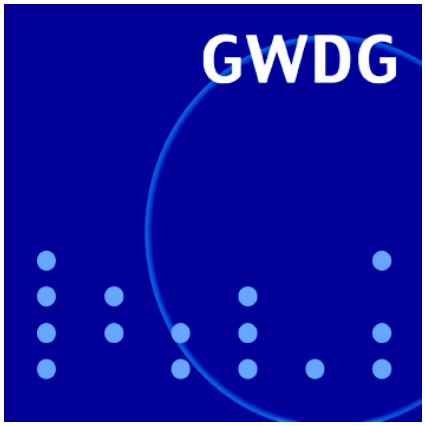

Firewallkonzept für das GÖNET

Mailservice

Microsoft Command Shell

Norman Virus Control

GWDG Nachrichten

2 / 2006

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Inhaltsverzeichnis

GWDG-Nachrichten für die Benutzer des Rechenzentrums

ISSN 0940-4686

29. Jahrgang, Ausgabe 2 / 2006

http://www.gwdg.de/GWDG-Nachrichten

Herausgeber: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Fassberg, 37077 Göttingen-Nikolausberg

Redaktion und
Herstellung: Dr. Thomas Otto Tel.: 0551 201-1828, E-Mail: Thomas.Otto@gwdg.de

1. Das Firewallkonzept der GWDG für das GÖNET

Eine Firewall ist heutzutage die entscheidende Basistechnologie zum Schutz vor Angriffen im Internet. Eine Verbindung zum Internet ohne echten Firewallschutz ist schon seit Jahren grob fahrlässig und gefährdet nicht nur das eigene System, sondern meist auch andere Kommunikationspartner. Die grundlegende Aufgabe einer Firewall ist, etwas vereinfacht formuliert, die Trennung des sicheren internen Netzwerkes von der unsicheren Außenwelt.

Ein Schutz, basierend auf dem eigenen Betriebssystem in Form einer Personal Firewall, ist zwar sinnvoll, aber lediglich als ergänzender Teil eines Gesamtschutzes zu sehen, zudem gerade Personal Firewalls oft entweder durch Benutzerhand oder Viren/Trojaner in ihrer Funktionsfähigkeit beeinträchtigt werden können. Hier sind zentrale Firewalllösungen eine wesentliche Ergänzung.

1.1 Welche Firewall ist die „richtige“?

Man kann drei grundlegend unterschiedliche Firewalltechniken unterscheiden, wobei jede eingesetzte Technik Vor- und Nachteile besitzt. Im Laufe der Entwicklung ist man von den schlichten **Paketfiltern** schon seit einiger Zeit in Richtung **Statefull Inspection Firewall** übergegangen. Paketfilter werden aufgrund diverser Nachteile nur noch selten eingesetzt. Statefull Inspection Firewalls bieten hingegen einen deutlich besseren Schutz und sind im Vergleich zu Paketfiltern (ACLs = **A**ccess **C**ontrol **L**ists) in ihrem Handling deutlich benutzerfreundlicher.

Neuere Entwicklungen wie **Layer 7 (Application Firewall)** bieten einen noch besseren Schutz und bilden derzeit das obere Ende der Firewallentwicklung. Diese Kombination aus Firewall und Proxy-Server, meist in Gestalt einer Appliance, können einen ausgereiften Schutz bieten. Im Folgenden werden die einzelnen Verfahren näher erklärt.

1.1.1 Paketfilter

Paketfilter in Form von ACLs sind auf Routern meist mit Basismitteln zu realisieren. Hierbei wird nach IP-Adressen, IP-Protokoll und ggf. TCP- oder UDP-Ports gefiltert. Überdies ist bei TCP-Verbindungen auch eine Filterung bestimmter TCP-Flags möglich (z. B.: ACK, SYN oder PSH). Der Vorteil bei dieser Art Filterung liegt in der hohen Geschwindigkeit. Die ACLs merken sich keinen Verbindungszustand und schauen nur in einer Tabelle nach, ob eine Verbindung zugelassen ist oder nicht. ACLs sind deshalb auf Routern zwar sehr schnell, aber auch „dumm“. Kommunikation über zustandslose Protokolle wie UDP oder ICMP kann von einer ACL-basierten Firewall nicht sinnvoll behandelt werden, da die zwischen den Kommunikationspartnern ausgehandelten Kommunikationsports einer Verbindung nicht von der Firewall erkannt werden können. Beispiele aus dem Bereich von VoIP oder Videoübertragungen (H.323 oder SIP) zeigen, dass ACLs diese Verbindungen nicht filtern können, was in der Folge zu einer viel zu weiten Öffnung der Firewall bei UDP führt und somit zu einem entscheidenden Sicherheitsverlust. Auch ein Protokollschutz bei „aktivem“ FTP kann ohne nahezu vollständige Öffnung der TCP-Ports (> 1024 - 65535) nicht durch ACLs abgebildet werden.

Eine Kontrolle, ob eine vermeintlich bestehende Verbindung tatsächlich korrekt aufgebaut worden ist, findet nicht statt. Gleiches gilt für eingehende Pakete, die zu einer gültigen Verbindung gehören.

Eine etwaige Kontrolle der Kommunikationsprotokolle in der höheren Anwendungsschicht ist bei ACLs schon prinzipbedingt nicht möglich.

Viele Attacken können mit ACLs nicht erkannt und damit auch nicht verhindert werden. Das betrifft u. a. auch Angriffe der Kategorie (d)DoS, MAC-Spoofing und Flooding.

ACLs können jedoch in Kombination mit „richtigen“ Firewalls einen sinnvollen Gesamtschutz darstellen. Als alleiniger Schutz sind ACLs und damit auch das dahinter befindliche Netz den modernen Angriffsverfahren oft schutzlos ausgeliefert.

1.1.2 Stateful Packet Inspection

Stateful Packet Inspection (SPI) ist eine spezielle Art der Überwachung, bei der die Daten paketweise daraufhin untersucht werden, ob die Firewall den Netzwerkverkehr für legitim hält oder nicht. Alle auffälligen oder unangeforderten Pakete können markiert, dokumentiert oder verworfen werden. Datenpakete werden nur dann von der Firewall durchgelassen, wenn diese zu einer gültigen Sitzung gehören, welche innerhalb des Netzwerks aufgebaut wurde, und wenn sie dem eingestellten Regelwerk entsprechen. Bei diesem Verfahren merkt sich die Firewall alle zu einer Sitzung gehörenden Pakete und Richtungen sowie etwaige Sequenznummern. Gerade diese Eigenschaft ist der entscheidende Unterschied zu einfachen ACLs.

Das folgende Bild soll das Verfahren verdeutlichen:

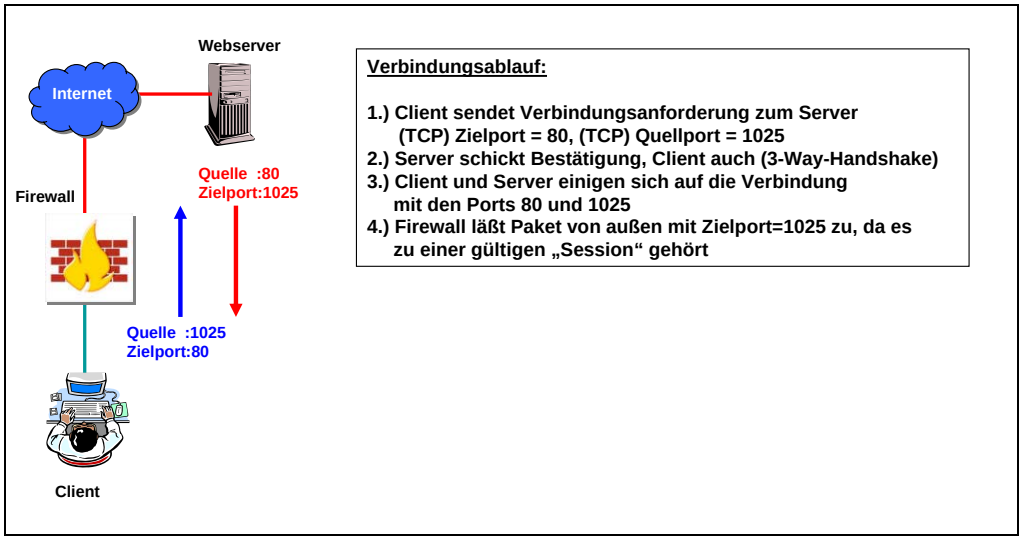

Abb. 1

Bei dieser Kommunikation wird ein Paket von außen nach innen durchgelassen, welches „normalerweise“ aufgrund der Filterregeln die Firewall nicht passieren dürfte. Da sich die Firewall alle initiierten Verbindungsdaten gemerkt hat, kann sie auch die zu der Sitzung gehörenden Pakete von außen entsprechend zuordnen und lässt diese durch (Statefull).

1.1.3 Application Firewall

Diese Firewalltechnologie besteht meistens aus einer Kombination von Proxyserver und Firewall. Hierbei gibt es keine direkte Kommunikation zwischen den Verbindungspartnern. Ein Proxyserver übernimmt den Datenverkehr und steht anstelle des tatsächlichen Partners in Kontakt zu beiden Verbindungspunkten. Überdies schaut sich eine Application Firewall die Datenpakete sehr genau an und kann auf Applikationsebene (Layer 7) die Korrektheit der Kommunikation bewerten und etwaige Maßnahmen ergreifen, wenn ein Eindringling versucht, Zugriff auf das Netzwerk zu bekommen. Wichtig für diese Art Firewall ist natürlich die exakte Kenntnis der höheren Protokolle (http, smtp, ftp usw.). Nachteilig ist hierbei oft die etwas reduzierte Performance (Datendurchsatz), wobei in der letzten Zeit mit der Einführung spezieller Netzwerk- und Filterprozessoren dieses Argument teilweise entkräftet werden konnte. Ein weiterer Nachteil sind durch den Proxyprozess entstehende Latenzen, die bei zeitkritischen Verbindungen, wie IP-Telefonie und Videokommunikation, zu Störungen führen können. Einen weiteren Nachteil bilden die Protokolle selbst. Komplexe, seltene oder proprietäre Kommunikationsprotokolle können von der Application-Firewall ggf. nicht erkannt und infolgedessen auch nicht „durchgelassen“ werden. Hier sind bei Änderungen oder Erweiterungen der höheren Protokolle immer entsprechende Updates der Layer-7-Firewall erforderlich. Des Weiteren müssen die zu schützenden Layer-7-Protokolle auch „Proxy“-fähig sein.

1.1.4 Betriebsarten einer Firewall

Viele Firewalls können in zwei grundlegend unterschiedlichen Modi betrieben werden. Die meisten können mit NAT (**N**etwork **A**ddress **T**ranslation) als Betriebsart umgehen, wenngleich nicht alle den sog. „transparenten“ Modus beherrschen.

1. Transparent Mode

Hierbei passieren die Pakete die Firewall transparent, wobei hinter sowie vor der Firewall das gleiche IP-Netz existieren kann. Transparente Firewalls lassen sich dadurch sehr einfach in bereits bestehende Netzstrukturen einbinden, ohne die IP-Landschaft ändern zu müssen. Filterregeln auf der Firewall definieren, wer, was, wie und wohin darf. Die Firewall wird in diesem Modus nicht als Gateway angesprochen und leitet somit, basierend auf dem bestehen-

den Regelwerk, die Pakete im Layer-2-Modus zu den anderen Interfaces weiter.

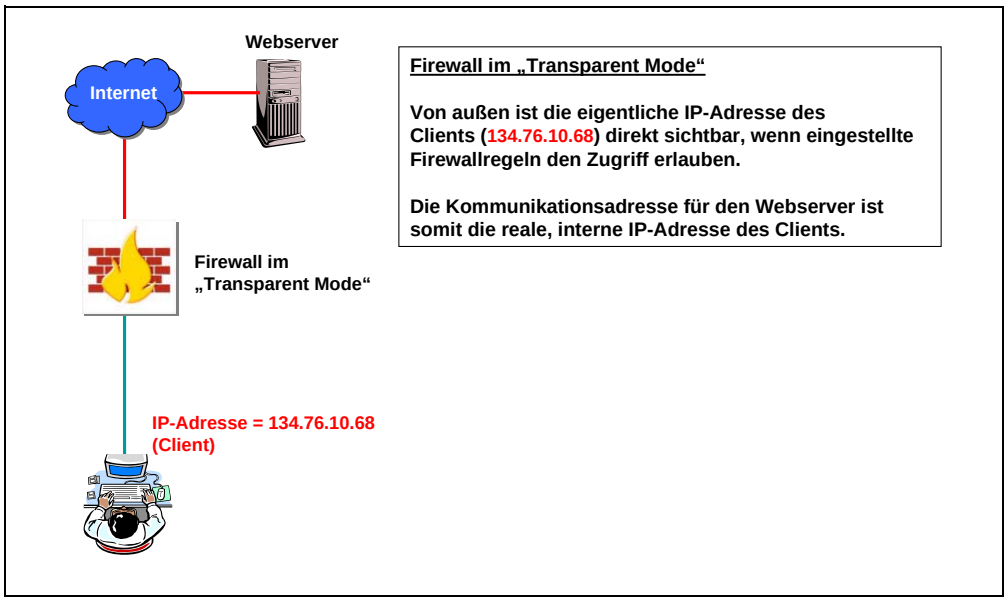

Abb. 2

Vorteile

- Transparente Firewalls sind einfach in bestehende Strukturen zu integrieren.
- Es müssen keine NAT-Tabellen in der Firewall gehalten werden.

