

Policy-basiertes Management für Netzsicherheit mit Flexibilität

Matthias Müller, Willi Fries, Reinhard Strebler, Hannes Hartenstein

Rechenzentrum der Universität Karlsruhe (TH)
76128 Karlsruhe
matthias.mueller@rz.uni-karlsruhe.de
wilhelm.fries@rz.uni-karlsruhe.de
reinhard.strebler@rz.uni-karlsruhe.de
hannes.hartenstein@rz.uni-karlsruhe.de

Abstract: In diesem Beitrag wird die Konzeption und Umsetzung eines Policy-basierten Managementverfahrens für die Einrichtung von Filterregeln im Campusnetz der Universität Karlsruhe vorgestellt. Hierbei war das Ziel, eine Sicherheitsstufe zwischen dem einfachen „Verstecken“ durch Verwendung privater IP-Adressen einerseits („Stufe 1“) und einer aufwendigen Firewall-Lösung andererseits („Stufe 3“) anzubieten. Dieses so genannte „Stufe 2“-Sicherheitsniveau bietet für eine große Mehrheit der Universitätseinrichtungen und Teilnetze eine ausreichende Netzsicherheit bei einem deutlichen Gewinn an Flexibilität durch dezentrale Administrierbarkeit im Vergleich zu einer „Stufe 3“ Lösung. Wir beschreiben in diesem Beitrag die grundsätzlichen Überlegungen zu den Anforderungen, die Architektur hinsichtlich der Einbettung in das Netzwerk sowie die Benutzeroberfläche, das XML-basierte Polycyschema und die Policy-Übersetzung in eine „Access Control List“ (ACL) und in IPTables. Erste Erfahrungen mit der vorgeschlagenen und umgesetzten Lösung im produktiven Einsatz bestätigen die Leistungsfähigkeit und den Flexibilitätsgewinn.

1 Einleitung

Ziel eines IT-Sicherheitsprozesses im Hochschulbereich ist – wie bei Unternehmensnetzen – das Erreichen und Aufrechterhalten eines „angemessenen“ Sicherheitsniveaus. Der Begriff der „Angemessenheit“ spiegelt wider, dass maximale Sicherheit ohne Berücksichtigung des Risikos und der „Tradeoffs“, etwa im Bezug auf Kosten und Aufwand, nicht das Ziel der Sicherheitsbemühungen sein kann. In einem Hochschulnetz mit seiner Vielzahl an eingebundenen Einrichtungen mit unterschiedlichen Anforderungen gibt es jedoch kein einfaches gemeinsames „Angemessenheitsniveau“. Unterschiedliche Einrichtungen oder Teilnetze haben zum einen unterschiedliche Sicherheitsanforderungen, zum anderen treten auch Unterschiede zu Tage bei der Frage, welchen Preis man für Sicherheit zu zahlen gewillt ist. In diesem Sinne gibt es auch keinen einfachen Netzperimeter zwischen Hochschulnetz und dem Rest der Welt: Teilnetze müssen auch gegeneinander geschützt werden.

Hinsichtlich präventiver Maßnahmen im Bereich der Netzsicherheit reicht das Spektrum von einem gänzlich offenen Zugang über die Verwendung privater IP-Adressen bis hin zum Einsatz von zertifizierten Firewalls. An der Universität Karlsruhe wurden bislang etwa die folgenden Sicherheitsstufen angeboten:

