

funkschau

Ausgabe 1-2/2012 27. Januar 2012 € 4,90 sfr 8,90

funkschau.de

 CALLCENTER
WORLD® 2012

„Entgegenkommen“ Was Kunden wollen

Seite 10

E-Mail-Dienste

De-Mail im Kreuzverhör

Seite 29

Im Test



- Sicherer Remote-Access
- Highspeed Wireless

ab Seite 12



Sonderdruck sayTEC

**M2M
Spezial**

Pläne der Netzbetreiber
und Diensteanbieter

ab Seite 36

Je nach Geschmack und Geldbeutel: „sayTRUST-Server“ als Software oder Appliance.



Sicher verbunden ohne VPN

„sayTRUST“ – Heimarbeitsplätze und mobile Mitarbeitern integriert „sayTRUST“ von Saytec Solutions ebenso einfach wie sicher und ganz ohne VPN-, SSL- oder IPSec-Hürden.

Für die Anbindung von mobilen Mitarbeitern, Heimarbeitsplätzen oder kleineren Zweigstellen ans Netzwerk der Zentrale ist die Nutzung virtueller privater Netzwerke (VPNs) der De-facto-Standard. Für die Benutzer ist diese Form des Zugangs transparent, aus Sicht der IT ist sie jedoch nicht unproblematisch: So funktionieren Client-Computer über IPSec-VPNs nur mit spezieller VPN-Client-Software und virtuellen Netzwerkkarten. Nach erfolgreicher Anmeldung sehen sie das gesamte Netzwerk, was nicht unbedingt immer wünschenswert ist. Da das Tunneling nicht auf Applikationsebene erfolgt, erhöht sich das Risiko fürs Firmennetzwerk, sich Viren, Trojaner oder Würmer einzufangen. Setzt die IT zur Vermeidung dieser Nachteile auf SSL-VPNs, handelt sie sich dafür andere Probleme ein: Ohne VPN-Client-Software funktionieren nur Web-Applikationen, die Clients übertragen zunächst alles ungefiltert zum VPN-Server, was teils aufwändige Richtlinien erfordert, und die Nutzung beliebiger Webbrowser bei Lösungen ohne Client-Software birgt Sicherheitsrisiken. In beiden Fällen ist die Benutzerverwaltung nicht ganz trivial und der Support oftmals aufwändig.

Diese und andere Probleme räumt Saytec Solutions bei einer Anbindung über ihr Saytrust-System aus dem Weg.

Saytrust baut zwar auch wie ein VPN einen Tunnel durchs Internet, die Verbindung erfolgt aber im Gegensatz zur VPN-Technik auf Applikationsebene, so dass hierbei zunächst einmal keine direkte Netzwerkkopplung entsteht. Die Anbindung eines Benutzers erfolgt sicher über biometrische oder PIN-Authentifizierung und 2048-Bit-Zertifikate entweder an ein Gesamtfirmennetzwerk, ein Teilsegment des Netzwerks oder gar an einen einzelnen PC innerhalb des Netzwerks. White- und Black-Listen für Applikationen steuern, welche Programme ein individueller Benutzer oder eine Gruppe von Benutzern über den Saytrust-Tunnel ausführen darf. Das schöne bei dieser Mehrstufen-Authentifizierung ist nicht nur, dass sie eine sichere Verbindung herstellt. Dies alles geschieht ohne zeitintensive Konfiguration auf den PCs der Benutzer und ohne Installation von Software auf den Clients. Zwar benötigt auch das Saytrust-System Client-Software, diese ist aber im Gegensatz zu anderen Lösungen auf einem Client-USB-Stick gespeichert.

