Virtuelle private Netze und Smartphones

Löchrige Netze

Android, iPhone und Web OS bringen diverse VPN-Technologien mit und lassen sich zudem mit Open VPN aufrüsten. Auch RIMs Blackberrys und das Merkel-Phone von T-Systems verschlüsseln auf Wunsch alle Daten. Dennoch ist Vorsicht geboten, denn oft ist die Sicherheit trügerisch. Markus Feilner, Ronny Weiss, Daniel Salcher

Wer sein Smartphone sicher ans eigenen Unternehmensnetz anbinden will, kommt um ein eigenes virtuelles privates Netz (VPN) nicht herum. Auf dem eigenen Linux-Server ist das schnell installiert, und die verbreiteten Handy-Betriebssysteme bieten dem Anwender von Haus aus Integrationsmöglichkeiten mit gängigen VPN-Standards. Dieser Artikel zeigt, was an VPN-Unterstützung bei modernen Smartphones mit Android, Web OS, I-OS und RIMs Blackberry an Bord ist und wie sie sich einrichten lassen, und bringt in einem Howto auch das freie Open VPN auf Android. Zum Schluss folgt ein Blick auf das vom Hersteller als hochsicher angepriesene Mobiltelefon aus dem Simko2-Projekt von T-Systems.

Android-Standards

Android-Anwender haben in der Regel beim Thema VPN die Auswahl aus vier Konfigurationsvorlagen, mit denen sich das Gerät an eigene VPN-Server anbinden lässt und so verschlüsselten Zugang zu den Unternehmensdaten erhält. Abbildung 1 zeigt die Menüs aus »Einstellungen | Drahtlos & Netzwerke | VPN-Einstellungen | VPN hinzufügen«, so wie sie auf den meisten Geräten verbaut sind, zum Beispiel in HTCs Desire-Serie oder Archos-Tablets.

Die Einfachheit der Clientkonfiguration darf den sicherheitsbewussten Anwender nicht über grundlegende VPN-Probleme hinwegtäuschen: L2TP und PPTP sind nach Expertenmeinung nicht mehr als sicher einzustufen und IPsec erweist sich immer wieder als schwierig zu konfigurieren, vor allem im Verbund mit proprietären Implementierungen von Herstellern wie Cisco. Hilfestellung beim Debuggen und Anbinden der Clients gibt der Linux-Magazin-Artikel [1], zum Thema Android und L2TP-IPsec-Insecurities siehe auch den Abschnitt zu Simko weiter unten in diesem Artikel.

Schwieriger zu installieren, dafür aber einfacher zu konfigurieren als IPsec und sicherer als andere Varianten, so präsentiert sich die VPN-Alternative Open VPN. Das SSL-VPN-Projekt findet immer mehr Anwendung auch im kommerziellen Umfeld, zum Beispiel bei Stratos Online-Festplatte Hidrive [2]. Der Artikel [3] beschreibt detailliert, worauf es beim Setup des Open-VPN-Servers für schmale Bandbreiten ankommt.

War die Installation auf Nokias N 900 und seinen Vorgängern noch mit einem simplen »apt-get install openvpn« erledigt, macht unter Android das System einige Schritte mehr notwendig (siehe Kasten „Android-Open-VPN-Howto“). Weil das freie VPN-Tool auf die (standardmäßig auf allen modernen Plattformen verfügbaren) TUN/TAP-Treiber für virtuelle Netzwerkinterfaces setzt, braucht der Admin unter Android Rootrechte, wenn er Open VPN einsetzen will. Das bedeutet nichts anderes als den Jailbreak [6]. Ob der aber im Einzelfall erlaubt oder erwünscht ist, muss im Unternehmen eine Policy der IT-Leitung entscheiden.

