UTM-Appliance für kleine Benutzergruppen im Test

Zwergenwacht

Wirksamer Schutz durch den Verbund abgestimmter Komponenten – das ist das Geheimnis so genannter UTM-Appliances (Unified Threat Management). Bisher waren sie oft nur für große Anwender erschwinglich. Nun ist am unteren Ende der Preisskala ein bemerkenswerter Wettbewerber aufgetaucht: Black Dwarf. Jens-Christoph Brendel

Für den Einsatz in großen Umgebungen gab es Kombinationen aus Firewall, VPN-Gateway und Proxy-Servern für die Absicherung von Netzwerk, Web und Mail schon lange. Für kleinere Umgebungen haben etwa Gateprotect, Zyxel, Astaro oder Sonicwall schon geraume Zeit ähnliche Angebote im Programm. Allerdings waren hier wie bei den großen Geschwistern oft Extrakosten pro Modul fällig und das Preisniveau lag in der Regel jenseits der 500-Euro-Marke. Mit ihrer Black Dwarf (schwarzer Zwerg) getauften Linux-Appliance brachten die Partner Wortmann und Securepoint nun eine UTM-Appliance auf den Markt, die diese Marke noch einmal deutlich unterschreitet: Nur noch knapp 370 Euro für alles soll die Wunderwaffe kosten. Was kann man für diesen Preis erwarten?

Anschluss finden

Eine erste Irritation erleben viele Anwender womöglich schon kurz nach dem Auspacken des zigarrenkastengroßen schwarz-roten Geräts (Abbildung 1). Es ist nämlich für eine Installation zwischen DSL-Modem und LAN gedacht, eine Stelle, die Benutzer eines WLAN-Routers, den die DSL-Provider heute standardmäßig mitliefern, gar nicht mehr erreichen. Stattdessen müssten Modem und Router getrennt sein. Ansonsten bliebe nur ein Anschluss auf der LAN-Seite des Routers, wo aber nicht nur kein Funk nutzbar wäre, sondern die Appliance wegen der Network Address Translation des Routers auch nicht mehr ohne Weiteres von außen zu erreichen wäre, was etwa das integrierte VPN-Gateway entwerten würde.

Ein funktionierender Workaround für diesen Fall ist, auf dem WLAN-Router alle Ports und Protokolle an die im LAN dahinter stehende Appliance weiterzuleiten. Die Fritzbox Fon WLAN 7170 beispielsweise kennt unter »Portfreigabe« eine Option »Exposed Host«, die sämtliche Zugriffe unter Umgehung ihrer eigenen Firewall an eine Adresse im LAN durchreicht.

Ist das Gerät erst einmal verkabelt und ins Netzwerk integriert, kann der Benutzer sofort via Webinterface auf die Administrationsoberfläche zugreifen (Abbildung 2). Die Gestaltung ist übersichtlich, wenn auch die dunkle, türkisfarbene Schrift der Menüs auf schwarzem Grund nicht unbedingt optimale Lesbarkeit garantiert. Nach einer Registrierung, die den Zugang

◀ Abbildung 1: An seiner Rückseite bietet der schwarze Zwerg Anschlüsse für DSL-Modem, LAN und DMZ sowie einen seriellen und zwei USB-Ports.

