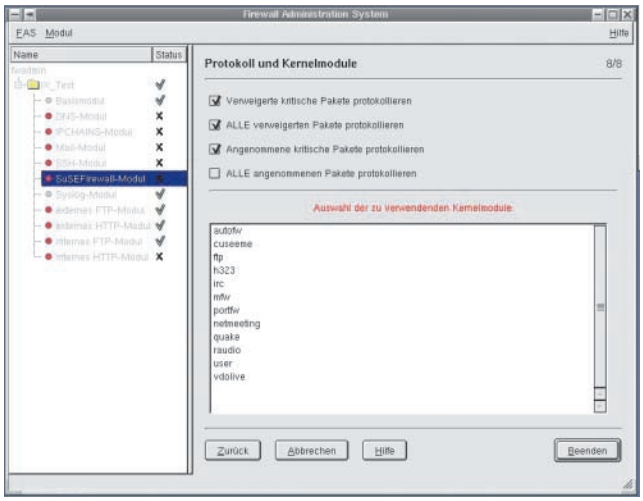
Suse Linux Firewall on CD VPN Edition

Brandsicherung

Lukas Grunwald



Gerade im Firmenumfeld spielen Virtual Private Networks bei der Vernetzung von Filialen eine große Rolle. Suse will sich mit der VPN Edition seiner Firewall on CD ein Stück von diesem Kuchen abschneiden.

Heute verfügt fast jedes aktive Netzgerät oder -Betriebssystem über eine so genannte Firewall. Viel zu oft benutzen Anwender und Anbieter den Begriff fälschlich als Synonym für einen Paketfilter. Der Kasten 'Firewall-Definition' zeigt, was der Autor darunter versteht. Ergänzend bieten inzwischen viele professionelle Firewall-Produkte IPSec-Implementierungen oder andere VPN-Funktionen.

Suses Firewall on CD besteht im Prinzip aus zwei Teilen. Die eigentliche Firewall startet und läuft von einer manipulationssicheren CD. Sicherheitsparameter und Firewallregeln liest das System beim Booten von einer Diskette ein. Die Verwaltung der Parameter sowie das Generieren der Parameterdiskette erfolgt auf einem dedizierten Administrationsrechner. Serviceseitig sorgt Suse zwölf Monate kostenlos für die Pflege der eingesetzten Programme und verschickt Updates und Sicherheits-Patches auf CDs.

Zum Lieferumfang gehören je eine CD für den Administrationsrechner, für die eigentliche Firewall sowie für den Quellcode. Auf einer zusätzlichen CD schickte Suse ein Update der eigentlichen Firewall. Dokumentation gibts in Deutsch und Englisch: Das 'normale', 366-seitige System- und Referenzhandbuch sowie das 176-seitige Firewall-on-CD-Handbuch. 30 Tage Installationssupport per E-Mail vervollständigen das Angebot.

Reichlich Software dabei

Zum Erstellen eines Regelsatzes für die Firewall muss man entweder das Firewall-Administration-System (FAS) auf einem Suse-7.2-System einspielen oder mit der Admin-CD einen neuen Rechner installieren. Beim Aufspielen des Verwaltungsrechners landen über 930 MByte auf dem System – viel zu viel für eine Administrations-Konsole, zumal sich unnötige Anwendungen wie Spiele oder der Musik-Ripper *cdparanoia* finden, die dort schon aus Sicherheitsgründen nichts zu suchen haben.

Auf dem Verwaltungssystem tummeln sich noch zahlreiche Binärprogramme mit Sicherheitslücken wie OpenSSH in der Version 2.9.9p2. Hier sollte Suse die Zusammenstellung dringend auf einen aktuellen Stand bringen. Das System ist zwar per Default sehr restriktiv konfiguriert, aktiviert aber der Administrator einen Standarddienst wie den SSH-Server, ist es unter Umständen ein leichtes Opfer für einen Innentäter, der die dort zentral gespeicherten Firewall-Konfigurationen manipulieren kann.

Hat der Benutzer auf dem Admin-System das FAS-Tool gestartet, kann er unterschiedliche Firewall-Konfigurationen verwalten. Dies erlaubt ein einfaches Security-Change-Management, wenn verschiedene Generationen von Regelsätzen zu dokumentieren und zu verwalten sind. Allergisch reagiert das FAS-Tool auf Leerzeichen im Namen der Konfiguration: Es gibt eine bezugslose Fehlermeldung aus, indem es vom Benutzer verlangt, alle Felder auszufüllen.