Äpfel, Palmen und Schwarzbeeren

Auch Apples iPhone bringt bereits standardmäßig VPN-Support mit, hier sind wie bei Android L2TP, PPTP und IPsec mit an Bord (Abbildung 2). Etwa seit Mai 2010 mehren sich die Berichte von Anwendern [7], die auf geknackten iPhones Open VPN betreiben, doch ist deren Vorgehen im Unternehmenseinsatz nicht zu empfehlen, schon weil Apple dies als Verstoß gegen seine AGBs ansieht. Immerhin bringt das iPhone als IPsec-Client gleich die Cisco-Variante mit,

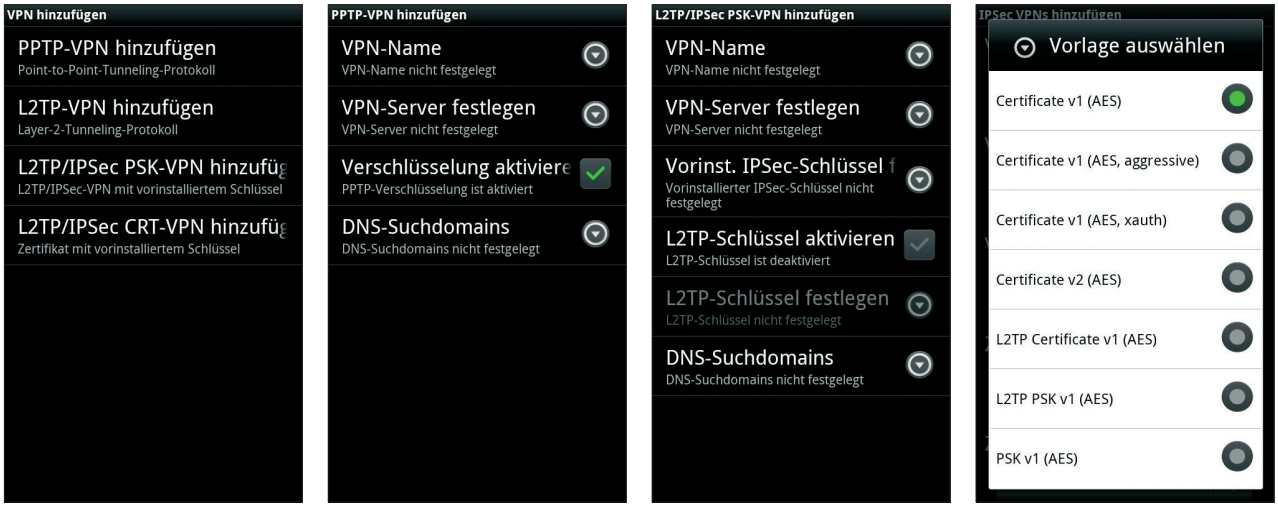

Abbildung 1: Von links nach rechts: Die Einstellungsmenüs für PPTP-, L2TP-, L2TP-VPN mit IPsec-PSK und L2TP/IPsec mit CRT-VPNs bei einem Froyo-Androiden.

die mit Hardware des Internetriesen problemlos funktionieren soll.

Palms Web OS bringt erst seit Version 2.1.0 (Abbildung 3) einen VPN-Einstellungsdialog mit, der unter anderem mit Cisco-Konzentratoren kommuniziert. Die Admins der Uni Clausthal haben dafür ein Howto ins Netz gestellt [8], das interessierte Anwender durch die Konfiguration führt und Probleme aufzeigt.

Weil in HPs Web OS ein Linux werkelt, auf das der Admin mit ein wenig SDK-Magie auch mit einer Shell zugreifen kann, funktioniert auch Open VPN recht problemlos mit den Pre-Smartphones. Ein vertrautes »sudo ipkg-opt install« installiert die VPN-Software und löst selbstständig notwendige Abhängigkeiten auf. »openvpn --config /opt/etc/openvpn/palmpre/palmpre.ovpn« startet einen ersten Tunnel testweise von der Kommandozeile und mit viel Protokoll-Output.

Die Shell ist mit installiertem SSH-Server auch von außen auf dem Smartphone erreichbar, was die Administration deutlich erleichtert. Voraussetzungen für die Installation sind allerdings die Preware(Optware)-Repositories auf dem Gerät und die Einhaltung des vom Hersteller angegebenen Wegs zum Jailbreak [6]. Details zur Open-VPN-Einrichtung liefert Web-OS-Internals [9].

