Praxistest: Komplette Firewall inklusive Konfigurationssoftware auf USB-Stick

Streichholzschachtel

Er ist kleiner als ein Feuerzeug, trotzdem verwandelt der Firestick jeden PC in eine Firewall. Der Rechner benötigt zwei Netzwerkkarten und muss vom USB-Stick booten, CD-ROM und Festplatte sind überflüssig. Der Praxistest zeigt Stärken und Schwächen dieser Neuentwicklung. Christian Ney

Linux-Firewalls gibt es zwar schon viele, aber die Software auf einen USB-Stick zu packen ist eine neue Idee. Der Hersteller Databay hat sein Java-Konfigurations-Frontend gleich mit auf dem Firestick [1] abgelegt. Damit trägt das nur daumengroße Gerät die gesamte benötigte Software. Der Stick arbeitet in zwei Modi: Während der Konfiguration steckt er im Rechner des Admin und lässt sich per Java-Programm beschreiben. Im Betrieb am Firewallrechner ist der Schreibschutz aktiviert.

Firewall und VPN

Ein optional erhältliches VPN-Modul ergänzt den Funktionsumfang um IPsec-Tunnel. Das Firewallregelwerk einrichten und einen Tunnel konfigurieren gelingt dank der grafischen Oberfläche auch mit Linux nicht vertrauten Anwendern, auf die Kommandozeile müssen sie nicht zurückgreifen.

Im GUI enthalten sind zudem Funktionen wie Update, Verwaltung verschiedener Konfigurationen, Backup und Restore. Da das GUI in Java programmiert ist, darf der Administrationsrechner mit einem beliebigen Betriebssystem laufen. Laut Hersteller ist als Voraussetzung nur ein aktuelles Sun-JRE (Java Runtime Environment) ab Version 1.4.1 nötig. Im Test lief die Software aber auch mit der Blackdown-Software.

Hardware-Ansprüche

Als Firewallrechner ist ein handelsüblicher x86-Rechner ausreichend. Er benötigt mindestens 128 MByte Speicher, zwei Netzwerkkarten und eine USB-1.1-Schnittstelle. Wer die erweiterten Fähigkeiten des Firestick – etwa die Proxy-Dienste – einsetzen will, sollte jedoch am Speicher nicht sparen. Selbst 256 MByte RAM sind nur für sehr wenige Nutzer ausreichend, da der Proxy sämtliche Daten im Speicher vorhalten muss. Zum Ausgleich darf der angehende Firewallbesitzer an den Laufwerken sparen: CD-ROM oder Festplatten sind unnötig.

Einfach einen ausgemusterten Computer zur Firestick-Firewall erklären ist aber nicht so einfach möglich: Der Rechner muss von der USB-Schnittstelle booten, das können nur neuere Modelle. Auch bei einer Neuanschaffung ist Vorsicht geboten, da manche aktuellen Rechner diese Option im Bios nicht vorsehen. Zu den Vorteilen siehe Kasten „Warum USB-Stick“.

Eine Firewall muss möglichst störungsfrei laufen, meist 24 Stunden täglich. Bei der Auswahl der Teile ist diese Dauerbelastung zu berücksichtigen. Wer auch für Ausfälle gewappnet sein muss, sollte sich gleich einen Ersatzrechner zulegen. Die zweite Maschine kann er dann mit Hilfe des Konfigurationswerkzeugs als Backup vorbereiten und muss ihn im Fall der Fälle dann nur noch mit dem Firestick booten.

Netzwerkkarten

Der Hersteller weist explizit darauf hin, dass der Firestick nicht als Personal Firewall gedacht ist. Es bringt also wenig, den Rechner nur mit einer Netzwerkkarte auszurüsten, mindestens zwei Interfaces sind Pflicht. Die Software erkennt alle unter Linux gängigen 10/100 MBit-Karten sowie diverse Gigabit-Netzwerkkarten. Bei Letzteren sind die Kerneltreiber aber noch nicht immer ganz ausgereift.

Mit WLAN-Karten arbeitet das Firestick-System noch nicht zusammen. Wer sein Funknetzwerk schützen möchte, muss dafür ein eigenes Netz zwischen Access Point und Firewall einrichten. Da die

Firestick

Kategorie: Linux-basierte Firewallsoftware auf USB-1.1-Stick, optional mit VPN-Funktion

Hardware: USB-Stick, 64 MByte, schaltbarer Schreibschutz

Konfiguration: Per Java-GUI auf einem Admin-PC; die Software und die Konfigurationsdateien liegen auf dem Firestick

Preis: Grundpreis 700 Euro, mit VPN-Option 1400 Euro; Vertrieb nur über Reseller

WEP-Verschlüsselung als unsicher gilt [2], bietet sich die VPN-Option an. An der Unterstützung für Karten mit bestimmten Prism-Chipsätzen arbeitet Databay derzeit. Da die Linux-Treiber für 54-MBit-Karten teilweise noch nicht ausgereift ist, treten hier jedoch noch Schwierigkeiten auf.