Konfiguration via GUI

Mit dem grafischem FAS-Tool (siehe Aufmacher-Screenshot) lassen sich alle Firewall-Einstellungen interaktiv eingeben, wobei es zwischen internen und externen Netzen sowie der DMZ unterscheidet. Das Handbuch liefert dazu eine gute Erklärung der verschiedenen Firewall-Konzepte. Per Drop-Down-Menüs erfolgt das Einrichten der Squid-ACLs, lediglich die regulären Ausdrücke für die Paketfilterkonfiguration muss der Benutzer in einem Editor-Fenster vornehmen. Allerdings fehlt eine Verwaltung von benutzer- beziehungsweise clientbasierten Sicherheitsrichtlinien sowie die Unterstützung zur Abbildung eines komplexen Firewall-Regelwerks.

Dieser Test erfolgte nur mit einer festplattenfreien (harddiskless) Variante mit einem externen Log-Host. Bei dieser lassen sich sämtliche Benutzer-Accounts auf der Firewall deaktivieren. Nach dem Erstellen der Konfiguration liegt diese zunächst auf dem Administrationsrechner und muss auf eine Diskette übertragen werden. Letzteres funktionierte über das grafische Frontend nicht, per Shellskript klappte es reibungslos. Potenziell ist das Verfahren instabil, da sich zum einen Disketten nur bedingt als persistente Datenträger eignen und zum anderen der Platz bei komplexeren Setups knapp werden kann.

Ein erster Test mit einem Pentium-III-PC mit einem Toshiba-SCSI-CD-Laufwerk an einem Adaptec 2940-Adapter schlug fehl: Nach dem Erkennen des SCSI-Controllers blieb das System mit der Fehlermeldung 'aic7xxx_dev_reset returns 8194' stehen. Erst nach dem Einbau eines ATAPI-CD-Laufwerks lief das System hoch und startete die Firewall.

Sollte in dem Firewall-Rechner – wie in manchem Industrie-PC – ein

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Firewall-Definition

Eine Firewall verbindet ein oder mehrere zu schützende Netze mit einem unsicherem Netz. Dazu benötigt sie unter anderem einen Paket-Filter, der nach bestimmten Regeln (den Firewall-Rules) entscheidet, welche Pakete passieren dürfen und welche nicht. Darüber hinaus gehören Proxys auf Protokoll-Ebene der Anwendungen ebenso dazu wie der Nachvollzugsaspekt oder Kontroll- und Beobachtungskomponenten für den Zustand der Firewall. Eine Alarmierungsfunktion sollte den Administrator automatisch darüber informieren, wenn ein Angriff gegen das zu schützende Netz erfolgt.

PCMCIA-Socket vorhanden sein, unterbricht die aktuelle Live-Firewall-CD (Version 1.5) ihren Startvorgang und verlangt nach einer Treiber-Diskette. Mit über drei Minuten dauerte der Bootvorgang zu lange. Andere *init*-Varianten sind hier deutlich schneller.

Nachvollziehbarkeit

Als ebenfalls unvollständig erwies sich das Syslog-Modul. Es unterstützt weder Methoden wie Secure-Syslog noch eine Sicherung der verlustanfälligen UDP-Pakete. Damit sich ein Ereignis einem bestimmten Zeitpunkt zuordnen lässt und sich Log- und Kundendateien bei einem Internet-Provider sicherstellen lassen, benötigt eine Firewall eine exakte Systemzeit. Dazu bietet Suse auf der VPN Edition einen NTP-Dienst an. Leider fehlt eine auf dem Stand der Technik befindliche kryptografische Zeitstempelsicherung.

Passen muss Suse in Sachen Alarmierung, der Administrator muss selber die Log-Dateien untersuchen. Treffen ein DoS-Angriff oder Port-Scans auf die Firewall, wäre eine Benachrichtigung wünschenswert, etwa via kryptografisch gesicherter SNMPv3-Informs oder signierten EMails.

Hat man – wie es das FAS-Tool anbietet – den Root-Zugang zur Verbesserung der Sicherheit deaktiviert, muss man das System neu starten, um Änderungen an den Firewall-Regeln vorzunehmen – ein schnelles Blockieren eines angreifendes Netzes ist so nur bedingt möglich. Die andere Option, einen SSH-Key zu hinterlegen, hat ihre Tücken im SSH-Modul: Den Versuch, eine SSH Version 2 DSA ID zu importieren, ignorierte der Administrationsrechner einfach, nur ein SSH-Version-1-Public-Key ließ sich reibungslos installieren, was einen Malus in Hinsicht der Sicherheit bedeutet.

