Virtuelle Firewalls im Münchner Wissenschaftsnetz (MWN)

Ralf Kornberger
Helmut Reiser
Claus Wimmer
Leibniz-Rechenzentrum München

1 Zusammenfassung

Beim Betrieb eines geographisch stark verteilten Netzes mit einem institutionenübergreifenden Versorgungsauftrag, bei dem die Organisationseinheiten zudem noch sehr unabhängig voneinander sind, kann mit einem nur zentralen Firewall-Ansatz den Sicherheitsbedürfnissen nicht begegnet werden. Individuelle Sicherheitspolicies müssen unterstützbar sein. Hier bieten virtuelle Firewall-Ansätze eine angemessene Möglichkeit. Eine virtuelle Firewall bezeichnet dabei eine Firewall-Instanz eines Kunden auf einer Netzkomponente, welche die Möglichkeit bietet mehrere unabhängige und mandantenfähige Firewall-Instanzen nebeneinander zu betreiben. Der Beitrag berichtet über Einsatzszenarien und –erfahrungen von virtuellen Firewalls im Münchener Wissenschaftsnetz, das vom Leibniz-Rechenzentrum betrieben wird. Nach der Vorstellung des Einsatzumfeldes wird die Anforderungsanalyse vorgestellt und auf ökonomische Aspekte eingegangen. Der Beitrag zeigt die verschiedenen Realisierungsgesichtspunkte und schließt mit einer Darstellung der Betriebserfahrungen.

2 Das Münchner Wissenschaftsnetz

Das Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften ist das Hochschulrechenzentrum für die Universitäten (Ludwig-Maximilians Universität (LMU), Technische Universität (TUM)) und Fachhochschulen im Großraum München. Es ist Zentrum für technisch-wissenschaftliches Hochleistungsrechnen (Nationales Supercomputing-Zentrum) für alle deutschen Hochschulen, es betreibt umfangreiche Platten- und automatisierte Magnetband-Speicher zur überregionalen Sicherung und Archivierung großer Datenmengen. Es stellt mit dem Münchner Wissenschaftsnetz (MWN) eine leistungsfähige Kommunikationsinfrastruktur auch für zahlreiche weitere Wissenschaftsinstitutionen bereit und ist Kompetenzzentrum für Kommunikationsnetze. Daneben bietet es eine Vielzahl von Diensten, Beratung, Kursen sowie Spezial-Hardware (z.B. im Bereich Visualisierung und Multimedia) für die Wissenschaftler im Großraum München an [1].

Über das MWN [2] werden mehr als 60 Standorte versorgt. Obwohl das Netz „Münchner“ Wissenschaftsnetz heißt, zeichnet es sich durch eine erhebliche räumliche Ausdehnung (vgl. Abbildung 1) aus. Es reicht im Süden von der Zugspitze und dem Wendelstein über das Münchner Stadtgebiet im Norden neben Garching und Freising, Weihenstephan bis nach Ingolstadt, Straubing und Triesdorf.

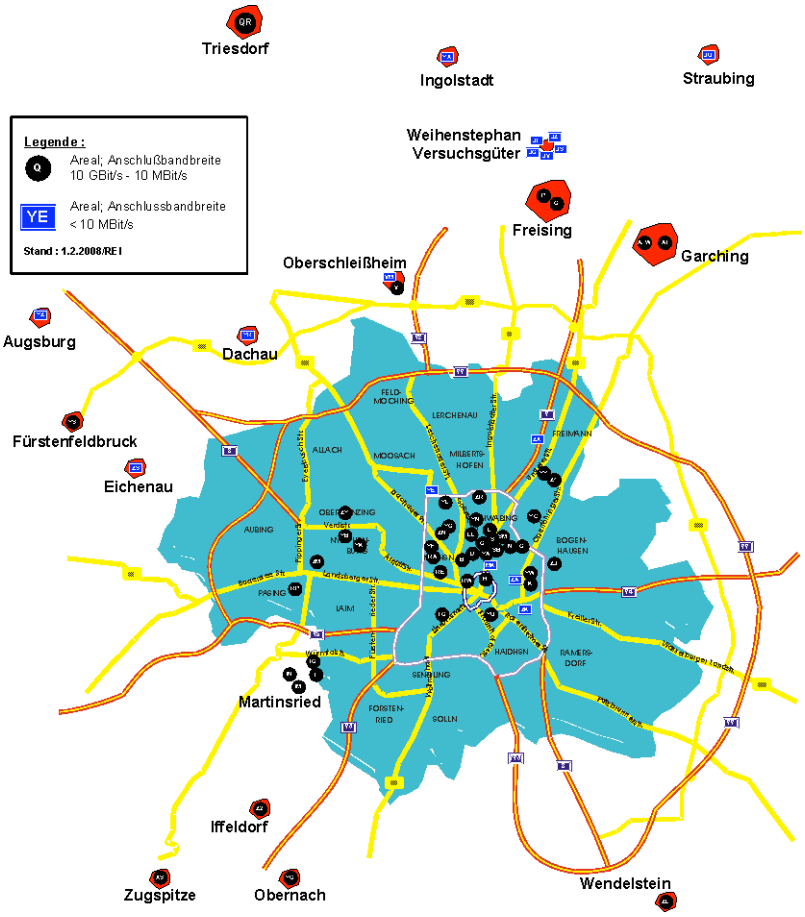

Abbildung 1: MWN geographische Ausdehnung (nicht Maßstabsgetreu)

Das Netz ist für alle Studenten, Wissenschaftler und sonstigen Mitarbeitern zugänglich, d.h. es hat eine potentielle Anzahl von mehr als 120.000 Nutzern. Derzeit sind rund 65.000 Systeme an das Netz angeschlossen, wobei der Anteil der Server ca. 5 % beträgt.

Das Backbone des MWN ist als Dreieck konzipiert (vgl. Abbildung 2), das aus Knotenzentralen an der TUM, der LMU und dem LRZ gebildet wird. Die Knotenstandorte sind über 10 Gigabit Ethernet (10 GE) untereinander verbunden. Durch diese Struktur wird eine Redundanz erreicht, die auch einen Faserbruch zwischen zwei Standorten tolerieren kann. Die Internet Anbindung ist ebenfalls mit 10 GE ausgelegt und erfolgt über das X-WiN des Deutschen Forschungsnetzes (DFN). Zusätzlich dazu gibt es eine redundante Anbindung mit 1 GE über einen lokalen Provider (M-Net), auf den der Internet-Verkehr im Fehlerfall automatisch, schnell und transparent umgeschaltet werden kann. Das Backbone und die Verbindungen zu entfernten Standorten sind größtenteils durch langfristig angemietete „dark-fibre“-Leitungen (Monomode-Lichtwellenleiter) realisiert.

Im Backbone wurden im Januar 2007 rund 2,4 Petabyte, über den Internet-Übergang wurden im gleichen Zeitraum knapp 300 Terabyte (170 TB eingehend und 120 TB ausgehend), übertragen.