Nachteil

- Die Auswahl an Firewallsystemen, die den transparenten Modus unterstützen, ist eingeschränkt.

2. NAT-Mode

Hierbei übernimmt die Firewall eine zentrale Rolle. IP-Adressen hinter der Firewall werden aufgrund von NAT-Regeln in andere IP-Adressen übersetzt. Dieses Verfahren ist vielen Benutzern eines DSL-Zugangs bereits bekannt. Entscheidender Vorteil ist die Tatsache, dass sich hinter einer oder mehrerer IP-Adresse(n) ein gesamtes Netzwerk an Rechnern befinden kann. Von außen ist es sehr schwer, wenngleich nicht unmöglich, herauszubekommen, welche oder wieviele Rechner überhaupt im Netz existieren.

Das folgende Bild stellt den Zusammenhang zwischen interner und externer IP-Adresse bei NAT dar:

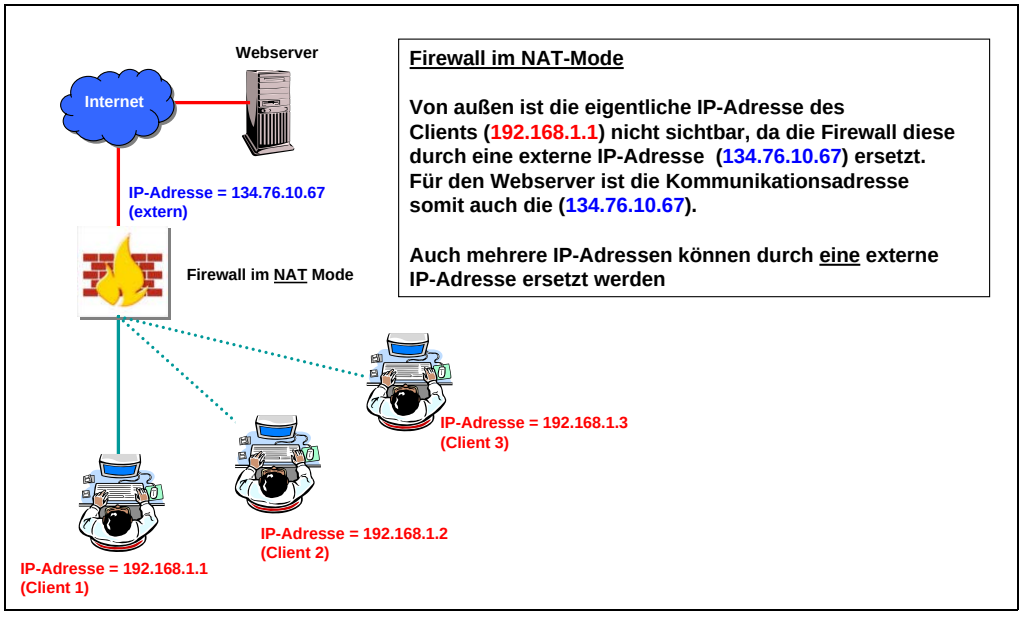

Abb. 3

Bei NAT können wiederum zwei unterschiedliche Varianten eingesetzt werden:

Statisches NAT

Beim statischen NAT (oder auch 1 zu 1-NAT) entspricht jeder internen IP-Adresse ein externes Pendant. Damit ist die Anzahl der IP-Adressen intern wie extern gleich.

Dynamisches NAT

Beim dynamischen NAT können mehrere interne Adressen sich eine externe Adresse teilen. Hierbei müssen aber ggf. die Ports von der Firewall verändert werden.

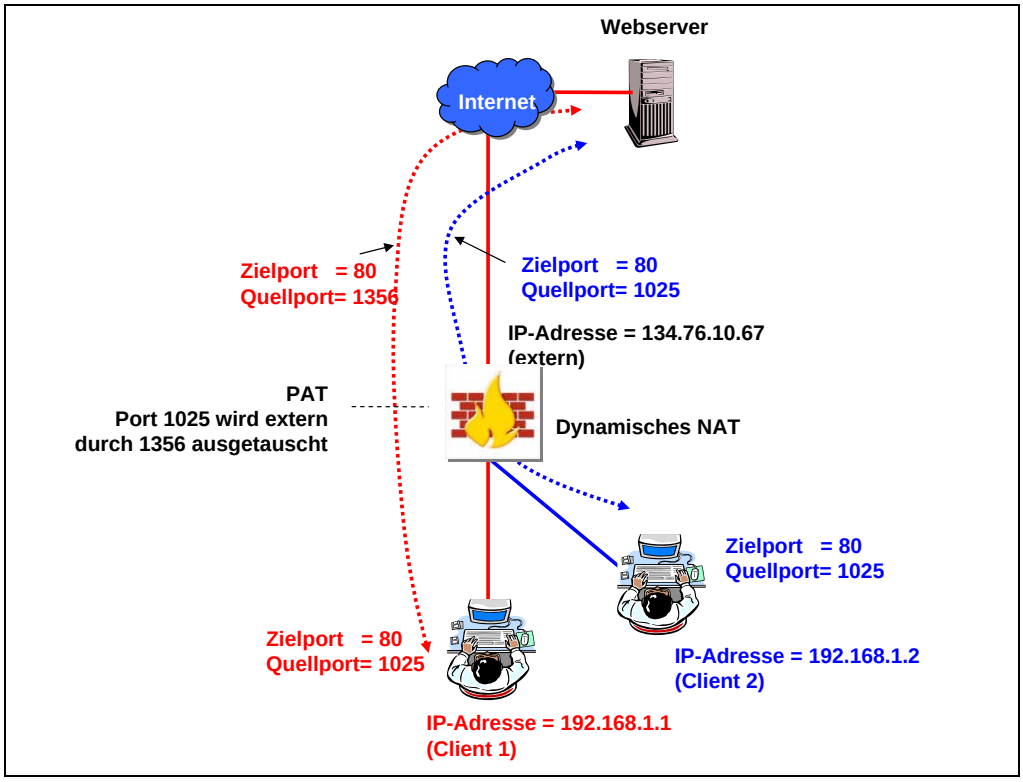

Abb. 4

Wenn die beiden Clients mit intern unterschiedlichen IP-Adressen eine Verbindung zum selben externen Webserver aufbauen, sind für den Webserver diese beiden Clients nicht mehr zu unterscheiden, da die externe Kommunikationsadresse in beiden Fällen identisch ist (134.76.10.67). Damit dennoch die rücklaufenden Pakete des Webservers den entsprechenden Clients zugeordnet werden können, ändert die Firewall die Port-Adresse und merkt sich die Kommunikationspartner inkl. Port in einer internen Tabelle (PAT = **P**ort **A**ddress **T**ranslation).

Vorteile

- Verbergen einer Netzstruktur hinter einer oder mehreren IP-Adressen
- Kein direkter Zugriff von außen auf interne Systeme
- Ein etwaiger Mangel an IP-Adressen kann durch NAT entspannt werden.

Nachteile

- Die Firewall muss neben Zustandstabellen auch NAT-Tabellen führen.
- Einige Protokolle können über eine NAT-Grenze hinweg nicht übertragen werden, da die tatsächliche Quelladresse innerhalb der übertragenen Pakete übermittelt wird und eine Rückverbindung damit ausgeschlossen ist (IPSec, H.323, ggf. SIP).
- Die bisherigen IP-Adressen in dem zu schützenden Netzwerk müssen geändert werden.

Werden nun alle Fähigkeiten der unterschiedlichen Firewalltechniken verglichen, ist ein eindeutiger „Gewinner“ nicht einfach auszumachen. In jedem Fall fällt die Entscheidung zu Ungunsten von ACL, da hier der Schutz zu gering ist.

Die einzusetzende Firewalltechnik muss die Summe der Bedürfnisse aller im GÖNET angebundenen Institute abdecken. Hier wäre auch eine

Kombination aus verschiedenen Techniken denkbar.

1.2 Firewalls im GÖNET

Bislang bestand der Firewallschutz im GÖNET aus ACLs auf den zentralen Routern. Diese ACLs haben einen grundlegenden Schutz vor unerlaubten Zugriffen ermöglicht. Die GWDG hat in der Vergangenheit verschiedene Firewallsysteme auf deren Eignung zum Schutz des GÖNET untersucht. Ziel war es, ein zentral zu verwaltendes Gesamtkonzept für das GÖNET zu etablieren. Allein aufgrund des geringen Schutzes und der komplexen Verwaltung der bisherigen ACLs musste ein neues Verfahren eingeführt werden.

Die Evaluierungsphase

Nur eine kleine Auswahl aus den auf dem Markt existierenden Firewalls ist für den Schutz des GÖNET geeignet. Viele Firewallhersteller konnten allein aufgrund der hohen Datenrate den Anforderungen nicht entsprechen. Immerhin muss auch der Internetzugang mit derzeit 1 Gbit/s durch eine Firewall so abgesichert werden, dass keine für den Benutzer spürbaren Engpässe entstehen.

Die folgenden Punkte waren entscheidend für die Auswahl der Firewall im GÖNET:

1. Einheitliches Management
2. Mehrmandantenfähigkeit
3. Fähigkeit zur Redundanz, Loadbalacing
4. Hoher Durchsatz
5. Einfache Regelstruktur (leicht erlernbar)
6. Transparenter Mode (Stealth Mode)
7. Einfache Integration in bestehende Netzwerkstruktur
8. Logging (syslog)
9. Kombination mit Viruserkennung
10. Erweiterbarkeit
11. Preis

Insbesondere die Punkte 1, 2 und 3 sowie 6 und 7 sind von größerer Relevanz.

Zu den Systemen der engeren Wahl zählten:

- Fortigate der Fa. Fortinet
- Checkpoint Firewall-I (als Appliance)
- CISCO PIX
- CISCO FWSM (**F**irewall **S**ervice **M**odul)

Fortigate Firewalls (`http://www.fortinet.com`) wurden bei der GWDG zweimal im Rahmen einer Teststellung untersucht. Diese Firewalls können in den zwei grundlegend unterschiedlichen Modi, transparent sowie NAT, betrieben werden. Das System hatte ein besonders gut gelungenes Managementinterface (Webinterface), sodass die Fortigate-Systeme nahezu intuitiv bedienbar sind. Allerdings sind während der Testphase Probleme mit zwei Interfaces derart aufgetreten, dass die an den Interfaces angeschlossenen Netze quasi „kurzgeschlossen“ waren. Dieser Fehler trat in den folgenden, neueren Geräten nicht mehr auf.

Checkpoint Firewall wurde nicht als Testsystem bei der GWDG getestet. Die Auswahl bestand eher aus einer eingehenden Recherche der Fähigkeiten. Checkpoint als Firewallhersteller hat eine große Verbreitung. Allerdings spricht der relativ hohe Anschaffungspreis gegen dieses System.

CISCO PIX als Firewalls sind in der GWDG in unterschiedlichen Größen seit längerem im Einsatz. Die Fähigkeiten der PIX-Reihe sind hinlänglich bekannt und würden für den Einsatz im GÖNET prinzipiell genügen. Der Vorteil liegt hier in dem guten Management und der großen Verbreitung.

CISCO FWSM sind Module, die in bestehende CISCO-Router integriert werden können. Der Durchsatz dieser Module ist mit angegebenen 5 - 5,5 Gbit/s sehr groß.

1.3 CISCO FWSM als Firewall für das GÖNET

Als geeignetes Firewallsystem kristallisierte sich im Laufe der Testphase das Firewall Service Modul von CISCO heraus. Neben der hohen Bandbreite war die Fähigkeit, sich in die bereits bestehenden Router desselben Herstellers zu integrieren, das entscheidende Argument. Damit ist es möglich, eine große Anzahl an „virtuellen“ Interfaces an die Firewall zu binden. Hierdurch ist eine Flexibilität gegeben, die andere Firewallhersteller allein aufgrund der Tatsache nicht erbringen können, dass diese als externe Geräte angebunden werden müssen.

