Ganzheitliche Sicherheit in DV-Netzen – Ein IP-Paketfilter als ein Baustein zur Schaffung einer ganzheitlichen Sicherheitsarchitektur in einem bestehenden Intranet

Thomas Wegner

1. Einleitung

Da sich Einzelbenutzer und Institutionen zunehmend Angriffen auf ihre Systemintegrität und Datensicherheit aus dem Internet ausgesetzt sehen, steigen ständig die Sicherheitsansprüche der vernetzten, über das gesamte Stadtgebiet verteilten Einrichtungen der Universität Rostock. Dieser Beitrag beschreibt den Einsatz und die Performanceanalyse eines IP-Paketfilters als ein Baustein auf dem Wege zur Schaffung einer ganzheitlichen Sicherheitsarchitektur in einem bestehenden Intranet. Im wesentlichen können zwei Verfahren für die notwendige Abschottung der DV-Systeme im lokalen Netzwerk sorgen, Virtual Privat Networks (VPN) und Firewalls. Das Ziel einer Performanceanalyse soll die Ermittlung der über ein LINUX-Firewall-System erreichbaren Datenübertragungsrate sein. Die untersuchten Netzwerkstrukturen und die dabei ermittelten Messwerte werden unter praktischen Gesichtspunkten hinsichtlich erforderlicher zukünftiger Netzerweiterungen diskutiert.

2. Die Sicherheit des Institutsnetzes im universitären Umfeld

Hauptanforderung an die Sicherheit im universitären Umfeld des im Bild 1 dargestellten Institutsnetzes ist der Schutz der System- und Datenintegrität. Mögliche Angriffspunkte auf dieses Campus-Netz sind:

- interne Angriffe aus dem LAN durch authentifizierte Nutzer und Computer
- interne Angriffe aus dem LAN durch Fremdsysteme
- interne Angriffe aus dem WLAN durch Eigen- und Fremdsysteme
- externe Angriffe aus dem WIN/Internet durch bekannte und nichtbekannte Nutzer und Computer
- interne und externe Angriffe auf das LANE-System des ATM-Backbone

Die durch den Einsatz von Firewalls und Virtual Privat Networks (VPN) möglichen Schutzmassnahmen lassen sich wie folgt klassifizieren:

- Access Security: Schutz der lokalen Systeme vor unerlaubtem Zugriff von innerhalb und außerhalb des LANs
- Content Security: Schutz der lokalen Anwendungen und Daten vor Veränderungen und schädlichen Inhalten, wie Viren oder Trojaner
- Authentication Security: Sichere Identifikation der Kommunikationspartner
- Crypto Security: Schutz der Daten hinsichtlich Vertraulichkeit und Integrität durch Verschlüsselung

Mit Layer-3-Firewalls (IP-Paketfilter) [2] und Application-Firewalls (Viren-Scanner, URL-Blocking, Java- und ActiveX-Screening) erreicht man Access- und Content-Security. Die Anwendung von Verfahren der Kryptographie (PGP) und der digitale Signatur gewährleisten die Authentication- und Crypto-Security für Daten.
Desktop-Firewalls können mit Hilfe von Protokollfiltern, Port-Blocking, Paket- und Anwendungsmonitoring/Reporting den persönliche Datenschutz am Arbeitsplatzrechner erhöhen. Filterfunktionen für das IP-Protokoll zur Realisierung eines Personal-Firewalls sind mittlerweile integraler Bestandteil der Betriebssysteme MS/Win2k unter SUSE/LINUX 7.x. VPNs ermöglicht Authentication- und Crypto-Security natürlich nur zwischen Netzen mit ähnlichem Sicherheitsniveau. Man unterscheidet VPNs mit Layer-2-Tunneling (PPTP, L2F, L2TP) und mit Layer-3-Tunneling (IPSec).