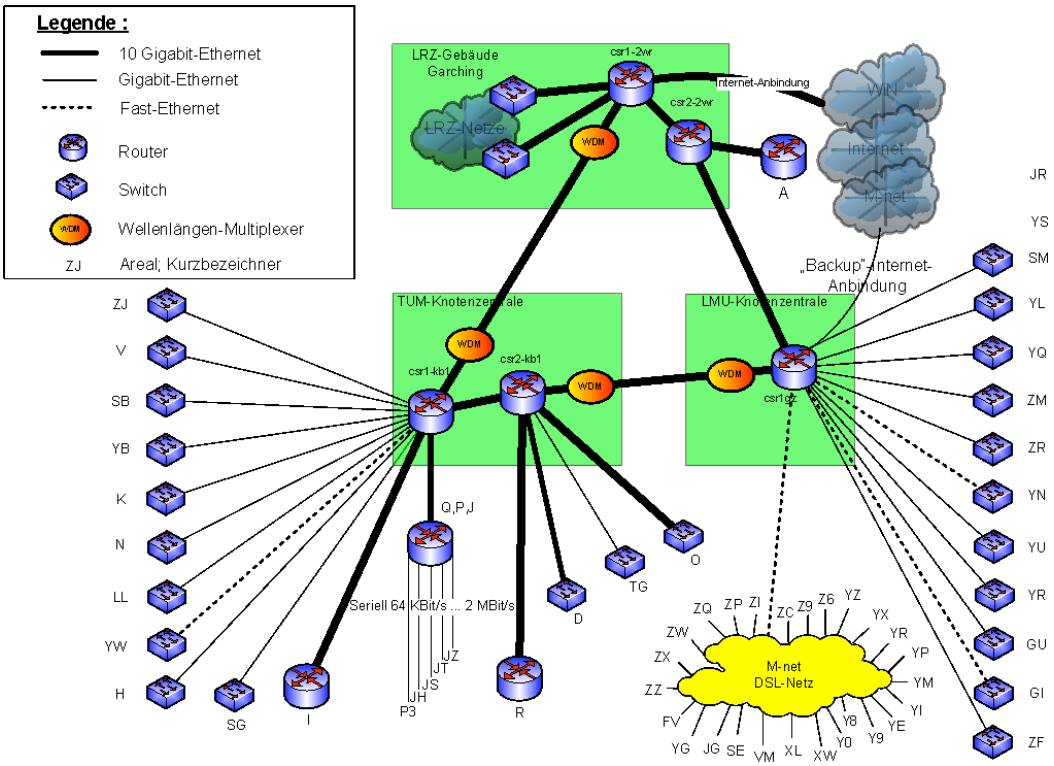

Abbildung 2: MWN Backbone

Technisch gesehen besteht das MWN aus 12 Routern, mehr als 860 Switches und rund 1000 Access-Points. An den Routern sind die jeweiligen Standorte bzw. Gebäude (gegliedert in sogenannte Areale) über Switches angebunden, d.h. im Edge Bereich erfolgt die Kommunikation auf Schicht 2. Hier handelt es sich um ein Netz in Switching-Technologie. Routing erfolgt nur im Backbone.

Das LRZ ist verantwortlich für die Planung, den Aufbau, Betrieb und Management des MWN. Die Verantwortung reicht bis zur „Datendose". Die dort angeschlossenen Systeme werden von den Lehr- und Forschungseinheiten oder den Instituten betrieben. Eine administrative Kontrolle über die Endsysteme hat das LRZ daher nicht. In den einzelnen Arealen gibt es jeweils lokale Administratoren—sogenannte Netzverantwortliche. Der Betrieb des Netzes erfolgt in Kooperation mit den Netzverantwortlichen, sie sind das Sprachrohr in die jeweilige Institution und unterstützen das LRZ.

Eine der vordringlichen Aufgaben ist die kontinuierliche Erhöhung des Sicherheitsniveaus und der Schutz der Systeme im Wissenschaftsnetz vor Angriffen von außen, aber auch gegen unberechtigte Übergriffe innerhalb der lokalen Netze. Zu einem der wichtigen Sicherheitsmechanismen gehört die Festlegung von Regeln, welche Systeme mit welchen anderen Rechnern über welche Protokolle kommunizieren dürfen. Technisch werden diese Regeln mit Hilfe von Firewalls umgesetzt. Das LRZ versucht hier auf zwei Wegen zu unterstützen. Einerseits kommt der Einsatz einer zentralen Firewall allen Nutzern des MWN zugute, ohne dass diese individuell aktiv werden müssten. Andererseits kann ein Regelsatz, der für alle Nutzer gilt, nur einen sehr allgemeinen Schutz bieten und nicht auf spezifische Anforderungen einzelner Kunden eingehen. Daher empfiehlt das LRZ seinen Kunden den Betrieb eigener Firewall-Systeme. In der Vergangenheit bedeutete dies für die einzelnen Lehr- und Forschungseinheiten oder Fakultäten, dass diese eigene Firewalls beschaffen, pflegen und warten sowie für den Unterhalt aufkommen mussten. Für das LRZ war es durch die Vielzahl der unterschiedlichen Firewall-Systeme schwierig den Kunden bei Problemen beratend zur Seite zu

stehen. Das LRZ suchte deshalb nach einer Lösung, um den Kunden einen kostengünstigen, zentral betriebenen, aber auf lokale Gegebenheiten anpassbaren und dezentral administrierbaren „mandantenfähigen Firewall-Dienst“ anzubieten. Ziel war es jedem Kunden seine eigene Firewall-Instanz anbieten zu können, ohne dafür dedizierte Hardware pro Firewall zu beschaffen.

3 Anforderungen an eine Kunden-Firewall

Das LRZ hat verschiedene Realisierungsalternativen untersucht, um seinen Kunden möglichst einfach Firewalls anbieten zu können. Dabei war die Leitidee, in jedem Fall Mandantenfähigkeit zu erreichen, d.h. jedem Kunden „seine eigene“ Firewall anzubieten. In diesem Abschnitt werden die Anforderungen an den neuen Dienst vorgestellt. Das zukünftige Firewall-Produkt muss natürlich die wichtigsten modernen Firewall-Techniken unterstützen - im folgenden Teilabschnitt werden diese kurz beschrieben. Abschnitt 3.2 befasst sich mit den LRZ-spezifischen Anforderungen. Das Kapitel schließt mit einer Betrachtung der ökonomischen Aspekte.

3.1 Technische Firewall-Anforderungen

Eine Firewall („Brandschutzmauer“) ist eine Netz-Sicherheitskomponente, die zwei oder mehrere Netzsegmente miteinander koppelt und den Datenverkehr kontrolliert. [3] [4] Dabei ist es das Ziel, innerhalb der Netzstruktur den Verbreitungsweg einer akuten Gefahr (z.B. unerwünschte Login-Versuche oder ein Computer-Wurm) einzuschränken. Zu diesem Zweck wird der Datenverkehr zwischen den Netzsegmenten von der Firewall klassifiziert und abhängig von der Klasse erlaubt oder verhindert.

3.1.1 Firewall-Typen

Firewalls lassen sich grundsätzlich in zwei Gruppen einteilen:

- *Netz-Firewalls*(oder kurz Firewalls) sind zumeist dedizierte Geräte (Hardware und Software), die mindestens zwei Netzsegmente voneinander trennen.
- *Personal Firewalls* bestehen aus einer Software, die entweder auf einem Rechner – Desktop oder Server – zusätzlich installiert wird oder bereits in das Betriebssystem integriert ist, und dienen nur dem Schutz genau dieses Rechners.

Der Schwerpunkt dieses Artikels liegt auf Netz-Firewalls; die Autoren verweisen zum Thema „Personal Firewalls“ auf weiterführende Literatur. [5]

Produkte aus dem Netz-Firewall-Bereich erlauben in der Regel zwei alternative Betriebsmodi:

- Im *Routing-Modus* arbeitet die Firewall als Router und ist deshalb im Netz sichtbar – wie jede andere Komponente auf Schicht 3.
- Im *Bridging-Modus* (auch Transparent-Modus) arbeitet die Firewall als Switch und ist deshalb im Netz nicht sichtbar und auch nur schwer zu entdecken. Ein Angriff auf die Firewall selbst wird dadurch erschwert.

3.1.2 Sicherheitszonen

Firewalls sind ein unverzichtbarer Bestandteil des Konzeptes verschiedener Sicherheitszonen. [6] Hinter diesem Konzept steckt die Idee, durch ein abgestuftes System von Netzbarrieren und Netzbereichen die Angriffsfläche der eigenen Netze zu verringern.

Sicherheitszonen umfassen ein oder mehrere Netzsegmente, deren Rechner im Hinblick auf die Sicherheitsleitline (Policy) [7] in einem oder mehreren relevanten Eigenschaften gleich oder ähnlich sind. Aus den relevanten Eigenschaften lässt sich für jede Sicherheitszone eine Vertrauensstufe ableiten. Die verschiedenen Vertrauensstufen bestimmen die Kommunikationsbeziehungen zwischen den Sicherheitszonen.

