Der eigene Hotspot

Egal, ob Sie sich zu Hause mit dem Notebook frei bewegen oder Ihrem Nachbarn die Mitbenutzung des DSL-Anschlusses ermöglichen wollen: pfsense ist erste Wahl, wenn es um die Hotspot-Einrichtung geht.

ACHIM WAGENKNECHT

Es gibt viele Möglichkeiten, einen Wireless Access-Point mit Open Source aufzubauen. Der Klassiker fli4l bietet Module für WLAN, schreckt Anwender aber mit einer textbasierten Konfiguration ab.

Das komfortable IPCop wiederum unterstützt Wireless lediglich halbherzig. Es ist zwar eine so genannte »blaue Netzwerkzone« für WLAN vorgesehen. Aber es lässt sich keine WLAN-Karte einbauen. Stattdessen muss an die Netzwerkkarte ein externer Access-Point angeschlossen werden. Ähnliches gilt für Chillispot. Das Programm unterstützt öffentliche Hotspots mit Captive Portal und WPA-Verschlüsselung, benötigt aber ebenfalls externe Access-Points.

Die in der Praxis mit Abstand vielfältigste und am einfachsten zu administrierende Lösung ist pfsense.

Sicher mit Captive Portal

Ein öffentlicher Hotspot wird so aufgebaut, dass zunächst alle Verbindungen akzeptiert werden. Damit das aber nicht unkontrolliert geschieht, fängt das Captive Portal alle Verbindungen ab und leitet sie auf eine Log-in-Seite um. Diese ist mit einem Authentifizierungsserver wie RADIUS oder einer speziellen Benutzerverwaltung verbunden.

Diese Lösung hat M0n0wall *(www.m0n0.ch/wall)* schon eingebaut. Man kann M0n0wall mit Hilfe einer WLAN-Karte in einen Access-Point verwandeln. Auch das Captive Portal ist schon integriert. Allerdings ist M0n0wall bei der Auswahl der Wireless-Karten wählerisch.

Das Programm basiert auf der nicht mehr aktuellen Version FreeBSD 4.11 und arbeitet folglich nur mit Karten zusammen, die von diesem Betriebssystem unterstützt werden – und solche Komponenten sind dünn gesät. Das sieht bei pfsense deutlich besser aus *(www.pfsense.org)*.

Sicher mit Captive Portal

Pfsense ist ein abgespaltener Entwicklungszweig von M0n0wall, ein so genannter Fork. Noch ist das Programm größtenteils mit M0n0wall identisch, aber in puncto WLAN gab es von Anfang an einen wichtigen Unterschied: Pfsense beruht auf FreeBSD 6.1 und unterstützt damit wesentlich mehr WLAN-Karten. Eine ausführliche Liste der unterstützten Hardware findet sich unter *www.pfsense.org/index.php?id=37*.

Minimalismus versus Featuritis

Die Zielsetzungen von M0n0wall und pfsense sind unterschiedlich: Der M0n0wall-Entwickler besteht darauf, weiterhin primär für Embedded-Plattformen zu entwickeln, obwohl die Mehrzahl der M0n0wall-Installationen auf PCs läuft. Der Programmierer opfert für seine Strategie auch mögliche Funktionalität. Firewall-Puristen werden ihm zustimmen, denn es gilt nach wie vor die Devise, dass Zusatzfunktionen nichts auf einer Firewall-Maschine zu suchen haben.

Scott Ullrich, Bill Marquette und Chris Buechler sehen das nicht ganz so eng. Sie wollen mit pfsense die vorhandene Hardware durch Zusatzdienste besser ausnutzen.

pfsense in der Praxis

Aus der Liste der von pfsense unterstützten Hardware wählen die Tester eine weit verbreitete WLAN-Karte – Netgear WG311T PCI. Die Karte enthält den Atheros-Chipsatz. Während M0n0wall die WLAN-Karte nicht erkennt, wird sie bei der Installation von pfsense problemlos als *ath0* angezeigt.