Neben Ethernet unterstützt der Firestick derzeit PPP, ISDN und DSL über PPPoE. Alle Varianten lassen sich mittels grafischer Oberfläche sehr einfach konfigurieren. Das GUI fragt die vom Provider zugeteilten Zugangsdaten ab. Für DSL kann der Admin sogar die MRU- und MTU-Größen einstellen.

Wer vom ISP ein kleines IP-Subnetz zugewiesen bekommen hat, kann mit so genannten virtuellen Interfaces einen oder mehrere Server hinter einer offiziell gerouteten Adresse verstecken (Destination-NAT, DNAT). Der Server selbst erhält eine private IP-Adresse, die Firewall leitet die Verbindungswünsche weiter. In diesen Fällen ist eine DMZ zu empfehlen, die sich als eigene Zone definieren und verwalten lässt.

Der Firestick enthält eine spezielle Linux-Distribution von Databay. Sie begnügt sich mit gerade mal 26 MByte; der USB-1.1-Stick fasst aber 64-MByte, mehr als genug Platz für mehrere Konfigurationen. Trotz ihrer geringen Größe enthält die Distribution auch Proxy-Dienste für HTTP, FTP, SMTP, POP3 und DNS. Sie entstammen ausgereiften Open-Source-Paketen, etwa Tinyproxy [3]. Die Firewall arbeitet auf Wunsch auch als DHCP-Client, -Server oder -Relay.

Firestick-OS

Zum Einsatz kommt ein angepasster Kernel 2.4.24. Neben Modulen für eine möglichst breite Hardware-Unterstützung sind einige Patches eingebunden, die die Sicherheit verbessern:

- NAT-Helper für Dienste wie IRC, FTP und H.323. Damit lassen sich Clients, die diese problematischen Protokolle verwenden, hinter der offiziellen IP-Adresse der Firewall verstecken.
- Das Firestick-OS verwendet zufällige TCP-Sequenznummern. Angreifer haben es damit schwerer, Netzwerkverkehr zu spoofen, auch das Fingerprinting (Ermitteln des eingesetzten Betriebssystems) ist erschwert.
- Zusätzlich ist der Kernel mit dem GR-Security-Patch [4] versehen. Dessen Bestandteil Pax [5] vereitelt das Ausnutzen eventueller Sicherheitslücken, speziell Buffer Overflows.

Auch bei der Konfiguration der Firewallregeln setzt Databay auf bewährte Open-Source-Technik: Beim Start des Rechners überträgt Shorewall [6] das Regelwerk in IPTables-Befehle.

Erste Amtshandlung: Software-Update

Schon beim Auspacken fallen zwei Zettel auf. Einer weist auf die Lizenzierung hin, siehe Kasten „Lizenzfragen“. Der zweite schlägt vor, noch vor der ersten Nutzung ein Update der Software durchzuführen (Abbildung 1). Der Text erklärt auch, wie dies im Einzelnen funktioniert. Der Admin steckt den Firestick dazu an einen beliebigen PC.

Je nach Herstellungsdatum des Sticks ist das Update sehr zu empfehlen. Kurz vor Ende dieses Tests hat Databay einige signifikante Verbesserungen eingeführt, die besonders Teile des GUI vereinfachen. So ist es jetzt möglich, Einträge in Listenfeldern zu filtern oder zu sortieren. Praktische Helfer wie der Subnetzrechner und der DNS-Resolver sind nun auf den ersten Blick direkt neben dem Eingabefeld für IP-Adressen sichtbar. Früher musste man sie erst in der Menüleiste aufspüren und starten.

Vor das Update hat Databay jedoch eine Registrierung gesetzt. Die hier angegebenen Daten dienen später zum Einloggen in einen geschützten Bereich der Firestick-Homepage. Dort kann man die persönlichen Daten ändern und einen Dyn-DNS-Namen für seinen Firestick eintragen. Rechner mit einer dynamischen IP-

Warum USB-Stick

Im Gegensatz zu bekannten Lösungen, die von Diskette oder CD booten oder auf der Festplatte installiert sind, arbeitet der Firestick als bootfähiger USB-Stick. Diese Technik bringt einige Vorteile mit sich:

- Kein mechanischer Verschleiß. Der USB-Stick ist nur zum Booten nötig, die Firewall bezieht danach alle Daten aus dem Arbeitsspeicher.
- Schreiben und Lesen sind im RAM schneller als auf Festplatten.
- Sollte doch einmal ein Cracker in die Firewall eindringen, lassen sich Rootkits und andere Hinterlassenschaften sehr einfach durch einen Neustart beseitigen. Pflicht bleibt es, mindestens das Root-Passwort zu ändern sowie die Lücke zu analysieren und zu schließen. Eine Neuinstallation kann aber entfallen.