In einem universitären Umfeld lassen sich beispielsweise die Mitarbeiterrechner eines Institutes in einer Sicherheitszone zusammenfassen. In der Regel sind diese Rechner im Hinblick auf Betriebssystem und Applikationsportfolio einander sehr ähnlich. Die Benutzer sind bekannt und ihre Anzahl ist überschaubar. Aufgrund des regelmäßigen Datenaustausches mit externen Internet-Diensten wie z.B. WWW oder E-Mail besteht jedoch die Gefahr einer Kompromittierung dieser Rechner. Deshalb liegt die Vertrauensstufe im mittleren Bereich. Das Internet kann als externe Sicherheitszone mit niedriger Vertrauensstufe aufgefasst werden, da dort sowohl Rechner als auch deren Benutzer unkontrollierbar sind. Eine Sicherheitszone mit hoher Vertrauensstufe könnte Verwaltungsrechner enthalten, die wegen der Bearbeitung vertrauenswürdiger oder personenbezogener Daten besonders zu schützen sind. Die Höhe der Vertrauensstufe einer Sicherheitszone sollte sich also umgekehrt proportional zur Wahrscheinlichkeit einer Kompromittierung der Rechner in der Sicherheitszone verhalten.

Im universitären Umfeld handelt es sich in den meisten Fällen um zunächst zwei Zonen, die auf jeden Fall voneinander getrennt werden sollen:

1. Externe Netze (WAN): Dabei handelt es sich fast immer um das Internet.
2. Interne Netze (LAN): Institutsnetz, z.B. Mitarbeiterrechner und PC-Pools.

Darüberhinaus kommen häufig drei weitere Zonen vor:

3. Demilitarisierte Zone (DMZ): In dieser Zone befinden sich Server, die Dienste für externe Netze anbieten und deshalb aus den externen Netzen erreichbar sein müssen.
4. Verwaltung: Hier befinden sich Rechner, auf welchen in der Regel sensitive Daten abgelegt und verarbeitet werden.
5. Management: In dieser Zone befinden sich alle Netzkomponenten wie z.B. Switches, Router und Firewalls (Out-of-Band Management).

3.1.3 Firewall-Technologie

Bei der Klassifizierung des Datenverkehrs stehen einer Firewall unterschiedliche Methoden zur Verfügung. Die wichtigsten Methoden werden inzwischen von fast allen gängigen Firewall-Produkten unterstützt.

Paketfilter

Jeder Typ von Firewall beherrscht zumindest das Filtern von Paketen der Internet-Protokolle auf der Grundlage von Quell-IP-Adresse, Quell-Port, Ziel-IP-Adresse und Ziel-Port. Eine Filterregel enthält ein Suchmuster aus mindestens einem spezifizierten Element des 4-Tupels und eine Aktion, z.B.“ Paket erlauben“ oder „Paket abweisen“. Der Paketfilter setzt sich aus einer Menge von Filterregeln zusammen, mit deren Hilfe über das „Schicksal“ eines Paketes entschieden wird, das aus einer der angebundenen Sicherheitszonen eintrifft.

Stateful Packet Inspection (SPI)

Stateful Packet Inspection ist eine Weiterentwicklung des einfachen Paketfilters. Dabei wird von der Firewall pro erlaubter Verbindung ein Eintrag in eine dynamische Zustandstabelle vorgenommen und damit der Verbindungsstatus festgehalten. Zusätzlich zum 4-Tupel aus IP-Adressen und Ports wird der aktuelle Verbindungsstatus bei der Entscheidungsfindung über das Schicksal der eintreffenden Pakete herangezogen. Durch den gespeicherten Verbindungsstatus ist es möglich, die Antwortpakete einer regulären, verbindungsinitiierenden Anfrage zuzuordnen und automatisch zu erlauben. Dadurch wird die Menge der Filterregeln reduziert und Rechner in einer zu schützenden Sicherheitszone nur bei Bedarf aus dem Internet erreichbar.

Application-Layer-Firewall

Eine Application-Layer-Firewall zieht zur Klassifizierung des Datenverkehrs zusätzlich noch den Inhalt der Pakete (Payload, Applikationsschicht) heran. Damit kann z.B. unerwünschtes Active-X aus WWW-Seiten oder ein bestimmtes Kommando aus einer FTP-Verbindung herausgefiltert werden. Außerdem können mit einem integrierten Proxy direkte Ende-zu-Ende Verbindungen unterbrochen werden, so dass die interne Netzstruktur von außen nicht mehr erkennbar ist.

Network Address Translation (NAT)

Durch die Umsetzung von internen privaten auf öffentliche IP-Adressen ermöglicht die NAT-Firewall den Internet-Zugang aus internen Sicherheitszonen. Denn im Gegensatz zu öffentlichen IP-Adressen werden private IP-Adressen per Konvention nicht weltweit geroutet und ermöglichen nur die Kommunikation innerhalb des privaten Subnetzes (das gilt nur für IPv4; IPv6 kennt keine privaten IP-Adressen). Umgekehrt ist ein externer Verbindungsaufbau zu internen Rechnern ohne Zutun der Firewall nicht möglich.

3.2 LRZ-spezifische Firewall-Anforderungen

Zusammen mit einer zeitgemäßen Firewall-Technologie war bei der Beschaffung des Firewall-Systems die Erfüllung der Anforderungen, die sich aus den besonderen Rahmenbedingungen im Münchner Wissenschaftsnetz ergeben, ausschlaggebend. Das zu beschaffende System sollte möglichst reibungslos in die Struktur des MWN integrierbar sein.

Die Einrichtungen, Fakultäten und Organisationen der verschiedenen Institutionen im MWN, respektive deren Unterorganisationseinheiten, wie z.B. Lehrstühle, Institute und Verwaltung, machen den Kundenstamm des LRZ aus. Die schiere Anzahl der Kunden (57 Fakultäten bzw. Fachbereiche und damit eine geschätzte Anzahl an Unterorganisationseinheiten im mittleren dreistelligen Bereich allein bei den Hauptkunden des LRZ [2]) legt es nahe, geeignete Dienste und deren Betrieb zu zentralisieren, um den Ressourceneinsatz effizient zu gestalten. Zu diesen Diensten sollten auch Netzsicherheitsmaßnahmen wie Firewalls gezählt werden. In diesem Fall stellt der Dienstleister den funktionalen Rahmen für eine Firewall zur Verfügung und der Kunde sorgt für die individuelle Anpassung. Damit soll eine sinnvolle Teilzentralisierung erreicht und gleichwohl die erforderliche Unabhängigkeit des Kunden gewährleistet werden. Es wäre auch vorstellbar, die individuelle Anpassung auf Anforderung des Kunden als Dienstleistung anzubieten, jedoch muss dafür ein erheblicher Support-Aufwand angesetzt werden – eine sorgfältige Abwägung des Aufwands und Ertrags bei der knappen Ressource Support ist hier Pflicht. Das LRZ hat sich in diesem Fall dafür entschieden, den Support-Aufwand zu Gunsten einer größeren Gestaltungsfreiheit des Kunden zu minimieren.

Das zu beschaffende System sollte eine unabhängige Firewall-Instanz pro Kunde ermöglichen und ihm die Möglichkeit geben, diese auch autonom zu administrieren. Daneben muss es effiziente Verfahren zur zentralen Kontrolle und Administration vieler verschiedener Firewall-Instanzen geben.

Da im MWN IPv6 und IPv4 parallel betrieben werden, muss die Firewall beide Versionen unterstützen und den Verkehr auch filtern können.

3.2.1 Strategische Lokation einer Firewall

Für das LRZ gibt es drei Alternativen, wie ein Firewall-Dienst platziert werden kann: Die Aufstellung der Firewall-Komponente am zentralen Netzübergang zum Internet, jeweils an einem der Backbone-Router oder jeweils direkt beim Kunden. Im Folgenden werden die Alternativen mit Blick auf die Konsequenzen kurz diskutiert.

