



Leibniz-Rechenzentrum

Mit Sicherheit richtig verbunden

Leibniz-Rechenzentrum hilft Studenten mit Cisco VPN-Lösungen bei der Recherche



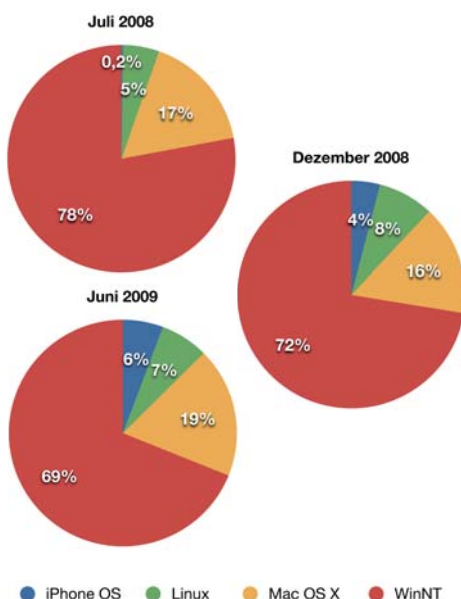
Cisco Remote-Access mit ASA5500 im Cluster-Verbund

Das Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften geht zurück auf eine im Jahr 1962 von Hans Piloty und Robert Sauer gegründete „Kommission für elektronisches Rechnen“, heute „Kommission für Informatik“. Unter ihrem Dach wurde das LRZ mit Mitteln des Freistaats Bayern als gemeinsames Rechenzentrum für Forschung und Lehre für alle Münchner Hochschulen geschaffen. Neben seiner Aufgabe als IT-Dienstleister für mehr als 100.000 Kunden an den Hochschulen in München und für die Bayerische Akademie der Wissenschaften, stellt das LRZ mit dem Münchner Wissenschaftsnetz (MWN) eine leistungsfähige Kommunikations-Infrastruktur bereit und ist ein Kompetenzzentrum für Datenkommunikationsnetze. Darüber hinaus ist das LRZ ein Zentrum für alle deutschen Hochschulen im Bereich des technisch-wissenschaftlichen Hochleistungsrechnens („Supercomputing-Zentrum“) und betreibt umfangreiche Platten- und automatisierte Kassetten-Speicher zur Sicherung großer Datenmengen.

Zahlreiche Organisationen sind an das Münchner Wissenschaftsnetz (MWN) angeschlossen und bieten Studenten und Hochschulmitarbeitern Zugang zu Datenbanken und Online-Zeitschriften an. Diese Dienste dürfen nur von Nutzern angefordert werden, die dazu berechtigt sind. Dazu setzt das LRZ VPN-Server ein, die diese Berechtigung überprüfen und eine gesicherte Verbindung herstellen. Einmal erfolgreich angemeldet, kann vom heimischen PC aus oder über das WLAN im MWN nach Fachliteratur oder Informationen recherchiert werden.

Wissenschaftliche Recherchen per Webzugang

Besonders die „Online Public Access Catalogs“ (OPACs) der Hochschulbibliotheken spielen eine große Rolle bei der Recherche über das MWN, denn der Zugang zu den OPAC-Diensten erfolgt in der Regel webbasiert. In den OPACs finden Interessierte kostenfrei Informationen über den Bestand aller Bibliotheken eines Landes. Neben reinen Literaturnachweisen stehen den Studierenden auch Inhaltsangaben oder Volltexte von Büchern und Zeitschriftenartikeln zur Verfügung. Zusätzlich hat das LRZ mit der Firma Gartner, einem der weltweit führenden Marktforschungsinstitute im IT-Bereich, einen Vertrag abgeschlossen. Allen Mitarbeitern und Studenten der Ludwig-Maximilians-Universität München (LMU), der Technischen Universität München (TUM) und der Bayerischen Akademie der Wissenschaften wird so der Zugang zum Core Research Paket von Gartner ermöglicht.



Anteile der Betriebssysteme am VPN-Verkehrsvolumen; starker Trend aufwärts mit Apples „iPhone“

Allgemein

Hintergrund

Das Leibniz-Rechenzentrum (LRZ) stellt in der Wissenschafts- und Hochschullandschaft Münchens mit dem Münchner Wissenschaftsnetz (MWN) eine leistungsfähige Kommunikationsinfrastruktur bereit und ist ein Kompetenzzentrum für Kommunikationsnetze. Grundlage der IT-Dienstleistungen für die Münchner Hochschulen ist das Konzept einer „verteilten, kooperativen DV-Versorgung“. Es erlaubt nicht nur den Zugang zum Internet, sondern vor allem auch den ständigen Zugriff auf Daten und Programme auf anderen Rechnern.

