IPFire.org
Michael Tremer
Gerhardstraße 8
D-45711 Datteln
Christian Schmidt
Weißer Weg 32
D-90491 Nürnberg
www.ipfire.org
info@ipfire.org

Pressemitteilung

Sehr geehrte Damen und Herren,

nach langjähriger Entwicklungszeit sind ich und mein Team froh Ihnen voller Stolz die Version 2.0 unserer Firewall, die sich somit ab dem 24. August 2007 im Beta-Stadium befindet, zu präsentieren. Basierte die Version 1.4.9, wie die Versionsnummer schon ahnen lässt, noch auf dem IPCop, so handelt es sich nun um eine fast vollständige Neuentwicklung auf Basis des Linux-from-Scratch (LFS) 6.2.

Als eine der schwierigsten Aufgaben stellte sich die Integration des Linux-Kernels 2.6, was einige umfassende Änderungen im System nach sich zog. Ähnelt die grafische Weboberfläche noch sehr dem Vorgänger, hat sich aber trotzdem „unter der Haube" eine kleine Revolution vollzogen. Das Ergebnis ist ein gehärtetes System auf dem allerneuesten Stand mit GCC 4.0.3 und dem stabilen Kernel der Serie 2.6.16.

Nachdem dieser maßgebliche Schritt vollzogen war, wurden die bisher zur Ausstattung gehörigen Features wieder integriert. Dazu gehören wichtige Dienste in einem Netzwerk wie ein DHCP- oder NTP-Server, sowie auch DynDNS-Updater um hier nur einige zu nennen. Die vollständige Liste finden Sie in der unten stehenden Tabelle.

Besonders hervorheben möchte ich an dieser Stelle die umfassende Möglichkeit VPN-Clients anzubinden. Neben IPSec bietet IPFire auch einen OpenVPN-Server mit dessen Hilfe man beliebige Clients kinderleicht einrichten kann. Dazu werden mit einem Wizard in unserer Weboberfläche Zertifikate generiert, die man anschließend zusammen mit der passenden Konfiguration als ZIP-Datei herunterladen kann. Auf dem Client muss man dann nur die passende Software installieren, da z.B. Microsoft Windows® von Haus aus keine Möglichkeit dazu bietet, und mit der Konfiguration starten. Aus Sicherheitsgründen wird eine Verbindung über PreSharedKeys nicht unterstützt. Weiterhin wird vor dem Aufbau der Verbindung nach einem Passwort für das Zertifikat gefragt.

Als weitere VPN-Lösung finden sie IPSec in der neuesten Version, welches in unserer Software hauptsächlich für die transparente Vernetzung mehrerer Standorte gedacht ist. Auch hier empfehlen wir die Nutzung von Zertifikaten, da dies die Sicherheit drastisch erhöht. Kompatibel ist das IPSec weiterhin mit der älteren Variante des IPCop sowie allen anderen OpenSwan-kompatiblen Geräten.

Um für die Übertragung der Daten durch den eben erwähnten VPN-Tunnel eine ausreichende Bandbreite zu gewährleisten gibt es ein Quality-of-Service (kurz QoS), welches selbstverständlich auch die Fähigkeit besitzt Voice-over-IP-Gespräche unterbrechungsfrei zu übertragen. Das ist besonders interessant für den über den Paketmanager installierbaren Private-Branch-Exchange Asterisk®. Einige wichtige Merkmale des QoS sind ein Level7-Filter, vollständige Unterstützung von Type-Of-Service-Bits (TOS-Bits) und die leichte Einrichtung, sowie die graphische Aufbereitung der Bandbreitennutzung durch die einzelnen Paketklassen.

Neben Asterisk® lassen sich aber noch einige weitere Addons in die Software installieren. Und das vollautomatisch durch den neuen Paketmanager mit dem Namen „Pakfire". Dieses

Michael Tremer
Gerhardstraße 8
D-45711 Datteln

Christian Schmidt
Weißer Weg 32
D-90491 Nürnberg

www.ipfire.org
info@ipfire.org

Software-Distributionssystem stellt auch sicherheitskritische Updates zur Verfügung und installiert diese auf Wunsch ganz von allein.

Diese Möglichkeit macht den IPFire schnell zu einer Multimedia-Plattform mit Streaming-Server für MP3- und OGG-Dateien oder stellt mit Hilfe von Samba Dateifreigaben und Druckdienste zu Verfügung. Sogar ein vollkommen ausgewachsener primärer Domänencontroller (PDC), welcher kompatibel zu NT4 von Microsoft ist, ist so auf Wunsch einzurichten.

Zusätzliche Sicherheit kann der Nutzer durch die Installation von Tripwire erlangen, welches das Dateisystem auf, zum Beispiel durch Rootkits, veränderte Dateien überprüft und ihm in einem Report präsentiert.

Waren in dem ersten IPFire-Release Pakete wie Samba und Asterisk® noch standardmäßig installiert und stellten den Ansatz des Projektes als eine Firewall in Frage, haben wir diese Kritik nun entgegengenommen und dem Nutzer die Wahl der Zusatzfunktionen selbst überlassen. Somit kann ein IPFire als reine Firewall, aber als auch Firewall mit Home-Server-Funktionen genutzt werden.

Wir haben die Software bereits einem Alpha-Stadium unterzogen und so bereits einige Bugs und Probleme festgestellt und gelöst. Da die Entwicklung und Integration der Features fast vollständig abgeschlossen ist haben wir uns nun entschlossen das nächste Entwicklungsstadium einzuleiten und mit Hilfe eines größeren Nutzerkreises die Qualität der Software weiter zu erhöhen und eventuell auch weitere Features zu integrieren.