Firewall am zentralen Internet-Übergang

Für eine Platzierung am Internet-Übergang spricht die absolut zentrale Position, die zu Installations- und Wartungszwecken eine gute Erreichbarkeit garantiert, da sich dann alle Komponenten im LRZ-Gebäude befinden. Allerdings stellt sich in diesem Fall das Problem, eine Datenübertragungsrate von 10 Gbit/s überwachen zu müssen – eine Aufgabe, die von einer einzigen Komponente nicht so ohne Weiteres zu bewältigen ist. Alternativ kann der Datenstrom über eine Farm von Firewall-Komponenten gelenkt werden. Jedoch muss dann das Problem der Verteilung des Datenstroms auf die einzelnen Mitglieder der Farm gelöst werden – eine nicht-triviale Aufgabe im Hinblick auf Stateful Packet Inspection und Application Layer Firewall. Dazu kommt, dass der gesamte Datenstrom an dieser Stelle in die einzelnen Kundendatenströme aufgespalten und separat gefiltert werden muss. Die Konfiguration der separaten Kundenfilter muss natürlich mandantenfähig sein. Fehlkonfigurationen in einer Kundenpartition dürfen in keinem Fall das gesamte System in Mitleidenschaft ziehen. Fällt diese zentrale Komponente aus, sind alle Kunden betroffen. Ein weiterer großer Nachteil dieser Konstruktion ist die fehlende Kontrolle über den Verkehr innerhalb des MWN, der ja an dieser Stelle gar nicht vorbei kommt.

Firewall beim Backbone-Router

Eine weitere Möglichkeit ist die Aufstellung der Firewall-Komponenten an den Standorten der Backbone-Router, d.h. an jeden Standort kommt mindestens eine Firewall-Komponente. Die Anzahl der benötigten Firewall-Komponenten richtet sich dann nach der Anzahl der Backbone-Router und bleibt damit selbst bei Hochverfügbarkeit des Dienstes unterhalb von 20 (vergl. Abbildung 2). Durch die verteilte Aufstellung ergibt sich eine Lastverteilung beim zu filternden Datenstrom. Außerdem rücken die Firewall-Komponenten näher an den Kunden heran, was die Aufspaltung des Gesamtdatenstroms in Kundendatenströme vereinfacht. Wie bei der Aufstellung am Internet-Übergang gilt, dass die Konfiguration der Kundenfilter mandantenfähig sein muss und bei einer Fehlkonfiguration auf einer Kundenpartition nicht das gesamte System betroffen sein darf. Allerdings reduziert sich bei einem Ausfall der Firewall-Komponente die Zahl der betroffenen Kunden auf genau jene, die über diese Firewall-Komponente angebunden sind.

Firewall direkt beim Kunden

Natürlich können Firewalls jeweils direkt beim Kunden aufgestellt werden. Dadurch erhöht sich jedoch die Anzahl der Komponenten drastisch und verdoppelt sich nochmal, falls Ausfallsicherheit gewährleistet werden soll. Ganz offensichtlich erhöht sich damit auch die Anzahl der Hardware-Komponenten, die von einem Defekt bedroht sind. Durch die Aufstellung in den Räumlichkeiten des Kunden wird außerdem die Zugänglichkeit bei Installation und Wartung erschwert. Eine Aufspaltung

des Datenstroms erübrigt sich, da nur noch der Kundendatenstrom vorliegt. Die Mandantenfähigkeit ist in diesem Fall nicht mehr erforderlich und von einem Ausfall einer Firewall-Komponente ist nur noch genau ein Kunde betroffen.

Daraus ergibt sich für das LRZ folgende Priorisierung der Aufstellorte für mandantenfähige Firewall-Komponenten:

1. Backbone-Router
2. Zentraler Internet-Übergang
3. Kunde

3.2.2 Auswahlentscheidung: Firewall Service Module

Für eine Realisierung des Firewall-Dienstes wurde der Einsatz folgender Produkte in Erwägung gezogen: Netscreen-5000 Serie der Firma Juniper (Einsatzort: zentraler Internet-Übergang), Firewall Service Module (FWSM) der Firma Cisco (Einsatzort: Backbone-Router) und Netfence der Firma Phion (Einsatzort: Kunde)). Bei der Produktauswahl zeigte sich, dass das FWSM der Firma Cisco das Anforderungsprofil des LRZ am ehesten erfüllt. Pro FWSM lassen sich virtuelle Firewall-Instanzen definieren, die sich voneinander unabhängig und zentral kontrolliert konfigurieren lassen. Was die Funktionalität angeht, werden alle oben aufgeführten Firewall-Technologien unterstützt. Zusätzlich ist es, und zwar mit Einschränkungen bei den Administrationsschnittstellen, möglich, IPv6-Verkehr zu filtern.

Das FWSM, als Erweiterungsmodul für die im MWN eingesetzten Router der Firma Cisco, hat zudem den Vorteil, dass keine zusätzlichen externen Netzkomponenten aufgestellt werden müssen. Damit wird der Aufwand für die Integration der Firewall-Komponenten in die bestehende Infrastruktur stark reduziert. Sowohl die angebotenen Administrationsschittstellen als auch die Integrationslogik sind größtenteils bereits bekannt und vertraut. Für eine zukünftige Erweiterung des Dienstes ist zudem von Bedeutung, dass pro Router mehrere FWSMs eingesetzt werden können, die dann zusammen den Dienst hochverfügbar machen.

3.3 ÖkonomischeAspekte - Total Cost of Ownership (TCO)

Bei der Auswahl neuer Komponenten und der Einführung eines neuen Dienstes müssen natürlich auch ökonomische Aspekte betrachtet werden. Dabei sind die Gesamtkosten (Total Cost of Ownership), die durch die Beschaffung, die Installation, den Betrieb und die Wartung und ggf. durch den Abbau des neuen Dienstes anfallen, zu berücksichtigen. Entscheidungsrelevant für das LRZ ist eine Gesamtbetrachtung sowohl der TCO des Kunden als auch der des LRZ.

3.3.1 TCO des Kunden

Einrichtungen und Organisationen im MWN sehen sich häufig mit der Situation konfrontiert, dass Rechner aus ihrem Bereich kompromittiert und in der Folge missbraucht werden. Die Wahrscheinlichkeit eines erfolgreichen Angriffs steigt erheblich, wenn keine netzseitigen Schutzmechanismen vorhanden sind. Wird ein kompromittierter Rechner entdeckt, zieht das unmittelbar personellen Aufwand für Schadensermittlung, Schwachstellensuche und eventuell Neuinstallation des betroffenen Rechners nach sich. Im schlimmsten Fall sind bei dem Angriff auch wichtige Daten verloren gegangen. Gingen von dem kompromittierten System außerdem weitere Angriffe aus und wurden diese auf den Zielsystemen bemerkt, muss auch noch eine Flut von Beschwerde-E-Mails bearbeitet werden. Spätestens an diesem Punkt wird über Gegenmaßnahmen, insbesondere den Einsatz einer Firewall-Komponente, nachgedacht.

Doch nicht jede Einrichtung oder Organisation verfügt über die nötigen Geldmittel, um eine Firewall-Komponente anzuschaffen. Und selbst für jene, die mit ausreichend finanziellen Mitteln ausgestattet sind, bedeutet die Anschaffung einer Firewall-Komponente zusätzlich zum personellen Aufwand für den Betrieb meistens auch noch finanziellen Aufwand für die regelmäßige Wartung (Wartungsvertrag). Wird ein kostengünstiges nicht-kommerzielles Produkt angeschafft, handelt man sich außerdem noch das Problem der Knowhow-Tradierung ein – ein nicht zu unterschätzendes Problem, wenn man die hohe Personalfluktuation im wissenschaftlichen Umfeld berücksichtigt.

Hier zeigt sich der Vorteil des Firewall-Dienstes, den das LRZ seinen Kunden anbietet. Der Kunde wird davon befreit, eine Produktevaluation durchzuführen, und muss keine teure Firewall-Komponente anschaffen. Er muss sich keine Gedanken über Installation und Wartung der Software bzw. Hardware machen. Für den Kunden bleibt lediglich der personelle Aufwand für den Betrieb seiner Firewall-Komponente übrig, d.h. die Konfiguration auf seine individuellen Bedürfnisse abzustellen und die korrekte Funktion anhand der Protokolldaten zu verifizieren.