Weitere Informationen zu CISCO FWSM sind unter dem URL

```
http://www.cisco.com/en/US/products/hw/
 switches/ps708/products_command_
 reference_chapter09186a00803504f5.html
```

zu finden.

Das Firewallmodul besitzt folgende Fähigkeiten:

- Als Modul in bestehende CISCO-Router integrierbar
- Nahezu gleiche Konfiguration wie PIX-Firewalls
- Variable, große Anzahl an Interfaces (VLANs)

- Hoher Durchsatz (bis 6 Gbit/s)
- Management IOS- sowie webbasiert durch PDM
- Betrieb im transparenten oder Routed Mode
- Multiple security contexts (mehrmandantenfähig)
- Special Features:

  ARP Inspection

  DNS Guard

  Flood Guard

  Frag Guard

  ICMP Filtering

  Mail Guard

  TCP Intercept

  Unicast Reverse

  Path Forwarding

1.3.1 VLAN als Interfaces

Bei dem Firewallmodul existieren aufgrund des Modulcharakters natürlich unmittelbar keine physikalischen Interfaces. Diese werden erst auf dem Router selbst durch VLANs (Virtual LANs) an das Modul gebunden. Ein VLAN wiederum kann dann an ein oder mehrere physikalische Interfaces des Routers angeschlossen sein. Damit erreicht man eine außerordentlich hohe Flexibilität hinsichtlich Anzahl und Lage der Interfaces. Da ein zentraler GÖNET-Router eine ganze Reihe von angeschlossenen Instituten mit dem GÖNET verbindet, ist als Einsatzort der Firewall der ohnehin zentrale Router nahezu ideal. Hier wird die Firewallfunktionalität dort eingesetzt, wo sie auch benötigt wird.

Als Router sind im GÖNET die CISCO Catalyst 6509 eingesetzt. Das folgende Bild stellt schematisch den Zusammenhang zwischen dem Firewallmodul und den Interfaces und der Verbindung über VLANs dar:

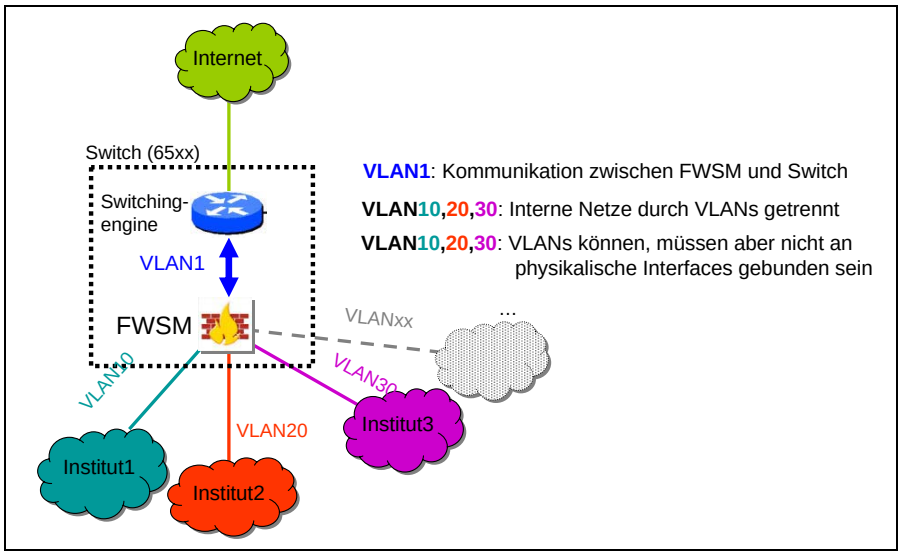

Abb. 5

Das CISCO FWSM beherrscht die zwei unterschiedlichen Betriebsmodi (Transparent sowie Routed). Der Routed Mode ist vergleichbar mit dem zuvor beschriebenen NAT-Mode. Je nach Einsatzort und Zweck ist entweder der transparente Modus oder der Routed Mode sinnvoller.

Für die Absicherung des GÖNET an der Übergangsstelle zum Internet ist bereits ein Firewallmodul im Transparent Mode in Betrieb. Ein Routed Mode wäre hier aufgrund der IP-Adressübersetzung (NAT) nicht sinnvoll. Firewalls an anderen Standorten des GÖNET, insbesondere zur Absicherung der

Institute, sollten hingegen im Routed Mode betrieben werden.

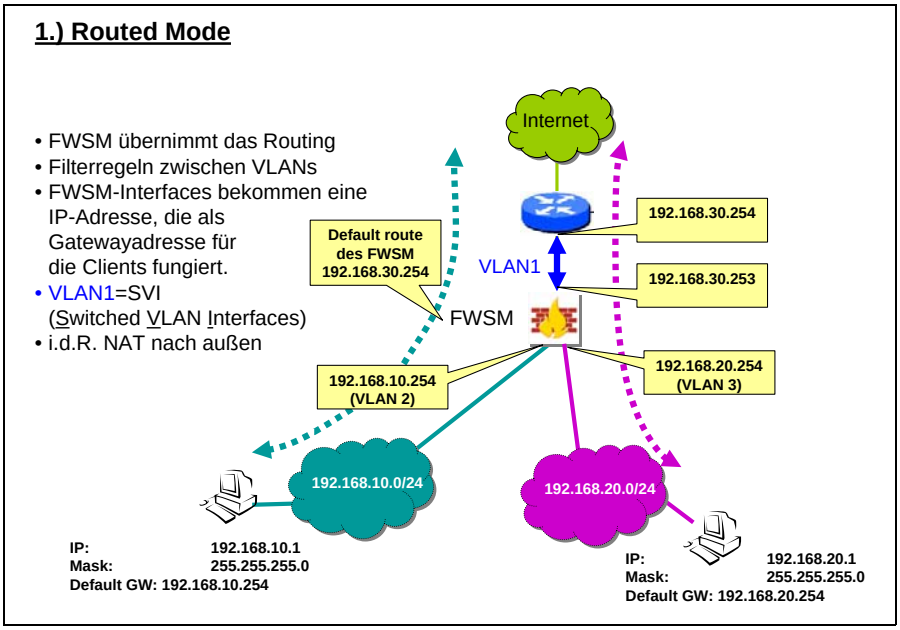

Abb. 6

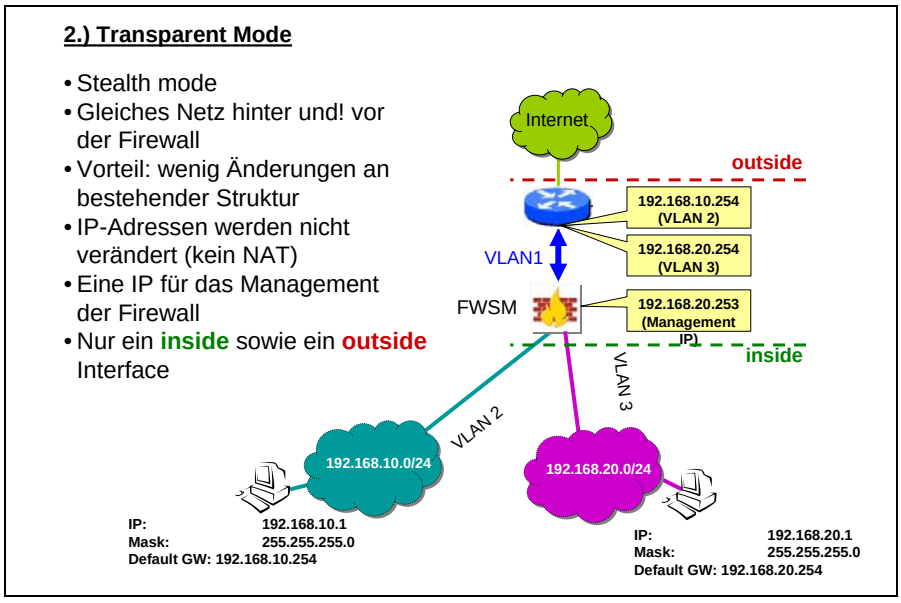

Abb. 7

1.3.2 Mehrere (virtuelle) Firewalls auf einem Modul

Auf einem Firewallmodul können bis zu 255 virtuelle Firewalls betrieben werden. Erst virtuelle Firewalls ermöglichen einen sinnvollen Einsatz im GÖNET. Hierbei kann den einzelnen Instituten jeweils eine eigene virtuelle Firewall zur Verfügung gestellt werden. Das Management dieser Firewall ist dabei vollständig getrennt und unabhängig voneinander. Andere Administratoren können nicht über die eigene virtuelle Firewallgrenze auf andere Firewalls zugreifen.

Wir haben im GÖNET bereits 3 x 20 Firewalllizenzen beschafft, die auf drei Routerstandorte verteilt jeweils 20 virtuelle Firewalls zulassen. Jede virtuelle Firewall kann mit mehreren VLANs (respektive Interfaces) angebunden sein.

Das folgende Bild zeigt den prinzipiellen Aufbau der Virtuellen Firewalls in einem Modul:

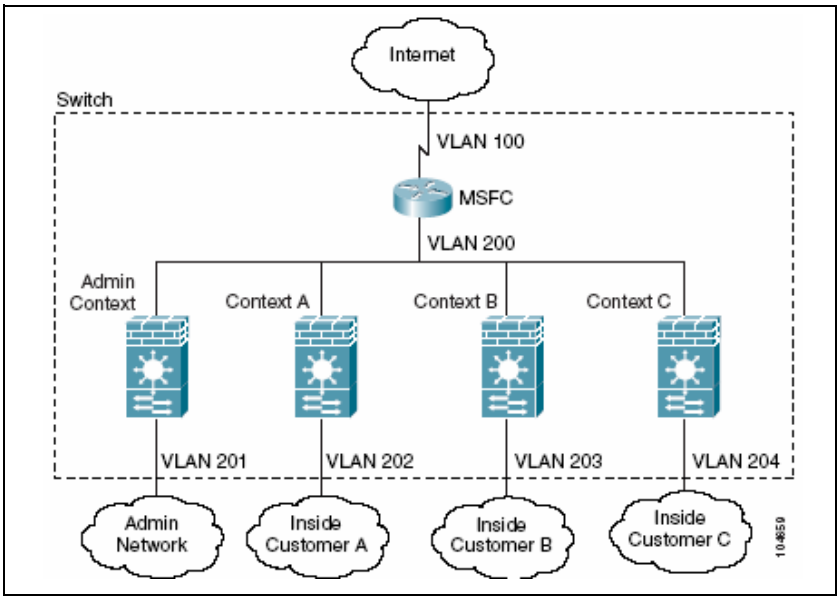

Abb. 8

1.4 Das Gesamtkonzept

Das gesamte Firewallkonzept für das GÖNET umfasst eine zentrale Firewall am Internetübergang und jeweils eine Firewall an jedem Routerstandort; in der Summe also fünf Firewallmodule. Konkret sind es die Standorte:

1. GWDG
2. Fernmeldezentrale
3. Theologicum
4. Neue Physik
5. Physiologie

1.4.1 Zweistufiger Ansatz

Stufe 1: eine zentrale Firewall (First Level Protection)

Hier bildet die zentrale Firewall am Internetübergang einen grundlegenden Schutz für das gesamte GÖNET. Durch schnell veränderbare Basisregeln ist an dieser Stelle ein Grundschutz für alle Institute wirksam. Sind neue Angriffswellen mit definierten Ports in Sicht, können hier die Zugriffe global für das gesamte GÖNET gefiltert werden. Gleiches gilt auch für Angriffe aus dem GÖNET in Richtung Internet.

Stufe 2: dezentrale Firewalls (Second Level Protection)

Die zweite Sicherheitsstufe wird durch eine detailreichere und vor allem auf das Institut abgestimmte Firewall realisiert. Hier sind spezielle Änderungen an den Regelsätzen auf Wunsch, auch durch das Institut, möglich, soweit ausreichende Kenntnisse im Institut vorhanden sind. Erst die Kombination aus beiden Stufen bildet einen optimalen Schutz vor illegalen Fremdzugriffen.