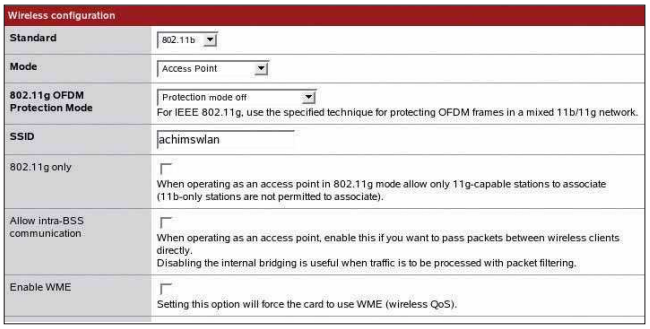
Installation elegant gelöst

Die Einrichtung ist bei pfsense wirklich benutzerfreundlich gelöst. Wer eine vorhandene Firewall auf PC-Basis mit IPCop oder dergleichen hat, kann problemlos den gleichen Computer für pfsense benutzen.

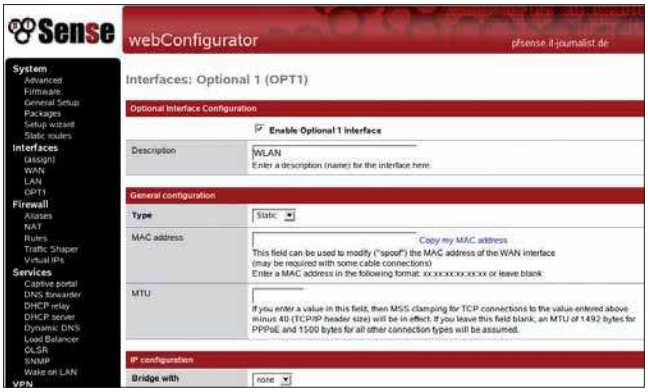
Die Konfiguration der Firewall sollten Sie allerdings unbedingt sichern. Pfsense kann als ISO-Image heruntergeladen und auf CD gebrannt werden. Praktisch: Die CD basiert auf dem bewährten BSD-Installer und lässt sich sowohl als Live-CD als auch zur Installation nutzen. So lassen sich alle Einstellungen erst einmal ausprobieren, bevor die Firewall auf der Festplatte installiert wird.

Erst wenn alle Netzwerkkarten konfiguriert sind und der Internet-Zugang steht, muss die alte Firewall der neuen Security-Software weichen. Sollte irgendetwas nicht klappen, nimmt man einfach die CD aus dem Laufwerk und kehrt zur vorherigen Firewall zurück. Interessantes Detail: Der pfsense-Router von der Live-CD läuft sogar dann weiter, während pfsense auf der Festplatte installiert wird. Lediglich beim abschließenden

Die erste Verbindung zum Internet lässt sich komfortabel per Wizard einrichten



Die WLAN-Karte ath0 wird der Netzwerk-Schnittstelle OPT1 zugeordnet



Die Wireless-Schnittstelle bekommt den Namen WLAN und eine feste IP-Adresse

Reboot wird die Netzwerk-Verbindung naturgemäß kurz unterbrochen.

Konfiguration

Für die ersten Konfigurationsschritte müssen Sie Tastatur und Bildschirm am Router-PC anschließen. Sehr gut: Sowohl die drahtgebundenen Netzwerkkarten als auch der WLAN-Adapter werden im Test automatisch erkannt. Auch die Zuordnung der Netzsegmente ist elegant gelöst: Zunächst werden alle Karten vom Netzwerk getrennt. Das Programm fordert den Anwender dann dazu auf, WAN oder LAN zu verbinden, und ordnet die entsprechende Karte anhand des Up-Status dem passenden Interface auf Betriebssystem-Ebene zu. Das mühsame Umstecken falsch zugeordneter Karten entfällt.

Sobald das LAN-Interface mit einer passenden IP-Nummer versehen ist, ist die Admin-Oberfläche von pfsense per Browser erreichbar. Die Zugangsdaten für den ersten Log-in lauten: Benutzer *admin*, Passwort *pfsense*. Monitor und Tastatur sollten trotzdem noch am Router bleiben, schon allein wegen des Menüpunkts *99: Auf Festplatte installieren*. Diese Funktion steht im Web-Interface nicht zur Verfügung.

Admin-Interface

Das Design des Admin-Interfaces lässt sich über Vorlagen, so genannte Themes, ändern. Wem das voreingestellte *Metal*-Design zu überladen ist, kann auf der Seite *System/General Setup* ein anderes Design wählen. Im Test erweist sich das Design *pfsense* ohne Drop-down-Menüs als gut, weil so die Menüpunkte sichtbar bleiben. Zudem reagiert das Web-Interface schneller, wenn das Javascript der Drop-down-Menüs nicht bremst.