Mit und ohne BES: RIM

Auf Blackberrys hält Research in Motion (RIM, [10]) alle Fäden in der Hand. Die Smartphones des kanadischen Anbieters kommunizieren grundsätzlich verschlüsselt mit ihrer Zentrale – doch hat das Konzept eine kleine Schwachstelle. Daten, die zwischen dem Blackberry Enterprise Server (BES, Abbildung 5) und den Smartphones hin- und herlaufen, sind mit dem Advanced Encryption Standard (AES) oder dem Triple Data Encryption Standard (Triple DES) End-to-End-verschlüsselt. Dieser Weg ist, geht es nach dem Hersteller, auch der zu bevorzugende für den Zugriff auf die Unternehmensdaten in der Zentrale, wo ja normalerweise auch der BES steht.

Allerdings bieten die Schwarzbeeren auch Support für IPsec, an weiteren VPN-Alternativen arbeitet man, erklärt Research in Motion auf Nachfrage des Linux-Magazins. Die Keys für die vom Hersteller eingebaute Standardverschlüsselung erzeugt der Admin auf dem BES und den Telefonen, sie sind damit ausschließlich im Besitz der Blackberry-Kunden, also außerhalb des Einflussbereichs von RIM.

Wer sein Blackberry ohne BES betreibt oder den eingebaute Messenger nutzt, um mit Personen außerhalb des eigenen Unternehmens zu kommunizieren, sollte sich aber keinen Illusionen hingeben. Schon länger ist bekannt, was unlängst bei den Krawallen in London für mediale Aufmerksamkeit sorgte. Die Blackberry-eigene Variante der Peer-to-Peer-Kommunikation zwischen beliebigen Blackberry-Usern gaukelt mehr Sicherheit vor, als sie bietet: Mit der eindeutigen PIN, die dem Anwenderaccount zugeordnet ist, kann ein User auch ohne BES einem anderen Nachrichten schicken (PIN-to-PIN-Kommunikation).

Nur scheinbar verschlüsselt

Die Messages scheinen zwar sicher verschlüsselt, aber weil RIM nur mit einem weltweit einheitlichen kryptographischen Key arbeitet, sprechen Webseiten wie Crackberry [11] nur von „Scrambled Messages“ und betonen, das sei keine wirksame Encryption.

Nur so kann RIM den englischen Behörden volle Kooperation bei der Aufklärung zusichern und sehr wahrscheinlich auch

Abbildung 2: Dreimal VPNs mit I-OS: L2TP, PPTP und Ciscos IPsec auf Apples iPhone.

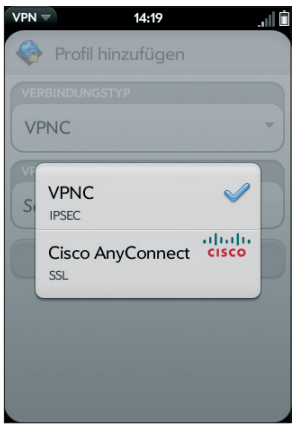

Abbildung 3: Erst seit Version 2.1 kann HPs Palm Pre mit Web OS VPNs konfigurieren.

den kompletten Datenverkehr über die eigenen Server entschlüsseln.

Eingebaute Unsicherheit

Alle beschriebenen Lösungen haben einen gravierenden Nachteil: Bei keinem der Geräte kann der Administrator von einem sicheren Endgerät ausgehen. Auf die Thematik eines sicheren Grundzustands bei einem Smartphone oder Tablet vom Bootloader bis zum Betriebssystem geht ein anderer Artikel in diesem Schwerpunkt detaillierter ein.

Doch schon im Bereich der VPNs zeigen sich bei Android, I-OS und Web OS teilweise eklatante Schwächen. So offeriert beispielsweise Android (übrigens RFC-konform) dem Anwender, der mit dem L2TP-Protokoll mit IPsec und Zertifikat-basierter Authentifizierung einen Tunnel aufbauen will, in einem Pop-up die Frage »Jedes Zertifikat aus unbekannter Quelle akzeptieren?«, wenn bei der Initialisierung etwas falsch lief.