3.3.2 TCO des Leibniz-Rechenzentrums

Zieht man das Wesen von Beschaffung, Installation und Wartung einer Firewall-Komponente in Betracht, wird klar, dass dieser Aufwand nicht von jeder Einrichtung und Organisation im MWN einzeln erbracht werden sollte. Wenn also diese Teilbereiche vom LRZ zentral für das MWN übernommen werden, bedeutet dies eine unmittelbare Ressourcenersparnis für das MWN insgesamt.

Durch die Ausführung der Firewall-Hardware als Erweiterungsmodul für die Backbone-Router, werden die Integrationsverluste der neuen Komponenten reduziert. Der Support-Aufwand pro Kunde wird dadurch beschränkt, dass der Betrieb, d.h. individuelle Konfiguration und Auswertung der Protokolldaten, dem Kunden überlassen wird.

Ein großer Vorteil sowohl für das LRZ als auch für die Kunden erwächst daraus, dass das LRZ diese Art von Firewalls auch für eigene Netze verwendet – durch den wechselseitigen Knowhow-Transfer wird ein deutlicher Synergie-Effekt erwartet und ist auch bereits spürbar.

4 Realisierung

Cisco bietet die Firewall-Service-Module (FWSM) neben seiner PIX-Firewall und der ASA-Plattform als Firewall-System an. Es handelt es sich um Einschübe („Blades“) für die 6500er- und 7600er-Serie der Catalyst-Router, die durch einen hohen Durchsatz (bis zu 6 GBit/s pro Blade) gekennzeichnet sind und sich gut in die MWN-Infrastruktur integrieren lassen (vgl. Abbildung 3). Kundennetze lassen sich einfach auf die FWSM aufschalten und ein autonomes Management durch die Kunden ist realisierbar.

Abbildung 3: Firewall-Service-Modul im Catalyst-6509-Router

Ein Firewall-Service-Modul ist genau genommen ein eigenständiger Rechner im Catalyst-Router. Als Managementplattform kommen zwei Pentium-3-Prozessoren mit je 1 GHz und 1GB-RAM und ein 128 MB Flashspeicher für Betriebssystem und Konfigurationen zum Einsatz.

4.1 Strategische Position der Blades

Die Firewall-Service-Module mit den virtuellen Instanzen für Kunden sind im MWN in die Core-Router im Routing-Backbone sowie an wichtigen Edge-Distribution-Routern integriert. Ziel dieser Strategie ist es, die Firewalls zwar zentral, aber möglichst nahe am Kunden zu platzieren. Das hat entscheidende Vorteile (vgl. Abschnitt 3.2.1).

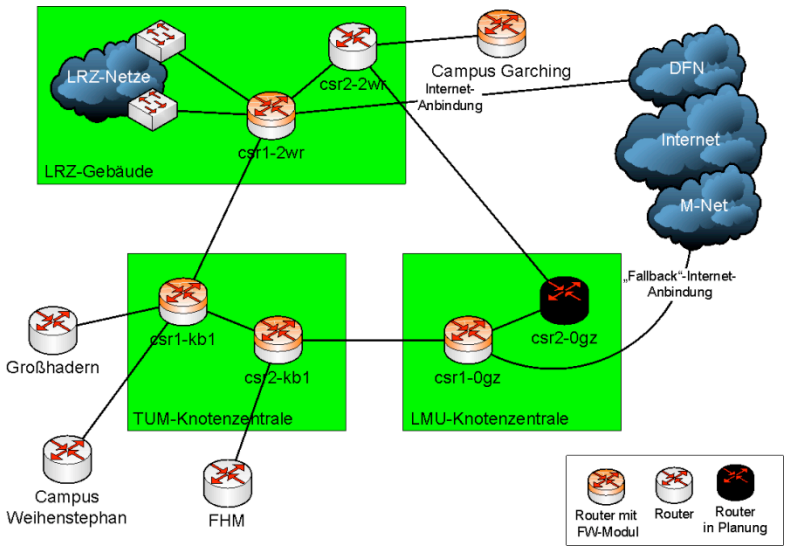

Abbildung 4: MWN mit Core- und Distribution-Routern mit und ohne Firewall-Service-Modul

Zur Zeit sind im MWN fünf Firewall-Service-Module im Einsatz. Sie sind in die zentralen Router im MWN-Backbone sowie in einem Campus-Distribution-Router eingebaut. Somit wird eine optimale Verteilung im MWN erreicht, um Kunden zentral, aber logisch vor Ort bedienen zu können.

Auf einem Firewall-Service-Modul können bis zu 250 virtuelle Firewalls parallel aktiviert und unabhängig voneinander betrieben werden. Für den Administrator einer Firewall-Instanz sind die anderen Instanzen auf demselben Firewall-Service-Modul nicht sichtbar und es besteht auch keine gegenseitige Zugriffsmöglichkeit. Für den Kunden entsteht der Eindruck eine „eigene“ Firewall zu besitzen.

4.2 Kundenanbindung

Eine Firewall ist der einzige Zugangspunkt in das Kundennetz und sollte möglichst „nahe“ an den zu schützenden Systemen plaziert werden. Da die Firewalls-Service-Module in die Backbone-Router eingebaut sind, liegen zwischen der Firewall und dem Kundennetz unter Umständen sehr viele Netzkomponenten.

Um die Firewall logisch vor dem Kundennetz zu plazieren, setzt das LRZ im MWN virtuelle lokale Netze, sog. VLANs, ein. Ein VLAN ist im IEEE Standard 802.1Q [8] definiert und soll LAN-Strukturen über mehrere Schicht-2-Komponenten hinweg ermöglichen. Ein VLAN bildet eine Broadcast-Domäne über Komponenten hinweg. Dazu wird der Ethernet-Frame um ein VLAN-ID-Feld erweitert, in dem die Nummer des VLANs kodiert wird. Damit ist es möglich Kundensubnetze, die sich über mehrere Switche und Gebäude erstrecken, zu einem logischen Subnetz zusammenfassen zu können. VLANs werden bisher schon im MWN eingesetzt. Daher ist es dann sehr einfach, die Kundensubnetze zum Firewall-Service-Modul zu bringen.

Das VLAN des Kunden wird bei einer virtuellen Firewall als internes VLAN bezeichnet. Es handelt sich dabei um die zu schützende Ressource. Als Zugangsnetz zur Firewall von außen dient das sog. externe VLAN, das für diesen Zweck neu eingerichtet wird. Desweiteren können an der virtuellen Firewall noch weitere Kunden-VLANs (vgl. Abschnitt 3.1.2), eingerichtet werden.

Ist ein Kunde an einer virtuellen Firewall interessiert, müssen zuerst einige Voraussetzungen geklärt werden, die der Kunde erfüllen muss. Er benötigt zwingend Kenntnisse zum Administrieren einer Firewall und eine gute bis sehr gute Kenntnis seiner Netzinfrastruktur. Das beinhaltet nicht nur seine Verkabelung vor Ort, sondern auch Kenntnisse der bisher verwendeten VLANs und der IP-Subnetze. Bei der Verkabelung ist darauf zu achten, dass es sich um eine strukturierte Verkabelung handelt, so dass VLANs verwendet werden können. In einigen wenigen Bereichen des MWN wird noch Koaxial-Verkabelung einsetzt. Diese Netze sind nicht VLAN-tauglich und können daher auch nicht über eine virtuelle Firewall abgesichert werden. Außerdem ist darauf zu achten, dass pro VLAN nur ein IP-Subnetz verwendet wird. Mehrere IP-Subnetze in einem VLAN („Multinetting“) sind mit den Cisco Firewall-Service-Modulen technisch nicht möglich.