Dieser Saytrust-Client-Stick dient zur Authentifizierung der Benutzer, er enthält aber auch ausgewählte mobile Anwendungen, die dem Benutzer in die Lage versetzen, rechnerunabhängig Anwendungen wie Textverarbeitung, Tabellenkalkulation, E-Mail, Internet

Alles, was Remote-Benutzer brauchen: Sicherheit, Client-Software und mobile Anwendungen auf einem Stick.

etc. zu nutzen. Der Stick funktioniert mit jedem beliebigen Windows-PC mit Internetzugang. Setzt ein Benutzer den Stick erstmalig ein, dann muss er zusätzlich je nach Typ des verwendeten Sticks eine PIN eingeben und/oder seinen Fingerabdruck registrieren. Die IT kann vorbereitete Sticks einfach per Post an Benutzer verschicken, sollte die entsprechenden PINs dann allerdings separat oder auf einem anderen Weg mitteilen. Jedenfalls reicht es, einem Benutzer Sticks, PIN und vielleicht eine Kurzanleitung zukommen zu lassen – kein Besuch vor Ort, keine Softwareinstallation vor Ort oder eine Remote-Session ist von Nöten.

Software oder Appliance

Der Client ist die eine Seite der Medaille, auf der andere Seite braucht es einen Server. Dieser ist vom Hersteller in Form von Software oder gleich fertig als Appliance erhältlich. Der Server nimmt die Clientverbindungen entgegen, verwaltet die Zertifikate, prüft die Berechtigungen der Benutzer und Gruppen und steuert die Zugänge sowie die UDP- und/oder TCP-Verbindungen der Gruppen und Benutzer. Die Server-Software zur Installation auf einem bereits vorhandenen Rechner unterstützt in der Grundversion fünf Benutzer. Die Appliances – alleamt 19-Zoll-Geräte, wie es sich gehört – unterstützen ab 50 Benutzer. Die größte Appliance, „sayTRUST unlimited“, kennt keine Einschränkung der Benutzeranzahl, enthält zwei 10/100/1000-GBit/s-Ethernet-Schnittstellen (und Platz für vier weitere Schnittstellen), vier 250-MByte-SATA-II-Platten für Hardware-RAID (Level 1 und 0), eine XeonQ-CPU, 8 GByte Arbeitsspeicher und ein redundant ausgelegtes Netzteil.

Der Saytrust-Server unterstützt Netzwerke über physische und virtuelle Schnittstellen und verträgt sich mit physischen und virtuellen DMZs sowie offiziellen und inoffiziellen DNS-Servern. Das System ist also sehr flexibel einsetzbar, beispielsweise zwischen der Firewall und dem Netzwerk, hinter der Firewall innerhalb des Netzwerks und hinter der Firewall mit mehreren Netzwerksegmenten verbunden. Für Tunnel bietet das System 65.000 frei wählbare Ports, was reichen sollte. Das System

unterstützt Tunneling übrigens nicht nur für TCP und UDP sondern auch für Remoteanwendungen wie ICA oder RDP und SIP (VoIP). Die Serverkonfiguration erfolgt über eine Webchnittstelle, die webgestützte Administration kann aber nur aus dem lokalen Netzwerk heraus erfolgen. Das ist wohl als Sicherheitsfeature gedacht, wobei wir uns aber durchaus Situationen vorstellen können, wo auch mal ein Zugriff von der anderen Seite aus erforderlich sein könnte. Die Verwaltung der Zertifikate (2048 Bit) auf dem Server ist einfach, ebenso die Verwaltung der PINs für diese Zertifikate. Bei der Konfiguration eines Client-Zertifikats stellt der Administrator unter anderem auch gleich ein, welche Applikationen zugelassen sind. Er kann den Netzwerkzugriff auf bestimmte Applikationen aber auch komplett verbieten. Eine einfache Kontrolle des Clients der Art „woher?“ und „wohin?“ ist bereits über IP-Adressbereiche durchführbar, außerdem gibt es natürlich eine Rechteverwaltung für Benutzer und Gruppen. Die durch einen Trust-Tunnel fließende Kommunikation wird verschlüsselt, beispielsweise mit AES 256, RC4-MD5 oder EXP-DES-CBC-MD5, um nur einige Verschlüsselungsverfahren zu nennen.