Folgendes Schema verdeutlicht das zweistufige Prinzip:

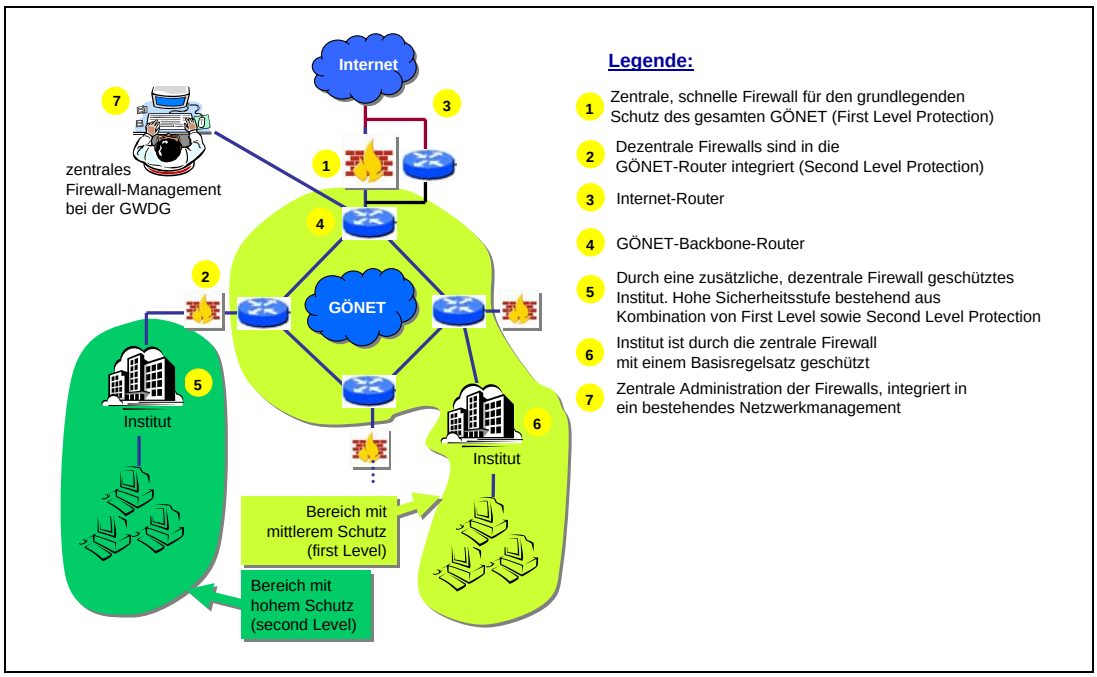

Abb. 9

1.4.2 Virtuelle Firewalls im GÖNET

Durch entsprechende Lizenzen haben wir derzeit bis zu 20 virtuelle Firewalls pro Routerstandort zur Verfügung. Eine geeignete Aufteilung nach Instituten werden wir in den kommenden Wochen und Monaten bedarfsgerecht vornehmen. Da ein vollständig getrenntes Management pro virtueller Firewall möglich ist, kann auch ein Institut selbst auf Wunsch das eigene System konfigurieren. Für das Management der virtuellen Firewall sind fundierte Kenntnisse erforderlich. Im Regelfall wird die GWDG die Administration der Firewalls übernehmen. Wenn ein Institut parallel zur GWDG die eigene virtuelle Firewall administrieren möchte, so bekommt der lokale Administrator einen Zugang mit seinem eigenen Account, den er bei der GWDG besitzt. Unsere zentralen RADIUS-Server ermöglichen einen authentifizierten Zugang zu den Firewalls auf Basis der Benutzerdatenbank der GWDG. Somit sind keine speziellen Benutzernamen/Passwörter erforderlich.

Das folgende Bild zeigt den Zusammenhang zwischen Firewallmodul und virtueller Firewall, wie es im GÖNET eingesetzt wird:

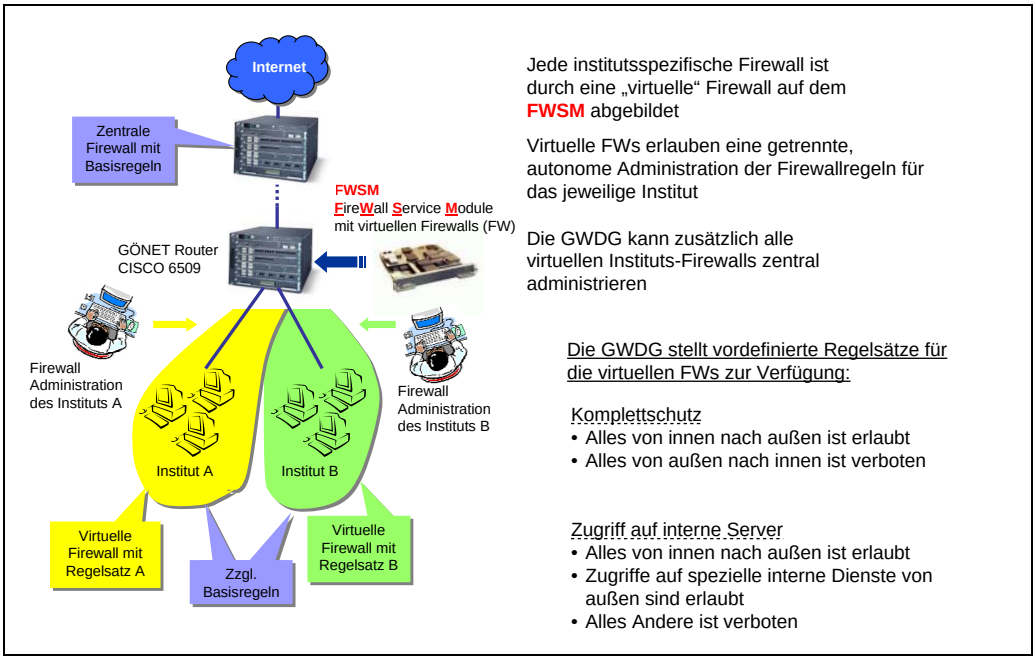

Abb. 10

Welche Firewalls sind derzeit im GÖNET in Betrieb?

1. Firewall der Universitäts-Verwaltung

   Im Oktober 2004 wurde die erste Firewall des Typs CISCO FWSM für den Schutz der Universitätsverwaltung durch die GWDG in Betrieb genommen. Mittlerweile konnten wir über einen längeren Zeitraum Erfahrungen im Betrieb sammeln und schlossen unsere Betrachtungen mit einem durchweg positiven Fazit ab. Diese Firewall befindet sich im Routed Mode und schützt mehrere Subnetze, die durch NAT nach außen kommunizieren. Gerade der Bereich der Verwaltung ist besonders sicherheitsrelevant und bedarf eines umfassenden Schutzes.

2. Zentrale Firewall am Internetübergang

   Im November 2005 wurde die zentrale Firewall am Internetzugang der GWDG in Betrieb genommen. Allerdings musste diese bereits nach einem Tag wieder deaktiviert werden, da ein Fehler in der Firmware des entsprechenden Routers (GR-GWDG1) eine korrekte Funktion nicht zuließ. CISCO hatte kurz darauf den Fehler in der Firmware behoben. Nachdem wir das korrigierte Firmware-Update nach ausführlichen Tests installiert hatten, wurde am 23.01.2006 die zentrale Firewall erneut in Betrieb genommen. Bislang gab es keinerlei Probleme während des Betriebs. Derzeit sind nur wenige Regeln auf der zentralen Firewall geschaltet. Bis Ende Februar werden alle bislang noch in ACLs vorliegenden Regeln in die Firewall übernommen sein.

3. Firewall für das Max-Planck-Institut für biophysikalische Chemie

   Am 11.01.2006 ist mit der NMR II der erste Teilbereich des Max-Planck-Instituts durch eine Firewall geschützt worden. Die Umstellung verlief nahezu komplikationsfrei. Weitere Institutsbereiche werden in den nächsten Wochen und Monaten folgen.

4. Firewall für das Max-Planck-Institut für Dynamik und Selbstorganisation

   Seit August 2005 ist ein (erster) Teilbereich des Max-Planck-Instituts auf dem Gelände am Fassberg ansässig. Er wird durch eine virtuelle Firewall bei der GWDG geschützt.

5. Niedersächsische Staats- und Universitätsbibliothek (SUB)

   In der vierten Woche dieses Jahres sind bereits wesentliche Vorbereitungen für den Anschluss der SUB abgeschlossen worden. Die Anbindung der SUB wird in Kürze erfolgen können.

6. Institutsfirewalls

   In den kommenden Wochen und Monaten werden nach einem festgelegten Plan die Firewallmodule in den anderen Routerstandorten in Betrieb genommen. Mit dieser Erweiterung kön-

nen dann die Institute selbst durch die zweite Sicherheitsstufe geschützt werden. Der Vorgang sollte dann bis Mitte des Jahres abgeschlossen sein.

Die folgende Tabelle gibt einen Überblick über bereits installierte sowie noch in Planung befindliche Firewallmodule:

Name der Firewall	Standort	Datum der Inbetriebnahme
Firewall der Universitäts-Verwaltung (Goßlerstr. 5/7)	Theologicum (Platz der Göttinger Sieben)	10/2004 (in Betrieb)
Zentrale Firewall am Internetübergang	GWDG	1/2006 (in Betrieb)
Firewall für das Max-Planck-Institut für biophysikalische Chemie	GWDG	1/2006 (in Betrieb)
Firewall für das Max-Planck-Institut für Dynamik und Selbstorganisation	GWDG	8/2005 (in Betrieb)
Niedersächsische Staats- und Universitätsbibliothek	Theologicum (Platz der Göttinger Sieben)	1/2006 (in Betrieb)
Studierenden-Hotline: Absicherung der Server	Theologicum (Platz der Göttinger Sieben)	Planung: Feb./März 2006
GWDG: Absicherung des GWDG-internen Servernetzes	GWDG	Planung: Feb./März 2006
GoeMobile: Absicherung des Göttinger Funk-LANs	GWDG	Planung: März/April 2006
Physiologie, weitere Institute in diesem Bereich	Physiologie (Humboldtallee)	Planung: März/April 2006
Neue Physik	Neue Physik (Friedrich-Hund-Platz)	Planung: März/April 2006
Theologicum, weitere Institute am Campus	Theologicum (Platz der Göttinger Sieben)	Planung: April/Mail 2006
Fernmeldezentrale	Fernmeldezentrale (Zimmermannstraße)	Planung: Mai/Juni 2006

1.4.3 Failover und Redundanz

Die Firewallmodule können redundant betrieben werden, sodass bei Ausfall eines Moduls ein anderes die Dienste übernimmt. Das kann entweder ein im gleichen Router installiertes Redundanzmodul sein oder eine Firewall an einem geographisch getrennten Routerstandort.

Ziel im GÖNET ist die Einrichtung von Redundanzszenarien über mehrere Routerstandorte hinweg, sodass im Fehlerfall ein anderer Routerstandort die Firewallfunktionalität automatisch übernehmen kann.

Folgendes Bild stellt diese Zusammenhänge dar:

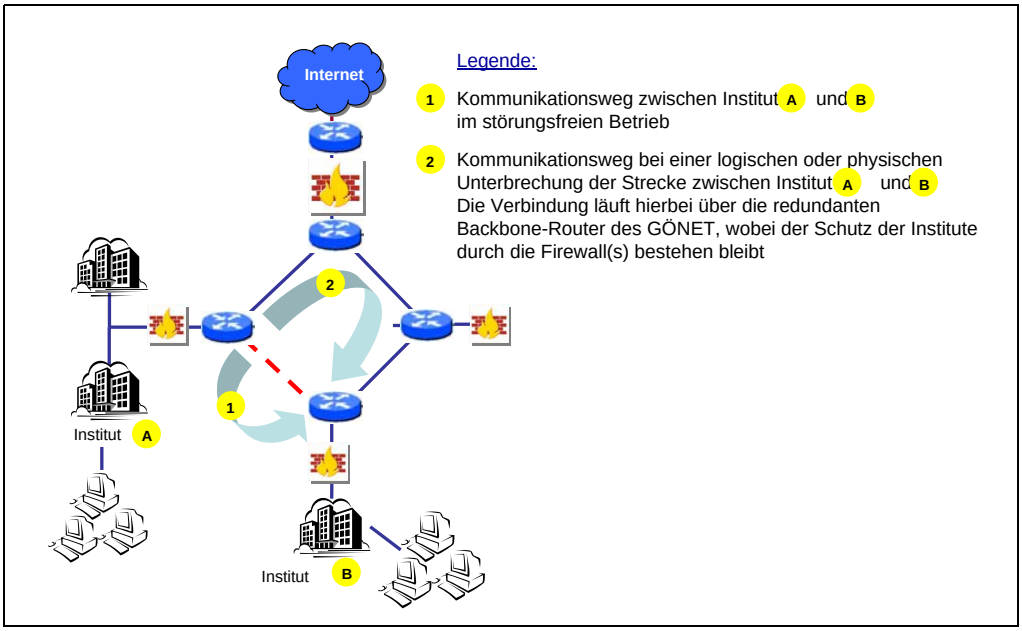

Abb. 11

Die redundante Installation über das gesamte GÖNET hinweg ist relativ komplex, sodass wir erst im Anschluss an die Installationen der Module gemäß der o. g. Tabelle auch die Redundanzen realisieren werden. Bis zu diesem Zeitpunkt haben wir mindestens ein Modul in „Reserve“, sodass wir im Fehlerfall durch Austausch eines defekten Moduls rasch reagieren können. Überdies haben wir einen Wartungsvertrag, der ein permanentes Softwareupdate der Module erlaubt.