Hat der Admin den sichersten Weg gewählt und den USB-Stick nach dem Booten entfernt, müsste er nach einem Ausfall vor Ort den Stick erneut anstöpseln. Ein Reboot aus der Ferne per Powerswitch gelingt nur, wenn der Firestick im Gerät stecken bleibt. Ein Teil der zusätzlichen Sicherheit löst sich damit aber in Wohlgefallen auf.

Als besonders praktisch erweist sich das Gerät, wenn die Firewall-Hardware den Anforderungen nicht mehr gerecht wird. Es genügt, einen neuen Rechner vorzubereiten und den altgedienten durch einfaches Umstecken zu ersetzen.

Lizenzfragen

Die Databay AG unterscheidet bei der Lizenzierung der auf dem Firestick enthaltenen Software zwischen der eigenen Linux-Distribution (genannt Firestick-OS) und der Konfigurationsoberfläche (Firestick-APP).

Die Softwarepakete des Firestick-OS liegen im Verzeichnis »/system«. Sie unterstehen verschiedenen Open-Source-Lizenzen, etwa der GPL, LGPL, BSD oder ISC-Lizenz. Im Wortlaut finden sich diese Lizenzen unter »/licenses«. Änderungen und Erweiterungen am Sourcecode, die Databay-Entwickler vorgenommen haben, flossen dabei in Form von Patches zurück an die Entwickler der jeweiligen Software. Wer selbst einen Blick in den Quellcode werfen möchte, kann ihn GPL-konform auf einer CD anfordern.

Die Module der Konfigurationssoftware sind unter »/fsadm/modules« zu finden. Diese Software und mehrere andere Dateien unterliegen einer unfreien Lizenz, die eine zeitlich begrenzte Nutzung der Software sowie der Updatefunktion zusichert. Zudem schränkt die Lizenz den Firestick-Betrieb auf höchstens zwei Rechner ein: Produktiv- und Backupsystem. Das GUI hingegen darf der Admin auf jedem beliebigen Rechner nutzen. Auch ist die Anzahl der Clients nicht eingeschränkt.

Sicherheitskopien darf der Firewall-Admin ausschließlich mit Hilfe der Sicherungsfunktion der Konfigurationsoberfläche durchführen. Sämtliche Pakete und Dateien inklusive ihrer Lizenz kann er im Control Center unter »Über | Lizenz lesen« einsehen.

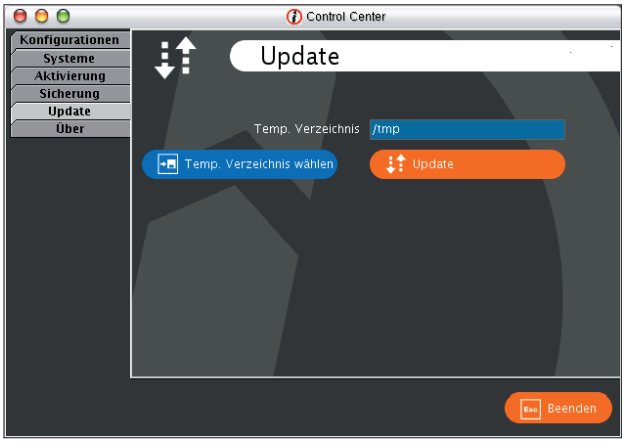

Abbildung 1: Der Hersteller empfiehlt dem neuen Firestick-Besitzer ein sofortiges Update. Damit hat er immer den aktuellen Release-Stand, selbst wenn das Herstellungsdatum schon etwas zurückliegt.

Abbildung 2: Das Control Center dient als zentrale Schaltstelle der Firestick-Software. Am linken Rand ist das Hauptmenü angeordnet, in der Mitte sind drei Konfigurationsvarianten gelistet.

Adresse lassen sich dann einfacher zu einem VPN verbinden.

Das Update läuft SSL-gesichert über einen Server von Databay. Sofern Neuerungen anstehen, informiert die Software den Admin über die Anzahl der aktualisierten Pakete. Was genau upgedatet werden soll, bleibt aber das Geheimnis dieser Routine. Wie lange das Laden und Installieren dauert, lässt sich einer Fortschrittsanzeige entnehmen. Nach Abschluss der Aktion ist das GUI neu zu starten, um in den Genuss einer eventuell erneuerten Oberfläche zu kommen.

Ziel erfassen: Der Firestick scannt die Hardware

Vor dem Konfigurieren der ersten Regeln sollte man den Firestick sein künftiges Zielsystem scannen lassen. Die Software identifiziert dabei die Netzwerkkarten, um sie den angeschlossenen Netzwerkzonen zuzuordnen. Diese Informationen landen auf dem USB-Stick und dienen als Basis für die Konfiguration. Wer auf den automatisierten Scan verzichtet, muss später sämtliche Netzwerkschnittstellen manuell anlegen.