Die Zugangsdaten für DSL werden unter *Interfaces/WAN* eingegeben. Neben PPPoE für DSL können Sie hier auch statische, DHCP- und PPTP-Zugänge einrichten. Sobald der Internet-Zugang funktioniert, empfiehlt es sich, die Konfiguration zu sichern. So lässt sich der Zugang bei späteren Fehlern jederzeit wiederherstellen. Die Funktion *Backup/Restore* finden Sie unter *Diagnostics*.

Die Optionen von pfsense sind umfangreich. Trotz der komfortablen Oberfläche können sich Fehler einschleichen. Es empfiehlt sich daher auch später, die Konfiguration nach jeder Änderung abzuspeichern.

WLAN aktivieren

Obwohl bei der Installation die Wireless-Karte erkannt wurde, ist sie noch nicht betriebsbereit. Sie muss erst unter *Interfaces/Assign* einer Netzwerk-Schnittstelle zugewiesen werden, was für WAN und LAN schon beim Setup am Terminal geschehen ist. Der Name für die Wireless-Schnittstelle ist frei wählbar; *WLAN* bietet sich an. Unter diesem Namen finden Sie das Interface dann im Menü wieder und können es konfigurieren. Wichtig bei der Konfiguration ist, das Häkchen bei *Enable* zu setzen, damit die Karte aktiv wird. Im Linux-Professionell-Praxistest bewährte sich die Konfiguration mit statischer IP-Adresse. Der Wireless-Zugang muss sich in einem anderen Netzwerk-Segment befinden als das LAN, also zum Beispiel:

```
LAN 192.168.1.1
WLAN 192.168.2.1
```

Bridging wird abgeschaltet. Der Abschnitt *Wireless Configuration* erscheint auf dieser Seite nur, wenn die Karte korrekt als Funk-Netzwerkkarte erkannt wurde. Der WLAN-Standard IEEE 802.11 steht in den Varianten b und g zur Verfügung. Im Test funktionierten beide, die neuere und schnellere Variante g ist zu bevorzugen. Der Modus wird auf *Access Point* gesetzt, damit pfsense als solcher funktioniert. Der *802.11g OFDM Protection Mode* dient dazu, ältere Geräte, die mit dem Protokoll IEEE 802.11b funken, reibungslos in das g-Netz einzubinden.

Service Set Identifier

Der Service Set Identifier, kurz SSID, ist der Name Ihres Access-Points. Diesen sendet die AP im Klartext durch den Äther. Clients können auf der Suche nach Anschluss entweder auf diesen Namen eingestellt werden oder sie benutzen den Platzhalter *ANY*, um sich einem beliebigen Hotspot anzuschließen. Der Broadcast des SSID kann von pfsense unterdrückt werden, was aber wenig sinnvoll ist, da er von WLAN-Sniffern trotzdem ermittelt werden kann, sobald ein legitimer Client eine Verbindung aufbaut.

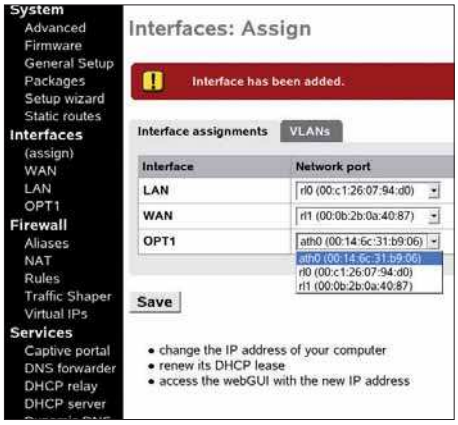
Wer will, kann mit einem Häkchen bei *802.11g only* ältere WLAN-Geräte vom Hotspot ausschließen. Wer den Clients erlauben

will, untereinander Daten auszutauschen, aktiviert die Option *Allow intra-BSS communication*. Das ist aber aus Sicherheitsgründen keinesfalls zu empfehlen, denn diese Datenpakete umgehen automatisch den Packet-Filter der Basisstation.

Sollen am Hotspot Datenpakete nach einer Quality-of-Service priorisiert werden, so muss die WLAN-Karte das unterstützen. Mit einem Klick bei *Enable WME* schalten Sie die entsprechende Option ein.