1.4.4 Erweiterungen: Viren- und Trojanererkennung durch Logfileauswertung

Die Firewallmodule schreiben die Zustände permanent in Logdateien (SYSLOG). Das können zugelassene sowie natürlich auch abgewiesene Verbindungen sein. Diese Loging-Informationen enthalten die Uhrzeit/Datum, die Quelle und Zieladressen, das Ereignis sowie die in der Verbindung verwendeten Ports. Diesen Umstand machen wir uns zunutze, indem wir die Logdateien entsprechend auswerten und dadurch etwaige Angriffe oder virulentes Verhalten innerhalb des GÖNET besser erkennen können. Die bereits im Göttinger Funk-LAN (GoeMobile) etablierten Verfahren zur Virenerkennung, die in den GWDG-Nachrichten 5/2004

`http://www.gwdg.de/forschung/publikationen/gwdg-nr/GN0405/gn0405_02.html`

dargestellt wurden, können hierdurch sinnvoll ergänzt und auf andere Netzbereiche ausgeweitet werden.

Beim Aufzeichnen der Verbindungsdaten geht es nicht um eine Kontrolle der Institute hinsichtlich ihres Netzwerkverhaltens, sondern vielmehr um die Möglichkeit der qualifizierten und schnellen Reaktion bei Ausnahmefällen wie Virenverbreitung oder Eindringversuchen. Überdies sind die Daten auch nicht personifiziert, sodass ein Rückschluss auf tatsächliche Personen nicht ohne Weiteres möglich ist.

1.5 Fazit und Ausblick

Die bisherigen Erfahrungen mit den Modulen sind überwiegend positiv. Die Integration in bestehende Netzstrukturen des GÖNET ist sehr gut. Der zweistufige Ansatz zur Gesamtsicherung ist auf die Bedürfnisse der Göttinger Wissenschaft abgestimmt und erlaubt überdies ein überschaubares Management und eine schnelle Reaktion auf etwaige Ausbreitungswellen von Viren, Trojanern und Würmern aus dem Internet. In Verbindung mit weiteren Schutzmechanismen, wie das kürzlich bei der GWDG in Betrieb gegangene Intrusion Prevention System (IPS) von Tippingpoint, haben wir einen Schutz etabliert, der mehr als den durchschnittlichen Bedürfnissen an Sicherheit gerecht wird. Selbstverständlich ist ein 100-prozentiger Schutz nie erreichbar, aber eine Annäherung an diese Schwelle sollte mehr als nur als ein Wunsch sein.

Der zweistufige Firewallansatz in Verbindung mit dem IPS-System stellt eine doppelte und gut ergänzende Verteidigungslinie zum Schutz des GÖNET dar.

In einer der kommenden GWDG-Nachrichten werden wir über die Integration des IPS, das zur automatischen Abwehr von diversen Angriffen geeignet ist, berichten. Überdies werden wir über den derzeitigen Stand der Entwicklung in diesem Bereich berichten.

Ißleiber

---

2. Mailservice der GWDG

Wie bereits in den GWDG-Nachrichten 10/2005 ausführlich dargelegt wurde, stellt die GWDG ihren Kunden seit dem Oktober 2005 mit dem Microsoft-Exchange-Cluster einen neuen leistungsfähigen Mailserver zur Verfügung. Daneben betreibt sie nach wie vor auch weiterhin den auf dem Betriebssystem UNIX/Linux basierenden bekannten Mailserver, der bereits seit vielen Jahren zuverlässig seinen Dienst verrichtet und darüber hinaus einige gerade für Institute interessante Funktionalitäten bietet. Auch wenn seit dem 17.10.2005 für Neukunden der **Exchange-Cluster** das Standard-Mailsystem darstellt, kann diese Aufgabe nach wie vor auch der **UNIX-Mailer** erfüllen, wozu der Antragsteller lediglich einen entsprechenden Vermerk im Benutzerantrag vornehmen muss. Im Folgenden soll kurz der Leistungsumfang dieses bewährten Mailsystems beschrieben werden.

2.1 UNIX-Mailserver

Aus Gründen der Performance wurde dieser Server schon vor geraumer Zeit physikalisch auf zwei Rechnersysteme verteilt: **mailer.gwdg.de** für den Mailversand und **mailbox.gwdg.de** für den Mailempfang. Damit bietet er die üblichen Standardprotokolle **SMTP**, **POP3** und **IMAP4** in sowohl verschlüsselter als auch unverschlüsselter Form, um eine komfortable Verwaltung über dedizierte Mailprogramme zu gewährleisten. Steht kein solches Programm zur Verfügung und will man nur über einen Webbrowser bequem auf die eigenen Mails zugreifen, erweist sich das Webmail-Interface als das geeignete Mittel. Derzeit bietet die GWDG zwei davon an: das schon etwas in die Jahre gekommene **IMHO-Webmail-Interface** und das modernere **Squirrelmail**. Wenn keine besonderen Gründe für den Einsatz des IMHO sprechen, sollte hier dem Squirrelmail der Vorzug gegeben werden, da es mit wesentlich mehr Komfort aufwartet und besser mit Dateianhängen umgehen kann.

2.2 SPAM- und Virenfilter

Was die großen Plagen wie Viren, Würmer und unliebsame Werbemails anbetrifft, wartet der UNIX-Mailer mit leistungsfähigen Schutzmaßnahmen auf. Zwei Virenscanner – **Sophos AntiVirus** und **ClamAV** – prüfen jede eintreffende Mail daraufhin, ob sich in ihr Viren oder Würmer befinden. Im Falle eines positiven Befunds wird die Annahme vom Mailer verweigert (s. auch die GWDG-Nachrichten 7/2003). Zur Bekämpfung der lästigen unliebsamen Werbemails (SPAM) prüft das Programm **SpamAssassin** jede eintreffende Nachricht daraufhin und vergibt einen Punktewert. Der Nutzer kann dann über spezielle Filter auf dem Mailer oder in seinem Mailprogramm bestimmen, was in Abhängigkeit dieses Punktewerts mit den Mails zu geschehen hat: Entweder werden sie gelöscht oder in einen dafür eigens vorgesehenen Ordner abgelegt, der dann von Zeit zu Zeit inspiziert werden kann. Dieser Prozedur muss sich jeder Nutzer unterwerfen, um so ein individuell auf seine Umgebung abgestimmtes Filterergebnis zu erzielen. Näheres hierzu kann auf der folgenden Seite nachgelesen werden:

```
http://www.gwdg.de/service/netze/
  mailer/filter/spam.html
```

Diese Funktion der SPAM- und Virenüberprüfung wird als ein spezieller Dienst auch denjenigen Instituten angeboten, die auf den Betrieb eines eigenen Mailers nicht verzichten wollen, aber den Aufwand scheuen, ein eigenes Filtersystem aufzusetzen und zu betreiben. In diesem Fall überprüft die GWDG die für diesen Mailer bestimmte eingehende Mail auf Virenbefall und nimmt eine SPAM-Bewertung vor. Durch einen entsprechenden MX-Eintrag im Domain Name System (DNS) wird dazu eine Umleitung aller für diesen Institutsmailer bestimmten Mails auf den Mailer der GWDG erzwungen, der nach erfolgter Prüfung und Bewertung nur die virenfreien Mails wiederum an den Institutsmailer weiterleitet. Für den Administrator des lokalen Systems entfällt somit ein nicht unerheblicher Betreuungsaufwand. Interessenten senden bitte eine Mail mit dem Betreff „SPAM/Virenfilterung“ an support@gwdg.de.

2.3 Virtuelle Mailer

Einige Institute betreiben aus den verschiedensten teilweise historischen Gründen einen eigenen Mailservice. Da der administrative Aufwand hierfür bisweilen die personellen Kapazitäten übersteigt, könnte hier das von der GWDG angebotene Konzept des „virtuellen Mailers“ eine interessante Lösung darstellen, gerade auch dann, wenn der

Grund des autonomen Mailservers in der Sicherstellung eines eigenen Adressbereichs begründet ist. Bei einem virtuellen Mailserver wird der bisher in eigener Regie und administrativer Verantwortung betriebene Mailservice unter Beibehaltung der bestehenden Adressstrukturen auf den Mailserver der GWDG abgebildet. Er läuft damit auf den Rechnersystemen der GWDG und wird durch die Mitarbeiter der GWDG betreut. Die Einzelheiten einer solchen Migration hängen natürlich stark von den lokalen Gegebenheiten des zu migrierenden Systems ab und müssen im Einzelfall besprochen und ausgearbeitet werden. Interessenten für diesen Service senden bitte eine Mail mit dem Betreff „Virtueller Mailer“ an support@gwdg.de.

Diese Ausführungen sollen unterstreichen, dass dem UNIX-Mailer nicht etwa die Ablösung durch den neuen Exchange-Clusters bevorsteht, sondern im Gegenteil sein Fortbestand nicht zuletzt auch aufgrund seiner interessanten hier dargelegten Möglichkeiten gesichert ist.

Gelbe, Handke, Reimann

---

3. Die neue Microsoft Command Shell

3.1 Einleitung

Windows Vista (vormals bekannt als Longhorn) wirft weit vor seiner Erscheinung auf dem Markt seine Schatten voraus. Viele neue Technologien, die in diesem Betriebssystem zum Einsatz kommen sollen, werden als Public Betas (öffentliche Tests) oder Community Technology Preview (Technikvorschau für die Gemeinschaft), kurz CTPs, schon jetzt für Windows XP und/oder Windows Server 2003 angeboten. Somit erhält jeder interessierte Nutzer/Programmierer die Möglichkeit, sich mit den kommenden Produkten und Technologien vertraut zu machen.

Die kommende Microsoft Command Shell, kurz MSH, vormals bekannt als Monad, bildet hierbei keine Ausnahme.

Das Testen dieser Technologien ist jetzt insoweit einfacher geworden, da das .NET-Framework 2.0 nun endlich in seiner endgültigen Fassung zur Verfügung steht. Dieser Artikel bezieht sich in seinen Erklärungen und Ausführungen auf die unter [1] und [2] angegebene Programmversion und Dokumentation.

3.2 Das neue Konzept der MSH

Mit der MSH wird es nun endlich mal eine „richtige“ Shell aus dem Hause Microsoft für Windows Vista geben. Mit „richtig“ ist eine Shell gemeint, wie es diese unter den UNIX-Derivaten schon lange gibt: KSH, SH, BASH, CSH usw. Da Command.com und CMD.Exe jetzt langsam aber sicher in die Jahre gekommen sind, sollte eine Ablösung kommen, die sich einerseits mit den heute bekannten UNIX-Shells messen kann und andererseits auf dem neuen objektorientierten Programmiermodell, nämlich dem .NET-Framework 2.0, aufsetzt. Dabei ist die schon mehrfach erwähnte MSH herausgekommen.

Die MSH basiert auf anderen Ansätzen als die bisher bekannten traditionellen Shells: Sie kommuniziert über das Objekt-Modell (OM) des .Net-Framework mit dem Betriebssystem und nicht direkt mit ihm. Weiterhin sind bei ihr viele der externen Kommandos, z. B. attrib.exe, von traditionellen Shells als interne Kommandos, Cmdlets (ausgesprochen „command-lets“), enthalten. Dieser Einbau der Kommandos hat den Vorteil, dass ein einheitlicher Interpreter für Parameter allen Cmdlets zur Verfügung steht und nicht jedes Kommando seinen eigenen Parameterinterpreter „mitbringt“. Auch so einfache aber wichtige Dinge wie die Ausgabeformatierung stehen damit zentral und einheitlich zur Verfügung. Somit muss das „Rad“ nicht immer für jedes Kommando neu erfunden werden.

Um diese Ziele zu erreichen, gibt es eine neue Kommandosprache, auf die gleich näher eingegangen wird.

3.3 Erste „Gehversuche“

Ab hier beginnt die Praxis. Aufgerufen wird die Shell über **MSH.EXE,** eingegeben in *Start* | *Ausführen…*, oder über die Verknüpfung *Start* | *Alle Programme* | *Microsoft Command Shell*.