Damit sich der Kunde mit der virtuellen Firewall und deren Konfiguration vertraut machen kann, wird ihm vom LRZ zuerst eine sog. „Schnupper-Firewall“ angeboten. Dabei handelt es sich um eine virtuelle Firewall, die noch nicht aktiviert ist. Der Kunde kann die Firewall zwar administrieren, seine Regeln haben aber noch keine Wirkung, da die Kundensubnetze noch nicht auf das Firewall-Modul im Router geschaltet wurden. Erst wenn der Kunde es wünscht, wird die Firewall „scharf geschaltet“ und die VLANs damit am Router über das Firewall-Modul geleitet.

Das LRZ setzt Kunden-Firewalls standardmäßig im Routing-Modus auf, wenn der Kunden nicht explizit eine Bridging-Firewall (auch transparente Firewall genannt) benötigt. Gründe hierfür sind vor allem Einschränkungen durch die Hardware. Bei einer Bridging-Firewall müssen sog. Bridge-Groups eingerichtet werden, die internes und externes VLAN zusammenfassen. Vom FWSM werden aber

maximal acht Bridge-Groups pro Modul unterstützt, was bei einer größeren Kundenanzahl auf einem Modul zu Engpässen führen würde. Außerdem wird im transparenten Modus IPv6, das im MWN genutzt wird, nicht unterstützt.

4.3 Management

Die Administration und das Management der Firewall-Infrastruktur muss unter zwei Gesichtspunkten betrachtet werden:

- Administration der Firewall-Service-Modul-Infrastruktur durch das LRZ (Infrastruktur-Management)
- Administration der virtuellen Firewall-Instanzen durch die Kunden selbst (Firewall-Management)

4.3.1 Infrastruktur-Management

Das LRZ betreut die MWN-weite Firewall-Infrastruktur. Das beinhaltet das Aufstellen, Konfigurieren und Pflegen der Firewall-Service-Module sowie die Sicherung der verschiedenen Konfigurationen der Kunden. Dabei werden drei verschiedene Werkzeuge eingesetzt:

- Cisco Security Manager [9](globale Konfiguration, LRZ-Administratoren)
- Adaptive Security Device Manager [10] (lokale Konfiguration im jeweiligen Module, Kunden und LRZ-Administratoren)
- Rancid [11] (zentrales Backup der Kunden-Konfigurationen)

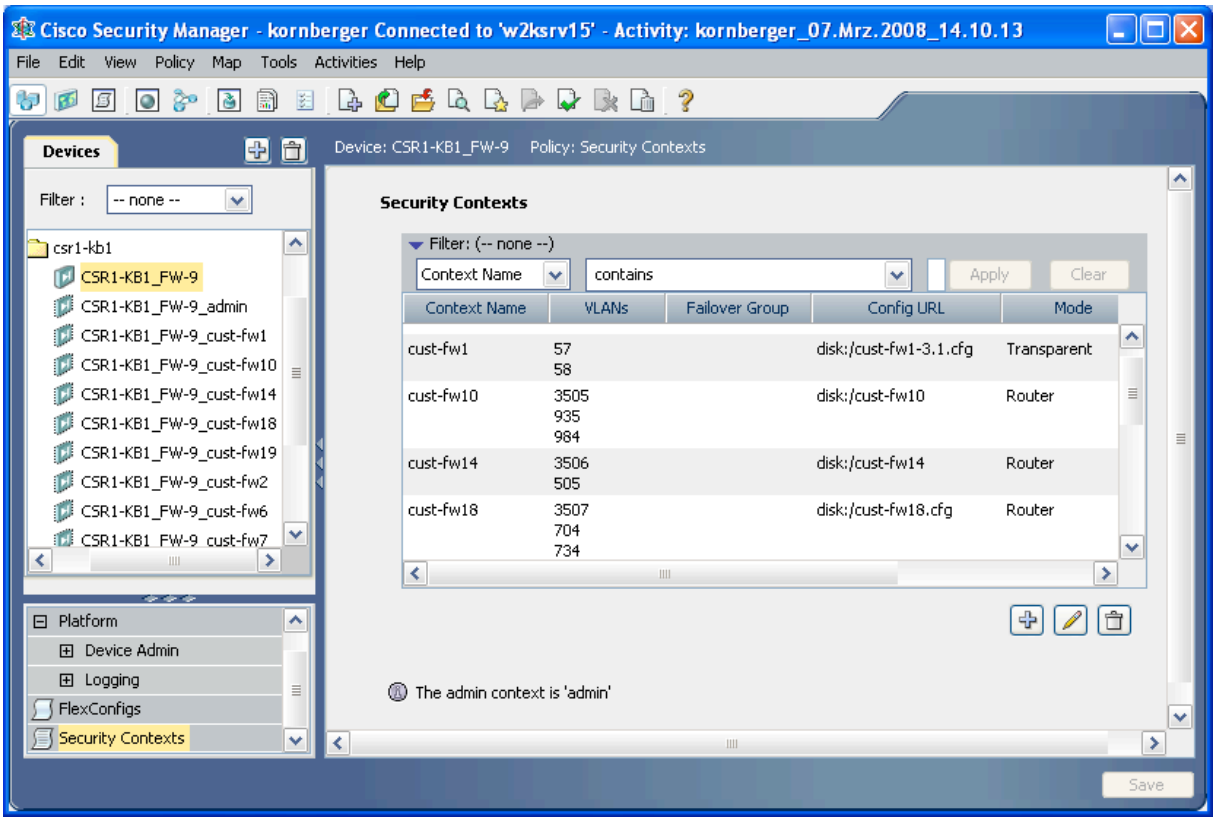

Abbildung 5: Cisco Security Manager (CSM): Liste der virtuellen Firewall-Instanzen eines Firewall-Service-Moduls

Als zentrales Management-System – nur für LRZ-Administratoren – wird der „Cisco Security Manager“ (CSM) [9]eingesetzt. Das LRZ nutzt den CSM, um neue virtuelle Firewall-Instanzen zu erstellen. Diese werden vorkonfiguriert, d.h. die Kunden-VLANs sowie das Transport-VLAN (nur bei

einer Routing-Firewall) werden eingerichtet. Desweiteren werden vom LRZ als sinnvoll erachtete Default-Einstellungen angewendet. So werden z.B. die Kunden-Accounts eingerichtet oder bestimmte Vorgaben bezüglich der Logging-Filter gemacht, so dass möglichst viele Informationen ins Log geschrieben werden, was für den Kunden zu Beginn sehr hilfreich bei der Fehleranalyse sein kann. Der Nutzer kann einige dieser Einstellungen ändern. Aber eine aus Sicherheitsgründen sehr restriktive Rechtevergabe verhindert, dass der Nutzer alle Parameter ändern kann. Beim Cisco-Firewall-Service-Modul benötigt das Ändern mancher Parameter (z.B. das Ändern des Passwortes des Kunden) Administratorrechte. Hätte der Benutzer diese Rechte, könnte er auch Parameter ändern, die unter Umständen auch andere Firewall-Instanzen betreffen oder auf diese zugreifen.

Sind die Kunden-Firewalls fertig vorkonfiguriert, werden sie „ausgerollt“, d.h. auf dem entsprechenden Firewall-Service-Modul im Router nahe am Kunden wird eine neue Instanz mit den voreingestellten Parametern erzeugt. Nachdem am Router dann das externe VLAN eingerichtet wurde, ist die „Schnupper-Firewall“ einsatzbereit.

Jedes Firewall-Service-Modul hat eine Admin-Instanz, über die die Administratoren des LRZs direkt auf das Modul und seine virtuellen Firewall-Instanzen zugreifen können. Dies geschieht über den Adaptive Security Device Manager“ (ASDM) [10]. So können Veränderungen an den Kunden-Firewalls konfiguriert werden. Das ist in der Praxis sehr viel effizienter als Änderungen über den CSM durchzuführen, da dort die aktuellen Konfigurationen nicht vorliegen und erst vom Firewall-Service-Modul heruntergeladen und nach einer Änderung wieder hochgeladen werden müssen. Prinzipiell können über die Admin-Instanz auch neue Firewall-Instanzen angelegt werden. Das LRZ nutzt diese Möglichkeit aus organisatorischen Gründen nicht und verwendet ausschließlich den CSM zum Anlegen neuer Kunden-Firewalls. Nur so können die oben genannten Default-Einstellungen mit wenigen Schritten – ohne alle manuell durchzuführen – auf die neue Firewall-Instanz angewendet werden. Über die Admin-Instanz können sich die LRZ-Administratoren auch live auf die Kunden-Instanz im jeweiligen Firewall-Service-Modul einloggen und mit dem Kunden Probleme analysieren sowie Hilfestellung und Tipps geben.