Schnell verbunden

Wie gestaltet sich die Verbindung mit dem Firmennetzwerk nun für den Benutzer? Denkbar einfach. Nachdem er den Client-Stick in einen USB-Port seines Computers eingesteckt hat, fordert ihn die Software automatisch auf, sich durch Fingerabdruck oder PIN-Eingabe zu authentisieren. Nach erfolgreicher Authentifizierung steht dem Benutzer sofort das für ihn vorbereitete Saytrust-Menü zur Verfügung. Dieses Menü ist in drei Bereiche unterteilt: ein zertifikatsgesteuerter Bereich, Anwendungskategorien, und die Applikationen der jeweiligen Kategorien. Im zertifikatsgesteuerten Bereich befinden sich Menüpunkte wie „Verbinden“, „Freigaben verbinden“, „USB-Stick auswerfen“ und „Update“. Über „Verbinden“ stellt das System entsprechend der Richtlinien auf dem Trust-Server die Verbindung her. Falls die Richtlinien zusätzlich eine Passwortabfrage verlangen, muss der Benutzer sich jetzt noch einmal mit seinem Passwort authentifizieren. Eine erfolgreiche Verbindung signalisiert der Client durch ein Ampelsymbol, in diesem Fall mit grünem Licht. Steht die Ampel also auf grün, dann kann der Benutzer auf der rechten Seite im Menü Anwendungen selektieren, beispielsweise Zugang zu einem Citrix-Server im Firmennetzwerk, Webseiten, Netzwerkfreigaben und mehr.

Je nach Konfiguration können entweder vorkonfigurierte Anwendungen vom Saytrust-Access-Client gestartet oder lokal installierte Anwendungen für eine sichere Kommunikati-

on mit dem Firmennetzwerk automatisch in den Saytrust-Tunnel verschoben werden. Diese Einstellungen hinterlegt der Administrator bei der Initialisierung. Für jede Verbindung sammelt Saytrust Informationen, die Benutzer mit entsprechender Berechtigung und Administratoren sich in Form von Statistiken, Protokollen und Auswertungen anzeigen lassen können. Dies beinhaltet Informationen über den Datentransfer und die getunnelten Applikationen.

Saytrust hinterließ einen guten Gesamteindruck, obwohl nicht wirklich alles so rund lief, wie wir uns das wünschten. Beispielsweise wackelte der USB-Stick in manchen USB-Ports doch arg herum, wodurch das Scannen des Fingerabdrucks gelegentlich zur Geduldssprobe wurde. Bei mobilen Computern geht es noch, denn die stellt man vor sich auf den Tisch und kann dann mit einer Hand den Stick festhalten, während ein Finger der anderen Hand gescannt wird. Nutzt der Benutzer aber einen Tower-PC, der unterm Schreibtisch steht, dann hilft eigentlich nur noch eine USB-Verlängerung. Im Test hatten wir außerdem Schwierigkeiten, via Citrix zur Verfügung gestellte Applikationen zu nutzen. Das lag aber vermutlich an der Serverkonfiguration, auf die wir keinen Einfluss hatten.

Das Gesamtsystem bietet hohe Sicherheit, erleichtert Administratoren und Supportern die Arbeit und verlangt den Benutzern nichts weiter ab (außer vielleicht Geduld bei den Fingerabdrücken). Wir können es mit gutem Gewissen jedem empfehlen, der eine brauchbare Alternative für Anbindungen über IPSec- oder SSL-VPNs sucht.

Steckbrief

sayTRUST Access 3.3

Hersteller: Saytec Solutions

Charakteristik: Remote-Access-/Tunneling-Komplettlösung

Preis: auf Anfrage

Web: www.saytec.eu

Plusminus:

- + Keine Softwareinstallation/-konfiguration auf den Clients erforderlich
- + Simple Nutzung durch die Benutzer
- + Gute Steuerungsmöglichkeiten durch Administratoren



 **Dirk Jarzyna**
Redaktion funkschau



Die Lösung für Lösungen.