Die schon erwähnten Cmdlets werden als Verb/Hauptwort-Paar eingeben, getrennt durch einen Bindestrich (z. B. Get-Process). Wie an diesem Beispiel ersichtlich, verwenden Cmdlets generell Singular, nicht Plural, also Get-Process und nicht Get-Processes.

Mit dem **Get-Help**-Cmdlet bekommt man Hilfeinformationen, ähnlich dem UNIX-**man**-Kommando. Weitere Beispiele sind:

Get-Help Get-Process

Get-Process -?

Get-Help about_while

Eine generelle Hilfe wird über **Help** zur Verfügung gestellt und mit **Help *** werden alle Hilfethemen aufgelistet.

Eine Liste aller Cmdlets wird mittels **Get-Command** angezeigt.

Über Aliasse oder Pseudonyme wird „Kompatibilität“ zu bekannten Kommandos aus traditionellen Shells hergestellt, wie z. B. **dir**, **type**, **cd ~** usw. Ein Alias wird mit **Set-Alias type Get-Content** gesetzt und mit **remove-item alias:type** entfernt.

Mit dem vorherigen Befehl gibt es einen schönen Übergang zu den „Drives“. Im vorherigen Befehl stellt **alias:** ein solches „Laufwerk“ dar. Mit dem Cmdlet **Get-Drive** werden alle „Drives“ aufgelistet, die die MSH zur Verfügung stellt. Neben den Cmdlets stellen die „Drives“ einen zusätzlichen Zugriff auf das System dar, wie z. B. auf die Systemregistrierung oder den Zertifikatsspeicher. Innerhalb dieser „Drives“ wird mit dem **CD**-Alias navigiert, da die Inhalte der Drives als Ordnerstruktur dargestellt werden. Mit **cd cert:**, **cd currentuser** und **cd My** navigiert man in den persönlichen Zertifikatsspeicher. Die darin enthaltenen Zertifikate werden einfach über **dir** angezeigt.

3.4 Die MSH-Sprache

Aus Gründen der Übersichtlichkeit und Länge des Artikels für diese GWDG-Nachrichten finden Interessenten den überwiegenden Teil der Beispieltabellen, die die MSH-Sprache erklären, sowie detaillierte Erläuterungen zum Arbeiten mit Objekten und zu speziellen Variablen im WWW unter [11].

Dort können nicht alle Möglichkeiten erläutert werden; dazu ist die MSH zu umfangreich. Die wichtigsten und interessantesten Möglichkeiten werden gezeigt und beschrieben. Nähere Definitionen zu den häufig gebrauchten Begriffen „foo“, „bar“ und dem Ergebnis „42“ sind in [3] und [4] zu finden.

3.5 Rohrpost

Die Daten, die die Kommandos aus dem bzw. von dem System erhalten, haben die Form von strukturierten Daten oder Objekten. Diese Daten werden beim Pipelining von einem Kommando zum nächsten weitergereicht, wie in einer Rohrleitung. Am Ende der Leitung werden die so bearbeiteten Daten dann in Text umgewandelt und ausgegeben. Das Pipe-Symbol ist der senkrechte Strich auf der Tastatur („|“).

Für Beispiele siehe u. a. Kapitel 3.9 „Hilfs-Cmdlets“.

3.6 Verwendung von Cmdlets

Das hilfreichste Cmdlet ist **Get-Command**. Dieses Kommando gibt alle Kommandos der MSH als Liste aus. Um die Liste einzugrenzen, kann man z. B. die Eingrenzung auf das Verb vornehmen. **Get-*** zeigt nur alle Kommandos an, deren Verb **Get** ist. **Get-Command** versteht aber auch noch die Parameter **–Verb** und **–Noun**.

Beispiel	Erklärung
Get-Command –Verb get	Zeigt alle Kommandos mit dem Verb **Get** an
Get-Command –Noun process	Zeigt alle Kommandos mit dem Hauptwort **Process** an

Ein weiteres hilfreiches Cmdlet ist **Get-Member**. Um z. B. etwas über die Methoden und Eigenschaften von **Get-Childitem** zu erfahren, braucht man nur folgende Aufrufe abzusetzen:

Beispiel	Erklärung
Get-Childitem | Get-Member –MemberType property	Listet alle Eigenschaften von Get-Childitem auf
Get-Childitem | Get-Member –MemberType method	Listet alle Methoden von Get-Childitem auf

3.7 Hilfs-Cmdlets

Bei den Hilfs-Cmdlets handelt es sich um Kommandos, die Ausgaben aus den Kommandos filtern, sortieren und gruppieren. Dies geschieht unter Zuhilfenahme der in Kapitel 3.5 beschriebenen Pipes. Nachfolgend je ein Beispiel:

Beispiel	Erklärung
Get-Process | Where {$_.Processname –like „*ls*“}	Es werden alle Prozesse angezeigt, die in ihrem Namen „ls“ haben.
Get-Process | Sort-Object @{ e={$_.Processname};asc=$true}	Alle Prozesse werden in aufsteigender Reihenfolge ihres Prozessnamens aufgelistet.
Get-Process | Group-Object {$_.mainmodule.fileversioninfo.companyname}	Die laufenden Prozesse werden nach den Firmennamen aufgelistet, die in ihren Dateinamen in der Dateiinformation enthalten sind.

3.8 MSH - die Shell Ihres Vertrauens?

Alle neueren Microsoft-Produkte beinhalten Möglichkeiten zum Signieren und/oder Verschlüsseln von Dateien und/oder Programmen mittels Zertifikaten. Beispiele sind Office 2003, SQL Server 2005 und die MSH.

In diesem Kapitel wird diese Möglichkeit kurz beschrieben, wobei vorausgesetzt wird, dass der Benutzer/Administrator über ein Zertifikat mit dem Verwendungszweck „Codesignatur“ verfügt. Informationen zur Beantragung sind im letzten Absatz dieses Kapitels zu finden.

Beispiel	Erklärung
$foo = get-childitem cert: \CurrentUser\My -recurse -codesigning	In die Variable **$foo** wird das Zertifikat gespeichert. Mit dem Aufruf **$foo** werden die grundlegenden Informationen zum Zertifikat angezeigt.
$foobar = set-authenticodesignature foobar.msh $foo	Mit dem Cmdlet **set-authenticodesignature** wird die Datei foobar.msh mit dem in der Variablen **$foo** enthaltenen Zertifikat digital signiert. Der Status dieser Operation wird in der Variablen **$foobar** gespeichert.
$foobar.status	Überprüft die Signatur von foobar.msh. Wenn die Datei nicht verändert wurde, wird **Valid** angezeigt.

In der originalen Datei foobar.msh stand nur „Hallo Welt“. Nach der Signierung steht in der Datei foobar.msh Folgendes:

```
Hallo Welt


# SIG # Begin signature block
#
MIIa/wYJKoZIhvcNAQcCoIIa8DCCGuwCAQExCzA
JBgUrDgMCGgUAMGkGCisGAQQB
#
gjcCAQSgWzBZMDQGCisGAQQBgjcCAR4wJgIDAQA
ABBAfzDtgWUsITrck0sYpfvNR

…. (der ganze Codesigning-Block soll hier nicht wiedergegeben werden)

#
OcrLPvHxycLY1rGNRUl3nmZXrucBxXgi6XFJFnu
NSNpCPOZSe9dHmJWJCZl1tMgz
# Oul/
# SIG # End signature block
```

Wie kann man nun steuern, dass z. B. nur signierte Anweisungsdateien in der MSH bzw. auf dem Computersystem ausgeführt werden? In der Systemregistrierung unter *HKLM:\Software\Microsoft\msh\Microsoft.Management.Automation.msh\ExecutionPolicy* kann eine Richtlinie eingestellt werden, wie Anweisungsdateien ausgeführt werden.

Richtlinie	Bedeutung
AllSigned	Alle .msh- und .mshxml-Anweisungsdateien müssen digital signiert sein.
RemoteSigned	Nur .msh- und .mshxml-Dateien aus dem Internet müssen digital signiert sein. Das ist auch die Standardeinstellung.
Unrestricted	Keine Anweisungsdatei muss digital signiert sein.

Um ein Zertifikat zu beantragen, gibt es für die Benutzer der GWDG die unter [9] genannte Zertifizierungsautorität. Speziell für Benutzer, die in die Active-Directory-Gesamtstruktur eingebunden sind, gibt es unter [8] eine Zertifizierungsautorität und für Max-Planck-Institute unter [10]. Für allgemeine und einführende Informationen sei auf die unter [6] und [7] genannten URLs verwiesen.

Direkte Fragen können an die in Kapitel 3.12 genannten E-Mail-Adressen gerichtet werden.

3.9 Erweiterbarkeit

In diesem Kapitel soll die Erweiterbarkeit und die damit verbundene Flexibilität der MSH kurz beschrieben werden. Es wird davon ausgegangen, dass Sie vorher in das Verzeichnis *C:\Programme\Microsoft Command Shell* gewechselt sind.

3.9.1 Cmdlets

In diesem Teil soll ein ganz einfaches Cmdlet geschrieben werden. In den unter [2] angegebenen Dokumenten wird dieses Thema sehr ausführlich behandelt.

Das Cmdlet, das hier entsteht, gibt einfach die Zeichenkette **FooBar** zurück. Der Anweisungsteil ist in der Programmiersprache C# geschrieben. Um Cmdlets zu entwickeln, kann jede vom .Net-Framework unterstützte Programmiersprache, die auch das Voranstellen von Eigenschaften zu Funktionen/Prozeduren (kurz Methoden) unterstützt, genommen werden. Genannt sei hier Visual Basic .Net.

Anweisungsteil	Erklärung
using System; using System.Management.Automation; [Cmdlet(“get”, “foobar”)] public class GetStringFooBar : Cmdlet {	Klassenbibliotheken des .Net-Frameworks und der MSH einbinden. Eigenschaft Verb/Hauptwort der Klasse GetStringFooBar setzen, die von der Klasse Cmdlet erbt.
protected override void EndProcessing() {	Die abstrakte/virtuelle Methode EndProcesing überschreiben.
WriteObject(“FooBar”); } }	Beim Aufruf der Methode wird FooBar ausgegeben.

Rufen Sie mit dem Befehl **notepad foobar.cs** den Editor auf und kopieren Sie den Anweisungsteil in das Textfenster! Bitte achten Sie darauf, dass Sie im Editor alle „“ neu setzen, da diese fehlerhaft kopiert werden! Speichern Sie die Datei! Die folgende Tabelle enthält die Anweisungen, um die Anweisungsdatei **foobar.cs** in eine Cmdlet-Datei umzuwandeln. Diese hat dann den Namen **foobar.dll**.

Befehl	Erklärung
$lib = „$MSHHOME/System.Management.Automation.dll“	Pfad zur Referenzbibliothek für die MSH setzen
$comp = „$env:windir/Microsoft.NET/Framework/v2.0.50727/csc“	Pfad und Anweisungsdateiumwandler (Compiler) setzen
&$comp /target:library /r:$lib foobar.cs	Aufruf des Compiler mit den benötigten Parametern

3.9.2 Make-Shell

Die MSH vertritt das Konzept von Mehrfach-Shells. Die Standard-MSH, wie sie sich nach der Installation präsentiert, kann nicht verändert werden.

Neu erstellte Shells enthalten die Ausführungsprogramme der MSH, Cmdlets und Cmdlet-Provider, die man selber entwickelt hat oder von Dritt-Anbietern erstanden hat.

Die Vorteile der Mehrfach-Shells sind:

- Zusammenstellen von Cmdlet-Paketen für bestimmte Aufgaben und Rollen
- Sicherstellung, dass alle Cmdlets zum Erstellungszeitpunkt zusammen lauffähig sind
- Die Möglichkeit, verschiedene Cmdlets in unterschiedlichen Prozessen laufen zu lassen

Um nun eine neue Shell zu erzeugen, in der wir unser eben gerade erstelltes Cmdlet testen können, muss der Befehl **make-shell** aufgerufen werden. Diesem Befehl werden folgende Parameter mit auf den Weg gegeben:

Parameter	Erklärung
-out FooBarMsh	Name der neuen Shell
-namespace GWDG.MSH	Namensraum für die neue Shell
-reference foobar.dll	Referenz auf das erstellte Cmdlet

Zusammengesetzt ergibt das die Befehlszeile

```
Make-Shell -out FooBarMsh -namespace GWDG.MSH -reference foobar.dll
```

Nach erfolgreicher Erstellung von **FooBarMsh.exe** im aktuellen Verzeichnis kann die Shell mit **.\FooBarMsh.exe** aufgerufen werden.

Bleibt noch der Test des Cmdlets: Rufen Sie dieses mit **get-foobar** auf! Es wird, wie erwartet, die Zeichenkette „foobar“ ausgegeben.