Sendeleistung vorgeben

Unter *Transmit Power* kann die Sendeleistung der WLAN-Karte eingestellt werden. Im Normalfall ist – wie voreingestellt – die



In dieser übersichtlichen Eingabemaske legen Sie fest, dass pfsense als Access-Point fungieren soll

höchste Sendeleistung sinnvoll. Wer aber Nachbarn am Lauschen hindern will, kann die Funkstärke hier reduzieren – zusätzlich zur WPA-Verschlüsselung.

Pfsense kann auf den Kanälen eins bis elf senden. Welche davon tatsächlich zur Verfügung stehen, hängt von der WLAN-Karte und den Clients ab. Der im Test verwendete Client unterstützt die Kanäle 10 bis 13. Lassen die Tester pfsense den Kanal automatisch wählen, kommt keine Verbindung zustande. Erst nachdem die WLAN-Karte manuell auf Kanal 10 oder 11 gesetzt wird, finden sich die Funk-Partner.

Internet-Verbindung

Mit der WLAN-Verbindung allein ist noch keine TCP/IP-Verbindung möglich. Diese lässt sich herstellen, indem Sie in pfsense auf der statischen IP der WLAN-Karte einen DHCP-Server einrichten. Unter *Services/DHCP-Server* lässt sich für jedes lokale Netzwerk-Segment ein eigener DHCP-Server einrichten. Die Einstellungen sind schnell erledigt: Ein Häkchen, um den Service zu aktivieren, Start- und End-Adresse des IP-Bereichs eingeben, speichern, fertig. Beim nächsten Connect steht dem Client auch eine TCP/IP-Verbindung zur Verfügung, was sich per Ping auf pfsense leicht verifizieren lässt.

Nur der Internet-Zugang funktioniert noch nicht. Das liegt daran, dass der Paketfilter auf der pfsense-Maschine keine Anweisung hat, Datenpakete von WLAN nach WAN durchzulassen. Eine entsprechende Regel muss erst unter *Firewall/Rules* definiert werden. Hier finden Sie drei Register: LAN, WAN und WLAN. Unter LAN ist eine allgemeine Durchlass-Regel für den Internet-Zugang vorgegeben. Wer die Einstellungen für WLAN übernimmt, kann nach dem Neuladen der Regeln drahtlos im Internet surfen.

Verschlüsselung einstellen

Das kann jetzt allerdings auch die gesamte Nachbarschaft. Um der unbefugten Nutzung einen Riegel vorzuschieben, sollte nach einem ersten kurzen Testlauf die WPA-Verschlüsselung aktiviert werden. Wer sich nur in der Wohnung mit dem Notebook frei bewegen will, hat die Konfiguration abgeschlossen. Wollen Sie den Access-Point aber auch als öffentlichen Hotspot einsetzen, müssen Sie noch das Captive Portal aktivieren. Die dafür zuständigen Einstellungen sind unter *Services* zu finden.

Geben Sie an, dass das Captive Portal aktiviert werden soll, und ordnen Sie diesem die WLAN-Schnittstelle zu. Als Methode zur Authentifizierung wählen Sie *local user manager*. Die weiteren Einstellungen können Sie unberührt lassen und auf *Save* klicken. In dem Moment werden alle bestehenden TCP/IP-Verbindungen zu WLAN-Clients unterbrochen. Die Funkstrecke bleibt aber bestehen. Wenn Sie jetzt noch unter dem Karteireiter *Users* Benutzernamen und Passwörter anlegen, ist das Captive Portal einsatzbereit: WLAN-Clients, die eine Internet-Verbindung aufbauen wollen, werden zur Log-in-Seite umgeleitet und bekommen erst dann Zugang, wenn sie Benutzernamen und Passwort richtig eingeben.

Feintuning von pfsense

Sollen einzelne Geräte das Captive Portal umgehen dürfen, so kann deren MAC-Adresse im Register *Pass-through MAC* eingetragen werden. Denken Sie aber daran, diese Einstellung anzupassen, wenn Sie am Client eine Netzwerkkarte austauschen.