Herausforderung

Studenten und Mitarbeiter der Hochschulen sollten die Möglichkeit bekommen, auch von externen Standorten wie zu Hause, aus dem Studentenwohnheim oder von unterwegs auf die geschützten Ressourcen der Universitäten zurückzugreifen. Die Lösung sollte dazu einfach zu administrieren sein, mitwachsen und sich gleichzeitig in die vorhandene Netzinfrastruktur integrieren lassen.

Lösung

Das LRZ hat bereits seit längerer Zeit eine sehr gute Zusammenarbeit mit Cisco unterhalten und zahlreiche Produkte im Einsatz. Bereits im Jahr 2003 setzte das LRZ eine VPN-Lösung von Cisco ein. Um den zukünftigen Anforderungen gerecht zu werden, stieg das LRZ 2007 auf die neue Cisco ASA-Produktreihe um.

Nutzen

- o einfache Administration
- o schnelle Integration in bestehende Netze
- o vollständige Abwicklung des RAS-VPN Verkehrs des LRZ für alle Studenten über ein Cluster
- o Höhere Performance und Skalierbarkeit
- o Absicherung des Zugangs
- o Zuordnung von Nutzern zu bestimmten Einrichtungen (Autorisierung)

Neue Anforderungen an VPN-Dienste

Studenten und Angehörige der Hochschulen können die Onlinedienste der Bibliotheken, also den Zugriff auf elektronische Zeitschriften und Datenbanken, nur nutzen, wenn sie anhand ihrer IP-Adresse eindeutig einer dieser Institutionen zugeordnet werden können. Bis 2003 setzte das LRZ auf Zugangsdienste auf Basis von PPTP (Point-to-Point Tunneling Protocol). Allerdings hatten diese einige Schwachstellen. Installation, Konfiguration und Betrieb erforderten schon bei einer kleinen Benutzergruppe einen sehr großen Betreuungsaufwand. Zudem war der PPTP-Client nur für Rechner mit einem Windows-Betriebssystem relativ leicht zu installieren. Für Linux oder Mac OS X musste der Client selbst übersetzt und installiert werden.

Im August 2003 wurde nach einer Testphase ein neuer VPN-Dienst von Cisco eingeführt. Bereits seit längerem arbeitet das LRZ mit Cisco zusammen und hat zahlreiche Produkte im Einsatz.

Umfassende Cisco-Lösung

Mit der Cisco VPN 3000 Serie bekam das LRZ erstmals eine umfassende Lösung, die sich durch Besonderheiten wie Clusterfähigkeit von mehreren Komponenten oder Redundanz der Hardware (Netzteil, Crypto-Engine) auszeichnet. Gleichzeitig ermöglicht die VPN 3000 Serie eine einfache Administration über das GUI, eine zentrale Verwaltung der VPN-Policy für alle Benutzer und die Anbindung an bestehende Infrastruktur. Hinzu kam ein kostenfreier VPN-Client, der mit allen populären Betriebssystemen eingesetzt werden kann. Für Linux steht neben dem Cisco-Client zusätzlich der Open Source VPN-Client vpnc im Quellcode zur Verfügung. Dieser ist inzwischen in den Standard-distributionen wie SuSE, Ubuntu oder Debian enthalten.

Seit 2005 hat sich der Datendurchsatz jährlich verdoppelt. Aufgrund der weiterhin steigenden Auslastung der vorhandenen VPN-Server musste das LRZ den VPN-Cluster weiter aufrüsten. 2007 setzte das LRZ auf die nochmals leistungsfähigere und weiterentwickelte Plattform Cisco ASA 5500. Diese Appliances sind in den bestehenden VPN-Cluster integriert und verwenden die vorhandene Infrastruktur für die Authentisierung und Autorisierung der Nutzer. Durch den Einsatz der neuen VPN-Server ließ sich schließlich die verfügbare VPN-Bandbreite von vormals 50 MBit/s mit einem VPN 3030 auf jetzt 1.450 MBit/s mit einem VPN 3030 und vier ASA5540 steigern.

Ausbau mit Blick in die Zukunft

Der ursprüngliche VPN-Dienst basierte auf der VPN 3000 Serie und ist mittlerweile komplett durch die ASA 5500 Serie abgelöst. Heute wird der VPN 3030 lediglich noch für LAN-to-LAN Kopplungen zur Anbindung von Außenstellen außerhalb des MWN genutzt, für deren Anbindung die Performance noch ausreichend ist.