- Stufe 0. Hier erfolgt die Kontrolle des Netzwerkverkehrs nur über Standardfilterlisten auf dem Uplinkrouter. Die Endsysteme verfügen über öffentliche IP-Adressen. Zuerst wurde hier eine Blacklist eingesetzt, die allerdings auf Grund der erhöhten Bedrohung aus dem Internet Ende 1999 durch eine Whitelist ersetzt wurde. Individuelle Änderungen an den Filtern sind allerdings nur durch den zentralen Netzbetreiber möglich und sorgen bei einer hohen Anzahl von Änderungen für einen hohen administrativen Aufwand.
- Stufe 1. Hier werden private IP-Adressen für die Endgeräte verwendet, es ist also keine direkte Ende-zu-Ende Kommunikation in das Internet möglich. Die Kommunikation dieser Systeme wird über zentrale Applikations-Gateways und dedizierte NAT-Router ermöglicht, die den reinen Client-Systemen über Proxyfunktionalität und Network Address Port Translation (NAPT) die Kommunikation in das Internet erlauben. Für Server-Systeme, die aus dem Internet erreichbar sein müssen, wird Network Address Translation (NAT) eingesetzt. Der Betreiber der Systeme kann hierbei über ein Webfrontend Filter für die Serversysteme selber definieren und so gezielt einzelne Dienste nach Außen anbieten. Eine gezielte Freigabe von Diensten nur für bestimmte IP-Subnetze ist hier nicht möglich. Die definierten Regeln werden zweimal täglich auf die dedizierten NAT-Router übertragen, ohne dass ein manueller Eingriff nötig ist.
- Stufe 3. Einzelne Einrichtung der Universität benötigen individuellere Maßnahmen zum Schutz des internen Netzes, z.B. muss auch der Verkehr zur Universität hin kontrolliert werden können. Für diese Anforderungen betreut das Rechenzentrum dedizierte Firewall-Systeme, die zwischen dem Netz der Einrichtung und dem Universitätsnetzwerk platziert sind. Die Administration dieser Firewallssysteme erfolgt durch die Netzwerkabteilung und erzeugt hier einen hohen administrativen Aufwand. Darüber hinaus ist bei diesem Konzept ein dediziertes Firewall-System pro Einrichtung erforderlich, wodurch höhere Kosten entstehen.

Letztere „Stufe 3“ bietet zwar in Bezug auf Filterung einen größtmöglichen Schutz, aber fordert auch ihren Preis: was für den Betreiber als Aufwand (und somit als Kosten) sichtbar wird, ist für den Nutzer in Form von Wartezeiten und fehlender Flexibilität spürbar (und somit entstehen auch auf Nutzerseite Kosten). Die „Stufe 1“-Lösung bietet deutlich mehr Administrierbarkeit durch den Anwender und damit auch Flexibilität, ist allerdings funktional häufig unzureichend, da ein feinere Aufteilung hinsichtlich der Freigabe bislang nicht möglich war. In diesem Beitrag stellen wir nun Konzeption und Umsetzung eines Policy-basierten Managements für die Einrichtung von Filterregeln im Campusnetz der Universität Karlsruhe vor: diese Konzeption beinhaltet eine „Stufe 2“-Sicherheitslösung sowie eine Integrationskonzept („Netzsicherheitskonzept“) hinsichtlich der Administrierbarkeit der verschiedenen Stufen. Das Ziel dieser „Sicherheitsstufe

2“, die in diesem Beitrag vorgestellt wird, ist es, ein Sicherheitsniveau zu erreichen, das zwischen dem reinen „Verstecken“ durch Verwendung privater IP-Adressen einerseits und einer aufwendigen Firewall-Lösung andererseits liegt, aber eine hohes Maße an Flexibilität bei der Administrierbarkeit durch den (autorisierten) Nutzer bietet.

Diese Arbeit ist wie folgt gegliedert: in Abschnitt 2 werden Anforderungen und Ziele präzisiert. In Abschnitt 3 wird die gewählte Architektur erläutert, deren entsprechende Umsetzung in Abschnitt 4 beschrieben wird. In Abschnitt 5 wird der gewählte Ansatz bewertet und es wird von ersten Erfahrungen im operativen Alltag berichtet. Abschnitt 6 beschließt diese Arbeit mit einem Ausblick.

2 Anforderungen und Ziele

Das neue Netzsicherheitskonzept für die „Stufe 2“ soll ein Sicherheitsniveau zwischen reinem Perimeterschutz und dedizierten Firewalls an den Einrichtungsgrenzen realisieren. Angestrebt wird hier ein Sicherheitsniveau, das für die meisten Einrichtungen der Universität ausreichend ist. Durch die gemeinsame Nutzung von Netzwerkkomponenten für mehrere Einrichtungen sollen hierbei die Kosten gesenkt werden, gleichzeitig aber eine Absicherung an der Einrichtungsgrenze erreicht werden.

Der Bereichsbetreuer soll dabei seine Netzsicherheitspolicy selber definieren können, ohne den zentralen Netzbetreiber damit beauftragen zu müssen. Benötigt wird deshalb ein hierarchisches Managementsystem, das die Delegation einzelner Bereiche an unterschiedliche Betreuer ermöglicht. Die Definition der Policy sollte dabei in den meisten Fällen über ein vereinfachtes Frontend möglich sein, das die Komplexität bei Standardaufgaben verbirgt. Für Sonderfälle muss allerdings die volle Funktionalität über ein erweitertes Frontend verfügbar sein. Einschränkungen wie sie bei „Stufe 1“ vorhanden sind (ein Dienst kann nur generell frei geschaltet werden), müssen beseitigt werden.