Die vorgegebene Portalseite ist nur ein Provisorium. Sie können eine eigene Portalseite erstellen und unter *Portal page contents* auf die pfsense-Maschine hochladen. Das Gleiche gilt für die Fehlerseite, die bei misslungenen Anmeldeversuchen erscheint. Falls Sie Grafiken oder PHP-include-Dateien verwenden wollen, können Sie diese Elemente im Register *File Manager* ebenfalls direkt auf pfsense speichern. Dabei müssen Sie aber sparsam sein, denn es sind insgesamt nur 256 KByte erlaubt.

Portalseite im Detail

Die Portalseite muss ein Formular mit einem Post-Request an die Variable *$PORTAL_ACTION$* enthalten. Der Submit-Button muss

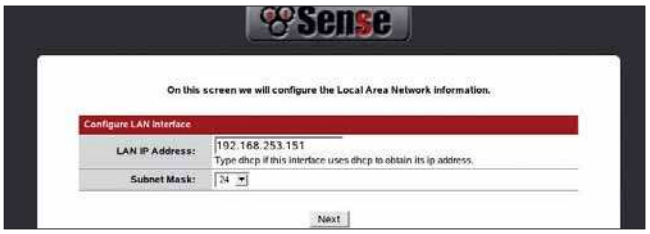
pfsense

Die Firewall-Distribution auf Basis von FreeBSD 6 läuft sowohl auf PCs als auch auf Embedded-Plattformen. Geeignet ist unter anderem die Embedded-Hardware von Soekris und PC Engines. Auf einem solchen Gerät installieren Sie pfsense, indem Sie das Image auf eine CF-Speicherkarte schreiben und diese in den Embedded-PC einstecken. Fertig ist die stromsparende und leise Firewall. Pfsense kann so viele Netzwerk-Schnittstellen verwalten, wie die Hardware verkraftet.

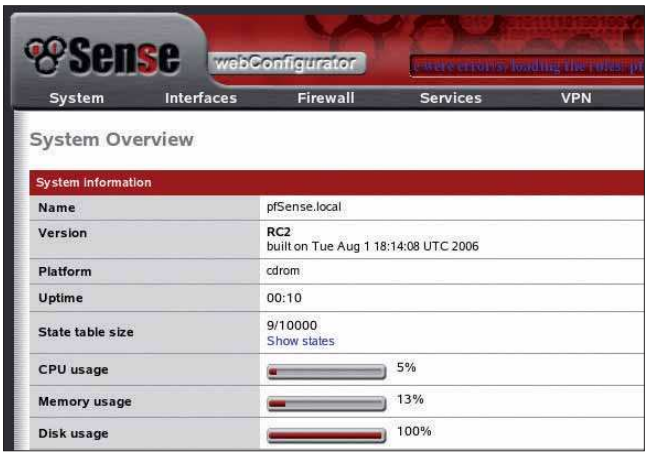
Pfsense bietet auch ein einfaches Konsolen-Menü. Dieses ist aber nur bei den ersten Konfigurationsschritten hilfreich. Ansonsten lässt sich das System viel komfortabler per Web-Interface bedienen. Das Gerät lässt sich per Web aktualisieren. Allerdings sind keine Patches vorgesehen, sondern das Betriebssystem wird vollständig ersetzt. Die Firewall-Regeln können in einem komfortablen Regel-Editor definiert werden. Hier lässt sich auch der Schutz vor ICMP-Attacken einrichten. Ein DNS-Proxy sorgt für schnelle Namensauflösung im Netz und ein Client für dynamische DNS-Dienste besorgt eine feste Adresse für die Nutzung von DSL.

Wer größere Netze mit pfsense absichern will, kann mehrere Geräte per Load-Balancing und Fail-over verbinden. Dieses Konstrukt lässt sich dann auch per SNMP überwachen. Wer will, kann seinen WLAN-Anschluss per OLSR für Freifunknetze öffnen. Aber auch die Privatsphäre ist gut geschützt. So können VPN-Verbindungen über IPsec, OpenVPN, PPPoE und PPTP hergestellt werden.

Damit die drahtlosen Clients sich automatisch zurechtfinden, bekommt das WLAN einen eigenen DHCP-Server



Für die Authentifizierung der Wireless-Nutzer sorgt das Captive Portal



Welcher Benutzer mit welchem Passwort die Verbindung herstellen darf, legen Sie im User Manager fest

accept heißen; in einem verborgenen Feld namens *redirurl* muss der Wert *$PORTAL_REDIRURL$* übermittelt werden.

