

Accounting für BinTec-Router: Brick-Statistik

Einleitung

Sollten sie einen Bianca/Brick-Router nutzen, um den Mitarbeitern Ihres Unternehmens den Zugang zum Internet zur Verfügung zu stellen oder eigene Angebote im Internet zu veröffentlichen, haben Sie sich sicherlich schon mindestens eine der folgenden Fragen gestellt:

- Welcher Mitarbeiter nutzt eigentlich den Internet-Zugang in welchem Umfang und wofür?
- Welche Verbindungen werden überhaupt aufgebaut?
- Woher kommen die (gestiegenen?) Provider- oder Telefonkosten?

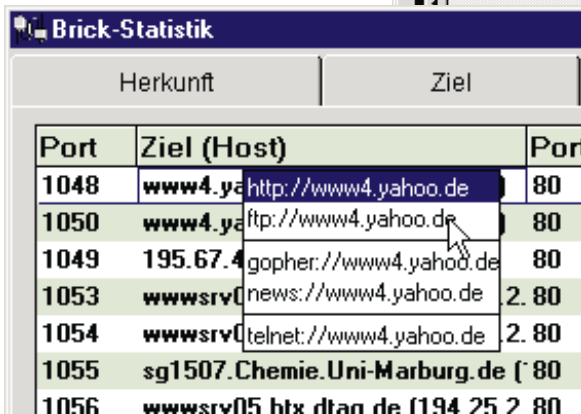
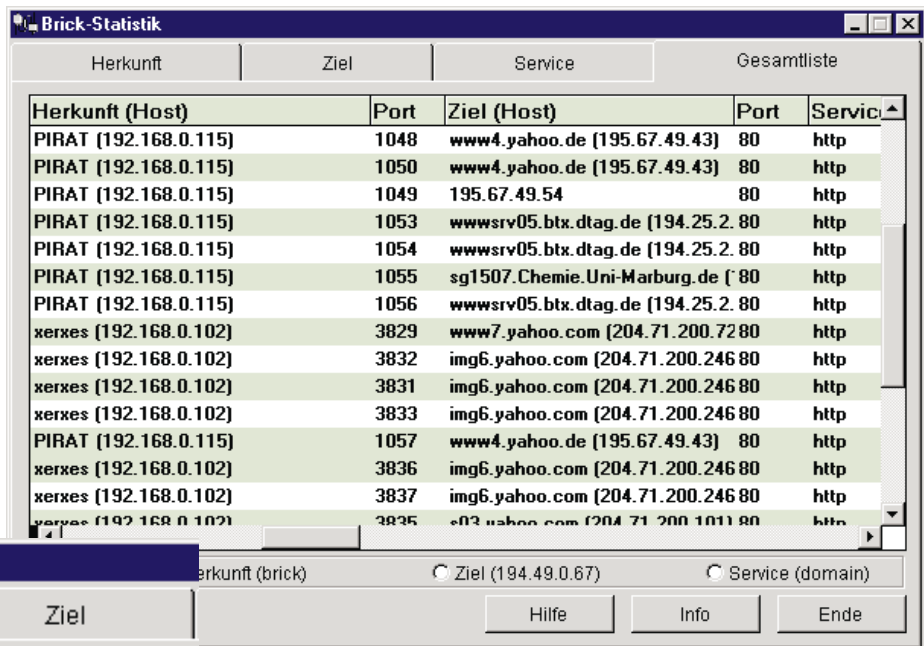
"Brick-Statistik" erlaubt es Ihnen, die mitunter wenig lesbaren Syslog-Nachrichten Ihrer Bianca/Brick auszuwerten, einfache Statistiken zu drucken und die Daten für komplexere Analysen z.B. in Microsoft Excel zu exportieren. Kosten-Controlling und ein regelmäßiges Security-Audit ("Wer verbindet eigentlich mit wem...?") werden so massiv vereinfacht.

Grundlagen

BinTec-Router verfügen über ein eingebautes IP-Accounting, daß eigentlich nur noch für das jeweiligen Interface im Setup aktiviert werden muß. Anschließend schickt der Router per SYSLOG entsprechende Daten an die eingetragenen Empfänger für SYSLOG-Nachrichten. Dies kann z.B. eine beliebige Arbeitsstation mit den mit dem Router gelieferten "DIME Tools" sein, es gibt aber auch eine Reihe von freien oder als Shareware verfügbaren SYSLOG-Daemons für Windows 95 oder Windows NT (man suche z.B. unter <http://www.shareware.com> nach "syslog"). Die so gesammelten Accounting-Daten müssen nur noch in eine einfach lesbare Form gebracht und ausgewertet werden.

Brick-Statistik

Genau diese Aufgabe übernimmt "Brick-Statistik". Das Programm "Brick-Statistik" extrahiert die IP-Accounting-Daten aus den SYSLOG-Dateien, dekodiert die verwendeten Dienste ("services") anhand der TCP- und UDP-Ports und löst die (für Menschen wenig aussagekräftigen) IP-Adressen in Host-Namen auf. Anschließend kann man sich übersichtlich und auch für Administratoren, die nicht "fließend TCP/IP sprechen" verständlich anzeigen lassen, wer wann wie lange und vor allem wohin Verbindungen z.B. in das InterNet hatte.



Statistiken und Protokolle lassen sich für weitere Auswertungen in verschiedenste Dateiformate exportieren.

Sollte einmal unklar sein, welche Informationen z.B. Die Web-Site, die im Protokoll aufgeführt ist, enthält, reicht ein Klick auf die rechte Maustaste, schon kann man den Host mit verschiedensten Protokollen kontaktieren (Interessant z.B. bei http-Verbindungen zu obskuren Web-Sites, die keinen regulären Host-Namen, sondern nur eine IP-Nummer haben).

Weitere Informationen zu "Brick-Statistik" sowie das vollständige Handbuch finden Sie unter <http://www.comp-comp.com/bristat>.