Für jeden Bereich muss ein VPN-Zugang möglich sein, bei dem der Bereichsbetreuer die erlaubten Benutzer definieren kann.

Aus Sicht des Netzbetreibers muss die Definition zentraler Policies für alle Bereiche einfach möglich sein. Zentrale Policies dürfen dabei von Bereichsbetreuern nicht außer Kraft gesetzt werden. Durch vereinfachtes Management zentraler Policies und Delegation der Policydefinition an die Bereichsbetreuer wird eine Senkung des Administrationsaufwands angestrebt. Um den Migrationsaufwand für die einzelnen Bereiche zu minimieren muss die Nutzung der „Stufe 2“ soweit möglich ohne Wechsel der IP-Adressen erfolgen können.

3 Architektur

Das neue Netzwerksicherheitskonzept der Universität Karlsruhe basiert auf der Trennung zwischen User-Interface, Datenhaltung und der technischen Realisierung im Netzwerk (siehe Abbildung 1).

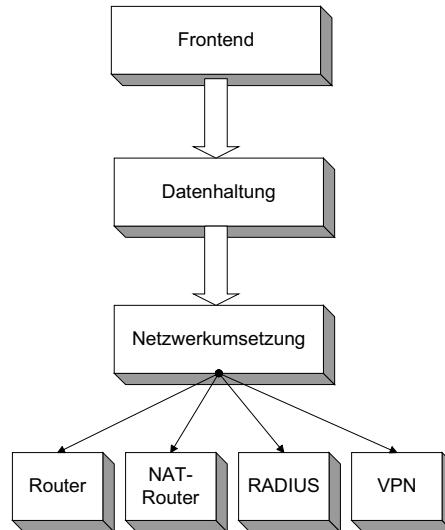


Abbildung 1 Schichtenmodell

Die strikte Trennung erlaubt durch definierte Schnittstellen Änderungen an einzelnen Teilsystemen durchzuführen, ohne dass die anderen Bereiche betroffen sind. Dies erfordert eine exakte Definition der Schnittstellen zwischen den einzelnen Schichten. Die Schnittstellen müssen dabei so flexibel sein, dass zukünftige Erweiterungen möglich sind wie etwa Erweiterungen um Quality of Service Definitionen für Voice over IP.

Dieses Schichtenmodell orientiert sich am IETF/DMTF policy framework [Ve02]. Das Frontend findet seine Entsprechung im „policy management tool“, das Datenmodell im „policy repository“. In der Netzwerkmsetzung werden aus der Policy statische Konfigurationen für die beteiligten Netzkomponenten („policy enforcement points“) erzeugt.

3.1 Benutzerfrontend

Bei dem Benutzerfrontend muss zwischen zwei verschiedenen Rollen unterschieden werden: Betreuer einzelner Universitätseinrichtungen auf der einen Seite und die Administration durch den zentralen Netzbetreiber.

Für den Betreuer ist das User-Interface deshalb auf die ihm möglichen Aufgaben beschränkt: die Definition der Netzsicherheitspolicy ist nur für seine Einrichtung möglich. Zentrale Policyvorgaben des Netzbetreibers können nicht außer Kraft gesetzt werden.

Der Administrator des zentralen Netzbetreibers benötigt dagegen Zugriff auf zusätzliche Konfigurationselemente, um die zentrale Policy zu definieren und Ausnahmen für einzelne Einrichtungen einzurichten.

Das Durchsetzen der Zugangsberechtigungen erfolgt hier nicht auf der Ebene des Benutzerinterfaces, sondern wird an der Schnittstelle zum Datenhaltungssystem kontrolliert

und durchgesetzt. Für diesen Bereich ist allein die Präsentation der Konfigurationsmöglichkeiten relevant.

