche Installationen, bzw. Einstellungen durchzuführen.

Gerade wenn für eine größere Anzahl mobiler Benutzer ein Zugang zum Firmennetzwerk eingerichtet werden muss, bedeutet dies neben hohem Zeitaufwand auch entsprechend hohe Kosten für Implementierung und Administration. Zudem ist für große IT-Infrastrukturen entsprechendes Equipment erforderlich. So beispielsweise ein VPN-Access-Gateway, eine ausreichende Anzahl an VPN-Client-Lizenzen, etc.

Damit nicht genug: der erforderliche Austausch von Zertifikaten, oder der Wechsel des Preshared-Keys muss vom verantwortlichen Betreuer eines IPsec-basierenden Zugangs administriert werden.

Darüber hinaus bestehen erhebliche Sicherheitsrisiken bei IPsec VPNs, da ein direkter Zugriff (ohne Proxy) bei vollständiger Offenlegung des gesamten Netzwerks erfolgt.

Bruce Schneier, ein in der IT-Welt bekannter Kryptographie-Experte, hat seine Erfahrungen dazu mit einem prägnanten Satz kommentiert:

Zitat:*

"IPsec was a great disappointment to us. Given the quality of the people that worked on it and the time that was spent on it, we expected a much better result."

übersetzt:

"IPsec war eine große Enttäuschung für uns. In Anbetracht der Qualifikation der Leute, die daran gearbeitet haben, und der Zeit, die dafür aufgebracht wurde, haben wir ein viel besseres Ergebnis erwartet."

*Quelle: <http://www.schneier.com/paper-ipsec.html>

SSL VPN

Um die genannten Problemen zu umgehen, setzen viele Hersteller auf die Technologie der "SSL-VPNs".

Bei SSL VPNs entfallen etliche der Kritikpunkte an IPsec. So muss z.B. nicht in jedem Fall eine weitere, virtuelle Netzwerkkarte am Client eingerichtet werden.

Die meisten SSL-VPN-Systeme arbeiten auf Basis eines Standardbrowsers, wobei Anwendungen über eine HTTPS-Schnittstelle angeboten werden. Über diese läuft dann auch der Datenaustausch. Deshalb muss man clientseitig lediglich seine Certificate Authority (CA) hinterlegen, sofern die Zertifikate nicht von einer öffentlichen CA signiert wurden.

Damit treten aber gleichzeitig wieder andere Probleme auf. So ist es nur möglich Anwendungen zu nutzen, die im Kontext des Browsers laufen. Das bedeutet, Java- oder Flashprogramme könnten getunnelt werden, oder auch ein anderes Browser-Applet.

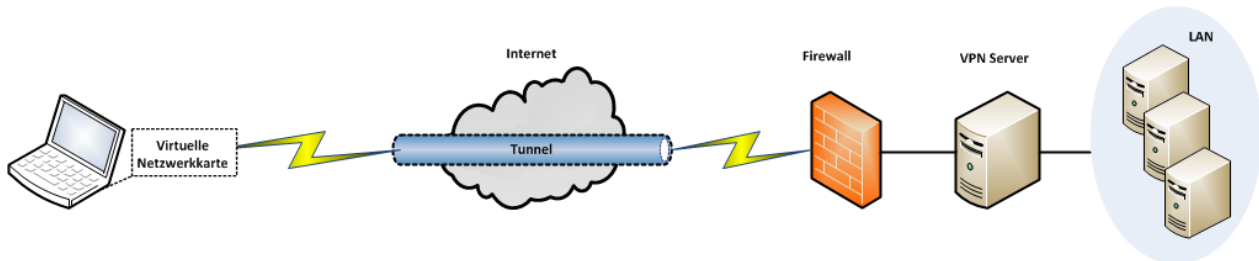
Wenn es aber darum geht ein komplettes Softwarepaket zu nutzen, welches nicht im Kontext des Browsers läuft, so stößt man an die Grenzen von SSL VPNs. Beispiel hierfür sind Client-/Server-Applikationen (wie z.B. SAP, Oracle, etc.). Durch Hinzufügen zusätzlicher Funktionen (z.B. Tunnel- und Portweitergabe) kann hier zwar ein Zugriff realisiert werden. Dabei ist jedoch wiederum eine Vielzahl von sicherheitsrelevanten Konfigurationen zu berücksichtigen, die oftmals nicht im erforderlichen Maße umgesetzt werden.

Ein weiterer Nachteil der meisten SSL VPN-Lösungen ist ein sehr komplexes Policy-Modell, welches neben hohem Verwaltungsaufwand auch Sicherheitsrisiken und/oder erhebliche Einbußen im Bedienungskomfort mit sich bringt.