3.9.3 Drives oder Cmdlet-Provider

Die Beschreibung zum Erstellen eines Drives bzw. Cmdlet-Providers würde den Rahmen dieses Artikels sprengen. Daher sei hier auf die unter [2] enthaltenen Dokumente verwiesen, die diesen Punkt sehr ausführlich behandeln.

3.10 Abschluss

Bleibt an dieser Stelle nur noch zu erwähnen, dass Sie die Shell mit **exit** beenden und verlassen können, oder Sie klicken auf das **x** des Fensters mit dem Titel **Microsoft Command Shell**.

Sollte bei Ihnen der Wunsch nach einem eigenen, ausführlicheren Artikel zum Thema Cmdlets und Cmdlet-Provider bestehen, so senden Sie bitte eine E-Mail an die Adresse des Verfassers: thinder@gwdg.de. Bei genügend großer Resonanz wird dann ein Folgeartikel zu diesem Thema verfasst werden.

3.11 Ausblick

Die MSH wird mittelfristig das Scripting unter Windows beinflussen. Sie wird die traditionellen Shells ablösen, wobei sie deren Stärken übernimmt und mit einer modernen und starken Anweisunssprache verbindet, die sich auf das MSH-Objekt-Modell und dem darunter liegenden .Net-Framework 2.0 abstützt. Die damit erreichte Erweiterbarkeit und Flexibilität verleiht der MSH die Fähigkeit, vielfältige administrative Aufgaben zu meistern. Unter [5] wird erwähnt, dass die MSH als administratives Kommando- und Scriptwerkzeug zum Einsatz kommen

wird. Somit wird sie dann auch für das Mailteam der GWDG und alle Administratoren interessant werden, die mittelfristig einen Exchange ‘12’-Server automatisiert warten und pflegen werden.

3.12 Kontakt für Fragen

Für Fragen unmittelbar zu diesem Artikel senden Sie bitte eine Mail an den Verfasser (thinder@gwdg.de). Bei Fragen zu den Zertifikaten senden Sie bitte eine Mail an gwdg-ca@gwdg.de (für MPG-Kunden speziell an mpg-ca@gwdg.de).

3.13 Literatur- und URL-Verzeichnis

[1] Windows „Monad“ Shell Beta 2 (for .NET-Framework 2.0 RC/RTM) x86:

http://www.microsoft.com/downloads/details.aspx?FamilyID=766e6908-354d-44d4-80fd-73e172b8e85d&DisplayLang=en

[2] Windows „Monad“ Shell Beta 2 Documentation Pack:

http://www.microsoft.com/downloads/details.aspx?FamilyID=8a3c71d1-18e5-49d7-952a-c55d694ecee3&DisplayLang=en

[3] Definition von „Foo Bar“ in RFC 3092, „Etymology of "Foo"“:

http://www.faqs.org/rfcs/rfc3092.html

[4] „Per Anhalter durch die Galaxis“ von Douglas Adams, der die Antwort auf alle Fragen bereithält.

[5] Microsoft Ships Exchange '12' Beta:

http://ENTmag.com/news/article.asp?editorialsid=7088

[6] Einstiegspunkt der GWDG-Zertifizierungsautorität (GWDG-CA):

https://ca.gwdg.de

[7] Einstiegspunkt der MPG-Zertifizierungsautorität (MPG-CA):

https://ca.mpg.de

[8] Active-Directory-Gesamtstruktur-Zertifizierungsautorität:

http://gwd-win-ca.gwdg.de

[9] Benutzer-Zertifizierungsautorität der GWDG:

https://ca3.gwdg.de

[10] Benutzer-Zertifizierungsautorität der MPG:

https://user-ca.mpg.de

[11] Die Tabellen, die den größten Teil des Sprachumfangs der MSH erklären:

http://sharepoint.gwdg.de/gwdg/GNArtZus/MSH/MSHBeispiele.aspx

Hindermann

---

4. Kündigung des Lizenzvertrages für Norman Virus Control

Die Institute der Universität Göttingen konnten bislang im Rahmen einer Campuslizenz auf allen ihren PCs die Antiviren-Software der Firma *Norman Data Defense Systems* einsetzen. Nun wird dieser Lizenzvertrag für **Norman Virus Control** von der Universität Göttingen zum 31.10.2006 gekündigt. Das bedeutet, dass ab dem 01.11.2006 kein Anspruch mehr auf Updates besteht. Nutzer dieses Virenscanners sollten somit rechtzeitig auf **Sophos Anti-Virus** der Firma *Sophos* umsteigen. Der einfachste Weg führt hier sicherlich über den Sophos-Update-Service der GWDG (s. auch die GWDG-Nachrichten 10/2003):

http://antivir.gwdg.de

Auf diesem Server findet sich auch eine ausführliche Anleitung, wie dabei vorzugehen ist. Bevor jedoch dieser Weg beschritten wird, sollte zuerst der Norman-Virenscanner deinstalliert werden, da ansonsten Kollisionen zu befürchten sind. Für die Installation des Sophos-Virenscanners ist ein Zugangskennwort erforderlich, welches beim Operating der GWDG (Tel.: 0551 201-1523) in Erfahrung gebracht werden kann. Sollten bei der Migration Probleme auftreten, bietet die GWDG hier selbstverständlich entsprechende Hilfestellung. Dazu kann eine Mail an die Adresse support@gwdg.de gesendet werden.

Reimann

5. Kurse des Rechenzentrums

5.1 Allgemeine Informationen zum Kursangebot der GWDG

5.1.1 Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

5.1.2 Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die

GWDG
Kursanmeldung
Postfach 2841
37018 Göttingen

oder per E-Mail an die Adresse auftrag@gwdg.de mit der Subject-Angabe „Kursanmeldung“ erfolgen. Für die schriftliche Anmeldung steht unter

http://www.gwdg.de/service/nutzung/antragsformulare/kursanmeldung.pdf

ein Formular zur Verfügung. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager - eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu authorisierte Person - oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils 7 Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit dem Dispatcher (Tel.: 0551 201-1523, E-Mail: auftrag@gwdg.de) möglich. Eine Anmeldebestätigung wird nur an auswärtige Institute oder auf besonderen Wunsch zugesendet. Falls eine Anmeldung wegen Überbelegung des Kurses nicht berücksichtigt werden kann, erfolgt eine Benachrichtigung.

5.1.3 Kosten bzw. Gebühren

Die Kurse sind - wie die meisten anderen Leistungen der GWDG - in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

5.1.4 Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu 8 Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

5.1.5 Kursorte

Die meisten Kurse finden in Räumen der GWDG oder des Max-Planck-Instituts für biophysikalische Chemie statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Fassberg, 37077 Göttingen, der Große Seminarraum im Allgemeinen Institutsgebäude dieses Instituts. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL

http://www.gwdg.de/gwdg/standort/lageplan

zu finden. Der gemeinsame Schulungsraum von GWDG und SUB befindet sich im Untergeschoss der Niedersächsischen Staats- und Universitätsbibliothek, Platz der Göttinger Sieben 1, 37073 Göttingen.

5.1.6 Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL

http://www.gwdg.de/service/kurse

zu finden. Anfragen zu den Kursen können an den Dispatcher per Telefon unter der Nummer 0551 201-1524 oder per E-Mail an die Adresse auftrag@gwdg.de gerichtet werden. Zweimal jährlich wird ein Katalog mit dem aktuellen GWDG-Kursprogramm versendet. Interessenten, die in den

Verteiler aufgenommen werden möchten, können dies per E-Mail an die Adresse gwdg@gwdg.de mitteilen.

5.2 Kurse von März bis Dezember 2006 in thematischer Übersicht

EDV-Grundlagen und Sonstiges

Kurse	Termine	Vortragende
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	• 15.03.2006	Dr. Heuer, Nolte, Wagenführ
	• 23.05.2006	Dr. Heuer, Nolte, Wagenführ
	• 12.07.2006	Dr. Heuer, Nolte, Wagenführ
	• 13.09.2006	Dr. Heuer, Nolte, Wagenführ
	• 15.11.2006	Dr. Heuer, Nolte, Wagenführ
Datenschutz - Verarbeitung personenbezogener Daten auf den Rechenanlagen der GWDG	• 04.07.2006	Dr. Grieger
Einführung in die Nutzung des Leistungsangebots der GWDG	• 01.03.2006	Dr. Grieger
	• 17.05.2006	Dr. Grieger
	• 06.09.2006	Dr. Grieger
	• 06.12.2006	Dr. Grieger
Einführung in Aufbau und Funktionsweise von PCs	• 26.06.2006	Eyßell
	• 31.10.2006	Eyßell
Einführung in die Bedienung von Windows-Oberflächen	• 27.06.2006 - 29.06.2006	Eyßell
	• 01.11.2006 - 03.11.2006	Eyßell
Führung durch das Rechnermuseum	• 10.03.2006	Eyßell
	• 21.04.2006	Eyßell
	• 19.05.2006	Eyßell
	• 16.06.2006	Eyßell
	• 14.07.2006	Eyßell
	• 01.09.2006	Eyßell
	• 29.09.2006	Eyßell
	• 10.11.2006	Eyßell
	• 15.12.2006	Eyßell

Betriebssysteme

Kurse	Termine	Vortragende
Linux: KDE-Desktop und Anwendungen	• 20.06.2006	Dr. Schwardmann
Schnellkurs UNIX für Windows-Benutzer mit Übungen	• 29.05.2006 - 30.05.2006 • 10.07.2006 - 11.07.2006 • 27.11.2006 - 28.11.2006	Dr. Bohrer Dr. Bohrer Dr. Bohrer
Grundkurs UNIX/Linux mit Übungen	• 14.03.2006 - 16.03.2006 • 17.10.2006 - 19.10.2006	Hattenbach Hattenbach
UNIX für Fortgeschrittene	• 03.04.2006 - 05.04.2006 • 06.11.2006 - 08.11.2006	Dr. Sippel Dr. Sippel
UNIX/Linux-Arbeitsplatzrechner - Installation und Administration	• 15.05.2006 - 16.05.2006 • 11.12.2006 - 12.12.2006	Dr. Heuer, Dr. Sippel Dr. Heuer, Dr. Sippel
UNIX/Linux-Server - Grundlagen der Administration	• 17.05.2006 - 18.05.2006 • 13.12.2006 - 14.12.2006	Dr. Heuer, Dr. Sippel Dr. Heuer, Dr. Sippel
UNIX/Linux - Systemsicherheit für Administratoren	• 19.05.2006 • 15.12.2006	Dr. Heuer, Dr. Sippel Dr. Heuer, Dr. Sippel
Windows 2000/XP/2003 in kleinen Netzwerken	• 24.04.2006 - 25.04.2006 • 13.11.2006 - 14.11.2006	Quentin Quentin
Die Windows-Active-Directory-Domäne	• 26.04.2006 - 28.04.2006 • 15.11.2006 - 17.11.2006	Quentin Quentin
Cluster- und Raid-Konfigurationen unter Windows 2003	• 02.03.2006 • 31.10.2006	Quentin Quentin

Netze / Internet

Kurse	Termine	Vortragende
Sicherheit im Internet für Anwender	• 09.06.2006 • 01.12.2006	Reimann Reimann
Web Publishing I	• 12.07.2006 - 13.07.2006	Reimann
Web Publishing II	• 31.08.2006 - 01.09.2006	Reimann

Grafische Datenverarbeitung

Kurse	Termine	Vortragende
Grundlagen der Bildbearbeitung mit Photoshop	• 06.09.2006 - 07.09.2006	Töpfer
Photoshop für Fortgeschrittene	• 22.03.2006 - 23.03.2006 • 09.10.2006 - 10.10.2006	Töpfer Töpfer

Sonstige Anwendungssoftware

Kurse	Termine	Vortragende
Einführung in das Computeralgebra-System Mathematica	• 11.10.2006 - 12.10.2006	Dr. Schwardmann
MindMapping mit MindManager	• 22.03.2006 • 05.10.2006	Reimann Reimann
Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG	• 20.04.2006 • 20.10.2006	Reimann Reimann
PDF-Dateien: Erzeugung und Bearbeitung	• 05.07.2006 - 06.07.2006	Dr. Baier
Neuer Kurs !!! PDF-Formulare mit Acrobat Professional und Adobe Designer erstellen	• 07.03.2006 • 05.09.2006	Dr. Baier Dr. Baier
PowerPoint	• 23.05.2006 - 24.05.2006 • 09.11.2006 - 10.11.2006	Reimann Reimann
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, YACOP	• 27.03.2006 - 30.03.2006 • 25.09.2006 - 28.09.2006	Dr. Bohrer, Dr. Liesegang Dr. Bohrer, Dr. Liesegang
DNA-Sequenzierung mit dem Staden Package	• 31.03.2006 • 29.09.2006	Dr. Liesegang Dr. Liesegang
Mit StarOffice zum Schwarzen Loch	• 14.11.2006	Dr. Grieger