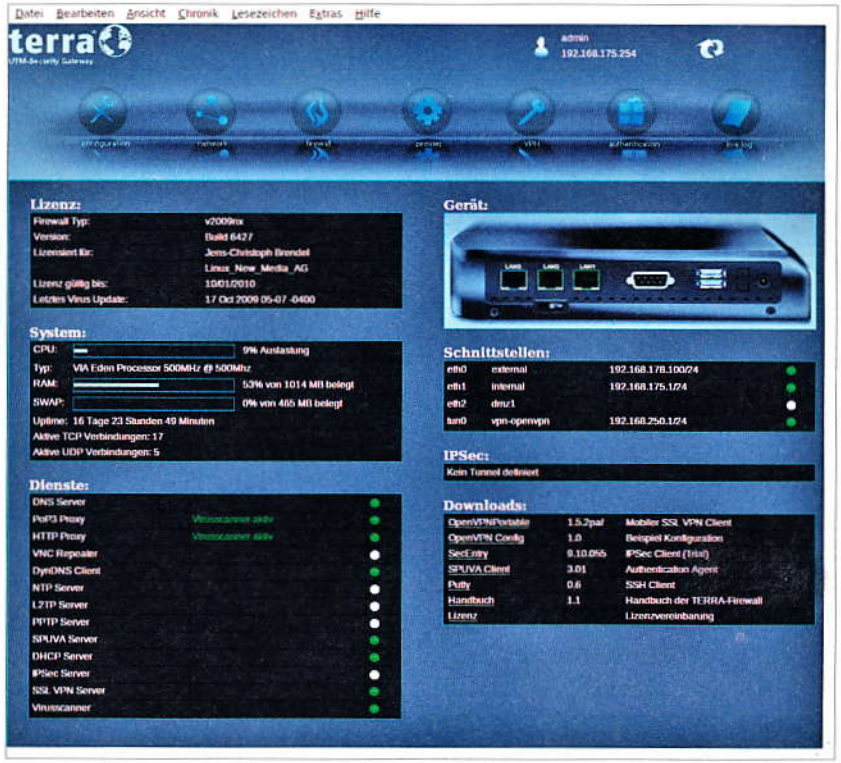
UTM-Appliance Black Dwarf

Hersteller: Securepoint/Wortmann
Internet: [http://www.terra-firewall.com]
Geeignet für: 1 bis 5 Nutzer
Funktionen: Firewall, VPN-Gateway, Mail- und HTTP-Proxy, Virenscanner, Spamfilter
Preis: 370 Euro

zu den Updates für die Firmware und vor allem den Virenscanner freischaltet und die der Benutzer nach einem Jahr periodisch kostenpflichtig erneuern muss, kann es losgehen.

Appliance einrichten

In den Menüs findet sich der erfahrene Admin schnell zurecht – allerdings nur, weil ihm die Funktionsprinzipien der einzelnen Module und die Terminologie sicher bereits vertraut sind. Absolute Einsteiger in Sachen Security wären wohl überfordert, zumal das mitgelieferte Handbuch keine zusammenhängenden Darstellungen von Konfigurationsabläufen bietet. Wesentlich besser ist da die online verfügbare überarbeitete Handbuch-Version [1]. Sie enthält einen



▶ **Abbildung 2: Die Startseite der Appliance bietet eine Statusübersicht und die Einstiegspunkte in die einzelnen Kapitel der Konfiguration.**

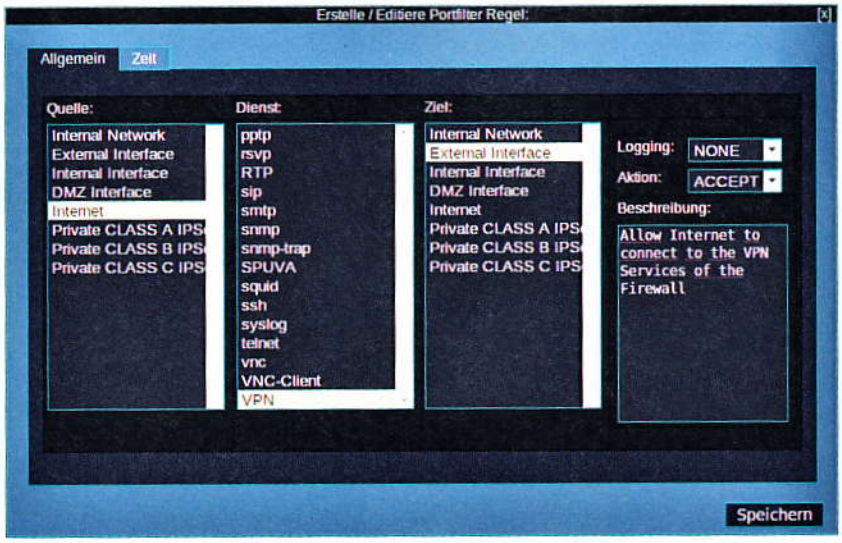


Abbildung 3: Die Firewall kann man einfach um neue Regeln – wie hier für einen VPN-Zugang – erweitern.

„Schritt-für-Schritt-Anleitungen" genannten Teil, der beispielsweise das komplexe Vorgehen beim Einrichten einer VPN-Verbindung Menü-übergreifend erklärt. Bei Problemen helfen auch die Support-Foren des Herstellers [2] sehr schnell und kompetent weiter.

Alternativ ist auch eine Konfiguration über ein Command-Line-Interface möglich, das nach einem SSH-Login auf der Appliance erreichbar ist. Über dessen Möglichkeiten schweigt sich das Handbuch aber konsequent aus.

Features

Das Kernstück der Appliance ist eine Firewall, für die sich in einer grafischen Oberfläche recht einfach Portfilter konfigurieren lassen (Abbildung 3). Für die Verwendung in Regeln darf der Admin sich eigene Services und Netzwerkobjekte definieren. Port-Weiterleitung und -Übersetzung sind möglich. Zusätzlich lässt sich der Geltungsbereich von Regeln zeitlich einschränken. Alle Aktionen der Firewall protokolliert auf Wunsch ein filterbares Log.