Die Firewall basiert auf dem Linux-Kernel 2.2.19 und bietet daher nur TCP- und UDP-Regeln an; Sicherungen gegen den Informationsabfluss von Innentätern fehlen total. Es ist zu hoffen, dass die kommende Linux-2.4-basierte Version auch Methoden gegen ARP- oder ICMP-Attacken und -Tunneln beinhaltet sowie DoS-Schutz und Algorithmen zur Bandbreiten-Beschränkung bieten wird. Das Setup-Tool läuft nur unter Suse Linux und keinem anderem Linux- oder Unix-Derivat.

Suse baut bei VPNs auf das Freeswan-Projekt (www.freeswan.org) und hat deren IPSec-Implementierung durch den PKI-Patch erweitert, damit sie Zertifikate benutzen kann. Eine Hakelei mit Freeswan ist, dass es keine einfache DES-Verschlüsselung unterstützt. Da DES den kleinsten gemeinsamen Nenner der bei IP-Sec vorgeschriebenen Kryptoalgorithmen darstellt, ist Freeswan zwar sicher, aber inkompatibel zu vielen anderen Produkten. Dies ist allerdings nicht Suse anzukreiden – die Freeswan-Entwickler unterstützen aus Prinzip nur 3DES.

Weiter ist das Trennen der Routing-Tabellen von IP-Sec und normalem Verkehr umständlich sowie fehleranfällig. Bei komplexeren Setups kann der Kernel für Pakete schon mal die falsche Route erwischen. Dies ist ein für die Kombination Linux/Freeswan bekanntes Problem. Suse empfiehlt daher, das dynamische Routing auf einer vorgelagerten Maschine durchzuführen.

Mit dem im Netz verfügbaren Wissen und viel Netzkenntnissen, die bei jedem Firewall-Administrator vorhanden sein sollten, lässt sich ein IP-Sec-Setup erzeugen – Anfänger oder normale Linux-Benutzer dürften damit aber ihre Schwierigkeiten haben.

DATEN UND PREISE

Suse Linux Firewall on CD VPN Edition

Systemvoraussetzungen: Intel- (kompatible) CPU, 128 MByte RAM, 1/2 GByte Plattenplatz Log-Host/Administrationsrechner

Lieferumfang: 3 CDs; je zwei Handbücher in Deutsch und Englisch; 30 Tage Installationssupport; 12 Monate Softwarepflege

Preis: 1850 €

Anbieter: Suse Business Partner www.suse.de/de/partner/search_partners/business_partners/reseller/index.html

Hakeleien mit Zertifikaten

Freeswan unterstützt keine zwei Enden mit dynamischer IP. Damit die Firewall mit einem Ende dynamisch arbeiten kann, ist ein Key-Paar bestehend aus einem öffentlichen und einem privaten Schlüssel zu erstellen. Dieses bezeichnet man als Zertifikat.

Ein Importieren eines Zertifikates von einer echten CA wie von einem Trustcenter ignorierte das System zunächst. Es tauchte erst nach dem Erzeugen einer Self-Signed-CA mit dem ersten selbst signierten Zertifikat auf. Die Speicherung auf der Administrationsmaschine erfolgt ohne zusätzliche Sicherungsmaßnahmen. Eine Anbindung an Key-Server oder komplexere Mechanismen wie TACAS+ sieht Suse nicht vor.

Eine Kernfrage beim Einsatz einer Firewall ist die Regelung der Haftung. Einige Firewall-Hersteller bieten ihren Kunden an, das gesicherte Setup durchzuführen und somit auch für Löcher in der Firewall zu haften. Suse weist sowohl im Handbuch als auch auf den CDs ausdrücklich auf einen totalen Haftungsausschluss hin.

Fazit

Ein kostenlos im Netz erhältliches Debian-System lässt sich mit ein wenig Sicherheitswissen – über das ein Firewall-Administrator verfügen sollte –, auf mindestens dem gleichen Sicherheitsniveau als Firewall betreiben. Selbst bei Suses Firewall muss der Administrator Teile seiner Konfiguration mit dem Editor anpassen, will er ein erhöhtes Sicherheitsniveau erreichen. Dabei steht für die Sicherheitsorganisation der gleiche Aufwand wie bei Debian an.

Alles in allem vermittelt das Suse-Produkt den Eindruck, mit der heißen Nadel gestrickt zu sein, und ist letztlich mancher GPL-Firewall oder manch kommerziellem Produkt wie Astaros Firewall unterlegen. Dies rechtfertigt nicht den hohen Preis. Wer eine Firewall mit kompatibler VPN-Lösung benötigt, wird bei OpenBSD 3.1 (www.openbsd.org) oder FreeBSD 4.61 (www.freebsd.org) eher fündig. (avr)

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.