Zur automatischen Sicherung der Konfigurationen der Kunden-Firewalls wird das Open-Source-Werkzeug Rancid [11]eingesetzt, da der CSM diese Funktionalität nicht bietet. Rancid sichert die Daten der Kunden jede Nacht in ein Subversion-Repository. Hat der Kunde ein Problem und wünscht das Wiederherstellen einer gesicherten Version („Restore“), genügt eine Email oder ein Anruf bei den LRZ-Firewall-Administratoren. Im CSM wird eine Datenbank mit den Konfigurationen sämtlicher virtueller Firewalls im MWN - aus allen Routern - im Auslieferungszustand gepflegt. Diese kann bisher nur manuell auf den aktuellen Stand aller virtuellen Firewall-Instanzen gebracht werden.

4.3.2 Firewall-Management

Aufgabe des Kunden ist es nun, „seine“ Firewall einzurichten. Am wichtigsten sind dabei die Firewallregeln. Sie bestimmen, welche Verkehrsbeziehungen erlaubt sind und welche verhindert werden. Dabei gilt die Default-Regel, dass alles, was nicht explizit erlaubt wird, verboten ist. Neben dem Konfigurieren der Firewall ist die zweite wichtige Aufgabe des Kunden das Auditing der Firewall-Regeln. Dazu ist es erforderlich, dass der Kunde regelmäßig die Logs seiner Firewall analysiert. So kann er testen, ob alles richtig konfiguriert ist, und eventuelle Angriffsversuche analysieren. Das LRZ empfiehlt allen Kunden hierzu einen eigenen externen Syslog-Server im Kunden-Subnetz aufzusetzen. Die virtuelle Firewall schickt alle Log-Meldungen dann an diesen Syslog-Server. Somit haben die Kunden ihre Logs vor Ort und können diese auch über längere Zeiträume hinweg

analysieren. Im Firewall-Service-Modul werden zwar auch Logs gespeichert, aber die interne Speicherkapzität pro Firewall-Instanz ist sehr gering – ca. 2000 Log-Zeilen, diese reichen je nach Aktivität keine zwei Minuten!

Kunden können ihre virtuelle Firewall auf zwei Arten verwalten: per Webinterface oder mit SSH.

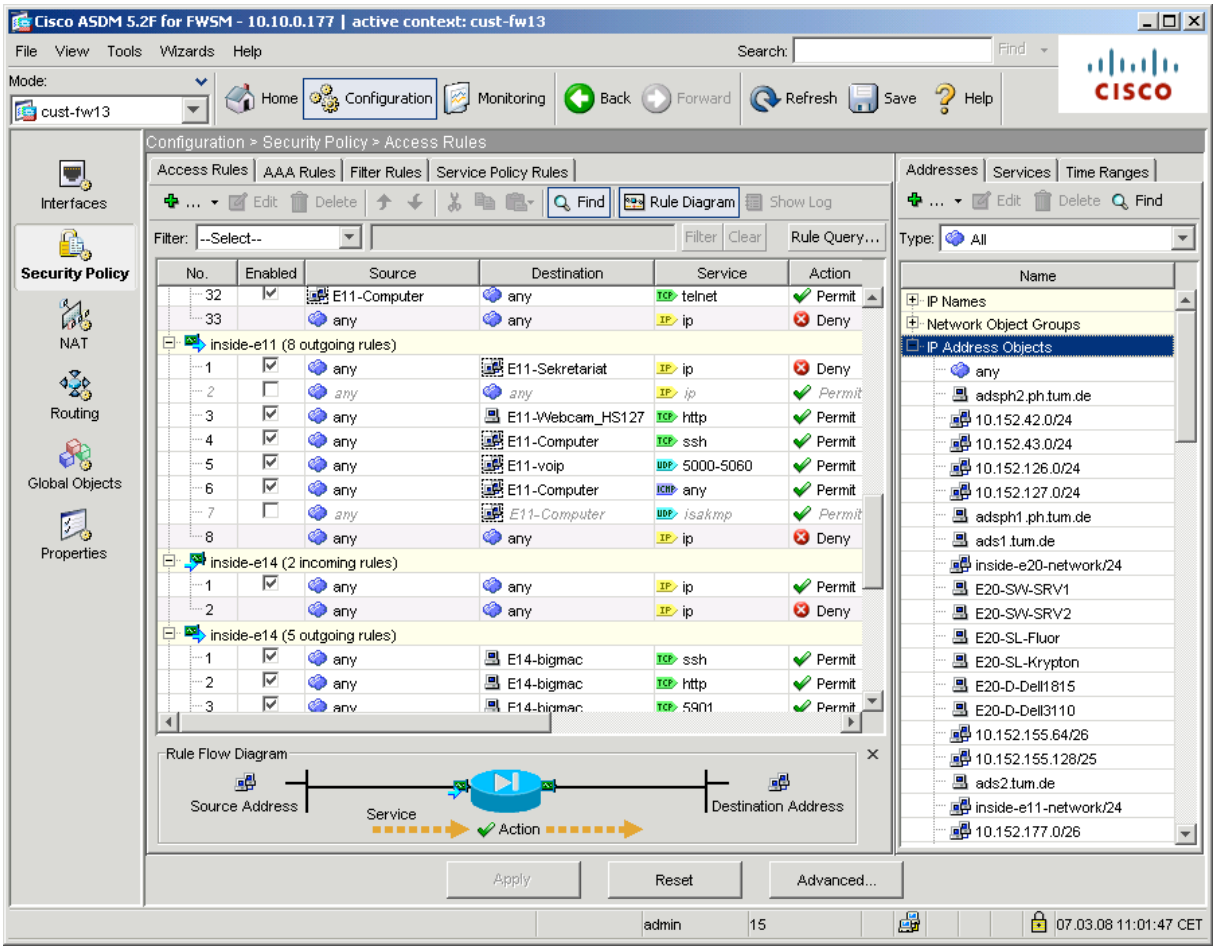

Abbildung 6: ADSM-Webinterface: Konfiguration der Firewall-Regeln

Über das Webinterface wird das Java-Applet des ASDM geladen, welches vom Browser (vgl. Abbildung 6) ausgeführt wird. Das LRZ empfiehlt seinen Kunden diese Oberfläche zu nutzen, da man zur Verwendung des SSH-Zugangs tiefergehende Kenntnisse im Umgang mit Cisco-IOS benötigt. Über beide Möglichkeiten lässt sich die virtuelle Firewall-Instanz konfigurieren. Mit dem ASDM kann der Kunde bequem seine Firewallregeln pflegen und über eingebaute Monitoring-Funktionen einfaches Trouble-Shooting selbst vornehmen.

5 Betriebserfahrungen, Zusammenfassung und Ausblick

Das LRZ begann im Sommer 2007 erste Erfahrungen mit wenigen ausgewählten Pilotkunden zu sammeln. Seit Dezember 2007 läuft die zweite Pilotphase, in der alle interessierten Institute im MWN – sofern realisierbar – eine virtuelle Firewall erhalten können. Derzeit betreut das LRZ bisher die ersten 30 Kunden erfolgreich beim Betrieb einer virtuellen Firewall.

Dieses Konzept findet im MWN großen Zuspruch und wird von Lehrstühlen gerne angenommen. In einigen Fakultäten haben sich auch mehrere Lehrstühle zusammengeschlossen und betreiben zusammen eine virtuelle Firewall, um den administrativen Aufwand zu minimieren.