3.2 Datenhaltung

Die Datenhaltung muss eine vom Benutzerfrontend und der Netzwerkimplementierung unabhängige Modellierung der Netzsicherheitspolicy ermöglichen. Zentrales Element des Datenmodells ist hier der Dienst, der von einer Universitätseinrichtung angeboten, genutzt oder verboten wird. Ein Dienst wird dabei durch Dienstparameter charakterisiert, die flexibel für zukünftige Anwendungen erweitert werden können. Durch eine hierarchische Organisation der Universitätseinrichtungen (Universität – Fakultät – Institut ...) wird die Modellierung zentral vorgegebener Policies ermöglicht, die auch für die untergeordneten Einrichtungen gelten.

3.3 Netzwerkkumsetzung

Netztechnisch wird die Kontrolle des Verkehrs am Netzübergang der Einrichtung zu dem Backbone der Universität vorgenommen. Sie wird deshalb als „Stufe 2“ bezeichnet und bringt damit auch das angestrebte Sicherheitsniveaus zwischen reiner Verkehrskontrolle zum Internet (Stufe 0 und 1) und individuellen Firewalls (Stufe 3) zum Ausdruck. Die Umsetzung erfolgt hier mit bereits vorhandener Hardware: Router und VPN Konzentratoren von Cisco und Linux basierte NAT-Router.

4 Umsetzung

4.1 Frontend

Eingesetzt wird ein webbasiertes Frontend um eine Unabhängigkeit von dem auf dem Client eingesetzten Betriebssystem zu erreichen und so jedem Betreuer die Konfiguration seiner Netzsicherheitspolicy zu ermöglichen.

Das Frontend ist dabei in 3 Bereiche geteilt: Verwaltung der Benutzer, die über VPN Zugang zu diesem Bereich erhalten, Nutzung/Verbot von Diensten und Anbieten von Diensten.

Bei der Auswahl der Dienste, die genutzt werden sollen, erhält der Betreuer eine Übersicht der aktuell getroffenen Definition und kann diese um weitere Dienste ergänzen, die vom zentralen Netzbetreiber oder anderen Universitätseinrichtungen zur Verfügung gestellt werden. Die Nutzung bzw. das Verbot der Dienste lässt sich dabei vom Betreuer auf Teilbereiche seiner Einrichtung beschränken.

Die Dienstdefinition ermöglicht es dem Betreuer, eigene Dienste anzubieten und fehlende Dienste (z.B. von externen Einrichtungen) zu modellieren. Für die Dienstbeschreibung stehen hier die üblichen TCP/IP Parameter zur Verfügung. Darüber hinaus ist eine

Auswahl möglich, für welche Einrichtungen die Nutzung des Dienstes erlaubt bzw. verboten ist.

Der Administrator des zentralen Netzbetreibers hat bei der Dienstbeschreibung die Option, diesen als administrativ zu kennzeichnen. Diese verhindert, dass normale Betreuer Änderungen an der Nutzung/Verbot vornehmen können.

4.2 Datenmodell

Zentrales Element des Datenmodells ist der Dienst (siehe Abbildung 2). Dieser wird von einer Einrichtung betrieben, definiert und anderen Einrichtungen zur Verfügung gestellt. Da sich nicht alle benötigten Dienstparameter im Vorfeld eindeutig festlegen lassen (TCP-basierte Dienste, IP-Protokoll basierte Dienste, Kombinationen, QoS-Parameter, IPv6 Erweiterungen), erfolgt die Modellierung der Dienstparameter dynamisch. Ein Dienstparameter wird über einen Dienstparametertyp definiert, der die benötigten Dienstparametertypschlüssel vorgibt. Dies ermöglicht eine problemlose Erweiterung der Dienstparametertypen, ohne eine Änderung des Datenmodells erforderlich zu machen. Jeder Dienst gehört zu einer Dienstkategorie (administrativ- oder benutzerdefiniert).

Ein Dienst wird durch genau eine Einrichtung definiert. Die Einrichtungen sind hierbei hierarchisch geordnet und durch die Organisationshierarchie der Universität bzw. netztechnische Strukturen fest vorgegeben. Darüber hinaus hat ein Betreuer die Möglichkeit Einrichtungen zu definieren, um auch externe Bereiche oder Teilbereich modellieren zu können. Den Einrichtungen sind dabei Subnetze, Benutzer und Gruppen zugeordnet.