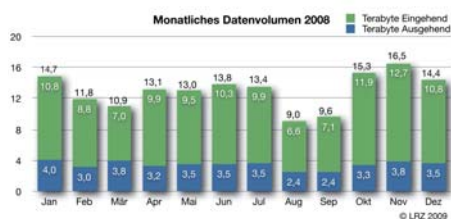
Stand heute setzt das LRZ vier Cisco ASA 5540 ein, die jeweils mit 1Gbit/s angeschlossen und zu einem VPN-Cluster zusammengefasst sind. Bei der Anmeldung werden die Nutzer direkt mit dem VPN-Server verbunden, der zu diesem Zeitpunkt die geringste Datenlast zu bewältigen hat. Die verfügbare Bandbreite der verschlüsselten Verbindungen beträgt 350Mbit/s pro eingesetzter ASA 5540. Authentifizierung und Autorisierung der Nutzer erfolgt über das RADIUS-Protokoll.

Während der Umstellung auf ASA nutzte das LRZ sowohl die bestehenden Geräte der VPN 3000 Serie als auch die neue ASA Plattform parallel in einem gemeinsamen Cluster.

Mit dem weiteren Ausbau erfolgte auch die Erweiterung auf neue VPN-Dienste. Telearbeiter des LRZ sind beispielsweise automatisch über VPN-Router inklusive VoIP-Diensten an das MWN angeschlossen. Der integrierte Cisco VPN-Client ermöglicht zudem auch den Zugriff über das sehr beliebte Apple iPhone. Durchschnittlich 20.000 VPN-Sessions verursachen die iPhone-Nutzer im



Die Cisco ASA 5500 Adaptive Security Appliance ist eine hoch integrierte Sicherheitslösung inklusive Firewall-, Network-Antivirus- und VPN-Dienste.



Entwicklung des monatlichen Datenvolumens im Jahr 2008.

Monat und bilden damit bereits sechs Prozent der VPN-Nutzer bei einem VPN-Gesamtverkehr, der aktuell bei mehr als 20 Terabyte im Monat liegt.

Inzwischen ist die Migration vollständig abgeschlossen. Der komplette Betrieb des VPN-Verkehrs erfolgt für alle Studenten und Angehörige der Hochschulen über das Cluster der ASA-Familie im LRZ. Insgesamt vier ASA5540 Appliances sind dazu für den Remote-Access im Einsatz. Eine Erweiterung der ASA-5540 auf SSL-VPN wird demnächst verfügbar sein. Diese wird durch den neuen Cisco AnyConnect Client angeboten und unterstützt jetzt auch Betriebssysteme wie Vista-64-Bit oder auch Windows-Mobile(5/6).



Cisco Systems GmbH
Kurfürstendamm 21-22
D-10719 Berlin

Cisco Systems GmbH
Neuer Wall 77
D-20354 Hamburg

Cisco Systems GmbH
Hansaallee 249
D-40549 Düsseldorf

Cisco Systems GmbH
Friedrich-Ebert-Allee 67-69
D-53113 Bonn

Cisco Systems GmbH
Ludwig-Erhard-Straße 3
D-65760 Eschborn

Cisco Systems GmbH
Wilhelmsplatz 11
(Herold Center)
D-70182 Stuttgart

Cisco Systems GmbH
Am Söldnermoos 17
D-85399 Hallbergmoos

Tel.: 00800-9999-0522
www.cisco.de

Für technische Beratung bezüglich der Cisco-Produktwahl oder Fragen zu Ihrem Netzwerkdesign wenden Sie sich bitte an das Cisco Technical Helpdesk unter der Rufnummer 00800-9999-0522 oder schreiben Sie eine E-Mail an information@external.cisco.com

Copyright © 1992–2008, Cisco Systems, Inc. Alle Rechte vorbehalten. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, das Cisco Systems-Logo, Registrar und SMARTnet sind eingetragene Marken von Cisco Systems, Inc. und/oder ihren verbundenen Unternehmen in den USA und bestimmten anderen Ländern.

Alle anderen in diesem Dokument oder auf der Website erwähnten Marken sind das Eigentum der jeweiligen Besitzer. Die Verwendung des Wortes „Partner“ impliziert keine Partnerschaftvereinbarung zwischen Cisco und einem anderen Unternehmen. (0208R)