Für den Scan ist die Firewallmaschine vom Firestick zu booten, der Schreibschutz muss deaktiviert sein. Netzwerkkabel dürfen noch nicht gesteckt, sollten aber bereits mit einem Hub oder einem Switch verbunden sein und bereitliegen. Ein Monitor ist nicht nötig, das System meldet sich akustisch.

Ein hoher, langer Signalton bedeutet, dass der Scan beginnt. Kurze Signaltöne fordern den Admin auf, die Interfaces nacheinander mit dem Netz zu verbinden. Ein einzelner Ton steht dabei für »eth0«, zwei Töne für »eth1« und so weiter. Pro Karte bleiben dabei 30 Sekunden Zeit, bis zwei kurze, unterschiedlich hohe Signale ertönen und der Scan beim nächsten Anschluss weitergeht. Drei kurze, hohe Töne signalisieren das Ende der gesamten Prozedur.

Bequemes Regelschieben im Java-GUI

Für die Konfiguration hat Databay ein Java-GUI entwickelt. Es läuft nicht auf der Firewall selbst, sondern auf der Workstation des Firewall-Administrators. Auf dem USB-Stick ist diese Software zusammen mit zwei Konfigurationsbeispielen abgelegt:

- Das rudimentäre Regelwerk »Demo1 NET-LOCAL« verbindet die Firewall per DSL mit dem Internet und erlaubt HTTP, FTP, SMTP, DNS und POP3 vom internen Netz nach draußen.
- Mit »Demo2 NET-LOCAL pro« arbeitet der Firewallrechner zusätzlich als DHCP-Server für die Rechner im LAN. Außerdem dürfen die Clients alle Dienste nur über die Proxys der Firewall nutzen.

Es ist zwar möglich, mit einer leeren Konfiguration anzufangen. Da sich die Optionsvielfalt aber nicht auf den ersten Blick erschließt, ist ein genauer Blick auf beide Beispiele sehr nützlich.

Beim Einstieg hilft die mitgelieferte Dokumentation leider nicht weiter: Dem Gerät lieg bis auf die beiden genannten Zettel kein informativ bedrucktes Papier bei. Immerhin findet sich ein HTML-Handbuch auf dem Stick, das die grundlegenden Dinge behandelt. Auch die Hilfefunktion des GUI greift nur auf diese Informationen zurück.

Leider bleiben nach der Lektüre viele Fragen offen. Ein Teil davon wird von der FAQ auf der Firestick-Webseite beantwortet, genauere Hinweise zur Einrichtung eines VPN sucht man allerdings auch dort vergeblich. Daher ist der Support oft zu konsultieren – er reagiert aber schnell und fachkundig. An der Dokumentation feilt Databay noch, Besserung ist also in Sicht.

Intuitive Werkzeuge

Glücklicherweise gestaltet sich die Arbeit mit dem Konfigurationswerkzeug recht intuitiv. Im Hauptmenü, hier »Control Center« genannt (Abbildung 2), lassen sich sämtliche Einstellungen vornehmen. Die Software kann mehrere Konfigurationen und Systeme verwalten, allerdings zieht die Lizenzierung eine klare Grenze (siehe Kasten „Lizenzfragen“). Vor der Inbetriebnahme einer Firewallmaschine ist eine so genannte Aktivierung erforderlich, die die Konfiguration auf einen Computer und dessen Backup-Rechner abstimmt.

Auch die Konfiguration lässt sich sichern: Ein Backup-Mechanismus speichert den ganzen Inhalt des Firestick in einer Zip-Datei. Die Update-Funktion ist ebenfalls im Control Center angesiedelt.

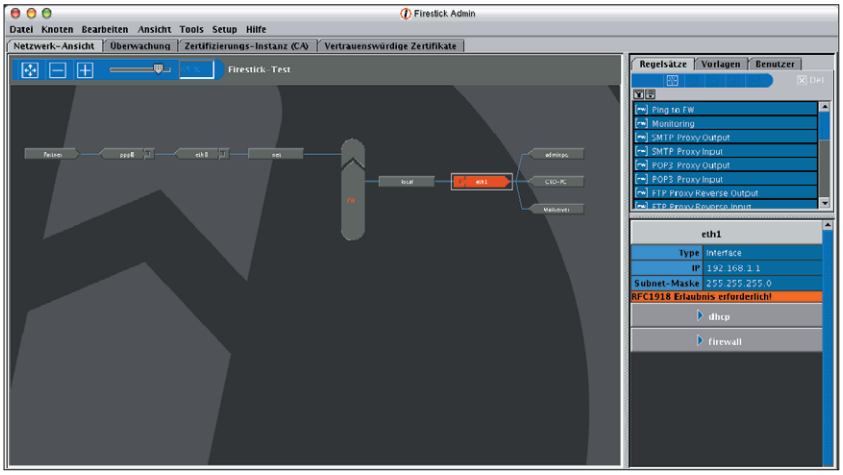

Abbildung 3: Der Konfigurationseditor bildet die Netzinfrastruktur als übersichtliche Grafik ab. Rechts unten meldet der Inspektor eventuelle Konfigurationsfehler: Hier fehlt eine Erlaubnis auf »eth1«.