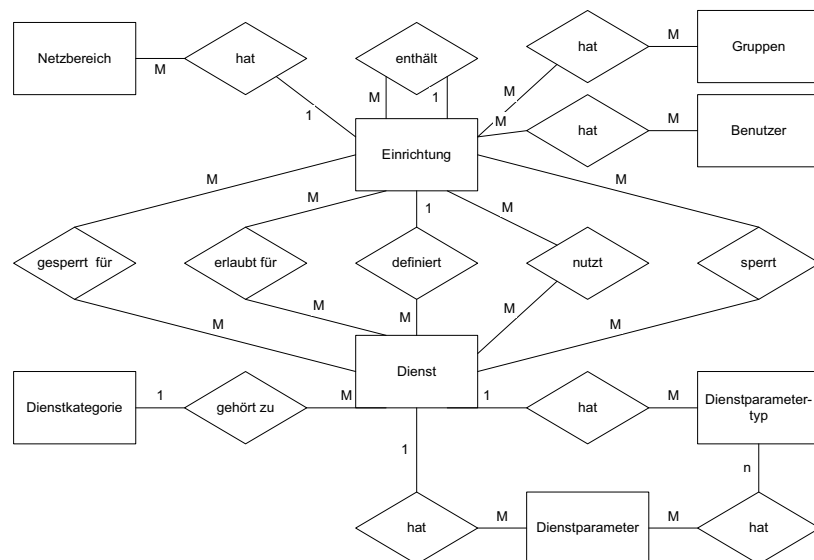


Abbildung 2 ER-Modell in Chen Notation

Die definierende Einrichtung kann dabei den Dienst für andere Einrichtungen erlauben oder verbieten. Analog kann eine Einrichtung angebotene Dienste nutzen, solange die Nutzung vom Dienstbetreiber erlaubt wurde. Die gezielte Sperre eines Dienstes ist dabei auch möglich. Über Sortierattribute kann darüber eine eindeutige Ordnung pro Einrichtung definiert werden.

Über die Einrichtung erfolgt hier die Kopplung zum schon bestehenden Teil des Datenbanksystems. Damit ist eine nahtlose Integration in bestehende Managementsysteme wie DNS-Verwaltung möglich. Darüber hinaus kann die bestehende Benutzer- und Rechteverwaltung genutzt werden, um Zugriffsrechte für einzelne Einrichtungen oder zu Administrationsfunktionen zu gewähren. Das Datenmodell lässt sich deshalb auch nicht durch eine einfache Modellierung der Schnittstellenbeschreibung ersetzen, da diese Informationen dort nicht vorhanden sind.

4.3 Schnittstellenbeschreibung Datenhaltung-Netzwerkumsetzung

Die Schnittstelle zwischen Datenhaltung und Netzwerkumsetzung ist durch ein mit RELAX NG [CM01] spezifiziertes XML Format definiert.

Kernelement der Schnittstelle ist die Policydefinition. Sie setzt sich aus zwei Basisblöcken zusammen: der Definition des Gültigkeitsbereichs und der diesem Bereich zugeordneten Regeln (siehe Abbildung 3).

```

<policydef>
<policy>
  <policyname>uni</policyname>
  <subnet><net>129.13.0.0/16</net><subnetname>uni/1</subnetname></subnet>
  <rule type="acl" action="deny" direction="out" class="200" seq="1001" src="localnets" dst="any" proto="ospf"/>
  <rule type="acl" action="deny" direction="out" class="200" seq="1003" src="localnets" dst="any" proto="udp" dstport="snmp"/>
</policy>
  <policyname>rz-netze-s1</policyname>
  <subnet><net>172.21.100.0/25</net><subnetname>rz-netze-s1/1</subnetname></subnet>
  <group>
    <groupid><groupname>rz-netze-s1</groupname><subnet>172.21.133.16/28</subnet></groupid>
    <userid><user>rz123</user><ip>172.21.133.17</ip></userid>
    <userid><user>rz84adm</user><ip>172.21.133.18</ip></userid>
  </group>
  <rule type="acl" action="permit" direction="out" class="100" seq="1000" src="localnets" dst="any" proto="udp" dstport="snmp"/>
  <rule type="acl" action="permit" direction="out" class="500" seq="1000" src="localnets" dst="uni" proto="any"/>
  <rule type="acl" action="permit" direction="out" class="500" seq="1001" src="localnets" dst="any" proto="any"/>
  <rule type="napt" action="permit" direction="out" class="900" seq="1000" src="localnets" dst="any" proto="any"/>
</policy>
</policydef>

```

Abbildung 3 Ausschnitt Policydatei

Der Gültigkeitsbereich erstreckt sich hier über die diesem Bereich zugeordneten Subnetze (<subnet>) und diesem Bereich zugeordnete Benutzer und Gruppen (<group>). Gruppen und einzelnen Benutzern können hierbei noch IP-Adressbereiche zugeordnet werden (<net> bzw. <ip>).