Dahinter kann sich durchaus ein Man-in-the-Middle-Angriff verstecken, etwa wenn ein Staat oder ein Admin Zugriff auf den Mobilfunkbetreiber hat und das Zertifikat während des Verbindungsaufbaus austauscht. Klickt der Anwender hier schnell auf »Ok«, kann der Admin des Mobilfunkrouters den ganzen Traffic mitlesen, obwohl sich der Benutzer sicher wähnt. Derartige Router gibt es im Internet für wenige Tausend Euro.

Ein weiteres Problem ergibt sich daraus, wie VPN-Key und -Zertifikat aufs Gerät kommen und wie sie dort abgelegt sind. iPhones oder andere Telefone ohne Kartenleser scheiden hier für sicherheitsbewusste Anwender von vornherein aus, wenn sie keinen sicheren Speicherbereich in Form einer verschlüsselbaren SD-Karte oder gar einer Cryptocard vorsehen. Aber auch bei allen anderen Geräten hat ein Angreifer prinzipiell immer die Möglichkeit, kritische VPN-Daten im Arbeitsspeicher auszulesen, zum Beispiel den benutzten Schlüssel.

Sicherer Speicher?

Auch wenn heutzutage fast jedes Smartphone vorgibt, mit VPNs verschiedener Couleur arbeiten zu können, sollte sich ein sicherheitsbewusster Admin deshalb nicht allzu beschützt wähnen. Schon der Speicherort der Verschlüsselungskeys und Zertifikate offenbart ein Minenfeld: Erst ab Android-Version 3 (Honeycomb) kann der Anwender alle privaten Daten auf dem Gerät verschlüsseln [12]. Die Datenverschlüsselung des iPhone hält Crypto-Experte Bruce Schneier für leicht zu knacken [13] und bei Web OS gibt es

Android-Open-VPN-Howto

Wer auf seinem Androiden das freie Open VPN installieren muss, darf sich auf einige Arbeit gefasst machen (Abbildung 4). Zunächst gilt es, das Gerät zu rooten (Jailbreak). Tools wie »SuperOneClick«, »SuperUser« oder »VISIONary« helfen dabei.

Anschließend bedarf es der Mini-SSH-Server-Suite Busybox, die im Android-Market in Paketen wie »Titanium Backup« enthalten ist. Dann lädt der Benutzer von [4] den »Tun.ko«-Treiber herunter, Hintergrundinformationen dazu liefert das Forum [5]. »Tun.ko« landet in einem eigens angelegten Ordner auf der SD-Karte zusammen mit der gewünschten Clientkonfiguration für Open VPN samt Zertifikaten und eventuell benötigter Keys.

Jetzt installiert der Anwender (wiederum aus dem Market) den »Open VPN Installer« und das Programm »OpenVPN Settings«. An einem Terminal auf dem Androiden verlinkt jetzt

```
ln -s /system/xbin/ifconfig /system/xbin/➥
bb/ifconfig
ln -s /system/xbin/route /system/xbin/bb/➥
route
```

die Open-VPN-Binaries. Das geht natürlich auch mit den SDK-Tools, hier mit Adb:

```
adb shell ln -s /system/xbin/ifconfig ➥
/system/xbin/bb/ifconfig
adb shell ln -s /system/xbin/route /system➥
/xbin/bb/route
```

Jetzt startet der »Open VPN Installer« und erhält als Installationsort »/system/xbin/« sowie als »Pfad zu route/ifconfig« den Parameter »/system/xbin/bb/«. Danach startet der Anwender »Open VPN Settings« und wechselt ins Menü »Advanced«. Dort muss »Load tun kernel module« angeschaltet, »TUN module settings:« auf »Load module using: insmod« gesetzt und als »Path to tun modul:« zum Beispiel »/sdcard/openvpn/tun.ko« eingetragen sein.