Das Anlegen einer neuen Konfiguration fördert den Konfigurationseditor (Abbildung 3) zutage. Seine Oberfläche ist in vier Bereiche aufgeteilt:

- Die Karteireiter oben öffnen den Editor (Netzwerk-Ansicht), die Log-Auswertung (Überwachung) sowie CA-Konfiguration und Zertifikatsverwaltung. Die beiden zuletzt genannten Punkte gehören zur VPN-Option.
- Oben rechts befinden sich Listen: Regelsätze, die später den Zugriff auf Netzwerkobjekte freigeben oder verbieten, sowie deren Vorlagen und die lokale Firewall-Benutzerdatenbank.
- Darunter ist der Inspektor anzutreffen, er zeigt Informationen über das jeweils gewählte Objekt.
- Den größten Teil des Fensters nimmt das grafisch dargestellte Regelwerk ein, in dem alle relevanten Objekte aufgeführt sind. Per Icon lässt sich die Ansicht ins Fenster einpassen, verkleinern oder vergrößern.

Das zentrale Element des Regelwerks ist »FW«, die Firewall. Externe Netze (»net«) sind links, interne (»local«) rechts davon angeordnet. Danach folgen die Schnittstellen der Firewall, hinter ihnen liegen die Netzwerkobjekte.

Drag & Drop und Kontextmenü

Über das Kontextmenü der Objekte lassen sich neue Knoten anfügen, alte löschen oder Einstellungen anzeigen und ändern. Per Drag & Drop kann man Knoten verschieben, wobei die Software prüft, ob die Aktion sinnvoll ist. Sie verhindert etwa das Andocken einer Netzwerkschnittstelle direkt an den Rumpf der Firewall – das Interface muss Mitglied einer Zone sein.

Sowohl Netzwerkschnittstellen als auch die Endknoten der Firewall erlauben es, die zugehörige IP-Adresse manuell oder per DHCP zu vergeben oder zu beziehen. Die manuelle Eingabe wird von zwei Helfern unterstützt: dem Subnetzrechner und dem DNS-Resolver. Ersterer berechnet anhand der Angaben die richtige Subnetzmaske und die Netzwerkadresse et cetera, der Resolver löst Rechnernamen per DNS auf ihre IP-Adresse auf.

Als recht praktisches Werkzeug erweist sich der Inspektor. Er verschafft einen Überblick über die Einstellungen eines Objekts wie IP-Adresse, das zugehörige Regelwerk sowie mögliche Konfigurationsfehler. Ungereimtheiten lassen sich so schnell beseitigen. Abbildung 3 zeigt ein Problem bei der LAN-internen IP-Adresse: Es fehlt die Option »RFC 1918 erlauben«. Dieses RFC spezifiziert die privaten Adressbereiche – im internen Netz sind private Adressen üblich und daher zu erlauben.

Das Firewallobjekt selbst enthält viele Konfigurationsoptionen (siehe Abbildung 4), von den allgemeinen Parametern wie Rechnername, Domainname und Standardgateway über die Konfiguration der Proxy-Dienste bis hin zur Einstellung des Logservers und der Protokollierung per Mail.

Abbildung 4: Das Firewallobjekt bietet vielfältige Konfigurationsoptionen. Neben den allgemeinen Parametern wie Rechnername und Standardgateway sind hier DNS und die Proxy-Dienste zu finden.

Hintergrundgeplänkel

Die Firewallregeln definiert man in Regelsätzen, einige generische Vorlagen sind bereits enthalten. Da der Firestick das Konzept „Verbiete standardmäßig alles“ verfolgt, sind die benötigten Dienste einzeln freizuschalten. Der Administrator kann die Regeln in beliebiger Reihenfolge anlegen, der Firestick setzt sie im Hintergrund in die korrekten IPTables-Befehle um. Sie werden erst beim Booten der Firewall aktiv.