Datensicherungs-Systeme

Mobile Zugangslösungen

Server und Workstation

Software-Entwicklung

NVR-Lösungen

NAS-Systeme

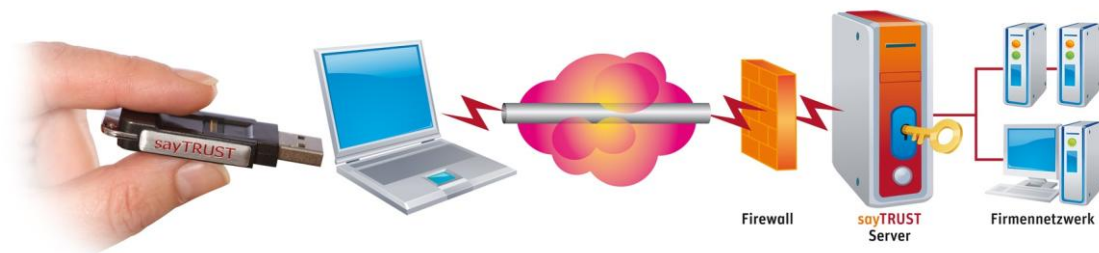


sayTEC Solutions GmbH
Landsberger Str. 320
80687 München
www.saytec.eu

Über sayTRUST ACCESS:

sayTRUST ACCESS ist die ideale und sichere Lösung zur Integration von Heimarbeitsplätzen und mobilen Mitarbeitern, bestehend aus einem Server und einer Clientkomponente.

Das sayTRUST ACCESS-System ermöglicht seinem Benutzer eine sichere Biometrie-, Pin- und 2048-Bit-zertifikatgesteuerte Anbindung an ein Firmennetzwerk, ein Teilssegment eines Netzwerks oder sogar nur an einen einzelnen PC innerhalb eines Firmennetzes.



Die "Dreistufenauthentifizierung" schafft die Möglichkeit einer sicheren Verbindung ohne aufwändige und kosten-, wie zeitintensive Konfigurationen auf dem Anwender-PC.

Ein weiterer Vorteil der sayTRUST ACCESS-Technologie: Maximale Sicherheit bei dennoch einfachster Handhabung. Sowohl bei der Konfiguration des sayTRUST ACCESS Servers über web GUI als auch in der Anwendung durch den Benutzer. Dabei ist der sayTRUST ACCESS-Client unabhängig von der Clienthardware.

Über sayTEC Solutions GmbH:

Hersteller für innovative und qualitativ hochwertige IT-Lösungen. Im Portfolio der sayTEC Solutions GmbH finden Kunden heute Produkte unter ausgewogenen Preis-/Leistungsgesichtspunkten für kleine und mittlere Unternehmen aus den Bereichen:

- Datensicherheit --- kombinierte Backup- und Archivierungslösungen
- IT-Security --- Mobiler Zugang zu Firmennetzwerken
- Netzwerksicherheit --- Firewalls
- Storage --- NAS-Lösungen
- Server, Workstations und Netzwerkkomponenten
- IT-Lösungen im maritimen Umfeld
- IT Lösungen für Automotiv

Produktentwicklung und Herstellung erfolgen zum überwiegenden Teil in Deutschland. Somit werden durch die sehr kurzen Kommunikationswege zwischen Entwicklung, Produktion, Marketing und Vertrieb nicht nur Prozesse optimiert, auch Kundenanforderungen können noch flexibler und schneller umgesetzt werden.

Der Einsatz hochwertiger Komponenten in den Produkten sichert Anwendern ein Höchstmaß an Investitionsschutz. Individuelle Lösungen bzw. Produktpassungen können nach Kundenwunsch realisiert werden.

sayTEC Solutions GmbH
Landsberger Straße 320
80687 München
Telefon: +49 (0)89 578361-400
info@saytec.eu
www.saytec.eu

Weitere Informationen können Sie auch per Email anfordern unter: marketing@saytec.eu