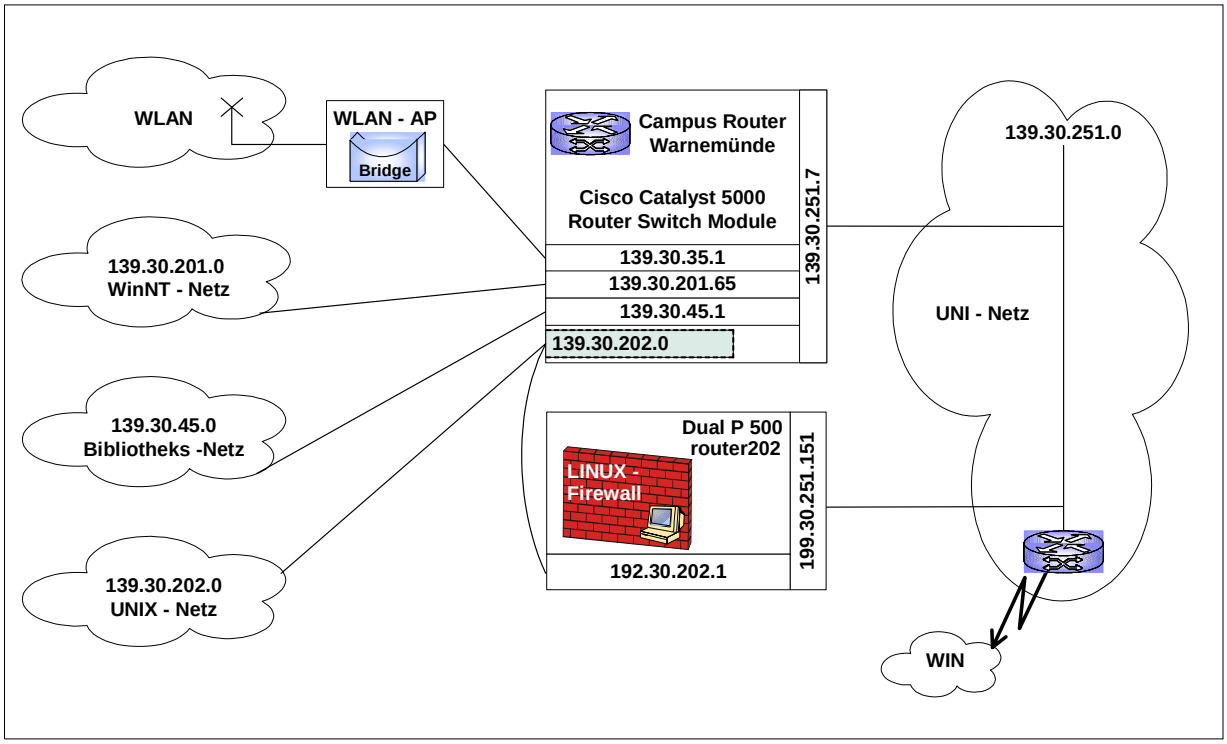

Bild 1: Die VLAN-Struktur des Campus-Netzes

Die steigende Anzahl und Komplexität der Computersysteme erhöhen laufend den Aufwand zur Absicherung des aktuellen Security-Patch-Levels der eingesetzten Betriebssysteme (SUN/SOLARIS, MS/WinNT, SUSE/LINUX).
In der ersten Ausbaustufe wurde das UNIX-Netz mit den SUN-SOLARIS-Workstations für den VLSI-Entwurf durch einen LINUXbasierten IP-Paketfilter geschützt. Das virtuelle Subnetz im ATM-LANE-System bleibt erhalten, aber es wird nicht mehr direkt über das RSM-Modul des Cisco Catalyst 5000 geroutet, sondern über den als Firewall-Router konfigurierten LINUX-PC. Das hat weiterhin den Vorteil, dass damit auch ein IP-Paketmonitor zur Verfügung steht, um Konfigurationsfehler im LAN zu erkennen.
Als nichttrivial erwies sich die Aufstellung und Beschreibung der notwendigen Input-, Output,- und Forward-Filterregeln für das Tool ipchain des LINUX-Kernels 2.2.14-SMP, da

für eine Vielzahl von Diensten (NFS, NIS+, DNS, FTP, NTP, SSH, POP3, usw.) und Protokollen (IP/TCP/UDP, HTTP, NETBIOSoverTCP/IP) die Filtermasken zu setzen waren. Folgende Ausstattungsmerkmale kennzeichnen den unter LINUX eingesetzten Firewall-PC:

- Dual Pentium III Board, 550 MHz, 512 Kbyte Cache, SUSE/LINUX 6.4
- 512 Mbyte Hauptspeicher
- PCI-Netzwerkadapter Intel PRO/100 Mbit/s
- 20 Gbyte IDE Festplatte

2. Die Performanceanalyse des Netzwerkes mit IP-Paketfilter

Das Ziel einer Performanceanalyse [3,4] sollte die Ermittlung der über das LINUX-Firewall-System (Dual Pentium 500 mit SUSE LINUX 6.4) erreichbaren Datenübertragungsrate sein, um festzustellen, ob sich das TCP/IP-Paketfiltering und -Monitoring auch nicht als Flaschenhals im Netzwerk erweisen würde

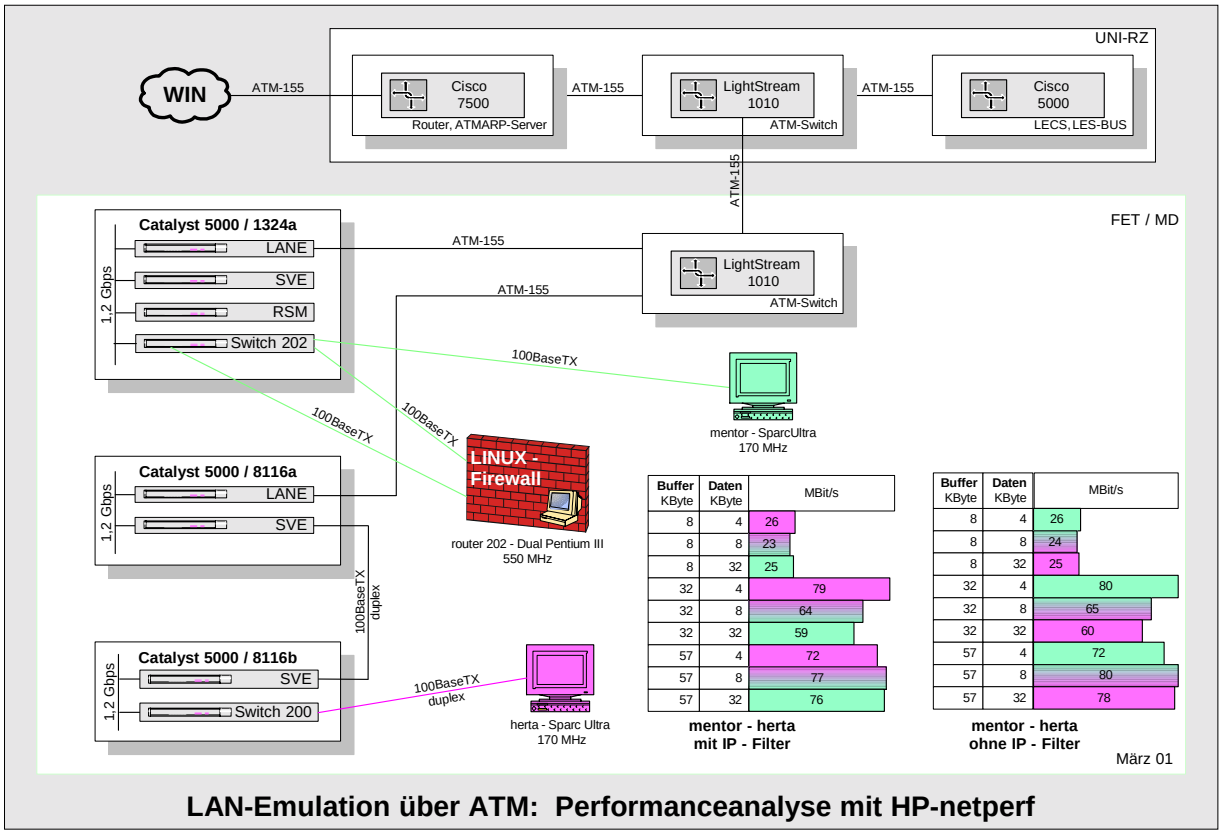

Bild 2: Die Struktur des mit HP-netperf untersuchten 100BaseT-VLANs

Für die Analyse eines Datennetzwerkes sind die verschiedensten Monitoring- und Benchmarking-Tools in Hard- und Software realisiert. Die Software Netperf von HP [1] ist ein Benchmark, mit dem verschiedene Aspekte der Netzwerkperformance über das TCP/IP-Protokoll gemessen werden können.

Entsprechend dem Client/Server-Modell wird beim Aufruf des Programms Netperf auf der Gegenstelle der Netserver-Prozeß durch den Inet-Dämon gestartet. Hauptanwendungsgebiet ist die Messung der Stream-Performance über TCP oder UDP zwischen zwei Systemen. Das in der freien Netperf-Distribution vorhandene tcp_stream_script variiert beim Test die Größen der Socket-Buffer auf Sender- und Empfängerseite mit verschiedenen Nachrichtenlängen.
Die Datenpfade der durch Netperf erzeugten Last und die ermittelten Messwerte sind im Bild 2 dargestellt. Es zeigt sich, dass beim Routerbetrieb die erreichbare Netzwerkgeschwindigkeit durch das LINUX-PC-System nicht beeinträchtigt wird. Sind die TCP/IP-Filterfunktionen über das Tool ipchain im LINUX-Kernel aktiviert, verschlechtert sich die Performance um ziemlich genau 1 Mbit/s.