Dabei spielt die Reihenfolge dann aber eine große Rolle, der Firestick ordnet sie anhand einer Logik hierarchisch an:

- Je enger begrenzt der Adressraum beziehungsweise das Subnetz eines Objekts ist, desto höher gewichtet der Firestick die Regeln. Das ist grundsätzlich der Fall bei Endknoten und der Firewall.
- Bei Netzwerkzonen ohne spezifische Netzwerkkonfiguration wird die Policy niedriger gewichtet. ▶

Ein Beispiel verdeutlicht diese Logik: Eine Firma möchte ihren Webserver in einer DMZ hinter der Firewall betreiben. Benötigte Dienste muss sie aufgrund der restriktiven Standardkonfiguration dieser Zone einzeln freigeben, in diesem Fall den Zugriff auf Port 80 (HTTP) aus dem externen »net« auf den Webserver. Da der eine feste IP-Adresse hat, greift die Zugriffsregel bereits vor der Regel, die den Verkehr unterbinden würde.

Umdenken bei den Regelsätzen

Administratoren, die den Umgang mit »iptables« auf der Kommandozeile gewohnt sind, müssen erst etwas umdenken, wenn sie Firestick-Regelsätze definieren. Ein Regelsatz ist vergleichbar mit einem Makro: Bestehend aus ein paar Bausteinen lässt sich mit seiner Hilfe der Zugriff auf einzelne Netzwerkobjekte steuern, wobei mehrere Objekte den gleichen Regelsatz nutzen können. Abbildung 5 zeigt, wie ein solcher Regelsatz aufgebaut ist:

- Die Spalte »Befehl« legt fest, welche Aktion die Firewall bei einer zutreffenden Regel ausführt. Möglich sind hier »ACCEPT«, »DROP«, »LOG« und »REJECT«.
- Die Regel ist definiert durch das Verbindungsprotokoll sowie Quell- und Zielport auf Quell- und Zielmaschine.
- Die letzte Spalte legt die Logebene fest. Damit lassen sich die Meldungen des Paketfilters klassifizieren.

Verwirrend sind die Bezeichnungen »Lokaler Port«, »Partner« und »Partner Port«. Der Pfeil zwischen den Feldern gibt die Richtung des Datenverkehrs an. In Abbildung 5 wäre der lokale Port also der bei IPTables bekannte Source-Port, der Partner wäre die Destination-IP und der Partner-Port der Destination-Port. Der abgebildete Regelsatz gestattet es also allen Rechnern, den Webserver auf dem »adminpc« anzusprechen.

Policy konsequent umgesetzt

Die Managementsoftware setzt die konfigurierte Sicherheitspolicy konsequent um. Aus dem Regelwerk erzeugt sie eine Konfiguration für Shorewall [6]. Diese Software liest die Konfiguration beim Start der Firewall und setzt die passenden »iptables«-Befehle ab.

Shorewall legt einzelne Chains nicht nur für jede Zone an, sondern beispielsweise auch für jede Netzwerkschnittstelle. Das bringt eine feingranulare Policy hervor. Shorewall macht sich dabei extensiv die IPTables-eigenen States zunutze: So ist es zum Beispiel möglich, zusammengehörige Verbindungen wie einen FTP-Transfer zu erkennen und anhand einer einzigen Regel zu erlauben. Selbst Besonderheiten wie „TCPMSS to PMTU Clamping“ setzt die Shorewall automatisch, wichtig ist das für PPPoE-Verbindungen wegen der kleineren MTU (Maximum Transfer Unit).

Drop oder Reject

Die mitgelieferten Beispiele lassen Pakete, die aus dem Raster des Sicherheitskonzept rausfallen, einfach per »DROP« im Datennirvana verschwinden. Sie unterscheiden auch nicht zwischen dem internen Netz und dem Gefahr verheißenden Internet. Sinnvoller wäre es an dieser Stelle, die Kommunikation geregelt mit »REJECT« abzubrechen statt den Client ahnungslos in einen Timeout laufen zu lassen. Sicherer wird der Paketfilter durch das Drop jedenfalls nicht – auch wenn einige Unverbesserliche an diese Form der „Security through Obscurity“ glauben.

Beim Logging erweisen sich die Voreinstellungen als recht sinnvoll. Einträge in den einzelnen Chains sind durch unterschiedliche Log-Präfixe gut zu unterscheiden. Um zu verhindern, dass ein Angreifer die Logs flutet und dadurch einen Denial of Service hervorruft, setzt die Limit-Option eine harte Grenze. Standardmäßig voreingestellt sind zehn Einträge pro Minute.

Somit entsteht eine Policy, die zwar nicht dem Kiss-Prinzip entspricht (Keep it simple, stupid), dafür untersucht sie den Netzwerkverkehr aber sehr genau. IPTables-Profis würden ein schlankeres Regelwerk erzeugen. In Shorewall steckt aber auch das Know-how von Firewall-Profis. Sie setzt die Policy sicherlich besser um als ein Anfänger, der mit »iptables« hantiert.