Benutzername und Passwort werden in Feldern mit den Namen *auth_user* beziehungsweise *auth_pass* gesendet. Zusammen ergibt das einen HTML-Quelltext, der in der Praxis ungefähr so aussieht:

```
<form method="post"
action="$PORTAL_ACTION$">
   <input name="auth_user"
type="text">
   <input name="auth_pass"
type="password">
   <input name="redirurl"
type="hidden"
value="$PORTAL_REDIRURL$">
   <input name="accept"
type="submit" value="Anmelden">
</form>
```

Damit die Benutzer sich auch selbst wieder abmelden können, aktivieren Sie die Option *Enable logout popup window*. Dieses automatisch geöffnete Fenster enthält Schaltflächen, mit denen der Benutzer seinen Account problemlos selbst schließen kann.

Wer einen öffentlichen Access-Point betreibt, will meist, dass die Benutzer nach dem Log-in noch eine Willkommens-Seite zu sehen bekommen. Mit pfsense ist das kein Problem: Tragen Sie die gewünschte Adresse einfach bei *Redirection URL* ein.

Benutzer sollten sorgfältig mit ihren Zugangsdaten umgehen. Sie sollten sie nicht weitergeben oder sich parallel mit mehreren Clients anmelden. Um das zu verhindern, kreuzen Sie *Disable concurrent logins* an. Wer seine Zugangsdaten an Freunde weitergibt, fliegt dann aus dem Netz, sobald sich einer dieser Freunde anmeldet.

Öffentlicher Hotspot

Das Captive Portal von pfsense ist keine spezielle Lösung für den Einsatz als öffentlicher Hotspot. Aber es lässt sich mit ein bisschen Programmierarbeit zu einer solchen Anwendung erweitern. Denkbar ist beispielsweise ein selbst programmiertes Script, das zufällig Benutzernamen und Passwort generiert, sobald ein Kunde ein Ticket kauft. Diese Zugangsdaten werden dann einerseits für den Kunden ausgedruckt und andererseits per HTTP-Script in die Benutzerverwaltung von pfsense eingetragen.

Wie lange WLAN-Sitzungen dauern dürfen, kann in der Timeout-Variablen des Captive Portals eingestellt werden. Die Redirect-Seite, die nach dem Log-in erscheint, sollte dann einen Countdown-Timer in Javascript enthalten, damit der Kunde nicht ohne Vorwarnung vom Netz getrennt wird.

Sicherer HTTPS-Log-in

Wer seinen Hotspot-Besuchern ein Log-in per HTTPS ermöglichen will, benötigt dazu auf jeden Fall ein Zertifikat im X.509-Format mit RSA-Privatschlüssel. Servername, Zertifikat und Schlüssel werden per Cut and Paste in die entsprechenden Eingabefelder unten auf der Einstellungsseite des Captive Portals eingetragen.

Log-in über RADIUS

Wer das Log-in noch komfortabler handhaben möchte, kann auch einen RADIUS-Server anbinden. Maximal zwei solcher Server können mit IP-Adresse, Port und Schlüssel eingetragen werden. Wer einen kommerziellen Hotspot betreibt, für den sind die Accounting-Funktionen von RADIUS für die Abrechnung überaus interessant. Um sie mit pfsense zu nutzen, aktivieren Sie die Option *send RADIUS accounting packets*.

RADIUS erlaubt auch flexiblere Log-in-Zeiten. Dazu werden im RADIUS-Server minutengenaue Nutzungszeiten eingetragen. Der Benutzer wird vom Captive Portal jede Minute erneut beim RADIUS-Server authentifiziert. Ist die Nutzungsdauer abgelaufen, wird die Verbindung getrennt.

Fazit: voll praxistauglich

Für einen Wireless Access-Point mit Open Source ist pfsense die optimale Lösung. Wer sich nur mit dem Laptop frei bewegen will, braucht lediglich eine passende WLAN-Karte in den pfsense-Rechner einzubauen und zu konfigurieren. Für Access-Points mit mehreren festen Benutzern ist das Captive Portal geeignet. Es leitet jeden Verbindungsversuch zunächst auf eine Log-in-Seite um. Und mit der Anbindung an einen RADIUS-Server und etwas zusätzlicher Programmierarbeit lässt sich mit pfsense sogar ein kommerzieller öffentlicher Hotspot aufbauen. ■