Jetzt kann der Smartphone-Besitzer noch etwaige Einstellungen anpassen und die Konfigurationsdatei überprüfen, dann das VPN aktivieren und zum Beispiel mit Netping (ebenfalls im Market) testen. Achtung: Die Datei »Tun.ko« muss zur jeweiligen Android-Version passen!

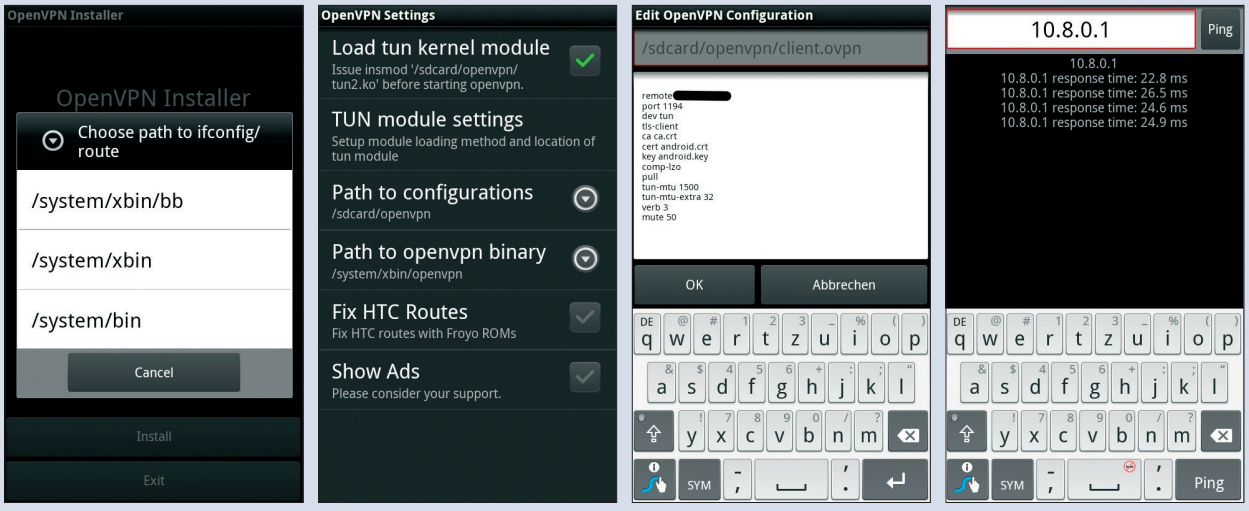

Abbildung 4: Open VPN lässt sich nur auf gerooteten Androiden installieren. Dann bedarf es noch der richtigen Pfade, Einstellungen und eines Tests mit Netping.

Data Encryption sogar nur als Zusatz-App, zum Beispiel Secret! [14]. Hinzu kommen noch manche Fehler in Protokollen, Stacks und Update-Mechanismen, die ein sicheres Endgerät fast unmöglich machen. Das aber wäre eine zentrale Voraussetzung für den geschützten Unternehmenszugang.

Simko2

Das besser zu machen, verspricht T-Systems mit den Simko2-Telefonen (Sichere Mobile Telekommunikation, [15]). Der deutsche IT-Konzern hat das L2TP-Protokoll verändert und dabei auch die erwähnte L2TP-IPsec-Lücke mit dem Man-in-the-Middle-Angriffsvektor geschlossen. Die Simko-Geräte setzen auf Technologie der Security-Spezialisten NCP [16] und Genua [17]. Das BSI hat die HTC-Telefone mit gehärtetem Windows Phone 6.5 auf Herz und Nieren getestet und für sicher gemäß der Geheimhaltungsstufe „Verschlusssache nur für den Dienstgebrauch“ befunden.