Admin-Pflicht: Die Regeln immer aktuell halten

Ein Policy ist meist ein recht dynamischer Prozess, bei dem sich immer wieder Dinge ändern. Neue Rechner, neue Partnergesellschaften, neue Dienste und Protokolle – ein Firewall-Administrator muss häufig an den Regelsätzen feilen. Selbst wenn nichts dergleichen eintritt, sollte er sein Sicherheitskonzept ständig hinterfragen und wenn möglich verbessern. Beim Firestick sind diese Änderungen problemlos. Der Admin muss das modifizierte Regelwerk nur im Control

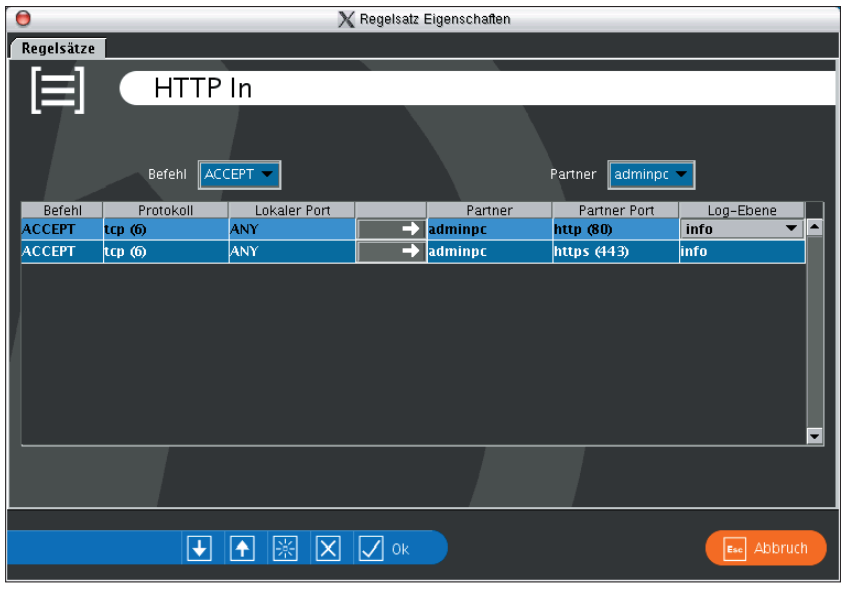

Abbildung 5: Pro Regelsatz sind mehrere einzelne Regeln möglich. Dieser Satz erlaubt es jedem Client, HTTP- und HTTPS-Verbindungen zum Rechner »adminpc« aufzunehmen.

Center aktivieren. Kleine Änderungen wie neu hinzugekommene Regeln werden sofort aktiv, wenn er den Firestick (mit angeschaltetem Schreibschutz) in die laufende Firewallmaschine steckt. Ein Reboot ist nicht erforderlich.
Rebooten muss er den Rechner nur bei größeren Änderungen, etwa bei neuen Adressen der Firewall-Netzwerkkarten oder grundlegenden Modifikationen an den VPN-Tunneln. Wer solch tiefe Einschnitte öfter erwartet, sollte einen Backuprechner mit Hilfe des Firestick vorbereiten, um die Ausfallzeit des Produktivsystems zu überbrücken.

Ereignisse aus der Vergangenheit

Trotz der begrenzten Ressourcen (RAM, USB-Stick) ist das für Firewalls sehr wichtige Thema Logging ansprechend gelöst. Standardmäßig erhält der Administrator Mails mit einer Zusammenfassung wichtiger Ereignisse, die in den Logs festgehalten wurden. Sämtliche Daten wie Absender- und Empfängeradresse, Prüfintervall und Mailserver lassen sich komfortabel in den Eigenschaften des Firewallobjekts definieren. Im schlimmsten Fall erhält der Admin dann jedoch alle 30 Sekunden eine Mail mit Logfile-Auszügen. Bei dieser Informationsflut den Überblick behalten ist kaum möglich.
Abhilfe schafft ein dedizierter Logserver, an den alle Systemmeldungen gehen. Hier bietet sich ein Linux-Rechner an, der Syslog-Nachrichten von entfernten Rechnern annimmt. Ein Angreifer müsste in diesem Fall neben der Firewall auch noch den Logserver knacken, um seine Spuren zu verwischen.
Auch die Managementsoftware selbst kann Systemlogs empfangen. Dazu ist der Admin-PC als Überwachungsserver in den Einstellungen der Firewall zu definieren, die daraufhin sämtliche Einträge an den Admin-PC sendet. Zusätzlich zu den Logs ist es dadurch möglich, fortlaufend die Auslastung der Netzwerkkarten und VPN-Tunnel im GUI zu beobachten.
Seit dem letzten größeren Update ist es zudem möglich, den so genannten Monitor auf der Festplatte des Admin-PC zu installieren. Leider kann man nicht mehr als einen Logserver definieren, um beide Möglichkeiten parallel zu nutzen.