Somit rufen wir alle interessierten Nutzer auf sich unsere Software herunterzuladen und sich aktiv an der Entwicklung zu beteiligen. Wir stellen dazu Ressourcen wie z.B. den Bugtracker unter http://bugtracker.ipfire.org bereit.

Für technisch versierte Nutzer, die bereits eine tiefergehende Erfahrung mit Linux aufweisen, findet sich der Quellcode in unserem SVN unter http://svn.ipfire.org. Jeder, der etwas zu dem Projekt beitragen möchte ist herzlich willkommen.

Doch nicht nur das KnowHow der Anwender ist bei den Entwicklern gefragt. Da das Projekt noch sehr jung ist, fehlt es leider immer wieder an Kapazitäten für den Download. Hier freuen wir uns alle sehr über Spenden jeder Art. Wie das funktioniert finden sie auf unserer Homepage.

Besuchen sie uns auf http://www.ipfire.org/.

Über zahlreiche Tester und Supporter für das Projekt würden wir uns sehr freuen.

Das IPFire.org-Team

IPFire.org
Michael Tremer
Gerhardstraße 8
D-45711 Datteln
Christian Schmidt
Weißer Weg 32
D-90491 Nürnberg
www.ipfire.org
info@ipfire.org

Tabelle 1:

Sicherheitseinrichtungen:
- Stateful Inspection Firewall basierend auf der Linux Netfilter-Architektur
- Intrusion Detection System mit Guardian Addons Erweiterung zum IPS System
- Filter für ungültige/nicht-standardgerechte Pakete
- Eigene Netzwerksegmente für Server (DMZ) und Wireless Lan mit angepassten Policies
- DoS- und DdoS-Schutz
- Application Proxies für HTTP und FTP (mit Zugangskontrolle und Content-Filter) und DNS
- Eingehende sowie Ausgehende Paketfilterung

Netzwerkdienste:
- DHCP-Server
- Dynamischer DNS-Dienst
- NTP-Server

HTTP-Proxy:
- Zwischenspeicherung von Web-Inhalten
- Inhaltsfilter auf Basis von Blocklisten und manuell festlegbaren Listen
- Zeitgesteuerte Sperrung des Zugangs für einzelne Nutzer oder ganze Gruppen
- Vereinfachte Verwaltung für Klassen- oder Konferenzräume
- Erweiterte Speicherung von Updates für Microsoft® Windows®, Symantec Antivirus, Adobe-Produkten, Avira Antivir und Avast Antivirus
- Authentifizierung am LDAP-,identd-, Radius- oder Windows-Server oder einer lokalen Nutzerdatenbank
- Transfer-Limitierung (Geschwindigkeit und/oder Volumen)

Network Address Translation (NAT):
- Portweiterleitung
- NAT zwischen den voneinander getrennten Subnetzen

Unterstützte Verbindungstypen:
- Ethernet-Verbindungen mit 10, 100 oder 1000MBit mit statischer IP-Adresse oder über das DHCP-Protokoll konfiguriert
- ADSL/SDSL mit PPPoE
- Automatische Wiederverbindung nach Trennung durch den Provider
- Wiederverbindung nach Zeitplan steuerbar

Traffic-Priorisierung:
- Quality of Service
- Level7-Filterung
- Setzen und erkennen von Type-of-Service-Bits

Konfiguration:
- SSL-verschlüsseltes Web-Administrations-Interface
- SSH-Server

Monitoring/Logging:
- Grafische Überwachung des Systems im Webinterface
- Einsehbare Log-Dateien mit automatischer Zusammenfassung der wichtigsten Ereignisse
- Exportfunktion der Logdateien (einzeln oder als gesamtes Backup)

DNS-Proxy:
- DNS-Forwarding
- lokale Host-/Zonen-Konfiguration

Addons (im Beta-Stadium):

Michael Tremer
Gerhardstraße 8
D-45711 Datteln

Christian Schmidt
Weißer Weg 32
D-90491 Nürnberg

www.ipfire.org
info@ipfire.org

Virtuelle Private Netzwerke:

- IPSec/OpenSwan 2
  - Netz-zu-Netz oder Netz-zu-Host (Roadwarrior)
  - IKE - PreSharedKey oder
  - X.509-Zertifikate aus integrierter oder externer CA
  - Automatische Erkennung mit nötigem Wiederaufbau der Tunnel-Verbindung und Dead-Peer-Detection
  - NAT-Traversal
  - Verschlüsselung durch AES, 3DES, Blowfish, Serpent oder Twofish
  - HMAC: SHA1, SHA256, SHA384, SHA512
  - Echtzeit-Kompression
- OpenVPN
  - Host-zu-Netz (Roadwarrior)
  - SSL-basierte Verschlüsselung: AES, Blowfish, Twofish, 3DES,...
  - Echtzeit-Kompression
  - Fertige Clientpakete damit eine Konfiguration am Client vereinfacht wird
  - Tunnel über multiples NAT
- PPTP-Passthrough

- Samba Dateiserver
- Tripwire
- MPFire – Mp3 Jukebox
- Asterisk Voice-over-IP Server
- Gnump3d – Mp3 Streaming Daemon
- Appeljuice und Rtorrent
- cftp und ncftp
- Clamav
- Ethereal
- uvm.