5.1 Auffälligkeiten / Probleme

Beim bisherigen Betrieb sind aber auch einige Punkte aufgefallen, die verbessert werden sollten. Das betrifft sowohl technische als auch administrative Gebiete. Die Firewall-Service-Module können zwar IPv6-Pakete filtern, aber nur im Routing-Modus. Im transparenten Modus („bridging firewall“) ist bisher kein IPv6 möglich. Außerdem verfügt der ASDM noch nicht über die Möglichkeit, Regeln und Parameter für IPv6 zu konfigurieren. Dieses ist zur Zeit (Softwareversion 5.2f) ausschließlich über Kommandozeile per SSH möglich. Weiterhin ist es zur Zeit nur eingeschränkt möglich, die Module per Simple-Network-Management-Protokoll (SNMP) abzufragen, um z.B. die ARP-Tabelle oder eine Liste der verwendeten VLANs zu erhalten. Beides ist bei einem Cisco-Router Stand der Technik. Stattdessen liefert das Modul per SNMP nur statistische Daten über die einzelnen Interfaces sowie einige technische Daten zum Modul selbst.

Im administrativen Bereich bereitet die Rechteverwaltung Probleme, da es kein ausreichend feingranular abgestuftes Rechtekonzept gibt. Somit entfallen bestimmte Self-Services des Kunden (z.B. das Ändern des Benutzerpasswortes) und der LRZ-Administrator muss hier tätig werden. Aus Sicherheitsgründen darf der Kunde auch keine vollen Administratorrechte bekommen, da er sonst auf andere Kunden-Instanzen zugreifen könnte. Dieser Umstand resultierte darin, dass das LRZ in sehr zeitaufwendiger Arbeit ein Rechtekonzept für Kunden erarbeiten musste, in dem praktisch jedes einzelne Kommando festgelegt werden muss, welches die Kunden ausführen dürfen.

Ein weiteres Problem tritt beim Management mittels ASDM auf, der eigentlich von alle LRZ-Kunden verwendet wird. ASDM stellt nicht alle Details in der Übersicht der Firewall-Filterregeln dar. Erst beim genaueren Ansehen einer Regel werden alle Details ersichtlich. Das hat in der Vergangenheit schon zu Missverständnissen und somit zu einer sehr zeitintensiven Fehlersuche geführt.

5.2 Performanz

Die zurzeit aktiven virtuellen Firewalls sind im MWN fast gleichmäßig über die fünf Firewall-Service-Module verteilt. Aber keines der Module ist hinsichtlich Datendurchsatz und Anzahl der möglichen Instanzen ausgelastet. Ab Herbst 2008 wird das LRZ voraussichtlich virtualisierte Server als neue Dienstleistung im MWN anbieten. Jeder dieser virtuellen Server könnte von einer virtuellen Firewall geschützt werden, sodass schnell eine dreistellige Anzahl virtueller Firewalls erreicht werden könnte. Von den jetzigen Performancedaten ausgehend sollte dies kein Problem darstellen. Verlässliche Aussagen sind aber derzeit noch nicht möglich. Im Rahmen studentischer Arbeiten soll die tatsächliche Performanz, vor allem der maximale Datendurchsatz eines Firewall-Service-Moduls evaluiert werden.

Die bisherige Erfahrung zeigt, dass eine Anzahl von über 100 virtuellen Firewalls administrativ gut handhabbar sein sollte. Der Zeitaufwand, eine Schnupper-Firewall einzurichten, beträgt ca. zwei bis vier Arbeitsstunden. Zuerst müssen die Rahmenbedingungen mit dem Kunden geklärt und seine Netzstruktur in der LRZ-Dokumentation recherchiert werden. Danach wird die neue virtuelle Firewall

im CSM konfiguriert und ausgerollt. Nun wird der Kunde telefonisch in die Bedienung des ASDM und die Konfiguration der virtuellen Firewall eingeführt. Diese Beratung variiert in der Praxis stark, je nach Kenntnisstand des Kunden. Soll die Schnupper-Firewall dann nach Terminabsprache mit dem Kunden in den produktiven Betrieb übergehen, so ist ca. eine weitere Arbeitsstunde notwendig, um die entsprechenden Änderungen am Router und ggf. an Switches vorzunehmen. Im weiteren Verlauf nimmt die Zeit für die Kundenbetreuung im Allgemeinen ab, sodass als Fazit festzustellen ist, dass der größte Teil der Arbeitszeit auf die initiale Einrichtung der virtuellen Firewall verwendet wird. Einzig das Trouble-Shooting kann noch einen größeren Aufwand für den LRZ-Administrator bedeuten, wobei dieser aber je nach Fall sehr stark variiert. Auf administrativer Seite muss außerdem noch kontinuierlich ein geringer Arbeitsaufwand investiert werden, um die Hard- und Software der Firewall-Service-Module zu warten.

Insgesamt bleibt festzustellen, dass die virtuelle Firewall sowohl aus Sicht der Kunden als auch aus Sicht der Betreiber ein voller Erfolg ist. Die Gesamtkosten für den Betrieb einer Firewall durch den Kunden konnten deutlich gesenkt werden. Die Nachfrage durch die Kunden ist entsprechend hoch. Gesamtwirtschaftlich betrachtet sind die für die virtuellen Firewalls im MWN anfallenden Kosten deutlich geringer als wenn die gleiche Anzahl an dedizierten Firewalls betrieben würde. Insgesamt kann mit diesem Konzept im MWN sehr einfach eine technologisch hochwertige Firewall realisiert und damit sowohl das Sicherheitsniveau des einzelnen Kunden als auch das des gesamten MWN erhöht werden. Der Administrationsaufwand für einen effizienten Betrieb von verhältnismäßig vielen Firewall-Instanzen ist auch mit den beschränkten Personalressourcen des LRZs zu bewältigen.

6 Literaturverzeichnis

1. **Leibniz-Rechenzentrum .** *Jahresbericht 2007.* Garching b. München : Leibniz-Rechenzentrum, 2008. http://www.lrz-muenchen.de/wir/berichte/Jber2007.pdf.

2. **Leibniz-Rechenzentrum.** *Das Münchner Wissenschaftsnetz (MWN) - Konzepte, Dienste, Infrastrukturen, Management.* München : Leibniz-Rechenzentrum, 2006. http://www.lrz-muenchen.de/services/netz/mwn-netzkonzept/mwn-netzkonzept.pdf.

3. **Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, and Deborah Russell.** *Building Internet Firewalls.* s.l. : O'Reilly Media, Inc., 2000.

4. **Bundesamt für Sicherheit in der Informationstechnik.** B 3.301 Sicherheitsgateway (Firewall). *IT-Grundschutzkataloge.* [Online] 2005. http://www.bsi.bund.de/gshb/deutsch/baust/b03301.htm.

5. **Stephen Northcutt, Karen Frederick, Scott Winters, Lenny Zeltser, Ronald W. Ritchey.** *Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems (Inside).* s.l. : Sams, 2005.

6. **Bundesamt für Sicherheit in der Informationstechnik.** M 2.70 Entwicklung eines Konzepts für Sicherheitsgateways. *IT-Grundschutz-Kataloge.* [Online] 2005. http://www.bsi.bund.de/gshb/deutsch/m/m02070.htm.

7. **Bundesamt für Sicherheit in der Informationstechnik .** M 2.71 Festlegung einer Policy für ein Sicherheitsgateway. *IT-Grundschutzkataloge.* [Online] 2005. http://www.bsi.bund.de/gshb/deutsch/m/m02071.htm.

8. **Institute of Electrical and Electronics Engineers (IEEE).** *Virtual Bridged Local Area Networks (IEEE Std 802.1Q).* New York : IEEE, 2006.

9. **Cisco Systems.** Cisco Security Manager 3.1 User Guide. [Online] 2007. http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.1/user/guide/ug31.html.

10. **Cisco Systems .** Adaptive Security Device Manager 5.2 User Guide. [Online] 2007. http://www.cisco.com/en/US/docs/security/asa/asa72/asdm52/user/guide/user.html.

11. **Shrubbery Networks.** RANCID - Really Awesome New Cisco conflg Differ. [Online] Shrubbery Networks, 2006. http://www.shrubbery.net/rancid/ .