Bei manchen Lösungen gibt es eine Art "Proxy-Programm" das die Netzwerkdaten des Programms transparent umleitet. Aber hierbei entsteht - wie bei IPsec - erheblicher Mehraufwand: das Proxy-Programm muss installiert, konfiguriert und administriert werden. Eventuelle Probleme mit installierter Firewall-Software oder Antiviren-Programmen müssen dabei parallel behandelt werden.

Selbst nach korrekter Installation wäre es theoretisch möglich, das auf dem Client installierten Proxy-Programm zu manipulieren und unerwünschte oder sogar schädliche Drittsoftware in das VPN zu schleusen.

Die Nachteile von IPsec und SSL in der Zusammenfassung:



IPSec VPN - Nachteile:

- Bei Verbindung des Client-Computer mit dem Firmennetz ist der Client praktisch „Vollmitglied“ des Firmennetzes, kann das gesamte Netzwerk sehen und auf Inhalte zugreifen.
- Hoher Installationsaufwand, nur mit Administrationsrechten (Client-Software, virtuelle Netzwerkkarten).
- Da keine Tunnelung auf Applikationsebene erfolgt, können Viren, Trojaner, etc. in das Firmennetz übertragen werden.
- Verbindung zum Firmennetz kann nur über den Client Computer erfolgen, auf dem auch die VPN-Software installiert wurde.
- Komplexe Benutzerverwaltung.
- Support ist in der Regel sehr aufwändig.

SSL VPN - Nachteile:

- Clientless-Lösungen beziehen sich nur auf Web-Applikationen
- Client-basierte Lösungen erfordern meist Java- oder ActiveX-basierte Applikationen
- Nicht web-basierende Applikationen erfordern clientseitige Installationen wie bei IPSec VPN-Lösungen (z.B. virtuelle Netzwerkkarten). Das VPN kann demzufolge nur über den dedizierten PC/Notebook genutzt werden.
- Client überträgt zunächst alles ungefiltert zum VPN Server → Policies müssen aufwändig erstellt werden.
- Die Nutzung beliebiger Webbrowser bei Clientless-Lösungen birgt Sicherheitsrisiken, wie z.B. die mögliche Übertragung von Viren, Trojaner, Malware, etc. in das Firmennetz; das Hinterlassen vertraulicher Informationen im Cache des Browsers; die Übertragung von Angriffen auf bereitgestellten Applikationen (wurm-infizierter Client Computer).
- Komplexe Benutzerverwaltung.

sayTRUST Access

Bei sayTRUST Access erfolgt der administrative Teil für die Einrichtung des Verbindungsaufbaus auf dem Server. Vom Administrator wird dabei auch für den jeweiligen Anwender ein eigenes Zertifikat erstellt und auf den für den Anwender vorgesehenen sayTRUST USB Access Client kopiert. Für einfache Zugriffe ist es dabei völlig ausreichend, eine Gruppe mit den gewünschten Rechten auf dem sayTRUST Access Server anzulegen und einen Client hinzuzufügen.

Sobald der Client auf einem sayTRUST USB Access Client (USB Stick) installiert und dem jeweiligen Anwender ausgehändigt wurde, ist dieser auch schon einsatzbereit. Dazu muss sich der Anwender lediglich entsprechend den Unternehmensrichtlinien über den sayTRUST USB Access Client authentisieren. Optional sind für sayTRUST Access auch USC Access Clients mit biometrischer Authentisierung erhältlich.

Der Benutzer kann dann auch nur auf die für ihn freigegebenen Ressourcen zugreifen. Alle anderen Zugriffe werden, entsprechend den Einstellungen am sayTRUST Access Server, komplett gesperrt oder nicht getunnelt.

Es besteht ebenfalls die Möglichkeit, nur bestimmte Anwendungen auf Grund ihres Programmnamens zu tunneln. Das bedeutet, nur Pakete dieser Anwendungen werden zum sayTRUST Server geschickt. Netzwerkdaten anderer Programme werden entweder verworfen, oder am Tunnel vorbei ganz normal ins Internet geleitet.

Mit sayTRUST Access können TCP-, bzw. UDP-basierende Anwendung getunnelt werden, die auf dem jeweiligen Client-PC installiert, oder auf dem sayTRUST USB Access Client (USB Stick) in Form einer portablen Version vorhanden sind.

sayTRUST Access ist also weder auf den Browser beschränkt, noch auf Proxy-Programme angewiesen.

Für die Verbindung in das Firmennetzwerk ist keinerlei Installation am jeweiligen Client-Rechner erforderlich!