Für „lückenlose Sicherheit“ (T-Systems) soll dabei ein angepasstes Betriebssystem mit eingebauter Crypto-SD-Card, End-to-End-Verschlüsselung und gehärtetem Bootloader sorgen. Die Zertifikate fürs VPN gelten per Default zwei Jahre und sind fest ins Gerät integriert, sodass das Smartphone eine Lebensdauer von 24 Monaten nicht überschreiten kann. Am Nachfolger mit Android und Dualboot arbeiten die Entwickler bereits. ■

Infos

[1] Wolfgang Langner, Markus Feilner, „Durchbruch“: Linux-Magazin 10/09, S. 56

[2] Strato Hidrive: [http://www.strato.de/hidrive]

[3] Markus Feilner, „GPRS, NX, Open VPN, Bluetooth“: Linux Technical Review 05/07, S. 84

[4] Tun.ko bei Google Code: [http://code.google.com/p/get-a-robot-vpnc/downloads/detail?name=tun.ko&can=2&q=]

[5] Entwicklerforum: [http://forum.xda-developers.com/archive/index.php/t-960642.html]

[6] Oleksandr Shneyder, Nils Faerber, Markus Feilner, „Endlich frei!“: Linux-Magazin 04/10, S. 46

[7] Open VPN auf iPhones: [http://chandraonline.net/blog/?p=22]

[8] IPsec mit dem Palm Pre: [https://www-secure.tu-clausthal.de/userdoku.rz/doku.php?id=vpn:webos]

[9] Open VPN mit Web OS: [http://www.webos-internals.org/wiki/OpenVPN_for_Palm_Pre]

[10] RIM-Blackberry: [http://de.blackberry.com]

[11] Warum PIN-to-PIN-Messaging unsicher ist: [http://crackberry.com/pin-pin-messaging-secure]

[12] Honeycomb kann Daten verschlüsseln: [http://www.engadget.com/2011/02/02/android-3-0-honeycomb-can-encrypt-all-your-data-needs-a-full/]

[13] Bruce Schneier hält nichts von der Verschlüsselung auf Apples iPhone 3G: [http://www.schneier.com/blog/archives/2009/07/iphone_encrypti.html]

[14] Secret!: [http://linkesoft.com/secret/]

[15] T-Systems stellt sichere Smartphones für Bundesbehörden vor: [http://www.telekom.com/dtag/cms/content/dt/de/595758?archivArticleID=791156]

[16] NCP: [http://www.ncp-e.com]

[17] Genua Security: [http://www.genua.de]

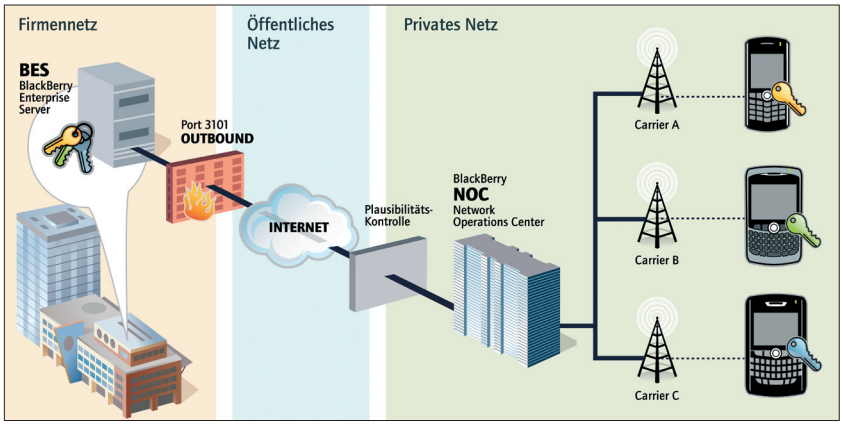

Abbildung 5: Die Blackberry-Infrastruktur setzt auf den zentralen Blackberry Enterprise Server (BES).

Wissbegierig?

Schulungen von Profis für Profis

it-sa 2011 – BESUCHEN SIE UNS!

Schulungen, E-Mail-Archivierung, Anti-Spam, Mailtrace. Unser Team steht Rede und Antwort:

it-sa in Nürnberg, Halle 12, Stand 472

LINUX HÖCHSTPERSÖNLICH.