Für die zugeordneten Regeln sind zurzeit drei verschiedene Typen definiert: *ACL*, *NAT* und *NAPT*. Gemeinsam sind allen Regeltypen die Attribute *action*, *direction*, *class*, *seq*, *src* und *dst*. Über *class* und *seq* wird dabei die korrekte Reihenfolge garantiert: *class* über Policy-Bereiche hinweg und *seq* innerhalb der aktuellen Policy. *src* und *dst* definieren Quelle und Ziel. Benutzbar sind hier sowohl IP-Adressbereiche als auch Referenzen auf andere Policybereich. Spezielle Bezeichner sind hier *localnets* (der aktuelle Gültigkeitsbereich) und *any*.

Die weiteren Attribute sind abhängig vom Regeltyp (*<type>*) und dem eingesetzten Protokoll (*<proto>*). Protokoll ist dabei nicht auf IP-Protokolle beschränkt, sondern kann auch Applikationsprotokolle wie SMTP referenzieren. Je nach gewählter technischer Umsetzung können dabei entweder Applikationsgateways oder IP-Filter zum Einsatz kommen.

Ein Policy-Element kann dabei weitere Policy-Elemente enthalten. Die Regeln der Parent-Policy vererben sich dabei auf alle enthalten Policy-Elemente.

4.4 Netzwerkimsetzung

Realisierung mit NAT an Bereichsgrenze

Im ersten Schritt erfolgte die netztechnische Umsetzung analog zur „Stufe 1“, d.h. die NAT-Router wurden an die Bereichsgrenzen angebunden und es erfolgte sowohl ein IP-Adressumsetzung zur Universität als auch ins Internet. Es stellte sich allerdings heraus, dass mit dieser Umsetzung nicht alle Anforderungen erfüllt werden konnten. Problematisch waren hier vor allem Protokolle, die nicht transparent über NAT oder NAPT umsetzbar sind wie Active Directory. Diese Probleme ließen sich allerdings über direktes Routing dieser Verbindungen zumindest innerhalb der Universität lösen – das dadurch entstehende DNS-Problem war allerdings nicht lösbar. Systeme, die sowohl Dienste über direktes Routing als auch über NAT anboten, waren dadurch über zwei IP-Adressen aus der Universität erreichbar. Damit war nicht eindeutig entscheidbar welche IP-Adresse bei der Namensauflösung zurückgeliefert werden musste.

Aktuelle Realisierung mit Filtern an Bereichsgrenze

Das Netzwerkdesign wurde deshalb angepasst und NAT/NAPT wird nur noch bei Bedarf zum Internet hin eingesetzt (siehe Abbildung 4).

Um das Design möglichst einfach zu gestalten, erfolgt die Durchsetzung der Filterregeln allein auf dem Zugangsinterface des Bereiches. Die NAT-Router treffen keinerlei Filterentscheidung, sondern leiten alles an die interne IP-Adresse weiter. Dies erzeugt unnötigen Verkehr im Backbone, da Pakete erst am Zugangsinterface verworfen werden, erleichtert aber die Fehlerdiagnose.