3. Zusammenfassung

Die Netzwerksicherheit in einem LAN kann durch den Einsatz eines Internet-Protokollfilters schon wesentlich verbessert werden. Um die Systemlast des LANE-Router-Switching-Moduls im IPoverATM-Netz nicht noch weiter zu erhöhen, wurde die Installation eines Standalone-Router-Firewalls auf PC/LINUX-Basis erwogen. Praktische Messungen der Netzwerk-performance zeigen, dass sich die erreichbare Übertragungsgeschwindigkeit durch den IP-Filteraufwand beim Software-Routing nur um ca. 1Mbit/s verringert. Dieser praktikable Wert spricht für die Implementierung des IP-Protokollstacks im LINUX-System.

4. Literatur

[1] http://www.cup.hp.com/netperf/NetperfPage.html
[2] Andreas Bonnard, Christian Wolff: Gesicherte Verbindung von Computernetzwerken mit Hilfe einer Firewall, Studie der SIEMENS AB Zentralabteilung Technik, München, 1997
[3] Thomas Wegner: Performanceanalyse an einer bestehenden IPoverATM 10BaseT-Netz-werkstruktur, Tagungsband Symposium Maritime Elektronik, S. 79-82, Rostock, April 1998
[4] Thomas Wegner: Performanceanalyse an einer bestehenden IPoverATM 100BaseT-Netzwerkstruktur, Tagungsband 2. IuK-Tage MV, Rostock, Juni 1999

Verfasser

Dipl.-Ing. Thomas Wegner
Universität Rostock
Fachbereich Elektrotechnik und Informationstechnik
Institut für Angewandte Mikroelektronik und Datentechnik
Richard Wagner Str. 31
18119 Rostock
Tel.: (0381) 498 3533, Fax: (0381) 498 1126
Email: weg@e-technik.uni-rostock.de