Die Filterung von Webinhalten und das Virenscannen realisiert ein HTTP-Proxy. Neben Black- und Whitelists für URLs existiert auch ein einfacher Contentfilter auf Basis von Suchwörtern, der aber prinzipbedingt nicht sonderlich überzeugt, zumal er nur eine Auswahl englischer Kategorien bietet und den Benutzer darüber im Unklaren lässt, welche Schlagwörter in welcher Sprache er mit welcher Kategorie verbindet.

Ein Mailproxy schützt den elektronischen Briefverkehr mit einem Spamfilter und ebenfalls vor Viren – allerdings nur, solange man sich auf POP3 beschränkt. Nutzer von IMAP-Accounts gehen leer aus. Sichere Remote-Zugänge offeriert ein VPN-Gateway, das IPsec, das Microsoft-typische PPTP beziehungsweise L2TP sowie SSL-VPN (sprich Open VPN) beherrscht. Mit all diesen Methoden sind über die Appliance leicht sichere Zugänge für Außendienstler oder Teleworker zu realisieren.

Angelehnt an das VPN-Tool verwaltet die Appliance auch Benutzer und X.509-Zertifikate (Abbildung 4). Die Zertifikate erstellt der Admin hier und exportiert sie dann. Für die User-Authentifizierung lässt sich statt der internen Datenbank auch ein LDAP-Server einbinden.

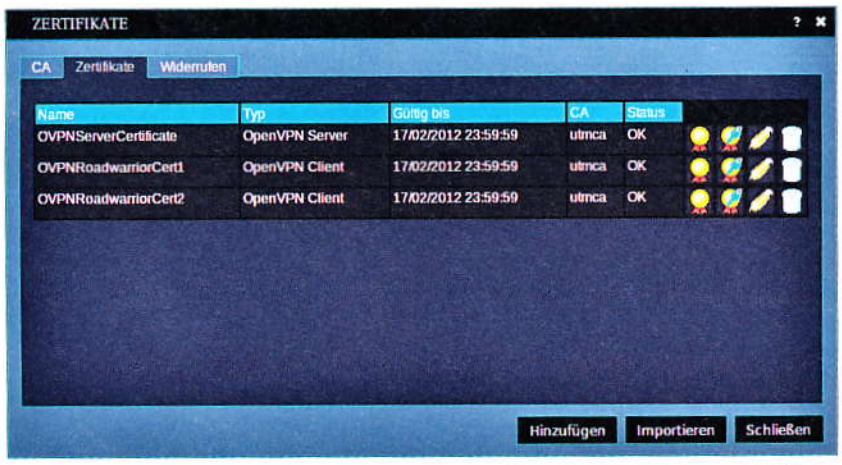


Abbildung 4: Das VPN-Tool der Appliance erzeugt die nötigen Zertifikate für die Root-Instanz und die Clients, die sich später leicht exportieren lassen.

Zwergenaufstand

Wer die kleinen Abstriche bei Dokumentation und Usability in Kauf nimmt und mit POP3 auskommt, der erhält mit dem schwarzen Zwerg eine UTM-Appliance, die einen Heimarbeitsplatz oder eine Außenstelle mit bis zu fünf Mitarbeitern zuverlässig gegen unerwünschte Zugriffe, Spam und Viren absichert. Ein Test mit gängigen Security-Scannern ergab keine Schwachpunkte. Die Contentfilter mögen als Kindersicherung durchgehen, eine hundertprozentige Abschottung gelingt mit ihnen aber nicht. Das dürfte beim Büroeinsatz aber ohnehin eher ein Randthema sein.

Das kleine lüfterlose Gerät ist schnell ins Netzwerk integriert, jedenfalls wenn entweder Modem und Router getrennt sind oder der Router die Weiterleitung aller Ports gestattet und das WLAN nicht in den Schutz einzubeziehen ist.

Die Konfiguration über das Webinterface geht leicht von der Hand, sofern der Benutzer sich mit den Konzepten und Begriffen auskennt. Das Handbuch assistiert bei der Bedienung, ersetzt aber keinen Grundkurs in Security. Was die Entscheidung versüßen dürfte, ist der sehr günstige Preis, mit dem bereits alle Module bezahlt sind. ■

Infos

[1] Handbuch-Update: [https://www.terra-firewall.com/d_dokumente.html]

[2] Support-Foren: [https://www.terra-firewall.com/forum/]