Programmiersprachen

Kurse	Termine	Vortragende
Einführung in die Programmiersprache Fortran 90/95	• 03.05.2006 - 04.05.2006	Dr. Schwardmann
Programmierung von Parallelrechnern	• 30.05.2006 - 01.06.2006 • 28.11.2006 - 30.11.2006	Prof. Haan, Dr. Boehme, Dr. Schwardmann Prof. Haan, Dr. Boehme, Dr. Schwardmann

5.3 Kurse von März bis Dezember 2006 in chronologischer Übersicht

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	01.03.2006 17.00 - 20.00 Uhr (SUB)	22.02.2006	0
Cluster- und Raid-Konfigurationen unter Windows 2003	Quentin	02.03.2006 09.15 - 12.30 Uhr und 13.30 - 16.15 Uhr	23.02.2006	4
Neuer Kurs !!! PDF-Formulare mit Acrobat Profes-sional und Adobe Designer erstellen	Dr. Baier	07.03.2006 09.15 - 12.00 Uhr und 13.00 - 16.00 Uhr	28.02.2006	4
Führung durch das Rechner-museum	Eyßell	10.03.2006 10.00 - 12.30 Uhr	03.03.2006	0
Grundkurs UNIX/Linux mit Übungen	Hattenbach	14.03.2006 - 16.03.2006 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	07.03.2006	12
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	15.03.2006 16.15 - 17.45 Uhr	08.03.2006	1
Photoshop für Fortgeschrittene	Töpfer	20.03.2006 - 21.03.2006 09.30 - 16.00 Uhr	13.03.2006	8
MindMapping mit MindManager	Reimann	22.03.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	15.03.2006	4
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, YACOP	Dr. Bohrer, Dr. Liesegang	27.03.2006 - 30.03.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	20.03.2006	16
DNA-Sequenzierung mit dem Staden Package	Dr. Liesegang	31.03.2006 09.30 - 12.30 Uhr und 13.30 - 16.00 Uhr	24.03.2006	4
UNIX für Fortgeschrittene	Dr. Sippel	03.04.2006 - 05.04.2006 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr	27.03.2006	12
Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG	Reimann	20.04.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	13.04.2006	4
Führung durch das Rechner-museum	Eyßell	21.04.2006 10.00 - 12.30 Uhr	14.04.2006	0
Windows 2000/XP/2003 in kleinen Netzwerken	Quentin	24.04.2006 - 25.04.2006 09.30 - 15.30 Uhr	17.04.2006	8
Die Windows-Active-Directory-Domäne	Quentin	26.04.2006 - 28.04.2006 09.30 - 15.30 Uhr (am 28.04. bis 13.00 Uhr)	19.04.2006	10

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Einführung in die Programmier-sprache Fortran 90/95	Dr. Schwardmann	03.05.2006 - 04.05.2006 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	26.04.2006	8
UNIX/Linux-Arbeitsplatzrechner - Installation und Administration	Dr. Heuer, Dr. Sippel	15.05.2006 - 16.05.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	08.05.2006	8
UNIX/Linux-Server - Grundlagen der Administration	Dr. Heuer, Dr. Sippel	17.05.2006 - 18.05.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	10.05.2006	8
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	17.05.2006 17.00 - 20.00 Uhr	10.05.2006	0
UNIX/Linux - Systemsicherheit für Administratoren	Dr. Heuer, Dr. Sippel	19.05.2006 09.30 - 12.30 Uhr und 13.30 - 15.00 Uhr	12.05.2006	4
Führung durch das Rechner-museum	Eyßell	19.05.2006 10.00 - 12.30 Uhr	12.05.2006	0
PowerPoint	Reimann	23.05.2006 - 24.05.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	16.05.2006	8
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	23.05.2006 16.15 - 17.45 Uhr	16.05.2006	1
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	29.05.2006 - 30.05.2006 13.00 - 16.30 Uhr	22.05.2006	4
Programmierung von Parallelrech-nern	Prof. Dr. Haan, Dr. Boehme, Dr. Schwardmann	30.05.2006 - 01.06.2006 09.15 - 12.15 Uhr und 13.30 - 16.30 Uhr	23.05.2006	12
Sicherheit im Internet für Anwender	Reimann	09.06.2006 09.15 - 12.00 Uhr	02.06.2006	2
Führung durch das Rechner-museum	Eyßell	16.06.2006 10.00 - 12.30 Uhr	09.06.2006	0
Linux: KDE-Desktop und Anwen-dungen	Dr. Schwardmann	20.06.2006 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	13.06.2006	4
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	26.06.2006 09.15 - 12.30 Uhr	19.06.2006	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	27.06.2006 - 29.06.2006 09.15 - 12.30 Uhr	20.06.2006	6
Datenschutz - Verarbeitung perso-nenbezogener Daten auf den Rechenanlagen der GWDG	Dr. Grieger	04.07.2006 09.00 - 12.00 Uhr	27.06.2006	2
PDF-Dateien: Erzeugung und Bearbeitung	Dr. Baier	05.07.2006 - 06.07.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	28.06.2006	8

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	10.07.2006 - 11.07.2006 13.00 - 16.30 Uhr	03.07.2006	4
Web Publishing I	Reimann	12.07.2006 - 13.07.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	05.07.2006	8
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	12.07.2006 16.15 - 17.45 Uhr	05.07.2006	1
Führung durch das Rechner-museum	Eyßell	14.07.2006 10.00 - 12.30 Uhr	07.07.2005	0
Web Publishing II	Reimann	31.08.2006 - 01.09.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	24.08.2006	8
Führung durch das Rechner-museum	Eyßell	01.09.2006 10.00 - 12.30 Uhr	25.08.2006	0
Neuer Kurs !!! PDF-Formulare mit Acrobat Profes-sional und Adobe Designer erstellen	Dr. Baier	05.09.2006 09.15 - 12.00 Uhr und 13.00 - 16.00 Uhr	29.08.2006	4
Grundlagen der Bildbearbeitung mit Photoshop	Töpfer	06.09.2006 - 07.09.2006 09.30 - 16.00 Uhr	30.08.2006	8
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	06.09.2006 17.00 - 20.00 Uhr (SUB)	30.08.2006	0
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	13.09.2006 16.15 - 17.45 Uhr	06.09.2006	1
Methoden und Werkzeuge der Sequenzanalyse: GCG, EMBOSS, YACOP	Dr. Bohrer, Dr. Liesegang	25.09.2006 - 28.09.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	18.09.2006	16
DNA-Sequenzierung mit dem Staden Package	Dr. Liesegang	29.09.2006 09.30 - 12.30 Uhr und 13.30 - 16.00 Uhr	22.09.2006	4
Führung durch das Rechner-museum	Eyßell	29.09.2006 10.00 - 12.30 Uhr	22.09.2006	0
MindMapping mit MindManager	Reimann	05.10.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	28.09.2006	4
Photoshop für Fortgeschrittene	Töpfer	09.10.2006 - 10.10.2006 09.30 - 16.00 Uhr	02.10.2006	8
Einführung in das Computeralgebra-System Mathematica	Dr. Schwardmann	11.10.2006 - 12.10.2006 09.00 - 12.00 Uhr und 13.00 - 16.00 Uhr	04.10.2006	8
Grundkurs UNIX/Linux mit Übungen	Hattenbach	17.10.2006 - 19.10.2006 09.15 - 12.00 Uhr und 13.30 - 16.00 Uhr	10.10.2006	12

Kurs	Vortragende	Termin	Anmelde-schluss	AE
Die Kommunikationsplattform Microsoft Exchange Server bei der GWDG	Reimann	20.10.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	13.10.2006	4
Cluster- und Raid-Konfigurationen unter Windows 2003	Quentin	31.10.2006 09.15 - 12.30 Uhr und 13.30 - 16.15 Uhr	24.10.2006	4
Einführung in Aufbau und Funktionsweise von PCs	Eyßell	31.10.2006 09.15 - 12.30 Uhr	24.10.2006	2
Einführung in die Bedienung von Windows-Oberflächen	Eyßell	01.11.2006 - 03.11.2006 09.15 - 12.30 Uhr	25.10.2006	6
UNIX für Fortgeschrittene	Dr. Sippel	06.11.2006 - 08.11.2006 09.15 - 12.00 Uhr und 13.15 - 15.30 Uhr	30.10.2006	12
PowerPoint	Reimann	09.11.2006 - 10.11.2006 09.15 - 12.00 Uhr und 13.00 - 15.00 Uhr	02.11.2006	8
Führung durch das Rechner-museum	Eyßell	10.11.2006 10.00 - 12.30 Uhr	03.11.2006	0
Windows 2000/XP/2003 in kleinen Netzwerken	Quentin	13.11.2006 - 14.11.2006 09.30 - 15.30 Uhr	06.11.2006	8
Mit StarOffice zum Schwarzen Loch	Dr. Grieger	14.11.2006 09.00 - 12.00 Uhr	07.11.2006	2
Die Windows-Active-Directory-Domäne	Quentin	15.11.2006 - 17.11.2006 09.30 - 15.30 Uhr (am 17.11. bis 13.30 Uhr)	08.11.2006	10
Broschürenerstellung, Spezial- und Posterdruck bei der GWDG	Dr. Heuer, Nolte, Wagenführ	15.11.2006 16.15 - 17.45 Uhr	08.11.2006	1
Schnellkurs UNIX für Windows-Benutzer mit Übungen	Dr. Bohrer	27.11.2006 - 28.11.2006 13.00 - 16.00 Uhr	20.11.2006	4
Programmierung von Parallelrech-nern	Prof. Dr. Haan, Dr. Boehme, Dr. Schwardmann	28.11.2006 - 30.11.2006 09.15 - 12.15 Uhr und 13.30 - 16.30 Uhr	21.11.2006	12
Sicherheit im Internet für Anwender	Reimann	01.12.2006	24.11.2006	2
Einführung in die Nutzung des Leistungsangebots der GWDG	Dr. Grieger	06.12.2006 17.00 - 20.00 Uhr	29.11.2006	0
UNIX/Linux-Arbeitsplatzrechner - Installation und Administration	Dr. Heuer, Dr. Sippel	11.12.2006 - 12.12.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	04.12.2006	8
UNIX/Linux-Server - Grundlagen der Administration	Dr. Heuer, Dr. Sippel	13.12.2006 - 14.12.2006 09.30 - 12.30 Uhr und 13.30 - 16.30 Uhr	06.12.2006	8

Kurs	Vortragende	Termin	Anmelde-schluss	AE
UNIX/Linux - Systemsicherheit für Administratoren	Dr. Heuer, Dr. Sippel	15.12.2006 09.30 - 12.30 Uhr und 13.30 - 15.00 Uhr	08.12.2006	4
Führung durch das Rechner-museum	Eyßell	15.12.2006 10.00 - 12.30 Uhr	08.12.2006	0

6. Betriebsstatistik Januar 2006

6.1 Nutzung der Rechenanlagen

Rechner	Zahl der Prozessoren	CPU-Stunden
DECalpha	8	107,90
IBM RS/6000 SP	152	12.294,54
IBM Regatta	124	70.977,76
Linux Parallel	252	164.448,31
Linux Opteron	96	52.274,58

6.2 Betriebsunterbrechungen

Rechner/PC-Netz	Störungen		System-pflege	
	Anzahl	Stunden	Anzahl	Stunden
UNIX-Cluster	0		0	
IBM SP/Regatta	0		0	
Linux Parallel	0		0	
Linux Opteron	0		0	
PC-Netz	0		0	
Nameserver	0		0	
Mailer	0		0	

7. Autoren dieser Ausgabe

Name	Artikel	E-Mail-Adresse / Telefon-Nr.
Bodo Gelbe	• Mailservice der GWDG	bgelbe@gwdg.de 0551 201-1522
Dr. Eckhard Handke	• Mailservice der GWDG	ehandke@gwdg.de 0551 201-1548
Thorsten Hindermann	• Die neue Microsoft Command Shell	thinder@gwdg.de 0551 201-1837
Andreas Ißleiber	• Das Firewallkonzept der GWDG für das GÖNET	aisslei@gwdg.de 0551 201-1815
Michael Reimann	• Mailservice der GWDG	Michael.Reimann@gwdg.de 0551 201-1826
Michael Reimann	• Kündigung des Lizenzvertrages für Norman Virus Control	Michael.Reimann@gwdg.de 0551 201-1826