Die Verwaltung der Client-Zertifikate erfolgt vollständig serverseitig. Gelöschte Client-Zertifikate werden automatisch auf eine Sperrliste gesetzt, damit die Verbindung zurückgewiesen wird, falls sich der "alte" Client dennoch verbinden möchte.

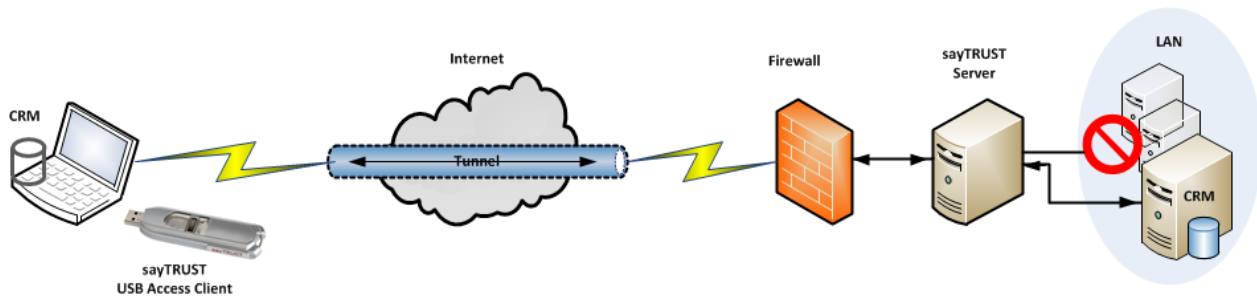
Selbst wenn es einem Anwender gelingen sollte, einen sayTRUST Access Client zu manipulieren, werden alle Daten die über den Tunnel in das Firmennetzwerk geleitet werden, serverseitig nochmals ausgewertet und ohne vorhandenen, gültigen Regelsatz verworfen.

Clientseitige Manipulationen sind somit nicht nur ungleich schwieriger, als bei SSL-VPNs – sondern auch absolut wirkungslos!

Die Konfiguration des sayTRUST Clients ist in mehreren Ebenen verschlüsselt und somit nicht durch den User änderbar. Konfigurationsmöglichkeiten des sayTRUST Access Client für den Benutzer können durch den Server eingeschränkt, bzw. auch komplett abgeschaltet werden. Bestimmte Einstellungen, wie z.B. Komplexität der Passwörter, können dabei erzwungen werden. Selbst Veränderungen der Sicherheits-Policies erfordern nicht den Austausch des sayTRUST Access Clients.

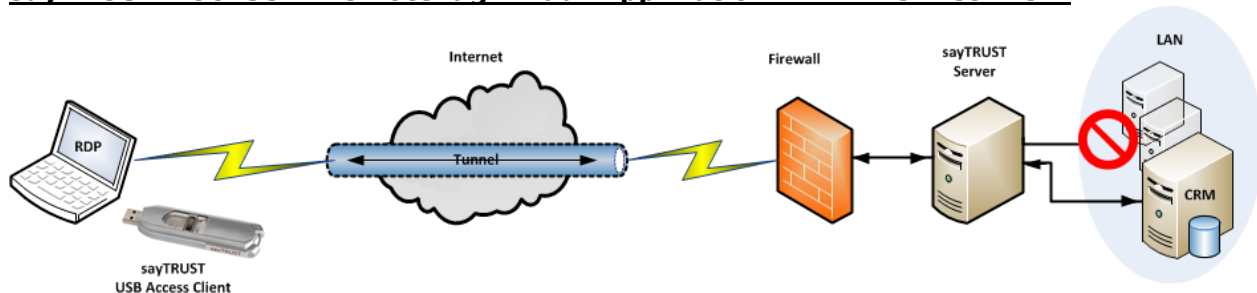
Anwendungsszenarien von sayTRUST Access

sayTRUST ACCESS - Lokale Applikation und Datenaustausch im Firmennetzwerk



- Der Client startet die CRM-Anwendung lokal von seinem Computer.
- Daten werden mit dem Applikations-Server im Firmennetzwerk repliziert.
- Der Datenaustausch erfolgt getunnelt und verschlüsselt gemäß den vom Administrator eingerichteten Regeln.

sayTRUST ACCESS – Remotezugriff auf Applikation im Firmennetzwerk



- Der Client startet die CRM-Anwendung z.B. via RDP oder Citrix vom Applikations-Server im Firmennetzwerk gemäß den eingerichteten Regeln.
- Der Client arbeitet direkt auf dem Applikations-Server. Die Remote-Verbindung wird getunnelt.
- Daten werden von und zum Client über den Tunnel verschlüsselt übertragen.

Vermeiden Sie mangelnde Sicherheit trotz hoher Investitionen!

Testen Sie sayTRUST!