Fazit

Der oft gehörte Spruch „Keine Linux-Kenntnisse erforderlich“ sollte bei einem elementaren Netzwerkelement wie einer Firewall zunächst stutzig machen. Die Gratwanderung zwischen dem Komfort einer grafischen Oberfläche und der Komplexität eines Paketfilters ist Databay aber gut gelungen. Die Kommandozeile wurde im Test ausschließlich benutzt, um ein wenig hinter die Kulissen zu blicken.
Das Gesamtkonzept und der Vertriebsweg sind auf kleinere Unternehmen ausgerichtet, die sich keine teure Firewall und keinen Firewallspezialisten leisten wollen. Für Installation und Support zeigen sich ein Berater sowie der Hersteller zuständig. Im laufenden Betrieb kann jeder netzwerktechnisch gebildete Admin nach kurzer Einarbeitung die Firewall bedienen. Bei allem Bedienkomfort sollte aber niemand vergessen, dass Paketfilter eine komplexe Angelegenheit sind, bei der schon kleine Fehler fatale Folgen nach sich ziehen. Zum Glück mindert die restriktive Grundeinstellung diese Gefahr.
Der einzige große Kritikpunkt ist die dürftige Dokumentation, die zum Beispiel bei der VPN-Konfiguration mehr Fragen offen lässt, als sie beantwortet. Sofern der Hersteller wie angekündigt nachbessert und zusätzlich ein paar Regelsätze mehr mitliefert, ist der Firestick durchaus empfehlenswert und rechtfertigt seinen hohen Preis. *(fjl)* ■

Tunnelgrabung

Mit dem optional erhältlichen VPN-Modul kann der Firewallbetreiber recht einfach IPsec-Verbindungen erzeugen. Die etwas hakelige Freeswan-Konfiguration per Kommandozeile entfällt. Der Firestick arbeitet mit X.509-Zertifikaten und harmoniert daher sehr gut mit anderen IPsec-Implementierungen. Die Zertifikate sind mit wenigen Klicks im Konfigurationswerkzeug erstellt. Dazu bringt der Firestick seine eigene Zertifizierungsinstanz (CA) mit, die er automatisch aktiviert, sobald der Admin ein CA-Zertifikat erzeugt.

Eigene CA integriert

Mit dem CA-Schlüssel lassen sich Zertifikate für Maschinen oder Benutzer ausstellen. Ein Stolperstein bei den Benutzerzertifikaten ist, dass der Admin jeden User erst in der Firestick-Benutzerverwaltung anlegen muss, die in der Netzwerkansicht zu finden ist. Als echte CA ist es auch möglich, Rückruflisten für Zertifikate (CRLs) und bereits bestehende Zertifikate zu importieren sowie selbst erzeugte Zertifikate zu widerrufen. Sogar das Verlängern eines Zertifikats ist hier eine Sache von zwei Mausklicks. Die sonst üblichen ellenlangen »openssl«-Kommandos bleiben dem Administrator erspart.
Sobald er ein Maschinenzertifikat erstellt hat, kann der Admin das VPN aktivieren und über den Eigenschaftendialog des Firewallobjekts VPN-Interfaces und die zugehörigen Tunnel aufbauen. Wie alle anderen Objekte kann er auch diese Schnittstellen sowie die angedockten Tunnel sehr komfortabel mit der Maus verschieben.

Vertriebswege

Der Firestick ist nicht direkt über die Databay AG zu beziehen. Das Vertriebsmodell sieht vor, das Gerät über Partnerfirmen zu vermarkten, die dann beispielsweise im Rahmen einer Beratertätigkeit die Firewall beim Kunden installieren und später betreuen. Der Grundpreis für den Firestick beträgt knapp 700 Euro, mit VPN-Option erhöht er sich auf 1400 Euro.
Zusätzliche Leistungen durch die Partner, also beispielsweise Installation oder Wartung, können in weiten Grenzen variieren. Ob ein Servicevertrag gerechtfertigt ist, muss jeder Kunde selbst entscheiden – um den Support kümmert sich sowieso der Hersteller selbst.

Infos

[1] Firestick: [http://www.firestick.de]
[2] Mark Vogelsberger, „Funk-Loch – WLAN-Sicherheit unter der Lupe“: Linux-Magazin 12/03, S. 36
[3] Tinyproxy: [http://tinyproxy.sf.net]
[4] GR-Security: [http://grsecurity.net]
[5] Pax: [http://pax.grsecurity.net]
[6] Shorewall: [http://shorewall.sf.net]

Der Autor

Christian Ney arbeitet als Unix- und Firewall-Administrator bei einer Regionalfluggesellschaft und beteiligt sich in seiner Freizeit an mehreren Open-Source-Projekten.