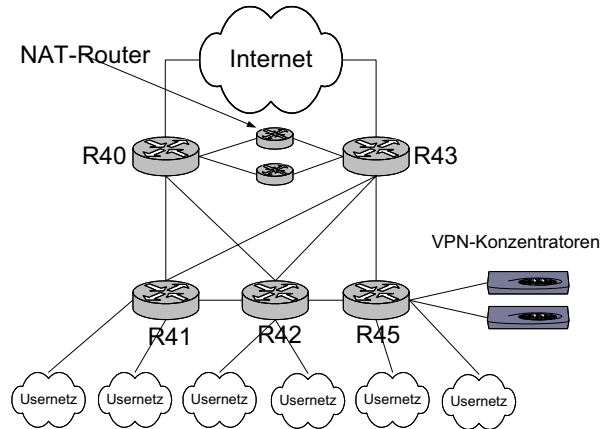


Abbildung 4 Netzdesign

Da die eingesetzten Cisco-Router keine Statefull-Packet-Inspection (SPI) beherrschen (auch keine Konkurrenzprodukte, dieses Feature scheint den Firewallprodukten vorbehalten zu sein), mussten die bestehenden Möglichkeiten dazu genutzt werden, um SPI möglichst nahe zu kommen. Cisco IOS bietet hier reflexive ACLs, die bei einem erlaubten Paket dynamisch ein ACL-Statement erzeugen, das den Rückweg erlaubt. Das Entfernen dieses ACL-Statements erfolgt allerdings rein zeitgesteuert, auch bei verbindungsorientierten Protokollen. Diese Timer werden dabei durch jedes neue Paket zurückgesetzt.

Die Anzahl der reflexiven ACL-Statements ist allerdings begrenzt (96k bei den an der Universität Karlsruhe eingesetzten Catalyst 6500 mit Supervisor Engine 720), was gerade durch das rein zeitgesteuerte Entfernen dieser Statements möglicherweise Probleme bereiten kann (das Öffnen einer Webseite kann unter Umständen schon über 30 TCP-Verbindungen aufbauen). Deshalb wird der Mechanismus der reflexiven ACLs nur für Nicht-TCP-Verbindungen eingesetzt. Für TCP-Verbindungen wird das established Flag verwendet. Für Regeln, die den Verbindungsaufbau von beiden Seiten aus zulassen, wird der Mechanismus überhaupt nicht benötigt.

Beim Einsatz privater IP-Adressen werden für die zentralen Linux-basierten NAT-Router entsprechende IPTables Befehle erzeugt, die eine Umsetzung der IP-Adresse entweder per NAT oder NAT zum Internet hin vornehmen.

Der VPN Zugang wird über je zwei VPN Konzentratoren in einer redundanten Load-Balancing Konfiguration realisiert, die von mehreren Bereichen - unabhängig vom Router über den der Anschluss erfolgt - genutzt werden können. Realisiert wird dies über das Erstellen einer VPN Gruppe, die einem Bereich zugeordnet ist und über einen festen IP Adressbereich verfügt. Über ACLs auf den Routern werden dazu für diese IP Adressbereiche die gleichen Regeln durchgesetzt und die Kommunikation zum eigentlichen Bereich erlaubt. Die Zugangsberechtigung einzelner Benutzer zu einer VPN Gruppe wird dabei von den zentralen RADIUS Servern geprüft.

Zur automatischen Umsetzung der Policies werden zusätzlich zur XML Datei (*policy.xml*) noch Informationen über die aktuelle Netztopologie benötigt (siehe Abbildung 4), damit für die einzelnen Bereiche der richtige Router und das VPN Konzentrator Paar konfiguriert werden kann.

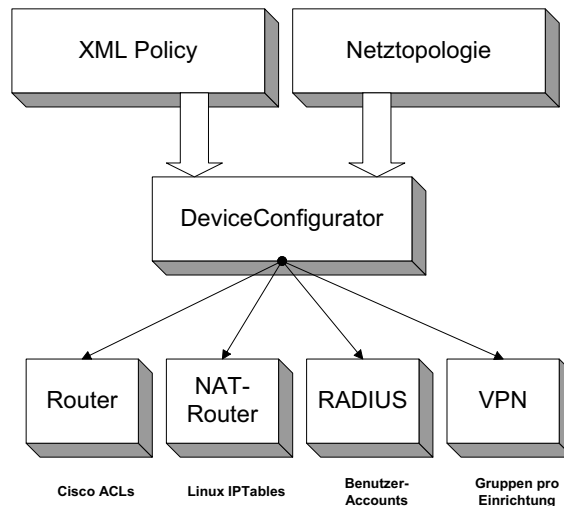


Abbildung 5 Konfigurationsablauf

Die Übertragung der eigentlichen Konfiguration erfolgt dabei über gerätespezifische Konfigurationsmechanismen (telnet/tftp, ssh/scp), da keine bei allen eingesetzten Geräte gemeinsame Konfigurationsschnittstelle existiert. Angestrebt wird hier die Konfiguration der Geräte über eine einheitliche Schnittstelle, etwa über NETCONF [En06]. Dafür müssen aber die eingesetzten Geräte diese Option unterstützen, um den Umstellungsaufwand zu rechtfertigen.

5 Erfahrungen und Bewertung

Die Umsetzung hat gezeigt, dass sich durch policy-basiertes Management das Netzsicherheitsniveau deutlich steigern lässt: die Absicherung der einzelnen Bereiche erfolgt direkt an der Bereichsgrenze und nicht mehr am Übergang zum Internet. Die netztechnische Umsetzung erreicht dabei allerdings nicht das Sicherheitsniveau einer dedizierten und zertifizierten Firewall. Die Anforderungen der meisten Bereiche können damit dennoch erfüllt werden.

Für den Betreuer steht hierbei der Self-Service im Vordergrund: er kann über ein Frontend die Netzsicherheitspolicy für seinen Bereich selbst definieren und ohne wesentliche Zeitverzögerung umsetzen.

Die Administratoren des zentralen Netzbetreibers haben mit der „Stufe 2“ ein Werkzeug zur Verfügung, mit dem einfach zentrale Policies an einer Stelle definiert und durchge-

setzt werden können. Dazu entfällt ein Großteil des Administrationsaufwands, da die Betreuer nur noch Ausnahmeregeln von zentralen Policies beantragen müssen.

Der große Aufwand, der bislang beim Wechseln zwischen den einzelnen Sicherheitsstufen angefallen ist, wurde auch minimiert. Für den Migration in die „Stufe 2“ entfällt ein Wechsel des IP-Adressbereich – in den meisten Fällen ist eine Änderung des Bereichsflags in der Datenbank und eine Konfigurationsänderung am Router ausreichend. Der bei der Netzwerkumsetzung benötigte Wechsel von der NAT-basierten zu einer Filterbasierten Netzstruktur hat gezeigt, dass die gewählte, mehrstufige Architektur eine einfache Migration zwischen unterschiedlichen Netzdesigns erlaubt: lediglich eine Umstellung am DeviceConfigurator wurde benötigt um alle beteiligten Bereiche auf die neue Netzstruktur umzustellen.

Ein Skalierungsproblem ist zum jetzigen Zeitpunkt noch nicht aufgetreten, die Auslastung der verfügbaren reflexiven ACL Statements liegt im Mittel bei 5% (bei Nutzung durch fünf Bereiche, darunter die Universitätsbibliothek). Mit einem Catalyst 6500 werden damit bis circa 75 Bereiche bedient werden können. Pro VPN-Concentrator-3060-Paar wird aktuell mit 150 Bereichen gerechnet, die abgedeckt werden können.

6 Ausblick

Die aktuelle Umsetzung bietet den Universitätseinrichtungen eine einfache Möglichkeit, ein gegenüber „Stufe 1“ deutlich erhöhtes Sicherheitsniveau zu erreichen. Dabei muss im Gegensatz zu einer dedizierten Firewall in „Stufe 3“ nicht auf die eigenständige Konfiguration verzichtet werden.

In der ersten Designphase wurde die „Stufe 2“ als zusätzliches Element eines mehrstufigen Netzsicherheitskonzepts entwickelt. Im Lauf der Entwicklung hat sich aber immer stärker gezeigt, dass durch die Abstraktion zwischen Policy-Definition und Netzwerkumsetzung dieses Modell für alle Bereiche der Universität verwendet werden kann. „Stufe 0“ und „Stufe 1“ können dabei sofort durch „Stufe 2“ mit einer entsprechenden offenen Konfiguration ersetzt werden. Bei erhöhten Sicherheitsanforderungen ist durch eine Erweiterung des DeviceConfigurators auch eine automatische bzw. halb-automatische Konfiguration dedizierter Firewallssysteme möglich. Es wird deshalb angestrebt, dieses System für alle Bereiche der Universität einzusetzen und den Benutzern damit ein Werkzeug zur konsistenten Definition ihrer Netzsicherheitspolicy an die Hand zu geben.

Literaturverzeichnis

- [CM01] Clark, J., Makoto M. et al.: RELAX NG Specification, <http://relaxng.org/spec-20011203.html>
- [En06] Enns, R. et al.: NETCONF Configuration Protocol, Internet Draft, Work in Progress, <http://www.ietf.org/internet-drafts/draft-ietf-netconf-prot-12.txt>
- [Ve02] Verma, D.: Simplifying Network Administration using Policy based Management, IEEE Network Magazine, March 2002